Linear Algebra 1

Lecture #7

Permutations and the symmetric group. Fields

Irena Penev

November 20, 2023

This lecture consists of two parts:

This lecture consists of two parts:

1. Permutations and the symmetric group

This lecture consists of two parts:

1. Permutations and the symmetric group
2. Fields

1. Permutations and the symmetric group

1. Permutations and the symmetric group

Definition

A *permutation* of a set X is any bijection from X to itself. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$.

1. Permutations and the symmetric group

Definition

A *permutation* of a set X is any bijection from X to itself. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$.

- For any set X, $(\mathrm{Sym}(X), \circ)$ is a group, called the *symmetric group on* X (here, $\circ$ is the composition of functions).

1. Permutations and the symmetric group

Definition

A *permutation* of a set X is any bijection from X to itself. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$.

- For any set X, $(\mathrm{Sym}(X), \circ)$ is a group, called the *symmetric group on* X (here, $\circ$ is the composition of functions).
  - Indeed, the composition of two permutations of X is a permutation of X, and so $\circ$ is a binary operation on $\mathrm{Sym}(X)$.

Definition

A *permutation* of a set X is any bijection from X to itself. The set of all permutations of X is denoted by $\text{Sym}(X)$.

- For any set X, $(\text{Sym}(X), \circ)$ is a group, called the *symmetric group on* X (here, $\circ$ is the composition of functions).
  - Indeed, the composition of two permutations of X is a permutation of X, and so $\circ$ is a binary operation on $\text{Sym}(X)$.
  - Moreover, it is clear that $\circ$ is associative; indeed, for any $\pi, \sigma, \tau \in \text{Sym}(X)$, we have that $\pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$, because for all $x \in X$, we have the following:

$$\begin{array}{rcl} \big(\pi \circ (\sigma \circ \tau)\big)(x) & = & \pi\big((\sigma \circ \tau)(x)\big) \\ & = & \pi\big(\sigma(\tau(x))\big) \\ & = & (\pi \circ \sigma)\big(\tau(x)\big) \\ & = & \big((\pi \circ \sigma) \circ \tau\big)(x). \end{array}$$

1. Permutations and the symmetric group

Definition

A *permutation* of a set X is any bijection from X to itself. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$.

- For any set X, $(\mathrm{Sym}(X), \circ)$ is a group, called the *symmetric group on* X (here, $\circ$ is the composition of functions).
  - Indeed, the composition of two permutations of X is a permutation of X, and so $\circ$ is a binary operation on $\mathrm{Sym}(X)$.
  - Moreover, it is clear that $\circ$ is associative; indeed, for any $\pi, \sigma, \tau \in \mathrm{Sym}(X)$, we have that $\pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$, because for all $x \in X$, we have the following:

$$\begin{array}{rcl} \big(\pi \circ (\sigma \circ \tau)\big)(x) & = & \pi\big((\sigma \circ \tau)(x)\big) \\ & = & \pi\big(\sigma(\tau(x))\big) \\ & = & (\pi \circ \sigma)\big(\tau(x)\big) \\ & = & \big((\pi \circ \sigma) \circ \tau\big)(x). \end{array}$$

  - The identity element of this group is the identity function Id_X.

1. Permutations and the symmetric group

Definition

A *permutation* of a set X is any bijection from X to itself. The set of all permutations of X is denoted by $\mathrm{Sym}(X)$.

- For any set X, $(\mathrm{Sym}(X), \circ)$ is a group, called the *symmetric group on* X (here, $\circ$ is the composition of functions).
  - Indeed, the composition of two permutations of X is a permutation of X, and so $\circ$ is a binary operation on $\mathrm{Sym}(X)$.
  - Moreover, it is clear that $\circ$ is associative; indeed, for any $\pi, \sigma, \tau \in \mathrm{Sym}(X)$, we have that $\pi \circ (\sigma \circ \tau) = (\pi \circ \sigma) \circ \tau$, because for all $x \in X$, we have the following:

$$\begin{array}{rcl} \big(\pi \circ (\sigma \circ \tau)\big)(x) & = & \pi\big((\sigma \circ \tau)(x)\big) \\ & = & \pi\big(\sigma(\tau(x))\big) \\ & = & (\pi \circ \sigma)\big(\tau(x)\big) \\ & = & \big((\pi \circ \sigma) \circ \tau\big)(x). \end{array}$$

  - The identity element of this group is the identity function Id_X.
  - The inverse element of any permutation $\pi \in \mathrm{Sym}(X)$ is the inverse permutation π^{-1}.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.
- Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.
- Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$.
- But now

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.
- Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$.
- But now
  - $(\sigma \circ \tau)(a) = \sigma\big(\tau(a)\big) = \sigma(c) = c$;

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.
- Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$.
- But now
  - $(\sigma \circ \tau)(a) = \sigma\big(\tau(a)\big) = \sigma(c) = c$;
  - $(\tau \circ \sigma)(a) = \tau\big(\sigma(a)\big) = \tau(b) = b$.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.
- Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$.
- But now
  - $(\sigma \circ \tau)(a) = \sigma\big(\tau(a)\big) = \sigma(c) = c$;
  - $(\tau \circ \sigma)(a) = \tau\big(\sigma(a)\big) = \tau(b) = b$.
- Since $b \neq c$, we have that $(\sigma \circ \tau)(a) \neq (\tau \circ \sigma)(a)$.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.
- Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$.
- But now
  - $(\sigma \circ \tau)(a) = \sigma\big(\tau(a)\big) = \sigma(c) = c$;
  - $(\tau \circ \sigma)(a) = \tau\big(\sigma(a)\big) = \tau(b) = b$.
- Since $b \neq c$, we have that $(\sigma \circ \tau)(a) \neq (\tau \circ \sigma)(a)$.
- So, $\sigma \circ \tau \neq \tau \circ \sigma$.

- If a set X has at most two elements, then it is easy to see that the group $\mathrm{Sym}(X)$ is abelian.
- However, if X has at least three elements, then X is **not** abelian, as we now show.
- Suppose that $|X| \geq 3$, and let a, b, c be pairwise distinct elements of X.
- Let $\sigma, \tau : X \to X$ be defined as follows:
  - $\sigma(a) = b$, $\sigma(b) = a$, and $\sigma(x) = x$ for all $x \in X \setminus \{a, b\}$;
  - $\tau(a) = c$, $\tau(c) = a$, and $\tau(x) = x$ for all $x \in X \setminus \{a, c\}$.
- Clearly, $\sigma, \tau \in \mathrm{Sym}(X)$.
- But now
  - $(\sigma \circ \tau)(a) = \sigma\big(\tau(a)\big) = \sigma(c) = c$;
  - $(\tau \circ \sigma)(a) = \tau\big(\sigma(a)\big) = \tau(b) = b$.
- Since $b \neq c$, we have that $(\sigma \circ \tau)(a) \neq (\tau \circ \sigma)(a)$.
- So, $\sigma \circ \tau \neq \tau \circ \sigma$.
- Thus, $\mathrm{Sym}(X)$ is not abelian.

- We particularly often consider $\mathrm{Sym}(X)$ for the case when $X = \{1, \ldots, n\}$ for some positive integer n.

- We particularly often consider $\mathrm{Sym}(X)$ for the case when $X = \{1, \ldots, n\}$ for some positive integer n.
- The set $\mathrm{Sym}(\{1, \ldots, n\})$ is also denoted by $\mathrm{Sym}(n)$, Sym_n, or S_n.

- We particularly often consider $\mathrm{Sym}(X)$ for the case when $X = \{1, \ldots, n\}$ for some positive integer n.
- The set $\mathrm{Sym}(\{1, \ldots, n\})$ is also denoted by $\mathrm{Sym}(n)$, Sym_n, or S_n.
- In this course, we will consistently use the notation S_n.

- We particularly often consider $\mathrm{Sym}(X)$ for the case when $X = \{1, \ldots, n\}$ for some positive integer n.
- The set $\mathrm{Sym}(\{1, \ldots, n\})$ is also denoted by $\mathrm{Sym}(n)$, Sym_n, or S_n.
- In this course, we will consistently use the notation S_n.
- The group $(S_n, \circ)$ is called the *symmetric group of degree n*.

- We particularly often consider $\mathrm{Sym}(X)$ for the case when $X = \{1, \ldots, n\}$ for some positive integer n.
- The set $\mathrm{Sym}(\{1, \ldots, n\})$ is also denoted by $\mathrm{Sym}(n)$, Sym_n, or S_n.
- In this course, we will consistently use the notation S_n.
- The group $(S_n, \circ)$ is called the *symmetric group of degree n*.
- Note that $|S_n| = n!$.

- A permutation $\pi \in S_n$ can be represented in the following way:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

- A permutation $\pi \in S_n$ can be represented in the following way:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

- So, in the top row, we have numbers $1, 2, \dots, n$, and in the bottom row, we have those same numbers in some order (determined by the permutation π).

- A permutation $\pi \in S_n$ can be represented in the following way:

$$\pi \quad = \quad \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}.$$

- So, in the top row, we have numbers $1, 2, \dots, n$, and in the bottom row, we have those same numbers in some order (determined by the permutation π).
- For example, the permutation $\pi \in S_4$ given by
  - $\pi(1) = 3$,
  - $\pi(2) = 2$,
  - $\pi(3) = 4$,
  - $\pi(4) = 1$

  can be represented as follows:

$$\pi \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

- We can also represent permutations in S_n in terms of cycles.

- We can also represent permutations in S_n in terms of cycles.
- Let us consider an example.

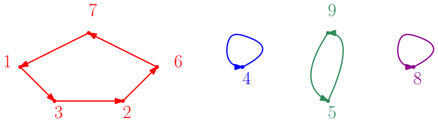
- We can also represent permutations in S_n in terms of cycles.
- Let us consider an example.
- Suppose we are given the following permutation in S_9:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 2 & 4 & 9 & 7 & 1 & 8 & 5 \end{pmatrix}.$$

- We can also represent permutations in S_n in terms of cycles.
- Let us consider an example.
- Suppose we are given the following permutation in S_9:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 2 & 4 & 9 & 7 & 1 & 8 & 5 \end{pmatrix}.$$

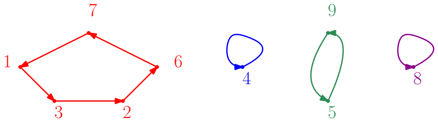
- We can represent this permutation geometrically, as shown below.



- We can also represent permutations in S_n in terms of cycles.
- Let us consider an example.
- Suppose we are given the following permutation in S_9:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 2 & 4 & 9 & 7 & 1 & 8 & 5 \end{pmatrix}.$$

- We can represent this permutation geometrically, as shown below.



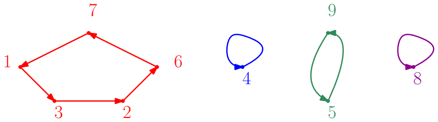
- We can "encode" the picture that we obtained as a "product of disjoint cycles":

$$\pi = (13267)(4)(59)(8).$$

- We can also represent permutations in S_n in terms of cycles.
- Let us consider an example.
- Suppose we are given the following permutation in S_9:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 6 & 2 & 4 & 9 & 7 & 1 & 8 & 5 \end{pmatrix}.$$

- We can represent this permutation geometrically, as shown below.

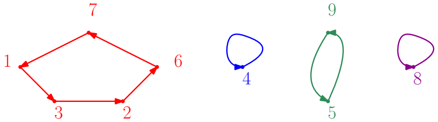


- We can "encode" the picture that we obtained as a "product of disjoint cycles":

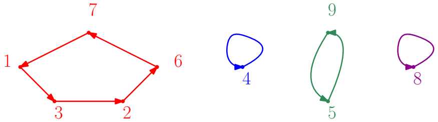
$$\pi = (13267)(4)(59)(8).$$

- The above is also referred to as a "disjoint cycle decomposition" of the permutation π.

- Reminder: $\pi = (13267)(4)(59)(8)$.

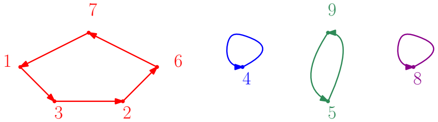


- Reminder: $\pi = (13267)(4)(59)(8)$.



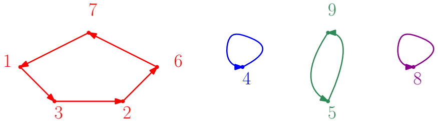
- The disjoint cycle decomposition of a permutation is unique up to cyclic permutation of the elements within each cycle, and up to a reordering of the cycles.

- Reminder: $\pi = (13267)(4)(59)(8)$.



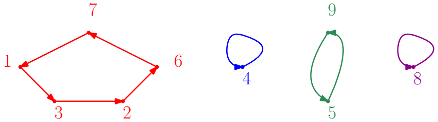
- The disjoint cycle decomposition of a permutation is unique up to cyclic permutation of the elements within each cycle, and up to a reordering of the cycles.
- For example, the permutation π above can also be expressed as follows: $\pi = (95)(26713)(8)(4)$.

- Reminder: $\pi = (13267)(4)(59)(8)$.



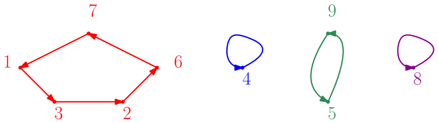
- The disjoint cycle decomposition of a permutation is unique up to cyclic permutation of the elements within each cycle, and up to a reordering of the cycles.
- For example, the permutation π above can also be expressed as follows: $\pi = (95)(26713)(8)(4)$.
- However, the first disjoint cycle decomposition is canonical/standard because it satisfies the following two properties:
  - within each cycle, the smallest number appears first;
  - the first elements of the cycles from the disjoint cycle decomposition form an increasing sequence.

- Reminder: $\pi = (13267)(4)(59)(8)$.

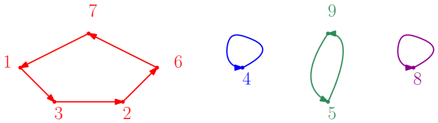


- The disjoint cycle decomposition of a permutation is unique up to cyclic permutation of the elements within each cycle, and up to a reordering of the cycles.
- For example, the permutation π above can also be expressed as follows: $\pi = (95)(26713)(8)(4)$.
- However, the first disjoint cycle decomposition is canonical/standard because it satisfies the following two properties:
  - within each cycle, the smallest number appears first;
  - the first elements of the cycles from the disjoint cycle decomposition form an increasing sequence.
- Usually, the canonical representation is preferred, but occasionally, it may be more practical to use a non-canonical one.

- Reminder: $\pi = (13267)(4)(59)(8)$.

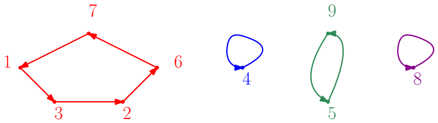


- Reminder: $\pi = (13267)(4)(59)(8)$.



- When the n from S_n is clear from context, one-element cycles may be omitted.

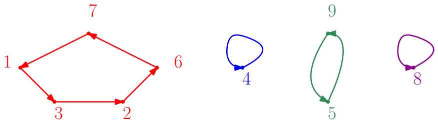
- Reminder: $\pi = (13267)(4)(59)(8)$.



- When the n from S_n is clear from context, one-element cycles may be omitted.
- So, if we know that we are working in S_9, then we may omit the one-element cycles (4) and (8) from the representation above, and write simply

$$\pi = (13267)(59).$$

- Reminder: $\pi = (13267)(4)(59)(8)$.

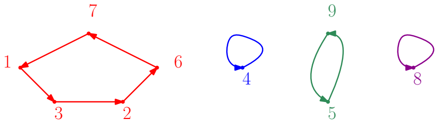


- When the n from S_n is clear from context, one-element cycles may be omitted.
- So, if we know that we are working in S_9, then we may omit the one-element cycles (4) and (8) from the representation above, and write simply

$$\pi = (13267)(59).$$

- In this case, the cycles (4) and (8) are understood from context.

- Reminder: $\pi = (13267)(4)(59)(8)$.



- When the n from S_n is clear from context, one-element cycles may be omitted.
- So, if we know that we are working in S_9, then we may omit the one-element cycles (4) and (8) from the representation above, and write simply

$$\pi = (13267)(59).$$

- In this case, the cycles (4) and (8) are understood from context.
- However, we can only do this when n has been specified beforehand!
  - Otherwise, cycles of length one must be included.

- **Notation:** When there is danger of confusion, we put commas between elements within cycles.

- **Notation:** When there is danger of confusion, we put commas between elements within cycles.
  - For instance, if we are working in S_{12}, then (123) is ambiguous.

- **Notation:** When there is danger of confusion, we put commas between elements within cycles.
  - For instance, if we are working in S_{12}, then (123) is ambiguous.
  - To avoid ambiguity, we write $(1, 2, 3)$ or $(12, 3)$, as appropriate.

- **Notation:** When there is danger of confusion, we put commas between elements within cycles.
  - For instance, if we are working in S_{12}, then (123) is ambiguous.
  - To avoid ambiguity, we write $(1, 2, 3)$ or $(12, 3)$, as appropriate.
  - However, if we are working in S_n, where n is a single-digit number, then there is no danger of confusion, and so we normally omit commas.

Example 2.3.1

Find the disjoint cycle decompositions of the following permutations.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

Solution.

Example 2.3.1

Find the disjoint cycle decompositions of the following permutations.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

Solution. We have:

(a) $\pi_1 = (125)(34)$;

Example 2.3.1

Find the disjoint cycle decompositions of the following permutations.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

Solution. We have:

(a) $\pi_1 = (125)(34)$;

(b) $\pi_2 = (134)(2)(56)$;

Example 2.3.1

Find the disjoint cycle decompositions of the following permutations.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

Solution. We have:

(a) $\pi_1 = (125)(34)$;

(b) $\pi_2 = (134)(2)(56)$;

- we could also have written $\pi \in S_6$, $\pi = (134)(56)$;

Example 2.3.1

Find the disjoint cycle decompositions of the following permutations.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix}$

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

Solution. We have:

(a) $\pi_1 = (125)(34)$;

(b) $\pi_2 = (134)(2)(56)$;
  - we could also have written $\pi \in S_6$, $\pi = (134)(56)$;

(c) $\pi_3 = (12543)$.

□

- It is also easy to go the other way around: from the disjoint cycle decomposition to the table representation.

- It is also easy to go the other way around: from the disjoint cycle decomposition to the table representation.
- For instance:
  - $(143)(26)(5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$;

- It is also easy to go the other way around: from the disjoint cycle decomposition to the table representation.
- For instance:
  - $(143)(26)(5) = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{array} \right)$;
  - $(154362) = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 4 & 2 \end{array} \right)$.

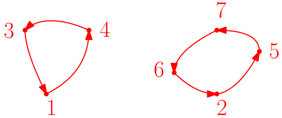
- By composing two permutations, we get another permutation.

- By composing two permutations, we get another permutation.
- For example:
  - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix};$

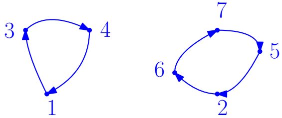
- By composing two permutations, we get another permutation.
- For example:
  - $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix};$
  - $(1)(23)(45) \circ (124)(35) = (134)(25).$

- The inverse of a permutation π in S_n can be obtained by starting with a disjoint cycle decomposition of π, and then reversing the order of elements in all cycles, i.e. turning each cycle of the form $(a_1 a_2 \ldots a_k)$ into $(a_k \ldots a_2 a_1)$.

- For example, in S_7:
  - if $\pi_1 = (143)(2576)$, then $\pi_1^{-1} = (341)(6752) = (134)(2675)$;

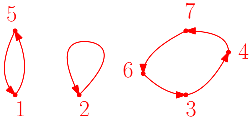


π_1

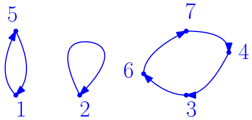


π_1^{-1}

  - if $\pi_2 = (15)(2)(3476)$, then
    $\pi_2^{-1} = (51)(2)(6743) = (15)(2)(3674)$.



π_2



π_2^{-1}

- **Notation:** The identity permutation in S_n is often denoted simply by 1.

- **Notation:** The identity permutation in S_n is often denoted simply by 1.
- So, in this context, we have that

$$1 \;=\; (1)(2)\ldots(n).$$

- **Notation:** The identity permutation in S_n is often denoted simply by 1.
- So, in this context, we have that

$$1 \;=\; (1)(2)\ldots(n).$$

- If we wish to emphasize n (or if we need to avoid confusion with other kinds of 1 that may appear in our proof/computation), then we can denote the identity permutation in S_n by 1_n.

Definition

Given a positive integer n and a permutation $\pi \in S_n$, the *sign* of π, denoted by $\mathrm{sgn}(\pi)$, is given by $\mathrm{sgn}(\pi) = (-1)^{n-k}$, where k is the number of cycles in the disjoint cycle decomposition of π **including the one-element cycles**.

Definition

Given a positive integer n and a permutation $\pi \in S_n$, the *sign* of π, denoted by $\mathrm{sgn}(\pi)$, is given by $\mathrm{sgn}(\pi) = (-1)^{n-k}$, where k is the number of cycles in the disjoint cycle decomposition of π **including the one-element cycles**.

- For instance:
  - for $\pi_1 = (1367)(2)(45)$ in S_7, we have

$$\mathrm{sgn}(\pi_1) = (-1)^{7-3} = 1;$$

Definition

Given a positive integer n and a permutation $\pi \in S_n$, the *sign* of π, denoted by $\operatorname{sgn}(\pi)$, is given by $\operatorname{sgn}(\pi) = (-1)^{n-k}$, where k is the number of cycles in the disjoint cycle decomposition of π **including the one-element cycles**.

- For instance:
  - for $\pi_1 = (1367)(2)(45)$ in S_7, we have
    $$\operatorname{sgn}(\pi_1) = (-1)^{7-3} = 1;$$
  - for $\pi_2 = (12)(345)(6)(7)$ in S_7, we have
    $$\operatorname{sgn}(\pi_2) = (-1)^{7-4} = -1.$$

Definition

Given a positive integer n and a permutation $\pi \in S_n$, the *sign* of π, denoted by $\text{sgn}(\pi)$, is given by $\text{sgn}(\pi) = (-1)^{n-k}$, where k is the number of cycles in the disjoint cycle decomposition of π **including the one-element cycles**.

- Equivalently, for $\pi \in S_n$, we have that $\text{sgn}(\pi) = (-1)^{n'-k'}$, where k' is the number of cycles in some disjoint cycles in some disjoint cycle decomposition of π (possibly with some one-element cycles omitted), and n' is the number of elements in those k' cycles.

Definition

Given a positive integer n and a permutation $\pi \in S_n$, the *sign* of π, denoted by $\mathrm{sgn}(\pi)$, is given by $\mathrm{sgn}(\pi) = (-1)^{n-k}$, where k is the number of cycles in the disjoint cycle decomposition of π **including the one-element cycles**.

- Equivalently, for $\pi \in S_n$, we have that $\mathrm{sgn}(\pi) = (-1)^{n'-k'}$, where k' is the number of cycles in some disjoint cycles in some disjoint cycle decomposition of π (possibly with some one-element cycles omitted), and n' is the number of elements in those k' cycles.
- The two definitions are equivalent because if d is the number of omitted one-element cycles in some disjoint cycle decomposition of π , then $n = n' + d$, and if we write the complete disjoint cycle decomposition of π including all one-element cycles, then we get $k = k' + d$ many cycles.

Definition

Given a positive integer n and a permutation $\pi \in S_n$, the *sign* of π, denoted by $\mathrm{sgn}(\pi)$, is given by $\mathrm{sgn}(\pi) = (-1)^{n-k}$, where k is the number of cycles in the disjoint cycle decomposition of π **including the one-element cycles**.

- Equivalently, for $\pi \in S_n$, we have that $\mathrm{sgn}(\pi) = (-1)^{n'-k'}$, where k' is the number of cycles in some disjoint cycles in some disjoint cycle decomposition of π (possibly with some one-element cycles omitted), and n' is the number of elements in those k' cycles.
- The two definitions are equivalent because if d is the number of omitted one-element cycles in some disjoint cycle decomposition of π , then $n = n' + d$, and if we write the complete disjoint cycle decomposition of π including all one-element cycles, then we get $k = k' + d$ many cycles. So, $n - k = n' - k'$, and consequently, $(-1)^{n-k} = (-1)^{n'-k'}$.

- For instance, for $\pi_3 = (123)(45)$ in S_7, we have

$$\mathrm{sgn}(\pi_3) \;\; = \;\; (-1)^{5-2} = -1.$$

- For instance, for $\pi_3 = (123)(45)$ in S_7, we have

$$\mathrm{sgn}(\pi_3) \;=\; (-1)^{5-2} = -1.$$

- Note that the one-element cycles (6) and (7) are implicitly understood for π_3, that is, $\pi_3 = (123)(45)(6)(7)$.

- For instance, for $\pi_3 = (123)(45)$ in S_7, we have

$$\mathrm{sgn}(\pi_3) \;\; = \;\; (-1)^{5-2} = -1.$$

- Note that the one-element cycles (6) and (7) are implicitly understood for π_3, that is, $\pi_3 = (123)(45)(6)(7)$.
- And indeed, we have

$$\mathrm{sgn}(\pi_3) \;\; = \;\; (-1)^{7-4} = -1,$$

as before.

- **Remark:** Note that for all positive integers n, the identity permutation in S_n has sign 1.
    - This is because the identity permutation in S_n has disjoint cycle decomposition $(1)(2)\dots(n)$, and so its sign is $(-1)^{n-n} = (-1)^0 = 1$.

- **Remark:** Note that for all positive integers n, the identity permutation in S_n has sign 1.
  - This is because the identity permutation in S_n has disjoint cycle decomposition $(1)(2)\ldots(n)$, and so its sign is $(-1)^{n-n} = (-1)^0 = 1$.

- **Terminology:** Permutations whose sign is $+1$ are called *even*, and permutations whose sign is -1 are called *odd*. Since the sign of the identity permutation is $+1$, the identity permutation is even.

Proposition 2.3.2

Let $n \geq 2$ be an integer, and let π be a permutation in S_n. Then $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$.

Proof.

Proposition 2.3.2

Let $n \geq 2$ be an integer, and let π be a permutation in S_n. Then $\mathrm{sgn}(\pi^{-1}) = \mathrm{sgn}(\pi)$.

Proof. This follows from the fact that π and π^{-1} have the same number of cycles in their disjoint cycle decompositions (when the one-element cycles are included).

- Slightly informally, a transposition is a permutation that swaps two elements and fixes all the remaining ones.

- Slightly informally, a transposition is a permutation that swaps two elements and fixes all the remaining ones.
- More formally, given an integer $n \geq 2$, a *transposition* in S_n is a permutation $\pi \in S_n$ for which there exist distinct $i, j \in \{1, \ldots, n\}$ s.t.
  - $\pi(i) = j$,
  - $\pi(j) = i$,
  - $\pi(\ell) = \ell$ for all $\ell \in \{1, \ldots, n\} \setminus \{i, j\}$.

- Slightly informally, a transposition is a permutation that swaps two elements and fixes all the remaining ones.
- More formally, given an integer $n \geq 2$, a *transposition* in S_n is a permutation $\pi \in S_n$ for which there exist distinct $i, j \in \{1, \ldots, n\}$ s.t.
    - $\pi(i) = j$,
    - $\pi(j) = i$,
    - $\pi(\ell) = \ell$ for all $\ell \in \{1, \ldots, n\} \setminus \{i, j\}$.
- Such a transposition is typically denoted by (ij), and the $n - 2$ many one-element cycles are implicitly understood.

- Slightly informally, a transposition is a permutation that swaps two elements and fixes all the remaining ones.
- More formally, given an integer $n \geq 2$, a *transposition* in S_n is a permutation $\pi \in S_n$ for which there exist distinct $i, j \in \{1, \ldots, n\}$ s.t.
  - $\pi(i) = j$,
  - $\pi(j) = i$,
  - $\pi(\ell) = \ell$ for all $\ell \in \{1, \ldots, n\} \setminus \{i, j\}$.
- Such a transposition is typically denoted by (ij), and the $n - 2$ many one-element cycles are implicitly understood.
- For instance, the following permutation in S_5 is a transposition:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = (25).$$

- Slightly informally, a transposition is a permutation that swaps two elements and fixes all the remaining ones.
- More formally, given an integer $n \geq 2$, a *transposition* in S_n is a permutation $\pi \in S_n$ for which there exist distinct $i, j \in \{1, \ldots, n\}$ s.t.
  - $\pi(i) = j$,
  - $\pi(j) = i$,
  - $\pi(\ell) = \ell$ for all $\ell \in \{1, \ldots, n\} \setminus \{i, j\}$.
- Such a transposition is typically denoted by (ij), and the $n-2$ many one-element cycles are implicitly understood.
- For instance, the following permutation in S_5 is a transposition:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} = (25).$$

- Note that this transposition could also have been written in the form $(1)(25)(3)(4)$.
  - More commonly, one-element cycles are omitted.

- **Remark:** Every transposition is its own inverse, that is, for any transposition $\tau = (ij)$ in S_n ($n \geq 2$), we have that $\tau^{-1} = \tau$.

- **Remark:** Every transposition is its own inverse, that is, for any transposition $\tau = (ij)$ in S_n ($n \geq 2$), we have that $\tau^{-1} = \tau$.
- The sign of any transposition is -1, and so transpositions are odd.

- **Remark:** Every transposition is its own inverse, that is, for any transposition $\tau = (ij)$ in S_n ($n \geq 2$), we have that $\tau^{-1} = \tau$.
- The sign of any transposition is -1, and so transpositions are odd.
    - This follows straight from the definition of the sign of a permutation.

- **Remark:** Every transposition is its own inverse, that is, for any transposition $\tau = (ij)$ in S_n $(n \geq 2)$, we have that $\tau^{-1} = \tau$.
- The sign of any transposition is -1, and so transpositions are odd.
  - This follows straight from the definition of the sign of a permutation.
  - Indeed, if τ is a transposition in S_n $(n \geq 2)$, then the disjoint cycle decomposition of τ consists of one cycle of length two and $n - 2$ many cycles of length one, and consequently, it consists of $n - 1$ cycles total (when cycles of length one are included).

- **Remark:** Every transposition is its own inverse, that is, for any transposition $\tau = (ij)$ in S_n ($n \geq 2$), we have that $\tau^{-1} = \tau$.
- The sign of any transposition is -1, and so transpositions are odd.
  - This follows straight from the definition of the sign of a permutation.
  - Indeed, if τ is a transposition in S_n ($n \geq 2$), then the disjoint cycle decomposition of τ consists of one cycle of length two and $n-2$ many cycles of length one, and consequently, it consists of $n-1$ cycles total (when cycles of length one are included).
  - So, $\mathrm{sgn}(\tau) = (-1)^{n-(n-1)} = -1$.

- As we shall see, for $n \geq 2$, any permutation can be written as a composition of transpositions.

- As we shall see, for $n \geq 2$, any permutation can be written as a composition of transpositions.
- For instance, in S_7, we have

$$(134)(2657) \quad = \quad (13) \circ (34) \circ (26) \circ (65) \circ (57).$$

- As we shall see, for $n \geq 2$, any permutation can be written as a composition of transpositions.
- For instance, in S_7, we have

$$(134)(2657) \quad = \quad (13) \circ (34) \circ (26) \circ (65) \circ (57).$$

  - The correctness of the above can easily be verified by checking that the image of each element of $\{1, \ldots, 7\}$ under the permutations $(134)(2657)$ and $(13) \circ (34) \circ (26) \circ (65) \circ (57)$ is the same.

- As we shall see, for $n \geq 2$, any permutation can be written as a composition of transpositions.
- For instance, in S_7, we have

$$(134)(2657) \quad = \quad (13) \circ (34) \circ (26) \circ (65) \circ (57).$$

  - The correctness of the above can easily be verified by checking that the image of each element of $\{1, \ldots, 7\}$ under the permutations $(134)(2657)$ and $(13) \circ (34) \circ (26) \circ (65) \circ (57)$ is the same.
- Moreover, this works in general, as the following proposition shows (next slide).

Proposition 2.3.3

Let $n \geq 2$ be an integer. Then any permutation in S_n can be written as a composition of transpositions.

Proof.

Proposition 2.3.3

Let $n \geq 2$ be an integer. Then any permutation in S_n can be written as a composition of transpositions.

Proof. The identity permutation in S_n can be written in the form $(12) \circ (12)$.

Proposition 2.3.3

Let $n \geq 2$ be an integer. Then any permutation in S_n can be written as a composition of transpositions.

Proof. The identity permutation in S_n can be written in the form $(12) \circ (12)$.

Let us now suppose that π is some permutation in S_n other than the identity.

Proposition 2.3.3

Let $n \geq 2$ be an integer. Then any permutation in S_n can be written as a composition of transpositions.

Proof. The identity permutation in S_n can be written in the form $(12) \circ (12)$.

Let us now suppose that π is some permutation in S_n other than the identity. Then π can be written as the product of one or more disjoint cycles of length at least two (one-element cycles are omitted in our expression, but are understood from context).

Proposition 2.3.3

Let $n \geq 2$ be an integer. Then any permutation in S_n can be written as a composition of transpositions.

Proof. The identity permutation in S_n can be written in the form $(12) \circ (12)$.

Let us now suppose that π is some permutation in S_n other than the identity. Then π can be written as the product of one or more disjoint cycles of length at least two (one-element cycles are omitted in our expression, but are understood from context). Let us say we have k cycles of length at least two:

$$\pi = (a_1^1 a_2^1 \ldots a_{\ell_1}^1) \ldots (a_1^k a_2^k \ldots a_{\ell_k}^k),$$

where the a_i^j's are pairwise distinct, and $\ell_1, \ldots, \ell_k \geq 2$.

Proposition 2.3.3

Let $n \geq 2$ be an integer. Then any permutation in S_n can be written as a composition of transpositions.

Proof. The identity permutation in S_n can be written in the form $(12) \circ (12)$.

Let us now suppose that π is some permutation in S_n other than the identity. Then π can be written as the product of one or more disjoint cycles of length at least two (one-element cycles are omitted in our expression, but are understood from context). Let us say we have k cycles of length at least two:

$$\pi = (a_1^1 a_2^1 \dots a_{\ell_1}^1) \dots (a_1^k a_2^k \dots a_{\ell_k}^k),$$

where the a_i^j's are pairwise distinct, and $\ell_1, \dots, \ell_k \geq 2$. But then

$$\pi = (a_1^1 a_2^1) \circ (a_2^1 a_3^1) \circ \cdots \circ (a_{\ell_1 - 1}^1 a_{\ell_1}^1) \circ \cdots \circ (a_1^k a_2^k) \circ (a_2^k a_3^k) \circ \cdots \circ (a_{\ell_k - 1}^k a_{\ell_k}^k),$$

and so π is the composition of transpositions. $\square$

Example 2.3.4

Express each of the following permutations in S_6 as the composition of transpositions.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix}$;

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$;

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$.

Solution.

Example 2.3.4

Express each of the following permutations in S_6 as the composition of transpositions.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix}$;

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$;

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$.

Solution.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix} = (2543) = (25) \circ (54) \circ (43)$;

Example 2.3.4

Express each of the following permutations in S_6 as the composition of transpositions.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix}$;

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$;

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$.

Solution.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix} = (2543) = (25) \circ (54) \circ (43)$;

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} = {\color{red}(12)}{\color{blue}(456)} = {\color{red}(12)} \circ {\color{blue}(45)} \circ {\color{blue}(56)}$;

Example 2.3.4

Express each of the following permutations in S_6 as the composition of transpositions.

(a) $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 3 & 4 & 6 \end{pmatrix}$;

(b) $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix}$;

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix}$.

Solution (continued).

(c) $\pi_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 5 & 2 & 1 & 4 \end{pmatrix} = (135)(264) = (13) \circ (35) \circ (26) \circ (64)$.

□

- We note that the same permutation can be expressed as the composition of transpositions in more than one way.

- We note that the same permutation can be expressed as the composition of transpositions in more than one way.
- For instance, in S_5, we have:
  - $(12345) = (12) \circ (23) \circ (34) \circ (45)$;
  - $(12345) = (12) \circ (23) \circ (34) \circ (45) \circ (35) \circ (35)$;
  - $(12345) = (15) \circ (14) \circ (13) \circ (12)$;
  - $(12345) =$ $(35) \circ (35) \circ (23) \circ (23) \circ (15) \circ (14) \circ (13) \circ (12) \circ (35) \circ (35)$.

- We note that the same permutation can be expressed as the composition of transpositions in more than one way.
- For instance, in S_5, we have:
  - $(12345) = (12) \circ (23) \circ (34) \circ (45)$;
  - $(12345) = (12) \circ (23) \circ (34) \circ (45) \circ (35) \circ (35)$;
  - $(12345) = (15) \circ (14) \circ (13) \circ (12)$;
  - $(12345) =$ $(35) \circ (35) \circ (23) \circ (23) \circ (15) \circ (14) \circ (13) \circ (12) \circ (35) \circ (35)$.
- However, as we shall see, for any given permutation π in S_n, where $n \geq 2$, in all representations of π as a composition of transpositions, the number of transpositions is of the same parity (i.e. it is either always even or always odd).

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

a. $\mathrm{sgn}(\pi) = (-1)^r$;
b. π is an even permutation iff r is even;
c. π is an odd permutation iff r is odd.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\mathrm{sgn}(\pi) = (-1)^r$;
(b) π is an even permutation iff r is even;
(c) π is an odd permutation iff r is odd.

- The main ingredient of the proof of Theorem 2.3.6 is the following proposition.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\text{sgn}(\pi) = (-1)^r$;

(b) π is an even permutation iff r is even;

(c) π is an odd permutation iff r is odd.

- The main ingredient of the proof of Theorem 2.3.6 is the following proposition.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

- (a) $\operatorname{sgn}(\pi) = (-1)^r$;
- (b) π is an even permutation iff r is even;
- (c) π is an odd permutation iff r is odd.

- The main ingredient of the proof of Theorem 2.3.6 is the following proposition.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\operatorname{sgn}(\tau \circ \pi) = \operatorname{sgn}(\pi \circ \tau) = -\operatorname{sgn}(\pi)$.

- We first prove Theorem 2.3.6 assuming Proposition 2.3.5, and then we actually prove Proposition 2.3.5.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\mathrm{sgn}(\tau \circ \pi) = \mathrm{sgn}(\pi \circ \tau) = -\mathrm{sgn}(\pi)$.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\mathrm{sgn}(\pi) = (-1)^r$;

(b) π is an even permutation iff r is even;

(c) π is an odd permutation iff r is odd.

Proof (assuming Proposition 2.3.5).

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\mathrm{sgn}(\tau \circ \pi) = \mathrm{sgn}(\pi \circ \tau) = -\mathrm{sgn}(\pi)$.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\mathrm{sgn}(\pi) = (-1)^r$;

(b) π is an even permutation iff r is even;

(c) π is an odd permutation iff r is odd.

Proof (assuming Proposition 2.3.5). Clearly, (b) and (c) follow from (a).

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\text{sgn}(\pi) = (-1)^r$;

(b) π is an even permutation iff r is even;

(c) π is an odd permutation iff r is odd.

Proof (assuming Proposition 2.3.5). Clearly, (b) and (c) follow from (a). Part (a) follows from Proposition 2.3.5 by an easy induction on r.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\mathrm{sgn}(\tau \circ \pi) = \mathrm{sgn}(\pi \circ \tau) = -\mathrm{sgn}(\pi)$.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\mathrm{sgn}(\pi) = (-1)^r$;

(b) π is an even permutation iff r is even;

(c) π is an odd permutation iff r is odd.

Proof (assuming Proposition 2.3.5). Clearly, (b) and (c) follow from (a). Part (a) follows from Proposition 2.3.5 by an easy induction on r. Let us give the details.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\text{sgn}(\pi) = (-1)^r$;

(b) π is an even permutation iff r is even;

(c) π is an odd permutation iff r is odd.

Proof (assuming Proposition 2.3.5). Clearly, (b) and (c) follow from (a). Part (a) follows from Proposition 2.3.5 by an easy induction on r. Let us give the details. We prove the following statement: "for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\text{sgn}(\pi) = (-1)^r$."

Proof (continued). Reminder: WTS for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\mathrm{sgn}(\pi) = (-1)^r$.

Proof (continued). Reminder: WTS for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$.

Base case: $r = 1$. Note that if π is the composition of one transposition, i.e. π is itself a transposition, then π is odd, and we have that $\operatorname{sgn}(\pi) = -1 = (-1)^r$.

Proof (continued). Reminder: WTS for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$.

Base case: $r = 1$. Note that if π is the composition of one transposition, i.e. π is itself a transposition, then π is odd, and we have that $\operatorname{sgn}(\pi) = -1 = (-1)^r$.

Induction step: Fix a positive integer r, and assume that for any permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$.

Proof (continued). Reminder: WTS for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\mathrm{sgn}(\pi) = (-1)^r$.

Base case: $r = 1$. Note that if π is the composition of one transposition, i.e. π is itself a transposition, then π is odd, and we have that $\mathrm{sgn}(\pi) = -1 = (-1)^r$.

Induction step: Fix a positive integer r, and assume that for any permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\mathrm{sgn}(\pi) = (-1)^r$.

Now, fix a permutation $\pi \in S_n$ in S_n s.t. π can be expressed as the composition of $r + 1$ transpositions, say
$\pi = (a_0 a_0') \circ (a_1 a_1') \circ \cdots \circ (a_r a_r')$.

Proof (continued). Reminder: WTS for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\text{sgn}(\pi) = (-1)^r$.

Base case: $r = 1$. Note that if π is the composition of one transposition, i.e. π is itself a transposition, then π is odd, and we have that $\text{sgn}(\pi) = -1 = (-1)^r$.

Induction step: Fix a positive integer r, and assume that for any permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\text{sgn}(\pi) = (-1)^r$.

Now, fix a permutation $\pi \in S_n$ in S_n s.t. π can be expressed as the composition of $r + 1$ transpositions, say $\pi = (a_0 a_0') \circ (a_1 a_1') \circ \cdots \circ (a_r a_r')$.

Then by the induction hypothesis, $\pi' := (a_1 a_1') \circ \cdots \circ (a_r a_r')$ satisfies $\text{sgn}(\pi') = (-1)^r$.

Proof (continued). Reminder: WTS for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$.

Base case: $r = 1$. Note that if π is the composition of one transposition, i.e. π is itself a transposition, then π is odd, and we have that $\operatorname{sgn}(\pi) = -1 = (-1)^r$.

Induction step: Fix a positive integer r, and assume that for any permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$.

Now, fix a permutation $\pi \in S_n$ in S_n s.t. π can be expressed as the composition of $r + 1$ transpositions, say
$\pi = (a_0 a_0') \circ (a_1 a_1') \circ \cdots \circ (a_r a_r')$.

Then by the induction hypothesis, $\pi' := (a_1 a_1') \circ \cdots \circ (a_r a_r')$ satisfies $\operatorname{sgn}(\pi') = (-1)^r$. But since $\pi = (a_0 a_0') \circ \pi'$, Proposition 2.3.5 guarantees that $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi')$.

Proof (continued). Reminder: WTS for every positive integer r and permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$.

Base case: $r = 1$. Note that if π is the composition of one transposition, i.e. π is itself a transposition, then π is odd, and we have that $\operatorname{sgn}(\pi) = -1 = (-1)^r$.

Induction step: Fix a positive integer r, and assume that for any permutation $\pi \in S_n$, if π is the composition of r transpositions, then $\operatorname{sgn}(\pi) = (-1)^r$.

Now, fix a permutation $\pi \in S_n$ in S_n s.t. π can be expressed as the composition of $r + 1$ transpositions, say $\pi = (a_0 a_0') \circ (a_1 a_1') \circ \cdots \circ (a_r a_r')$.

Then by the induction hypothesis, $\pi' := (a_1 a_1') \circ \cdots \circ (a_r a_r')$ satisfies $\operatorname{sgn}(\pi') = (-1)^r$. But since $\pi = (a_0 a_0') \circ \pi'$, Proposition 2.3.5 guarantees that $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi')$. So, $\operatorname{sgn}(\pi) = -\operatorname{sgn}(\pi') = -(-1)^r = (-1)^{r+1}$. This completes the induction. $\square$

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\mathrm{sgn}(\tau \circ \pi) = \mathrm{sgn}(\pi \circ \tau) = -\mathrm{sgn}(\pi)$.

- **Warning:** In general, $\tau \circ \pi \neq \pi \circ \tau$.

Proof of Proposition 2.3.5.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

- **Warning:** In general, $\tau \circ \pi \cancel{=} \pi \circ \tau$.

Proof of Proposition 2.3.5. The Claim below proves one part of the proposition ("$\text{sgn}(\tau \circ \pi) = -\text{sgn}(\pi)$"). The other part ("$\text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$") can be proven using the Claim and certain basic properties of permutations (as we shall see below).

> ***Claim.*** *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\mathrm{sgn}(\tau \circ \pi) = \mathrm{sgn}(\pi \circ \tau) = -\mathrm{sgn}(\pi)$.

- **Warning:** In general, $\tau \circ \pi \cancel{=} \pi \circ \tau$.

Proof of Proposition 2.3.5. The Claim below proves one part of the proposition ("$\mathrm{sgn}(\tau \circ \pi) = -\mathrm{sgn}(\pi)$"). The other part ("$\mathrm{sgn}(\pi \circ \tau) = -\mathrm{sgn}(\pi)$") can be proven using the Claim and certain basic properties of permutations (as we shall see below).

> ***Claim.*** *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

- **Warning:** In general, $\tau \circ \pi \xcancel{=} \pi \circ \tau$.

Proof of Proposition 2.3.5. The Claim below proves one part of the proposition ("$\text{sgn}(\tau \circ \pi) = -\text{sgn}(\pi)$"). The other part ("$\text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$") can be proven using the Claim and certain basic properties of permutations (as we shall see below).

> ***Claim.*** *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $\text{sgn}(\tau \circ \pi) = -\text{sgn}(\pi)$.*

Proof of the Claim. Fix $\pi, \tau \in S_n$, and assume that $\tau = (ij)$ is a transposition (here, i and j are some two distinct elements of $\{1, \dots, n\}$).

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

- **Warning:** In general, $\tau \circ \pi \cancel{=} \pi \circ \tau$.

Proof of Proposition 2.3.5. The Claim below proves one part of the proposition ("$\text{sgn}(\tau \circ \pi) = -\text{sgn}(\pi)$"). The other part ("$\text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$") can be proven using the Claim and certain basic properties of permutations (as we shall see below).

> ***Claim.*** *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim. Fix $\pi, \tau \in S_n$, and assume that $\tau = (ij)$ is a transposition (here, i and j are some two distinct elements of $\{1, \dots, n\}$). There are two cases to consider: when i and j are in the same cycle of the disjoint cycle decomposition of π, and when they are in different cycles.

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 1: i and j are in the same cycle of the disjoint cycle decomposition of π.

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 1: i and j are in the same cycle of the disjoint cycle decomposition of π. After possibly swapping the order of our disjoint cycles, and cyclically permuting the elements of the cycle that contains i and j, we may assume that our disjoint cycle decomposition of π is given by

$$\pi \;\; = \;\; (i \;\, a_1 \dots a_p \;\, j \;\, b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

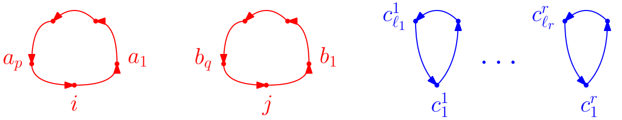
Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 1: i and j are in the same cycle of the disjoint cycle decomposition of π. After possibly swapping the order of our disjoint cycles, and cyclically permuting the elements of the cycle that contains i and j, we may assume that our disjoint cycle decomposition of π is given by

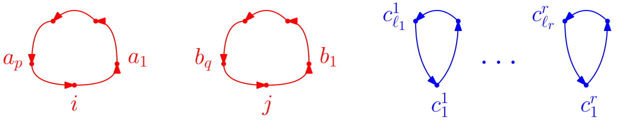
$$\pi \quad = \quad (i \ a_1 \dots a_p \ j \ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

In the permutation $\tau \circ \pi$, the red cycle essentially gets "split up" into two, while the blue cycles remain unaffected, as follows (next slide):

$$\begin{aligned}\tau \circ \pi &= (ij) \circ (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r) \\ &= \underbrace{(i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)}_{=:\pi'}.\end{aligned}$$

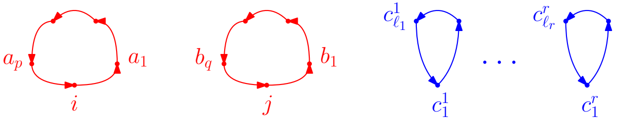


$$\begin{aligned}\tau \circ \pi &= (ij) \circ (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r) \\ &= \underbrace{(i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)}_{=:\pi'}.\end{aligned}$$



We now see that the disjoint cycle decomposition of $\tau \circ \pi$ has one cycle more than the disjoint cycle decomposition of π,

$$\begin{aligned}\tau \circ \pi &= (ij) \circ (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r) \\ &= \underbrace{(i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)}_{=:\pi'}.\end{aligned}$$



We now see that the disjoint cycle decomposition of $\tau \circ \pi$ has one cycle more than the disjoint cycle decomposition of π, and it follows that $\mathrm{sgn}(\tau \circ \pi) = -\mathrm{sgn}(\pi)$.

- Indeed, the disjoint cycle decomposition of π has $r+1$ cycles, whereas the disjoint cycle decomposition of $\tau \circ \pi$ has $r+2$ cycles. Therefore, $\mathrm{sgn}(\tau \circ \pi) = (-1)^{n-(r+2)} = (-1)^{n-(r+1)-1} = -(-1)^{n-(r+1)} = -\mathrm{sgn}(\pi)$.

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 2: i and j are in different cycles of the disjoint cycle decomposition of π.

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 2: i and j are in different cycles of the disjoint cycle decomposition of π.

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 2: i and j are in different cycles of the disjoint cycle decomposition of π. After possibly swapping the order of our disjoint cycles, and cyclically permuting the elements of the cycles that contain i and j, we may assume that our disjoint cycle decomposition of π is given by

$$\pi = (i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)$$

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 2: i and j are in different cycles of the disjoint cycle decomposition of π. After possibly swapping the order of our disjoint cycles, and cyclically permuting the elements of the cycles that contain i and j, we may assume that our disjoint cycle decomposition of π is given by

$$\pi = (i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)$$

We then have that

$$\begin{aligned} \pi &= (i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r) \\ &\overset{(*)}{=} (ij) \circ (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r), \end{aligned}$$

where (*) follows from the argument given in Case 1.

Claim. *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proof of the Claim (continued). Reminder: $\tau = (ij)$.

Case 2: i and j are in different cycles of the disjoint cycle decomposition of π. After possibly swapping the order of our disjoint cycles, and cyclically permuting the elements of the cycles that contain i and j, we may assume that our disjoint cycle decomposition of π is given by

$$\pi \quad = \quad (i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r)$$

We then have that

$$\begin{aligned} \pi \quad &= \quad (i\ a_1 \dots a_p)(j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r) \\ &\overset{(*)}{=} \quad (ij) \circ (i\ a_1 \dots a_p\ j\ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r), \end{aligned}$$

where (*) follows from the argument given in Case 1. We now compose both sides with $\tau = (ij)$ on the left, and we obtain (next slide):

$$(ij) \circ \pi \quad = \quad (ij) \circ (ij) \circ (i \ a_1 \dots a_p \ j \ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

$$(ij) \circ \pi \quad = \quad (ij) \circ (ij) \circ (i \; a_1 \ldots a_p \; j \; b_1 \ldots b_q)(c_1^1 \ldots c_{\ell_1}^1) \ldots (c_1^r \ldots c_{\ell_r}^r).$$

Since $(ij) = \tau$ and $(ij) \circ (ij) = 1_n$, we deduce that

$$\tau \circ \pi \quad = \quad (i \; a_1 \ldots a_p \; j \; b_1 \ldots b_q)(c_1^1 \ldots c_{\ell_1}^1) \ldots (c_1^r \ldots c_{\ell_r}^r).$$

$$(ij) \circ \pi \quad = \quad (ij) \circ (ij) \circ (i \; a_1 \dots a_p \; j \; b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

Since $(ij) = \tau$ and $(ij) \circ (ij) = 1_n$, we deduce that

$$\tau \circ \pi \quad = \quad (i \; a_1 \dots a_p \; j \; b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

As we can see, in the permutation $\tau \circ \pi$, the two red cycles of π essentially get "merged" into one, while the blue cycles remain unaffected.

$$(ij) \circ \pi \quad = \quad (ij) \circ (ij) \circ (i \ a_1 \dots a_p \ j \ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

Since $(ij) = \tau$ and $(ij) \circ (ij) = 1_n$, we deduce that

$$\tau \circ \pi \quad = \quad (i \ a_1 \dots a_p \ j \ b_1 \dots b_q)(c_1^1 \dots c_{\ell_1}^1) \dots (c_1^r \dots c_{\ell_r}^r).$$

As we can see, in the permutation $\tau \circ \pi$, the two red cycles of π essentially get "merged" into one, while the blue cycles remain unaffected. But now the disjoint cycle decomposition of $\tau \circ \pi$ has one cycle less than the disjoint cycle decomposition of π, and it follows that $\text{sgn}(\tau \circ \pi) = -\text{sgn}(\pi)$.

- Indeed, the disjoint cycle decomposition of π has $r + 2$ cycles, whereas the disjoint cycle decomposition of $\tau \circ \pi$ has $r + 1$ cycles. Therefore, $\text{sgn}(\tau \circ \pi) = (-1)^{n-(r+1)} = (-1)^{n-(r+2)+1} = -(-1)^{n-(r+2)} = -\text{sgn}(\pi)$.

This completes the proof of the Claim. ♦

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

Proof (continued). We have now proven the Claim below.

> ***Claim.*** *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

Proof (continued). We have now proven the Claim below.

> ***Claim.*** *For all $\pi, \tau \in S_n$ s.t. τ is a transposition, we have that $sgn(\tau \circ \pi) = -sgn(\pi)$.*

Now, fix $\pi, \tau \in S_n$ s.t. τ is a transposition. By the Claim, we have that $\text{sgn}(\tau \circ \pi) = -\pi$. On the other hand,

$$\begin{array}{rcll} \text{sgn}(\pi \circ \tau) & = & \text{sgn}\Big((\pi \circ \tau)^{-1}\Big) & \text{by Proposition 2.3.2} \\ & = & \text{sgn}\big(\tau^{-1} \circ \pi^{-1}\big) & \text{by Proposition 1.10.17(c) (or by Proposition 2.2.4(f))} \\ & = & \text{sgn}\big(\tau \circ \pi^{-1}\big) & \text{because } \tau \text{ is a transposition, and so } \tau^{-1} = \tau \\ & = & -\text{sgn}(\pi^{-1}) & \text{by the Claim applied to } \pi^{-1} \text{ and } \tau \\ & = & -\text{sgn}(\pi) & \text{by Proposition 2.3.2.} \end{array}$$

$\square$

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

Proposition 2.3.5

Let $n \geq 2$ be an integer. Then for all $\pi, \tau \in S_n$ s.t. τ is a **transposition**, we have that $\text{sgn}(\tau \circ \pi) = \text{sgn}(\pi \circ \tau) = -\text{sgn}(\pi)$.

Theorem 2.3.6

Let $n \geq 2$. Then for any permutation $\pi \in S_n$, if π can be expressed as a composition of r transpositions, then

(a) $\text{sgn}(\pi) = (-1)^r$;

(b) π is an even permutation iff r is even;

(c) π is an odd permutation iff r is odd.

Theorem 2.3.7

Let $n \geq 2$ be an integer, and let $\sigma, \pi \in S_n$. Then $\mathrm{sgn}(\sigma \circ \pi) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\pi)$.

Proof.

Theorem 2.3.7

Let $n \geq 2$ be an integer, and let $\sigma, \pi \in S_n$. Then $\mathrm{sgn}(\sigma \circ \pi) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\pi)$.

Proof. This easily follows from Proposition 2.3.3 and Theorem 2.3.6.

Theorem 2.3.7

Let $n \geq 2$ be an integer, and let $\sigma, \pi \in S_n$. Then $\operatorname{sgn}(\sigma \circ \pi) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\pi)$.

Proof. This easily follows from Proposition 2.3.3 and Theorem 2.3.6. Let us give the details.

Theorem 2.3.7

Let $n \geq 2$ be an integer, and let $\sigma, \pi \in S_n$. Then $\mathrm{sgn}(\sigma \circ \pi) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\pi)$.

Proof. This easily follows from Proposition 2.3.3 and Theorem 2.3.6. Let us give the details. By Proposition 2.3.3, we can express σ and π as compositions of transpositions, say

- $\sigma = (s_1 s_1') \circ (s_2 s_2') \circ \cdots \circ (s_k s_k')$;
- $\pi = (t_1 t_1') \circ (t_2 t_2') \circ \cdots \circ (t_\ell t_\ell')$.

By Theorem 2.3.6(a), we have that $\mathrm{sgn}(\sigma) = (-1)^k$ and $\mathrm{sgn}(\pi) = (-1)^\ell$.

Theorem 2.3.7

Let $n \geq 2$ be an integer, and let $\sigma, \pi \in S_n$. Then $\mathrm{sgn}(\sigma \circ \pi) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\pi)$.

Proof. This easily follows from Proposition 2.3.3 and Theorem 2.3.6. Let us give the details. By Proposition 2.3.3, we can express σ and π as compositions of transpositions, say

- $\sigma = (s_1 s_1') \circ (s_2 s_2') \circ \cdots \circ (s_k s_k')$;
- $\pi = (t_1 t_1') \circ (t_2 t_2') \circ \cdots \circ (t_\ell t_\ell')$.

By Theorem 2.3.6(a), we have that $\mathrm{sgn}(\sigma) = (-1)^k$ and $\mathrm{sgn}(\pi) = (-1)^\ell$.

On the other hand,
$\sigma \circ \pi = (s_1 s_1') \circ (s_2 s_2') \circ \cdots \circ (s_k s_k') \circ (t_1 t_1') \circ (t_2 t_2') \circ \cdots \circ (t_\ell t_\ell')$,
and so again by Theorem 2.3.6(a), we have that
$\mathrm{sgn}(\sigma \circ \pi) = (-1)^{k+\ell}$.

Theorem 2.3.7

Let $n \geq 2$ be an integer, and let $\sigma, \pi \in S_n$. Then $\text{sgn}(\sigma \circ \pi) = \text{sgn}(\sigma)\text{sgn}(\pi)$.

Proof. This easily follows from Proposition 2.3.3 and Theorem 2.3.6. Let us give the details. By Proposition 2.3.3, we can express σ and π as compositions of transpositions, say

- $\sigma = (s_1 s_1') \circ (s_2 s_2') \circ \cdots \circ (s_k s_k')$;
- $\pi = (t_1 t_1') \circ (t_2 t_2') \circ \cdots \circ (t_\ell t_\ell')$.

By Theorem 2.3.6(a), we have that $\text{sgn}(\sigma) = (-1)^k$ and $\text{sgn}(\pi) = (-1)^\ell$.

On the other hand,
$\sigma \circ \pi = (s_1 s_1') \circ (s_2 s_2') \circ \cdots \circ (s_k s_k') \circ (t_1 t_1') \circ (t_2 t_2') \circ \cdots \circ (t_\ell t_\ell')$, and so again by Theorem 2.3.6(a), we have that $\text{sgn}(\sigma \circ \pi) = (-1)^{k+\ell}$.

So, $\text{sgn}(\sigma \circ \pi) = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \text{sgn}(\sigma)\text{sgn}(\pi)$. $\square$

- For an integer $n \geq 2$, let A_n be the set of all even permutations in S_n.

- For an integer $n \geq 2$, let A_n be the set of all even permutations in S_n.
- Let us show that $(A_n, \circ)$ is a subgroup of $(S_n, \circ)$, where $\circ$ is the composition of functions.

- For an integer $n \geq 2$, let A_n be the set of all even permutations in S_n.
- Let us show that $(A_n, \circ)$ is a subgroup of $(S_n, \circ)$, where $\circ$ is the composition of functions.
- We apply Theorem 2.2.9.

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, $\forall a \in H\colon\ a^{-1} \in H$.

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, $\forall a \in H$: $a^{-1} \in H$.

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, $\forall a \in H$: $a^{-1} \in H$.

- The identity element of S_n is the identity permutation 1_n, which is obviously even, and therefore belongs to A_n.

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, $\forall a \in H$: $a^{-1} \in H$.

- The identity element of S_n is the identity permutation 1_n, which is obviously even, and therefore belongs to A_n.
- Next, by Theorem 2.3.7, a composition of two even permutations is even, and consequently, A_n is closed under $\circ$.

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

- The identity element of S_n is the identity permutation 1_n, which is obviously even, and therefore belongs to A_n.
- Next, by Theorem 2.3.7, a composition of two even permutations is even, and consequently, A_n is closed under $\circ$.
- Finally, by Proposition 2.3.2, the sign of a permutation in S_n is equal to the sign of its inverse, and in particular, the inverse of an even permutation is even; so, A_n is closed under 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:

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, $\forall a \in H$: $a^{-1} \in H$.

- The identity element of S_n is the identity permutation 1_n, which is obviously even, and therefore belongs to A_n.
- Next, by Theorem 2.3.7, a composition of two even permutations is even, and consequently, A_n is closed under $\circ$.
- Finally, by Proposition 2.3.2, the sign of a permutation in S_n is equal to the sign of its inverse, and in particular, the inverse of an even permutation is even; so, A_n is closed under inverses.
- Theorem 2.2.9 now guarantees that A_n is indeed a subgroup of S_n.

- **Terminology:** For an integer $n \geq 2$, the group $(A_n, \circ)$ is called the *alternating group of degree n*.

- **Terminology:** For an integer $n \geq 2$, the group $(A_n, \circ)$ is called the *alternating group of degree n*.
  - Typically, we just say that A_n is the alternating group of degree n, and the operation $\circ$ (composition of functions) is understood from context.

- **Terminology:** For an integer $n \geq 2$, the group $(A_n, \circ)$ is called the *alternating group of degree n*.
  - Typically, we just say that A_n is the alternating group of degree n, and the operation $\circ$ (composition of functions) is understood from context.
- We remark that the set of odd permutations in S_n ($n \geq 2$), call it O_n, does **not** form a subgroup of S_n.
  - Indeed, the identity permutation 1_n is even and therefore does not belong to O_n; so, by Theorem 2.2.9, O_n is not a subgroup of S_n.

- **Terminology:** For an integer $n \geq 2$, the group $(A_n, \circ)$ is called the *alternating group of degree n*.
  - Typically, we just say that A_n is the alternating group of degree n, and the operation $\circ$ (composition of functions) is understood from context.
- We remark that the set of odd permutations in S_n ($n \geq 2$), call it O_n, does **not** form a subgroup of S_n.
  - Indeed, the identity permutation 1_n is even and therefore does not belong to O_n; so, by Theorem 2.2.9, O_n is not a subgroup of S_n.
- **Remark:** O_n is **not** standard notation for the set of odd permutations in S_n; in fact, no standard notation exists for this set.

- **Terminology:** For an integer $n \geq 2$, the group $(A_n, \circ)$ is called the *alternating group of degree n*.
    - Typically, we just say that A_n is the alternating group of degree n, and the operation $\circ$ (composition of functions) is understood from context.
- We remark that the set of odd permutations in S_n ($n \geq 2$), call it O_n, does **not** form a subgroup of S_n.
    - Indeed, the identity permutation 1_n is even and therefore does not belong to O_n; so, by Theorem 2.2.9, O_n is not a subgroup of S_n.
- **Remark:** O_n is **not** standard notation for the set of odd permutations in S_n; in fact, no standard notation exists for this set.
- However, A_n is indeed the standard notation for the set of even permutations in S_n.

Definition

Let n be a positive integer. An *inversion* of a permutation $\pi \in S_n$ is an ordered pair (i, j) of numbers in $\{1, \ldots, n\}$ s.t. $i < j$ and $\pi(i) > \pi(j)$.

Definition

Let n be a positive integer. An *inversion* of a permutation $\pi \in S_n$ is an ordered pair (i, j) of numbers in $\{1, \ldots, n\}$ s.t. $i < j$ and $\pi(i) > \pi(j)$.

Example 2.3.8

The permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

in S_7 has the following four inversions: $(1,2), (4,5), (4,6), (5,6)$.

Definition

Let n be a positive integer. An *inversion* of a permutation $\pi \in S_n$ is an ordered pair (i, j) of numbers in $\{1, \ldots, n\}$ s.t. $i < j$ and $\pi(i) > \pi(j)$.

Example 2.3.8

The permutation

$$\pi \quad = \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

in S_7 has the following four inversions: $(1, 2), (4, 5), (4, 6), (5, 6)$.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\mathrm{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\mathrm{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\operatorname{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof. We proceed by induction on the number r of inversions.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\operatorname{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof. We proceed by induction on the number r of inversions.

Base case: $r = 0$.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\mathrm{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof. We proceed by induction on the number r of inversions.

Base case: $r = 0$. The only permutation with no inversions is the identity permutation,

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\operatorname{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof. We proceed by induction on the number r of inversions.

Base case: $r = 0$. The only permutation with no inversions is the identity permutation, and its sign is 1. Since $(-1)^0 = 1$, this is what we needed.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\operatorname{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof. We proceed by induction on the number r of inversions.

Base case: $r = 0$. The only permutation with no inversions is the identity permutation, and its sign is 1. Since $(-1)^0 = 1$, this is what we needed.

Induction step: Fix a non-negative integer r, and assume inductively that any permutation in S_n that has exactly r inversions has sign $(-1)^r$. WTS any permutation in S_n that has exactly $r + 1$ inversions has sign $(-1)^{r+1}$.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\operatorname{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof (continued). Fix a permutation $\pi \in S_n$, and assume that it has exactly $r + 1$ inversions.

- Note that this implies that $n \geq 2$.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\text{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof (continued). Fix a permutation $\pi \in S_n$, and assume that it has exactly $r + 1$ inversions.

- Note that this implies that $n \geq 2$.

In particular, π has at least one inversion, and it follows that there exists some $p \in \{1, \ldots, n-1\}$ s.t. $(p, p+1)$ is an inversion of π.

- Otherwise, we would have that $\pi(1) < \pi(2) < \cdots < \pi(n)$, and then π would be the identity permutation, contrary to the fact that it has at least one inversion.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\operatorname{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof (continued). Fix a permutation $\pi \in S_n$, and assume that it has exactly $r + 1$ inversions.

- Note that this implies that $n \geq 2$.

In particular, π has at least one inversion, and it follows that there exists some $p \in \{1, \dots, n-1\}$ s.t. $(p, p+1)$ is an inversion of π.

- Otherwise, we would have that $\pi(1) < \pi(2) < \cdots < \pi(n)$, and then π would be the identity permutation, contrary to the fact that it has at least one inversion.

Now, consider the transposition $\tau := \big(\pi(p)\pi(p+1)\big)$ in S_n, and set $\pi' := \tau \circ \pi$, so that

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & {\color{red}p} & {\color{blue}p+1} & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & {\color{blue}\pi(p+1)} & {\color{red}\pi(p)} & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has.

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has. To see this, we note the following:

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has. To see this, we note the following:

- inversions (i, j) of π s.t. $i, j \notin \{p, p+1\}$ are still inversions of π';

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has. To see this, we note the following:

- inversions (i,j) of π s.t. $i,j \notin \{p, p+1\}$ are still inversions of π';
- inversions of the form (i,p) of π correspond to inversions $(i,p+1)$ of π';

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has. To see this, we note the following:

- inversions (i,j) of π s.t. $i,j \notin \{p, p+1\}$ are still inversions of π';
- inversions of the form (i,p) of π correspond to inversions $(i, p+1)$ of π';
- inversions of the form $(i, p+1)$ of π, where $i < p$, correspond to inversions (i,p) of π';

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has. To see this, we note the following:

- inversions (i, j) of π s.t. $i, j \notin \{p, p+1\}$ are still inversions of π';
- inversions of the form (i, p) of π correspond to inversions $(i, p+1)$ of π';
- inversions of the form $(i, p+1)$ of π, where $i < p$, correspond to inversions (i, p) of π';
- inversions of the form (p, j) of π, where $p+1 < j$, correspond to inversions $(p+1, j)$ of π';

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & \color{red}{p} & \color{blue}{p+1} & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \color{blue}{\pi(p+1)} & \color{red}{\pi(p)} & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has. To see this, we note the following:

- inversions (i,j) of π s.t. $i,j \notin \{p, p+1\}$ are still inversions of π';
- inversions of the form (i,p) of π correspond to inversions $(i, p+1)$ of π';
- inversions of the form $(i, p+1)$ of π, where $i < p$, correspond to inversions (i,p) of π';
- inversions of the form (p,j) of π, where $p+1 < j$, correspond to inversions $(p+1, j)$ of π';
- inversions of the form $(p+1, j)$ of π correspond to inversions (p,j) of π';

Proof (continued). Reminder:

$$\pi' = \begin{pmatrix} 1 & \dots & p-1 & p & p+1 & p+2 & \dots & n \\ \pi(1) & \dots & \pi(p-1) & \pi(p+1) & \pi(p) & \pi(p+2) & \dots & \pi(n) \end{pmatrix}.$$

Then π' has exactly r inversions, i.e. exactly one inversion less than π has. To see this, we note the following:

- inversions (i,j) of π s.t. $i,j \notin \{p, p+1\}$ are still inversions of π';
- inversions of the form (i,p) of π correspond to inversions $(i, p+1)$ of π';
- inversions of the form $(i, p+1)$ of π, where $i < p$, correspond to inversions (i,p) of π';
- inversions of the form (p,j) of π, where $p+1 < j$, correspond to inversions $(p+1, j)$ of π';
- inversions of the form $(p+1, j)$ of π correspond to inversions (p,j) of π';
- π' has no other inversions, and in particular $(p, p+1)$ is **not** an inversion of π'.

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\mathrm{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof (continued). Reminder: $\pi' = \tau \circ \pi$ and π' has exactly r inversions (i.e. exactly one inversion less than π).

Theorem 2.3.9

Let n be a positive integer. Then all permutations $\pi \in S_n$ satisfy $\mathrm{sgn}(\pi) = (-1)^r$, where r is the number of inversions of π.

Proof (continued). Reminder: $\pi' = \tau \circ \pi$ and π' has exactly r inversions (i.e. exactly one inversion less than π).

But now

$$
\begin{array}{rcll}
(-1)^r & = & \mathrm{sgn}(\pi') & \text{by the induction hypothesis,} \\
 & & & \text{since } \pi' \text{ has exactly } r \text{ inversions} \\
 & = & \mathrm{sgn}(\tau \circ \pi) & \text{because } \pi' = \tau \circ \pi \\
 & = & -\mathrm{sgn}(\pi) & \text{by Proposition 2.3.5,} \\
 & & & \text{since } \tau \text{ is a transposition,}
\end{array}
$$

and it follows that $\mathrm{sgn}(\pi) = (-1)^{r+1}$. This completes the induction. $\square$

- **Remark:** In the induction step of the proof of Theorem 2.3.9, it was important that we chose an inversion of the form $(p, p+1)$, and not just any inversion of our permutation π.

- **Remark:** In the induction step of the proof of Theorem 2.3.9, it was important that we chose an inversion of the form $(p, p+1)$, and not just any inversion of our permutation π.
- To explain why, let us take a look at an example.

- **Remark:** In the induction step of the proof of Theorem 2.3.9, it was important that we chose an inversion of the form $(p, p+1)$, and not just any inversion of our permutation π.
- To explain why, let us take a look at an example.
- Consider the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

from Example 2.3.8.

- **Remark:** In the induction step of the proof of Theorem 2.3.9, it was important that we chose an inversion of the form $(p, p+1)$, and not just any inversion of our permutation π.
- To explain why, let us take a look at an example.
- Consider the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

  from Example 2.3.8.
- We could choose the inversion $(4, 5)$, and consider the transposition $\tau := \left(\pi(4)\pi(5)\right) = (65) = (56)$ and the permutation

$$\pi' := \tau \circ \pi = (56) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 5 & 6 & 4 & 7 \end{pmatrix}$$

- **Remark:** In the induction step of the proof of Theorem 2.3.9, it was important that we chose an inversion of the form $(p, p+1)$, and not just any inversion of our permutation π.
- To explain why, let us take a look at an example.
- Consider the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

from Example 2.3.8.
- We could choose the inversion $(4, 5)$, and consider the transposition $\tau := \left(\pi(4)\pi(5)\right) = (65) = (56)$ and the permutation

$$\pi' := \tau \circ \pi = (56) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 5 & 6 & 4 & 7 \end{pmatrix}$$

- Note that π' has three inversions, whereas π has four.

- Reminder:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}.$$

- Reminder:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & {\color{red}4} & {\color{blue}5} & 6 & 7 \\ 2 & 1 & 3 & {\color{red}6} & {\color{blue}5} & 4 & 7 \end{pmatrix}.$$

- If we had, instead, chosen an arbitrary inversion of π, then the number of inversions would not necessarily decrease by one, and we could not apply the induction hypothesis.

- Reminder:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}.$$

- If we had, instead, chosen an arbitrary inversion of π, then the number of inversions would not necessarily decrease by one, and we could not apply the induction hypothesis.
- Indeed, suppose we chose the inversion $(4, 6)$ of our permutation π (above) and then considered the transposition $\tau' := \big(\pi(4)\pi(6)\big) = (64) = (46)$ and the permutation

$$\pi'' := \tau' \circ \pi = (46) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

- Reminder:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}.$$

- If we had, instead, chosen an arbitrary inversion of π, then the number of inversions would not necessarily decrease by one, and we could not apply the induction hypothesis.
- Indeed, suppose we chose the inversion $(4, 6)$ of our permutation π (above) and then considered the transposition $\tau' := \left(\pi(4)\pi(6)\right) = (64) = (46)$ and the permutation

$$\pi'' := \tau' \circ \pi = (46) \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 6 & 5 & 4 & 7 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 5 & 6 & 7 \end{pmatrix}.$$

- Note that π'' has only one inversion (namely, $(1, 2)$), whereas π has four.

Definition

A *field* is an ordered triple $(\mathbb{F}, +, \cdot)$, where $\mathbb{F}$ is a set, and $+$ and $\cdot$ are binary operations on $\mathbb{F}$ (i.e. functions from $\mathbb{F} \times \mathbb{F}$ to $\mathbb{F}$), called *addition* and *multiplication*, respectively, satisfying the following axioms:

1. addition and multiplication are associative, that is, for all $a, b, c \in \mathbb{F}$, we have that $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
2. addition and multiplication are commutative, that is, for all $a, b \in \mathbb{F}$, we have that $a + b = b + a$ and $a \cdot b = b \cdot a$;
3. there exist distinct elements $0_{\mathbb{F}}, 1_{\mathbb{F}} \in \mathbb{F}$ s.t. for all $a \in \mathbb{F}$, $a + 0_{\mathbb{F}} = a$ and $a \cdot 1_{\mathbb{F}} = a$; $0_{\mathbb{F}}$ is called the *additive identity* of $\mathbb{F}$, and $1_{\mathbb{F}}$ is called the *multiplicative identity* of $\mathbb{F}$;
4. for every $a \in \mathbb{F}$, there exists an element in $\mathbb{F}$, denoted by $-a$ and called the *additive inverse* of a, s.t. $a + (-a) = 0_{\mathbb{F}}$;
5. for all $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, there exists an element in $\mathbb{F}$, denoted by a^{-1} and called the *multiplicative inverse* of a, s.t. $a \cdot a^{-1} = 1_{\mathbb{F}}$;
6. multiplication is distributive over addition, that is, for all $a, b, c \in \mathbb{F}$, we have that $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Example 2.4.1

All the following are fields:

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

Example 2.4.1

All the following are fields:

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

- Note that $(\mathbb{Z}, +, \cdot)$ is **not** a field. This is because elements of $\mathbb{Z} \setminus \{-1, 0, 1\}$ do not have multiplicative inverses.

Example 2.4.1

All the following are fields:

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

- Note that $(\mathbb{Z}, +, \cdot)$ is **not** a field. This is because elements of $\mathbb{Z} \setminus \{-1, 0, 1\}$ do not have multiplicative inverses.
- As we shall see (Theorem 2.4.3), $(\mathbb{Z}_p, +, \cdot)$ is a field for every **prime** number p.

Example 2.4.1

All the following are fields:

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

- Note that $(\mathbb{Z}, +, \cdot)$ is **not** a field. This is because elements of $\mathbb{Z} \setminus \{-1, 0, 1\}$ do not have multiplicative inverses.
- As we shall see (Theorem 2.4.3), $(\mathbb{Z}_p, +, \cdot)$ is a field for every **prime** number p.
- **Notation:**

Example 2.4.1

All the following are fields:

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

- Note that $(\mathbb{Z}, +, \cdot)$ is **not** a field. This is because elements of $\mathbb{Z} \setminus \{-1, 0, 1\}$ do not have multiplicative inverses.
- As we shall see (Theorem 2.4.3), $(\mathbb{Z}_p, +, \cdot)$ is a field for every **prime** number p.

- **Notation:**
  - If operations $+$ and $\cdot$ are understood from context, then we typically just say "field $\mathbb{F}$" instead of "field $(\mathbb{F}, +, \cdot)$."

Example 2.4.1

All the following are fields:

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

- Note that $(\mathbb{Z}, +, \cdot)$ is **not** a field. This is because elements of $\mathbb{Z} \setminus \{-1, 0, 1\}$ do not have multiplicative inverses.
- As we shall see (Theorem 2.4.3), $(\mathbb{Z}_p, +, \cdot)$ is a field for every **prime** number p.

- **Notation:**
  - If operations $+$ and $\cdot$ are understood from context, then we typically just say "field $\mathbb{F}$" instead of "field $(\mathbb{F}, +, \cdot)$."
  - For $a, b \in \mathbb{F}$, we typically write ab instead of $a \cdot b$, and we typically write $a - b$ instead of $a + (-b)$.

Example 2.4.1

All the following are fields:

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

- Note that $(\mathbb{Z}, +, \cdot)$ is **not** a field. This is because elements of $\mathbb{Z} \setminus \{-1, 0, 1\}$ do not have multiplicative inverses.
- As we shall see (Theorem 2.4.3), $(\mathbb{Z}_p, +, \cdot)$ is a field for every **prime** number p.
- **Notation:**
  - If operations $+$ and $\cdot$ are understood from context, then we typically just say "field $\mathbb{F}$" instead of "field $(\mathbb{F}, +, \cdot)$."
  - For $a, b \in \mathbb{F}$, we typically write ab instead of $a \cdot b$, and we typically write $a - b$ instead of $a + (-b)$.
  - As usual, unless parentheses indicate otherwise, we perform multiplication before performing addition. So, for $a, b, c \in \mathbb{F}$, we write $ab + c$ instead of $(a \cdot b) + c$, and similarly, we write $a + bc$ instead of $a + (b \cdot c)$.

- **Remark:** Axioms 1, 2, and 3 imply that $(\mathbb{F}, +)$ and $(\mathbb{F}, \cdot)$ are monoids with identity elements $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$, respectively. Proposition 2.1.1 guarantees that $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$ are unique.
    - When there is no danger of confusion, we write 0 and 1 instead of $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$, respectively.

- **Remark:** Axioms 1, 2, and 3 imply that $(\mathbb{F}, +)$ and $(\mathbb{F}, \cdot)$ are monoids with identity elements $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$, respectively. Proposition 2.1.1 guarantees that $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$ are unique.
    - When there is no danger of confusion, we write 0 and 1 instead of $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$, respectively.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.[a]

---

[a] This statement may require some clarification. Here, $-a$ is the additive inverse of a. On the other hand, $(-1)a$ is the product of -1 (the additive inverse of the multiplicative identity) and a. So, $-a$ is not simply a shorthand for $(-1)a$. The two quantities are indeed equal, but this requires proof!

- Proof: Later!

- **Remark:** Axioms 1, 2, and 3 imply that $(\mathbb{F}, +)$ and $(\mathbb{F}, \cdot)$ are monoids with identity elements $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$, respectively. Proposition 2.1.1 guarantees that $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$ are unique.
  - When there is no danger of confusion, we write 0 and 1 instead of $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$, respectively.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

a. for all $a \in \mathbb{F}$, $0a = a0 = 0$;
b. for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;
c. for all $a \in \mathbb{F}$, $(-1)a = -a$.[a]

[a] This statement may require some clarification. Here, $-a$ is the additive inverse of a. On the other hand, $(-1)a$ is the product of -1 (the additive inverse of the multiplicative identity) and a. So, $-a$ is not simply a shorthand for $(-1)a$. The two quantities are indeed equal, but this requires proof!

- Proof: Later!
- First, some remarks (next slide).

- **Remarks:**

- **Remarks:**
  1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.

- **Remarks:**
  1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.
  2. By Proposition 2.4.2, for any $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, we have $ab \neq 0_{\mathbb{F}}$, i.e. $ab \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.

- **Remarks:**
    1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.
    2. By Proposition 2.4.2, for any $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, we have $ab \neq 0_{\mathbb{F}}$, i.e. $ab \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
        - This, together with axioms 1 and 3, implies that $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is a monoid with identity element $1_{\mathbb{F}}$.

- **Remarks:**
  1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.
  2. By Proposition 2.4.2, for any $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, we have $ab \neq 0_{\mathbb{F}}$, i.e. $ab \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - This, together with axioms 1 and 3, implies that $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is a monoid with identity element $1_{\mathbb{F}}$.
     - Next, by Proposition 2.4.2, and by axioms 2 (commutativity of addition) and 3 ($0_{\mathbb{F}} \neq 1_{\mathbb{F}}$), we have that we have that $a0_{\mathbb{F}} = 0_{\mathbb{F}}a = 0_{\mathbb{F}} \neq 1_{\mathbb{F}}$.

- **Remarks:**
  1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.
  2. By Proposition 2.4.2, for any $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, we have $ab \neq 0_{\mathbb{F}}$, i.e. $ab \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - This, together with axioms 1 and 3, implies that $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is a monoid with identity element $1_{\mathbb{F}}$.
     - Next, by Proposition 2.4.2, and by axioms 2 (commutativity of addition) and 3 ($0_{\mathbb{F}} \neq 1_{\mathbb{F}}$), we have that we have that $a0_{\mathbb{F}} = 0_{\mathbb{F}}a = 0_{\mathbb{F}} \neq 1_{\mathbb{F}}$.
     - This, together with axiom 5 implies that the multiplicative inverse of any element $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ also belongs to $\mathbb{F} \setminus \{0_{\mathbb{F}}\}$.

- **Remarks:**
  1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.
  2. By Proposition 2.4.2, for any $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, we have $ab \neq 0_{\mathbb{F}}$, i.e. $ab \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - This, together with axioms 1 and 3, implies that $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is a monoid with identity element $1_{\mathbb{F}}$.
     - Next, by Proposition 2.4.2, and by axioms 2 (commutativity of addition) and 3 ($0_{\mathbb{F}} \neq 1_{\mathbb{F}}$), we have that we have that $a0_{\mathbb{F}} = 0_{\mathbb{F}}a = 0_{\mathbb{F}} \neq 1_{\mathbb{F}}$.
     - This, together with axiom 5 implies that the multiplicative inverse of any element $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ also belongs to $\mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - So, $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is an abelian group with identity element $1_{\mathbb{F}}$.

- **Remarks:**
  1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.
  2. By Proposition 2.4.2, for any $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, we have $ab \neq 0_{\mathbb{F}}$, i.e. $ab \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - This, together with axioms 1 and 3, implies that $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is a monoid with identity element $1_{\mathbb{F}}$.
     - Next, by Proposition 2.4.2, and by axioms 2 (commutativity of addition) and 3 ($0_{\mathbb{F}} \neq 1_{\mathbb{F}}$), we have that we have that $a0_{\mathbb{F}} = 0_{\mathbb{F}}a = 0_{\mathbb{F}} \neq 1_{\mathbb{F}}$.
     - This, together with axiom 5 implies that the multiplicative inverse of any element $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ also belongs to $\mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - So, $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is an abelian group with identity element $1_{\mathbb{F}}$.
     - By Proposition 2.2.1, it follows that every element $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ has a **unique** multiplicative inverse a^{-1}.

- **Remarks:**
  1. Axioms 1, 2, 3, and 4 imply that $(\mathbb{F}, +)$ is an abelian group with identity element $0_{\mathbb{F}}$. By Proposition 2.2.1, this implies that each element $a \in \mathbb{F}$ has a **unique** additive inverse $-a$.
  2. By Proposition 2.4.2, for any $a, b \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$, we have $ab \neq 0_{\mathbb{F}}$, i.e. $ab \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - This, together with axioms 1 and 3, implies that $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is a monoid with identity element $1_{\mathbb{F}}$.
     - Next, by Proposition 2.4.2, and by axioms 2 (commutativity of addition) and 3 ($0_{\mathbb{F}} \neq 1_{\mathbb{F}}$), we have that we have that $a0_{\mathbb{F}} = 0_{\mathbb{F}}a = 0_{\mathbb{F}} \neq 1_{\mathbb{F}}$.
     - This, together with axiom 5 implies that the multiplicative inverse of any element $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ also belongs to $\mathbb{F} \setminus \{0_{\mathbb{F}}\}$.
     - So, $(\mathbb{F} \setminus \{0_{\mathbb{F}}\}, \cdot)$ is an abelian group with identity element $1_{\mathbb{F}}$.
     - By Proposition 2.2.1, it follows that every element $a \in \mathbb{F} \setminus \{0_{\mathbb{F}}\}$ has a **unique** multiplicative inverse a^{-1}.
  3. By axioms 2 and 6, for all $a, b, c \in \mathbb{F}$, we have that $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$, or written in a simplified manner, $(b + c)a = ba + ca$.
     - Indeed, for $a, b, c \in \mathbb{F}$, we have that $(b + c)a \overset{\text{ax. 2.}}{=} a(b + c) \overset{\text{ax. 6.}}{=} ab + ac \overset{\text{ax. 2.}}{=} ba + ca$.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof. We first prove (a). Fix $a \in \mathbb{F}$.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof. We first prove (a). Fix $a \in \mathbb{F}$. Since multiplication in the field $\mathbb{F}$ is commutative, we know that $0a = a0$.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof. We first prove (a). Fix $a \in \mathbb{F}$. Since multiplication in the field $\mathbb{F}$ is commutative, we know that $0a = a0$. So, it suffices to show that $a0 = 0$.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof. We first prove (a). Fix $a \in \mathbb{F}$. Since multiplication in the field $\mathbb{F}$ is commutative, we know that $0a = a0$. So, it suffices to show that $a0 = 0$.

First, note that

$$a0 \overset{(*)}{=} a(0+0) \overset{(**)}{=} a0 + a0,$$

where (*) follows from the fact that $0 + 0 = 0$ (because 0 is the additive identity of the field), and (**) follows from axiom 6 of the definition of a field.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof. We first prove (a). Fix $a \in \mathbb{F}$. Since multiplication in the field $\mathbb{F}$ is commutative, we know that $0a = a0$. So, it suffices to show that $a0 = 0$.

First, note that

$$a0 \overset{(*)}{=} a(0+0) \overset{(**)}{=} a0 + a0,$$

where (*) follows from the fact that $0 + 0 = 0$ (because 0 is the additive identity of the field), and (**) follows from axiom 6 of the definition of a field. We have now established that $a0 = a0 + a0$, and it follows that (next slide):

Proof (continued). Reminder: $a0 = a0 + a0$.

0	$=$	$-(a0) + a0$	because $-(a0)$ is the additive inverse of $a0$
	$=$	$-(a0) + (a0 + a0)$	because $a0 = a0 + a0$ (proven above)
	$=$	$(-(a0) + a0) + a0$	because $+$ is associative
	$=$	$0 + a0$	because $-(a0)$ is the additive inverse of $a0$
	$=$	$a0$	because 0 is the additive identity of the field $\mathbb{F}$.

Thus, $a0 = 0$. This proves (a).

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

- (a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;
- (b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;
- (c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof (continued). Next, we prove (b).

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof (continued). Next, we prove (b). Fix $a, b \in \mathbb{F}$ s.t. $ab = 0$.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

a. for all $a \in \mathbb{F}$, $0a = a0 = 0$;
b. for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;
c. for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof (continued). Next, we prove (b). Fix $a, b \in \mathbb{F}$ s.t. $ab = 0$. WTS $a = 0$ or $b = 0$.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof (continued). Next, we prove (b). Fix $a, b \in \mathbb{F}$ s.t. $ab = 0$. WTS $a = 0$ or $b = 0$. We may assume that $b \neq 0$, for otherwise we are done.

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof (continued). Next, we prove (b). Fix $a, b \in \mathbb{F}$ s.t. $ab = 0$. WTS $a = 0$ or $b = 0$. We may assume that $b \neq 0$, for otherwise we are done. But now b has a multiplicative inverse b^{-1},

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

- (a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;
- (b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;
- (c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

Proof (continued). Next, we prove (b). Fix $a, b \in \mathbb{F}$ s.t. $ab = 0$. WTS $a = 0$ or $b = 0$. We may assume that $b \neq 0$, for otherwise we are done. But now b has a multiplicative inverse b^{-1}, and we compute:

$$a = a \cdot 1 = a(bb^{-1}) \overset{(*)}{=} (ab)b^{-1} \overset{(**)}{=} 0b^{-1} \overset{(***)}{=} 0,$$

where (*) follows from the associativity of multiplication, (**) follows from the fact that $ab = 0$, and (***) follows from (a).

Proof (continued). It remains to prove (c).

Proof (continued). It remains to prove (c). Fix $a \in \mathbb{F}$.

Proof (continued). It remains to prove (c). Fix $a \in \mathbb{F}$. WTS $(-1)a = -a$.

Proof (continued). It remains to prove (c). Fix $a \in \mathbb{F}$. WTS $(-1)a = -a$. First, we have that

$$0 \stackrel{(*)}{=} 0a = (1-1)a = 1a + (-1)a = a + (-1)a,$$

where (*) follows from (a). Consequently,

$$\begin{aligned}
-a &= -a + 0 && \text{because 0 is the additive identity of the field } \mathbb{F} \\
&= -a + (a + (-1)a) && \text{because } 0 = a + (-1)a \text{ (proven above)} \\
&= (-a + a) + (-1)a && \text{because } + \text{ is associative} \\
&= 0 + (-1)a && \text{because } -a \text{ is the additive inverse of } a \\
&= (-1)a && \text{because 0 is the additive identity of the field } \mathbb{F}.
\end{aligned}$$

This proves (c). $\square$

Proposition 2.4.2

Let $(\mathbb{F}, +, \cdot)$ be a field. Then all the following hold:

(a) for all $a \in \mathbb{F}$, $0a = a0 = 0$;

(b) for all $a, b \in \mathbb{F}$, if $ab = 0$, then $a = 0$ or $b = 0$;

(c) for all $a \in \mathbb{F}$, $(-1)a = -a$.

- We now consider **finite** fields.

- We now consider **finite** fields.
- As we shall see, for all **prime** numbers p, $\mathbb{Z}_p$ is a field.
  - However, for positive integers n that are not prime, $(\mathbb{Z}_n, +, \cdot)$ is **not** a field.

- We now consider **finite** fields.
- As we shall see, for all **prime** numbers p, $\mathbb{Z}_p$ is a field.
  - However, for positive integers n that are not prime, $(\mathbb{Z}_n, +, \cdot)$ is **not** a field.
- To prove this, we will need Fermat's Little Theorem.

- We now consider **finite** fields.
- As we shall see, for all **prime** numbers p, $\mathbb{Z}_p$ is a field.
  - However, for positive integers n that are not prime, $(\mathbb{Z}_n, +, \cdot)$ is **not** a field.
- To prove this, we will need 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 **finite** fields.
- As we shall see, for all **prime** numbers p, $\mathbb{Z}_p$ is a field.
  - However, for positive integers n that are not prime, $(\mathbb{Z}_n, +, \cdot)$ is **not** a field.
- To prove this, we will need 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 $a^{p-1} = 1$.

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof. By Proposition 0.2.11, addition and multiplication are associative and commutative in $\mathbb{Z}_p$, and multiplication is distributive over addition in $\mathbb{Z}_p$.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof. By Proposition 0.2.11, addition and multiplication are associative and commutative in $\mathbb{Z}_p$, and multiplication is distributive over addition in $\mathbb{Z}_p$. So, $(\mathbb{Z}_p, +, \cdot)$ satisfies axioms 1, 2, and 6 from the definition of a field.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof. By Proposition 0.2.11, addition and multiplication are associative and commutative in $\mathbb{Z}_p$, and multiplication is distributive over addition in $\mathbb{Z}_p$. So, $(\mathbb{Z}_p, +, \cdot)$ satisfies axioms 1, 2, and 6 from the definition of a field.

Further, $0 := [0]_p$ is the additive identity and $1 := [1]_p$ is the multiplicative identity of $(\mathbb{Z}_p, +, \cdot)$.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof. By Proposition 0.2.11, addition and multiplication are associative and commutative in $\mathbb{Z}_p$, and multiplication is distributive over addition in $\mathbb{Z}_p$. So, $(\mathbb{Z}_p, +, \cdot)$ satisfies axioms 1, 2, and 6 from the definition of a field.

Further, $0 := [0]_p$ is the additive identity and $1 := [1]_p$ is the multiplicative identity of $(\mathbb{Z}_p, +, \cdot)$. Moreover, $[0]_p \neq [1]_p$, since $0 \not\equiv 1 \pmod{p}$. Thus, $(\mathbb{Z}_p, +, \cdot)$ satisfies axiom 3 from the definition of a field.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof. By Proposition 0.2.11, addition and multiplication are associative and commutative in $\mathbb{Z}_p$, and multiplication is distributive over addition in $\mathbb{Z}_p$. So, $(\mathbb{Z}_p, +, \cdot)$ satisfies axioms 1, 2, and 6 from the definition of a field.

Further, $0 := [0]_p$ is the additive identity and $1 := [1]_p$ is the multiplicative identity of $(\mathbb{Z}_p, +, \cdot)$. Moreover, $[0]_p \neq [1]_p$, since $0 \not\equiv 1 \pmod{p}$. Thus, $(\mathbb{Z}_p, +, \cdot)$ satisfies axiom 3 from the definition of a field.

Further, for all $a \in \mathbb{Z}$, the additive inverse of $[a]_p$ in $(\mathbb{Z}_p, +, \cdot)$ is $[-a]_p$, and so axiom 4 is satisfied.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof (continued). Finally, by Fermat's Little Theorem, every number $a \in \mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse, namely, a^{p-2}, and it follows that axiom 5 is satisfied.

Fermat's Little Theorem

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

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Proof (continued). Finally, by Fermat's Little Theorem, every number $a \in \mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse, namely, a^{p-2}, and it follows that axiom 5 is satisfied.

This proves that $(\mathbb{Z}_p, +, \cdot)$ is indeed a field, which is what we needed to show. $\square$

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

- **Remark:** For a positive integer n that is **not** prime, $(\mathbb{Z}_n, +, \cdot)$ is not a field.

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

- **Remark:** For a positive integer n that is **not** prime, $(\mathbb{Z}_n, +, \cdot)$ is not a field.
    - If $n = 1$, then this follows from the fact that $\mathbb{Z}_n = \mathbb{Z}_1$ has only one element, whereas every field has at least two elements (namely, the additive and multiplicative identities, which cannot be equal by axiom 3 of the definition of a field).

Theorem 2.4.3

For every **prime** number p, $(\mathbb{Z}_p, +, \cdot)$ is a field.

- **Remark:** For a positive integer n that is **not** prime, $(\mathbb{Z}_n, +, \cdot)$ is not a field.
    - If $n = 1$, then this follows from the fact that $\mathbb{Z}_n = \mathbb{Z}_1$ has only one element, whereas every field has at least two elements (namely, the additive and multiplicative identities, which cannot be equal by axiom 3 of the definition of a field).
    - Now, let us suppose that $n \geq 2$ is composite, say $n = pq$ where $p, q \geq 2$ are integers. Then $[p]_n[q]_n = [pq]_n = [n]_n = 0$. So, if $(\mathbb{Z}_n, +, \cdot)$ were a field, Proposition 2.4.2(b) would imply that at least one of $[p]_n$ and $[q]_n$ is 0, a contradiction.

Theorem 2.4.4

Let $n \geq 2$ be an integer. Then there exists a field of size n iff n is a power of a prime.[a] Moreover, if n is a power of a prime, then up to "isomorphism" (i.e. up to renaming the operations and elements of the field), there is exactly one field of size n, and it is denoted by $\mathbb{F}_n$.[b]

[a] "n is a power of a prime" means that there exists some prime number p and a positive integer m s.t. $n = p^m$.

[b] Technically, the field is $(\mathbb{F}_n, +, \cdot)$, but we typically write just $\mathbb{F}_n$.

Proof. Omitted.

Theorem 2.4.4

Let $n \geq 2$ be an integer. Then there exists a field of size n iff n is a power of a prime.[a] Moreover, if n is a power of a prime, then up to "isomorphism" (i.e. up to renaming the operations and elements of the field), there is exactly one field of size n, and it is denoted by $\mathbb{F}_n$.[b]

---

[a] "n is a power of a prime" means that there exists some prime number p and a positive integer m s.t. $n = p^m$.

[b] Technically, the field is $(\mathbb{F}_n, +, \cdot)$, but we typically write just $\mathbb{F}_n$.

Proof. Omitted.

- **Remark:** For a prime number p, we have that $\mathbb{F}_p = \mathbb{Z}_p$.

Theorem 2.4.4

Let $n \geq 2$ be an integer. Then there exists a field of size n iff n is a power of a prime.[a] Moreover, if n is a power of a prime, then up to "isomorphism" (i.e. up to renaming the operations and elements of the field), there is exactly one field of size n, and it is denoted by $\mathbb{F}_n$.[b]

---

[a] "n is a power of a prime" means that there exists some prime number p and a positive integer m s.t. $n = p^m$.

[b] Technically, the field is $(\mathbb{F}_n, +, \cdot)$, but we typically write just $\mathbb{F}_n$.

Proof. Omitted.

- **Remark:** For a prime number p, we have that $\mathbb{F}_p = \mathbb{Z}_p$.
  - However, if $n = p^m$, where p is a prime number and $m \geq 2$ is an integer, then $\mathbb{F}_n \neq \mathbb{Z}_n$ (this is because $\mathbb{F}_n$ is a field, but $\mathbb{Z}_n$ is **not** a field).

- Let $\mathbb{F}$ be a field. For $a \in \mathbb{F} \setminus \{0\}$, we sometimes use the notation $\frac{1}{a}$ instead of a^{-1} (the multiplicative inverse of a in the field $\mathbb{F}$).

- Let $\mathbb{F}$ be a field. For $a \in \mathbb{F} \setminus \{0\}$, we sometimes use the notation $\frac{1}{a}$ instead of a^{-1} (the multiplicative inverse of a in the field $\mathbb{F}$).
    - For instance, in $\mathbb{Z}_3$, we have $\frac{1}{1} = 1^{-1} = 1$ and $\frac{1}{2} = 2^{-1} = 2$ (because in $\mathbb{Z}_3$, we have that $2 \cdot 2 = 1$).

- Let $\mathbb{F}$ be a field. For $a \in \mathbb{F} \setminus \{0\}$, we sometimes use the notation $\frac{1}{a}$ instead of a^{-1} (the multiplicative inverse of a in the field $\mathbb{F}$).
  - For instance, in $\mathbb{Z}_3$, we have $\frac{1}{1} = 1^{-1} = 1$ and $\frac{1}{2} = 2^{-1} = 2$ (because in $\mathbb{Z}_3$, we have that $2 \cdot 2 = 1$).
- In a similar vein, for scalars $a, b \in \mathbb{F}$ s.t. $b \neq 0$, we sometimes write $\frac{a}{b}$ instead of $b^{-1}a$.

- Let $\mathbb{F}$ be a field. For $a \in \mathbb{F} \setminus \{0\}$, we sometimes use the notation $\frac{1}{a}$ instead of a^{-1} (the multiplicative inverse of a in the field $\mathbb{F}$).
    - For instance, in $\mathbb{Z}_3$, we have $\frac{1}{1} = 1^{-1} = 1$ and $\frac{1}{2} = 2^{-1} = 2$ (because in $\mathbb{Z}_3$, we have that $2 \cdot 2 = 1$).
- In a similar vein, for scalars $a, b \in \mathbb{F}$ s.t. $b \neq 0$, we sometimes write $\frac{a}{b}$ instead of $b^{-1}a$.
    - For example, in $\mathbb{Z}_5$, we have that $3^{-1} = 2$ (because $3 \cdot 2 = 1$), and so $\frac{4}{3} = 3^{-1} \cdot 4 = 2 \cdot 4 = 3$.

- Let $\mathbb{F}$ be a field. For $a \in \mathbb{F} \setminus \{0\}$, we sometimes use the notation $\frac{1}{a}$ instead of a^{-1} (the multiplicative inverse of a in the field $\mathbb{F}$).
    - For instance, in $\mathbb{Z}_3$, we have $\frac{1}{1} = 1^{-1} = 1$ and $\frac{1}{2} = 2^{-1} = 2$ (because in $\mathbb{Z}_3$, we have that $2 \cdot 2 = 1$).
- In a similar vein, for scalars $a, b \in \mathbb{F}$ s.t. $b \neq 0$, we sometimes write $\frac{a}{b}$ instead of $b^{-1}a$.
    - For example, in $\mathbb{Z}_5$, we have that $3^{-1} = 2$ (because $3 \cdot 2 = 1$), and so $\frac{4}{3} = 3^{-1} \cdot 4 = 2 \cdot 4 = 3$.
- It is sometimes more convenient to use the notation $\frac{1}{a}$ instead of a^{-1}, and $\frac{a}{b}$ instead of $b^{-1}a$.

- Let $\mathbb{F}$ be a field. For $a \in \mathbb{F} \setminus \{0\}$, we sometimes use the notation $\frac{1}{a}$ instead of a^{-1} (the multiplicative inverse of a in the field $\mathbb{F}$).
    - For instance, in $\mathbb{Z}_3$, we have $\frac{1}{1} = 1^{-1} = 1$ and $\frac{1}{2} = 2^{-1} = 2$ (because in $\mathbb{Z}_3$, we have that $2 \cdot 2 = 1$).
- In a similar vein, for scalars $a, b \in \mathbb{F}$ s.t. $b \neq 0$, we sometimes write $\frac{a}{b}$ instead of $b^{-1}a$.
    - For example, in $\mathbb{Z}_5$, we have that $3^{-1} = 2$ (because $3 \cdot 2 = 1$), and so $\frac{4}{3} = 3^{-1} \cdot 4 = 2 \cdot 4 = 3$.
- It is sometimes more convenient to use the notation $\frac{1}{a}$ instead of a^{-1}, and $\frac{a}{b}$ instead of $b^{-1}a$.
- However, when working over a finite field such as $\mathbb{Z}_p$ (for a prime number p), we **never** leave a fraction as a final answer, and instead, we always simplify.

Definition

The *characteristic* of a field $\mathbb{F}$ is the smallest positive integer n (if it exists) s.t. in the field $\mathbb{F}$, we have that

$$\underbrace{1 + \cdots + 1}_{n} \;=\; 0,$$

where the 1's and the 0 are understood to be in the field $\mathbb{F}$. If no such n exists, then $\text{char}(\mathbb{F}) := 0$.

Definition

The *characteristic* of a field $\mathbb{F}$ is the smallest positive integer n (if it exists) s.t. in the field $\mathbb{F}$, we have that

$$\underbrace{1 + \cdots + 1}_{n} \;=\; 0,$$

where the 1's and the 0 are understood to be in the field $\mathbb{F}$. If no such n exists, then $\mathrm{char}(\mathbb{F}) := 0$.

- Note that fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all have characteristic 0.

Definition

The *characteristic* of a field $\mathbb{F}$ is the smallest positive integer n (if it exists) s.t. in the field $\mathbb{F}$, we have that

$$\underbrace{1 + \cdots + 1}_{n} \quad = \quad 0,$$

where the 1's and the 0 are understood to be in the field $\mathbb{F}$. If no such n exists, then $\text{char}(\mathbb{F}) := 0$.

- Note that fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all have characteristic 0.
- On the other hand, for all prime numbers p, we have that $\text{char}(\mathbb{Z}_p) = p$.

Definition

The *characteristic* of a field $\mathbb{F}$ is the smallest positive integer n (if it exists) s.t. in the field $\mathbb{F}$, we have that

$$\underbrace{1 + \cdots + 1}_{n} \;=\; 0,$$

where the 1's and the 0 are understood to be in the field $\mathbb{F}$. If no such n exists, then $\mathrm{char}(\mathbb{F}) := 0$.

- Note that fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all have characteristic 0.
- On the other hand, for all prime numbers p, we have that $\mathrm{char}(\mathbb{Z}_p) = p$.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field. We may assume that $\mathrm{char}(\mathbb{F}) \neq 0$, for otherwise we are done.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field. We may assume that $\text{char}(\mathbb{F}) \neq 0$, for otherwise we are done. So, $\text{char}(\mathbb{F})$ is a positive integer.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field. We may assume that $\mathrm{char}(\mathbb{F}) \neq 0$, for otherwise we are done. So, $\mathrm{char}(\mathbb{F})$ is a positive integer.

By the definition of a field, we have that $1 \neq 0$, and so $\mathrm{char}(\mathbb{F}) \geq 2$.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field. We may assume that $\text{char}(\mathbb{F}) \neq 0$, for otherwise we are done. So, $\text{char}(\mathbb{F})$ is a positive integer.

By the definition of a field, we have that $1 \neq 0$, and so $\text{char}(\mathbb{F}) \geq 2$. Now, suppose that $\text{char}(\mathbb{F})$ is not prime, and fix integers $p, q \geq 2$ s.t. $\text{char}(\mathbb{F}) = pq$.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field. We may assume that $\text{char}(\mathbb{F}) \neq 0$, for otherwise we are done. So, $\text{char}(\mathbb{F})$ is a positive integer.

By the definition of a field, we have that $1 \neq 0$, and so $\text{char}(\mathbb{F}) \geq 2$. Now, suppose that $\text{char}(\mathbb{F})$ is not prime, and fix integers $p, q \geq 2$ s.t. $\text{char}(\mathbb{F}) = pq$. Then

$$\Big(\underbrace{1 + \cdots + 1}_{p}\Big)\Big(\underbrace{1 + \cdots + 1}_{q}\Big) \;=\; \underbrace{1 + \cdots + 1}_{pq} \;=\; 0.$$

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field. We may assume that $\text{char}(\mathbb{F}) \neq 0$, for otherwise we are done. So, $\text{char}(\mathbb{F})$ is a positive integer.

By the definition of a field, we have that $1 \neq 0$, and so $\text{char}(\mathbb{F}) \geq 2$. Now, suppose that $\text{char}(\mathbb{F})$ is not prime, and fix integers $p, q \geq 2$ s.t. $\text{char}(\mathbb{F}) = pq$. Then

$$\Big(\underbrace{1+\cdots+1}_{p}\Big)\Big(\underbrace{1+\cdots+1}_{q}\Big) \;=\; \underbrace{1+\cdots+1}_{pq} \;=\; 0.$$

Since $\mathbb{F}$ is a field, Proposition 2.4.2(b) guarantees that at least one of the numbers $\underbrace{1+\cdots+1}_{p}$ and $\underbrace{1+\cdots+1}_{q}$ is zero.

Theorem 2.4.5

The characteristic of any field is either 0 or a prime number.

Proof. Let $\mathbb{F}$ be a field. We may assume that $\text{char}(\mathbb{F}) \neq 0$, for otherwise we are done. So, $\text{char}(\mathbb{F})$ is a positive integer.

By the definition of a field, we have that $1 \neq 0$, and so $\text{char}(\mathbb{F}) \geq 2$. Now, suppose that $\text{char}(\mathbb{F})$ is not prime, and fix integers $p, q \geq 2$ s.t. $\text{char}(\mathbb{F}) = pq$. Then

$$\Big(\underbrace{1+\dots+1}_{p}\Big)\Big(\underbrace{1+\dots+1}_{q}\Big) \;=\; \underbrace{1+\dots+1}_{pq} \;=\; 0.$$

Since $\mathbb{F}$ is a field, Proposition 2.4.2(b) guarantees that at least one of the numbers $\underbrace{1+\dots+1}_{p}$ and $\underbrace{1+\dots+1}_{q}$ is zero. But this is impossible since $0 < p, q < \text{char}(\mathbb{F})$. $\square$