Permutation groups

GU4041, fall 2023

Columbia University

October 22, 2023

Outline

Permutations

By a *permutation* of the set S, we mean a bijective function $\sigma : S \to S$. This definition will only be used when S is a finite set.

Let $n \in \mathbb{N}$. The *symmetric group on n letters* is the group of all permutations of the set $\{1, 2, \ldots, n\}$. (The terminology is classical; the "letters" are in fact numbers, although they could be any objects whatsoever.)

It is well known that there are $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (3) \cdot (2) \cdot (1)$ permutations of a collection $X = \{x_0, \ldots, x_{n-1}\}$ of n elements.

Here is the argument: let σ be a permutation of X. There are n choices for $\sigma(x_0)$. Then $\sigma(x_1) \in X \setminus \{\sigma(x_0)\}$, which has $n-1$ elements. Similarly, at the ith stage, there are $n-i$ choices for $\sigma(x_i)$. Thus the total number of choices is precisely $n!$.

Permutations

By a *permutation* of the set S, we mean a bijective function $\sigma : S \to S$. This definition will only be used when S is a finite set.

Let $n \in \mathbb{N}$. The *symmetric group on n letters* is the group of all permutations of the set $\{1, 2, \ldots, n\}$. (The terminology is classical; the "letters" are in fact numbers, although they could be any objects whatsoever.)

It is well known that there are $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (3) \cdot (2) \cdot (1)$ permutations of a collection $X = \{x_0, \ldots, x_{n-1}\}$ of n elements.

Here is the argument: let σ be a permutation of X. There are n choices for $\sigma(x_0)$. Then $\sigma(x_1) \in X \setminus \{\sigma(x_0)\}$, which has $n-1$ elements. Similarly, at the ith stage, there are $n-i$ choices for $\sigma(x_i)$. Thus the total number of choices is precisely $n!$.

Permutations

By a *permutation* of the set S, we mean a bijective function $\sigma : S \to S$. This definition will only be used when S is a finite set.
Let $n \in \mathbb{N}$. The *symmetric group on n letters* is the group of all permutations of the set $\{1, 2, \ldots, n\}$. (The terminology is classical; the "letters" are in fact numbers, although they could be any objects whatsoever.)
It is well known that there are $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (3) \cdot (2) \cdot (1)$ permutations of a collection $X = \{x_0, \ldots, x_{n-1}\}$ of n elements.
Here is the argument: let σ be a permutation of X. There are n choices for $\sigma(x_0)$. Then $\sigma(x_1) \in X \setminus \{\sigma(x_0)\}$, which has $n-1$ elements. Similarly, at the ith stage, there are $n-i$ choices for $\sigma(x_i)$. Thus the total number of choices is precisely $n!$.

Permutations

By a *permutation* of the set S, we mean a bijective function $\sigma : S \to S$. This definition will only be used when S is a finite set.

Let $n \in \mathbb{N}$. The *symmetric group on n letters* is the group of all permutations of the set $\{1, 2, \ldots, n\}$. (The terminology is classical; the "letters" are in fact numbers, although they could be any objects whatsoever.)

It is well known that there are $n! = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (3) \cdot (2) \cdot (1)$ permutations of a collection $X = \{x_0, \ldots, x_{n-1}\}$ of n elements.

Here is the argument: let σ be a permutation of X. There are n choices for $\sigma(x_0)$. Then $\sigma(x_1) \in X \setminus \{\sigma(x_0)\}$, which has $n-1$ elements. Similarly, at the ith stage, there are $n-i$ choices for $\sigma(x_i)$. Thus the total number of choices is precisely $n!$.

Notation for permutations

We see that the symmetric group has $n!$ elements. However, it is denoted S_n – or $\mathfrak{S}_n$, if we want to be old-fashioned. This is the only exception to our rule that a group denoted H_m has m elements.

An element $\sigma \in S_n$ is traditionally denoted by a matrix with n columns and 2 rows, where the top row is always $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \end{pmatrix}$, and the second row shows the effect of the permutation, like this:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Thus if $n = 4$, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Notation for permutations

We see that the symmetric group has $n!$ elements. However, it is denoted S_n – or $\mathfrak{S}_n$, if we want to be old-fashioned. This is the only exception to our rule that a group denoted H_m has m elements.

An element $\sigma \in S_n$ is traditionally denoted by a matrix with n columns and 2 rows, where the top row is always $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \end{pmatrix}$, and the second row shows the effect of the permutation, like this:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Thus if $n = 4$, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

Notation for permutations

We see that the symmetric group has $n!$ elements. However, it is denoted S_n – or $\mathfrak{S}_n$, if we want to be old-fashioned. This is the only exception to our rule that a group denoted H_m has m elements.

An element $\sigma \in S_n$ is traditionally denoted by a matrix with n columns and 2 rows, where the top row is always $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \end{pmatrix}$, and the second row shows the effect of the permutation, like this:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Thus if $n = 4$, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

A cycle

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

takes 1 to 2, 2 to 4, 3 to 1, and 4 to 3.

Another way to represent this permutation is

$$1 \to 2 \to 4 \to 3 \to 1,$$

but this notation only works if all the numbers are in a single cycle. This leads to the introduction of *cycle* notation. The above cycle is written

$$\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$$

This is a 4-*cycle* because it has to be repeated 4 times to return to the initial state.

A cycle

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

takes 1 to 2, 2 to 4, 3 to 1, and 4 to 3.
Another way to represent this permutation is

$$1 \to 2 \to 4 \to 3 \to 1,$$

but this notation only works if all the numbers are in a single cycle.
This leads to the introduction of *cycle* notation. The above cycle is written

$$\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$$

This is a 4-*cycle* because it has to be repeated 4 times to return to the initial state.

A cycle

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

takes 1 to 2, 2 to 4, 3 to 1, and 4 to 3.
Another way to represent this permutation is

$$1 \to 2 \to 4 \to 3 \to 1,$$

but this notation only works if all the numbers are in a single cycle. This leads to the introduction of *cycle* notation. The above cycle is written

$$\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$$

This is a 4-*cycle* because it has to be repeated 4 times to return to the initial state.

A cycle

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

takes 1 to 2, 2 to 4, 3 to 1, and 4 to 3.
Another way to represent this permutation is

$$1 \to 2 \to 4 \to 3 \to 1,$$

but this notation only works if all the numbers are in a single cycle. This leads to the introduction of *cycle* notation. The above cycle is written

$$\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$$

This is a 4-*cycle* because it has to be repeated 4 times to return to the initial state.

Some examples

In the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

we observe that $1 \to 3 \to 1$ and $2 \to 4 \to 2$.

So its cycle decomposition is

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$$

IMPORTANT POINT The cycles $\begin{pmatrix} 1 & 3 \end{pmatrix}$ and $\begin{pmatrix} 3 & 1 \end{pmatrix}$ are equal. In fact $\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ can also be written

$$\begin{pmatrix} 2 & 4 & 3 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} 4 & 3 & 1 & 2 \end{pmatrix}$$

Some examples

In the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

we observe that $1 \to 3 \to 1$ and $2 \to 4 \to 2$.
So its cycle decomposition is

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$$

IMPORTANT POINT The cycles $\begin{pmatrix} 1 & 3 \end{pmatrix}$ and $\begin{pmatrix} 3 & 1 \end{pmatrix}$ are equal. In fact $\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ can also be written

$$\begin{pmatrix} 2 & 4 & 3 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} 4 & 3 & 1 & 2 \end{pmatrix}$$

Some examples

In the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

we observe that $1 \to 3 \to 1$ and $2 \to 4 \to 2$.
So its cycle decomposition is

$$\begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}$$

IMPORTANT POINT The cycles $\begin{pmatrix} 1 & 3 \end{pmatrix}$ and $\begin{pmatrix} 3 & 1 \end{pmatrix}$ are equal. In fact $\begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ can also be written

$$\begin{pmatrix} 2 & 4 & 3 & 1 \end{pmatrix}$$

or

$$\begin{pmatrix} 4 & 3 & 1 & 2 \end{pmatrix}$$

Notation that is best read at leisure

Suppose X is the set $\{1, 2, \ldots, n\}$. Let $X^1 \subset X$, with $|X^1| = n_1$.
Suppose $\sigma \in S_n$ is a permutation with the following property: we can label the elements of X^1 $a_1, \ldots, a_{n_1}$ in such a way that

$$\sigma(a_1) = a_2; \sigma(a_2) = a_3; \ldots \sigma(a_i) = a_{i+1} \ldots \sigma(a_{n_1}) = a_1;$$

and $\sigma(a) = a$ if $a \in X \setminus X^1$.
Then σ is said to be a *cycle*, or an n_1-cycle, and can be written

$$\sigma = (a_1\ a_2\ \ldots\ a_{n_1}).$$

Notation that is best read at leisure

Suppose X is the set $\{1, 2, \ldots, n\}$. Let $X^1 \subset X$, with $|X^1| = n_1$. Suppose $\sigma \in S_n$ is a permutation with the following property: we can label the elements of X^1 $a_1, \ldots, a_{n_1}$ in such a way that

$$\sigma(a_1) = a_2; \sigma(a_2) = a_3; \ldots \sigma(a_i) = a_{i+1} \ldots \sigma(a_{n_1}) = a_1;$$

and $\sigma(a) = a$ if $a \in X \setminus X^1$.
Then σ is said to be a *cycle*, or an n_1-cycle, and can be written

$$\sigma = (a_1 \; a_2 \; \ldots \; a_{n_1}).$$

Notation that is best read at leisure

Suppose X is the set $\{1, 2, \dots, n\}$. Let $X^1 \subset X$, with $|X^1| = n_1$.
Suppose $\sigma \in S_n$ is a permutation with the following property: we can label the elements of X^1 $a_1, \dots, a_{n_1}$ in such a way that

$$\sigma(a_1) = a_2; \sigma(a_2) = a_3; \dots \sigma(a_i) = a_{i+1} \dots \sigma(a_{n_1}) = a_1;$$

and $\sigma(a) = a$ if $a \in X \setminus X^1$.
Then σ is said to be a *cycle*, or an n_1-cycle, and can be written

$$\sigma = (a_1\ a_2\ \dots\ a_{n_1}).$$

Theorem best read at leisure

Theorem

Any permutation $\sigma \in S_n$ has a cycle decomposition. Precisely, there is a unique partition $X = X^1 \coprod X^2 \coprod \cdots \coprod X^r$ of X into r disjoint subsets, with $n_j = |X^j|$ and

$$n = n_1 + n_2 + \cdots + n_r,$$

and for each j, an n_j-cycle

$$\sigma_j = (a^j_1 \ a^j_2 \ \ldots \ a^j_{n_j})$$

where $X^j = \{a^j_1, a^j_2, \ldots, a^j_{n_j}\}$, such that

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_r.$$

Another example

If

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

we see

$$1 \to 3 \to 6 \to 2 \to 1; \;\; 4 \to 4; \;\; 5 \to 5$$

So the cycle decomposition is a product of a 4-cycle and two 1-cycles:

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

For simplicity we ALWAYS leave out the 1-cycles and just write

$$\sigma = \begin{pmatrix} 1 & 3 & 6 & 2 \end{pmatrix}$$

Another example

If

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

we see

$$1 \to 3 \to 6 \to 2 \to 1; \;\; 4 \to 4; \;\; 5 \to 5$$

So the cycle decomposition is a product of a 4-cycle and two 1-cycles:

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

For simplicity we ALWAYS leave out the 1-cycles and just write

$$\sigma = \begin{pmatrix} 1 & 3 & 6 & 2 \end{pmatrix}$$

Another example

If

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

we see

$$1 \to 3 \to 6 \to 2 \to 1; \quad 4 \to 4; \quad 5 \to 5$$

So the cycle decomposition is a product of a 4-cycle and two 1-cycles:

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

For simplicity we ALWAYS leave out the 1-cycles and just write

$$\sigma = \begin{pmatrix} 1 & 3 & 6 & 2 \end{pmatrix}$$

Disjoint cycles commute!

For example if

$$\rho = \begin{pmatrix}1 & 4 & 2\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix},$$

we can also write

$$\rho = \begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 4 & 2\end{pmatrix};$$

it doesn't matter how the cycles are ordered.

In the above example,

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

Above we wrote

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \dots \cdot \sigma_r$$

but we could write

$$\sigma = \sigma_{i_1} \cdot \sigma_{i_2} \cdot \dots \cdot \sigma_{i_r}$$

for any reordering (permutation!) of the indices $1, 2, \dots, r$.

Disjoint cycles commute!

For example if

$$\rho = (1 \quad 4 \quad 2)\,(3 \quad 5)\,,$$

we can also write

$$\rho = (3 \quad 5)\,(1 \quad 4 \quad 2)\,;$$

it doesn't matter how the cycles are ordered.
In the above example,

$$\tau = (1 \quad 3)\,(2 \quad 4) = (2 \quad 4)\,(1 \quad 3)\,.$$

Above we wrote

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \dots \cdot \sigma_r$$

but we could write

$$\sigma = \sigma_{i_1} \cdot \sigma_{i_2} \cdot \dots \cdot \sigma_{i_r}$$

for any reordering (permutation!) of the indices $1, 2, \dots, r$.

Disjoint cycles commute!

For example if

$$\rho = \begin{pmatrix}1 & 4 & 2\end{pmatrix}\begin{pmatrix}3 & 5\end{pmatrix},$$

we can also write

$$\rho = \begin{pmatrix}3 & 5\end{pmatrix}\begin{pmatrix}1 & 4 & 2\end{pmatrix};$$

it doesn't matter how the cycles are ordered.

In the above example,

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

Above we wrote

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_r$$

but we could write

$$\sigma = \sigma_{i_1} \cdot \sigma_{i_2} \cdot \cdots \cdot \sigma_{i_r}$$

for any reordering (permutation!) of the indices $1, 2, \ldots, r$.

Orbit of a permutation

Let X be a finite set and σ a permutation of X.
The orbits of σ are the subsets $X^j \in X$ such that,

1. for any $x \neq y \in X^j$, there is an integer $m > 0$ such that $\sigma^m(x) = y$, and
2. if $x \in X^j$ then $\sigma(x) \in X^j$.

In other words, setting $n_j = |X_j|$, for for any $x \in X^j$, $\sigma^{n_j}(x) = x$ and X^j is a set of the form

$$\{x, \sigma(x), \sigma^2(x), \ldots \sigma^{n_j - 1}(x)\}$$

for any $x \in X_j$.

Orbit of a permutation

Let X be a finite set and σ a permutation of X.
The orbits of σ are the subsets $X^j \in X$ such that,

1. for any $x \neq y \in X^j$, there is an integer $m > 0$ such that $\sigma^m(x) = y$, and
2. if $x \in X^j$ then $\sigma(x) \in X^j$.

In other words, setting $n_j = |X_j|$, for for any $x \in X^j$, $\sigma^{n_j}(x) = x$ and X^j is a set of the form

$$\{x, \sigma(x), \sigma^2(x), \ldots \sigma^{n_j-1}(x)\}$$

for any $x \in X_j$.

Orbit of a permutation

Let X be a finite set and σ a permutation of X.
The orbits of σ are the subsets $X^j \in X$ such that,

1. for any $x \neq y \in X^j$, there is an integer $m > 0$ such that $\sigma^m(x) = y$, and
2. if $x \in X^j$ then $\sigma(x) \in X^j$.

In other words, setting $n_j = |X_j|$, for for any $x \in X^j$, $\sigma^{n_j}(x) = x$ and X^j is a set of the form

$$\{x, \sigma(x), \sigma^2(x), \ldots \sigma^{n_j-1}(x)\}$$

for any $x \in X_j$.

Orbit of a permutation

Let X be a finite set and σ a permutation of X.
The orbits of σ are the subsets $X^j \in X$ such that,

1. for any $x \neq y \in X^j$, there is an integer $m > 0$ such that $\sigma^m(x) = y$, and
2. if $x \in X^j$ then $\sigma(x) \in X^j$.

In other words, setting $n_j = |X_j|$, for for any $x \in X^j$, $\sigma^{n_j}(x) = x$ and X^j is a set of the form

$$\{x, \sigma(x), \sigma^2(x), \ldots \sigma^{n_j-1}(x)\}$$

for any $x \in X_j$.

Any permutation defines an equivalence relation

We define a relation on X: we say $xR_\sigma y$ if there exists some $m > 0$ such that $\sigma^m(x) = y$. This is an equivalence relation:

- (reflexive) Since S_n is a finite group, $\sigma^M = e$ for some $M > 0$; then $\sigma^M(x) = x$ for all x.
- (symmetric) If $\sigma^m(x) = y$ then $\sigma^{-m}(y) = x$, but $\sigma^{-m} = \sigma^{M-m} = \sigma^{dM-m}$ for any d, and for d sufficiently large $dM - m > 0$.
- (transitive) If $\sigma^m(x) = y$ and $\sigma^{m'}(y) = z$ then $\sigma^{m+m'}(x) = z$.

The orbits define a partition

Theorem

The equivalence classes for the relation R_σ are precisely the orbits of σ. They define a partition of X.

Proof.

For each j σ induces a permutation σ_j of X^j that ignores the elements of the $X^i, i \neq j$. The word "induces" means: the bijection $\sigma : X \to X$ restricts to a bijection $\sigma_j : X^j \to X^j$.

Then $\sigma = \prod_j \sigma_j$ (in any order).
We check this by looking more closely at the group structure. □

The orbits define a partition

Theorem

The equivalence classes for the relation R_σ are precisely the orbits of σ. They define a partition of X.

Proof.

For each j σ induces a permutation σ_j of X^j that ignores the elements of the $X^i, i \neq j$. The word "induces" means: the bijection $\sigma : X \to X$ restricts to a bijection $\sigma_j : X^j \to X^j$.

Then $\sigma = \prod_j \sigma_j$ (in any order).
We check this by looking more closely at the group structure. □

The orbits define a partition

Theorem

The equivalence classes for the relation R_σ are precisely the orbits of σ. They define a partition of X.

Proof.

For each j σ induces a permutation σ_j of X^j that ignores the elements of the $X^i, i \neq j$. The word "induces" means: the bijection $\sigma : X \to X$ restricts to a bijection $\sigma_j : X^j \to X^j$.

Then $\sigma = \prod_j \sigma_j$ (in any order).
We check this by looking more closely at the group structure. □

The orbits define a partition

Theorem

The equivalence classes for the relation R_σ are precisely the orbits of σ. They define a partition of X.

Proof.

For each j σ induces a permutation σ_j of X^j that ignores the elements of the $X^i, i \neq j$. The word “induces” means: the bijection $\sigma : X \to X$ restricts to a bijection $\sigma_j : X^j \to X^j$.

Then $\sigma = \prod_j \sigma_j$ (in any order).
We check this by looking more closely at the group structure. □

The orbits define a partition

Theorem

The equivalence classes for the relation R_σ are precisely the orbits of σ. They define a partition of X.

Proof.

For each j σ induces a permutation σ_j of X^j that ignores the elements of the $X^i, i \neq j$. The word "induces" means: the bijection $\sigma : X \to X$ restricts to a bijection $\sigma_j : X^j \to X^j$.

Then $\sigma = \prod_j \sigma_j$ (in any order).
We check this by looking more closely at the group structure. □

The group structure

The product of the permutations $\sigma \cdot \tau$ is: first apply τ, then apply σ.
In other words: Then $\sigma \cdot \tau$ is the permutation in S_n, with the property that, for any $i \in \{1, 2, \ldots, n\}$

$$\sigma \cdot \tau(i) = \sigma(\tau(i)).$$

In other words, multiplication in S_n is just composition of (bijective) functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$: $\sigma \cdot \tau = \sigma \circ \tau$. This is associative:

$$\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho.$$

Since any $\sigma \in S_n$ is bijective, it has an inverse σ^{-1}. And of course the identity is the permutation that doesn't move anything.
So S_n is indeed a group.

The group structure

The product of the permutations $\sigma \cdot \tau$ is: first apply τ, then apply σ. In other words: Then $\sigma \cdot \tau$ is the permutation in S_n, with the property that, for any $i \in \{1, 2, \ldots, n\}$

$$\sigma \cdot \tau(i) = \sigma(\tau(i)).$$

In other words, multiplication in S_n is just composition of (bijective) functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$: $\sigma \cdot \tau = \sigma \circ \tau$. This is associative:

$$\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho.$$

Since any $\sigma \in S_n$ is bijective, it has an inverse σ^{-1}. And of course the identity is the permutation that doesn't move anything.
So S_n is indeed a group.

The group structure

The product of the permutations $\sigma \cdot \tau$ is: first apply τ, then apply σ. In other words: Then $\sigma \cdot \tau$ is the permutation in S_n, with the property that, for any $i \in \{1, 2, \ldots, n\}$

$$\sigma \cdot \tau(i) = \sigma(\tau(i)).$$

In other words, multiplication in S_n is just composition of (bijective) functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$: $\sigma \cdot \tau = \sigma \circ \tau$. This is associative:

$$\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho.$$

Since any $\sigma \in S_n$ is bijective, it has an inverse σ^{-1}. And of course the identity is the permutation that doesn't move anything.
So S_n is indeed a group.

The group structure

The product of the permutations $\sigma \cdot \tau$ is: first apply τ, then apply σ. In other words: Then $\sigma \cdot \tau$ is the permutation in S_n, with the property that, for any $i \in \{1, 2, \ldots, n\}$

$$\sigma \cdot \tau(i) = \sigma(\tau(i)).$$

In other words, multiplication in S_n is just composition of (bijective) functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$: $\sigma \cdot \tau = \sigma \circ \tau$. This is associative:

$$\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho.$$

Since any $\sigma \in S_n$ is bijective, it has an inverse σ^{-1}. And of course the identity is the permutation that doesn't move anything.
So S_n is indeed a group.

The group structure

The product of the permutations $\sigma \cdot \tau$ is: first apply τ, then apply σ. In other words: Then $\sigma \cdot \tau$ is the permutation in S_n, with the property that, for any $i \in \{1, 2, \ldots, n\}$

$$\sigma \cdot \tau(i) = \sigma(\tau(i)).$$

In other words, multiplication in S_n is just composition of (bijective) functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$: $\sigma \cdot \tau = \sigma \circ \tau$. This is associative:

$$\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho.$$

Since any $\sigma \in S_n$ is bijective, it has an inverse σ^{-1}. And of course the identity is the permutation that doesn't move anything.

So S_n is indeed a group.

The group structure

The product of the permutations $\sigma \cdot \tau$ is: first apply τ, then apply σ.
In other words: Then $\sigma \cdot \tau$ is the permutation in S_n, with the property that, for any $i \in \{1, 2, \ldots, n\}$

$$\sigma \cdot \tau(i) = \sigma(\tau(i)).$$

In other words, multiplication in S_n is just composition of (bijective) functions from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$: $\sigma \cdot \tau = \sigma \circ \tau$. This is associative:

$$\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho.$$

Since any $\sigma \in S_n$ is bijective, it has an inverse σ^{-1}. And of course the identity is the permutation that doesn't move anything.
So S_n is indeed a group.

Matrix notation is bad for writing the inverse

If

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

then obviously you get σ^{-1} by exchanging the two rows:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 6 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

But just as obviously this is not written in standard form: you have to move the columns around:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Matrix notation is bad for writing the inverse

If

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

then obviously you get σ^{-1} by exchanging the two rows:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 6 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

But just as obviously this is not written in standard form: you have to move the columns around:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Matrix notation is bad for writing the inverse

If

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

then obviously you get σ^{-1} by exchanging the two rows:

$$\sigma^{-1} = \begin{pmatrix} 3 & 1 & 6 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

But just as obviously this is not written in standard form: you have to move the columns around:

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Matrix notation is even worse for multiplication

The simplest way to show this is to illustrate it with an example.

Suppose $n = 4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix};$$

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

We compute: $\sigma \cdot \tau(1) = \sigma(\tau(1)) = \sigma(4) = 3$. Similarly, $\sigma \cdot \tau(2) = \sigma(1) = 2$; $\sigma \cdot \tau(3) = \sigma(3) = 1$; and $\sigma \cdot \tau(4) = \sigma(2) = 4$.

Thus

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Matrix notation is even worse for multiplication

The simplest way to show this is to illustrate it with an example. Suppose $n = 4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix};$$

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

We compute: $\sigma \cdot \tau(1) = \sigma(\tau(1)) = \sigma(4) = 3$. Similarly, $\sigma \cdot \tau(2) = \sigma(1) = 2$; $\sigma \cdot \tau(3) = \sigma(3) = 1$; and $\sigma \cdot \tau(4) = \sigma(2) = 4$.

Thus

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Matrix notation is even worse for multiplication

The simplest way to show this is to illustrate it with an example. Suppose $n = 4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix};$$

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

We compute: $\sigma \cdot \tau(1) = \sigma(\tau(1)) = \sigma(4) = 3$. Similarly, $\sigma \cdot \tau(2) = \sigma(1) = 2$; $\sigma \cdot \tau(3) = \sigma(3) = 1$; and $\sigma \cdot \tau(4) = \sigma(2) = 4$.

Thus

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Matrix notation is even worse for multiplication

The simplest way to show this is to illustrate it with an example. Suppose $n = 4$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix};$$

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

We compute: $\sigma \cdot \tau(1) = \sigma(\tau(1)) = \sigma(4) = 3$. Similarly, $\sigma \cdot \tau(2) = \sigma(1) = 2$; $\sigma \cdot \tau(3) = \sigma(3) = 1$; and $\sigma \cdot \tau(4) = \sigma(2) = 4$.

Thus

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

It's not easier in cycle notation

We have

$$\sigma = \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}; \ \tau = \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}$$

and

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 3 \end{pmatrix} (= \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix}).$$

Howie's notes also suggests a shortcut for computing σ^{-1} on p. 28. Here the cycle notation can be more helpful.

It's not easier in cycle notation

We have

$$\sigma = \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}; \ \tau = \begin{pmatrix} 1 & 4 & 2 \end{pmatrix}$$

and

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 3 \end{pmatrix} (= \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix}).$$

Howie's notes also suggests a shortcut for computing σ^{-1} on p. 28. Here the cycle notation can be more helpful.

An equivalence relation on S_n

We can define an equivalence relation $\sim$ on S_n: two permutations $\sigma, \sigma' \in S_n$ satisfy $\sigma \sim \sigma'$ if and only if their cycle decompositions have the same lengths.

Theorem

Suppose $\sigma, \sigma' \in S_n$ both have cycle decompositions with partition $n = n_1 + n_2 + \cdots + n_r$. Then there exists $\lambda \in S_n$ such that

$$\sigma' = \lambda \sigma \lambda^{-1}.$$

Thus the set S_n has a partition according to the shape of the cycle decomposition.

The relation $\sigma' = \lambda \sigma \lambda^{-1}$ is called *conjugacy*.

An equivalence relation on S_n

We can define an equivalence relation $\sim$ on S_n: two permutations $\sigma, \sigma' \in S_n$ satisfy $\sigma \sim \sigma'$ if and only if their cycle decompositions have the same lengths.

Theorem

Suppose $\sigma, \sigma' \in S_n$ both have cycle decompositions with partition $n = n_1 + n_2 + \cdots + n_r$. Then there exists $\lambda \in S_n$ such that

$$\sigma' = \lambda \sigma \lambda^{-1}.$$

Thus the set S_n has a partition according to the shape of the cycle decomposition.

The relation $\sigma' = \lambda \sigma \lambda^{-1}$ is called *conjugacy*.

An equivalence relation on S_n

We can define an equivalence relation $\sim$ on S_n: two permutations $\sigma, \sigma' \in S_n$ satisfy $\sigma \sim \sigma'$ if and only if their cycle decompositions have the same lengths.

Theorem

Suppose $\sigma, \sigma' \in S_n$ both have cycle decompositions with partition $n = n_1 + n_2 + \cdots + n_r$. Then there exists $\lambda \in S_n$ such that

$$\sigma' = \lambda\sigma\lambda^{-1}.$$

Thus the set S_n has a partition according to the shape of the cycle decomposition.
The relation $\sigma' = \lambda\sigma\lambda^{-1}$ is called *conjugacy*.

Proof

The proof of the theorem is in the online notes. It will be sketched on the board with an example.

Transpositions

A *transposition* in S_n is a cycle of the form $\tau_{ij} = \begin{pmatrix} i & j \end{pmatrix}$ where $1 \leq i \neq j \leq n$. In other words, τ_{ij} exchanges i and j and leaves the other numbers unchanged. It is a cycle of length 2.

Then obviously $\tau_{ij} \cdot \tau_{ij}$ is the identity element e.
We will see later in the course that every $\sigma \in S_n$ can be written as a product of transpositions.

This product expression is not unique – for example, the identity element e can be written $\tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij}$ and in infinitely many other ways – it suffices to keep adding pairs of τ_{ij}.

What is unique, however, is the *sign* of σ.

Transpositions

A *transposition* in S_n is a cycle of the form $\tau_{ij} = \begin{pmatrix} i & j \end{pmatrix}$ where $1 \leq i \neq j \leq n$. In other words, τ_{ij} exchanges i and j and leaves the other numbers unchanged. It is a cycle of length 2.

Then obviously $\tau_{ij} \cdot \tau_{ij}$ is the identity element e.
We will see later in the course that every $\sigma \in S_n$ can be written as a product of transpositions.

This product expression is not unique – for example, the identity element e can be written $\tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij}$ and in infinitely many other ways – it suffices to keep adding pairs of τ_{ij}.

What is unique, however, is the *sign* of σ.

Transpositions

A *transposition* in S_n is a cycle of the form $\tau_{ij} = \begin{pmatrix} i & j \end{pmatrix}$ where $1 \leq i \neq j \leq n$. In other words, τ_{ij} exchanges i and j and leaves the other numbers unchanged. It is a cycle of length 2.

Then obviously $\tau_{ij} \cdot \tau_{ij}$ is the identity element e.
We will see later in the course that every $\sigma \in S_n$ can be written as a product of transpositions.

This product expression is not unique – for example, the identity element e can be written $\tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij}$ and in infinitely many other ways – it suffices to keep adding pairs of τ_{ij}.

What is unique, however, is the *sign* of σ.

Transpositions

A *transposition* in S_n is a cycle of the form $\tau_{ij} = \begin{pmatrix} i & j \end{pmatrix}$ where $1 \leq i \neq j \leq n$. In other words, τ_{ij} exchanges i and j and leaves the other numbers unchanged. It is a cycle of length 2.

Then obviously $\tau_{ij} \cdot \tau_{ij}$ is the identity element e.
We will see later in the course that every $\sigma \in S_n$ can be written as a product of transpositions.

This product expression is not unique – for example, the identity element e can be written $\tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij} \cdot \tau_{ij}$ and in infinitely many other ways – it suffices to keep adding pairs of τ_{ij}.

What is unique, however, is the *sign* of σ.

Sign of a transposition

Theorem

If σ can be written in one way as a product of an even number of transpositions, then every such expression for σ has an even number of transpositions.

It follows that if σ can be written in one way as an odd number of transpositions then *every* such expression for σ has an odd number of transpositions.

We define the sign of σ, denoted $sgn(\sigma)$ to be 1 if it can be written as a product of an even number of transpositions, and -1 if it can be written as a product of an odd number of transpositions.

In particular $sgn(\tau_{ij}) = -1$ for any $i \neq j$.

Sign of a transposition

Theorem

If σ can be written in one way as a product of an even number of transpositions, then every such expression for σ has an even number of transpositions.

It follows that if σ can be written in one way as an odd number of transpositions then *every* such expression for σ has an odd number of transpositions.

We define the sign of σ, denoted $sgn(\sigma)$ to be 1 if it can be written as a product of an even number of transpositions, and -1 if it can be written as a product of an odd number of transpositions.

In particular $sgn(\tau_{ij}) = -1$ for any $i \neq j$.

Sign of a transposition

Theorem

If σ can be written in one way as a product of an even number of transpositions, then every such expression for σ has an even number of transpositions.

It follows that if σ can be written in one way as an odd number of transpositions then *every* such expression for σ has an odd number of transpositions.
We define the sign of σ, denoted $sgn(\sigma)$ to be 1 if it can be written as a product of an even number of transpositions, and -1 if it can be written as a product of an odd number of transpositions.
In particular $sgn(\tau_{ij}) = -1$ for any $i \neq j$.

Sign of a transposition

Theorem

If σ can be written in one way as a product of an even number of transpositions, then every such expression for σ has an even number of transpositions.

It follows that if σ can be written in one way as an odd number of transpositions then *every* such expression for σ has an odd number of transpositions.
We define the sign of σ, denoted $sgn(\sigma)$ to be 1 if it can be written as a product of an even number of transpositions, and -1 if it can be written as a product of an odd number of transpositions.
In particular $sgn(\tau_{ij}) = -1$ for any $i \neq j$.

Adjacent transpositions

We say τ_{ij} is an adjacent transposition if $j = i + 1$. It can be shown that every $\sigma \in S_n$ can be written as a product of adjacent transpositions.

The *length* of σ is then the shortest expression of σ as a product of adjacent transpositions. We will not be discussing length in this course.

Adjacent transpositions

We say τ_{ij} is an adjacent transposition if $j = i + 1$. It can be shown that every $\sigma \in S_n$ can be written as a product of adjacent transpositions.

The *length* of σ is then the shortest expression of σ as a product of adjacent transpositions. We will not be discussing length in this course.

Factorization in transpositions

Proposition

Any element of S_n can be wntten as the product of transpositions.

Proof: Suppose σ has a cycle decomposition

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_r$$

with σ_i a k_i-cycle. It suffices to check that each σ_i can be written as the product of transpositions. So we may assume σ is itself a k-cycle:

$$\sigma = (a_1 \ \ldots \ a_k) \, .$$

We induct on k, clearly all right if $k \leq 2$. So we assume $k > 2$.

Factorization in transpositions

Proposition

Any element of S_n can be wntten as the product of transpositions.

Proof: Suppose σ has a cycle decomposition

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \cdots \cdot \sigma_r$$

with σ_i a k_i-cycle. It suffices to check that each σ_i can be written as the product of transpositions. So we may assume σ is itself a k-cycle:

$$\sigma = (a_1 \ \ldots \ a_k) \, .$$

We induct on k, clearly all right if $k \leq 2$. So we assume $k > 2$.

Factorization in transpositions

Proposition

Any element of S_n can be wntten as the product of transpositions.

Proof: Suppose σ has a cycle decomposition

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \dots \cdot \sigma_r$$

with σ_i a k_i-cycle. It suffices to check that each σ_i can be written as the product of transpositions. So we may assume σ is itself a k-cycle:

$$\sigma = (a_1 \ \dots \ a_k) \, .$$

We induct on k, clearly all right if $k \leq 2$. So we assume $k > 2$.

Factorization in transpositions

Proposition

Any element of S_n can be wntten as the product of transpositions.

Proof: Suppose σ has a cycle decomposition

$$\sigma = \sigma_1 \cdot \sigma_2 \cdot \dots \cdot \sigma_r$$

with σ_i a k_i-cycle. It suffices to check that each σ_i can be written as the product of transpositions. So we may assume σ is itself a k-cycle:

$$\sigma = (a_1 \ \dots \ a_k) \, .$$

We induct on k, clearly all right if $k \leq 2$. So we assume $k > 2$.

Factorization in transpositions

Consider

$$\tau_1 = (a_1\ a_2),\ \ \tau_2 = (a_2\ \ldots\ a_k),\ \ \tau = \tau_1 \cdot \tau_2.$$

By induction τ_2 of length $k-1$ is a product of transpositions, and therefore so is τ.

So we want to show $\sigma = \tau$. But $\tau(a_1) = \tau_1(a_1) = a_2$,

$$3 \leq i \leq k-1 \Rightarrow \tau(a_i) = \tau_2(a_i) = a_{i+1}.$$

$$\tau(a_2) = \tau_1(\tau_2(a_2)) = \tau_1(a_3) = a_3.$$

$$\tau(a_k) = \tau_1(\tau_2(a_k)) = \tau_1(a_2) = a_1.$$

Thus $\sigma = \tau$ and we conclude.

Factorization in transpositions

Consider

$$\tau_1 = (a_1\ a_2),\ \ \tau_2 = (a_2\ \ldots\ a_k),\ \ \tau = \tau_1 \cdot \tau_2.$$

By induction τ_2 of length $k-1$ is a product of transpositions, and therefore so is τ.
So we want to show $\sigma = \tau$. But $\tau(a_1) = \tau_1(a_1) = a_2$,

$$3 \leq i \leq k-1 \Rightarrow \tau(a_i) = \tau_2(a_i) = a_{i+1}.$$

$$\tau(a_2) = \tau_1(\tau_2(a_2)) = \tau_1(a_3) = a_3.$$

$$\tau(a_k) = \tau_1(\tau_2(a_k)) = \tau_1(a_2) = a_1.$$

Thus $\sigma = \tau$ and we conclude.

Factorization in transpositions

Consider

$$\tau_1 = (a_1\ a_2),\ \ \tau_2 = (a_2\ \ldots\ a_k),\ \ \tau = \tau_1 \cdot \tau_2.$$

By induction τ_2 of length $k-1$ is a product of transpositions, and therefore so is τ.
So we want to show $\sigma = \tau$. But $\tau(a_1) = \tau_1(a_1) = a_2$,

$$3 \leq i \leq k-1 \Rightarrow \tau(a_i) = \tau_2(a_i) = a_{i+1}.$$

$$\tau(a_2) = \tau_1(\tau_2(a_2)) = \tau_1(a_3) = a_3.$$
$$\tau(a_k) = \tau_1(\tau_2(a_k)) = \tau_1(a_2) = a_1.$$

Thus $\sigma = \tau$ and we conclude.

Factorization in transpositions

Consider

$$\tau_1 = (a_1\ a_2),\ \ \tau_2 = (a_2\ \dots\ a_k),\ \ \tau = \tau_1 \cdot \tau_2.$$

By induction τ_2 of length $k-1$ is a product of transpositions, and therefore so is τ.
So we want to show $\sigma = \tau$. But $\tau(a_1) = \tau_1(a_1) = a_2$,

$$3 \leq i \leq k-1 \Rightarrow \tau(a_i) = \tau_2(a_i) = a_{i+1}.$$

$$\tau(a_2) = \tau_1(\tau_2(a_2)) = \tau_1(a_3) = a_3.$$
$$\tau(a_k) = \tau_1(\tau_2(a_k)) = \tau_1(a_2) = a_1.$$

Thus $\sigma = \tau$ and we conclude.

The parity is well defined

Unlike the cycle decomposition, the decomposition as a product of transpositions is *not unique*. For example the identity in S_n can be written

$$e = (1\ 2)(1\ 2).$$

But we can restate the theorem:

Theorem

Suppose σ can be written in two different ways as the product

$$\sigma = \tau_1 \cdot \cdots \cdot \tau_k = \alpha_1 \cdot \cdots \cdot \alpha_{k'}$$

where all the τ_i and α_j are transpositions.
Then $k \equiv k' \pmod 2$.

The parity is well defined

Unlike the cycle decomposition, the decomposition as a product of transpositions is *not unique*. For example the identity in S_n can be written

$$e = (1\ 2)(1\ 2).$$

But we can restate the theorem:

Theorem

Suppose σ can be written in two different ways as the product

$$\sigma = \tau_1 \cdot \dots \cdot \tau_k = \alpha_1 \cdot \dots \cdot \alpha_{k'}$$

where all the τ_i and α_j are transpositions.
Then $k \equiv k' \pmod 2$.

The parity is well defined

Unlike the cycle decomposition, the decomposition as a product of transpositions is *not unique*. For example the identity in S_n can be written

$$e = (1\ 2)(1\ 2).$$

But we can restate the theorem:

Theorem

Suppose σ can be written in two different ways as the product

$$\sigma = \tau_1 \cdot \dots \cdot \tau_k = \alpha_1 \cdot \dots \cdot \alpha_{k'}$$

where all the τ_i and α_j are transpositions.
Then $k \equiv k' \pmod 2$.

The sign homomorphism

Corollary

There is a homomorphism

$$sgn : S_n \to \{\pm 1\}$$

$$sgn(\sigma) = (-1)^k$$

if σ is the product of k transpositions.

The kernel of sgn is a subgroup $A_n \subset S_n$ of index 2 called the *alternating group*.

Proof of the theorem, I

Suppose

$$\sigma = \beta_1 \cdot \dots \cdot \beta_k = \alpha_1 \cdot \dots \cdot \alpha_{k'}.$$

Then $e = \prod_{i=1}^{k} \beta_i \cdot [\prod_j \alpha_1 \cdot \dots \cdot \alpha_{k'}]^{-1}$ or

$$e = \beta_1 \cdot \dots \cdot \beta_k \cdot \alpha_{k'}^{-1} \cdot \ldots \alpha_2^{-1} \cdot \alpha_1^{-1}$$

$$e = \beta_1 \cdot \dots \cdot \beta_k \cdot \alpha_{k'} \cdot \ldots \alpha_2^{-1} \cdot \alpha_1$$

because each transposition is its own inverse.
So e is the product of $m = k + k'$ transpositions. It suffices to show that $m = k + k'$ is even.

Proof of the theorem, I

Suppose

$$\sigma = \beta_1 \cdot \cdots \cdot \beta_k = \alpha_1 \cdot \cdots \cdot \alpha_{k'}.$$

Then $e = \prod_{i=1}^{k} \beta_i \cdot [\prod_j \alpha_1 \cdot \cdots \cdot \alpha_{k'}]^{-1}$ or

$$e = \beta_1 \cdot \cdots \cdot \beta_k \cdot \alpha_{k'}^{-1} \cdot \ldots \alpha_2^{-1} \cdot \alpha_1^{-1}$$

$$e = \beta_1 \cdot \cdots \cdot \beta_k \cdot \alpha_{k'} \cdot \ldots \alpha_2^{-1} \cdot \alpha_1$$

because each transposition is its own inverse.
So e is the product of $m = k + k'$ transpositions. It suffices to show that $m = k + k'$ is even.

Proof of the theorem, I

Suppose

$$\sigma = \beta_1 \cdot \cdots \cdot \beta_k = \alpha_1 \cdot \cdots \cdot \alpha_{k'}.$$

Then $e = \prod_{i=1}^{k} \beta_i \cdot [\prod_j \alpha_1 \cdot \cdots \cdot \alpha_{k'}]^{-1}$ or

$$e = \beta_1 \cdot \cdots \cdot \beta_k \cdot \alpha_{k'}^{-1} \cdot \ldots \alpha_2^{-1} \cdot \alpha_1^{-1}$$

$$e = \beta_1 \cdot \cdots \cdot \beta_k \cdot \alpha_{k'} \cdot \ldots \alpha_2^{-1} \cdot \alpha_1$$

because each transposition is its own inverse.

So e is the product of $m = k + k'$ transpositions. It suffices to show that $m = k + k'$ is even.

Proof of the theorem, I

Suppose

$$\sigma = \beta_1 \cdot \dots \cdot \beta_k = \alpha_1 \cdot \dots \cdot \alpha_{k'}.$$

Then $e = \prod_{i=1}^{k} \beta_i \cdot [\prod_j \alpha_1 \cdot \dots \cdot \alpha_{k'}]^{-1}$ or

$$e = \beta_1 \cdot \dots \cdot \beta_k \cdot \alpha_{k'}^{-1} \cdot \dots \alpha_2^{-1} \cdot \alpha_1^{-1}$$

$$e = \beta_1 \cdot \dots \cdot \beta_k \cdot \alpha_{k'} \cdot \dots \alpha_2^{-1} \cdot \alpha_1$$

because each transposition is its own inverse.
So e is the product of $m = k + k'$ transpositions. It suffices to show that $m = k + k'$ is even.

Proof of the theorem, II

The theorem is thus equivalent to

Theorem

Suppose $e \in S_n$ is the product of m transpositions $e = \tau_1 \cdot \cdots \cdot \tau_m$. Then m is even.

The proof is an induction on m. We have

$$e = [\tau_1 \cdot \cdots \cdot \tau_{m-2}]\tau_{m-1} \cdot \tau_m.$$

Proof of the theorem, II

The theorem is thus equivalent to

Theorem

Suppose $e \in S_n$ is the product of m transpositions $e = \tau_1 \cdot \cdots \cdot \tau_m$. Then m is even.

The proof is an induction on m. We have

$$e = [\tau_1 \cdot \cdots \cdot \tau_{m-2}]\tau_{m-1} \cdot \tau_m.$$

Proof of the theorem, III

$$e = [\tau_1 \cdot \cdots \cdot \tau_{m-2}]\tau_{m-1} \cdot \tau_m.$$

There are four possibilities.

1. $\tau_{m-1} = \tau_m = (a\ b)$;
2. $\tau_{m-1} = (c\ d)$, $\tau_m = (a\ b)$ all different.
3. $\tau_{m-1} = (a\ c)$, $\tau_m = (a\ b)$, a, b, c distinct.
4. $\tau_{m-1} = (b\ c)$, $\tau_m = (a\ b)$

Case (1) is easy: $\tau_{m-1} \cdot \tau_m = e$ so $m \equiv m - 2 \pmod 2$ and we conclude by induction. In the other cases we aim to move a to the left until there is no more room.

Proof of the theorem, IV

In case (2) $(c\ d) \cdot (a\ b) = (a\ b) \cdot (c\ d)$.
In case (3) $(a\ c) \cdot (a\ b) = (a\ b) \cdot (b\ c)$. (CHECK!)
In case (4) $(b\ c) \cdot (a\ b) = (a\ c) \cdot (b\ c)$. (CHECK!)
In any case a is in τ_{m-1} and is NOT in τ_m. Now continue with the pair τ_{m-2}, τ_{m-1}. We again have four cases.
We repeat the analysis. After each step a moves to the left and is absent from the subsequent transpositions: either a cancels as in case (1), which concludes by induction, or

$$e = \tau_1 \cdot \ldots (a\ b') \cdot \tau_i \cdot \tau_{i+1} \cdot \cdots \cdot \tau_m$$

for some $b' \neq a$, where a is NOT in $\tau_i, \tau_{i+1}, \ldots \tau_m$.

Proof of the theorem, IV

In case (2) $(c\ d) \cdot (a\ b) = (a\ b) \cdot (c\ d)$.
In case (3) $(a\ c) \cdot (a\ b) = (a\ b) \cdot (b\ c)$. (CHECK!)
In case (4) $(b\ c) \cdot (a\ b) = (a\ c) \cdot (b\ c)$. (CHECK!)
In any case a is in τ_{m-1} and is NOT in τ_m. Now continue with the pair τ_{m-2}, τ_{m-1}. We again have four cases.
We repeat the analysis. After each step a moves to the left and is absent from the subsequent transpositions: either a cancels as in case (1), which concludes by induction, or

$$e = \tau_1 \cdot \ldots (a\ b') \cdot \tau_i \cdot \tau_{i+1} \cdot \cdots \cdot \tau_m$$

for some $b' \neq a$, where a is NOT in $\tau_i, \tau_{i+1}, \ldots \tau_m$.

Proof of the theorem, IV

In case (2) $(c\ d) \cdot (a\ b) = (a\ b) \cdot (c\ d)$.
In case (3) $(a\ c) \cdot (a\ b) = (a\ b) \cdot (b\ c)$. (CHECK!)
In case (4) $(b\ c) \cdot (a\ b) = (a\ c) \cdot (b\ c)$. (CHECK!)
In any case a is in τ_{m-1} and is NOT in τ_m. Now continue with the pair τ_{m-2}, τ_{m-1}. We again have four cases.
We repeat the analysis. After each step a moves to the left and is absent from the subsequent transpositions: either a cancels as in case (1), which concludes by induction, or

$$e = \tau_1 \cdot \ldots (a\ b') \cdot \tau_i \cdot \tau_{i+1} \cdot \cdots \cdot \tau_m$$

for some $b' \neq a$, where a is NOT in $\tau_i, \tau_{i+1}, \ldots \tau_m$.

Proof of the theorem, conclusion

So if a survives to the end, we have

$$e = (a\, b') \cdot \prod_{i=2}^{m} \tau_i$$

where $\tau_i(a) = a$ for $i \geq 2$.
Apply both sides to a:

$$a = e(a) = [(a\, b') \cdot \prod_{i=2}^{m} \tau_i](a) = (a\, b')(a) = b'.$$

This is a contradiction, so we conclude by induction.

Proof of the theorem, conclusion

So if a survives to the end, we have

$$e = (a\ b') \cdot \prod_{i=2}^{m} \tau_i$$

where $\tau_i(a) = a$ for $i \geq 2$.
Apply both sides to a:

$$a = e(a) = [(a\ b') \cdot \prod_{i=2}^{m} \tau_i](a) = (a\ b')(a) = b'.$$

This is a contradiction, so we conclude by induction.

Proof of the theorem, conclusion

So if a survives to the end, we have

$$e = (a\, b') \cdot \prod_{i=2}^{m} \tau_i$$

where $\tau_i(a) = a$ for $i \geq 2$.
Apply both sides to a:

$$a = e(a) = [(a\, b') \cdot \prod_{i=2}^{m} \tau_i](a) = (a\, b')(a) = b'.$$

This is a contradiction, so we conclude by induction.

A_4

The alternating group A_n is of index 2 in S_n, hence is normal.
However, the kernel of any homomorphism $f : G \to G'$ is always normal. Indeed, if $N = \ker f$, $n \in N$, $g \in G$, then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = e.$$

The order of A_4 is $|S_4|/2 = 4!/2 = 12$. We can write all the elements as products $(a\ b)(c\ d)$.

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

and all the 3-cycles:

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$$

and their squares. This makes $3 + 2 \cdot 4 = 11$, and the identity is the last one.

A_4

The alternating group A_n is of index 2 in S_n, hence is normal. However, the kernel of any homomorphism $f : G \to G'$ is always normal. Indeed, if $N = \ker f$, $n \in N$, $g \in G$, then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = e.$$

The order of A_4 is $|S_4|/2 = 4!/2 = 12$. We can write all the elements as products $(a\ b)(c\ d)$.

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

and all the 3-cycles:

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$$

and their squares. This makes $3 + 2 \cdot 4 = 11$, and the identity is the last one.

A_4

The alternating group A_n is of index 2 in S_n, hence is normal. However, the kernel of any homomorphism $f : G \to G'$ is always normal. Indeed, if $N = \ker f$, $n \in N$, $g \in G$, then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = e.$$

The order of A_4 is $|S_4|/2 = 4!/2 = 12$. We can write all the elements as products $(a\ b)(c\ d)$.

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

and all the 3-cycles:

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$$

and their squares. This makes $3 + 2 \cdot 4 = 11$, and the identity is the last one.

A_4

The alternating group A_n is of index 2 in S_n, hence is normal. However, the kernel of any homomorphism $f : G \to G'$ is always normal. Indeed, if $N = \ker f$, $n \in N$, $g \in G$, then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = e.$$

The order of A_4 is $|S_4|/2 = 4!/2 = 12$. We can write all the elements as products $(a\ b)(c\ d)$.

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

and all the 3-cycles:

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$$

and their squares. This makes $3 + 2 \cdot 4 = 11$, and the identity is the last one.

A_4

The alternating group A_n is of index 2 in S_n, hence is normal. However, the kernel of any homomorphism $f : G \to G'$ is always normal. Indeed, if $N = \ker f$, $n \in N$, $g \in G$, then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = e.$$

The order of A_4 is $|S_4|/2 = 4!/2 = 12$. We can write all the elements as products $(a\ b)(c\ d)$.

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

and all the 3-cycles:

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$$

and their squares. This makes $3 + 2 \cdot 4 = 11$, and the identity is the last one.

A_4

The alternating group A_n is of index 2 in S_n, hence is normal. However, the kernel of any homomorphism $f : G \to G'$ is always normal. Indeed, if $N = \ker f$, $n \in N$, $g \in G$, then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = e.$$

The order of A_4 is $|S_4|/2 = 4!/2 = 12$. We can write all the elements as products $(a\ b)(c\ d)$.

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

and all the 3-cycles:

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$$

and their squares. This makes $3 + 2 \cdot 4 = 11$, and the identity is the last one.

A_4

The alternating group A_n is of index 2 in S_n, hence is normal. However, the kernel of any homomorphism $f : G \to G'$ is always normal. Indeed, if $N = \ker f$, $n \in N$, $g \in G$, then

$$f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g) \cdot e \cdot f(g^{-1}) = e.$$

The order of A_4 is $|S_4|/2 = 4!/2 = 12$. We can write all the elements as products $(a\ b)(c\ d)$.

$$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$$

and all the 3-cycles:

$$(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$$

and their squares. This makes $3 + 2 \cdot 4 = 11$, and the identity is the last one.

$S_4 \setminus A_4$

The complement of A_4 is S_4 is the coset of elements whose sign is -1.

There are 6 transpositions corresponding to the choice of any pair of two elements, and 6 4-cycles.

$S_4 \setminus A_4$

The complement of A_4 is S_4 is the coset of elements whose sign is -1.

There are 6 transpositions corresponding to the choice of any pair of two elements, and 6 4-cycles.