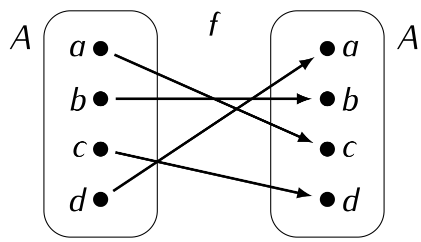
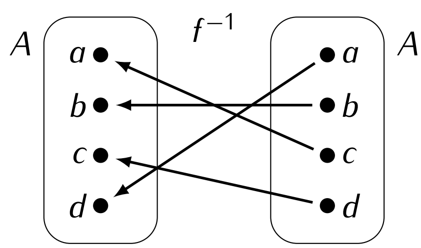
Definition 7.1

Let A be a set. A *permutation* of A is a function $f\colon A \to A$ which is both 1-1 and onto.



Note. For every permutation f we have the inverse function f^{-1} such that $f \circ f^{-1}(x) = x$ and $f^{-1} \circ f(x) = x$ for all $x \in A$.



Definition 7.2

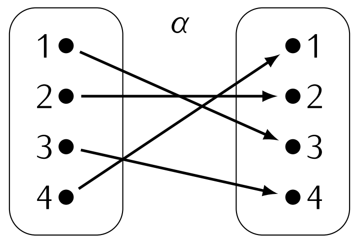
Let A be a set. The *permutation group* of A is a group $S(A)$ defined as follows:

- **Elements of $S(A)$:** permutations $f\colon A \to A$.
- **Group operation:** composition of functions $g \circ f$.
- **The identity element:** the function $\varepsilon\colon A \to A$, $\varepsilon(x) = x$ for all $x \in A$.
- **The inverse of f:** the inverse permutation f^{-1}.

Definition 7.3

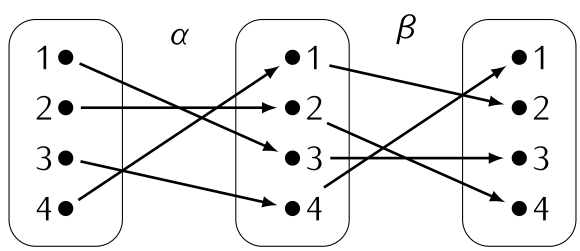
For $n \geq 1$ the group S_n is the group of permutations of the set $A = \{1, 2, \ldots, n\}$. This group is called the *symmetric group on n letters*.

Matrix notation of permutations:



$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}$$

Composition:



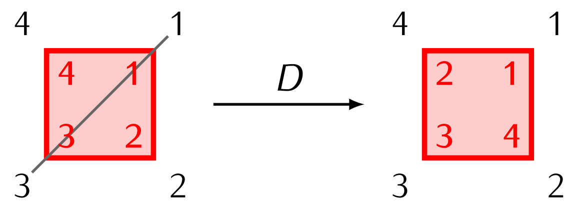
$$\begin{aligned} \beta \circ \alpha &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \end{aligned}$$

Theorem 7.4

For any $n \geq 1$ we have $|S_n| = n!$

Dihedral groups and permutation groups

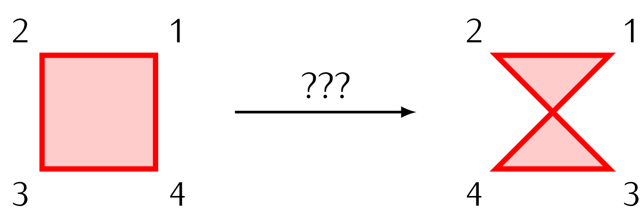
Let P_n be a regular polygon with n vertices. Label the vertices with numbers $1, 2, \ldots, n$. Since every symmetry of P_n send vertices to vertices, it defines a certain permutation of vertices:



$$D = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix}$$

Since composition of symmetries corresponds to composition of permutations of vertices, we can identify the dihedral group D_n with a subgroup of the group of permutations S_n. Note that not every permutation in S_n comes from a symmetry of P_n. E.g.:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}$$



Note. The groups S_n are non-abelian for $n > 2$, e.g:

$$\overset{\alpha}{\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}} \circ \overset{\beta}{\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}} = \overset{\alpha\circ\beta}{\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}}$$

$$\overset{\beta}{\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}} \circ \overset{\alpha}{\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}} = \overset{\beta\circ\alpha}{\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}}$$

Definition 7.5

Let $\alpha \in S_n$ and let $i \in \{1, \ldots, n\}$. We will say that α *moves* i if $\alpha(i) \neq i$. If $\alpha(i) = i$ we will say that α *fixes* i.

Example. The permutation

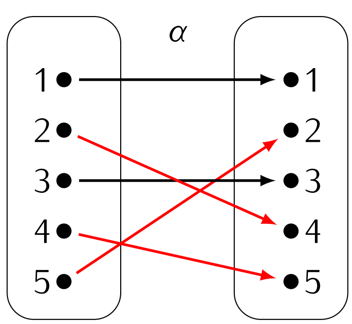
$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{bmatrix}$$

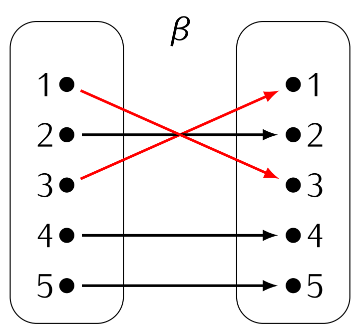
moves 1, 2 and 4, and fixes 3.

Definition 7.6

We will say that permutations $\alpha, \beta \in S_n$ are *disjoint* if there is no $i \in \{1, \ldots, n\}$. which is moved by both α and β.

Example.





$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{bmatrix}$$

Theorem 7.7

If $\alpha, \beta \in S_n$ are disjoint permutations then

$$\alpha \circ \beta = \beta \circ \alpha$$

Moreover,

$$\alpha \circ \beta(i) = \begin{cases} \alpha(i) & \text{if } i \text{ is moved by } \alpha \\ \beta(i) & \text{if } i \text{ is moved by } \beta \\ i & \text{otherwise} \end{cases}$$

Proof. Assume that $i \in \{1, \dots, n\}$ is an element moved by α. Then α also moves $\alpha(i)$. It follows that both i and $\alpha(i)$ are fixed by β, so we have

$$\beta \circ \alpha(i) = \alpha(i) = \alpha \circ \beta(i)$$

By the same argument, if i is moved by β then

$$\alpha \circ \beta(i) = \beta(i) = \beta \circ \alpha(i)$$

Finally, it both α and β fix i then

$$\alpha \circ \beta(i) = i = \beta \circ \alpha(i)$$

$\square$

Definition 7.8

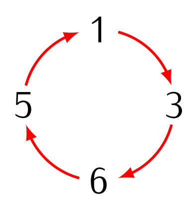
A permutation $\alpha \in S_n$ is a *cycle of length r* (or *r-cycle*) if there are distinct elements $i_1, i_2, \dots i_r \in \{1, 2, \dots, n\}$ such that

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \quad \dots \quad \alpha(i_{r-1}) = i_r, \quad \alpha(i_r) = i_1$$

and α fixes all other elements of $\{1, \dots, n\}$.

Example.

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{bmatrix}$$



Cycle notation. A permutation α such that

$$\alpha(i_1) = i_2, \quad \alpha(i_2) = i_3, \quad \dots \quad \alpha(i_{r-1}) = i_r, \quad \alpha(i_r) = i_1$$

and which fixes all other elements is denoted by $(i_1, i_2, \dots, i_r)$.

Example.

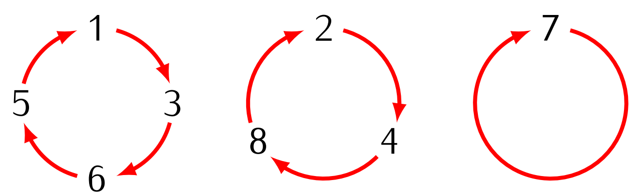
$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{bmatrix} = (1,3,5,6) = (3,5,6,1) = (5,6,1,3) = (6,1,3,5)$$

Theorem 7.9

Every permutation in S_n is either a cycle or a product of disjoint cycles.

Example.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 2 & 1 & 5 & 7 & 4 \end{bmatrix} = (1,3,6,5) \circ (2,8,4) \circ (7) = (1,3,6,5) \circ (2,8,4)$$



Lemma 7.10

Let $\alpha \in S_n$, and let $i_0 \in \{1, \dots, n\}$ be an element moved by α. Then:

1) There exists $r > 1$ such that $\alpha^r(i_0) = i_0$
2) If $r > 1$ is the smallest integer satisfying $\alpha^r(i_0) = i_0$ then all elements

$$i_0, \alpha(i_0), \alpha^2(i_0), \dots, \alpha^{r-1}(i_0)$$

are distinct.

Proof. Consider the sequence

$$i_0 = \alpha^0(i_0),\ \alpha^1(i_0),\ \alpha^2(i_0),\ \dots$$

Since all elements of this sequence come from the finite set $\{1, \dots, n\}$, there must an integer $r \geq 1$ such that the elements $i_0, \alpha(i_0), \alpha^2(i_0), \dots, \alpha^{r-1}(i_0)$ are distinct and $\alpha^r(i_0)$ is equal to one of the previous elements. We will show that $\alpha^r(i_0) = i_0$. Indeed, otherwise $\alpha^r(i_0) = \alpha^k(i_0)$ for some $1 \leq k < r$. This gives

$$\alpha(\alpha^{r-1}(i_0)) = \alpha(\alpha^{k-1}(i_0))$$

and since α is a 1-1 function, we obtain

$$\alpha^{r-1}(i_0) = \alpha^{k-1}(i_0)$$

This contradicts the assumption that the elements $i_0, \alpha(i_0), \ldots, \alpha^{r-1}(i_0)$ are distinct. □

Proof of Theorem 7.9. Let $\alpha \in S_n$. We will argue that α can be written as a product of cycles by induction with respect to the number k of elements of $\{1, \ldots, n\}$ moved by k. If $k = 0$ then α fixes all elements, so it is the identity permutation, which is a 1-cycle.

Assume then that all permutations moving k or fewer elements can be written as a product of disjoint cycles and that α moves $k + 1$ elements. Let $i_0 \in \{1, \ldots, n\}$ be an element moved by α. By Lemma 7.10 there is $r > 1$ such that the elements

$$i_0,\ \alpha(i_0),\ \alpha^2(i_0), \ldots, \alpha^{r-1}(i_0)$$

are all distinct and $\alpha^r(i_0) = i_0$. Denote for $k = 1, \ldots, r-1$ denote $i_k = \alpha^k(i_0)$. Notice that $\alpha(i_k) = i_{k+1}$ for $k < r-1$ and $\alpha(i_{r-1}) = i_0$. Let $\beta \in S_n$ be a permutation defined as follows:

$$\beta(i) = \begin{cases} i & \text{if } i \in \{i_0, \ldots, i_{r-1}\} \\ \alpha(i) & \text{otherwise} \end{cases}$$

Notice that the cycle $(i_0, i_1, \ldots, i_{r-1})$ and β are disjoint permutations. Thus, we can use Theorem 7.7 to show that $\alpha = (i_0, i_1, \ldots, i_{r-1}) \circ \beta$. Then, since β moves fewer elements than α, by the inductive assumption we can write β as a product of disjoint cycles:

$$\beta = \gamma_1 \circ \cdots \circ \gamma_m$$

Therefore we obtain a decomposition of α into a product of disjoint cycles:

$$\alpha = (i_0, i_1, \ldots, i_{r-1}) \circ \gamma_1 \circ \cdots \circ \gamma_m$$

□

Recall:

- The *least common multiple* of integers $n_1, n_2, \ldots, n_k \geq 1$ is the smallest positive integer, denoted by $\mathrm{lcm}(n_1, \ldots, n_k)$, which is divisible by each of these numbers.
- If $m > 0$ is an integer divisible by $n_1, \ldots, n_k$ then m is divisible by $\mathrm{lcm}(n_1, \ldots, n_k)$.

Theorem 7.11

Assume that a permutation $\alpha \in S_n$ has a decomposition into disjoint cycles

$$\alpha = \gamma_1 \circ \cdots \circ \gamma_m$$

where γ_i is a cycle of length $r_i > 1$. Then the order of α is given by

$$|\alpha| = \mathrm{lcm}(r_1, r_2, \ldots, r_m)$$

Proof. First, notice that if γ is an r-cycle then $|\gamma| = r$. Let

$$\alpha = \gamma_1 \circ \cdots \circ \gamma_m$$

where γ_i is an r_i-cycle, and let $p = \mathrm{lcm}(r_1, \ldots, r_m)$. By Theorem 7.7 disjoint cycles commute, so

$$\alpha^p = (\gamma_1 \circ \cdots \circ \gamma_m)^p = \gamma_1^p \circ \cdots \circ \gamma_m^p = \varepsilon$$

where ε is the identity permutation. By Theorem 4.3 we obtain that $|\alpha|$ divides p.

Next, we claim that $\gamma_i^{|\alpha|} = \varepsilon$ for each i. Indeed, since the cycles are disjoint, elements moved by $\gamma_i^{|\alpha|}$ are fixed by $\gamma_j^{|\alpha|}$ for all $j \neq i$, so if $\gamma_i^{|\alpha|}$ moves some element, then the same element is moved by $\gamma_1^{|\alpha|} \circ \cdots \circ \gamma_m^{|\alpha|}$. This however cannot happen because

$$\gamma_1^{|\alpha|} \circ \cdots \circ \gamma_m^{|\alpha|} = (\gamma_1 \circ \cdots \circ \gamma_m)^{|\alpha|} = \alpha^{|\alpha|} = \varepsilon$$

In this way we obtained that r_i divides $|\alpha|$ for $i = 1, \ldots, m$, and so p divides $|\alpha|$. Therefore $|\alpha| = p$.

$\square$

Exercise. Compute the order of the following permutation in S_8:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 2 & 1 & 5 & 7 & 4 \end{bmatrix}$$

Exercise. Find all possible orders of elements of S_5.

Exercise. Compute the number of permutations of order 10 in S_8

Exercise. Consider the following permutation in S_8:

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 2 & 1 & 5 & 7 & 4 \end{bmatrix}$$

Compute α^{-1}.

Definition 7.12

A *transposition* in S_n is a cycle (i_1, i_2) of length 2.

Theorem 7.13

Every premutation in S_n can be written as a product of transpositions.

Proof. By Theorem 7.9 every permutation is product of cycles, so it is enough to show that every cycle can be written as a product of transpositions. This is true, since if $(i_1, i_2, \dots, i_r)$ is a cycle in S_n then

$$(i_1, i_2, \dots, i_r) = (i_1, i_r) \circ (i_1, i_{r-1}) \circ \cdots \circ (i_1, i_2)$$

□

Note. A permutation can be written as a product of cycles in many different ways:

$$\begin{aligned}
\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix} &= \\
&= (1,3) \circ (1,2) \\
&= (2,3) \circ (1,3) \\
&= (1,3) \circ (4,2) \circ (1,2) \circ (1,4) \\
&= (2,4) \circ (1,2) \circ (2,3) \circ (1,4)
\end{aligned}$$

Theorem 7.14

Let $\alpha \in S_n$ and let

$$\alpha = \beta_1 \circ \beta_2 \circ \cdots \circ \beta_r$$

be a decomposition of α into a product of transpositions.

- If the number r is even, then every other decomposition of α into transpositions consists of an even number of transpositions.
- If r is odd, then every other decomposition of α into transpositions consists of an even number of transpositions.

Lemma 7.15

Let $\beta_1, \ldots, \beta_r$ be transpositions in S_n such that

$$\beta_1 \circ \beta_2 \circ \cdots \circ \beta_r = \varepsilon$$

where ε is the identity permutation. Then r is an even number.

Proof. We will prove by induction with respect to k the following statement:

For any $k \geq 2$, if $\beta_1 \circ \beta_2 \circ \cdots \circ \beta_r = \varepsilon$ and $r \leq k$ then r is an even number.

If $k = 2$ this holds, since the only way to write ε as a product of 1 or 2 transpositions is $\beta \circ \beta^{-1}$, which uses 2 transpositions.

For the inductive step, assume then that the statement holds for some k. We need to show that it also holds for $k+1$. Let then $\beta_1, \ldots, \beta_r$ be transpositions such that $r \leq k+1$ and

$$\beta_1 \circ \beta_2 \circ \cdots \circ \beta_r = \varepsilon \tag{$*$}$$

Assume that one of the transpositions β_i is of the form (a, b) for some $a, b \in \{1, \ldots, n\}$. One can check that the following identities hold:

- $(a, b) \circ (c, d) = (c, d) \circ (a, b)$
- $(a, b) \circ (b, c) = (b, c) \circ (a, c)$

Here a, b, c, d are distinct elements of the set $\{1, \ldots, n\}$. These identities say that when multiplying transpositions, we can move the transposition involving a toward the right side without changing the number of transpositions. Using this observation, we can rewrite the equation $(*)$ as follows:

$$\gamma_1 \circ \cdots \circ \gamma_{r-k} \circ (a, b_1) \circ (a, b_2) \circ \ldots \circ (a, b_k) = \varepsilon \tag{$**$}$$

where $\gamma_1, \ldots, \gamma_{r-k}$ are transpositions that do not involve a. If $b_1 \neq b_i$ for $i = 2, \ldots k$, then the permutation given by the left hand side of the equation $(**)$ would send b_1 to a, which is impossible. This means that there is $i > 1$ such that $b_1 \neq b_2, \ldots, b_{i-1}$ and $b_1 = b_i$. We will need one more identity:

- $(a, b) \circ (a, c) = (b, c) \circ (a, b)$ for distinct elements a, b, c.

Using this identity, we can bring the equation $(**)$ to the following form:

$$\gamma_1 \circ \ldots \circ \gamma_{r-k} \circ (b_1, b_2) \circ \ldots \circ (b_1, b_{i-1}) \circ (a, b_1) \circ (a, b_i) \circ (a, b_{i+1}) \circ \ldots \circ (a, b_n) = \varepsilon$$

Since $b_1 = b_i$ we have $(a, b_1) \circ (a, b_i) = \varepsilon$, and the above equation becomes

$$\gamma_1 \circ \ldots \circ \gamma_{r-k} \circ (b_1, b_2) \circ \ldots \circ (b_1, b_{i-1}) \circ (a, b_{i+1}) \circ \ldots \circ (a, b_n) = \varepsilon$$

This expresses ε as a product of $r-2$ transpositions. Since $r \leq k+1$, thus $r-2 \leq k$, and so, by the inductive assumption, $r-2$ must be an even number. Therefore r is an even number as well. $\square$

Proof of Theorem 7.14. Assume that a permutation α can be written as a product of transpositions in two different ways:

$$\begin{aligned} \alpha =& \beta_1 \circ \beta_2 \circ \cdots \circ \beta_r \\ \alpha =& \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s \end{aligned}$$

Then we have

$$\begin{aligned} \varepsilon &= \alpha \circ \alpha^{-1} \\ &= (\beta_1 \circ \beta_2 \circ \cdots \circ \beta_r) \circ (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s)^{-1} \\ &= (\beta_1 \circ \beta_2 \circ \cdots \circ \beta_r) \circ (\gamma_s^{-1} \circ \gamma_{s-1}^{-1} \circ \cdots \circ \gamma_1^{-1}) \\ &= (\beta_1 \circ \beta_2 \circ \cdots \circ \beta_r) \circ (\gamma_s \circ \gamma_{s-1} \circ \cdots \circ \gamma_1) \end{aligned}$$

This means that ε is a product of $r+s$ transpositions. Since by Lemma 7.15, $r+s$ is an even number, thus either both r and s are even numbers or they are both odd. $\square$

Definition 7.16

A permutation $\alpha \in S_n$ is *even* if it can be written as a product of even number of transpositions and it is *odd* if it can be written as a product of an odd number of tranpositions.

Theorem 7.17

The subset of S_n consisting of all even permutations is a subgroup of S_n.

Definition 7.18

The subgroup of S_n consisting of even permutations is called an *alternating group on n letters* and it is denoted by A_n

Definition 7.19

The *sign* of a permutation $\alpha \in S_n$ is defined as follows:

$$\operatorname{sign}(\alpha) = \begin{cases} +1 & \text{if } \alpha \text{ is even} \\ -1 & \text{if } \alpha \text{ is odd} \end{cases}$$

Note. Recall that for a square matrix A we can compute its determinant $\det A$. The determinant can be defined using permutations and their signs as follows. For a matrix

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \dots & a_{n,n} \end{bmatrix}$$

we set

$$\det A = \sum_{\alpha \in S_n} \operatorname{sign}(\alpha) \cdot a_{1,\alpha(1)} \cdot a_{2,\alpha(2)} \cdot \ldots \cdot a_{n,\alpha(n)}$$