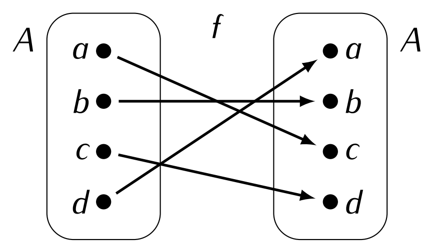
Definition 10.1

A *permutation* of a set A is a function $f\colon A \to A$ which is a bijection.



Definition 10.2

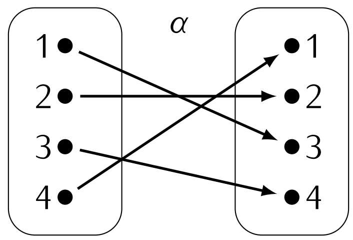
Let A be a set. The *permutation group* of A is a group $S(A)$ defined as follows:

- **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}.

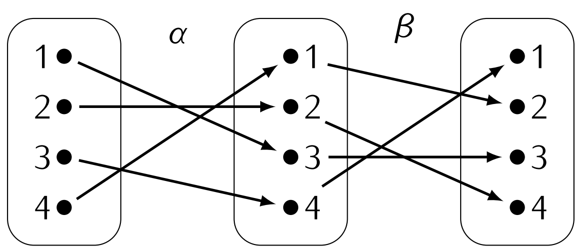
Definition 10.3

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:



Composition:



Theorem 10.4

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

Dihedral groups and permutation groups

Note. The groups S_n are non-abelian for $n > 2$

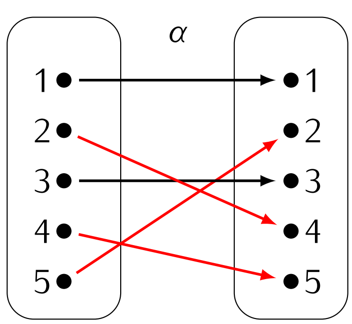
Definition 10.5

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.

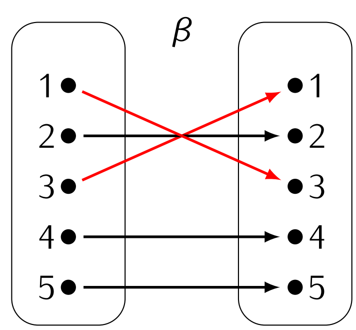
Definition 10.6

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.



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



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

Theorem 10.7

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

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

Moreover,

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

Definition 10.8

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

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

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

Theorem 10.9

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

Lemma 10.10

Let $\alpha \in S_n$, and let $i_0 \in \{1, \ldots, n\}$ 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

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

are distinct.

Poof of Theorem 10.9.

Recall that the least common multiple of integers $n_1, n_2, \ldots, n_k \geq 1$ is the smallest positive integer $\operatorname{lcm}(n_1, \ldots, n_k)$ which is divisible by each of these numbers.

Theorem 10.11

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

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

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. Compute the number of permutations of order 3 in S_7.

Definition 10.12

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

Theorem 10.13

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

Theorem 10.14

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 odd number of transpositions.

Lemma 10.15

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.

Definition 10.16

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 10.17

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

Definition 10.18

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

Theorem 10.19

For $n \geq 2$ the alternating group A_n has order $\frac{n!}{2}$.

Definition 10.20

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

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