9.A Permutation groups

The permutation groups form an important class of groups. For a non-empty set X, let $S(X) := \{\sigma : X \longrightarrow X \mid \sigma \text{ bijective map}\}$ denote the permutation group on X. Its elements are called the permutations on X, they are bijective maps from X onto itself. The binary operation on $S(X)$ is the composition $\circ$ of maps; its neutral element is the identity map $id_X : X \longrightarrow X$, $x \longmapsto x$ and for $\sigma \in S(X)$, the inverse map σ^{-1} of σ is the inverse of σ in $S(X)$. For $\sigma, \tau \in S(X)$, we often simply write $\sigma\tau$ instead of $\sigma \circ \tau$. (We emphasize here that we always perform the composition of maps from right to left and this is also done for permutations of a set. Therefore, for $\sigma, \tau \in S(\{1, \dots, n\}) =: S_n$ in $\sigma\tau = \sigma \circ \tau$ first we apply τ and then σ, for example, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$.)

Let us recall that: Every group is a subgroup of a permutation group. More precisely:

9.A.1 Theorem of Cayley *Let G be a group. For $a \in G$, let $\lambda_a : G \longrightarrow G$, $x \longmapsto ax$, be the left-multiplication by a. Then λ_a is a permutation on G, i.e. $\lambda_a \in S(G)$ and the map $\lambda : G \longrightarrow S(G)$, $a \longmapsto \lambda(a) := \lambda_a$, $a \in G$, is an injective group homomorphism*

Proof Since the equation $ax = b$ has unique solution in the group G (see), λ_a is bijective. For $x \in G$, $\lambda_{ab}(x) = (ab)x = a(bx) = \lambda_a(\lambda_b(x))$, we have $\lambda_{ab} = \lambda_a \circ \lambda_b$, i.e. $\lambda(ab) = \lambda(a) \circ \lambda(b)$ for all $a, b \in G$ and hence λ is a group homomorphism. From $\lambda(a) = \lambda(b)$, i.e. $\lambda_a = \lambda_b$, it follows that $a = ae = \lambda_a(e) = \lambda_b(e) = be = b$. This proves the injectivity of λ.

For a singleton $X = \{x\}$, $S(X) = \{id_X\}$. In the case $X = \{x, y\}$, $x \neq y$, $S(X) = \{id_X, \sigma\}$, where σ is the permutation with $\sigma(x) := y$ and $\sigma(y) := x$ and $S(X)$ is a cyclic group of order 2 (with generator σ). We have already seen that if X has more than two elements, then $S(X)$ is not commutative. Even more:

9.A.2 Lemma *Let X be any set with at lest three (distinct) elements. Then the center $Z(S(X)) := \{\sigma \in S(X) \mid \sigma\tau = \tau\sigma \text{ for all } \tau \in S(X)\}$ of $S(X)$ is trivial, i.e. $Z(S(X)) = \{id_X\}$.*

Proof For $\sigma \in S(X)$, $\sigma \neq id_X$, we must show that $\sigma \notin Z(S(X))$. Since $\sigma \neq id_X$, there exists $x \in X$ with $y := \sigma(x) \neq x$. By assumption on X, there exists $z \in X$ with $z \neq x$ and $z \neq y$. Let $\tau : X \to X$ be the permutation which interchange y and z, and maps other elements onto themselves, in particular, $\tau(x) = x$ and $\tau(y) = z$. It follows that

$(\sigma\tau)(x) = \sigma(\tau(x)) = \sigma(x) = y$ and $(\tau\sigma)(x) = \tau(\sigma(x)) = \tau(y) = z$ and hence $\sigma\tau \neq \tau\sigma$. Therefore $\sigma \notin Z(G(X))$.

The following assertion shows that the structure of the group $G(X)$ depends only on the cardinality $\#X$ of X.

9.A.3 Proposition *Let X and X' be two sets of the same cardinality, i.e. there is a bijective map $f: X \longrightarrow X'$. Then the map*

$$\kappa_f : G(X) \longrightarrow G(X'), \quad \sigma \longmapsto f\sigma\bar{f}^1,$$

is an isomorphism of groups.

Proof Since $f\sigma\bar{f}^1$ is a composite of bijective maps, it is again bijective, i.e. $f\sigma\bar{f}^1 \in G(X')$. Further, $\kappa_f(\sigma\tau) = f(\sigma\tau)\bar{f}^1 = (f\sigma\bar{f}^1)(f\tau\bar{f}^1) = \kappa_f(\sigma)\kappa_f(\tau)$ and hence κ_f is a group homomorphism. Finally, the map $\kappa_{\bar{f}^1} : G(X') \longrightarrow G(X)$ defined by $\kappa_{\bar{f}^1}(\sigma') = \bar{f}^1\sigma' f$ is clearly the inverse of κ_f, i.e. $\kappa_f^{-1} = (\kappa_f)^{-1}$. Therefore κ_f is bijective.

We now turn our attention to the permutation groups of finite sets. If X is a finite set of cardinality $n \geq 1$, then there exists a bijective map $f: \mathbb{N}_n^+ := \{1, \cdots, n\} \longrightarrow X$ and hence by 3.C.3

we can identify $\mathfrak{S}(X)$ with the permutation group $\mathfrak{S}(\mathbb{N}_n^+) = \mathfrak{S}(\{1,\dots,n\})$. In the following we simply write $\mathfrak{S}_n$ instead of $\mathfrak{S}(\{1,\dots,n\})$ and restrict our investigation to the permutation groups $\mathfrak{S}_n$, $n \geq 1$.

Therefore by the theorem of Cayely 9.A.1, every finite group G of order n can be identified with a subgroup of $\mathfrak{S}_n$.

For writing permutation $\sigma \in \mathfrak{S}_n$ concretely, we also use the notation:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$ where for $i = 1,\dots,n$, $\sigma(i)$ denote the image of i under σ. For example, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ is the permutation $\sigma \in \mathfrak{S}_3$ with $\sigma(1) = 3$, $\sigma(2) = 1$ and $\sigma(3) = 2$.

The group $\mathfrak{S}_n$ can be embedded in a group $\mathfrak{S}_{n+1}$ by extending every permutation $\sigma \in \mathfrak{S}_n$ by putting $\sigma(n+1) := n+1$. In this way $\mathfrak{S}_n$ is a subgroup of $\mathfrak{S}_{n+1}$. With this more we can compute the cardinality of $\mathfrak{S}_n$ by induction on n:

9.A.4 Proposition $\#\mathfrak{S}_n = n! = 1 \cdot 2 \cdot \dots \cdot n$.

Proof By induction on n. For $n = 1$ the assertion is trivial. For the proof of inductive step, we identify $\mathfrak{S}_n$ with a subgroup of $\mathfrak{S}_{n+1}$ as above.

For $i=1,\dots,n$, let $\tau_i \in \mathfrak{S}_{n+1}$ be the permutation which interchange i and $n+1$, and keep all other elements in $\{1,\dots,n+1\}$ fixed. Then $\tau_i(n+1)=i$, $\tau_i(i)=n+1$ and $\tau_i^2 = id_{\{1,\dots,n+1\}}$

Note that every element $\sigma \in \mathfrak{S}_{n+1}$ has a unique representation of the form $\sigma = \tau_i \sigma'$ with $i \in \{1,\dots,n+1\}$ and $\sigma' \in \mathfrak{S}_n$, since from such a representation $\sigma(n+1) = \tau_i(\sigma'(n+1)) = \tau_i(n+1) = i$ and $\tau_i \circ \sigma = \tau_i^2 \sigma' = \sigma'$ are uniquely determined. Now, put $i := \sigma(n+1)$ and $\sigma' := \tau_i \circ \sigma$. Then $\sigma' \in \mathfrak{S}_n$, since $\sigma'(n+1) = \tau_i \sigma(n+1) = \tau_i(i) = n+1$ and $\tau_i \sigma' = \tau_i^2 \sigma = \sigma$. This proves that:

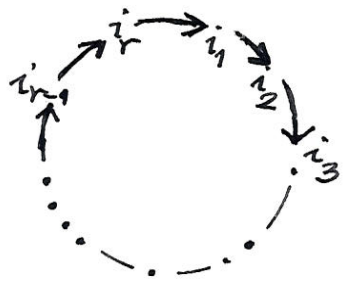
The map $\mathbb{N}_{n+1}^+ \times \mathfrak{S}_n \longrightarrow \mathfrak{S}_{n+1}$ defined by $(i,\sigma) \longmapsto \tau_i \circ \sigma$ is bijective and hence (by induction hypothesis)

$$\#\mathfrak{S}_{n+1} = \#(\mathbb{N}_{n+1}^+ \times \mathfrak{S}_n) = \#\mathbb{N}_{n+1}^+ \cdot \#\mathfrak{S}_n = (n+1)\cdot(\#n!) = (n+1)!.$$

We would like to give a lucid representations of elements of $\mathfrak{S}_n$ into so called canonical cycle-decomposition. For this we begin with a special class of nice permutations.

9.A.5 Definition A permutation $\sigma \in \mathfrak{S}_n$ is called a cycle if there exist distinct elements $i_1,\dots,i_r \in \{1,\dots,n\}$ such that $\sigma(i_1)=i_2$, $\sigma(i_2)=i_3$,

$\dots, \sigma(i_{r-1}) = i_r$, $\sigma(i_r) = i_1$ and $\sigma(i) = i$ for all $i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_r\}$.
If $r = 2$ then such a cycle is called a <u>transposition</u>.
A cycle σ is uniquely determined by the elements $i_1, \dots, i_r$ and their succession (order). It is usually denoted by the symbol $\langle i_1, i_2, \dots, i_r \rangle$ and pictorially by the diagram



With this description of σ it is clear that we may choose to start with arbitrary i_j, $j = 1, \dots, r$, i.e. $\langle i_1, \dots, i_r \rangle = \langle i_j, \dots, i_r, i_1, \dots, i_{j-1} \rangle$ for all $j = 2, \dots, r$. Therefore transpositions are cycles of the form $\langle i_1, i_2 \rangle$; it unterchanges i_1 and i_2 and keep all other elements fixed. Naturally, a cycle of the form $\langle i_1 \rangle$ is the identity of $\{1, 2, \dots, n\}$. The integer r is called the <u>length</u> of the cycle $\sigma = \langle i_1, \dots, i_r \rangle$ and is denoted by $\ell(\sigma)$.

9.A.6 Lemma For a cycle $\sigma = \langle i_1, \dots, i_r \rangle$ in the group S_n, we have:
(1) $\operatorname{Ord} \sigma = r$ (2) $\sigma^{-1} = \langle i_r, i_{r-1}, \dots, i_2, i_1 \rangle$.

<u>Proof</u> For $k = 1, \dots, r$, $\sigma^k(i_1) = i_{k+1} \neq i_1$ and so $\sigma^k \neq id$. Moreover, $\sigma^r(i_1) = i_1$ and since $\langle i_1, \dots, i_r \rangle = \langle i_j, \dots, i_r, i_1, \dots, i_{j-1} \rangle$, we have $\sigma^r(i_j) = i_j$ for all

$j=2,\cdots,r$. Therefore $\sigma^r = id$ and hence r is the smallest number k with $\sigma^k = id$, i.e. $\operatorname{Ord}\sigma = r$.

(2) Inverse of σ mean changing the direction of arrow in the above picture, therefore $\sigma^{-1} = \langle i_r, i_{r-1}, \cdots, i_2, i_1 \rangle$

For further investigations the following concept is very useful:

9.A.7 Definition For a permutation $\sigma \in S_n$, the subset $\operatorname{Supp}(\sigma) := \{i \in \mathbb{N}_n^+ \mid \sigma(i) \neq i\}$ is called the support of σ. The support of σ is precisely consists of those $i \in \{1,\cdots,n\}$ which are "moved" by σ. For example, the support of a cycle $\langle i_1,\cdots,i_r\rangle$, $r \geq 2$ is the set $\{i_1,\cdots,i_r\}$. The identity is the only permutation with the empty support.

9.A.8 Lemma For $\sigma \in S_n$ and $i \in \mathbb{N}_n^+$, we have $i \in \operatorname{Supp}(\sigma)$ if and only if $\sigma(i) \in \operatorname{Supp}(\sigma)$. In particular, $\operatorname{Supp}(\sigma)$ is invariant under σ, in fact $\sigma(\operatorname{Supp}(\sigma)) = \operatorname{Supp}(\sigma)$.

Proof Since σ is injective, $\sigma(i) \neq i$ if and only if $\sigma(\sigma(i)) \neq \sigma(i)$.

Permutations with disjoint supports are called disjoint permutations. Permutations with disjoint supports have simple computation rules:

9.A.9 Proposition Let $\sigma, \tau \in S_n$ be such that $\operatorname{Supp}(\sigma) \cap \operatorname{Supp}(\tau) = \emptyset$. Then:

(1) $\sigma\tau = \tau\sigma$, i.e. σ and τ commute.

(2) $\mathrm{Supp}(\sigma\tau) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$.

(3) $\sigma\tau\,|\,\mathrm{Supp}(\sigma) = \sigma\,|\,\mathrm{Supp}(\sigma)$ and

$\sigma\tau\,|\,\mathrm{Supp}(\tau) = \tau\,|\,\mathrm{Supp}(\tau)$

Proof First, let $i \in \mathrm{Supp}(\sigma)$. Then $\sigma(i) \in \mathrm{Supp}(\sigma)$ by 9.A.8. Since $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \phi$, $i \notin \mathrm{Supp}(\tau)$ and $\sigma(i) \notin \mathrm{Supp}(\tau)$. Therefore $\tau(i) = i$ and $\tau(\sigma(i)) = \sigma(i)$. This proves that

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

$\sigma\tau\,|\,\mathrm{Supp}(\sigma) = \sigma\,|\,\mathrm{Supp}(\sigma) = \tau\sigma\,|\,\mathrm{Supp}(\sigma)$.

Analogously, $\tau\sigma\,|\,\mathrm{Supp}(\tau) = \tau\,|\,\mathrm{Supp}(\tau) = \sigma\tau\,|\,\mathrm{Supp}(\tau)$

For $i \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$, we have $\sigma(i) = i$ and $\tau(i) = i$ and so $\sigma(\tau(i)) = i = \tau(\sigma(i))$.

This proves all assertions.

We now prove the canonical cycle decomposition theorem:

(canonical cycle decomposition)

9.A.10 Theorem Every permutation $\sigma \in S_n$, $\sigma \neq id$ can be written as product of cycles with non-empty and pairwise disjoint supports. Moreover this decomposition is uniquely determined up to the sequence of factors (and is called the canonical cycle decomposition of σ).

Proof We shall prove the assertion by induction on the cardinality $\#\mathrm{Supp}(\sigma)$ of the support of σ. Since $\sigma \neq id$, $\mathrm{Supp}(\sigma) \neq \phi$, i.e. there exists $i \in \mathbb{N}_n^+$ with $\sigma(i) \neq i$. There exists numbers $j \in \mathbb{N}^+$ such that $\sigma^j(i) = i$, for example $j = \mathrm{ord}\,\sigma$ (since

$\sigma^{\operatorname{ord}\sigma} = id$). We choose the smallest r among these numbers j. From $\sigma(i) \neq i$, it follows that $r \geq 2$. Then $i_1 := i$, $i_2 := \sigma(i_1)$, $\dots$, $i_r := \sigma(i_{r-1})$ are pairwise distinct, for, if $i_j = \sigma^{j-1}(i)$ and $i_j = i_k$, then $\sigma^{j-1}(i) = \sigma^{k-1}(i)$ for i, j with $1 \leq j < k \leq r$ and hence $\sigma^{k-j}(i) = i$ with $1 \leq k-j < r$ which contradicts the minimality of r.

We put $\sigma_1 := \langle i_1, \dots, i_r \rangle$ and $\tilde{\sigma} = \sigma_1^{-1}\sigma$. Then σ_1 is a cycle with $\operatorname{Supp}(\sigma_1) \neq \phi$ and $\sigma = \sigma_1 \tilde{\sigma}$. By construction $\sigma|\{i_1, \dots, i_r\} = \sigma_1|\{i_1, \dots, i_r\}$ and hence $\tilde{\sigma}(i) = \sigma_1^{-1}\sigma(i) = i$ for $i \in \{i_1, \dots, i_r\} = \operatorname{Supp}(\sigma_1)$. This proves that $\operatorname{Supp}(\sigma_1) \cap \operatorname{Supp}(\tilde{\sigma}) = \phi$. Now by 9.A.9-(2) $\operatorname{Supp}(\sigma) = \operatorname{Supp}(\sigma_1) \cup \operatorname{Supp}(\tilde{\sigma})$ and hence $\#\operatorname{Supp}(\tilde{\sigma}) < \#\operatorname{Supp}(\sigma)$. In the case $\tilde{\sigma} = id$ $\sigma = \sigma_1$ is the required cycle decomposition. If $\tilde{\sigma} \neq id$, then by induction hypothesis there exists a cycle decomposition $\tilde{\sigma} = \sigma_2 \cdots \sigma_s$ of required properties. Then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_s$ is the corresponding cycle decomposition of σ. Since $\operatorname{Supp}(\sigma_j) \subseteq \operatorname{Supp}(\tilde{\sigma})$ for $j = 2, \dots, s$ and $\operatorname{Supp}(\tilde{\sigma}) \cap \operatorname{Supp}(\sigma_1) = \phi$, it follows that $\operatorname{Supp}(\sigma_j) \cap \operatorname{Supp}(\sigma_1) = \phi$ for $j = 2, \dots, s$. This proves that the cycle decomposition $\sigma = \sigma_1 \sigma_2 \cdots \sigma_s$ satisfies the required properties.

Suppose now $\sigma = \sigma_1' \cdots \sigma_t'$ be another (such a) cycle decomposition of σ. Consider an element $i \in \mathbb{N}_n^+$ with $\sigma(i) \neq i$. Then $i \in \operatorname{Supp}\sigma_j'$ for some $j = 1, \dots, t$

Since $\mathrm{Supp}(\sigma_j') \cap \mathrm{Supp}(\sigma_k') = \phi$ for all $1 \le j, k \le t$, $\sigma_j' \cdot \sigma_k' = \sigma_k' \sigma_j'$ for all $1 \le j, k \le t$ by 9.A.9-(1).

We may therefore assume that $i \in \mathrm{Supp}\, \sigma_1'$.

In any case by 9.A.9-(3) $\sigma \big| \mathrm{Supp}(\sigma_1) = \sigma_1 \big| \mathrm{Supp}(\sigma_1)$ and $\sigma \big| \mathrm{Supp}(\sigma_1') = \sigma_1' \big| \mathrm{Supp}(\sigma_1')$. Therefore both the cycles σ_1 and σ_1' are of the form $\langle i, \sigma(i), \cdots, \sigma^{r-1}(i) \rangle$ and hence are equal, (i.e. $\sigma_1 = \sigma_1'$) in the group S_n. By cancelling them we get $\tilde{\sigma} = \sigma_2 \cdots \sigma_s = \sigma_2' \cdots \sigma_t'$. Now by induction hypothesis the cycle decomposition of $\tilde{\sigma}$ and hence that of σ is unique

9-A.11 Example Let σ be the following permutation in S_{20}:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 17 & 3 & 11 & 5 & 4 & 2 & 19 & 12 & 9 & 15 & 7 & 1 & 10 & 18 & 20 & 14 & 8 & 16 & 6 & 13 \end{pmatrix}$$

The canonical cycle decomposition is :

$\langle 1, 17, 8, 12 \rangle \langle 2, 3, 11, 7, 19, 6 \rangle \langle 4, 5 \rangle \langle 10, 15, 20, 13 \rangle \langle 14, 18, 16 \rangle$

The support of σ is the subset $\{1, \cdots, 20\} \setminus \{9\}$.

From the canonical cycle decomposition $\sigma = \sigma_1 \cdots \sigma_r$, it follows that the powers of σ $\sigma^m = \sigma_1^m \cdots \sigma_r^m$, $m \in \mathbb{Z}$, can be computed easily, since the powers of (given) cycles can be done so.

In particular, we get the formula for the order of σ:

$$\operatorname{Ord}\sigma = \operatorname{LCM}(\operatorname{ord}\sigma_1, \cdots, \operatorname{ord}\sigma_r)$$
$$= \operatorname{LCM}(\ell(\sigma_1), \cdots, \ell(\sigma_r))$$

Since the order of a cycle is clearly equal to its length.

The above permutation $\sigma \in S_{20}$ in 3.C.11 has the order $\operatorname{Ord}\sigma = \operatorname{LCM}(4, 6, 2, 4, 3) = 12$.

The inverse σ^{-1} of σ can also be given immediately by using the canonical cycle decomposition $\sigma = \sigma_1 \cdots \sigma_r$, namely

$$\sigma^{-1} = \sigma_r^{-1} \cdots \sigma_1^{-1} = \sigma_1^{-1} \cdots \sigma_r^{-1}$$

and for a cycle $\langle i_1, \cdots, i_k \rangle$, we have

$$\langle i_1, \cdots, i_k \rangle^{-1} = \langle i_k, i_{k-1}, \cdots, i_1 \rangle = \langle i_1, i_k, \cdots, i_2 \rangle.$$

In the above example for σ^{-1} has the canonical cycle decomposition:

$$\sigma^{-1} = \langle 1, 12, 8, 17 \rangle \langle 2, 6, 19, 7, 11, 3 \rangle \langle 4, 5 \rangle \langle 10, 13, 20, 15 \rangle \langle 14, 16, 18 \rangle.$$

A cycle $\langle i_1, \cdots, i_k \rangle$ of length k is a product of $k-1$ transpositions:

$$\langle i_1, \cdots, i_k \rangle = \langle i_1, i_2 \rangle \langle i_2, i_3 \rangle \cdots \langle i_{k-1}, i_k \rangle$$

Therefore every permutation $\sigma \in S_n$ is a product of transpositions:

9.A.12 Lemma *Every permutation $\sigma \in S_n$ is a product of transpositions.*

Proof (direct) Let $\sigma \in S_n$, $\sigma \neq \mathrm{id}$ and let $j_1 := \sigma(i_1) \neq i_1$. Then $\sigma' := \langle i_1, j_1 \rangle \sigma$ is a permutation with fixed point i_1, i.e. $\sigma' | \mathbb{N}_n^+ \setminus \{i_1\} \in S(\mathbb{N}_n^+ \setminus \{i_1\})$

and hence (by induction (on n)) $\sigma' = \langle i_2, j_2 \rangle \cdots \langle i_s, j_s \rangle$ is a product of transpositions. Therefore σ is a product $\sigma = \langle i_1, j_1 \rangle \sigma' = \langle i_1, j_1 \rangle \cdots \langle i_s, j_s \rangle$ of transpositions.

The representation of a permutation as product of transpositions is (in contrast to the canonical cycle decomposition) naturally not unique. For example, in any such representation can be enlarged by inserting $id = \tau \cdot \tau$ for some transposition τ. However, we shall show that the parity of the number of transpositions in any such representation of σ is uniquely determined.

The representation of σ as product of transposition obtained by using the canonical cycle decomposition of σ has exactly $n-s$ transpositions, where s is the number of orbits of σ (we have also counted singleton orbits). This makes the following definition:

9.A.12 Definition Let $\sigma \in S_n$ and let $s \in \mathbb{N}^+$ be the number of orbits of σ. Then

$$\operatorname{Sign} \sigma := (-1)^{n-s}$$

is called the signum (or signature) of σ.
A permutation σ is called even if $\operatorname{Sign} \sigma = 1$; otherwise it is called odd.

Let $I_1, \cdots, I_s$ be the orbits of $I = \{1, 2, \cdots, n\}$. Then $n - s = \left(\sum_{k=1}^{s} \#I_k\right) - s = \sum_{i=1}^{s} \left(\#I_k - 1\right)$ and hence $\operatorname{Sign}\sigma = \prod_{k=1}^{s} (-1)^{\#I_k - 1}$. We note this: The signature of σ is $\operatorname{sign}\sigma = (-1)^m$, where m is the number of orbits of even cardinality.

9.A.13 Examples. The identity is an even permutation. A transposition is an odd permutation; in general, a cycle of length k has signature $(-1)^{k-1}$. The permutation σ in Example 9.A.11 is even, since there are exactly 4 orbits of even cardinality.

We now prove the following basic theorem:

9.A.14 Theorem Let $\sigma \in \mathfrak{S}_n$ and let $\sigma = \tau_1 \cdots \tau_k$ be a representation of σ as a product of k transpositions $\tau_1, \cdots, \tau_k$. Then $\operatorname{Sign}\sigma = (-1)^k$.

Proof By induction on k. It is enough to show that σ and $\tau\sigma$ for arbitrary transposition τ, have different signatures, i.e. $\operatorname{Sign}\tau\sigma = -\operatorname{Sign}\sigma$. For this it is enough to show that the number of orbits of σ and of $\tau\sigma$ differ by 1.

Let $\tau = \langle i, j \rangle$. The orbits of σ which neither contain i nor contain j are clearly also orbits of $\tau\sigma$.

We therefore need only to consider orbits of σ which contain i or j. We consider two cases:

Case 1 Both i and j belong to the same orbit of σ, in this case the canonical cycle decomposition of σ is of the form:

$$\sigma = \langle i_1, \cdots, i_r, i_{r+1}, \cdots, i_s \rangle \cdots$$

with $i_1 = i$ and $i_{r+1} = j$. Then

$$\tau\sigma = \langle i_1, \cdots, i_r \rangle \langle i_{r+1}, \cdots, i_s \rangle \cdots$$

and hence the number of orbits of $\tau\sigma$ is exactly one more than the number of orbits of σ.

Case 2 i and j belong to the different orbits of σ; in this case the canonical cycle decomposition of σ is of the form:

$$\sigma = \langle i_1, \cdots, i_r \rangle \langle j_1, \cdots, j_s \rangle \cdots$$

with $i_1 = i$ and $j_1 = j$. Then

$$\tau\sigma = \langle i_1, \cdots, i_r, j_1, \cdots, j_s \rangle \cdots$$

and hence the number of orbits of $\tau\sigma$ is exactly one less than the number of orbits of σ.

In particular, by 9.A.14 the number of factors in any representation of an even (resp. odd) permutation as product of transpositions remain even (resp. odd). Further, we have:

9.A.15 Theorem The map

$$\mathrm{Sign} : \mathfrak{S}_n \longrightarrow \{1,-1\},\ \sigma \mapsto \mathrm{Sign}\,\sigma,$$

is a homomorphism of groups, i.e. for $\sigma, \tau \in \mathfrak{S}_n$, we have $\mathrm{Sign}(\sigma\tau) = (\mathrm{Sign}\,\sigma)(\mathrm{Sign}\,\tau)$

Proof We write $\sigma = \sigma_1 \cdots \sigma_s$ and $\tau = \tau_1 \cdots \tau_t$ as product of transpositions $\sigma_1, \cdots, \sigma_s$, resp. $\tau_1, \cdots, \tau_t$ and get a representation $\sigma\tau = \sigma_1 \cdots \sigma_s \tau_1 \cdots \tau_t$. By 9.A.14 we have

$$\mathrm{Sign}(\sigma\tau) = (-1)^{s+t} = (-1)^s \cdot (-1)^t = (\mathrm{Sign}\,\sigma)(\mathrm{Sign}\,\tau).$$

An important particular subgroup of $\mathfrak{S}_n$ is the kernel of Sign, i.e. the subgroup of all even permutations of $\{1,2,\cdots,n\}$.

9.A.16 Definition The subgroup of even permutations of $\{1,2,\cdots,n\}$ is called the alternating group of $\{1,2,\cdots,n\}$ and is usually denoted by $\mathfrak{A}_n = \mathfrak{A}(\{1,2,\cdots,n\})$.

Since $\mathfrak{A}_n$ is the kernel of the group homomorphism $\mathrm{Sign} : \mathfrak{S}_n \longrightarrow \{\pm 1\}$, it is a normal subgroup of $\mathfrak{S}_n$. Moreover, the index of $\mathfrak{A}_n$ in $\mathfrak{S}_n$ is equal to 2 and the two cosets are precisely $\mathfrak{A}_n$ the set of all even permutations and $\mathfrak{S}_n - \mathfrak{A}_n = \tau\mathfrak{A}_n = \mathfrak{A}_n\tau$ the set of all odd permutations, where $\tau \in \mathfrak{S}_n$ is an arbitrary odd permutation, for example, a transposition. Therefore $\#\mathfrak{A}_n = n!/2$ and

the cardinality of the odd permutations is also $n!/2$.

The signature of a permutation $\sigma \in S_n$ can also be determined by using the so called inversions of σ. For $\sigma \in S_n$, a pair $(i,j) \in I \times I$, $I = \{1,2,\cdots,n\}$ is called an inversion of σ if $i<j$, but $\sigma(i) > \sigma(j)$. The number of inversions of σ is denoted by $F(\sigma)$.

9.A.17 Examples (1) The transposition $\langle i,j\rangle \in S_n$, $1 \le i < j \le n$ have the inversions $(i,i+1), \cdots, (i,j); (i+1,j), \cdots, (j-1,j)$. Therefore $F(\langle i,j\rangle) = 2(j-i)-1$

(2) For the permutation $\sigma := \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix} \in S_n$, all (i,j) with $1 \le i < j \le n$ are inversions ations and hence $F(\sigma) = \binom{n}{2}$.

(3) The permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix} \in S_5$ have the inversions $(1,2)$, $(1,4)$, $(3,4)$ and $(3,5)$ and hence $F(\sigma) = 4$.

We now prove the following:

9.A.18 Theorem Let $\sigma \in \mathfrak{S}_n$ be a permutation. Then $\operatorname{Sign}\sigma = (-1)^{F(\sigma)}$.

Proof Since by Example 9.A.17-(1) a transposition has odd number of inversions it is enough to prove that:
For $\sigma, \tau \in \mathfrak{S}_n$, we have $(-1)^{F(\sigma\tau)} = (-1)^{F(\sigma)} \cdot (-1)^{F(\tau)}$.
Clearly for $\sigma \in \mathfrak{S}_n$, we have:

$$(-1)^{F(\sigma)} = \prod_{1 \le i < j \le n} \operatorname{Sign}\left(\sigma(j) - \sigma(i)\right)$$

With this we get:

$$\begin{aligned}(-1)^{F(\sigma\tau)} &= \prod_{1 \le i < j \le n} \operatorname{Sign}\left(\sigma\tau(j) - \sigma\tau(i)\right) \\ &= (-1)^{F(\tau)} \prod_{1 \le i < j \le n} \operatorname{Sign}\left(\sigma(s) - \sigma(r)\right) \\ &= (-1)^{F(\tau)} \cdot (-1)^{F(\sigma)}\end{aligned}$$

The last but one equality follows from the fact that there are exactly $F(\tau)$ pairs $(\tau(i), \tau(j))$, $1 \le i < j \le n$, in which the components are interchanged and this set is precisely the set of pairs (r,s), $1 \le r < s \le n$.

9.A.19 Example The permutation σ in Example 9.A.17 (2) has signature $\operatorname{Sign}\sigma = (-1)^{\binom{n}{2}}$ by 9.A.18. This can also be deduced from the canonical cycle decomposition of $\sigma = \langle 1, n\rangle\langle 2, n-1\rangle \cdots \langle [n/2], n+1-[n/2]\rangle$ which has $[n/2]$ (disjoint) transpositions. Further,

$$(-1)^{[n/2]} = (-1)^{\binom{n}{2}} = \begin{cases} 1, & \text{if } n \equiv 0,1 \pmod 4, \\ -1, & \text{if } n \equiv 2,3 \pmod 4. \end{cases}$$

9.A.20 Example (Conjugate permutations, Type of a permutation) A bijective map $f: X \longrightarrow X'$ induces an isomorphism of groups $\kappa_f : \mathfrak{S}(X) \longrightarrow \mathfrak{S}(X')$, $\sigma \longmapsto f \sigma f^{-1}$. Under this map the k-cycle $\langle x_1, \dots, x_k \rangle$ is mapped onto the k-cycle $\langle f(x_1), \dots, f(x_k) \rangle$. In the case when X (and hence X') is a finite set, the canonical cycle decomposition of $f \sigma f^{-1}$ is obtained by replacing cycles in the canonical cycle decomposition of σ by its f-image. In particular, for $\sigma, \tau \in \mathfrak{S}_n$, the canonical cycle decomposition of the conjugate permutation $\tau \sigma \tau^{-1}$ is obtained from the canonical cycle decomposition of σ by replacing cycles by their τ-images.

For a permutation $\sigma \in \mathfrak{S}_n$ and $1 \le k \le n$, let ν_k be the number of k-cycles in the canonical cycle decomposition of σ. The sequence $\nu(\sigma) = (\nu_1, \dots, \nu_n)$ is called the (cycle) type of σ. The type $\nu(\sigma) = (\nu_1, \dots, \nu_n)$ defines a partition of n, i.e. $1 \cdot \nu_1 + 2 \cdot \nu_2 + \dots + n \cdot \nu_n = n$.

With this we have proved:

9.A.21 Theorem *Two permutations $\sigma, \tau \in \mathfrak{S}_n$ are conjugates in $\mathfrak{S}_n$ if and only if they have the same type, i.e. $\nu(\sigma) = \nu(\tau)$.*

The number of conjugacy classes in $\mathfrak{S}_n$ is called the *class number* of $\mathfrak{S}_n$; it is the number $P(n)$ of partitions of n, i.e.

$$P(n) = \#\left\{(\nu_1, \cdots, \nu_n) \in \mathbb{N}^n \;\middle|\; \sum_{i=1}^{n} i \cdot \nu_i = n\right\}.$$

For small values of n, we can compute the numbers $P(n)$ easily

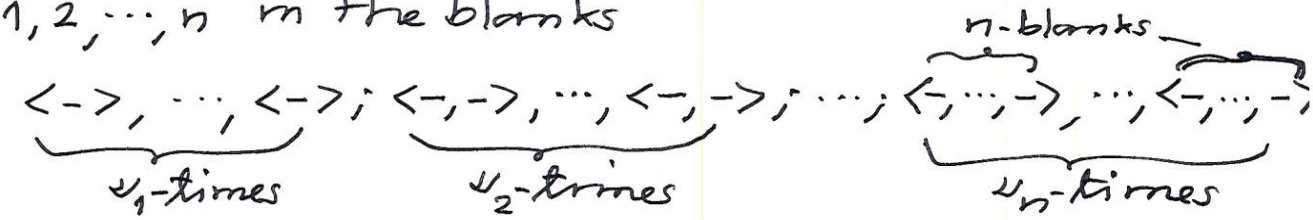
n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(n)$	1	1	2	3	5	7	11	15	22	30	42	56	77	101	135	176

22 Lemma *Let $(\nu_1, \cdots, \nu_n) \in \mathbb{N}^n$. The number of permutations $\sigma \in \mathfrak{S}_n$ with $\nu(\sigma) = (\nu_1, \cdots, \nu_n)$ is*

$$\frac{n!}{\nu_1! \cdots \nu_n!\, 1^{\nu_1} \cdots n^{\nu_n}}.$$

In particular, for $k \in \mathbb{N}^+$, the number of k-cycles in $\mathfrak{S}_n$ is $\dfrac{n!}{(n-k)!\, 1^{n-k}\, k^1}$ *(since the type of a k-cycle is $(n-k, 0, \cdots, 0, 1, 0 \cdots, 0) = (n-k)e_1 + e_k$)*

Proof Consider the number of ways of writing $1, 2, \cdots, n$ in the blanks



There are exactly $n!$ ways of writing $1, 2, \dots n$ in blank spaces, but many of these may be considered equal, for instance, for each i, the ν_i (disjoint) i-cycles can be rearranged among themselves. Therefore we must divide $n!$ by $\nu_1! \cdots \nu_n!$ to avoid duplications. Further each i-cycle can be written in i-different ways, e.g. $\langle a_1, \dots, a_i \rangle = \langle a_2, a_3, \dots, a_i, a_1 \rangle = \cdots = \langle a_i, a_1, \dots, a_{i-1} \rangle$.

Therefore again we need to divide $\frac{n!}{\nu_1! \cdots \nu_n!}$ by $1^{\nu_1} 2^{\nu_2} \cdots n^{\nu_n}$ to avoid duplication. This proves the assertion.

9.A.23 Example (Structure of the groups $\mathfrak{A}_n$ and $\mathfrak{S}_n$) Since the group $\mathfrak{A}_n$ is the kernel of the group homomorphism Sign from the group $\mathfrak{S}_n$ into the commutative group $\{1, -1\}$, it follows that $\mathfrak{A}_n \subseteq [\mathfrak{S}_n, \mathfrak{S}_n]$ = the commutator subgroup of $\mathfrak{S}_n$, see Example 6.A.13. Moreover: $\mathfrak{A}_n$ is the commutator subgroup of $\mathfrak{S}_n$ for every $n \in \mathbb{N}$.

For, if $a, b, c, d \in \{1, \dots, n\}$ with $a \neq b$ and $c \neq d$ and if $\tau \in \mathfrak{S}_n$ is a permutation with $\tau(a) = c$, $\tau(b) = d$, then by Example 9.A.20

$$\langle a, b \rangle \langle c, d \rangle = \langle a, b \rangle \tau \langle a, b \rangle \tau^{-1}$$

is a commutator. Now, since $\langle a, b \rangle \langle c, d \rangle$ generate the group $\mathfrak{A}_n$ by Theorem 9.A.14 the assertion follows.

Therefore the sign homomorphism is (for $n \geq 2$) is essentially the only non-trivial homomorphism from S_n into an abelian group.

For $n \geq 5$ the commutator group of the group A_n is the group A_n itself.

Since

$$\langle a,b,c\rangle = \langle a,b,d\rangle \langle c,e,a\rangle \langle a,b,d\rangle^{-1} \langle c,e,a\rangle^{-1}$$

for pairwise distinct a,b,c,d,e, the assertion (follows) from this and the fact that for every $n \in \mathbb{N}$, the 3-cycles $\langle a,b,c\rangle$ generate the group A_n.

For, if a,b,c,d are pairwise distinct, then

$$\langle a,b\rangle\langle b,c\rangle = \langle a,b,c\rangle$$

and

$$\begin{aligned}\langle a,b\rangle\langle c,d\rangle &= \langle a,b\rangle\langle b,c\rangle\langle b,c\rangle\langle c,d\rangle \\ &= \langle a,b,c\rangle\langle b,c,d\rangle .\end{aligned}$$

Moreover, the group A_n, $n \geq 5$ are simple. For a proof, see

The group A_5 of order 60 is the smallest non-abelian group in the following sense:
every non-abelian simple group of order ≤ 60 is isomorphic to A_5.
For $n \geq 5$, A_n is the only non-trivial normal subgroup in the group S_n, see Test-Exercise

The group S_1 is the trivial group, the group S_2 is cyclic, the group S_3 is isomorphic to the Dihedral group D_3 and the group $A_3 \cong \mathbb{Z}_3$ is the only non-trivial normal subgroup in S_3.

The group S_4 has the normal chain

$$\{id\} \subsetneq V_4 \subsetneq A_4 \subsetneq S_4$$

with quotients $S_4/A_4 \cong S_3$ and $A_4/V_4 \cong A_3$.

Further the groups V_4 and A_4 are the only non-trivial normal subgroups in the group S_4 and V_4 is also the only non-trivial normal subgroup in the group A_4, see Test-Exercise

Note that $V_4 = \{id, \langle 1,2\rangle\langle 3,4\rangle, \langle 1,3\rangle\langle 2,4\rangle, \langle 1,4\rangle\langle 2,3\rangle\}$

9.A.24 Example (Cycle polynomials and Pólya's counting formula)