I- Finite sets rearrangements

1) Definition of permutation

Let E be a finite set with n elements.

Def 1, A permutation of E is a bijection $\sigma : E \to E$. The set of all permutations of E is denoted $\mathfrak{S}(E)$.

Prop 2 : $(\mathfrak{S}(E), \circ)$ is a group, isomorphic to $\mathfrak{S}(\llbracket 1, n \rrbracket)$ which is denoted by $\mathfrak{S}_n$, and called the symmetric group. It has $n!$ elements.

Ex 3 : If $n = 2$, then $\mathfrak{S}(E) \simeq \{\pm 1\}$.

Notat: If $\sigma \in \mathfrak{S}_n$, we can write σ as two rows : $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$

Def 5 : Let $\sigma \in \mathfrak{S}_n$. The support of σ is $\{ i \in \llbracket 1, n \rrbracket, i \neq \sigma(i) \}$. If the support of σ is $\llbracket 1, n \rrbracket$, we say that σ is a derangement.

Prop 6, The number of derangement D_n in $\mathfrak{S}_n$ is $n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = \left\lfloor \frac{n!}{e} \right\rfloor$.

Prop 7 : The group $\mathfrak{S}_n$ acts on $\llbracket 1, n \rrbracket$. This action is n-transitive and faithful. Conversely, if a group G acts on $\llbracket 1, n \rrbracket$ with a n-transitive and faithful action, then $G \simeq \mathfrak{S}_n$.

2) Cycles and orbits

Def 8 : Let $\sigma \in \mathfrak{S}_n$. For $i \in \llbracket 1, n \rrbracket$, the orbit of i under the action of σ is the set $\{ \sigma^k(i), k \in \mathbb{N} \}$.

Def 9 : Let $i_1, \dots, i_r \in \llbracket 1, n \rrbracket$ be distinct integers. A cycle of lenght r, or r-cycle, is a permutation σ such that :
$\forall k \in \llbracket 1, r \rrbracket$, $\sigma(i_k) = i_{k+1}$, and $\forall i \in \llbracket 1, n \rrbracket \setminus \{i_1, \dots, i_r\}$, $\sigma(i) = i$.
We denote such a cycle by $(i_1\ i_2 \cdots i_r)$.

Rem 10 : A permutation σ is a cycle iff it has only one orbit that is not one point.

Ex 11 : Any 2-cycle is called a transposition.
Any n-cycle (with $n = \mathrm{Card}(E)$) is called a circular permutation.

Prop 12 : Let γ be a r-cycle. Then the order of γ is r in $\mathfrak{S}_n$.

Prop 13 : Let γ_1, γ_2 be two cycles with disjoint supports. Then $\gamma_1 \gamma_2 = \gamma_2 \gamma_1$.

Thm 14 : Let $\sigma \in \mathfrak{S}_n$. Then σ is a product of cycles with disjoint supports, and this factorization is unique up to the order in which the factors occur. (see annex)

Ex 15 : If we take $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$, then $\sigma = (1\ 5\ 3)(2\ 4)$.

Prop 16 : In $\mathfrak{S}_n$, there are $(r-1)! \binom{n}{r}$ r-cycles.

Ex 17 : If we take $n = 4$ and $r = 3$: there are 8 3-cycles in $\mathfrak{S}_4$, which are $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$ and $(2\ 3\ 4)$, $(2\ 4\ 3)$.

3) Interchanges and signature

Def 18 : Let $\sigma \in \mathfrak{S}_n$. We say that a couple $(i, j) \in \llbracket 1, n \rrbracket^2$ is an interchange for σ when $i < j$ and $\sigma(i) > \sigma(j)$.
We denote by $\varepsilon(\sigma) := (-1)^k$ where k is the number of interchanges for σ.

Prop 19 : The application $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ defines a group homomorphism, non trivial.

Ex 20 : For a transposition $(i\ j)$, we have $\varepsilon(i\ j) = -1$.
In general, if γ is a r-cycle, then $\varepsilon(\gamma) = (-1)^{r+1}$.

Def 21 : We denote by $\mathcal{A}_n$ the kernel of ε, and it is called the alternating group.

Prop 22 : Let $\sigma \in \mathfrak{S}_n$, and k the number of orbits under the action of σ on $\llbracket 1, n \rrbracket$. Then $\varepsilon(\sigma) = (-1)^{n-k}$.

Ex 23 : If $\sigma = (1\ 3\ 4)(2\ 5)(6\ 8)(7)$, then $\varepsilon(\sigma) = (-1)^{9-4} = -1$.

Prop 24 : The homomorphism ε is the only non trivial homomorphism from $\mathfrak{S}_n$ toward $\{\pm 1\}$.

Application 25 : It exists only two representations of $\mathfrak{S}_n$ of degree 1, the trivial representation and the signature.

Ex 26 : (determinant) : Let $\mathbb{K}$ be a field and $B : (\mathbb{K}^n)^n \to \mathbb{K}$ an alternating n-linear form. Then for all $(x_1, \dots, x_n) \in (\mathbb{K}^n)^n$, for all $\sigma \in \mathfrak{S}_n$, $B(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) B(x_1, \dots, x_n)$.
In consequence, it exists only one alternating n-linear form such that $B(e_1, \dots, e_n) = 1$ if $(e_1, \dots, e_n)$ is the canonical basis.

II - Group structure of $\mathfrak{S}_n$

1) Generating sets and subgroups.

Rem 27: One can understand the group action of G on X by the giving of a homorphism $\varphi : G \to \mathfrak{S}(X)$. It is the principle of the following theorem.

Thm 28 (Cayley): Let G be a finite group of order n. Then G is isomorphic to a subgroup of $\mathfrak{S}_n$.

Ex 29: One can see the cyclic group $\mathbb{Z}/n\mathbb{Z}$ as the group generated by a circular permutation:
$\sigma = (1\ 2\ 3\ \dots\ n)$.

Prop 30: Let γ be a r-cycle: $\gamma = (a_1 \dots a_r)$. Then γ is a product of $r-1$ transpositions:
$\gamma = (a_1\ a_2)(a_2\ a_3)\dots(a_{r-1}\ a_r)$.

Coro 31: The set of transpositions generates $\mathfrak{S}_n$.

Prop 32: The set $\{(1\ i),\ i \in [\![2,n]\!]\}$ generates $\mathfrak{S}_n$, as well as the set $\{(i\ i+1),\ i \in [\![1,n-1]\!]\}$.

Ex 33: Let $n = 5$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} = (2\ 5\ 4)$.
Then $\sigma = (1\ 2)(1\ 5)(1\ 2)(1\ 5)(1\ 4)(1\ 5)$
$= (3\ 4)(2\ 3)(3\ 4)(4\ 5)(3\ 4)(4\ 5)(2\ 3)(3\ 4)(4\ 5)(1\ 2)(2\ 3)$
$\times (3\ 4)(4\ 5)$

2) Conjugacy

Def 34: Let $\sigma, \sigma' \in \mathfrak{S}_n$. We say that σ and σ' are conjugate when there is $g \in \mathfrak{S}_n$ such that $\sigma' = g\sigma g^{-1}$.

Prop 35: Let γ be a r-cycle. The conjugacy class of γ is the set of all r-cycles. Likewise, two permutations are conjugate iff they have the same structure as product of disjoint supports cycles.

Ex 36: $\sigma = (1\ 3\ 4)(5\ 2)(6)$ and $\sigma' = (2\ 5\ 6)(1\ 4)(3)$ are conjugate, via $g := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 1 & 3 \end{pmatrix}$.

Coro 37: The number of conjugacy classes in $\mathfrak{S}_n$ is the number of partitions of n.

Ex 38: In $\mathfrak{S}_4$ there are 5 conjugacy classes:
$4 = 4+0 = 3+1 = 2+1+1 = 2+2 = 1+1+1+1$
4-cycles, 3-cycles, 2-cycles, double transpositions, identity

Thm 39: The alternating group $\mathcal{A}_n$ is simple if $n \geq 5$.

Coro 40: The only normal subgroups of $\mathfrak{S}_n$ are $\{\mathrm{id}\}$, $\mathfrak{S}_n$ and $\mathcal{A}_n$, if $n \geq 5$.

Prop 41: The group $\mathcal{A}_4$ is not simple; the subgroup $V_4 := \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is normal.

Rem 42: The fact that $\mathcal{A}_n$ is simple for $n \geq 5$ implies that there is no solution in radicals for polynomial equations of degree greater than 5.

Thm 43 (Brauer): Let $\sigma, \sigma' \in \mathfrak{S}_n$. They are conjugate iff their permutations matrices are similar. DEV 1

3) Automorphisms of the symmetric group

Def 44: Let $\sigma \in \mathfrak{S}_n$. The application $\Phi_\sigma : \mathfrak{S}_n \to \mathfrak{S}_n$, $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ is an automorphism, and is called inner automorphism. The group of inner automorphisms is denoted by $\mathrm{Int}(\mathfrak{S}_n)$.

Prop 45: For $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$.

Prop 46: $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Int}(\mathfrak{S}_6)$.

Coro 47: For $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) \simeq \mathfrak{S}_n$.

Ex 48: For $n = 3$, $\mathrm{Aut}(\mathfrak{S}_3) \simeq \mathfrak{S}_3 = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 2\ 3), (1\ 3\ 2), (2\ 3)\}$

Ex 49: For $n = 2$: $\mathfrak{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{Aut}(\mathfrak{S}_2) \simeq \{0\}$.

Prop 50: For $n \neq 6$, $\mathrm{Aut}(\mathcal{A}_n) \simeq \mathfrak{S}_n$.

III - The symmetric group in geometry.

1) Isometry groups

Ex 51: Let P_3 be a 3-sided regular polygon. The symmetry group of P_3 is called the dihedral group D_3. It is isomorphic to $\mathfrak{S}_3$. (see annex)

More generally, the symmetry group of a n-sided regular polygon, called D_n, is isomorphic to a subgroup of $\mathfrak{S}_n$.

Prop 52: Let t_n be a regular simplex of $\mathbb{R}^n$. Then the isometry group of t_n is $\mathfrak{S}_{n+1}$, and the group of direct isometries is $\mathcal{A}_{n+1}$.

Thm 53: The finite subgroups of $SO_3(\mathbb{R})$ are:
- the cyclic groups $\mathbb{Z}/n\mathbb{Z}$, $n \geq 1$;
- the dihedral groups $\mathbb{D}_m$, $m \geq 1$;
- the groups of direct isometries of regular polyhedrons: the tetrahedron, the cube, the octahedron, the dodecahedron and the isocahedron. (see annex)

Prop 54: The group of direct isometries of a tetrahedron is isomorphic to $\mathcal{A}_4$.
The group of direct isometries of the cube is isomorphic to $\mathfrak{S}_4$. DEV 2

Prop 55: The group of direct isometries of a dodecahedron is isomorphic to $\mathcal{A}_5$.

2) Link with group representations

Prop 56: The isomorphism between $\mathcal{A}_4$ and the group of direct isometries of a tetrahedron gives a representation of $\mathcal{A}_4$, of degree 3, denoted by $\mathcal{C}$.

Nota 57: Let denote by C_1, C_2, C_3 and C_4 the four conjugacy classes of $\mathcal{A}_4$:

$C_1 = \{id\}$, $C_2 = \{\text{double-transpositions}\}$,
$C_3 = \{(123), (134), (243), (142)\}$;
$C_4 = \{(132), (143), (234), (124)\}$.

Prop 58: The representation $\mathcal{C}$ is irreducible, and the associated character ψ is:
$\psi(id) = 3$, $\psi((12)(34)) = -1$, $\psi((123)) = \psi((132)) = 0$.
Then, we have the character table of ψ:

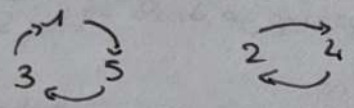
	C_1	C_2	C_3	C_4
χ_0	1	1	1	1
χ_1	1	1	j	j^2
χ_2	1	1	j^2	j
ψ	3	-1	0	0

with $j = e^{\frac{2i\pi}{3}}$.

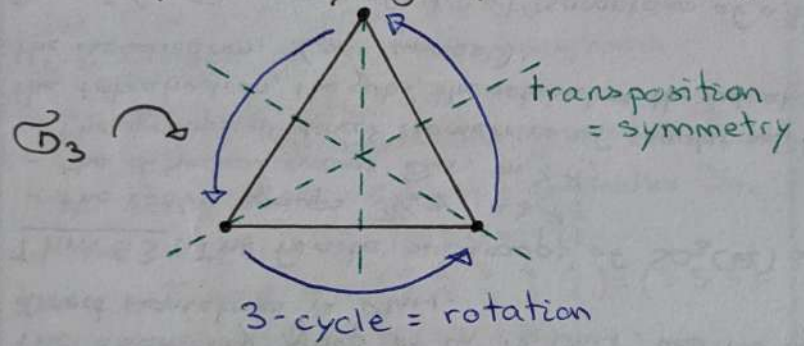
Annex :

- Factorization in disjoint supports cycles:

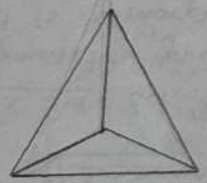
If $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 5\ 3)(2\ 4)$,
we can write



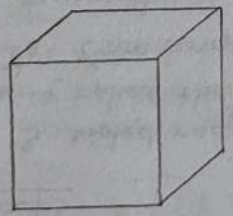
- The symmetry group of a triangle:



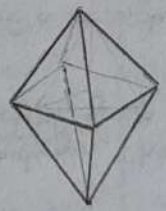
- Finite subgroups of $SO_3(\mathbb{R})$: platonic solids



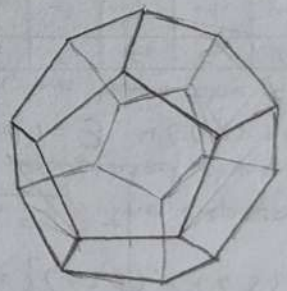
tetrahedron
(4 faces)



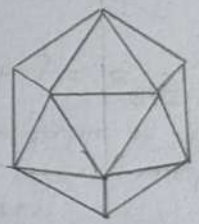
cube
(6 faces)



octahedron
(8 faces)



dodecahedron
(12 faces)



isocahedron
(20 faces)