Memento 4/6 - Permutations.

1. Groupe Soit E un ensemble et $\star$ une loi de composition interne, i.e. une application de $E \times E \to E$. Le couple $(E, \star)$ est un *groupe* si et seulement si :

(1) Il existe $e \in E$, tel que $\forall x \in E,\ x \star e = e \star x = x$, appelé *élément neutre* ;

(2) La loi $\star$ est *associative*, i.e. $\forall (x, y, z) \in E^3,\ (x \star y) \star z = x \star (y \star z)$;

(3) Tout élement x admet un *symétrique* noté x^{-1} tel que $x \star x^{-1} = x^{-1} \star x$.

On appelle *centre* d'un groupe G, l'ensemble noté $Z(G)$ des éléments qui commutent, i.e. $Z(G) = \{x \in G \mid \forall y \in G, x * y = y * x\}$. Si $Z(G) = G$, alors la loi $\star$ et le groupe G sont dits *commutatifs*. Quand un groupe est fini son cardinal s'appelle *l'ordre* du groupe. Pour tout élément $x \in G$ et $k \in \mathbf{Z}$, on note $x^k := x \star x \star \cdots \star x$ avec k termes si $k > 0$ (si $k < 0$, on remplace chaque terme x par x^{-1}).

L'*ordre* d'un élément $g \in G$, est le plus petit entier p tel que $g^p = e$ et le théorème de Lagrange prouve que $p \mid \#G$ et s'il existe un élement $g \in G$ dont l'ordre est égal à $\#G$ alors ce groupe est dit *cyclique*. Soient H un sous-ensemble de G, l'ensemble noté $\langle H \rangle$ constitué par toutes les compositions possibles d'éléments de H et leurs symétriques est un sous-groupe de G appelé *sous-groupe engendré* par H et les éléments de H sont appelés *générateurs* de $\langle H \rangle$.

2. Permutations On appelle *permutation* d'un ensemble E toute bijection de $E \to E$. L'ensemble des bijections sur E muni de la loi de composition $\circ$ est un groupe appelé *groupe symétrique* ou *groupe des permutations* de E. On le note $\mathfrak{S}(E)$ ou plus simplement $\mathfrak{S}_n$ dans le cas où $E = [1, n]$ avec $n \in \mathbf{N}$. L'ordre de $\mathfrak{S}_n$ est égal à $n!$

L'élément neutre du groupe $\mathfrak{S}_n$ est l'application identique $x \mapsto x$ et ce groupe n'est commutatif que pour les valeurs $n = 1, 2$. Sa richesse est principalement liée à sa non-commutativité. Le *support* d'une permutation $\sigma \in \mathfrak{S}(E))$ est le sous-ensemble des éléments de E qui ne sont pas invariants par σ, i.e. $\mathrm{supp}(\sigma) := \{i \in [1, n] \mid \sigma(i) \neq i\}$. Une permutation $\sigma \in \mathfrak{S}_n$ est souvent décrite sous forme matricielle, la première ligne de la matrice est constituée des n entiers 1 à n et la deuxième contient respectivement l'image de ces entiers. La permutation suivante de $\mathfrak{S}_5$

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

a pour support $\{1, 3, 4, 5\}$, les seuls éléments invariants étant les entiers 2 et 6.

Définition 1. *Soit $\sigma \in \mathfrak{S}(E)$. On définit une relation d'équivalence R_σ sur E par $x\ R_\sigma\ y \Leftrightarrow \exists k \in \mathbf{Z} \mid y = \sigma^k(x)$ dont les classes sont appelées les* orbites de E *suivant σ. On appelle* p-cycle *toute permutation σ telle qu'une seule orbite a un cardinal $p > 1$, appelé* longueur du cycle. *Un cycle de longueur* 2 *est appelé* transposition.

La permutation (1) est un cycle de longueur 4, en effet une seule des trois orbites $\{1, 3, 4, 5\}$, $\{2\}$ et $\{6\}$ n'est pas réduite à un élément. On montre aisément que si σ est un cycle de longueur p alors $\{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{p-1}\}$ est l'orbite du cycle quel que soit l'élément x de l'orbite qui caractérise le cycle. Ceci justifie l'écriture $(x, \sigma(x), \sigma^2(x), \ldots, \sigma^{p-1})$ d'un cycle. Ainsi le cycle σ ci-dessus s'écrit $\sigma = (1\ 3\ 4\ 5)$.

Par analogie avec la multiplication, on parle souvent du "produit" pour désigner la composition $\sigma \circ \tau$ de deux permutations σ et τ et on omet d'écrire $\circ$. Si σ et τ sont des cycles à supports disjoints, alors ils commutent, i.e. $\sigma\tau = \tau\sigma$.

Théorème 2. *Toute permutation $\sigma \in \mathfrak{S}_n$ non identique se décompose de manière unique (à l'ordre des facteurs près) en produit de cycles à supports disjoints. Toute permutation se décompose en produit de transpositions.*

Définition 3. *On appelle* signature *d'une permutation $\sigma \in \mathfrak{S}_n$ l'entier $\epsilon(\sigma) := (-1)^{n-k}$ où k est le nombre d'orbites suivant σ.*

L'identité crée n orbites, d'où $\epsilon(\mathrm{Id}) = 1$, une transposition τ en crée $n-1$ donc $\epsilon(\tau) = -1$ et un cycle σ de longueur p en crée $(n-p)+1$ donc $\epsilon(\sigma) = (-1)^{p-1}$. Si σ est un p-cycle, alors $\sigma^{p-1} = \mathrm{Id}$. Une transposition τ est donc une involution.

Théorème 4. *L'application ϵ est un morphisme du groupe de $(\mathfrak{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$. Ainsi si σ et σ' sont deux permutations, alors $\epsilon(\sigma\sigma') = \epsilon(\sigma)\epsilon(\sigma')$.*

Les permutations de signature positive sont dites *paires*, les autes *impaires*. L'ensemble des permutations paires est le noyau de ϵ, c'est donc un sous-groupe de $\mathfrak{S}_n$ appelé *groupe alterné* et noté $\mathfrak{A}_n$. On montre que $\#\mathfrak{A}_n = n!/2$.

3. Conjugaison

Définition 5. *Deux éléments x et y d'un groupe $(G, \star)$ sont dits* conjugués, *s'il existe un élément $g \in G$ tel que $y = g^{-1} \star x \star g$.*

Cette notion n'a aucun intérêt si le groupe est commutatif puisque les classes sont alors réduites à un singleton, en effet si y est en relation avec x alors $y = g^{-1} \star x \star g$ et donc $y = (g^{-1} \star g) \star x = x$. Cette relation entre x et y exprime le fait que l'action de y sur un ensemble E (ou sur le groupe G lui-même) peut être réalisée par x en "translatant" l'ensemble E. Il s'agit d'une relation d'équivalence et les classes d'équivalence pour cette relation sont appelées *classes de conjugaison*, elles regroupent donc les éléments du groupe qui agissent de la même façon. La classe de conjugaison de l'élément neutre est réduite à lui-même puisqu'il commute avec tous les éléments.

Lemme 6. *Soient τ une permutation et $\sigma = (i_1, i_2, \ldots, i_p)$ un p-cycle. Le conjugué $\tau^{-1}\sigma\tau$ est égal au p-cycle $(\tau(i_1), \tau(i_2), \ldots, \tau(i_p))$.*

Ce lemme associé au théorème 2 permet de calculer aisément le conjugué d'une permutation quelconque.

Définition 7. *On appelle* type *d'une permutation σ le r-uplet $(p_1, p_2, \ldots, p_r)$ constitué par les r longueurs de ses cycles dans l'ordre croissant.*

Lemme 8. *Deux permutations σ et σ' sont conjuguées si et seulement si elles sont de même type.*

Le type d'un p-cycle est donc (p) et tous les p-cycles sont conjugués.