# FICHE D'ENTRAINEMENT CAPES EXTERNE

Enquête sur $S_n$ et son acolyte $A_n$
$X = \{1, \ldots, n\}$ $S_n = \{\text{permutations de } X\}$
Une permutation $\sigma \in S_n$ est représentée par

$$\begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$$

Si $(\sigma, \tau) \in S_n^2$ $\sigma \circ \tau$ est la permutation définie par $(\sigma \circ \tau)(i) = \sigma(\tau(i))$

1) $|S_n| = n!$
2) Pour $n = 4$ on considère

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Calculer $\sigma \circ \tau$, $\tau \circ \sigma, \tau^{-1}, \sigma^{-1}, \tau \circ \sigma \circ \tau^{-1}, \ldots$
Calculer $< \sigma, \tau >$ (sous-groupe engendré par $\sigma$ et $\tau$)

3) Soit $\gamma \in S_n$ tel que $\gamma$ permute cycliquement $i_1, \ldots, i_r$ et laisse fixe les éléments de $\{1, 2, \ldots, n\} \backslash \{i_1, \ldots, i_r\}$.
On a donc $\sigma(i_1) = i_2, \gamma(i_2) = i_3, \ldots, \gamma(i_r) = i_1$ et $\gamma(j) = j$ pour $j \in \{1, \ldots, n\} \backslash \{i_1, \ldots, i_r\}$.
$\gamma$ est alors appelé un cycle (de longueur $r$) et noté $(i_1, \ldots, i_r)$.
Un cycle de de longueur 2 est une transposition.
   a) Calculer $(1, i) \circ (1, j)$; $(1, i) \circ (1, j) \circ (1, i)$ (où $i, j \in \{1, \ldots, n\}$
   b) Si $\gamma = (i_1, \ldots, i_r) \in S_n$, calculer $\gamma^2, \gamma^3, \ldots, \gamma^k, \ldots$ pour $1 \leq k \leq r$
   c) Conclure que $\gamma^r = id$ mais $\gamma^k \neq 1$ si $1 \leq k < r$. Donc $\gamma$ est d'ordre $r$ dans le groupe $S_n$.
4) Deux cycles $\gamma$ et $\gamma'$ sont disjoints si les représentants de $\gamma$ et $\gamma'$ n'ont pas d'éléments communs (i.e. Si $i \in \{1, \ldots, n\}$ est tel que $\gamma(i) \neq i$ alors $\gamma'(i) = i$)
   a) Montrer que si $\gamma$ et $\gamma'$ sont disjoints alors $\gamma \circ \gamma' = \gamma' \circ \gamma$
   b) Soit $\alpha \in S_n$ $\alpha = (i_1, \ldots, i_r) \circ (j_1, \ldots, j_s) \circ \ldots \circ (l_1, \ldots, l_u)$ où les cycles $\gamma_1 = (i_1, \ldots, i_r), \gamma_2 = (j_1, \ldots, j_s), \ldots, \gamma_k = (l_1, \ldots, l_u)$ sont disjoints. Montrer que $\alpha$ est d'ordre $m$ dans $S_n$. Où $m = ppcm(r, s, \ldots, u)$
5) a) Montrer que toute permutation se décompose en cycles disjoints
   b) Si $\sigma = \gamma_1 \ldots \gamma_r = \gamma'_1 \ldots \gamma'_s$ sont deux décompositions en cycles disjoints, montrer que $r = s$ et qu'il existe une permutation $\varphi \in S_r$ tel que $\gamma'_i = \gamma_{\varphi(i)}$ pour tout $i \in \{1, \ldots, r\}$. Donc : toute permutation se décompose donc de manière unique en cycles disjoints.
6) a) Montrer que $(i_1, \ldots, i_r) = (i_1, i_r) \circ \ldots \circ (i_1, i_3) \circ (i_1, i_2)$
   b) Montrer que toute permutation se décompose en un produit de transpositions.
7) Soit $S_n$ $\exists$ $\alpha = (i_1, \ldots, i_r) \circ (j_1, \ldots, j_s) \circ \ldots \circ (l_1, \ldots, l_u)$ une $(= la)$ décomposition en cycles disjoints de $\alpha$.
   a) Montrer que $\alpha$ est un produit de $(r-1) + (s-1) + \ldots + (u-1)$ transpositions
   b) Trouver un exemple de permutations admettant plusieurs décompositions en produits de transpositions (aide : $(1, 2, 3) = (1, 3)(1, 2) = \ldots$)
   c) Montrer que $(a, b) \circ (a, e_1, \ldots, e_t, b, d_1, \ldots, d_k) = (b, d_1, \ldots, d_k) \circ (a, e_1, \ldots, e_t)$ et $(a, b) \circ (b, d_1, \ldots, d_k) \circ (a, e_1, \ldots, e_t) = (a, e_1, \ldots, e_t, b, d_1, \ldots, d_k)$
   d) On pose $N(\alpha) = (r-1) + (s-1) + \ldots + (u-1)$. Puisque la décomposition en cycles disjoints est unique, $N(\alpha)$ est déterminé de manière unique par $\alpha$ et de plus $\alpha$ se décompose en produit de $N(\alpha)$ transpositions.

Montrer que

$$N((a,b)\circ\alpha) = \begin{cases} N(\alpha)-1 \text{ Si } a \text{ et } b \text{ apparaissent dans le même cycle de la décomposition de } \alpha \\ N(\alpha)+1 \text{ Si } a \text{ et } b \text{ apparaissent dans des cycles différents} \end{cases}$$

(aide : utiliser c) et remarquer que $N(a, e_1, \ldots, e_t, b, d_1, \ldots, d_k) = t + k + 1 \ldots$)

e) $N((a_1,b_1)\circ\ldots\circ(a_l,b_l)\circ\alpha)$ a même parité que $N(\alpha)$ ssi $l$ est pair

f) Si $\alpha = (a_1,b_1)\circ(a_2,b_2)\circ\ldots\circ(a_r,b_r) = (c_1,d_1)\circ\ldots\circ(c_s,d_s)$. Alors $(-1)^r = (-1)^s$. Ce nombre est appelé la signature de $\alpha$ : $sign(\alpha)$.

8) $\alpha \in S_n$ est dite paire si elle se décompose en un nombre pair de transpositions, $\alpha$ est impaire sinon $sign(\alpha) = 1$ si $\alpha$ pair; $sign(\alpha) = -1$ si $\alpha$ impaire

a) Montrer que $sign(\alpha\circ\beta) = sign(\alpha)\circ sign(\beta)$

b) Montrer que $A_n = \{\alpha \in S_n \mid \alpha \text{ est paire}\}$ est un sous-groupe normal de $S_n$

c) Calculer $|A_n|$ ($A_n$ : le groupe alterné)

9) Montrer que si $n \geq 3$ alors $A_n$ est engendré par les cycles de longueur 3

10) $\alpha \in S_n$. Montrer que $\alpha\circ(i_1,\ldots,i_r)\circ\alpha^-1 = (\alpha(i_1),\ldots,\alpha(i_r))$

Pistes à suivre : $A_n$ est simple si $n \geq 5$; Thm de Cayley; $S_n$ est complet si $n \neq 2$ et 6; ...

1) Les triplets pythagoriciens : on cherche tous les triplets $(x,y,z) \in \mathbb{Z}^3$ tels que $x^2+y^2 = z^2$. (on peut supposer $(x,y,z) = 1$.

a) Montrer que $x$ et $y$ ne peuvent être tous deux impairs. On suppose $y$ pair dans la suite. Montrer alors que $x$ est impair ...et $z$ ?

b) Montrer que $(z+x, z-x) = 2$. Poser $z+x = 2a$ $z-x = 2b$ $(a,b) = 1$

c) Montrer que les décompositions en facteurs premiers de $a$ et $b$ n'ont que des exposants pairs et poser $a = u^2$ $b = v^2$ $(u,v) = 1$

d) Conclure $z = u^2+v^2$, $x = u^2-v^2$ et $y = 2uv$ et de plus $u, v$ de parité différente.

e) Conclure.

2) On veut montrer que $x^4+y^4 = z^4$ n'admet pas de solution entière autre que $(0,0,0)$ (Fermat) $(x,y,z) = 1$

a) Montrer qu'il suffit de prouver que $x^4+y^4 = z^2$ n'a pas de solution non triviale. On suppose qu'elle en a : soit $x,y,z$ tel que $(x,y,z) = 1$ $x^4+y^4 = z^2$ et $z > 0$ $z$ minimal

b) Montrer qu'on peut supposer $x, z$ impairs et $y$ pair

c) Montrer qu'il existe $(u,v) \in \mathbb{Z}^2$ $(u,v) = 1$ $u$ et $v$ de parité différente tel que $x^2 = u^2-v^2$ $y^2 = 2uv$ $z = u^2+v^2$

d) Montrer qu'il existe $(a,b) \in \mathbb{Z}^2$ premier entre eux de parité différente tel que $x = a^2-b^2$ $v = 2ab$ $u = a^2+b^2$

e) Montrer qu'$y^2 = 4ab(a^2+b^2)$ et en déduire que $a = \alpha^2$ $b = \beta^2$ et $a^2+b^2 = \tau^2$ où $(\alpha,\rho,\tau) \in \mathbb{N}^3$

f) Montrer que $\tau^2 = \alpha^4+\rho^4$ et $0 \leq \tau < z$. Conclure ($\tau^2 = u < u^2+v^2 = z^2 \ldots$).