Corrigé Travaux dirigés iL01 : Mathématiques Discrètes, Feuille 2 vendredi 16 septembre 2005

1. Pour $\pi \in \mathbf{S}_n$ on appelle *conjugué* de π toute permutation π' qui peut être écrite comme $\pi' = \sigma\circ\pi\circ\sigma^{-1}$ pour une $\sigma \in \mathbf{S}_n$.

a. Montrer que c'est une relation symétrique (c'est-à-dire que π est aussi conjugué de π' ; on dira simplement que π et π' sont conjugués) et transitive (tout conjugué de π' est aussi conjugué de π). Comme c'est évidemment aussi une relation reflexive (π est conjugué de π), il s'agit donc d'une relation d'équivalence, dont les classes sont appelées classe de conjugaison.

$\surd$ *Quand $\pi' = \sigma\circ\pi\circ\sigma^{-1}$, alors π est aussi conjugué de π' car $\pi = \sigma^{-1}\circ\pi'\circ\sigma$, et tout conjugué $\pi'' = \rho\circ\pi'\circ\rho^{-1}$ de π' est aussi conjugué de π : $\pi'' = \rho\circ\sigma\circ\pi\circ\sigma^{-1}\circ\rho^{-1} = (\rho\circ\sigma)\circ\pi\circ(\rho\circ\sigma)^{-1}$.*

b. Montrer que si $(a_1\ a_2\ \cdots\ a_l)$ est un cycle de π, et $\pi' = \sigma\circ\pi\circ\sigma^{-1}$, alors $(\sigma_{a_1}\ \sigma_{a_2}\ \cdots\ \sigma_{a_l})$ est un cycle de π'. En déduire que π et π' ont le même nombre d'orbites de l éléments, pour toute valeur de l. (On dit aussi qu'ils sont du même type, ou le type d'une permutation est la liste des cardinaux des ses orbites en ordre faiblement décroissant ; par exemple la permutations $(1\ 4\ 6)\circ(2\ 8)\circ(5\ 7)\in\mathbf{S}_8$ est de type $(3,2,2,1)$, et $(1\ 3)\circ(2\ 4\ 8)\circ(5\ 6)$ est du même type.)

$\surd$ *Définissons pour convenance $a_{l+1} = a_1$, alors le fait que $(a_1\ a_2\ \cdots\ a_l)$ est un cycle de π veut dire que $\pi_{a_i} = a_{i+1}$ pour $i \in [l]$. Posons $b_i = \sigma_{a_i}$ pour $i \in [l+1]$, et montrons que $\pi'_{b_i} = b_{i+1}$: on a $\pi'_{b_i} = (\sigma\circ\pi\circ\sigma^{-1})_{\sigma_{a_i}} = (\sigma\circ\pi)_{a_i} = \sigma_{\pi_{a_i}} = \sigma_{a_{i+1}} = b_{i+1}$. Ainsi $(b_1\ \cdots\ b_l)$ est un cycle de π', obtenu d'un cycle de la même longueur de π par l'application de σ à chaque nombre dans le cycle ; on peut retrouver le cycle de départ par l'application de σ^{-1} aux nombres dans de cycle de π', ce qui établit une bijection préservant la longueur entre les cycles de π et de π', d'où clairement π et π' ont le même nombre de cycles de chaque longueur.*

c. Montrer réciproquement que si $\pi, \pi' \in \mathbf{S}_n$ sont du même type, alors ils sont conjugués.

$\surd$ *On écrit une décomposition en cycles de π dans laquelle la longueur des cycles est faiblement décroissante, et on y ajoute à la fin des 1-cycles pour tous les points fixes de π, en sorte que tous les nombres de $[1,n]$ apparaissent une seule fois. Si l'on écrit une décomposition du même type pour π', alors les parenthèses seront aux mêmes endroits car π et π' sont du même type de cycles. Soit alors $\sigma \in \mathbf{S}_n$ la permutation qui envoie $i \in \mathbf{N}$ vers le nombre qui, dans la décomposition de π', occupe la place correspondante à celle occupée par i dans la décomposition de π (autrement dit, une représentation en deux lignes de σ peut être donnée dont la première ligne est obtenue en enlevant les parenthèses de la décomposition de π, et la seconde ligne de la même façon de π'). Alors il est clair de ce qui précède que $\pi' = \sigma\circ\pi\circ\sigma^{-1}$. Par exemple pour la paire de permutations de type $(3,2,2,1)$ mentionnée dans le point précédent, on peut écrire $\begin{smallmatrix}\pi= & (1\ 4\ 6)(2\ 8)(5\ 7)(3)\\ \pi'= & (2\ 4\ 8)(5\ 6)(1\ 3)(7)\end{smallmatrix}$ et en déduire $\pi' = \sigma\circ\pi\circ\sigma^{-1}$ pour $\sigma = \left(\begin{smallmatrix}1&4&6&2&8&5&7&3\\2&4&8&5&6&1&3&7\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&2&3&4&5&6&7&8\\2&5&7&4&1&8&3&6\end{smallmatrix}\right)$.*

2. Soient σ, π des cycles. On a vu qu'ils commutent ($\sigma\circ\pi = \pi\circ\sigma$) si leurs supports sont disjoints. La réciproque n'est pas vraie (par exemple ils commutent si $\sigma = \pi$), et le but de cet exercice est de prouver une condition précise pour leur commutation. On va démontrer que σ et π commutent si et seulement si l'une des deux conditions suivantes est vérifiées : (1) les supports de σ et de π sont disjoints, ou (2) σ est une puissance de π (c'est-à-dire, il existe k tel que $\sigma = \pi^k$). Mais d'abord un considère une question liée.

a. Si π est un cycle de longueur l, pour quelles valeurs de k la puissance π^k est-elle aussi un cycle ?

$\surd$ *On écrira $\pi = (a_0\ \cdots\ a_{l-1})$ pour le cycle, alors $\pi^k(a_i) = a_{i+k \bmod l}$. Par conséquent les points de $A = \{a_0,\ldots,a_{l-1}\}$ sont soit tous fixes pour π^k (si l divise k), soit tous mobiles pour π^k. En tout cas π^k fixe les points en dehors de A, donc pour que π^k soit un cycle, il faut et il suffit que A soit une orbite de π^k. Or, l'orbite $\langle\pi^k\rangle\cdot a_0$ de a_0 par π^k est égale à $\{\, a_{ki \bmod l} \mid i\in\mathbf{Z}\,\}$, et comme $ki \bmod l$ ne dépend que de la classe de i modulo l, ceci est égal à $\{\, a_{ki \bmod l} \mid 0 \le i < l\,\}$. Il s'agit de trouver quand cette orbite est de cardinal l et donc égale à A, ce qui est le cas si et seulement si kl est le plus petit multiple commun de k et l (car si $ki \equiv ki' \pmod l$ avec $0\le i < i' < l$, alors $k(i'-i)$ est un multiple commun de k et l strictement plus petit que kl). Il faut et il suffit donc que k et l soient premiers entre eux.*

b. Est-ce que les conditions (1) et (2) peuvent être simultanément vérifiées ? Montrer que si l'une d'elles est vérifiée, alors σ et π commutent.

$\surd$ *Le support d'une puissance π^k est le même que celui de π (sauf si π^k est l'identité, c'est à dire si k est un multiple de la longueur l du cycle π, mais ce n'est pas possible si $\sigma = \pi^k$ est un cycle), donc si (2) est vérifié, (1) ne l'est pas. On sait que deux cycles dont les supports sont disjoints commutent (c'est même vrai pour deux permutations quelconques dont les supports sont disjoints). Dans le cas (2) on a $\sigma = \pi^k$ donc $\pi \circ \sigma = \pi^k \circ \pi = \pi^{k+1} = \pi^k \circ \pi = \sigma \circ \pi$, et on a également commutation.*

c. Pour montrer la réciproque on suppose que σ et π commutent. Qu'est-ce qu'on peut dire alors du conjugué $\pi' = \sigma \circ \pi \circ \sigma^{-1}$ de π ? Montrer que si l'on suppose en plus que σ fixe un au moins un point du support de π, alors la condition (1) est vérifiée.

$\surd$ *La commutation s'exprime aussi comme $\pi = \sigma \circ \pi \circ \sigma^{-1}$. En écrivant $\pi = (a_0 \ \cdots \ a_{k-1})$, ce qui veut dire que $a_i = \pi^i(a_0)$ pour $0 \leq i < k$, on a donc également $\pi = (\sigma_{a_0} \ \cdots \ \sigma_{a_{k-1}})$. Si $\sigma(a_0) = a_0$ on a alors également $\sigma(a_i) = \pi^i(\sigma(a_0)) = \pi^i(a_0) = a_i$. Tous les points a_i étant fixes pour σ, le support $\{a_0, \ldots, a_{k-1}\}$ de π est disjoint de celui de σ, et la condition (1) est vérifiée.*

d. Montrer finalement que si σ et π commutent et σ fixe aucun point du support de π, alors la condition (2) est vérifiée.

$\surd$ *Le support de $\pi = (\sigma_{a_0} \ \cdots \ \sigma_{a_{k-1}})$ est $\{\sigma(a_0), \ldots, \sigma(a_{k-1})\}$, ce qui est aussi égal à $\{a_0, \ldots, a_{k-1}\}$ donc il existe j avec $0 \leq j < k$ tel que $\sigma_{a_0} = a_j$; l'hypothèse exclut le cas $j = 0$. Pour $0 \leq i < l$ on a $\sigma_{a_i} = \pi^i(\sigma_{a_0}) = \pi^i(a_j) = a_{i+j \bmod k}$, donc σ coïncide avec π^k sur le support $\{a_0, \ldots, a_{k-1}\}$ de π. Comme σ est un cycle, il doit fixer les autres points de $[1, n]$, ce qui fait aussi π^k, donc les deux sont égaux. Apparemment π^k est un cycle, c'est à dire k et l sont premiers entre eux.*

3. Dans le cours on a vu que toute permutation $\pi \in \mathbf{S}_n$ peut être obtenue par la composition d'une suite de transpositions, et qu'en plus on pourra restreindre ces transpositions d'être choisies parmi les éléments de $\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$, c'est-à-dire parmi les transpositions de voisins, aussi appelées transpositions simples. Montrer que plus généralement si $i_2, \ldots, i_n$ est une suite d'entiers qui vérifie $1 \leq i_k < k$ pour $k = 2, \ldots, n$ (on note que cela ne laisse aucun choix pour $i_2 = 1$), alors toute permutation $\pi \in \mathbf{S}_n$ peut être obtenue comme la composition d'une suite de transpositions choisies parmi les éléments de $\{(i_2\ 2), (i_3\ 3), \ldots, (i_n\ n)\}$. Indication: on pourrait utiliser une récurrence sur la valeur $\max(\{0\} \cup \{\, i \in [1, n] \mid \pi_i \neq i \,\})$ du plus grand point mobile de π.

$\surd$ *On montrera par récurrence sur j que toute permutation π dont le support est contenu dans $[1, j]$ s'écrit comme composition de transpositions choisies parmi $\{(i_2\ 2), (i_3\ 3), \ldots, (i_j\ j)\}$. C'est trivial pour $j = 0$ ou $j = 1$ (car le support d'une permutation ne peut pas avoir cardinal 1); supposons que c'est établi pour tout $j < k$. Soit donc π une permutation dont le support est contenu dans $[1, k]$ et contient le point k; comme les points $> k$ sont fixes et k est mobile, on doit avoir $\pi_k < k$. L'idée est d'obtenir π en effectuant d'abord une permutation σ dont le support est contenu dans $[1, k-1]$, puis la transposition $(i_k\ k)$, et finalement une autre permutation σ' fixant $k, \ldots, n$ comme σ; au total $\pi = \sigma \circ (i_k\ k) \circ \sigma'$. En posant $\rho = \sigma \circ (i_k\ k)$, il faut avoir $\pi_k = \rho_k = \sigma_{i_k}$. Comme π_k et i_k sont $< k$, on peut prendre pour σ la transposition $(i_k\ \pi_k)$ (ou $\sigma = \mathrm{id}$ si $i_k = \pi_k$), et l'écrire comme composition de transpositions choisies parmi $\{(i_2\ 2), (i_3\ 3), \ldots, (i_{k-1}\ k-1)\}$ d'après l'hypothèse de récurrence. On a donc $\rho_i = \pi_i$ pour $i \geq k$ (pour $i = k$ on vient de l'assurer, et tout $i > k$ est fixé par ρ comme par π). Alors, $\sigma' = \rho^{-1} \circ \pi$ fixe $k, \ldots, n$ et par une autre application de l'hypothèse de récurrence on l'écrit comme composition de transpositions choisies parmi $\{(i_2\ 2), (i_3\ 3), \ldots, (i_{k-1}\ k-1)\}$. Ainsi on a écrit π comme composition de transpositions choisies parmi $\{(i_2\ 2), (i_3\ 3), \ldots, (i_k\ k)\}$.*