Corrigé Travaux dirigés iL01 : Mathématiques Discrètes, Feuille 3 vendredi 23 septembre 2005

1. On désignera dans cet exercice le nombre d'orbites d'une permutation $\sigma \in \mathbf{S}_n$ par $m(\sigma)$. Dans le cours on a montré les deux faits suivants. (1) Si $\sigma \in \mathbf{S}_n$, et $\tau = (i\ j) \in \mathbf{S}_n$ est une transposition, alors le nombre d'orbites de $\sigma \circ \tau$ est donné par

$$m(\sigma \circ \tau) = \begin{cases} m(\sigma)+1 & \text{si } i \text{ et } j \text{ sont dans la même orbite de } \sigma, \\ m(\sigma)-1 & \text{si } i \text{ et } j \text{ sont dans des orbites différentes de } \sigma. \end{cases}$$

(2) Pour tout l-cycle γ il existe une écriture de γ comme la composée de $l-1$ transpositions: $(a_1\ \cdots\ a_l) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{l-1}\ a_l)$.

a. Rappeler l'argument qui montre que toute permutation $\sigma \in \mathbf{S}_n$ peut être écrite comme la composée de $n - m(\sigma)$ transpositions.

$\surd$ *Le nombre $n-m(\sigma)$ est égal au somme sur les cycles γ de σ de la quantité $l(\gamma)-1$, où $l(\gamma)$ désigne la longueur du cycle γ (car un l cycle contribue l a nombre n des points et 1 au nombre $m(\sigma)$ d'orbites ; les points fixes de σ contribuent 1 à chacune des deux quantités et donc 0 à $n-m(\sigma)$). Alors en écrivant chaque cycle γ comme composée de $l(\gamma)-1$ transpositions et en composant les expressions ainsi obtenues on obtient une écriture de σ du type cherché.*

b. Écrire de deux façons distinctes $\left(\begin{smallmatrix}1&2&3&4&5&6&7\\5&2&6&7&3&1&4\end{smallmatrix}\right) \in \mathbf{S}_7$ comme la composée de 4 transpositions.

$\surd$ *Cette permutation est égal à $(1\ 5\ 3\ 6) \circ (4\ 7)$ et s'écrit donc $(1\ 5)(5\ 3)(3\ 6)(4\ 7)$, ou encore $(4\ 7)(1\ 5)(5\ 3)(3\ 6)$ ou $(1\ 5)(4\ 7)(5\ 3)(3\ 6)$, mais aussi, $(5\ 3)(3\ 6)(6\ 1)(4\ 7)$ et il en reste, comme l'écriture $(1\ 3)(4\ 7)(1\ 6)(1\ 5)$ qui n'utilise pas la propriété (2).*

c. Montrer que le nombre $n - m(\sigma)$ de transpositions dans le point a est le minimum possible, c'est à dire que pour toute écriture de $\sigma \in \mathbf{S}_n$ comme la composée de k transpositions on aura $k \geq n - m(\sigma)$. [Indication : utiliser une récurrence sur la longueur de l'écriture.]

$\surd$ *On montre par récurrence sur k que toute composée $\sigma = \gamma_1 \circ \cdots \circ \gamma_k$ de k transpositions vérifie $m(\sigma) \geq n-k$, ce qui est équivalent à dire que aucun $\sigma \in \mathbf{S}_n$ ne peut être écrit comme composée de k transpositions avec $k < n - m(\sigma)$. Une composée de 0 transpositions donne id, qui vérifie bien $m(\mathrm{id}) = n \geq n$, donc pour $k = 0$ c'est bon. Soit donc $\sigma = \gamma_1 \circ \cdots \circ \gamma_k$ une composée de $k > 0$ transpositions. Par récurrence on suppose que $\sigma' = \sigma \circ \gamma_k = \gamma_1 \circ \cdots \circ \gamma_{k-1}$ vérifie $m(\sigma') \geq n-(k-1)$. D'après la propriété (1) on a $m(\sigma) = m(\sigma' \circ \gamma_k) \in \{m(\sigma')+1, m(\sigma')-1\}$ et donc $m(\sigma) \geq m(\sigma')-1 \geq n-k$, comme voulu.*

d. Sans utiliser la décomposition donnée explicitement dans la propriété (2), déduire l'énoncé de la question a directement de la propriété (1). Observer que ceci montre l'existence d'une écriture d'un l-cycles comme composée de $l-1$ transpositions, qui est peut-être différente de celle de la propriété (2).

$\surd$ *On raisonne par récurrence sur $n-m(\sigma)$. Si $n-m(\sigma) = 0$, chaque orbite est réduit à un point, et donc $\sigma = \mathrm{id}$, et dans ce cas une écriture vide convient. Supposons donc $n - m(\sigma) = k > 0$, et on suppose par récurrence que toute permutation $\pi \in \mathbf{S}_n$ avec $n - m(\pi) < k$ peut être écrite comme la composée de $n - m(\pi)$ transpositions. Comme le nombre d'orbites est strictement inférieur au nombre de points, il en existe une contenant au moins deux points (principe des tiroirs). On fixe une telle paire de points $\{i, j\}$ et on pose $\tau_k = (i\ \ j)$ et $\sigma' = \sigma \circ \tau_k$. D'après la propriété (1), on a $n - m(\sigma') = k-1$, donc par l'hypothèse de récurrence il existe une écriture $\sigma' = \tau_1 \circ \cdots \circ \tau_{k-1}$ de σ' comme composée de $k-1$ transpositions, et il en découle que $\sigma = \sigma' \circ \tau_k = \tau_1 \circ \cdots \circ \tau_k$ est une écriture de σ comme composée de k transpositions.*

e. On considère une décomposition d'une permutation $\sigma \in \mathbf{S}_n$ avec $\sigma \neq \mathrm{id}$ comme la composée de $n - m(\sigma)$ transpositions. En utilisant la propriété (1), montrer que la dernière transposition de la décomposition (celle la plus à droite) est une transposition de deux points d'une même orbite de σ (par exemple pour $\left(\begin{smallmatrix}1&2&3&4&5&6&7\\5&2&6&7&3&1&4\end{smallmatrix}\right) = (1\ 5\ 3\ 6) \circ (4\ 7)$, elle peut être $(1\ 5)$ ou $(4\ 7)$ ou $(1\ 3)$, mais pas $(1\ 4)$ ou $(2\ 7)$). En déduire par récurrence que toutes les autres transpositions de la décomposition ont aussi cette propriété d'échanger des points d'une même orbite.

$\surd$ *En reprenant le point précédent, si l'on avait pris $\tau_k = (i\ \ j)$ avec i et j dans les orbites différentes, on aurait eu $n - m(\sigma') = k+1$, ce qui d'après le point c rend une écriture $\sigma' = \tau_1 \circ \cdots \circ \tau_{k-1}$ impossible (il faudrait au moins $k+1$ transpositions), et une écriture $\sigma = \tau_1 \circ \cdots \circ \tau_k$ est donc aussi impossible. On prend donc un «bon» τ_k comme dans le point précédent, alors toutes les orbites* *de σ' sont contenues dans une seul orbite de σ : celles de σ' contentent i ou j sont des parties de l'orbite de σ content i et j, et les autres sont restées inchangées. Donc si l'on suppose par récurrence que toutes les transpositions utilisées dans l'écriture de σ' ont forcément leur support dans une seule orbite de σ', ils le seront aussi dans une seule orbite de σ, et pour la dernière transposition τ_k on vient de montrer la même propriété, donc toutes les τ_i utilisées dans l'écriture de σ ont forcément leur support dans une seule orbite de σ.*

f. On peut déduire du point précédent que le problème de trouver toutes les décompositions de $\sigma \in \mathbf{S}_n$ comme la composée de $n - m(\sigma)$ transpositions se réduit au cas particulier où σ est une l-cycle, et que pour ce cas on peut supposer que $n = l$ (c'est à dire on peut oublier les points qui ne sont pas dans le support du cycle). Indiquer comment on fait ces réductions ; par exemple pour la première réduction, en supposant qu'on connaisse pour chaque cycle de σ la liste de toutes ses décompositions en $l-1$ transpositions (où l est la longueur du cycle), montrer comment on peut en déduire la liste de toutes les décompositions de $\sigma \in \mathbf{S}_n$ en $n - m(\sigma)$ transpositions.

$\surd$ *On a vu dans le point précédent que pour trouver une décomposition de longueur minimale d'une permutation $\sigma \in \mathbf{S}_n$ comme composée de transpositions, on ne peut utiliser que des transpositions dont le support (la paire de points échangés) est contenu dans celui de σ, ce qui permet d'oublier les points fixe de σ. (Plus explicitement, si le nombre de points mobiles est n', on peut re-numéroter ces points $1, \ldots, n'$, trouver les décompositions pour la permutation correspondante dans $\mathbf{S}_{n'}$, et traduire les transpositions dans ces décompositions en termes de l'ancien numérotage.) Pour la réduction au cas des cycles, si pour chacun des cycles de σ on connaît toutes ses décompositions en $l-1$ transpositions, alors en choisissant une décomposition pour chaque cycle et les composant, on trouve toujours une décomposition de longueur $n-m(\sigma)$ de σ (car $n-m(\sigma)$ est égal à la somme sur tous les cycles de $l-1$, où l est la longueur du cycle). Mais dans cette composée, les transpositions venant de cycles distincts ont forcément des supports disjoints, et commutent donc entre eux. Ceci permet de permuter les transpositions dans la décomposition de σ, pourvu que l'ordre relatif des facteurs d'un même cycle soit toujours préservé. Comme pour chaque transposition on peut reconnaître (à l'aide de son support) le cycle auquel il appartient, on pourra toujours démêler les transpositions, et retrouver la décomposition initiale de σ utilisée.*
Il reste à vérifier que ce procédé produira toutes les décompositions possibles de σ de longueur $n - m(\sigma)$. On sait déjà que dans une telle décomposition toutes les transpositions opèrent dans le support d'un seul cycle de σ. Si on choisit un tel cycle γ et un point quelconque i dans son support, et on fait opérer les transpositions dans la décomposition sur i, seules les transpositions de points du support de γ peuvent faire bouger i. Par conséquent la composée de toutes ces transpositions aura le même effet sur i que σ tout entier, et donc que γ. La même conclusion est vraie pour tous les points du support de γ, donc la composée des transpositions mentionnées est égale à γ. Ainsi on extrait de la décomposition de σ des décompositions de chacun de ces cycles, et on voit que la décomposition de σ peut effectivement être obtenue par le procédé de choisir des décompositions minimales pour ses cycles, et de mêler les facteurs de cycles distincts.

g. Pour un 3-cycle donné, quel est le nombre de ses décompositions en 2 transpositions ? Et pour un 4-cycle γ donné, quel est le nombre de ses décompositions $\gamma = \sigma \circ \tau$ avec τ une transposition et σ un 3-cycle. Et pour le même γ, combien de telles décompositions avec τ une transposition et σ une permutation ayant deux 2-cycles à supports disjoints (donc de type $(2, 2)$ si $n = 4$). Du coup, quel est le nombre de ses décompositions de γ en 3 transpositions (en tenant compte de l'ordre, même pour les transpositions qui commutent entre eux) ?

$\surd$ *Pour un 3-cycle $(a\ b\ c)$ on peut choisir $(a\ b)$, $(a\ c)$ ou $(b\ c)$ comme dernier facteur, et ainsi trouver 3 décompositions $(a\ c) \circ (a\ b)$, $(b\ c) \circ (a\ c)$, et $(a\ b) \circ (b\ c)$. Pour un 4-cycle $\gamma = (a\ b\ c\ d) \in \mathbf{S}_n$ on a $\binom{4}{2} = 6$ choix différents pour la transposition finale τ dans un décomposition $\gamma = \sigma \circ \tau$ avec $n-m(\sigma) = (4-1)-1 = 2$. Cela laisse les possibilités que σ est un 3-cycle ou que σ est la composée de deux transpositions à supports disjoints. La première possibilité s'applique si la transposition permute deux points successifs dans le 4-cycle, donc si $\tau \in \{(a\ b), (b\ c), (c\ d), (d\ a)\}$, la seconde possibilité si $\tau \in \{(a\ c), (b\ d)\}$, donc les nombres des décompositions sont 4 et 2 (car en tout cas τ détermine $\sigma = \gamma \circ \tau$). Dans le cas où σ est un 3-cycle, il possède 3 décompositions et deux transpositions. Dans le cas où σ possède deux 2-cycles, chacun ne possède évidemment qu'une seul «décomposition» de longueur 1, mais on peut mêler ces facteurs de deux manières (car ils commutent). On trouve ainsi $4 \times 3 + 2 \times 2 = 16$ décompositions différentes pour γ.*

h. [Si vous avez le courage.] En généralisant le type de questions du point précédent, essayer de formuler une relation de récurrence qui permette de calculer pour chaque l le nombre de décompositions d'un l-cycle donné en $l-1$ transpositions. Finalement donner une formule qui donne le nombre de décompositions d'une permutation $\sigma \in \mathbf{S}_n$ du type $\lambda = (\lambda_1, \ldots, \lambda_k)$ comme la composée de $n - m(\sigma) = n - k$ transpositions. [Pour plus de renseignements sur la fonction de l définie par la récurrence, aller à `http://www.research.att.com/~njas/sequences/` et taper les premières valeurs 1, 1, 3, ...]

$\surd$ *On désignera par $f(l)$ le nombre de décompositions d'un l-cycle donné en $l-1$ transpositions, donc on a déjà trouvé $f(2) = 1$, $f(3) = 3$ et $f(4) = 16$. On posera également $f(1) = 1$ pour représenter le fait que 'id' se décompose en 0 transpositions d'une façon unique. La première chose à étudier est comment trouver le type d'une permutation réduite $\sigma = \gamma \circ \tau$ avec γ un l-cycle et τ une transposition de deux points de son support. On peur écrire la situation toujours comme $\gamma = (a_0 \ \cdots \ a_{l-1})$ et $\tau = (a_0 \ a_i)$ avec $0 < i < l$, et dans ce cas $\sigma = (a_1 \ \cdots \ a_i) \circ (a_0 \ a_{i+1} \ \cdots \ a_{l-1})$, qui est de type $(i, l-i)$. Il y a une ambiguïté due au choix du point a_0 (on pourrait aussi choisir l'autre point a_i du support de τ), ce qui permet de remplacer i par $l-i$ (le type $(i, l-i)$ est le même que $(l-i, i)$) ; ainsi on peut s'arranger pour que $0 < i \leq \frac{l}{2}$. Pour un type donné $(i, l-i)$ il existe l choix différents pour τ (chaque point du support pouvant être choisi pour a_0, l'autre point du support de τ étant déterminé par comme $a_i = \sigma^i(a_0)$), sauf que si $i = \frac{l}{2}$ deux choix pour a_0 donne la même transposition τ, d'où il n'y aura que $\frac{l}{2}$ choix différents dans ce cas. Pour le i-cycle et le $l-i$-cycle de σ il existe $f(i)$ respectivement $f(l-i)$ différentes décompositions de longueur $i-1$ respectivement $l-i-1$. Pour un choix donné d'une paire de décompositions, on peut mêler leurs $l-2$ facteurs de $\binom{l-2}{i-1}$ façon différentes. Ainsi on trouve la formule récurrente*

$$f(l) = \begin{cases} l \sum_{i=1}^{\frac{l-1}{2}} f(i) f(l-i) \binom{l-2}{i-1} & \text{si } l \text{ impair,} \\ \left(l \sum_{i=1}^{\frac{l}{2}-1} f(i) f(l-i) \binom{l-2}{i-1} \right) + \frac{l}{2} f\left(\frac{l}{2}\right)^2 \binom{l-2}{\frac{l}{2}-1} & \text{si } l \text{ pair,} \end{cases}$$

Par exemple on a $f(5) = 5\big(f(1)f(4)\binom{3}{0} + f(2)f(3)\binom{3}{1}\big) = 5(1 \times 16 \times 1 + 1 \times 3 \times 3) = 125$, ainsi que $f(6) = 6\big(f(1)f(5)\binom{4}{0} + f(2)f(4)\binom{4}{1}\big) + 3f(3)^2\binom{4}{2} = 6(1 \times 125 \times 1 + 1 \times 16 \times 4) + 3 \times 9 \times 6 = 1296$. La formule récurrente peut être simplifiée à

$$f(l) = \frac{l}{2} \sum_{i=1}^{l-1} f(i) f(l-i) \binom{l-2}{i-1}.$$

Pour une permutation de type $(\lambda_1, \ldots, \lambda_k)$ le nombre d'écritures sera $\frac{(n-k)! f(\lambda_1) \cdots f(\lambda_k)}{(\lambda_1 - 1)! \cdots (\lambda_k - 1)!}$, car des écritures de pour chaque cycle de σ, de longueurs respectives $\lambda_i - 1$ pour $i = 1, \ldots, k$, se mêlent de $\frac{(n-k)!}{(\lambda_1-1)! \cdots (\lambda_k-1)!}$ manières différentes. On a a priori très peu de raison de croire que la récurrence pour $f(l)$ permet une solution en formule close, mais les valeurs calculées suggèrent que $f(l)$ est une puissance de l, plus précisément

$$f(l) = l^{l-2} \qquad \text{pour } l \geq 1 \ ;$$

le site Web mentionné le confirme (et il donne également d'autres problèmes énumératifs donnant la même suite de nombres, notamment le nombre d'arbres sur n points étiquetés). Il n'est pas simple d'arriver à cette solution à partir de la récurrence, et il n'est même pas facile de voir que la formule proposée est une solution, c'est à dire que $l^{l-2} = \frac{l}{2} \sum_{i=1}^{l-1} \binom{l-2}{i-1} i^{i-2} (l-i)^{l-i-2}$ est valable pour tout $l \geq 2$.

2. On place les nombres $0, 1, \ldots, 15$ dans l'ordre sur les cases d'un carré 4×4. On va simuler un jeu bien connu, où 0 représente une case vide, et les autres cases sont remplies avec le nombre indiqué. On autorise donc comme opération la transposition du nombre 0 avec l'un de ses voisins, placé directement à gauche, à droite, en haut ou en bas du nombre 0 (par exemple dans la position initiale la transposition de 0 avec 1 ou avec 4 est possible. Montrer qu'il est impossible d'atteindre la position qui diffère de celle du départ par la transposition des nombres 14 et de 15.

$\surd$ *On montrera que toute position qu'on peut obtenir avec la case vide dans sa position initiale représente une permutation paire des cases remplies, ce qui exclut la possibilité de réaliser ainsi une transposition de deux cases replies comme 14 et 15. Comme ne sont autorisées que les transpositions qui déplacent le nombre 0, il suffit de montrer que le nombre total de ses déplacements est toujours pair quand ce nombre revient à sa position de départ. Mais si l'on colorie les cases comme un échiquier, chaque mouvement fait changer la couleur de la case contenant 0, d'où son nombre de mouvements est toujours pair quand il revient sur une case de sa couleur initiale, en particulier quand il revient sur sa case de départ.*