

Automorphismes de S_n (Perrin page 30-31)

Pierre Lissy

May 7, 2010

Remarque 1. Comme $\text{Int}(S_n) \simeq S_n/Z(S_n) = S_n$, on aura montré que $\text{Aut}(S_n) \simeq S_n$.

Les cas $n=1,2$ sont peu intéressants (ils sont intérieurs, ouais...). On suppose ici donc $n \geq 3$.

Lemme 1. On considère un automorphisme de S_n . Si cet automorphisme transforme toutes les transpositions en des transpositions, alors le morphisme est intérieur.

Proof. S_n est engendré par les permutations de la forme $\tau_i = (1, i)$. $\varphi(\tau_i)$ est une transposition. De plus, comme τ_i et τ_j sont non disjoints alors les images sont non disjointes. Si $\tau_2 = (\alpha_1, \alpha_2)$ et $\tau_3 = (\alpha_1, \alpha_3)$. Si $\varphi(\tau_i) = (\alpha_2, \alpha_i)$ alors comme les τ_i sont de support non disjoint on a nécessairement $i = 3$ et $(\alpha_1, \alpha_2)(\alpha_1, \alpha_3)(\alpha_2, \alpha_3) = (\alpha_1, \alpha_3)$, mais ceci entraîne en composant par φ^{-1} , $(12)(13)(1i) = (13)$, ce qui est impossible. Les α_i sont distincts, sinon on aurait pas injectivité de φ . On a donc construit une permutation $\alpha : i \mapsto \alpha_i$, et on a sur le système générateur τ_i , on a $\alpha\tau_i\alpha^{-1} = (\alpha_1, \alpha_i) = \varphi(\tau_i)$. Donc φ est l'automorphisme intérieur (i_α). $\square$

Lemme 2. Le centralisateur d'un élément s ayant k_1 points fixe, k_2 transpositions, etc avec $\sum k_i = n$ dans sa décomposition en cycles de support disjoints est de cardinal: $c(s) = \prod k_i! i^{k_i}$.

Proof. Faisons-le d'abord pour $n = ki$, ie un produit de k i -cycles à support disjoints. Alors en utilisant la formule de conjugaison des cycles et l'unicité de la décomposition en cycles disjoints, on obtient que l'élément du centralisateur doit nécessairement permuter les supports des cycles constituant s , ce qui nous donne $k!$ choix possibles. Mais après, si $w(x)$ est l'orbite de x alors $g(w(x))$ ne dépend évidemment que de $g(x)$, et du coup on aura choisi un élément du centralisateur une fois qu'on aura choisi un représentant dans chaque orbite, ce qui nous donne i^k choix possibles. D'où dans ce cas $k!i^k$ choix possibles.

Dans le cas d'un produit de cycles de longueurs différentes, on remarque que l'élément du centralisateur stabilise le produit des orbites de même taille (noté Ω_i) (puisque l'image d'une orbite doit être une orbite de même taille), de plus l'égalité définissant le centralisateur passe à la trace dans Ω_i . Ainsi on obtient bien grâce au point précédent ce qu'on veut. $\square$

C'est maintenant fini; En effet, si τ est une transposition alors $\varphi(\tau)$ est d'ordre 2, donc produit de k transpositions disjointes. On a clairement comme φ est bijective l'égalité $c(\varphi(\tau)) = \varphi(c(\tau))$ (une des inclusions est claire et cardinal après). Donc d'après le lemme précédent, on a $2(n-2)! = 2^k(k!)(n-2k)!$. Clairement $k \leq n/2$ par définition. $k = 0$ est impossible. Donc soit $k=1$ et dans ce cas on a bien $2(n-2)! = 2(n-2)!$. Sinon k est au moins égal à 2. $(n-2)! = (n-2)(n-3) \dots (n-2k+1)(n-2k)!$ donc $(n-2)(n-3) \dots (n-2k+1) = 2^{k-1}k!$. Remarquons que $k = 2$, n quelconque est impossible (pas de solution à $(n-2)(n-3) = 4$). De même, le cas $k = 3$ donne l'équation $(n-2)(n-3)(n-4)(n-5) = 24$ qui a pour unique solution $n = 6$ mais justement on a écarté ce cas. Supposons dorénavant $k \geq 4$. On remarque qu'en utilisant $2 \geq 2k$, on obtient $(n-2)(n-3) \dots (n-2k+1) \geq (2k-2)! > 2^{k-2}(k!)(k-1)!$. Mais $2^{k-2}k!(k-1)! > 2^k k!$ dès que $k \geq 4$, on ne peut donc pas avoir de solutions de l'équation ci-dessus. Ainsi sauf peut-être dans le cas $n = 6$, on a $k = 1$ et φ envoie les transpositions sur les transpositions. Citons le cas $n = 6$: on a des automorphismes qui ne sont pas intérieurs, plus précisément $\text{Aut}(S_n) \simeq \text{Int}(S_n) \rtimes \mathbb{Z}/2\mathbb{Z}$ mais on ne peut pas directement le montrer à l'aide du raisonnement précédent (il faut faire un autre raisonnement)