Concours Agrégation, Mathématiques générales

Leçon 05- Groupe des permutations d'un ensemble fini. Applications.

Commentaires du jury 2015 :

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple). Il est important de savoir déterminer les classes de conjugaisons du groupe symétrique par la décomposition en cycles, et, pour les candidats confirmés, dominer les problèmes de dénombrement qui en résultent. Des dessins ou des graphes illustrent de manière commode ce que sont les permutations. Par ailleurs, un candidat qui se propose de démontrer que tout groupe simple d'ordre 60 est isomorphe à A_5 devrait savoir donner des applications à la simplicité d'un groupe. L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Comme pour toute structure algébrique, il est souhaitable de s'intéresser aux automorphismes d'un groupe, par exemple, à ceux du groupe symétrique. On note que les candidats connaissent en général les applications du groupe symétrique aux polyèdres réguliers de l'espace.

Commentaires du jury 2016 :

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple). Il est important de savoir déterminer les classes de conjugaisons du groupe symétrique par la décomposition en cycles, d'être capable de donner des systèmes de générateurs. L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Les applications sont nombreuses, il est très naturel de parler des déterminants, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant aux automorphismes du groupe symétrique, à des problèmes de dénombrement ou aux représentations des groupes des permutations.

Remarques : Attention à la notion de cycle (c'est fonction des ouvrages !), en particulier proscrire l'abus qui consiste à parler de cycles de longueur 1. Il faut savoir justifier l'existence de l'homomorphisme signature (on pourra consulter [F. M. 2] p.135). On ne propose pas le développement sur $Aut(S_n)$ (voir [F. M. 1] $n°68$).

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf

Développements conseillés :

(1) Un théorème de Brauer sur la conjugaison des matrices de permutations en caractéristique nulle, [F. M. 1] $n°31$ p. 57. Pour la caractéristique quelconque voir [F. M. 2] p. 161.

(2) Un groupe simple d'ordre 60 est isomorphe à A_5, [F. M. 2] p. 146. Pour la simplicité des groupes A_n voir [F. M. 2] p. 137.

(3) Représentations irréductibles de S_n de degré $n-1$, [F. M. 1] $n°82$ p. 221 et [F. M. 2] p. 164.

Exercice 1 L'homomorphisme signature, [F. M. 2] p.135.

Exercice 2 Décomposition en transpositions [F. M. 1] $n°$ 62 (pour une variante avec les graphes voir [F. M. 2] p. 143 + [F. M. 2] Compléments et errata.

Exercice 3 Calcul de signatures. [F. M. 1] $n°72$ seulement les questions 0 et 4.

Exercice 4 Générateurs de A_n et sous-groupes distingués de S_n [F. M. 1] $n°64$ p. 155

Exercice 5 Commutateurs de S_n et A_n [F. M. 1] $n°63$ p. 153

Exercice 6 Classes de conjugaisons de A_4 (pour le cas général de A_n voir [F. M. 2] p.140).

Preuve. Les 2-2 cycles sont conjugués. En effet puisqu'ils sont conjugués dans S_4 il suit par exemple qu'il existe $\sigma \in S_4$ avec $\sigma(1,2)(3,4)\sigma^{-1} = (1,3)(2,4)$ et donc $(1,3)\sigma(1,2)(3,4)\sigma^{-1}(1,3)^{-1} = (1,3)(2,4)$. Mais σ ou $(1,3)\sigma$ appartient à A_4 ; ainsi les 2-2 cycles sont conjugués dans A_4 comme dans S_4 coïncident.

Voyons les 3-cycles. Soit $\sigma := (1,2,3)$. On considère l'action de A_4 par conjugaison sur lui-même, le stabilisteur $(A_4)_\sigma = \{\tau \in A_4 \mid (1,2,3) = (\tau(1),\tau(2),\tau(3))$; ainsi si $\tau \in (A_4)_\sigma$ alors le support de τ est inclus dans $\{1,2,3\}$ et puisque $\tau \in A_4$, il suit que $(A_4)_\sigma =< \sigma >$. Ainsi $|orb(\sigma) = \frac{|A_4|}{|(A_4)_\sigma|} = 4$. Puisque les 3-cycles sont conjugués dans S_4 ils donnent naissance à 2-classes de conjugaison dans A_4. ///

Exercice 7 Sous-groupes d'ordre p de S_n [F. M. 1] $n°66$ p. 160

Exercice 8 p-sous-groupes de Sylow de S_n, [F. M. 1] $n°69$ p. 165.

Le cas $n = p$ ou p^2 (exercice corrigé).

Soit $n \in \mathbb{N}^\star$ et p un nombre premier. On note S_n le groupe symétrique sur $\{1,2,....,n\}$.

(1) Les p sous-groupes de Sylow de S_p

(a) Si $a \in \mathbb{N}$, on note $r(a)$ l'entier de $\{1,2,...,p\}$ avec $p|(a - r(a))$. Soit $1 \leq k \leq p-1$, montrer que $(1,2,...,p)^k$ est égal au cycle $(r(1), r(1+k), r(1+2k), ..., r(1+(p-1)k))$ de longueur p.

Preuve. Soit $0 \leq i \leq j \leq p-1$, alors $1 + ik = 1 + jk \mod p$ si et seulement $p|(j-i)k$ i.e. $i = j$. Il suit que $|\{r(1), r(1+k), r(1+2k), ..., r(1+(p-1)k)\} = p$. Puisque $(1,2,...,p)^k(j) = r(j+k)$ pour $1 \leq j \leq p$ il suit que les deux permutations coïncident.///

(b) Montrer que les p sous-groupes de Sylow de S_p sont cycliques d'ordre p et que leurs éléments sont soit l'identité, soit des cycles de longueur p.

Preuve. Par le théorème de Sylow les p sous-groupes de Sylow sont conjugués. La question précédente montre que le groupe $< (1,2,...,p) >$ est cyclique d'ordre p et que ses éléments sont soit l'identité, soit des cycles de longueur p. Ces propriétés étant stables par conjugaison le résultat suit.///

(c) Soit n_p le nombre de p sous-groupes de Sylow de S_p . Vérifier que n_p divise $(p-1)!$ et que $n_p = 1 \mod p$.

Preuve. Le nombre de p cycles est égal au nombre de p-uplets d'éléments distincts de $\{1,2,...,p\}$ en identifiant les p écritures d'un p cycle. Il y en a donc $\frac{p!}{p} = (p-1)!$ (on peut aussi bien compter les orbites de 1). Ainsi $n_p = \frac{(p-1)!}{p-1} = (p-2)!$. Le théorème de Wilson dit que $(p-1)! = -1 \mod p$; ainsi $n_p = 1 \mod p$.///

(2) Les p sous-groupes de Sylow de S_{p^2}

(a) Soit $0 \leq i \leq p-1$ et σ_i le cycle $(1+ip, 2+ip, ..., p+ip) \in S_{p^2}$. Soit $H :=< \sigma_0, ..., \sigma_{p-1} > \subset S_{p^2}$. Montrer que H est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^p$.

Preuve. Les cycles σ_i sont à supports disjoints, ainsi l'application $\varphi : \mathbb{Z}^p \to S_{p^2}$ avec $\varphi(a_0, a_1, ..., a_{p-1}) = \sigma_0^{a_0}...\sigma_{p-1}^{a_{p-1}}$ est un homomorphisme de groupes dont le noyau est $(p\mathbb{Z})^p$. D'autre part soit $\pi : \mathbb{Z}^p \to (\mathbb{Z}/p\mathbb{Z})^p$ l'homomorphisme obtenu par réduction modulo p sur chaque composante ; son noyau est aussi $(p\mathbb{Z})^p$. On conclut avec le théorème de factorisation des homomorphismes de groupes.///

(b) Soit τ défini par $\tau(x) = x + p \mod p^2$ pour $x \in \{1, 2, ..., p^2\}$. Montrer que $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$ pour $0 \leq i \leq p-2$ et $\tau\sigma_{p-1}\tau^{-1} = \sigma_0$.

Preuve. On a $\tau\sigma_i\tau^{-1} = (\tau(1+ip), \tau(2+ip), ..., \tau(p+ip))$ *et puisque* $\tau(1+ip) = 1 + (i+1)p \mod p^2$, *il suit que* $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$ *pour* $0 \leq i \leq p-2$ *et* $= \sigma_0$ *pour* $i = p-1$.///

(c) Soit $K =< \tau >$. Montrer que $H \cap K = Id$.

Preuve. Le groupe $H \cap K$ *est un sous-groupe de* $< \tau >$, *ainsi il existe* $0 \leq a \leq p-1$ *avec* $H \cap K =< \tau^a >$. *Il suit de b) que* $\tau^a\sigma_i\tau^{-a} = \sigma_{t_i}$ *avec* $t_i = a + i \mod p$ *et puisque* H *est abélien on a* $t_i = i$, *d'où* $a = 0$.///

(d) Soit $Syl_p := HK := \{hk \mid h \in H,\ k \in K$. Montrer que Syl_p est un sous-groupe de Sylow de S_{p^2}.

Preuve. Le groupe H *est stable par conjugaison par* σ_i *par* τ *(question b), ainsi* $hkh'k' = h(kh'k^{-1})kk' \in HK$ *pour* $h, h' \in H$ *et* $k, k' \in K$ *et* $(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in HK$. *Enfin il suit de c) que* $|HK| = |H||K| = p^2$.///

(e) Montrer que les p sous-groupes de Sylow de S_{p^2} sont isomorphes au produit semi-direct $(\mathbb{Z}/p\mathbb{Z})^p \times_\tau \mathbb{Z}/p\mathbb{Z}$ où $\mathbb{Z}/p\mathbb{Z}$ agit via τ sur $(\mathbb{Z}/p\mathbb{Z})^p$ par permutation circulaire des p composantes.

Preuve. On calcule $\tau\sigma_0^{a_0}...\sigma_{p-1}^{a_{p-1}}\tau^{-1} = \sigma_1^{a_0}...\sigma_{p-1}^{a_{p-2}}\sigma_0^{a_{p-1}} = \sigma_0^{a_{p-1}}\sigma_1^{a_0}...\sigma_{p-1}^{a_{p-2}}$. *Ainsi avec a)* τ *agit sur* $(a_0, a_1, ..., a_{p-1})$ *par* $\tau \star (a_0, a_1, ..., a_{p-1}) = (a_1, a_2, ..., a_{p-1}, a_0)$.///

(f) Eléments d'ordre p^2 dans le groupe Syl_p.

Montrer que $\rho := (\prod_{1 \leq i \leq p-1} \sigma_i)\tau$ est d'ordre p^2.

Preuve. Soit $\pi := \prod_{0 \leq i \leq p-1} \sigma_i$, *facilement* $\tau\pi\tau^{-1} = \pi$; *ainsi* $\tau\rho\tau^{-1} = (\sigma_0\sigma_1^{-1})\rho$. *On déduit que pour* $1 \leq a \leq p$, *on a* $(*)$ $\rho^a = (\prod_{0 \leq k \leq a-1} \sigma_k^{-1})\pi^a\tau^a$. *Ainsi* $\rho^p = \pi^{-1}$ *et* ρ *est d'ordre* p^2.

Remarque. La formule $(*)$ *vaut pour* $a \geq 1$ *avec la convention que* $\sigma_k = \sigma_{r(k)}$ *où* $r(k)$ *est le reste de la division de* k *par* p. *Ainsi* $\tau\rho\tau^{-1} = \rho^a$ *si et seulement si* $\rho^{a-1} = \sigma_0\sigma_1^{-1}$ *ce qui implique* $a = p+1$ *et donc que* $p = 2$. *Il suit que si* $< \rho >$ *est distingué dans* Syl_p, *alors* $p = 2$. ///