Théorème de Brauer

Leçons concernées

* **101 :** Groupe opérant sur un ensemble. Exemples et applications.
* **105 :** Groupe des permutations d'un ensemble fini. Applications.
* **108 :** Exemples de parties génératrices d'un groupe. Applications.
* **150 :** Exemples d'actions de groupes sur les espaces de matrices.
* **190 :** Méthodes combinatoires, problèmes de dénombrement.

Théorème. *Soit $\mathbb{K}$ un corps de caractéristique nulle. Soit n entier naturel non nul et σ, τ deux permutations de S_n. On définit P_σ la matrice de passage de la base canonique de $\mathbb{K}^n$ $(e_1, ..., e_n)$ dans la base $(e_{\sigma(1)}, ..., e_{\sigma(n)})$, de sorte que $P_\sigma x = (x_{\sigma^{-1}(1)}, ..., x_{\sigma^{-1}(n)})$.*
Alors σ et τ sont conjugués dans S_n si et seulement si P_σ et P_τ sont semblables.

Ainsi, la conjugaison dans S_n se transporte de la même manière que la conjugaison des matrices de permutations dans $GL_n(\mathbb{K})$.

Preuve : Le sens direct est ... direct, car l'application qui à σ associe P_σ est un morphisme de groupe.

La réciproque est plus délicate. Soient σ et τ dans S_n tels que P_σ et P_τ sont semblables dans $GL_n(\mathbb{K})$. On démontre un premier lemme :

Lemme. *σ et τ sont conjugués si et seulement si pour tout $p \in [\![1; n]\!]$, $c_p(\sigma) = c_p(\tau)$ où c_p désigne le nombre de p-cycles dans la décomposition en produit de cycles à support disjoints.*

Ce résultat est direct en sachant que, pour tout $a_1, ..., a_p$ des entiers entre 1 et n, et pour tout $\gamma \in S_n$, $\gamma(a_1, ..., a_p)\gamma^{-1} = (\gamma(a_1), ..., \gamma(a_p))$.

Nous allons alors regarder le vecteur $x = (c_1(\sigma) - c_1(\tau), ..., c_n(\sigma) - c_n(\tau))$, que nous voulons nul afin de démontrer le théorème. L'astuce sera de trouver une matrice inversible B telle que $Bx = 0$.

Intéressons nous, pour $\gamma \in S_n$, à $V^\gamma = Ker(P_\gamma - I)$ le sous-espace propre associé à la valeur propre 1 pour P_γ. Calculons la dimension de cet espace. Si on pose $y = (y_1, ..., y_n)$, $y \in P_\gamma$ si et seulement si $P_\gamma y = y$, c'est-à-dire $\forall i \in [\![1; n]\!]$, $y_{\gamma(i)} = y_i$. En multipliant à gauche l'égalité par P_γ, on remarque alors que ceci est équivalent à dire que pour tout i et j entre 1 et n, $y_i = y_j$ dès que i et j sont dans la même orbite sous l'action de $< \gamma >$ sur $[\![1; n]\!]$.
On obtient ainsi que $dim(V^\gamma)$ est égal au nombre d'orbites pour cette action, c'est-à-dire le nombres de cycles dans la décomposition à supports disjoints de γ (en comptant les cycles de longueur 1), soit : $dim(V^\gamma) = \displaystyle\sum_{p=1}^{n} c_p(\gamma)$.

Puisque P_σ et P_τ sont semblables, il en est de même pour leur puissance, donc pour tout k entier non nul, P_{σ^k} et P_{τ^k} sont semblables, leur sous-espaces propres sont alors isomorphes. Ainsi on a l'égalité

$dim(V^{\sigma^k}) = dim(V^{\tau^k})$. Que nous donne cette égalité ?

Pour répondre à cette question, donnons un autre lemme, qui va nous permettre de voir le nombre de cycles dans la décomposition de σ^k et τ^k :

Lemme. *Soit $c = (a_1, ..., a_p)$ un p-cycle, et soit k entier naturel non nul. Alors c^k est produit de cycles de longueur $\frac{p}{p \wedge k}$ qui sont au nombre de $p \wedge k$.*

Pour démontrer ce lemme, regardons le comportement de l'action de $< c^k >$ sur $[\![1; n]\!]$. Il suffit de regarder son comportement sur les éléments de son support. Soit i entre 1 et p et soit $\omega(a_i)$ l'orbite de a_i sous cette action. Alors $\omega(a_i) = \{a_{i+mk} \mid m \in \mathbb{N}^*\}$ où les indices sont bien-sûr pris modulo p. Pour chercher le nombre d'élément de cette orbite, cherchons m le plus petit entier non nul tel que $mk = 0[p]$. Pour ce faire, $p|mk$ si et seulement si $\frac{p}{p \wedge k}|m\frac{k}{p \wedge k}$ si et seulement si $\frac{p}{p \wedge k}|m$ d'après le lemme de Gauss. L'orbite est donc de longueur $\frac{p}{p \wedge k}$, et puisque le support de c possède p éléments, il doit y avoir $p \wedge k$ tels cycles. Le lemme est démontré.

Ainsi, chaque p-cycle dans la décomposition en produit de cycles à supports disjoints de σ va rapporter $p \wedge k$ orbites. Donc les p-cycles vont tous rapporter $c_p(\sigma)p \wedge k$ orbites. En sommant sur tous les p-cycles, on obtient au final, par égalité des dimensions, $\displaystyle\sum_{p=1}^{n} c_p(\sigma)p \wedge k = \sum_{p=1}^{n} c_p(\tau)p \wedge k$. Donc, si $B = (i \wedge j)_{1 \leq i,j \leq n}$, alors $Bx = 0$. Reste à montrer que B est inversible.

Si nous définissons $A = (a_{ij})$ où a_{ij} vaut 1 si i divise j, et 0 sinon, alors un calcul direct nous montre que ${}^tAdiag(\varphi(1), ..., \varphi(n))A = B$, en utilisant l'égalité $i \wedge j = \displaystyle\sum_{d|i \wedge j} \varphi(d) = \sum_{d|i \text{ et } d|j} \varphi(d)$. Puisque A est triangulaire supérieure de diagonale 1, A est bien sûr inversible. Enfin, la matrice diagonale composé des indicatrices d'Euler ne fait intervenir que des éléments non nuls, puisque la caractéristique du corps est nul.

Ceci démontre alors que B est inversible, et donc $x = 0$, ce qui prouve le théorème.