
Théorème de Brauer

Lemme — Soit $c = (a_1 \dots a_p) \in \mathfrak{S}_n$ un p -cycle. Soit $k \in \mathbb{N}^*$. Alors c^k est un produit de $k \wedge p$ cycles de longueur $\frac{p}{k \wedge p}$.

DÉMONSTRATION

Soit $i \in \llbracket 1; p \rrbracket$.

L'orbite de a_i sous l'action de $\langle c^k \rangle$ est l'ensemble $\{a_{i+km}, m \in \mathbb{N}\}$ où l'indice $i + km$ est considéré modulo p .

On cherche le plus petit $m \in \mathbb{N}^*$ tel que $km \equiv 0 [p]$.

$$\begin{aligned} p \mid km &\Leftrightarrow \frac{p}{k \wedge p} \mid \frac{k}{k \wedge p} m \\ &\Leftrightarrow \frac{p}{k \wedge p} \mid m \text{ par théorème de Gauß car } \frac{p}{k \wedge p} \wedge \frac{k}{k \wedge p} = 1. \end{aligned}$$

Donc l'orbite de a_i sous l'action de $\langle c^k \rangle$ est $\left\{ a_{i+km}, 0 \leq m < \frac{p}{k \wedge p} \right\}$.

Ainsi le cycle dans la décomposition de c^k contenant a_i est de cardinal $\frac{p}{k \wedge p}$.

Comme cette conclusion est vraie pour tout a_i , c^k est produit de $\frac{p}{k \wedge p}$ -cycles.

Pour des raisons de cardinal, il y en a $k \wedge p$. $\square$

Théorème

Soit K un corps de caractéristique nulle. Soit $n \in \mathbb{N}^*$.

Soient $\sigma, \tau \in \mathfrak{S}_n$. On note P_σ et P_τ les matrices de permutation associées.

Alors σ et τ sont conjuguées dans $\mathfrak{S}_n$ si et seulement si P_σ et P_τ sont conjuguées dans $\mathcal{M}_n(K)$.

DÉMONSTRATION

$\Rightarrow$ Par hypothèse, il existe $\gamma \in \mathfrak{S}_n$ tel que $\sigma = \gamma\tau\gamma^{-1}$.

Comme l'application $\mathfrak{S}_n \rightarrow \text{GL}_n(K)$ définie par $s \mapsto P_s$ est un morphisme,

$$P_\sigma = P_\gamma P_\tau P_\gamma^{-1}.$$

⇐ On cherche à montrer que σ et τ sont de même type.

Si pour tout $p \in \llbracket 1; n \rrbracket$, on note $c_p(\sigma)$ et $c_p(\tau)$ le nombre de p -cycles de respectivement τ et σ , on cherche à montrer que

$$\forall p \in \llbracket 1; n \rrbracket, c_p(\sigma) = c_p(\tau).$$

On cherche à montrer qu'il existe $B \in \text{GL}_n(K)$ tel que $Bx = 0$ où $x = (c_1(\sigma) - c_1(\tau), \dots, c_n(\sigma) - c_n(\tau))$.

Soit $\gamma \in \mathfrak{S}_n$.

On pose $V_\gamma = \ker(P_\gamma - I_n)$ sous-espace propre de P_γ .

Soit $y \in \mathbb{R}^n$.

$$y \in V_\gamma \Leftrightarrow P_\gamma y = y \Leftrightarrow \forall k \in \mathbb{N}, P_\gamma^k y = y \Leftrightarrow \forall k \in \mathbb{N}, \forall i \in \llbracket 1; n \rrbracket, y_{\gamma^k(i)} = y_i.$$

Donc $y \in V_\gamma$ si et seulement si $y_i = y_j$ dès que i et j sont dans la même orbite de $\llbracket 1; n \rrbracket$ sous l'action de $\langle \gamma \rangle$.

On en déduit que la dimension de V_γ est le nombre d'orbites de $\llbracket 1; n \rrbracket$ sous l'action de $\langle \gamma \rangle$, c'est-à-dire son nombre de cycles (en comptant les cycles de longueur 1).

$$\dim V_\gamma = \sum_{p=1}^n c_p(\gamma).$$

Comme P_σ et P_τ sont semblables, c'est aussi le cas de P_σ^k et P_τ^k pour tout $k \in \mathbb{N}$. Donc V_{σ^k} et V_{τ^k} sont isomorphes. En particulier,

$$\dim V_{\sigma^k} = \dim V_{\tau^k}$$

soit

$$\sigma^k \text{ et } \tau^k \text{ ont le même nombre de cycles}$$

soit d'après le lemme

$$\sum_{p=1}^n (k \wedge p) [c_p(\sigma) - c_p(\tau)] = 0$$

soit

$$Bx = 0 \text{ où } B = (i \wedge j)_{1 \leq i, j \leq n}.$$

On pose $A = (a_{i,j})_{1 \leq i,j \leq n}$ où $a_{i,j} = \begin{cases} 1 & \text{si } i \mid j \\ 0 & \text{sinon} \end{cases}$.

Alors

$$\begin{aligned}
 {}^t A \cdot \text{diag}(\varphi(1) \dots \varphi(n)) \cdot A &= {}^t A \cdot (\varphi(i) a_{i,j})_{1 \leq i,j \leq n} \text{ où } \varphi \text{ est l'indicatrice d'Euler} \\
 &= \left(\sum_{k=1}^n a_{k,i} \varphi(k) a_{k,j} \right)_{1 \leq i,j \leq n} \\
 &= \left(\sum_{k \mid i \text{ et } k \mid j} \varphi(k) \right)_{1 \leq i,j \leq n} \\
 &= \left(\sum_{k \mid i \wedge j} \varphi(k) \right)_{1 \leq i,j \leq n} \\
 &= (i \wedge j)_{1 \leq i,j \leq n} \\
 &= B.
 \end{aligned}$$

Comme A est triangulaire supérieure à diagonale de 1 et D est diagonale à coefficients strictement positifs, $B = {}^t A \cdot \text{diag}(\varphi(1) \dots \varphi(n)) \cdot A$ est inversible.

□