

Lemme. σ et $\tau \in S_n$ sont conjuguées si et seulement si elles admettent le même nombre de cycle de longueur k pour tout k dans leur décomposition en cycles à support disjoints.

Démonstration. **Pour le sens direct :** Facile. Le résultat provient de la formule de conjugaison des cycles.

Pour le sens réciproque : On procède ici par construction. Écrivons

$$\sigma = (s_{1,1}..s_{k_1,1})...(s_{1,r}..s_{k_r,r}) \text{ et } \tau = (t_{1,1}..t_{k_1,1})...(t_{1,r}..t_{k_r,r})$$

les décomposition en cycles à support disjoints de σ et τ , y compris les cas $k_i = 1$. On a $\{s_{i,j}\} = \{t_{i,j}\} = \{1, ..., n\}$, donc $\alpha : s_{i,j} \mapsto t_{i,j}$ est une application surjective de $\{1, ..., n\}$ dans lui-même. α est donc un élément de S_n , et on peut vérifier que

$$\tau = \alpha \sigma \alpha^{-1}$$

i.e. σ et τ sont conjuguées. □

Soit $\mathbb{K}$ un corps de caractéristique nulle, et pour $\sigma \in S_n$, on note $P_\sigma = (\delta_{i,\sigma(j)}) \in GL_n(\mathbb{K})$.

Théorème (Brauer). σ et $\tau \in S_n$ sont conjuguées si et seulement si P_σ et $P_\tau \in GL_n(\mathbb{K})$ sont similaires.

Démonstration. **Pour le sens direct :** Facile vu que $\sigma \mapsto P_\sigma$ est un morphisme (vous pouvez présenter brièvement le calcul si vous voulez).

Pour le sens réciproque : On note $(e_1, ..., e_n)$ la base canonique de $\mathbb{K}^n$, et pour $\sigma \in S_n$, $\tilde{\sigma} \in GL(\mathbb{K}^n)$ défini par $\tilde{\sigma}(e_i) = e_{\sigma(i)}$, l'endomorphisme canoniquement associé à P_σ . Pour $q \in \mathbb{N}^*$, on pose $c_q = (1 \dots q) \in S_q$, on a :

$$P_{c_q} := \tilde{P}_q = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & (0) & \\ & \ddots & \ddots & \\ (0) & & 1 & 0 \end{pmatrix} \in \mathcal{M}_q(\mathbb{K})$$

Donc $\chi_{P_{c_q}} = X^q - 1$.

Soit $\sigma \in S_n$. $\sigma = \mu_1 \dots \mu_r$ sa décomposition en cycles à supports disjoints. On note : $\mu_i = (a_{i,1} \dots a_{i,q_i})$; $S_i = \text{supp}(\mu_i)$; $\mathcal{B}_i = (e_{a_{i,1}} \dots e_{a_{i,q_i}})$; $W_i = \text{Vect}(\mathcal{B}_i)$; $S = (\bigsqcup_i S_i)^C$; $\mathcal{B}_S = (e_j)_{j \in S}$; $\mathcal{B} = \mathcal{B}_1 \sqcup \dots \sqcup \mathcal{B}_r \sqcup \mathcal{B}_S$

Chaque W_i est stable par $\tilde{\mu}_i$ et $\tilde{\mu}_i|_{W_i}$ va se comporter comme un $\tilde{c}_{q_i}$ dans la base $\mathcal{B}_i$. Ainsi, en étudiant $\tilde{\sigma}$ dans la base $\mathcal{B}$, on a :

$$P_\sigma \sim \begin{pmatrix} \tilde{P}_{q_1} & & \\ & \ddots & (0) \\ (0) & & \tilde{P}_{q_r} \\ & & & I_{|S|} \end{pmatrix} \text{ et donc } \chi_{\tilde{\sigma}} = \prod_{i=1}^r (X^{q_i} - 1) \times (X - 1)^{|S|}$$

soit encore, en notant $d_k(\sigma)$ le nombre de k -cycles dans la décomposition de σ :

$$\chi_{\tilde{\sigma}} = \prod_{k=1}^n (X^k - 1)^{d_k(\sigma)}$$

Maintenant, si P_σ et P_τ sont similaires, alors $\chi_{\tilde{\sigma}} = \chi_{\tilde{\tau}}$. Soit $\omega \in \mathbb{K}^{alg}$ une racine primitive m -ième de l'unité. En étudiant la multiplicité de ω dans la relation précédente, on a :

$$\forall m, \sum_{m|k} d_k(\sigma) = \sum_{m|k} d_k(\tau) \quad (*)$$

On va en déduire que $d_k(\sigma) = d_k(\tau)$ pour tout k . Supposons par l'absurde que ce n'est pas le cas, i.e. $\exists k \mid d_k(\sigma) \neq d_k(\tau)$. Comme $d_i(\sigma) = d_i(\tau) = 0 \forall i > n$, soit k' le plus grand indice tel que $d_{k'}(\sigma) \neq d_{k'}(\tau)$. La relation $(*)$ dans le cas $m = k'$ donne :

$$\sum_{k'|k} d_k(\sigma) = \sum_{k'|k} d_k(\tau)$$

or, par hypothèse sur k' , si $k'|k$ et $k' \neq k$, alors $d_k(\sigma) = d_k(\tau)$. Il ne reste alors que $d_{k'}(\sigma) = d_{k'}(\tau)$, c'est une contradiction (on pouvait aussi procéder par récurrence descendante forte à partir de n , mais l'hérédité fait intervenir exactement le même raisonnement, mais c'est vous qui voyez ce que vous préférez).

Ainsi $d_k(\sigma) = d_k(\tau)$ pour tout k , et le lemme nous permet d'en déduire que σ et τ sont conjuguées.

□