Pour $\sigma \in S_n$, on note $P_\sigma := (\delta_{i,\sigma(j)})_{1\leq i,j\leq n}$.

Théorème 0.0.1 :

> Soit $\mathbb{K}$ un corps de caractéristique nulle, $\sigma, \tau \in S_n$, $n \geq 2$.
> σ et τ sont conjuguées si et seulement si P_σ et P_τ sont semblables dans $\mathcal{M}_n(\mathbb{K})$.

Tout d'abord, notons que $\phi : \sigma \in S_n \mapsto P_\sigma \in GL_n(\mathbb{K})$ est un morphisme de groupes. Donc si σ et τ sont conjuguées dans S_n, alors P_σ et P_τ sont semblables dans $GL_n(\mathbb{K})$.

Réciproquement, soit $\sigma, \tau \in S_n$. Supposons que P_σ et P_τ soient semblables dans $GL_n(\mathbb{K})$. Pour $p \in [\![1,n]\!]$, on note $c_p(\sigma)$ le nombre de p-cycles dans la décomposition en cycles à support disjoint de σ.
Remarque : $c_1(\sigma)$ désigne le nombre de points fixes de σ.
$c_p(\sigma)$ est le nombre d'orbites de cardinal p pour l'action naturelle de $<\sigma>$ sur $[\![1,n]\!]$.

Notons $v := (c_p(\sigma) - c_p(\tau))_{1\leq p\leq n}$. Notre but est de trouver $B \in GL_n(\mathbb{K})$ telle que $Bv = 0$. On aura alors que $\forall p \in [\![1,n]\!],\ c_p(\sigma) = c_p(\tau)$, i.e. σ et τ sont conjuguées.

L'hypothèse donne que pour tout $k \geq 1$, P_{σ^k} et P_{τ^k} sont semblables. Donc si l'on note $n_\sigma := \dim\ker(P_\sigma - I_n)$, on a $\forall k \geq 1,\ n_{\sigma^k} = n_{\tau^k}$.
On remarque que $w \in \ker(P_\sigma - I_n)$ si et seulement si $\forall i,\ w_{\sigma^{-1}(i)} = w_i$, si et seulement si $w_i = w_j$ dès lors que i et j appartiennent à la même orbite sous l'action de $<\sigma>$ sur $[\![1,n]\!]$. Donc n_σ correspond au nombre d'orbites sous l'action de $<\sigma>$ sur $[\![1,n]\!]$, et donc $n_\sigma = \sum_{p=1}^n c_p(\sigma)$.

Lemme 0.0.2 :

> Soit $k \geq 1$ et $c = (a_1 \cdots a_p) \in S_n$ un p-cycle. Alors c^k se décompose en produit de $p \wedge k$ cycles à supports disjoints de longueur $p/(p\wedge k)$.

Démonstration. L'orbite de a_i sous l'action de c^k est $\{a_{i+nk\ [p]} \mid n \in \mathbb{Z}\}$, de cardinal le plus petit entier $r \geq 1$ tel que $kr = 0\ [p]$. Or

$$p \mid rk \ \Leftrightarrow\ \frac{p}{p\wedge k} \mid r\frac{k}{p\wedge k} \ \Leftrightarrow\ \frac{p}{p\wedge k} \mid r \text{ (lemme de Gauss)}$$

Donc $r = p/(p\wedge k)$. □

Ainsi, on obtient pour tout $k \geq 1$, $n_{\tau^k} = n_{\sigma^k} = \sum_{p=1}^n c_p(\sigma)(p\wedge k)$, ce qui sécrit matriciellement sous la forme $Bv = 0$, avec $B = (i \wedge j)_{1\leq i,j\leq n}$.

Lemme 0.0.3 :

> B est inversible.

Démonstration. On écrit, en notant ϕ l'indicatrice d'Euler et $a_{n,m} = \mathbf{1}_{n\mathbb{Z}}(m)$:

$$i \wedge j = \sum_{d\mid(i\wedge j)} \phi(d) = \sum_{d=1}^n \phi(d) a_{d,i} a_{d,j}$$

En particulier, si l'on pose $A = (a_{i,j})_{1\leq i,j\leq n}$ (matrice triangulaire supérieure avec des 1 sur la diagonale) et $\Phi = \mathrm{diag}(\phi(1), \cdots, \phi(n))$, on obtient $B = A\Phi A^T$. Donc $\det(B) = \prod_{k=1}^n \phi(k) \neq 0$. □