

Théorème 0.0.1 :

Soit G un groupe d'ordre $n \in \mathbb{N}^*$.

La table de caractères de G est à valeurs entières si et seulement si pour tout $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$ et tout $g \in G$, g^k et g sont dans la même classe de conjugaison.

On fait agir $(\mathbb{Z}/n\mathbb{Z})^* \curvearrowright G$ par $k \cdot g = g^k$. On note $P_n \subset \llbracket 1, n \rrbracket$ l'ensemble des entiers premiers avec n et Φ_n le polynôme cyclotomique d'ordre n .

Lemme 0.0.2 :

Si $\omega \in \mathbb{C}$ est une racine primitive n -ième de l'unité, alors pour tout $k \in P_n$, il existe un unique $\zeta_k \in \text{Aut}(\mathbb{Q}[\omega])$ tel que $\zeta_k(\omega) = \omega^k$ et ζ_k fixe \mathbb{Q} .

Démonstration. Existence :

Comme Φ_n est irréductible et que $\Phi_n(\omega) = 0$, le morphisme d'évaluation en ω induit un isomorphisme $\mathbb{Q}[X]/(\Phi_n) \rightarrow \mathbb{Q}[\omega] \simeq \mathbb{Q}(\omega)$ (car ω est algébrique sur \mathbb{Q}). De même en changeant ω par ω^k et on obtient que $\mathbb{Q}[\omega^k] \simeq \mathbb{Q}[\omega]$. On note ζ_k cet isomorphisme. Comme $\mathbb{Q}[\omega^k] \subset \mathbb{Q}[\omega]$, on a l'existence.

Unicité :

ω engendre $\mathbb{Q}[\omega]$. □

Lemme 0.0.3 :

Si $\alpha \in \mathbb{Z}[\omega]$, alors

$$(\forall k \in P_n, \zeta_k(\alpha) = \alpha) \Leftrightarrow \alpha \in \mathbb{Z}$$

Démonstration. \Leftarrow : Ok.

\Rightarrow : On décompose α dans la base $(\omega^k)_{0 \leq k \leq |P_n|} : \alpha = \sum_{i=0}^{\phi(n)-1} a_i \omega^i$, $a_i \in \mathbb{Z}$. Les conditions $\zeta_k(\alpha) = \alpha$ s'écrivent $Va = \alpha(1, \dots, 1)$ où $V = (\omega^{ij})_{i \in P_n, 0 \leq j < \phi(n)}$ et $a = (a_1, \dots, a_{\phi(n)-1})$. On note que si $e_1 = (1, 0, \dots, 0)$ alors $Ve_1 = (1, \dots, 1)$ et donc $Va = \alpha Ve_1$. Comme V est une matrice de Vandermonde et que les ω^k sont deux à deux distincts pour $k \in P_n$, V est inversible et $a = \alpha e_1$. D'où $\alpha \in \mathbb{Z}$. □

Supposons que pour tout $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$ et tout $g \in G$, g^k et g sont dans la même classe de conjugaison.

On fait maintenant agir $(\mathbb{Z}/n\mathbb{Z})^*$ sur l'ensemble des fonctions centrales par $\bar{k} \cdot f : g \mapsto f(g^k)$.

Ainsi, pour tout caractère χ de G et tout $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^*$, $\bar{k} \cdot \chi = \zeta_k \circ \chi$. En effet, si $g \in G$ et ρ est une représentation de caractère χ , $\chi(g)$ est la somme des valeurs propres de $\rho(g)$, qui sont de racines n -ièmes λ_i de l'unité ($\rho(g)^n = id$), donc $\chi(g) \in \mathbb{Z}[\omega]$. De plus $\chi(g^k)$ est la somme des λ_i^k . Donc $\chi(g^k) = \zeta_k(\chi(g))$.

Ainsi, comme χ est invariante par $(\mathbb{Z}/n\mathbb{Z})^*$ (par hypothèse), on obtient pour tout $k \in P_n$, $\zeta_k \circ \chi = \chi$. Le lemme 2 donne alors que χ est à valeurs entières.

Application : la table de S_n est à valeurs entières (pour tout $n \geq 1$)

Soit $k \in P_n$ et $\sigma \in S_n$. On cherche à montrer que σ^k et σ sont conjugués. Par décomposition en cycles à supports disjoints, on peut supposer que σ est un m -cycle, $m \leq n$.

Comme tous les m -cycles sont conjugués et que σ^k est un m -cycle, on a le résultat.