théorème. *Soit G un groupe de cardinal n. Si $\forall k \in \mathbb{N}^*$ premier à n et pour tout $g \in G$ g et g^k sont conjuués.*

Démonstration. *On note $\mathcal{P}_n = \{k \in \{1,..,n\} |\ k \text{ premier a } n\}$ qui est en bijection avec $(\mathbb{Z}/n\mathbb{Z})^*$ et $\omega \in \mathbb{U}_n$ une racine primitive n ième de l'unité.*

On sait que le polynôme cyclotomique $\Phi_n(X) = \prod_{k\in\mathcal{P}_n} X - \omega^k x$ est irréductible sur $\mathbb{Q}$ unitaire à coefficient dnas $\mathbb{Z}$ donc irréductible sur $\mathbb{Z}$. On a donc par irréductibilité de Φ_n unicité du corps de rupture

$$\begin{aligned}\mathbb{Q}[X]/(\Phi_n) &\simeq \mathbb{Q}[\omega] = \mathbb{Q}(\omega)\\ &\simeq \mathbb{Q}(\omega^k)\end{aligned}$$

Pour $k \in \mathcal{P}_n$ il existe un isomorphisme

$$\begin{array}{rccc}\zeta_k & : & \mathbb{Q}(\omega) & \to & \mathbb{Q}(\omega^k)\\ & & \omega & \to & \omega^k\\ & & a \in \mathbb{Q} & \to & a\end{array}$$

Or $\mathbb{Q}(\omega) \subset \mathbb{Q}(\omega^k)$ et les deux sont des $\mathbb{Q}$ espaces vectoriels de dimension $\varphi(n)$ donc $\mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$ et ζ_k est un automorphisme de corps

Voyons que $(\mathbb{Z}/n\mathbb{Z})^* \curvearrowright \mathbb{Z}[\omega]$. ζ_k est un automorphisme de l'anneau $\mathbb{Z}[\omega]$ et si $k \equiv k'\ [n]$ alors $\omega^k = \omega^{k'}$ donc

$$\begin{array}{ccc}(\mathbb{Z}/n\mathbb{Z})^* & \to & Aut(\mathbb{Z}[\omega])\\ k & \to & \zeta_{k|\mathbb{Z}[\omega]}\end{array}$$

est bien définit et est clairement un morphisme de groupe. D'où l'action énoncée.

Voyons que $Fix(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}$. Comme pour tout $k \in \mathbb{Z}^*$, ζ_k préserve $\mathbb{Z}$ cette inclusion est claire. Soit $\alpha \in fix(\mathbb{Z}/n\mathbb{Z})^*$. Il existe $P \in \mathbb{Z}[X]$ tel que $\alpha = P(\omega)$. Comme Φ_n est unitaire on a part la division euclidienne dans $\mathbb{Z}$, $P = Q\Phi_n + R$ avec $deg(R) < deg(\Phi_n)$ ou $R = 0$. On note $R = \sum_{i=0}^{\varphi(n)-1} a_i X^i$ avec $a_i \in \mathbb{Z}$. On a alors $\alpha = P(\omega) = R(\omega)$ car $\Phi_n(\omega) = 0$. Le système d'équation $\forall k \in \mathcal{P}_n$, $\zeta_k(\alpha) = \alpha$ s'ecrit alors :

$$\begin{aligned}\begin{pmatrix}\alpha\\ \vdots\\ \alpha\end{pmatrix} &= \begin{pmatrix}\zeta_1(\alpha)\\ \vdots\\ \zeta_{k_{\varphi(n)}}(\alpha)\end{pmatrix} = \begin{pmatrix}\sum_{i=0}^{\varphi(n)-1} a_i\omega^i\\ \vdots\\ \sum_{i=0}^{\varphi(n)-1} a_i\omega^{ik_{\varphi(n)}}\end{pmatrix}\\ &= \begin{pmatrix}1 & \omega & \dots & \omega^{\varphi(n)-1}\\ 1 & \omega^2 & \dots & \omega^{2(\varphi(n)-1)}\\ \vdots & \vdots & \ddots & \vdots\\ 1 & \omega^{k_{\varphi(n)}} & \dots & \omega^{k_{\varphi(n)}(\varphi(n)-1)}\end{pmatrix}\begin{pmatrix}a_0\\ \vdots\\ a_{\varphi(n)-1}\end{pmatrix} := Va\end{aligned}$$

$V \in Gl_{\varphi(n)}(\mathbb{C})$ car elle est de Vandermonde les coefficients $(\omega^k)_{k\in\mathcal{P}_n}$ sont tous distincts. Soit $e =^T (1,...,1)$ et $e_1 =^T (1,0,...,0)$ On peut ecrire les système ci dessus $\alpha e = Va$ et on a $Ve_1 = e$. D'où

$$Va = \alpha e = \alpha V e_1 = V(\alpha e_1)$$

puis comme V est inversible il vient finalement $a = \alpha e_1$ d'ou $\alpha = a_0 \in \mathbb{Z}$

Soit $\mathcal{F} \subset \mathbb{C}^G$ l'ensemble des fonctions centrales de G sur $\mathbb{C}$. On a alors $(\mathbb{Z}/n\mathbb{Z})^* \curvearrowright \mathcal{F}$ par l'application

$$\begin{array}{rccc}\Phi & : & (\mathbb{Z}/n\mathbb{Z})^* & \to & \mathfrak{S}(\mathcal{F})\\ & & k & \to & (f \to (g \to f(g^k)))\end{array}$$

qui est la composée des actions

$$\begin{array}{ccc}(\mathbb{Z}/n\mathbb{Z})^* & \to & \mathfrak{S}(G)\\ k & \to & (g \to g^k)\end{array}$$

(qui est bien définie car si $k \equiv k'[n]$ alors $g^k = g^{k'}$) et de

$$\begin{array}{ccc}\mathfrak{S}(G) & \to & \mathfrak{S}(\mathcal{F})\\ \sigma & \to & (f \to f \circ \sigma)\end{array}$$

qui est clairement une action.

Si g et h sont conjugué alors g^k et h^k sont aussi conjugués donc $k \cdot f \in \mathcal{F}$

Soit χ un caractère de G, alors $\forall g \in G,\ k \in (\mathbb{Z}/n\mathbb{Z})^*,\ \chi(g^k) = \zeta_k(\chi(g))$. En effet $\chi(g) = \sum_{\lambda \in sp(\varphi)} \lambda$ ou φ est une représentation de G. Soit $\lambda \in sp(\varphi(g))$, x un vecteur propre non nul associé à λ. Comme $g^n = e_G$ on a

$$x = Ix = \varphi(g^n)x = \varphi(g)^n x = \lambda^n x$$

Donc $\lambda^n = 1$, λ est une racine n ième de l'unité donc il existe $k_\lambda \in \{0, ..., n-1\}$ tel que $\lambda = \omega^{k_\lambda}$. Ainsi

$$\chi(g^k) = \sum_{\lambda \in sp(\varphi)} \lambda^{k_\lambda} = \sum_{\lambda \in sp(\varphi)} (\omega^k)^{k_\lambda} = \zeta_k(\chi(g))$$

Et on a de plus que $\chi(g) \in \mathbb{Z}[\omega]$

$$\begin{aligned} \chi \text{ invariant par } (\mathbb{Z}/n\mathbb{Z})^* &\iff \forall g \in G,\ \chi(g) \in Fix(\mathbb{Z}/n\mathbb{Z})^* \\ &\iff \forall g \in G \chi(g) \in \mathbb{Z} \end{aligned}$$

Si pour tout k premier à n, pour tout $g \in G$, g et g^k sont conjugués, alors comme χ est centrale $\chi(g) = \chi(g^k)$ c'est à dire $k \cdot \chi = \chi$ donc $Im\chi \subset \mathbb{Z}$