[N H262 t.2] pp. 343 & 349

Leçons :
101 ~
105 $\mathfrak{S}_n$
125 L:K
141 Poly. irréd. rupture
(144) racines
((104))
103 conjug.

Condition pour que la table de caractères d'un groupe soit dans $\mathbb{Z}$

Soit G un groupe fini, de cardinal n.

Si pour tout $k \in \mathbb{N}^*$ premier à n

et pour tout $g \in G$: g et g^k sont conjugués

Alors la table de caractères de G est à valeurs entières

Notons $\mathcal{P}_n := \{k \in [\![1, n]\!], \ k \text{ premier à } n\}$

($\mathcal{P}_n$ est en bijection avec $\mathbb{Z}/n\mathbb{Z}^\times$),

et soit $\omega \in \mathbb{U}_n$ une racine primitive n-ième de l'unité

1) Étape ① $\exists!\ \sigma_k \in \mathrm{Aut}\, \mathbb{Q}[\omega]$, $\sigma_k(\omega) = \omega^k$

On sait que le polynôme cyclotomique

$$\Phi_n(X) = \prod_{k \in \mathcal{P}_n} X - \omega^k \quad \in \mathbb{Z}[X]$$

est irréductible (et unitaire) sur $\mathbb{Q}$ donc sur $\mathbb{Z}$

On a donc, comme Φ_n est irréductible ; unicité du corps de rupture :

$$\mathbb{Q}[X]/(\Phi_n) \simeq \mathbb{Q}[\omega] = \mathbb{Q}(\omega)$$

ω est algébrique

si précise $\omega^k \leftarrow\!\!\shortmid \overline{X} \mapsto \omega$

$$\simeq \mathbb{Q}(\omega^k) \quad \text{pour } k \in \mathcal{P}_n$$

Donc si $k \in \mathcal{P}_n$, il existe un isomorphisme

(de corps ou d'anneaux (la m̂ chose))

$$\sigma_k : \begin{cases} \mathbb{Q}[\omega] \longrightarrow \mathbb{Q}[\omega^k] \\ a \in \mathbb{Q} \longmapsto a \\ \omega \longmapsto \omega^k \end{cases}$$

mais $\mathbb{Q}[\omega] \subset \mathbb{Q}[\omega^k]$

et $\mathbb{Q}[\omega]$, $\mathbb{Q}[\omega^k]$ sont 2 $\mathbb{Q}$-ev de dim $d^\circ \Phi_n = \varphi(n)$

donc $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^k]$

pas besoin : 1 isomorphisme + 1 inclusion => bijection

$$\begin{tikzcd}
\mathbb{Q}[\omega] & \mathbb{Q}[X] \arrow[l, "ev"'] \arrow[r, "ev"] \arrow[d] & \mathbb{Q}[\omega^k] \\
& \mathbb{Q}[X]/(\Phi_n) \arrow[ul, bend left, "\varphi_1"] \arrow[ur, bend right, "\varphi_k"'] &
\end{tikzcd}$$

$\sigma_k = \varphi_k \circ \varphi_1^{-1}$

et σ_k est un automorphisme de corps.

Il est unique car déterminé par $\sigma_k(1), \sigma_k(\omega)$

↳ pour parler de l'ac° de groupe ?

Étape ② $(\mathbb{Z}/n\mathbb{Z})^\times \circlearrowright \mathbb{Z}[\omega]$

$\sigma_k|_{\mathbb{Z}[\omega]}$ est un automorphisme de l'anneau $\mathbb{Z}[\omega]$

et si $k \equiv k' \, [n]$, $\omega^k = \omega^{k'}$

donc $\begin{cases} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathrm{Aut}\, \mathbb{Z}[\omega] \\ \bar{k} & \longmapsto & \sigma_k|_{\mathbb{Z}[\omega]} \end{cases}$

est bien défini et est un mdg

car $(\omega^k)^{k'} = \omega^{kk'}$

Donc $(\mathbb{Z}/n\mathbb{Z})^\times$ agit par automorphismes d'anneaux sur $\mathbb{Z}[\omega]$.

Étape ③ $\{\alpha \in \mathbb{Z}[\omega] \mid \forall k : \sigma_k(\alpha) = \alpha\} =: \mathrm{Fix}\, (\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}$

$\boxed{\supset}$ Comme σ_k préserve $\mathbb{Z}$, c'est clair

$\boxed{\subset}$ Soit $\alpha \in \mathrm{Fix}\, (\mathbb{Z}/n\mathbb{Z})^\times$.

Il existe $P \in \mathbb{Z}[X]$ tel que $\alpha = P(\omega)$,

mais comme $\Phi_n \in \mathbb{Z}[X]$ est unitaire, par

attention division euclidienne dans $\mathbb{Z}[X]$:

$$P = Q\Phi_n + R, \quad R = \sum_0^{\varphi(n)-1} a_i X^i, \; a_i \in \mathbb{Z}$$

et $\underline{\alpha = P(\omega) = R(\omega) = \sum_0^{\varphi(n)-1} a_i \omega^i}$

Mais le système d'équations

$$\sigma_k(\alpha) = \alpha, \quad k \in \mathcal{P}_n$$

s'écrit alors :

$$\mathcal{P}_n = \{1, k_2, \dots, k_{\varphi(n)}\}$$

$$\begin{pmatrix} \alpha \\ \vdots \\ \alpha \end{pmatrix} = \begin{pmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_{k_{\varphi(n)}}(\alpha) \end{pmatrix} = \begin{pmatrix} \sum a_i \omega^i \\ \vdots \\ \sum a_i \omega^{ki} \\ \vdots \\ \sum a_i \omega^{k_{\varphi(n)} i} \end{pmatrix} \quad k \in \mathcal{P}_n$$

$$= \underbrace{\begin{pmatrix} 1 & \omega & \omega^2 & \cdots & \omega^{\varphi(n)-1} \\ \vdots & & \vdots & & \vdots \\ 1 & \omega^k & \omega^{2k} & \cdots & \omega^{k(\varphi(n)-1)} \\ \vdots & & \vdots & & \vdots \\ 1 & \omega^{k_{\varphi(n)}} & \omega^{2k_{\varphi(n)}} & \cdots & \omega^{k_{\varphi(n)}(\varphi(n)-1)} \end{pmatrix}}_{V} \underbrace{\begin{pmatrix} a_0 \\ \vdots \\ a_{\varphi(n)-1} \end{pmatrix}}_{a}$$

$\alpha e =$

où $e = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} \in \mathbb{Q}^{\varphi(n)}$

$a \in \mathbb{Q}^{\varphi(n)}$

$V \in \mathcal{M}_{\varphi(n)}(\cancel{\mathbb{Q}}\ \mathbb{C})$

$$V = \left(\omega^{ki}\right)_{\substack{k \in \mathcal{P}_n \\ 0 \leq i \leq \varphi(n)-1}} = \left(\omega^{k_j (j-1)}\right)_{1 \leq j \leq \varphi(}$$

$\in GL_{\varphi(n)}(\cancel{\mathbb{Q}})\ \mathbb{C}$

car c'est la matrice de Vandermonde des $(\omega^k)_{k \in \mathcal{P}_n}$ tous distincts

On $V e_1 = e$

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

$a = \alpha e_1$ (V inversible)

soit $\underline{\alpha = a_0 \in \mathbb{Z}}$

$\mathcal{C}\ell$ = espace des fonctions centrales de $G \subset \mathbb{C}^G$

Étape 4 $\quad (\mathbb{Z}/n\mathbb{Z})^\times \curvearrowright \mathcal{C}\ell$

$$\Phi : \begin{cases} (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathfrak{S}(\mathbb{C}^G) \\ \bar{k} \longmapsto (f \longmapsto (g \mapsto f(g^k))) \end{cases}$$

est bien définie et une action de gpes car la composée des actions de gpes :

$$\begin{cases} (\mathbb{Z}/n\mathbb{Z})^\times \to \mathfrak{S}(G) \\ \bar{k} \longmapsto (g \mapsto g^k) \end{cases} \qquad \begin{cases} \mathfrak{S}(G) \to \mathfrak{S}(\mathbb{C}^G) \\ \sigma \longmapsto (f \mapsto f\circ\sigma) \end{cases}$$

↳ bien définie car $g^n = e_G$ $\qquad$ ↳ action à droite

et $f \in \mathcal{C}\ell$ est centrale,

comme (g et h conjugués) $\Rightarrow$ (g^k et h^k conjugués),

$k \cdot f \in \mathbb{C}^G$ est encore cste sur les CDC,

donc $\mathcal{C}\ell \subset \mathbb{C}^G$ est stable sous l'action

Étape 5 $\quad \forall \chi \in \cancel{\hat{G}}, \quad \forall g \in G : \quad \forall \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times : \quad \chi(g^k) = \sigma_k(\chi(g))$

En effet, $\chi(g) = \sum \lambda_i$ où λ_i sont des vp de $\rho(g)$

mais $g \cdot x = \lambda_i x \Rightarrow x = g^n \cdot x = \lambda_i^n x \Rightarrow \lambda_i \in \mathbb{U}_n$

donc les λ_i sont des ω^{k_i}

donc $\underline{\chi(g^k) = \sum \lambda_i^k = \sum \omega^{k k_i} = \sigma_k(\chi(g))}$

Et de plus : $\boxed{\chi(g) \in \mathbb{Z}[\omega]}$

6 $\quad$ χ invariant par $(\mathbb{Z}/n\mathbb{Z})^\times \iff \operatorname{im} \chi \subset \mathbb{Z}$

$\chi \in \operatorname{Fix} (\mathbb{Z}/n\mathbb{Z})^\times \iff \forall g \in G : \chi(g) \in \operatorname{Fix} (\mathbb{Z}/n\mathbb{Z})^\times$ $\quad$ action sur $\mathbb{Z}[\omega]$ σ_k

grâce à (2) $\quad \iff \forall g \in G : \underline{\chi(g) \in \mathbb{Z}}$

7 $\quad$ Si $k \wedge n = 1$ et g et g^k sont conjugués $\forall g$,

alors comme χ est centrale $\chi(g) = \chi(g^k)$ $\forall g$

soit $\bar{k} \cdot \chi = \chi \overset{(6)}{\Longrightarrow} \operatorname{im} \chi \subset \mathbb{Z}$