poly de Samuel Tapie

Developpement: Entiers algébriques et caractères

leçons 107 144

Théorème: Soit G un groupe fini. Le degré de toute représentation irréductible de G divise le cardinal de G.

Lemme 1: Soit χ un caractère de G. Alors $\forall g \in G$, le nbre complexe $\chi(g)$ est entier sur $\mathbb{Z}$, i.e. $\exists P \in \mathbb{Z}[X]$ unitaire tq $P(\chi(g)) = 0$.

Preuve lemme 1:

Soit ρ une représentation de G, de caractère χ : $\chi(g) = \text{Trace}(\rho(g))$.

Puisque G est fini, g est d'ordre fini et donc $\rho(g)$ également. $X^n - 1$ est donc un polynôme annulateur de $\rho(g)$, si n est l'ordre de G. Ainsi $\rho(g)$ diagonalisable, ses vp sont des racines $n^{ièmes}$ de l'unité et $\chi(g)$ est donc égale à une somme de racine $n^{ième}$ de l'unité. Or une telle racine est entière sur $\mathbb{Z}$ (polynôme annulateur: $X^n - 1$). Il en est donc de même pour $\chi(g)$, car les entiers algébriques forment un anneau. ∎

Lemme 2: Soit χ caractère irréductible de G, $g \in G$ et $C(g)$ la classe de conjugaison de g. Alors $|C(g)| \cdot \frac{\chi(g)}{\chi(e)}$ est entier sur $\mathbb{Z}$.

Preuve lemme 2:

Soit $\rho : G \to GL(V)$ une représentation irréductible de caractère χ. Soit $\varphi : V \to V$

$$\varphi = \sum_{h \in C(g)} \rho(h)$$

① Hq φ est un G endomorphisme de ρ:

$$\varphi \circ \rho(g) = \sum_{h \in C(g)} \rho(h) \circ \rho(g) = \sum_{h \in C(g)} \rho(hg) = \sum_{h \in C(g)} \rho(gg^{-1}hg) = \sum_{h \in C(g)} \rho(g) \circ \rho(g^{-1}hg)$$

$$= \rho(g) \circ \left(\sum_{h \in C(g)} \rho(g^{-1}hg) \right) = \rho(g) \circ \left(\sum_{t \in C(g)} \rho(t) \right)$$

$$= \rho(g) \circ \varphi$$

② On applique Schur:

φ non nul, donc φ homothétie: $\varphi = \lambda \, Id_V$, $\lambda \in \mathbb{C}$.

On a $\lambda \cdot \dim(V) = \text{Tr}(\varphi) = \sum_{h \in C(g)} \text{Tr}(\rho(h)) = \sum_{h \in C(g)} \chi(h) = |C(g)| \cdot \chi(g)$

donc $\lambda = |C(g)| \cdot \frac{\chi(g)}{\chi(e)}$ et il s'agit de démontrer que λ entier sur $\mathbb{Z}$.

③ On le montre:

On considère ρ_{reg} la représentation régulière de G. ρ étant irréductible, ρ est une sous représentation de ρ_{reg}. On décompose donc (par le théorème de Maschke) ρ_{reg} en somme directe de deux sous représentations : $\mathbb{C}^G = V \oplus W$ avec la restriction de ρ_{reg} à V étant équivalente à ρ.

Soit ψ l'endomorphisme de $\mathbb{C}^G$ donné par $\psi = \sum_{h \in C(g)} \rho_{reg}(h)$. De la même manière que précédement, on montre que ψ est un G endomorphisme de ρ_{reg} et induit donc un endomorphisme de V dans V, endomorphisme que n'est autre que φ par définition de ces deux morphismes. Ainsi, $\lambda \sigma_\rho$ de ψ, et si A est la matrice de ψ dans la base $(e_x)_{x \in G}$, on a $\det(\lambda I - A) = 0$. Mais $\forall x \in G$, $\psi(e_x) = \sum_{h \in C(g)} e_{hx}$ donc les coefficients de A sont égaux à 0 ou 1 et le polynôme $\det(XI - A)$ est un polynôme unitaire à coefficients dans $\mathbb{Z}$.

□

Preuve du théorème:

Soit ρ une représentation irréductible de caractère χ. Soit $g_1, \dots, g_N$ des représentants des classes de conjugaison de G et C_i la classe de g_i.

χ irréductible donc $\langle \chi, \chi \rangle = 1 = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \cdot \chi(g) = \frac{1}{|G|} \sum_{i=1}^{N} \sum_{g \in C_i} \overline{\chi(g)} \cdot \chi(g)$

$$= \frac{1}{|G|} \sum_{i=1}^{N} |C_i| \cdot \overline{\chi(g_i)} \cdot \chi(g_i)$$

donc $$\frac{|G|}{\chi(e)} = \sum_{i=1}^{N} |C_i| \cdot \frac{\chi(g_i)}{\chi(e)} \cdot \overline{\chi(g_i)}$$

Mais par le lemme 2 $|C_i| \cdot \frac{\chi(g_i)}{\chi(e)}$ entier sur $\mathbb{Z}$, et par le lemme 1 $\overline{\chi(g_i)} = \chi(g_i^{-1})$ est également entier sur $\mathbb{Z}$. Par conséquent, $\frac{|G|}{\chi(e)}$ est entier sur $\mathbb{Z}$. Etant rationnel, ce nombre est dans $\mathbb{Z}$, ce qui montre que $\deg(\rho) = \chi(e)$ divise $|G|$.

□

À savoir pour ce dev

① Les entiers algébriques sur A forment un anneau.

Soit α, β deux entiers algébriques, $\alpha_1, \dots, \alpha_n$ $\beta_1, \dots, \beta_m$ leurs conjugués (i.e. racines des pol minimaux respectifs sur $\mathbb{Q}$).

Il suffit de mq le pol unitaire $\prod_{i=1}^{n} \prod_{j=1}^{m} (X - [\alpha_i + \beta_j]) \in \mathbb{Z}[X]$ pour mq $\alpha + \beta$ entier algébrique !

Les relat° coefficients racines donnent que, au signe près, les coef de ce polynôme sont les polynômes symétriques élémentaires en les $(\alpha_i + \beta_j)$. Il suffit de mq une telle expression est de la forme $P(\underbrace{A_1(\alpha_1, \dots, \alpha_n)}_{A_1 \in \mathbb{Z}[X_1, \dots, X_n] \text{ symétrique idem}}, A_2(\beta_1, \dots, \beta_m)) \in \mathbb{Z}[X, Y]$.

② Un rationnel $\frac{p}{q}$ entier sur $\mathbb{Z}$ est relatif !

En effet, $\mathbb{Z}$ factoriel donc intégralement clos, c'est son corps de fract $\mathbb{Q}$ tq son anneau des entiers (à $\mathbb{Q}$) est $\mathbb{Z}$.