Entiers algébriques et représentations irréductibles

Leçons : 107, 144, 152

Réf. : Rombaldi

Théorème 1 :

Soit $\overline{\mathbb{Z}} = \{ \zeta \in \mathbb{C} \mid \exists P \in \mathbb{Z}[X] \text{ unitaire}, P(\zeta) = 0 \}$.

Alors $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$

Théorème 2 :

Soit G un groupe fini. Alors le degré de toute représentation irréductible de G divise $|G|$.

Théorème 1 :

1). $0, 1 \in \overline{\mathbb{Z}}$ (annulés respectivement par X et $X-1$)

Soient $\alpha, \beta \in \overline{\mathbb{Z}}$.

Soit $f = X^m + a_{m-1} X^{m-1} + \dots + a_0 \in \mathbb{Z}[X]$ t.q. $f(\alpha) = 0$ $(m \geq 1)$

$g = X^n + b_{n-1} X^{n-1} + \dots + b_0 \in \mathbb{Z}[X]$ t.q. $g(\beta) = 0$ $(n \geq 1)$

. Soit $\tilde{f}(x) = (-1)^n f(-x)$.

Alors, $\tilde{f} \in \mathbb{Z}[X]$, est unitaire et $\tilde{f}(-\alpha) = 0$

donc $-\alpha \in \overline{\mathbb{Z}}$

2) $\alpha+\beta \in \overline{\mathbb{Z}}$

Soit $f(x), g(y-x) \in \mathbb{Z}[x,y] = \mathbb{Z}[y][x]$.

Alors $S(y) = \mathrm{Res}_x(f(x), g(y-x)) \in \mathbb{Z}[y]$

On "regarde" $g(y-x)$ dans $\mathbb{Z}[y][x]$:

$$g(y-x) = (y-x)^n + \dots + b_1(y-x) + b_0$$
$$= (-1)^n x^n + c_{n-1}(y)x^{n-1} + \dots + c_1(y)x + c_0(y)$$

Alors : $\forall\, 1 \le i \le n-1$, $\deg c_{n-1}(y) < n$

$c_0(y) \in \mathbb{Z}[y]$, $\deg c_0(y) = n$ et $c_0(y)$ est unitaire

Soit $\phi : \mathbb{Z}[y] \longrightarrow \mathbb{C}$ morphisme d'anneaux
$Q(y) \longmapsto Q(\alpha+\beta)$

Rq : pour pouvoir utiliser le lemme de spécialisation, il faut que pour chacun des deux polynômes, ϕ(coefficient dominant) $\neq 0$.

On a $\phi(1) = 1 \neq 0$ ($f(x)$ est de coefficient dominant 1)
$\phi((-1)^n) = (-1)^n \neq 0$

Donc par le lemme de spécialisation,

$$\phi(S(y)) = \mathrm{Res}_x(\phi(f(x)), \phi(g(y-x)))$$
$$S(\alpha+\beta) = \mathrm{Res}_x(f(x), g(\alpha+\beta-x))$$
($f(x) \in \mathbb{C}[x]$)

On a $f(\alpha) = 0 = g(\alpha+\beta-\alpha)$ donc $f(x)$ et $g(\alpha+\beta-x)$ ont un facteur commun de degré ≥ 1, donc $S(\alpha+\beta) = 0$

(6)

Prop 5 est unitaire

$$S(Y) = \det \begin{pmatrix} 1 & a_{n-1} & \cdots & a_0 & & 0 \\ & \ddots & & & \ddots & \\ 0 & & 1 & a_{n-1} & \cdots & a_0 \\ (-1)^n c_{n-1}(Y) & \cdots & c_0(Y) & & & \\ & \ddots & & & \ddots & \\ 0 & & (-1)^n c_{n-1}(Y) & \cdots & & c_0(Y) \end{pmatrix} \quad (n \text{ lignes en haut, } m \text{ lignes en bas}) = D \in \mathcal{O}_{m+n}(\mathbb{Z}[Y])$$

$$S(Y) = \sum_{\sigma \in S_{n+m}} \varepsilon(\sigma) \prod_{i=1}^{m} d_{i\sigma(i)} \prod_{j=m+1}^{m+n} d_{j\sigma(j)}$$

Le terme de plus haut degré en Y est obtenu lorsque

$\forall\, n+1 \le j \le m+n,\ \sigma(j) = j$

Soit σ une telle permutation, on a alors $\sigma(\{1 \dots n\}) \subset \{1 \dots n\}$ qui agit donc sur la sous matrice $\square$

S'il existe $1 \le i \le n$ tel que $\sigma(i) \neq i$, alors $\prod_{i=1}^{n} d_{i\sigma(i)} = 0$.

Donc la seule permutation contribuant au terme de plus haut degré de $S(Y)$ est $\sigma = id$

Donc $S(Y) = (c_0(Y))^m + T(Y)$ $\deg T(Y) < \deg (c_0(Y))^m$

et $c_0(Y)$ est unitaire donc S est unitaire, et $\alpha + \beta \in \overline{\mathbb{Z}}$

3) $\alpha\beta \in \overline{\mathbb{Z}}$

On considère $f(X),\ X^m g\left(\frac{Y}{X}\right) \in \mathbb{Z}[Y][X]$

et $P(Y) = \mathrm{Res}_X\left(f(X),\ X^m g\left(\frac{Y}{X}\right)\right) \in \mathbb{Z}[Y]$

s'annule là

$$P(Y) = \det \begin{pmatrix} 1 & \cdots & a_0 & & 0 \\ & \ddots & & \ddots & \\ 0 & & 1 & \cdots & a_0 \\ b_0 & b_1 Y & \cdots & Y^n & \\ & \ddots & & & \ddots \\ 0 & & b_0 & b_1 Y & \cdots & Y^n \end{pmatrix}$$

est également unitaire donc $\alpha\beta \in \overline{\mathbb{Z}}$

Théorème 2 :

a) Notations

$|G| = n \geq 1$, $\rho : G \longrightarrow GL(V)$ une représentation irréductible de degré d et de caractère $\chi : G \longrightarrow \mathbb{C}$.

On pose $G = \coprod_{i=1}^{r} C_i$ où les C_i sont les classes de conjugaison de G

1) $\forall g \in G$, $\chi(g) \in \overline{\mathbb{Z}}$

Soit $g \in G$, $\rho(g)^n = \rho(g^n) = \rho(1) = id_V$

donc $\boxed{Sp(\rho(g)) \subset U_n}$

Or, $\forall \lambda \in U_n$, λ annule $X^n - 1 \in \mathbb{Z}[X]$ unitaire donc $\lambda \in \overline{\mathbb{Z}}$

$\chi(g) = \sum_{\lambda \in Sp(\rho(g))} \lambda \in \overline{\mathbb{Z}}$ car $\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$

donc $\boxed{\chi \text{ est à image dans } \overline{\mathbb{Z}}}$

2) On pose $\forall 1 \leq i \leq r$, $u_i = \sum_{g \in C_i} \rho(g) \in \mathcal{L}(V)$. $\forall g$ u_i est une homothétie.

Soit $h \in G$. $\rho(h)^{-1} \circ u_i \circ \rho(h) = \sum_{g \in C_i} \rho(h^{-1} g h)$

Or, $C_i \longrightarrow C_i$, $g \longmapsto h^{-1} g h$ est une bijection

donc $\rho(h)^{-1} \circ u_i \circ \rho(h) = \sum_{g' \in C_i} \rho(g') = u_i$

ρ étant irréductible, par le lemme de Schur,

$\boxed{\exists \lambda_i \in \mathbb{C} \;/\; u_i = \lambda_i id_V}$

(G)

3) $\prod_g \lambda_i \in \overline{\mathbb{Z}} \quad \forall\, 1 \le i \le n$

Soit $g \in G$. $\lambda_i\, \rho(g) = u_i \circ \rho(g) = \sum_{g' \in C_i} \rho(g'g) = \sum_{h \in G} a_{g,h}\, \rho(h)$

où $a_{g,h} = \begin{cases} 1 \text{ si } \exists\, g' \in C_i \ / \ h = g'g \\ 0 \text{ sinon} \end{cases}$

donc $\boxed{\sum_{h \in G} (\lambda_i\, \delta_{g,h} - a_{g,h})\, \rho(h) = 0 \quad \forall g \in G \quad (*)}$

Soit $B = \mathcal{L}(V)$. $(B, +, \circ)$ est alors un anneau (non commutatif).

Soit $A = (a_{g,h})_{g,h \in G} \in \mathcal{M}_n(\mathbb{Z}) \subset \mathcal{M}_n(\mathbb{C})$.

++ On peut voir $\mathcal{M}_n(\mathbb{C})$ comme un sous-anneau de $\mathcal{M}_n(B)$

(on peut voir $\lambda \in \mathbb{C}$ comme l'homothétie $\lambda\, id_V$)

Soit $R = \left[\rho(h)\right]_{h \in G} \in B^n$

Alors $(*) \Leftrightarrow (\lambda_i I_n - A)\, R = 0$ $\Big\}$ $\vdash \mathrm{Com}(\lambda_i I_n - A) \times$

$\Rightarrow \boxed{\det(\lambda_i I_n - A)\, R = 0}$

Rq : B est un anneau non commutatif mais la multiplication dans $\mathcal{M}_n(B)$ reste associative

On a donc $\det(\lambda_i I_n - A)\, \rho(h) = 0 \quad \forall h \in G$

donc $\boxed{\chi_A(\lambda_i) = \det(\lambda_i I_n - A) = 0}$

Or $\chi_A \in \mathbb{Z}[X]$ est unitaire (même démonstration que si $A \in \mathcal{M}_n(K)$)

donc $\boxed{\lambda_i \in \overline{\mathbb{Z}} \quad \forall\, 1 \le i \le n}$

4) Conclusion

$\lambda_i \, id_V = u_i = \sum_{g \in C_i} \rho(g)$

donc $Tr_\pi(u_i) = d\,\lambda_i = \sum_{g \in C_i} \chi(g)$

et χ est une fonction centrale donc constante sur C_i de valeur $\chi(C_i)$

donc $\boxed{d\,\lambda_i = |C_i|\,\chi(C_i)}$

Enfin, χ est irréductible donc par relation d'orthogonalité des caractères

$$(\chi \mid \chi) = 1 = \frac{1}{n} \sum_{g \in G} |\chi(g)|^2 = \frac{1}{n} \sum_{i=1}^{n} |C_i| \, |\chi(C_i)|^2$$

$$1 = \frac{1}{n} \sum_{i=1}^{n} |C_i| \, \chi(C_i) \, \overline{\chi(C_i)} = \frac{1}{n} \sum_{i=1}^{n} d\,\lambda_i \, \overline{\chi(C_i)}$$

donc $\boxed{\frac{n}{d} = \sum_{i=1}^{n} \lambda_i \, \overline{\chi(C_i)}}$

$\forall\, 1 \le i \le n$, $\lambda_i \in \overline{\mathbb{Z}}$

$\chi(C_i) \in \overline{\mathbb{Z}}$ d'après 1) donc $\overline{\chi(C_i)} \in \overline{\mathbb{Z}}$ (...)

$\overline{\mathbb{Z}}$ ayant une structure d'anneaux, on a donc $\boxed{\frac{n}{d} \in \overline{\mathbb{Z}}}$

$\frac{n}{d} \in \mathbb{Q}$ et $\frac{n}{d} \in \overline{\mathbb{Z}}$ donc $\overset{(**)}{\frac{n}{d}} \in \mathbb{Z}$ donc $\boxed{d \mid n}$

Rq : (**) Si $\frac{p}{q} \in \mathbb{Q} \cap \overline{\mathbb{Z}}$ où $p \wedge q = 1$, $\exists\, f = X^n + a_{n-1} X^{n-1} + \dots + a_0 \in \mathbb{Z}[X]$ tel que $f\left(\frac{p}{q}\right) = 0 = \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_0 \quad (\times q^n)$

donc $p^n + \underbrace{\sum_{i=0}^{n-1} a_i \, p^i \, q^{n-i}}_{q \mid \cdot} = 0$

donc $\begin{cases} q \mid p^n \\ q \wedge p = 1 \end{cases} \Rightarrow q = 1$ et $\frac{p}{q} \in \mathbb{Z}$.