

# Anneau des entiers algébriques et degré d'une représentation irréductible

Émile Séguret

Pour les leçons : 107, 144, 152

## Références :

- Mathématiques pour l'agrégation - Rombaldi (page 581, attention sa matrice de Sylvester est fausse),
- Nouvelles histoires hédonistes de groupes et de géométrie - Caldero Germoni (page 346 exercice 37)

**Prérequis.** Notion de résultant, propriétés importantes, notamment :  $P, Q \in k[X]$  ont une racine commune dans une extension de  $k$  si, et seulement si,  $\text{Res}(P, Q) = 0$  (rappelée dans le Rombaldi). Définition de l'ensemble des entiers algébriques de  $\mathbf{C}$  :  $\overline{\mathbf{Z}} = \{z \in \mathbf{C}, \exists P \in \mathbf{Z}[X] \text{ unitaire, } P(z) = 0\}$ . On a par exemple  $\mathbf{Q} \cap \overline{\mathbf{Z}} = \mathbf{Z}$  et  $\mathbf{U}_n \subset \overline{\mathbf{Z}}$  pour tout  $n \geq 1$ . Et il est bon de savoir que  $\alpha \in \overline{\mathbf{Z}}$  si, et seulement si, son polynôme minimale sur  $\mathbf{Q}$  est à coefficients entiers.

**Avertissements.** Ce développement est long et nécessite une maîtrise du résultant et de la théorie des représentations (savoir faire la leçon 107).

## Théorème.

1.  $\overline{\mathbf{Z}}$  est un sous-anneau de  $\mathbf{C}$ ,
2. Soit  $\rho : G \rightarrow \text{GL}(V)$  une représentation irréductible d'un groupe fini  $G$ , de caractère  $\chi$ . Alors son degré  $d = \dim(V)$  divise  $n$  l'ordre de  $G$ .

**Démonstration de 1.** Comme 0 et 1 sont dans  $\overline{\mathbf{Z}}$ , il suffit de montrer que si  $\alpha, \beta \in \overline{\mathbf{Z}}$  alors  $-\alpha, \alpha + \beta, \alpha\beta \in \overline{\mathbf{Z}}$ . Notons  $P, Q \in \mathbf{Z}[X]$  unitaires, annulant respectivement  $\alpha$  et  $\beta$  :

$$P = X^m + a_{m-1}X^{m-1} + \cdots + a_0, \quad Q = X^n + b_{n-1}X^{n-1} + \cdots + b_0.$$

- $-\alpha \in \overline{\mathbf{Z}}$  :  $(-1)^m P(-X)$  est unitaire dans  $\mathbf{Z}[X]$  et annule  $-\alpha$ .
- $\alpha + \beta \in \overline{\mathbf{Z}}$  :

Considérons  $P(X-Y), Q(Y) \in \mathbf{Z}[X][Y] \subset \mathbf{Q}(X)[Y]$  vu comme des polynômes en  $Y$  à coefficients dans le corps  $\mathbf{Q}(X)$ . Soit  $R(X) = \text{Res}_Y(P(X-Y), Q(Y)) \in \mathbf{Q}(X)$  (on élimine la variable  $Y$ ). Comme  $P(\alpha + \beta - Y)$  et  $Q(Y)$  sont deux polynômes de  $\mathbf{C}[Y]$  qui s'annulent en  $\beta \in \mathbf{C}$ , alors, d'après la propriété rappelée en prérequis,  $R(\alpha + \beta) = 0$ .

Montrons que  $R$  est en fait dans  $\mathbf{Z}[X]$  et unitaire. On a :

$$P(X-Y) = \sum_{k=0}^m a_k (X-Y)^k = \sum_{k=0}^m a_k \sum_{j=0}^k \binom{k}{j} X^{k-j} (-1)^j Y^j = \sum_{j=0}^m c_j(X) Y^j.$$

Avec  $c_j(X) = (-1)^j \sum_{k=j}^m a_k \binom{k}{j} X^{k-j} \in \mathbf{Z}[X]$  de degré  $m - j$ . On a  $c_0(X) = P(X)$  et  $c_m(X) = (-1)^m a_m = (-1)^m \neq 0$ , donc  $P(X - Y)$  est de degré  $m$  en  $Y$  (important pour écrire le déterminant de Sylvester ci-dessous). Par définition (ou plutôt, ma convention) de la matrice de Sylvester :

$$R(X) = \begin{vmatrix} c_0(X) = P(X) & & & & b_0 & & \\ & c_1(X) & P(X) & & \vdots & \ddots & \\ & \vdots & c_1(X) & \ddots & \vdots & & b_0 \\ c_m(X) & & \vdots & \ddots & P(X) & b_{n-1} & \vdots \\ & c_m(X) & & c_1(X) & 1 & \ddots & \vdots \\ & & & \ddots & & \ddots & b_{n-1} \\ & & & & c_m(X) & & 1 \end{vmatrix}$$

Via la formule du déterminant (avec la somme sur les permutations de  $\mathbf{S}_{m+n}$ ) et en isolant la permutation Id, on obtient  $R(X) = P(X)^n \times 1^m + T(X)$ . Où  $T \in \mathbf{Z}[X]$  est de degré strictement plus petit que celui de  $P$ , car  $c_j \in \mathbf{Z}[X]$  avec  $\deg(c_j) < m$  si  $j \geq 1$ . Conclusion :  $R \in \mathbf{Z}[X]$  est unitaire et annule  $\alpha + \beta$ .

- $\alpha\beta \in \overline{\mathbf{Z}}$  :

On utilise les mêmes arguments que ci-dessus. On considère cette fois-ci

$$R(X) = \text{Res}_Y \left( Y^m P \left( \frac{X}{Y} \right), Q(Y) \right) \in \mathbf{Q}(X), \text{ qui s'annule en } \alpha\beta.$$

Comme  $Y^m P \left( \frac{X}{Y} \right) = \sum_{k=0}^m (a_{m-k} X^{m-k}) Y^k$ , alors :

$$R(X) = \begin{vmatrix} a_m X^m & & & & b_0 & & \\ \vdots & \ddots & & & \vdots & \ddots & \\ \vdots & & a_m X^m & & \vdots & & b_0 \\ a_0 & & \vdots & 1 & \vdots & & \\ & \ddots & \vdots & & \ddots & \vdots & \\ & & a_0 & & & \ddots & 1 \end{vmatrix} \in \mathbf{Z}[X] \text{ est unitaire car } a_m = 1.$$

**Démonstration de 2.** Écrivons  $G = C_1 \cup \dots \cup C_r$  comme union disjointe de ses  $r$  classes de conjugaisons. On procède en quatre étapes.

- D'abord  $\chi$  est constant sur les classes de conjugaisons de  $G$  et à valeurs dans  $\overline{\mathbf{Z}}$ . En effet, si  $g \in G$ , alors  $\rho(g)^n = \text{Id}$ , donc  $\rho(g)$  est diagonalisable à valeurs propres  $\lambda_1, \dots, \lambda_d \in \mathbf{U}_n \subset \overline{\mathbf{Z}}$  et donc  $\chi(g) = \text{Tr } \rho(g) = \lambda_1 + \dots + \lambda_d \in \overline{\mathbf{Z}}$  d'après le premier point.
- Pour tout  $1 \leq i \leq r$ , on note  $u_i = \sum_{g \in C_i} \rho(g) \in \text{End}(V)$  (endomorphisme du  $\mathbf{C}$ -ev  $V$ ). Ce sont même des endomorphismes de  $G$ -représentation puisque, pour tout  $h \in G$ ,

$$u_i \circ \rho(h) = \sum_{g \in C_i} \rho(gh) = \sum_{g' \in C_i} \rho(hg') = \rho(h) \circ u_i,$$

où l'on a posé  $g' = h^{-1}gh$ , réalisant une bijection de  $C_i$ . D'après le lemme de Schur, comme  $\rho$  est irréductible, on peut écrire  $u_i = \lambda_i \text{Id}$ , avec  $\lambda_i \in \mathbf{C}$ .

— Montrons que pour tout  $1 \leq i \leq r$ ,  $\lambda_i \in \overline{\mathbf{Z}}$ . Soit  $g \in G$ ,

$$\lambda_i \rho(g) = u_i \circ \rho(g) = \sum_{g' \in C_i} \rho(g'g) = \sum_{h \in G} a_{g,h} \rho(h), \text{ avec } a_{g,h} \in \{0, 1\}.$$

Donc pour tout  $g \in G$ ,  $\sum_{h \in G} (\lambda_i \delta_{g,h} - a_{g,h}) \rho(h) = 0$ .

Soient  $A = (a_{g,h})_{g,h \in G} \in M_n(\mathbf{Z})$  et  $R = (\rho(h))_{h \in G} \in \text{End}(\mathbf{V})^n$ . Alors  $(\lambda_i I_n - A)R = 0$  dans  $\text{End}(\mathbf{V})^n$ . On multiplie cette égalité par  ${}^t\text{Com}(\lambda_i I_n - A)$  pour obtenir :  $\det(\lambda_i I_n - A) R = 0$ . Si l'on note  $\chi_A \in \mathbf{Z}[X]$  le polynôme caractéristique (donc unitaire) de  $A$ , alors  $\chi_A(\lambda_i) R = 0$ . Pour la coordonnée  $h = 1$  (neutre de  $G$ ), on obtient  $0 = \chi_A(\lambda_i) \rho(1) = \chi_A(\lambda_i) \text{Id}$ , donc  $\chi_A(\lambda_i) = 0$ .

— Concluons. Soit  $1 \leq i \leq r$ , on prend la trace

$$d\lambda_i = \text{Tr } u_i = \sum_{g \in C_i} \chi(g) = |C_i| \chi(C_i).$$

Comme  $\chi$  est irréductible,  $\langle \chi, \chi \rangle = 1$ , de sorte que

$$n = |G| = \sum_{g \in G} |\chi(g)|^2 = \sum_{i=1}^r |C_i| \chi(C_i) \overline{\chi(C_i)} = \sum_{i=1}^r d\lambda_i \overline{\chi(C_i)}.$$

Or, on a vu que  $\chi(C_i) \in \overline{\mathbf{Z}}$ , donc  $\overline{\chi(C_i)} \in \overline{\mathbf{Z}}$  (si  $P(z) = 0$ , alors  $P(\bar{z}) = 0$  puisque  $P$  est à coefficients entiers, donc réels). D'où

$$\frac{n}{d} = \sum_{i=1}^r \lambda_i \overline{\chi(C_i)} \in \overline{\mathbf{Z}}, \text{ par le point 1.}$$

Finalement  $\frac{n}{d} \in \overline{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$ , c'est-à-dire  $d$  divise  $n$ .