Titre : **Entiers algébriques et représentations irréductibles**
Recasages : 107,144,152
Thème : Arithmétique des polynômes, représentations des groupes, algèbre linéaire
Références : Rombaldi - Algèbre à l'agrégation

On considère G un groupe fini, et $\overline{Z} \subset \mathbb{C}$ l'ensemble des entiers algébriques :

$$\overline{Z} := \{z \in \mathbb{C} \mid \exists P \in \mathbb{Z}[X] \text{ unitaire tel que } P(z) = 0\}$$

Théorème 1. *L'ensemble des entiers algébriques forme un sous-anneau de $\mathbb{C}$. Par conséquent, le degré de toute représentation irréductible de G sur $\mathbb{C}$ divise $|G|$.*

On commence par remarquer que 1 et 0 sont dans $\overline{Z}$, il suffit donc de montrer que celui-ci est stable par addition, passage à l'opposé et multiplication. Soient donc $\alpha, \beta \in \overline{Z}$, respectivement annulés par les polynômes unitaires

$$P(X) = \sum_{k=0}^{n} a_k X^k, \quad S(X) = \sum_{k=0}^{m} b_k X^k \in \mathbb{Z}[X]$$

On a $(-1)^n P(-X)$ annule $-\alpha$, qui est donc dans $\overline{Z}$.

Montrons que $\alpha+\beta \in \overline{Z}$. On se place dans $\mathbb{Q}(X)[Y]$ où l'on considère les polynômes $P(X-Y)$ et $S(Y)$, on peut considérer le résultant (en Y) de ces polynômes, qui est donc un élément de $\mathbb{Q}(X)$:

$$R(X) := \mathrm{Res}_Y(P(X-Y), S(Y))$$

Comme les polynômes complexes $P(\alpha+\beta-Y), S(Y) \in \mathbb{C}[Y]$ admettent β comme racine commune, on a résultant $R(\alpha+\beta) = 0$[1]. Donc $\alpha+\beta$ est racine du polynôme $R(X)$, dont il reste à montrer qu'il est unitaire à coefficients entiers : On a

$$P(X-Y) = \sum_{k=0}^{n} a_k (X-Y)^k = \sum_{k=0}^{n} a_k \sum_{i=0}^{k} \binom{k}{i} (-1)^i X^{k-i} Y^i = \sum_{i=0}^{n} (-1)^i Y^i \sum_{k=i}^{n} a_k \binom{k}{i} X^{k-i}$$

On pose $c_i(X) = (-1)^i \sum_{k=i}^{n} a_k \binom{k}{i} X^{k-i}$ le i-ème coefficient de $P(X-Y)$ dans $\mathbb{Q}(X)[Y]$, on remarque que $c_0(X) = \sum_{k=0}^{n} a_k X^k = P(X)$, et $c_n(X) = (-1)^n a_n = (-1)^n \neq 0$, donc $P(X-Y)$ est de degré n, le résultant $R(X)$ est donné par

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

En considérant la formule explicite du déterminant (somme sur les permutations de $\mathfrak{S}_n$) et en isolant la permutation triviale, on obtient $R(X) = (P(X))^m + T(X)$ où $T(X)$ est à coefficients entiers et de degré inférieur strictement à celui de P^m (car $c_i(X)$ est de degré $< n$ pour $i \geqslant 1$), on a bien le résultat voulu.

1. le résultant de deux polynômes de $k[X]$ est nul ssi ils ont une racine commune dans une extension de k

Montrons que $\alpha\beta \in \overline{Z}$. On utilise un argument similaire en considérant le résultant

$$U(X) = \mathrm{Res}_Y\left(Y^n P\left(\frac{X}{Y}\right), S(Y)\right) \in \mathbb{Q}(X)$$

celui ci s'annule bien en $\alpha\beta$. On a $Y^n P\left(\frac{X}{Y}\right) = \sum_{k=0}^{n} a_k X^k Y^{n-k} = \sum_{k=0}^{n} a_{n-k} X^{n-k} Y^k$ et donc

$$U(X) = \begin{vmatrix} a_n X^n & & & b_0 & & \\ a_{n-1}X^{n-1} & \ddots & & \vdots & \ddots & \\ \vdots & \ddots & a_n X^n & \vdots & & b_0 \\ a_0 & & a_{n-1}X^{n-1} & 1 & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_0 & & & 1 \end{vmatrix}$$

On a bien $U(X) \in \mathbb{Z}[X]$ unitaire par le même argument que pour R, ce qui termine de montrer le premier point.

Pour le second point, soit $n = |G|$, $\rho : G \to Gl(V)$ une représentation irréductible de degré d de G et χ son caractère associé. On pose également $G = C_1 \sqcup \cdots \sqcup C_r$ les classes de conjugaisons de G.
Le caractère χ, constant sur les classes de conjugaisons, est à valeurs dans $\overline{Z}$, en effet, on sait que $\rho(g)$ est diagonalisable et admet seulement des racines n-èmes de l'unité pour valeurs propres, or celles-ci sont dans $\overline{Z}$ (elles annulent $X^n - 1$), $\chi(g)$ est donc dans $\overline{Z}$ comme somme d'éléments de $\overline{Z}$.
Posons

$$\forall i \in [\![1, r]\!], u_i := \sum_{g \in C_i} \rho(g) \in \mathcal{L}(V)$$

On a $u_i \in \mathrm{Hom}_{\mathbb{C}G}(V, V)$ car

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

Comme V est irréductible, le lemme de Schur donne $u_i = \lambda_i Id_V$ pour un $\lambda_i \in \mathbb{C}$.
On montre que pour $i \in [\![1, r]\!]$, on a $\lambda_i \in \overline{Z}$: pour $g \in G$, on a

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

avec $a_{g,h} \in \{0, 1\}$ [2]. On a donc

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

On pose $A = (a_{g,h})_{g,h \in G} \in \mathcal{M}_n(\mathbb{Z})$, et $(\rho(h))_{h \in G} \in \mathcal{L}(V)^n$, on a $(\lambda_i I_n - A)R = 0$ dans $\mathcal{L}(V)^n$. En multipliant cette égalité par ${}^t\mathrm{Com}(\lambda_i I_n - A)$, on a $\det(\lambda_i I_n - A)R = 0$, comme R admet $\rho(1) = I_d$ comme coefficient, on en déduit $\det(\lambda_i I_n - A) = 0$, donc λ_i est racine du polynôme

2. c'est juste une astuce de notation, $a_{g,h}$ est une indicatrice, qui vaut 1 si et seulement si $h = g'g$ pour un $g' \in C_i$

caractéristique de A, qui est unitaire à coefficients dans $\mathbb{Z}$: on a bien $\lambda_i \in \overline{Z}$.
Concluons : Pour $i \in [\![1, r]\!]$, on a

$$d\lambda_i = \mathrm{tr}(u_i) = \sum_{g \in C_i} \chi(g) = |C_i|\chi(C_i)$$

Mais, comme χ est irréductible, on a

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

Or, $\overline{\chi(C_i)}$ est dans $\overline{Z}$ (les racines complexes d'un polynôme à coefficients entiers, a fortiori réels, sont stables par conjugaisons), donc $\frac{n}{d}$ est un rationnels et un entier algébrique : c'est un entier, donc d divise n.