Entiers algébriques + application.

Leçons: 144, 152

Réf: Rombaldi p 531, Caldero NH262 Tome 2 p 346.

Théorème: L'ensemble $\mathcal{A} = \{\lambda \in \mathbb{C} : \exists P \in \mathbb{Z}[X] \text{ unitaire}, P(\lambda) = 0\}$ des nombres algébriques est un sous-anneau de $\mathbb{C}$.

Dém: $\mathcal{A}$ contient 0 et 1 respectivement annulés par X et $X-1$.
Si $\lambda \in \mathcal{A}$ est annulé par le polynôme unitaire $P \in \mathbb{Z}[X]$ de degré $n \geq 1$, $Q(X) = (-1)^n P(-X)$ est unitaire de degré $n \geq 1$ dans $\mathbb{Z}[X]$ et annule $-\lambda$.

Si $\lambda \in \mathcal{A}$ est annulé par $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ et $\mu \in \mathcal{A}$ par $Q = X^m + b_{m-1}X^{m-1} + \cdots + b_0 \in \mathbb{Z}[X]$
montrons que $R(X) = \mathrm{Res}_Y(P(X-Y), Q(Y))$ est unitaire, de degré nm dans $\mathbb{Z}[X]$ et annulateur de $\lambda+\mu$.
Comme $P(\lambda+\mu-Y)$ et $Q(Y)$ admettent μ comme racine commune, leur résultant $R(\lambda+\mu)$ est nul. Il reste donc à montrer que $R \in \mathbb{Z}[X]$ et unitaire. Pour cela on écrit, avec $a_n = 1$:

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

$$= \sum_{\ell=0}^{n} (-1)^\ell \left(\sum_{k=\ell}^{n} \binom{k}{\ell} a_k X^{k-\ell} \right) Y^\ell$$

$$= \sum_{\ell=0}^{n} c_\ell(X) Y^\ell \in \mathbb{Q}(X)[Y].$$

$c_\ell(X)$ vit dans $\mathbb{Z}[X]$ et est de degré $n-\ell$.

$c_0(X) = \sum_{k=0}^{n} a_k X^k = P(X)$ et $c_n(X) = (-1)^n a_n = (-1)^n \neq 0$.

Donc $P(X-Y)$ est degré n dans $\mathbb{Q}(X)[Y]$.
Par ailleurs le résultant $R(X)$ est donné par :

$$R(X) = \underbrace{\begin{vmatrix} c_0(X) & & & b_0 & & \\ c_1(X) & c_0(X) & & b_1 & b_0 & \\ \vdots & \vdots & \ddots & \vdots & b_1 & \ddots \\ c_m(X) & & c_0(X) & & \vdots & b_0 \\ & c_m(X) & \vdots & b_m & & \vdots \\ & & \ddots & & b_m & \\ & & c_n(X) & & & b_m \end{vmatrix}}_{D = (d_{i,j})}$$

Parmi les $c_i(X)$, $c_0(X)$ est celui de + haut degré donc la meilleure contribution possible consiste à prendre tous les $c_0(X)$ i.e imposer $\sigma(i) = i$ pour $i = 1 \dots m$ et en fait cela force $\sigma = id$ sinon le produit s'annule (à cause des 0 sous les b_i).

$$= \sum_{\sigma} \varepsilon(\sigma) \prod_{i} d_{i,\sigma(i)}$$

$$= c_0(X)^m b_m^m + T(X) \quad \text{(en isolant } \sigma = id\text{)} \qquad b_m = 1.$$

$$= P(X)^m + T(X)$$

avec $T(X)$ à coefficients entiers et de degré $< \deg P(X)^m$ car $\forall i \geq 1$, $c_i(X)$ est de degré $< n$.

Comme P est unitaire, R est donc encore unitaire et dans $\mathbb{Z}[X]$.

même arguments, juste donner le résultant qu'on considère et passer à la suite.

De la même manière, avec $Y^m P\left(\frac{X}{Y}\right) = \sum_{k=0}^{m} a_k X^k Y^{m-k} \in \mathbb{Q}(X)[Y]$

le résultant $S(X) = \mathrm{Res}_Y\left(Y^m P\left(\frac{X}{Y}\right), Q(Y)\right)$ est un polynôme à coefficients entiers, de degré mn et unitaire.

Par ailleurs, comme $Y^m P\left(\frac{\lambda\mu}{Y}\right)$ et $Q(Y)$ admettent μ comme racine commune, leur résultant $S(\lambda\mu)$ est nul.

Ainsi $\mathcal{A}$ contient 0, 1, est stable par opposé, addition et multiplication. C'est donc un sous-anneau de $\mathbb{C}$. □

Ce résultat donne une application en théorie des représentations :

Caldero p346 || si G est un groupe fini, le degré de toute représentation irréductible de G sur $\mathbb{C}$ divise $|G|$.

Dém: Soit $n = |G|$, $\rho : G \to GL(V)$ une représentation irréductible de degré d et χ son caractère associé. On pose $G = C_1 \sqcup \cdots \sqcup C_r$ où les C_i sont les classes de conjugaison de G.

(1) Montrons que χ, constant sur les classes de conjugaison de G, est à valeurs dans $\mathcal{A}$.

$\chi(g)$ est la somme des valeurs propres de $\rho(g)$. Or d'après le théorème de Lagrange, $\rho(g)^n = \rho(g^n) = \rho(1) = id_V$ donc les valeurs propres de $\rho(g)$ sont des racines n-ième de l'unité, qui sont dans $\mathcal{A}$ (car annulées par $X^n - 1 \in \mathbb{Z}[X]$ qui est unitaire).
Comme $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$, $\chi(g)$ est donc toujours dans $\mathcal{A}$.

(2) Montrons que $\forall 1 \le i \le r$, $u_i = \sum_{g \in C_i} \rho(g) \in Z(V)$ est une homothétie.

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

$= \sum_{g' \in C_i} \rho(g')$ car $g \mapsto h^{-1} g h$ est une bijection.

$= u_i$

Comme ρ est irréductible, le lemme de Schur assure que u_i est une homothétie : $\exists \lambda_i \in \mathbb{C}$ tq $u_i = \lambda_i \, id_V$.

(3) Montrons que $\lambda_i \in \mathcal{A}$.

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

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

Ce qui on réécrit : $\sum_{h \in G} (\lambda_i \delta_{g,h} - a_{g,h}) \rho(h) = 0 \quad \forall g \in G \quad (*)$

On pose $A = (a_{g,h})_{g,h \in G} \in \mathcal{M}_n(\mathbb{Z})$ et $R = (\rho(h))_{h \in G} \in \mathcal{L}(V)^n$ de sorte que (*) devienne :

$$(A - \lambda_i I_n) R = 0$$

En multipliant par ${}^t\mathrm{Com}(A - \lambda_i I_n)$, on a $\det(A - \lambda_i I_n) R = 0$ dans $\mathcal{L}(V)^n$. Or R admet $\rho(1) = \mathrm{id}_V$ pour coefficient donc on a en particulier $\det(A - \lambda_i I_n) = 0$. Ainsi λ_i annule χ_A qui est unitaire à coefficients entiers, d'où $\lambda_i \in \mathcal{A}$.

④ Conclusion.

Pour $1 \leq i \leq r$, $d\lambda_i = \mathrm{Tr}(u_i) = \sum_{g \in C_i} \chi(g) = |C_i| \chi(C_i)$ car χ est constant sur les classes de conjugaison.

Comme χ est irréductible, la relation de normalité des caractères donne :

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

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

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

D'après ① et ③, $\lambda_i \in \mathcal{A}$ et $\chi(C_i) \in \mathcal{A}$ donc $\overline{\chi(C_i)} \in \mathcal{A}$ et comme $\mathcal{A}$ est un sous-anneau de $\mathbb{C}$, on obtient $\frac{n}{d} \in \mathcal{A}$.

$\frac{n}{d}$ est un rationnel et un entier algébrique, c'est donc un entier tout court. Donc $d \mid n$.

□

Détails

Caldero p342 • Si un caractère d'un groupe fini G a ses valeurs dans $\mathbb{Q}$, alors ses valeurs sont dans $\mathbb{Z}$.

D'après Lagrange, le caractère $\chi(g)$ est un entier algébrique comme somme d'entiers algébriques (ce sont les valeurs propres de $\rho(g)$ qui sont des racines de l'unité). Il existe donc $P \in \mathbb{Z}[X]$ unitaire qui annule $\chi(g)$. On écrit $\chi(g) = \frac{p}{q}$ avec p et q premiers entre eux dans $\mathbb{Z}$.

$$P\left(\frac{p}{q}\right) = 0 = \frac{p^m}{q^m} + a_{m-1}\frac{p^{m-1}}{q^{m-1}} + \dots + a_0 \quad \text{donc} \quad p^m + \underbrace{\sum_{i=0}^{m-1} a_i p^i q^{m-i}}_{\text{divisible par } q} = 0$$

Donc $q \mid p^m$ et $q \wedge p^m$ donc par lemme de Gauss, $q \mid 1$

d'où $\chi(g) = \frac{p}{q} \in \mathbb{Z}$.

Caldero p264 • Lemme de Schur : soient $\rho : G \to GL(V)$ et $\rho' : G \to GL(V')$ deux représentations irréductibles et $\varphi : V \to V'$ un morphisme de représentations. Alors : i) φ est soit nul, soit un isomorphisme.
ii) si $V = V'$ et $\mathbb{K}$ est algébriquement clos, φ est une homothétie

i) φ est un morphisme de représentations donc $\varphi \circ \rho(g) = \rho'(g) \circ \varphi \quad \forall g \in G$
Le noyau et l'image de φ sont donc stables par G : ce sont deux sous-représentations. Par irréductibilité de ρ et ρ', on peut affirmer que φ est nul ou injectif et qu'il est nul ou surjectif. Bref φ est nul ou bijectif.

ii) Si $\mathbb{K}$ est algébriquement clos, un élément φ de $\mathrm{End}_{\mathbb{K}}(V)$ admet une valeur propre $\lambda \in \mathbb{K}$. Mais alors $\ker(\varphi - \lambda \mathrm{Id}_V)$ est une sous-représentation de V non réduite à $\{0\}$. Par irréductibilité de V, on a $V = \ker(\varphi - \lambda \mathrm{Id}_V)$ i.e. $\varphi = \lambda \mathrm{Id}_V$.

- On a équivalence entre : i) $\mathrm{Res}(P,Q) \neq 0$
  ii) $\forall R \in k_{n+m}[X]$, $\exists U \in k_n[X]$, $V \in k_m[X]$, $R = UP + VQ$
  iii) $\exists U \in k_n[X]$, $V \in k_m[X]$, $UP + VQ = 1$.
  iv) P et Q sont premiers entre eux.
  v) Si K/k est une extension sur laquelle P ou Q est scindé, P et Q n'ont aucune racine commune dans K.

La non-annulation de $\mathrm{Res}(P,Q)$ équivaut à la surjectivité de l'application linéaire associée, d'où i) $\Leftrightarrow$ ii). Ensuite ii) $\Rightarrow$ iii) $\Rightarrow$ iv). Montrons iv) $\Rightarrow$ ii). Pour $R \in k_{n+m}[X]$, il existe bien sûr $U, V \in k[X]$ tq $UP + VQ = R$ (sans condition de degré). Notons $\tilde{U} = U - AQ \in k_n[X]$ le reste de la division euclidien de U par Q. Posons $\tilde{V} = V + AP$. On a aussitôt $\tilde{U}P + \tilde{V}Q = R$. D'autre part, comme $\tilde{V}Q = R - \tilde{U}P$ et que R et $\tilde{U}P$ sont de degré $< n+m$, on a $\tilde{V} \in k_m[X]$.
Or P et Q ont même pgcd dans $k[X]$ et dans $K[X]$ (l'algorithme d'Euclide se déroulant de la même manière quelque soit le corps sur lequel on se place) donc on a iv) $\Leftrightarrow$ v).

Autre façon de montrer i) $\Leftrightarrow$ v) : on montre que $\forall \lambda \in A$, $\mathrm{Res}((X-\lambda)P, Q) = \mathrm{Res}(P,Q) \cdot \mathrm{Res}((X-\lambda), Q)$. Comme on sait que $\mathrm{Res}(P(X+\lambda), Q(X+\lambda)) = \mathrm{Res}(P,Q)$, on peut supposer $\lambda = 0$. Sur la dernière colonne de la matrice $\mathrm{Syl}(XP, Q)$, tous les coeff. sont nuls sauf éventuellement le dernier qui vaut $Q(0)$. Donc en développant le calcul par rapport à cette colonne, on a $\mathrm{Res}(XP, Q) = \mathrm{Res}(P,Q) \cdot Q(0)$ et on remarque que $\mathrm{Res}(X, Q) = Q(0)$. En outre, on a montré $\mathrm{Res}(X-\lambda, Q) = Q(\lambda)$. Par récurrence, on obtient que si $a_1, \dots, a_m \in A$ et qu'on suppose que $P = (X-a_1)\cdots(X-a_m)$, alors $\mathrm{Res}(P,Q) = \prod_{i=1}^{m} Q(a_i)$ ce qui fournit l'équivalence i) $\Leftrightarrow$ v).