Anneau des entiers algébriques

30 juin 2013

Définition. On dit que $\alpha \in \mathbb{C}$ est algébrique sur $\mathbb{Q}$ s'il existe $P(X) \in \mathbb{Q}[X]$ unitaire non nul tel que $P(\alpha) = 0$. On dit que α est un entier algébrique s'il existe $P(X) \in \mathbb{Z}[X]$ unitaire non nul tel que $P(\alpha) = 0$.

Théorème. *Soient α et β algébriques sur $\mathbb{Q}$ (respectivement entiers algébriques). Alors, $\alpha+\beta$ et $\alpha\beta$ sont algébriques sur $\mathbb{Q}$ (resp. entiers algébriques). En particulier, les algébriques sur $\mathbb{Q}$ et les entiers algébriques forment un anneau unitaire.*

Démonstration. Commençons par étudier le cas de la somme : Soient $A(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0 \in \mathbb{Q}[X]$ et $B(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0 \in \mathbb{Q}[X]$ tels que $A(\alpha) = 0$ et $B(\beta) = 0$. On pose $S(Y) = R_X(A(X), B(Y-X))$ le résultant de $A(X) \in \mathbb{Q}[X]$ et $B(Y-X) \in \mathbb{Q}[Y][X]$. Alors, on a $S(\alpha+\beta) = 0$. En effet, pour $Y = \alpha + \beta$, $X = \alpha$ est une racine commune de $A(X)$ et $B(\alpha+\beta-X)$ donc $S(\alpha+\beta) = 0$ par propriété du resultant. Par ailleurs, $S(Y) \in \mathbb{Q}[Y]$ et est non nul. Il existe $(P_i(Y))_{0\leq i\leq n} \in \mathbb{Q}[Y]$ tels que $B(Y-X) = P_n(Y)X^n + \ldots + P_0(Y)$ d'où :

$$S(Y) = \begin{vmatrix} 1 & 0 & \cdots & 0 & P_n(Y) & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ a_1 & & & 1 & \vdots & & & P_n(Y) \\ a_0 & \ddots & & \vdots & P_0(Y) & & & \vdots \\ 0 & \ddots & \ddots & \vdots & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & a_1 & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & P_0(Y) \end{vmatrix} \in \mathbb{Q}[Y]$$

Supposons à présent que $A(X)$ et $B(X) \in \mathbb{Z}[X]$. On calcule $B(Y-X)$ par la formule de Taylor :

$$B(Y-X) = B(Y) - XB'(Y) + \frac{X^2}{2}B"(Y) + \cdots + (-1)^{n-1}X^{n-1}\frac{B^{(n-1)}(Y)}{(n-1)!} + (-1)^n X^n \in \mathbb{Z}[Y][X]$$

En effet, $\frac{B^{(n-k)}(Y)}{(n-k)!} = \frac{n.(n-1).....(k+1).Y^k + \cdots + (n-k+1)....2.Y + (n-k)!}{(n-k)!} = \begin{pmatrix} n \\ k \end{pmatrix} Y^k + \cdots + (n-k+1)Y + 1 \in \mathbb{Z}[Y]$

Le seul terme en Y^n provient de $B(Y)$ car le degré partiel en Y de $B^{(k)}(Y)$ pour $1 \leq k \leq n$ est $\deg_Y(B^{(k)}(Y)) \leq n-1$. Or, $B(Y) = Y^n + \ldots + b_0$ donc le coefficient en Y^n de $B(Y-X)$ est 1. De plus,

$$S(Y) = \begin{vmatrix} 1 & 0 & \cdots & 0 & (-1)^n & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ a_1 & & & 1 & -B'(Y) & & & (-1)^n \\ a_0 & \ddots & & \vdots & B(Y) & \ddots & & \vdots \\ 0 & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 & \vdots & \ddots & \ddots & -B'(Y) \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & B(Y) \end{vmatrix} \in \mathbb{Z}[Y]$$

Son terme dominant est Y^{mn}. En effet, pour obtenir le coefficient dominant, on est obligé de garder tous les termes en $B(Y)$ donc de développer successivement par rapport à la dernière colonne. On obtient que le terme dominant

de $S(Y)$ est égal à celui de $B(Y)^m \begin{vmatrix} 1 & 0 & \cdots & 0 \\ a_{n-1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ a_0 & \cdots & a_{n-1} & 1 \end{vmatrix} = B(Y)^m$ qui est Y^{mn}. Ainsi, $S(Y) \in \mathbb{Z}[Y]$ et est unitaire et non nul. Un raisonnement similaire nous permet de dire que $S(Y)$ est non nul dans le cas où $A(X)$ et $B(X) \in \mathbb{Q}[X]$. On conclut que $\alpha + \beta$ est algébrique sur $\mathbb{Q}$ (resp. entier algébrique).

On étudie à présent $\alpha\beta$. On recommence l'étude précédente avec $P(Y) = R_X(A(X), X^n B(\frac{Y}{X}))$. L'écriture a un sens puisque $X^n B(\frac{Y}{X}) \in \mathbb{Q}[X, Y]$ car $\deg B(X) = n$. Pour $Y = \alpha\beta$, $X = \alpha$ est une racine commune de $A(X)$ et $X^n B(\frac{Y}{X})$ donc $P(\alpha\beta) = 0$. De la même manière que précédemment, $X^n B(\frac{Y}{X}) \in \mathbb{Q}[Y][X]$ donc $P(Y) \in \mathbb{Q}[Y]$ et est non nul. Si $A(X)$ et $B(X) \in \mathbb{Z}[X]$,

$$X^n B\left(\frac{Y}{X}\right) = b_0 X^n + b_1 Y X^{n-1} + \cdots + b_1 Y^{n-1} X + Y^n$$

$$P(Y) = \begin{vmatrix} 1 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 & \vdots & & \ddots & 0 \\ a_1 & & & 1 & b_{n-1}Y^{n-1} & & & b_0 \\ a_0 & \ddots & & \vdots & Y^n & \ddots & & \vdots \\ 0 & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 & \vdots & \ddots & \ddots & b_{n-1}Y^{n-1} \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & Y^n \end{vmatrix} \in \mathbb{Z}[Y]$$

et comme précédemment, le terme de plus haut degré est Y^{mn}. On conclut donc que $\alpha\beta$ est algébrique sur $\mathbb{Q}$ (resp. entier algébrique). □

Leçons concernées :

142 Algèbre des polynômes à plusieurs indéterminées. Applications.

143 Résultant. Applications.

144 Racines d'un polynôme. Fonctions symétriques élémentaires. Localisation des racines dans les cas réel et complexe.

152 Déterminant. Exemples et applications.

Références

[1] Aviva Spzirglas. L3 Algèbre. Pearson Education.