Éléments entiers sur $\mathbb{Z}$

Définition : Soit $x \in \mathbb{C}$. On dit que x est entier sur $\mathbb{Z}$ s'il existe $a_1, ..., a_n \in \mathbb{Z}$ tels que :

$$x^n + a_1 x^{n-1} + ... + a_n = 0 \ .$$

exemple : $\sqrt{2}$ est entier sur $\mathbb{Z}$

Proposition 1 *Soit $p/q \in \mathbb{Q}$. Si p/q est entier sur $\mathbb{Z}$, alors $p/q \in \mathbb{Z}$.*

Démonstration : On peut supposer p et q premiers entre eux. Alors :

$$p^n + a_1 p^{n-1} q + ... + a_n q^n = 0 \ .$$

Donc $q | p^n$. Or q est premier à p donc $q = \pm 1$. *q.e.d.*

Proposition 2 *Soit $x \in \mathbb{C}$. Sont équivalentes :*

i) x est entier sur $\mathbb{Z}$;

ii) $\mathbb{Z}[x]$ est un $\mathbb{Z}-$module de type fini ;

iii) il existe un anneau A qui contient x et 1 et qui est un $\mathbb{Z}-$module de type fini.

Démonstration : i) $\Rightarrow$ ii) : supposons que $x^n + a_1 x^{n-1} + ... + a_n = 0$ pour certains $a_i \in \mathbb{Z}$. Alors le $\mathbb{Z}-$module de type fini $\mathbb{Z} + ... + \mathbb{Z}x^{n-1}$ est stable par multiplication par $\mathbb{Z}$ et par x c'est donc $\mathbb{Z}[x]$.

ii) $\Rightarrow$ iii) : facile.

iii) $\Rightarrow$ i) : Soit A un anneau qui contient x, 1 et qui est de type fini comme $\mathbb{Z}-$module. Soient $b_1, ..., b_n$ des générateurs.

Pour tout i, on a : $x b_i = a_{i,1} b_1 + ... + a_{i,n} b_n$ pour certains $a_{i,j} \in \mathbb{Z}$.

Soit M la matrice $xI_n - (a_{i,j}) \in \mathscr{M}_n(A)$.

Si $v = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in A^n$, alors on a $Mv = 0$.

Notons N la transposée de la comatrice de M. On a : $NM = \det M I_n$.

Donc : $NMv = 0 \Rightarrow \det M b_i = 0$ pour tout $1 \leq i \leq n$. Donc $\det M = 0$ car 1 est une combinaison $\mathbb{Z}-$linéaire des b_i.

Or $\det M$ est le polynôme caractéristique de la matrice $(a_{i,j}) \in \mathscr{M}_n(\mathbb{Z})$ évalué en x. Ce polynôme caractéristique est donc un polynôme à coefficients entiers unitaire qui annule x. *q.e.d.*

Corollaire 3 *Soient $x, y \in \mathbb{C}$ entiers sur $\mathbb{Z}$, alors $x+y$ et xy sont entiers sur $\mathbb{Z}$.*

Démonstration : Montrons par exemple que xy est entier sur $\mathbb{Z}$: soient $b_1, ..., b_m$ des générateurs du $\mathbb{Z}-$module $\mathbb{Z}[x]$ et $c_1, ..., c_n$ des générateurs du $\mathbb{Z}-$module $\mathbb{Z}[y]$. Alors $\mathbb{Z}[x]\mathbb{Z}[y]$ est un $\mathbb{Z}-$module de type fini engendré par les $b_i c_j$. C'est aussi un anneau qui contient 1 et xy. *q.e.d.*

Notation : on pose $\overline{\mathbb{Z}}$ le sous-anneau de $\mathbb{C}$ formé des éléments entiers sur $\mathbb{Z}$.

Corollaire 4 *Soit $f(X)$ un polynôme unitaire à coefficients entiers. Alors tous les facteurs unitaires de $f(X)$ dans $\mathbb{Q}[X]$ sont à coefficients entiers.*

Démonstration : Soit $p(X)$ un facteur unitaire de $f(X)$ dans $\mathbb{Q}(X)$. On a :

$$p(X) = (X - x_1)...(X - x_d)$$

pour certains $x_i \in \mathbb{C}$. Le coefficient de $p(X)$ de degré k est :

$$a_k = \sum_{i_1<...<i_{d-k}} x_{i_1}...x_{i_{d-k}} \ .$$

Les x_i sont en particulier racines de f donc entiers sur $\mathbb{Z}$. On a donc $a_k \in \overline{\mathbb{Z}}$. Or $a_k \in \mathbb{Q}$ car $p(X)$ est à coefficients dans $\mathbb{Q}$. Comme $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$, on a : $a_k \in \mathbb{Z}$ pour tout k. *q.e.d.*

Application : irréductibilité des polynômes cyclotomiques

Soit $\Phi_n(X) := \prod_{\substack{k=1 \\ k\wedge n=1}}^{n-1} (X - e^{2ik\pi/n})$.

Le polynôme $\Phi_n(X)$ est unitaire à coefficients entiers. Soit $f(X)$ le polynôme minimal unitaire de $e^{2i\pi/n}$ sur $\mathbb{Q}$. On a $f(X)|X^n-1$ donc $f(X) \in \mathbb{Z}[X]$ d'après le corollaire précédent.

Nous allons montrer que si p est un nombre premier qui ne divise pas n, si z est une racine de f, alors z^p est aussi une racine de f.

Par l'absurde : Si z est une racine de f et si pourtant $f(z^p) \neq 0$, alors notons $z_1, ..., z_d$ les racines (distinctes) de f. On a :

$$f(z^p) = (z^p - z_1)...(z^p - z_d) \ .$$

Soit $\Delta = (-1)^{n(n-1)/2} \prod_{i\neq j}(u_i - u_j)$, où les u_i sont les racines $n-$ièmes de 1, le discriminant de $X^n - 1$. C'est un élément entier sur $\mathbb{Z}$ car les u_i le sont.

Comme les z_i et z^p sont des racines $n-$ièmes de 1, on a :

$$f(z^p)|\Delta$$

dans $\overline{\mathbb{Z}}$. Or, dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a :

$$f(X^p) = f(X)^p$$

d'où : $f(X^p) = f(X) \bmod p\mathbb{Z}[X]$. On en déduit que $f(z^p) = 0 \bmod p\overline{\mathbb{Z}}$.

Donc $p|\Delta$ dans $\overline{\mathbb{Z}}$. Autrement dit, il existe $q \in \overline{\mathbb{Z}}$ tel que $pq = \Delta$. On a $q = \Delta/p \in \mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. Ainsi, $p|\Delta$ dans $\mathbb{Z}$.

Or, on a :

$$\begin{aligned}\Delta &= (-1)^{n(n-1)/2} \prod_{i=1}^{n} (X^n - 1)'(u_i) \\ &= \pm \prod_{i=1}^{n} n u_i^{n-1} \\ &= \pm n^n \ .\end{aligned}$$

Donc $p|n^n$ ce qui est absurde car on a supposé que p ne divise pas n.

Soit k un entier premier à n. On a $k = p_1...p_r$ pour certains nombres premiers p_i qui ne divisent pas n.

Comme $z^k = ((z^{p_1})^{p_2})^{\cdots}$, on a par récurrence : z^k racine de f. Donc $\Phi_n(X)$ divise $f(X)$. Comme $f(X)$ divise $\Phi_n(X)$, on obtient $\Phi_n(X) = f(X)$ et $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$.

Exemple : $\Phi_4(X) = X^2 + 1$.