Critère d'irréductibilité

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **17 (1971)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **14.07.2024**

UN CRITÈRE D'IRRÉDUCTIBILITÉ DES POLYNOMES

par Maurice MIGNOTTE

NOTATIONS

A désigne un anneau commutatif unitaire tel que tout élément non nul de A n'a qu'un nombre fini de diviseurs.

P est un polynôme de degré $d \geqslant 1$ de $A[x]$.

$u = u(P) =$ nombre d'éléments $a \in A$ tels que $P(a)$ soit une « unité » de A.

$i = i(P) =$ nombre d'éléments $a \in A$ tels que $P(a)$ soit irréductible dans A.

Remarquons d'abord que 1 n'a qu'un nombre fini de diviseurs, ainsi il n'y a qu'un nombre fini d'unités $e_1, e_2, \ldots, e_k$ dans A.

Soient $a_{j,1}, \ldots, a_{j,u_j}$ les éléments tels que $P(a) = e_j, j = 1, \ldots, k$. A étant intègre, on a l'inégalité $u_j \leqslant d$. Donc $u = u_1 + \ldots + u_k$ est fini. Par contre, il peut se faire que i ne soit pas fini, si tel est le cas, dans tout ce qui suit on pourra remplacer i par un entier i' assez grand.

CRITÈRE D'IRRÉDUCTIBILITÉ

Théorème : Il existe une constante c (ne dépendant que de A) telle que l'inégalité

$$i + 2u - d > c$$

implique l'irréductibilité de P sur $A[x]$.

Démonstration:

Supposons que l'on ait $P = Q.R$ avec $Q, R \in A[x]$, avec $\deg(Q)$, $\deg(R) \geqslant 1$.
Les implications

$$P(a) \text{ irréductible} \Rightarrow Q(a) \text{ ou } R(a) \text{ inversible},$$
$$P(a) \text{ inversible} \Rightarrow Q(a) \text{ et } R(a) \text{ inversibles},$$

conduisent à l'inégalité

$$u(Q) + u(R) \geqslant i + 2u$$

ou encore à

$$f(Q) + f(R) \geqslant i + 2u - d$$

avec

$$f(Q) = u(Q) - \deg(Q), \; f(R) = u(R) - \deg(R).$$

Supposons que l'on ait montré l'existence d'une constante F telle que $f(S) \leqslant F$ pour tout $S \in A[x]$, il est clair que le théorème sera vrai avec $c = 2F$.

Soit, par exemple, $u_1 = \max\limits_{1 \leq j \leq k} (u_j)$ et $u_2 = \max\limits_{2 \leq j \leq k} (u_j)$.

Si $u_2 = 0$, alors on a $f \leqslant 0$, il n'y a rien à démontrer.

Sinon on peut écrire

$$P(X) = (X - a_{1,1}) \dots (X - a_{1,u_1}) P_1(X) + e_1$$

avec

$$P_1(X) \in A[X], \qquad et \qquad P(a_{2,1}) = e_2.$$

Ainsi les $a_{2,1} - a_{1,k}$ sont des diviseurs de $e_1 - e_2$ il n'y en a qu'un nombre fini n, par suite $u_1 \leqslant n$. Il en résulte que

$$f = u - d \leqslant ku_1 - d \leqslant kn - 1.$$

Comme il n'y a qu'un nombre fini de choix possibles de $e_1 - e_2$, l'existence de F est bien démontrée. Ceci achève la démonstration.

Exemples

$A = \mathbf{Z}$; $c = 4$ convient.

$A =$ anneau des entiers d'un corps quadratique imaginaire

Si $A = \mathbf{Z}[i]$, $c = 8$ convient $(i^2 = -1)$.

Si $A = \mathbf{Z}[j]$, $c = 16$ convient $(j^3 = 1)$.

Sinon $c = 4$ convient.

$A = \mathbf{F}_q[X]$, $\mathbf{F}_q$ corps fini à q éléments, il est clair que $c = 2((q-1)^2 - 1)$ convient.

(Reçu le 1er juin 1971)

Maurice Mignotte
Faculté des Sciences
Place du 8-Mai 1945
F-93 — Saint-Denis