Critère d'irréductibilité d'Eisenstein

Dorian Cacitti-Holland

2020-2021

Références.

1. Théorie de Galois d'Yvan Gozard
2. Cours d'algèbre de Daniel Perrin

Leçons.

1. 120 Anneaux $\mathbb{Z}/n\mathbb{Z}$, applications
2. 121 Nombres premiers, applications
3. 141 Polynômes irréductibles à une indéterminée, corps de rupture, exemple et applications
4. 142 PGCD et PPCM, algorithmes de calcul, applications

Théorême. Soit A un anneau factoriel et $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ de degré $n \in \mathbb{N}^*$ tel qu'il existe $p \in A$ irréductible tel que :

1. p ne divise pas a_n
2. $\forall k \in [\![0, n-1]\!], p \mid a_k$
3. p^2 ne divise pas a_0

Alors P est irréductible sur $Frac(A)$.

Démonstration. On suppose par l'absurde qu'il existe $(U, V) \in Frac(A)[X]$ tel que

$$P = UV, deg(U) \geq 1, deg(V) \geq 1$$

Lemme. Il existe $(Q, R) \in A[X]$ tel que

$$P = QR, deg(Q) \geq 1, deg(R) \geq 1$$

Démonstration. Soit a PPCM des dénominateurs des coefficients non nuls de U et V, alors

$$a^2 P = (aU)(aV) = Q_0 R_0$$

Avec $Q_0 = aU \in A[X], R_0 = aV \in A[X]$.
On écrit $Q_0 = c(Q_0)Q_1, R_0 = c(R_0)R$ avec $Q_1, R \in A[X]$ primitifs.
On a donc par lemme de Gauss sur le contenu,

$$a^2 P = c(Q_0)c(R_0)Q_1 R = a^2 c(P)Q_1 R$$

Or $a \neq 0$ comme produit de tels élements et A intègre, d'où

$$P = c(P)Q_1R = QR$$

Avec $c(P) \in A$ et $Q = c(P)Q_1 \in A[X]$, ce qui conclut. □

On écrit

$$Q = \sum_{i=0}^{r} b_i X^i, R = \sum_{j=0}^{s} c_j X^j$$

avec $b_r c_s = a_n \neq 0, r \geq 1, s \geq 1$.
En particulier $r = n - s \leq n - 1$ et $s = n - r \leq n - 1$.
Soit $\varphi : A \longrightarrow A/pA$ la surjection canonique, alors φ est un morphisme d'anneaux que l'on prolonge naturellement en un morphisme d'anneaux

$$\begin{array}{rccc} & A[X] & \longrightarrow & A/pA[X] \\ \overline{\varphi} : & S = \sum_{k=0}^{t} d_k X^k & \longmapsto & \sum_{k=0}^{t} \varphi(d_k) X^k \end{array}$$

Ainsi

$$\overline{\varphi}(P) = \overline{\varphi}(Q)\overline{\varphi}(R) = \left(\sum_{i=0}^{r} \varphi(b_i) X^i \right) \left(\sum_{j=1}^{s} \varphi(c_j) X^j \right)$$

Or $\forall k \in [\![0, n-1]\!], p \mid a_k$, donc

$$\overline{\varphi}(P) = \varphi(a_n) X^n$$

Ainsi, avec ce qui précède, grâce à la factorialité de $Frac(A/pA)[X]$ et l'irréductibilité de X,

$$X \mid \varphi(Q) \text{ et } X \mid \varphi(R) \text{ dans } Frac(A/pA)[X]$$

D'où

$$\varphi(b_0) = 0 = \varphi(c_0) \text{ ie } p \mid b_0, p \mid c_0$$

Par conséquent $p^2 \mid b_0 c_0 = a_0$ ce qui est absurde. □

Corollaire. Dans ce cas, si de plus P est primitif alors P est irréductible sur A.

Démonstration. Soit $(Q, R) \in A[X]^2$ tel que

$$P = QR$$

Alors en particulier

$$(Q, R) \in (Frac(A)[X])^2$$

Or d'après le théorème précédent, P est irréductible sur $Frac(A)$, d'où

$$Q \in Frac(A)^* \text{ ou } R \in Frac(A)^*$$

Quitte à échanger les rôles de Q et R, supposons

$$Q \in Frac(A)^* \cap A[X] = A^*$$

Or

$$c(P) = c(Q)c(R) = Qc(R)$$

D'où, dans A,

$$Q \mid c(P)$$

Or P est primitif, donc $c(P) \in A^\times$, ainsi

$$Q \in A^\times$$

Ce qui prouve que P est irréductible sur A. □

Exemple. (S'il reste du temps) Soit $p \in \mathbb{N}$ premier, alors $P = \sum_{i=0}^{p-1} X^i$ irréductible dans $\mathbb{Z}[X]$

Démonstration. Comme

$$(X-1)P = X^p - 1$$

On a

$$P(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1} = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i$$

Or

$$\forall i \in [\![0, p-2]\!], p \mid p \dots (p-i) = (i+1)! \binom{p}{i+1}$$

Donc, par théorème de Gauss

$$\forall i \in [\![0, p-2]\!], p \mid \binom{p}{i+1}$$

De plus p ne divise pas $\binom{p}{p-1+1} = 1$ et p^2 ne divise pas $\binom{p}{1} = p$.
On peut donc appliquer ce qui précède pour conclure que $P(X+1)$ est irréductible sur $\mathbb{Z}$, donc P également. □