Critère d'Eisenstein

Développement pour les leçons 122 [1], 125 [2], 141 [3].

1 Introduction

Soit A un anneau factoriel et p un élément premier de A. On note K le corps de fraction de A. Le critère d'Eisenstein est un critère d'irréductibilité de polynômes de $A[X]$ dans $K[X]$. Plus précisément, si $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ vérifie :

1. $p \nmid a_N$.
2. $\forall i < n, p \mid a_i$.
3. $p^2 \nmid a_0$.

Alors P est irréductible sur $K[X]$. La stratégie de la preuve est simple : on va tout d'abord démontrer le lemme des contenus, qui nous permettra de montrer que l'irréductibilité sur $A[X]$ implique l'irréductibilité sur $K[X]$ en raisonnant par contraposée. Enfin, on démontrera à proprement parler le critère d'Eisenstein en raisonnant par l'absurde. On donnera à la fin du document une application classique de ce critère d'irréductibilité.

2 Développement

Dans la suite, $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ et on notera $c(P)$ son contenu, c'est à dire le PGCD de ses coefficients.

Étape 1 : On va démontrer ici le lemme des contenus, à savoir que si $P, Q \in A[X]$, alors $c(PQ) = c(P)c(Q)$. Dans un premier temps, supposons que $c(P) = c(Q) = 1$. Montrons alors que $c(PQ) = 1$.

Par l'absurde, supposons que $c(PQ) \neq 1$. alors il existe un élément premier $p \in A$ tel que p divise chaque coefficient de PQ dans $A[X]$. Mais p étant premier dans A, l'idéal (p) est premier dans $A[X]$ et donc $A[X]/(p)$ est intègre et on a que

$$\overline{PQ} = \overline{P}\,\overline{Q} = \overline{0} \quad \Rightarrow \quad \overline{P} = \overline{0} \text{ ou } \overline{Q} = \overline{0}$$

ce qui contredit le fait que $c(P) = c(Q) = 1$. Dans le cas général, on écrit $P = c(P)P'$ et $Q = c(Q)Q'$ avec $c(P') = c(Q') = 1$. On a donc que

$$c(PQ) = c(c(P)P'c(Q)Q') = c(P)c(Q)c(P'Q') = c(P)c(Q)$$

ce qui termine la démonstration.

Étape 2 : Montrons ici que P irréductible sur $A[X]$ implique que P est irréductible sur $K[X]$. Pour cela, on va raisonner par contraposé. Supposons que $P \in A[X]$ soit réductible dans $K[X]$. Notons $P = c(P)P'$ avec P' primitif. On a alors P' réductible dans $K[X]$ et donc $P' = Q'R'$ avec $Q', R' \in K[X]$ tout deux de degrés strictement plus petit que le degré de P. Notons q et r les produits des dénominateurs des coefficients de Q' et de R' et notons $Q = qQ'$ et $R = rR'$. Alors $Q, R \in A[X]$ et on a que $qrP' = QR$. Ainsi, en passant au contenu, on a que $qr = c(Q)c(R)$. Ainsi, on obtient que

$$P = c(P)P' = c(P)\frac{QR}{qr} = c(P)\frac{QR}{c(Q)c(R)} = \left(c(P)\frac{Q}{c(Q)}\right)\left(\frac{R}{c(R)}\right)$$

et donc P est réductible dans $A[X]$.

Étape 3 : Soit $P \in A[X]$ qui vérifie les hypothèses du critère d'Eisenstein. Il suffit de montrer que P est irréductible dans $A[X]$ afin d'obtenir qu'il l'est dans $K[X]$. Supposons donc par l'absurde que P n'est pas irréductible dans $A[X]$. Alors il existe $Q = \sum_{i=0}^{k} q_i X^i$ et $R = \sum_{j=0}^{\ell}$ dans $A[X]$ de degrés plus petit que $n = \deg P$ et tels que $P = QR$. Par hypothèse, en réduisant modulo (p), on obtient l'égalité

$$\overline{a_n} X^n = \overline{Q}\,\overline{R}$$

Or, on sait que $a_n = q_k r_\ell$ et donc $deg\overline{Q} = k$ et $\deg \overline{R} = \ell$. De même, l'intégrité de $A[X]/(p)$ nous donne directement que $\overline{Q}$ et $\overline{R}$ sont des monômes. En effet, s'ils n'étaient pas des monômes, on aurait un coefficient de $\overline{P}$ de degré $< n$, ce qui contredit l'hypothèse de départ. Or, on a notamment que $\overline{q_0} = \overline{r_0} = \overline{0}$ et donc $p \mid q_0$ et $p \mid r_0$ et ainsi on a que $p^2 \mid a_0$ ce qui contredit l'hypothèse initiale. Ainsi, on obtient que P est irréductible sur $A[X]$ et donc sur $K[X]$ par ce qui précède. □

1. Anneaux principaux. Applications.
2. Extensions de corps. Exemples et applications.
3. Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

3 Applications

Le cas où $A = \mathbb{Z}$ et où p est un nombre premier est le plus fréquent. On donnera par la suite un autre cas plus exotique et plus rigolo.

Exemple 1 : Soit p un nombre premier et $\phi_p(X) = \sum_{i=0}^{p-1} X^i = X^{p-1} + \cdots + X + 1$ le p-ième polynôme cyclotonique. Alors ϕ_p est irréductible. Pour ce faire, on va appliquer le critère d'Eisenstein au polynôme translaté $\phi_p(X+1)$. On a alors

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

Or, on voit alors que

1. On a $p \nmid \binom{p}{p} = 1$.
2. On a pour tout $1 \leq i < p$ que $p \mid \binom{p}{i}$.
3. On a $p^2 \nmid \binom{p}{p-1} = p$.

Ainsi, par le critère d'Eisenstein, $\phi_p(X+1)$ est irréductible. Pour passer à $\phi_p(X)$, on suppose que $\phi_p(X) = P(X)Q(X)$, alors $\phi_p(X+1) = P(X+1)Q(X+1)$ est irréductible et on conclut directement.

Exemple 2 : On considère ici $A = K[X]$ avec K un corps différent de $\mathbb{F}_2$. On considère dans $A[Y]$ (qui est bien factoriel) le polynôme

$$P(Y) = Y^2 - X(X-1)(X-\lambda)$$

avec $\lambda \neq 0, 1$. Alors P est irréductible. On considère en effet l'élément premier X (premier car $A[Y]/(X) \simeq K[Y]$ qui est intègre). On a bien $X \nmid 1$, $X \nmid X(X-1)(X-\lambda)$ et $X^2 \nmid X(X-1)(X-\lambda)$.

4 Bibliographie

C'est fait dans *Algèbre, le grand combat* (me demandez plus à quelle page...). C'est aussi dans le Perrin.