Critère d'Eisenstein

Notions utilisées : Corps finis, anneau intègre, polynômes primitifs.

Prérequis : notion de polynôme primitif, de divisibilité dans un anneau factoriel.

Motivations

Le critère d'Eisenstein permet de donner une méthode efficace basée sur la réduction modulo p pour savoir si un polynôme est irréductible ou non. Il existe une version sur le corps des fractions d'un anneau factoriel ; ici on se contente de l'énoncer sur $\mathbb{Z}$ et son corps des fractions $\mathbb{Q}$.

Théorème 1. *Soit $P := \sum_{k=0}^{n} c_k X^k \in \mathbb{Z}[X]$. On suppose qu'il existe $p \in \mathbb{N}$ un nombre premier tel que :*

- *Pour tout $k \in [\![0, n-1]\!]$, p divise c_k,*
- *p ne divise pas c_n*
- *p^2 ne divise pas c_0.*

Alors P est irréductible dans $\mathbb{Q}[X]$. Si de plus P est primitif alors P est irréductible dans $\mathbb{Z}[X]$

Pour démontrer ceci, on se propose de démontrer en premier lieu les deux lemmes suivants :

Lemme 2. *Soient $A, B \in \mathbb{Z}[X]$ deux polynômes primitifs. Alors leur produit est un polynôme primitif.*

Lemme 3. *Soient $A, B \in \mathbb{Z}[X]$. Alors $c(AB) = c(A)c(B)$ où c désigne le contenu (PGCD des coefficients) d'un polynôme.*

Preuve du premier lemme. On note $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{m} b_k X^k$. Supposons par l'absurde que leur produit $C = \sum_{k=0}^{n+m} c_k X^k$ soit non primitif. Alors par définition du contenu, il existe un entier $l \in \mathbb{Z} \setminus \{-1, 1\}$ tel que l divise tous les c_k. En particulier il existe un nombre premier $p \in \mathbb{N}$ tel que p divise tous les c_k. L'idée est alors d'effectuer une réduction modulo p pour aboutir à une contradiction (on cherche à aboutir à la conclusion que A ou B n'est pas primitif).

Dans $\mathbb{Z}/p\mathbb{Z}[X]$ on a $\overline{AB} = \overline{A}\,\overline{B} = \overline{C} = \overline{0}$ où $\bar{\cdot}$ désigne la réduction modulo p. Mais $\mathbb{Z}/p\mathbb{Z}$ est un corps, et donc $\mathbb{Z}/p\mathbb{Z}[X]$ est un anneau intègre. On en déduit que ou bien $\overline{A} = 0$ ou bien $\overline{B} = 0$ (ou bien les deux). Supposons par exemple $\overline{A} = 0$, quitte à échanger les rôles. On en déduit alors que p divise tous les a_k, et donc que A n'est pas primitif, ce qui contredit notre hypothèse initiale. Cela conclut la preuve du premier lemme. □

Preuve du second lemme. On remarque que si $\lambda \in \mathbb{Z}$ alors pour tout polynôme P, $c(\lambda P) = \lambda c(P)$. En effet, si x, y, z sont des éléments d'un anneau factoriel, alors

$$\mathrm{PGCD}(xy, xz) = \prod_{p \in \mathcal{P}} p^{\min(v_p(xy), v_p(xz))} = \prod_{p \in \mathcal{P}} p^{v_p(x) + \min(v_p(y), v_p(z))} = x \times \mathrm{PGCD}(y, z).$$

On a ici utilisé la définition du PGCD dans un anneau factoriel et du fait que la valuation p-adique d'un produit est la somme des valuations p-adiques (cela se montre avec l'unicité de la DFI dans un anneau factoriel).[1] On a donc $c\left(\frac{A}{c(A)}\frac{B}{c(B)}\right) = 1$ d'après le premier lemme, et d'après la remarque qui précède on en déduit $\frac{1}{c(A)}\frac{1}{c(B)}c(AB) = 1$ d'où le résultat annoncé. □

Preuve du critère d'Eisenstein. Soit $P := \sum_{k=0}^{n} c_k X^k \in \mathbb{Z}[X]$ et p comme dans l'énoncé.

Etape 1 : Preuve en admettant la réductibilité dans $\mathbb{Z}[X]$

Tout d'abord, admettons le résultat suivant :

Lemme 4. *Si P est réductible dans $\mathbb{Q}[X]$, alors il l'est dans $\mathbb{Z}[X]$ au sens où il existe A et B dans $\mathbb{Z}[X]$ non constants tels que $P = AB$.*[2]

Si l'on dispose de ce résultat, alors la preuve du critère d'Eisenstein peut se faire par l'absurde. Supposons par l'absurde que P soit réductible dans $\mathbb{Q}[X]$. On a alors $P = AB$ avec A et B non constants et à coefficients entiers. On effectue alors une réduction modulo p en notant $1 < k < n$ le degré de A et $1 < l < n$ celui de B. On a $\overline{P} = \overline{c_n} X^n$ d'une part et $\overline{P} = \overline{AB}$ d'autre part. En particulier $\overline{a_k b_l} = \overline{c_n}$ et donc les coefficients dominants de A et B sont non nuls dans $\mathbb{Z}/p\mathbb{Z}$. Alors, par unicité de la décomposition en facteurs irréductibles du polynôme P dans l'anneau factoriel $\mathbb{F}_p[X]$, $\overline{A} = \overline{a_k} X^k$ et $\overline{P} = \overline{b_l} X^l$.
En particulier en regardant le coefficient constant, $\overline{a_0}$ et $\overline{b_0}$ sont nuls dans $\mathbb{Z}/p\mathbb{Z}$ et donc p^2 divise c_0, ce qui contredit l'une des hypothèses de l'énoncé. Le résultat est donc démontré.

Etape 2 : Preuve de la réductibilité dans $\mathbb{Z}[X]$

Montrons le lemme précédemment admis. Puisque P est réductible dans $\mathbb{Q}[X]$, on a $P = QR$ avec $Q, R \in \mathbb{Q}[X]$ non constants. Notons $\alpha = c(P)$ et $\tilde{P} := P/\alpha$. On a $\tilde{P}$ réductible dans $\mathbb{Q}[X]$: il existe $\tilde{Q}$ et $\tilde{R}$ non constants dans $\mathbb{Q}[X]$ tels que $\tilde{P} = \tilde{Q}\tilde{R}$. Notons alors β (resp. γ) le produit des dénominateurs des coefficients de $\tilde{Q}$ (resp. $\tilde{R}$). Les polynômes $B := \beta\tilde{Q}$ et $C := \gamma\tilde{R}$ sont à coefficients entiers et donc

1. On prendra garde à garder en tête que les p sont les représentants des éléments irréductibles de l'anneau A quotienté par la relation d'équivalence "association" (différer multiplicativement d'un inversible).
2. Les inversibles de $A[X]$ avec A intègre sont inclus dans les constantes (ce sont en fait les éléments de $A^\times$).

$\beta\gamma\tilde{P} = BC \in \mathbb{Z}[X]$. En particulier en passant au contenu on a, puisque $\tilde{P}$ est primitif, $\beta\gamma = c(B)c(C)$. Donc

$$P = \alpha\tilde{P} = \alpha\left(\frac{1}{\beta}B\frac{1}{\gamma}C\right) = \left(\frac{\alpha}{c(B)}B\frac{1}{c(C)}C\right)$$

et donc P est bien produit de deux polynômes à coefficients entiers non constants. □

Remarque 5. *Il ne faut pas hésiter à en faire des caisses, car le développement est assez court. On peut par exemple*

- *Insister sur l'existence du contenu en rappelant que $\mathbb{Z}[X]$ est un anneau factoriel est donc que le PGCD est bien défini, au signe près ici vu la tête des inversibles.*
- *Aller jeter un oeil sur la page wikipédia anglaise du critère d'Eisenstein qui propose un exemple intéressant faisant le lien avec les polynomes cyclotomiques.*

Références

[XENSAl1] Francinou, Gianella, Nicolas, Oraux X-ENS, Algèbre 1