Critère d'Eisenstein

Mohamed NASSIRI

Références :

Théorie de Galois : Niveau L3-M1, Ivan Gozard - p.10 → 12

Recasage :

• • • • • 122 : Anneaux principaux. Applications.
• • • • • 125 : Extensions de corps. Exemples et applications.
• • • • • 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Résumé :

En considérant un anneau factoriel A, le critère d'Eisenstein est un critère très simple et très pratique pour montrer l'irréductibilité dans $K[X] = \mathrm{Frac}A[X]$ (même dans $A[X]$ en fonction du contenu) d'un polynôme à coefficient dans A.

Prérequis :

Anneau factoriel - Anneau quotient - Eléments irréductibles et premiers - Artihmétique et irréductibilité des polynômes

---

Théorème : Soient A un anneau factoriel, $K = \mathrm{Frac}A$ son corps des fractions et
$P = a_nX^n + ... + a_1X + a_0 \in A[X]$
(i) P est irréductible dans $A[X]$ si et seulement si P irréductible dans $K[X]$ et $c(P) = 1$.
(ii) Soit p un élément irréductible de A tel que

$$(i)\ p \nmid a_n \quad , \quad (ii)\ p \mid a_0, ..., a_{n-1} \quad , \text{et} \quad (iii)\ p^2 \nmid a_0$$

Alors P est irréductible dans $K[X]$

Démonstration.

(i)

Rappel : Soit A un anneau factoriel. Pour tout polynôme non nul $P \in A[X]$, on appelle *contenu* de P et on note $c(P)$, le pgcd des coefficients de P.
P est dit *primitif* si et seulement si $c(P) = 1$.

$\underline{\Rightarrow :}$ Supposons P est irréductible dans $A[X]$.
Comme $c(P)$ divise P dans $A[X]$, alors $c(P) \in A^*$, et donc $c(P) = 1$ (le pgcd est défini à un inversible près).
Supposons $P = QR$ avec $Q, R \in K[X]$ de degré supérieur ou égal à 1. Soit a un multiple commun à tous les dénominateurs des coefficients non nuls de Q et R. Alors, on a

$$a^2P = (aQ)(aR) = UV \qquad (\dagger)$$

où $U = aQ \in A[X]$ et $V = aR \in A[X]$. Avec (†), on obtient, d'une part

$$a^2 c(P) = c(a^2 P) = c(UV) = c(U)c(V) \qquad (\sharp)$$

En notant $U = c(U)U_1$ et $V = c(V)V_1$ avec $U_1, V_1 \in A[X]$ et $c(U_1) = c(V_1) = 1$, avec (†), on obtient, d'autre part

$$a^2 P = c(U)c(V)U_1 V_1 \qquad (\sharp\sharp)$$

Les relations ($\sharp$) et ($\sharp\sharp$) nous donnent

$$a^2 P = a^2 c(P)U_1 V_1 \underset{a \in A^*}{\Leftrightarrow} P = c(P)U_1 V_1$$

Cette dernière égalité est absurde puisque $c(P)U_1$ et V_1 sont des éléments de $A[X]$ de degré supérieur ou égal à 1. Ainsi, P est irréductible dans $K[X]$.

$\underline{\Leftarrow :}$ Supposons P irréductible dans $K[X]$ et primitif.
Si $P = QR$ avec $Q, R \in A[X]$, donc en particulier dans $K[X]$, alors $Q \in K^*$ ou $R \in K^*$. Sans perte de généralités, supposons $Q \in K^*$. Donc $Q \in A^*$, et ainsi $Q \mid c(P)$. Or comme P est primitif, on a $Q \in A^*$, et ainsi P est irréductible dans $A[X]$.

(ii) Soit l'anneau-quotient $B = A/pA$.
Raisonnons par l'absurde, et supposons que $P = UV$ avec $U, V \in K[X]$ de degré supérieur ou égal à 1. Par ce qui précède ($(i) \Rightarrow$), on a $P = RS$ $R, S \in A[X]$ de degré supérieur ou égal à 1, où on peut écrire

$$R(X) = \sum_{i=0}^{r} b_i X^i, \quad S(X) = \sum_{j=0}^{s} c_j X^j, \qquad \text{avec } b_r c_s = a_n \neq 0,\ r \geq 1,\ \text{et } s \geq 1$$

et puisque $r + s = n$, $r \leq n-1$ et $s \leq n-1$. Soit ψ la surjection canonique de A sur B que l'on prolonge de façon naturelle de la façon suivante :

$$\begin{array}{ll} \psi : A \to B & \widehat{\psi} : A[X] \to B[X] \\ a \mapsto \psi(a) & \sum \lambda_k X^k \mapsto \sum \psi(\lambda_k) X^k \end{array}$$

$\widehat{\psi}$ est manifestement un morphisme d'anneaux. On a

$$\widehat{\psi}(P(X)) = \widehat{\psi}(R(X))\widehat{\psi}(S(X)) = \sum_{i=0}^{r} \psi(b_i) X^i \sum_{j=0}^{s} \psi(c_j) X^j$$

Comme $\psi(a_k) = 0$ pour $0 \leq k \leq n-1$, on a

$$\widehat{\psi}(P(X)) = \psi(a_n) X^n$$

En considérant le terme de degré 0, on montre que

$$\psi(b_0)\psi(c_0) = 0$$

Comme p est irréductible, et A est factoriel, l'anneau-quotient $B = A/pA$ est intègre, donc $B[X]$ est intègre. Donc $\psi(b_0) = 0$ ou $\psi(c_0) = 0$, mais on n'a pas $\psi(b_0) = \psi(c_0) = 0$, sinon b_0 et c_0 seraient divisibles par p et donc $a_0 = b_0 c_0$ serait divisible par p. Ce qui est exclu.
Sans perte de généralités, supposons $\psi(b_0) = 0$ ou $\psi(c_0) \neq 0$. Si tous les $\psi(b_i)$ étaient nuls, on aurait en particulier $\psi(b_r) = 0$, et donc $\psi(a_n) = \psi(b_r)\psi(c_s) = 0$. Ce qui est exclu.
D'où l'existence d'un unique entier $i \in [\![0, r-1]\!]$ tel que $\psi(b_0) = ... = \psi(b_i) = 0$ et $\psi(b_{i+1}) \neq 0$. On a donc

$$\psi(a_{i+1}) = \sum \psi(b_k)\psi(c_{i+1-k}) = \underbrace{\psi(b_{i+1})}_{\neq 0}\underbrace{\psi(c_0)}_{\neq 0}$$

On a donc $\psi(a_{i+1}) \neq 0$, ce qui est absurde puisque $\psi(a_{i+1}) = 0$ pour $i + 1 \leq r \leq n-1$ □

Remarques :

- **Eléments irréductibles et premiers**
- **Lemme de Gauss**

> **Lemme de Gauss :** Soit A un anneau factoriel.
> (i) Le produit de deux polynômes primitifs est primitif.
> (ii) $\forall (P,Q) \in (A[X]\backslash\{0\})^2,\ c(PQ) = c(P)c(Q)$.

Démonstration :
(i) Soit P, Q non nuls dans $A[X]$ avec $c(P) = c(Q) = 1$. Supposons que $c(PQ) \neq 1$. Alors il existe un élément irréductible $p \in A$ tel que p divise tous les coefficients de PQ. Comme p et irréductible et A est factoriel, alors l'anneau $B = A/pA$ est intèbre, et donc l'anneau $B[X]$ est intègre.
Soit ψ la surjection canonique de A sur B que l'on prolonge de façon naturelle de la façon suivante :

$$\begin{aligned} \psi : A &\to B & \qquad \widehat{\psi} : A[X] &\to B[X] \\ a &\mapsto \psi(a) & \sum \lambda_k X^k &\mapsto \sum \psi(\lambda_k) X^k \end{aligned}$$

$\widehat{\psi}$ est manifestement un morphisme d'anneaux. On a

$$0 = \widehat{\psi}(PQ) = \widehat{\psi}(P)\widehat{\psi}(Q) \quad \Rightarrow \quad \widehat{\psi}(P) = 0 \text{ ou } \widehat{\psi}(Q) = 0$$

Mais ceci contredit le fait que $c(P) = c(Q) = 1$.

(ii) On peut écrire $P = c(P)R$ et $Q = c(Q)S$ où $R, S \in A[X]$ avec $c(R) = c(S) = 1$. Par suite, $PQ = c(P)c(Q)RS$ avec, par ce qui précède, $c(RS) = 1$. Donc, on obtient $c(PQ) = c(P)c(Q)$.

□

- **Irréductibilité de $\Phi_{p,\mathbb{Q}}$:**
Grâce au critère d'Eisenstein, on peut montrer que, pour tout p premier, le polynôme $\Phi_{p,\mathbb{Q}}(X) = \sum_{i=0}^{p-1} X^i$ est irréductible dans $\mathbb{Z}[X]$. En effet, posons le polynôme

$$P(X) = \Phi_{p,\mathbb{Q}}(X+1) = \sum_{i=0}^{p-1} (X+1)^i$$

On a donc

$$\begin{aligned} P(X) = \frac{1-(X+1)^p}{1-(X+1)} &= \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + \binom{p}{p-1} X^{p-2} + ... + \binom{p}{2} X + \binom{p}{1} \in \mathbb{Z}[X] \\ &:= a_p X^{p-1} + a_{p-1} X^{p-2} + ... + a_1 X + a_0 \end{aligned}$$

Pour montrer que P est irréductible, on va utiliser le critère d'Eisenstein avec le nombre premier p. On a bien $p \nmid a_p = 1$ et que $p^2 \nmid a_0 = \binom{p}{1} = p$. Il reste donc à vérifier que $p \mid a_0, ..., a_{p-1}$ $(i.e.)$ $p \mid \binom{p}{k}$ pour tout $1 \leq k \leq p-1$.
Or, pour tout $1 \leq k \leq p-1$, on a

$$k! \binom{p}{k} = p(p-1)...(p-k+1)$$

Donc $p \mid k!\binom{p}{k}$, mais comme $k < p$, p est premier avec $k!$ et donc $p \mid \binom{p}{k}$.
Ainsi par le critère d'Eisenstein, P est irréductible dans $\mathbb{Q}[X]$, et dans $\mathbb{Z}[X]$ car il est unitaire.

Revenons à $\Phi_{p,\mathbb{Q}}$! Supposons, par l'absurde, que $\Phi_{p,\mathbb{Q}}$ soit composé. Il existe donc deux polynômes $U, V \in \mathbb{Q}[X]$ tels que

$$\Phi_{p,\mathbb{Q}}(X) = U(X)V(X)$$

vérifiant $\deg U < \Phi_{p,\mathbb{Q}}$ et $\deg V < \Phi_{p,\mathbb{Q}}$. Mais alors,

$$P(X) = \Phi_{p,\mathbb{Q}}(X+1) = U(X+1)V(X+1)$$

Comme $\deg U(X+1) = \deg U < \Phi_{p,\mathbb{Q}}$ et $\deg V(X+1) = \deg V < \Phi_{p,\mathbb{Q}}$. On en déduit donc que P n'est pas irréductible. Contradiction !

Par conséquent, $\Phi_{p,\mathbb{Q}}$ est irréductible dans $\mathbb{Q}[X]$, et dans $\mathbb{Z}[X]$ car il est unitaire.

- **Critère d'irréductibilité modulo un idéal premier :**

Théorème : Soient A un anneau factoriel, $K = \mathrm{Frac}(A)$ son corps des fractions et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ de degré $n \geq 1$.
Soient I un idéal premier de A, $B = A/I$ l'anneau quotient (qui est donc intègre) et $L = \mathrm{Frac}(B)$ le corps des fractions de B. On suppose que $a_n \notin I$.
Si le réduit $\overline{P}$ de P modulo I est irréductible dans $L[X]$, alors P est irréductible dans $K[X]$.

Démonstration :

□

Application : Avec $A = \mathbb{Z}$, $I = (p)$ où p est un nombre premier, alors $K = \mathbb{Q}$ et $B = \mathbb{F}_p = L$, on a, par exemple, que $P(X) = X^3 - 127X^2 + 3608X + 19$ est irréductible dans $\mathbb{Z}[X]$ ($p = 2$).

- **Deux critères d'irréductibilité avec les extensions de corps :**

Théorème :
Critère 1 : Soit $P \in K[X]$ un polynôme de degré $n \geq 1$. $P(X)$ est irréductible dans $K[X]$ si et seulement si $P(X)$ n'a pas de racine dans les extensions L de K telles que $[L : K] \leq n/2$.
Critère 2 : Soient $P \in K[X]$ un polynôme irréductible de degré $n \geq 1$ et L une extension de degré m de K avec $\mathrm{pgcd}(m, n) = 1$. Alors $P(X)$ est irréductible dans $L[X]$.

Démonstration :

□

Application - *Critère 1* : $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$ car il n'a pas de racines dans $\mathbb{F}_2$, ni $\mathbb{F}_4$.
Application - *Critère 2* : $X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$.

- **Une preuve dans $\mathbb{Z}$:**
Cette preuve dans $\mathbb{Z}$ adaptée de *Algèbre 1 Oraux X-ENS, Serge Francinou, Hervé Gianella et Serge Nicolas (p.188 → 190)* n'est là que pour avoir un feeling de ce que l'on fait dans le cas général car dans $\mathbb{Z}$, on manipule de "vrais nombres".

Théorème : Soit $P = a_n X^n + ... + a_1 X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que :

$$(i)\ p \nmid a_n \quad , \quad (ii)\ p \mid a_0, ..., a_{n-1} \quad \text{,et} \quad (iii)\ p^2 \nmid a_0$$

Alors P est irréductible dans $\mathbb{Q}[X]$.

Démonstration :
Etape 1 - Montrons que le produit de deux polynômes primitifs est primitif et $c(AB) = c(A)c(B)$:

- Soit $A = \sum_{k=0}^{n} a_k X^k$, $B = \sum_{k=0}^{m} b_k X^k$, et $C = \sum_{k=0}^{n+m} c_k X^k = AB$
Supposons A et B primitif, et que C ne le soit pas. Il existe donc un nombre premier p qui divise tous les c_k.
Ainsi $\overline{C} = 0$ dans $\mathbb{Z}/p\mathbb{Z}$[X] et donc $\overline{AB} = \overline{AB} = \overline{C} = 0$. Mais $\mathbb{Z}/p\mathbb{Z}$[X] est intègre, donc $\overline{A} = 0$ ou $\overline{B} = 0$ $(i.e)$ p qui divise tous les a_k ou p qui divise tous les b_k. Ce qui est absurde car A et B sont primitifs ...
- $AB = c(A)c(B)\frac{A}{c(A)}\frac{B}{c(B)}$. Or $\frac{A}{c(A)}$ et $\frac{B}{c(B)}$ sont primitifs, donc leur produit aussi d'après ce qui précède.
En passant au contenu dans la première égalité, on a $c(AB) = c(A)c(B)$.

Etape 2 - Montrons que si A n'est pas irréductible dans $\mathbb{Q}$[X] alors $A = BC$, B, $C \in \mathbb{Z}$[X] avec $\deg B, \deg C < \deg A$:

Soit $\alpha = c(A)$, $A' = \frac{1}{\alpha}A \in \mathbb{Z}$[X] et est primitif. A est composé donc A' aussi. On a donc $A' = B'C'$ avec B' et $C' \in \mathbb{Q}$[X] vérifiant $\deg B', \deg C' < \deg A' = \deg A$.
Soit β et γ le produit des dénominateurs des coefficients de B' et C'. Alors $B = \beta B'$ et $C = \gamma C' \in \mathbb{Z}$[X] et on a $\beta\gamma A' = BC$.
En passant au contenu, on a $\beta\gamma = c(B)c(C)$. Par conséquent :

$$A = \alpha A' = \alpha B'C' = \alpha\left(\frac{1}{\beta}B\right)\left(\frac{1}{\gamma}C\right) = \alpha\left(\frac{1}{c(B)}B\right)\left(\frac{1}{c(C)}C\right) = \underbrace{\left(\frac{\alpha}{c(B)}B\right)}_{\in\mathbb{Z}[X]}\underbrace{\left(\frac{1}{c(C)}C\right)}_{\in\mathbb{Z}[X]}$$

Etape 3 - Montrons le critère d'Eisenstein à proprement parler :

Supposons par l'absurde que A soit non irréductible. Par ce qui précède, il existe $B, C \in \mathbb{Z}$[X], de degré inférieur strictement à n, tels que $A = BC$.
Ecrivons $B = b_k X^k + ... + b_1 X + b_0$ et $C = c_l X^l + ... + c_1 X + c_0$.
On a donc $\overline{a_n}X^n = \overline{BC}$ et $a_n = b_k c_l$ n'étant pas divisible par p, on a $\overline{b_k} \neq 0$ et $\overline{c_l} \neq 0$.
Par unicité de la décomposition en irréductible dans $\mathbb{Z}/p\mathbb{Z}$[X], on a $\overline{B} = \overline{b_k}X^k$ et $\overline{C} = \overline{c_l}X^l$.
On a alors $\overline{b_0} = \overline{c_0} = 0$ $(i.e.)$ $p \mid b_0$ et $p \mid c_0$ donc $p^2 \mid a_0 = b_0 c_0$. Absurde.

□