

Dev n° 11

Ref: Rombaldi p 383-385
 Site: "Pierre Laisel"

Titre: Critère Eisenstein

On prend A factoriel et K le corps de fraction de A .

Le but du dev. va être de démontrer le thm suivant:

Thm:

Soit $P(x) = \sum_{k=0}^n a_k x^k$ un polynôme non constant dans $A[x]$ de $\deg \geq 2$.

Si $\exists p$ t.q.:

- $p \mid a_0, \dots, a_{n-1}$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Alors, P est irréductible dans $K[x]$.

Par cela on a besoin de montrer le lemme de Gauss:

Lemme: (de Gauss)

Soit $P, Q \in A[x] \setminus \{0\}$.

On a $c(PQ) = c(P)c(Q)$

Lemme:

$P \in A[x]$ irréductible $\Rightarrow$ irréductible sur $K[x]$.

Démon: (Gauss)

• Cas primitif:

Soit $P, Q \in A[x]$ t.q. $c(P) = c(Q) = 1$.

Par l'absurde, s.g. $c(PQ) \neq 1$.

Alors, $\exists p \in A$ premier t.q. divise chaque coefficient de PQ dans $A[x]$.

Mais, comme p premier dans A , l'idéal (p) est premier dans

$A[x]$ et donc $\frac{A[x]}{(p)}$ est intègre et on a:

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

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

• Dans le cadre générale:

On écrit $P = c(P)\tilde{P}$ et $Q = c(Q)\tilde{Q}$ avec $c(\tilde{P}) = c(\tilde{Q}) = 1$.

On a:

$$\begin{aligned} c(PQ) &= c(c(P)\tilde{P}c(Q)\tilde{Q}) \\ &= c(P)\underbrace{c(\tilde{P})}_{=1}c(Q)\underbrace{c(\tilde{Q})}_{=1} = c(P)c(Q). \end{aligned}$$

□

Démon: (Lemme)

P.q. P irréductible sur $A[x] \Rightarrow P$ irréductible sur $K[x]$.

Par contraposé, s.g. $P \in A[x]$ soit réductible dans $K[x]$.

Notons $P = c(P)\tilde{P}$ avec $\tilde{P}$ primitif dans $A[x]$

Comme P réductible dans $K[x]$ on a de même pour $\tilde{P}$:

$\tilde{P} = \tilde{Q}\tilde{R}$ avec $\tilde{Q}, \tilde{R} \in K[x]$, $\deg \tilde{Q}, \deg \tilde{R} < \deg(\tilde{P})$ et non constant.

Notons $r\tilde{Q} = R$ et $q\tilde{R} = Q$ de sorte que Q et $R \in A[x]$.

On a: $RQ = r q \tilde{R} \tilde{Q} = r q \tilde{P}$

Donc, $qr = c(Q)c(R) = 1/c(P)$

Ainsi, on a:

$$P = c(P)\tilde{P} = c(P)\frac{QR}{qr} = c(P)\frac{QR}{c(Q)c(R)} = QR.$$

Et, donc P est réductible dans $A[x]$ □

$$P = c(r) \cdot r = c(r) \cdot \frac{r^n}{q \cdot r} = c(r) \cdot \frac{r^{n-1}}{c(0) \cdot c(r)} = \dots$$

Et, donc P est réductible dans $\mathbb{A}[X] \square$

Démonstration (thm)

Soit $P \in \mathbb{A}[X]$ vérifiant les h. du thm et $P(x) = \sum_{k=0}^n a_k x^k$
Il suffit de m.g. P irréductible dans $\mathbb{A}[X]$ puis utiliser le lemme.

Par l'absurde, s.g. P réductible dans $\mathbb{A}[X]$.

Alors, $\exists Q = \sum_{i=0}^k q_i x^i$ et $R = \sum_{j=0}^p r_j x^j$ dans $\mathbb{A}[X]$ avec $k, p < n$, et t.q. $P = QR$.

Par hypothèse, en réduisant mod p , on a: $\overline{a_n} x^n = \overline{Q} \overline{R}$

Or, $a_n = q_k r_p$.

Donc, $\deg \overline{Q} = k$ et $\deg \overline{R} = p$.

De même, $\mathbb{A}/(p)[X]$ est intègre.

$\overline{Q}$ et $\overline{R}$ monômes sinon il y aurait un des coefficients $\neq \overline{0}$ de $\overline{P}$ de degré $< n$, ce qui contredit $p \nmid a_0, \dots, a_{n-1}$.

Donc, $\overline{q_0} = \overline{r_0} = \overline{0} \Rightarrow p \mid r_0$ et $p \mid q_0 \Rightarrow a_0 = r_0 q_0$ donc $p^2 \mid a_0 \Rightarrow$
Absurde.

Donc, P irréductible sur $\mathbb{A}[X]$ et donc $\mathbb{K}[X] \square$

Annexe:

• Application:

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 $\phi_p(X) = \sum_{i=0}^{p-1} X^i = X^{p-1} + \dots + X + 1$ le p -ième polynôme cyclotomique. 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 $X^2 \nmid X(X-1)(X-\lambda)$.

• réciproque lemme 2.

Si P irr. + primitif dans $\mathbb{K}[X]$ alors P irr. sur $\mathbb{A}[X]$.

• Ex. pol. irr. dans $\mathbb{K}[X]$ mais pas dans $\mathbb{A}[X]$:

$2(x^4 - 9x - 3)$ irréductible dans $\mathbb{Q}[x]$ par Eisenstein ($p=3$) mais se factorise non trivialement dans $\mathbb{Z}[x]$.

Ici $\mathbb{A}[X] = \mathbb{Z}[X]$ et $\mathbb{K}[X] = \text{Frac } \mathbb{A}[X]$.

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 $c(P) = 1$.

• Détails pourquoi $\overline{R}$ et $\overline{Q}$ sont des monômes:

$$Q = \sum_{i=0}^k q_i x^i \quad R = \sum_{j=0}^p r_j x^j$$

On note :

$$i_0 = \min \{ 0 \leq i \leq k \mid \overline{q_i} \neq \overline{0} \} \quad \text{dans } \mathbb{A}/(p).$$

$$j_0 = \min \{ 0 \leq j \leq p \mid \overline{r_j} \neq \overline{0} \}$$

On note :

$$i_0 = \min \{ 0 \leq i \leq k \mid \overline{q_i} \neq \overline{0} \} \quad \text{dans } A/(p).$$

$$j_0 = \min \{ 0 \leq j \leq p \mid \overline{r_j} \neq \overline{0} \}$$

Par l'ABSURDE on s.q. $i_0 + j_0 < n$.

Dans $R(x) \cong \mathbb{Q}(x) = X^{i_0+j_0} \overline{q_{i_0}} \overline{r_{j_0}} + \dots + X^0 \overline{q_k} \overline{r_p}$

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

Par unicité de la décomposition dans $A/(p)[x]$ on a

$$\overline{q_{i_0}} \overline{r_{j_0}} = \overline{0} \Rightarrow \overline{q_{i_0}} = \overline{0} \text{ ou } \overline{r_{j_0}} = \overline{0} \text{ par intégrité}$$

Cela contredit la déf de i_0 ou j_0 .

• Dans un anneau A , si a et b sont deux éléments non nuls de A , on dit que :

- d est un PGCD (plus grand commun diviseur) de a et b si les diviseurs communs à a et b sont les diviseurs de d ;
- m est un PPCM (plus petit commun multiple) de a et b si les multiples communs à a et b sont les multiples de m .

• Un idéal propre I de A est premier si et seulement si

$$\forall a, b \in A \quad [ab \in I \Rightarrow (a \in I \text{ ou } b \in I)].$$

• Dans un anneau commutatif, un élément p est dit **premier** s'il n'est ni nul ni inversible et si, pour tout produit ab divisible par p , l'un des deux facteurs a ou b est divisible par p .

• Question celle.

Il q. RM $x^{101} + 101x^{100} + 101$ est irréductible dans $\mathbb{Z}[x]$.

Méthode calculer $R(x-1)$.

$$\begin{aligned} \text{On a } R(x-1) &= (x-1)^{101} + 101(x-1)^{100} + 101 \\ &= x^{101} + 101x^{100} + \sum_{k=1}^{100} \binom{101}{k} x^k (-1)^{101-k} - 1 + 101x^{100} + 101 \sum_{i=1}^{99} \binom{100}{i} x^i (-1)^{100-i} + 101 \\ &= x^{101} + 101x^{100} + \sum_{k=1}^{100} \left(\binom{101}{k} x^k + \binom{100}{k} x^k \right) + 101 \end{aligned}$$

On a tout les coeff. $a_{101}, \dots, a_0$ divisible par 101 et $101^2 \mid 101 = a_0$.
Par Eisenstein on a $R(x)$ est irréductible sur $\mathbb{Q}[x]$.

• (p) premier $\Leftrightarrow A/(p)$ intègre:

$$\begin{aligned} \Rightarrow \text{Soit } a, b \in A \text{ t.q. } a \cdot b \in I &\Rightarrow \overline{a \cdot b} = \overline{0} \\ &\Rightarrow \overline{a} \cdot \overline{b} = \overline{0} \\ &\Rightarrow \overline{a} = \overline{0} \text{ ou } \overline{b} = \overline{0} \text{ comme } A/(p) \text{ intègre} \\ &\Rightarrow a \in (p) \text{ ou } b \in (p) \\ &\text{Donc } (p) \text{ premier.} \end{aligned}$$

$\Rightarrow$ S.q. (p) premier donc $\forall c \in (p), c = ap$ avec $a \in A$.

$$\begin{aligned} \text{Soit } \overline{a}, \overline{b} \in A/(p) : \overline{a} \cdot \overline{b} = \overline{0} &\Leftrightarrow \overline{ab} = \overline{0} \\ &\Leftrightarrow ab = 0 \\ &\Leftrightarrow ab - 0 \in (p) \quad (p) \text{ premier} \\ &\Rightarrow a \in (p) \text{ ou } b \in (p) \\ &\Rightarrow \overline{a} = \overline{0} \text{ ou } \overline{b} = \overline{0} \text{ dans } A/(p) \\ &\quad (\text{déf de } A/(p) \text{ intègre}) \end{aligned}$$

Démo: (Lemme)

Il y a P irré. sur $A[X] \Rightarrow$ irré. sur $K[X]$.

Par contraposé, s.g. P reduc. dans $K[X]$.

Notons, $c(P)\tilde{P} = P$ avec $c(\tilde{P}) = 1$.

Comme P reduc. on a aussi $\tilde{P}$ sur $K[X]$:

$$\tilde{P} = \tilde{Q}\tilde{R} \text{ avec } \tilde{Q} \text{ et } \tilde{R} \in K[X] \text{ et } 1 \leq \deg \tilde{Q} \leq \deg \tilde{R} < \deg P.$$

$$\text{Notons } R = r\tilde{R} \text{ et } Q = q\tilde{Q} \text{ avec } Q, R \in A[X]$$

$$\text{Alors, } QR = r q \tilde{P}.$$

$$\text{Donc, } qr = c(Q)c(R)$$

$$\text{Ainsi, } P = c(P)\tilde{P} = Q \cdot R.$$

□

Critère Eisenstein

11

A factoriel et K corps de fraction de A .

Thm:

$$P(X) = \sum_{i=0}^n a_i X^i \in A[X] \text{ avec } n \geq 2.$$

$$\text{Si } \exists p \text{ t.q. : } \begin{aligned} &- p \mid a_0, \dots, a_{n-1} \\ &- p \nmid a_n \\ &- p^2 \nmid a_0 \end{aligned}$$

Alors, P est irréductible dans $K[X]$.

Lemme: (Gauss)

$$P, Q \in A[X] \setminus \{0\}, \text{ Alors, } c(PQ) = c(P)c(Q)$$

Lemme:

$$P \in A[X] \text{ irré} \Rightarrow \text{irré sur } K[X]$$

Démo: (Gauss)

Soit $P, Q \in A[X]$ t.q. $c(P) = c(Q) = 1$.

Par l'absurde, s.g. $c(PQ) \neq 1$.

Alors, $\exists p \in A$ premier t.q. p divise tout les coef. de PQ dans $A[X]$

Mais comme p premier dans A , (p) est premier dans $A[X]$ et donc $\frac{A[X]}{(p)}$ est intègre et on a que

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

Soit $P = c(P)\tilde{P}$ et $Q = c(Q)\tilde{Q}$ avec $\tilde{P}$ et $\tilde{Q}$ primitif.

$$\text{On a que } c(PQ) = c(c(P)\tilde{P} c(Q)\tilde{Q}) = c(P)c(Q)c(\tilde{P})c(\tilde{Q}) = c(P)c(Q)$$

□

Démo: (thm)

Soit $P \in A[X]$ vérifiant les hyp. du thm.

Il suffit de m.q. P irré. dans $A[X]$.

Par l'absurde, s.g. P reduc. dans $A[X]$.

$$\text{Alors, } \exists Q = \sum_{i=0}^k q_i X^i \text{ et } R = \sum_{j=0}^p r_j X^j \in A[X] \text{ de } \deg < \deg P$$

$$\text{t.q. } P = QR.$$

$$\text{Par hyp on a } \overline{a_n} X^n = \overline{Q}\overline{R} \pmod{p}$$

$$\text{Or, } a_n = q_k r_p.$$

$$\text{Donc, } \deg \tilde{Q} = k \text{ et } \deg \tilde{R} = p.$$

De même, $A_{(p)}[X]$ est intègre.

$\tilde{Q}$ et $\tilde{R}$ monômes sinon il y aurait des coef $\neq 0$ de $\deg < n$.

$$\text{Donc, } \overline{q_0} = \overline{r_0} = \overline{0} \Rightarrow p \mid q_0 \text{ et } p \mid r_0 \Rightarrow a_0 = r_0 q_0 \text{ donc } p^2 \mid a_0$$

□