

121
122
~~123~~
141
142

Critère
d'Eisenstein

- Algèbre, Gourdon, p 62
- Algèbre, Perrin, p 57 et 76
- Théorie de Galois, Gorenstein, p 10

An lieu de prendre $\mathbb{Z}$, on prend A un anneau factoriel et $K = \text{Frac}(A)$ son corps des fractions (qui existe car A est intègre).

PER

Def 1: Soit $P \in A[x]$. On appelle contenu de P , noté $c(P)$, un PGCD de ses coefficients.
Si $c(P) = 1$, on dit que P est primitif.

en +

Remarque:

- Le contenu est défini à un inversible près.
- Soit $P \in A[x]$. Alors $P = c(P) P_1$ où P_1 est un poly primitif de $A[x]$.
- Tout poly unitaire est primitif.

602

10

Lemme 2: Soit $P, Q \in A[x]$. Alors
 $c(PQ) = c(P) \cdot c(Q)$

Dém: On suppose d'abord que P et Q sont primitifs, c'est-à-dire $c(P) = c(Q) = 1$. On veut que $c(PQ) = 1$.

Par l'absurde, si $c(PQ) \neq 1$. Alors, il existe $p \in A$ irréductible qui divise tous les coeffs de PQ dans A . Or $A/(p)$ est intègre et donc $A/(p)[x]$ est intègre.

Alors: $\overline{PQ} = \overline{P} \cdot \overline{Q} = \overline{0}$, ce qui implique $\overline{P} = \overline{0}$ ou $\overline{Q} = \overline{0}$.

Cela contredit le fait que $c(P) = c(Q) = 1$, car sinon on aurait que p divise tous les coeffs de P ou de Q .

Dans le cas général, on écrit $P = c(P) P_1$ et $Q = c(Q) Q_1$ avec $P_1, Q_1 \in A[x]$.

$A/(p)$ pas un corps car A factoriel donc (p) est premier mais pas maximal

tel que $c(P_1) = c(Q_1) = 1$

$$\begin{aligned} \text{Ainsi : } c(PQ) &= c(c(P) \cdot P_1 \cdot c(Q) \cdot Q_1) \\ &= c(P) \cdot c(Q) \cdot c(P_1 Q_1) \\ &= c(P) \cdot c(Q) \end{aligned}$$

□

600

62

Lemme 3 : Si ϕ ^{est de degré ≥ 1 et} est irréductible dans $A[x]$, il est irréductible dans $K[x]$ et primitif

$\frac{\phi}{c(\phi)}$ non inversible
dans $A[x]$ car
de deg ≥ 1

Dém : On a que ϕ est primitif car sinon on peut le décomposer comme $\phi = c(\phi) \times \frac{\phi}{c(\phi)}$ qui seraient deux éléments non inversibles de $A[x]$.

On montre qu'il est irréductible dans $K[x]$.

On suppose que $\phi = PQ$ avec $P, Q \in K[x]$

Soit d le produit des dénominateurs des coefficients de P ($d \in A^*$). Alors $P_1 = dP \in A[x]$

De même, $\exists \beta \in A^*$ tq $Q_1 = \beta Q \in A[x]$

On a : $d\beta\phi = P_1 Q_1$

En passant aux contenus, d'après le lemme 1,

$$d\beta c(\phi) = d\beta = c(P_1) c(Q_1)$$

Alors :

$$\phi = PQ = \frac{P_1}{d} \frac{Q_1}{\beta} = \frac{P_1}{c(P_1)} \times \frac{Q_1}{c(Q_1)} \quad \text{et ces deux poly sont dans } A[x]$$

On ϕ est irréductible dans $A[x]$, donc l'un des deux facteurs est inversible dans $A[x]$, donc de degré 0. Ainsi P_1 ou Q_1 est de degré 0, donc inversible dans $K[x]$.

Donc ϕ est irréductible dans $K[x]$

PER 76 . Critère d'Eisenstein :

Soit $P(x) = \sum_{i=0}^n a_i x^i \in A[x]$ un poly non constant.

Soit $p \in A$ un élément irréductible. On suppose :

$K_{A/(p)} = \text{comp des fractions de } A/(p)$

1) $p \nmid a_n$

2) $p \mid a_i \quad \forall i \in \llbracket 0; n-1 \rrbracket$

3) $p^2 \nmid a_0$

Alors P est irréductible dans $K[x]$

(et donc aussi dans $A[x]$ si P est primitif).

Dém : Par l'absurde, on suppose P réductible dans $K[x]$. Par le lemme 3, P est réductible dans $A[x]$; il existe $Q(x) = \sum_{i=0}^a q_i x^i$ et $R(x) = \sum_{i=0}^b r_i x^i$ dans $A[x]$, de degré strictement plus petit que $n = \deg(P)$, tq $P = QR$. On regarde alors l'égalité dans $A/(p)[x]$ et d'après les hypothèses, on obtient :

$$\overline{a_n} x^n = \overline{Q} \cdot \overline{R}$$

On a $a_n = q_a r_b$ n'est pas divisible par p et comme $A/(p)[x]$ est intègre, alors $\overline{q_a} \neq \overline{0}$ et $\overline{r_b} \neq \overline{0}$. Comme x est irréductible dans l'anneau principal $K_{A/(p)}[x]$, c'est la décomposition de $\overline{P}$ en produit d'irréductibles dans cet anneau.

Ils sont facteurs irréductibles de $\overline{Q}$ et $\overline{R}$ et donc x , de sorte que $\overline{Q} = \overline{q_a} x^a$ et $\overline{R} = \overline{r_b} x^b$. Alors $\overline{q_i} = \overline{r_i} = \overline{0}$ donc $p \mid q_i$ et $p \mid r_i$, donc $p^2 \mid q_0 r_0 = a_0$. Contradiction.

Donc P est irréductible dans $K[x]$.

Application 1 :

Dans $\mathbb{Z}[x]$, il existe des polynômes irréductibles de tout degré $n \geq 1$.

On prend par exemple $x^n - 2$ pour $n \geq 1$ et on lui applique le critère d'Eisenstein.

Et même irred dans $\mathbb{Z}[x]$ car primitif

Application 2.

Soit p un nbn premier et $\Phi_p(x) = x^{p-1} + \dots + x + 1$ le p -ième poly cyclotomique. Alors Φ_p est irréductible dans $\mathbb{Q}[x]$.

En effet, on regarde $\Phi_p(x+1)$

$$\text{On a que } (x+1)^p \Phi_p(x) = x^p - 1$$

$$\text{donc } \Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{h=1}^p \binom{p}{h} x^{h-1}$$

On voit alors que :

$$1) \quad p \nmid \binom{p}{1} = 1$$

$$2) \quad \forall h \in [1, p-1], \quad p \nmid \binom{p}{h}$$

$$\text{car } \binom{p}{h} = \frac{p!}{h!(p-h)!} \quad \text{donc } p! = \binom{p}{h} h! (p-h)!$$

et comme $p > h$ et $p > p-h$, alors $p \nmid \binom{p}{h}$

$$3) \quad p^2 \nmid \binom{p}{1} = p$$

Donc $\Phi_p(x+1)$ est irréductible sur $\mathbb{Q}[x]$

Pour passer à $\Phi_p(x)$, on suppose que $\Phi_p(x) = p(x)q(x)$ et alors $\Phi_p(x+1) = p(x+1)q(x+1)$ est réductible.

Donc $\Phi_p(x)$ est irréductible sur $\mathbb{Q}[x]$.

Remarques :

1) On a le résultat général :

Soit A un anneau factoriel et K son corps des fractions.

Les éléments irréductibles de $A[x]$ sont :

- les éléments irréductibles de A .
- les poly de degré ≥ 1 qui sont primitifs et irréductibles dans $K[x]$