

# Critère d'Eisenstein

Ici, nous démontrons le célèbre critère d'Eisenstein que l'on utilise énormément en pratique pour montrer qu'un polynôme est irréductible.

Soit  $A$  un anneau commutatif et unitaire.

**Notation 1.** Soit  $P \in A[X]$ . On note  $\gamma(P)$  le contenu du polynôme  $P$ .

**Lemme 2.** Soit  $p \in A$  tel que  $(p)$  est premier. Alors  $A/(p)$  est intègre.

[ULM18]  
p. 32

*Démonstration.* Soient  $\bar{a}, \bar{b} \in A/(p)$ . On suppose  $\bar{a}\bar{b} = 0$ . Comme  $\overline{ab} = \bar{a}\bar{b}$ , on a  $ab \in (p)$ . Donc par hypothèse,

$$\begin{aligned} a \in (p) \text{ ou } b \in (p) \\ \implies \bar{a} = 0 \text{ ou } \bar{b} = 0 \end{aligned}$$

et ainsi  $A/(p)$  est bien intègre. □

**Lemme 3.** Si  $A$  est intègre, alors  $A[X]$  l'est aussi.

p. 22

*Démonstration.* Soient  $P, Q \in A[X]$  non nuls, de degrés respectifs  $n \geq 1$  et  $m \geq 1$  que l'on écrit  $P = \sum_{i=0}^n a_i X^i$  et  $Q = \sum_{j=0}^m b_j X^j$ . Alors, le coefficient de  $X^{n+m}$  dans le produit  $PQ$  est  $a_n b_m$ . Comme  $a_n \neq 0$ ,  $b_m \neq 0$  et  $A$  est intègre, ce coefficient est non nul. Donc en particulier, le produit  $PQ$  est non nul. □

**Lemme 4.** On suppose  $A$  factoriel. Soit  $a \in A$  irréductible. Alors  $(a)$  est premier.

p. 64

*Démonstration.* On suppose que  $a \mid bc$  avec  $b, c \in A$ . Alors, il existe  $d \in A$  tel que

$$ad = bc \tag{*}$$

Si  $b$  est inversible, alors  $a \mid c$ . De même, si  $c$  est inversible, alors  $a \mid b$ . Supposons donc que  $b$  et  $c$  ne sont pas inversibles. Comme  $a$  est irréductible, on en déduit que  $d$  est un élément non nul et non inversible de  $A$ . Il existe donc des décompositions en irréductibles

$$b = \beta_1 \dots \beta_n, c = \gamma_1 \dots \gamma_m \text{ et } d = \delta_1 \dots \delta_k$$

avec  $n, m, k \in \mathbb{N}^*$ . Par conséquent, en injectant dans (\*):

$$a\delta_1 \dots \delta_k = \beta_1 \dots \beta_n \gamma_1 \dots \gamma_m$$

Comme la factorisation en irréductibles est unique à l'ordre près, il existe  $\beta_i$  ou  $\gamma_j$  qui est associé à  $a$ . Si bien que  $a$  divise  $b$  ou  $c$ ; c'est ce que l'on voulait démontrer. □

**Lemme 5** (Gauss). On suppose  $A$  factoriel. Alors :

- (i) Le produit de deux polynômes primitifs est primitif.
- (ii)  $\forall P, Q \in A[X] \setminus \{0\}, \gamma(PQ) = \gamma(P)\gamma(Q)$ .

*Démonstration.* (i) Soient  $P, Q \in A[X]$  tels que  $\gamma(P) = \gamma(Q) = 1$ . Supposons  $\gamma(PQ) \neq 1$ . Alors, il existe  $p \in A$  irréductible tel que  $p$  divise tous les coefficients de  $PQ$ . Donc, dans  $A/(p)$ ,  $\overline{PQ} = \overline{P}\overline{Q} = 0$ .

Mais, par le Lemme 4,  $(p)$  est premier. Donc par le Lemme 2  $A/(p)$  est intègre, et en particulier,  $A/(p)[X]$  l'est aussi par le Lemme 3. Ainsi,  $\overline{P} = 0$  ou  $\overline{Q} = 0$  : absurde.

- (ii) En factorisant, on écrit  $P = \gamma(P)R$  et  $Q = \gamma(Q)S$  où  $R, S \in A[X]$  avec  $\gamma(R) = \gamma(S) = 1$ . D'où  $PQ = \gamma(P)\gamma(Q)RS$  avec  $\gamma(RS) = 1$  par (i). Ainsi,  $\gamma(PQ) = \gamma(P)\gamma(Q)$ . □

**Théorème 6** (Critère d'Eisenstein). Soient  $\mathbb{K}$  le corps des fractions de  $A$  et  $P = \sum_{i=0}^n a_i X^i \in A[X]$  de degré  $n \geq 1$ . On suppose que  $A$  est factoriel et qu'il existe  $p \in A$  irréductible tel que :

- (i)  $p \mid a_i, \forall i \in \llbracket 0, n-1 \rrbracket$ .
- (ii)  $p \nmid a_n$ .
- (iii)  $p^2 \nmid a_0$ .

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

*Démonstration.* Par l'absurde, on suppose  $P = UV$  avec  $U, V \in \mathbb{K}[X]$  de degré supérieur ou égal à 1. Soit  $a$  un multiple commun à tous les dénominateurs des coefficients non nuls de  $U$  et  $V$ . On a

$$a^2 P = \underbrace{aU}_{=U_1 \in A[X]} \underbrace{aV}_{=V_1 \in A[X]}$$

On applique le Lemme 5 pour obtenir :

$$a^2 \gamma(P) = \gamma(U_1) \gamma(V_1) \quad (*)$$

En factorisant, on écrit  $U_1 = \gamma(U_1)U_2$  et  $V_1 = \gamma(V_1)V_2$  avec  $U_2, V_2 \in A[X]$ . Il vient :

$$a^2 P = \gamma(U_1) \gamma(V_1) U_2 V_2 \stackrel{(*)}{=} a^2 \gamma(P) U_2 V_2$$

Et comme  $a \in A \setminus \{0\}$  et que  $A$  est intègre, on a  $P = \gamma(P)U_2V_2$  avec  $U_2, V_2 \in A[X]$  de degré supérieur ou égal à 1.

On pose  $U_2 = \sum_{i=0}^r b_i X^i$  et  $V_2 = \sum_{j=0}^s c_j X^j$  avec  $b_r c_s = a_n \neq 0$  par définition de  $P$ . Dans  $A/(p)$ , on a

$$\overline{P} \underset{= \overline{a_n} X^n}{=} \overline{U_2 V_2} = \overline{U_2} \overline{V_2}$$

et en particulier, le terme de degré 0,  $\overline{b_0 c_0} = \overline{b_0} \overline{c_0}$  est nul. Mais,  $p$  est irréductible et  $A$  est factoriel, donc au vu du Lemme 4,  $(p)$  est premier et  $A/(p)$  est intègre par le Lemme 2. Donc par le Lemme 3,  $A/(p)[X]$  est aussi intègre. D'où  $\overline{b_0} = 0$  ou  $\overline{c_0} = 0$  (mais pas les deux car sinon  $p^2 \mid b_0 c_0 = a_0$ , ce qui serait en contradiction avec (iii)).

On suppose donc  $\overline{b_0} = 0$  et  $\overline{c_0} \neq 0$ . Si on avait  $\forall i \in \llbracket 0, r \rrbracket, \overline{b_i} = 0$ , on aurait en particulier  $\overline{b_r} = 0$ , et donc  $\overline{b_r c_s} = \overline{a_n} = 0$  (exclu par (i)). Donc,

$$\exists i \in \llbracket 0, r-1 \rrbracket \text{ tel que } \overline{b_0} = \dots = \overline{b_i} = 0 \text{ et } \overline{b_{i+1}} \neq 0$$

Ainsi,

$$\overline{a_{i+1}} = \sum_{k=0}^{i+1} \overline{b_k c_{i+1-k}} = \underbrace{\overline{b_{i+1}}}_{\neq 0} \underbrace{\overline{c_0}}_{\neq 0} \neq 0$$

ce qui est absurde au vu de la condition (i) car  $i \in \llbracket 0, r-1 \rrbracket$  avec  $r-1 \leq n-1$ . □

**Application 7.** Soit  $n \in \mathbb{N}^*$ . Il existe des polynômes irréductibles de degré  $n$  sur  $\mathbb{Z}$ .

**[PER]**  
p. 67

*Démonstration.* On applique le Théorème 6 au polynôme  $P = X^n - 2$  avec le premier  $p = 2$  qui nous donne l'irréductibilité du polynôme sur  $\mathbb{Q}$ . Reste à montrer qu'il est irréductible sur  $\mathbb{Z}$ .

Or, en supposant  $P$  réductible sur  $\mathbb{Z}$ , on peut écrire  $P = QR$  avec  $Q, R \in \mathbb{Z}[X]$  de degré supérieur ou égal à 1 car  $P$  est primitif. Mais à fortiori,  $Q, R \in \mathbb{Q}[X]$  et ne sont pas inversibles donc  $P$  est réductible sur  $\mathbb{Q}$  : absurde. □

# Bibliographie

## **Théorie de Galois**

[GOZ]

Ivan GOZARD. *Théorie de Galois. Niveau L3-M1*. 2<sup>e</sup> éd. Ellipses, 1<sup>er</sup> avr. 2009.

<https://www.editions-ellipses.fr/accueil/4897-15223-theorie-de-galois-niveau-l3-m1-2e-edition-9782729842772.html>.

## **Cours d'algèbre**

[PER]

Daniel PERRIN. *Cours d'algèbre. pour l'agrégation*. Ellipses, 15 fév. 1996.

<https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html>.

## **Anneaux, corps, résultants**

[ULM18]

Felix ULMER. *Anneaux, corps, résultants. Algèbre pour L3/M1/agrégation*. Ellipses, 28 août 2018.

<https://www.editions-ellipses.fr/accueil/9852-20186-anneaux-corps-resultants-algebre-pour-l3-m1-agregation-9782340025752.html>.