Critère d'Eisenstein

Leçons concernées

* **141 :** Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
* **142 :** PGCD et PPCM, algorithmes de calcul. Applications.

Réference

* *Perrin - Cours d'algèbre*

Nous allons démontrer le critère d'Eisenstein, qui est un critère intéressant pour montrer qu'un anneau sur un anneau factoriel est irréductible.
Soit A un anneau factoriel. Pour $P \in A[X]$, son contenu $c(P)$ est le pgcd de ses coefficients. On commence par prouver le lemme suivant :

Lemme. *Soient $Q, R \in A[X]$. Alors $c(QR) = c(Q)c(R)$.*

Démonstration. Soit $P = QR$. Commençons par prouver que si Q et R sont primitifs ($c(Q) = c(R) = 1$), alors P est aussi primitif. Pour cela, supposons par l'absurde que ce n'est pas le cas. On prends alors un irréductible $p \in A$ qui divise tous les coefficients de P.
Projetons l'égalité $P = QR$ dans $A/(p)[X]$; on obtient alors $\overline{QR} = 0$ dans $A/(p)[X]$. Mais, p étant irréductible, l'idéal (p) est en particulier premier, et donc $A/(p)$ est intègre. Donc, $A/(p)[X]$ est aussi intègre. Ainsi, $\overline{Q} = 0$ ou $\overline{R} = 0$, mais aucune de ces possibilités n'est possible puisque cela voudrait dire que p divise tous les coefficients de Q ou de R, et donc que l'un ou l'autre n'est pas primitif, ce qui est exclu. P est donc lui aussi primitif.
Dans le cas non primitive, on écrit $P = c(Q)c(R)\dfrac{Q}{c(Q)}\dfrac{R}{c(R)}$. Les polynômes $Q/c(Q)$ et $R/c(R)$ sont primitifs, donc leur produit de même d'après ce que nous avons démontré. Or, si $\alpha \in A$, $c(\alpha P) = \alpha c(P)$ (homogénéité du pgcd). Donc $c(P) = c(Q)c(R)$.

□

Démontrons à présent le critère d'Eisenstein :

Théorème. *Soit $P \in A[X]$ que nous écrivons $P(X) = \sum_{k=0}^{n} a_k X^k$. Soit $K = Fr(A)$ le corps des fractions de A. On suppose qu'il existe un irréductible $p \in A$ satisfaisant les conditions suivantes :*

- *$p \mid a_k$ pour $k = 0, ..., n-1$*
- *$p \nmid a_n$*
- *$p^2 \nmid a_0$*

Alors P est irréductible dans $K[X]$ (et donc dans $A[X]$ si $c(P) = 1$).

Démonstration. Ecrivons $P = QR$ avec $Q, R \in K[X]$. Montrons tout d'abord qu'on peut écrire $P = \tilde{Q}\tilde{R}$ avec $\tilde{Q}, \tilde{R} \in A[X]$. Pour cela, on prends $a \in A$ et $b \in A$ tels que $(aQ) \in A[X]$ et $(bR) \in A[X]$ (il suffit pour cela de prendre le produit des dénominateurs dans les deux cas). On a alors l'égalité, dans $A[X]$, $abP = (aQ)(bR)$. Prenons le contenu : on trouve alors, d'après le lemme, $abc(P) = c(aQ)c(bR)$ soit $ab = \frac{1}{c(P)}c(aQ)c(bR)$.
On réécrit alors $P = \dfrac{1}{ab}(aQ)(bR) = c(P)\dfrac{aQ}{c(aQ)}\dfrac{bR}{c(bR)}$ qui est alors un produit de polynômes dans $A[X]$.

On peut alors se ramener au cas où $P = QR$ où $Q, R \in A[X]$. Si tel est le cas, projetons cette égalité dans $A/(p)[X]$, comme tout à l'heure. Nous avons alors, en vu des hypothèses, $\overline{a_n}X^n = \overline{QR}$ avec $\overline{a_n} \neq \overline{0}$. Nous sommes dans un anneau factoriel, donc d'après l'unicité de la décomposition en produit de facteurs irréductibles, $\overline{Q}$ et $\overline{R}$ sont de la forme $\overline{Q} = \overline{b}X^r$ et $\overline{R} = \overline{c}X^s$ avec $\overline{a_n} = \overline{b}\overline{c}$ et $r + s = n$.

Supposons par l'absurde que Q et R sont non constants. On remarque que, nécessairement, puisque $r + s = n$, b et c sont respectivement les coefficients dominants de Q et de R (sinon l'écriture $P = QR$ engendrerait un soucis de degré), et nous avons alors $r = deg(Q)$ et $s = deg(R)$. Puisque nous avons supposé Q et R non constants, cela signifie que $r, s > 0$. Ainsi, p divise le coefficient constant de Q, et le coefficient constant de R. Or, le produit des deux donne a_0. On obtient ainsi $p^2 \mid a_0$ ce qui est exclut.

P est ainsi irréductible dans $K[X]$.

□

Remarques :
- Ne pas hésiter à remplacer A par $\mathbb{Z}$ et ainsi K par $\mathbb{Q}$ dans certaines leçons.
- Application directe : $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \geq 1$. Ceci permet de voir que, contrairement au cas réel ou complexe, il existe des polynômes irréductibles de degré aussi grand qu'on veut dans $\mathbb{Q}[X]$.
- Une autre application : on peut prouver que $\phi_p(X)$ est irréductible grâce à Eisenstein, pour p premier. En effet, on montre pour cela, car c'est équivalent, que $\phi_p(X + 1)$ est irréductible. Or $\phi_p(X + 1) = \dfrac{(X+1)^p - 1}{X} = \displaystyle\sum_{k=1}^{p} \binom{p}{k} X^{k-1}$. Or, l'égalité $\binom{p}{k} = \dfrac{p}{k}\binom{p-1}{k-1}$ pour $k \neq 1$ soit $k\binom{p}{k} = p\binom{p-1}{k-1}$ permet de conclure, en sachant que $k < p$, que p divise $\binom{p}{k}$ par lemme de Gauss. Donc p divise tous les coefficients de ce polynôme, sauf le premier (qui est 1), et p^2 ne divise pas $\binom{p}{1} = p$. D'après le critère d'Eisenstein, ce polynôme, et donc ϕ_p, est irréductible.