6.8 Factorialité des anneaux de polynômes, critères d'irréductibilité

Dans cette section, on démontre en particulier le théorème 8, à savoir le résultat suivant : si A est un anneau factoriel, $A[X]$ est factoriel. On donne également, pour un anneau factoriel, des critères d'irréductibilté dans $A[X]$ et dans $\mathrm{Frac}(A)[X]$. Il est important dans ce qui suit de bien avoir assimilé les notions de A-associations et de A-pgcd définies dans la section précédente. *Il peut être utile (voire conseillé), en première lecture, de supposer dans tout ce qui suit que* $A = \mathbf{Z}$.

Définition 34. Soit A un anneau factoriel et $P \in \mathrm{Frac}(A)[X]$ un polynôme. On appelle contenu du polynôme P, et on note $c(P)$, tout A-pgcd des coefficients de P.

On dit que le polynôme P est primitif si $c(P) \sim_A 1$.

Remarque. Par A-pgcd des coefficients de P, on entend plus précisément ce qui suit : écrivons $P = \sum_{n \geqslant 0} a_n X^n$ avec $(a_n) \in \mathrm{Frac}(A)^{(\mathbf{N})}$ et soit E une partie de finie de $\mathbf{N}$ tel que pour tout $n \in \mathbf{N} \setminus E$ on a $a_n = 0$. Alors $c(P)$ est un A-pgcd de la famille $\{a_n\}_{n \in E}$. La dernière assertion de la proposition 33 montre que $c(P)$ ne dépend pas (à A-association près) du choix d'une telle partie E.

Remarque. En toute rigueur, le contenu n'est défini qu'à A-association près. Toute égalité que l'on écrit faisant intervenir des contenus doit être comprise à A-association près.

Proposition 35. *Soit A un anneau factoriel et $P \in A[X]$.*

1. *Si P est le polynôme nul, $c(P) = 0$, et ceci caractérise le polynôme nul.*
2. *Soit $P \in A[X]$ un polynôme unitaire. Alors P est primitif.*
   Plus généralement, si $P \in \mathrm{Frac}(A)[X]$ est unitaire, alors $\frac{1}{c(P)} \in A$.
3. *Soit $P \in \mathrm{Frac}(A)[X]$. On a $P \in A[X]$ si et seulement si $c(P) \in A$. En particulier tout polynôme primitif de $\mathrm{Frac}(A)[X]$ est un élément de $A[X]$.*
4. *Pour tout $a \in \mathrm{Frac}(A)$, on a $c(aP) \sim_A ac(P)$.*
5. *On suppose $P \neq 0$. Alors $c(P) \neq 0$ et $\frac{P}{c(P)}$ est un polynôme primitif.*

Démonstration. Ceci découle aussitôt des propositions 32 et33. □

Proposition 36. *Soit A un anneau factoriel et $P, Q \in \mathrm{Frac}(A)[X]$. Alors $c(PQ) \sim_A c(P)c(Q)$.*

Démonstration. Montrons tout d'abord que le produit de deux polynômes primitifs est primitif. Soit $P, Q \in A[X]$ des polynôme primitifs. D'après le théorème 25, il suffit de montrer que pour tout élément irréductible π de A, il existe un coefficient de PQ qui n'est pas divisble par π. Soit $B = A/\langle\pi\rangle$, $\overline{P}$, $\overline{Q}$ et $\overline{PQ} = \overline{P} \cdot \overline{Q}$ les images respectives de P, Q et PQ dans $B[X]$. Il s'agit de montrer que $\overline{PQ}$ est non nul. Or par hypothèse $\overline{P}$ et $\overline{Q}$ sont non nuls. En outre, comme π est irréductible et A est factoriel, l'idéal $\langle\pi\rangle$ est un idéal premier de A. Donc B est intègre, donc également $B[X]$. Donc $\overline{PQ} = \overline{P} \cdot \overline{Q}$ est non nul, ce qui conclut.

Soit à présent P et Q des polynômes de $A[X]$ quelconques. Si $P = 0$ ou $Q = 0$, l'égalité $c(P)c(Q) = c(PQ)$ est immédiate. Sinon, on a $c(P) \neq 0$ et $c(Q) \neq 0$, et d'après la proposition 35 les polynômes $\frac{P}{c(P)}$ et $\frac{Q}{c(Q)}$ sont des éléments primitifs de $A[X]$. Donc $\frac{1}{c(P)c(Q)}PQ$ est un élément primitif de $A[X]$. Toujours d'après la proposition 35, on a alors

$$1 \sim_A c\left(\frac{1}{c(P)c(Q)}PQ\right) \sim_A \frac{1}{c(P)c(Q)}c(PQ)$$

d'où le résultat. □

Lemme 37. *Soit A un anneau factoriel, $P \in A[X]$ un polynôme primitif, $Q, R \in \mathrm{Frac}(A)[X]$ tels que $P = QR$. Alors il existe des éléments primitifs $\tilde{Q}$, $\tilde{R}$ de $A[X]$, associés respectivement à Q et R dans $\mathrm{Frac}(A)[X]$, et tels que $P = \tilde{Q}\tilde{R}$.*

Démonstration. D'après la proposition 36 et les hypothèses, on a

$$1 \sim_A c(QR) \sim_A c(Q)c(R).$$

On en déduit qu'on a $c(Q)c(R) \in A^\times$. Posons $\widetilde{Q} = \frac{1}{c(Q)}Q$ et $\widetilde{R} = \frac{1}{c(R)}R$. Alors $\widetilde{Q}$ et $\widetilde{R}$ sont primitifs (proposition 35) et on a

$$P \sim_A \frac{1}{c(Q)c(R)}P \sim_A \widetilde{Q}\widetilde{R}.$$

□

Théorème 38. *Soit A un anneau factoriel. L'ensemble des éléments irréductibles de $A[X]$ est la réunion disjointes des deux ensembles suivants :*

1. *l'ensemble des polynômes constants qui sont des éléments irréductibles de A*
2. *l'ensemble des polynômes qui sont primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$*

Exemple. Tout polynôme *unitaire* de degré 1 est un élément irréductible de $A[X]$. Mais si a est un élément non nul et non inversible de A, le polynôme $aX + a$ est un polynôme de degré 1 qui n'est pas irréductible dans $A[X]$.

Démonstration. Exercice 5.14 □

Démonstration. (du théorème 8) Soit A un anneau factoriel. Il s'agit de montrer que $A[X]$ est factoriel. Montrons tout d'abord l'existence d'une décomposition en irréductibles.

Soit P un élément non nul et non inversible de $A[X]$. D'après la proposition 35, $Q = \frac{1}{c(P)}P$ est un élément primitif de $A[X]$

Soit $Q = \prod_{i=1}^{r} P_i$ une décomposition de Q en produit de polynôme irréductibles de $\mathrm{Frac}(A)[X]$. D'après le lemme 37, quitte à remplacer P_i par un polynôme associé dans $\mathrm{Frac}(A)[X]$ (donc encore irréductible dans $\mathrm{Frac}(A)[X]$), on peut supposer que les P_i sont des polynômes primitifs.

Ainsi les polynômes P_i sont irréductibles dans $A[X]$ d'après le théorème 38.

Comme $P = c(P)Q$, en décomposant $c(P)$ en irréductibles dans A, on obtient d'après le théorème 38 une décomposition de P en produit d'irréductibles de $A[X]$.

Montrons l'unicité de la décomposition à permutation et association près.

Supposons qu'on a une égalité

$$\prod_{i=1}^{r_1} a_i \prod_{i=1}^{r_2} P_i = \prod_{j=1}^{s_1} b_j \prod_{j=1}^{s_2} Q_j$$

où les a_i et b_j sont des éléments irréductibles de A, les P_i et Q_j sont des polynômes primitifs irréductibles dans $\mathrm{Frac}(A)[X]$, et r_1, r_2, s_1 et s_2 sont des entiers positifs. L'unicité de la décomposition dans $\mathrm{Frac}(A)[X]$ montre qu'on a nécessairement $r_2 = s_2$ et que quitte à renuméroter on a : pour tout $1 \leqslant i \leqslant s_1$, P_i et Q_i sont associés. Soit $1 \leqslant i \leqslant s_1$. Soit $\alpha_i \in \mathrm{Frac}(A)^\times$ tel que $P_i = \alpha_i Q_i$. En prenant les contenus, on trouve que $\alpha_i \sim_A 1$. Ainsi $\alpha_i \in A^\times \subset A[X]^\times$. Quitte à remplacer Q_i par $\alpha_i Q_i$, ce qui est loisible vu l'énoncé d'unicité visé, on a donc $P_i = Q_i$. On en déduit $\prod_{i=1}^{r_1} a_i = \prod_{j=1}^{s_1} b_j$ et on conclut en utilisant l'unicité de la factorisation dans l'anneau factoriel A. □

Corollaire 39. *Si A est un anneau factoriel et n est un entier strictement positif, l'anneau $A[X_1, \ldots, X_n]$ est factoriel.*

En particulier, si $\mathbf{K}$ est un corps, l'anneau $\mathbf{K}[X_1, \ldots, X_n]$ est factoriel.

Nous terminons ce chapitre par quelques critères d'irréductibilité dans les anneaux de polynômes.

Basiquement, l'idée est la suivant : soit A et B des anneaux intègres et $\varphi\colon A \to B$ un morphisme d'anneaux. Si $f \in A[X]$ a un coefficient dominant non tué par φ et est un produit

de deux polynômes non constants, $\varphi(f)$ sera un produit de deux polynômes non constants dans $B[X]$. Par contraposée, des propriétés d'« irréductibilité » de $\varphi(f)$ conduiront à des propriétés d'« irréductibilité » de f. L'exemple le plus basique est le résultat suivant (vu en TD) : soit $\mathbf{K} \to \mathbf{L}$ une extension de corps et $P \in \mathbf{K}[X]$; si P est irréductible dans $\mathbf{L}[X]$, il l'est aussi dans $\mathbf{K}[X]$. De manière générale, des critères efficaces sont obtenues en prenant pour φ un certain morphisme quotient, mais il faut faire attention au sens d'irréductible dans l'anneau $A[X]$ lorsque A n'est plus un corps (d'où les guillemets ci-dessus). Ceci motive notamment l'hypothèse de factorialité dans les énoncés ci-dessous.

Théorème 40. *Soit A un anneau factoriel, π un élément irréductible de A, B l'anneau intègre $A/\pi A$ et $\varphi\colon A \to B$ le morphisme quotient. On note encore φ l'unique morphisme d'anneau $A[X] \to B[X]$ qui envoie X sur X et induit φ en restriction à A (morphisme de « réduction modulo π » des coefficients d'un polynôme de $A[X]$)*

Soit $P \in A[X]$. On suppose que $\deg(\varphi(P)) = \deg(P)$ *et que $\varphi(P)$ est irréductible dans* $\mathrm{Frac}(A/\pi)[X]$. *Alors P est irréductible dans* $\mathrm{Frac}(A)[X]$.

Démonstration. L'hypothèse $\deg(\varphi(P)) = \deg(P)$ montre que π ne divise pas le coefficient dominant de P. En particulier π ne divise pas $c(P)$. Ainsi, si $Q \in A[X]$ est un polynôme primitif tel que $P = c(P)Q$, on a $\deg(\varphi(Q)) = \deg(Q)$, P et Q sont associés dans $\mathrm{Frac}(A)[X]$ et $\varphi(P)$ et $\varphi(Q)$ sont associés dans $\mathrm{Frac}(B)[X]$. Vu l'énoncé à démontrer, on peut donc supposer que $P = Q$, c'est à dire on peut supposer que P est primitif. Raisonnons par contraposée et supposons que $P = QR$, où Q et R sont des polynômes non constants de $\mathrm{Frac}(A)[X]$. Comme P est primitif, d'après le lemme 37, et quitte à remplacer Q et R par des éléments associées, on peut supposer Q et R sont des éléments de $A[X]$. On a alors $\varphi(P) = \varphi(Q)\varphi(R)$, d'où on tire $\deg(\varphi(P)) = \deg(\varphi(Q)) + \deg(\varphi(R))$. Comme φ ne peut que diminuer le degré et que $\deg(\varphi(P)) = \deg(P) = \deg(Q) + \deg(P)$, $\varphi(Q)$ et $\varphi(R)$ sont non constants, ce qui montre que $\varphi(P)$ n'est pas irréductible dans $\mathrm{Frac}(B)[X]$. □

Exemple. On peut appliquer ce critère à $X^4 + X^3 + 2X + 3 \in \mathbf{Z}[X]$ et $\pi = 2$. En effet on peut montrer que $X^4 + X^3 + [1]_2$ est irréductible dans $\mathbf{F}_2[X]$: il n'a pas de racine dans $\mathbf{F}_2$ et il n'est pas divisible par l'unique polynôme irréductible de degré 2 de $\mathbf{F}_2[X]$, à savoir $X^2 + X + [1]_2$.

On peut aussi appliquer ce critère à $X^2 + 1 + XYR(Y) + YS(Y) \in \mathbf{R}[X, Y]$ et $\pi = Y$.

Remarque. Ce qui fait notamment la souplesse du critère est la diversité de choix qui s'offre a priori pour l'irréductible π. Par exemple pour $A = \mathbf{Z}$, il suffit de trouver *un* nombre premier p tel que la réduction modulo p de P est irréductible dans $\mathbf{F}_p[X]$ pour conclure.

En dépit de cela, il existe en général des polynômes irréductibles dans $A[X]$ pour lesquels on ne pourra pas appliquer ce critère. Un exemple classique est le polynôme $X^4 + 1$, qui est

irréductible dans $\mathbf{Q}[X]$ (donc dans $\mathbf{Z}[X]$) mais qui est réductible modulo n'importe quel nombre premier (*cf.* l'exercice 5.6).

Le critère d'Eisenstein est également un critère d'irréductibilité basé sur la réduction modulo un irréductible π, mais de manière un peu plus fine, puisque dans le cadre d'application de ce critère le polynôme réduit modulo π sera réductible, ce qui permettra quand même au vu des hypothèses faites de conclure à l'irréductibilité du polynôme initial via une analyse plus poussée.

Théorème 41. Critère d'Eisenstein

Soit A un anneau factoriel, π un élément irréductible de A, B l'anneau intègre $A/\pi A$ et $\varphi\colon A \to B$ le morphisme quotient. On note encore φ l'unique morphisme d'anneau $A[X] \to B[X]$ qui envoie X sur X et induit φ en restriction à A (morphisme de « réduction modulo π » des coefficients d'un polynôme de $A[X]$)

Soit $n \geqslant 1$ un entier et $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme de degré n.

On suppose que pour tout $0 \leqslant i \leqslant n-1$, π divise a_i, que π ne divise pas a_n et que π^2 ne divise pas a_0.

Alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Démonstration. Soit $Q \in A[X]$ le polynôme primitif $\frac{1}{c(P)}P$. Il suffit de montrer que Q est irréductible dans $\mathrm{Frac}(A)[X]$. Par hypothèse π ne divise pas $c(P)$. Ainsi Q vérifie les mêmes hypothèses que P vis-à-vis des valuations π-adiques des coefficients.

Montrer que Q est irréductible dans $\mathrm{Frac}(A)[X]$ est équivalent d'après le lemme 37 à montrer le résultat suivant : si Q s'écrit comme un produit RS avec $R, S \in A[X]$, alors R ou S est constant.

Par hypothèse, on a $\varphi(P) = \alpha X^n$, où α est un élément non nul de $A/\pi A$. Par ailleurs si on a une décomposition de P comme ci-dessous, on a $\pi(P) = \pi(R)\varphi(S)$. Comme $A/\pi A$ est intègre, on en déduit qu'il existe $0 \leqslant m, r \leqslant n$ tels que $m + r = n$, $\beta, \gamma \in A/\pi A$ tels que $\varphi(R) = \beta X^m$ et $\varphi(S) = \gamma X^r$. Si $(m, r) \neq (0, 0)$, π divise $R(0)$ et $S(0)$, donc π^2 divise $R(0)S(0) = P(0)$ ce qui contredit les hypothèses. Ainsi on a par exemple $m = n$ et $r = 0$. Comme par ailleurs $\deg(R) + \deg(S) = n$ et $m \leqslant \deg(R)$ et $r \leqslant \deg(S)$, on a nécessairement $\deg(R) = n$ et $\deg(S) = 0$ □

Exemple. Pour tout nombre premier p et tout entier strictement positif n, le polynôme $X^n - p$ est irréductible dans $\mathbf{Q}[X]$ (et dans $\mathbf{Z}[X]$) ; pour le voir, on applique Eisenstein avec $\pi = p$. Il existe donc des polynômes irréductibles de tout degré dans $\mathbf{Q}[X]$.

Exemple. Soit $\mathbf{K}$ un corps, n un entier strictement positif et $P(Y) \in \mathbf{K}[Y]$ tel que $P(0) \neq 0$. Alors le polynôme $X^n - YP(Y)$ est irréductible dans $\mathbf{K}[X, Y]$. Pour le voir on applique Eisenstein avec $A = \mathbf{K}[Y]$ et $\pi = Y$.