Contenu et automorphismes de $k(X)$

Dans le premier paragraphe je fais quelques rappels sur le théorème qui affirme que si A est un anneau factoriel, alors $A[X]$ (et par récurrence, aussi $A[X_1, \ldots, X_n]$) est un anneau factoriel. On peut considérer cela comme un résultat bien connu, et l'utiliser sans démonstration pour proposer en développement le calcul du groupe des k-automorphismes du corps $k(X)$. C'est l'objet du deuxième paragraphe.

1 Factorialité des anneaux de polynômes et lemme de Gauss

La démonstration du théorème qui affirme que *si A est factoriel, alors $A[X]$ est factoriel* utilise de façon cruciale la notion de contenu : pour $P \in A[X]$, son *contenu* noté $c(P)$ est le pgcd de ses coefficients. Comme pour le pgcd, ce contenu est bien défini à multiplication près par un inversible de A. La propriété essentielle est connue sous le nom de *lemme de Gauus* :

Lemme 1 (Gauss) : *Soit A un anneau factoriel et P, Q deux polynômes à coefficients dans A. Alors $c(PQ) = c(P)c(Q)$.*

Si $c(P) = 1$ on dit que P est un polynôme *primitif*. On a l'énoncé précisément :

Théorème 2 : *Soit A factoriel et $\{a_p\}_{p\in\mathcal{P}}$ une famille d'irréductibles. Alors $A[X]$ est un anneau factoriel, avec pour famille explicite d'irréductibles la réunion de :*

(1) *la famille $\{a_p\}_{p\in\mathcal{P}}$, et*

(2) *la famille des polynômes non constants et primitifs de $A[X]$, irréductibles dans $K[X]$.*

Par exemple la famille des nombres premiers et des polynômes non constants de $\mathbb{Z}[X]$, à coefficients premiers entre eux, et irréductibles dans $\mathbb{Q}[X]$, est une famille d'irréductibles de $\mathbb{Z}[X]$.

On trouve les démonstrations correspondantes dans les livres d'algèbre commutative.

2 Application aux automorphismes de $k(X)$

On peut faire un développement sur les automorphismes de $k(X)$, soit en prenant pour acquis le théorème, soit en n'admettant que le lemme de Gauss et en prouvant le corollaire suivant :

Corollaire 3 : *Soit A un anneau factoriel, K son corps de fractions, $P \in A[X]$ tel que $c(P) = 1$. Alors, P est irréductible dans $A[X]$ ssi il est irréductible dans $K[X]$.*

Preuve : Supposons P irréductible dans $K[X]$. Si $P = QR$ dans $A[X]$, cette égalité étant valable aussi dans $K[X]$, alors soit Q soit R est une constante non nulle de K, disons Q. Donc d'après le lemme de Gauss $1 = c(P) = c(Q)c(R) = ac(R)$, et on déduit que $Q = a$ est en fait inversible dans A, donc P est irréductible dans $A[X]$.

Réciproquement, supposons P irréductible dans $A[X]$. Supposons que $P = QR$ avec Q et R dans $K[X]$. Il est clair qu'il existe des éléments $\lambda, \mu \in K^\times$ tels que $Q = \lambda Q'$ et $R = \mu R'$ avec Q', R' dans $A[X]$ et de contenu 1. On a donc $P = \lambda\mu Q'R'$ et en utilisant encore le lemme de Gauss, $1 = \lambda\mu$. Il s'ensuit que $P = Q'R'$ et comme P irréductible dans $A[X]$ par hypothèse, Q' ou R' est un inversible de A. Donc Q ou R est un inversible de K. □

Théorème 4 : *Le morphisme* $\mathrm{GL}_2(k) \to \mathrm{Aut}_k(k(x))$ *donné par*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \left(X \mapsto \frac{aX+b}{cX+d} \right)$$

induit un isomorphisme entre $\mathrm{PGL}_2(k)$ *et le groupe des* k*-automorphismes du corps des fractions rationnelles* $k(X)$*.*

Preuve : Soit et montrons comment on en déduit le théorème.

Il est facile de vérifier que l'application de l'énoncé du théorème est bien un morphisme de groupes et que de plus, une matrice $(2,2)$ induit l'identité de $k(X)$ ssi c'est une homothétie. On a donc une injection de $\mathrm{PGL}_2(k)$ dans $\mathrm{Aut}_k(k(x))$ et il ne reste qu'à montrer qu'elle est surjective. Soit $\varphi\colon k(X) \to k(X)$ un automorphisme, notons $F = \varphi(X) = U(X)/V(X)$. L'image de φ est le corps $k(F)$, donc si c'est un automorphisme on a $[k(X) : k(F)] = 1$. Écrivons $F = U(X)/V(X)$ sous forme irréductible, et posons $n = \max\{\deg(U), \deg(V)\}$. Si on montre que $[k(X) : k(F)] = n$, on obtient $n = 1$ et le résultat en découle immédiatement.

Il nous reste à montrer que $[k(X) : k(F)] = n$. D'abord, il est clair que X est algébrique sur $k(F)$ car annulé par le polynôme de degré n :

$$P(T) \overset{\text{déf}}{=} V(T)F - U(T)\,.$$

Il nous suffit maintenant de montrer que P est irréductible dans $k(F)[T]$. L'égalité

$$\underbrace{[k(X) : k]}_{\infty} = \underbrace{[k(X) : k(F)]}_{\text{fini}}\,[k(F) : k]$$

montre que F est transcendant sur k, donc $k[F]$ est un anneau de polynômes. La clé de la preuve est que $P(T) = V(T)F - U(T)$ est irréductible dans $k[T][F]$:

- si on a admis le théorème 2, cela provient du fait qu'il est de degré 1 en F et primitif ;
- si on n'a admis que le corollaire 3, on dit que P est de degré 1 en F donc irréductible dans $k(X)[F]$, et comme il est primitif, il est irréductible dans $k[X][F]$ d'après ce corollaire.

Comme $k[T][F] = k[F][T]$, on en déduit que le polynôme $P(T)$ est irréductible dans $k[F][T]$, donc dans $k(F)[T]$, cqfd. □