

C. MALLOL

Sur les f-morphismes

Publications des séminaires de mathématiques et informatique de Rennes, 1980, fascicule S3

« Colloque d'algèbre », , p. 131-150

http://www.numdam.org/item?id=PSMIR_1980__S3_131_0

© Département de mathématiques et informatique, université de Rennes, 1980, tous droits réservés.

L'accès aux archives de la série « Publications mathématiques et informatiques de Rennes » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SUR LES f-MORPHISMES

par

C. MALLOL

1- Sur les f-morphismes

1.1- Préliminaires :

Soient A un anneau intègre et unitaire et $A[X_1, \dots, X_n]$ l'anneau de polynômes à n variables à coefficients dans A .

Une application φ de $A[X_1, \dots, X_n]$ dans $A[X_1, \dots, X_n]$ est un A-endomorphisme, si pour tout élément $P(X_1, \dots, X_n)$ de $A[X_1, \dots, X_n]$ on a $\varphi(P(X_1, \dots, X_n)) = P(\varphi(X_1), \dots, \varphi(X_n))$.

Un A-endomorphisme bijectif de $A[X_1, \dots, X_n]$ est appelé un A-automorphisme.

Deux questions sont depuis longtemps posées : i) la classification des A-automorphismes de $A[X_1, \dots, X_n]$; ii) G étant un groupe de A-automorphismes de $A[X_1, \dots, X_n]$, déterminer la structure de l'ensemble des invariants de G , i.e., le sous-anneau de $A[X_1, \dots, X_n]$, noté $A[X_1, \dots, X_n]^G$, défini par $A[X_1, \dots, X_n]^G = \{P/P \in A[X_1, \dots, X_n], \varphi(P) = P, \forall \varphi \in G\}$.

Dans le cas d'une variable, les deux questions ont été résolues, la première par R. Gilmer (cf. [1]) et la seconde par P. Samuel (cf. [2]). Cependant, pour $n \geq 2$ on connaît très peu de choses. En effet, à partir de $n \geq 2$ les problèmes acquièrent une très grande complexité calculatoire. Il s'ajoute à cela le fait que les méthodes utilisées pour $n = 1$ ne marchent plus pour $n \geq 2$, par exemple, les méthodes basées sur le terme de plus haut degré d'un polynôme à une variable.

Bien qu'il existe un résultat de Nagata (cf. [3]) concernant la classification des K-automorphismes de $K[X, Y]$ où K est un corps commutatif, il en reste beaucoup à faire.

Si A et B sont deux anneaux intègres et unitaires et $f : A \rightarrow B$ un homo-

morphisme unitaire d'anneaux, un f-morphisme de $A[X]$ dans $B[Y]$ est une application $\varphi : A[X] \rightarrow B[Y]$ telle que si $P = \sum_{i=0}^n \alpha_i X^i$ est dans $A[X]$, alors $\varphi(P) = \sum_{i=0}^n f(\alpha_i) \varphi(X)^i$.

Bien qu'étant une généralisation de la notion de A-endomorphisme, les f-morphismes ont été introduits comme une technique en vue d'étudier les problèmes à deux ou plusieurs variables. En effet, si $\varphi : A[X, Y] \rightarrow A[X, Y]$ est un A-auto-morphisme et si $\varphi|_{A[X]}$ est la restriction de φ à $A[X]$, alors φ peut être considéré, de façon naturelle, comme un $\varphi|_{A[X]}$ -morphisme défini dans $A[X][Y]$ à valeurs dans $A[\varphi(X)][\varphi(Y)]$.

1.2- Sur les f-morphismes.

Soient A et B deux anneaux et $f : A \rightarrow B$ un homomorphisme d'anneaux. On dira que l'application $\varphi : A[X] \rightarrow B[Y]$ est un f-morphisme si $\varphi(\sum_{i=0}^n \alpha_i X^i) = \sum_{i=0}^n f(\alpha_i) \varphi(X)^i$, pour tout polynôme $\sum_{i=0}^n \alpha_i X^i$ de $A[X]$. On notera $\text{Hom}_f(A[X], B[Y])$ l'ensemble des f-morphismes de $A[X]$ dans $B[Y]$.

Il est clair que si $A = B$ et $f = \text{id}_A$, alors un f-morphisme de $A[X]$ dans $A[Y]$ n'est autre que un A-homomorphisme d'anneaux au sens habituel.

Comme, par définition, pour tout $\varphi \in \text{Hom}_f(A[X], B[Y])$ on a $\varphi|_A = f$, il en résulte que $f \neq 0$ entraîne $\varphi \neq 0$. Ainsi, si A et B sont deux anneaux unitaires et $f : A \rightarrow B$ un homomorphisme unitaire d'anneaux, alors $B \neq \{0\}$ entraîne $f \neq 0$ donc $\varphi \neq 0$.

Dorénavant, on supposera A et B intègres et unitaires et $f : A \rightarrow B$ un homomorphisme unitaire d'anneaux.

1.2.1- Proposition. Soient $f \in \text{Hom}(A, B)$ et $\varphi \in \text{Hom}_F(A[X], B[Y])$. Si φ est injectif, il en est de même de f .

En effet, soit $\alpha \in \text{Ker}(f)$. Comme φ est injectif $\varphi(\alpha) = f(\alpha) = 0$ entraîne $\alpha = 0$.

1.2.2- Proposition. Soient $f \in \text{Hom}(A, B)$ et $\varphi \in \text{Hom}_F(A[X], B[Y])$. On a :

- (i) $(\text{Ker } f)[X] \subset \text{Ker } \varphi$;
- (ii) si $\varphi(X) \notin B$, $\text{Ker } \varphi = (\text{Ker } f)[X]$.

En effet, la condition (i) est évidente et pour ce qui est de (ii), posons $\varphi(X) = \sum_{j=0}^m \beta_j Y^j$ où $m \geq 1$ et $\beta_m \neq 0$. Soit maintenant $P = \sum_{i=0}^n \alpha_i X^i \in \text{Ker } \varphi$. On a $0 = \varphi(P) = \sum_{i=0}^n f(\alpha_i) \left(\sum_{j=0}^m \beta_j Y^j \right)^i$ et on déduit facilement que $f(\alpha_n) \beta_m^n = 0$, d'où $f(\alpha_n) = 0$. Par récurrence, on a $f(\alpha_i) = 0$ pour tout $0 \leq i \leq n$, donc $P \in (\text{Ker } f)[X]$.

1.2.3- Corollaire. Soient $f \in \text{Hom}(A, B)$ et $\varphi \in \text{Hom}_F(A[X], B[Y])$. Si $\varphi(X) \notin B$, les conditions suivantes sont équivalentes :

- (i) φ est injectif ; (ii) f est injectif.

En effet, ceci découle des propositions 1.2.1- et 1.2.2-.

1.2.4- Proposition. Soient $f \in \text{Hom}(A, B)$ et $\varphi \in \text{Hom}_F(A[X], B[Y])$. Les conditions suivantes sont équivalentes : (i) $\text{Ker } \varphi = (\text{Ker } f)[X]$; (ii) l'ensemble $\{1, \varphi(X), \varphi(X)^2, \dots\}$ est un système linéairement indépendant du $\text{Im}(f)$ -module $B[Y]$.

En effet, soit $I \subset \mathbb{N}$, I ensemble fini. Si $\sum_{i \in I} f(\alpha_i) \varphi(X)^i = 0$ alors $\varphi(\sum_{i \in I} \alpha_i X^i) = 0$ donc $\sum_{i \in I} \alpha_i X^i \in \text{Ker } \varphi$, et si l'on suppose que $\text{Ker } \varphi = (\text{Ker } f)[X]$, alors $\alpha_i \in \text{Ker } f$ pour tout $i \in I$, soit $f(\alpha_i) = 0$ pour tout $i \in I$. Donc

$\{1, \varphi(X), \varphi(X)^2, \dots\}$ est un système linéairement indépendant du $\text{Im}(f)$ -module $B[Y]$.

Ceci nous dit que (i) $\Rightarrow$ (ii).

Montrons que (ii) $\Rightarrow$ (i). Si $\sum_{i \in I} \alpha_i X^i \in \text{Ker } \varphi$, alors $0 = \varphi(\sum_{i \in I} \alpha_i X^i) = \sum_{i \in I} f(\alpha_i) \varphi(X)^i$ et d'après l'hypothèse $f(\alpha_i) = 0$ pour tout i dans I . Ceci nous montre que $\sum_{i \in I} \alpha_i X^i$ appartient à $(\text{Ker } f)[X]$.

1.2.5- Corollaire. Soient f dans $\text{Hom}(A, B)$ et φ dans $\text{Hom}_f(A[X], B[Y])$. Les conditions suivantes sont équivalentes : (i) φ est injectif ;
(ii) f est injectif et $\{1, \varphi(X), \varphi(X)^2, \dots\}$ est un système linéairement indépendant du $\text{Im}(f)$ -module $B[Y]$.

En effet, (i) $\Rightarrow$ (ii) est une conséquence des propositions 1.2.1- et 1.2.2- et (ii) $\Rightarrow$ (i) résulte de la proposition 1.2.4-.

1.2.6- Proposition. Soient f dans $\text{Hom}(A, B)$ et φ dans $\text{Hom}_f(A[X], B[Y])$. Les conditions sont équivalentes : (i) φ est surjectif; (ii) f est surjectif et $\varphi(X) = \beta_0 + \beta_1 Y$, $\beta_0, \beta_1 \in B$, β_1 étant un élément inversible de B .

En effet, si φ est surjectif, il est clair que $\varphi(X) \notin B$, donc si P est un élément de $A[X] - (A + (\text{Ker } f)[X])$ on a $\varphi(P) \notin B$. On déduit $B = \varphi(A) = f(A)$, donc f est surjectif. Posons maintenant $\varphi(X) = \sum_{j=0}^m \beta_j Y^j$ où $m \geq 1$ et $\beta_m \neq 0$, et soit $Q = \sum_{i=0}^n \alpha_i X^i$ un élément de $A[X]$ tel que $\varphi(Q) = Y$ et $f(\alpha_n) \neq 0$. On a alors $Y = \varphi(Q) = \sum_{i=0}^n f(\alpha_i) (\sum_{j=0}^m \beta_j Y^j)^i$ et comme $f(\alpha_n) \beta_m^n \neq 0$ on déduit que $n.m=1$ ce qui entraîne $n=m=1$, donc, $\varphi(X) = \beta_0 + \beta_1 Y$ et β_1 un élément inversible de B . Ceci nous dit que (i) $\Rightarrow$ (ii). Montrons que (ii) $\Rightarrow$ (i). Si $\varphi(X) = \beta_0 + \beta_1 Y$ et si β_1 est un élément inversible de B on obtient $Y = \beta_1^{-1}(\varphi(X) - \beta_0)$; f étant surjectif, soient γ et δ deux éléments de A tels que $f(\gamma) = \beta_0$ et $f(\delta) = \beta_1^{-1}$. On a $Y = \varphi(\delta X - \delta \gamma)$ ce

qui montre que φ est surjectif.

1.2.7- Corollaire. Soient f dans $\text{Hom}(A, B)$ et φ dans $\text{Hom}_f(A[X], B[Y])$. Les conditions suivantes sont équivalentes : (i) φ est bijectif ; (ii) φ est surjectif et f est injectif.

En effet, ceci découle du corollaire 1.2.3- et de la proposition 1.2.6-.

1.2.8- Corollaire. Soit $\varphi : A[X] \rightarrow A[Y]$ un A -homomorphisme de $A[X]$ dans $A[Y]$. On a : (i) φ est injectif si et seulement si $\varphi(X) \notin A$; (ii) φ est surjectif si et seulement si φ est bijectif, si et seulement si $\varphi(X) = \alpha + \beta Y$ et β est un élément inversible de A .

Ceci découle des résultats précédents.

Le corollaire 1.2.8- nous dit que si $\varphi : A[X] \rightarrow A[X]$ est un A -endomorphisme de $A[X]$, alors φ est un A -automorphisme de $A[X]$ si et seulement si $\varphi(X) = \alpha + \beta X$ où $\alpha, \beta \in A$ et $\beta \in U(A)$. Cette classification des A -automorphismes de $A[X]$ est due à R. Gilmer (cf. [1]). On note $U(A)$ le groupe multiplicatif des éléments inversibles de A .

1.2.9- Remarque. Soit $\varphi : A[X] \rightarrow A[Y]$ un A -homomorphisme injectif ; φ n'est pas nécessairement surjectif, même si le degré du polynôme $\varphi(X)$ est égal à 1. En effet, le $\mathbb{Z}$ -homomorphisme $\varphi : \mathbb{Z}[X] \rightarrow \mathbb{Z}[Y]$ défini par $\varphi(X) = 1 + 2Y$ n'est pas surjectif, car l'élément 2 n'est pas inversible dans $\mathbb{Z}$ (!).

Ce qui suit est un résultat de Abhyankar-Heinzer-Eakin (cf. [4]). La notion de f -morphisme permet une démonstration brève de tel résultat.

1.2.10- Proposition. Soit $\varphi : A[X,Y] \rightarrow A[X,Y]$ un A-endomorphisme de $A[X,Y]$. Si φ est surjectif, alors φ est bijectif.

En effet, si φ est surjectif alors $\varphi(X) \notin A$, car, sinon on aurait $A[X,Y] = A[\varphi(Y)]$ ce qui est impossible. Cela nous dit que $\varphi|_{A[X]} : A[X] \rightarrow A[\varphi(X)]$ est un A-homomorphisme surjectif d'anneaux de polynômes donc, d'après le corollaire 1.2.8-, injectif. Mais φ est, de façon naturelle, un $\varphi|_{A[X]}$ -morphisme surjectif et d'après le corollaire 1.2.7-, φ est bijectif.

La proposition 1.2.10- nous dit que si $\varphi : A[X,Y] \rightarrow A[T,S]$ est un A-homomorphisme surjectif, il est aussi injectif.

1.2.11- Proposition. Soient $f : A \rightarrow B$ un isomorphisme d'anneaux et $\varphi : A[X,Y] \rightarrow B[T,S]$ un f-morphisme surjectif. Alors φ est injectif.

En effet, soient $\varphi_1 : A[X,Y] \rightarrow A[T,S]$ et $\varphi_2 : A[T,S] \rightarrow B[T,S]$ les applications définies par $\varphi_1(\sum_{i,j} \alpha_{ij} X^i Y^j) = \sum_{i,j} \alpha_{ij} T^i S^j$ et

$$\varphi_2(\sum_{k,l} \beta_{kl} T^k S^l) = \sum_{k,l} f(\beta_{kl}) T^k S^l.$$

Ainsi définies, φ_1 et φ_2 font commuter le diagramme

$$\begin{array}{ccc} A[X,Y] & \xrightarrow{\varphi} & B[T,S] \\ \varphi_1 \searrow & & \nearrow \varphi_2 \\ & A[T,S] & \end{array}$$

i.e., $\varphi = \varphi_2 \circ \varphi_1$, et d'après des résultats précédents, φ_1 et φ_2 sont bijectifs, donc φ est bijectif.

1.2.12- Proposition. Soit $\varphi : A[X,Y,Z] \rightarrow A[X,Y,Z]$ un A-endomorphisme de $A[X,Y,Z]$. Si φ est surjectif, alors φ est injectif.

En effet, comme $\varphi(X) \notin A$, $\varphi|_{A[X]}$ est un A -homomorphisme bijectif de $A[X]$ dans $A[\varphi(X)]$. Comme φ est, de façon naturelle, un $\varphi|_{A[X]}$ -morphisme surjectif de $A[X][Y, Z]$ dans $A[\varphi(X)][\varphi(Y), \varphi(Z)]$, d'après la proposition 1.2.11-, il est bijectif.

Compte tenu que la démarche utilisée pour aboutir au résultat de la proposition 1.2.12- peut-être répétée pour un nombre d'indéterminées $n \geq 3$, on peut écrire :

1.2.13- Proposition. Tout A -endomorphisme surjectif de $A[X_1, \dots, X_n]$ dans $A[X_1, \dots, X_n]$ est injectif.

On étudie maintenant à l'aide de la technique des f -morphisms, quelques A -automorphismes de $A[X, Y]$.

1.3- Applications et exemples. Soit $\varphi : A[X, Y] \rightarrow A[X, Y]$ un A -automorphisme de $A[X, Y]$ tel que $\varphi(X) = \alpha + \beta X$, α et β éléments de A , $\beta \in U(A)$. Il est clair que $\varphi|_{A[X]} : A[X] \xrightarrow{\sim} A[X]$ est un A -automorphisme de $A[X]$, d'où on déduit que $\varphi(Y) = P(X) + \gamma Y$ avec $P(X) \in A[X]$ et γ est un élément inversible de A .

1.3.1- Proposition. Soit φ un A -automorphisme de $A[X, Y]$. Les conditions suivantes sont équivalentes : (i) $\varphi|_{A[X]} : A[X] \rightarrow A[X]$ est un A -automorphisme de $A[X]$;
(ii) $\varphi(X) = \alpha + \beta X$, α et β éléments de A et β inversible dans A ;
(iii) $\varphi(X)$ est un élément de $A[X]$.

En effet, il est clair que (i) $\Leftrightarrow$ (ii) et que (ii) $\Rightarrow$ (iii). Montrons que (iii) $\Rightarrow$ (i). Si $\varphi(X) \in A[X]$, alors $\varphi(Y) \notin A[X]$, donc $\varphi(Y) = \sum_{k=1}^{\infty} \gamma_{k,1} X^k Y^1$ et

il existe $\gamma_{kl} \neq 0$ tel que $l \neq 0$. Soit $P = \sum_{i,j} \alpha_{ij} X^i Y^j$ le seul élément de $A[X, Y]$ tel que $\varphi(P) = X$. On obtient ainsi l'équation $X = \sum_{i,j} \alpha_{ij} \varphi(X)^i (\sum_{k,l} \gamma_{kl} X^k Y^l)^j$ (*)
 Soient, maintenant, $l_0 = \max\{l/\gamma_{kl} \neq 0\}$, $k_0 = \max\{k/\gamma_{kl_0} \neq 0\}$; $j_0 = \max\{j/\alpha_{ij} \neq 0\}$ et $i_0 = \max\{i/\alpha_{ij_0} \neq 0\}$. A partir de l'équation (*) on déduit que $\varphi(X)^{i_0} X^{k_0} Y^{j_0}$.
 $Y^{l_0} j_0$ est un élément de $A[X]$, d'où $l_0 j_0 = 0$ et comme par construction $l_0 \neq 0$, on obtient $j_0 = 0$. Ceci nous dit que $P \in A[X]$, ce qui montre que $\varphi|_{A[X]} : A[X] \xrightarrow{\sim} A[X]$.

Soit maintenant $\varphi : A[X, Y] \rightarrow A[X, Y]$ le A -endomorphisme de $A[X, Y]$ défini par $\varphi(X) = \alpha X + P(Y)$ et $\varphi(Y) = Q(\varphi(X)) + \beta Y$, où α et β sont des éléments de A , $P(Y)$ un élément de $A[Y]$ et $Q(\varphi(X))$ un polynôme en $\varphi(X)$. Si α et β sont inversibles dans A , alors φ est un A -automorphisme de $A[X, Y]$. En effet, il suffit de voir que $Y = \varphi(\beta^{-1}Y - \beta^{-1}Q(X))$ et $X = \varphi(\alpha^{-1}X - \alpha^{-1}P(\beta^{-1}Y - \beta^{-1}Q(X)))$, ce qui montre que φ est surjectif, donc bijectif.

Montrons maintenant que si φ est un A -automorphisme de $A[X, Y]$ tel que $\varphi(X) = \alpha X + P(Y)$ où $\alpha \in U(A)$ et $P(Y) \in A[Y]$, alors $\varphi(Y) = Q(\varphi(X)) + \beta Y$, où β est un élément inversible de A et Q est un polynôme en $\varphi(X)$.

En effet, on remarque que $X = \alpha^{-1}\varphi(X) - \alpha^{-1}P(Y)$, d'où $A[X, Y] = A[\varphi(X), Y]$. Ceci nous dit que φ peut être considéré comme un $\varphi|_{A[X]}$ -morphisme de $A[X][Y]$ dans $A[\varphi(X)][Y]$ et, par suite $\varphi(Y) = Q(\varphi(X)) + \beta Y$, où β est un élément inversible de A .

On voit donc que si φ est un A -automorphisme de $A[X, Y]$ tel que $A[X, Y] = A[\varphi(X), Y]$, alors $\varphi(Y) = Q(\varphi(X)) + \beta Y$, où β est un élément inversible de A et $Q(\varphi(X))$ est un polynôme en $\varphi(X)$.

Réciproquement, si φ un A -automorphisme de $A[X, Y]$ tel que $\varphi(Y) = Q(\varphi(X)) + \beta Y$, où β est un élément inversible de A et $Q(\varphi(X))$ un polynôme en $\varphi(X)$, on obtient $\varphi^{-1}(Y) = \beta^{-1} Y - \beta^{-1} Q(X)$, d'où $\varphi^{-1}(X) = \alpha X + P(\varphi^{-1}(Y))$ où α est un élément inversible de A et $P(\varphi^{-1}(Y))$ un polynôme en $\varphi^{-1}(Y)$. On déduit donc que $\varphi(X) = \alpha^{-1} X - \alpha^{-1} P(Y)$ et ceci nous permet d'énoncer la proposition suivante :

1.3.2- Proposition. Soit φ un A -endomorphisme de $A[X, Y]$. Les conditions suivantes sont équivalentes : (i) $\varphi(X) = \alpha X + P(Y)$ et $\varphi(Y) = \beta Y + Q(\varphi(X))$, où α et β sont deux éléments inversibles de A ; (ii) φ est bijectif et $\varphi(X) = \alpha X + P(Y)$ où α est un élément inversible de A ; (iii) φ est bijectif et $A[X, Y] = A[\varphi(X), Y]$.

Ces résultats nous montrent que la classification des A -automorphismes de $A[X, Y]$ est beaucoup plus complexe que dans le cas d'une variable. Si K est un corps commutatif, d'après Nagata (cf. [3]) l'ensemble $\text{Aut}_K(K[X, Y])$ est engendré par les K -automorphismes du type $X \rightarrow aX + bY + c$ et $Y \rightarrow \alpha X + \beta Y + \gamma$ où $a, b, c, \alpha, \beta, \gamma \in K$ et $a\beta - b\alpha \neq 0$ et les K -automorphismes du type $X \rightarrow aX + P(Y)$ et $Y \rightarrow bY + c$ où $a, b, c \in K$, $a \neq 0$, $b \neq 0$ et $P(Y) \in K[Y]$.

Compte tenu de ce résultat de Nagata et des renseignements fournis par la proposition 1.3.2-, deux questions se posent de façon naturelle. La première est sur le rapport qui peut exister entre l'ensemble $\text{Aut}_A(A[X_1, X_2])$ et les ensembles N_{ij} , où $(i, j) \in \{1, 2\}^2$, définis par $N_{i,j} = \{\varphi \mid \varphi \in \text{Aut}_A(A[X_1, X_2]), A[X_i, X_j] = A[\varphi(X_i), X_j]\}$. Deuxièmement, étant donné un A -automorphisme φ de $A[X_1, X_2]$, étudier le degré de X_i , $i = 1, 2$, dans le polynôme $\varphi(X_k)$, $k = 1, 2$. Ce travail ne traite pas ces deux questions.

1.4- La notion de f-invariant

Dans ce qui suit on donne une généralisation de la notion d'invariant et de l'ensemble des invariants d'un A-endomorphisme.

Soit $f \in \text{Hom}(A, B)$. On appellera f-morphisme canonique de $A[X]$ dans $B[Y]$ l'application $I_f : A[X] \rightarrow B[Y]$ définie par $I_f(\sum_{i=0}^n \alpha_i X^i) = \sum_{i=0}^n f(\alpha_i) Y^i$ pour tout élément $\sum_{i=0}^n \alpha_i X^i$ de $A[X]$.

Soit φ un élément de $\text{Hom}_f(A[X], B[Y])$. On appellera ensemble des f-invariants de φ , l'ensemble $A[X]^\varphi$ défini par $A[X]^\varphi = \{P \mid P \in A[X], \varphi(P) = I_f(P)\}$.

Soit maintenant, G un sous-ensemble de $\text{Hom}_f(A[X], B[Y])$. L'ensemble des f-invariants de G est l'ensemble $A[X]^G$ défini par $A[X]^G = \{P \mid P \in A[X], \varphi(P) = I_f(P), \forall \varphi \in G\}$.

D'après les définitions précédentes, il est clair que si φ est un élément de $\text{Hom}_f(A[X], B[Y])$ alors $A[X]^\varphi = A[X]^{\{\varphi\}} = \text{Ker}(I_f - \varphi)$.

1.4.1- Proposition. Soient $f \in \text{Hom}(A, B)$, $g \in \text{Hom}(B, C)$ et $I_f : A[X] \rightarrow B[Y]$, $I_g : B[Y] \rightarrow C[Z]$ les morphismes canoniques respectifs. Alors $I_g \circ f = I_g \circ I_f$. De plus, si f est bijectif il en est de même de I_f et $(I_f)^{-1} = I_{f^{-1}}$.

La démonstration est immédiate.

1.4.2- Proposition. Soient f un élément de $\text{Hom}(A, B)$ et G un sous-ensemble de $\text{Hom}_f(A[X], B[Y])$. On a : (i) $A + (\text{Ker } f)[X] \subset A[X]^G$; (ii) $A[X]^G$ est un sous-anneau de $A[X]$; (iii) $A[X]^G = \bigcap_{\varphi \in G} A[X]^\varphi$; (iv) si $G = \text{Hom}_f(A[X], B[Y])$, alors $A[X]^G = A + (\text{Ker } f)[X]$.

En effet, si $P = \alpha + \sum_{i=0}^n \alpha_i X^i$ est un élément de $A + (\text{Ker } f)[X]$, on a $I_f(P) = f(\alpha) = \varphi(P)$ pour tout élément de $\text{Hom}_f(A[X], B[Y])$. Ceci montre (i). Pour ce qui est de (ii), d'après (i) on voit que $A[X]^G \neq \emptyset$. Soient P, Q deux éléments

de $A[X]^G$. On a $\varphi(PQ) = \varphi(P)\varphi(Q) = I_f(P)I_f(Q) = I_f(PQ)$ et $\varphi(P+Q) = \varphi(P)+\varphi(Q) = I_f(P)+I_f(Q) = I_f(P+Q)$, ce qui montre que $A[X]^G$ est un sous-anneau de $A[X]$. Pour démontrer (iii), soit P un élément de $A[X]^G$. On a les équivalences suivantes :

$$P \in A[X]^G \Leftrightarrow \varphi(P) = I_f(P), \forall \varphi \in G \Leftrightarrow P \in A[X]^\varphi, \forall \varphi \in G \Leftrightarrow P \in \bigcap_{\varphi \in G} A[X]^\varphi.$$

Finalement, soit $\varphi \in \text{Hom}_f(A[X], B[Y])$ défini par $\varphi(X) = \beta \in B$. Il est clair que $A[X]^\varphi = A + (\text{Ker } f)[X]$, ce qui montre (iv).

1.4.3- Théorème. Soient f dans $\text{Hom}(A, B)$ et G un sous-ensemble de $\text{Hom}_f(A[X], B[Y])$ tel que $A[X]^G \not\subseteq A + (\text{Ker } f)[X]$. On a alors : i) pour tout $\varphi \in G$, $\varphi(X) = \beta_0 + \beta_1 Y$, avec $\beta_0, \beta_1 \in B$, β_1 étant inversible et d'ordre fini ; ii) il existe $P = \sum_{i=0}^{n-1} \alpha_i X^i + \alpha_n X^n$ dans $A[X]^G$, $f(\alpha) \neq 0$, tel que pour tout $Q \in A[X]^G$ on a $\alpha^k Q \in A + (\text{Ker } f)[X][P]$ pour un élément $k \in \mathbb{N}$.

En effet, comme $A[X]^G \not\subseteq A + (\text{Ker } f)[X]$, soit $Q \in A[X]^G$, $Q = \sum_{j=0}^m \alpha_j X^j$ tel que $f(\alpha_m) \neq 0$ et $m > 0$. Soit $\varphi \in G$. On a $\varphi(Q) = I_f(Q)$. Posons $\varphi(X) = \sum_{i=0}^n \beta_i Y^i$, $\beta_n \neq 0$. On a donc les égalités suivantes : $\varphi(Q) = \sum_{j=0}^m f(\alpha_j) \varphi(X)^j = \sum_{j=0}^m f(\alpha_j) \left(\sum_{i=0}^n \beta_i Y^i \right)^j = \sum_{j=0}^m f(\alpha_j) \sum_{i=0}^{jn} \beta_i^j Y^i = \sum_{i=0}^{mn} \left(\sum_{j=0}^m f(\alpha_j) \beta_i^j \right) Y^i = I_f(Q)$. Si l'on prend de chaque côté de l'égalité le terme de plus grand degré, on obtient $f(\alpha_m) \beta_n^{mn} Y^{mn} = f(\alpha_m) Y^m$, d'où $m \cdot n = m$ et comme $m \neq 0$, on a $n=1$. Cela nous dit que $\varphi(X) = \beta_0 + \beta_1 Y$ et β_1 est un élément inversible de B d'ordre fini, i.e., $\beta_1^m = 1$. Ceci montre (i). Pour ce qui est de (ii), soit $n = \min\{k \in \mathbb{N} \mid \exists Q \in A[X]^G, Q \notin A + (\text{Ker } f)[X] \text{ et } \deg(Q) = k\}$. Soit maintenant $P \in A[X]^G$, $P \notin A + (\text{Ker } f)[X]$, tel que $\deg(P) = n$ et posons $P = \sum_{i=0}^n \alpha_i X^i$. On a $f(\alpha_n) \neq 0$; en effet si $f(\alpha_n) = 0$, alors $n \geq 2$ car sinon P appartiendrait à $A + (\text{Ker } f)[X]$. Cela nous dit que $P' = P - \alpha_n Y^n$ est un élément de $A[X]^G$ qui n'appartient pas à $A + (\text{Ker } f)[X]$, ce qui contredit la définition de n . On a, donc $f(\alpha_n) \neq 0$ ce qui entraîne que $\deg(P) = \deg(\varphi(P)) = \deg(I_f(P)) = n$. Posons $\alpha = \alpha_n$ et soit $Q \in A[X]^G$, $Q = \sum_{j=0}^m \beta_j X^j$ tel que $f(\beta_m) \neq 0$. On a alors $Q \notin A + (\text{Ker } f)[X]$ et

$\deg(P) \leq \deg(Q)$. Il existe donc L_1 et R_1 éléments de $A[X]$, uniques, tels que $\alpha Q = L_1 P + R_1$ et $\deg(R_1) < \deg(P)$. Si $\varphi \in G$, on a les égalités suivantes : $\alpha \varphi(Q) = \varphi(L_1) \varphi(P) + \varphi(R_1) = \varphi(L_1) I_f(P) + \varphi(R_1)$, et comme $\varphi(Q) = I_f(Q)$, on obtient $\varphi(L_1) I_f(P) + \varphi(R_1) = I_f(L_1) I_f(P) + I_f(R_1)$. Puisque $\deg(\varphi(R_1)) < n$ et $\deg(I_f(R_1)) < n$ on a $\varphi(L_1) = I_f(L_1)$ et $\varphi(R_1) = I_f(R_1)$, c'est-à-dire, L_1 et R_1 sont deux éléments de $A[X]^G$, et en particulier $R_1 \in A + (\text{Ker } f)[X]$. Or, si $L_1 \in A + (\text{Ker } f)[X]$ la démonstration est achevée. Par contre si $L_1 \notin A + (\text{Ker } f)[X]$ on répète avec L_1 la démarche précédente concernant Q , et ainsi de suite. On obtient ainsi $\alpha^k Q = P(P(\dots P(L_k P + R_k) + \alpha R_{k-1}) \dots) + \alpha^{k-2} R_2) + \alpha^{k-1} R_1$ où $L_k, R_k, R_{k-1}, \dots, R_1$ appartiennent à $A + (\text{Ker } f)[X]$, ce qui donne $\alpha^k Q = L_k P^k + R_k P^{k-1} + \alpha R_{k-1} P^{k-2} + \dots + \alpha^{k-2} R_2 P + \alpha^{k-1} R_1$, donc $\alpha^k Q \in (A + (\text{Ker } f)[X])[P]$. Finalement soit T un élément quelconque de $A[X]^G$. Si $T \notin A + (\text{Ker } f)[X]$, il est clair que l'on peut écrire $T = T_1 + T_2$ où $T_1 \in A + (\text{Ker } f)[X]$ et $T_2 = \sum_{s=0}^t \gamma_s X^s$ tel que $f(\gamma_t) \neq 0$. Il existe alors $\ell \in \mathbb{N}$ tel que $\alpha^\ell T_2 \in [A + (\text{Ker } f)[X]][P]$, d'où $\alpha^\ell T = \alpha^\ell T_1 + \alpha^\ell T_2$ appartient à $(A + (\text{Ker } f)[X])[P]$.

1.4.4- Remarque. Il est clair que, sous les mêmes conditions du théorème 1.4.3., si l'élément α est inversible, alors $A[X]^G = (A + (\text{Ker } f)[X])[P]$. Si, de plus, l'application f est bijective, le polynôme P peut être déterminé à un scalaire près.

1.4.5- Proposition. Soient $f : A \rightarrow B$ un isomorphisme d'anneaux et φ un élément de $\text{Hom}_f(A[X], B[Y])$ tel que $\varphi(X) = \beta_0 + \beta_1 Y$, où β_1 est un élément inversible de B d'ordre n . On a :

- (i) si $\beta_1^i - 1$ est un élément inversible pour tout i vérifiant $1 \leq i \leq n-1$, alors $A[X]^\varphi \neq A$;
- (ii) si B est un corps, $A[X]^\varphi \neq A$.

En effet, soient $\gamma_0, \gamma_1 \in A$ tels que $f(\gamma_0) = \beta_0$ et $f(\gamma_1) = \beta_1$. On déduit, des hypothèses faites, que $\gamma_1^i - 1$ est un élément inversible pour tout i tel que $1 \leq i \leq n-1$. Soit α un élément non nul de A et posons, pour tout j , $1 \leq j \leq n-1$, $\alpha_{n-j} = (\gamma_1^j - 1)^{-1} \left(\sum_{k=0}^{j-1} \alpha_{n-k} \binom{n-k}{n-j} \gamma_0^{j-k} \right)$, et $\alpha_n = \alpha$. Si $P = \sum_{s=1}^n \alpha_s X^s \in A[X]$, alors, par construction, $P \notin A$ et un calcul simple nous montre que $\varphi(P) = I_f(P)$, d'où $A[X]^\varphi \neq A$. Ceci montre (i). Pour ce qui est de (ii), il suffit d'appliquer (i).

1.5- Le f -produit dans $\text{Hom}_f(A[X], B[Y])$.

Soient f dans $\text{Hom}(A, B)$, φ dans $\text{Hom}_f(A[X], B[Y])$ et ψ dans $\text{End}_B(B[Y])$. On appellera B-endomorphisme associé à φ et on notera φ^f , le B-endomorphisme défini par $\varphi^f(Y) = \varphi(X)$. On appellera f-morphisme associé à ψ et on notera ${}^f\psi$, le f-morphisme défini par ${}^f\psi(X) = \psi(Y)$.

Si f est bijectif, on appellera A-endomorphisme associé à φ et on notera φ_* , le A-endomorphisme défini par $\varphi_*(X) = I_f^{-1}(\varphi(X))$.

1.5.1- Proposition. Soit $f \in \text{Hom}(A, B)$. On a :

- (1) $\varphi = \varphi^f \circ I_f$ pour tout $\varphi \in \text{Hom}_f(A[X], B[Y])$;
- (2) $(I_f)^f = \text{Id}_{B[Y]}$ et ${}^f(\text{Id}_{B[Y]}) = I_f$;
- (3) si f est bijectif, alors $(I_f)_* = \text{Id}_{A[X]}$ et $\varphi_* = I_f^{-1} \circ \varphi^f \circ I_f$;
- (4) pour tout φ élément de $\text{Hom}_f(A[X], B[Y])$ et pour tout ψ élément de $\text{End}_B(B[Y])$, on a ${}^f(\varphi^f) = \varphi$ et $({}^f\psi)^f = \psi$;
- (5) l'application $\varphi \rightarrow \varphi^f$ de $\text{Hom}_f(A[X], B[Y])$ dans $\text{End}_B(B[Y])$ est une bijection dont l'inverse est l'application $\psi \rightarrow {}^f\psi$ où $\psi \in \text{End}_B(B[Y])$;
- (6) si $\varphi \in \text{Hom}_f(A[X], B[Y])$ on a les isomorphismes $\text{Im}(\varphi) \xrightarrow{\sim} A[X]/\text{Ker } \varphi \xrightarrow{\sim} \text{Im}(I_f)/\text{Ker } \varphi^f$;
- (7) si f est bijectif, alors $\text{Ker } \varphi_* = \text{Ker } \varphi$ pour tout φ élément de $\text{Hom}_f(A[X], B[Y])$.

En effet, si φ est un élément de $\text{Hom}_f(A[X], B[Y])$, on a $(\varphi^f \circ I_f)(X) = \varphi^f(I_f(X)) = \varphi^f(Y) = \varphi(X)$, ce qui montre (1). Les égalités $(I_f)^f(Y) = I_f(X) = Y$ et ${}^f(\text{Id}_{B[Y]})(X) = \text{Id}_{B[Y]}(Y) = Y$ montrent (2). Si f est bijectif, on a $(I_f)_*(X) = I_f^{-1}(I_f(X)) = X$ ce qui montre (3). Pour montrer (4) notons que ${}^f(\varphi^f)(X) = \varphi^f(Y) = \varphi(X)$ et $({}^f\psi)^f(Y) = {}^f\psi(X) = \psi(Y)$ pour tout $\varphi \in \text{Hom}_f(A[X], B[Y])$ et $\psi \in \text{End}_B(B[Y])$. Il est clair que (5) découle de (2) et (4). Pour ce qui est de (6), soit g l'application de $A[X]/\text{Ker } \varphi$ dans $\text{Im}(I_f)/\text{Ker } \varphi^f$ définie par $g(P + \text{Ker } \varphi) = I_f(P) + \text{Ker } \varphi^f$. L'application g est bien définie: $P_1 + \text{Ker } \varphi = P_2 + \text{Ker } \varphi$ entraîne $\varphi(P_1 - P_2) = 0$ d'où $\varphi(P_1) = \varphi(P_2)$ soit encore $\varphi^f(I_f(P_1)) = \varphi^f(I_f(P_2))$ et, par suite, $I_f(P_1) - I_f(P_2) \in \text{Ker } \varphi^f$. Il est clair que g est une application surjective. Finalement, si $g(P + \text{Ker } \varphi) = 0$, on a $I_f(P) \in \text{Ker } \varphi^f$ ce qui entraîne $\varphi(P) = 0$, d'où $P \in \text{Ker } \varphi$, donc g est injective. Pour ce qui est de (7), on sait que $\varphi_* = I_f^{-1} \circ \varphi$, donc $\varphi_*(P) = 0$ si et seulement si $\varphi(P) = 0$.

Soient f dans $\text{Hom}(A, B)$ et φ_1, φ_2 deux éléments de $\text{Hom}_f(A[X], B[Y])$. On appellera f -produit (ou f -composé) de φ_1 par φ_2 le f -morphisme de $A[X]$ dans $B[Y]$, noté $\varphi_2 \circ_f \varphi_1$, défini par $(\varphi_2 \circ_f \varphi_1)(X) = \varphi_2^f(\varphi_1(X))$. Il s'ensuit que si $\varphi_1(X) = \sum_{i=0}^n \alpha_i Y^i$ et $\varphi_2(X) = \sum_{j=0}^m \beta_j Y^j$, alors $(\varphi_2 \circ_f \varphi_1)(X) = \sum_{i=0}^n \alpha_i (\sum_{j=0}^m \beta_j Y^j)^i$.

1.5.2- Proposition. Soit f dans $\text{Hom}(A, B)$. On a :

- (i) $\varphi \circ_f I_f = I_f \circ_f \varphi = \varphi$ pour tout $\varphi \in \text{Hom}_f(A[X], B[Y])$;
- (ii) si $\varphi_1, \varphi_2 \in \text{Hom}_f(A[X], B[Y])$, alors $(\varphi_1 \circ_f \varphi_2)^f = \varphi_1^f \circ \varphi_2^f$;
- (iii) si $\psi_1, \psi_2 \in \text{End}_B(B[Y])$, alors ${}^f(\psi_1 \circ \psi_2) = {}^f\psi_1 \circ_f {}^f\psi_2$.

En effet, si φ est un f -morphisme de $A[X]$ dans $B[Y]$, on a $\varphi \circ_f I_f = {}^f\varphi \circ I_f = \varphi$ et $I_f \circ_f \varphi = (I_f)^f \circ \varphi = \text{Id}_{B[Y]} \circ \varphi = \varphi$, ce qui montre (i). Pour ce qui est de (ii), notons que $(\varphi_1 \circ_f \varphi_2)^f(Y) = (\varphi_1 \circ_f \varphi_2)(X) = \varphi_1^f(\varphi_2(X)) = \varphi_1^f(\varphi_2^f(Y)) = (\varphi_1^f \circ \varphi_2^f)(Y)$.

Finalement, montrons (iii). On a ${}^f(\psi_1 \circ \psi_2)(X) = (\psi_1 \circ \psi_2)(Y) = \psi_1(\psi_2(Y)) = ({}^f\psi_1)^f \circ \psi_2(Y) = (({}^f\psi_1)^f \circ {}^f\psi_2)(X) = ({}^f\psi_1 \circ_f {}^f\psi_2)(X)$.

1.5.3- Proposition. Soient f un élément de $\text{Hom}(A, B)$, G un sous-groupe (pour le f -produit) de $\text{Hom}_f(A[X], B[Y])$ et H un sous-groupe de $\text{End}_B(B[Y])$. Posons $G^f = \{\varphi^f / \varphi \in G\}$ et ${}^fH = \{{}^f\psi / \psi \in H\}$. Alors G^f est un sous-groupe de $\text{End}_B(B[Y])$, fH est un sous-groupe de $\text{Hom}_f(A[X], B[Y])$ et les applications $G \rightarrow G^f, \varphi \rightarrow \varphi^f$ et $H \rightarrow {}^fH, \psi \rightarrow {}^f\psi$ sont des isomorphismes de groupes.

En effet, compte tenu des résultats précédents, il ne nous reste qu'à démontrer que $(\varphi^{-1})^f = (\varphi^f)^{-1}$ pour tout $\varphi \in G$ et ${}^f(\psi^{-1}) = ({}^f\psi)^{-1}$ pour tout $\psi \in H$. Pour cela, notons que $I_f = \varphi^{-1} \circ_f \varphi$, donc $\text{Id}_{B[Y]} = (I_f)^f = (\varphi^{-1} \circ_f \varphi)^f = (\varphi^{-1})^f \circ \varphi^f$, ce qui entraîne que $(\varphi^f)^{-1} = (\varphi^{-1})^f$. Le même type de raisonnement nous montre que ${}^f(\psi^{-1}) = ({}^f\psi)^{-1}$ pour tout $\psi \in \text{End}_B(B[Y])$.

1.5.4- Proposition. Soient $f : A \rightarrow B$ un isomorphisme d'anneaux et φ un f -morphisme de $A[X]$ dans $B[Y]$. Le diagramme

$$\begin{array}{ccc} A[X] & \xrightarrow{\varphi} & B[Y] \\ \varphi_* \downarrow & & \downarrow \varphi^f \\ A[X] & \xrightarrow{\varphi} & B[Y] \end{array}$$

est commutatif.

En effet, $\varphi^f \circ \varphi = (\varphi \circ I_f^{-1}) \circ \varphi = \varphi \circ (I_f^{-1} \circ \varphi) = \varphi \circ \varphi_*$.

1.5.5- Proposition. Soient $f \in \text{Hom}(A, B)$, f bijectif et G un sous-groupe de $\text{Hom}_f(A[X], B[Y])$. Posons $G_* = \{\varphi_* / \varphi \in G\}$. L'application $G \rightarrow G_*$, $\varphi \mapsto \varphi_*$ est alors un isomorphisme de groupes.

En effet, on sait déjà que $(I_f)_* = \text{Id}_{A[X]}$. Par ailleurs, soient $\varphi_1, \varphi_2 \in \text{Hom}_f(A[X], B[Y])$. On a $(\varphi_1 \circ_f \varphi_2)_* = I_f^{-1} \circ (\varphi_1 \circ_f \varphi_2) = I_f^{-1} \circ (\varphi_1^f \circ \varphi_2) = (I_f^{-1} \circ \varphi_1^f) \circ \varphi_2 = (I_f^{-1} \circ (\varphi_1 \circ I_f^{-1})) \circ \varphi_2 = (I_f^{-1} \circ \varphi_1) \circ (I_f^{-1} \circ \varphi_2) = (\varphi_1)_* \circ (\varphi_2)_*$.

1.5.6- Proposition. Soient $f \in \text{Hom}(A, B)$ et G un sous-groupe de $\text{Hom}_f(A[X], B[Y])$. Alors $A[X]^G = I_f^{-1}(B[Y]^{G^f})$.

En effet, si $P \in A[X]^G$, on a $\varphi(P) = I_f(P)$ pour tout $\varphi \in G$, donc $\varphi^f(I_f(P)) = I_f(P)$, ce qui montre que $P \in I_f^{-1}(B[Y]^{G^f})$. Réciproquement, si $Q \in I_f^{-1}(B[Y]^{G^f})$, on a $\varphi^f(I_f(Q)) = I_f(Q)$ pour tout $\varphi \in G$, d'où $\varphi(Q) = I_f(Q)$ pour tout $\varphi \in G$.

On rappelle le résultat suivant, dû à P. Samuel (cf. [2]) : Soient A un anneau commutatif, intègre et unitaire et G un groupe fini de A -automorphismes de $A[X]$. Alors $A[X]^G = A[\bigcup_{\sigma \in G} \sigma(X)]$.

1.5.7- Corollaire. Soient $f : A \rightarrow B$ un isomorphisme d'anneaux et G un sous-groupe fini de $\text{Hom}_f(A[X], B[Y])$. Alors $A[X]^G = A[\prod_{\varphi \in G} \varphi_*(X)]$.

En effet, on sait que $A[X]^G = I_f^{-1}(B[Y]^{G^f})$ et comme G est fini, il en est de même de G^f , donc $B[Y]^{G^f} = B[\prod_{\varphi \in G} \varphi^f(Y)]$. Comme f est bijectif, il en est de même de I_f , donc $A[X]^G = f^{-1}(B)[\prod_{\varphi \in G} (I_f^{-1} \circ \varphi^f)(Y)] = A[\prod_{\varphi \in G} \varphi_*(X)]$.

Finalement, on étudiera l'ensemble $A[X]^G$ quand G est un groupe infini de f -morphisms de $A[X]$ dans $B[Y]$ et pour ce faire, on utilisera le résultat suivant dû à B. Costillon (cf. [5]) : soient A un anneau commutatif, intègre et unitaire et G un groupe infini de A -automorphismes de $A[X]$. Alors $A[X]^G = A$.

1.5.8- Proposition. Soient $f \in \text{Hom}(A, B)$ et G un sous-groupe infini de $\text{Hom}_f(A[X], B[Y])$. Alors $A[X]^G = A + (\text{Ker } f)[X]$.

En effet, on sait que l'application $\varphi \rightarrow \varphi^f$ de G dans G^f est injective, donc G infini entraîne G^f infini. On a donc $B[Y]^{G^f} = B$ et, par suite, $A[X]^G = I_f^{-1}(B) = A + (\text{Ker } f)[X]$.

Note. Les techniques ci-dessus développées peuvent être étendues aux séries formelles (voir [7] pour le cas d'une variable) et aux séries formelles restreintes (voir [8] pour le cas d'une variable).

2 - Sur la structure des groupes finis de A-automorphismes de $A[X]$

Cette partie de notre travail est une étude simple et naïve qui analyse la structure des groupes finis des A-automorphismes de $A[X]$, A étant un anneau unitaire, intègre et commutatif.

Soit A un anneau commutatif, intègre et unitaire. On rappelle que, étant donné un A-automorphisme φ de $A[X]$, alors $\varphi(X) = \alpha + \beta X$ avec α, β des éléments de A et $\beta \in U(A)$ (cf. [1]).

Si G est un groupe fini de A-automorphismes de $A[X]$, soit g l'application de G dans A définie par $g(\varphi) = \beta$ où $\varphi \in G$ est tel que $\varphi(X) = \alpha + \beta X$. Il est clair que g ainsi défini est un morphisme multiplicatif de G dans $(A, \cdot)$. Si l'on pose $G_0 = g(G)$ on voit que G_0 est un sous-groupe de $(A, \cdot)$ et la suite $0 \rightarrow \text{Ker}(g) \rightarrow G \rightarrow G_0 \rightarrow 0$ est exacte. Or, on sait que les seuls sous-groupes multiplicatifs d'un corps sont les groupes cycliques (cf. [6]), d'où on déduit que les seuls sous-groupes multiplicatifs finis d'un anneau intègre - par passage au corps des fractions - sont les groupes cycliques. Cela nous dit que G_0 est cyclique isomorphe à $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ pour n convenable, $n \in \mathbb{N}$. Posons $G_0 = \langle \beta \rangle$, $\beta \in U(A)$ et soit φ un élément de G tel que $g(\varphi) = \beta$ (i.e. $\varphi(X) = \alpha + \beta X$). Comme $\text{Ker}(g)$ est un sous-groupe formé par les éléments ψ de G de la forme $\psi(X) = \gamma + X$ on a $\varphi \circ \psi \circ \varphi^{-1} \in \text{Ker}(g)$, donc le sous-groupe $\langle \varphi \rangle$ opère sur $\text{Ker}(g)$ par des automorphismes intérieures d'où on déduit le résultat suivant :

2.1. Proposition. Sans les conditions précédentes, G est le produit semi-direct de $\text{Ker}(g)$ par $\langle \varphi \rangle$.

On notera : $G = \text{Ker}(g) \ltimes \langle \varphi \rangle$.

Mais on sait que $\langle \varphi \rangle$ est isomorphe à $\mathbb{Z}_n$ pour un entier n convenable, $n \in \mathbb{N}$ et comme $\text{Ker}(g)$ est réduit à l'élément neutre si la caractéristique de l'anneau est zéro, on a :

2.2. Proposition. Soit A un anneau de caractéristique zéro. Alors tout sous-groupe fini du groupe des A -automorphismes de $A[X]$ est cyclique.

Supposons maintenant que $\text{carac}(A) = p > 0$ et soit ψ un A -automorphisme de la forme $\psi(X) = \gamma + X$. Il est clair que l'ordre de ψ est p , d'où on déduit :

2.3. Proposition. Soit G un groupe fini de A -automorphismes de $A[X]$ où A est un anneau de caractéristique p . Si l'ordre $\sigma(G)$ de G est plus petit ou égal à p , G est cyclique. Plus précisément, si $\sigma(G) < p$ alors $\text{Ker}(g)$ est réduit à l'élément neutre ; si $\sigma(G) = p$, $G = \text{Ker}(g)$.

Si $\text{carac}(A) = p$ on sait que tout élément de $\text{Ker}(g)$ à ordre p , d'où on déduit que $\text{Ker}(g)$ est isomorphe à $(\mathbb{Z}_p)^m$ pour un entier m convenable $m \in \mathbb{N}$. De plus si $\beta \in A$ est tel que $\beta^p = 1$ alors $\beta = 1$. Ainsi, si l'on note $\mathbb{Z}_0 = \{0\}$, on a :

2.4. Proposition : Soit G un sous-groupe fini du groupe des A -automorphismes de $A[X]$. Alors G est isomorphe au produit semi-direct de $(\mathbb{Z}_p)^m$ par $\mathbb{Z}_n$ où $p = \text{carac}(A)$, $n, m \in \mathbb{N}$ et n et p premiers entre eux.

2.5. Proposition. Soit G un sous-groupe fini du groupe des A -automorphismes de $A[X]$. Alors l'ordre de G est paire si et seulement si il existe $\varphi \in G$ tel que $\varphi^2 = \text{id}_{A[X]}$.

En effet, on sait que G est isomorphe au produit semi-direct $(\mathbb{Z}_p)^m \rtimes \mathbb{Z}_n$ où $p = \text{carac}(A)$, $n, m \in \mathbb{N}$ et $(p, n) = 1$, donc l'ordre de G est égal à $n.p^m$. Il suffit un simple calcul sur le nombre $n.p^m$ pour aboutir à l'énoncé de la proposition.

REFERENCES

- [1] R. Gilmer, "R-automorphismes of $R[X]$ ", Proc. London Math. Soc. 18 (1968), 328-336.
- [2] P. Samuel, "Groupes finis d'automorphismes des anneaux de séries formelles", Bull. Sc. Math. France 2ème série, 90 (1966), 97-101.
- [3] M. Nagata, "On automorphisms group of $K[X,Y]$ ", Math., Kyoto Univ. Konokuniga, Tokio, 1972.
- [4] S. Abhyankar, W. Heinzer et P. Eakin, "On the uniqueness of the coefficient ring in polynomial rings", J. Algebre 23 (1972), 310-342.
- [5] B. Costillon, "Réciproque à un théorème de Samuel", C.R. Acad. Sc. Paris, t. 283, série A, 141-142.
- [6] P. Samuel, "Théorie algébrique des nombres", Hermann, Paris 1967.
- [7] R. Gilmer, "R-automorphismes de $R[[X]]$ ", Michigan Math. 17 (1970), 15-21.
- [8] J. B. Castillon et A. Micali, "A-endomorphismes de $A\{X\}$ ", Manuscripta Mathematica 25 (1978), 249-261.