COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

Chapitre 2 Polynômes et fonctions polynomiales à plusieurs variables sur un corps fini

Cours de l'institut Fourier, tome 4 (1971), p. 1-7

<http://www.numdam.org/item?id=CIF_1971__4__A2_0>

© Institut Fourier – Université de Grenoble, 1971, tous droits réservés.

L'accès aux archives de la collection « Cours de l'institut Fourier » 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/

Chapitre 2

Polynômes et fonctions polynomiales à plusieurs variables sur un corps fini

Dans tout ce chapitre (et dans le suivant), K désignera un corps fini à $q = p^f$ éléments, n un entier strictement positif, $X = (X_1, \ldots, X_n)$ un système de n indéterminées sur K, et $K[X] = K[X_1, \ldots, X_n]$ l'anneau des polynômes en $X_1, \ldots, X_n$ à coefficients dans K ; les éléments $x = (x_1, \ldots, x_n)$ de K^n seront qualifiés éventuellement de points (ou de vecteurs ...); si $F \in K[X]$, on appellera fonction polynomiale associée à F l'application $x \longmapsto F(x)$ (ou, plus explicitement, $(x_1, \ldots, x_n) \longmapsto F(x_1, \ldots, x_n)$) de K^n dans K.

(2.1). Polynômes réduits et polynômes identiquement nuls.

Définition 1. - On notera $\mathcal{U}$ l'idéal de l'anneau $K[X]$ engendré par les n polynômes $X_i^q - X_i$ ($i = 1, 2, \ldots, n$).

Définition 2. - Etant donné $F \in K[X]$, on dira que F est

réduit si son degré par rapport à chacune des n variables X_i est inférieur ou égal à $q - 1$;

identiquement nul si sa fonction polynomiale associée est nulle (autrement dit si $F(x) = 0$ pour tout $x \in K^n$) ;

on notera respectivement R et I les sous-ensembles de $K[X]$ formés

des polynômes réduits et des polynômes identiquement nuls.

Il est clair que R est un sous-espace vectoriel de $K[X]$, et que I est un idéal de $K[X]$; en outre, chaque polynôme $X_i^q - X_i$ étant identiquement nul, on a l'inclusion $\mathcal{N} \subset I$: nous verrons plus loin qu'il y a en fait égalité.

Lemme 1. - Pour tout $F \in K[X]$, il existe un polynôme réduit $G \in K[X]$ tel que l'on ait $F \equiv G \pmod{\mathcal{N}}$.

Démonstration. Par linéarité, on peut se ramener au cas où F est un monôme $X_1^{d_1} X_2^{d_2} \dots X_n^{d_n}$; pour tout i, posons

r_i = le reste de division par q de d_i', où d_i' est défini par la double condition $d_i = q^h . d_i'$, $(q, d_i') = 1$.

Il est clair alors que

$$X_1^{d_1} X_2^{d_2} \dots X_n^{d_n} \equiv X_1^{r_1} X_2^{r_2} \dots X_n^{r_n} \pmod{\mathcal{N}},$$

et que le monôme de droite est réduit: le lemme est donc démontré.

Lemme 2. - Si un polynôme réduit F est en même temps identiquement nul, alors il est nul (c'est-à-dire "formellement nul": tous ses coefficients sont nuls).

Démonstration. On raisonne par récurrence sur n.

I) La propriété est vraie pour $n = 1$. Soit en effet $F(X_1)$ un polynôme réduit et identiquement nul par rapport à l'unique variable X_1 : d'une part il est de degré $\leq q - 1$, et d'autre part il admet pour racines les q éléments de K : le nombre de racines de $F(X_1)$ est donc strictement supérieur à son degré, d'où $F(X_1) = 0$, c.q.f.d.

II) Si la propriété est vraie pour $n-1$ variables ($n \geqslant 2$), elle est encore vraie pour n variables. Soit en effet F un polynôme réduit à n variables; on peut écrire

$$F(X_1, X_2, \ldots, X_n) = F_0(X_2, \ldots, X_n) + F_1(X_2, \ldots, X_n) X_1 + \ldots$$
$$\ldots + F_{q-1}(X_2, \ldots, X_n) X_1^{q-1},$$

les F_j étant q polynômes réduits à $n-1$ variables $X_2, \ldots, X_n$. Dire que F est identiquement nul équivaut alors à dire que, quel que soit $(x_2, \ldots, x_n) \in K^{n-1}$, le polynôme réduit et à une seule variable X_1 :

$$F_0(x_2, \ldots, x_n) + F_1(x_2, \ldots, x_n) X_1 + \ldots + F_{q-1}(x_2, \ldots, x_n) X_1^{q-1},$$

est identiquement nul; d'après la première partie de la démonstration, il est donc nul; autrement dit, on a (quel que soit $(x_2, \ldots, x_n) \in K^{n-1}$, rappelons-le)

$$F_0(x_2, \ldots, x_n) = F_1(x_2, \ldots, x_n) = \ldots = F_{q-1}(x_2, \ldots, x_n) = 0 ;$$

ceci signifie que les polynômes F_j (réduits) sont eux-mêmes identiquement nuls: comme ils ne contiennent que $n-1$ variables, l'hypothèse de récurrence donne alors $F_0 = F_1 = \ldots = F_{q-1} = 0$, donc $F = 0$, c.q.f.d.

Lemme 3. - En tant qu'espace vectoriel, $K[X]$ est somme directe de ses sous-espaces R et $\mathcal{U}$, soit

$$K[X] = R \oplus \mathcal{U}. \tag{1}$$

Démonstration. Le lemme 1 peut s'écrire

$$K[X] = R + \mathcal{U} ; \tag{2}$$

d'autre part, le lemme 2 peut s'écrire $R \cap I = \{0\}$, ce qui implique,

puisque $\mathfrak{r} \subset I$, que

(3) $$R \cap \mathfrak{r} = \{0\} ;$$

(1) résulte alors immédiatement de (2) et de (3).

Théorème 1. - Soit $F \in K[X]$ un polynôme.

(i) Il existe un polynôme réduit F^* et un seul tel que $F \equiv F^* \pmod{\mathfrak{r}}$.

(Ceci servira de définition de la notation F^*).

(ii) Les trois assertions suivantes sont équivalentes:

(a) F est identiquement nul (c'est-à-dire $F \in I$);

(b) $F^* = 0$;

(c) $F \in \mathfrak{r}$.

(iii) En particulier, $\mathfrak{r} = I$.

Démonstration. (i) C'est une simple reformulation du lemme 3.

(ii) Ecrivons $F = F^* + H$, $F^* \in R$, $H \in \mathfrak{r}$; comme $\mathfrak{r} \subset I$, F est identiquement nul si et seulement si F^* est lui-même identiquement nul; l'implication de (a) vers (b) résulte alors du lemme 2; celle de (b) vers (c) résulte de la définition de H (donc en fait du lemme 3); enfin, celle de (c) vers (a) résulte de l'inclusion $\mathfrak{r} \subset I$.

(iii) D'après (ii), l'assertion (a): $F \in I$, équivaut à l'assertion (c): $F \in \mathfrak{r}$; d'où $\mathfrak{r} = I$.

(2.3). Fonctions polynomiales sur K^n.

Soient A l'ensemble (en fait, la K-algèbre) de toutes les applications de K^n dans K, et $\varphi : K[X] \longrightarrow A$ l'homomorphisme de K-algèbres qui, à tout polynôme $F \in K[X]$, fait correspondre la fonction

polynomiale associée à F .

Lemme 4. - Le noyau de φ est l'idéal $\mathfrak{a}$ de $K[X]$.

Démonstration. Par définition même, ce noyau est I , et nous venons de voir (théorème 1, (iii)) que $I = \mathfrak{a}$.

Lemme 5. - L'homomorphisme φ est surjectif.

Démonstration. Les lemmes 3 et 4 montrent que $\Phi = \varphi(K[X])$ est un espace vectoriel isomorphe à R ; comme R admet pour base sur K l'ensemble des monômes réduits, et qu'il y a exactement q^n tels monômes, on a $\dim_K(\Phi) = \dim_K(R) = q^n$, et par conséquent

$$\mathrm{card}(\Phi) = q^{q^n} .$$

D'autre part, il est clair que

$$\mathrm{card}(A) = \mathrm{card}(K)^{\mathrm{card}(K^n)} = q^{q^n} ;$$

$\Phi = \varphi(K[X])$ et A ont donc le même nombre d'éléments, d'où l'égalité de ces deux ensembles et le fait que φ est surjectif.

Remarque. - On peut donner du lemme 5 une autre démonstration, indépendante des résultats du §(2.1), et qui montre mieux ce qui se passe. Pour tout $a = (a_1, \dots, a_n) \in K^n$, notons f_a la fonction caractéristique de a à valeurs dans K , définie par $f_a(x) = 1$ si $x = a$, et $f_a(x) = 0$ si $x \neq a$; la famille $(f_a)_{a \in K^n}$ est visiblement une base de A sur K ; il suffit donc, pour prouver le lemme 5, de montrer que chaque f_a est une fonction polynomiale: or, si on pose

$$F_a(X) = \prod_{i=1}^{n} \left(1 - (X_i - a_i)^{q-1} \right) , \tag{4}$$

on vérifie sans peine que $\varphi(F_a) = f_a$ (utiliser le théorème 2 du §(1.2), et plus précisément le fait que si $x \in K$, alors $x^{q-1} = 0$ ou 1 selon que $x = 0$ ou que $x \neq 0$).

Théorème 2. - Soit f une application (quelconque) de K^n dans K : il existe un polynôme réduit F et un seul tel que f soit la fonction polynomiale associée à F.

Démonstration. Il suffit d'utiliser les lemmes 4 et 5, qui montrent que φ donne lieu à un isomorphisme $K[X]/\mathfrak{r} \xrightarrow{\sim} A$, et le lemme 3, selon lequel $K[X] = R \oplus \mathfrak{r}$.

Remarque. - Ce polynôme réduit F est donné explicitement par la formule

$$F(X) = \sum_{a \in K^n} f(a)\, F_a(X) \quad , \tag{5}$$

(F_a étant défini en (4)): en effet, il est clair que la fonction polynomiale associée à ce polynôme est précisément f, et par ailleurs ce polynôme est réduit, puisque chaque F_a est visiblement réduit.

(2.3). Somme de toutes les valeurs prises par un polynôme.

Théorème 3. - Soit $F \in K[X] = K[X_1, \ldots, X_n]$ un polynôme de degré total d ; alors, si $d < n(q-1)$, on a

$$\sum_{x \in K^n} F(x) = 0 \quad . \tag{6}$$

Démonstration. Par linéarité, on peut se ramener au cas où F est un monôme, disons

$$F(X) = X_1^{d_1} X_2^{d_2} \ldots X_n^{d_n} \quad ,$$

avec $d_1 + d_2 + \ldots + d_n < n(q-1)$; on a alors

$$(7) \qquad \sum_{x \in K^n} F(x) = \prod_{i=1}^{n} \sum_{x_i \in K} x_i^{d_i} ,$$

et l'inégalité relative au degré total de F montre que pour un i au moins, on a $d_i < q - 1$; il suffit évidemment de montrer que, dans (7), le facteur correspondant du produit, à droite, est nul, et on est ainsi ramené à prouver simplement le lemme suivant:

Lemme 6. - Soit d un entier tel que $0 \leq d < q - 1$; alors

$$(8) \qquad \sum_{x \in K} x^d = 0 .$$

Démonstration. Si $d = 0$, on a affaire à une somme de q termes tous égaux à 1 , dans le corps K dont la caractéristique p divise $q = p^f$: cette somme est donc bien nulle. Considérons maintenant le cas général où $0 < d < q - 1$; comme K^* contient $q - 1$ éléments, mais au plus d racines $d^{\text{ièmes}}$ de l'unité, il existe au moins un $y \in K^*$ tel que

$$(9) \qquad y^d \neq 1 ;$$

comme l'application $x \longmapsto yx$ de K^* dans K^* est une bijection de ce groupe sur lui-même, on peut écrire

$$\sum_{x \in K} x^d = \sum_{x \in K} (yx)^d = y^d \sum_{x \in K} x^d ,$$

et par conséquent

$$(y^d - 1) \sum_{x \in K} x^d = 0 ;$$

il suffit alors de simplifier par le facteur $(y^d - 1)$, comme l'inégalité (9) nous le permet, pour obtenir l'égalité (8) cherchée.