COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

Chapitre 4 Formes additives sur un corps fini

Cours de l'institut Fourier, tome 4 (1971), p. 1-8

<http://www.numdam.org/item?id=CIF_1971__4__A4_0>

Chapitre 4

Formes additives sur un corps fini

Soient K un corps, n et d deux entiers ≥ 1, et $F \in K[X] = K[X_1, \ldots, X_n]$ une forme de degré d, c'est-à-dire un polynôme homogène et degré total d, par rapport à $X_1, \ldots, X_n$. Il est clair que $F(0, \ldots, 0) = 0$, donc que l'origine de K^n est un zéro (trivial!) de F ; si F admet un <u>zéro non trivial</u>, autrement dit, si F s'annule en un point de K^n différent de l'origine, on dit que F est <u>isotrope</u>. Dans un autre ordre d'idées, si F ne comporte que des monômes <u>purs</u>, c'est-à-dire du type $a_i X_i^d$, on dit que F est une forme <u>additive</u> (ou encore diagonale): une forme additive s'écrit donc

$$(1) \qquad F(X) = a_1 X_1^d + a_2 X_2^d + \ldots + a_n X_n^d .$$

Le but de ce (court) chapitre 4 est d'étudier certaines propriétés des formes additives sur un <u>corps fini</u> K sans utiliser les résultats des chapitres 2 et 3; en fait, la finitude du corps K interviendra surtout par l'intermédiaire des deux propriétés suivantes (on désigne comme d'habitude par p et $q = p^f$ la caractéristique et le nombre d'éléments de K):

(I) Dans K, l'élément -1 est somme de puissances $d^{\text{ièmes}}$.

(En effet, puisqu'on est en caractéristique p, $-1 = \underbrace{1^d + \ldots + 1^d}_{p-1 \text{ fois}}$).

(II) Le groupe quotient K^*/K^{*d} est d'ordre fini.

Ces deux propriétés ne sont pas l'apanage des corps finis; les corps p-adiques, par exemple, les possèdent également: ainsi, le théorème 2, énoncé et démontré au § (4.2) ci-dessous, est valable, mutatis mutandis, pour un corps p-adique; nous reviendrons sur ce point en remarque.

(4.1). Sommes de puissances $d^{\text{ièmes}}$ dans un corps fini.

Soit d un exposant $\geqslant 1$, et soit K un corps possédant la propriété (I), par exemple un corps fini; désignons par K_d le sous-ensemble de K formé des sommes de puissances $d^{\text{ièmes}}$, c'est-à-dire des éléments du type

$$x_1^d + x_2^d + \dots + x_n^d \quad , \tag{2}$$

avec $n \geqslant 1$, d'ailleurs quelconque, et $x_1, x_2, \dots, x_n \in K$. Il est clair que K_d est un sous-corps de K : en effet, K_d est stable pour l'addition, la multiplication et le passage à l'opposé (à cause de (I)); il contient 0 et 1 ; enfin, si $x \neq 0$ est un élément de K_d, on a également $x^{-1} \in K_d$, puisque $x^{-1} = x^{d-1}(x^{-1})^d$, que $(x^{-1})^d$ (qui est une puissance $d^{\text{ième}}$) appartient à K_d, et que K_d est stable pour la multiplication. Voyons ce qu'on peut dire de plus lorsque K est un corps fini.

Théorème 1. - Soient K un corps fini à $q = p^f$ éléments, d un entier $\geqslant 1$, et posons

(3) $\overline{d} = (q-1, d)$ (le plus grand commun diviseur de $q-1$ et d);

(4) $[q ; d]$ = la plus petite puissance p^g de p ayant les deux propriétés suivantes:

1/ g divise f ;

2/ le quotient $(p^f - 1)/(p^g - 1)$ divise d .

Alors

(i) K_d est l'unique sous-corps de K contenant exactement $[q ; d]$ éléments: $K_d = F_{[q ; d]}$.

(ii) Tout élément de K_d est somme d'au plus $\overline{d}$ puissances $d^{\text{ièmes}}$ (et a fortiori d'au plus d puissances $d^{\text{ièmes}}$).

Démonstration. (i) K^* est un groupe cyclique d'ordre $q - 1$, et ses sous-groupes correspondent donc bijectivement aux diviseurs positifs de $q - 1$. D'autre part, K étant un corps fini à p^f éléments, ses sous-corps correspondent bijectivement aux diviseurs positifs de f (voir chapitre 1, remarque 3 suivant le théorème 5). Comme les deux assertions " g divise f " et " $p^g - 1$ divise $p^f - 1$ " sont équivalentes (petit exercice d'arithmétique...), on peut énoncer la propriété suivante:

Lemme. - Pour qu'un sous-groupe H de K^* soit de la forme L^* , L étant un sous-corps de K , il faut et il suffit que l'ordre de H soit de la forme $p^g - 1$, g divisant f .

Par ailleurs, le groupe K^{*d} est d'ordre $(q - 1)/\overline{d}$ (chapitre 1, théorème 4, (ii)) et K_d est le plus petit sous-corps L de K tel que $K^{*d} \subset L$, ou encore que $K^{*d} \subset L^*$. Appliquons le lemme: $K_d = F_{p^h}$, h étant le plus petit diviseur positif g de f tel que

$$(q - 1)/\overline{d} \quad \text{divise} \quad p^g - 1 \ ,$$

ce qui équivaut évidemment (puisque $q = p^f$) à

$$(p^f - 1)/(p^g - 1) \quad \text{divise le p.g.c.d.} \quad \overline{d} \ ,$$

assertion elle-même équivalente à

$$(p^f - 1)/(p^g - 1) \quad \text{divise} \quad d \ ;$$

ceci prouve (i).

(ii) Pour tout $n \geqslant 1$, désignons par S_n l'ensemble des éléments de K^* qui sont de la forme $x_1^d + x_2^d + \ldots + x_n^d$ (les $x_i \in K$, certains x_i éventuellement nuls). Il est clair que

$$(5) \qquad K^{*d} = S_1 \subset S_2 \subset \ldots \subset S_n \subset S_{n+1} \subset \ldots ,$$

et que, dans le groupe K^*, chaque ensemble S_n est <u>saturé modulo</u> K^{*d}, c'est-à-dire invariant (globalement) par la multiplication par un élément de K^{*d}, donc réunion d'un certain nombre de classes de K^* modulo K^{*d}. Comme K^*/K^{*d} est d'ordre $\bar{d}$ (K^* est en effet d'ordre $q - 1$, et K^{*d} d'ordre $(q - 1)/\bar{d}$: voir chapitre 1), la suite (5) présente certainement <u>au plus</u> $\bar{d} - 1$ inclusions <u>strictes</u>. D'autre part, un raisonnement par récurrence sans malice montre que si, pour une valeur N de l'indice, on a $S_N = S_{N+1}$, alors, pour tout $n \geqslant N$, on a également $S_n = S_{n+1}$: il en résulte que dans la suite (5), les inclusions strictes occupent les premières places. On déduit de ces deux remarques que nécessairement

$$\ldots \subset S_{\bar{d}} = S_{\bar{d}+1} = \ldots ,$$

donc que tout élément de K_d^* (et aussi de K_d) est somme de $\bar{d}$ puissances $d^{\text{ièmes}}$, ce qui prouve (ii).

<u>Remarque 1</u>. - Il est facile de voir que l'inégalité $[q \ ; d] < q$ implique l'inégalité $q < d^2$: pour d donné, il n'existe donc qu'un <u>nombre fini</u> de corps finis $K = F_q$ tels que $K_d \neq K$; ce phénomène: $K_d \neq K$, est "pathologique" et ne se produit que lorsque K est "trop petit". On

peut d'ailleurs montrer que si K est un corps parfait infini satisfaisant à la condition (I) (-1 est somme de puissances $d^{\text{ièmes}}$), alors on a toujours $K_d = K$ (voir par exemple [10] , théorème (2.8)).

Voici la situation la plus simple où l'on ait $K_d \neq K$: $K = F_4$, $d = 3$; on a alors $K_d = F_2$.

Remarque 2. - La démonstration de (ii) a utilisé uniquement le fait que le groupe quotient K^*/K^{*d} est d'ordre $\overline{d}$. Cette méthode de démonstration est donc applicable à certains corps infinis K tels que le groupe K^*/K^{*d} soit fini: on peut ainsi prouver immédiatement que tout élément du corps p-adique Q_p (p premier impair) est somme de quatre carrés.

(4.2). Représentation d'éléments d'un corps fini par une forme additive.

Soit $F = F(X_1 , \dots , X_n)$ une forme de degré d sur un corps quelconque K . Si $a \in K^*$ et si F représente a (c'est-à-dire s'il existe $x = (x_1 , \dots , x_n) \in K^n$ tel que $F(x) = a$), alors, par homogénéité, F représente également tout élément de aK^{*d} , qui est la classe de a (modulo K^{*d}) dans le groupe multiplicatif K^* : on dit que F représente la classe aK^{*d} .

Proposition 1 (Demy'anov: voir [4]). - Soit K un corps possédant la propriété (I) (-1 est somme de puissances $d^{\text{ièmes}}$), par exemple un corps fini, et soit $F(X) = a_1X_1^{\,d} + a_2X_2^{\,d} + \dots + a_nX_n^{\,d}$ une forme additive de degré d , à n variables, à coefficients dans K . Alors, si F est non isotrope, F représente au moins n classes distinctes modulo K^{*d} . (Noter que si F est non isotrope, tous les a_i sont

certainement différents de 0 , et les n variables X_i figurent effectivement dans F).

Démonstration. Par récurrence sur le nombre de variables. Pour $n = 1$, F représente la classe $a_1 K^{*d}$, et la propriété est vraie. Supposons donc la proposition démontrée pour $n - 1$ variables et prouvons-la pour n variables. Posons $G(X) = a_1 X_1^d + a_2 X_2^d + \ldots + a_{n-1} X_{n-1}^d$; en tant que forme à $n - 1$ variables, G est non isotrope, et, par hypothèse de récurrence, elle représente $n - 1$ classes (au moins) modulo K^{*d} ; soit B la réunion de ces classes. Comme toute classe représentée par G est a fortiori représentée par F , il suffit de prouver qu'il existe un élément b de K^* n'appartenant pas à B et cependant représenté par F . Deux cas:

1^er cas: $a_n \notin B$. Il suffit évidemment dans ce cas de faire $b = a_n$.

2ème cas: $a_n \in B$. Il est clair alors que $-a_n \notin B$ (sinon F serait visiblement isotrope). Soit s l'entier ainsi défini:

la forme $a_n(X_1^d + \ldots + X_s^d)$ ne représente, dans K^* , que des éléments de B , mais la forme $a_n(X_1^d + \ldots + X_{s+1}^d)$ représente au moins un élément de K^* n'appartenant pas à B .

(Un tel s existe: car si, pour tout entier positif t , on pose $H_t(X) = a_n(X_1^d + \ldots + X_t^d)$, on voit que pour $t = 1$, H_t représente exactement $a_n K^{*d} \subset B$, tandis que, pour t suffisamment grand, la forme $X_1^d + \ldots + X_t^d$ représente -1 (propriété (I)), ce qui implique que H_t représente $-a_n \notin B$). Par définition de s , on peut trouver $b \in K^*$, $b \notin B$, et $y_1 , \ldots , y_s , y_{s+1} \in K$, tels que

$$a_n(y_1^d + \ldots + y_s^d + y_{s+1}^d) = b ,$$

mais que

$$a_n(y_1^d + \ldots + y_s^d) \in B .$$

D'autre part, par définition de B, il existe $x_1, \ldots, x_{n-1} \in K$ tels que

$$a_1x_1^d + a_2x_2^d + \ldots + a_{n-1}x_{n-1}^d = a_n(y_1^d + \ldots + y_s^d) ;$$

posons $x_n = y_{s+1}$: on trouve, en ajoutant $a_nx_n^d = a_ny_{s+1}^d$ aux deux membres de cette dernière égalité,

$$a_1x_1^d + a_2x_2^d + \ldots + a_nx_n^d = b ;$$

F représente donc $b \notin B$, c.q.f.d.

Outre son intérêt propre, cette proposition 1 a celui de donner le théorème suivant:

Théorème 2. - Soient K un corps fini à q éléments, $F(X)$ une forme additive de degré d à n variables sur K, et posons $\bar{d} = (q - 1 , d)$. Alors, si $n \geqslant \bar{d} + 1$, la forme F est isotrope.

Démonstration. On peut évidemment se borner au cas où $n = \bar{d} + 1$. On a alors $F(X) = a_1X_1^d + \ldots + a_{\bar{d}}X_{\bar{d}}^d + a_{\bar{d}+1}X_{\bar{d}+1}^d = G(X) + a_{\bar{d}+1}X_{\bar{d}+1}^d$, avec $G(X) = a_1X_1^d + \ldots + a_{\bar{d}}X_{\bar{d}}^d$. Trois cas peuvent alors se présenter:

1^{er} cas: G est isotrope; F est alors évidemment a fortiori isotrope.

$2^{ème}$ cas: $a_{\bar{d}+1} = 0$; F admet alors le zéro non trivial $(0 , 0 ,\ldots, 1)$ et est donc isotrope.

$3^{ème}$ cas: G n'est pas isotrope et $a_{\bar{d}+1}$ n'est pas nul; la proposition 1 montre alors que G représente au moins $\bar{d}$ classes de K^* modulo K^{*d} ; mais $\bar{d}$ est précisément l'ordre du groupe K^*/K^{*d} : G représente donc

en fait tout élément de K^*, et en particulier $-a_{d+1}$, ce qui implique évidemment que F est isotrope.

Le théorème 2 se trouve ainsi démontré.

Remarque. Le théorème 2 repose finalement sur le fait que -1 est somme de puissances $d^{\text{ièmes}}$ dans K, et sur le fait que K^*/K^{*d} est un groupe fini. Comme on l'a déjà remarqué, certains corps infinis possèdent ces deux propriétés, notamment les corps p-adiques; la proposition 1 et la méthode de démonstration du théorème 2 permettent ainsi de prouver facilement que si p est un nombre premier impair, toute forme additive de degré d à $d^2 + 1$ variables (ou plus) sur le corps Q_p est isotrope (cette propriété est d'ailleurs vraie aussi pour Q_2): voir à ce propos l'article de Demy'anov déjà cité, ainsi que [22].