§1. Equations diagonales homogènes.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1973)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **29.06.2024**

CHAPITRE 4

ÉQUATIONS DIAGONALES (I)

Une équation *diagonale* est une équation de la forme $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n} = b$; si $d_1 = \ldots = d_n$, l'équation est (abusivement) dite *homogène*; ce chapitre est consacré à l'existence de solutions d'équations diagonales homogènes (§ 1) puis quelconques (§ 3) sur un corps fini k; le paragraphe 2 résout le « problème de Waring » pour k, ce qui revient, pour un exposant d fixé, à déterminer les entiers n et les éléments b de k tels que l'équation $X_1^d + \ldots + X_n^d = b$ admette une solution sur k; enfin, le paragraphe 4 donne quelques indications sur les équations *multilinéaires* (pour une définition, voir sect. 4.1), avec une application aux équations diagonales homogènes de degré 2.

Les méthodes utilisées dans ce chapitre sont très élémentaires: les résultats obtenus sont en conséquence assez pauvres (et aussi assez disparates); pour des résultats plus précis sur les équations diagonales (et notamment pour l'évaluation exacte ou approchée du nombre de solutions), se reporter au chapitre 6; voir également les Notes en fin de chapitre. On conserve ici les conventions en vigueur dans les chapitres 2 et 3; en particulier, k désigne toujours un corps fini à $q = p^f$ éléments.

§ 1. *Equations diagonales homogènes.*

1.1. Si $F \in k[X]$ est une forme (c'est-à-dire un polynôme homogène) de degré $d \geqslant 1$, il est clair que $F(0, \ldots, 0) = 0$; s'il existe un point $\mathbf{x}$ de k^n autre que $(0, \ldots, 0)$ tel que $F(\mathbf{x}) = 0$, on dit que F est *isotrope* sur k, ou que *F représente (proprement)* 0 *sur k*. Si d'autre part a est un élément non nul de k, et s'il existe un point $\mathbf{x}$ de k^n tel que $F(\mathbf{x}) = a$, on dit que F représente a sur k; par homogénéité, F représente alors tout élément de la forme ab^d $(b \in k^*)$; F représente donc en fait toute la classe de a (mod k^{*d}) dans le groupe multiplicatif k^*.

THÉORÈME 1. — *Soit $F = a_1 X_1^d + \ldots + a_n X_n^d \in k[X]$ une forme diagonale de degré $d \geqslant 1$, à n variables. Si F n'est pas isotrope, elle représente au moins n classes de k^** (mod k^{*d}).

Démonstration. — On procède par récurrence sur n. Si $n = 1$, F représente a_1 (qui n'est pas nul, puisque F est non isotrope): F représente donc une classe, celle de a_1. Supposons alors le théorème démontré pour $n - 1$ variables ($n \geqslant 2$) et prouvons-le pour n variables. Posons $G = a_1 X_1^d + \dots + a_{n-1} X_{n-1}^d$; en tant que forme à $n - 1$ variables, G est non isotrope, et représente donc, par hypothèse de récurrence, au moins $n - 1$ classes (mod k^{*d}); soit C la réunion de ces classes. Comme toute classe représentée par G est a fortiori représentée par F, il suffit de prouver qu'il existe dans k^* un élément b n'appartenant pas à C, et cependant représenté par F. On distinguera deux cas:

(1) $a_n \notin C$: on peut alors prendre $b = a_n$.

(2) $a_n \in C$: il est clair dans ce cas que $-a_n \notin C$ (si G représentait $-a_n$, F serait isotrope). Soit alors m l'entier ainsi défini:

> la forme $a_n (X_1^d + \dots + X_m^d)$ ne représente que des éléments de C, mais la forme $a_n (X_1^d + \dots + X_{m+1}^d)$ représente au moins un élément de k^* n'appartenant pas à C.

Un tel m existe effectivement; car si, pour tout $r \geqslant 1$, on pose $H_r = a_n (X_1^d + \dots + X_r^d)$, on voit que H_1 représente uniquement $a_n k^{*d} \subset C$, mais que, pour r assez grand (par exemple, pour $r \geqslant p - 1$), H_r représente $-a_n \notin C$ (parce que $-1 = 1^d + \dots + 1^d$ ($p - 1$ fois): k est de caractéristique p). Par définition de m, on peut trouver b appartenant à k^* mais non à C, et $y_1, \dots, y_m, y_{m+1}$ appartenant à k, tels que

$$a_n (y_1^d + \dots + y_m^d + y_{m+1}^d) = b, \tag{1.1.1}$$

mais que

$$a_n (y_1^d + \dots + y_m^d) \in C.$$

Par définition de C, il existe alors $x_1, \dots, x_{n-1}$ dans k tels que

$$a_1 x_1^d + \dots + a_{n-1} x_{n-1}^d = a_n (y_1^d + \dots + y_m^d).$$

Posons $x_n = y_{m+1}$ et ajoutons $a_n x_n^d$ aux deux membres de cette égalité; compte tenu de (1.1.1), on obtient

$$a_1 x_1^d + \dots + a_n x_n^d = b,$$

et F représente bien $b \notin C$.
Ceci règle le deuxième cas et achève de prouver le théorème 1.

1.2. Le nombre total de classes de k^* (mod k^{*d}) est égal à $\delta = (q-1, d)$ (chap. 1, prop. 7, cor. 1); le théorème 1 admet donc les deux conséquences suivantes:

COROLLAIRE 1. — *Si* $F = a_1 X_1{}^d + \ldots + a_n X_n{}^d$ *est non isotrope, et si* $n = \delta$, *alors* F *représente tout élément de* k.

COROLLAIRE 2. — *Si* $F = a_1 X_1{}^d + \ldots + a_n X_n{}^d$ *est une forme diagonale de degré* d *à* n *variables et si* $n > \delta$, *alors* F *est certainement isotrope.*

1.3. La section 2.3 du chapitre 1 montre que, dans ce qui précède, on aurait pu remplacer partout d par δ, ou, ce qui revient au même, supposer que d divise $q-1$, et remplacer δ par d. Le corollaire 1 apparaît alors comme un cas particulier du théorème 4 du chapitre 3, et le corollaire 2, comme un cas particulier du théorème de Chevalley (chap. 3, th. 1, cor. 1). Quant au théorème 1, il admet l'interprétation « probabiliste » suivante: si $b \in k^*$, si $n \leqslant \delta$, et si le premier membre de l'équation $a_1 X_1{}^d + \ldots + a_n X_n{}^d = b$ est une forme non isotrope, la « probabilité » pour que l'équation admette une solution dans k^n est au moins égale à n/δ.

Pour d'autres résultats sur les équations diagonales homogènes, voir les sections 2.3, 3.4, 4.3, et les Notes en fin de chapitre.

§ 2. *Sommes de puissances d-ièmes.*

2.1. Soient toujours k un corps fini à $q = p^f$ éléments, et d un entier $\geqslant 1$; notons k_d le sous-ensemble de k formé des sommes $x_1{}^d + \ldots + x_n{}^d$, avec $n \geqslant 1$ quelconque et $x_1, \ldots, x_n \in k$; k_d est évidemment un *sous-corps* de k: en effet, il est stable pour l'addition et la multiplication; il contient 0, 1, et aussi $-1 = 1^d + \ldots + 1^d$ ($p-1$ fois); enfin, si $x \in k_d$ et si $x \neq 0$, alors $x^{-1} \in k_d$, puisqu'on peut écrire $x^{-1} = x^{d-1}(x^{-1})^d$, que $(x^{-1})^d \in k_d$, et que k_d est stable pour la multiplication.

2.2. Le théorème ci-dessous détermine explicitement k_d:

THÉORÈME 2. — *Etant donné* $k = \mathbf{F}_q$ *et* d, *posons toujours* $\delta = (q-1, d)$, *et notons d'autre part* q_1 *la plus petite puissance* p^g *de* p *telle que* (1) g *divise* f; (2) *le quotient* $(p^f-1)/(p^g-1)$ *divise* d. *Alors :*

(i) k_d *est égal à l'unique sous-corps de* k *contenant* q_1 *éléments (ce qu'on peut écrire* $k_d = \mathbf{F}_{q_1}$*).*

(ii) *Tout élément de* k_d *est somme d'au plus* δ *puissances d-ièmes.*