Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 19 (1973)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI

Autor: Joly, Jean-René

Kapitel: §2. Sommes de puissances d-ièmes.

DOI: https://doi.org/10.5169/seals-46287

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* $F = a_1X_1{}^d + ... + a_nX_n{}^d$ *est non isotrope, et si* $n = \delta$, *alors* F *représente tout élément de* k.

COROLLAIRE 2. — *Si* $F = a_1X_1{}^d + ... + a_nX_n{}^d$ *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 $a_1X_1{}^d + ... + a_nX_n{}^d = b$ 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 $x_1{}^d + ... + x_n{}^d$, avec $n \geqslant 1$ quelconque et $x_1, ..., x_n \in k$; 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 $-1 = 1^d + ... + 1^d$ $(p-1$ 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.*

Démonstration. — (i) k^* est un groupe cyclique d'ordre $q - 1$, et ses sous-groupes correspondent bijectivement aux diviseurs positifs de $q - 1$; par ailleurs, k étant un corps à p^f éléments, ses sous-corps correspondent bijectivement aux diviseurs positifs de f (chap. 1, prop. 4). Comme g divise f si et seulement si $p^g - 1$ divise $p^f - 1$ (petit exercice d'arithmétique), on peut énoncer:

Lemme 1. — *Pour qu'un sous-groupe H de k^* soit le groupe multiplicatif d'un sous-corps de k, il faut et il suffit que l'ordre de H soit de la forme $p^g - 1$, g étant un diviseur de f.*

Mais le groupe k^{*d} est d'ordre $(q-1)/\delta$ (chap. 1, prop. 7); d'autre part, k_d est évidemment le plus petit sous-corps l de k tel que $k^{*d} \subset l^*$; si alors on pose $k_d = \mathbf{F}_{q_1}$, $q_1 = p^{f_1}$, le lemme 1 montre que f_1 est le plus petit diviseur positif g de f tel que $(q-1)/\delta$ divise $p^g - 1$, c'est-à-dire (puisque $\delta = (q-1, d)$ et que $q = p^f$) tel que $(p^f-1)/(p^g-1)$ divise d, C.Q.F.D.

(ii) Pour tout $n \geqslant 1$, notons S_n l'ensemble des éléments de k^* qui sont de la forme $x_1{}^d + \ldots + x_n{}^d$ (les $x_i \in k$, certains x_i pouvant être nuls); il est clair que

$$k^{*d} = S_1 \subset S_2 \subset \ldots \subset S_n \subset S_{n+1} \subset \ldots \subset k_d{}^* , \tag{2.2.1}$$

et que, dans k^*, chaque S_n est réunion d'un certain nombre de classes (mod k^{*d}); comme le nombre total de ces classes est égal à δ, la suite (2.2.1) comporte au maximum $\delta - 1$ inclusions strictes. D'autre part, il est évident que si, pour une valeur n_0 de l'indice, on a $S_{n_0} = S_{n_0+1}$, alors, pour tout $n \geqslant n_0$, on a également $S_n = S_{n+1}$; dans la suite (2.2.1), les inclusions strictes occupent donc nécessairement les premières places. Il résulte de ces deux remarques qu'à partir du rang δ, toutes les inclusions de la suite (2.2.1) sont en fait des égalités, et que $k_d{}^* = S_\delta$, C.Q.F.D.

2.3. Tirons les conséquences de ce théorème. Tout d'abord, pour d fixé, on a « le plus souvent » $k_d = k$; en effet, il résulte de la définition de q_1 que si $k_d \neq k$, alors $p^{f/2} < d$, ou encore $q < d^2$; en particulier:

Corollaire 1. — *Pour d fixé, il n'existe qu'un nombre fini de corps k tels que $k_d \neq k$.*

Supposons maintenant k fixé. Si $f = 1$, donc si $k = \mathbf{F}_p$, on a évidemment $k_d = k$ quel que soit d. En revanche, si $f \geqslant 2$, on peut toujours trouver d tel que $k_d \neq k$, par exemple $d = p^{f-1} + \ldots + p + 1$: le théorème 2, (i) donne alors $f_1 = 1$ et $q_1 = p$, donc $k_d = \mathbf{F}_p$ (ce qui est évident directement, puisque, pour tout $x \in k$, x^d est dans ce cas la norme de x dans l'extension $k/\mathbf{F}_p$: chap. 1, sect. 3.3). Ainsi:

COROLLAIRE 2. — *Soit* $k = \mathbf{F}_q$, $q = p^f$. *Si* $f \geqslant 2$, *il existe au moins un exposant* d *tel que* $k_d \neq k$.

(Il en existe même une infinité: car si d est tel que $k_d \neq k$, la même propriété est vraie pour tout multiple de d; mais ceci n'a pas grande signification, car d intervient en réalité par l'intermédiaire de $\delta = (q-1, d)$, qui ne peut prendre qu'un nombre fini de valeurs).

Supposons toujours k fixé, avec $f \geqslant 2$, et soit d un entier tel que $k_d \neq k$; avec les notations du théorème 2, on a $k_d = \mathbf{F}_{q_1}$; si $b \in k^*$, on aura donc $b \in k_d$ si et seulement si $b^{q_1-1} = 1$; les parties (i) et (ii) du théorème donnent alors:

COROLLAIRE 3. — *Si* $b^{q_1-1} = 1$, *et si* $n \geqslant \delta$, *l'équation diagonale* $X_1^d + \ldots + X_n^d = b$ *admet une solution dans* k^n.

(ii) *Si au contraire* $b^{q_1-1} \neq 1$, *alors, si grand que soit n, l'équation* $X_1^d + \ldots + X_n^d = b$ *n'admet aucune solution dans* k^n.

Exemple: $k = \mathbf{F}_4$, $d = 3$; on a $k_d = \mathbf{F}_2 \neq k$; si $b \in \mathbf{F}_4$, $b \neq 0, 1$, l'équation $X_1^3 + \ldots + X_n^3 = b$ n'a pas de solution sur $\mathbf{F}_4$, si grand que soit le nombre d'inconnues, n.

§ 3. *Equations diagonales quelconques.*

3.1. Passons maintenant aux équations diagonales quelconques, donc de la forme $F = b$, avec

$$F = a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n},$$

les $d_i \geqslant 1$, les $a_i \in k$ (on les supposera tous différents de zéro, ce qui ne diminue pas la généralité) et $b \in k$ (et éventuellement nul). Désignons par N le nombre de solutions de l'équation $F = b$ dans k^n, et par $\overline{N}$ le reste de division de N par p (ou encore, l'élément $N.1$ de $k = \mathbf{F}_q$). Enfin, pour simplifier les calculs, posons $\delta_i = (q-1, d_i)$ $(i=1, \ldots, n)$, puis

$$\Phi = a_1 X_1^{\delta_1} + \ldots + a_n X_n^{\delta_n},$$

$a_0 = -b$, et $G = a_0 + \Phi$. Il est clair alors que le nombre de solutions dans k^n de l'équation $G = 0$ est égal au nombre de solutions dans k^n de $F = b$, donc à N (voir chap. 1, sect. 2.3; bien entendu, les *ensembles* de