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: Chapitre 4 ÉQUATIONS DIAGONALES (I)
DOI: https://doi.org/10.5169/seals-46287

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 $G = a_1 X_1^d + \ldots + a_{n-1} X_{n-1}^d$; 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 $a_n(X_1^d + \ldots + X_m^d)$ ne représente que des éléments de C, mais la forme $a_n(X_1^d + \ldots + X_{m+1}^d)$ 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 $H_r = a_n(X_1^d + \ldots + X_r^d)$, 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 $-1 = 1^d + \ldots + 1^d$ ($p - 1$ fois): k est de caractéristique p). Par définition de m, on peut trouver b appartenant à k^* mais non à C, et $y_1, \ldots, y_m, y_{m+1}$ appartenant à k, tels que

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

mais que

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

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

$$a_1 x_1^d + \ldots + a_{n-1} x_n^d{}_{-1} = a_n(y_1^d + \ldots + y_m^d)\,.$$

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

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

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

COROLLAIRE 2. — *Si* $F = a_1X_1^d + \ldots + a_nX_n^d$ *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 $a_1X_1^d + \ldots + a_nX_n^d = b$ 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 $x_1^d + \ldots + x_n^d$, 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.*

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

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

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 direc-

tement, 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 $k_d = \mathbf{F}_{q1}$; si $b \in k^*$, on aura donc $b \in k_d$ si et seulement si $b^{q1-1} = 1$; les parties (i) et (ii) du théorème donnent alors:

COROLLAIRE 3. — *Si* $b^{q1-1} = 1$, *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* $b^{q1-1} \neq 1$, *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

$$F = a_1 X_1^{d1} + \ldots + a_n X_n^{dn},$$

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

solutions de ces deux équations sont en général distincts). En outre, dans le polynôme G, chaque exposant divise $q-1$.

3.2. On peut alors évaluer N par la « méthode de Lebesgue » (chap. 3, § 2 et Notes). On a en effet (loc. cit.)

$$(3.2.1) \qquad \overline{N} = \sum_{\mathbf{x}\in k^n} (1 - G(\mathbf{x})^{q-1}) = -\sum_{\mathbf{x}\in k^n} G(\mathbf{x})^{q-1}.$$

Ecrivons $G(\mathbf{x}) = a_0 + a_1 x_1^{\delta_1} + \ldots + a_n x_n^{\delta_n}$, et développons $G(\mathbf{x})^{q-1}$; il vient

$$(3.2.2) \qquad N = -\sum_{\mathbf{x}\in k^n} \sum_{\mathbf{j}} \binom{q-1}{\mathbf{j}} a_0^{j_0} a_1^{j_1} \ldots a_n^{j_n} x_1^{\delta_1 j_1} \ldots x_n^{\delta_n j_n},$$

la seconde sommation portant sur l'ensemble des vecteurs entiers $\mathbf{j} = (j_0, \ldots, j_n)$ tels que (1) $j_i \geqslant 0$ pour $i = 0, \ldots, n$; (2) $j_0 + \ldots + j_n = q-1$, et le symbole $\binom{q-1}{\mathbf{j}}$ désignant le « coefficient multinomial » $(q-1)!/j_0! \ldots j_n!$ Mais (chap. 3, sect. 2.1) on a $\sum_{x\in k} x^u = -1$ si $u > 0$ et si $q-1$ divise u, et $\sum_{x\in k} x^u = 0$ sinon; ceci permet de simplifier la formule (3.2.2) et d'énoncer:

LEMME 2. — *Soit J l'ensemble des vecteurs entiers $\mathbf{j} = (j_0, \ldots, j_n)$ tels que*

(1) $j_0 \geqslant 0$, $j_i > 0$ *pour* $i = 1, \ldots, n$;

(2) $j_0 + j_1 + \ldots + j_n = q-1$;

(3) $(q-1)/\delta_i$ *divise* j_i *pour* $i = 1, \ldots, n$;

alors $\overline{N}$ est donné par la formule

$$(3.2.3) \qquad \overline{N} = (-1)^{n+1} \sum_{\mathbf{j}\in J} \binom{q-1}{\mathbf{j}} a_0^{j_0} a_1^{j_1} \ldots a_n^{j_n}.$$

3.3. Première conséquence de ce lemme:

THÉORÈME 3. — *Si les entiers δ_i satisfont à la condition*

$$(H1) \qquad 1/\delta_1 + \ldots + 1/\delta_n > 1,$$

le nombre N de solutions de $F = b$ dans k^n est divisible par p.

Démonstration. — Si la condition (H1) est vérifiée, l'ensemble J défini dans le lemme 2 est vide, et on a bien $\overline{N} = 0$.

Ce théorème montre notamment que si les exposants de F satisfont à la condition

(*H2*) $\quad 1/d_1 + \ldots + 1/d_n > 1,$

le nombre N est divisible par p. Si $d_1 = \ldots = d_n = d$ (cas homogène), (H2) se réduit à l'inégalité $n > d$, et on retombe sur un cas particulier du théorème de Chevalley-Warning (chap. 3, th. 1). En revanche, dans le cas non homogène, la condition (H2) peut être réalisée en même temps que l'inégalité $n \leqslant d$:

Exemple: des équations diagonales telles que

$$X_1^2 + X_2^3 + X_3^5 + 1 = 0\,; \qquad X_1^2 + X_2^3 + X_3^6 + X_4^6 = 0\,,$$

ont, sur un corps fini quelconque k, un nombre de solutions divisible par la caractéristique p de k (ce nombre est d'ailleurs non nul, donc $\geqslant p$, car la première équation a pour solution $(1, -1, 0)$, la seconde, $(1, -1, 0, 0)$); or, pour la première équation, $n = 3 \leqslant d = 5$; pour la seconde, $n = 4 \leqslant d = 6$.

3.4. Autre conséquence du lemme 2:

THÉORÈME 4. — *Supposons réalisées les deux conditions suivantes :*

(H3) $\quad 1/\delta_1 + \ldots + 1/\delta_n = 1;$

(H4) *Chaque* $\delta_i\ (1 \leqslant i \leqslant n)$ *divise* $p - 1$.

Alors, quel que soit $b \in k$, *l'équation* $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n} = b$ *admet au moins une solution dans* k^n.

Démonstration. — Avec les notations des sections 3.1 et 3.2, il suffit de prouver que, dans le lemme 2, $\overline{N} \neq 0$. Mais la condition (H3) entraîne que J est réduit au seul élément $\mathbf{h} = (0, h_1, \ldots, h_n)$, avec $h_i = (q-1)/\delta_i$ pour $i = 1, \ldots, n$; le lemme donne donc

$$\overline{N} = (-1)^{n+1} \binom{q-1}{\mathbf{h}} a_1^{h_1} \ldots a_n^{h_n}\,;$$

comme les a_i ont été supposés non nuls, il reste à prouver que, sous l'hypothèse (H4), le coefficient $\binom{q-1}{\mathbf{h}}$ n'est pas divisible par p, ou encore, v_p désignant la valuation p-adique, que

$$v_p((q-1)!) = v_p(h_1!) + \ldots + v_p(h_n!)\,;$$

mais ceci résulte facilement de l'estimation bien connue

$$v_p(m!) = [m/p] + [m/p^2] + \ldots$$

valable pour tout entier $m \geqslant 1$ (la notation [...] signifie: partie entière de ...; cette estimation se déduit immédiatement de l'écriture de m en base p).

Dans le cas homogène, le théorème 4 peut s'énoncer:

THÉORÈME 5. — *Soit* $F = a_1 X_1^d + \ldots + a_n X_n^d$ *une forme diagonale homogène de degré d à n variables ; posons* $\delta = (q-1, d)$ *; alors, si* $n = \delta$, *et si* δ *divise* $p - 1$, *la forme F représente tout élément non nul de k.*

Ce résultat étend le théorème 2 à des formes F non isotropes; signalons que le théorème 5 reste vrai si on remplace l'hypothèse (H4) par l'hypothèse plus faible: $\delta \leqslant p - 1$ (voir Schwarz (1950)); en revanche, si $\delta \geqslant p$, le théorème 5 peut tomber en défaut: ainsi, dans l'exemple donné à la fin du paragraphe 2, la forme $X_1^3 + X_2^3 + X_3^3$ sur $k = \mathbf{F}_4$ (avec $n = d = \delta = q - 1 = 3$) représente seulement les éléments de $\mathbf{F}_2$; et de fait, $\delta = 3 \geqslant p = 2$.

Notons enfin que si $q = p$, les conditions: δ_i divise $p - 1$, δ divise $p - 1$, sont automatiquement vérifiées: sur un corps fini *premier*, les théorèmes 4 et 5 sont donc valables sans restriction.

§ 4. *Equations multilinéaires.*

4.1. Soit toujours k un corps fini à $q = p^f$ éléments, soient r et d deux entiers $\geqslant 1$, et soit $n = rd$. On se propose dans cette section de calculer le nombre $N(F, b)$ de solutions dans k^n de l'équation $F = b$ $(b \in k)$, le polynôme F étant de la forme

$$(4.1.1) \qquad F = a_1 X_1 \ldots X_d + a_2 X_{d+1} \ldots X_{2d} + \ldots + a_r X_{n-d+1} \ldots X_n$$

(un tel polynôme est parfois dit abusivement *multilinéaire*). Il est clair qu'on peut supposer tous les a_j non nuls (chap. 3, th. 5) et qu'on peut même (quitte éventuellement à multiplier les deux membres de l'équation par b^{-1}, et à faire une « homothétie » sur certaines variables) supposer $a_1 = \ldots = a_r = 1$, et $b = 0$ ou 1. On est ainsi ramené à calculer les nombres de solutions dans k^n des deux équations $F_{r,d} = 0$ et $F_{r,d} = 1$, avec

$$(4.1.2) \qquad F_{r,d} = X_1 \ldots X_d + X_{d+1} \ldots X_{2d} + \ldots + X_{n-d+1} \ldots X_n ,$$

nombres qu'on notera respectivement $N(r, d)$ et $N_1(r, d)$.

4.2. THÉORÈME 6. — *Les nombres* $N(r, d)$ *et* $N_1(r, d)$ *sont donnés par*

$$(4.2.1) \qquad N(r, d) = q^{n-1} + (q-1)\, q^{r-1} A(q, d)^r ,$$

$$(4.2.2) \qquad N_1(r, d) = q^{n-1} - q^{r-1} A(q, d)^r ,$$

avec par définition $A(q, d) = q^{d-1} - (q-1)^{d-1}$.

Démonstration. — On établit les deux formules *simultanément* par récurrence sur l'entier r. Si $r = 1$, et donc $n = d$, on voit directement que $N(1, d) = q^n - (q-1)^n$, et que $N_1(1, d) = (q-1)^{n-1}$, ce qui coïncide bien avec les valeurs données dans ce cas par (4.2.1) et (4.2.2). Supposons alors ces formules prouvées jusqu'à un entier $r - 1 \geqslant 1$, et démontrons-les pour l'entier r. En classant les solutions de l'équation $F_{r,d} = 0$ selon la valeur prise par le monôme $X_{n-d+1} \ldots X_n$, on obtient

$$\begin{aligned} N(r, d) &= \sum_{c \in k} N(F_{r-1,d}, c)\, N(F_{1,d}, -c) \\ &= N(r-1, d)\, N(1, d) + (q-1)\, N_1(r-1, d)\, N_1(1, d) \end{aligned}$$

(voir sect. 4.1). L'hypothèse de récurrence donne la valeur des quatre termes $N(r-1, d)$, $N(1, d)$, $N_1(r-1, d)$ et $N_1(1, d)$, et on vérifie, après calcul, que la valeur ainsi obtenue pour $N(r, d)$ coïncide bien avec celle fournie par (4.2.1). Raisonnement analogue pour (4.2.2). (On peut aussi déduire directement (4.2.2) de (4.2.1) en remarquant que, puisque toutes les équations $F_{r,d} = b$ ($b \in k^*$) ont même nombre de solutions, $N_1(r, d)$, on a évidemment $q^n = N(r, d) + (q-1)\, N_1(r, d)$).

Corollaire 1. — *Si, dans l'équation* $F = b$ *(voir* (4.1.1)*), les coefficients* a_j *sont tous différents de* 0 *(et si en outre, quand* $r = 1$, b *est également différent de* 0*), alors* $N(F, b)$ *est un polynôme en* q, *à coefficients entiers rationnels, de terme dominant* q^{n-1}. *En particulier, si on considère* q *comme « infiniment grand », on peut écrire*

$$N(F, b) = q^{n-1} + O(q^{n-2}).$$

On reviendra longuement sur ce genre de résultat aux chapitres 6, 7, 8 et 9.

4.3. Le théorème 6 permet en particulier de déterminer le nombre N de solutions dans k^n d'une équation diagonale homogène de degré 2,

$$a_1 X_1^2 + \ldots + a_n X_n^2 = b, \tag{4.3.1}$$

($a_1, \ldots, a_n, b \in k$); on peut naturellement supposer tous les coefficients a_i différents de 0; on peut également supposer $p \neq 2$ (en caractéristique 2, on a $N = q^{n-1}$); comme la détermination de N sera effectuée ultérieurement (chap. 6, sect. 1.3) par un autre procédé, on se bornera ici à indiquer la démarche du calcul, en laissant au lecteur le soin d'en expliciter les détails.

(1) Pour $n = 1$, on a évidemment $N = 1$ si $b = 0$; sinon, on a $N = 2$ ou 0 selon que $a_1 b \in k^{*2}$ ou que $a_1 b \notin k^{*2}$.

(2) Pour $n = 2$, on vérifie sans peine, soit par le calcul, soit par un raisonnement géométrique, que N est donné par les formules ci-dessous:

$$\text{pour } b = 0, N = \begin{cases} 2q - 1, \text{ si } -a_1 a_2 \in k^{*2}, \\ 1, \text{ si } -a_1 a_2 \notin k^{*2}; \end{cases}$$

$$\text{pour } b \neq 0, N = \begin{cases} q - 1, \text{ si } -a_1 a_2 \in k^{*2}, \\ q + 1, \text{ si } -a_1 a_2 \notin k^{*2}. \end{cases}$$

Supposons maintenant $n \geqslant 3$. Comme toute forme quadratique à trois variables ou plus sur k est isotrope (théorème de Chevalley: chap. 3, th. 1, cor. 1), la théorie générale de la réduction des formes quadratiques (voir [**17**], chap. IV, notamment pp. 60-62) montre qu'on peut (par une transformation linéaire inversible à coefficients dans k, ce qui n'affecte pas la valeur de N) mettre le premier membre de (4.3.1) sous l'une des deux formes suivantes:

$$(4.3.2) \qquad Y_1 Y_2 + \ldots + Y_{2r-1} Y_{2r} + a Y_n^2,$$

avec $n = 2r + 1$ et $a = (-1)^r a_1 \ldots a_n$, *si n est impair*;

$$(4.3.3) \qquad Y_1 Y_2 + \ldots + Y_{2r-1} Y_{2r} + Y_{n-1}^2 + a Y_n^2,$$

avec $n = 2r + 2$ et $a = (-1)^2 a_1 \ldots a_n$, *si n est pair.*
(La valeur de a s'obtient en écrivant l'invariance du discriminant).

(3) Calculons alors N quand n est *impair*, $n = 2r + 1$. En classant (comme dans la démonstration du théorème 6) les solutions de $F = b$ (F étant mis sous la forme (4.3.2)) suivant la valeur prise par le monôme aY_n^2, on obtient, avec les notations de la section 4.1,

$$(4.3.4) \qquad N = \sum_{c \in k,\, c \neq b} N_1(r, 2)\, N(aY_n^2, c) + N(r, 2)\, N(aY_n^2, b).$$

$N(r, 2)$ et $N_1(r, 2)$ sont donnés par le théorème 6, $N(aY_n^2, c)$ et $N(aY_n^2, b)$ sont donnés par (1); si on remarque que k^* contient $(q-1)/2$ carrés et autant de non-carrés, on arrive finalement à ceci:

$$\text{pour } b = 0, N = q^{n-1};$$

$$\text{pour } b \neq 0, N = \begin{cases} q^{n-1} + q^{(n-1)/2}, \text{ si } (-1)^{(n-1)/2} a_1 \ldots a_n b \in k^{*2}, \\ q^{n-1} - q^{(n-1)/2}, \text{ si } (-1)^{(n-1)/2} a_1 \ldots a_n b \notin k^{*2}. \end{cases}$$

(4) Le calcul de N quand n est *pair* se fait de la même manière: on réécrit la formule (4.3.4) en y remplaçant aY_n^2 par Y_{n-1}^2, $+ aY_n^2$, on utilise le théorème 6 et les formules de (2), et on obtient finalement ceci:

$$\text{pour } b = 0, N = \begin{cases} q^{n-1} + q^{n/2} - q^{(n/2)-1}, \text{ si } (-1)^{n/2} a_1 \dots a_n \in k^{*2}, \\ q^{n-1} - q^{n/2} + q^{(n/2)-1}, \text{ si } (-1)^{n/2} a_1 \dots a_n \notin k^{*2}; \end{cases}$$

$$\text{pour } b = 0, N = \begin{cases} q^{n-1} - q^{(n/2)-1}, \text{ si } (-1)^{n/2} a_1 \dots a_n \in k^{*2}, \\ q^{n-1} + q^{(n/2)-1}, \text{ si } (-1)^{n/2} a_1 \dots a_n \notin k^{*2}. \end{cases}$$

Notes sur le chapitre 4

§ **1**: la méthode de démonstration du théorème 1 est empruntée à Demyanov (1956). Cette méthode s'applique également aux équations diagonales homogènes sur un corps p-adique; à ce sujet, voir également Schwarz (1956), Davenport-Lewis (1963), et surtout [7], pp. 101-138, et [**13**], pp. 17-22 et 40-52.

§ **2**: le théorème 3, (ii) et son corollaire 1 sont dus à Tornheim (1938); voir aussi Schwarz (1948, a). Pour l'application du théorème 3, (i) au problème de Waring dans un anneau d'entiers algébriques, voir Bateman-Stemmler (1962) pour un exposant d premier, et Joly (1968) pour un exposant d quelconque.

§ **3**: les théorèmes 4 et 5 sont dus à Morlaye (1971); voir également Schwarz (1948, b; 1950) et Carlitz (1956, b).

§ **4**: pour une autre démonstration du théorème 7, voir Porter (1966, e).

Les équations diagonales sur un corps fini ont suscité une vaste littérature; mentionnons seulement ici (en dehors des articles déjà cités, et de ceux qui le seront au chapitre 6) Cohen (1956), Chowla-Mann-Straus (1959), Gray (1960), Chowla (1961), Tietäväinen (1968), et Lewis (1960).