

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. Equations diagonales avec terme constant.
DOI:	https://doi.org/10.5169/seals-46287

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 25.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

est lui-même le nombre de points rationnels sur k de n'importe quel hyperplan défini sur k . Ce corollaire 3 montre également que si q est supérieur à une certaine constante ne dépendant que de d et n , alors $N \geq 1$: l'équation $F = 0$ admet donc une solution dès que q est assez grand.

Le corollaire 3 est un cas particulier d'un résultat très général qui sera démontré au chapitre 8 (th. 4): on examinera plus en détail à cette occasion les conséquences qu'on peut tirer d'une inégalité telle que (1.2.9).

Revenons au corollaire 1; si I est vide, on a $A_1 = 0$; ainsi:

COROLLAIRE 4. — *Si l'ensemble I est vide, on a $N = q^{n-1}$.*

Un cas où I est vide est celui où l'un des δ_i est égal à 1 (on a même alors $A_2 = 0$); mais dans cette situation, l'égalité $N = q^{n-1}$ peut se prouver directement: il suffit de remarquer (comme au chap. 4, sect. 3.1) qu'on ne modifie pas N en remplaçant dans F les d_i par les δ_i , et de noter par ailleurs que si dans une équation diagonale l'un des exposants (disons d_1) est égal à 1, alors le nombre total de solutions de l'équation est q^{n-1} : car on peut se fixer arbitrairement les valeurs de X_2, \dots, X_n dans k (d'où q^{n-1} possibilités), et $F = 0$ devient alors une équation du premier degré en l'unique variable X_1 .

Un cas plus général où I est vide est celui où l'un des entiers δ_i est premier avec les $n - 1$ autres (on laisse au lecteur le soin de le vérifier); ceci se produit notamment si l'un des d_i est premier avec les $n - 1$ autres. Exemple: quel que soit q , des équations telles que

$$X^2 + Y^3 + Z^3 = 0; \quad X^2 + Y^2 + Z^5 = 0,$$

admettent exactement q^2 solutions sur $k = \mathbf{F}_q$.

Un autre cas où I est vide est celui où n est impair, et où $d_i = 2$ pour $i = 1, \dots, n$; ce cas a déjà été vu au chapitre 4, section 4.3, (3), et sera examiné à nouveau dans la section 3.1 ci-dessous.

§ 2. Equations diagonales avec terme constant.

On suppose maintenant $b \neq 0$, et on cherche à évaluer $N(b)$.

2.1. Désignons par $L(U) = L(U_1, \dots, U_n)$ la forme linéaire $b^{-1}a_1U_1 + \dots + b^{-1}a_nU_n$, et pour tout i ($1 \leq i \leq n$) et tout $u_i \in k$, notons $m_i(u_i)$ le nombre de solutions dans k de l'équation à une variable U_i : $U_i^{d_i} = u_i$ (chap. 5, sect. 1.5); χ_i désignant un caractère multiplicatif de k d'ordre $\delta_i = (q-1, d_i)$, on a alors (*loc. cit.*, prop. 5)

$$(2.1.1) \quad m_i(u_i) = \sum_{j_i=0}^{\delta_i-1} \chi_i^{j_i}(u_i);$$

par ailleurs, il est clair que

$$(2.1.2) \quad N(b) = \sum_{\mathbf{u} \in H} m_1(u_1) \dots m_n(u_n),$$

H désignant l'hyperplan affine de k^n formé des points $\mathbf{u} = (u_1, \dots, u_n)$ tels que $L(\mathbf{u}) = 1$; (2.1.1) et (2.1.2) donnent alors

$$(2.1.3) \quad N(b) = \sum_{\mathbf{u} \in H} \prod_{i=1}^n \sum_{j_i=0}^{\delta_i-1} \chi_i^{j_i}(u_i).$$

Isolons dans le membre de droite les q^{n-1} termes (égaux à 1) correspondant à $\mathbf{j} = 0$ (c'est-à-dire à $(i_1, \dots, j_n) = (0, \dots, 0)$) et, pour les autres, intervertissons l'ordre des sommes; il vient

$$(2.1.4) \quad N(b) = q^{n-1} + \sum_{\mathbf{j} \neq 0} \sum_{\mathbf{u} \in H} \prod_{i=1}^n \chi_i^{j_i}(u_i).$$

Or, un raisonnement analogue à celui fait au chapitre 5, section 4.2, montre que si \mathbf{j} n'est pas nul, mais si l'une au moins des composantes j_i de \mathbf{j} est nulle, alors $\sum_{\mathbf{u} \in H} \prod_{i=1}^n \chi_i^{j_i}(u_i) = 0$; (2.1.4) se réduit donc à

$$(2.1.5) \quad N(b) = q^{n-1} + \sum_{\mathbf{j} \in J} \sum_{\mathbf{u} \in H} \prod_{i=1}^n \chi_i^{j_i}(u_i),$$

J ayant la même signification qu'au paragraphe 1.

Effectuons alors le changement de variables $\mathbf{u} \mapsto \mathbf{x}$ défini par $x_i = b^{-1}a_i u_i$ ($1 \leq i \leq n$), et désignons par H_1 l'hyperplan affine de k^n formé des $\mathbf{x} = (x_1, \dots, x_n)$ tels que $x_1 + \dots + x_n = 1$; (2.1.5) devient

$$(2.1.6) \quad N(b) = q^{n-1} + \sum_{\mathbf{j} \in J} \prod_{i=1}^n \bar{\chi}_i^{j_i}(b^{-1}a_i) \sum_{\mathbf{x} \in H_1} \prod_{i=1}^n \chi_i^{j_i}(x_i).$$

La quantité $\sum_{\mathbf{x} \in H_1} \prod_{i=1}^n \chi_i^{j_i}(x_i)$ n'est autre que la somme de Jacobi $\pi(\chi_1^{j_1}, \dots, \chi_n^{j_n})$ (chap. 5, déf. 3), qu'on notera $\pi(\mathbf{j})$ pour alléger l'écriture; convenons d'autre part, pour tout $\mathbf{j} \in J$, de poser

$$(2.1.7) \quad C(b, \mathbf{j}) = \prod_{i=1}^n \bar{\chi}_i^{j_i}(b^{-1}a_i);$$

(si on fait $\chi_i = \theta^{hi}$ comme au paragraphe 1, on a en particulier $C(1, j) = C(j)$); on arrive alors à ceci:

THÉORÈME 2. — *Le second membre b étant supposé non nul, et les quantités $C(b, j)$ et $\pi(j)$ étant définies comme ci-dessus, le nombre $N(b)$ de solutions dans k^n de l'équation diagonale $F = b$ est donné exactement par*

$$(2.1.8) \quad N(b) = q^{n-1} + \sum_{j \in J} C(b, j) \pi(j).$$

COROLLAIRE 1. — *Posons (comme dans le corollaire 2 du théorème 1) $A_2 = \text{card}(J) = (\delta_1 - 1) \dots (\delta_n - 1)$; on a alors l'inégalité*

$$(2.1.9) \quad |N(b) - q^{n-1}| \leq A_2 q^{(n-1)/2}.$$

Démonstration. — Il suffit de remarquer que dans la formule (2.1.8), chaque quantité $C(b, j)$ est une racine de l'unité, donc un nombre complexe de module 1, et que chaque quantité $\pi(j)$ est une somme de Jacobi non triviale à n caractères relative à k , donc un nombre complexe de module au plus égal à $q^{(n-1)/2}$ (chap. 5, prop. 10, cor. 1).

Pour $n \geq 2$, on a évidemment $(n-1)/2 \leq n - (3/2)$; ainsi:

COROLLAIRE 2. — *Il existe une constante A_2 , ne dépendant que du degré et du nombre de variables de F , et telle que (si $n \geq 2$)*

$$(2.1.10) \quad |N(b) - q^{n-1}| \leq A_2 q^{n-(3/2)}.$$

Ce corollaire appelle naturellement les mêmes remarques que le corollaire 3 du théorème 1.

2.2. Supposons toujours $b \neq 0$, et soit N_1 le nombre de solutions dans k^{n+1} de l'équation diagonale sans second membre

$$(2.2.1) \quad a_1 X_1^{d_1} + \dots + a_n X_n^{d_n} - b X_{n+1}^{q-1} = 0;$$

on vérifie sans peine que N , $N(b)$ et N_1 sont liés par

$$(2.2.2) \quad N_1 = N + (q-1)N(b);$$

mais le théorème 1 permet d'exprimer N et N_1 à l'aide de sommes de Gauss: (2.2.2) permettrait donc également d'exprimer $N(b)$ à l'aide de sommes de Gauss; la formule qui en résulterait est peu maniable, et il est inutile de l'écrire ici explicitement: signalons simplement que cette formule est identique à celle qu'on pourrait déduire de (2.1.8) en appliquant la proposition 10 du chapitre 5 à chacune des sommes de Jacobi $\pi(j)$ qui y figurent.