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: §. 1. Equations diagonales sans 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: 09.12.2025

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

Gauss et de Jacobi; si on sait calculer ces sommes, on obtient explicitement $N(b)$; sinon, l'évaluation du module des sommes de Gauss et de Jacobi donnée au chapitre 5 (prop. 8, prop. 9, cor. 1 et prop. 10, cor. 1) permet d'écrire une estimation approchée de $N(b)$; cette estimation est (sauf dans des cas exceptionnels) de la forme $N(b) = q^{n-1} + O(q^{n-(3/2)})$, q étant considéré comme « infiniment grand », et la constante impliquée par le O ne dépendant que du nombre de variables n et des degrés partiels d_i: c'est là un type de résultat dont on a déjà vu un exemple au chapitre 4 (th. 6, cor. 1), et qu'on retrouvera systématiquement au chapitre 8.

Dans tout le présent chapitre, les notations sont les suivantes: k désigne un corps fini à $q = p^f$ éléments; n est un entier $\geqslant 2$; $a_1, \ldots, a_n$ sont n éléments de k, qu'on suppose tous différents de 0; $d_1, \ldots, d_n$ sont n entiers $\geqslant 1$; F désigne le polynôme diagonal $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n}$; b est un élément quelconque de k; $N(b)$ désigne le nombre de solutions dans k^n de l'équation $F = b$; si $b = 0$ (équation « sans second membre » ou « sans terme constant »), on écrit N au lieu de $N(0)$; enfin, pour $i = 1, \ldots, n$, on pose $\delta_i = (q-1, d_i)$ et $h_i = (q-1)/\delta_i$.

§ 1. *Equations diagonales sans terme constant.*

On s'intéresse d'abord au cas où $b = 0$, et on cherche à évaluer $N = N(0)$. La lettre β désigne un caractère additif non trivial de k, fixé une fois pour toutes.

1.1. On aura besoin du résultat suivant:

LEMME 1. — *Soient γ un caractère additif non trivial de k, d un entier $\geqslant 1$, et χ un caractère multiplicatif de k, d'ordre $\delta = (q-1, d)$. Alors*

$$\sum_{x \in k} \gamma(x^d) = \sum_{j=1}^{\delta-1} \tau(\chi^j \mid \gamma). \tag{1.1.1}$$

Démonstration. — Si, pour tout $a \in k$, $m(a)$ désigne le nombre de solutions dans k de l'équation $X^d = a$, le membre de gauche de (1.1.1) peut évidemment s'écrire $\sum_{a \in k} m(a)\gamma(a)$; mais on a vu (chap. 5, prop. 5) que $m(a)$ est égal à $\sum_{j=0}^{\delta-1} \chi^j(a)$; ledit membre de gauche vaut donc $\sum_{j=0}^{\delta-1} \sum_{a \in k} \chi^j(a)\gamma(a)$, ce qui se décompose en

$$\sum_{j=0}^{\delta-1} \chi^j(0)\gamma(0) + \sum_{a \in k^*} \chi^0(a)\gamma(a) + \sum_{j=1}^{\delta-1} \sum_{a \in k^*} \chi^j(a)\gamma(a);$$

dans cette somme de trois termes, le premier vaut 1 (chap. 5, convention (1.4.1)), et le second, qui est une somme de Gauss correspondant au caractère multiplicatif trivial χ^0 et au caractère additif non trivial γ, vaut -1 (chap. 5, sect. 2.2, (i)). Seul reste donc le troisième terme, évidemment égal au membre de droite de (1.1.1): le lemme est ainsi prouvé.

1.2. Calculons alors N; partons de la formule (1.3.1) du chapitre 5, et isolons, dans la somme de droite, les q^n termes (égaux à 1) correspondant à $y = 0$; il vient

$$N = q^{n-1} + q^{-1} \sum_{y \in k^*} \sum_{\mathbf{x} \in k^n} \beta(yF(\mathbf{x})),$$

ou encore, compte tenu de la définition de F et du fait que β est un caractère additif,

$$N = q^{n-1} + q^{-1} \sum_{y \in k^*} \prod_{i=1}^{n} B(i, y), \tag{1.2.1}$$

avec par définition $B(i, y) = \sum_{x_i \in k} \beta(ya_i x_i^{d_i})$; le lemme 1, appliqué au caractère additif non trivial $\gamma = \beta_{ya_i}$, et la proposition 6 du chapitre 5, permettent de transformer le second membre et d'écrire

$$B(i, y) = \sum_{j_i=1}^{\delta_i - 1} \bar{\chi}^{j_i}(ya_i)\, \tau(\chi_i^{j_i}). \tag{1.2.2}$$

Désignons alors par θ un caractère multiplicatif d'ordre $q-1$ de k, fixé une fois pour toutes (par exemple celui défini au chapitre 5 par (1.4.2)) et faisons $\chi_i = \theta^{h_i}$; (1.2.2) devient

$$B(i, y) = \sum_{j_i=1}^{\delta_i - 1} \bar{\theta}^{j_i h_i}(ya_i)\, \tau(\theta^{j_i h_i}). \tag{1.2.3}$$

Notons J l'ensemble des vecteurs entiers $\mathbf{j} = (j_1, \ldots, j_n)$ tels que $1 \leqslant j_i \leqslant \delta_i - 1$ pour $i = 1, \ldots, n$; pour tout $\mathbf{j} \in J$, posons $s(\mathbf{j}) = j_1/\delta_1 + \ldots + j_n/\delta_n$; désignons par I le sous-ensemble de J formé des $\mathbf{j}$ tels que $s(\mathbf{j})$ soit entier; enfin, pour tout $\mathbf{j} \in J$, posons

$$C(\mathbf{j}) = \prod_{i=1}^{n} \bar{\theta}^{j_i h_i}(a_i); \qquad T(\mathbf{j}) = \prod_{i=1}^{n} \tau(\theta^{j_i h_i}). \tag{1.2.4}$$

Avec ces notations, (1.2.1) et (1.2.3) donnent

$$N = q^{n-1} + q^{-1} \sum_{\mathbf{j} \in J} S(\mathbf{j})\, C(\mathbf{j})\, T(\mathbf{j}), \tag{1.2.5}$$

$S(\mathbf{j})$ désignant (provisoirement) la quantité $\sum_{y \in k^*} \theta^{(q-1)s(\mathbf{j})}(y)$; mais les relations d'orthogonalité (1.1.1) (chap. 5, sect. 1.1) montrent que $S(\mathbf{j}) = 0$, *sauf si* $(q-1)\, s(\mathbf{j})$ *est divisible par* $q-1$ (c'est-à-dire si $s(\mathbf{j})$ est entier, donc par définition si $\mathbf{j} \in I$) *auquel cas* $S(\mathbf{j}) = q-1$; cette remarque permet, dans (1.2.5), de limiter la sommation aux $\mathbf{j} \in I$, et de remplacer tous les termes $S(\mathbf{j})$ par $q-1$; on arrive ainsi au résultat suivant:

THÉORÈME 1. — *L'ensemble* I *et les quantités* $C(\mathbf{j})$ *et* $T(\mathbf{j})$ *étant définis comme ci-dessus, le nombre* N *de solutions dans* k^n *de l'équation diagonale* $F = 0$ *est donné exactement par*

$$N = q^{n-1} + q^{-1}(q-1) \sum_{\mathbf{j} \in I} C(\mathbf{j})\, T(\mathbf{j}). \tag{1.2.6}$$

COROLLAIRE 1. — *Si* $A_1 = \mathrm{card}\,(I)$, *on a l'inégalité*

$$|N - q^{n-1}| \leqslant A_1 (q-1)\, q^{(n/2)-1}. \tag{1.2.7}$$

Démonstration. — Il suffit de remarquer que, dans la formule (1.2.6), chaque quantité $C(\mathbf{j})$ est une racine de l'unité, donc un nombre complexe de module 1, et que chaque quantité $T(\mathbf{j})$ est un produit de n sommes de Gauss non triviales relatives à k, donc un nombre complexe de module $q^{n/2}$ (chap. 5, prop. 8).

COROLLAIRE 2. — *Si* $A_2 = \mathrm{card}\,(J) = (\delta_1 - 1) \ldots (\delta_n - 1)$, *on a l'inégalité*

$$|N - q^{n-1}| \leqslant A_2 q^{n/2}. \tag{1.2.8}$$

Démonstration. — C'est une conséquence immédiate de (1.2.7), puisque $A_1 \leqslant A_2$ (en effet, $I \subset J$) et que $q - 1 \leqslant q$.

La constante A_2 ne dépend essentiellement que du degré $d = \sup d_i$ de F, et du nombre de variables n figurant dans F; d'autre part, pour $n \geqslant 3$, on a évidemment $n/2 \leqslant n - (3/2)$; le corollaire 2 permet donc d'énoncer ceci:

COROLLAIRE 3. — *Il existe une constante* A_2 *ne dépendant que du degré et du nombre de variables de* F, *et telle que (si* $n \geqslant 3$*)*

$$|N - q^{n-1}| \leqslant A_2 q^{n-(3/2)}. \tag{1.2.9}$$

Ainsi, pour $n \geqslant 3$, l'hypersurface $F = 0$ (qui est alors absolument irréductible, ce qui ne serait pas le cas pour $n \leqslant 2$) a un nombre N de points rationnels sur k qui est voisin (en un sens bien précis) de q^{n-1}: ce q^{n-1}

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 $N \geqslant 1$: 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 $X_2, \ldots, X_n$ 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 $i = 1, \ldots, n$; 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 $L(U) = L(U_1, \ldots, U_n)$ la forme linéaire $b^{-1}a_1U_1 + \ldots + b^{-1}a_nU_n$, et pour tout i ($1 \leqslant i \leqslant n$) 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)