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: §4. Equations multilinéaires.
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: 15.07.2025

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

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 $X_{n-d+1} \dots X_n$, 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,

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

($a_1, \dots, a_n, b \in k$); 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:

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

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

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 $a Y_n^2$, on obtient, avec les notations de la section 4.1,

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

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

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

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

(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).