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: §3. Equations diagonales quelconques.
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: 05.07.2025

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

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 $k_d = \mathbf{F}_{q_1}$; 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

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.)

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

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 $\bar{N}$ est donné par la formule

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

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 $\bar{N} = 0$.

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

(*H*2) $\quad 1/d_1 + \ldots + 1/d_n > 1,$

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) $\quad$ *Chaque* δ_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*

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

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