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. Démonstration du théorème 1.
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

Ces diverses propriétés étant établies, prouvons maintenant (toujours en supposant $0 \leqslant j < q - 1$) que $\sigma(j) = s(j)$; les propriétés (i), puis (v), puis (ii) et (iii), montrent d'abord que pour $0 \leqslant j \leqslant p - 1$, on a $s(j) = j = j_0 = \sigma(j)$; les propriétés (ii) et (iv) donnent d'autre part

$$s(j) \leqslant s(j_0) + s(j_1) + \ldots + s(j_{f-1});$$

comme $0 \leqslant j_i \leqslant p - 1$ pour $i = 0, \ldots, f - 1$, ces deux remarques impliquent, pour $0 \leqslant j < q - 1$,

$$s(j) \leqslant j_0 + j_1 + \ldots + j_{f-1} = \sigma(j); \tag{1.4.9}$$

l'égalité $s(j) = \sigma(j)$ résulte alors de (1.4.9), de la propriété (vi), et de l'égalité $\sum_{0 \leqslant j < q-1} \sigma(j) = f(p-1)(q-2)/2$, qui se vérifie facilement par récurrence sur f. La proposition 1 se trouve ainsi démontrée.

§ 2. *Démonstration du théorème* 1.

Cette démonstration se fera en quatre étapes.

2.1. *Introduction du polynôme* $C(Y)$. Soit T le sous-ensemble de B formé de 0 et des éléments de T^*; pour tout $t \in T$, soit $\bar{t}$ l'image de t dans $k = B/\mathfrak{P}$; l'application $t \mapsto \bar{t}$ est alors une bijection de T sur k (sect. 1.1 et 1.2), dont la bijection inverse est le caractère θ, prolongé comme toujours par $\theta(0) = 0$. Soit d'autre part β le caractère additif de k défini par $\beta(x) = \zeta^{Tr(x)}$ $(x \in k)$; comme card $(T) = q$, il existe évidemment un polynôme à une variable Y et un seul, soit $C(Y)$, de degré $q - 1$, à coefficients dans L, et tel que $C(t) = \beta(\bar{t})$ pour tout $t \in T$; posons

$$C(Y) = c_0 + c_1 Y + \ldots + c_{q-1} Y^{q-1}. \tag{2.1.1}$$

LEMME 1. — *Avec les notations du paragraphe* 1, *on a*

$$c_0 = 1;\ c_{q-1} = -q/(q-1);\ \textit{et}\ c_j = \tau(j)/(q-1) \quad \textit{pour}\ 1 \leqslant j \leqslant q - 2. \tag{2.1.2}$$

En effet, pour $0 \leqslant j \leqslant q - 1$, on a, par définition de $\tau(j)$, de θ et de $C(Y)$,

$$\tau(j) = \sum_{x \in k^*} \theta^{-j}(x)\beta(x) = \sum_{t \in T^*} t^{-j}\beta(\bar{t}) = \sum_{t \in T^*} t^{-j} C(t);$$

il suffit alors, pour obtenir les relations (2.1.2), de remplacer, dans le membre de droite, $C(t)$ par son expression développée $c_0 + c_1 t + \ldots + c_{q-1} t^{q-1}$, et de remarquer comme au paragraphe 1 que

$$(2.1.3) \qquad \sum_{t \in T^*} t^u = \begin{cases} q-1\,, & \text{si } u \equiv 0 \pmod{q-1}\,; \\ 0\,, & \text{sinon.} \end{cases}$$

LEMME 2. — *Avec les notations du paragraphe* 1, *on a, pour tout j tel que* $0 \leqslant j \leqslant q-1$, *l'égalité*

$$(2.1.4) \qquad \operatorname{ord}(c_j) = \sigma(j)\,.$$

Si $0 \leqslant j < q-1$, il suffit d'appliquer le lemme 1, la proposition 1, et de remarquer que $\operatorname{ord}\big(1/(q-1)\big) = 0$. Si $j = q-1$, on a $j_0 = j_1 = \ldots = j_{f-1} = p-1$, donc $\sigma(j) = f(p-1)$; on a d'autre part (lemme 1) $\operatorname{ord}(c_j) = \operatorname{ord}\big(-q/(q-1)\big) = \operatorname{ord}(q) = \operatorname{ord}(p^f) = f \operatorname{ord}(p) = f(p-1)$ (sect. 1.3); d'où $\operatorname{ord}(c_j) = \sigma(j)$ également pour $j = q-1$.

2.2. *Evaluation de N à l'aide des c_j.* Commençons par introduire un supplément de notations; $\mathbf{x} = (x_0, \ldots, x_n)$ désignera un point quelconque de k^{n+1}; U désignera l'ensemble des suites $\mathbf{u} = (u_1, \ldots, u_n)$ d'entiers rationnels non négatifs telles que $\|\mathbf{u}\| = u_1 + \ldots + u_n \leqslant d = \deg(F)$; enfin, si $\mathbf{u} \in U$, $X^{\mathbf{u}}$ désignera le monôme $X_1^{u_1} \ldots X_n^{u_n}$, $\mathbf{u}'$ désignera la suite $(1, u_1, \ldots, u_n)$, et $X^{\mathbf{u}'}$ désignera le monôme $X_0 X_1^{u_1} \ldots X_n^{u_n} = X_0 X^{\mathbf{u}}$; convention analogue pour $\mathbf{x}^{\mathbf{u}}$ et $\mathbf{x}^{\mathbf{u}'}$ si $\mathbf{x} \in k^{n+1}$, etc.

Cela étant, on a (chap. 5, prop. 3)

$$(2.2.1) \qquad N = q^{-1} \sum_{\mathbf{x} \in k^{n+1}} \beta\big(x_0 F(x_1, \ldots, x_n)\big)\,;$$

d'autre part, on peut écrire (en notant $a_{\mathbf{u}}$ ($\mathbf{u} \in U$) les coefficients de F) $F(X_1, \ldots, X_n) = \sum_{\mathbf{u} \in U} a_{\mathbf{u}} X^{\mathbf{u}}$, donc $X_0 F(X_1, \ldots, X_n) = \sum_{\mathbf{u} \in U} a_{\mathbf{u}} X^{\mathbf{u}'}$; comme β est un caractère additif, (2.2.1) peut se réécrire

$$(2.2.2) \qquad N = q^{-1} \sum_{\mathbf{x} \in k^{n+1}} \prod_{\mathbf{u} \in U} \beta(a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'})\,.$$

Posons alors, quels que soient $\mathbf{u} \in U$ et $x_i \in k$, $b_{\mathbf{u}} = \theta(a_{\mathbf{u}})$ et $t_i = \theta(x_i)$; posons également $\mathbf{t} = (t_0, \ldots, t_n)$; on a $b_{\mathbf{u}} \in T$, $t_i \in T$, $b_{\mathbf{u}} t^{\mathbf{u}'} \in T$, et $\bar{b}_{\mathbf{u}} \bar{\mathbf{t}}^{\mathbf{u}'} = a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'}$; ainsi,

$$\beta(a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}'}) = C(b_{\mathbf{u}} \mathbf{t}^{\mathbf{u}'}) = \sum_{0 \leqq j \leqq q-1} c_j b_{\mathbf{u}}^{\,j} \mathbf{t}^{j\mathbf{u}'}\,,$$

$\mathbf{t}^{ju'}$ signifiant évidemment $t_0{}^j t_1{}^{ju_1} \dots t_n{}^{ju_n}$; et (2.2.2) devient

$$(2.2.3) \qquad N = q^{-1} \sum_{\mathbf{t} \in T^{n+1}} \prod_{\mathbf{u} \in U} \sum_{0 \leq j \leq q-1} c_j b_{\mathbf{u}}{}^j \mathbf{t}^{ju'} .$$

Soit M l'ensemble de toutes les applications de U dans $\{0, 1, \dots, q-1\}$ (c'est-à-dire l'ensemble de toutes les « façons d'associer un j à chaque $\mathbf{u}$ »); la distributivité de la multiplication par rapport à l'addition permet de mettre le second membre de (2.2.3) sous la forme

$$q^{-1} \sum_{j \in M} \sum_{\mathbf{t} \in T^{n+1}} \prod_{\mathbf{u} \in U} c_{j(\mathbf{u})} b_{\mathbf{u}}{}^{j(\mathbf{u})} \mathbf{t}^{j(\mathbf{u})\mathbf{u}'} .$$

Pour chaque $j \in M$, posons $b^{(j)} = \prod_{\mathbf{u} \in U} b_{\mathbf{u}}{}^{j(\mathbf{u})}$ ($b^{(j)}$ est donc un élément de T), et désignons par $\mathbf{e}_j{}'$ la suite

$$\sum_{\mathbf{u} \in U} j(\mathbf{u})\, \mathbf{u}' = \left(\sum j(\mathbf{u}), \sum j(\mathbf{u})\, u_1, \dots, \sum j(\mathbf{u})\, u_n\right).$$

L'égalité (2.2.3) peut alors s'écrire

$$(2.2.4) \qquad N = q^{-1} \sum_{j \in M} b^{(j)} \prod_{\mathbf{u} \in U} c_{j(\mathbf{u})} \sum_{\mathbf{t} \in T^{n+1}} \mathbf{t}^{\mathbf{e}_j{}'} .$$

2.3. *Réduction du problème.* Dans (2.2.4), tous les termes du membre de droite (abstraction faite du facteur q^{-1}) sont dans l'anneau B des entiers de L; il suffit donc pour prouver le théorème 1 de montrer ceci:

(2.3.1) *Quel que soit $j \in M$, l'entier algébrique $\prod_{\mathbf{u} \in U} c_{j(\mathbf{u})} \sum_{\mathbf{t} \in T^{n+1}} \mathbf{t}^{\mathbf{e}_j{}'}$ est divisible (dans B) par q^{b+1}.*

Convenons d'écrire $q - 1 \mid \mathbf{e}_j{}'$ si $q - 1$ divise chacune des $n + 1$ composantes de $\mathbf{e}_j{}'$, et $q - 1 \nmid \mathbf{e}_j{}'$ dans le cas contraire; d'après (2.1.3), on a

$$(2.3.2) \qquad \sum_{\mathbf{t} \in T^{n+1}} \mathbf{t}^{\mathbf{e}_j{}'} = \begin{cases} q^{n+1}, \text{ si } \mathbf{e}_j{}' = (0, 0, \dots, 0); \\ 0, \text{ si } q - 1 \nmid \mathbf{e}_j{}'; \\ (q-1)^{s+1} q^{n-s}, \text{ si } \mathbf{e}_j{}' \neq (0, 0, \dots, 0), \text{ si } q - 1 \mid \mathbf{e}_j{}', \\ \text{et si } \mathbf{e}_j \text{ (c'est-à-dire } \mathbf{e}_j{}' \text{ privé de sa première composante) possède exactement } s \text{ composantes non nulles;} \end{cases}$$

et il suffit en fait, pour établir (2.3.1), donc le théorème 1, de prouver ceci:

LEMME 3. — *Si $j \in M$ est tel que $\mathbf{e}_j'$ soit différent de* $(0, 0, \ldots, 0)$, *soit « divisible » par $q - 1$, et que $\mathbf{e}_j$ possède exactement s composantes non nulles, alors l'entier algébrique $q^{n-s} \prod_{\mathbf{u} \in U} c_{j(\mathbf{u})}$ est divisible (dans B) par q^{b+1}.*

2.4. *Démonstration du lemme* 3. Pour tout $\mathbf{u} \in U$ et tout $j \in M$, écrivons l'entier $j(\mathbf{u})$ en base p:

$$j(\mathbf{u}) = j_0(\mathbf{u}) + j_1(\mathbf{u})\, p + \ldots + j_{f-1}(\mathbf{u})\, p^{f-1}$$

$(0 \leqslant j_i(\mathbf{u}) \leqslant p - 1;\ 0 \leqslant i \leqslant f - 1)$; ceci définit $j_i(\mathbf{u})$ pour $0 \leqslant i < f$; étendons cette définition en convenant de poser, pour tout entier rationnel z, $j_z(\mathbf{u}) = j_{i(z)}(\mathbf{u})$, où $i(z)$ est le reste de division de z par f; enfin, pour tout entier rationnel h, posons

$$j^{(h)}(\mathbf{u}) = j_{-h}(\mathbf{u}) + j_{1-h}(\mathbf{u})\, p + \ldots + j_{f-1-h}(\mathbf{u})\, p^{f-1}$$

(les $j^{(h)}(\mathbf{u})$ sont les entiers rationnels déduits de $j(\mathbf{u})$ par permutation circulaire des chiffres de $j(\mathbf{u})$ en base p). Il est clair qu'on ne change rien aux égalités (2.3.2) en y remplaçant j par $j^{(h)}$, ce qui équivaut à effectuer sur T la permutation $t \mapsto t^{p^h}$; en particulier, cette substitution ne modifie pas la valeur de s; ainsi, sous les hypothèses du lemme 3, on a

$$(2.4.1) \qquad s(q-1) \leqslant \| \mathbf{e}_{j(h)} \| = \| \sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u})\, u \| \leqslant d \sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u}) .$$

Mais $\sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u})$ est la première composante de $\mathbf{e}_{j(h)}'$: c'est donc (toujours avec les hypothèses du lemme 3) un entier strictement positif divisible par $q - 1$; si $(s/d)^*$ désigne le plus petit entier supérieur ou égal à s/d, (2.4.1) implique alors

$$(q-1)(s/d)^* \leqslant \sum_{\mathbf{u} \in U} j^{(h)}(\mathbf{u}) ;$$

dans cette égalité, donnons à h les valeurs $0, 1, \ldots, f - 1$, et additionnons; compte tenu de la définition de $j^{(h)}(\mathbf{u})$, il vient

$$f(q-1)(s/d)^* \leqslant \sum_{0 \leqslant h \leqslant f-1} \sum_{\mathbf{u} \in U} \sum_{0 \leqslant i \leqslant f-1} j_{i-h}(\mathbf{u})\, p^i ,$$

ou encore (en intervertissant l'ordre des sommations, en utilisant la notation $\sigma(j)$, et en remplaçant q par p^f),

$$f(p^f - 1)(s/d)^* \leqslant (p^{f-1} + \ldots + p + 1) \sum_{\mathbf{u} \in U} \sigma(j(\mathbf{u})) .$$

Comme $\sum_{\mathbf{u}\in U} \sigma(j(\mathbf{u})) = \operatorname{ord}\left(\prod_{\mathbf{u}\in U} c_{j(\mathbf{u})}\right)$ (lemme 2 et première formule (1.3.1)), cette dernière inégalité peut s'écrire, après division par $p^{f-1} + \ldots + p + 1$,

$$f(p-1)(s/d)^* \leqslant \operatorname{ord}\left(\prod_{\mathbf{u}\in U} c_{j(\mathbf{u})}\right);$$

compte tenu de (1.3.1) et (1.3.4), on a alors

$$f(p-1)(n-s+(s/d)^*) \leqslant \operatorname{ord}\left(q^{n-s}\prod_{\mathbf{u}\in U} c_{j(\mathbf{u})}\right). \tag{2.4.2}$$

Mais le symbole ord est relatif à *n'importe quel* idéal premier $\mathfrak{P}$ de B divisant p, et on a (sect. 1.1, (1.1.3)) $pB = \prod_{\mathfrak{P}|p} \mathfrak{P}^{p-1}$, donc, puisque $q = p^f$, $qB = \prod_{\mathfrak{P}|p} \mathfrak{P}^{f(p-1)}$; ainsi, étant donné (2.4.2), il suffit, pour prouver le lemme 3 (donc le théorème 1), d'établir la propriété suivante:

(2.4.3) *Pour tout entier s tel que $0 \leqslant s \leqslant n$, on a l'inégalité*

$$n - s + (s/d)^* \geqslant b + 1 .$$

Démontrons (2.4.3); il est clair que pour tout entier positif t, on a $t \geqslant ((s+t)/d)^* - (s/d)^*$: car, pour $t = 0$, les deux membres sont égaux, et d'autre part le membre de droite, considéré comme fonction de t, croît « moins vite » que t; dans cette inégalité, faisons alors $t = n - s$; il vient

$$n - s + (s/d)^* \geqslant (n/d)^* ;$$

mais par définition même $(n/d)^* = b + 1$: ce qui prouve (2.4.3) et achève la démonstration du théorème 1.

§ 3. *Généralisations et compléments.*

3.1. Le théorème 1 s'étend sans difficulté au cas d'un système d'équations:

THÉORÈME 2. — *Soit $F_1, \ldots, F_s$ une famille de s polynômes de degrés respectifs $d_1, \ldots, d_s$, à n variables et à coefficients dans k; posons $d = d_1 + \ldots + d_s$, et soit b le plus grand entier strictement inférieur à n/d. Si alors N désigne le nombre de solutions dans k^n du système d'équations*

$$F_1 = 0, \ldots, F_s = 0 , \tag{3.1.1}$$

N est divisible par q^b.

Démonstration. — On se sert du lemme combinatoire suivant: