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. Le « second » théorème de Warning.

DOI: https://doi.org/10.5169/seals-46287

§ 3. *Le « second » théorème de Warning.*

3.1. Il s'agit du résultat suivant, établi par Warning, en même temps que le théorème 1, dans son article déjà cité (Warning (1935)):

THÉORÈME 3. — *Mêmes données et hypothèses (en particulier $n > d$) que dans le théorème* 1. *Alors, si $N > 0$ (donc si le système (*1.1.1*) admet au moins une solution), on a en fait $N \geqslant q^{n-d}$.*

Démonstration. — Plaçons-nous dans l'espace affine k^n, et soit toujours V l'ensemble des solutions de (1.1.1); pour abréger, convenons (dans cette section seulement) de dire *variété* au lieu de *sous-variété affine de k^n*; *alors :*

LEMME 1. — *Si W_1 et W_2 sont deux variétés parallèles de dimension $d = d_1 + \ldots + d_s$ (voir th.* 1*), on a la congruence*

$$\operatorname{card}(W_1 \cap V) \equiv \operatorname{card}(W_2 \cap V) \pmod{p}. \tag{3.1.1}$$

Prouvons ce lemme. On peut se limiter au cas où $W_1 \neq W_2$, puis, quitte à effectuer un changement de coordonnées dans k^n (ce qui ne modifie pas les d_j), supposer que W_1 et W_2 sont définies respectivement par les systèmes d'équations $X_1 = 0$, $X_2 = 0, \ldots, X_{n-d} = 0$, et $X_1 = 1$, $X_2 = 0, \ldots, X_{n-d} = 0$. Introduisons le polynôme (à une seule variable T)

$$R(T) = T^{q-1} - 1 = \prod_{a \in k^*} (T - a),$$

puis le polynôme (à n variables $X_1, \ldots, X_n$, mais ne dépendant en fait que de $X_1, \ldots, X_{n-d}$)

$$G(X) = (-1)^{n-d} R(X_2) \ldots R(X_{n-d}) \prod_{a \neq 0,1} (X_1 - a);$$

G est un polynôme de degré total $(n-d)(q-1) - 1$; de plus, il vaut évidemment -1 sur W_1, 1 sur W_2 et 0 ailleurs; $\bar{F}$ désignant toujours le polynôme défini par (1.1.2) (sect. 1.1), $H = G\bar{F}$ est donc un polynôme à n variables, de degré total $(n-d)(q-1) - 1 + d(q-1) = n(q-1) - 1 < n(q-1)$, et ce polynôme vaut -1 sur $W_1 \cap V$, 1 sur $W_2 \cap V$, et 0 partout ailleurs; d'où:

$$\sum_{\mathbf{x} \in k^n} H(\mathbf{x}) = \big(\operatorname{card}(W_2 \cap V) - \operatorname{card}(W_1 \cap V)\big) . 1; \tag{3.1.2}$$

mais le théorème 2 est applicable à H: le second membre de (3.1.2) est donc égal à 0, dans le corps k de caractéristique p, ce qui équivaut à (3.1.1), et prouve le lemme 1.

Passons à la démonstration du théorème 3, et distinguons deux cas:

(1) *Il existe au moins une variété W de dimension d telle que* card $(W \cap V) \not\equiv 0 \pmod{p}$: le lemme 1 montre alors que pour toute variété W' parallèle à W et de même dimension d, on a également card $(W' \cap V) \not\equiv 0 \pmod{p}$; comme il existe exactement q^{n-d} telles variétés W' (W comprise), qu'elles forment une partition de k^n, et que chacune d'elles contient évidemment au moins un point de V, l'inégalité $N \geqslant q^{n-d}$ se trouve immédiatement établie dans ce premier cas.

(2) *Pour toute variété W de dimension d, on a* card $(W \cap V) \equiv 0 \pmod{p}$; puisque V contient (par hypothèse) au moins un point, on peut cependant affirmer ceci: il existe un entier $m\,(1 \leqslant m \leqslant d)$ possédant la propriété suivante:

> *pour toute variété M de dimension m, on a* card $(M \cap V) \equiv 0 \pmod{p}$, *mais il existe une variété L de dimension $m - 1$ telle que* card $(L \cap V) \not\equiv 0 \pmod{p}$.

Fixons une telle variété L, et désignons par a le reste de division de card $(L \cap V)$ par p; on a donc $1 \leqslant a \leqslant p - 1$. Considérons maintenant les variétés M de dimension m passant par L; il y en a exactement

$$(q^{n-m+1} - 1)/(q - 1) = q^{n-m} + \ldots + q + 1$$

(nombre de points rationnels sur k dans l'espace projectif de dimension $n - m$); chacune de ces variétés M contient au moins a points de V (ceux qui sont dans $L \cap V$), et comme par ailleurs card $(M \cap V) \equiv 0 \pmod{p}$, chaque différence ensembliste $M - L$ contient au moins $p - a \geqslant 1$ points de V; mais les différences $M - L$ forment une partition de $k^n - L$; ainsi,

$$N = \text{card}(V) > q^{n-m} + \ldots + q + 1 > q^{n-d},$$

ce qui règle le second cas et achève de prouver le théorème 3.

3.2. On verra au paragraphe suivant (sect. 4.3) que, sous les hypothèses du théorème 3, l'inégalité $N \geqslant q^{n-d}$ est la meilleure possible.

§ **4.** *Polynômes normiques et théorème de Terjanian.*

4.1. Le théorème 1 utilise de façon essentielle l'hypothèse $n > d$. Si $n \leqslant d$, il tombe en défaut, comme on peut le voir sur l'exemple suivant (dans cet exemple et dans tout le reste de ce chapitre, on se limite au cas d'un seul polynôme: $s = 1$):