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. Généralisations et compléments.
DOI: https://doi.org/10.5169/seals-46287

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

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

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

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

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:

LEMME 1. — *Soit $V_1, ..., V_s$ une famille de s ensembles finis. Posons $V = \bigcap_{i \leq j \leq s} V_j$, et, pour toute partie R de $S = \{1, ..., s\}$, posons $U_R = \bigcup_{j \in R} V_j$ (pour $R = \emptyset$, $U_R = \emptyset$). On a alors*

$$\text{card}(V) = \sum_{R \subset S} (-1)^{\text{card}(R)-1} \text{card}(U_R). \tag{3.1.2}$$

Ce lemme se prouve facilement par récurrence sur s. Appliquons-le à la démonstration du théorème 2: pour tout $j \in S = \{1, ..., s\}$, soit V_j l'ensemble des zéros dans k^n de l'unique polynôme F_j; avec les notations du lemme, V est alors l'ensemble des solutions dans k^n du système (3.1.1), on a $N = \text{card}(V)$, et (3.1.2) montre qu'il suffit de prouver que, pour chaque $R \subset S$, card (U_R) est divisible par q^b. Si $R = \emptyset$, $U_R = \emptyset$, card $(U_R) = 0$, et il n'y a rien à démontrer; sinon, posons $F_R = \prod_{j \in R} F_j$: U_R est alors l'ensemble des zéros dans k^n du polynôme F_R, et si b_R est le plus grand entier strictement inférieur à $n/\deg(F_R)$, le théorème 1 montre que card (U_R) est divisible par q^{bR}; mais $\deg(F_R) = \sum_{j \in R} \deg(F_j) \leqslant \sum_{j \in S} \deg(F_j) = d$, d'où $n/d \leqslant n/\deg(F_R)$ et $b \leqslant b_R$; card (U_R), divisible par q^{bR}, est divisible a fortiori par q^b, C.Q.F.D.

3.2. Le théorème 1, pour *une* équation, est « le meilleur possible » au sens suivant: *quels que soient n et d, il existe F, de degré d, à n variables et à coefficients dans k, tel que (avec les notations du théorème 1) q^b soit la plus haute puissance de q divisant N.* (Prendre par exemple pour F le polynôme $G_{n,d} = X_1 \ldots X_d + X_{d+1} \ldots X_{2d} + \ldots + X_{(b-1)d+1} \ldots X_{bd} + X_{bd+1} \ldots X_n$; pour ce polynôme, le nombre N peut être déterminé explicitement à l'aide du théorème 6 du chapitre 4: on laisse au lecteur le soin de faire les calculs en détail). En revanche, le théorème 2, pour un système de s équations, peut être amélioré; en fait, on a le résultat suivant, dû à Katz (1971):

THÉORÈME 3. — *Mêmes données et notations que dans le théorème 2. Si $\delta = \sup_{1 \leq j \leq s} d_j$, et si b_1 désigne le plus grand entier supérieur ou égal à $(n-d)/\delta$, alors N est divisible par q^{b1}.*

Ce théorème 3 (qui, pour $s = 1$, coïncide évidemment avec le théorème 1) est lui-même « le meilleur possible »; en fait, on peut montrer (en utilisant des polynômes du type $G_{n,d}$ ci-dessus et des polynômes normiques, et en raisonnant comme au chapitre 4, section 4.3) que, *quels que soient n, s, et $d_1, ..., d_s$, il existe une famille $F_1, ..., F_s$ satisfaisant aux hypothèses des*

théorèmes 2 et 3 et telle que N soit égal exactement à q^{b_1}. Pour la construction d'une telle famille de polynômes, et pour la démonstration du théorème 3, voir Katz (1971) (respectivement § 4 et § 3); voir également les Notes en fin de chapitre.

3.3. Pour des équations *de forme particulière*, le théorème 1 peut dans certains cas être amélioré. Ainsi, en combinant le théorème 1 du chapitre 6 avec les « relations de Stickelberger » (prop. 1), on obtient sans difficulté le résultat suivant:

THÉORÈME 4. — *Soit* $F = a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n}$ *un polynôme diagonal à coefficients dans le corps premier* $k = \mathbf{F}_p$. *Pour* $i = 1, \ldots, n$, *posons* $\delta_i = (p-1, d_i)$, *et soit* b_2 *le plus grand entier strictement inférieur à* $1/\delta_1 + \ldots + 1/\delta_n$. *Alors, si* $a \in k$, *et si N désigne le nombre de solutions dans* k^n *de l'équation* $F = a$, *N est divisible par* p^{b_2}.

Ce résultat reste d'ailleurs vrai sur un corps fini quelconque k à $q = p^f$ éléments, à condition de supposer que chaque $\delta_i = (q-1, d_i)$ divise $p - 1$: N est alors divisible par q^{b_2}; cet exposant b_2 peut encore être « amélioré » si $a = 0$ (voir Joly (1971)). On notera l'analogie entre le théorème 4 ci-dessus et le théorème 3 du chapitre 4.

Notes sur le chapitre 7

§ **1**: la démonstration de la proposition 1 donnée ici est due à Hilbert (« Zahlbericht »); cette proposition est en fait une conséquence d'un résultat plus précis (« congruences de Stickelberger »):

$$\tau(j) \equiv -\lambda^{\sigma(j)}/\rho(j) \pmod{\mathfrak{P}^{\sigma(j)+1}}$$

(avec par définition $\rho(j) = j_0!\, j_1!\, \ldots\, j_{f-1}!$); voir Stickelberger (1890), Davenport-Hasse (1934), ou [11], chap. IV, § 3. Pour une interprétation analytique p-adique de ces congruences, voir Dwork (1960).

§ **2-3**: dans Ax (1964), le cadre de la démonstration du théorème 1 est, non pas le corps de nombres $L = \mathbf{Q}(\omega, \zeta)$, mais le corps $\mathbf{Q}_p(\omega, \zeta)$ des racines $p(q-1)$-ièmes de l'unité dans une clôture algébrique du corps p-adique $\mathbf{Q}_p$ (avec les notations du § 1, ce corps $\mathbf{Q}_p(\omega, \zeta)$ est d'ailleurs isomorphe à $L_{\mathfrak{P}}$, complété $\mathfrak{P}$-adique de L); à cette différence près, la démonstration donnée ici est exactement celle d'Ax; elle est (selon Ax lui-même) « suggérée par certaines idées de Dwork [dans sa démonstration