SÉMINAIRE N. BOURBAKI

JEAN DELSARTE

Nombre de solutions des équations polynomiales sur un corps fini

Séminaire N. Bourbaki, 1952, exp. n° 39, p. 321-329

<http://www.numdam.org/item?id=SB_1948-1951__1__321_0>

Séminaire BOURBAKI
(Mars 1951)

NOMBRE DE SOLUTIONS DES ÉQUATIONS POLYNOMIALES SUR UN CORPS FINI [2]

par Jean DELSARTE.

1. Sommes de Gauss sur un corps fini.

Soit K un corps fini à q éléments ; on notera K^0 le groupe multiplicatif de ses éléments inversibles. Soient encore

χ un caractère multiplicatif non principal,

ψ un caractère additif distinct de l'unité.

Une somme de Gauss sur K est donnée par la formule

$$g(\chi) = \Sigma \chi(x)\ \psi(x)$$

où x décrit K ou K^0, au choix, puisque $\psi(0)$ est nul. Le changement de x en tx, où t appartient à K^0, donne

$$g(\chi) = \chi(t)\ \Sigma \chi(x)\psi(tx)$$

ce qui prouve que le changement du caractère additif ψ en un autre dans la définition de la somme de Gauss ne fait que multiplier celle-ci par un facteur connu.

Il existe une proposition classique sur la valeur du module d'une somme de Gauss ; on a

$$g(\chi)\ \overline{g}(\chi) = \sum_{x\neq 0} \sum_{y\neq 0} \chi(xy^{-1})\psi(x-y) = \sum_{x\neq 0} \chi(x).\ \sum_{y\neq 0} \psi[(x-1)y]$$

ou la sommation en y sur K^0 donne $q-1$, si $x = 1$, et -1 dans le cas contraire. On en déduit immédiatement que

$$|g(\chi)| = \sqrt{q}$$

2. Extensions finies d'un corps fini : théorème de Hasse-Davenport.

Soit K' une extension finie de K, de degré ν sur K ; pour y dans K', désignons par $N(y)$ et $T(y)$ la norme et la trace de y sur K. Il existe un générateur z de K'^0 tel que $N(z) = w$, où w est un générateur de K^0. Soient alors χ'_α et χ_α les caractères multiplicatifs de K' et de K respectivement, qui sont tels que

$$\chi'_\alpha(z) = \chi_\alpha(w) = \exp(2\pi i\alpha)$$

où α est un rationnel tel que $(q-1)\alpha \equiv 0 \pmod 1$. On sait alors que l'on a

$$\chi'_\alpha(y) = \chi_\alpha[N(y)]$$

On prolonge de même le caractère additif ψ sur K' par la formule

$$\psi'(y) = \psi[T(y)]$$

Soient alors $g'(\chi'_\alpha)$ la somme de Gauss sur K' relative au caractère additif ψ' et $g(\chi_\alpha)$ la somme de Gauss sur K relative au caractère additif ψ. Le théorème de Hasse-Davenport affirme que l'on a

$$-g'(\chi'_\alpha) = [-g(\chi_\alpha)]^\nu$$

REMARQUE. - La définition des sommes de Gauss s'étend facilement au cas où on les calcule pour le caractère multiplicatif principal χ_0 ; elles valent alors -1 ; le théorème de Hasse-Davenport s'étend encore à ce cas, mais le théorème donnant le module d'une somme de Gauss n'est plus valable.

Je renvoie au mémoire de WEIL [2] ou à celui de HASSE [1] pour la démonstration. On utilise une fonction L sur l'anneau des polynomes sur K ; considérons ceux qui sont unitaires :

$$F(X) = X^n + c_1 X^{n-1} + \ldots + c_n \qquad (n \geqslant 1)$$

Soit

$$\lambda(F) = \chi_\alpha(c_n)\,\psi(c_1)$$

on a

$$\lambda(F_1 \cdot F_2) = \lambda(F_1)\,\lambda(F_2)$$

On notera $n(F)$ le degré d'un polynome unitaire F ; soit U une indéterminée, il vient formellement

$$1 + \sum_F \lambda(F)\, U^{n(F)} = \prod_P [1 - \lambda(P)\, U^{n(P)}]^{-1}$$

Au premier membre, la somme est étendue à tous les polynomes F unitaires de degré au moins égal à 1 ; au second membre, le produit est étendu aux polynomes unitaires irréductibles sur K. On vérifie qu'en fait seuls interviennent au premier membre les polynomes du premier degré, ce qui fournit la formule

$$1 + g(\chi_\alpha)U = \prod_P [1 - \lambda(P)\, U^{n(P)}] - 1$$

Il y a une formule du même type pour l'extension K' . En examinant ensuite les facteurs irréductibles P' , sur K' , d'un polynome unitaire P , irréductible sur K , et en comparant les normes et les traces, on constate que $\lambda'(P')$ est une certaine puissance entière de $\lambda(P)$, d'où résulte ensuite sans peine la formule de Hasse-Davenport.

3. Quelques formules énumératives.

Soit E_s l'espace à s dimensions sur K , regardé comme le produit direct de s anneaux identiques à K . Dans cet espace considérons la variété définie par l'équation

$$\mathcal{F} \equiv \sum_{i=1}^{r} a_i x_1^{m_{1i}} \dots x_s^{m_{si}} = 0$$

où les a_i appartiennent à K^0 , $(i = 1 , 2 , \dots , r)$, équation sans terme constant. Le nombre d'éléments de K , à savoir q , est supposé assez grand pour que $q - 1$ ne divise aucun des exposants positifs m_{ij} . Soit ψ un caractère additif sur K ; nous nous proposons d'abord de calculer la somme $S = \sum \psi(\mathcal{F})$ où les x_j , $(j = 1 , 2 , \dots , s)$ décrivent indépendamment K . On commencera par calculer la somme $\overline{S}$ obtenue en supposant seulement que les x_j décrivent indépendamment K^0 .

Soit donc

$$(1) \qquad y_i = x_1^{m_{1i}} \dots x_s^{m_{si}} \quad ; \quad (i = 1 , 2 , \dots , r)$$

où le point $x = (x_1 , x_2 , \dots , x_s)$ décrit le groupe des éléments inversibles de l'anneau E_s , produit direct du corps K , s fois par lui-même, (variété de Véronèse). Les formules (1) définissent un homomorphisme de E_s^0 dans E_r^0 , les notations étant évidentes. Soit N le noyau de cet homomorphisme, soit d le nombre de points de ce noyau, soit G l'image ; on a évidemment

$$(2) \qquad \overline{S} = \sum \psi(\mathcal{F}) = d \sum \psi(ay)$$

où $a = (a_1 , a_2 , \dots , a_r)$ est un point de E_r^0 et où y décrit G . Le produit ay est calculé dans l'anneau E_r , et ψ est un caractère additif particulier de cet anneau.

Soit maintenant χ un caractère du groupe des éléments inversibles de E_r ; on a, pour $y = (y_1 , y_2 , \dots , y_r)$ appartenant à E_r^0

$$\chi(y) = \chi_1(y_1) \chi_2(y_2) \dots \chi_r(y_r)$$

où $(\chi_1, \ldots, \chi_r)$ est un système de r caractère multiplicatifs de K. Indroduisons l'orthogonal $\tilde{G}$ du groupe G, ensemble des caractères χ tels que $\chi(y) = 1$ pour y décrivant G. Un tel caractère reste constant sur les classes modulo G dans E_r^0. Considérons maintenant la somme

$$T = \sum_{\chi \in \tilde{G}} \sum_{y \in E_r^0} \chi(y)\, \psi(ay) \tag{3}$$

Sommons d'abord en χ sur $\tilde{G}$; pour y fixé, la somme partielle vaut zéro, sauf si y appartient à G, auquel cas elle vaut $d(q-1)^{r-s}$, qui est l'ordre de G. Par suite

$$T = d(q-1)^{r-s} \sum_{y \in G} \psi(ay)$$

ou encore

$$T = (q-1)^{r-s} \cdot \overline{S}$$

d'où enfin

$$\overline{S} = \frac{1}{(q-1)^{r-s}} \cdot \sum_{\chi \in \tilde{G}} \sum_{y \in E_r^*} \chi(y)\, \psi(ay) \tag{4}$$

Introduisons maintenant les sommes de Gauss. Nous les calculerons sur K, avec le caractère additif ψ, et nous poserons, pour le caractère multiplicatif $\chi = (\chi_1, \chi_2, \ldots, \chi_r)$ de E_r^0,

$$\mathcal{G}(\chi) = g(\chi_1)\ g(\chi_2) \ldots g(\chi_r)$$

Comme $\psi(ay) = \psi(a_1 y_1) \ldots \psi(a_r y_r)$, on trouve immédiatement, d'après la définition des sommes de Gauss donnée plus haut,

$$\sum_{y \in E_r^*} \chi(y)\, \psi(ay) = \overline{\chi}(a)\, \mathcal{G}(\chi) \tag{5}$$

et par suite

$$\overline{S} = \frac{1}{(q-1)^{r-s}} \sum_{\chi \in \tilde{G}} \overline{\chi}(a)\, \mathcal{G}(\chi) \tag{6}$$

Voici une application de ce résultat. Proposons-nous de calculer le nombre de solutions, dans E_s^0, de l'équation $\mathcal{F} = 0$. Soit $\overline{N}$ ce nombre. Posons maintenant

$$\overline{S}(\psi) = \Sigma \psi(\mathcal{F})$$

où les x décrivant toujours E_s^0 ; calculons $\Sigma \overline{S}(\psi)$ quand ψ décrit l'ensemble des caractères additifs non principaux de K. Cette somme s'écrit

$$\sum_{\psi}\sum_{\chi}\psi(\mathcal{F})$$

sommant en ψ, pour x fixé, on trouve -1, si $\mathcal{F}$ n'est pas nul, et $q-1$ dans le cas contraire ; on a donc

$$\sum \overline{S}(\psi) = (q-1)\overline{N} - [(q-1)^s - \overline{N}] = q\overline{N} - (q-1)^s$$

car le nombre des x pour lesquels $\mathcal{F}$ n'est pas nul, est $(q-1)^s - \overline{N}$. Fixons maintenant un caractère additif non principal ψ_0 ; ψ en étant un autre, on a, pour tout élément de K, $\psi(x) = \psi_0(ux)$ où u appartient à K^0, et si u décrit K^0, ψ décrit l'ensemble des caractères additifs non principaux de K. On a ensuite

$$g(\chi_1) = \sum_{x_1 \in K^0} \chi_1(x_1)\,\psi(x_1) = \sum_{x_1 \in K^0} \chi_1(x_1)\,\psi_0(u\,x_1)\ ,$$

d'où

$$g(\chi_1) = \overline{\chi}_1(u)\ g_0(\chi_1)$$

la somme de Gauss g_0 étant cette fois rapportée au caractère additif ψ_0. On trouve de même

$$\mathcal{G}(\chi) = \lambda(u)\,\mathcal{G}_0(\chi)$$

comme formule de transformation des sommes de Gauss relatives à l'anneau E_r ; λ désigne un caractère multiplicatif de K^0 : $\lambda = \chi_1\chi_2\cdots\chi_r$. Finalement, il vient

$$\overline{S}(\psi) = \frac{1}{(q-1)^{r-s}} \sum_{\chi \in \widetilde{G}} \lambda(u)\ \overline{\chi}(a)\ \mathcal{G}_0(\chi)\ ;$$

Pour sommer $\overline{S}(\psi)$ suivant les caractères additifs ψ non principaux, il suffit de sommer en u sur K^0. Si χ est un caractère multiplicatif donné de E_r, λ est un caractère multiplicatif connu de K^0, et $\sum_{u \in K^0} \lambda(u)$ vaut 0 ou $q-1$, suivant que λ n'est pas, ou est, le caractère multiplicatif principal. On a donc

$$(7) \qquad \sum_{\psi} \overline{S}(\psi) = \frac{1}{(q-1)^{r-s-1}} \sum_{\chi \in \widetilde{G}^*} \chi(a)\ \mathcal{G}_0(\chi)$$

où $\widetilde{G}^*$ est le sous-groupe de $\widetilde{G}$ défini par la condition que $\chi_1\chi_2\cdots\chi_r$ soit le caractère multiplicatif principal de K^0.

On déduit sans peine de là :

$$(8) \qquad \overline{N} = \frac{1}{q}\left[(q-1)^s + \frac{1}{(q-1)^{r-s-1}} \sum_{\chi \in \widetilde{G}^*} \overline{\chi}(a)\ \mathcal{G}_0(\chi)\right].$$

4. La série de Artin-Weil.

Reprenons le corps fini K, et considérons ses diverses extensions K' finies ; K'_ν désignera l'extension finie de degré ν. Reprenant le polynome $\mathcal{F}$, à coefficients dans K^0, on notera N_ν et $\bar{N}_\nu$ les nombres de systèmes de solutions de l'équation $\mathcal{F} = 0$, dans K'_ν et dans K'^0_ν respectivement. Enfin, U étant une indéterminée, on formera les séries

$$F(U) = \sum_{\nu=1}^{\infty} N_\nu U^\nu \tag{9}$$

$$\bar{F}(U) = \sum_{\nu=1}^{\infty} \bar{N}\, U^\nu \tag{10}$$

dont la première est par définition la série de Artin-Weil. Une conjecture de Weil est que la série F est une fonction rationnelle de U. C'est ce qu'on vérifie facilement si le polynome $\mathcal{F}$ est à une seule indéterminée : c'est encore ce que WEIL a démontré dans le cas où ce polynome contient deux indéterminées, (cas des courbes). Ce n'est pas ici le lieu de parler de cette démonstration, profonde et difficile [3], [4].

La conjecture de Weil peut encore se vérifier dans d'autres cas, ainsi qu'on va le voir, et il est possible que la méthode employée ici donne une voie d'accès à la démonstration générale. On peut d'ailleurs formuler une conjecture voisine : partons d'un caractère additif non principal sur K ; soit ψ ; prolongeons-le aux extensions K' comme il a été dit au paragraphe 2, et notons S_ν et $\bar{S}_\nu$ les sommes des valeurs de $\psi(\mathcal{F})$ quand les variables décrivent indépendamment K'_ν et K'^0_ν respectivement. Soit encore

$$H(U) = \sum_{\nu=1}^{\infty} S_\nu U^\nu \tag{11}$$

$$\bar{H}(U) = \sum_{\nu=1}^{\infty} \bar{S}_\nu U^\nu \tag{12}$$

On peut aussi conjecturer que ces fonctions sont rationnnelles, et l'analyse qui suit en donne une preuve dans certains cas.

Traitons le cas de la série $\bar{F}(U)$ pour commencer. La formule (8) donne la valeur des coefficients $\bar{N}_\nu$. Nous choisirons une fois pour toutes un générateur w de K^0 ; un caractère multiplicatif χ de K^0 sera défini si on se donne un rationnel α, modulo 1, tel que $(q-1)\alpha \equiv 0 \pmod 1$, si l'on pose

$\chi(w) = \exp 2\pi i\alpha$, et on notera maintenant ce caractère χ_α . De même, un caractère χ du groupe multiplicatif E_r^0 sera défini par la donnée de r nombres rationnels $\alpha_1 , \alpha_2 , \dots , \alpha_r$, modulo 1 , tels que pour chaque indice, $(q - 1)\alpha_i \equiv 0 , \pmod 1$ Enfin le groupe $\hat{G}^*$ qui figure dans la sommation (8) est défini par $s + 1$ congruences linéaires, homogènes, prises modulo 1 , que doivent vérifier les r rationnels α_i pour que le caractère χ appatienne à $\hat{G}^*$.

Nous désignerons par (C) le système de ces congruences. Suivant l'idée de Weil, partons d'une suite de rationnels α_j , $(i = 1 , \dots , r)$,. pris modulo 1 , et satisfaisant seulement au système de congruences (C) ; pour cette suite, que nous noterons (α) , soit $\mu = \mu(\alpha))$, le plus petit entier tel que

$$(q^\mu - 1)\alpha_i \equiv 0 , \pmod 1 , \text{ pour } i = 1 , 2 , \dots , r .$$

Alors les extensions K'_ν de K telles que $(q^\nu - 1)\alpha_i \equiv 0 , \pmod 1$ sont celles pour lesquelles ν est un multiple de μ , et ce sont celles-là seulement. Choisissons dans K_μ^0 un élément générateur permettant de définir, comme plus haut, un caractère multiplicatif par un rationnel modulo 1 , et tout caractère multiplicatif de l'anneau produit direct de r corps identiques à K_μ , par une suite (α) de r rationnels modulo 1 . Soient $\chi_{(\alpha)}$ un tel caractère, et $G_0(\chi_{(\alpha)})$ la somme de Gauss correspondante, sur l'anneau, (relative au prolongement de ψ_0 à K_μ) .

Passons maintenant à l'extension finie de degré $\lambda\mu$ sur K ; on la regardera comme une extension de degré λ sur K'_μ ; toujours à partir de la même suite (α) , introduisons le caractère multiplicatif $\chi'_{(\alpha)}$ et la somme de Gauss correspondante $G'_0(\chi'_{(\alpha)})$. La façon de faire le prolongement du caractère multiplicatif a été indiquée en 2 ; d'ailleurs les a_i appartiennent au corps de base ; on a donc

$$\chi'_{(\alpha)}(a) = [\chi_{(\alpha)}(a)]^\lambda ; \tag{13}$$

puis, par Hasse-Davenport,

$$G'_0(\chi'_{(\alpha)}) = (-1)^{r(\lambda+1)} [G_0(\chi_{(\alpha)})]^\lambda ; \tag{14}$$

Revenons maintenant à la série $\overline{F}(U)$. Le terme en $\frac{1}{q^\nu}(q^\nu - 1)^s$ dans l'expression (8), donne évidemment une contribution dans $\overline{F}(U)$ qui est une fonction rationnelle de U . Considérons ensuite les termes de cette série provenant de la suite (α) , solution fixée du système de congruences (C) . Ces termes n'interviennent que dans

les extensions de degré $\nu = \lambda\mu$, où $\mu = \mu(\alpha))$. Si on tient compte des formules (13) et (14) ci-dessus, l'ensemble de ces termes donne une sommation en λ qui s'écrit

$$(-1)^r \sum_{\lambda=1}^{\infty} \frac{U^{\lambda\mu}}{(q^{\lambda\mu}-1)^{r-s-1}} [\chi_{(\alpha)}(a)]^{\lambda} [-\zeta_0(\chi_{(\alpha)})]^{\lambda}$$

Cette sommation est élémentaire, et donne une fonction rationnelle de U , si l'on a

$$s + 1 - r \geqslant 0 \tag{15}$$

Il reste maintenant à faire la somme de ces fonctions rationnelles pour tous les systèmes (α) possibles. Or ces derniers sont les divers systèmes de solutions, en rationnels modulo 1 , de $s + 1$ congruences linéaires et homogènes à r inconnues ; la condition d'inégalité (15) exprime qu'il y a au moins autant de congruences que d'inconnues ; la matrice rectangulaire des coefficients des premiers membres de ces congruences n'est autre d'ailleurs que la matrice des exposants m_{ij} dont sont affectées les variables dans les r monomes constituant le polynome $\mathfrak{F}$, et on peut supposer que le rang de cette matrice est r , sans quoi, on pourrait restreindre le nombre des variables dans $\mathfrak{F}$. Finalement l'inégalité (15) permet d'affirmer qu'il n'y a qu'un nombre fini de systèmes (α) de rationnels modulo 1 , satisfaisant aux congruences (C) . D'où suit, sous la condition (15), le fait que la fonction $\overline{F}(U)$ est rationnelle.

Passons au cas de la fonction $F(U)$. Pour calculer les valeurs des entiers N_ν, (ou des nombres S_ν), il faut ajouter à $\overline{N}_\nu$ (ou $\overline{S}_\nu$) les contributions apportées par les points de E_s qui sont des diviseurs de 0 dans cet anneau, c'est-à-dire pour lesquels un certain nombre de coordonnées sont nulles, les autres appartenant à K^0 ; annulant donc certaines coordonnées, on voit qu'il y a 2^s manières distinctes de le faire, ce qui donne autant de termes dans les expressions des N_ν (ou S_ν), chacun de ces termes se calculant par des formules de type (8), (ou (6)), dans lesquelles il faut seulement remplacer $\mathfrak{F}$ par le polynome $\mathfrak{F}'$ obtenu en annulant certaines des variables. Après cette annulation, le polynome $\mathfrak{F}'$ comportera s' variables et r' termes, ces entiers étant respectivement inférieurs à s et r ; si la condition (15) est vérifiée pour ces nouveaux entiers, la part correspondante dans $F(U)$ est une fonction rationnelle , et finalement, on pourra affirmer que $F(U)$ est une fonction rationnelle si, pour chacun des 2^s choix de systèmes d'x annulés, on a $s' + 1 - r'$ positif ou nul. La recherche de toutes les matrices $((m_{ji}))$ formées d'entiers positifs ou nuls

satisfaisant à toutes ces conditions est un problème combinatoire assez ennuyeux ; mais il est certain qu'il en existe, comme on le voit en prenant une matrice carrée dont tous les éléments sont nuls, sauf les diagonaux, (cas précisément traité par Weil dans [2].

On traite de façon analogue le cas des séries H et $\overline{H}$ relatives aux sommes S. La seule différence est que la condition (15) est remplacée par

$$s - r \geqslant 0 \tag{16}$$

Les conclusions sont les mêmes.

Toutes ces séries deviennent très complexes lorsque les conditions (15) ou (16) ne sont plus remplies, et leur étude directe paraît difficile.

REMARQUE. - Les formules énumératives (6) et (8) donnent facilement des majorations intéressantes, en tenant compte de la majoration connue du module d'une somme de Gauss. (Nous avons rappelé en 1 que ce module vaut $\sqrt{q}$ pour les sommes de Gauss non triviales, et 1 pour les sommes triviales). On peut donc adopter la majoration $\sqrt{q}$, ce qui donne la majoration $q^{r/2}$ pour les sommes de Gauss relatives à l'anneau E_r. Le nombre de termes de la sommation figurant au second membre de la formule (6) est l'ordre du groupe $\widetilde{G}$, à savoir $d(q-1)^{r-s}$, en reprenant des notations antérieures. On en déduit, par (6), la majoration

$$|S| \leqslant d\, q^{r/2} \tag{17}$$

On trouverait aussi une majoration analogue pour $\overline{N}$.

BIBLIOGRAPHIE

[1] DAVENPORT (H.) und HASSE (H.). - Die Nullstellen der Kongruenzzeta-funktionen in gervissen zyklischen Fällen, J. für reine und ang. Math., t. 172, 1935, p. 151-182.

[2] WEIL (André). - Numbers of solutions of equations in finite fields, Bull. Amer. math. Soc., t. 55, 1949, p. 497-508.

[3] WEIL (André). - Sur les courbes algébriques et les variétés qui s'en déduisent. - Paris, Hermann, 1948 (Act. scient. et ind. n°1041, Publ. Inst. Math. Univ. Strasbourg n°7).

[4] WEIL (André). - Variétés abéliennes et courbes algébriques. - Paris, Hermann, 1948 (Act. scient. et ind. n°1064, Publ. Inst. Math. Univ. Strasbourg n°8).