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: §4. Sommes de Jacobi à n caractères.
DOI: https://doi.org/10.5169/seals-46287

§ 4. *Sommes de Jacobi à n caractères.*

4.1. Soient n un entier $\geqslant 1$, et $\chi_1, ..., \chi_n$ n caractères multiplicatifs de k. Désignons par H l'ensemble des points $\mathbf{x} = (x_1, ..., x_n)$ de k^n tels que $x_1 + ... + x_n = 1$; c'est un hyperplan affine de k^n, et on a en particulier card $(H) = q^{n-1}$.

DÉFINITION 3. — *On appelle* somme de Jacobi *associée à* $\chi_1, ..., \chi_n$ *la quantité*

$$\pi(\chi_1, ..., \chi_n) = \sum_{\mathbf{x} \in H} \chi_1(x_1) ... \chi_n(x_n) . \tag{4.1.1}$$

C'est évidemment un entier du corps des racines $(q-1)$-ièmes de l'unité. Pour $n = 1$, on a $\pi(\chi_1) = 1$; pour $n = 2$, on retrouve les sommes de Jacobi à deux caractères étudiées au paragraphe précédent; dans ce qui suit, on pourra donc supposer $n \geqslant 3$.

4.2. Si un au moins des caractères χ_i est trivial, on a une somme de Jacobi « triviale » qui se calcule explicitement:

(i) *si tous les* χ_i *sont triviaux, on a* $\pi(\chi_1, ..., \chi_n) = q^{n-1}$;

(ii) *si la famille* χ_i *comporte au moins un caractère trivial et au moins un caractère non trivial, on a* $\pi(\chi_1, ..., \chi_n) = 0$.

(Prouvons cette dernière égalité, qui n'est pas absolument évidente: quitte éventuellement à renuméroter les caractères, on peut supposer $\chi_1 \neq \varepsilon, ..., \chi_m \neq \varepsilon$, mais $\chi_{m+1} = ... = \chi_n = \varepsilon$, avec $1 \leqslant m \leqslant n-1$; comme alors $\chi_{m+1}(y) = ... = \chi_n(y) = 1$ pour tout élément y de k, et que le système de $m+1$ équations linéaires

$$X_1 + ... + X_n = 1 , \quad X_1 = x_1, ..., \quad X_m = x_m ,$$

admet exactement q^{n-m-1} solutions dans k^n quels que soient les m éléments $x_1, ..., x_m$ de k, on voit que

$$\pi(\chi_1, ..., \chi_n) = q^{n-m-1} \Big(\sum_{x_1 \in k} \chi_1(x_1) \Big) ... \Big(\sum_{x_m \in k} \chi_m(x_m) \Big) ;$$

mais chacune des sommes du membre de droite est nulle (utiliser (1.1.1) et (1.4.1)); en définitive, on a donc bien $\pi(\chi_1, ..., \chi_n) = 0$, C.Q.F.D.)

4.3. Passons maintenant au cas non trivial.

PROPOSITION 10. — *Supposons* $\chi_i \neq \varepsilon$ *pour* $i = 1, ..., n$. *Alors*

(i) *Si* $\chi_1 \dots \chi_n = \varepsilon$, *on a*

$$\pi(\chi_1, ..., \chi_n) = \chi_n(-1)\pi(\chi_1, ..., \chi_{n-1}). \tag{4.3.1}$$

(ii) *Si au contraire* $\chi_1 \dots \chi_n \neq \varepsilon$, *la somme de Jacobi* $\pi(\chi_1, ..., \chi_n)$ *peut s'exprimer à l'aide de sommes de Gauss non triviales par la formule*

$$\pi(\chi_1, ..., \chi_n) = \tau(\chi_1) \dots \tau(\chi_n)/\tau(\chi_1 \dots \chi_n). \tag{4.3.2}$$

(Les $n + 1$ sommes de Gauss figurant dans le membre de droite sont supposées calculées à l'aide d'un même caractère additif non trivial β de k).

Démonstration. — (i) Ecrivons pour abréger $\pi = \pi(\chi_1, ..., \chi_n)$, et posons

$$\rho = \sum \chi_1(x_1) \dots \chi_{n-1}(x_{n-1}) \tag{4.3.3}$$

(somme étendue à l'ensemble des points $(x_1, ..., x_{n-1})$ de k^{n-1} tels que $x_1 + \dots + x_{n-1} = 0$), puis

$$\sigma = \sum \chi_1(x_1) \dots \chi_n(x_n) \tag{4.3.4}$$

(somme étendue à l'ensemble des points $(x_1, ..., x_n)$ de H tels que $x_n \neq 1$). Il est clair que $\pi = \rho + \sigma$, et il suffit donc, pour prouver l'égalité (4.3.1), d'établir les deux égalités ci-dessous:

$$\rho = 0; \quad \sigma = -\chi_n(-1)\pi(\chi_1, ..., \chi_{n-1}). \tag{4.3.5}$$

Démontrons la première. Comme $\chi_{n-1}(0) = 0$, on peut, dans (4.3.3), limiter la sommation aux points tels que $x_{n-1} \neq 0$, puis faire le changement de variables $(x_1, ..., x_{n-2}, x_{n-1}) \mapsto (y_1, ..., y_{n-2}, t)$ défini par

$$t = -x_{n-1}, \; ty_1 = -x_1, ..., \; ty_{n-2} = -x_{n-2}.$$

(4.3.3) se transforme alors en

$$\rho = \chi_{n-1}(-1)\pi(\chi_1, ..., \chi_{n-2}) \sum_{t \in k^*} (\chi_1 \dots \chi_{n-1})(t);$$

mais par hypothèse, $\chi_1 \dots \chi_{n-1} = \chi_n^{-1} \neq \varepsilon$; compte tenu de (1.1.1), la somme figurant dans le membre de droite est alors nulle, et on a bien $\rho = 0$.

Démontrons la seconde égalité (4.3.5). Faisons, dans le membre de droite de (4.3.4), le changement de variables $(x_1, ..., x_{n-1}, x_n) \mapsto (y_1, ..., y_{n-1}, t)$ défini par

$$y_1 = x_1/(1-x_n), ..., y_{n-1} = x_{n-1}/(1-x_n), t = x_n/(1-x_n) .$$

(4.3.4) se transforme en

$$\sigma = \Big(\sum_{t \neq 0, -1} \chi_n(t) \Big) \left(\sum \chi_1(y_1) \cdots \chi_{n-1}(y_{n-1}) \right),$$

la deuxième somme étant étendue aux points $(y_1, ..., y_{n-1})$ de k^{n-1} tels que $y_1 + ... + y_{n-1} = 0$; cette deuxième somme est donc égale par définition à $\pi(\chi_1, ..., \chi_{n-1})$; comme la première somme figurant dans le membre de droite vaut $-\chi_n(-1)$ (utiliser (1.1.1)), on aboutit bien à la seconde égalité (4.3.5), ce qui achève de démontrer (i).

(ii) Même méthode que pour la proposition 9, (ii) (qui correspond au cas $n = 2$); on laisse au lecteur le soin d'effectuer le détail du calcul.

COROLLAIRE 1. — *Mêmes données que dans la proposition* 10.

(i) *Si* $\chi_1 \cdots \chi_n = \varepsilon$, *on a*

$$|\pi(\chi_1, ..., \chi_n)|^2 = q^{n-2} . \tag{4.3.6}$$

(ii) *Si au contraire* $\chi_1 \cdots \chi_n \neq \varepsilon$, *on a*

$$|\pi(\chi_1, ..., \chi_n)|^2 = q^{n-1} . \tag{4.3.7}$$

(iii) *Dans les deux cas, on a pour la somme de Jacobi* $\pi(\chi_1, ..., \chi_n)$ *la majoration en module*

$$|\pi(\chi_1, ..., \chi_n)| \leqslant q^{(n-1)/2} . \tag{4.3.8}$$

Démonstration. — (4.3.7) résulte de (4.3.2) et de (2.3.4); (4.3.6) résulte *alors* de (4.3.1) et de (4.3.7); enfin, (4.3.8) est une conséquence immédiate de (4.3.6) et (4.3.7).

Appendice. — *Détermination effective des sommes de Gauss et de Jacobi.*

A.1. Commençons par les sommes de Jacobi (et limitons-nous au cas de deux caractères). Le problème est le suivant: étant donné un corps fini k, et deux caractères multiplicatifs χ et ψ de k, donnés *explicitement*, déterminer *directement* (c'est-à-dire sans remonter à la définition) et *sans ambi-*

guïté la valeur de l'entier algébrique $\pi(\chi, \psi)$. Ce problème est difficile en général, mais, pour $k = \mathbf{F}_p$ et χ, ψ d'ordre peu élevé, il peut être résolu de façon élémentaire. Voyons-le sur deux exemples:

Exemple 1. — Posons $\rho = e^{2\pi i/3}$, $A = \mathbf{Z}[\rho]$; soit p un nombre premier $\equiv 1 \pmod 3$, et soit $p = \lambda\bar{\lambda}$ sa décomposition en facteurs irréductibles dans A, λ et $\bar{\lambda}$ étant entièrement déterminés (à la conjugaison près) par la condition $\lambda \equiv \bar{\lambda} \equiv 1 \pmod 3$. Posons $k = A/\lambda A \simeq \mathbf{F}_p$, et soit $\left(\frac{\cdot}{\lambda}\right)_3$ le symbole de restes cubiques modulo λ dans A, défini pour tout $x \in A$ par

(A.1.1) $\left(\frac{x}{\lambda}\right)_3 = 0$, *si* $x \equiv 0 \pmod \lambda$; *une puissance de* ρ, *sinon*;

$$\left(\frac{x}{\lambda}\right)_3 \equiv x^{(p-1)/3} \pmod \lambda \text{ } \textit{dans les deux cas.}$$

Ce symbole s'identifie à un caractère multiplicatif d'ordre 3 de k, qu'on notera χ. On peut alors envisager la somme de Jacobi $\pi(\chi, \chi)$, qui est un élément parfaitement déterminé de A:

PROPOSITION 11. — *On a* $\pi(\chi, \chi) = -\lambda$.

Démonstration. — Posons $\pi = \pi(\chi, \chi)$. (A.1.1) et la définition de χ permettent d'écrire $\pi = \sum_{x \in k} \chi(x)\chi(1-x) \equiv \sum_{x \in k} P(x) \pmod \lambda$, avec $P(X) = X^{(p-1)/3}(1-X)^{(p-1)/3}$; comme $\deg(P) = 2(p-1)/3 < p-1$, cette somme est nulle (dans $k = A/\lambda A$; voir chap. 3, th. 2), et π est donc divisible par λ; mais par ailleurs $\pi\bar{\pi} = p$ (prop. 9, cor. 1): π est donc un facteur irréductible de p dans A. Au total, π est donc associé à λ dans A, et on a $\pi = \varepsilon\lambda$, ε étant une racine 6-ième de l'unité. Soient maintenant ζ une racine primitive p-ième de l'unité dans $\mathbf{C}$, β le caractère additif de k défini par $\beta(x) = \zeta^x$ $(x \in k)$, et τ la somme de Gauss $\tau(\chi \mid \beta)$; on a $\tau^3 = p\pi$ (prop. 9, cor. 2), donc, puisque $p \equiv 1 \pmod 3$, $\pi \equiv \tau^3 \equiv (\sum_{x \in k^*} \chi(x)\zeta^x)^3 \equiv \sum_{x \in k^*} \chi^3(x)\zeta^{3x} = \sum_{x \in k^*} \zeta^{3x} = -1 \pmod 3$ (noter que $\chi^3(x) = 1$ pour tout $x \in k^*$ et que ζ^3 est une racine primitive p-ième de l'unité).

En résumé, on a donc $\pi = \varepsilon\lambda \equiv -1$ (mo 3), avec $\lambda \equiv 1 \pmod 3$ et $\varepsilon =$ une racine 6-ième de l'unité: ceci implique $\varepsilon = -1$ (essayer les six valeurs possibles de ε), donc finalement $\pi = -\lambda$, C.Q.F.D.

Exemple 2. — Posons $i = \sqrt{-1}$, $A = \mathbf{Z}[i]$; soit p un nombre premier $\equiv 1 \pmod 4$, et soit $p = \lambda\bar{\lambda}$ sa décomposition en facteurs irréductibles dans A, λ et $\bar{\lambda}$ étant entièrement déterminés (à la conjugaison près) par la condition $\lambda \equiv \bar{\lambda} \equiv 1 \pmod{2+2i}$. Posons (comme dans l'exemple 1) $k = A/\lambda A \simeq \mathbf{F}_p$, soient $\left(\frac{\cdot}{\lambda}\right)_2$ et $\left(\frac{\cdot}{\lambda}\right)_4$ les symboles de restes quadratiques et biquadratiques modulo λ dans A (définis comme le symbole de restes cubiques dans l'exemple 1), et soient φ et ψ les caractères multiplicatifs de k correspondants.

PROPOSITION 12. — *On a* $\pi(\varphi, \psi) = -\lambda$.

Démonstration. — Posons $\pi = \pi(\varphi, \psi)$. On vérifie immédiatement, comme pour la proposition 11, que $\pi = \varepsilon\lambda$, ε étant maintenant une racine 4-ième de l'unité. On peut déterminer ε par un argument géométrique très élégant, dû à Jacobi, et dont on verra une autre application au chapitre 9 (sect. 5.2). Soit N le nombre de solutions dans k^2 de l'équation $X^4 + Y^2 = 1$; comme $p \equiv 1 \pmod 4$, k contient quatre racines 4-ièmes de l'unité (chap. 1, prop. 7, (ii)), et cette équation admet deux solutions (x, y) telles que $x = 0$, quatre solutions (x, y) telles que $y = 0$, les autres solutions (x, y) (telles que $xy \neq 0$) se groupant huit par huit de façon évidente; ainsi, $N \equiv 6 \pmod 8$. D'autre part, on verra au chapitre 6 (sect. 3.3, formule (3.3.2)) que

$$(A.1.2) \quad N = p - 1 + \pi(\varphi, \psi) + \pi(\varphi, \bar{\psi}) = p - 1 + \pi + \bar{\pi};$$

posons alors $\pi = a + bi$ $(a, b \in \mathbf{Z})$; (A.1.2) donne dans ces conditions $a \equiv 3 \pmod 4$ lorsque $p \equiv 1 \pmod 8$, et $a \equiv 1 \pmod 4$ lorsque $p \equiv 5 \pmod 8$; comme $p = a^2 + b^2$, on voit d'autre part que $b \equiv 0 \pmod 4$ lorsque $p \equiv 1 \pmod 8$, et que $b \equiv 2 \pmod 4$ lorsque $p \equiv 5 \pmod 8$; ainsi, dans les deux cas, $-\pi = -a - bi \equiv 1 \pmod{2+2i}$, donc $-\varepsilon\lambda \equiv \lambda \pmod{2+2i}$, donc $\varepsilon = -1$ (essayer les quatre valeurs possibles de ε), et finalement $\pi = \varepsilon\lambda = -\lambda$, C.Q.F.D.

Pour d'autres exemples analogues, voir [**8**], pp. 465-469.

A.2. Passons aux sommes de Gauss. Le problème est maintenant de déterminer sans ambiguïté une somme $\tau(\chi \mid \beta)$, χ et β étant deux caractères d'un corps fini k, l'un multiplicatif, l'autre additif, et supposés donnés explicitement. Si δ est l'ordre de χ, il est en général possible, au moins pour les

petites valeurs de δ, de déterminer explicitement $\omega(\chi \mid \beta) = \tau(\chi \mid \beta)^\delta$ à l'aide de la formule (3.3.4) (prop. 9, cor. 2). On peut alors écrire $\tau(\chi \mid \beta) = \varepsilon\tau_0$, ε étant une racine δ-ième de l'unité, et τ_0 étant un nombre complexe entièrement défini par les deux conditions ${\tau_0}^\delta = \omega(\chi \mid \beta)$, $0 \leqslant \arg(\tau_0) < 2\pi/\delta$. Le problème est donc de déterminer explicitement ε: sauf pour $\delta = 2$, ce dernier problème n'est pas résolu complètement à l'heure actuelle; c'est ce qu'illustrent bien les deux exemples suivants:

Exemple 1. — Soient p un nombre premier impair, $k = \mathbf{F}_p$, φ le caractère de Legendre de k, et β le caractère additif de k défini par $\beta(x) = e^{2\pi ix/p}$ $(x \in k)$. Posons $\tau = \tau(\varphi \mid \beta)$; τ est un nombre complexe parfaitement défini, et la proposition 7 montre que $\tau^2 = \varphi(-1)\,p = (-1)^{(p-1)/2}\,p$, d'où

$$(A.2.1) \qquad \tau = \begin{cases} \pm p^{1/2}, \text{ si } p \equiv 1 \pmod 4, \\ \pm ip^{1/2}, \text{ si } p \equiv 3 \pmod 4. \end{cases}$$

Problème (dit « du signe de la somme de Gauss »): dans les formules (A.2.1), quel est, en fonction de p, le « bon » signe ? En fait, c'est *toujours* le signe $+$; mais, alors que le calcul de τ^2 est immédiat, la détermination du signe de τ est relativement difficile (Gauss lui-même mit, paraît-il, huit ans à trouver une solution...). A ce sujet (et notamment pour une démonstration), voir [**8**], pp. 469-478.

Exemple 2. — Reprenons les hypothèses et notations de l'exemple 1 (sect. A.1), et soit β le caractère additif de k défini par $\beta(x) = e^{2\pi ix/p}$ $(x \in k)$. Posons maintenant $\tau = \tau(\chi \mid \beta)$ (cette somme de Gauss est dite traditionnellement « somme de Kummer »); c'est un nombre complexe parfaitement défini, et la proposition 9 (cor. 2) montre que $\tau^3 = p\pi(\chi, \chi) = -\lambda p$ (sect. A.1, prop. 11). Si alors τ_0 désigne la racine cubique de $-\lambda p$ (dans $\mathbf{C}$) telle que $0 \leqslant \arg(\tau_0) < 2\pi/3$, on a

$$(A.2.2) \qquad \tau = \varepsilon\tau_0, \quad \text{avec} \quad \varepsilon = 1, \rho \text{ ou } \rho^2.$$

Problème (dit « de la somme de Kummer »): dans la formule (A.2.2), quelle est la « bonne » valeur de ε ? Ce problème, posé dans les années 1840/1850 par Kummer (entre autres) n'est toujours pas résolu (voir [**8**], pp. 478-489). Cassels a formulé récemment une conjecture conforme aux valeurs numériques de τ effectivement calculées pour $p \leqslant 5\,000$ (et $p \equiv 1 \pmod 3$), mais cette conjecture reste à démontrer (voir Cassels (1970)).

Le cas $\delta = 4$ est également examiné (mais non résolu !) dans [**8**], pp. 489-494.