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: Chapitre 5 SOMMES DE GAUSS ET DE JACOBI
DOI: https://doi.org/10.5169/seals-46287

CHAPITRE 5

SOMMES DE GAUSS ET DE JACOBI

Le premier paragraphe de ce chapitre donne la description du groupe des caractères additifs et du groupe des caractères multiplicatifs d'un corps fini, et montre comment ces caractères peuvent servir au calcul du nombre de solutions d'une équation (prop. 3 et 5). Le reste du chapitre est consacré à une étude élémentaire des sommes de Gauss et de Jacobi; ces sommes sont des entiers algébriques, construits à l'aide de caractères, et dont l'utilisation, combinée avec les propositions 3 et 5, permettra notamment (1) de calculer le nombre de solutions d'une équation diagonale quelconque (chap. 6); (2) de calculer dans certains cas la fonction zêta de l'ensemble algébrique défini par une telle équation (chap. 9); (3) de démontrer le théorème d'Ax, c'est-à-dire la relation de divisibilité $q^b \mid N$ annoncée au chapitre 3 (chap. 7). Pour d'autres utilisations classiques des sommes de Gauss et de Jacobi (étude des corps cyclotomiques, démonstration élémentaire des lois de réciprocité, etc.), voir **[8]**, § 20, **[11]**, chap. IV, ou **[3]**, chap. 5; voir également les Notes en fin de chapitre.

On conserve ici encore les conventions et notations des chapitres précédents; en particulier, k désigne toujours un corps fini à $q = p^f$ éléments.

§ 1. *Caractères additifs et caractères multiplicatifs d'un corps fini.*

1.1. Rappelons que si G est un groupe fini commutatif, on appelle *caractère* de G tout homomorphisme $\chi: G \to \mathbf{C}^*$, de G dans le groupe multiplicatif du corps des nombres complexes; les caractères de G forment de manière naturelle un groupe multiplicatif, dit *dual* de G, et noté $\widehat{G}$ (ou $X(G)$); l'élément neutre de G est le caractère ε défini par $\varepsilon(x) = 1$ pour tout $x \in G$: on l'appelle *caractère trivial* (ou *principal*); si $x \in G$, si $\chi \in \widehat{G}$, et si m désigne l'ordre de G, on a $\chi(x)^m = \chi(x^m) = \chi(e) = 1$ (e désignant l'élément neutre de G); les valeurs d'un caractère χ de G sont donc des racines m-ièmes de l'unité; en particulier, si χ^{-1} est l'inverse de χ dans G, et si $x \in G$, alors $\chi^{-1}(x) = \overline{\chi(x)}$ (complexe conjugué de $\chi(x)$): c'est pour-

quoi le caractère χ^{-1} est généralement noté $\bar{\chi}$, et appelé *caractère conjugué* de χ.

On aura besoin par la suite des deux résultats suivants (pour des démonstrations, d'ailleurs immédiates, voir [**17**], pp. 103-107):

(i) *Les groupes G et $\widehat{G}$ sont isomorphes (non canoniquement) ; en particulier, $\widehat{G}$ a même ordre que G.*

(ii) (Relations d'orthogonalité). — *Si χ est un caractère de G, on a*

$$\sum_{x \in G} \chi(x) = \begin{cases} \mathrm{card}(G), & si\ \chi = \varepsilon ; \\ 0, & si\ \chi \neq \varepsilon . \end{cases} \tag{1.1.1}$$

De même, si x est un élément de G, on a

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} \mathrm{card}(G), & si\ x = e ; \\ 0, & si\ x \neq e . \end{cases} \tag{1.1.2}$$

On va appliquer ce qui précède au groupe additif k^+ de k (sect. 1.2), puis au groupe multiplicatif k^* (sect. 1.3); $\widehat{k^+}$ sera dit *dual additif* de k, et $\widehat{k^*}$, *dual multiplicatif;* les éléments de $\widehat{k^+}$ et de $\widehat{k^*}$ seront qualifiés respectivement de *caractères additifs* et de *caractères multiplicatifs* de k.

1.2. Commençons par l'étude des caractères additifs; on peut en construire de la manière suivante: soit Tr l'application trace relative à l'extension $k/\mathbf{F}_p$, et soit ζ une racine primitive p-ième de l'unité dans $\mathbf{C}$ (par exemple $e^{2\pi i/p}$); pour tout élément x de k, posons

$$\beta(x) = \zeta^{Tr(x)} \tag{1.2.1}$$

(ce qui a un sens, puisque $Tr(x) \in \mathbf{F}_p$ est un entier rationnel modulo p); alors β est évidemment un caractère additif de k, et ce caractère n'est pas trivial (parce que la trace est surjective: chap. 1, prop. 9). Plus généralement, si $y \in k$, et si on pose $\beta_y(x) = \beta(xy)$ $(x, y \in k)$, β_y est un caractère additif de k, et ce caractère n'est trivial que si $y = 0$.

Il se trouve que le procédé ci-dessus fournit *tous* les caractères additifs de k; de façon précise:

PROPOSITION 1. — *Soit β un caractère additif non trivial de k (par exemple celui défini par (1.2.1)) et, pour tout x et tout y dans k, posons*

(1.2.2) $$\beta_y(x) = \beta(xy).$$

Alors l'application $y \mapsto \beta_y$ *est un isomorphisme du groupe additif* k^+ *sur son dual* $\widehat{k^+}$.

Démonstration. — Cette application est évidemment un homomorphisme de groupes; compte tenu de la propriété (i) (sect. 1.1), il suffit de prouver que cet homomorphisme est injectif; mais par hypothèse, β est non trivial; il existe donc $a \in k$ tel que $\beta(a) \neq 1$; soit alors $y \in k$, $y \neq 0$; si on pose $x = ay^{-1}$, on a évidemment $\beta_y(x) = \beta(a) \neq 1$, donc $\beta_y \neq \varepsilon$, C.Q.F.D.

PROPOSITION 2. — *Soient* β *un caractère additif non trivial de* k *et* a *un élément quelconque de* k. *Alors*

(1.2.3) $$\sum_{y \in k} \beta(ay) = \begin{cases} q, & si\ a = 0; \\ 0, & si\ a \neq 0. \end{cases}$$

Démonstration. — (1.2.3) résulte, soit de (1.1.1) appliqué au caractère fixe β_a et à l'élément y parcourant k^+, soit de (1.1.2) appliqué à l'élément fixe a et au caractère β_y parcourant $\widehat{k^+}$.

1.3. La proposition 2 donne un moyen de compter les solutions d'une équation polynomiale:

PROPOSITION 3. — *Soit* F *un polynôme à* n *variables et à coefficients dans* k. *Si* β *désigne un caractère additif non trivial de* k, *le nombre* N *de solutions dans* k^n *de l'équation* $F = 0$ *est donné par*

(1.3.1) $$N = q^{-1} \sum_{y,\, \mathbf{x}} \beta\big(yF(x_1, \ldots, x_n)\big),$$

la sommation étant étendue à tous les points $(y, x_1, \ldots, x_n)$ *de* k^{n+1}.

Démonstration. — Soit $V \subset k^n$ l'ensemble des solutions de $F = 0$. Si $\mathbf{x} \in V$, donc si $F(\mathbf{x}) = 0$, (1.2.3), appliqué à $a = F(\mathbf{x})$, donne

$$\sum_{y \in k} \beta\big(yF(\mathbf{x})\big) = q,$$

et par conséquent

(1.3.2) $$\sum_{\mathbf{x} \in V} \sum_{y \in k} \beta\big(yF(\mathbf{x})\big) = qN.$$

Si au contraire $\mathbf{x} \notin V$, donc si $F(\mathbf{x}) \neq 0$, (1.2.3) donne

$$\sum_{y \in k} \beta(yF(\mathbf{x})) = 0 ;$$

donc

$$\sum_{\mathbf{x} \in V} \sum_{y \in k} \beta(yF(\mathbf{x})) = 0 . \tag{1.3.3}$$

Il suffit alors d'additionner (1.3.2) et (1.3.3) et de multiplier les deux membres par q^{-1} pour obtenir la formule (1.3.1). Cette formule sera utilisée systématiquement aux chapitres 6, 7 et 9.

1.4. Passons à l'étude des caractères multiplicatifs de k. Notons d'abord que si $\chi : k^* \to \mathbf{C}^*$, est un tel caractère, sa valeur en 0 n'est pas définie; pour des raisons de commodité, on conviendra *toujours* de prolonger χ en une application $k \to \mathbf{C}^*$, en posant

$$\chi(0) = \begin{cases} 1 , \text{ si } \chi = \varepsilon ; \\ 0 , \text{ si } \chi \neq \varepsilon . \end{cases} \tag{1.4.1}$$

Avec cette convention, on a $\chi(xy) = \chi(x)\chi(y)$ quels que soient $x, y \in k$.

D'autre part, on peut construire un caractère multiplicatif d'ordre $q - 1$ (donc un générateur de $\widehat{k^*}$: voir (i), sect. 1.1) de la façon suivante: soit ω une racine primitive $(q-1)$-ième de l'unité dans $\mathbf{C}$ (par exemple $e^{2\pi i/(q-1)}$), et soit g un générateur du groupe cyclique k^*; pour tout $x \in k^*$, il existe $i \in \mathbf{Z}$ tel que $x = g^i$; désignons par $\mathrm{ind}(x)$ la classe de i modulo $q - 1$ et posons

$$\theta(x) = \omega^{ind(x)} ; \tag{1.4.2}$$

alors θ est bien un caractère multiplicatif d'ordre $q - 1$ de k (c'est un isomorphisme de k^* sur le groupe des racines $(q-1)$-ièmes de l'unité dans $\mathbf{C}$).

Enfin, on a évidemment le résultat suivant:

PROPOSITION 4. — *Soit θ un caractère multiplicatif d'ordre $q - 1$ de k (par exemple celui défini par (1.4.2)). Alors l'application $h \mapsto \theta^h$ définit de manière naturelle un isomorphisme du groupe cyclique $\mathbf{Z}/(q-1)\mathbf{Z}$ sur le groupe $\widehat{k^*}$, dual de k^*.*

1.5. Soit maintenant χ un caractère multiplicatif quelconque de k, et soit δ l'ordre de χ (en tant qu'élément de $\widehat{k^*}$). Si $x \in k^*$, on a $\chi(x^\delta) =$

$\chi^\delta(x) = 1$, et χ est trivial sur $k^{*\delta}$; χ définit donc un caractère (qu'on notera encore χ) du groupe quotient $k^*/k^{*\delta}$; mais δ divise évidemment $q-1$, et ce quotient est d'ordre δ (chap. 1, prop. 7, cor. 1); ainsi, le sous-groupe (cyclique, d'ordre δ) de $\widehat{k^*}$ engendré par χ s'identifie au dual du groupe (cyclique, d'ordre δ) $k^*/k^{*\delta}$, et le noyau de χ est exactement $k^{*\delta}$.

Cela étant:

PROPOSITION 5. — *Soit d un entier $\geqslant 1$, et posons $\delta = (q-1, d)$. Soit d'autre part χ un caractère multiplicatif d'ordre δ de k (par exemple $\theta^{(q-1)/\delta}$, θ étant défini par (1.4.2)), et soit a un élément non nul de k. Alors:*

(i) *Pour que a soit une puissance d-ième dans k, il faut et il suffit que $\chi(a) = 1$.*

(ii) *Le nombre $m(a)$ de solutions dans k de l'équation à une variable $X^d = a$ est donné par*

$$m(a) = \sum_{j=0}^{\delta-1} \chi^j(a). \tag{1.5.1}$$

(iii) *Avec la convention (1.4.1), l'égalité (1.5.1) reste vraie pour $a = 0$.*

Démonstration. — La proposition 7 du chapitre 1 permet de supposer que $d = \delta$. (i) résulte alors du fait que le noyau de χ est $k^{*\delta}$. Prouvons (ii), et notons $\bar{a}$ la classe de a (mod $k^{*\delta}$); les relations d'orthogonalité (1.1.2), appliquées à $G = k^*/k^{*\delta}$, à $x = \bar{a}$, et aux caractères χ^j $(0 \leqslant j \leqslant \delta - 1)$ qui forment le dual de G (voir ci-dessus) donnent

$$\sum_{j=0}^{\delta-1} \chi^j(a) = \begin{cases} \delta, & \text{si } a \in k^{*\delta}; \\ 0, & \text{si } a \notin k^{*\delta}. \end{cases}$$

D'autre part, $m(a)$ vaut δ si $a \in k^{*\delta}$ (k^* contient δ racines δ-ièmes de l'unité) et 0 sinon; (ii) se trouve ainsi établi. Enfin (iii) est évident: car $m(0) = 1$, $\chi^0(0) = \varepsilon(0) = 1$, et $\chi^j(0) = 0$ pour $1 \leqslant j \leqslant \delta - 1$, puisque, pour ces valeurs de j, $\chi^j \neq \varepsilon$.

La formule (1.5.1) sera utilisée au chapitre 6. La partie (i) de la proposition 5 est essentiellement équivalente à l'extension du critère d'Euler donnée au chapitre 1 (prop. 7, cor. 2). Si d'ailleurs on suppose p (donc q) impair, et $d = 2$ (donc $\delta = 2$), le caractère χ de la proposition 5 est entièrement déterminé (il est égal à $\theta^{(q-1)/2}$); ce caractère vaut 1 sur les carrés de k^*, et -1 sur les non-carrés: on l'appelle *caractère de Legendre*; pour $q = p$, il coïncide évidemment avec le *symbole de Legendre*.

§ 2. *Sommes de Gauss.*

2.1. Soient χ un caractère multiplicatif et β un caractère additif de k.

DÉFINITION 1. — *On appelle* somme de Gauss *associée à χ et β la quantité*

$$\tau(\chi|\beta) = \sum_{x \in k^*} \chi(x)\beta(x). \tag{2.1.1}$$

Les valeurs prises par β et χ étant des racines p-ièmes de l'unité, et 0 ou des racines $(q-1)$-ièmes de l'unité, $\tau(\chi \mid \beta)$ est un entier du corps des racines $p(q-1)$-ièmes de l'unité.

Si le caractère β est fixé une fois pour toutes (par exemple, si $\beta(x) = \zeta^{Tr(x)}$, avec $\zeta = e^{2\pi i/p}$: sect. 1.2), on écrit $\tau(\chi)$ au lieu de $\tau(\chi \mid \beta)$, et (pour $y \in k$) $\tau_y(\chi)$ au lieu de $\tau(\chi \mid \beta_y)$ (sect. 1.2): on a donc

$$\tau_y(\chi) = \sum_{x \in k^*} \chi(x)\beta(xy). \tag{2.1.2}$$

2.2. Si l'un des caractères χ et β est trivial, la somme de Gauss associée est également « triviale » et sa valeur se calcule immédiatement à l'aide des relations d'orthogonalité (1.1.1) appliquées à χ ou à β:

(i) *si χ est trivial, mais non β, on a* $\tau(\chi \mid \beta) = -1$;

(ii) *si β est trivial, mais non χ, on a* $\tau(\chi \mid \beta) = 0$;

(iii) *enfin, si χ et β sont tous deux triviaux, on a* $\tau(\chi \mid \beta) = q - 1$.

2.3. Passons au cas non trivial. On suppose $\chi \neq \varepsilon$, on fixe une fois pour toutes un caractère additif non trivial β, et on met tous les caractères additifs non triviaux de k sous la forme β_y $(y \in k^*)$ (prop. 1); les sommes de Gauss non triviales associées à χ sont alors les $\tau_y(\chi)$ $(y \in k^*)$.

PROPOSITION 6. — *Si $\bar{\chi}$ désigne le caractère conjugué de χ (sect. 1.1), on a*

$$\tau_y(\chi) = \bar{\chi}(y)\tau(\chi). \tag{2.3.1}$$

Démonstration. — Puisque $y \neq 0$, l'application $x \mapsto xy$ est une permutation de k^*; il suffit alors d'écrire

$$\tau_y(\chi) = \sum_{x \in k^*} \chi^{-1}(y)\chi(xy)\beta(xy) = \bar{\chi}(y) \sum_{x \in k^*} \chi(xy)\beta(xy)$$

et de faire le changement de variable $z = xy$ pour obtenir (2.3.1).

PROPOSITION 7. — *On a (toujours pour $\chi \neq \varepsilon$)*

$$\tau(\chi)\tau(\bar{\chi}) = q\chi(-1). \tag{2.3.2}$$

Démonstration. — Par définition, $\tau(\chi)\tau(\bar{\chi}) = \sum_{x\in k^*}\sum_{y\in k^*}\chi(x)\bar{\chi}(y)\beta(x)\beta(y)$; mais $\chi(x)\bar{\chi}(y) = \chi(x)\chi^{-1}(y) = \chi(xy^{-1})$, et $\beta(x)\beta(y) = \beta(x+y)$. si on fait le changement de variables $(x, y) \mapsto (y, z)$ défini par $z = xy^{-1}$, on obtient donc

$$\tau(\chi)\tau(\bar{\chi}) = \sum_{y\in k^*}\sum_{z\in k^*}\chi(z)\beta\big(y(z+1)\big). \tag{2.3.3}$$

Le second membre se fractionne en deux sommes partielles correspondant respectivement à $z = -1$ et à $z \neq -1$; comme $\beta(0) = 1$, la première somme vaut $(q-1)\chi(-1)$; quant à la seconde, elle peut s'écrire

$$\sum_{z\neq -1}\chi(z)\sum_{y\in k^*}\beta\big(y(z+1)\big);$$

mais la proposition 2, appliquée à $a = z + 1$, montre que pour tout $z \neq -1$, la somme portant sur $y \in k^*$ vaut $-\beta(0) = -1$; par ailleurs, (1.1.1), appliqué au groupe k^* et au caractère χ, donne

$$\sum_{z\neq -1}\chi(z) = -\chi(-1);$$

la deuxième somme partielle vaut donc $\chi(-1)$; si alors on reporte dans (2.3.3) les valeurs des deux sommes partielles, on obtient

$$\tau(\chi)\tau(\bar{\chi}) = (q-1)\chi(-1) + \chi(-1),$$

c'est-à-dire (2.3.2).

PROPOSITION 8. — *On a (en supposant toujours $\chi \neq \varepsilon$)*

$$|\tau(\chi)|^2 = q. \tag{2.3.4}$$

Démonstration. — Par définition, $|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)}$; on peut donc écrire $|\tau(\chi)|^2 = \sum_{x\in k^*}\sum_{y\in k^*}\chi(x)\bar{\chi}(y)\beta(x)\beta(y)$; mais $\bar{\chi}(y) = \chi^{-1}(y) = \chi(y^{-1})$, et de même $\bar{\beta}(y) = \beta(-y)$; le terme général de la somme ci-dessus est alors égal à $\chi(xy^{-1})\beta(x-y)$, ou encore (en remplaçant y par $-y$, ce qui ne change pas la somme) à $\chi(-1)\chi(xy^{-1})\beta(x+y)$: la proposition 8 résulte donc de la proposition 7, et du fait que $\chi(-1)^2 = \chi((-1)^2) = \chi(1) = 1$.

§ 3. *Sommes de Jacobi à deux caractères.*

3.1. Soient maintenant χ et ψ deux caractères multiplicatifs du corps fini k.

DÉFINITION 2. — *On appelle* somme de Jacobi *associée à χ et ψ la quantité*

$$\pi(\chi, \psi) = \sum_{x \in k} \chi(x)\,\psi(1-x)\,. \tag{3.1.1}$$

Comme le second membre de (3.1.1) peut également s'écrire $\sum_{x+y=1} \chi(x)\,\psi(y)$ on voit que $\pi(\chi, \psi) = \pi(\psi, \chi)$. Il est clair d'autre part que $\pi(\chi, \psi)$ est un entier du corps des racines $(q-1)$-ièmes de l'unité.

3.2. Si l'un des deux caractères χ et ψ est trivial, la somme de Jacobi est également « triviale » et sa valeur se calcule immédiatement à l'aide des relations d'orthogonalité (1.1.1) et de la convention (1.4.1):

(i) *si* $\chi = \psi = \varepsilon$, *on a* $\pi(\chi, \psi) = q$;

(ii) *si* $\chi = \varepsilon$ *et* $\psi \neq \varepsilon$ *(ou l'inverse), on a* $\pi(\chi, \psi) = 0$.

3.3. Passons au cas non trivial.

PROPOSITION 9. — *Supposons χ et ψ non triviaux. Alors*

(i) *Si* $\chi\psi = \varepsilon$, *on a*

$$\pi(\chi, \psi) = -\chi(-1)\,. \tag{3.3.1}$$

(ii) *Si au contraire* $\chi\psi \neq \varepsilon$, *la somme de Jacobi* $\pi(\chi, \psi)$ *se calcule à l'aide des sommes de Gauss non triviales* $\tau(\chi)$, $\tau(\psi)$ *et* $\tau(\chi\psi)$ *par la formule*

$$\pi(\chi, \psi) = \tau(\chi)\,\tau(\psi)/\tau(\chi\psi)\,. \tag{3.3.2}$$

(Les trois 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) Si $\chi\psi = \varepsilon$, on a $\psi = \chi^{-1}$, et on peut écrire

$$\pi(\chi, \psi) = \sum_{x \neq 0,\,1} \chi(x)\,\chi^{-1}(1-x) = \sum_{x \neq 0,\,1} \chi(x/(1-x))\,;$$

mais le quotient $y = x/(1-x)$ est une fonction homographique régulière de x, et quand x prend toute valeur possible dans k, sauf 0 et 1, y prend toute valeur possible dans k, sauf 0 et -1; ainsi, $\pi(\chi, \psi) = \sum_{y \in k^*} \chi(y)$

$-\chi(-1)$ et (3.3.1) résulte alors de (1.1.1) appliqué au caractère multiplicatif non trivial χ.

(ii) La définition des sommes de Gauss et la convention (1.4.1) permettent d'écrire

$$\tau(\chi)\tau(\psi) = \sum_{x\in k}\sum_{y\in k}\chi(x)\psi(y)\beta(x+y);$$

dans le second membre, faisons le changement de variables $(x, y) \mapsto (z, t)$ défini par $z = x + y$ et $tz = x$ (l'apparition de la valeur 0 n'est pas gênante, du fait que $\chi(0) = \psi(0) = 0$: on laisse au lecteur le soin d'examiner ce point en détail); il vient

$$\tau(\chi)\tau(\psi) = \sum_{z\in k}\sum_{t\in k}\chi(z)\chi(t)\psi(z)\psi(1-t)\beta(z),$$

ou encore

$$\tau(\chi)\tau(\psi) = \Big(\sum_{z\in k}(\chi\psi)(z)\beta(z)\Big)\Big(\sum_{t\in k}\chi(t)\psi(1-t)\Big),$$

c'est-à-dire finalement, puisque $(\chi\psi)(0) = 0$,

$$\tau(\chi)\tau(\psi) = \tau(\chi\psi)\pi(\chi, \psi),$$

C.Q.F.D.

COROLLAIRE 1. — *Si les trois caractères χ, ψ et $\chi\psi$ sont non triviaux, on a*

$$|\pi(\chi, \psi)|^2 = q. \tag{3.3.3}$$

Démonstration. — Utiliser la proposition 9, (ii), puis la proposition 8.

COROLLAIRE 2. — *Supposons toujours le caractère χ non trivial, et notons δ son ordre. On a alors*

$$\tau(\chi)^\delta = q\chi(-1)\pi(\chi, \chi)\pi(\chi, \chi^2)\ldots\pi(\chi, \chi^{\delta-2}). \tag{3.3.4}$$

Démonstration. — Pour $1 \leqslant j \leqslant \delta - 2$, la proposition 9, (ii) donne

$$\pi(\chi, \chi^j) = \tau(\chi)\tau(\chi^j)/\tau(\chi^{j+1});$$

en multipliant membre à membre ces $\delta - 2$ égalités, on obtient

$$\pi(\chi, \chi)\pi(\chi, \chi^2)\ldots\pi(\chi, \chi^{\delta-2}) = \tau(\chi)^{\delta-1}/\tau(\chi^{\delta-1});$$

mais $\chi^{\delta-1} = \chi^{-1} = \bar{\chi}$; il suffit alors de multiplier les deux membres de cette dernière égalité par $\tau(\chi)\tau(\bar{\chi}) = q\chi(-1)$ pour obtenir (3.3.4).

§ 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.

Notes sur le chapitre 5

§ **1**: le fait que $\mathbf{F}_p^+$ est en dualité avec lui-même par $(x, y) \mapsto e^{2\pi ixy/p}$ est évident, et connu « depuis toujours ». Les caractères multiplicatifs de $\mathbf{F}_p$ se sont introduits progressivement à partir du milieu du XVIII^e siècle avec l'étude des restes quadratiques (Euler, Legendre, Gauss), cubiques (Gauss, Jacobi, Eisenstein) et biquadratiques (Gauss, Jacobi).

§ **2**: les sommes de Gauss apparaissent (sous la forme déguisée des *périodes cyclotomiques*) dans la dernière section des *Disquisitiones Arithmeticae*: Gauss les utilise pour étudier, avant la lettre, le groupe de Galois de l'extension $\mathbf{Q}(e^{2\pi i/p})/\mathbf{Q}$; à ce sujet, voir par exemple [**8**], pp. 453-460. Par la suite, les sommes de Gauss reparaissent systématiquement dans les travaux arithmétiques de Gauss, Jacobi, Eisenstein, Kummer, Stickelberger, en relation notamment avec l'étude des lois de réciprocité, et avec la représentation des nombres premiers par des formes quadratiques binaires à coefficients entiers; pour une synthèse de ces travaux, voir le livre centenaire de Bachmann (*Die Lehre von der Kreistheilung*, Teubner, Leipzig, 1872), ainsi que Stickelberger (1890). (L'utilisation de la somme de Gauss $\tau = \sum_{x \bmod p} \left(\frac{x}{p}\right) e^{2\pi ix/p}$ pour démontrer la loi de réciprocité quadratique est bien connue: voir [**8**], pp. 116-117, ou [**17**], chap. 1, sect. 3.3).

§ **3-4**: les sommes de Jacobi apparaissent également dans les travaux mentionnés ci-dessus; elles y sont *définies* à partir des sommes de Gauss par une formule qui coïncide avec la formule (3.3.2). Elles sont étudiées systématiquement chez Stickelberger (1890), Davenport-Hasse (1934) et Weil (1949) (ce dernier article contient d'ailleurs d'intéressantes indications historiques).

CHAPITRE 6

ÉQUATIONS DIAGONALES (II)

Ce chapitre utilise les propositions 3 et 5 du chapitre 5 pour établir des formules donnant le nombre exact $N(b)$ de solutions dans k^n d'une équation diagonale $a_1 X_1^{d_1} + \ldots + a_n X_n^{d_n} = b$ à coefficients dans k (k désigne toujours un corps fini à q éléments). Ces formules font intervenir des sommes de