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