COURS DE L'INSTITUT FOURIER

JEAN-RENÉ JOLY

Chapitre 5 Caractères des corps finis Sommes de Gauss et de Jacobi

Cours de l'institut Fourier, tome 4 (1971), p. 1-26

<http://www.numdam.org/item?id=CIF_1971__4__A5_0>

Chapitre 5

Caractères des corps finis

Sommes de Gauss et de Jacobi

(5.1). Caractères des groupes abéliens finis.

La dualité des groupes abéliens finis est exposée simplement et rapidement dans [Se], pp. 103-106; nous nous bornerons donc ici à exposer ce qui nous sera utile par la suite (cette limitation n'apportera d'ailleurs aucune simplification notable!).

Soit G un groupe abélien fini d'ordre n, noté multiplicativement. On appelle caractère de G tout homomorphisme de G dans le groupe multiplicatif C^* du corps des nombres complexes; les caractères de G forment de manière naturelle un groupe multiplicatif: ce groupe des caractères est dit groupe dual de G, on le note $\hat{G}$. Si $x \in G$ et si $\chi \in \hat{G}$, on a $x^n = 1$, et $\chi(x)^n = \chi(x^n) = \chi(1) = 1$: le caractère χ prend donc en fait ses valeurs dans le sous-groupe W_n de C^* formé des n racines $n^{\text{ièmes}}$ de l'unité. Conséquences:

Proposition 1. - Si $\chi \in \hat{G}$, l'inverse de χ dans le groupe $\hat{G}$ n'est autre que le caractère conjugué $\overline{\chi}$ de χ (défini par $\overline{\chi}(x) = \overline{\chi(x)}$ pour tout $x \in G$, la barre notant la conjugaison complexe).

Beweis. Klar.

Proposition 2. - Supposons G cyclique (toujours d'ordre n) et soit s

un générateur de G ; alors l'application $\chi \longmapsto \chi(s)$ est un isomorphisme de $\hat{G}$ sur le groupe W_n des racines $n^{\text{ièmes}}$ de l'unité.

Beweis. Klar.

Proposition 3. - Soit p un nombre premier, et supposons que le groupe fini G est d'exposant p, c'est-à-dire qu'il possède la propriété suivante:

(1) pour tout $x \in G$, $x^p = 1$.

Alors, si on identifie W_p à $F_p = Z/pZ$, et si on considère G comme espace vectoriel sur F_p (l'"addition" $G \times G \longrightarrow G$ étant la loi multiplicative $(x, y) \longmapsto xy$ de G, et la "multiplication scalaire" $F_p \times G \longrightarrow G$ étant l'exponentiation $(a, x) \longmapsto x^a$, ce qui a un sens grâce à (1)), le dual $\hat{G}$ du groupe G est identique au dual de l'espace vectoriel G.

Beweis. Nochmals klar.

Proposition 4. - Soit G un groupe abélien fini, et supposons-le soit cyclique, soit d'exposant premier. Alors $\hat{G}$ est isomorphe (non canoniquement) à G, et en particulier, G et $\hat{G}$ ont le même ordre:

$$\text{card}(G) = \text{card}(\hat{G}) . \tag{2}$$

Démonstration. Dans le premier cas (G cyclique), on a, avec les notations de la proposition 2, $\hat{G} \simeq W_n$, et W_n est cyclique d'ordre n, comme G. Dans le second cas (G d'exposant premier), il suffit d'utiliser la proposition 3, et le fait qu'en dimension finie, le dual d'un espace vectoriel E est isomorphe à E.

Remarque. - En fait, la proposition 4 est vraie pour n'importe quel groupe abélien fini G (décomposer G en produit direct de groupes cycliques).

Corollaire. - Mêmes hypothèses que dans la proposition 4. Alors, quel que soit $x \neq 1$ dans G, il existe $\chi \in \hat{G}$ tel que $\chi(x) \neq 1$.

Démonstration. Soit $H \neq \{1\}$ le sous-groupe de G engendré par x : on a évidemment $\mathrm{card}(G/H) < \mathrm{card}(G)$. Supposons alors que pour tout caractère χ de G, on ait $\chi(x) = 1$, donc aussi $\chi(H) = 1$; un argument classique de passage au quotient donnerait alors un isomorphisme $\hat{G} \xrightarrow{\sim} \widehat{(G/H)}$; mais G/H est de même nature (i.e. cyclique, ou d'exposant premier) que G ; on aurait donc (proposition 4)

$$\mathrm{card}\widehat{(G/H)} = \mathrm{card}(G/H),$$

et par conséquent

$$\mathrm{card}(G) = \mathrm{card}(\hat{G}) = \mathrm{card}\widehat{(G/H)} = \mathrm{card}(G/H) < \mathrm{card}(G) :$$

absurde! Le corollaire est ainsi démontré.

Remarque. - Compte tenu de la précédente remarque, ce corollaire est en fait valable pour n'importe quel groupe abélien fini (et même d'ailleurs pour n'importe quel groupe abélien): voir [Se], p. 104, pour une autre démonstration (utilisant le fait que C^* est un groupe "divisible").

Enonçons enfin les relations d'orthogonalité:

Proposition 5. - Soit G un groupe abélien fini, d'ordre n, et supposons-le soit cyclique, soit d'exposant premier (*).

(i) Soit x un élément fixé de G ; alors

(*) Ici encore, bien entendu, ces hypothèses sont en fait inutiles...

$$(3) \qquad \sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n \text{ , si } x = 1 \text{ ,} \\ 0 \text{ , si } x \neq 1 \text{ .} \end{cases}$$

(ii) Soit χ un caractère fixé de G ; alors

$$(4) \qquad \sum_{x \in G} \chi(x) = \begin{cases} n \text{ , si } \chi = 1 \text{ ,} \\ 0 \text{ , si } \chi \neq 1 \text{ .} \end{cases}$$

Démonstration. (i) Si $x = 1$, on a $\chi(x) = 1$ pour tout $\chi \in \hat{G}$, et l'égalité (3) tient alors à ce que $\text{card}(\hat{G}) = n$. Supposons maintenant $x \neq 1$; d'après le corollaire ci-dessus, il existe $\chi_0 \in \hat{G}$ tel que

$$(5) \qquad \chi_0(x) \neq 1 \text{ ;}$$

l'application $\chi \mapsto \chi\chi_0$ étant une bijection de $\hat{G}$ sur lui-même, on peut écrire $\sum_{\chi} \chi(x) = \sum_{\chi} \chi\chi_0(x) = \chi_0(x) \sum_{\chi} \chi(x)$, d'où

$$(\chi_0(x) - 1) \sum_{\chi \in \hat{G}} \chi(x) = 0 \text{ ;}$$

il suffit alors de simplifier par le facteur $\chi_0(x) - 1$ (ce que (5) nous autorise à faire) pour obtenir l'égalité cherchée. (Comparer ce raisonnement à celui du chapitre 2, théorème 3, lemme).

(ii) Méthode analogue: si $\chi = 1$, l'égalité (4) est évidente. Sinon, il existe, par définition même de l'écriture $\chi \neq 1$, un $x_0 \in G$ tel que $\chi(x_0) \neq 1$: on conclut alors comme en (i).

(5.2). Caractères additifs et multiplicatifs d'un corps fini.

Soit K un corps fini à $q = p^f$ éléments; K^* désignera comme

d'habitude le groupe multiplicatif de K ; nous noterons d'autre part K^+ le groupe additif de K : ce sont respectivement un groupe cyclique d'ordre $q - 1$, et un groupe d'exposant premier p (noté additivement!!!): voir chapitre 1, théorème 3; les résultats du paragraphe précédent s'appliquent donc à ces deux groupes; en particulier, $\widehat{K^+} \simeq K^+$, $\widehat{K^*} \simeq K^*$, et les relations d'orthogonalité (3) et (4) sont valables tant pour les caractères additifs de K (i.e. les caractères de K^+) que pour les caractères multiplicatifs de K (i.e. les caractères de K^*). Le but de ce paragraphe est d'écrire un peu plus explicitement ces isomorphismes et ces relations d'orthogonalité. Nous noterons généralement θ , λ ,... les caractères additifs, et χ , ψ ,... les caractères multiplicatifs.

Caractères additifs.

Théorème 1. - Soit Tr l'application trace relative à l'extension galoisienne K/F_p , et soit ζ une racine primitive $p^{\text{ième}}$ de l'unité dans C . Quels que soient x , $y \in K$, posons

$$\theta_y(x) = \zeta^{Tr(xy)} \tag{6}$$

(ce qui a un sens, puisque $Tr(xy) \in F_p = Z/pZ$ s'identifie à une classe d'entiers modulo p , et que par ailleurs $\zeta^p = 1$). Alors

(i) Quel que soit $y \in K$, $x \longmapsto \theta_y(x)$ est un caractère additif de K .

(ii) L'application $y \longmapsto \theta_y$ est un isomorphisme du groupe additif K^+ sur le groupe (multiplicatif) $\widehat{K^+}$ des caractères additifs de K .

Démonstration. (i) La trace étant un homomorphisme de K^+ dans F_p^+ , on a, quels que soient y , x_1 , $x_2 \in K$,

$$\theta_y(x_1 + x_2) = \zeta^{\mathrm{Tr}((x_1 + x_2)y)} = \zeta^{\mathrm{Tr}(x_1y) + \mathrm{Tr}(x_2y)} =$$
$$= \zeta^{\mathrm{Tr}(x_1y)} \cdot \zeta^{\mathrm{Tr}(x_2y)} = \theta_y(x_1)\ \theta_y(x_2)\ ,$$

c.q.f.d.

(ii) En inversant les rôles de x et y, le calcul ci-dessus montre que, quels que soient x, y_1, $y_2 \in K$, on a

$$\theta_{y_1 + y_2}(x) = \theta_{y_1}(x)\ \theta_{y_2}(x)\ ,$$

et $y \longmapsto \theta_y$ est bien un homomorphisme de K^+ dans $\widehat{K^+}$. Reste à prouver que cet homomorphisme est bijectif, ou simplement (K^+ et $\widehat{K^+}$ ayant le même ordre: proposition 4) qu'il est injectif, c'est-à-dire de noyau nul. Soit donc $y \in K$ tel que $\theta_y(x) = 1$ pour tout $x \in K$: on a alors $\mathrm{Tr}(xy) = 0$ pour tout $x \in K$; mais l'extension K/F_p est galoisienne (chapitre 1, théorème 5), et la forme F_p-bilinéaire sur K définie par $(x, y) \longmapsto \mathrm{Tr}(xy)$ est donc <u>régulière</u> (ou <u>non-dégénérée</u>; voir par exemple [La], p. 211, th. 9); d'où finalement $y = 0$, c.q.f.d.

<u>Théorème 2</u>. -. (i) Soit x un élément de K ; alors

$$(7) \qquad \sum_{\theta \in \widehat{K^+}} \theta(x) = \begin{cases} q\ , & \text{si } x = 0\ , \\ 0\ , & \text{si } x \neq 0\ . \end{cases}$$

(ii) Soit θ un caractère additif de K ; alors

$$(8) \qquad \sum_{x \in K} \theta(x) = \begin{cases} q\ , & \text{si } \theta = 1\ , \\ 0\ , & \text{si } \theta \neq 1\ . \end{cases}$$

<u>Démonstration</u>. Appliquer les relations (3) et (4) de la proposition 5 au groupe (additif!) K^+, qui est d'ordre q.

Caractères multiplicatifs.

Convention fondamentale. Soit χ un caractère multiplicatif de K ; c'est un homomorphisme de K^* dans C^*, et par conséquent χ n'est pas défini en 0 ; une telle situation serait gênante dans la pratique (voir par exemple au paragraphe suivant la définition des sommes de Gauss et de Jacobi). C'est pourquoi on convient généralement (et nous adopterons toujours cette convention dans ce qui suit) de prolonger χ en une application de K dans C en posant

$$\chi(0) = \begin{cases} 1 , & \text{si } \chi = 1 , \\ 0 , & \text{si } \chi \neq 1 . \end{cases} \tag{9}$$

Avec cette convention, on conserve la propriété de multiplicativité de χ : quels que soient x , $y \in K$, $\chi(xy) = \chi(x)\chi(y)$.

Cela étant:

Théorème 3. - Soient g un générateur du groupe cyclique K^* et ω une racine primitive $(q-1)^{\text{ième}}$ de l'unité dans C ; tout $x \in K^*$ s'écrit g^j , $j \in Z$: notons $\mathrm{ind}(x)$ la classe de j modulo $q-1$; enfin, pour tout $x \in K^*$ et tout $h \in Z$, posons

$$\chi_h(x) = \omega^{h\,\mathrm{ind}(x)} \tag{10}$$

(ce qui a un sens, puisque $h\,\mathrm{ind}(x) \in Z/(q-1)Z$ est une classe d'entiers modulo $q-1$, et que $\omega^{q-1} = 1$). Alors

(i) Quel que soit $h \in Z$, $x \longmapsto \chi_h(x)$ est un caractère multiplicatif de K .

(ii) L'application $h \longmapsto \chi_h(x)$ est un homomorphisme de Z sur le

groupe $\widehat{K^*}$ des caractères multiplicatifs de K ; le noyau est égal à $(q-1)\mathbf{Z}$, et cet isomorphisme établit un isomorphisme du groupe additif $\mathbf{Z}/(q-1)\mathbf{Z}$ sur le dual multiplicatif de K.

Démonstration. Analogue à celle du théorème 1 (plus facile, même), et laissée au lecteur.

Théorème 4. - (i) Soit x un élément de K ; alors

$$(11) \qquad \sum_{\chi \in \widehat{K^*}} \chi(x) = \begin{cases} 1 , & \text{si } x = 0 , \\ q-1 , & \text{si } x = 1 , \\ 0 , & \text{dans les autres cas.} \end{cases}$$

(ii) Soit χ un caractère multiplicatif de K ; alors

$$(12) \qquad \sum_{x \in K} \chi(x) = \begin{cases} q , & \text{si } \chi = 1 , \\ 0 , & \text{si } \chi \neq 1 . \end{cases}$$

Démonstration. Appliquer les relations (3) et (4) de la proposition 5 au groupe K^*, qui est d'ordre $q-1$, et tenir compte de la convention (9).

(5.3). Sommes de Gauss attachées à un corps fini.

Soient, comme précédemment, K un corps fini à $q = p^f$ éléments, Tr l'application trace relative à l'extension $K/\mathbf{F}_p$ et ζ une racine primitive $p^{\text{ième}}$ de l'unité dans le corps $\mathbf{C}$ des nombres complexes; si a et x sont des éléments de K, posons ici encore

$$\theta_a(x) = \zeta^{\mathrm{Tr}(ax)} ;$$

lorsque a parcourt K, θ_a parcourt le groupe des caractères additifs

de K (théorème 1).

Définition 1. - Soient χ un caractère multiplicatif de K, a un élément de K et θ_a le caractère additif correspondant. On appelle somme de Gauss (ou parfois somme trigonométrique, ou résolvante de Lagrange, ou résolvante d'Eisenstein, ou encore résolvante de Kummer) associée à χ et a (ou mieux à χ et $\theta = \theta_a$) la quantité

$$(13) \qquad \tau_a(\chi) = \sum_{x \in K} \chi(x)\,\theta_a(x) = \sum_{x \in K} \chi(x)\,\theta(x) \qquad (*)$$

($\tau_a(\chi)$ dépend donc de χ, de a et aussi de ζ : mais cette dernière dépendance n'apparaît pas dans la pratique; on peut d'ailleurs choisir une fois pour toutes $\zeta = e^{2\pi i/p}$).

Les valeurs prises respectivement par θ_a et χ étant des racines $p^{\text{ièmes}}$ de l'unité, et 0 ou des racines $(q-1)^{\text{ièmes}}$ de l'unité, il est clair que $\tau_a(\chi)$ est un entier du corps cyclotomique des racines $p(q-1)^{\text{ièmes}}$ de l'unité.

Pour $\chi = 1$ ou $a = 0$ (c'est-à-dire $\theta_a = 1$), on a des sommes de Gauss triviales, dont la valeur se calcule facilement (grâce notamment aux relations d'orthogonalité (8) et (12)):

(14) si $\chi = 1$ et $a = 0$, $\tau_a(\chi) = q$;

(15) si $\chi = 1$ et $a \neq 0$, $\tau_a(\chi) = 0$;

(16) si $\chi \neq 1$ et $a = 0$, $\tau_a(\chi) = 0$.

Passons donc au cas non trivial: dans toute la suite de ce paragraphe, nous supposerons en principe $\chi \neq 1$ et $a \neq 0$ (c'est-à-dire $\theta_a \neq 1$).

Proposition 1. - Posons pour simplifier

(*) Autre notation: $\tau(\chi|\theta)$.

(17) $$\tau(\chi) = \tau_1(\chi) = \sum_{x \in K} \chi(x)\, \zeta^{\mathrm{Tr}(x)} \ ;$$

alors

(18) $$\tau_a(\chi) = \bar{\chi}(a)\tau(\chi) \ .$$

Démonstration. Puisque $a \neq 0$, l'application $x \longmapsto y = ax$ est une bijection de K sur K ; on a donc

$$\tau_a(\chi) = \sum_x \chi(x)\, \zeta^{\mathrm{Tr}(ax)} = \sum_x \chi^{-1}(a)\, \chi(ax)\, \zeta^{\mathrm{Tr}(ax)}$$

$$= \bar{\chi}(a) \sum_x \chi(ax)\, \zeta^{\mathrm{Tr}(ax)} = \bar{\chi}(a) \sum_y \chi(y)\, \zeta^{\mathrm{Tr}(y)},$$

c.q.f.d. (Ici et dans la suite, un symbole de sommation tel que $\sum_x$ signifie $\sum_{x \in K}$).

La proposition 1 permet de se limiter à l'étude des sommes de Gauss du type $\tau(\chi)$.

Proposition 2. - On a l'égalité

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

Démonstration. Par définition (et en posant naturellement $\theta(x) = \theta_1(x) = \zeta^{\mathrm{Tr}(x)}$), on a

$$\tau(\chi)\tau(\bar{\chi}) = \tau(\chi)\tau(\chi^{-1}) = \sum_{x,y} \chi(x)\chi(y^{-1})\,\theta(x)\,\theta(y)$$

$$= \sum_{x,y} \chi(xy^{-1})\,\theta(x+y) \ .$$

Mais $\chi \neq 1$, donc $\chi(0) = 0$ et on peut se borner à étendre les sommations ci-dessus à $K^* \times K^*$, ce qui permet de faire un changement de variables x, $y \longmapsto y$, z avex $z = xy^{-1}$; dès lors,

$$\tau(\chi)\tau(\bar{\chi}) = \sum_{y,z \neq 0} \chi(z)\,\theta(y(z+1)) \ .$$

Le second membre se fractionne en deux "paquets" correspondant respectivement à $z = -1$ et à $z \neq -1$:

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1) \sum_{y \neq 0} \theta(0) + \sum_{z \neq 0,-1} \chi(z) \sum_{y \neq 0} \theta_{z+1}(y)$$

$$= \chi(-1)(q-1) + \sum_{z \neq 0,-1} \chi(z) \sum_{y \neq 0} \theta_{z+1}(y).$$

Or, pour $z \neq -1$, $\sum_{y \in K} \theta_{z+1}(y) = 0$ (théorème 2, (8)), donc $\sum_{y \neq 0} \theta_{z+1}(y) = -\theta_{z+1}(0) = -1$; on vérifie de la même manière que $\sum_{z \neq 0,-1} \chi(z) = -\chi(-1)$; finalement,

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

c.q.f.d.

Proposition 3. - On a l'égalité

$$|\tau(\chi)|^2 = q , \tag{20}$$

(d'où notamment $\tau(\chi) \neq 0$).

Démonstration. En effet (toujours avec $\theta(x) = \zeta^{\mathrm{Tr}(x)}$), on a

$$|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \sum_{x,y} \chi(x)\bar{\chi}(y)\,\theta(x)\,\bar{\theta}(y)$$

$$= \sum_{x,y} \chi(xy^{-1})\,\theta(x-y).$$

La démonstration se termine alors comme pour la proposition 2.

(5.4). Sommes de Jacobi à deux caractères.

Mêmes notations qu'au paragraphe précédent.

Définition 2. - Soient χ et ψ deux caractères multiplicatifs de K. On appelle somme de Jacobi associée à χ et ψ la quantité

$$\pi(\chi,\psi) = \sum_{x \in K} \chi(x)\psi(1-x) . \tag{21}$$

Notons qu'on peut écrire plus symétriquement

$$\pi(\chi,\psi) = \sum_{x+y=1} \chi(x)\psi(y) , \tag{21'}$$

et que $\pi(\chi,\psi)$ est un entier du corps cyclotomique des racines $(q-1)^{\text{ièmes}}$ de l'unité: même argument que pour les sommes de Gauss.

Pour χ ou $\psi = 1$, on a des sommes de Jacobi triviales, dont la valeur se calcule immédiatement (ne pas oublier la convention (9)):

(22) si $\chi = \psi = 1$, $\pi(\chi,\psi) = q$;

(23) si $\chi = 1$ et $\psi \neq 1$ (ou l'inverse), $\pi(\chi,\psi) = 0$.

Passons donc au cas non trivial: dans ce qui suit, nous supposons en principe χ et ψ tous deux différents du caractère unité 1.

Proposition 4. - Soient $\chi \neq 1$ et $\psi \neq 1$. Alors

(i) Si $\chi\psi = 1$, on a

$$\pi(\chi,\psi) = -\chi(-1) ; \tag{24}$$

(ii) si au contraire $\chi\psi \neq 1$, 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

$$\pi(\chi,\psi) = \tau(\chi)\,\tau(\psi)/\tau(\chi\psi) . \tag{25}$$

Démonstration. (i) Si $\chi\psi = 1$, c'est que $\psi = \chi^{-1}$; on a donc

$$\pi(\chi,\psi) = \sum_{x \neq 0,1} \chi(x)\,\chi^{-1}(1-x) = \sum_{x \neq 0,1} \chi\left(\frac{x}{1-x}\right) .$$

Mais le quotient $y = \dfrac{x}{1-x}$ est une fonction homographique régulière de x, et quand x prend toute valeur dans K, sauf 0 et 1, y prend également toute valeur dans K, sauf 0 et -1 ; ainsi

$$\pi(\chi,\psi) = \sum_{y \neq 0,-1} \chi(y) = \sum_{y \in K} \chi(y) - \chi(0) - \chi(-1).$$

D'après (12), (9) et l'hypothèse $\chi \neq 1$, les deux premiers termes du membre de droite sont nuls, et on obtient bien finalement l'égalité (24).

(ii) Par définition des sommes de Gauss, et toujours avec $\theta(x) = \zeta^{\mathrm{Tr}(x)}$,

$$\tau(\chi)\tau(\psi) = \Big[\sum_x \chi(x)\theta(x)\Big]\Big[\sum_y \psi(y)\theta(y)\Big]$$

$$= \sum_x \sum_y \chi(x)\psi(y)\theta(x+y).$$

Faisons le changement de variables $x, y \longmapsto z, t$ défini par $x + y = z$ et $x = zt$ (c'est une bijection de $K^* \times K^*$ sur $K^* \times K^*$ et c'est ce qui compte, puisque $\chi(0) = \psi(0) = 0$) ; on arrive à

$$\tau(\chi)\tau(\psi) = \sum_z \sum_t \chi(z)\chi(t)\psi(z)\psi(1-t)\theta(z)$$

$$= \Big[\sum_z (\chi\psi)(z)\,\theta(z)\Big]\Big[\sum_t \chi(t)\psi(1-t)\Big] = \tau(\chi\psi)\,\pi(\chi,\psi).$$

Comme $\tau(\chi\psi) \neq 0$ (proposition 3), l'égalité (25) se trouve démontrée.

Corollaire. - Si χ, ψ et $\chi\psi \neq 0$, alors

(26) $$|\pi(\chi,\psi)|^2 = q.$$

Démonstration. Utiliser les relations (20) et (25)

Proposition 5. - Soit toujours χ un caractère multiplicatif différent du

caractère unité 1 , et soit r l'ordre de χ (en tant qu'élément du groupe multiplicatif K^* : noter que r est un diviseur de $q-1$); alors

$$(27) \qquad \tau(\chi)^r = \chi(-1)\, q\, \pi(\chi,\chi)\, \pi(\chi,\chi^2) \dots \pi(\chi,\chi^{r-2}) .$$

Démonstration. Pour $1 \leq j \leq r-2$, la proposition 4, (25) permet d'écrire

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

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

$$\pi(\chi,\chi)\,\pi(\chi,\chi^2)\dots\pi(\chi,\chi^{r-2}) = \frac{\tau(\chi)^{r-1}}{\tau(\chi^{r-1})} ;$$

il suffit alors de remarquer que $\chi^{r-1} = \chi^{-1} = \overline{\chi}$ et de multiplier les deux membres par $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)\, q$ (proposition 2) pour arriver à l'égalité (27).

Il est d'usage de poser $\omega(\chi) = \tau(\chi)^r$; la formule (27) donne donc une expression de $\omega(\chi)$ à l'aide de sommes de Jacobi associées à χ et à ses puissances; comme les valeurs prises par χ sont évidemment des racines $r^{\text{ièmes}}$ de l'unité, la proposition 5 admet la conséquence suivante:

Corollaire. - Le nombre complexe $\omega(\chi)$ est un entier du corps cyclotomique des racines $r^{\text{ièmes}}$ de l'unité.

(5.5). Sommes de Jacobi à n caractères.

Mêmes notations qu'au paragraphe précédent.

Définition 3. - Soient n un entier positif et $\chi_1, \dots, \chi_n$ n caractères multiplicatifs de K . On appelle somme de Jacobi associée à ces

caractères la quantité

$$(28) \qquad \pi(\chi_1, \dots, \chi_n) = \sum_{x}{}_1 \, \chi_1(x_1)\chi_2(x_2)\dots\chi_n(x_n) ,$$

la notation $\sum_{x}{}_1$ signifiant que le point $x = (x_1, \dots, x_n)$ parcourt l'ensemble H des solutions (dans K^n) de l'équation

$$(29) \qquad X_1 + X_2 + \dots + X_n = 1 .$$

Pour $n = 1$, on a évidemment $\pi(\chi_1) = 1$; pour $n = 2$, on retombe sur la définition 2 du paragraphe précédent. Dans ce qui suit, on pourra supposer constamment que $n \geqslant 3$.

Si l'un au moins des caractères χ_i est égal au caractère unité 1, on a des sommes de Jacobi triviales; de façon précise

si $\chi_1 = \chi_2 = \dots = \chi_n = 1$, on a l'égalité

$$(30) \qquad \pi(\chi_1, \dots, \chi_n) = q^{n-1}$$

(observer que H est un hyperplan affine de dimension $n-1$ sur K et qu'il contient donc q^{n-1} points);

si un χ_i au moins est <u>égal à</u> 1, et si un χ_j au moins est <u>différent de</u> 1, on a l'égalité

$$(31) \qquad \pi(\chi_1, \dots, \chi_n) = 0 .$$

Démontrons l'égalité (31), qui n'est pas tout à fait évidente. Quitte éventuellement à renuméroter les caractères, on peut supposer $\chi_1 \neq 1$, $\chi_2 \neq 1, \dots, \chi_s \neq 1$, mais $\chi_{s+1} = \dots = \chi_n = 1$, avec $1 \leqslant s \leqslant n-1$. Comme alors $\chi_{s+1}(y) = \dots = \chi_n(y) = 1$ pour tout élément y de K, et que le système de $s+1$ équations (évidemment indépendantes)

$$\begin{cases} X_1 + X_2 + \dots + X_n = 1 \\ X_1 = x_1 \\ X_2 = x_2 \\ \dots\dots \\ X_s = x_s \end{cases}$$

admet exactement q^{n-s-1} solutions $x \in K^n$, quels que soient x_1, x_2, $\dots$, x_s dans K, on voit que

$$\pi(\chi_1, \dots, \chi_n) = q^{n-s-1} \Big(\sum_{x_1} \chi_1(x_1) \Big) \dots \Big(\sum_{x_s} \chi_s(x_s) \Big) .$$

Mais, dans le membre de droite, chacune des sommes entre parenthèses est nulle (théorème 4, (12)): d'où effectivement l'égalité (31).

Passons maintenant au cas non trivial où tous les caractères χ_i sont différents de 1 :

Proposition 6. - Supposons $\chi_1 \neq 1, \dots, \chi_n \neq 1$. Alors

(i) Si $\chi_1 \chi_2 \dots \chi_n = 1$, on a

$$\pi(\chi_1, \dots, \chi_n) = -\chi_n(-1)\, \pi(\chi_1, \dots, \chi_{n-1}) . \tag{32}$$

(ii) Si au contraire $\chi_1 \chi_2 \dots \chi_n \neq 1$, on a

$$\pi(\chi_1, \dots, \chi_n) = \frac{\tau(\chi_1)\, \tau(\chi_2) \dots \tau(\chi_n)}{\tau(\chi_1 \chi_2 \dots \chi_n)} . \tag{33}$$

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

$$\pi_0 = \sum_{x_1 + \dots + x_{n-1} = 0} \chi_1(x_1) \chi_2(x_2) \dots \chi_{n-1}(x_{n-1}) , \tag{34}$$

$$\sigma = \sum_{\substack{x_1 + \dots + x_n = 1 \\ x_n \neq 1}} \chi_1(x_1) \chi_2(x_2) \dots \chi_n(x_n) . \tag{35}$$

Il est clair que $\pi = \pi_0 + \sigma$, et il suffit donc, pour prouver (32), de démontrer les deux égalités suivantes:

$$\pi_0 = 0 \quad ; \tag{36}$$

$$\sigma = -\chi_n(-1)\pi(\chi_1, \dots, \chi_{n-1}) . \tag{37}$$

Démontrons (36). Puisque $\chi_{n-1} \neq 1$, on a $\chi_{n-1}(0) = 0$, donc

$$\pi_0 = \sum_{x_{n-1} \neq 0} \chi_{n-1}(x_{n-1}) \sum_{(-x_{n-1})} \chi_1(x_1) \dots \chi_{n-2}(x_{n-2}) ,$$

la somme notée $\sum_{(-x_{n-1})}$ étant étendue à l'ensemble des familles $(x_1 , \dots , x_{n-2})$ telles que $x_1 + \dots + x_{n-2} = -x_{n-1}$. Faisons le changement de variables défini par les équations

$$y_1 = -x_1/x_{n-1} , \dots , y_{n-2} = -x_{n-2}/x_{n-1} ,$$
$$t = -x_{n-1} .$$

On vérifie alors sans peine que l'expression donnée ci-dessus de π_0 se transforme en

$$\pi_0 = \chi_{n-1}(-1)\pi(\chi_1, \dots, \chi_{n-2}) \sum_t (\chi_1\chi_2 \dots \chi_{n-1})(t) .$$

Or, par hypothèse, $\chi_1\chi_2 \dots \chi_{n-1} = \chi_n^{-1} \neq 1$: le théorème 4, (12) donne alors

$$\sum_t (\chi_1\chi_2 \dots \chi_{n-1})(t) = 0 ,$$

ce qui démontre (36). Prouvons maintenant (37): faisons cette fois-ci le changement de variables défini par les équations

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

On obtient pour σ l'expression

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

Or le premier facteur vaut $-\chi_n(-1)$ (comparer avec la démonstration de la relation (24)); quant au second facteur, il est égal par définition à $\pi(\chi_1, \ldots, \chi_{n-1})$, de sorte que la relation (37) se trouve elle aussi démontrée. Ceci achève la démonstration de (i).

(ii) Calcul analogue à celui fait pour prouver l'égalité (25) (qui correspond au cas particulier $n = 2$): le lecteur bovin et incrédule le fera à titre d'exercice.

Corollaire. - Mêmes données que dans la proposition 6.

(i) Si $\chi_1 \chi_2 \cdots \chi_n = 1$, on a

$$|\pi(\chi_1, \ldots, \chi_n)|^2 = q^{n-2}. \tag{38}$$

(ii) Si au contraire $\chi_1 \chi_2 \cdots \chi_n \neq 1$, on a

$$|\pi(\chi_1, \ldots, \chi_n)|^2 = q^{n-1}. \tag{39}$$

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

$$|\pi(\chi_1, \ldots, \chi_n)| \leq q^{(n-1)/2}. \tag{40}$$

Démonstration. L'égalité (39) (la seconde dans le corollaire) résulte des formules (33) et (20); l'égalité (38) résulte alors des égalités (39) et (32); enfin, (40) est une conséquence triviale de (38) et (39).

(5.6). Relations de Stickelberger.

D'après la proposition 3 du paragraphe 3, la valeur absolue archimédi-

enne d'une somme de Gauss non triviale est égale (avec les notations habituelles) à $q^{1/2}$; le but du présent paragraphe est d'obtenir une évaluation correspondante pour les valeurs absolues non-archimédiennes prolongeant la valeur absolue p-adique de Q .

Soient donc toujours K un corps fini à $q = p^f$ éléments, notons ω et ζ une racine primitive $(q-1)^{\text{ième}}$ et une racine primitive $p^{\text{ième}}$ de l'unité dans le corps C des nombres complexes, et posons $E = Q(\omega)$, O_E = l'anneau des entiers de E , $F = E(\zeta) = Q(\omega, \zeta)$, O_F = l'anneau des entiers de F . Les résultats généraux relatifs à la décomposition des idéaux premiers dans les corps cyclotomiques (voir par exemple [Ws] , chapitre 7, ou [CF] , chapitre III) permettent d'énoncer les propriétés suivantes:

(i) Posons $g = \varphi(q-1)/f$; alors p est non ramifié dans E , et se décompose dans E en g facteurs premiers de degré f :

$$p O_E = \mathfrak{y}_1 \mathfrak{y}_2 \cdots \mathfrak{y}_g \quad ; \tag{41}$$

en particulier, chaque corps résiduel $O_E / \mathfrak{y}_i$ est isomorphe à K .

(ii) Chaque $\mathfrak{y}_i$ est totalement ramifié dans F , l'indice de ramification étant égal à $[F : E] = p - 1$; on a donc une décomposition du type

$$\mathfrak{y}_i O_F = \mathfrak{p}_i^{p-1} \quad ; \tag{42}$$

le degré résiduel en $\mathfrak{p}_i \mid \mathfrak{y}_i$ est égal à 1 , et le corps résiduel $O_F / \mathfrak{p}_i$ est encore isomorphe à K .

(iii) En conséquence, p se décompose dans F de la manière suivante:

$$p O_F = \mathfrak{p}_1^{p-1} \mathfrak{p}_2^{p-1} \cdots \mathfrak{p}_g^{p-1} \quad . \tag{43}$$

Remarquons que "tous les $\mathcal{Y}_i$ se valent" et que "tous les $\mathcal{P}_i$ se valent", du fait qu'ils sont permutés transitivement par le groupe de Galois de l'extension abélienne F/Q : dans ce qui suit, nous choisirons <u>une fois pour toutes</u> un $\mathcal{Y}_i$ et le $\mathcal{P}_i$ correspondant, et nous les noterons simplement $\mathcal{Y}$ et $\mathcal{P}$; en outre, <u>nous identifierons</u> $O_E/\mathcal{Y}$ <u>et</u> $O_F/\mathcal{P}$ <u>à</u> K.

Notons maintenons T^* le sous-groupe de F^* engendré par ω : T^* est cyclique, d'ordre $q-1$, c'est le groupe des racines $(q-1)^{\text{ièmes}}$ de l'unité dans F ; de plus

(iv) La restriction à T^* de l'homomorphisme canonique $O_F \longrightarrow O_F/\mathcal{P} = K$ est un isomorphisme du groupe T^* sur le groupe K^*.

Si alors on compose l'isomorphisme inverse $K^* \longrightarrow T^*$ avec l'injection canonique $T^* \longrightarrow C^*$, on obtient un caractère multiplicatif de K, d'ordre $q-1$, à valeurs dans F, et qui engendre le dual $\widehat{K^*}$ de K^* : ce caractère sera noté χ.

Encore une notation: pour tout élément α non nul de F, nous noterons $\mathrm{ord}(\alpha)$ l'exposant de $\mathcal{P}$ dans la décomposition en facteurs premiers de l'idéal fractionnaire principal αO_F (ord est donc tout simplement la valuation $\mathcal{P}$-adique normalisée de F); les propriétés suivantes sont immédiates:

(v) $\mathrm{ord}(\alpha) \geqslant 0$ pour tout $\alpha \in O_F$.

(vi) $\mathrm{ord}(p) = p-1$ (conséquence de la formule (43)).

(vii) $\mathrm{ord}(\alpha\beta) = \mathrm{ord}(\alpha) + \mathrm{ord}(\beta)$ pour tout α et tout β non nuls dans F.

(viii) $\mathrm{ord}(\alpha+\beta) \geqslant \inf(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$ pour tout α et tout β non nuls dans F.

Considérons maintenant pour tout entier relatif j l'élément

$$\tau(j) = \sum_{x \in K^*} \chi^{-j}(x)\, \zeta^{\mathrm{Tr}(x)} , \tag{44}$$

qui est évidemment un entier de F (Tr désigne comme toujours la trace relative à l'extension K/F_p). Comme χ est un caractère d'ordre $q-1$, nous pourrons en fait nous limiter aux valeurs de j telles que

$$0 \leq j < q-1 .$$

Il est clair en outre que

$$\tau(0) = -1 ; \tag{45}$$

si au contraire $j \neq 0$, on a (χ étant étendu en une application de K tout entier dans C avec la convention habituelle $\chi(0) = 0$) $\chi^{-j}(0) = 0$, ce qui permet, dans le membre de droite de (44), d'étendre la sommation à K tout entier; on voit alors que $\tau(j)$ est une somme de Gauss (nous y voilà!); plus précisément, le caractère additif choisi étant évidemment $x \longmapsto \zeta^{\mathrm{Tr}(x)}$, on peut écrire

$$\tau(j) = \tau(\chi^{-j}) ; \tag{46}$$

cela étant, la valuation $\mathfrak{P}$-adique normalisée $\mathrm{ord}(\tau(j))$ des sommes de Gauss $\tau(j)$ est donnée par le théorème suivant:

Théorème 5 (Stickelberger). - Soit j un entier tel que $0 \leq j < q-1$, et soit

$$j = j_0 + j_1 p + \ldots + j_{f-1} p^{f-1} \tag{47}$$

l'"écriture de j en base p ", avec $0 \leq j_i < p$ pour $i = 0, 1, \ldots, f-1$; posons $\sigma(j) = j_0 + j_1 + \ldots + j_{f-1}$ = la "somme des chiffres de j en base p "; on a alors l'égalité

(48) $$\mathrm{ord}(\tau(j)) = \sigma(j) .$$

Démonstration. Posons a priori $\mathrm{ord}(\tau(j)) = s(j)$: il s'agit donc de prouver que pour tout j tel que $0 \leq j < q-1$, on a

(49) $$s(j) = \sigma(j) .$$

Mais $s(j)$ possède la série de propriétés suivantes:

(I) $s(0) = 0$.

Car $\tau(0) = -1$ est une unité du corps F .

(II) $s(j) \geq 0$ pour tout j .

Car $\tau(j)$ est un entier du corps F .

(III) $s(j+k) \leq s(j) + s(k)$.

Pour j ou $k = 0$, il n'y a rien à prouver; pour $j + k = q - 1$, on a $s(j+k) = s(0) = 0 \leq s(j) + s(k)$ (d'après (I) et (II)). Supposons donc $j \neq 0$, $k \neq 0$ et $j + k \neq q - 1$; la proposition 4, (ii) nous donne alors

(50) $$\tau(\chi^{-(j+k)}) = \pi\, \tau(\chi^{-j})\tau(\chi^{-k}) ,$$

avec $\pi = \pi(\chi^{-j}, \chi^{-k}) \in O_E \subset O_F$; l'inégalité à prouver résulte alors de la propriété (vii) et de la propriété (v) ci-dessus.

(IV) $s(j+k) \equiv s(j) + s(k) \pmod{p-1}$.

Pour j ou $k = 0$, rien à prouver; pour $j + k = q - 1$, on a $\tau(j) = \tau(\chi^{-j})$, $\tau(k) = \tau(\chi^{j})$, donc, d'après la proposition 2, $\tau(j)\tau(k) = \tau(\bar{\chi}^{j})\tau(\chi^{j}) = \chi^{j}(-1)\, q = \chi^{j}(-1)\, p^{f}$, d'où, par la propriété (vi), $s(j) + s(k) = \mathrm{ord}(p^{f}) = f\,\mathrm{ord}(p) = f(p-1)$,

donc $s(j) + s(k) \equiv 0 = s(0) = s(j+k) \pmod{p-1}$, ce qui règle ce cas particulier. Supposons maintenant $j \neq 0$, $k \neq 0$ et $j + k \neq q - 1$; la relation (50) (voir (III) ci-dessus) donne alors

$$s(j + k) = s(j) + s(k) + \mathrm{ord}(\pi) ,$$

avec $\mathrm{ord}(\pi) \equiv 0 \pmod{p-1}$ puisque $\pi \in 0_E$ (utiliser (vi)), ce qui règle le cas général.

(V) $s(jp^i) = s(j)$ pour tout exposant i.

On peut supposer $j \neq 0$ et $i \geqslant 1$; on a alors $jp^i \not\equiv 0 \pmod{q-1}$, et par conséquent

$$\tau(j) = \sum \chi^{-j}(x)\, \zeta^{\mathrm{Tr}(x)} , \tag{51}$$

$$\tau(jp^i) = \sum \chi^{-jp^i}(x)\, \zeta^{\mathrm{Tr}(x)} ; \tag{52}$$

mais il est clair que pour tout $x \in K$, on a $\chi^{-jp^i}(x) = \chi^{-j}(x^{p^i})$ d'une part, et $\mathrm{Tr}(x) = \mathrm{Tr}(x^{p^i})$ d'autre part (puisque x et x^{p^i} sont conjugués sur F_p); en faisant le changement de variable $y = x^{p^i}$ dans le membre de droite de (52), on voit ainsi que $\tau(jp^i) = \tau(j)$ et a fortiori que $s(j) = s(jp^i)$, c.q.f.d.

(VI) $s(1) = 1$.

Posons $\lambda = \zeta - 1$; le polynôme minimal de ζ sur E (ou sur Q) étant $X^{p-1} + X^{p-2} + \ldots + X + 1 = (X^p - 1)/(X - 1)$, le polynôme minimal de λ est évidemment $((X+1)^p - 1)/X = X^{p-1} + pX^{p-2} + \ldots + p$, donc un <u>polynôme d'Eisenstein</u>: il en résulte immédiatement que

$$\mathrm{ord}(\lambda) = 1 \tag{53}$$

(λ est donc une "uniformisante locale" en $\mathfrak{P}$). Ecrivons alors la défini-

tion de $\tau(1)$ en y remplaçant ζ par $1 + \lambda$:

$$(54) \qquad \tau(1) = \tau(\chi^{-1}) = \sum_{x \in K^*} \chi^{-1}(x)(1 + \lambda)^{Tr(x)} ,$$

d'où, en utilisant la formule du binôme, et compte tenu de (53),

$$(55) \qquad \tau(1) \equiv \sum_{x \in K^*} \chi^{-1}(x)(1 + \lambda\, \underline{Tr}(x)) \pmod{\mathfrak{P}^2} ,$$

$\underline{Tr}(x)$ désignant par exemple, dans cette dernière formule, l'unique entier compris entre 0 et $p - 1$ et dont l'image canonique dans F_p soit égale à $Tr(x)$; faisons le changement de variable défini par $t = \chi(x)$; comme évidemment $\underline{Tr}(x) \equiv t + t^p + \ldots + t^{p^{f-1}} \pmod{\mathfrak{P}}$, la congruence (56) devient

$$(57) \qquad \tau(1) \equiv \sum_{t \in T^*} t + \lambda \sum_{t \in T^*} t^{-1}(t + t^p + \ldots + t^{p^{f-1}}) \pmod{\mathfrak{P}^2} ;$$

mais T^* est le groupe des racines $(q - 1)^{\text{ièmes}}$ de l'unité dans C ; d'où, pour tout entier rationnel u ,

$$\sum_{t \in T^*} t^u = \begin{cases} q - 1 & \text{si } q - 1 \text{ divise } u , \\ 0 & \text{sinon ;} \end{cases}$$

moyennant quoi la congruence (57) se réduit à

$$(59) \qquad \tau(1) \equiv \lambda(q - 1) \equiv -\lambda \pmod{\mathfrak{P}^2} ,$$

d'où évidemment $s(1) = ord(\tau(1)) = ord(\lambda) = 1$, c.q.f.d.

(VII) $\displaystyle\sum_{0 \leq j < q-1} s(j) = f(p - 1)(q - 2)/2 .$

En effet, on a déjà remarqué (voir la démonstration de (IV)) que

$$(60) \qquad s(j) + s(q - 1 - j) = f(p - 1) ;$$

comme $s(0) = s(q - 1) = 0$, la formule (60) donne, en faisant varier

j de 1 à q - 2 et en additionnant:

$$(61) \qquad \sum_{0 \leq j < q-1} (s(j) + s(q-1-j)) = 2 \sum_{0 \leq j < q-1} s(j) = f(p-1)(q-2) ,$$

c.q.f.d.

Ces diverses propriétés de $s(j)$ étant établies, prouvons maintenant que $s(j) = \sigma(j)$. Les relations (I), (II), (III) et (IV) montrent immédiatement que pour $0 \leq j \leq p-1$, on a

$$(62) \qquad s(j) = j = j_0 = \sigma(j) ;$$

les relations (II) et (VI) donnent d'autre part

$$(63) \qquad s(j) \leq s(j_0) + s(j_1) + \ldots + s(j_{f-1}) ;$$

comme $0 \leq j_i \leq p-1$ pour $i = 0, 1, \ldots, f-1$, les relations (62) et (63) impliquent, pour $0 \leq j < q-1$, l'inégalité

$$(64) \qquad s(j) \leq j_0 + j_1 + \ldots + j_{f-1} = \sigma(j) ;$$

l'égalité $s(j) = \sigma(j)$ résulte alors de (64), de la propriété (VII) et de l'égalité

$$(65) \qquad \sum_{0 \leq j < q-1} \sigma(j) = f(p-1)(q-2)/2 ,$$

qui se vérifie immédiatement par récurrence sur f . Le théorème 5 se trouve ainsi démontré.

Remarque. - On peut en fait démontrer le résultat suivant, plus précis que la simple égalité (48):

si, comme précédemment, $j = j_0 + j_1 p + \ldots + j_{f-1} p^{f-1}$, si $\sigma(j) = j_0 + j_1 + \ldots + j_{f-1}$, et si de plus on pose

$$(66) \qquad \rho(j) = j_0!\, j_1! \ldots j_{f-1}! ,$$

alors on a la congruence ("congruence de Stickelberger"):

$$\tau(j) \equiv -\frac{\lambda^{\sigma(j)}}{\rho(j)} \pmod{\mathfrak{p}^{\sigma(j)+1}} . \tag{67}$$

Pour une démonstration de cette congruence, voir [15] ou [4] (méthode élémentaire) ou encore [6] (méthode d'analyse p-adique). La démonstration du théorème 5 donnée ci-dessus est tirée de [4], Anhang, II. On notera que la propriété (VI) est un cas particulier de la congruence (67).

Le théorème 5 sera utilisé uniquement au chapitre 7, pour la démonstration du théorème d'Ax.