Théorie des Nombres

Besançon

Année 1977-1978

SOMMES DE GAUSS

SUR LES CORPS FINIS

Georges GRAS

Faculté des Sciences

Mathématiques

25030 BESANCON CEDEX

SOMMES DE GAUSS SUR LES CORPS FINIS

par Georges GRAS

(E. R. A. au C. N. R. S. n° 070 654)

INTRODUCTION

Nous nous proposons de rassembler ici les éléments de la théorie classique des sommes de GAUSS sur les corps finis puis de dégager de cette étude des conséquences propres à éclairer certains problèmes sur les classes d'idéaux des corps abéliens.

Le lecteur peut se convaincre du fait que les notions de sommes de GAUSS plus générales que l'on peut définir, se ramènent, "essentiellement", aux sommes de GAUSS sur les corps finis (se reporter par exemple à [10] et [14] pour cela) ; ceci justifie que nous nous limitions à ce cas ; d'autant plus que nous avons en vue les applications aux classes d'idéaux des corps abéliens.

On sait que la contribution essentielle dans le domaine des sommes de GAUSS sur les corps finis est celle de STICKELBERGER ([16]) ; nous verrons d'ailleurs dans ce travail que la plupart des résultats importants (par exemple les relations de DAVENPORT-HASSE [2]) découlent de ceux de STICKELBERGER. On peut même dire que ces résultats reposent sur ce qu'on appelle les "congruences de STICKELBERGER".

Les chapitres I et II contiennent les résultats élémentaires classiques sur les sommes de GAUSS sur les corps finis et notamment les résultats de STICKELBERGER ; le chapitre III est consacré à la démonstration des relations de DAVENPORT-HASSE (th. III 1), relations dont nous donnons ensuite une interprétation (th. III 2) au moyen de certaines quantités $\tau(L)$ associées à tout corps abélien L et qui sont en relation avec les "ARTIN root numbers". L'introduction de ces nombres $\tau(L)$ apporte une simplification appréciable à la théorie ; de plus, l'étude de leurs propriétés nous permet, dans le chapitre IV, de donner (th. IV 1 ou th. IV 1') une nouvelle forme plus forte du théorème de STICKELBERGER (sur l'annulation des classes d'idéaux des corps abéliens) qui ne semble pas pouvoir se déduire de l'énoncé classique. Des exemples numériques sont développés à titre d'illustration des phénomènes étudiés.

Pour les trois premiers chapitres, nous avons utilisé abondamment les rédactions de [2], [4], [11] (IV, §3) et [14].

N'ayant pas abordé dans ce travail les résultats sur le "module des relations" et la notion de "Grössencharaktere" concernant les sommes de GAUSS, nous renvoyons le lecteur à [15]* (et à la bibliographie qui y est incluse) qui est précisément consacrée à un exposé systématique de ces deux questions.

* Thèse que nous avons reçue après la rédaction de ce travail et grâce à V. ENNOLA que nous remercions.

I

DEFINITIONS ET PROPRIETES ELEMENTAIRES DES SOMMES DE GAUSS

1) Définitions ([2], p. 152 ; [4], §I ; [10], §2 ; [11], IV, §3 ; [12]).

a) Définition à l'aide des corps finis. Soit p un nombre premier et soit $q = p^n$, $n \geq 1$. On appelle k le corps fini $\mathbb{F}_q$ extension de $\mathbb{F}_p$. On appelle T la trace de k à $\mathbb{F}_p$ (c'est une application $\mathbb{F}_p$-linéaire surjective).

On désigne par $\mathfrak{X}$ le groupe des caractères de degré 1 de k^* à valeurs dans $\mathbb{C}^*$; comme k^* est cyclique d'ordre q-1, $\mathfrak{X}$ est cyclique d'ordre q-1 et on appelle φ un générateur de $\mathfrak{X}$. On prolonge les éléments de $\mathfrak{X}$ à k en posant $\varphi^{\alpha}(0) = 0$, pour tout $\alpha \in \mathbb{Z}$.

On choisit une fois pour toutes une racine primitive p^e de l'unité ζ (par exemple $\zeta = \exp(2i\pi/p)$).

Définition I 1. Pour tout a premier à p et pour tout $\psi \in \mathfrak{X}$, on pose :

$$\tau_a(\psi) = -\sum_{x \in k} \psi(x)\, \zeta^{aT(x)} \quad .$$

Ceci est une somme de GAUSS relative au caractère ψ ; dans cette expression, a (premier à p) est défini modulo p et on confondra le plus souvent a et sa classe modulo p. Lorsque a = 1, on dit que la somme de GAUSS est normée et on omet l'indice 1. On remarque que si m est l'ordre de ψ alors $\tau_a(\psi)$ est un entier du corps $\mathbb{Q}^{(pm)}$ (on a évidemment $m \mid q-1$).

b) <u>Définitions et notations générales</u>. Les notations adoptées ci-dessous sont valables dans toute la suite. En principe, on a toujours dans le contexte un nombre premier p fixé et une puissance de p, $q = p^n$, $n \geq 1$. Considérons le schéma suivant :

$$\begin{tikzcd}
\mathbb{Q}' \arrow[r, dash] \arrow[d, dash, "p-1"'] & \bar{L}' \arrow[r, dash] \arrow[d, dash] & L' \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}'^{(m_L)} \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}'^{(p^{n_L}-1)} \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}'^{(q-1)} \arrow[d, dash, "p-1"] \\
\mathbb{Q} \arrow[r, dash] & \bar{L} \arrow[r, dash] & L \arrow[r, dash] & \mathbb{Q}^{(m_L)} \arrow[r, dash] & \mathbb{Q}^{(p^{n_L}-1)} \arrow[r, dash] & \mathbb{Q}^{(q-1)}
\end{tikzcd}$$

Si L est un sous-corps quelconque de $\mathbb{Q}^{(q-1)}$, on désigne par $\bar{L}$ le corps de décomposition de p dans L par rapport à $\mathbb{Q}$. On pose $L' = L\mathbb{Q}^{(p)}$; comme $p \nmid q-1$, les extensions L'/L et $\mathbb{Q}^{(q-1)}/L$ sont linéairement disjointes. On remarque que $\bar{L}'$ est le corps de décomposition de p dans l'extension $L'/\mathbb{Q}'$; pour éviter toute ambiguïté, on pose $\overline{L'} = \bar{L}'$.

On appelle A_L et A'_L les anneaux d'entiers de L et L'. On appelle $\mathfrak{P}_L$ un idéal premier de L au-dessus de p dans L et $\mathfrak{P}'_L$ l'unique idéal de L' au-dessus de $\mathfrak{P}_L$ (qui est totalement ramifié dans L'/L).

On désigne par λ_L le degré résiduel de p dans $L/\mathbb{Q}$ ($\lambda_L = [L : \bar{L}]$) et on désigne par m_L le conducteur de L ($m_L \mid q-1$). On appelle enfin n_L la plus petite puissance de p telle que $p^{n_L} \equiv 1 \bmod m_L$ (on a donc $n_L = [\mathbb{Q}^{(m_L)} : \overline{\mathbb{Q}^{(m_L)}}]$ et $\lambda_L | n_L | n$).

On pose $G_L = \mathrm{Gal}(L/\mathbb{Q})$ et $G'_L = \mathrm{Gal}(L'/\mathbb{Q}')$; on appelle H le groupe $\mathrm{Gal}\left(\mathbb{Q}'^{(q-1)}/\mathbb{Q}^{(q-1)}\right) \simeq \mathrm{Gal}(\mathbb{Q}'/\mathbb{Q})$ et Γ le groupe $\mathrm{Gal}\left(\mathbb{Q}'^{(q-1)}/\mathbb{Q}\right)$ (on a $\Gamma \simeq G'_{\mathbb{Q}^{(q-1)}} \times H$).

D'une façon générale, on note $\sigma_t \in \Gamma$, le symbole d'ARTIN usuel $\left(\frac{\mathbb{Q}'^{(q-1)}}{t}\right)$, $(t, p(q-1)) = 1$, ainsi que, par abus, les restrictions $\left(\frac{L}{t}\right)$ ou $\left(\frac{L'}{t}\right)$ de ces automorphismes aux sous-corps de $\mathbb{Q}'^{(q-1)}$.

On définit enfin $\nu'_{L/K} = \sum_{s'} s'$, $s' \in \mathrm{Gal}(L'/K')$ et $\nu_{L/K} = \sum_{s} s$, $s \in \mathrm{Gal}(L/K)$, pour tout K, L, $K \subset L \subset \mathbb{Q}^{(q-1)}$.

Dans le cas où $L = \mathbb{Q}^{(q-1)}$ on simplifie quelques unes des notations en posant notamment :

$$A = A_{\mathbb{Q}^{(q-1)}} \quad , \quad A' = A'_{\mathbb{Q}^{(q-1)}} \quad ,$$

$$\mathfrak{P} = \mathfrak{P}_{\mathbb{Q}^{(q-1)}} \quad , \quad \mathfrak{P}' = \mathfrak{P}'_{\mathbb{Q}^{(q-1)}} \quad \text{(fixés arbitrairement),}$$

$$G = G_{\mathbb{Q}^{(q-1)}} \quad , \quad G' = G'_{\mathbb{Q}^{(q-1)}}.$$

c) <u>Interprétation arithmétique de la première définition.</u>

Il est commode, pour une étude arithmétique des sommes de GAUSS, d'interpréter k et $\mathfrak{X}$ de la façon suivante :

On considère $\mathfrak{P}'$ (idéal premier au-dessus de p dans $\mathbb{Q}'^{(q-1)}$ choisi une fois pour toutes). On a $A'/\mathfrak{P}' \simeq k$; $\mathfrak{P}'$ étant fixé, on peut poser $k = A'/\mathfrak{P}'$.

On sait que le groupe W_{q-1} des racines $(q-1)^e$ de l'unité contenues dans A' est canoniquement isomorphe à k^*.

<u>Définition</u> I 2. L'isomorphisme réciproque (qui identifie k^* à W_{q-1}) définit (pour $\mathfrak{P}'$ fixé) un générateur privilégié de $\mathfrak{X}$ dont on considère l'inverse dans $\mathfrak{X}$ noté φ : on a donc, en notant $\bar{u}$ l'image de $u \in A'$ dans k,

$\varphi(\overline{u}) \equiv u^{-1} \bmod \mathfrak{P}'$ pour tout u, $u \notin \mathfrak{P}'$, et $\varphi(\overline{\xi}) = \xi^{-1}$ pour tout $\xi \in W_{q-1}$.

Remarque 11. Outre le signe – utilisé par certains auteurs (HASSE notamment) dans la définition des sommes de GAUSS, il semble qu'il serait préférable de définir $\tau_a(\psi)$ par $\tau_a(\psi) = -\sum_{x \in k} \psi^{-1}(x)\zeta^{aT(x)}$ selon un principe fréquent : ceci éviterait d'avoir à utiliser pour φ l'inverse de l'isomorphisme canonique.

2) Propriétés immédiates des sommes de GAUSS.

Proposition 11. On a les propriétés suivantes $\big((a,p) = 1,\ \psi \in \mathfrak{X}\big)$:

(i) $\tau_{ab}(\psi) = \psi^{-1}(b)\,\tau_a(\psi)$, pour tout b premier à p,

(ii) $\tau_a(1) = 1$,

(iii) $\tau_a(\psi)\,\tau_a(\psi)^{\sigma_{-1}} = q$, lorsque $\psi \neq 1$, où σ_{-1} désigne la conjugaison complexe,

(iv) $\tau_a(\psi)\,\tau_a(\psi^{-1}) = \psi(-1)q$, lorsque $\psi \neq 1$,

(v) $\tau_a(\psi^{p^r}) = \tau_a(\psi)$, pour tout $r \geq 0$.

démonstration

(i) On a $\tau_{ab}(\psi) = -\sum_{x \in k} \psi(x)\zeta^{abT(x)} = -\sum_{x \in k} \psi(x)\zeta^{aT(bx)}$; en posant bx = y dans k, on obtient

$$\tau_{ab}(\psi) = -\sum_{y \in k} \psi(yb^{-1})\zeta^{aT(y)} = -\psi^{-1}(b)\sum_{y \in k} \psi(y)\zeta^{aT(y)} = \psi^{-1}(b)\tau_a(\psi).$$

(ii) On a $\tau_a(1) = -\sum_{x \in k^*} \zeta^{aT(x)} = 1 - \sum_{x \in k} \zeta^{aT(x)}$; soit U le noyau de la trace T qui est surjective ; on a donc, en décomposant k mod U :

$$\tau_a(1) = 1 - \sum_{x \in U} (\zeta^{\circ} + \zeta^{a} + \dots + \zeta^{(p-1)a}) = 1.$$

(iii) D'après (i), on peut supposer a = 1. On a

$$\tau(\psi)\,\tau(\psi)^{\sigma_{-1}} = \sum_{x \in k^*} \psi(x)\zeta^{T(x)} \sum_{y \in k^*} \psi^{-1}(y)\zeta^{-T(y)} = \sum_{x,\, y \in k^*} \psi(xy^{-1})\zeta^{T(x-y)} ;$$

on pose $z = xy^{-1}$ et on obtient

$$\sum_{y,\, z \in k^*} \psi(z)\zeta^{T(yz-y)} = \sum_{z \in k^*} \psi(z) \sum_{y \in k^*} \zeta^{T(y(z-1))} \;;$$

pour $z \neq 1$, $\sum_{y \in k^*} \zeta^{T(y(z-1))} = -1$ (cf. démonstration de (ii))

et pour $z = 1$, cette expression vaut $q-1$;

$$\tau(\psi)\, \tau(\psi)^{\sigma_{-1}} = -\sum_{\substack{z \in k^* \\ z \neq 1}} \psi(z) + q-1 = 1 + q-1 = q$$

(car $\sum_{z \in k^*} \psi(z) = 0$, pour $\psi \neq 1$).

(iv) On a $\tau_a(\psi^{-1})^{\sigma_{-1}} = -\sum_{x \in k^*} \psi(x)\, \zeta^{-aT(x)} = \tau_{-a}(\psi) = \psi(-1)\, \tau_a(\psi)$(d'après (i)) d'où $\tau_a(\psi^{-1}) = \psi^{-1}(-1)\, \tau_a(\psi)^{\sigma_{-1}} = \psi(-1)\, \tau_a(\psi)^{\sigma_{-1}}$ et la relation en résulte.

(v) On a $\tau_a(\psi^{p^r}) = -\sum_{x \in k^*} \psi^{p^r}(x)\, \zeta^{aT(x)} = -\sum_{x \in k^*} \psi(x^{p^r})\, \zeta^{aT(x)}$;

or l'application $x \to x^{p^r}$ est la puissance r^e de l'automorphisme de FROBENIUS de k ; il suffit de poser $y = x^{p^r}$, y parcourant alors k^* et comme $T(y) = T(x)$, le résultat en découle.

Examinons maintenant l'action de Γ sur les sommes de GAUSS. On rappelle que les éléments de Γ sont notés σ_t $\big(t,\ p(q-1)\big) = 1$; il faut remarquer que lorsque $p(q-1)$ n'est pas un conducteur (cas $p = 2$ et cas où $q-1 \equiv 2 \bmod 4$) σ_t a un sens pour t pair mais l'action de σ_t sur les nombres $\psi(x)$ n'est pas nécessairement l'élévation à la puissance t ; c'est par contre le cas dès que l'on choisit t impair (ce qui est toujours possible).

<u>Proposition</u> 12. Pour tout $\sigma_b \in \Gamma$, $\big(b,\ p(q-1)\big) = 1$, on a $\tau_a(\psi)^{\sigma_b} = \psi^{-b}(b)\, \tau_a(\psi^b)$ (cette relation est encore vraie si σ_b est considéré comme élément de $\mathrm{Gal}(\mathbb{Q}'^{(m)}/\mathbb{Q})$, où m est l'ordre de ψ, à condition

de supposer b premier à pm). En particulier, si $\sigma_b \in G'$ (i. e. $b \equiv 1 \bmod p$) alors $\tau_a(\psi)^{\sigma_b} = \tau_a(\psi^b)$ et si $\sigma_b \in H$ $\big($i. e. $b \equiv 1 \bmod (q-1)\big)$ alors $\tau_a(\psi)^{\sigma_b} = \psi^{-1}(b)\ \tau_a(\psi)$.

démonstration.

On a, puisque b est supposé premier à p et à l'ordre de ψ, $\tau_a(\psi)^{\sigma_b} = -\sum_{x \in k^*} \psi(x)^b \zeta^{abT(x)} = \tau_{ab}(\psi^b) = \psi^{-b}(b)\ \tau_a(\psi^b)$ $\big($Prop. I1, (i)$\big)$.

Lorsque $b \equiv 1 \bmod p$, $\psi^{-b}(b) = \psi^{-b}(1) = 1$ et lorsque $b \equiv 1 \bmod (q-1)$, $\psi^b = \psi$, d'où les cas particuliers de la proposition.

Corollaire I1. Soit $\psi \in \mathfrak{X}$, ψ d'ordre $m | q-1$, soit a, $(a,p) = 1$ et soit $d = \dfrac{m}{(m, \frac{q-1}{p-1})}$. Alors $\tau_a(\psi)^d \in \mathbb{Q}^{(m)}$ et d est le plus petit entier positif ayant cette propriété.

Soit $\sigma_b \in H$; alors $\tau_a(\psi)^{\sigma_b} = \psi^{-1}(b)\ \tau_a(\psi)$. On a $\psi^{-1}(b)^d = \varphi^{-c\frac{q-1}{m}d}(b)$ (où l'on a posé $\psi = \varphi^{\frac{q-1}{m}c}$ avec $(c, m) = 1$) ; posons $\frac{q-1}{p-1} = \Delta\delta$ et $m = \Delta d\big((\delta, d) = 1,\ \Delta = (m, \frac{q-1}{p-1})\big)$; alors $\psi^{-1}(b)^d \equiv b^{c\frac{q-1}{m}d} \equiv b^{c(p-1)\delta} \equiv 1 \bmod \mathfrak{P}'$; d'où $\psi^{-1}(b)^d = 1$, quel que soit $\sigma_b \in H$, et $\tau_a(\psi)^d \in \mathbb{Q}^{(m)}$. Inversement, si $\tau_a(\psi)^\lambda \in \mathbb{Q}^{(m)}$ c'est que $\psi^{-1}(b)^\lambda = 1$ pour tout b mod p, $b \equiv 1 \bmod (q-1)$, soit $b^{c\frac{q-1}{m}\lambda} \equiv 1 \bmod p$, pour tout b ; ceci veut dire que $c\frac{q-1}{m}\lambda \equiv 0 \bmod (p-1)$ soit $c\frac{q-1}{m}\lambda = \mu(p-1)$ soit $c\,\Delta\delta\lambda = \mu\,\Delta d$ soit $c\,\delta\lambda = \mu d$; or $(c, d) = 1$ et $(\delta, d) = 1$, d'où $\lambda = \frac{\mu}{c\,\delta}\,d$ est multiple de d.

Remarque I2. On a le schéma d'inclusions suivant :

$$\mathbb{Q} \text{———} \mathbb{Q}^{(d)} \text{———} \overline{\mathbb{Q}^{(m)}} \text{———} \mathbb{Q}^{(m)}.$$

On sait que $\mathrm{Gal}(\mathbb{Q}^{(m)}/\overline{\mathbb{Q}^{(m)}})$ est engendré par σ_p (puisque

$p \nmid m)$; il suffit donc de vérifier que $p \equiv 1 \bmod d$; or si on pose $\frac{q-1}{p-1} = \Delta\delta$ et $m = \Delta d$, $(\delta, d) = 1$, on a $p-1 = \frac{q-1}{\Delta\delta} = \frac{(q-1)d}{m\delta} = \frac{q-1}{m\delta} d$ $\left(\frac{q-1}{m\delta}\right.$ étant entier car $\left.(\delta, d) = 1\right)$.

Corollaire 12. Soit $\psi \in \mathfrak{X}$, ψ d'ordre $m \mid q-1$. Alors $\tau_a(\psi) \in \overline{\mathbb{Q}'^{(m)}}$ $\left((a, p) = 1\right)$.

Soit $\sigma_c \in \mathrm{Gal}(\mathbb{Q}'^{(m)}/\overline{\mathbb{Q}'^{(m)}})$, $c \equiv 1 \bmod p$, $(c, m) = 1$: on a $\tau_a(\psi)^{\sigma_c} = \psi^{-c}(c)\ \tau_a(\psi^c) = \tau_a(\psi^c)$; or par hypothèse c est congru modulo m à une puissance de p , donc $\tau_a(\psi^c) = \tau_a(\psi)$ $\left(\text{Prop. } 11, \ (v)\right)$.

Ce corollaire, assez important, montre notamment que les sommes de GAUSS sont congrues à des rationnels modulo $\mathfrak{P}'$, rationnels qui seront déterminés dans le chapitre II.

On peut alors déterminer un corps d'appartenance de $\tau_a(\psi)$:

Corollaire 13. Soit $d = \frac{m}{(m, \frac{q-1}{p-1})}$, m ordre de ψ ; on sait (Rem. 12) que $d \mid p-1$. Alors $\tau_a(\psi)$ appartient au composé du corps $\overline{\mathbb{Q}^{(m)}}$ et de l'unique sous-corps de $\mathbb{Q}'$ de degré d sur $\mathbb{Q}$.

On utilise le corol. 11 dans l'extension de KUMMER $\mathbb{Q}'^{(q-1)}/\mathbb{Q}^{(q-1)}$: on a en particulier $\tau_a(\psi)^d \in \mathbb{Q}^{(q-1)}$ et $\tau_a(\psi)$ est dans l'extension de degré d sur $\mathbb{Q}^{(q-1)}$ contenue dans $\mathbb{Q}'^{(q-1)}$; d'où le résultat compte tenu du corol. 12.

Proposition 13. Pour tout χ et $\psi \in \mathfrak{X}$ le quotient $\frac{\tau(\chi)\ \tau(\psi)}{\tau(\chi\psi)}$ est un entier du corps $\mathbb{Q}^{(q-1)}$. Si en outre $\chi\psi \neq 1$, alors on a $\frac{\tau(\chi)\ \tau(\psi)}{\tau(\chi\psi)} = -\sum_{t \in k} \chi(t)\ \psi(1-t)$.

<u>démonstration</u>.

Le cas $\chi\psi = 1$ étant évident (cf. Prop. 11), on suppose $\chi\psi \neq 1$. On a $\tau(\chi)\,\tau(\psi) = \sum_{x,\, y \in k} \chi(x)\,\psi(y)\,\zeta^{T(x+y)}$; on pose $x+y = z$, $z \in k$ et $\tau(\chi)\,\tau(\psi) = \sum_{\substack{x \in k^* \\ z \in k}} \chi(x)\,\psi(z-x)\,\zeta^{T(z)}$. Pour $z = 0$, la somme $\sum_{x \in k^*} \chi(x)\,\psi(-x)$ est nulle car $\chi\psi \neq 1$. Dans les cas $z \in k^*$, on pose $x = tz$, $t \in k^*$, et on a alors $\tau(\chi)\,\tau(\psi) = \sum_{t,\, z \in k^*} \chi(t)\,\chi(z)\,\psi\big(z(1-t)\big)\,\zeta^{T(z)} =$

$$\sum_{t \in k^*} \chi(t)\,\psi(1-t) \sum_{z \in k^*} \chi(z)\,\psi(z)\,\zeta^{T(z)} = -\,\tau(\chi\psi) \sum_{t \in k^*} \chi(t)\,\psi(1-t).$$

Ceci démontre l'intégralité de $\frac{\tau(\chi)\,\tau(\psi)}{\tau(\chi\psi)}$, son appartenance à $\mathbb{Q}^{(q-1)}$ et la relation proposée.

II

CONGRUENCES ET RELATIONS DE STICKELBERGER

1) Congruences de STICKELBERGER. On désire établir une congruence modulo $\mathfrak{P}'$ relative aux sommes de GAUSS. Soit $\psi = \varphi^{\alpha}$, $0 \leq \alpha < q-1$. Soit $\alpha = \alpha_o + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$, $0 \leq \alpha_i \leq p-1$, l'écriture en base p de α (les α_i sont donc non tous égaux à p-1).

Définition II 1. On pose $s(\alpha) = \alpha_o + \alpha_1 + \ldots + \alpha_{n-1}$ (somme des chiffres) et $\gamma(\alpha) = \alpha_o!\ \alpha_1! \ldots \alpha_{n-1}!$ (produit des factorielles des chiffres).

On a le résultat suivant $\left([16]\ ;\ \text{cf. } [2], [4], [11]\right)$ où l'on pose $\pi = \zeta - 1$:

Théorème II 1. Soit α tel que $0 \leq \alpha < q-1$; alors on a :

$$\frac{\tau(\varphi^{\alpha})}{\pi^{s(\alpha)}} \equiv \frac{1}{\gamma(\alpha)} \text{ modulo } \mathfrak{P}'.$$

démonstration.

Le cas $\alpha = 0$ étant évident, on suppose $\alpha \geq 1$. On fait la démonstration par récurrence sur l'entier $s(\alpha)$, nombre qui est compris entre 1 et $n(p-1) - 1$.

(i) $s(\alpha) = 1$. Nécessairement $\alpha = p^r$, $0 \leq r < n$ et dans ce cas $\tau(\varphi^{\alpha}) = \tau(\varphi)$ (Prop. I1, (v)). Or on a
$\tau(\varphi) = -\sum\limits_{x \in k} \varphi(x)\, \zeta^{T(x)} = -\sum\limits_{x \in k} \varphi(x) \left(\zeta^{T(x)} - 1\right)$ car $\sum\limits_{x \in k} \varphi(x) = 0$ ($\varphi = 1$ suppose q = 2 soit $\alpha = 0$ qui est écarté). On sait que $\dfrac{\zeta^{T(x)} - 1}{\zeta - 1} \equiv T(x) \bmod \pi$,

d'où

$$\frac{\tau(\varphi)}{\pi} \equiv -\sum_{x \in k} \varphi(x)\, T(x) \bmod \pi \equiv -\sum_{\omega \in W_{q-1}} \omega^{-1}\, T(\omega) \bmod \pi \;;$$

or $T(\omega) \equiv \omega + \omega^{p} + \ldots + \omega^{p^{n-1}} \bmod \mathfrak{P}'$,

d'où $\dfrac{\tau(\varphi)}{\pi} \equiv -\sum\limits_{\omega \in W_{q-1}} \left(1 + \omega^{p-1} + \ldots + \omega^{p^{n-1}-1}\right) \equiv -(q-1) \equiv 1 \bmod \mathfrak{P}'$. Ceci démontre le cas (i).

(ii) Supposons la propriété démontrée pour tout $\beta \geq 1$ tel que $s(\beta) \leq \lambda$. Soit $\alpha < q-1$ tel que $s(\alpha) = \lambda + 1 \geq 2$. On a $\alpha = \alpha_o + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$, $0 \leq \alpha_i \leq p-1$. Il existe i, $0 \leq i \leq n-1$, tel que $\alpha_i \neq 0$; si i est choisi minimum, alors $\alpha = \alpha_i p^i + \ldots + \alpha_{n-1}\, p^{n-1} = p^i\left(\alpha_i + \ldots + \alpha_{n-1}\, p^{n-1-i}\right)$ et on aura $\tau(\varphi^{\alpha}) = \tau(\varphi^{\alpha'})$ avec $\alpha' = \alpha_i + \ldots + \alpha_{n-1}\, p^{n-1-i}$ (Prop. 11) ; on peut donc supposer quitte à remplacer α par α' que $i = 0$ (i. e. $\alpha_o > 0$) (on a toujours $s(\alpha') = s(\alpha)$ et $\gamma(\alpha') = \gamma(\alpha)$). Posons alors $\beta = \alpha - 1$. On a $\beta \geq 1$ et l'écriture en base p de β est bien $\beta = \alpha_o - 1 + \alpha_1 p + \ldots + \alpha_{n-1}\, p^{n-1}$, d'où $s(\beta) = s(\alpha) - 1 = \lambda$. Par hypothèse de récurrence on a

$$\frac{\tau(\varphi^{\beta})}{\pi^{s(\beta)}} \equiv \frac{1}{\gamma(\beta)} \bmod \mathfrak{P}'.$$

On a $\varphi^{\alpha} = \varphi^{\beta}\, \varphi$ et en utilisant la proposition 13 on peut écrire $\dfrac{\tau(\varphi^{\beta})\, \tau(\varphi)}{\tau(\varphi^{\alpha})} = -\sum\limits_{t \in k} \varphi(t)\, \varphi^{\beta}(1-t)$.

Calculons le membre de droite modulo $\mathfrak{P}'$;

Il revient au même de calculer mod $\mathfrak{P}'$:

$\rho = -\sum\limits_{\omega \in W_{q-1}} \omega^{-1}(1-\omega)^{q-1-\beta}$. Soit $\gamma = q-1-\beta$;

on a $\rho \equiv -\sum\limits_{\omega \in W_{q-1}} \omega^{-1} \sum\limits_{k=0}^{\gamma} (-1)^k\, C_{\gamma}^{k}\, \omega^{k} \bmod \mathfrak{P}'$

$$\equiv -\sum_{k=0}^{\gamma} (-1)^k\, C_{\gamma}^{k} \sum_{\omega \in W_{q-1}} \omega^{k-1} \bmod \mathfrak{P}'.$$

Or il y a une seule valeur de k ($k = 1$), $0 \leq k \leq \gamma$, telle que $k-1 \equiv 0 \bmod q-1$; d'où $\rho \equiv C^1_\gamma\ (q-1) \bmod \mathfrak{P}'$, $\rho \equiv -\gamma \bmod \mathfrak{P}'$ soit $\rho \equiv 1 + \alpha_o - 1 \equiv \alpha_o \bmod \mathfrak{P}'$.

Ceci prouve que $\dfrac{\tau(\varphi^\beta)\ \tau(\varphi)}{\tau(\varphi^\alpha)}$ est une $\mathfrak{P}'$-unité donc que

$\dfrac{\tau(\varphi^\alpha)}{\pi^{s(\beta)+1}} = \dfrac{\tau(\varphi^\alpha)}{\pi^{s(\alpha)}}$ est une $\mathfrak{P}'$-unité congrue à

$$\frac{1}{\gamma(\beta)}\ \frac{1}{\gamma_o} = \frac{1}{(\alpha_o-1)!\ldots\alpha_{n-1}!}\ \frac{1}{\alpha_o} = \frac{1}{\gamma(\alpha)} \bmod \mathfrak{P}'.$$

Ceci démontre le théorème II 1 ("congruences de Stickelberger").

On en déduit une factorisation des sommes de GAUSS :

Corollaire II 1. On a $\tau(\varphi^\alpha)A' = \prod_{\sigma_b \in G'_{\mathbb{Q}(q-1)}} \mathfrak{P}'^{\,s\left([\alpha b]_{q-1}\right)\sigma_b^{-1}}$

où σ_b, $b \equiv 1 \bmod p$, $(b,\ q-1) = 1$, parcourt un système de représentants de G' modulo le groupe de décomposition de p dans $\mathbb{Q}'^{(q-1)}/\mathbb{Q}'$ et où $[\ ]_{q-1}$ désigne la fonction résidu positif modulo $q-1$.

En effet, si $\mathfrak{P}'^{\sigma_b^{-1} v}$, $v \geq 0$, $\sigma_b \in G'_{\mathbb{Q}(q-1)}$, est la $\mathfrak{P}'^{\sigma_b^{-1}}$-contribution à $\tau(\varphi^\alpha)A'$, on voit en conjuguant par σ_b que $\tau(\varphi^\alpha)^{\sigma_b} A' = \tau(\varphi^{\alpha b})\ A'$ a pour $\mathfrak{P}'$-contribution $\mathfrak{P}'^v$, d'où $v = s\left([\alpha b]_{q-1}\right)$ d'après le résultat général. La factorisation s'obtient en considérant les idéaux premiers distincts au-dessus de p et en remarquant que d'après la prop. I 1 (iii) seuls ces idéaux sont à considérer.

Corollaire II 2. Soit $\mathcal{S}$ le Γ-module engendré par les sommes de GAUSS $\tau_a(\psi)$, a mod p, $\psi \in \mathfrak{X}$:

(i) Si $p \neq 2$, le $\mathbb{Z}$-module de torsion de $\mathcal{S}$ est W_{p-1} ;

(ii) si $p = 2$, le $\mathbb{Z}$-module de torsion est $\{\pm 1\}$ ou est trivial.

En effet, si $p \neq 2$, $q-1$ est pair et comme $\mathcal{S} \subset \mathbb{Q}^{\left(p(q-1)\right)}$, il ne peut y avoir que de la $p(q-1)$-torsion. Vérifions qu'il n'y a pas de p-torsion : Un élément de $\mathcal{S}$ peut s'écrire $\xi \prod_i \tau(\psi_i)^{n_i}$, $n_i \in \mathbb{Z}$, $\psi_i \in \mathfrak{X}$, $\xi^{q-1} = 1$ (en tenant compte de l'action de H et de la proposition 11, (i)) ; or si $\zeta = \xi \prod_i \tau(\psi_i)^{n_i}$, soit $\sigma_b \in H$, $\sigma_b \neq 1$ (ce qui est possible car $p \neq 2$) ; alors

$$\zeta^{\sigma_b} = \zeta^b = \xi^{\sigma_b} \prod_i \tau(\psi_i)^{n_i \sigma_b} = \xi \prod_i \psi_i^{-n_i}(b) \prod_i \tau(\psi_i)^{n_i} = \xi' \zeta, \quad \xi'^{q-1} = 1 ;$$

ceci conduit à $\zeta^b = \zeta$, ce qui est absurde lorsque $p \neq 2$.

Toute somme de GAUSS est congrue à un rationnel mod $\mathfrak{P}'$ et de plus, on a $\tau_a(\psi)^{\sigma_b} = \psi^{-b}(b)\ \tau_a(\psi^b)$ pour $\sigma_b \in \Gamma$, or $\left(\psi^{-1}(b)\right)^{p-1} = 1$; ainsi tout élément de torsion de $\mathcal{S}$ est dans W_{p-1} nécessairement (on vérifie enfin que $W_{p-1} \subset \mathcal{S}$). D'où (i).

Si $p = 2$, on vérifie que, pour des raisons de congruences à des rationnels modulo $\mathfrak{P}'$, il n'y a pas de $q-1$-torsion. Mais ici $H = (1)$ et il peut y avoir a priori de la 2-torsion.

Donnons un exemple pour lequel $-1 \in \mathcal{S}$: Soit $q = 16$ $(n = 4)$ et considérons les sommes de GAUSS $\tau(\varphi^3)$ et $\tau(\varphi^5)$. Comme $\overline{\mathbb{Q}^{(5)}} = \overline{\mathbb{Q}^{(3)}} = \mathbb{Q}$, on en déduit que $\tau(\varphi^3)$ et $\tau(\varphi^5)$ sont égales à ± 4. On peut engendrer $\mathbb{F}_{16}^*$ par t, racine du polynome irréductible sur $\mathbb{F}_2$: $X^4 + X + 1$; on en déduit alors le tableau suivant, où l'on a posé $\varphi(t) = j\,\xi$ $(j^3 = 1,\ \xi^5 = 1)$:

x	0	1	t	t^2	t^3	$t+1$	t^2+1	t^3+t^2	t^3+t+1	t^2+1	t^3+t	t^2+t+1	t^3+t^2+t	t^3+t^2+t+1	t^3+t^2+1	t^3+1
$\mathrm{Tr}\,x$	0	0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
$\varphi^3(x)$	0	1	ξ^3	ξ	ξ^4	ξ^2	1	ξ^3	ξ	ξ^4	ξ^2	1	ξ^3	ξ	ξ^4	ξ^2
$\varphi^5(x)$	0	1	j^2	j	1	j^2	j	1	j^2	j	1	j^2	j	1	j^2	j

D'où $\tau(\varphi^3) = -4$ et $\tau(\varphi^5) = +4$, soit $-1 \in \mathcal{S}$.

2) Changement de corps k. Etant donné m diviseur de $q-1$, $q = p^n$, soit $\tilde{n}$ un multiple de n : $\tilde{n} = \lambda n$ et soit $\tilde{q} = p^{\tilde{n}}$; alors $\tilde{q}-1$ est aussi un multiple de m et on peut définir les sommes de GAUSS notées $\tilde{\tau}$ à partir du corps fini à $\tilde{q}$ éléments $\tilde{k}$. Soit $\tilde{\varphi}$ le caractère générateur de $\tilde{\mathfrak{X}}$ correspondant à $\tilde{k}$. On peut supposer que $\tilde{k} = \tilde{A}'/\tilde{\mathfrak{P}}'$ où l'idéal premier $\tilde{\mathfrak{P}}'$ de $\mathbb{Q}'^{(\tilde{q}-1)}$, qui permet de définir $\tilde{\varphi}$, est au-dessus de l'idéal $\mathfrak{P}'$ associé à φ. On se propose de comparer $\tau_a(\varphi^{\frac{q-1}{m}b})$ et $\tilde{\tau}_a(\tilde{\varphi}^{\frac{\tilde{q}-1}{m}b})$, $(a,p) = 1$, $1 \leq b < m$.

$$\text{On a } \tilde{q}-1 = \Lambda(q-1) \text{ avec } \Lambda = 1 + p^n + \ldots + p^{(\lambda-1)n}.$$

Lemme III. Soient s et $\tilde{s}$ les fonctions "sommes de chiffres" relatives à n et $\tilde{n}$ et soient de même γ et $\tilde{\gamma}$ les fonctions "factorielles" relatives à n et $\tilde{n}$: alors $\tilde{s}(\Lambda\alpha) = \lambda\, s(\alpha)$ et $\tilde{\gamma}(\Lambda\alpha) = \gamma(\alpha)^\lambda$, pour $0 \leq \alpha < q-1$.

Soit $\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_{n-1}p^{n-1}$, $\alpha < q-1$, $0 \leq \alpha_i \leq p-1$; alors $\Lambda\alpha$ est inférieur à $\tilde{q}-1$ et est égal à

$\alpha_0 + \alpha_1 p + \ldots + \alpha_{n-1}p^{n-1} + \alpha_0 p^n + \alpha_1 p^{n+1} + \ldots + \alpha_{n-1}p^{2n-1} + \ldots$
$+ \alpha_0 p^{(\lambda-1)n} + \ldots + \alpha_{n-1}p^{\lambda n-1}$ qui est bien l'écriture en base p de $\Lambda\alpha$; d'où $\tilde{s}(\Lambda\alpha) = \lambda\, s(\alpha)$ et $\tilde{\gamma}(\Lambda\alpha) = \gamma(\alpha)^\lambda$.

On sait que $\dfrac{\tau_a\left(\varphi^{\frac{q-1}{m}b}\right)}{\pi^{s\left(\frac{q-1}{m}b\right)}}$ est une $\mathfrak{P}'$-unité et que $\dfrac{\tilde{\tau}_a\left(\tilde{\varphi}^{\frac{\tilde{q}-1}{m}b}\right)}{\pi^{\tilde{s}\left(\frac{\tilde{q}-1}{m}b\right)}}$ est une $\mathfrak{P}'$-unité ; or $\frac{\tilde{q}-1}{m}b = \Lambda\,\frac{q-1}{m}b$ et d'après le lemme précédent $\tilde{s}\left(\frac{\tilde{q}-1}{m}b\right) = \lambda\, s\left(\frac{q-1}{m}b\right)$ (puisque b est choisi inférieur à m, on a bien $0 \leq \frac{q-1}{m}b < q-1$). Comme b est quelconque, on en déduit en conjuguant que, en idéaux dans $A'_{\mathbb{Q}(m)}$, on a $\tilde{\tau}_a\left(\tilde{\varphi}^{\widetilde{\frac{q-1}{m}b}}\right)A'_{\mathbb{Q}(m)} = \left(\tau_a\left(\varphi^{\frac{q-1}{m}b}\right)A'_{\mathbb{Q}(m)}\right)^{\lambda}$.

On est donc amené à considérer $\rho = \dfrac{\tau_a\left(\varphi^{\frac{q-1}{m}b}\right)^{\lambda}}{\tilde{\tau}_a\left(\tilde{\varphi}^{\widetilde{\frac{q-1}{m}b}}\right)}$; d'après ce que l'on vient de voir, ρ est une unité.

Comme $\tilde{\varphi}^{\widetilde{\frac{q-1}{m}b}}(a) = \left(\varphi^{\frac{q-1}{m}b}(a)\right)^{\Lambda} = \left(\varphi^{\frac{q-1}{m}b}(a)\right)^{\lambda}$, on peut supposer $a = 1$ pour les calculs.

Soit $\sigma_c \in H$; $\rho^{\sigma_c} = \dfrac{\varphi^{-\lambda\frac{q-1}{m}b}(c)}{\tilde{\varphi}^{-\widetilde{\frac{q-1}{m}b}}(c)}\rho = \dfrac{\varphi^{-\lambda\frac{q-1}{m}b}(c)}{\tilde{\varphi}^{-\Lambda\frac{q-1}{m}b}(c)}\rho$.

Or $\tilde{\varphi}^{-\frac{q-1}{m}b}(c) \in W_{p-1}$ (car $c^{p-1} \equiv 1 \bmod p$)

d'où $\tilde{\varphi}^{-\Lambda\frac{q-1}{m}b}(c) = \tilde{\varphi}^{-\lambda\frac{q-1}{m}b}(c)$; comme φ et $\tilde{\varphi}$ coïncident sur W_{p-1} notamment, on a $\rho^{\sigma_c} = \rho$ pour tout $\sigma_c \in H$, et $\rho \in \mathbb{Q}^{(m)}$.

On a enfin $\rho\,\rho^{\sigma-1}$, ce qui fait que ρ est une racine de l'unité de $\mathbb{Q}^{(m)}$. Montrons, par une congruence mod $\tilde{\mathfrak{P}}'$, qu'elle est égale à 1 :

On a $\dfrac{\tau\left(\varphi^{\frac{q-1}{m}b}\right)}{\pi^{s\left(\frac{q-1}{m}b\right)}} \equiv \dfrac{1}{\gamma\left(\frac{q-1}{m}b\right)}$ mod $\tilde{\mathfrak{P}}'$ puisque $\tilde{\mathfrak{P}}'/\mathfrak{P}'$

et de même $\dfrac{\tilde{\tau}\left(\tilde{\varphi}^{\widetilde{\frac{q-1}{m}b}}\right)}{\pi^{\lambda s\left(\frac{q-1}{m}b\right)}} \equiv \dfrac{1}{\tilde{\gamma}\left(\Lambda\frac{q-1}{m}b\right)}$ mod $\tilde{\mathfrak{P}}'$. D'après le lemme III on a

$\tilde{\gamma}\left(\Lambda\frac{q-1}{m}b\right) = \gamma\left(\frac{q-1}{m}b\right)^{\lambda}$, d'où :

Proposition III. Avec les notations précédentes, on a l'égalité,

$\tilde{\tau}_a\left(\tilde{\varphi}^{\widetilde{\frac{q-1}{m}b}}\right) = \tau_a\left(\varphi^{\frac{q-1}{m}b}\right)^{\lambda}$, $0 \le b < m$, $(a, p) = 1$.

Dans la pratique, il est donc suffisant d'étudier les sommes de GAUSS d'un caractère d'ordre m relativement à $q = p^n$, la plus petite puissance de p congrue à 1 modulo m. Lorsque c'est le cas, nous dirons que les sommes de GAUSS sont réduites.

3) <u>Relations de STICKELBERGER</u>. D'après le corollaire II 1 on peut écrire $(0 \leq \alpha < q-1)$:

$$\tau(\varphi^{\alpha})^n A' = \prod_{\sigma_b \in G'} \mathfrak{P}'^{s\left([\alpha b]_{q-1}\right)\sigma_b^{-1}}.$$

Quitte à conjuguer cette relation, on peut toujours supposer que α est de la forme $\frac{q-1}{m}$ $(m \mid q-1)$. Dans ce cas $\tau(\varphi^{\alpha}) \in \mathbb{Q}'^{(m)}$.
Si $b \equiv 1 \bmod mp$ alors $\frac{q-1}{m} b \equiv \frac{q-1}{m} \bmod p(q-1)$ et $s\left(\left[\frac{q-1}{m} b\right]_{q-1}\right) = s\left(\frac{q-1}{m}\right)$

d'où : $\tau\left(\varphi^{\frac{q-1}{m}}\right)^n A'_{\mathbb{Q}^{(m)}} = \prod_{\sigma_b \in G'_{\mathbb{Q}^{(m)}}} \mathfrak{P}'^{\lambda s\left(\left[\frac{q-1}{m} b\right]_{q-1}\right)\sigma_b^{-1}}_{\mathbb{Q}^{(m)}}$, où λ est le degré résiduel de p dans $\mathbb{Q}^{(q-1)}/\mathbb{Q}^{(m)}$; dans le produit précédent, b parcourt l'ensemble des entiers b, $1 \leq b < mp$, $(b, mp) = 1$, $b \equiv 1 \bmod p$ et σ_b n'est autre que le symbole d'ARTIN $\left(\frac{\mathbb{Q}'^{(m)}}{b}\right)$. Comme $\frac{q-1}{m} b$ est défini modulo $q-1$, b est défini modulo m et en fait on peut faire porter le produit sur les b, $1 \leq b < m$, $(b, m) = 1$ puisqu'il n'y a qu'un seul idéal premier $\mathfrak{P}'_{\mathbb{Q}^{(m)}}$ au-dessus de $\mathfrak{P}_{\mathbb{Q}^{(m)}}$. Si σ_b appartient à une classe modulo le groupe de décomposition de p dans $\mathbb{Q}^{(m)}/\mathbb{Q}$, alors $b \equiv cp^r \bmod m$;

si $\frac{q-1}{m} b = \alpha_0 + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$,
alors $\frac{q-1}{m} cp^r = \alpha_0 p^r + \alpha_1 p^{r+1} + \ldots + \alpha_{n-1-r} p^{n-1} + \alpha_{n-r} p^n + \ldots + \alpha_{n-1} p^{n-1+r} \equiv$
$\alpha_{n-r} + \alpha_{n-r+1} p + \ldots + \alpha_{n-1} p^{r-1} + \alpha_0 p^r + \ldots + \alpha_{n-1-r} p^{n-1} \bmod q-1.$
Ceci prouve que $s\left(\left[\frac{q-1}{m} cp^r\right]_{q-1}\right) = s\left(\frac{q-1}{m} c\right)$.

On peut donc écrire, en remarquant que $n = \lambda n_{\mathbb{Q}^{(m)}}$ où $n_{\mathbb{Q}^{(m)}}$ est le degré résiduel de p dans $\mathbb{Q}^{(m)}/\mathbb{Q}$:

$$\tau\left(\varphi^{\frac{q-1}{m}}\right) A'_{\mathbb{Q}^{(m)}} = \prod_{\sigma_b \in G'_{\mathbb{Q}^{(m)}}} \mathfrak{P}'^{\,s\left(\frac{q-1}{m} b\right)\sigma_b^{-1}}_{\mathbb{Q}^{(m)}}$$

(en prenant les nombres b entre 1 et m).

Résumons ce résultat partiel dans un lemme :

<u>Lemme</u> II 2. Si $m \mid q-1$, on a $\tau\left(\varphi^{\frac{q-1}{m}}\right) A'_{\mathbb{Q}^{(m)}} = \prod_{\sigma_b \in G'_{\mathbb{Q}^{(m)}}} \mathfrak{P}'^{\,s\left(\frac{q-1}{m} b\right)\sigma_b^{-1}}_{\mathbb{Q}^{(m)}}$.

<u>Proposition</u> II 2. On a $\tau\left(\varphi^{\frac{q-1}{m}}\right)^m A_{\mathbb{Q}^{(m)}} = \mathfrak{P}_{\mathbb{Q}^{(m)}}^{\lambda \sum_{b=1}^{m *} b\,\sigma_b^{-1}}$, la sommation $\sum^*$ étant étendue aux b, $1 \leq b \leq m$, $(b, m) = 1$ et λ étant le degré résiduel de p dans $\mathbb{Q}^{(q-1)}/\mathbb{Q}^{(m)}$.

<u>démonstration</u>

Démontrons d'abord le lemme suivant :

<u>Lemme</u> II 3. Soit α tel que $0 \leq \alpha < q-1$. Alors on a

$s(\alpha) = (p-1) \sum_{j=0}^{n-1} \left(\frac{p^j \alpha}{q-1} - \left[\frac{p^j \alpha}{q-1}\right]\right)$, où $[\ \ ]$ désigne la partie entière.

En effet, si $\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$, $0 \leq \alpha_i \leq p-1$

on a $\alpha_j = \left[\frac{\alpha}{p^j}\right] - p\left[\frac{\alpha}{p^{j+1}}\right]$ et $s(\alpha) = \sum_{j=0}^{n-1} \alpha_j = \alpha + (1-p) \sum_{j=1}^{n} \left[\frac{\alpha}{p^j}\right]$

$$= \alpha + (1-p) \sum_{j=0}^{n-1} \left[\frac{\alpha p^j}{q}\right] ;$$

on écrit $\alpha = \alpha \frac{(p-1)(1+p+\ldots+p^{n-1})}{q-1}$

et $s(\alpha) = (p-1)\left(\sum_{j=0}^{n-1} \frac{\alpha p^j}{q-1} - \sum_{j=0}^{n-1} \left[\frac{\alpha p^j}{q}\right]\right)$

or on vérifie que $\left[\frac{\alpha p^j}{q-1}\right] = \left[\frac{\alpha p^j}{q}\right]$, pour $0 \leq j \leq n-1$, et le lemme en résulte.

On a alors en posant $\alpha = \frac{q-1}{m}$ et en réutilisant la formule du début du paragraphe : $\tau(\varphi^\alpha)^n A'_{\mathbb{Q}^{(m)}} = \mathfrak{P}'_{\mathbb{Q}^{(m)}}{}^{\lambda \sum_b s(\alpha b)\sigma_b^{-1}}$, $1 \leq b \leq m$, $(m,b) = 1$.

On a $\sum_b s(\alpha b)\sigma_b^{-1} = \sum_b \sum_{j=0}^{n-1} (p-1)\left(\frac{p^j b}{m} - \left[\frac{p^j b}{m}\right]\right)\sigma_b^{-1}$ (lemme II 3) ; or

$p^j b - m\left[\frac{p^j b}{m}\right]$ est le reste modulo m de $p^j b$, ce reste parcourt donc pour

j fixé le même ensemble que b, d'où, en posant $a = p^j b - m\left[\frac{p^j b}{m}\right]$, on a

$\sigma_a^{-1} = \sigma_{p^j}^{-1}\sigma_b^{-1}$ et $m\sum_b s(\alpha b)\sigma_b^{-1} = (p-1)\sum_{j=0}^{n-1} \sigma_p^j \sum_a a\sigma_a^{-1}$. Or σ_p^j parcourt le

groupe de décomposition de p dans $\mathbb{Q}'^{(m)}/\mathbb{Q}'$, d'où

$$\tau(\varphi^\alpha)^m A'_{\mathbb{Q}^{(m)}} = \mathfrak{P}'_{\mathbb{Q}^{(m)}}{}^{\lambda(p-1)\sum_a a\sigma_a^{-1}} = \left(\mathfrak{P}_{\mathbb{Q}^{(m)}} A'_{\mathbb{Q}^{(m)}}\right)^{\lambda \sum_a a\sigma_a^{-1}},$$ d'où la proposition puisque $\tau(\varphi^\alpha) \in \mathbb{Q}^{(m)}$.

<u>Remarque</u> II 1. Dans la pratique, on construit des sommes de GAUSS réduites ; dans ce cas $\lambda = 1$.

<u>Définition</u> II 2. Si m est un conducteur, l'élément $S_{\mathbb{Q}^{(m)}} = \frac{1}{m}\sum_{a=1}^{m}{}^{*} a\sigma_a^{-1}$ de $\mathbb{Q}[G_{\mathbb{Q}^{(m)}}]$ s'appelle l'élément de STICKELBERGER relatif à $\mathbb{Q}^{(m)}$

($\sum^*$ signifie que la sommation porte sur les a, $(a,m) = 1$).

Si $K \subset \mathbb{Q}^{(m)}$ est de conducteur m, on pose $S_K = \frac{1}{m}\sum_{a=1}^{m}{}^{*} a\left(\frac{K}{a}\right)^{-1} \in \mathbb{Q}[G_K]$.

<u>Remarque</u> II 2. Si m = 2d (d impair), m n'est pas un conducteur ; cepen-

dant l'élément correspondant $\frac{1}{2d}\sum_{a=1}^{2d}{}^{*}\, a\,\sigma_a^{-1}$ existe (il permet de factoriser les sommes de GAUSS $\tau(\varphi^{\frac{q-1}{2d}b})$) mais il n'est pas rattaché au corps $\mathbb{Q}^{(m)} = \mathbb{Q}^{(d)}$. On peut d'ailleurs vérifier facilement (cf. [5], p. 40) que $\frac{1}{2d}\sum_{a=1}^{2d}{}^{*}\, a\,\sigma_a^{-1} = \left(1 - (\frac{\mathbb{Q}^{(d)}}{2})^{-1}\right) S_{\mathbb{Q}^{(d)}} + \frac{1}{2}\, \nu_{\mathbb{Q}^{(d)}/\mathbb{Q}}$.

Corollaire II 3. On a, lorsque m est un conducteur :

$$\tau(\varphi^{\frac{q-1}{m}})^m A_{\overline{\mathbb{Q}^{(m)}}} = \mathfrak{P}_{\overline{\mathbb{Q}^{(m)}}}^{\lambda\, m S_{\mathbb{Q}^{(m)}}} .$$

Soit K une extension abélienne de $\mathbb{Q}$, de conducteur m ; on suppose que les sommes de GAUSS considérées ici sont réduites ($\lambda = 1$). On désigne par $\overline{S}_{\mathbb{Q}^{(m)}}$ (resp. $\overline{S}_K$) l'image canonique de $S_{\mathbb{Q}^{(m)}}$ (resp. S_K) dans $\mathbb{Q}[G_{\overline{\mathbb{Q}^{(m)}}}]$ (resp. $\mathbb{Q}[G_{\overline{K}}]$).

Lemme II 4. Soit $\omega' \in \mathbb{Z}[G'_K]$ et soit ω sa projection canonique dans $\mathbb{Z}[G_K]$. On suppose que $\Omega = S_K\,\omega$ est à coefficients dans $\mathbb{Z}$; alors $\mathfrak{P}_{\overline{K}}^{\Omega}$ est principal dans $\overline{K}$: $\mathfrak{P}_{\overline{K}}^{S_K \omega} = \nu_{\overline{\mathbb{Q}^{(m)}}/\overline{K}}\, \tau(\varphi^{\frac{q-1}{m}})^{\omega'} A_{\overline{K}}$.

On sait que (Corol. II 3) $\tau(\varphi^{\frac{q-1}{m}})^m A_{\overline{\mathbb{Q}^{(m)}}} = \mathfrak{P}_{\overline{\mathbb{Q}^{(m)}}}^{m S_{\mathbb{Q}^{(m)}}}$, d'où, par $\nu_{\overline{\mathbb{Q}^{(m)}}/\overline{K}}$: $\left(\nu_{\overline{\mathbb{Q}^{(m)}}/\overline{K}}\, \tau(\varphi^{\frac{q-1}{m}})^{m\omega}\right) A_{\overline{K}} = \mathfrak{P}_{\overline{K}}^{m\Omega}$

soit $\left(\nu_{\overline{\mathbb{Q}^{(m)}}/\overline{K}}\, \tau(\varphi^{\frac{q-1}{m}})^{m\overline{\omega}}\right) A_{\overline{K}} = \mathfrak{P}_{\overline{K}}^{m\overline{\Omega}}$, puisque $\tau(\varphi^{\frac{q-1}{m}})^m \in \mathbb{Q}^{(m)}$, en notant $\overline{\omega}$ et $\overline{\Omega}$ les projections canoniques de ω et Ω dans $\mathbb{Z}[G_{\overline{K}}]$. Montrons que

$\theta' = \nu'_{\overline{\mathbb{Q}^{(m)}}/\overline{K}} \; \tau\left(\varphi^{\frac{q-1}{m}}\right)^{\omega'} \in \overline{K}$. On a $\theta'^m \in \overline{\mathbb{Q}^{(m)}}$ et $\theta'^m A_{\overline{K}} = \mathfrak{P}_{\overline{K}}^{m\overline{\Omega}}$ puissance m^e d'idéal de $\overline{K}$. Considérons alors $\mathbb{Q}^{(m)}(\theta') \subset \mathbb{Q}'^{(m)}$; $\mathbb{Q}^{(m)}(\theta')/\mathbb{Q}^{(m)}$ est, d'après ce qui précède, une extension de KUMMER ramifiée au plus pour les diviseurs premiers de m, ce qui est impossible, sauf si $\theta' \in \mathbb{Q}^{(m)}$. Comme $\tau\left(\varphi^{\frac{q-1}{m}}\right) \in \overline{\mathbb{Q}'^{(m)}}$ (corol. I 2), alors $\theta' \in \overline{K}'$, d'où $\theta' \in \overline{K}' \cap \mathbb{Q}^{(m)} = \overline{K}$.

Ce qui précède conduit à l'énoncé classique du théorème de STICKELBERGER :

<u>Théorème</u> II 2. Soit K une extension abélienne de $\mathbb{Q}$ de conducteur m. Soit $G_K = \mathrm{Gal}(K/\mathbb{Q})$ et soit S_K la projection canonique de $S_{\mathbb{Q}^{(m)}}$ dans $\mathbb{Q}[G_K]$. Alors l'idéal $S_K \mathbb{Z}[G_K] \cap \mathbb{Z}[G_K]$ de $\mathbb{Z}[G_K]$ annule le groupe des classes d'idéaux de K.

Pour les propriétés de S_K se reporter à [5] (pp. 39-45).

Signalons pour terminer que FRÖHLICH [3] a donné (au moins dans le cas où K est un corps cyclotomique) une nouvelle démonstration du théorème d'annulation précédent sans utiliser les sommes de GAUSS (mais en se donnant néanmoins l'élément de STICKELBERGER S_K).

III

RELATIONS DE DAVENPORT-HASSE
INTERPRETATION AU MOYEN DES $\tau(L)$.

1) <u>Résultat général</u>. Dans [2], DAVENPORT et HASSE ont montré qu'il existait certaines relations non triviales entre les sommes de GAUSS. Le résultat est le suivant ($q = p^n$ est une puissance de p fixée quelconque et $\mathfrak{X}$ est le groupe des caractères de $\mathbb{F}_q^*$) :

<u>Théorème</u> III 1. Soit $\chi \in \mathfrak{X}$ et soit ψ un élément d'ordre $m \mid q-1$ de $\mathfrak{X}$. Alors on a $\prod_{\mu=0}^{m-1} \tau_a(\psi^\mu \chi) = \tau_{ma}(\chi^m) \prod_{\mu=0}^{m-1} \tau_a(\psi^\mu)$, pour tout a, $(a,p) = 1$.

<u>démonstration</u>

Il suffit de démontrer le théorème pour $a = 1$ (vérification immédiate).

On pose $\rho(m,\chi) = \dfrac{\prod_{\mu=0}^{m-1} \tau(\psi^\mu \chi)}{\tau_m(\chi^m) \prod_{\mu=0}^{m-1} \tau(\psi^\mu)}$, pour tout $m \mid q-1$ et tout $\chi \in \mathfrak{X}$; ψ est alors, dans le membre de droite un élément d'ordre m de $\mathfrak{X}$ (on vérifie facilement que $\rho(m,\chi)$ ne dépend que de m et χ et non du choix de ψ). On va démontrer ensuite arithmétiquement que $\rho(m,\chi) = 1$. La démonstration nécessite quatre lemmes.

<u>Lemme</u> III 1. Les nombres $\rho(m,\chi)$ ont les propriétés suivantes :

(i) $\rho(m,\chi) \in \mathbb{Q}^{(q-1)}$,

(ii) Pour tout $\sigma_b \in G$, $(b, q-1) = 1$, $\rho(m,\chi)^{\sigma_b} = \rho(m,\chi^b)$,

(iii) $\rho(m,\chi)\, \rho(m,\chi)^{\sigma_{-1}} = 1$.

Soit $\sigma_c \in H$ ($c \equiv 1 \bmod (q-1)$). Alors

$$\rho(m,\chi)^{\sigma_c} = \frac{\prod_{\mu=0}^{m-1} \psi^{-\mu}(c)\chi^{-1}(c)}{\chi^{-m}(c)\prod_{\mu=0}^{m-1}\psi^{-\mu}(c)}\ \rho(m,\chi) = \rho(m,\chi). \text{ D'où (i).}$$

Si $\sigma_b \in G'$ ($b \equiv 1 \bmod p$) alors

$$\rho(m,\chi)^{\sigma_b} = \frac{\prod_{\mu=0}^{m-1} \tau\left(\psi^{\mu b}\chi^{b}\right)}{\tau_m\left(\chi^{mb}\right)\prod_{\mu=0}^{m-1}\tau\left(\psi^{\mu b}\right)},$$ comme $(b, q-1) = 1$, $(b,m) = 1$ et μb modulo m parcourt l'intervalle $[0, m-1]$, d'où

$$\rho(m,\chi)^{\sigma_b} = \frac{\prod_{\lambda=0}^{m-1} \tau\left(\psi^{\lambda}\chi^{b}\right)}{\tau_m\left(\chi^{mb}\right)\prod_{\lambda=0}^{m-1}\tau(\psi^{\lambda})} = \rho(m,\chi^{b}), \text{ d'où (ii).}$$

Démontrons enfin (iii) : toute somme de GAUSS a pour module q sauf celle du caractère unité (égale à 1) ; si $\psi^{\mu}\chi = 1$ pour un certain μ_o (alors unique), c'est que $\chi = \psi^{-\mu_o}$ et alors $\chi^m = 1$ $\left(\tau(\psi^{\mu_o}\chi)\right.$ ainsi que $\tau_m(\chi^m)$ valent $\left.1\right)$ et dans ce cas $\rho(m,\chi)\ \rho(m,\chi)^{\sigma_{-1}} = \dfrac{q^{m-1}}{q^{m-1}} = 1$. Sinon on voit qu'aucun caractère (hormis ψ^{μ} pour $\mu = 0$) n'est égal à 1 et $\rho(m,\chi)\ \rho(m,\chi)^{\sigma_{-1}} = \dfrac{q^m}{q\, q^{m-1}} = 1$.

<u>Lemme</u> **III 2.** Les relations de DAVENPORT-HASSE sont vérifiées (i. e. $\rho(m,\chi) = 1$, pour tout $m|q-1$ et tout $\chi \in \mathfrak{X}$) si et seulement si on a $\rho(\ell,\chi) = 1$ pour tout $\chi \in \mathfrak{X}$ et pour tout nombre premier $\ell | q-1$.

Etant donné $\rho(m,\chi)$, $\chi \in \mathfrak{X}$, $m|q-1$, la démonstration se fait par récurrence sur le nombre de diviseurs premiers (comptés avec leur ordre de multiplicité) de m (le cas $m = 1$ est trivial et le cas $m = \ell$ est l'hypothèse : on suppose donc $m = \ell m'$). On a donc $\rho(m',\chi) = 1$ pour tout $\chi \in \mathfrak{X}$.

En particulier $\rho(m',\chi^{\ell}) = 1$, ce qui se traduit (en remarquant qu'un caractère d'ordre m' est ψ^{ℓ}) par :

$\prod_{\lambda=0}^{m'-1} \tau\left(\psi^{\lambda\ell}\,\chi^{\ell}\right) = \tau_{m'}\left(\chi^{\ell m'}\right) \prod_{\lambda=0}^{m'-1} \tau\left(\psi^{\lambda\ell}\right)$; on a aussi par hypothèse,

$\rho(\ell, \psi^{\lambda}\chi) = 1$ et $\rho(\ell,\psi^{\lambda}) = 1$; ce qui se traduit, en posant $\psi_o = \psi^{m'}$ par :

$$\tau_{\ell}\left(\psi^{\lambda\ell}\chi^{\ell}\right) = \prod_{\mu=0}^{\ell-1} \frac{\tau(\psi_o^{\mu}\,\psi^{\lambda}\chi)}{\tau(\psi_o^{\mu})} \quad \text{et} \quad \tau_{\ell}\left(\psi^{\lambda\ell}\right) = \prod_{\mu=0}^{\ell-1} \frac{\tau(\psi_o^{\mu}\,\psi^{\lambda})}{\tau(\psi_o^{\mu})}\ .$$

On en déduit l'égalité suivante (où ℓ^{*} est inverse de ℓ modulo p) :

$$\prod_{\lambda=0}^{m'-1}\prod_{\mu=0}^{\ell-1} \frac{\tau_{\ell^*}(\psi_o^{\mu}\,\psi^{\lambda}\,\chi)}{\tau_{\ell^*}(\psi_o^{\mu})} = \tau_{m'}\left(\chi^{\ell m'}\right) \prod_{\lambda=0}^{m'-1}\prod_{\mu=0}^{\ell-1} \frac{\tau_{\ell^*}(\psi_o^{\mu}\,\psi^{\lambda})}{\tau_{\ell^*}(\psi_o^{\mu})}\ ,$$

soit $\prod_{\lambda=0}^{m'-1}\prod_{\mu=0}^{\ell-1} \tau_{\ell^*}\left(\psi_o^{\mu}\,\psi^{\lambda}\,\chi\right) = \tau_{m'}\left(\chi^{\ell m'}\right) \prod_{\lambda=0}^{m'-1}\prod_{\mu=0}^{\ell-1} \tau_{\ell^*}\left(\psi_o^{\mu}\,\psi^{\lambda}\right)$.

On a $\psi_o^{\mu}\,\psi^{\lambda} = \psi^{m'\mu+\lambda}$; lorsque $0 \le \mu \le \ell-1$ et $0 \le \lambda \le m'-1$, $m'\mu+\lambda$ parcourt l'intervalle $[0,\ m'\ell-1]$, d'où

$\prod_{\nu=0}^{m-1} \tau_{\ell^*}(\psi^{\nu}\chi) = \tau_{m'}(\chi^{m}) \prod_{\nu=0}^{m-1} \tau_{\ell^*}(\psi^{\nu})$ soit

$\prod_{\nu=0}^{m-1} \frac{\tau(\psi^{\nu}\chi)}{\tau(\psi^{\nu})} = \chi^{-m}(\ell)\,\tau_{m'}(\chi^{m}) = \tau_{m}(\chi^{m})$, ce qui est bien la relation de

DAVENPORT-HASSE proposée.

Lemme III 3. On a $\rho(\ell,\chi) = 1$ pour tout $\chi \in \mathfrak{X}$, et tout ℓ premier, $\ell \mid q-1$.

Ceci se fait en deux étapes :

a) On montre d'abord un lemme qui donne une expression différente de la congruence de STICKELBERGER :

Lemme III 4. Soit $\alpha = \alpha_o + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$, $0 \leq \alpha_i \leq p-1$, $\alpha < q-1$. Alors on a : $\dfrac{\alpha!}{(-p)^{\frac{\alpha - s(\alpha)}{p-1}}} \equiv \gamma(\alpha) \bmod p$.

Décomposons le produit $\alpha!$ selon les intervalles (éventuellement vides) suivants :

$[1, \alpha_o]$, $[\alpha_o+1, \alpha_o+\alpha_1 p]$, ..., $[\alpha_o+\ldots+\alpha_{k-1} p^{k-1}+1, \alpha_o+\ldots+\alpha_k p^k]$, ..., $[\alpha_o+\ldots+\alpha_{n-2} p^{n-2}+1, \alpha_o+\ldots+\alpha_{n-1} p^{n-1}]$; le produit des termes du $(k+1)^e$ intervalle, $k \geq 1$, a pour p-valuation (avec la convention que si l'intervalle est vide, cette p-valuation est 0) :

$$\left[\frac{\alpha_o+\ldots+\alpha_k p^k}{p}\right] + \ldots + \left[\frac{\alpha_o+\ldots+\alpha_k p^k}{p^k}\right] - \left(\left[\frac{\alpha_o+\ldots+\alpha_{k-1} p^{k-1}}{p}\right] + \ldots + \left[\frac{\alpha_o+\ldots+\alpha_{k-1} p^{k-1}}{p^{k-1}}\right]\right) = \alpha_1+\alpha_2 p+\ldots+\alpha_k p^{k-1} + \alpha_2+\alpha_3 p+\ldots+$$

$$\alpha_k p^{k-2} + \ldots + \alpha_k - \left(\alpha_1+\alpha_2 p+\ldots+\alpha_{k-1} p^{k-2} + \alpha_2+\alpha_3 p+\ldots+\alpha_{k-1} p^{k-3}+\ldots+\alpha_{k-1}\right)$$

$$= \alpha_k\left(p^{k-1}+\ldots+p+1\right) = \alpha_k \frac{p^k-1}{p-1}.$$ Donc la p-valuation de $\alpha!$ est

$$\alpha_1 + \alpha_2 \frac{p^2-1}{p-1} + \ldots + \alpha_{n-1} \frac{p^{n-1}-1}{p-1} = \frac{1}{p-1}\left(\alpha_1(p-1)+\ldots+\alpha_{n-1}(p^{n-1}-1)\right) =$$

$$\frac{1}{p-1}\left(\alpha - s(\alpha)\right).$$

Déterminons maintenant pour tout k, $0 \leq k \leq n-1$, les multiples de p^k (non multiples de p^{k+1}) de l'intervalle $[1, \alpha]$: ce sont les nombres p^k, $2p^k$, ..., $\Lambda_k p^k$ (en omettant les multiples de p^{k+1}) où $\Lambda_k = \left[\frac{\alpha}{p^k}\right] = \alpha_k + \alpha_{k+1} p + \ldots + \alpha_{n-1} p^{n-1-k}$; le produit correspondant (i. e. de ces nombres divisés auparavant par p^k) est égal à :

$$\prod_{\substack{i=1 \\ i \not\equiv 0(p)}}^{\Lambda_k} i = \{1.2\ldots(p-1)\}\{(p+1)\ldots(2p-1)\}\ldots\{((\Lambda_{k+1}-1)p+1)\ldots(\Lambda_{k+1}p-1)\} \times$$

$\left\{\left(\Lambda_{k+1}\, p+1\right)\ldots\left(\Lambda_{k+1}\, p+\alpha_k\right)\right\}$ (pour le dernier produit entre accolades, si $\alpha_k = 0$ le produit vaut 1) avec $\Lambda_{k+1} = \left[\frac{\alpha}{p^{k+1}}\right] = \alpha_{k+1} + \ldots + \alpha_{n-1}\, p^{n-2-k}$ $\left(\text{ici } k < n-1 \text{ ; pour } k = n-1,\ \Lambda_k = \alpha_{n-1} \text{ et } \Lambda_n = 0\right)$; soit $\prod_{\substack{i=1\\ i\not\equiv 0(p)}}^{\Lambda_k} \equiv$ $\left((p-1)!\right)^{\Lambda_{k+1}} \alpha_k! \bmod p$; or $(p-1)! \equiv -1 \bmod (p)$ et on obtient un résidu égal à $(-1)^{\Lambda_{k+1}} \alpha_k! \bmod p$. D'où $\dfrac{\alpha!}{p^{\frac{\alpha-s(\alpha)}{p-1}}} \equiv \gamma(\alpha)\, (-1)^{\sum_{k=0}^{n-1} \Lambda_{k+1}} \bmod p$;

or $(-1)^p \equiv -1 \bmod p$ et $\sum_{k=0}^{n-1} \Lambda_{k+1} = \alpha_1 + \alpha_2(p+1) + \ldots + \alpha_{n-1}(p^{n-2} + \ldots + 1) = \dfrac{\alpha - s(\alpha)}{p-1}$, d'où le lemme.

<u>Corollaire</u> III 1. On a, pour tout α, $0 \leq \alpha < q-1$:

$$\frac{\tau(\varphi^\alpha)\,\alpha!}{\pi^\alpha} \equiv 1 \bmod \mathfrak{P}'.$$

On a en effet $\dfrac{\tau(\varphi^\alpha)}{\pi^{s(\alpha)}} \equiv \dfrac{1}{\gamma(\alpha)} \bmod \mathfrak{P}'$ soit

$\dfrac{\tau(\varphi^\alpha)}{\pi^{s(\alpha)}}\ \dfrac{\alpha!}{(-p)^{\frac{\alpha-s(\alpha)}{p-1}}} \equiv 1 \bmod \mathfrak{P}'$. Or on vérifie facilement que

$\dfrac{(-1)^{p-1}\, p}{\pi^{p-1}} \equiv (p-1)! \equiv -1 \bmod \pi$ soit $\dfrac{-p}{\pi^{p-1}} \equiv 1 \bmod \pi$ et

$\pi^{s(\alpha)}\, (-p)^{\frac{\alpha-s(\alpha)}{p-1}} \equiv \pi^{s(\alpha)+\alpha-s(\alpha)} = \pi^\alpha \bmod \pi^{\alpha+1}$; d'où le résultat.

b) Démontrons maintenant que $\rho(\ell,\chi) = 1$.

Pour cela on va démontrer que pour tout idéal $\mathfrak{P}$ de $\mathbb{Q}^{(q-1)}$ au-dessus de p, on a $\rho(\ell,\chi) \equiv 1 \bmod \mathfrak{P}$; il en résultera que $\rho(\ell,\chi)$ est premier à p donc est une unité ; étant de module 1 ce sera une racine de l'unité facilement identifiable.

Quitte à conjuguer, d'après le lemme III 1, (ii), on peut se limiter à démontrer que $\rho(\ell,\chi) \equiv 1 \bmod \mathfrak{P}$ pour tout χ et pour un unique $\mathfrak{P}$ au-dessus de p dans $\mathbb{Q}^{(q-1)}$.

On a $\rho(\ell,\chi) = \dfrac{\prod_{\mu=0}^{\ell-1} \tau(\psi^{\mu}\chi)}{\tau_{\ell}(\chi^{\ell})\prod_{\mu=0}^{\ell-1}\tau(\psi^{\mu})} = \dfrac{\prod_{\mu=0}^{\ell-1}\tau\left(\varphi^{\frac{q-1}{\ell}\mu + \frac{q-1}{m}b}\right)}{\tau_{\ell}\left(\varphi^{\frac{q-1}{m}b\ell}\right)\prod_{\mu=0}^{\ell-1}\tau\left(\varphi^{\frac{q-1}{\ell}\mu}\right)}$

si $\chi = \varphi^{\frac{q-1}{m}b}$, $(b,m) = 1$, $1 \leq b < m$.

On transforme cette expression : si $\ell \nmid m$, on pose $b\ell = \lambda m + r$ $\quad 0 \leq r < m$ et alors $\frac{q-1}{m}b = \frac{q-1}{m\ell}b\ell = \frac{q-1}{m\ell}(\lambda m + r) = \lambda\frac{q-1}{\ell} + \frac{q-1}{m\ell}r$;

si $\ell | m$, $m = \ell m'$ et on pose $b = \lambda' m' + r'$, $0 \leq r' < m'$ et

$\frac{q-1}{m}b = \frac{q-1}{\ell m'}(\lambda' m' + r') = \lambda'\frac{q-1}{\ell} + \frac{q-1}{\ell m'}r'$.

Dans le premier cas,

$$\rho(\ell,\chi) = \frac{1}{\tau_{\ell}\left(\varphi^{\frac{q-1}{m}r}\right)} \prod_{\mu=0}^{\ell-1} \frac{\tau\left(\varphi^{\frac{q-1}{\ell}\mu + \frac{q-1}{m\ell}r}\right)}{\tau\left(\varphi^{\frac{q-1}{\ell}\mu}\right)}$$ (par changement d'indice de sommation convenable) ;

dans le second on a $\rho(\ell,\chi) = \dfrac{1}{\tau_{\ell}\left(\varphi^{\frac{q-1}{m'}r'}\right)} \prod_{\mu=0}^{\ell-1} \dfrac{\tau\left(\varphi^{\frac{q-1}{\ell}\mu + \frac{q-1}{m}r'}\right)}{\tau\left(\varphi^{\frac{q-1}{\ell}\mu}\right)}$.

Dans tous les cas, on peut donc écrire

$\rho(\ell,\chi) = \dfrac{1}{\tau_{\ell}\left(\varphi^{x\ell}\right)} \prod_{\mu=0}^{\ell-1} \dfrac{\tau\left(\varphi^{\frac{q-1}{\ell}\mu + x}\right)}{\tau\left(\varphi^{\frac{q-1}{\ell}\mu}\right)}$ avec $0 \leq x < \frac{q-1}{\ell}$, x entier ; on remarque aussi que l'on a $0 \leq \frac{q-1}{\ell}\mu + x < q-1$ et $0 \leq \frac{q-1}{\ell}\mu < q-1$.

On peut donc écrire, d'après le corollaire III 1 :

$$\rho(\ell,\chi) \equiv \frac{\prod_{\mu=0}^{\ell-1} \frac{\pi^{A_\mu}}{A_\mu !}}{\tau_\ell(\varphi^{x\ell}) \prod_{\mu=0}^{\ell-1} \frac{\pi^{B_\mu}}{B_\mu !}} \text{ modulo } \mathfrak{P}', \text{ avec :}$$

$A_\mu = \frac{q-1}{\ell}\mu + x$ et $B_\mu = \frac{q-1}{\ell}\mu$ $\left(x = \frac{q-1}{m\ell} r \text{ si } \ell \nmid m,\ \frac{q-1}{m} r' \text{ si } \ell | m\right)$.

On a $\tau_\ell(\varphi^{x\ell}) = \varphi^{-x\ell}(\ell)\, \tau(\varphi^{x\ell})$ avec $\varphi^{-x\ell}(\ell) \equiv \ell^{x\ell}$ mod $\mathfrak{P}'$; d'où :

$$\rho(\ell,\chi) \equiv \frac{1}{\ell^{\ell x} \frac{\pi^{\ell x}}{(\ell x)!}} \prod_{\mu=0}^{\ell-1} \left(\pi^{A_\mu - B_\mu} \frac{B_\mu !}{A_\mu !}\right) \text{ mod } \mathfrak{P}'.$$

On a $\sum_{\mu=0}^{\ell-1} (A_\mu - B_\mu) - \ell x = \sum_{\mu=0}^{\ell-1} \left(\frac{q-1}{\ell}\mu + x - \frac{q-1}{\ell}\mu\right) - \ell x = 0$

d'où : $\rho(\ell,\chi) \equiv \frac{(\ell x)!}{\ell^{\ell x}} \prod_{\mu=0}^{\ell-1} \frac{B_\mu !}{A_\mu !}$ mod $\mathfrak{P}'$.

Posons $F(x) = \frac{\ell^{\ell x}}{(\ell x)!} \prod_{\mu=0}^{\ell-1} \left(\frac{q-1}{\ell}\mu + x\right)!$, pour $0 \leq x < \frac{q-1}{\ell}$.

Pour $x \geq 1$, $\frac{F(x)}{F(x-1)} = \ell^{\ell x - \ell(x-1)} \frac{(\ell(x-1))!}{(\ell x)!} \prod_{\mu=0}^{\ell-1} \frac{\left(\frac{q-1}{\ell}\mu + x\right)!}{\left(\frac{q-1}{\ell}\mu + x - 1\right)!} =$

$\ell^\ell \prod_{\mu=0}^{\ell-1} \frac{\left(\frac{q-1}{\ell}\mu + x\right)}{(\ell x - \mu)} = \prod_{\mu=0}^{\ell-1} \frac{(q-1)\mu + \ell x}{-\mu + \ell x}$; or la relation $x < \frac{q-1}{\ell}$ entraîne que $\ell x - \mu$ et $(q-1)\mu - \ell x$ ont même p-participation ainsi $\frac{F(x)}{F(x-1)} \equiv 1$ mod p et $\frac{F(x)}{F(0)} \equiv 1$ mod p. On applique ceci à $\rho(\ell,\chi)$ et on obtient $\rho(\ell,\chi) \equiv 1$ mod $\mathfrak{P}'$. On a donc démontré que la racine de l'unité $\rho(\ell,\chi)$ est congrue à 1 modulo $\mathfrak{P}'$; comme elle est, pour $p \neq 2$, un élément de W_{p-1}

(cf. Corol. II 2), il en résulte que $\rho(\ell,\chi) = 1$. Pour $p = 2$, on a a priori $\rho(\ell,\chi) = \pm 1$. On utilise alors une congruence modulo ℓ : Soit ξ une racine d'ordre ℓ de l'unité et soit $\varpi = \xi - 1$; comme $\ell \mid 2^n - 1$, ℓ est impair et on a pour tout $x \in k$, $\psi(x) \equiv 1 \mod \varpi$; de plus ϖ est premier à p donc on peut écrire

$$\tau(\psi^\mu\chi) = -\sum_{x\in k} \psi^\mu(x)\,\chi(x)\,\zeta^{T(x)} \equiv -\sum_{x\in k} \chi(x)\,\zeta^{T(x)} \equiv \tau(\chi) \mod \varpi$$

et $\tau(\psi^\mu) \equiv 1 \mod \varpi$. D'où $\rho(\ell,\chi) \equiv \dfrac{\tau(\chi)^\ell}{\tau_\ell(\chi^\ell)} \mod \varpi$;

or $\tau(x)^\ell \equiv \left(-\sum_{x\in k} \chi(x)\,\zeta^{T(x)}\right)^\ell \equiv -\sum_{x\in k} \chi^\ell(x)\,\zeta^{\ell T(x)} \equiv \tau_\ell(\chi^\ell) \mod \varpi$.

Ainsi $\rho(\ell,\chi) \equiv 1 \mod \varpi$ et nécessairement, on a $\rho(\ell,\chi) = 1$.

Ceci achève la démonstration des relations de DAVENPORT-HASSE sur les sommes de GAUSS.

Nous allons montrer dans le §2 suivant comment interpréter d'une façon plus arithmétique, ces relations, en définissant certaines quantités $\tau(L)$ associées aux extensions abéliennes de $\mathbb{Q}$.

2) <u>Définition et propriétés de $\tau(L)$</u>. On suppose maintenant $p \neq 2$.

a) <u>Définition de</u> $\tau\left(\mathbb{Q}^{(m)}\right)$. Soit m premier à p un conducteur de corps cyclotomique (i. e. si m est pair, alors $m \equiv 0 \mod 4$) et soit $q = p^n$ la plus petite puissance de p congrue à 1 mod m. Soit $\mathfrak{X}$ le groupe des caractères de $\mathbb{F}_q^*$. Soit $\chi_o = \varphi^{\frac{q-1}{2}}$ l'unique élément d'ordre 2 de $\mathfrak{X}$; on a $\tau(\chi_o) \in \mathbb{Q}'$.
On a aussi (Prop. III 1) $\tau(\chi_o) = \tau\left(\varphi_1^{\frac{p-1}{2}}\right)^n$, φ_1 étant le générateur de $\mathfrak{X}_1$ correspondant à $\mathbb{F}_p^*$.

<u>Définition</u> III 1. Soit m un conducteur de corps cyclotomique, soit n le degré résiduel de p dans $\mathbb{Q}^{(m)}/\mathbb{Q}$ et soit $q = p^n$. On pose :

$$\tau\left(\mathbb{Q}^{(m)}\right) = \varphi(2)^{\frac{q-1}{2}}\ \tau_{\frac{q-1}{m}}\left(\varphi^{\frac{q-1}{m}}\right)\tau_{\frac{q-1}{m}}\left(\varphi^{\frac{q-1}{2}}\right)^{-1},$$

la construction des sommes de GAUSS ci-dessus étant relative au corps fini $\mathbb{F}_q$.

Si l'on se reporte à l'exposé de [13] (chap. II, Déf. 7.2) ainsi qu'au travail original de HASSE ([9]), on constate que $\tau(\mathbb{Q}^{(m)})$ est, à une racine de l'unité près, le "ARTIN root number" relatif au caractère abélien $\varphi^{\frac{q-1}{m}}$.

On constate que $\tau(\mathbb{Q}^{(m)})$ est un élément de $\mathbb{Q}'^{(m)}$ qui se trouve en fait dans $\overline{\mathbb{Q}'^{(m)}}$ (corol. I 2).

b) <u>Définition de</u> $\tau(L)$. Soit L un corps abélien quelconque et soit m_L son conducteur. Le corps $\overline{L}$ est égal à $L \cap \overline{\mathbb{Q}^{(m_L)}}$.

<u>Définition</u> III 2. On pose $\tau(L) = \nu'_{\overline{\mathbb{Q}^{(m_L)}}/\overline{L}}\left(\tau(\mathbb{Q}^{(m_L)})\right)$.

Ceci est justifié car $\tau\left(\mathbb{Q}^{(m_L)}\right) \in \overline{\mathbb{Q}'^{(m_L)}}$.

Il en résulte alors que $\tau(L) \in \overline{L'}$. On vérifie facilement que $\tau(L)^{2m_L} \in \overline{L}$ (ceci ayant lieu pour $\tau\left(\mathbb{Q}^{(m_L)}\right)$). On peut d'ailleurs préciser davantage en utilisant le corollaire I 3.

On se propose d'étudier l'action de $\nu'_{\overline{L}/\overline{K}}$ sur $\tau(L)$ pour tout sous-corps K de L. Pour cela on commence par étudier l'action de $\nu'_{L/K}$.

Soient L et K, $K \subset L$, quelconques. On appelle m_L (resp. m_K) le conducteur de L (resp. K). On rappelle que $\tau(L)$ est construite à partir de $\mathbb{F}_{q_L}$ ($q_L = p^{n_L}$) et que $\tau(K)$ est construite à partir de $\mathbb{F}_{q_K}$ ($q_K = p^{n_K}$) n_L et n_K désignant les degrés résiduels de p dans $\mathbb{Q}^{(m_L)}$ et $\mathbb{Q}^{(m_K)}$ respectivement. On a le schéma suivant :

$$\begin{tikzcd}
 & L \arrow[r, no head] \arrow[d, no head] & L\mathbb{Q}^{(m_K)} \arrow[r, no head] \arrow[d, no head] & \mathbb{Q}^{(m_L)} \\
K \arrow[r, no head] & L \cap \mathbb{Q}^{(m_K)} \arrow[r, no head] & \mathbb{Q}^{(m_K)} &
\end{tikzcd}$$

Comme $\mathbb{Q}'/\mathbb{Q}$ est linéairement disjointe de toutes les extensions du schéma ci-dessus, on peut écrire (en remarquant que $[\mathbb{Q}^{(m_L)} : \overline{L\mathbb{Q}^{(m_L)}}] = n_L/\lambda_L$) :

$$\nu'_{L/K}\ \tau(L)^{n_L/\lambda_L} = \nu'_{L/K}\left(\nu'_{\mathbb{Q}^{(m_L)}/L}\left(\tau(\mathbb{Q}^{(m_L)})\right)\right) =$$

$$\nu'_{\mathbb{Q}^{(m_L)}/K}\left(\tau(\mathbb{Q}^{(m_L)})\right) = \nu'_{\mathbb{Q}^{(m_K)}/K}\ \nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau(\mathbb{Q}^{(m_L)})\right) \quad ;$$

or $\quad \nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau(\mathbb{Q}^{(m_L)})\right) \in \overline{\mathbb{Q}'^{(m_K)}}$, car $\overline{\mathbb{Q}^{(m_K)}} = \overline{\mathbb{Q}^{(m_L)}} \cap \mathbb{Q}^{(m_K)}$,

d'où $\nu'_{L/K}\left(\tau(L)^{n_L/\lambda_L}\right) = \nu'_{\overline{\mathbb{Q}^{(m_K)}}/\overline{K}}\left(\nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau(\mathbb{Q}^{(m_L)})\right)\right)^{n_K/\lambda_K}$,

puisque, de même, $[\mathbb{Q}^{(m_K)} : \overline{K\mathbb{Q}^{(m_K)}}] = n_K/\lambda_K$.

Nous allons faire le calcul de $\nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau(\mathbb{Q}^{(m_L)})\right)$ par récurrence sur le nombre de diviseurs premiers (comptés avec leur ordre de multiplicité) de $\frac{m_L}{m_K}$.

<u>Lemme</u> III 5. Soit q une puissance quelconque de $p \neq 2$ et soit m un diviseur quelconque de q-1 (on n'impose ni le fait que q soit la plus petite puissance de p congrue à 1 mod m, ni que m soit un conducteur). Alors soit ℓ un diviseur premier de m :

(i) si $\ell^2 | m$, $\nu'_{\mathbb{Q}^{(m)}/\mathbb{Q}^{(m/\ell)}}\left(\tau_{\frac{q-1}{m}}(\varphi^{\frac{q-1}{m}})\right) = \chi_o^\ell(\ell)\,\tau_{\frac{q-1}{m}}(\chi_o)^{\ell-1}\,\tau_{\frac{q-1}{m/\ell}}\left(\varphi^{\frac{q-1}{m/\ell}}\right)$;

(ii) si $\ell^2 \nmid m$, $\nu'_{\mathbb{Q}^{(m)}/\mathbb{Q}^{(m/\ell)}}\left(\tau_{\frac{q-1}{m}}(\varphi^{\frac{q-1}{m}})\right) =$

$$\chi_o^\ell(\ell)\,\tau_{\frac{q-1}{m}}(\chi_o)^{\ell-1}\left(\tau_{\frac{q-1}{m/\ell}}\left(\varphi^{\frac{q-1}{m/\ell}}\right)\right)^{1-\left(\frac{\mathbb{Q}'^{(\frac{m}{\ell})}}{\ell}\right)^{-1}}.$$

Cas où $\ell^2 | m$. On a alors (que m, m/ℓ soient ou non des conducteurs) :

$$\mathrm{Gal}\left(\mathbb{Q}'^{(m)}/\mathbb{Q}'^{(m/\ell)}\right) = \left\{1, \sigma_{1+\frac{m}{\ell}p}, \dots, \sigma_{1+(\ell-1)\frac{m}{\ell}p}\right\},$$

d'où, en posant $\nu' = \nu'_{\mathbb{Q}^{(m)}/\mathbb{Q}^{(m/\ell)}}$ et $\alpha = \frac{q-1}{m}$ pour simplifier :

$$\nu'\,\tau_\alpha(\varphi^\alpha) = \prod_{\mu=0}^{\ell-1}\tau_\alpha\left(\varphi^{\alpha(1+\mu\frac{m}{\ell}p)}\right) = \prod_{\mu=0}^{\ell-1}\tau_\alpha\left(\varphi^\alpha\varphi^{\alpha\mu\frac{m}{\ell}p}\right);$$

or $\varphi^{\frac{m}{\ell}\alpha} = \varphi^{\frac{q-1}{\ell}} = \psi$ (caractère d'ordre ℓ de $\mathfrak{X}$) et

$\nu'\,\tau_\alpha(\varphi^\alpha) = \prod_{\mu=0}^{\ell-1}\tau_\alpha\left(\psi^{\mu p}\varphi^\alpha\right) = \prod_{\mu=0}^{\ell-1}\tau_\alpha\left(\psi^\mu\varphi^\alpha\right)$ puisque $(p,\ell) = 1$. On utilise alors la relation de DAVENPORT-HASSE (Th. III 1) qui conduit à

$$\nu'\,\tau_\alpha(\varphi^\alpha) = \tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)\prod_{\mu=0}^{\ell-1}\tau_\alpha(\psi^\mu).$$

<u>Lemme</u> **III 6.** On a $\prod_{\mu=0}^{\ell-1}\tau_\alpha(\psi^\mu) = \chi_o^\ell(\ell)\,\tau_\alpha(\chi_o)^{\ell-1}$.

Si $\ell = 2$, $\psi = \chi_o$ et $\prod_{\mu=0}^{1}\tau_\alpha(\chi_o^\mu) = \tau_\alpha(1)\,\tau_\alpha(\chi_o) = \tau_\alpha(\chi_o)$;

or on a bien $\chi_o^2(2) = 1$.

Si $\ell \neq 2$, considérons $\prod_{\mu=0}^{\ell-1}\tau_\alpha(\psi^\mu) = \prod_{\mu=1}^{\frac{\ell-1}{2}}\left(\tau_\alpha(\psi^\mu)\,\tau_\alpha(\psi^{\ell-\mu})\right) =$

$\prod_{\mu=1}^{\frac{\ell-1}{2}} \psi^{\mu}(-1) q = q^{\frac{\ell-1}{2}}$ car ψ est d'ordre impair (cf. Prop. 11, (iv)) et

$\psi(-1) = 1$. Or (Prop. 11, (iii) et prop. 12) $\tau_\alpha(\chi_o)\, \tau_\alpha(\chi_o)^{\sigma_{-1}} = q =$

$\chi_o(-1)\, \tau_\alpha(\chi_o)^2$ et $q^{\frac{\ell-1}{2}} = \chi_o(-1)^{\frac{\ell-1}{2}}\, \tau_\alpha(\chi_o)^{\ell-1}$. Montrons alors que

$\chi_o(-1)^{\frac{\ell-1}{2}} = \chi_o(\ell)$: on a $\chi_o = \varphi^{\frac{q-1}{2}} = \varphi^{\frac{p-1}{2}(1+p+\ldots+p^{n-1})}$,

soit $\chi_o(-1) = (-1)^{\frac{p-1}{2}n}$; or $\chi_o(\ell) \equiv \ell^{\frac{p-1}{2}n}$ mod p. On a donc

$\chi_o(\ell) = \left(\frac{\ell^n}{p}\right) = \left(\frac{\ell}{p}\right)^n$ (symbole de LEGENDRE) ; or par réciprocité quadra-

tique on a $\left(\frac{\ell}{p}\right) = \left(\frac{p}{\ell}\right)(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}$ soit $\left(\frac{\ell}{p}\right)^n = \left(\frac{p}{\ell}\right)^n (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}n} =$

$\left(\frac{p^n}{\ell}\right)(-1)^{\frac{p-1}{2}\frac{\ell-1}{2}n}$; mais $p^n \equiv 1$ mod ℓ, d'où

$\chi_o(\ell) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}n} = \chi_o(-1)^{\frac{\ell-1}{2}}$.

Donc $q^{\frac{\ell-1}{2}} = \chi_o(\ell)\, \tau_\alpha(\chi_o)^{\ell-1} = \chi_o^{\ell}(\ell)\, \tau_\alpha(\chi_o)^{\ell-1}$.

On a donc $\nu'\left(\tau_\alpha(\varphi^\alpha)\right) = \chi_o^{\ell}(\ell)\, \tau_\alpha(\chi_o)^{\ell-1}\, \tau_{\alpha\ell}(\varphi^{\alpha\ell})$, d'où (i).

Cas où $\ell^2 \nmid m$. On a alors (que m, m/ℓ soient ou non des conducteurs) :

$$\mathrm{Gal}\left(\mathbb{Q}'^{(m)}/\mathbb{Q}'^{(m/\ell)}\right) = \left\{\sigma_{1+\mu\frac{m}{\ell}p},\ 0 \leq \mu \leq \ell-1,\ 1+\mu\frac{m}{\ell}p \not\equiv 0\ (\ell)\right\}.$$

Soit μ^* la valeur (unique) de μ telle que $1 + \mu^* \frac{m}{\ell} p \equiv 0$ mod ℓ

(on pose $1 + \mu^* \frac{m}{\ell} p = \gamma \ell$).

On a $\nu' \tau_\alpha(\varphi^\alpha) = \dfrac{\prod_{\mu=0}^{\ell-1} \tau_\alpha\left(\varphi^{\alpha(1+\mu\frac{m}{\ell}p)}\right)}{\tau_\alpha\left(\varphi^{\alpha\gamma\ell}\right)} = \dfrac{\prod_{\mu=0}^{\ell-1} \tau_\alpha\left(\varphi^\alpha \psi^\mu\right)}{\tau_\alpha\left(\varphi^{\alpha\gamma\ell}\right)} =$

$\chi_o^\ell(\ell)\, \tau_\alpha(\chi_o)^{\ell-1} \dfrac{\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)}{\tau_\alpha\left(\varphi^{\alpha\ell\gamma}\right)}$ (en utilisant une partie du calcul relatif au

cas (i)) $= \chi_o^\ell(\ell)\, \tau_\alpha(\chi_o)^{\ell-1} \dfrac{\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)}{\tau_\alpha\left(\varphi^\alpha \psi^{\mu^* p}\right)}$, où $\psi = \varphi^{\frac{q-1}{\ell}}$.

Introduisons le symbole d'ARTIN $s_\ell = \left(\dfrac{\mathbb{Q}'^{(\frac{m}{\ell})}}{\ell}\right)$ qui a un sens puisque $\ell \nmid \frac{m}{\ell}p$. On a $\gamma\ell \equiv 1 \mod \frac{m}{\ell}p$; par conséquent

$$s_\ell = \left(\frac{\mathbb{Q}'^{(\frac{m}{\ell})}}{\ell}\right) = \left(\frac{\mathbb{Q}'^{(\frac{m}{\ell})}}{\gamma}\right)^{-1} \in \mathrm{Gal}\left(\mathbb{Q}'^{(\frac{m}{\ell})}/\mathbb{Q}\right).$$

Etudions alors $\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)^{1-s_\ell^{-1}}$; on a (puisque $s_\ell^{-1} = s_\gamma$)

$\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)^{s_\ell^{-1}} = \varphi^{-\alpha\ell\gamma}(\gamma)\, \tau_{\alpha\ell}\left(\varphi^{\alpha\ell\gamma}\right)$ (d'après la prop. 12, compte tenu du fait que l'on a γ premier à l'ordre de $\varphi^{\alpha\ell}$).

Comme $\varphi^{\alpha\ell} = \varphi^{\frac{q-1}{m}\ell}$ est d'ordre $\frac{m}{\ell}$, $\varphi^{\alpha\ell\gamma} = \varphi^{\alpha(1+\mu^*\frac{m}{\ell}p)} = \varphi^\alpha \psi^{\mu^* p}$.

D'où $\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)^{s_\ell^{-1}} = \varphi^{-\alpha}(\gamma)\, \psi^{-\mu^* p}(\gamma)\, \tau_{\alpha\ell}\left(\varphi^\alpha \psi^{\mu^* p}\right) = \tau_{\alpha\ell\gamma}\left(\varphi^\alpha \psi^{\mu^* p}\right) =$

$\tau_\alpha\left(\varphi^\alpha \psi^{\mu^* p}\right)$ car $\alpha\ell\gamma \equiv \alpha \mod p$, et $\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)^{1-s_\ell^{-1}} = \dfrac{\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)}{\tau_\alpha\left(\varphi^\alpha \psi^{\mu^* p}\right)}$;

d'où $\nu' \tau_\alpha(\varphi^\alpha) = \chi_o^\ell(\ell)\, \tau_\alpha(\chi_o)^{\ell-1}\, \tau_{\alpha\ell}(\varphi^{\alpha\ell})^{1-s_\ell^{-1}}$, ce qui achève la démonstration.

<u>Remarque</u> III 1. Lorsque $\ell^2 | m$, on peut convenir du fait que

$\left(\frac{\mathbb{Q}'^{(\frac{m}{\ell})}}{\ell}\right)^{-1} = 0$ (y compris dans le cas m = 4d, d impair et $\ell = 2$ où, pourtant, le symbole d'ARTIN est défini). Examinons le cas particulier $\ell = 2$, m = 4d, d impair afin d'éviter l'ambiguïté ci-dessus dans les formules (ce cas correspond au seul cas où m et m/2 ne sont pas simultanément des conducteurs) :

$$\text{On a } \nu'_{\mathbb{Q}(4d)/\mathbb{Q}(d)}\, \tau_{\frac{q-1}{4d}}\left(\varphi^{\frac{q-1}{4d}}\right) = \nu'_{\mathbb{Q}(2d)/\mathbb{Q}(d)}\, \nu'_{\mathbb{Q}(4d)/\mathbb{Q}(2d)}\, \tau_{\frac{q-1}{4d}}\left(\varphi^{\frac{q-1}{4d}}\right) =$$

$$\nu'_{\mathbb{Q}(2d)/\mathbb{Q}(d)}\left(\tau_{\frac{q-1}{4d}}(\chi_o)\; \tau_{\frac{q-1}{2d}}(\varphi^{\frac{q-1}{2d}})\right) \quad \left(\text{d'après (i)}\right)$$

$$= \tau_{\frac{q-1}{4d}}(\chi_o)\; \tau_{\frac{q-1}{2d}}(\chi_o)\left(\tau_{\frac{q-1}{d}}(\varphi^{\frac{q-1}{d}})\right)^{1-\left(\frac{\mathbb{Q}'(d)}{2}\right)^{-1}} \quad \left(\text{d'après (ii)}\right) \text{ ; or}$$

$$\tau_{\frac{q-1}{2d}}(\chi_o) = \chi_o(2)\, \tau_{\frac{q-1}{4d}}(\chi_o) \quad \text{et} \quad \nu'_{\mathbb{Q}(4d)/\mathbb{Q}(d)}\, \tau_{\frac{q-1}{4d}}\left(\varphi^{\frac{q-1}{4d}}\right) =$$

$$\tau_{\frac{q-1}{4d}}(\chi_o)^2\, \chi_o(2)\left(\tau_{\frac{q-1}{d}}(\varphi^{\frac{q-1}{d}})\right)^{1-\left(\frac{\mathbb{Q}'(d)}{2}\right)^{-1}}, \text{ ce qui s'écrit encore}$$

$$\nu'_{\mathbb{Q}(4d)/\mathbb{Q}(d)}\left(\chi_o(2)\, \tau_{\frac{q-1}{4d}}(\varphi^{\frac{q-1}{4d}})\, \tau_{\frac{q-1}{4d}}(\chi_o)^{-1}\right)$$

$$= \left(\chi_o(2)\, \tau_{\frac{q-1}{d}}(\varphi^{\frac{q-1}{d}})\, \tau_{\frac{q-1}{d}}(\chi_o)^{-1}\right)^{1-\left(\frac{\mathbb{Q}'(d)}{2}\right)^{-1}} \quad \text{car on vérifie directement que}$$

$\tau_{\frac{q-1}{d}}(\chi_o)^{s_2^{-1}} = \chi_o(2)\, \tau_{\frac{q-1}{d}}(\chi_o)$ (ce résultat ne découle pas de la proposition I 2 car 2 n'est pas premier à l'ordre de χ_o).

Corollaire III 2. On a dans tous les cas (avec la convention $\left(\frac{\mathbb{Q}'(f)}{\ell}\right) = 0$ si $\ell | f$, f étant un conducteur) et pour tout m qui est un conducteur :

(i) $\nu'_{\mathbb{Q}(m)/\mathbb{Q}(m/\ell)}\left(\chi_o(2)\,\tau_{\frac{q-1}{m}}\left(\varphi^{\frac{q-1}{m}}\right)\,\tau_{\frac{q-1}{m}}(\chi_o)^{-1}\right) =$

$$\left(\chi_o(2)\,\tau_{\frac{q-1}{m/\ell}}\left(\varphi^{\frac{q-1}{m/\ell}}\right)\,\tau_{\frac{q-1}{m/\ell}}(\chi_o)^{-1}\right)^{1-\left(\frac{\mathbb{Q}'(m/\ell)}{\ell}\right)^{-1}}$$, si m/ℓ est un conducteur ;

(ii) $\nu'_{\mathbb{Q}(4d)/\mathbb{Q}(d)}\left(\chi_o(2)\,\tau_{\frac{q-1}{4d}}\left(\varphi^{\frac{q-1}{4d}}\right)\,\tau_{\frac{q-1}{4d}}(\chi_o)^{-1}\right) =$

$$\left(\chi_o(2)\,\tau_{\frac{q-1}{d}}\left(\varphi^{\frac{q-1}{d}}\right)\,\tau_{\frac{q-1}{d}}(\chi_o)^{-1}\right)^{1-\left(\frac{\mathbb{Q}'(d)}{2}\right)^{-1}}$$, si m = 4d, d impair.

Le cas (ii) étant résolu, plaçons-nous dans le cas (i), en posant $\delta = 0$ si $s_\ell = 0$, $\delta = 1$ sinon. On a $\tau_{\frac{q-1}{m/\ell}}(\chi_o)^{1-s_\ell^{-1}} = \tau_{\frac{q-1}{m/\ell}}(\chi_o)^{1-\delta}\,\chi_o(\ell)^{\delta}$

(Dans le cas $\ell \neq 2$, $s_\ell \neq 0$ c'est la prop. I 2 ; dans le cas $\ell = 2$, $s_2 \neq 0$ c'est le calcul direct évoqué à la fin de la Rem. III 1).

On peut donc écrire ;

$$\nu'_{\mathbb{Q}(m)/\mathbb{Q}(m/\ell)}\left(\chi_o(2)\,\tau_{\frac{q-1}{m}}\left(\varphi^{\frac{q-1}{m}}\right)\,\tau_{\frac{q-1}{m}}(\chi_o)^{-1}\right) =$$

$$\chi_o(2)^{\ell-\delta}\,\tau_{\frac{q-1}{m}}(\chi_o)^{\delta-\ell}\,\chi_o(\ell)^{\ell}\,\tau_{\frac{q-1}{m}}(\chi_o)^{\ell-1}\left(\tau_{\frac{q-1}{m/\ell}}\left(\varphi^{\frac{q-1}{m/\ell}}\right)\right)^{1-s_\ell^{-1}} =$$

$$\chi_o(2)^{\ell-\delta}\chi_o^{\ell}(\ell)\,\tau_{\frac{q-1}{m}}(\chi_o)^{\delta-1}\left(\chi_o(2)\,\tau_{\frac{q-1}{m/\ell}}\left(\varphi^{\frac{q-1}{m/\ell}}\right)\tau_{\frac{q-1}{m/\ell}}(\chi_o)^{-1}\right)^{1-s_\ell^{-1}}\chi_o(2)^{\delta-1}$$

$$\chi_o(\ell)^{\delta}\,\tau_{\frac{q-1}{m/\ell}}(\chi_o)^{1-\delta} =$$

$\left(\chi_o(2)\,\chi_o(\ell)\right)^{\ell-1}\left(\chi_o(2)\,\tau_{\frac{q-1}{m/\ell}}\left(\varphi^{\frac{q-1}{m/\ell}}\right)\tau_{\frac{q-1}{m/\ell}}(\chi_o)^{-1}\right)^{1-s_\ell^{-1}}$. Or on a

$\left(\chi_o(2)\,\chi_o(\ell)\right)^{\ell-1} = 1$ quel que soit ℓ ; d'où le corollaire.

Revenons maintenant à l'étude de l'action de la norme sur les $\tau(L)$.

Soient K et L, $K \subset L$, deux extensions abéliennes de $\mathbb{Q}$ de conducteurs m_K et m_L respectivement ; on pose $q_K = p^{n_K}$ et $q_L = p^{n_L}$; on appelle φ_K et φ_L les caractères générateurs correspondant respectivement à $\mathbb{F}_{q_K}$ et $\mathbb{F}_{q_L}$ et on pose $\chi_o^K = \varphi_K^{\frac{q_K-1}{2}}$ et $\chi_o^L = \varphi_L^{\frac{q_L-1}{2}}$.

Lemme III 7. On a $\nu'_{L/K}\left(\tau(L)\right)^{n_L/\lambda_L} = \tau(K)^{n_L/\lambda_K}\, W'_{L/K}$ où

$$W'_{L/K} = \prod_{\substack{\ell \mid m_L \\ \ell \nmid m_K}} \left(1 - \left(\frac{\overline{K}'}{\ell}\right)^{-1}\right).$$

On avait établi la relation $\nu'_{L/K}\,\tau(L)^{n_L/\lambda_L} =$

$\nu'_{\overline{\mathbb{Q}^{(m_K)}}/\overline{K}}\ \nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau\left(\mathbb{Q}^{(m_L)}\right)\right)^{n_K/\lambda_K}$. On utilise le corollaire III 2 ; on écrit : $m_L = 2^A p_1^{a_1} \dots p_s^{a_s}\, \ell_1^{b_1} \dots \ell_t^{b_t}$,

$$m_K = 2^a p_1^{c_1} \dots p_s^{c_s}\ ,\ s,t \geq 0\ ,\ \text{avec } a_i \geq c_i \geq 1\ ,\ b_j \geq 1,$$

$p_j \neq p_i$ nombres premiers impairs, pour $i = 1,\dots, s$, $j = 1,\dots, t$; enfin $A \geq a \geq 0$, $A \neq 1$, $a \neq 1$.

Soit $m' = 2^A p_1^{c_1} \dots p_s^{c_s}\, \ell_1 \dots \ell_t$ (m' est un conducteur) ;

alors le corollaire III 2, (i), conduit à :

$$\nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m')}}\left(\tau\left(\mathbb{Q}^{(m_L)}\right)\right) = \chi_o^L(2)\,\tau_{\frac{q_L-1}{m'}}\left(\varphi_L^{\frac{q_L-1}{m'}}\right)\tau_{\frac{q_L-1}{m'}}(\chi_o^L)^{-1}\,.$$

a) Iterration sur la puissance de 2 (si $A > 0$). Posons

$m'' = 2^a p_1^{c_1} \ldots p_s^{c_s}\, \ell_1 \ldots \ell_t$. ($m''$ est un conducteur) et distinguons deux cas :

(i) $A>a>0$, alors on obtient (corol. III 2, (i)) :

$$\nu'_{\mathbb{Q}^{(m')}/\mathbb{Q}^{(m'')}}\left(\chi_o^L(2)\,\tau_{\frac{q_L-1}{m'}}\left(\varphi_L^{\frac{q_L-1}{m'}}\right)\tau_{\frac{q_L-1}{m'}}\left(\chi_o^L\right)^{-1}\right) =$$

$$\chi_o^L(2)\,\tau_{\frac{q_L-1}{m''}}\left(\varphi_L^{\frac{q_L-1}{m''}}\right)\tau_{\frac{q_L-1}{m''}}(\chi_o^L)^{-1}\,.$$

(ii) $A>0$, $a = 0$, alors on applique le cas (i) ci-dessus jusqu'à avoir atteint le nombre $4p_1^{c_1} \ldots p_s^{c_s}\, \ell_1 \ldots \ell_t$ puis on applique le cas (ii) du corollaire III 2 : on obtient donc :

$$\nu'_{\mathbb{Q}^{(m')}/\mathbb{Q}^{(m'')}}\left(\chi_o^L(2)\,\tau_{\frac{q_L-1}{m'}}\left(\varphi_L^{\frac{q_L-1}{m'}}\right)\tau_{\frac{q_L-1}{m'}}(\chi_o^L)^{-1}\right) =$$

$$\left(\chi_o^L(2)\,\tau_{\frac{q_L-1}{m''}}\left(\varphi_L^{\frac{q_L-1}{m''}}\right)\tau_{\frac{q_L-1}{m''}}(\chi_o^L)^{-1}\right)^{1-\left(\frac{\mathbb{Q}'(m'')}{2}\right)^{-1}}\,.$$

b) Iterration sur les ℓ_j (si $t \geq 1$). On applique le corollaire III 2, (i) qui donne :

$$\nu'_{\mathbb{Q}^{(m'')}/\mathbb{Q}^{(m_K)}}\left(\chi_o^L(2)\,\tau_{\frac{q_L-1}{m''}}\left(\varphi_L^{\frac{q_L-1}{m''}}\right)\tau_{\frac{q_L-1}{m''}}(\chi_o^L)^{-1}\right) =$$

$$\left(\chi_o^L(2)\,\tau_{\frac{q_L-1}{m_K}}\left(\varphi_L^{\frac{q_L-1}{m_K}}\right)\tau_{\frac{q_L-1}{m_K}}(\chi_o^L)^{-1}\right)^{\prod_{j=1}^{t}\left(1-\left(\frac{\mathbb{Q}'^{(m_K)}}{\ell_j}\right)^{-1}\right)}$$ en tenant

compte des restrictions successives des symboles d'ARTIN

$\left(\frac{\mathbb{Q}'^{\left(\frac{m''}{\ell_1\cdots\ell_u}\right)}}{\ell_u}\right)^{-1}$, $u = 1,\ldots,t$, qui, par hypothèse, ne sont jamais nuls.

D'où : en tenant compte éventuellement du cas $A > 0$, $a = 0$, on obtient :

$$\nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau\left(\mathbb{Q}^{(m_L)}\right)\right) = \left(\chi_o^L(2)\,\tau_{\frac{q_L-1}{m_K}}\left(\varphi_L^{\frac{q_L-1}{m_K}}\right)\tau_{\frac{q_L-1}{m_K}}(\chi_o^L)^{-1}\right)^{W''_{L/K}}$$

avec $W''_{L/K} = \prod_{\substack{\ell \mid m_L \\ \ell \nmid m_K}}\left(1-\left(\frac{\mathbb{Q}'^{(m_K)}}{\ell}\right)^{-1}\right)$.

On a donc $q_L-1 = \Lambda_{L/K}(q_K-1)$ et d'après la proposition III, on a

pour $(a,p) = 1$: $\tau_a\left(\varphi_L^{\frac{q_L-1}{m_K}}\right) = \tau_a\left(\varphi_K^{\frac{q_K-1}{m_K}}\right)^{n_L/n_K}$ et $\tau_a\left(\varphi_L^{\frac{q_L-1}{2}}\right) =$

$\tau_a\left(\varphi_K^{\frac{q_K-1}{2}}\right)^{n_L/n_K}$. De plus, on a par définition

$$\tau\left(\mathbb{Q}^{(m_K)}\right) = \chi_o^K(2)\,\tau_{\frac{q_K-1}{m_K}}\left(\varphi_K^{\frac{q_K-1}{m_K}}\right)\tau_{\frac{q_K-1}{m_K}}\left(\varphi_K^{\frac{q_K-1}{2}}\right)^{-1}.$$

On a, puisque χ_o^L et $\left(\chi_o^K\right)^{n_L/n_K}$ coïncident sur $\mathbb{F}_p$ notamment,

$$\nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau\left(\mathbb{Q}^{(m_L)}\right)\right) = \left(\chi_o^K(2)\,\tau_{\frac{q_L-1}{m_K}}\left(\varphi_K^{\frac{q_K-1}{m_K}}\right)\tau_{\frac{q_L-1}{m_K}}\left(\varphi_K^{\frac{q_K-1}{2}}\right)^{-1}\right)^{n_L/n_K W'_{L/K}};$$

mais $\frac{q_L - 1}{m_K} = \frac{q_K - 1}{m_K} \Lambda_{L/K}$ avec $\Lambda_{L/K} \equiv 1 \bmod p$, donc l'indice $\frac{q_L - 1}{m_K}$ peut être remplacé par $\frac{q_K - 1}{m_K}$ dans l'expression précédente. On a donc obtenu :

$$\nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau(\mathbb{Q}^{(m_L)})\right) = \tau\left(\mathbb{Q}^{(m_K)}\right)^{n_L/n_K W''_{L/K}} \text{, d'où}$$

$$\nu'_{L/K}\left(\tau(L)\right)^{n_L/\lambda_L} = \nu'_{\overline{L}/\overline{K}}\, \tau(L)^{(n_L/\lambda_L)(\lambda_L/\lambda_K)} = \tau(K)^{n_L/\lambda_K W''_{L/K}}$$

soit, par restriction de $W''_{L/K}$, $\nu'_{\overline{L}/\overline{K}}\, \tau(L)^{n_L/\lambda_K} = \tau(K)^{n_L/\lambda_K W'_{L/K}}$.

On obtient alors $\nu'_{\overline{L}/\overline{K}}\, \tau(L) = \xi_{L/K}\, \tau(K)^{W'_{L/K}}$, où $\xi_{L/K}$ est une racine de l'unité telle que $\xi_{L/K}^{n_L/\lambda_K} = 1$. On remarque que $\xi_{L/K} \in \overline{K}'$ (car $\nu'_{\overline{L}/\overline{K}}\, \tau(L) \in \overline{K}'$ et $\tau(K) \in \overline{K}'$) ; de plus $\xi_{L/K} \in \mathcal{S}$ et d'après le corollaire II 2, on a $\xi_{L/K}^{p-1} = 1$ et ceci montre que $\xi_{L/K} \in \overline{K}$. On a donc démontré :

<u>Théorème</u> III 2. Soient L et K deux corps abéliens avec $K \subset L$; soient m_L (resp. m_K) le conducteur de L (resp. K), n_L (resp. n_K) le degré résiduel de p dans $\mathbb{Q}^{(m_L)}$ (resp. $\mathbb{Q}^{(m_K)}$), λ_L (resp. λ_K) le degré résiduel de p dans L (resp. K) et soit $W'_{L/K} = \prod_{\substack{\ell \mid m_L \\ \ell \nmid m_K}} \left(1 - \left(\frac{\overline{K}'}{\ell}\right)^{-1}\right)$. Alors il existe une racine de l'unité $\xi_{L/K}$ appartenant à $\overline{K}$ telle que $\xi_{L/K}^{n_L/\lambda_K} = 1$ et $\xi_{L/K}^{p-1} = 1$, vérifiant :

$$\nu'_{\overline{L}/\overline{K}}\left(\tau(L)\right) = \xi_{L/K}\, \tau(K)^{W'_{L/K}} .$$

3) <u>Un exemple numérique.</u> Montrons sur un exemple que la racine de l'unité $\xi_{L/K}$ n'est pas triviale en général. Prenons $p = 7$, pour L le corps $\mathbb{Q}^{(3.19)} = \mathbb{Q}^{(57)}$ et pour K le sous-corps $\mathbb{Q}^{(3)}$. On a le schéma suivant :

$$\begin{tikzcd}
\overline{K} = K = \mathbb{Q}^{(3)} \arrow[r, dash, "6"] \arrow[d, dash, "2"'] & \overline{L} \arrow[r, dash, "3"] & L = \mathbb{Q}^{(57)} \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}^{(342)} \\
\mathbb{Q} \arrow[rr, dash] & & \mathbb{Q}^{(19)} &
\end{tikzcd}$$

On a $m_L = 57$, $m_K = 3$, $\lambda_L = n_L = 3$; le corps $\overline{L}$ est donc l'unique sous-corps tel que $[L : \overline{L}] = 3$; on a enfin $\lambda_K = n_K = 1$ et $\overline{K} = K$.

On remarque que 19 est totalement décomposé dans K donc on a $\left(\frac{\mathbb{Q}^{(3)}}{19}\right) = 1$. On a $W'_{L/K} = \left(1 - \left(\frac{\mathbb{Q}^{(21)}}{19}\right)^{-1}\right)$; on vérifie que

$$\tau_{\frac{q_K - 1}{3}}\left(\varphi_K^{\frac{q_K-1}{3}}\right) \in K = \mathbb{Q}^{(3)}$$ (cf. corol. 11) ; on a donc

$$\left(\tau_{\frac{q_K-1}{3}}(K)\right)^{W'_{L/K}} = \left(\tau_{\frac{q_K-1}{3}}(K)\right)^{\left(1 - \left(\frac{\mathbb{Q}^{(3)}}{19}\right)^{-1}\right)} = 1 \text{ ; on a}$$

$$\tau(K)^{W'_{L/K}} = \tau_{\frac{q_K-1}{3}}\left(\chi_o^K\right)^{-W'_{L/K}} = \chi_o^K(19) = \left(\frac{19}{7}\right) = -1.$$ On a donc

$\nu'_{\overline{L}/\overline{K}}\ \tau(L) = -\ \xi_{L/K}$ ici.

Nous allons déterminer $\xi_{L/K}$ en calculant $\nu'_{\overline{L}/\overline{K}}\left(\tau(L)\right)$ directement et en identifiant $\xi_{L/K}$ (qui est d'ordre diviseur de $p-1$) par une congruence modulo $\mathfrak{P}'$. Soit φ le générateur habituel de $\mathfrak{X}$ d'ordre