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], §1 ; [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 $\alpha \in \mathbb{Z}$.

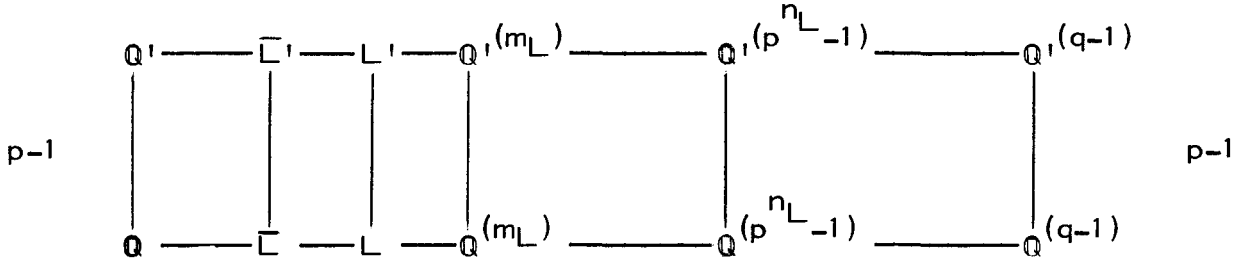
On choisit une fois pour toutes une racine primitive p^e de l'unité ζ $\left(\text{par exemple } \zeta = \exp(2i\pi/p)\right)$.

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) Définitions et notations générales. 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 :



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 $\lambda_L \mid n_L \mid n$).

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 :

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

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

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

c) Interprétation arithmétique de la première définition.

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^*.

Définition 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 $\overline{u}$ l'image de $u \in A'$ dans k,

$\varphi(\bar{u}) \equiv u^{-1} \bmod \mathfrak{P}'$ pour tout u, $u \notin \mathfrak{P}'$, et $\varphi(\bar{\xi}) = \xi^{-1}$ 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 $\left((a,p) = 1,\ \psi \in \mathfrak{X}\right)$:

(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 :

$$\tau_a(1) = 1 - \sum_{x \in U} (\zeta^0 + \zeta^a + \ldots + \zeta^{(p-1)a}) = 1.$$

(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 $\sigma_b \in H$ (i. e. $b \equiv 1 \bmod (q-1)$) 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, $\tau_a(\psi)^{\sigma_b} = -\sum_{x \in k^*} \psi(x)^b \zeta^{abT(x)} = \tau_{ab}(\psi^b) = \psi^{-b}(b)\,\tau_a(\psi^b)$ (Prop. 11, (i)).

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 11. Soit $\psi \in \mathfrak{X}$, ψ d'ordre $m \mid q-1$, soit a, $(a,p) = 1$ et soit $d = \frac{m}{(m, \frac{q-1}{p-1})}$. 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 $m = \Delta d$ $\left((\delta, d) = 1,\ \Delta = (m, \frac{q-1}{p-1})\right)$; 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 12. 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 $\frac{\tau(\chi)\,\tau(\psi)}{\tau(\chi\psi)} = -\sum_{t \in k} \chi(t)\, \psi(1-t)$.

démonstration.

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 $\dfrac{\tau(\chi)\,\tau(\psi)}{\tau(\chi\psi)}$, 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 $\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$, $0 \leq \alpha_i \leq p-1$, l'écriture en base p de α (les α_i sont donc non tous égaux à p-1).

Définition II 1. On pose $s(\alpha) = \alpha_0 + \alpha_1 + \ldots + \alpha_{n-1}$ (somme des chiffres) et $\gamma(\alpha) = \alpha_0!\ \alpha_1! \ldots \alpha_{n-1}!$ (produit des factorielles des chiffres).

On a le résultat suivant ([16] ; cf. [2], [4], [11]) 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. 11, (v)). Or on a $\tau(\varphi) = -\sum_{x \in k} \varphi(x)\, \zeta^{T(x)} = -\sum_{x \in k} \varphi(x) \left(\zeta^{T(x)} - 1\right)$ car $\sum_{x \in k} \varphi(x) = 0$ ($\varphi = 1$ supposé $q = 2$ soit $\alpha = 0$ qui est écarté). On sait que $\frac{\zeta^{T(x)} - 1}{\zeta - 1} \equiv T(x) \bmod \pi$,

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 $\frac{\tau(\varphi)}{\pi} \equiv -\sum_{\omega \in W_{q-1}} \left(1 + \omega^{p-1} + \ldots + \omega^{p^{n-1}-1}\right) \equiv -(q-1) \equiv 1 \bmod \mathfrak{P}'$. 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. I 1) ; 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 $\nu(\alpha') = \nu(\alpha)$). 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

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

On a $\varphi^{\alpha} = \varphi^{\beta}\, \varphi$ et en utilisant la proposition I 3 on peut écrire $\frac{\tau(\varphi^{\beta})\, \tau(\varphi)}{\tau(\varphi^{\alpha})} = -\sum_{t \in k} \varphi(t)\, \varphi^{\beta}(1-t)$.

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

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

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

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

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

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 $\rho \equiv C_{\gamma}^{1} (q-1) \bmod \mathfrak{P}'$, $\rho \equiv -\gamma \bmod \mathfrak{P}'$ 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 III ("congruences de Stickelberger").

On en déduit une factorisation des sommes de GAUSS :

Corollaire III. 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 $\tau_a(\psi)$, $a \bmod p$, $\psi \in \mathfrak{X}$:

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

On a $\tilde{q}-1 = \Lambda(q-1)$ 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 $0 \le \alpha < q-1$.

Soit $\alpha = \alpha_0 + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$, $\alpha < q-1$, $0 \le \alpha_i \le p-1$; 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 $\tilde{\mathfrak{P}}'$-unité ; or $\dfrac{\tilde{q}-1}{m}b = \Lambda\,\dfrac{q-1}{m}b$ et d'après le lemme précédent $\tilde{s}\left(\dfrac{\tilde{q}-1}{m}b\right) = \lambda\, s\left(\dfrac{q-1}{m}b\right)$ (puisque b est choisi inférieur à m, on a bien $0 \le \dfrac{q-1}{m}b < q-1$). Comme b est quelconque, on en déduit en conjuguant

que, en idéaux dans $A'_{\mathbb{Q}}(m)$, on a $\tilde{\tau}_a\left(\tilde{\varphi}^{\frac{\tilde{q-1}}{m}b}\right)A'_{\mathbb{Q}}(m) = \left(\tau_a(\varphi^{\frac{q-1}{m}b})A'_{\mathbb{Q}}(m)\right)^{\lambda}$.

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

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

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

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

et de même $\dfrac{\tilde{\tau}\left(\tilde{\varphi}^{\frac{\tilde{q-1}}{m}b}\right)}{\pi^{\lambda s\left(\frac{q-1}{m}b\right)}} \equiv \dfrac{1}{\tilde{\gamma}\left(\Lambda\frac{q-1}{m}b\right)} \bmod \tilde{\mathfrak{P}}'$. 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,

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

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) Relations de STICKELBERGER. D'après le corollaire III 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 : $\tau\left(\varphi^{\frac{q-1}{m}}\right)^n A'_{\mathbb{Q}^{(m)}} = \prod_{\sigma_b \in G'_{\mathbb{Q}^{(m)}}} \mathfrak{P}'^{\lambda s\left(\left[\frac{q-1}{m} b\right]_{q-1}\right)}_{\mathbb{Q}^{(m)}} \sigma_b^{-1}$, 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 $\frac{q-1}{m} b = \alpha_o + \alpha_1 p + \ldots + \alpha_{n-1} p^{n-1}$,
alors $\frac{q-1}{m} cp^r = \alpha_o p^r + \alpha_1 p^{r+1} + \ldots + \alpha_{n-1-r} p^{n-1} + \alpha_{n-r} p^n + \ldots + \alpha_{n-1} p^{n-1+r} \equiv$

$\alpha_{n-r} + \alpha_{n-r+1} p + \ldots + \alpha_{n-1} p^{r-1} + \alpha_o p^r + \ldots + \alpha_{n-1-r} p^{n-1} \bmod q-1$.

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 $\mathbb{Q}^{(m)}/\mathbb{Q}$:

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

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

Résumons ce résultat partiel dans un lemme :

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

Proposition 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 $\mathbb{Q}^{(q-1)}/\mathbb{Q}^{(m)}$.

démonstration

Démontrons d'abord le lemme suivant :

Lemme 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 $\alpha = \alpha \dfrac{(p-1)(1+p+\ldots+p^{n-1})}{q-1}$

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 dé-

but du paragraphe : $\tau(\varphi^\alpha)^n A'_{\mathbb{Q}}(m) = \mathfrak{P}'^{\lambda \sum_b s(\alpha b)\sigma_b^{-1}}_{\mathbb{Q}}(m)$, $1 \leq b \leq m$, $(m, b) = 1$.

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

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

sition puisque $\tau(\varphi^\alpha) \in \mathbb{Q}^{(m)}$.

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

Définition 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 $S_K = \frac{1}{m} \sum_{a=1}^{m}{}^{*} a\left(\frac{K}{a}\right)^{-1} \in \mathbb{Q}[G_K]$.

Remarque 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 $\tau\left(\varphi^{\frac{q-1}{2d}b}\right)$) 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 :

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

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 $\overline{K}$: $\mathfrak{P}_{\overline{K}}^{S_K\omega} = \nu_{\overline{\mathbb{Q}^{(m)}}/\overline{K}}\,\tau\left(\varphi^{\frac{q-1}{m}}\right)^{\omega'} A_{\overline{K}}$.

On sait que (Corol. II 3) $\tau\left(\varphi^{\frac{q-1}{m}}\right)^m A_{\overline{\mathbb{Q}^{(m)}}} = \mathfrak{P}_{\overline{\mathbb{Q}^{(m)}}}^{mS_{\mathbb{Q}(m)}}$, 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 $\left(\nu_{\overline{\mathbb{Q}^{(m)}}/\overline{K}}\,\tau(\varphi^{\frac{q-1}{m}})^{m\varpi}\right)A_{\overline{K}} = \mathfrak{P}_{\overline{K}}^{m\overline{\Omega}}$, puisque $\tau\left(\varphi^{\frac{q-1}{m}}\right)^m \in \overline{\mathbb{Q}^{(m)}}$, en notant ϖ 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 :

Théorème 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) Résultat général. 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 $\mathbb{F}_q^*$) :

Théorème 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, $(a, p) = 1$.

démonstration

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.

Lemme 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

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

$$\rho(m,\chi)^{\sigma_b} = \frac{\prod_{\lambda=0}^{m-1} \tau\left(\psi^{\lambda}\chi^{b}\right)}{\tau_m\left(\chi^{mb}\right)\prod_{\lambda=0}^{m-1}\tau(\psi^{\lambda})} = \rho(m,\chi^{b}),$$ 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 $\left.\tau_m(\chi^m)\right)$ valent 1 $\big)$ et dans ce cas $\rho(m,\chi)\,\rho(m,\chi)^{\sigma_{-1}} = \frac{q^{m-1}}{q^{m-1}} = 1$. Sinon on voit qu'aucun caractère (hormis ψ^{μ} pour $\mu = 0$) n'est égal à 1 et $\rho(m,\chi)\,\rho(m,\chi)^{\sigma_{-1}} = \frac{q^m}{q\,q^{m-1}} = 1$.

Lemme III 2. Les relations de DAVENPORT-HASSE sont vérifiées (i. e. $\rho(m,\chi) = 1$, pour tout $m \mid q-1$ 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 $\ell \mid q-1$.

Etant donné $\rho(m,\chi)$, $\chi \in \mathfrak{X}$, $m \mid q-1$, 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 :

$[1, \alpha_o]$, $[\alpha_o+1,\ \alpha_o+\alpha_1 p], \ldots,$ $[\alpha_o+\ldots+\alpha_{k-1} p^{k-1}+1,\ \alpha_o+\ldots+\alpha_k p^k], \ldots,$ $[\alpha_o+\ldots+\alpha_{n-2} p^{n-2}+1,\ \alpha_o+\ldots+\alpha_{n-1} p^{n-1}]$; 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, $2p^k, \ldots, \Lambda_k p^k$ (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 :

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

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

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

Corollaire 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 $\frac{\tau(\varphi^\alpha)}{\pi^{s(\alpha)}} \equiv \frac{1}{\gamma(\alpha)}$ mod $\mathfrak{P}'$ soit

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

$\frac{(-1)^{p-1}\, p}{\pi^{p-1}} \equiv (p-1)! \equiv -1$ mod π soit $\frac{-p}{\pi^{p-1}} \equiv 1$ mod π et

$\pi^{s(\alpha)}\, (-p)^{\frac{\alpha-s(\alpha)}{p-1}} \equiv \pi^{s(\alpha)+\alpha-s(\alpha)} = \pi^\alpha$ mod $\pi^{\alpha+1}$; 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 $\rho(\ell, \chi) \equiv 1$ mod $\mathfrak{P}$; 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 $\chi = \varphi^{\frac{q-1}{m}b}$, $(b,m)=1$, $1 \le b < m$.

On transforme cette expression : si $\ell \nmid m$, on pose $b\ell = \lambda m + r$ $0 \le r < m$ 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 $\ell \mid m$, $m = \ell m'$ et on pose $b = \lambda' m' + r'$, $0 \le r' < m'$ 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,

$\rho(\ell,\chi) = \dfrac{1}{\tau_\ell\left(\varphi^{\frac{q-1}{m}r}\right)}\prod_{\mu=0}^{\ell-1}\dfrac{\tau\left(\varphi^{\frac{q-1}{\ell}\mu+\frac{q-1}{m\ell}r}\right)}{\tau\left(\varphi^{\frac{q-1}{\ell}\mu}\right)}$ (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 $0 \le x < \frac{q-1}{\ell}$, x entier ; on remar-

que 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 :

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

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

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 :

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

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

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 $x \in k$, $\psi(x) \equiv 1 \bmod \varpi$; de plus ϖ est premier à p donc on peut écrire

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

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

$$\text{or } \tau(x)^\ell \equiv \Big(-\sum_{x \in k} \chi(x)\, \zeta^{T(x)}\Big)^\ell \equiv -\sum_{x \in k} \chi^\ell(x)\, \zeta^{\ell T(x)} \equiv \tau_\ell(\chi^\ell) \bmod \varpi .$$

Ainsi $\rho(\ell,\chi) \equiv 1 \bmod \varpi$ 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) Définition et propriétés de $\tau(L)$. On suppose maintenant $p \neq 2$.

a) Définition de $\tau\big(\mathbb{Q}^{(m)}\big)$. Soit m premier à p un conducteur de corps cyclotomique (i. e. si m est pair, alors $m \equiv 0 \bmod 4$) 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. II 1) $\tau(\chi_o) = \tau\Big(\varphi_1^{\frac{p-1}{2}}\Big)^n$, φ_1 étant le générateur de $\mathfrak{X}_1$ correspondant à $\mathbb{F}_p^*$.

Définition II 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 :

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

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 $\tau\left(\mathbb{Q}^{(m)}\right)$ est, à une racine de l'unité près, le "ARTIN root number" relatif au caractère abélien $\varphi^{\frac{q-1}{m}}$.

On constate que $\tau\left(\mathbb{Q}^{(m)}\right)$ est un élément de $\mathbb{Q}'^{(m)}$ qui se trouve en fait dans $\overline{\mathbb{Q}'^{(m)}}$ (corol. 12).

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

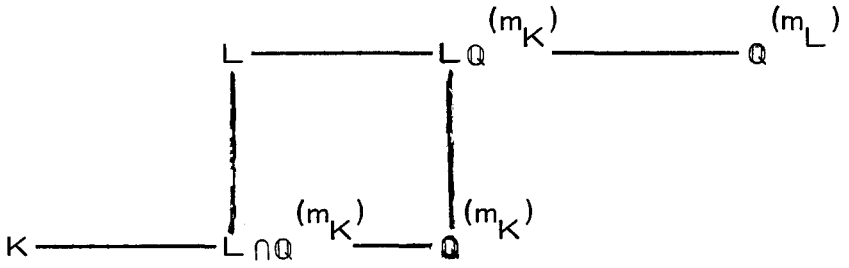
Définition III 2. On pose $\tau(L) = \nu'_{\mathbb{Q}^{(m_L)}/\overline{L}}\left(\tau(\mathbb{Q}^{(m_L)})\right)$.

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 13.

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 :



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

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

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

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

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

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

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

Lemme 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) :

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

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 $\chi_o(\ell) \equiv \ell^{\frac{p-1}{2}n} \bmod p$. 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 $p^n \equiv 1 \bmod \ell$, 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) :

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

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

(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 $\gamma\ell \equiv 1 \bmod \frac{m}{\ell}p$; 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 $\alpha\ell\gamma \equiv \alpha \bmod p$, 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 $\nu' \tau_\alpha(\varphi^\alpha) = \chi_o^\ell(\ell)\,\tau_\alpha(\chi_o)^{\ell-1}\,\tau_{\alpha\ell}\left(\varphi^{\alpha\ell}\right)^{1-s_\ell^{-1}}$, ce qui achève la démonstration.

Remarque 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) :

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

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

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

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

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

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

$= \left(\chi_o(2)\, \tau_{\frac{q-1}{d}}\left(\varphi^{\frac{q-1}{d}}\right) \tau_{\frac{q-1}{d}}(\chi_o)^{-1}\right)^{1-\left(\frac{\mathbb{Q}'(d)}{2}\right)^{-1}}$ 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 $\ell \mid f$, 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 $\nu'_{L/K}\,\tau(L)^{n_L/\lambda_L} = \nu'_{\mathbb{Q}^{(m_K)}/\overline{K}}\,\nu'_{\mathbb{Q}^{(m_L)}/\mathbb{Q}^{(m_K)}}\left(\tau\left(\mathbb{Q}^{(m_L)}\right)\right)^{n_K/\lambda_K}$. On utilise le corollaire III 2 ; on écrit : $m_L = 2^A p_1^{a_1} \dots p_s^{a_s} \ell_1^{b_1} \dots \ell_t^{b_t}$,

$m_K = 2^a p_1^{c_1} \dots p_s^{c_s}$, $s, t \geq 0$, 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 :

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

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)) :

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

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

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

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

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

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

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

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

compte des restrictions successives des symboles d'ARTIN

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

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

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

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

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

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

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

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

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 :

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

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

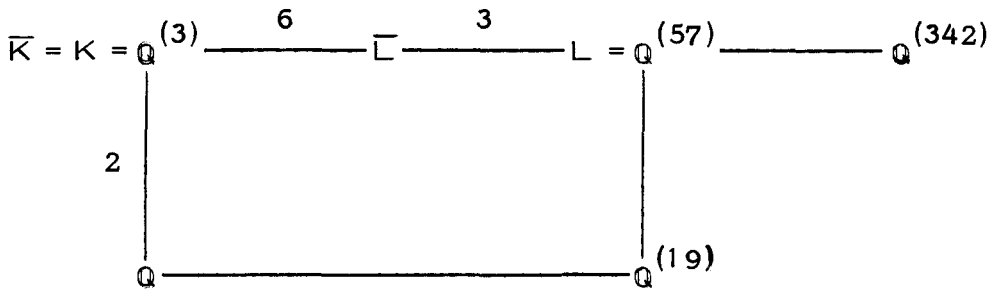
soit, par restriction de $W''_{L/K}$, $\nu'_{\overline{L}/\overline{K}}\tau(L)^{n_L/\lambda_K} = \tau(K)^{n_L/\lambda_K W'_{L/K}}$.

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) Un exemple numérique. 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 :



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

$342 = 6 \times 3 \times 19$. On a $\tau(L) = \tau\left(\mathbb{Q}^{(57)}\right) = \chi_o(2)\ \tau_6\left(\varphi^6\right)\ \tau_6\left(\varphi^{3.57}\right)^{-1}$.

On constate que $\tau_6\left(\varphi^6\right) \in \bar{L}$ (cf. corol. 13). On a $\varphi^{-6}(6) = 1$,

$\chi_o(2) = 1$ et $\varphi^{-3.57}(6) = -1$, donc $\tau(L) = -\tau\left(\varphi^6\right)\ \tau\left(\varphi^{3.57}\right)^{-1}$.

Déterminons Gal $(\bar{L}/\bar{K})$ (d'ordre 6) : on vérifie que l'image $\bar{\sigma}_{10}$ de $\sigma_{10} \in$ Gal $\left(\mathbb{Q}^{(57)}/\mathbb{Q}^{(3)}\right)$ dans Gal $\left(\mathbb{Q}^{(57)}/\mathbb{Q}^{(3)}\right)/<\sigma_7>$ est génératrice : on a $<\bar{\sigma}_{10}> = \left\{\bar{1}\ ,\ \bar{\sigma}_{10}\ ,\ \bar{\sigma}_{43}\ ,\ \bar{\sigma}_{31}\ ,\ \bar{\sigma}_{25}\ ,\ \bar{\sigma}_{22}\right\}$ et

$$\nu'_{\bar{L}/\bar{K}}\ \tau(L) = \tau\left(\varphi^{3.57}\right)^{-6}\ \tau\left(\varphi^6\right)\ \tau\left(\varphi^{60}\right)\ \tau\left(\varphi^{258}\right)\ \tau\left(\varphi^{186}\right)\ \tau\left(\varphi^{150}\right)\ \tau\left(\varphi^{132}\right).$$

On a le tableau suivant :

α	écriture en base 7	$s(\alpha)$	$\gamma(\alpha)$ mod 7
171	$3 + 3.7 + 3.49$	9	-1
6	$6 + 0.7 + 0.49$	6	-1
60	$4 + 1.7 + 1.49$	6	3
258	$6 + 1.7 + 5.49$	12	-1
186	$4 + 5.7 + 3.49$	12	-3
150	$3 + 0.7 + 3.49$	6	1
132	$6 + 4.7 + 2.49$	12	1

On utilise le th. III :

$$\nu'_{\bar{L}/\bar{K}}\left(\tau(L)\right) \equiv \left(\frac{\tau\left(\varphi^{3.57}\right)}{\pi^9}\right)^{-6} \frac{\tau\left(\varphi^6\right)}{\pi^6}\ \frac{\tau\left(\varphi^{60}\right)}{\pi^6}\ \frac{\tau\left(\varphi^{258}\right)}{\pi^{12}}\ \frac{\tau\left(\varphi^{186}\right)}{\pi^{12}}\ \frac{\tau\left(\varphi^{150}\right)}{\pi^6}\ \frac{\tau\left(\varphi^{132}\right)}{\pi^{12}}$$

$$\equiv \left(\frac{1}{\gamma(171)}\right)^{-6} \frac{1}{\gamma(6)}\ \frac{1}{\gamma(60)}\ \frac{1}{\gamma(258)}\ \frac{1}{\gamma(186)}\ \frac{1}{\gamma(150)}\ \frac{1}{\gamma(152)}$$

$$\equiv (-1)^6\ (-1)\ (3^{-1})\ (-1)\ (-3^{-1})\ (1)\ (1) \equiv 3 \bmod \mathfrak{P}'$$

Par conséquent $\xi_{L/K} \equiv 4 \bmod \mathfrak{P}'$ soit $\xi_{L/K}$ est racine de l'unité d'ordre 3 $\left(\xi_{L/K} = \varphi(2)\right)$. Cet ordre est le maximum possible ici.

On constate alors qu'il est impossible de modifier $\tau(L)$ par une racine de l'unité de telle sorte que la norme obtenue soit égale à 1 ou -1 ; ceci montre bien que $\xi_{L/K}$ n'est pas dûe à une "mauvaise" définition de $\tau(L)$.

Remarque III 2. Si on remplace $L = \mathbb{Q}^{(57)}$ par L_1 où L_1 est le sous-corps intermédiaire entre K et L de degré 3 sur K, on peut aussi étudier $\xi_{L_1/K}$. Or L_1 étant de conducteur 57, on a $\tau(L_1) = \nu_{\overline{L}/\overline{L}_1}\ \tau(L)$, mais alors $\nu_{\overline{L}_1/\overline{K}}\ \tau(L_1) = \nu_{\overline{L}_1/\overline{K}}\ \nu_{\overline{L}/\overline{L}_1}\ \tau(L) = \nu_{\overline{L}/\overline{K}}\ \tau(L)$ que l'on vient de calculer. Cet exemple nous servira aussi pour une illustration ultérieure d'un phénomène particulier (cf. Rem. IV 4, chap. IV, §3).

IV

APPLICATION A L'ANNULATION DES CLASSES D'IDEAUX DES CORPS ABELIENS

1) Elément de STICKELBERGER modifié (dans tout le chapitre, on suppose $p \neq 2$).

Soit K un corps abélien de conducteur m_K.

Nous allons étudier l'élément $\dot{S}_K = S_K - \frac{1}{2}[\mathbb{Q}^{(m_K)} : K]\, \nu_{K/\mathbb{Q}}$, qui semble constituer, contrairement à S_K, le "véritable" élément de STICKELBERGER (cf. [1], où il est montré comment est obtenu $\dot{S}_K$ à l'aide des fonctions ζ partielles). En ce qui nous concerne, nous allons montrer que $\dot{S}_K$ est canoniquement associé au nombre $\tau(K)$ que nous avons défini (chap. III, §2, Déf. III 2).

Proposition IV 1. Soit K un corps de conducteur m_K. On a dans $\overline{K}$ la factorisation :

$$\tau(K)^{\dot{m}_K} A_{\overline{K}} = \mathfrak{P}_{\overline{K}}^{\dot{m}_K \dot{S}_K}, \text{ où } \dot{m}_K = m_K \text{ (resp. } 2m_K) \text{ si } m_K \text{ est pair (resp. impair).}$$

démonstration

D'après le corollaire II 3, on a $\tau_{\alpha_K}\left(\varphi^{\alpha_K}\right)^{m_K} A_{\mathbb{Q}^{(m_K)}} = \mathfrak{P}_{\mathbb{Q}^{(m_K)}}^{m_K S_{(m_K)}^{\mathbb{Q}}}$

avec $\alpha_K = \dfrac{q_K - 1}{m_K}$. On a donc par définition de $\tau\left(\mathbb{Q}^{(m_K)}\right)$:

$$\tau\left(\mathbb{Q}^{(m_K)}\right)^{2m_K} A_{\mathbb{Q}^{(m_K)}} = \mathfrak{P}_{\mathbb{Q}^{(m_K)}}^{2m_K S_{(m_K)}^{\mathbb{Q}} - m_K \nu_{\mathbb{Q}^{(m_K)}/\mathbb{Q}}} =$$

$\mathfrak{P}_{\mathbb{Q}(m_K)}^{2m_K \dot{S}_{\mathbb{Q}(m_K)}}$ par définition de $\dot{S}_{\mathbb{Q}(m_K)}$ et par le fait que $\tau_{\alpha_K}(\chi_o^K)^2 = \pm p^{n_K}$; la proposition en résulte en prenant les normes dans $\mathbb{Q}^{(m_K)}/\overline{K}$ (si m_K est pair on peut alors diviser les exposants par 2, comme on le vérifie facilement).

Lemme IV1. (i) Soit $\omega \in \mathbb{Z}[G_K]$ tel que $\Omega = \omega \dot{S}_K \in \mathbb{Z}[G_K]$; alors $\mathfrak{P}_{\overline{K}}^{\Omega}$ est principal dans $\overline{K}$ (de façon précise $\mathfrak{P}_{\overline{K}}^{\Omega} = \tau(K)^{\omega'} A_{\overline{K}}$ avec $\tau(K)^{\omega'} \in \overline{K}$, ω' désignant un relèvement quelconque de ω dans $\mathbb{Z}[G'_K]$).

(ii) soit $\omega' \in \mathbb{Z}[G'_K]$ et soit ω sa projection canonique dans $\mathbb{Z}[G_K]$; si $\tau(K)^{\omega'} \in \overline{K}$, alors l'image $\dot{S}_K \overline{\omega}$ de $\dot{S}_K \omega$ dans $\mathbb{Q}[G_{\overline{K}}]$ est dans $\mathbb{Z}[G_{\overline{K}}]$.

On a $\tau(K)^{\dot{m}_K \omega} A_{\overline{K}} = \mathfrak{P}_{\overline{K}}^{\dot{m}_K \omega \dot{S}_K} = \mathfrak{P}_{\overline{K}}^{\dot{m}_K \Omega}$, puissance $(\dot{m}_K)^e$ d'un idéal de $\overline{K}$; le raisonnement fait dans le lemme II4 s'applique encore ici sans modification avec $\dot{m}_K$ au lieu de m_K (mais $\dot{m}_K$ divise encore $q_K - 1$) : on a $\tau(K)^{\omega'} \in \overline{K}$ et $\mathfrak{P}_{\overline{K}}^{\Omega} = \tau(K)^{\omega'} A_{\overline{K}}$ en appelant ω' un relèvement quelconque de ω dans $\mathbb{Z}[G'_K]$; d'où (i).

Si $\tau(K)^{\omega'} \in \overline{K}$, on peut poser $\tau(K)^{\omega'} A_{\overline{K}} = \mathfrak{P}_{\overline{K}}^{\overline{\Omega}}$, $\overline{\Omega} \in \mathbb{Z}[G_{\overline{K}}]$, d'où $\dot{m}_K \overline{\omega} \overline{\dot{S}_K} = \dot{m}_K \overline{\Omega}$ soit $\overline{\omega} \overline{\dot{S}_K}$ entier dans $\mathbb{Z}[G_{\overline{K}}]$.

On est amené à déterminer $\dot{\mathfrak{A}}_K = \left\{\omega \in \mathbb{Z}[G_K],\ \omega \dot{S}_K \in \mathbb{Z}[G_K]\right\}$; on a alors $\dot{S}_K \mathbb{Z}[G_K] \cap \mathbb{Z}[G_K] = \dot{\mathfrak{A}}_K \dot{S}_K$. Notons de même ([5], pp. 34-37) $\mathfrak{A}_K = \left\{\omega \in \mathbb{Z}[G_K],\ \omega S_K \in \mathbb{Z}[G_K]\right\}$ et soit $\dot{\Lambda}_K$ (resp. Λ_K) le plus petit entier positif non nul tel que $\dot{\Lambda}_K \dot{S}_K \in \mathbb{Z}[G_K]$ (resp. $\Lambda_K S_K \in \mathbb{Z}[G_K]$).

On obtient le résultat suivant :

Proposition IV 2. (i) On a $\dot{\mathfrak{A}}_K = \left(\ldots, \left(\frac{K}{a}\right) - a, \ldots ; \dot{\Lambda}_K\right)$, où les entiers a, $(a, m_K) = 1$ parcourent un système complet de résidus mod m_K, impairs;

(ii) Si $[\mathbb{Q}^{(m_K)} : K]$ est pair, alors $\dot{\mathfrak{A}}_K = \mathfrak{A}_K$;

(iii) Si $[\mathbb{Q}^{(m_K)} : K]$ est impair alors on a $\left(\dot{\Lambda}_K\right)_\ell = \left(\Lambda_K\right)_\ell$ pour tout ℓ premier impair et $\left(\dot{\Lambda}_K\right)_2 = 2$ si m_K est impair $\left(\left(\Lambda_K\right)_2 = 1\right)$ et $\left(\dot{\Lambda}_K\right)_2 = \left(\Lambda_K\right)_2 = \left(m_K\right)_2$, si m_K est pair.

démonstration

On a $\left(\left(\frac{K}{a}\right) - a\right)\dot{S}_K = \left(\left(\frac{K}{a}\right) - a\right)S_K - \frac{1}{2}[\mathbb{Q}^{(m_K)} : K](1-a)v_{K/\mathbb{Q}}$;

or $\left(\left(\frac{K}{a}\right) - a\right)S_K$ est entier ([5], Lemme II 6) et $1 - a$ est pair, d'où une inclusion pour (i). Si $\omega \in \dot{\mathfrak{A}}_K$, $\omega = \sum_{\sigma \in G_K} x_\sigma \sigma$; on peut écrire

$\omega \dot{S}_K = \sum_{\sigma \in G_K} x_\sigma (\sigma - a_\sigma)\dot{S}_K + r\dot{S}_K$, où a_σ impair est défini par $\left(\frac{K}{a_\sigma}\right) = \sigma$ et où $r \in \mathbb{Z}$; on a donc $r\dot{S}_K \in \mathbb{Z}[G_K]$, d'où $r \equiv 0 \bmod \dot{\Lambda}_K$. D'où (i).

L'assertion (ii) est évidente ; pour l'assertion (iii), seul le calcul de $\left(\dot{\Lambda}_K\right)_2$ pour $[\mathbb{Q}^{(m_K)} : K]$ impair et m_K pair reste à expliciter. On pose $m_K = 2^A m'_K$, m'_K impair, $A \geq 2$. Posons $H_K = \mathrm{Gal}\left(\mathbb{Q}^{(m_K)}/K\right)$ et soit $\alpha_\sigma = \sum_a a$ (sommation sur les a, $1 \leq a < m_K$, $\left(a, m_K\right) = 1$ et $\sigma_a^{-1} H_K = \sigma$ pour tout $\sigma \in G_K$).

On a $m_K \dot{S}_K = \sum_{\sigma \in G_K} \left(\alpha_\sigma - \frac{m_K}{2}[\mathbb{Q}^{(m_K)} : K]\right)\sigma$ (cf. [5], Déf. II 2).

Posons $\dot{\alpha}_\sigma = \alpha_\sigma - \frac{m_K}{2}[\mathbb{Q}^{(m_K)} : K]$, pour tout $\sigma \in G_K$; on a ([5], lemme II 7) $\alpha_\sigma \equiv c\,\alpha_1 \bmod m_K$, $(c, m_K) = 1$, d'où $\dot{\alpha}_\sigma \equiv c\,\alpha_1 - \frac{m_K}{2}[\mathbb{Q}^{(m_K)} : K] \equiv$

$$c\left(\dot{\alpha}_1 + \frac{m_K}{2}[\mathbb{Q}^{(m_K)} : K]\right) - \frac{m_K}{2}[\mathbb{Q}^{(m_K)} : K] \equiv$$

$$c\,\dot{\alpha}_1 - \frac{m_K}{2}[\mathbb{Q}^{(m_K)} : K]\,(1 - c) \equiv c\,\dot{\alpha}_1 \bmod m_K, \text{ car } c \text{ est impair.}$$

Or α_1 est impair : en effet, soit $k_o = K \cap \mathbb{Q}^{(2^A)}$; on a $[\mathbb{Q}^{(2^A)} : k_o] = [\mathbb{Q}^{(2^A)}K : K]$ qui divise $[\mathbb{Q}^{(2^A m'_K)} : K]$ (impair) d'où les inclusions $\mathbb{Q}^{(2^A)} \subset K \subset \mathbb{Q}^{(2^A m'_K)}$ et α_1 est somme d'un nombre impair d'entiers a tels que $a \equiv 1 \bmod 2^A$; d'où α_1 impair et $\dot{\alpha}_1$ impair (car $\frac{m_K}{2}$ est encore pair) ainsi que tous les $\dot{\alpha}_\sigma$, d'où $\left(\dot{\Lambda}_K\right)_2 = 2^A$ ici.

Remarque IV 1. On a donc montré que l'on a $\dot{\Lambda}_K = \Lambda_K$ dans tous les cas sauf dans le cas où $[\mathbb{Q}^{(m_K)} : K]$ et m_K sont impairs, auquel cas, on a $\left(\dot{\Lambda}_K\right)_2 = 2$ et $\left(\Lambda_K\right)_2 = 1$.

2) Résultats sur l'annulation des 2-classes d'idéaux des extensions abéliennes imaginaires de $\mathbb{Q}$.

Soit L un corps abélien distinct de $\mathbb{Q}$, de conducteur m_L. On appelle L_+ le sous-corps réel maximal de L. Considérons $\tau(L)$ (relativement à $p \neq 2$ quelconque).

Lemme IV 2. On a $\tau(L)^{1+\sigma_{-1}} = 1$. Si $\overline{L}$ est réel alors $\tau(L) = \pm 1$. En particulier, si $L \neq \mathbb{Q}$ est réel alors $\tau(L) = \pm 1$.

Donnons d'abord un exemple de corps L imaginaire pour lequel L est réel (donc $\tau(L) = \pm 1$) avec $\tau(L) = -1$.

On prend $L = \mathbb{Q}^{(7)}$ et $p = 13$; comme $13 \equiv -1 \bmod 7$ on aura $q_L = 13^2 \left(n_L = 2\right)$ soit :

$$\tau(L) = \chi_o(2)\, \tau_{24}\left(\varphi^{24}\right) \tau_{24}\left(\chi_o\right)^{-1}.$$

On a $\chi_o(2) = \varphi^{84}(2) \equiv 2^{-84} \bmod 13$; or $84 = 7 \times 12$ d'où $\chi_o(2) = 1$ ainsi que $\varphi^{24}(a)$ pour tout entier a. On a donc $\tau(L) = \tau\left(\varphi^{24}\right) \tau\left(\chi_o\right)^{-1}$. Comme $n_L = 2$, $\tau\left(\chi_o\right) = \tau\left(\varphi_1^6\right)^2$ (φ_1 relatif à $\mathbb{F}_{13}$), donc $\tau\left(\chi_o\right) \in \mathbb{Q}$; de même on vérifie (corol. 13) que $\tau\left(\varphi^{24}\right) \in \mathbb{Q}^{(7)}$ (donc à $\overline{\mathbb{Q}^{(7)}} = \mathbb{Q}_+^{(7)}$).

Pour voir si $\tau(L) = +1$ ou -1, on utilise les congruences habituelles : $\tau(L) = \tau\left(\varphi^{24}\right) \tau\left(\varphi^{84}\right)^{-1} \equiv \frac{\gamma(84)}{\gamma(24)} \bmod \mathfrak{P}'$. On a $84 = 6 + 6.13$ et $24 = 11 + 1.13$; d'où $\gamma(84) \equiv (6!)^2 \equiv -1 \bmod 13$ et $\gamma(24) \equiv 11! \equiv 1 \bmod 13$ et ceci démontre que l'on a bien $\tau(L) = -1$ (Remarquer que cette propriété ne provient ni du terme $\chi_o(2)$ ni de la normalisation (τ_α) adoptée, au moins pour cet exemple).

démonstration du lemme

On a $\tau\left(\mathbb{Q}^{(m_L)}\right) = \chi_o(2)\, \tau_{\alpha_L}\left(\varphi^{\alpha_L}\right) \tau_{\alpha_L}\left(\chi_o\right)^{-1}$,

où $\alpha_L = \frac{q_L - 1}{m_L}$ et $\tau\left(\mathbb{Q}^{(m_L)}\right) \in \overline{\mathbb{Q}'^{(m_L)}}$ (corol. 12) ; on a $\tau\left(\mathbb{Q}^{(m_L)}\right)^{1+\sigma_{-1}} = q\, q^{-1} = 1$ (car φ^{α_L} et χ_o sont distincts du caractère unité) ; on a donc de même $\tau(L)^{1+\sigma_{-1}} = 1$.

On a $\tau(L) \in \overline{L}'$ et $\tau(L)^{2m_L} \in \overline{L}$ supposé réel (cf. Déf. III 1), donc $\tau(L)^{2m_L(1+\sigma_{-1})} = \tau(L)^{4m_L} = 1$ et $\tau(L)$ est une racine de l'unité appartenant à $\overline{L}'$ et d'après le corollaire II 2 sur la $\mathbb{Z}$-torsion dans $\mathcal{S}$, puisque $\overline{L}' = \overline{L}\mathbb{Q}^{(p)}$ $(p \neq 2)$, on a $\tau(L) = \pm 1$.

Corollaire IV1. Si L est imaginaire on a pour tout $\omega' \in \mathbb{Z}[G_L']$ tel que $\tau(L)^{\omega'} \in L$, $v_{L/L_+} \tau(L)^{\omega'} = +1$.

Supposons maintenant L imaginaire.

Lemme IV3. Il existe $\dot{T}_L \in \mathbb{Q}[G_L]$, défini modulo $\left(1 + \left(\frac{L}{-1}\right)\right)\mathbb{Q}[G_L]$, tel que $\dot{S}_L = \left(1 - \left(\frac{L}{-1}\right)\right)\dot{T}_L$; on peut prendre par exemple $\dot{T}_L = \frac{1}{m_L} \sum_{a=1}^{m_L/2}{}^{*} \left(\frac{L}{a}\right)^{-1} \left(a - \frac{m_L}{2}\right)$. Enfin pour tout $\omega \in \mathbb{Z}[G_L]$ tel que $\omega \dot{S}_L$ soit entier, il existe un représentant $\dot{T}_L^{\omega}$ de $\dot{T}_{L\,\omega}$ modulo $\left(1 + \left(\frac{L}{-1}\right)\right)\mathbb{Q}[G_L]$ appartenant à $\mathbb{Z}[G_L]$ et vérifiant $\dot{T}_L^{\omega}\left(1 - \left(\frac{L}{-1}\right)\right) = \dot{S}_{L\,\omega}$. L'élément $\dot{T}_L^{\omega}$ est alors défini modulo $\left(1 + \left(\frac{L}{-1}\right)\right)\mathbb{Z}[G_L]$.

On a par définition $S_L = \frac{1}{m_L} \sum_{a=1}^{m_L}{}^{*} \left(\frac{L}{a}\right)^{-1} a =$

$\frac{1}{m_L} \sum_{a=1}^{m_L/2}{}^{*} \left(\left(\frac{L}{a}\right)^{-1} a + \left(\frac{L}{m_L - a}\right)^{-1} (m_L - a)\right)$ (car si m_L est pair, $\frac{m_L}{2} \equiv 0 \bmod 2$ et si m_L est impair, $\frac{m_L}{2}$ n'est pas entier)

soit $\frac{1}{m_L} \sum_{a=1}^{m_L/2}{}^{*} \left(\frac{L}{a}\right)^{-1} a + \sum_{a=1}^{m_L/2}{}^{*} \left(\frac{L}{-a}\right)^{-1} - \frac{1}{m_L} \sum_{a=1}^{m_L/2}{}^{*} \left(\frac{L}{-a}\right)^{-1} a$ et

$\dot{S}_L = \left(1 - \left(\frac{L}{-1}\right)\right) \frac{1}{m_L} \sum_{a=1}^{m_L/2}{}^{*} \left(\frac{L}{a}\right)^{-1} a + \left(\frac{L}{-1}\right) \sum_{a=1}^{m_L/2}{}^{*} \left(\frac{L}{a}\right)^{-1} - \frac{1}{2}[\mathbb{Q}^{(m_L)} : L] v_{L/\mathbb{Q}}$;

On peut écrire $\frac{1}{2}[\mathbb{Q}^{(m_L)} : L] v_{L/\mathbb{Q}} = \frac{1}{2} \sum_{a=1}^{m_L}{}^{*} \left(\frac{L}{a}\right)^{-1} =$

$\frac{1}{2} \sum_{a=1}^{m_L/2}{}^{*} \left(\left(\frac{L}{a}\right)^{-1} + \left(\frac{L}{-a}\right)^{-1}\right) = \frac{1}{2}\left(1 + \left(\frac{L}{-1}\right)\right) \sum_{a=1}^{m_L/2}{}^{*} \left(\frac{L}{a}\right)^{-1}$

et $\dot{S}_L = \left(1 - \left(\frac{L}{-1}\right)\right)\frac{1}{m_L} \sum_{a=1}^{m_L/2 *} \left(\frac{L}{a}\right)^{-1} a - \frac{1}{2}\left(1 - \left(\frac{L}{-1}\right)\right) \sum_{a=1}^{m_L/2 *} \left(\frac{L}{a}\right)^{-1}$,

d'où la valeur de $\dot{T}_L$.

Si maintenant on a $\omega \dot{S}_L \in \mathbb{Z}[G_L]$, alors

$\Omega = \dot{T}_L \left(1 - \left(\frac{L}{-1}\right)\right)\omega$ est entier et on a $\Omega\left(1 + \left(\frac{L}{-1}\right)\right) = 0$; or dans $\mathbb{Z}[G_L]$

ceci équivaut à $\Omega \in \left(1 - \left(\frac{L}{-1}\right)\right)\mathbb{Z}[G_L]$ soit $\Omega = \left(1 - \left(\frac{L}{-1}\right)\right)T$, $T \in \mathbb{Z}[G_L]$;

d'où $\left(\dot{T}_L \omega - T\right)\left(1 - \left(\frac{L}{-1}\right)\right) = 0$ dans $\mathbb{Q}[G_L]$ soit

$\dot{T}_L \omega - T \in \left(1 + \left(\frac{L}{-1}\right)\right)\mathbb{Q}[G_L]$; ainsi T est l'élément $\dot{T}_L^{\omega}$ cherché.

Soit alors $\omega \in \mathbb{Z}[G_L]$ tel que $\dot{S}_L \omega \in \mathbb{Z}[G_L]$; alors (lemme IV 1)

$\mathfrak{P}_{\overline{L}}^{\dot{S}_L \omega} = \tau(L)^{\omega'} A_{\overline{L}}$ avec $\tau(L)^{\omega'} \in \overline{L}$ (ω' relèvement de ω dans $\mathbb{Z}[G'_L]$). On a

alors (corol. IV1) $\nu_{L/L_+}\left(\tau(L)^{\omega'}\right) = +1$ et on peut appliquer le théorème 90

de HILBERT qui affirme qu'il existe $\theta_\omega \in L$ tel que $\tau(L)^{\omega'} = \theta_\omega^{1-\sigma_{-1}}$. On

remarque que l'on peut prendre $\theta_\omega = 1 + \tau(L)^{\omega'}$ $\left(\text{si } \tau(L)^{\omega'} \neq -1\right)$ car

$$\theta_\omega^{1-\sigma_{-1}} = \frac{1 + \tau(L)^{\omega'}}{1 + \tau(L)^{\omega'\sigma_{-1}}} = \frac{1 + \tau(L)^{\omega'}}{\tau(L)^{\omega'(1+\sigma_{-1})} + \tau(L)^{\omega'\sigma_{-1}}} = \tau(L)^{\omega'}$$; ceci prouve

aussi que θ_ω peut être pris dans $\overline{L}$ $\left(\text{si } \tau(L)^{\omega'} \neq -1 \text{ et } \overline{L} \text{ non réel}\right)$;

si $\tau(L)^{\omega'} = -1$ avec $\overline{L} \subset L_+$, on remarque que les calculs qui vont suivre

sont valables.

On a par ailleurs avec un choix convenable de $\dot{T}_L^{\omega}$

(lemme IV 3) $\mathfrak{P}_{\overline{L}}^{\dot{S}_L \omega} = \mathfrak{P}_{\overline{L}}^{(1-\sigma_{-1})\dot{T}_L^{\omega}} = \theta_\omega^{1-\sigma_{-1}} A_{\overline{L}}$ et $\left(\mathfrak{P}_{\overline{L}}^{\dot{T}_L \omega} \theta_\omega^{-1} A_{\overline{L}}\right)^{1-\sigma_{-1}} = (1)$,

$\mathfrak{P}_{\overline{L}}^{\dot{T}_L \omega} = \theta_\omega A_{\overline{L}}\, \mathfrak{a}_\omega$, où $\mathfrak{a}_\omega$ est un idéal invariant dans L/L_+ (qui est en fait

dans $\overline{L}$ en toute généralité). Cette relation s'écrit aussi $\mathfrak{P}_L^{\dot{T}_L \omega} = \theta_\omega A_L \mathfrak{a}_\omega$; on a donc prouvé :

Proposition IV 3. Soit L un corps abélien imaginaire de sous-corps réel maximal L_+. Soit $\mathbb{H}(L)$ le groupe des classes au sens ordinaire de L et soit $\mathbb{H}_1^0(L/L_+)$ le sous-groupe de $\mathbb{H}(L)$ formé des classes des idéaux invariants dans L/L_+. Alors pour tout $\omega \in \mathbb{Z}[G_L]$ tel que $\dot{S}_L \omega \in \mathbb{Z}[G_L]$, tout élément T_L^ω de $\mathbb{Z}[G_L]$ (vérifiant $T_L^\omega \left(1 - \left(\frac{L}{-1}\right)\right) = \dot{S}_L \omega$) annule le groupe $\mathbb{H}(L)/\mathbb{H}_1^0(L/L_+)$.

On sait que $\dot{S}_L \dot{\mathfrak{A}}_L$ est un idéal de $\mathbb{Z}[G_L]$ et que tout élément $\Omega \in \dot{S}_L \dot{\mathfrak{A}}_L$ est de la forme $\left(1 - \left(\frac{L}{-1}\right)\right) T$, $T \in \mathbb{Z}[G_L]$, défini modulo $\left(1 + \left(\frac{L}{-1}\right)\right)\mathbb{Z}[G_L]$ (d'après le lemme IV 3). Par conséquent $\dot{S}_L \dot{\mathfrak{A}}_L$ est de la forme $\left(1 - \left(\frac{L}{-1}\right)\right)\dot{\mathfrak{B}}_L$ où $\dot{\mathfrak{B}}_L$ est l'idéal de $\mathbb{Z}[G_L]$ engendré par les éléments T et par $1 + \left(\frac{L}{-1}\right)$ (l'idéal $\dot{\mathfrak{B}}_L$ est alors égal à $\left\{T \in \mathbb{Z}[G_L],\right.$ $\left. T\left(1 - \left(\frac{L}{-1}\right)\right) \in \dot{S}_L \dot{\mathfrak{A}}_L\right\}$).

Définition IV 1. On définit $\dot{\mathfrak{B}}_L$ comme le plus grand idéal de $\mathbb{Z}[G_L]$ défini par $\dot{S}_L \dot{\mathfrak{A}}_L = \left(1 - \left(\frac{L}{-1}\right)\right)\dot{\mathfrak{B}}_L$.

Corollaire IV 2. L'idéal $\dot{\mathfrak{B}}_L$ annule $\mathbb{H}(L)/\mathbb{H}_1^0(L/L_+)$.

Donnons un exemple montrant que l'idéal $\dot{\mathfrak{B}}_L$ n'est pas nécessairement l'idéal $\dot{T}_L \dot{\mathfrak{A}}_L$ bien que l'on ait $\dot{T}_L \dot{\mathfrak{A}}_L \left(1 - \left(\frac{L}{-1}\right)\right) = \dot{S}_L \dot{\mathfrak{A}}_L$:

Soit $L = \mathbb{Q}^{(5)}$; on a $\dot{S}_L = \frac{1}{10}\left(-3 - \sigma + \sigma^3 + 3\sigma^2\right)$, avec $\sigma = \sigma_3$, $\left(\text{d'où } \left(\frac{L}{-1}\right) = \sigma^2\right)$. On a donc $\dot{T}_L = \frac{-1}{10}(3 + \sigma)$ modulo $(1 + \sigma^2)$.

On a alors $10\dot{S}_L = (3 + \sigma)(\sigma^2 - 1)$ et $(\sigma - 3)\dot{S}_L = 1 - \sigma^2$, ce qui fait que

l'idéal $\dot{\mathfrak{B}}_L$ est l'idéal unité.

Soit $T = \dot{T}_L + A(1+\sigma^2)$, $A \in \mathbb{Q}[G_L]$; calculons $T(\sigma-3)$:

on a $T(\sigma-3) = 1 + \frac{1}{10}(-1+10A\sigma-30A)(1+\sigma^2)$; comme A est défini modulo $1-\sigma^2$, on peut supposer $A = u+v\sigma$, $u, v \in \mathbb{Q}$ et

$T(\sigma-3) = 1 + \frac{1}{10}(-1+10v-30u+\sigma(10u-30v))(1+\sigma^2)$; une étude élémentaire montre alors que quels que soient u et v, $T(\sigma-3)$ n'appartient jamais à $\mathbb{Z}[G_L]$.

On peut cependant remarquer que lorsque $\dot{\mathfrak{A}}_L = (1)$ (i. e. $\dot{S}_L$ est dans $\mathbb{Z}[G_L]$) alors $\dot{\mathfrak{B}}_L$ est engendré par $1+\left(\frac{L}{-1}\right)$ et par un représentant convenable de $\dot{T}_L$ modulo $\left(1+\left(\frac{L}{-1}\right)\right)\mathbb{Q}[G_L]$ qui se détermine en pratique par la "division" de $\dot{S}_L$ par $1-\left(\frac{L}{-1}\right)$ dans $\mathbb{Z}[G_L]$ (nous appelons encore $\dot{T}_L$ ce représentant pour simplifier).

Remarquons aussi que le fait d'adjoindre $1+\left(\frac{L}{-1}\right)$ aux générateurs de $\dot{\mathfrak{B}}_L$ rend ce dernier unique sans modifier les propriétés d'annulation que nous considérons.

Remarque IV 2. Compte tenu du fait que $\dot{S}_L \dot{\mathfrak{A}}_L = \left(1-\left(\frac{L}{-1}\right)\right)\dot{\mathfrak{B}}_L$, on peut déduire facilement de l'énoncé classique du théorème de STICKELBERGER que l'idéal $\dot{\mathfrak{B}}_L$ annule $\mathbb{H}(L)/\mathbb{H}_1(L/L_+)$ (où $\mathbb{H}_1(L/L_+)$ désigne le sous-groupe des classes de L invariantes dans L/L_+) ; mais d'après la suite exacte classique (où E( ) désigne le groupe des unités) :

$$1 \to \mathbb{H}_1^0(L/L_+) \to \mathbb{H}_1(L/L_+) \to E(L_+) \cap N_{L/L_+} L^*/N_{L/L_+} E(L) \to 1 ,$$

on constate que le quotient $\mathbb{H}_1(L/L_+)/\mathbb{H}_1^0(L/L_+)$ n'est pas trivial en général (puisque L est imaginaire, ce quotient dépend, essentiellement, du groupe des unités totalement positives de L_+). Il semble donc déjà que le résultat de la proposition IV 3 ne se déduise pas de celui du th. II 2.

Nous allons maintenant démontrer que le résultat précédent (Prop. IV 3) peut s'améliorer encore très substantiellement ; de façon précise nous allons montrer que dans l'énoncé précédent on peut remplacer $\mathbb{H}_1^0(L/L_+)$ par les classes réelles de L_+ étendues à L, à une modification près que nous allons expliquer. Ces propriétés ne concernant que les 2-classes d'idéaux au sens ordinaire, nous allons raisonner avec les 2-groupes de SYLOW des groupes de classes (ce que nous indiquerons dans les notations en remplaçant la lettre $\mathbb{H}$ par la lettre $\mathfrak{H}$). Ces 2-SYLOW seront alors considérés comme $\mathbb{Z}_2[G_L]$- modules.

Soit donc L une extension abélienne imaginaire quelconque ; soit M l'unique sous-extension de L telle que $[L : M] = d$ soit impair et $[M : \mathbb{Q}]$ une puissance de 2. On sait que le 2-groupe des classes $\mathfrak{H}(L)$ de L est une somme directe de la forme

$$\mathfrak{H}(L) = \mathfrak{H}(L)^e \oplus \mathfrak{H}(L)^{1-e}$$

où $e = \frac{1}{d} \nu_{L/M}$; dans cette décomposition $\mathfrak{H}(L)^e$ est canoniquement isomorphe à $\mathfrak{H}(M)$ et $\mathfrak{H}(L)^{1-e}$ peut être vu comme le sous-groupe de $\mathfrak{H}(L)$ formé des classes de norme 1 dans L/M. Nous allons voir que les classes provenant de M (i. e. de la composante $\mathfrak{H}(L)^e$) constituent une obstruction à la propriété d'annulation de $\mathfrak{H}(L)/j_{L/L_+}\mathfrak{H}(L_+)$ que nous avons en vue. Donnons un exemple numérique montrant cette obstruction :

Soit $L = M = \mathbb{Q}(\sqrt{-15})$ (on a donc $\mathfrak{H}(L)^e = \mathfrak{H}(L)$ ici) ; on vérifie que $\dot{S}_L = \left(\frac{L}{-1}\right) - 1$, soit $\dot{T}_L = 1$ et $\dot{\mathfrak{B}}_L = (1)$. Si p est un nombre premier tel que $\mathfrak{P}_L$ (idéal premier au-dessus de p dans L) représente la classe d'ordre 2 de $\mathfrak{H}(L)$, alors on peut écrire $\mathfrak{P}_L^{\dot{T}_L} = \theta A_L \mathfrak{a}$, $\theta \in L$, $\mathfrak{a}$ idéal ambige dans $L/\mathbb{Q}$; or $\mathfrak{P}_L^{\dot{T}_L} = \mathfrak{P}_L$ étant non principal, $\mathfrak{a}$ ne peut être un idéal rationnel et contient de façon "non triviale" l'un des idéaux premiers ramifiés

dans $L/\mathbb{Q}$. Donc ici, $\dot{T}_L$ n'annule pas $\mathcal{H}(L)/j_{L/L_+}\mathcal{H}(L_+) = \mathcal{H}(L)$.

Remarquons que cette situation (cas cyclique d'ordre une puissance de 2) correspond à un cas particulier de la définition des invariants "classes" (cf. [5], Déf. 118, p. 65-66) qui est suggéré par la forme même des résultats analytiques (cf. Th. 112, p. 31 de [5]) ; nous y reviendrons à la fin de ce paragraphe.

On peut alors énoncer le résultat suivant :

Théorème IV1. Soit L une extension abélienne imaginaire quelconque et soit Δ_L le plus grand sous-groupe d'ordre impair de G_L ; on pose $e = \frac{1}{|\Delta_L|}\sum_{s\in\Delta_L} s$. Soient $\mathcal{H}(L)$, $\mathcal{H}(L_+)$ les 2-groupes de SYLOW des groupes des classes au sens ordinaire de L et L_+ et soit j_{L/L_+} l'extension des classes réelles de L_+ à L. Alors il existe un élément $\dot{T}'_L$ de $\mathbb{Z}_2[G_L]$ défini modulo $\left(1+\left(\frac{L}{-1}\right)\right)\mathbb{Z}_2[G_L]$ par l'égalité $\dot{S}_L(1-e) = \dot{T}'_L\left(1-\left(\frac{L}{-1}\right)\right)$ et qui annule le module $\mathcal{H}(L)^{1-e}/j_{L/L_+}\mathcal{H}(L_+)^{1-e}$.

démonstration

Si le conducteur de L est puissance d'un nombre premier, il n'y a qu'un seul idéal premier ramifié dans L et il est principal, donc $IH_1^0(L/L_+) = j_{L/L_+}IH(L_+)$ et notre théorème se réduit à la proposition IV 3.

Supposons maintenant le conducteur de L divisible par au moins deux nombres premiers distincts.

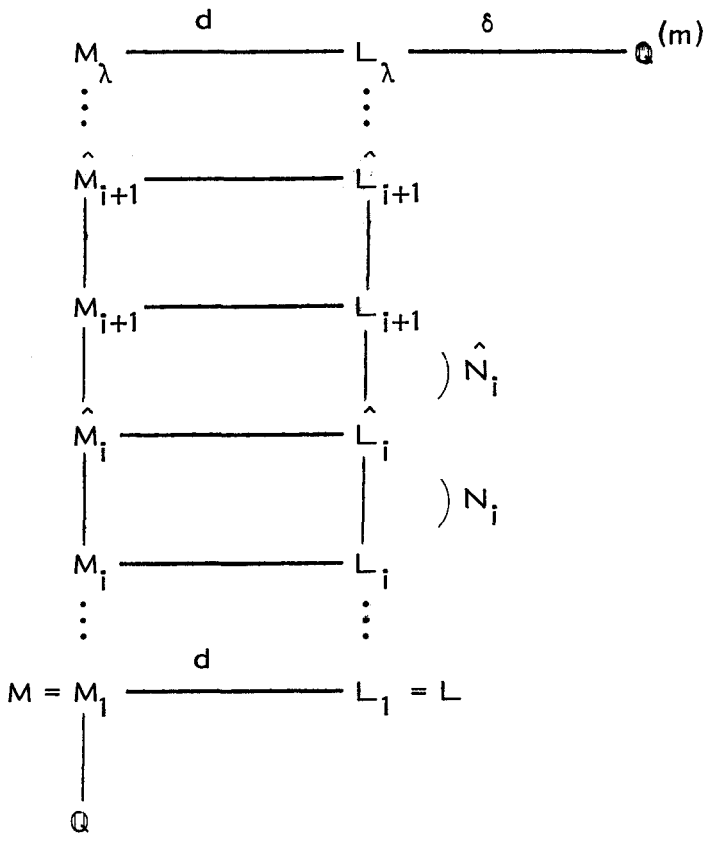
Lemme IV4. Soit m un conducteur de corps cyclotomique, $m > 1$. Alors l'extension $\mathbb{Q}^{(m)}/\mathbb{Q}_+^{(m)}$ est non ramifiée pour les idéaux premiers si et seulement si m est divisible par au moins deux diviseurs premiers distincts.

Il est bien connu que si $m = \ell^k$ (ℓ premier) alors $\mathbb{Q}^{(m)}/\mathbb{Q}$ est totalement ramifiée en ℓ.

Il suffit donc de prouver que si m est divisible par au moins deux diviseurs premiers distincts, alors $\mathbb{Q}^{(m)}/\mathbb{Q}_+^{(m)}$ est non ramifiée pour les idéaux : Soit ℓ un diviseur premier de m et posons $m' = m/\ell^k$, ℓ^k étant la plus grande puissance de ℓ divisant m. Par hypothèse, on a $m' > 1$ et m' est un conducteur de corps cyclotomique. Le corps d'inertie pour ℓ dans $\mathbb{Q}^{(m)}/\mathbb{Q}$ est le corps $\mathbb{Q}^{(m')}$ qui est imaginaire ; par conséquent ℓ est bien non ramifié dans $\mathbb{Q}^{(m)}/\mathbb{Q}_+^{(m)}$ puisque $\mathbb{Q}_+^{(m)}$ ne peut contenir $\mathbb{Q}^{(m')}$.

Lemme IV 5. Soit m un multiple du conducteur du corps L. Alors on a $h(L)^{1-e} \subset N_{\mathbb{Q}^{(m)}/L}\, h(\mathbb{Q}^{(m)})$.

Considérons le schéma suivant ($\lambda \geq 1$) :



Dans ce schéma les extensions L_λ , M_λ , M_1 sont définies par les conditions $[\mathbb{Q}^{(m)} : M_\lambda]$ est impair, $[M_\lambda : \mathbb{Q}]$ est puissance de 2, $M_1 = M_\lambda \cap L$ et $L_\lambda = L M_\lambda$ (d et δ sont donc impairs).

Dans l'extension L_λ/L_1 appelons $\{\hat{L}_i/L_i\}_{i = 1,\ldots, \lambda-1}$ une famille de sous-extensions de L_λ/L_1 telles que :

(i) $\hat{L}_i/L_i$ est non ramifiée pour les idéaux,

(ii) On a $L_1 \subset \hat{L}_1 \subset \ldots \subset L_i \subset \hat{L}_i \subset L_{i+1} \subset \ldots \subset \hat{L}_{\lambda-1} \subset L_\lambda$,

(iii) les extensions $L_\lambda/\hat{L}_{\lambda-1}$,..., $L_{i+1}/\hat{L}_i$,..., $L_2/\hat{L}_1$ ne contiennent aucune sous-extension non ramifiée pour les idéaux.

On définit alors les extensions correspondantes dans M_λ/M_1 : M_i et $\hat{M}_i$, $i = 1,\ldots, \lambda-1$, en posant $\hat{M}_i = M_\lambda \cap \hat{L}_i$ et $M_i = M_\lambda \cap L_i$, pour $i = 1,\ldots, \lambda-1$. Il est clair que la famille $\{\hat{M}_i/M_i\}_{i = 1,\ldots, \lambda-1}$ a, dans M_λ/M_1 , les propriétés analogues à (i), (ii) et (iii).

On sait que dans une extension E/F la norme de $\mathcal{H}(E)$ coïncide avec $\mathcal{H}(F)$ si E/F ne contient aucune sous-extension de degré puissance de 2 non ramifiée partout (i. e. pour les idéaux et les places à l'infini). Si E/F est de degré une puissance de 2 et est non ramifiée partout, alors $N_{E/F}\, \mathcal{H}(E)$ est d'indice $[E : F]$ dans $\mathcal{H}(F)$ et $N_{E/F}\, \mathcal{H}(E)$ est le sous-groupe de $\mathcal{H}(F)$ canoniquement associé à E/F par la théorie du corps de classes.

On a ici $\mathcal{H}(\hat{L}_i)^e \simeq \mathcal{H}(\hat{M}_i)$ et $\mathcal{H}(L_i)^e \simeq \mathcal{H}(M_i)$. Désignons par N_i (resp. $\hat{N}_i$) la norme dans $\hat{L}_i/L_i$ (resp. $L_{i+1}/\hat{L}_i$), $i = 1,\ldots, \lambda-1$. On a donc $\mathrm{Gal}\,(\hat{L}_i/L_i) \simeq \mathcal{H}(L_i)/N_i\, \mathcal{H}(\hat{L}_i) \simeq \left(\mathcal{H}(L_i)^e/N_i\, \mathcal{H}(\hat{L}_i)^e\right) \oplus \left(\mathcal{H}(L_i)^{1-e}/N_i\, \mathcal{H}(\hat{L}_i)^{1-e}\right)$

et le premier terme de la somme directe est isomorphe à $\mathcal{H}(M_i)/N_i\,\mathcal{H}(\hat{M}_i) \simeq \mathrm{Gal}\,(\hat{M}_i/M_i)$, par le corps de classes ; d'où puisque $\mathrm{Gal}\,(\hat{M}_i/M_i) \simeq \mathrm{Gal}\,(\hat{L}_i/L_i) : \mathcal{H}(L_i)^{1-e}/N_i\,\mathcal{H}(\hat{L}_i)^{1-e} = (1)$ soit $\mathcal{H}(L_i)^{1-e} = N_i\,\mathcal{H}(\hat{L}_i)^{1-e}$. Comme les normes de la forme $\hat{N}_i$ sont surjectives, on aura $\mathcal{H}(L)^{1-e} = N_{L_\lambda/L}\,\mathcal{H}(L_\lambda)^{1-e}$ et comme de même $\mathcal{H}(L_\lambda) = N_{\mathbb{Q}^{(m)}/L_\lambda}\,\mathcal{H}\big(\mathbb{Q}^{(m)}\big)$, on en déduit $\mathcal{H}(L)^{1-e} \subset N_{\mathbb{Q}^{(m)}/L}\,\mathcal{H}\big(\mathbb{Q}^{(m)}\big)$, d'où le lemme.

Soit alors h une classe de $\mathcal{H}(L)^{1-e}$; soit h' une classe de $\mathbb{Q}^{(m)}$ telle que $N_{\mathbb{Q}^{(m)}/L}\,h' = h$ (lemme IV 5). On sait que l'on peut représenter h' par un idéal premier de degré résiduel 1 dans $\mathbb{Q}^{(m)}/\mathbb{Q}$ que l'on peut choisir premier à m (cf. [11]). Soit $\mathfrak{P}_{\mathbb{Q}^{(m)}}$ cet idéal ; alors posons $\mathfrak{P}_L = N_{\mathbb{Q}^{(m)}/L}\,\mathfrak{P}_{\mathbb{Q}^{(m)}}$; il est clair que $\mathfrak{P}_L$ représente h et est totalement *décomposé* dans $L/\mathbb{Q}$.

Appelons Δ le plus grand sous-groupe d'ordre impair de $G_{\mathbb{Q}^{(m)}}$ (on suppose $\Delta \neq (1)$ sinon le théorème est trivial). Soit e_μ l'idempotent de l'algèbre semi-simple $\mathbb{Z}_2[\Delta]$ associé à un caractère 2-adique irréductible non trivial μ de Δ ; soit r' un caractère de degré 1 divisant μ. On sait que $\mathbb{Z}_2[\Delta]e_\mu$ est isomorphe à l'anneau des entiers $\mathbb{Z}_2^{(g)}$ du corps cyclotomique 2-adique $\mathbb{Q}_2^{(g)}$, g étant l'ordre du caractère r' (l'isomorphisme étant réalisé par l'application $\sigma e_\mu \to r'(\sigma)$ pour tout $\sigma \in \Delta$).

Soit alors a un entier impair premier à m tel que $\sigma_a \in \Delta$ et tel que $r'(\sigma_a) \neq 1$ (ceci est possible puisque r' n'est pas le caractère unité). On sait que $\Omega = \dot{S}_{\mathbb{Q}^{(m)}}\,(\sigma_a - a) \in \mathbb{Z}_2[G_{\mathbb{Q}^{(m)}}]$ (Prop. IV 2) ; montrons que

$(\sigma_a - a)e_\mu$ est inversible dans $\mathbb{Z}_2[\Delta]e_\mu$: il suffit pour cela d'étudier $r'\big((\sigma_a - a)e_\mu\big) = r'(\sigma_a) - a \in \mathbb{Z}_2^{(g)}$; posons $\xi = r'(\sigma_a)$, c'est une racine de l'unité d'ordre non puissance de 2 donc $\xi - a \equiv \xi - 1 \mod 2$ est inversible dans $\mathbb{Z}_2^{(g)}$. Soit ωe_μ l'inverse de $(\sigma_a - a)e_\mu$, $\omega \in \mathbb{Z}_2[\Delta]$; on a donc $(\sigma_a - a)\omega e_\mu = e_\mu$, ce qui fait que l'on a les égalités suivantes dans $\mathbb{Q}_2[G_{\mathbb{Q}}(m)]$:

$$\dot{S}_{\mathbb{Q}(m)} (\sigma_a - a)e_\mu = \Omega e_\mu \text{ , soit}$$

$$\dot{S}_{\mathbb{Q}(m)} (\sigma_a - a)\omega e_\mu = \Omega\omega e_\mu \text{ , soit}$$

$$\dot{S}_{\mathbb{Q}(m)} e_\mu = \Omega\omega e_\mu \text{ ; or } \Omega\omega e_\mu \in \mathbb{Z}_2[G_{\mathbb{Q}}(m)] \text{ ce qui prouve que}$$

$\dot{S}_{\mathbb{Q}(m)} e_\mu$ est entier pour tout $\mu \neq 1$. Par sommation et en remarquant que $\sum_{\mu \neq 1} e_\mu = 1 - E$, $E = \frac{1}{|\Delta|} \sum_{s \in \Delta} s$, on a $\dot{S}_{\mathbb{Q}(m)} (1 - E) \in \mathbb{Z}_2[G_{\mathbb{Q}}(m)]$. L'élément $\dot{S}_{\mathbb{Q}(m)} (1 - E)$ étant orthogonal à $1 + \sigma_{-1}$, il en résulte qu'il existe $\dot{T}'_{\mathbb{Q}}(m) \in \mathbb{Z}_2[G_{\mathbb{Q}}(m)]$ tel que $\dot{S}_{\mathbb{Q}(m)} (1 - E) = \dot{T}'_{\mathbb{Q}}(m) (1 - \sigma_{-1})$ (on vérifie facilement que l'on a $\dot{T}'_{\mathbb{Q}}(m) \equiv \dot{T}_{\mathbb{Q}}(m) (1 - E) \mod (1 + \sigma_{-1})\, \mathbb{Q}_2[G_{\mathbb{Q}}(m)]$, $\dot{T}_{\mathbb{Q}}(m)$ étant l'élément défini dans le lemme IV 3). Il convient maintenant de supposer que m est le conducteur de L ; alors par projection de cette égalité dans $\mathbb{Q}_2[G_L]$, compte tenu du fait que $1 - E$ a pour image $1 - e$, que $\dot{S}_{\mathbb{Q}(m)}$ a pour image $\dot{S}_L$, on a donc prouvé l'existence d'un élément $\dot{T}'_L \in \mathbb{Z}_2[G_L]$ tel que $\dot{T}'_L\left(1 - \left(\frac{L}{-1}\right)\right) = \dot{S}_L(1 - e)$. Montrons pour terminer que $\dot{T}'_L$ a la propriété d'annulation cherchée.

En utilisant les arguments de la proposition IV 3 (dans $\mathbb{Q}^{(m)}$ et pour l'élément $\omega = 1 - E$), on peut écrire :

$$\mathfrak{P}_{\mathbb{Q}^{(m)}}^{\dot{T}'_{\mathbb{Q}^{(m)}}} = \Theta A_{\mathbb{Q}^{(m)}}\mathfrak{A}\ ,\ \Theta \in \mathbb{Q}^{(m)}\ ,\ \mathfrak{A}\ \text{idéal invariant par}\ \left\{1,\ \sigma_{-1}\right\}\ ;$$

comme $\mathbb{Q}^{(m)}/\mathbb{Q}_+^{(m)}$ est non ramifiée pour les idéaux, il en résulte que $\mathfrak{A}$ est l'étendu d'un idéal de $\mathbb{Q}_+^{(m)}$: $\mathfrak{A}_+$.

D'après ce qui précède et du fait que $\tau(L)$ est ici égale à $\nu'_{\mathbb{Q}^{(m)}/L}\,\tau\left(\mathbb{Q}^{(m)}\right)$ on obtient par $N_{\mathbb{Q}^{(m)}/L}$:

$$\mathfrak{P}_L^{\dot{T}'_L} = \Theta A_L\,\mathfrak{a}_+\ ,\ \Theta = N_{\mathbb{Q}^{(m)}/L}\,\Theta \in L \text{ et } \mathfrak{a}_+ = N_{\mathbb{Q}^{(m)}/L}\,\mathfrak{A}_+ \text{ est l'étendu}$$

d'un idéal de L_+. Comme $\mathfrak{P}_L$ représente la classe $h \in \mathcal{H}(L)^{1-e}$ le théorème en résulte.

Remarque IV3. (i) En pratique, l'élément $\dot{T}'_L$ s'obtient à partir de $\dot{S}_L$ par "division" de $\dot{S}_L(1-e)$ par $1-\left(\frac{L}{-1}\right)$ dans $\mathbb{Z}_2[G_L]$.

(ii) Si $\dot{S}_L$ est entier, alors $\dot{S}_L = \dot{T}_L\left(1-\left(\frac{L}{-1}\right)\right)$, $\dot{T}_L \in \mathbb{Z}[G_L]$, et on peut prendre $\dot{T}'_L = \dot{T}_L$; c'est bien un élément annulant $\mathcal{H}(L)^{1-e}/j_{L/L_+}\,\mathcal{H}(L_+)^{1-e}$.

Montrons que ce résultat est d'une certaine manière en rapport avec une conjecture que nous avons formulée dans [5] (p. 69) au sujet de l'annulation des classes d'idéaux.

Pour éviter toute confusion de notations avec ce qui a précédé dans la théorie des sommes de GAUSS, nous changeons certaines des notations en usage dans [5] de la façon suivante : On appelle ρ' un caractère de degré 1 de Gal $(\mathbb{Q}^a/\mathbb{Q})$ (où $\mathbb{Q}^a$ est l'extension abélienne maximale de $\mathbb{Q}$ contenue dans une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$) ; on appelle ρ le caractère rationnel au-dessus de ρ' et on désigne par ϕ le carac-

tère ℓ-adique au-dessus de ρ' (ℓ nombre premier fixé) ; on sait qu'à ρ correspond l'extension cyclique K_ρ de degré g_ρ égal à l'ordre de ρ'. On appelle enfin G_ρ, f_ρ le groupe Gal $(K_\rho/\mathbb{Q})$ et le conducteur de K_ρ.

On suppose ici $\ell = 2$ et ρ impair (i. e. K_ρ imaginaire). On a défini dans [5] (Déf. II 8) les invariants analytiques $m_\emptyset(h)$ de la façon suivante (où $\rho'|\emptyset$ et où $\hat{\mathfrak{p}}_\rho$ désigne l'idéal maximal de $\mathbb{Z}_2^{(g_\rho)}$) :

Définition IV 2. On pose :

(i) $\frac{1}{2} B_1(\rho'^{-1}) \mathbb{Z}_2^{(g_\rho)} = \hat{\mathfrak{p}}_\rho^{m_\emptyset(h)}$, si g_ρ n'est pas une puissance de 2,

(ii) $\frac{1}{2} B_1(\rho'^{-1}) \mathbb{Z}_2^{(g_\rho)} = \hat{\mathfrak{p}}_\rho^{m_\emptyset(h)-1}$, si g_ρ est puissance de 2 avec $K_\rho \neq \mathbb{Q}^{(4)}$,

(iii) $m_\emptyset(h) = 0$ si $K_\rho = \mathbb{Q}^{(4)}$.

Ici $B_1(\rho'^{-1})$ désigne le nombre de BERNOULLI généralisé associé au caractère ρ'. On a donc $\frac{1}{2} B_1(\rho'^{-1}) = \rho'(\dot{T}_{K_\rho})$.

Dans [6] (§11, 2, b, α) nous avons défini la notion de caractère modéré associé à un caractère, de la façon suivante : on écrit $\rho' = r'\gamma'$ (γ' d'ordre puissance de ℓ ($\ell = 2$ ici) et r' d'ordre premier à ℓ) ; soient μ le caractère ℓ-adique au-dessus de r' et r le caractère rationnel au-dessus de r', alors les caractères r', μ, r sont appelés respectivement les caractères modérés de degré 1, ℓ-adique et rationnel associés respectivement à ρ', $\emptyset$ et ρ.

Avec ces notations et en appelant $\mathcal{H}^-(K_\rho)$ le sous-groupe des classes relatives de $\mathcal{H}(K_\rho)$ on a $\mathcal{H}_\emptyset = \mathcal{H}^-(K_\rho)^{e_\mu}$ (la μ-composante de $\mathcal{H}^-(K_\rho)$). La conjecture formulée dans [5] (p. 69) est que $\hat{\mathfrak{p}}_\rho^{m_\emptyset(h)}$ annule

le $\mathbb{Z}_2^{(g_\rho)}$-module $\mathcal{H}_\emptyset$.

On a la suite :

$$1 \to \mathcal{H}^-(K_\rho) \to \mathcal{H}(K_\rho) \xrightarrow{N_{K_\rho/K_{\rho_+}}} \mathcal{H}(K_{\rho_+}) \to 1$$

qui est exacte ; en effet, la norme $N_{K_\rho/K_{\rho_+}}$ est surjective car K_ρ/K_{ρ_+} est ramifiée pour les places à l'infini. Il en résulte que l'on a les suites exactes :

$$1 \to \mathcal{H}_\emptyset \to \mathcal{H}(K_\rho)^{e_\mu} \to \mathcal{H}(K_{\rho_+})^{e_\mu} \to 1$$

ce qui fait que $|\mathcal{H}_\emptyset| = \dfrac{|\mathcal{H}(K_\rho)^{e_\mu}|}{|\mathcal{H}(K_{\rho_+})^{e_\mu}|}$; le module $\mathcal{H}(K_{\rho_+})$ s'identifie à $j_{K_\rho/K_{\rho_+}}\mathcal{H}(K_{\rho_+}) \subset \mathcal{H}(K_\rho)$ (où $j_{K_\rho/K_{\rho_+}}$ désigne l'extension des classes dans K_ρ/K_{ρ_+}) ; en effet $j_{K_\rho/K_{\rho_+}}$ est injectif ici ([5], Prop. III, p. 28) car $K_\rho/\mathbb{Q}$ est cyclique.

Ainsi $\mathcal{H}_\emptyset$ et $\mathcal{H}(K_\rho)^{e_\mu}/j_{K_\rho/K_{\rho_+}}\mathcal{H}(K_{\rho_+})^{e_\mu}$ ont même ordre mais ne sont pas nécessairement isomorphes ; on a donc obtenu (le cas $\mu = 1$ qui correspond à la μ-composante $\mathcal{H}(K_\rho)^e$ de $\mathcal{H}(K_\rho)$ étant contenu dans le th. III 1 de [6]) et en considérant les modules ci-dessus comme des $\mathbb{Z}_2^{(g_\rho)}$-modules :

Théorème IV 1'. Pour tout caractère 2-adique $\emptyset$ impair de caractère modéré associé μ, $\hat{p}_\rho^{m_\emptyset(h)}$ annule $\mathcal{H}(K_\rho)^{e_\mu}/j_{K_\rho/K_{\rho_+}}\mathcal{H}(K_{\rho_+})^{e_\mu}$, où $m_\emptyset(h)$ est

l'invariant analytique (Déf. IV 2) défini au moyen du demi nombre de Bernoulli généralisé $\frac{1}{2} B_1(\rho'^{-1})$.

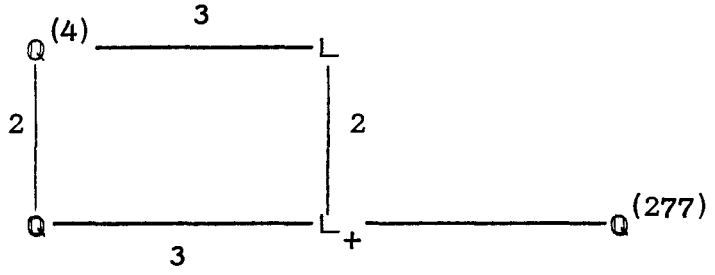
Remarque IV 4. Le résultat précédent ne permet pas d'affirmer que $\mathcal{H}_\phi$ est annulé par $\hat{p}_\rho^{m_\phi(h)}$; on peut cependant obtenir ce résultat conjectural dans des cas particuliers ; par exemple :

Corollaire IV 3. Si la μ-composante de $\mathcal{H}(K_{\rho_+})$ est triviale alors $\hat{p}_\rho^{m_\phi(h)}$ annule $\mathcal{H}_\phi$.

Ce corollaire améliore le th. III 1 de [6] comme on peut le voir en prenant pour K_ρ le corps $\mathbb{Q}^{(29)}$: On vérifie que $\mathcal{H}(K_{\rho_+})$ est trivial (ainsi le corollaire précédent s'applique pour les deux caractères 2-adiques ϕ et $\overline{\phi}$ divisant ρ) ; mais les hypothèses du th. III 1 de [6] ne sont pas toutes vérifiées (il y a dans K_{ρ_+} des unités totalement positives non triviales, ce qui fait d'ailleurs que l'on a $|\mathcal{H}_\phi| = 2^3$ et $|\mathcal{H}_{\overline{\phi}}| = 1$ (cf. [6], Rem. IV 3)). Donnons maintenant deux exemples numériques pour illustrer les résultats précédents.

a) Exemple 1. Corps de degré 6 de conducteur 4 x 277.

On a le schéma suivant :



On rappelle les informations numériques suivantes : on a $|\mathcal{H}(L_+)| = 4$ et la classe de l'idéal $\mathfrak{p}_2$ de L_+ au-dessus de 2 engendre $\mathcal{H}(L_+)$ ([7], [8], p. 96) ; 2 est ramifié dans L/L_+ et est totalement décom-

posé dans $L_+/\mathbb{Q}$; les seules unités totalement positives de L_+ sont les carrés d'unités ([8], p. 96).

La formule des classes ambiges dans L/L_+ donne donc ici :

$|\mathcal{H}_1| = 16$ (cf. par exemple [6], §1).

Un calcul direct de $\dot{S}_L$ donne :

$\dot{S}_L = 4(1-\sigma^3)(\sigma^2+\sigma)$ soit $\dot{T}_L = 4(\sigma^2+\sigma)$ (σ engendrant Gal $(L/\mathbb{Q})$) ; le calcul des nombres de BERNOULLI correspondants montre immédiatement que le nombre de 2-classes relatives $\mathcal{H}^-$ de L est :

$|\mathcal{H}^-| = 16$ (on a de façon évidente $\mathcal{H}^- = \mathcal{H}_\emptyset$ ici).

En tant que $\mathbb{Z}_2^{(3)}$-module (obtenu par l'homomorphisme $\sigma \to -j$) $\mathcal{H}^-$ est isomorphe soit à $\mathbb{Z}_2^{(3)}/(4)$ soit à $\mathbb{Z}_2^{(3)}/(2) \times \mathbb{Z}_2^{(3)}/(2)$.

De même $\mathcal{H}_1$ peut être considéré comme un module sur $\mathbb{Z}_2^{(3)}$ (par l'homomorphisme $\sigma \to j$) et $\mathcal{H}_1$ est isomorphe soit à $\mathbb{Z}_2^{(3)}/(4)$ soit à $\mathbb{Z}_2^{(3)}/(2) \times \mathbb{Z}_2^{(3)}/(2)$.

Considérons l'idéal premier $\mathfrak{P}_2$ au-dessus de p_2 dans L. Comme $p_2 A_L = \mathfrak{P}_2^2$, il en résulte que $cl_L(\mathfrak{P}_2)^2 = cl_L(p_2 A_L) = j_{L/L_+} h_o$ où h_o est la classe $cl_{L_+}(p_2)$ d'ordre 2 ; ceci fait que $h = cl_L(\mathfrak{P}_2)$ est d'ordre 4 (on sait que j_{L/L_+} est injectif). Or $h \in \mathcal{H}_1$ d'où nécessairement :

$$\mathcal{H}_1 \simeq \mathbb{Z}_2^{(3)}/(4) .$$

Appelons $\mathcal{H}_1^{(2)}$ et $\mathcal{H}^{-(2)}$ les classes ambiges et relatives de L annulées par 2. On a $\mathcal{H}_1^{(2)} = \mathcal{H}^{-(2)} = \mathcal{H}_1 \cap \mathcal{H}^-$ (en effet, si $h \in \mathcal{H}_1 \cap \mathcal{H}^-$ alors $h^{1-\sigma_{-1}} = h^{1+\sigma_{-1}} = 1$ et si $h \in \mathcal{H}_1^{(2)}$ alors $h \in \mathcal{H}^{-(2)}$ et inversement ; on a d'ailleurs $\mathcal{H}_1 \cap \mathcal{H}^- = j_{L/L_+}\mathcal{H}(L_+)$). Il en résulte que le 2-rang de $\mathcal{H}^{-(2)}$

est 2 c'est-à-dire que nécessairement :

$$\mathcal{H}^- \simeq \mathbb{Z}_2^{(3)}/(4).$$

Considérons maintenant le groupe $\mathcal{H}_1\,\mathcal{H}^-$: on a $|\mathcal{H}_1\,\mathcal{H}^-| = \dfrac{|\mathcal{H}_1|\,|\mathcal{H}^-|}{|\mathcal{H}_1 \cap \mathcal{H}^-|} = 64$; d'où $\mathcal{H}(L) = \mathcal{H}_1\,\mathcal{H}^-$. On a alors $\mathcal{H}(L)^2 = \mathcal{H}_1^2\,(\mathcal{H}^-)^2$ soit, d'après ce que l'on a dit ci-dessus sur les structures de $\mathcal{H}_1$ et $\mathcal{H}^-$, $\mathcal{H}(L)^2 = j_{L/L_+}\mathcal{H}(L_+)$. On a donc démontré que :

(i) le module $\mathcal{H}(L)/j_{L/L_+}\mathcal{H}(L_+)$ est d'exposant 2,

(ii) le module $\mathcal{H}^-$ est d'exposant 4.

Ceci illustre le fait que l'on peut avoir un annulateur pour $\mathcal{H}^-$ strictement supérieur à celui de $\mathcal{H}(L)/j_{L/L_+}\mathcal{H}(L_+)$ (cf. Rem. IV 4). On remarque que dans cet exemple, on a $\mathcal{H}(L)^{1-\sigma_{-1}} = (\mathcal{H}^-)^{1-\sigma_{-1}} = (\mathcal{H}^-)^2$, ce qui fait que $\mathcal{H}(L)^{1-\sigma_{-1}}$ est d'exposant moitié de celui de $\mathcal{H}^-$. Il est de toute façon facile de montrer que l'on a les inégalités suivantes (pour tout corps L imaginaire cyclique sur $\mathbb{Q}$) :

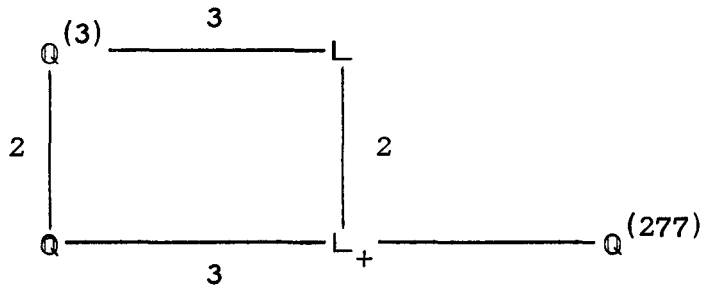
$$\mathrm{Exp}\left(\mathcal{H}(L)^{1-\sigma_{-1}}\right) \leq \mathrm{Exp}\left(\mathcal{H}(L)^-\right) \leq 2\,\mathrm{Exp}\left(\mathcal{H}(L)^{1-\sigma_{-1}}\right)$$

$$\mathrm{Exp}\left(\mathcal{H}(L)^{1-\sigma_{-1}}\right) \leq \mathrm{Exp}\left(\mathcal{H}(L)/j_{L/L_+}\mathcal{H}(L_+)\right) \leq 2\,\mathrm{Exp}\left(\mathcal{H}(L)^{1-\sigma_{-1}}\right),$$

où Exp désigne l'exposant d'un groupe.

b) <u>Exemple</u> 2. Corps de degré 6 de conducteur 3 x 277.

On a le schéma :



Ici 3 est inerte dans $L_+/\mathbb{Q}$ et ramifié dans L/L_+. La formule des classes ambiges dans L/L_+ donne ici :

$|\mathcal{H}_1| = 4$; on a donc $\mathcal{H}_1 \simeq \mathbb{Z}_2^{(3)}/(2)$.

Le calcul de $\dot{S}_L$ donne $\dot{S}_L = 4(1-\sigma^3)(\sigma^2+2\sigma+1)$, ce qui conduit à $|\mathcal{H}^-| = 16$ et $|\mathcal{H}(L)| = 64$. Comme dans l'exemple 1, on a $\mathcal{H}^- \cap \mathcal{H}_1 = (\mathcal{H}^-)^{(2)} = \mathcal{H}_1^{(2)} = j_{L/L_+}\left(\mathcal{H}(L_+)\right)$ ce qui fait que l'on a :

$$\mathcal{H}^- \simeq \mathbb{Z}_2^{(3)}/(4).$$

On sait que dans cet exemple on peut affirmer que $\mathcal{H}^- = \mathcal{H}(L)^{1-\sigma_{-1}}$ (cf. [6], §III, 2, ou voir directement que cette propriété provient du fait que $\mathcal{H}_1 = j_{L/L_+}\mathcal{H}(L_+)$). Soit alors h^* un élément d'ordre 4 de $\mathcal{H}^-$ et soit $h \in \mathcal{H}(L)$ telle que $h^* = h^{1-\sigma_{-1}}$; montrons que h est d'ordre 8 et engendre $\mathcal{H}(L)$:

Si on avait $h^4 = 1$, on aurait $h^{2(1-\sigma_{-1})} = h^{*2}$ qui serait une classe réelle d'ordre 2 ; mais $h^{2(1-\sigma_{-1})} = h^{2(1+\sigma_{-1})}$ puisque $h^4 = 1$, d'où $h^{*2} = 1$ car $h^{1+\sigma_{-1}}$ est une classe réelle d'ordre 2 au plus, ce qui est absurde. Donc h est d'ordre 8. Montrons que les groupes engendrés par h et h^σ ont une intersection réduite à 1 : si $h^a = h^{b\sigma}$, alors $a = 2^k x$, $b = 2^k y$, $x, y \in \{1, 3, 5, 7\}$, $0 \le k \le 3$. En posant $h' = h^{2^k y}$, on peut écrire $h'^\sigma = h'^z$, $z \in \{1, 3, 5, 7\}$ et $h'^{\sigma^2} = h'^{z^2} = h'$; donc h'

est ambige dans $L/\mathbb{Q}$[3] donc nécessairement $h' = 1$, soit $a \equiv b \equiv 0 \bmod 8$. Donc h engendre $\mathcal{H}(L)$. On a $\mathcal{H}(L)/j_{L/L_+}\mathcal{H}(L_+)$ qui est d'exposant 4 ainsi que $\mathcal{H}^-$.

On rappelle que $\dot{T}_L = 4(\sigma^2+2\sigma+1)$, donc l'exemple 2 illustre le fait que $\dot{T}_L$ annule bien $\mathcal{H}^-$ et $\mathcal{H}(L)/j_{L/L_+}\mathcal{H}(L_+)$ mais n'annule pas $\mathcal{H}(L)$ en entier. On remarque aussi sur cet exemple que $\mathcal{H}(L)^{\dot{T}_L}$ est engendré par $h^{\dot{T}_L} = h^{4(\sigma^2+2\sigma+1)}$; or h^4 est une classe d'ordre 2, h_o, telle que $h_o^{1-\sigma^{-1}} \in (\mathcal{H}^-)^4 = (1)$ donc h_o est réelle et non triviale ; comme $h_o^{\sigma^2+2\sigma+1} = h_o^{\sigma}$, ceci prouve que le th. IV1 (ou le th. IV1') ne peut être amélioré en général.

Conclusion. On constate que le théorème IV1' peut constituer un point de départ de l'étude de la conjecture "$\hat{p}_\rho^{m_\emptyset(h)}$ annule $\mathcal{H}_\emptyset$". Des résultats dans cette direction, que nous venons d'obtenir, seront publiés ultérieurement.

3) Autres résultats sur l'annulation des classes d'idéaux des extensions abéliennes imaginaires de $\mathbb{Q}$.

Soit L une extension abélienne imaginaire de $\mathbb{Q}$ et soit K un sous-corps de L tel que L/K soit cyclique et pour lequel la projection canonique $W_{L/K}$ de $W'_{L/K}$ dans $\mathbb{Z}[G_K]$ soit nulle (cas où il existe un nombre premier ℓ divisant m_L et non m_K et totalement décomposé dans $\overline{K}$) ; si l'on veut que cette condition soit indépendante du choix de p, on fait l'hypothèse suivante qui entraîne encore $W_{L/K} = 0$: on suppose que ℓ est un nombre premier qui divise m_L et non m_K et qui est totalement décomposé dans K. On a alors (th. III 2) pour tout $\omega' \in \mathbb{Z}[G'_L]$ tel que $\tau(L)^{\omega'}$ et $\tau(K)^{\omega'}$ soient dans $\overline{L}$ et $\overline{K}$ respectivement :

$\nu_{\overline{L}/\overline{K}}\left(\tau(L)^{\omega'}\right) = \xi_{L/K}^{\omega'}$ soit encore $\nu_{L/K}\left(\tau(L)^{\omega'}\right) = \xi'_{L/K}$, $\xi'_{L/K}$ racine

de l'unité égale à la puissance $\left(\lambda_L/\lambda_K\right)^{\text{eme}}$ de $\xi^{\omega'}_{L/K}$; or $\xi^{\lambda_L/\lambda_K}_{L/K}$ est annulée par n_L/λ_L (qui est le degré résiduel de p dans $\mathbb{Q}^{(m_L)}/L$) ainsi que par $p-1$ (cf. th. III 2).

Soit a un entier fixé impair premier à m_L ; on sait que $\left(\left(\frac{L}{a}\right)-a\right)\dot{S}_L$ est dans $\mathbb{Z}[G_L]$ et par conséquent (lemme IV 1, (i)) $\tau(L)^{\left(\frac{L'}{a}\right)-a} A_{\overline{L}} = \mathfrak{P}_{\overline{L}}^{\left(\left(\frac{L}{a}\right)-a\right)\dot{S}_L}$ dans $\overline{L}$. On a $\nu_{L/K}\left(\tau(L)^{\left(\frac{L'}{a}\right)-a}\right) = \xi_{L/K}^{\left(\frac{L'}{a}\right)-a} = \xi_{L/K}^{a-a} = 1$. Supposons alors l'extension L/K cyclique et appliquons le théorème 90 de HILBERT : il existe $\theta \in L$ tel que $\tau(L)^{\left(\frac{L'}{a}\right)-a} = \theta^{\sigma_{L/K}-1}$, où $\sigma_{L/K}$ est un générateur de Gal (L/K). Puisque d'après [5] (Th. II 3, (iii)) on a aussi dans $\mathbb{Z}[G_L]$, $N_{L/K}\left(\dot{S}_L\left(\left(\frac{L}{a}\right)-a\right)\right) = 0$ (grâce à l'hypothèse $W_{L/K} = 0$), on en déduit que $\dot{S}_L\left(\left(\frac{L}{a}\right)-a\right) = \left(\sigma_{L/K}-1\right)\dot{T}^a_{L/K}$ où $\dot{T}^a_{L/K} \in \mathbb{Q}[G_L]$ est défini modulo $\nu_{L/K}$. On a donc :

$$\mathfrak{P}_L^{\left(\left(\frac{L}{a}\right)-a\right)\dot{S}_L} = \theta^{\sigma_{L/K}-1} A_L = \mathfrak{P}_L^{\left(\sigma_{L/K}-1\right)\dot{T}^a_{L/K}} \text{ et}$$

$$\mathfrak{P}_L^{\dot{T}^a_{L/K}} = \theta A_L \mathfrak{a}_{L/K} \text{ où } \mathfrak{a}_{L/K} \text{ est un idéal de L invariant dans L/K.}$$

On a donc prouvé dans ce cas :

Proposition IV 4. Soit L une extension abélienne imaginaire et soit K un sous-corps imaginaire de L tel que L/K soit cyclique et tel qu'il existe un diviseur premier ℓ de m_L ne divisant pas m_K et totalement décomposé

dans K. Soit $\mathbb{H}(L)$ le groupe des classes de L et soit $\mathbb{H}_1^0(L/K)$ le sous-groupe de $\mathbb{H}(L)$ formé des classes des idéaux invariants dans L/K. Alors pour tout a , $(a, m_L) = 1$, a choisi impair, l'élément $\dot{T}^a_{L/K}$ défini par $\dot{S}_L\left(\left(\frac{L}{a}\right) - a\right) = \dot{T}^a_{L/K}\left(\sigma_{L/K} - 1\right)$ dans $\mathbb{Z}[G_L]$, annule le module $\mathbb{H}(L)/\mathbb{H}_1^0(L/K)$.

Remarque IV 5. Si $\dot{S}_L$ est entier, alors on peut prendre $\dot{T}^a_L = \left(\left(\frac{L}{a}\right) - a\right)\dot{T}_L$ $\left(\dot{T}_L \in \mathbb{Z}[G_L]\right)$.

Remarque IV 6. On remarque dans l'énoncé de la proposition IV 4 que les ω utilisés tels que $\omega \dot{S}_L$ soit entier sont les $\left(\frac{L}{a}\right) - a$ de $\dot{\mathfrak{A}}_K$ et $\dot{\Lambda}_K$ n'est pas cité : en effet on n'a pas nécessairement $\xi_{L/K}^{\dot{\Lambda}_K} = 1$ comme le montre l'exemple du chap. III, §3 (Rem. III 2) : pour le corps L_1 , $\xi_{L_1/K}$ sera une racine de l'unité d'ordre 3, mais on vérifie facilement (calcul direct ou utilisation de la Prop. II 5 de [5]) que $\dot{S}_{L_1}$ est entier donc que $\dot{\Lambda}_{L_1} = 1$. On ne peut donc pas améliorer la proposition dans ce sens, sauf peut-être dans des cas particuliers.

Donnons maintenant un exemple numérique illustrant la proposition précédente.

Soit L le composé de $\mathbb{Q}_+^{(7)}$ avec le corps $\mathbb{Q}(\sqrt{-31})$ et soit $K = \mathbb{Q}(\sqrt{-31})$; on a $m_L = 31 \times 7$ et $m_K = 31$. On vérifie que 7 est totalement décomposé dans K. On obtient :

$\dot{S}_L = 1 - \sigma^2 - \sigma^3 + \sigma^5 = \left(\sigma^2 - 1\right)\left(\sigma^3 - 1\right)$, avec $\sigma = \left(\frac{L}{3}\right)$.

Si on prend a = 3, d'après la proposition IV 4,

$\dot{T}^a_{L/K} = \left(\sigma - 3\right)\left(\sigma^3 - 1\right)$ annule le module $\mathbb{H}(L)/\mathbb{H}_1^0(L/K)$. Plaçons-nous

au niveau des 3-groupes de SYLOW. Un calcul direct (formule analytique pour les classes relatives) donne :

$$|\text{Ш}(K)| = 3 ,$$

$$|\text{Ш}(L)| = 9$$

(si on appelle ρ le caractère rationnel associé à L, alors $|\text{Ш}_\rho| = 3$). Comme ici $\text{Ш}^0_1(L/K) = \text{Ш}_1(L/K)$, l'application de la formule des classes ambiges donne $|\text{Ш}_1(L/K)| = 9$; on a donc $\text{Ш}(L) = \text{Ш}_1(L/K)$. Comme ici $\text{Ш}(L)$ est formé de classes relatives, on peut considérer $\text{Ш}(L)/\text{Ш}_1(L)$ $\left(\text{ainsi que } \text{Ш}(L)/j_{L/K}\text{Ш}(K)\right)$ comme des $\mathbb{Z}_3^{(3)}$-modules (par l'homomorphisme $\sigma \to -j$) car ils sont annulés par $1+\sigma^2+\sigma^4$ et $1+\sigma^3$; or l'image de $\left(\sigma-3\right)\left(\sigma^3-1\right)$ par cet homomorphisme est inversible dans $\mathbb{Z}_3^{(3)}$; ainsi on retrouve l'égalité $\text{Ш}(L) = \text{Ш}_1(L)$ mais $\left(\sigma-3\right)\left(\sigma^3-1\right)$ n'annule pas le module $\text{Ш}(L)/j_{L/K}\text{Ш}(K)$ qui est d'ordre 3. Ceci montre en particulier que l'on ne peut espérer une situation analogue à celle du théorème IV 1 où l'on aurait $\dot{T}^a_{L/K}(1-e)$ annule $\text{Ш}(L)^{1-e}/j_{L/K}\text{Ш}(K)^{1-e}$ (e ayant une définition analogue mais relativement aux 3-composantes) ; autrement dit, dans l'écriture $\mathfrak{P}_L^{\dot{T}^a_{L/K}} = \theta A_L\, \mathfrak{a}_{L/K}$, l'idéal $\mathfrak{a}_{L/K}$ (invariant dans L/K) n'est pas nécessairement équivalent à un idéal de K étendu et peut faire intervenir "effectivement" les idéaux ramifiés dans L/K.

BIBLIOGRAPHIE

[1] Coates J., p-adic L-functions and Iwasawa's theory, Durham symposium in algebraic number theory, Academic Press (1977).

[2] Davenport H., Hasse H., Die Nullstellen der Kongruenzzeta-funktionen in gewissen zyklischen Fällen, J. reine ang. Math., 172 (1935), 151-182.

[3] Fröhlich A., Stickelberger without Gauss sums, Durham symposium in algebraic number theory, Academic Press (1977).

[4] Gillard R., Relations de Stickelberger, Séminaire de théorie des nombres (1974), Grenoble.

[5] Gras G., Application de la notion de φ-objet à l'étude du groupe des classes d'idéaux des extensions abéliennes, Publ. math. Univ. Besançon (1975-76), Fasc 2.

[6] Gras G., Nombre de φ-classes invariantes - Application aux classes des corps abéliens, Bull. Soc. Math. de France, 106 (1978) (à paraître).

[7] Gras M.-N., Sur le nombre de classes du sous-corps cubique de $\mathbb{Q}^{(p)}\left(p \equiv 1\ (3)\right)$, thèse de 3^e cycle, Grenoble (1971).

[8] Gras M.-N., Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$, Jour. für die reine und angew. Math. 277 (1975), 89-116.

[9] Hasse H., Artinsche Führer, Artinsche L-Funktionen und Gausssche Summen über endlich-algebraischen Zahlkörpern, Acta Salmanticensia, Mathematicas, IV, (1954).

[10] Lamprecht E., Allgemeine Theorie der Gaussschen Summen in endlichen kommutativen Ringen, Math. Nachr. 9 (1953), 149-196.

[11] Lang S., Algebraic Number theory, Addison-Wesley Publ. (1970).

[12] Leopoldt H.-W., Zur Arithmetik in abelschen Zahlkörpern J. reine Angew. Math., 209 (1962), 54-71.

[13] Martinet J., Character theory and Artin L-functions, Durham symposium in algebraic number theory, Academic Press (1977).

[14] Narkiewicz W., Elementary and analytic Theory of algebraic Numbers, P.W.N., Warszawa (1974).

[15] Schmidt C.-G., Über gausssche Summen als Grössencharaktere und Kreiseinheiten sowie derem beziehungen untereinander, Dissertation, Univ. Karlsruhe (1977).

[16] Stickelberger L., Über eine Verallgemeinerung der Kreisteilung, Math. Ann. 37 (1890), 321-367.