SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

ROLAND GILLARD

Relations de Stickelberger

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 1, p. 1-10

<http://www.numdam.org/item?id=STNG_1974-1975__4__A1_0>

RELATIONS DE STICKELBERGER

par

Roland GILLARD

Il s'agit de relations dans le groupe des classes d'idéaux d'une extension abélienne de $\mathbb{Q}$ (cf. th. 2 ci-dessous).

I - SOMMES DE GAUSS.

Notations :

- p nombre premier
- f entier strictement positif ; $q = p^f$
- ω racine primitive de 1 d'ordre p
- W_{q-1} groupe des racines de 1 d'ordre divisant $q-1$
- L le corps $\mathbb{Q}(\omega, W_{q-1})$
- A l'anneau des entiers de L
- $\mathfrak{P}$ un idéal premier de A au-dessus de p
- φ l'homomorphisme $A \to A/\mathfrak{P} = F$
- T la trace de F à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
- χ homomorphisme de F^* dans W_{q-1} prolongé par $\chi(0) = 0$
- χ_1 l'homomorphisme du type précédent qui vérifie : $\forall a \in F^*$, $\varphi \circ \chi_1(a) = a^{-1}$
- χ_o l'homomorphisme trivial $F^* \to W_{q-1}$.

Pour tout x dans F on notera $\omega^{T(x)}$ le nombre ω^n avec $n \in \mathbb{Z}$, $\varphi(n) = T(x)$; ce nombre ne dépend pas de l'élément n choisi puisque $\omega^p = 1$.

A χ on associera la somme de Gauss :

$$\boxed{\tau(\chi) = \sum_{x \in F} \chi(x)\omega^{T(x)}} \quad .$$

Il est clair qu'une telle somme est dans A . Le lemme 1 montre des propriétés multiplicatives de τ :

LEMME 1. On a les relations suivantes :

i) si $\chi \neq \chi_o$, $\tau(\chi)\tau(\chi^{-1}) = \chi(-1)q$

ii) $\forall r \in \mathbb{N}$, $\tau(\chi^{p^r}) = \tau(\chi)$

iii) si χ et χ' sont dans $\mathrm{Hom}(F^*, W_{q-1})$ et si $\chi.\chi' \neq \chi_o$:

$$\tau(\chi)\tau(\chi') = \left[\sum_{x \in F} \chi(x)\chi'(1-x) \right] \tau(\chi\chi') \quad .$$

Démonstration : Posons $\lambda(x) = \omega^{T(x)}$.

i) On calcule de deux façons différentes l'expression suivante, fonction de z , élément de F :

$$A(z) = \sum_{x,y \in F} \chi(x)\lambda(yx)\lambda(zy) = \sum_{x,y \in F} \chi(x)\lambda(y(x+z)) \quad .$$

Le changement de x en $x-z$ dans la sommation donne :

$$A(z) = \sum_{x,y} \chi(x-z) \sum_{y} \lambda(yx) \quad .$$

Pour $x \neq 0$ la somme en y est nulle, pour $x = 0$ elle vaut q :

$$A(z) = q.\chi(-z) \quad .$$

On peut aussi commencer par évaluer $B(y)$ (pour y dans F) défini par

$$B(y) = \sum_{x} \chi(x)\lambda(yx) \quad .$$

$B(0)$ est nul. Si y est non nul, on peut faire le changement de sommation défini par $t = xy$ on trouve immédiatement

$$B(y) = \chi^{-1}(y)\tau(\chi)$$

cette formule est encore valide pour $y = 0$ puisqu'on a posé $\chi^{-1}(0) = 0$ Ainsi :

$$A(z) = \sum_{y \in F} \chi^{-1}(y)\ \tau(\chi)\lambda(zy) = \tau(\chi) \sum_{y \in F} \chi^{-1}(y)\lambda(zy) \quad .$$

Un calcul analogue à celui fait pour $B(y)$ donne donc :

$$A(z) = \tau(\chi)\ \tau(\chi^{-1})\ \chi(z) \quad .$$

La formule de i) en résulte en faisant $z = 1$.

ii) La fonction de F sur lui-même définie par $x \to x^{p^r}$ est est un automorphisme et $T(x) = T(x^{p^r})$. La formule de ii) résulte du changement de sommation correspondant.

iii) Transformons le produit $\tau(\chi)\tau(\chi')$ par un changement de sommation :

$$\tau(\chi)\tau(\chi') = \sum_{xy} \chi(x)\chi'(y)\,\lambda(x+y)$$
$$= \sum_{xy} \chi(x)\,\chi'(y-x)\lambda(y) \quad .$$

Comme $\chi\chi' \neq \chi_o$ la somme sur x relative à $y = 0$ est nulle. Pour les autres valeurs de y , on fait le changement de sommation défini par $x = yt$.

$$\tau(\chi)\,\tau(\chi') = \sum_{y\in F^*} \sum_{x} \chi(xy)\;\chi'(y-xy)\;\lambda(y)$$
$$= \Big[\sum_{x} \chi(x)\chi'(1-x)\Big]\Big[\sum_{y\in F} (\chi\chi')(y)\lambda(y)\Big] \quad .$$

THEOREME 1. Soit χ le caractère χ_1^{ν} avec ν entier $1 \leq \nu < q-1$. Ecrivons ν en base p : $\nu = \nu_o + p\nu_1 + \ldots + \nu_{f-1}p^{f-1}$. Les coefficients ν_i sont donc compris entre 0 et $p-1$ et ne peuvent ni être tous nuls ni tous égaux à $(p-1)$. Si on introduit les nombres $s(\nu)$ et $\gamma(\nu)$:

$$s(\nu) = \sum_{i=0}^{f-1} \nu_i \quad , \quad \gamma(\nu) = \prod_{i=0}^{f-1} (\nu_i!) \quad .$$

Alors $\dfrac{\tau(\chi)}{(\omega-1)^{s(\nu)}}$ est une $\mathfrak{P}$-unité de A congrue à $-\dfrac{1}{\gamma(\nu)}$ modulo $\mathfrak{P}$.

La démonstration se fait par récurrence sur l'exposant ν :

1. $\nu = 1$.

$$\tau(\chi_1) = \sum_{a\in F^*} \chi_1(a)\omega^{T(a)} \quad .$$

Dans la sommation pour $a \in F^*$ on peut remonter $T(a)$ en un entier positif. La formule du binôme permet de trouver $\xi_a \in A$ tel que :

$$\omega^{T(a)} = 1 + T(a)(\omega-1) + \xi_a(\omega-1)^2 \quad .$$

Ainsi :

$$\tau(\chi_1) = \sum_{a\in F^*} \chi_1(a)\,[(\omega-1)T(a) + \xi_a(\omega-1)^2] \quad .$$

L'élément $\frac{\tau(\chi_1)}{\omega-1}$ est donc dans A et son image par φ est donc :

$$\sum_{a\in F^*} a^{-1}(a+a^p+\ldots+a^{p^{f-1}}) = \sum_{a\in F^*} 1 = \varphi(q-1) = \varphi(-1) .$$

2. $p \nmid \nu$. Alors $\nu_o \neq 0$. On utilise la partie iii) du lemme 1 ce qui conduit à calculer $\rho = \varphi(\sum_x \chi_1(x)\chi_1^{\nu-1}(1-x))$:

$$\rho = \sum_{x\neq 0} x^{-1}(1-x)^{q-\nu} = \sum_{x\neq 0} \sum_{j=0}^{q-\nu} (-1)^j x^{j-1} C^j_{q-\nu} .$$

Après avoir interverti l'ordre des sommations, on voit que pour $j \neq 1$ la somme correspondante en x est nulle, ce qui donne :

$$\rho = \sum_{x\neq 0} \varphi(-(q-\nu)) = \varphi(-(q-1)(q-\nu)) = \varphi(-\nu_o) \neq 0 .$$

L'hypothèse de récurrence et la relation $s(\nu) = s(\nu-1) + 1$ valable parce que ν_o est non nul montre que l'ordre de $\tau(\chi_1^\nu)$ est le même que celui de $(\omega-1)^{s(\nu)}$. L'image par φ du quotient s'obtient à l'aide de l'hypothèse de récurrence et l'évaluation de ρ ci-dessus c'est donc

$$\varphi\left(\frac{-1}{\gamma(\nu-1)\cdot(\nu_o)}\right) = \varphi\left(\frac{-1}{\gamma(\nu)}\right) .$$

3. $p|\nu$. cf. lemme 1, ii) .

Donnons une expression de $s(\nu)$. Pour cela notons par $\{x\}$ pour x dans $\mathbb{Q}$ la partie fractionnaire de x , c'est-à-dire la différence $x-[x]$ de x et de sa partie entière. Les hypothèses sur ν étant celles du théorème 1 on a :

LEMME 2. $s(\nu) = (p-1)\sum_{j=0}^{f-1} \{\frac{p^j\nu}{q-1}\}$.

En effet, le chiffre ν_j de ν écrit en base p est donné par :

$$\nu_j = [\frac{\nu}{p^j}] - p[\frac{\nu}{p^{j+1}}] .$$

En ajoutant cette relation aux relations semblables on obtient :

$$s(\nu) = \sum_{j=0}^{f-1} \nu_j = \nu - (p-1)\sum_{0}^{f-1} [\frac{\nu p^j}{q}] = \left[\sum_{j=0}^{f-1} \frac{\nu p^j}{q-1} - \sum_{j=0}^{f-1} [\frac{\nu p^j}{q}]\right](p-1) .$$

Le lemme résulte alors des égalités suivantes valides parce que $1 \leq \nu \leq q-1$:

$$[\frac{\nu p^j}{q-1}] = [\frac{\nu p^j}{q}] \quad .$$

En effet, si n entier vérifiait $\frac{\nu p^j}{q-1} \geq n > \frac{\nu p^j}{q}$ on aurait les inégalités suivantes qui mènent à une contradiction, $\frac{qn}{p^j}$ étant entier :

$$\nu < \frac{qn}{p^j} \leq \frac{q}{p^j}\,\frac{\nu p^j}{q-1} = \nu + \frac{\nu}{q-1} < \nu+1 \ .$$

II - RELATIONS DE STICKELBERGER.

Soient k un corps abélien sur $\mathbb{Q}$, m un multiple de son conducteur et p un nombre premier ne divisant pas m. On choisit une racine primitive ζ_{mp} d'ordre mp de 1. On pose $\zeta_m = \zeta_{mp}^p$ et $\omega = \zeta_{mp}^m$. Pour chaque idéal premier $\mathfrak{Q}$ de $\mathbb{Q}(\zeta_m)$ au-dessus de p on note $\mathfrak{P}$ sa restriction à k et $\mathfrak{R}$ son (unique) prolongement à $\mathbb{Q}(\zeta_{mp})$. Soient g, G, $\mathcal{G}$ les groupes de Galois de k, $\mathbb{Q}(\zeta_m)$, $\mathbb{Q}(\zeta_{mp})$ sur $\mathbb{Q}$. On désigne par $q = p^f$ la plus petite puissance de p congrue à 1 modulo m. Notons $\mathcal{O}$ et $\mathcal{O}'$ les anneaux d'entiers de $\mathbb{Q}(\zeta_m)$ et $\mathbb{Q}(\zeta_{mp})$.

A l'idéal premier $\mathfrak{Q}$, on associe un caractère $\chi_{\mathfrak{Q}}$ du corps résiduel $\mathcal{O}/\mathfrak{Q}$ (isomorphe à F le corps à q éléments du § I) à valeurs dans le groupe W_m des racines $m^{\text{ièmes}}$ de 1. Pour $x \in \mathcal{O}$, considérons le symbole de puissance $[\frac{x}{\mathfrak{Q}}]$ défini comme étant la racine $m^{\text{ième}}$ de 1 congrue à $x^{\frac{q-1}{m}}$ modulo $\mathfrak{Q}$. Il est clair que $[\frac{x}{\mathfrak{Q}}]$ ne dépend que de la classe de x modulo $\mathfrak{Q}$. On a donc défini un homomorphisme $\chi_{\mathfrak{Q}}$ de $(\mathcal{O}/\mathfrak{Q})^*$ dans W_m, grâce au passage au quotient $\psi_{\mathfrak{Q}} : \mathcal{O} \to \mathcal{O}/\mathfrak{Q}$.

Si on choisit (cf. notations de I) un prolongement $\mathfrak{P}'$ de $\mathfrak{Q}$ à L (*) et si on choisit pour φ l'application de passage au quotient correspondante, le caractère $\chi_{\mathfrak{Q}}$ est donc la puissance $(-\frac{q-1}{m})$ du caractère χ_1 lié à φ. Notons $\tau(\mathfrak{Q})$ la somme de Gauss $\tau(\chi_{\mathfrak{Q}}^{-1})$: le théorème 1 de I permet de décomposer l'idéal $\tau(\mathfrak{Q})\mathcal{O}'$ de $\mathbb{Q}(\zeta_{mp})$; comme $(\omega-1)$ est un idéal premier de $\mathbb{Q}(\omega)$ non ramifié dans $\mathbb{Q}(\zeta_{mp})$ la contribution $n_{\mathfrak{R}}$

(*) ici $L = \mathbb{Q}(\omega, W_{q-1}) \supset \mathbb{Q}(\zeta_{mp})$; $\mathfrak{P}'$ joue le rôle tenu par $\mathfrak{P}$ au I.

du prolongement $\mathfrak{R}$ de $\mathfrak{Q}$ dans $\tau(\mathfrak{Q})\mathcal{O}'$ est :

$$n_{\mathfrak{R}} = s(\frac{q-1}{m}) \ .$$

La partie i) du lemme 1 de I montre que seuls les conjugués de $\mathfrak{R}$ interviennent dans $\tau(\mathfrak{Q})\mathcal{O}'$. Pour t dans $\mathbb{Z}$ $(t,m) = 1$ notons σ_t l'automorphisme de $\Phi(\zeta_m)$ défini par $\zeta_m \to \zeta_m^t$. Considérons le prolongement $\bar{\sigma}_t$ de σ_t à $\Phi(\zeta_{mp})$ laissant $\Phi(\omega)$ invariant. Lorsque t décrit un système de représentants de $\mathbb{Z}$ modulo m , t restant premier à m , les idéaux $\bar{\sigma}_t^{-1}(\mathfrak{R})$ décrivent f fois l'ensemble des conjugués de $\mathfrak{R}$. La contribution de $\bar{\sigma}_t^{-1}(\mathfrak{R})$ dans $\tau(\mathfrak{Q})\mathcal{O}'$ est la même que celle de $\mathfrak{R}$ dans $\bar{\sigma}_t(\tau(\mathfrak{Q}))$ c'est-à-dire dans $\tau(\chi_{\mathfrak{Q}}^{-t})$ c'est donc (pour $0 \le t \le q-1$)

$$n_{\bar{\sigma}_t^{-1}(\mathfrak{R})} = s(\frac{q-1}{m}t) \ .$$

On a donc :

$$(\tau(\mathfrak{Q})\mathcal{O}')^f = \mathfrak{R}^{\sum s(\frac{q-1}{m}t)\bar{\sigma}_t^{-1}} \ . \qquad (1)$$

Dans cette formule la sommation se fait sur l'ensemble I des t , $0 \le t \le m$ $(t,m) = 1$. Transformons le deuxième membre. Soit θ :

$$\theta = \sum_{t\in I} s(\frac{q-1}{m}t)\,\bar{\sigma}_t^{-1} = \sum_{t\in I} \sum_{j=0}^{f-1} (p-1)\{\frac{p^j t}{m}\}\,\bar{\sigma}_t^{-1} \ .$$

Lorsque t parcourt I , il en est de même pour j fixé de $m\{\frac{p^j t}{m}\} = a$ ce qui conduit à faire le changement de variable correspondant ; alors $\bar{\sigma}_a = \bar{\sigma}_{p^j} \cdot \bar{\sigma}_t = (\bar{\sigma}_p)^j \bar{\sigma}_t$. Ainsi :

$$\theta = \frac{p-1}{m} \sum_{j=0}^{f-1} (\bar{\sigma}_p)^j \sum_{a\in I} a\bar{\sigma}_a^{-1} \ .$$

Lorsque j varie de 0 à f-1 $(\sigma_p)^j$ parcourt le groupe de décomposition de p dans $\Phi(\zeta_m)/\Phi$ et $(\bar{\sigma}_p)^j$ parcourt le groupe de décomposition de $\mathfrak{R}$ dans $\Phi(\zeta_{mp})/\Phi(\omega)$ on a donc $\mathfrak{R}^{\bar{\sigma}_p} = \mathfrak{R}$.

La relation (1) peut donc encore s'écrire :

$$[\tau(\mathfrak{Q})\mathcal{O}']^m = \mathfrak{R}^{(p-1)\sum_{a\in I} a\bar{\sigma}_a^{-1}} \cdot \mathfrak{R}^{\sum_{a\in I} a\bar{\sigma}_a^{-1}} = (\mathfrak{Q}\mathcal{O}')^{\sum_{a\in I} a\bar{\sigma}_a^{-1}} \ .$$

D'où $(\tau(\mathfrak{Q})\mathcal{O}')^m = \mathfrak{Q}^{\sum_{a\in I} a\bar{\sigma}_a^{-1}} \mathcal{O}'$. Dans cette formule on peut remplacer chaque $\bar{\sigma}_a$ par le σ_a qu'il prolonge.

Pour chaque idéal premier $\mathfrak{Q}_i$ au-dessus de $\mathfrak{p}$ dans $\mathbb{Q}(\zeta_m)$ et donc conjugué de $\mathfrak{Q}$ on peut définir de façon analogue une somme de Gauss $\tau(\mathfrak{Q}_i)$. Désignons par $\tau(\mathfrak{p})$ le produit de ces sommes de Gauss. Par multiplicativité on déduit immédiatement :

$$(\tau(\mathfrak{p})\mathcal{O}')^m = \mathfrak{p}^{\sum_{a\in I} a\sigma_a^{-1}} \mathcal{O}' \quad . \qquad (2)$$

Dans cette formule on peut remplcer chaque σ_a par sa restriction $\sigma(a) \in g$. Définissons l'élément suivant de $\mathbb{Q}[g]$ (appelé élément de Stickelberger) :

$$\alpha = \frac{1}{m} \sum_{a\in I} a\sigma(a)^{-1} \quad .$$

Soit δ un élément quelconque de $\mathbb{Z}[g] \cap \alpha\mathbb{Z}[g]$ de sorte qu'on peut écrire $\delta = \alpha\eta$ avec un élément η dans $\mathbb{Z}[g]$. De la relation (2), on déduit (en relevant η en un élément $\bar{\eta}$ de $\mathbb{Z}[\zeta]$) :

$$(\tau(\mathfrak{p})\mathcal{O}')^{m\bar{\eta}} = \mathfrak{p}^{m\alpha\bar{\eta}}\mathcal{O}' = \mathfrak{p}^{m\delta}\mathcal{O}'$$

d'où

$$\boxed{(\tau(\mathfrak{p})\mathcal{O}')^{\bar{\eta}} = \mathfrak{p}^{\delta}.\mathcal{O}'} \quad . \qquad (3)$$

LEMME 3. <u>L'élément</u> $\tau(\mathfrak{p})^{\bar{\eta}}$ <u>est en fait dans</u> k .

<u>Démonstration</u> : On va étudier l'action de ζ sur les sommes de Gauss $\tau(\mathfrak{Q})$ relatives aux diviseurs $\mathfrak{Q}$ de $\mathfrak{p}$ dans $\mathbb{Q}(\zeta_m)$.

$$\tau(\mathfrak{Q}) = \sum \chi_{\mathfrak{Q}}^{-1}(x)\, \omega^{T(x)} \quad .$$

La somme est faite sur les $x \in \mathcal{O}/\mathfrak{Q}$; $T(x)$ désigne la trace de $\mathcal{O}/\mathfrak{Q}$ à $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$. Choisissons un système X de représentants de $\mathcal{O}$ modulo $\mathfrak{Q}$. Pour a dans X on aura à considérer un entier n_a congru à $\sum_{j=0}^{f-1} a^{p^j}$ modulo $\mathfrak{Q}$.

On peut alors écrire $\tau(\mathfrak{Q})$ sous la forme :

$$\tau(\mathfrak{Q}) = \sum_{\substack{a\in X \\ \psi_{\mathfrak{Q}}(a)\neq 0}} \left[\frac{a}{\mathfrak{Q}}\right]^{-1} \omega^{n_a} \quad .$$

Soit s un entier premier à $p\cdot m$; désignons par $\bar{\sigma}_s$ l'élément de $\mathcal{G}$ défini par $\zeta_{mp} \to \zeta_{mp}^s$. D'après l'interprétation de $[\frac{a}{\mathfrak{Q}}]$ à l'aide d'une congruence modulo $\mathfrak{Q}$, il est clair que

$$\bar{\sigma}_s([\frac{a}{\mathfrak{Q}}]^{-1}) = [\frac{\bar{\sigma}_s(a)}{\bar{\sigma}_s(\mathfrak{Q})}]^{-1} .$$

D'autre part, si

$$n_a \equiv \sum_{j=0}^{f-1} a^{p^j} \mod \mathfrak{Q}$$

on aura

$$n_a \equiv \sum_{j=0}^{f-1} \bar{\sigma}_s(a)^{p^j} \mod \bar{\sigma}_s(\mathfrak{Q}) .$$

Ceci montre que ω^{n_a} est encore égal à ω élevé à la puissance donnée par la trace de la classe $\sigma_s(a)$ modulo $\sigma_s(\mathfrak{Q})$ dans $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$. Ainsi on a :

$$\bar{\sigma}_s(\tau(\mathfrak{Q})) = \sum \chi_{\bar{\sigma}_s(\mathfrak{Q})}^{-1}(x)\ \omega^{sT'(x)} .$$

Dans la sommation x décrit $\mathcal{O}/\bar{\sigma}_s(\mathfrak{Q})$ et T' désigne la trace de ce corps à $\mathbb{F}_p$. Comme s est premier à p on peut faire le changement de variable défini en remplaçant x par $s^{-1}.x$. On obtient :

$$\bar{\sigma}_s(\tau(\mathfrak{Q})) = [\frac{s}{\bar{\sigma}_s(\mathfrak{Q})}].\tau(\bar{\sigma}_s(\mathfrak{Q}))$$

ou encore :

$$\bar{\sigma}_s(\tau(\mathfrak{Q})) = \bar{\sigma}_s([\tfrac{s}{\mathfrak{Q}}])\ .\ \tau(\bar{\sigma}_s(\mathfrak{Q})) = [\tfrac{s}{\mathfrak{Q}}]^s.\tau(\bar{\sigma}_s(\mathfrak{Q})) .$$

Par multiplicativité, on déduit :

$$\boxed{\bar{\sigma}_s(\tau(\mathfrak{P})) = \zeta\ .\ \tau(\bar{\sigma}_s(\mathfrak{P}))} \qquad (4)$$

où ζ est une racine de 1 d'ordre m en fait égale à 1 dès que s est congru à 1 modulo p (propriété des $[\frac{\ }{\mathfrak{Q}}]$) et $\tau(\bar{\sigma}_s(\mathfrak{P}))$ est défini comme $\tau(\mathfrak{P})$ en remplaçant $\mathfrak{P}$ par son conjugué $\bar{\sigma}_s(\mathfrak{P})$. Supposons que $\bar{\sigma}_s$ laisse $\mathbb{Q}(\zeta_m)$ invariant : la formule (4) montre que $\tau(\mathfrak{P})^m$ est invariant. Ceci prouve que $\tau(\mathfrak{P})^m$ est dans $\mathbb{Q}(\zeta_m)$; il en est de même de $\tau(\mathfrak{P})^{m\bar{\eta}}$. D'après (3), l'idéal de $\mathbb{Q}(\zeta_m)$ engendré par cet élément est la puissance $m^{\text{ième}}$ d'un autre idéal. Considérons l'extension obtenue par adjonction de $\tau(\mathfrak{P})^{\bar{\eta}}$ à $\mathbb{Q}(\zeta_m)$; d'après ce qui précède cette extension ne peut être ra-

mifiée que pour les idéaux divisant m . Comme m et p sont premiers les idéaux au-dessus de p ne peuvent donc pas être ramifiés. Comme l'extension $\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m)$ est totalement ramifiée pour les idéaux premiers au-dessus de p ceci implique que $\tau(\mathfrak{P})^{\bar{\eta}}$ est dans $\mathbb{Q}(\zeta_m)$.

Pour montrer que $\tau(\mathfrak{P})^{\bar{\eta}}$ est en fait dans k on peut se limiter aux éléments $\bar{\sigma}_s$ provenant d'un s entier congru à 1 modulo p ; pour de tels $\bar{\sigma}_s$ on a d'après (4) :

$$\bar{\sigma}_s(\tau(\mathfrak{P})) = \tau(\bar{\sigma}_s(\mathfrak{P})) \ .$$

Si un tel $\bar{\sigma}_s$ laisse k invariant, il laisse a fortiori $\mathfrak{P}$ invariant et donc $\tau(\mathfrak{P})$ et $\tau(\mathfrak{P})^{\bar{\eta}}$ ce qui achève la preuve du lemme.

THEOREME 2. *Soient k une extension abélienne de $\mathbb{Q}$, m un multiple de son conducteur, de sorte qu'on a $k \subset \mathbb{Q}(\zeta_m)$. Pour a entier et premier à m considérons l'automorphisme $\sigma(a)$, restriction à k de l'automorphisme de $\mathbb{Q}(\zeta_m)$ défini par $\zeta_m \to \zeta_m^a$. Soient g le groupe de Galois de k sur $\mathbb{Q}$ et α l'élément de $\mathbb{Q}[g]$ ainsi défini :*

$$\alpha = \frac{1}{m} \sum_{\substack{a=1 \\ (a,m)=1}}^{m} a\,\sigma(a)^{-1} \ .$$

Alors l'idéal $\mathbb{Z}[g] \cap \alpha\mathbb{Z}[g]$ de $\mathbb{Z}[g]$ annule le groupe des classes de k .

Soient $\delta \in \mathbb{Z}[g] \cap \alpha\mathbb{Z}[g]$ et c une classe d'idéaux de k il s'agit de voir que la classe δc est la classe principale. On sait que c contient un idéal premier $\mathfrak{P}$ premier à m . Soit p le nombre premier correspondant à $\mathfrak{P}$; on peut faire la construction de $\tau(\mathfrak{P})$. Le théorème résulte alors de la formule (3) et du lemme 3.

BIBLIOGRAPHIE

[1] - S. LANG - Algebraic Number Theory. Chap. IV.

[2] - LEOPOLDT - Zur Arithmetik in abelschen Zahlkörpern. Journal de Crelle n° 209, Annexe A, pp. 67-69.

[3] - WEIL A. - La cyclotomie jadis et naguère. Séminaire Bourbaki n° 452 (juin 74).

-:-:-:-