

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

© Institut Fourier – Université de Grenoble, 1974-1975, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

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 $A \rightarrow A/\mathfrak{p} = F$
 - 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 :
 $\forall a \in F^* \quad , \quad \varphi \circ \chi_1(a) = a^{-1}$
 - χ_0 l'homomorphisme trivial $F^* \rightarrow W_{q-1}$.

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 :

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

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 $\chi \neq \chi_0$, $\tau(\chi)\tau(\chi^{-1}) = \chi(-1)q$
- ii) $\forall r \in \mathbb{N}$, $\tau(\chi^{q^r}) = \tau(\chi)$
- iii) si χ et χ' sont dans $\text{Hom}(F^*, W_{q-1})$ et si $\chi \cdot \chi' \neq \chi_0$:

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

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

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

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

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

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

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

$$A(z) = q \cdot \chi(-z)$$

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

$$B(y) = \sum_x \chi(x)\lambda(yx)$$

$B(0)$ 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 :

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

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

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

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

ii) La fonction de F sur lui-même définie par $x \rightarrow x^{p^r}$ 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 :

$$\begin{aligned}\tau(\chi)\tau(\chi') &= \sum_{xy} \chi(x)\chi'(y) \lambda(x+y) \\ &= \sum_{xy} \chi(x)\chi'(y-x)\lambda(y) .\end{aligned}$$

Comme $\chi\chi' \neq \chi_0$ la somme sur x relative à $y = 0$ est nulle. Pour les autres valeurs de y , on fait le changement de sommation défini par $x = yt$.

$$\begin{aligned}\tau(\chi)\tau(\chi') &= \sum_{y \in F^*} \sum_x \chi(xy) \chi'(y-xy) \lambda(y) \\ &= \left[\sum_x \chi(x)\chi'(1-x) \right] \left[\sum_{y \in F} (\chi\chi')(y)\lambda(y) \right] .\end{aligned}$$

THEOREME 1. Soit χ le caractère χ_1^ν avec ν entier $1 \leq \nu < q-1$. Ecrivons ν en base p : $\nu = \nu_0 + p\nu_1 + \dots + \nu_{f-1}p^{f-1}$. 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 $\gamma(\nu)$:

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

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

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

1. $\nu = 1$.

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

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 :

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

Ainsi :

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

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

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

2. $p \nmid \nu$. Alors $\nu_0 \neq 0$. On utilise la partie iii) du lemme 1 ce qui conduit à calculer $\rho = \varphi \left(\sum_x \chi_1(x) \chi_1^{\nu-1}(1-x) \right)$:

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

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

$$\rho = \sum_{x \neq 0} \varphi(-(q-\nu)) = \varphi(-(q-1)(q-\nu)) = \varphi(-\nu_0) \neq 0 .$$

L'hypothèse de récurrence et la relation $s(\nu) = s(\nu-1) + 1$ valable parce que ν_0 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

$$\varphi\left(\frac{-1}{\gamma(\nu-1) \cdot (\nu_0)}\right) = \varphi\left(\frac{-1}{\gamma(\nu)}\right) .$$

3. $p \mid \nu$. 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 :

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

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

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

En ajoutant cette relation aux relations semblables on obtient :

$$s(\nu) = \sum_{j=0}^{f-1} \nu_j = \nu - (p-1) \sum_0^{f-1} \left[\frac{\nu p^j}{q} \right] = \left[\sum_{j=0}^{f-1} \frac{\nu p^j}{q-1} - \sum_{j=0}^{f-1} \left[\frac{\nu p^j}{q} \right] \right] (p-1) .$$

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

$$\left[\frac{vp^j}{q-1} \right] = \left[\frac{vp^j}{q} \right] .$$

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

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

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, \mathfrak{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 èmes de 1. Pour $x \in \mathcal{O}$, considérons le symbole de puissance $\left[\frac{x}{\mathfrak{q}} \right]$ défini comme étant la racine m ème de 1 congrue à $x \frac{q-1}{m}$ modulo \mathfrak{q} . Il est clair que $\left[\frac{x}{\mathfrak{q}} \right]$ 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 $\psi_{\mathfrak{q}} : \mathcal{O} \rightarrow \mathcal{O}/\mathfrak{q}$.

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 $\left(-\frac{q-1}{m}\right)$ 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 :

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

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 $\mathbb{Q}(\zeta_m)$ défini par $\zeta_m \rightarrow \zeta_m^t$. Considérons le prolongement $\bar{\sigma}_t$ de σ_t à $\mathbb{Q}(\zeta_{mp})$ laissant $\mathbb{Q}(w)$ 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 $0 \leq t \leq q-1$)

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

On a donc :

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

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

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

Lorsque t parcourt I, il en est de même pour j fixé de $m \left\{ \frac{p^j t}{m} \right\} = a$ ce qui conduit à faire le changement de variable correspondant ; alors $\bar{\sigma}_a = \bar{\sigma}_{p^j} \cdot \bar{\sigma}_t$ et $\bar{\sigma}_t = (\bar{\sigma}_p)^j \bar{\sigma}_a$. 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 $f-1$ $(\bar{\sigma}_p)^j$ parcourt le groupe de décomposition de p dans $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ et $(\bar{\sigma}_p)^j$ parcourt le groupe de décomposition de \mathfrak{R} dans $\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(w)$ on a donc $\mathfrak{R}^{\bar{\sigma}_p} = \mathfrak{R}$.

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

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

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 :

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

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

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

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

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

d'où

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

LEMME 3. L'élément $\tau(\mathfrak{P})^{\bar{\eta}}$ est en fait dans k .

Démonstration : On va étudier l'action de \mathfrak{G} 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 $\zeta_{mp} \rightarrow \zeta_{mp}^s$. D'après l'interprétation de $\left[\frac{a}{\mathfrak{Q}}\right]$ à l'aide d'une congruence modulo \mathfrak{Q} , il est clair que

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

D'autre part, si

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

on aura

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

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 $s^{-1} \cdot x$. On obtient :

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

ou encore :

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

Par multiplicativité, on déduit :

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

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 $\left[\frac{s}{\mathfrak{Q}}\right]$) 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 $\tau(\mathfrak{P})^{\bar{n}}$ est dans $\mathbb{Q}(\zeta_m)$.

Pour montrer que $\tau(\mathfrak{P})^{\bar{n}}$ 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 $\tau(\mathfrak{P})^{\bar{n}}$ 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 $\zeta_m \rightarrow \zeta_m^a$. Soient \mathfrak{g} le groupe de Galois de k sur \mathbb{Q} et α l'élément de $\mathbb{Q}[\mathfrak{g}]$ ainsi défini :

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

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

Soient $\delta \in \mathbb{Z}[\mathfrak{g}] \cap \alpha \mathbb{Z}[\mathfrak{g}]$ 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).

-:-:-