Théorie des Nombres .

- Besançon -

Année 1975-1976

APPLICATION DE LA NOTION DE φ-OBJET A L'ETUDE DU GROUPE DES CLASSES D'IDEAUX DES EXTENSIONS ABELIENNES .

Georges GRAS
Faculté des Sciences. Mathématiques
25030 Besançon Cedex

APPLICATION DE LA NOTION DE φ-OBJET A L'ETUDE DU GROUPE DES CLASSES D'IDEAUX DES EXTENSIONS ABELIENNES .

par Georges GRAS

Résumé . Cet article est composé des deux parties suivantes :

(i) Une partie algébrique (Chap. I) où l'on procède à l'étude systématique de certaines familles M de $\mathfrak{G}$-modules (appellées les $\mathfrak{G}$-familles), $\mathfrak{G}$ désignant le groupe de Galois de l'extension abélienne maximale de $\mathbb{Q}$. Cette étude conduit à la définition de sous-modules M_φ (φ parcourant certains ensembles de caractères de $\mathfrak{G}$) dont les éléments sont appellés les φ-objets (relativement à M) . Cette famille de sous-modules permet dans certains cas notamment dans le cas dit des $\mathfrak{G}'$-familles d'éclairer assez bien la structure des $\mathfrak{G}$-modules constituant M (compte tenu du fait que l'on n'est pas dans le cas où les algèbres de groupes utilisées sont semi-simples) .

(ii) Une partie arithmétique (Chap. II , III et IV) où l'on applique les résultats sur les φ-objets au cas des groupes des classes des extensions abéliennes de $\mathbb{Q}$. Différents résultats sur les classes relatives et les classes réelles sont obtenus : la généralisation au cas non semi-simple de l'interprétation arithmétique de Leopoldt pour les classes réelles, une interprétation analogue pour les classes relatives , une interprétation du théorème de Stickelberger , une généralisation d'une formule d'Iwasawa sur l'ordre du groupe des classes relatives et un certain nombre de résultats relatifs aux Γ-extensions cyclotomiques des extensions abéliennes de $\mathbb{Q}$. Enfin cette étude permet de définir , dans le cas général , des invariants " classes " $m_\phi(\mathcal{H})$, $m_\phi(\mathcal{H}')$ et des invariants " analytiques " $m_\phi(h)$, $m_\phi(h')$, ϕ parcourant l'ensemble des caractères ℓ-adiques de $\mathfrak{G}$, et de poser le problème de la comparaison de ces invariants .

L'idée de la définition des φ-objets doit beaucoup à l'étude des travaux de Leopoldt et aux rédactions qui en ont été faites par B. Oriat dans [17] et [18] .

Chap. I

Définition et étude générale des φ-objets .

1) Introduction . Dans [15] Leopoldt a défini des groupes d'unités que nous appellerons (comme dans [18]) des χ-unités . Nous allons dans ce chapitre donner une définition plus générale de la notion de φ-objet , φ n'étant plus nécessairement un caractère rationnel irréductible et les modules intervenant dans la définition des φ-objets , n'étant pas nécessairement $\mathbb{Z}$-libres comme c'est le cas des groupes d'unités définis dans [15] .

2) Extensions abéliennes de $\mathbb{Q}$ - Caractères .

Soit $\mathbb{Q}^a$ l'extension abélienne maximale de $\mathbb{Q}$ contenue dans une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ avec le schéma d'inclusions suivant (ℓ étant un nombre premier donné , Ω_ℓ une clôture algébrique de $\mathbb{Q}_\ell$ et $\hat{\Omega}_\ell$ un complété de Ω_ℓ) :

$$\begin{tikzcd}[arrows=dash]
 & \mathbb{Q}_\ell \arrow[r] \arrow[d] & \mathbb{Q}_\ell\mathbb{Q}^a \arrow[r] \arrow[d] & \Omega_\ell \arrow[r] \arrow[d] & \hat{\Omega}_\ell \\
\mathbb{Q} \arrow[r] & \mathbb{Q}_\ell \cap \mathbb{Q}^a \arrow[r] & \mathbb{Q}^a \arrow[r] & \overline{\mathbb{Q}} &
\end{tikzcd}$$

On pose $\mathfrak{G} = \mathrm{Gal}\,(\mathbb{Q}^a/\mathbb{Q})$ et on note $\mathfrak{X}'$ l'ensemble des caractères de degré 1 de $\mathfrak{G}$, à valeurs dans Ω_ℓ , et dont le noyau est fermé et d'indice fini dans $\mathfrak{G}$. On définit les ensembles de caractères rationnels $\mathfrak{X}$, ℓ-adiques Φ et les ensembles de caractères correspondants pour un sous-corps K : $\mathfrak{X}'_K$, $\mathfrak{X}_K$, Φ_K . Pour la définition de g_χ , K_χ , G_χ , f_χ , $\chi \in \mathfrak{X}$, cf. [8] , [15] ou [18] .

3) Définition des $\mathfrak{G}$-familles et des $\mathfrak{G}'$-familles .

Soit $\mathcal{K}$ la famille des extensions finies de $\mathbb{Q}$ contenues dans

$\mathbb{Q}^a$. On suppose donné une famille M de $\mathbb{Z}[\mathfrak{G}]$ -modules $M = (M(K))_{K \in \mathcal{X}}$ indexée par $\mathcal{X}$ et , éventuellement , deux familles d'applications ($N_{L/K}$) et ($j_{L/K}$) indexées par l'ensemble des sous-extensions L/K , L , K $\in \mathcal{X}$. Nous allons faire des hypothèses sur ces familles . Avant nous précisons les notations suivantes :

Si $K \in \mathcal{X}$ et si $\sigma \in \mathfrak{G}$, on note σ_K l'image de σ dans $\mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{G}/\mathrm{Gal}(\mathbb{Q}^a/K)$. Pour une extension L/K , L , K $\in \mathcal{X}$, on pose $G(L/K) = \mathrm{Gal}(L/K)$ et on pose $\nu_{L/K} = \sum_{s \in G(L/K)} s \in \mathbb{Z}[G(L/K)]$.

a) <u>Hypothèses sur les familles</u> $(M(K))_{K \in \mathcal{X}}$, $(N_{L/K})$ et $(j_{L/K})$.
On considère les trois conditions suivantes :

(i) Pour tout $K \in \mathcal{X}$, pour tout $x \in M(K)$ et tout $\sigma \in \mathfrak{G}$, x^σ ne dépend que de la classe de σ modulo $G(\mathbb{Q}^a/K)$ (Autrement dit, les M(K) sont canoniquement des $G(K/\mathbb{Q})$-modules par la loi $x^{\sigma_K} = x^\sigma$) .

(ii) Pour toute sous-extension L/K , L , K $\in \mathcal{X}$, $N_{L/K}$ est un homomorphisme de $\mathfrak{G}$ -modules de M(L) dans M(K) , $j_{L/K}$ est un homomorphisme de $\mathfrak{G}$ -modules de M(K) dans M(L) et on suppose que pour tout triplet K , L , E $\in \mathcal{X}$, $K \subset L \subset E$, on a les formules de transitivité :

$$N_{L/K} \circ N_{E/L} = N_{E/K} \quad \text{et} \quad j_{E/L} \circ j_{L/K} = j_{E/K} .$$

(iii) On a $j_{L/K} \circ N_{L/K} = \nu_{L/K}$, pour K , L $\in \mathcal{X}$, $K \subset L$, $\nu_{L/K}$ étant ici identifié à l'homomorphisme de $G(L/\mathbb{Q})$-modules défini par $\nu_{L/K}(x) = \prod_{s \in G(L/K)} x^s$, pour tout $x \in M(L)$.

<u>Définition</u> I 1 . Si $M = (M(K))_{K \in \mathcal{X}}$ vérifie la condition (i) , nous dirons que cette famille est une $\mathfrak{G}$ -famille .

Si en plus, on dispose de deux familles $(N_{L/K})$ et $(j_{L/K})$ vérifiant les conditions (ii) et (iii) , nous dirons que la famille M est une $\mathfrak{G}'$-famille (les homomorphismes $N_{L/K}$ et $j_{L/K}$ étant supposés associés à M sans ambiguité) .

b) <u>Propriétés immédiates des $\mathfrak{G}'$-familles</u> .

Proposition I 1 . Pour tout $K \in \mathcal{X}$, $\nu_{K/K}$, $N_{K/K}$, $j_{K/K}$ sont l'identité sur $M(K)$.

démonstration

Ceci est déjà vrai pour $\nu_{K/K}$. D'après (iii) , on a $j_{K/K} \circ N_{K/K} = id$; $N^2_{K/K} = N_{K/K}$ et $j^2_{K/K} = j_{K/K}$ (d'après (ii)) entraînent $j_{K/K} \circ N^2_{K/K} = N_{K/K} = j_{K/K} \circ N_{K/K} = id$ et $j^2_{K/K} \circ N_{K/K} = j_{K/K} = j_{K/K} \circ N_{K/K} = id$.

Proposition I 2 . Si l'application $N_{L/K}$ est surjective ou si l'application $j_{L/K}$ est injective , alors $N_{L/K} \circ j_{L/K}$ est l'élévation à la puissance $[L:K]$ dans $M(K)$.

démonstration

Supposons $N_{L/K}$ surjective .

Soit $x \in K$, $x = N_{L/K}(y)$ et $j_{L/K}(x) = j_{L/K} \circ N_{L/K}(y) = \prod_{s \in G(L/K)} y^s$ et $N_{L/K} \circ j_{L/K}(x) = N_{L/K}\left(\prod_{s \in G(L/K)} y^s\right) = \prod_{s \in G(L/K)} (N_{L/K}\, y)^s$, mais $N_{L/K}(y) = x \in K$ et le produit est égal à $(N_{L/K}(y))^{[L:K]} = x^{[L:K]}$. Si on suppose $j_{L/K}$ injective , alors $j_{L/K} \circ N_{L/K} \circ j_{L/K}(x) = \nu_{L/K}(j_{L/K}(x)) = \prod_{s \in G(L/K)} (j_{L/K}(x))^s = \prod_{s \in G(L/K)} j_{L/K}(x^s) = j_{L/K}(x)^{[L:K]}$ ce qui conduit à $N_{L/K} \circ j_{L/K}(x) = x^{[L:K]}$.

c) Exemples . Les exemples les plus simples de telles familles sont obtenus pour les familles M suivantes :

(i) $M(K)$ est le groupe des unités de K ;

(ii) $M(K)$ est le groupe des classes de K ;

dans ces deux cas l'opération est celle de Galois et les applications $N_{L/K}$

et $j_{L/K}$ sont bien connues .

(iii) Soit A un anneau ; on pose $M(K) = A[G(K/\mathbb{Q})]$; $M(K)$ est un $\mathfrak{S}$-module si l'on pose , pour $\sigma \in \mathfrak{S}$ et $\omega \in A[G(K/\mathbb{Q})]$, $\sigma.\omega = \sigma_K \omega$ (produit dans $A[G(K/\mathbb{Q})]$) . Les fonctions $N_{L/K}$ sont définies par $N_{L/K}(\sigma_L) = \sigma_K$, pour tout $\sigma_L \in G(L/\mathbb{Q})$ et par prolongement par A-linéarité à $A[G(L/\mathbb{Q})]$. Si $\sigma_K \in G(K/\mathbb{Q})$, on pose $j_{L/K}(\sigma_K) = \sum_{\tau \in G(L/K)} \tau\sigma_L = \nu_{L/K}\sigma_L$ et on étend par A-linéarité .

On vérifie facilement que l'on a une $\mathfrak{S}$'-famille .

Remarque I 1 . Dans le cas $M(K) = A[G(K/\mathbb{Q})]$, les homomorphismes $N_{L/K}$ et $j_{L/K}$ sont respectivement surjectifs et injectifs quels que soient $L, K \in \mathfrak{X}$, $K \subset L$, et l'application $N_{L/K}$ est un homomorphisme de A-algèbres alors que $j_{L/K}$ n'est qu'un homomorphisme de A-modules (cette propriété de $N_{L/K}$ provient de la propriété universelle des algèbres de groupes puisque la restriction de $N_{L/K}$ à $G(L/\mathbb{Q})$ est un homomorphisme de $G(L/\mathbb{Q})$ sur $G(K/\mathbb{Q})$).

4) Définition des sous-modules M_φ , M_χ et M'_χ .

a) Rappels sur la Γ_k-conjugaison (*) ([19]) . Soit A un sous-anneau de Ω_ℓ. On suppose que A est un anneau de Dedekind à corps résiduels finis tel que $A[\zeta]$ soit un anneau de Dedekind quelle que soit la racine de l'unité ζ (par exemple $A = \mathbb{Z}$, $A = \mathbb{Z}_\ell$ ou $A = \mathbb{Z}_{(\ell)}$) .

Soit $\chi \in \mathfrak{X}$. Soit alors P_χ le g_χ^e polynome cyclotomique global ; on note encore P_χ son image canonique dans $A[X]$. Soit k le corps des fractions de A dans Ω_ℓ et soit k'_χ/k l'extension obtenue en adjoignant les racines g_χ^e de l'unité ; on rappelle que k'_χ/k est une extension abélienne dont le groupe de Galois est canoniquement isomorphe à un sous-groupe de $(\mathbb{Z}/g_\chi\mathbb{Z})^*$. On pose $\Gamma_{k,\chi} = \mathrm{Gal}(k'_\chi/k)$. On définit , comme dans [19] une relation d'équivalence dans $\mathfrak{X}'$ que l'on appelle la Γ_k-conjugaison en posant pour $\tau \in \Gamma_{k,\chi}$: $\chi'^{\tau} = \chi'^{a}$, $a \in \mathbb{Z}$ représentant τ

(*) hypothèse inutile ici ; sera utilisée par la suite .

dans $(\mathbb{Z}/g_\chi\mathbb{Z})^*$. Si σ_χ est un générateur de G_χ, alors les $\chi'^\tau(\sigma_\chi)$, pour $\tau \in \Gamma_{k,\chi}$, sont les conjugués de $\chi'(\sigma_\chi)$ dans k'_χ/k. On définit alors les fonctions φ :

$$\varphi = \sum_{\tau \in \Gamma_{k,\chi}} \chi'^\tau \ ;$$

ces fonctions sont appellées les caractères irréductibles sur k. Comme applications de $\mathfrak{G}$ dans Ω_ℓ, les applications φ sont à valeurs dans A. On utilise comme dans [8] la notation $\chi' | \varphi$ pour dire que χ' est un terme de φ.

Les caractères rationnels sont obtenus avec $A = \mathbb{Z}$, les caractères ℓ-adiques sont obtenus avec $A = \mathbb{Z}_\ell$.

b) Correspondance entre caractères et polynomes cyclotomiques.

Dans $k[X]$, P_χ se décompose en un produit de polynomes irréductibles tous distincts $Q_{\chi,i}$; chacun de ces polynomes $Q_{\chi,i}$ se décompose en polynomes du premier degré dans k'_χ. Les racines de ces polynomes étant des racines primitives g_χ^e de l'unité, chaque $Q_{\chi,i}$ est de degré $[k'_\chi : k]$. Si ζ_i est une racine de $Q_{\chi,i}$ dans k'_χ, les autres racines sont les ζ_i^τ pour $\tau \in \Gamma_{k,\chi}$; ainsi ces ensembles de racines correspondent bijectivement aux ensembles de la forme $(\chi'(\sigma_\chi))_{\tau \in \Gamma_{k,\chi}}$, $\chi' \in \mathfrak{X}'_{K_\chi}$ d'ordre g_χ parcourant un système représentatif de caractères pour la Γ_k-conjugaison. On peut donc indexer de façon non canonique les diviseurs irréductibles de P_χ à l'aide des caractères φ obtenus à partir des caractères χ' d'ordre g_χ.

On pose $P_\varphi = \prod_{\chi' | \varphi} (X - \chi'(\sigma_\chi))$; c'est un polynome de $A[X]$ irréductible sur k. Ceci suppose qu'un choix des générateurs σ_χ a été effectué une fois pour toutes : P_φ dépend du choix de σ_χ, cependant, on a $\prod_{\varphi | \chi} P_\varphi = P_\chi$, pour tout $\chi \in \mathfrak{X}$.

c) Définition des modules M_φ.

Définition I 2. Soit M une $\mathfrak{G}$-famille. On suppose que l'anneau A est tel que pour tout $K \in \mathcal{K}$, $M(K)$ est un $A[G(K/\mathbb{Q})]$-module. On pose pour $\varphi|\chi$:

$$M_\varphi = \left\{ x \in M(K_\chi) \ , \ P_\varphi(\sigma_\chi)x = 1 \right\} \quad ;$$

les éléments de M_φ sont les φ -objets dont nous avons parlé dans l'introduction ; M_φ est un sous-$A[G_\chi]$-module de $M(K_\chi)$.

Proposition I 3 . Le sous-module M_φ ne dépend pas du choix de σ_χ mais uniquement du caractère φ .

démonstration

On a $P_\varphi(\sigma_\chi) = \prod_{\chi'|\varphi} (\sigma_\chi - \chi'(\sigma_\chi))$ et pour $(a, g_\chi) = 1$, soit $\sigma_\chi{}^a$ un autre générateur de G_χ avec lequel on obtient le polynome $P'_\varphi = \prod_{\chi'|\varphi} (X - \chi'(\sigma_\chi^a))$; $P_\varphi(\sigma_\chi{}^a) = \prod_{\chi'|\varphi} (\sigma_\chi{}^a - \chi'(\sigma_\chi{}^a))$, soit $P'_\varphi(\sigma_\chi^a) = \prod_{\chi'|\varphi} (\sigma_\chi - \chi'(\sigma_\chi))(\sigma_\chi{}^{a-1} + \dots \pm \chi'^{a-1}(\sigma_\chi))$ et de la même manière, on aura $P_\varphi(\sigma_\chi) = \prod_{\chi'|\varphi} (\sigma_\chi^a - \chi'^a(\sigma_\chi))(\sigma_\chi{}^{a(a^*-1)} + \dots \pm \chi'^{a(a^*-1)}(\sigma_\chi))$,

où a^* est tel que $aa^* \equiv 1 \bmod g_\chi$. Les relations $P'_\varphi(\sigma_\chi^a) \in P_\varphi(\sigma_\chi) A[G_\chi]$ et $P_\varphi(\sigma_\chi) \in P'_\varphi(\sigma_\chi^a) A[G_\chi]$ montrent l'invariance de la définition . On notera désormais de la façon suivante qui ne fait plus référence à σ_χ :

$$M_\varphi = \left\{ x \in M(K_\chi) \ , \ P_\varphi x = 1 \right\} \quad , \text{ pour } \varphi|\chi.$$

d) Cas particulier des caractères rationnels . On a donc $M_\chi = \left\{ x \in M(K_\chi) \ , \ P_\chi x = 1 \right\}$. On a alors le résultat suivant qui permet une autre interprétation de M_χ , uniquement dans le cas des caractères rationnels :

Théorème I 1 . Soit M une $\mathfrak{S}$-famille . On a :

$$M_\chi = \left\{ x \in M(K_\chi) \ , \ \nu_{K_\chi/K} \, x = 1 \ , \text{ pour tout } K \subsetneq K_\chi \right\} .$$

démonstration (d'après une communication personnelle de J. Martinet en date du 23/10/1968) .

Trois lemmes préliminaires sont nécessaires .

<u>Lemme</u> I 1 . Soit $n \geqslant 1$ et soit p un nombre premier quelconque . Notons P_n le n^e polynome cyclotomique de $\mathbb{Z}[X]$:

(i) $P_n(X^p) = P_{np}(X)$, si p divise n ,

(ii) $P_n(X^p) = P_{np}(X)\, P_n(X)$, si p ne divise pas n .

Il suffit de comparer les ensembles de racines (qui sont distinctes) des polynomes des deux membres .

<u>Remarque</u> I 2 . Ce résultat permet de déduire le résultat utile suivant : Si $n > 1$ est distinct d'une puissance d'un nombre premier alors $P_n(1) = 1$. On a ensuite $P_{p^k}(1) = p$, pour tout $k \geqslant 1$ et enfin $P_1(1) = 0$.

En effet, $P_p(1) = p$, d'où , pour $k \geqslant 2$, $P_{p^k}(1) = P_{p^{k-1}p}(1) = P_{p^{k-1}}(1)$, d'après (i) ; d'où le résultat . Si n n'est pas une puissance de p , on écrit $n = p^k n_o$, avec $n_o \neq 1$ et $p \nmid n_o$, $k \geqslant 1$; (ii) donne $P_{n_o}(1) = P_{n_o p}(1)\, P_{n_o}(1)$; comme $P_{n_o}(1) \neq 0$ (car $n_o \neq 1$) , $P_{n_o p}(1) = 1$, (i) permet alors de conclure pour $P_{n_o p^k}$.

<u>Lemme</u> I 2 . Soit $n = p_1 p_2 \dots p_t$, p_i nombres premiers distincts , avec $t \geqslant 2$. Alors pour tout couple (i, j) , $i \neq j$, il existe A_i^j , $A_j^i \in \mathbb{Z}[X]$ tels que $A_i^j P_{\frac{n}{p_i}} + A_j^i P_{\frac{n}{p_j}} = 1$.

On démontre ceci par récurrence sur $t \geqslant 2$.

Si $t = 2$, alors $n = p_1 p_2$ et $P_{\frac{n}{p_1}} = X^{p_2 - 1} + \dots + X + 1$, $P_{\frac{n}{p_2}} = X^{p_1 - 1} + \dots + X + 1$. Si on appelle polynome géométrique , tout polynome de la forme $X^n + X^{n-1} + \ldots + X + 1$, $n \geqslant 0$, ou le polynome 0 , alors , si P et Q sont géométriques , $Q \neq 0$, le reste de la division euclidienne de P par Q est un polynome géométrique et le quotient est dans $\mathbb{Z}[X]$: en effet , si $m \geqslant n$, si $m+1 = q(n+1) + r$, $0 \leqslant r < n$, on a $X^m + \ldots + X + 1 = (X^n + \ldots + X + 1)(X^{m+1-(n+1)} + X^{m+1-2(n+1)} + \ldots + X^{m+1-q(n+1)}) + 1 + X + \ldots + X^{r-1}$ (si $r > 0$) , 0 sinon . En particulier , l'algorithme du p.g.c.d. donne un polynome géométrique . Comme le seul polynome géométrique constant non nul est 1 , il en résulte que si P et Q sont premiers entre eux dans $\mathbb{Q}[X]$, le p.g.c.d. trouvé sera 1 ; la relation de Bezout est alors possible dans $\mathbb{Z}[X]$; ce qui est le cas pour P_{p_1} et P_{p_2} .

Supposons $t \geqslant 3$. Soient p_i , p_j , q trois nombres premiers distincts divisant n . On pose $n' = \frac{n}{q}$; par hypothèse de récurrence , on a dans $\mathbb{Z}[X]$:

$$A'^j_i(X)\, P_{\frac{n'}{p_i}}(X) + A'^i_j(X)\, P_{\frac{n'}{p_j}}(X) = 1 \quad , \text{ ce qui donne}$$

$$A'^j_i(X^q)\, P_{\frac{n'}{p_i}}(X^q) + A'^i_j(X^q)\, P_{\frac{n'}{p_j}}(X^q) = 1 \quad , \text{ d'où la relation}$$

puisque ici (ii) donne : $P_{\frac{n'}{p_i}}(X^q) = P_{\frac{n}{p_i}}(X)\, P_{\frac{n'}{p_i}}(X)$ et

$P_{\frac{n'}{p_j}}(X^q) = P_{\frac{n}{p_j}}(X)\, P_{\frac{n'}{p_j}}(X)$.

<u>Lemme</u> I 3 . Soit $n > 1$; posons $N_{n,p}(X) = \sum_{i=0}^{p-1} X^{\frac{n}{p} i}$ pour tout p premier divisant n . Alors il existe des polynomes $A_p(X)$ de $\mathbb{Z}[X]$ tels que :

$$P_n(X) = \sum_{p \mid n} A_p(X)\, N_{n,p}(X) \quad .$$

Soit q un diviseur premier de n . Montrons que si la propriété est vraie pour n , elle est vraie pour nq :

$$P_n(X^q) = P_{nq}(X) = \sum_{p\mid n} A_p(X^q)\, N_{n,p}(X^q) \quad ;$$

or $N_{n,p}(X^q) = \sum_{i=0}^{p-1} X^{\frac{n}{p} q i} = N_{nq,p}(X)$, d'où le résultat .

Il en résulte que si la propriété est vraie pour tous les nombres n sans facteur carré , elle est vraie pour tout $n > 1$.

$$\text{Si } n = p_1 \,,\; P_{p_1}(X) = X^{p_1 - 1} + \ldots + X + 1 = N_{p_1,p_1}(X) \quad ;$$

on démontre par récurrence sur le nombre de diviseurs ; si $n = p_1 \ldots p_t$, $t \geqslant 2$, on pose $n_j = \frac{n}{p_j}$ pour tout j . Par hypothèse ,

$$P_{n_j}(X) = \sum_{\substack{i=1\\ i\neq j}}^{t} A_i^j(X)\, N_{n_j,p_i}(X) \quad , \text{ d'où , en posant } A_j^j = 0 \; :$$

$$P_{n_j}(X^{p_j}) = P_n(X)\, P_{n_j}(X) = \sum_{i=1}^{t} A_i^j(X^{p_j})\, N_{n,p_i}(X) \quad ;$$

comme on a $t \geqslant 2$, on peut appliquer le lemme I 2 : on utilise une relation de Bezout dans $\mathbb{Z}[X]$ entre deux des P_{n_j} , ce qui conduit au résultat.

On a donc démontré que l'idéal engendré dans $\mathbb{Z}[X]$ par les $N_{n,p}(X)$ est égal à $P_n(X)\mathbb{Z}[X]$: en effet, on vient de voir que $P_n(X)$ appartient à cet idéal ; il suffit alors de voir que $N_{n,p}(X) = P_p(X^{\frac{n}{p}})$, or toute racine d'ordre n de l'unité annule $N_{n,p}(X)$ donc $P_n(X)$ divise $N_{n,p}(X)$ dans $\mathbb{Z}[X]$ car les polynomes sont unitaires .

On applique alors ces résultats à $P_\chi(\sigma_\chi) = P_{g_\chi}(\sigma_\chi)$ et aux $N_{g_\chi,p}(\sigma_\chi) = \nu_{K_\chi/k_p}$, où k_p est , pour tout $p \mid g_\chi$, l'unique sous-extension de K_χ telle que $[K_\chi : k_p] = p$. Le théorème en résulte immédiatement .

<u>Remarque</u> I 3 . Ce résultat est à rapprocher des résultats de Leopoldt (cf. [15], Satz 4) ; cependant , Leopoldt suppose que les modules considérés sont sans $\mathbb{Z}$-torsion et sa démonstration n'est pas généralisable aux modules de torsion puisqu'elle est obtenue en considérant les $\mathbb{Q}[G_\chi]$-modules $\mathbb{Q} \otimes M(K_\chi)$.

e) <u>Application à la définition de</u> M'_χ . On suppose maintenant que M est une $\mathfrak{S}'$-famille . On pose par analogie :

$$M'_\chi = \{ x \in M(K_\chi) , \ N_{K_\chi/K}\, x = 1 \ , \text{ pour tout } K \subsetneq K_\chi \} .$$

On a donc, puisque $j_{K_\chi/K} \circ N_{K_\chi/K} = \nu_{K_\chi/K}$, $M'_\chi \subset M_\chi$.

Par conséquent, M'_χ est un sous-module de M_χ . On aura $M_\chi = M'_\chi$ pour le caractère χ si et seulement si les restrictions aux sous-modules $N_{K_\chi/K}(M(K_\chi))$ des applications $j_{K_\chi/K}$ sont injectives (pour tout $K \subset K_\chi$).

f) <u>Les</u> M_φ <u>comme</u> $A^{(g_\chi)}$<u>-modules</u> . On rappelle que les M_φ sont des sous-$A[G_\chi]$-modules de $M(K_\chi)$ annulés par $P_\varphi(\sigma_\chi)$. On peut donc les considérer comme des $A[G_\chi]/(P_\varphi(\sigma_\chi))$-modules . Or $P_\varphi \in A[X]$ et est unitaire , donc $A[G_\chi]/(P_\varphi(\sigma_\chi)) \simeq A[X]/(X^{g_\chi}-1 \, , P_\varphi(X)) \simeq A[X]/(P_\varphi(X)) \simeq A^{(g_\chi)}$ (en vertu de l'hypothèse faite sur A , $A^{(g_\chi)}$ engendré par A et les racines de P_φ est un anneau de Dedekind) .
L'isomorphisme (non canonique) peut être réalisé par l'application déduite de la correspondance $\sigma \longrightarrow \chi'(\sigma)$ pour tout $\sigma \in G_\chi$, avec $\chi' | \varphi$ fixé .
On remarquera que pour $\varphi | \chi$, les M_φ sont tous des $A^{(g_\chi)}$-modules , mais les lois scalaires ne sont pas les mêmes .

Dans le cas des caractères rationnels et pour une $\mathfrak{S}'$-famille, les M'_χ sont des sous-$\mathbb{Z}^{(g_\chi)}$-modules de M_χ . On vérifie facilement que si les applications normes $N_{K_\chi/K}$ sont surjectives pour tout $K \subset K_\chi$, alors M_χ / M'_χ a pour exposant un diviseur du produit $\prod_{\substack{p | g_\chi \\ p \text{ premier}}} p$.

5) <u>Un calcul d'indice dans un cas particulier</u> . Soit M une $\mathfrak{G}$-famille . On suppose donné une autre $\mathfrak{G}$-famille $N = (N(K))_{K\in\mathfrak{X}}$. On suppose que pour tout K , N(K) est un sous-A-module de M(K) ; c'est donc un sous-$A[G(K/\mathbb{Q})]$ -module . On aura donc :

$N_\varphi = \{ x \in N(K_\chi) \ , \ P_\varphi x = 1 \} = M_\varphi \cap N(K_\chi)$, pour $\varphi|\chi$, φ irréductible sur k ; N_φ est un sous-$A^{(g_\chi)}$-module de M_φ . On fait alors l'hypothèse suivante : M_φ et N_φ sont des A-modules sans torsion et de rang 1 en tant que $A^{(g_\chi)}$-modules . Il en résulte que M_φ et N_φ sont sans $A^{(g_\chi)}$- torsion (car $A^{(g_\chi)}$ est un anneau de Dedekind) . D'après le théorème de structure des modules sans torsion sur un anneau de Dedekind , M_φ est isomorphe à un idéal entier non nul $\mathfrak{A}$ de $A^{(g_\chi)}$ et dans cet isomorphisme , N_φ a pour image un idéal $\mathfrak{B}$ multiple de $\mathfrak{A}$. Il en résulte que $M_\varphi/N_\varphi \simeq A^{(g_\chi)}/(\mathfrak{B}/\mathfrak{A})$. On a alors , en posant $\mathfrak{B}/\mathfrak{A} = \mathfrak{C}$ (idéal entier non nul) :

$$|M_\varphi/N_\varphi| = |A^{(g_\chi)}/\mathfrak{C}| = |A/N_{k'_\chi/k}\,\mathfrak{C}|.$$

Résumons le principe du calcul :

<u>Proposition</u> I 4 . Soient M et N deux $\mathfrak{G}$-familles de $A[\mathfrak{G}]$-modules sans A-torsion ; on suppose N(K) sous-module de M(K) pour tout $K \in \mathfrak{X}$. Pour $\varphi|\chi$, φ irréductible sur k , soient M_φ et N_φ les sous-modules correspondants en φ . On suppose M_φ et N_φ de rang 1 sur $A^{(g_\chi)}$. Alors l'indice de N_φ dans M_φ est fini et est de la forme :

$$|A/N_{k'_\chi/k}\,\mathfrak{C}|$$

où $\mathfrak{C}$ est un idéal de $A^{(g_\chi)}$ défini de la façon suivante : Soit $M_\varphi \longrightarrow \mathfrak{A}$ un isomorphisme de M_φ sur un idéal entier de $A^{(g_\chi)}$ et soit $\mathfrak{B}$ l'image de N_φ par cet isomorphisme , alors $\mathfrak{C} = \mathfrak{B}/\mathfrak{A}$.

6) <u>Cas d'une</u> $\mathfrak{G}$<u>'-famille où les</u> M(K) <u>sont finis</u> . Soit M une $\mathfrak{G}$'-famille et soit $L\in\mathfrak{X}$ fixé ; on a alors le résultat suivant :

Proposition 15 . Soit $L \in \mathcal{X}$. On suppose que $L/\mathbb{Q}$ est cyclique et que $M(L)$ est un groupe fini . On suppose que pour toute sous-extension K/k de $L/\mathbb{Q}$, la fonction $N_{K/k}$ est surjective ; alors les M'_χ sont finis (pour tout $\chi \in \mathfrak{X}_L$) et on a :

$$|M(L)| = \prod_{\chi \in \mathfrak{X}_L} |M'_\chi| \ .$$

démonstration

Pour faire la démonstration , on peut toujours supposer que les $M(K)$, $K \subset L$, sont des ℓ-groupes : en effet , les ℓ-Sylow des $M(K)$ constituent une $\mathfrak{S}'$-famille si on restreint les applications $N_{L/K}$ et $j_{L/K}$ à ces ℓ-Sylow . On vérifie que les applications $N_{L/K}$ sont encore surjec - tives . Lorsque les $M(K)$ sont des ℓ-groupes , on a le résultat suivant:

Lemme 14 . Si $[K:k]$ est premier à ℓ et l'application $N_{K/k}$ surjective, l'homomorphisme $j_{K/k}$ est injectif .

En effet , soit $y \in M(k)$ tel que $j_{K/k}(y) = 1$; on sait (cf. Prop. 12) que , puisque $N_{K/k}$ est surjective , $N_{K/k} \circ j_{K/k}$ est l'élévation à la puissance $[K:k]$, donc on aura $y^{[K:k]} = 1$ et comme l'ordre de y est premier à $[K:k]$, on en déduit $y = 1$.

Posons $G(L/\mathbb{Q}) = H \times G'$, où H est le ℓ-Sylow de $G(L/\mathbb{Q})$ et G' un sous-groupe d'ordre premier à ℓ . On a le schéma suivant :

$$\begin{tikzcd}
 & G' & & \\
L'_n \arrow[r, dash] \arrow[d, dash] & K_{\psi_n} \arrow[r, dash] \arrow[d, dash] & L_n = L \arrow[d, dash] & \\
L'_i \arrow[r, dash] \arrow[d, dash] & K_{\psi_i} \arrow[r, dash] \arrow[d, dash] & L_i \arrow[d, dash, "\ell^i"] & H \\
L'_0 = \mathbb{Q} \arrow[r, dash] & K_{\psi_0} = K_\psi \arrow[r, dash] & L_0 &
\end{tikzcd}$$

Comme H est cyclique (d'ordre ℓ^n) , l'ensemble des sous-corps de L est de la forme $\{K_{\psi_i}\}$ ($\psi_i \in \mathfrak{X}_L$) où K_{ψ_i} est le composé de K_ψ et de L_i' où K_ψ est le corps correspondant à un élément $\psi = \psi_o$ de $\mathfrak{X}_{L_o}$ (L_o corps fixe par H) et où L_i' est l'unique sous-extension de L_n' (corps fixe par G') de degré ℓ^i sur $\mathbb{Q}$ ($0 \leqslant i \leqslant n$) . Soit $M^*(K_{\psi_i})$ le noyau de la restriction à $M(K_{\psi_i})$ de $N_{\psi_i} = N_{K_{\psi_i}/K_{\psi_{i-1}}}$, pour $i \geqslant 1$, et soit $M^*(K_{\psi_o}) = M(K_{\psi_o})$.

On a les suites exactes de $G(L/\mathbb{Q})$-modules :

$$1 \longrightarrow M^*(K_{\psi_i}) \longrightarrow M(K_{\psi_i}) \xrightarrow{N_{\psi_i}} M(K_{\psi_{i-1}}) \longrightarrow 1 \ , \quad \text{pour } i \geqslant 1 \ .$$

On peut les considérer comme suites exactes de G'-modules donc de $\mathbb{Z}_{(\ell)}[G']$ - modules . Les idempotents de cette algèbre sont ceux de $\mathbb{Q}[G']$ et sont de la forme e'_ψ , pour $\psi \in \mathfrak{X}_{L_o}$, $e'_\psi = \frac{1}{|G'|} \sum_{\sigma \in G'} \psi(\sigma^{-1})\sigma$ (en convenant, dans l'écriture $\psi(\sigma^{-1})$, d'identifier canoniquement G' ainsi que les groupes $G(L_i/L_i')$ avec $G(L_o/\mathbb{Q})$) . D'après Leopoldt (cf. [10] et [12] , partie V , § 2) , comme les applications N sont surjectives et les applications j injectives relativement aux sous-extensions de degré premier à ℓ de $L/\mathbb{Q}$, il va en résulter que :

$M(L_i)^{e'_\psi}$ s'identifie canoniquement à $M(K_{\psi_i})^{e_\psi}$,

$M^*(L_i)^{e'_\psi}$ " " $M^*(K_{\psi_i})^{e_\psi}$, où l'on note par abus $e_\psi = \frac{1}{g_\psi} \sum_{\sigma \in G(K_{\psi_n}/L_n')} \psi(\sigma^{-1})\sigma$. Redonnons brièvement la démonstration dans le cadre plus général des $\mathfrak{G}$'-familles constituées de ℓ-groupes non nécessairement finis :

En décomposant G' modulo $G(L_n/K_{\psi_n})$, on peut écrire $e'_\psi = \frac{\nu_{L_n/K_{\psi_n}}}{[L_n:K_{\psi_n}]} e_\psi$;

or $\nu_{L_n/K_{\psi_n}} M(L_i) = \nu_{L_i/K_{\psi_i}}(M(L_i)) = j_{L_i/K_{\psi_i}} \circ N_{L_i/K_{\psi_i}}(M(L_i)) =$

$j_{L_i/K_{\psi_i}}(M(K_{\psi_i})) \simeq M(K_{\psi_i})$; d'où , puisque $[L_n:K_{\psi_n}]$ est premier à ℓ ,

$M(L_i)^{e'_\psi} \simeq M(K_{\psi_i})^{e_\psi}$. De même , $M^*(L_i)^{e'_\psi} \simeq N_{L_i/K_{\psi_i}}(M^*(L_i))^{e_\psi}$;

il suffit alors de vérifier que , pour $i \geqslant 1$, $N_{L_i/K_{\psi_i}}(M^*(L_i)) = M^*(K_{\psi_i})$:

une inclusion étant évidente , soit $x \in M^*(K_{\psi_i})$; on a $x = N_{L_i/K_{\psi_i}} y$,

$y \in M(L_i)$ et $N_{\psi_i} N_{L_i/K_{\psi_i}} y = 1$ soit $N_{L_i/K_{\psi_{i-1}}} y = 1$ soit

$N_{L_{i-1}/K_{\psi_{i-1}}} N_{L_i/L_{i-1}} y = 1$; par application de $j_{L_{i-1}/K_{\psi_{i-1}}}$ on obtient

$N_{L_i/L_{i-1}} \nu_{L_i/K_{\psi_i}} y = 1$, donc $\nu_{L_i/K_{\psi_i}} y \in M^*(L_i)$; or $\nu_{L_i/K_{\psi_i}} x =$

$x^{[L_i:K_{\psi_i}]} = N_{L_i/K_{\psi_i}} \nu_{L_i/K_{\psi_i}} y \in N_{L_i/K_{\psi_i}}(M^*(L_i))$; comme ℓ ne divise pas $[L_i:K_{\psi_i}]$, il est clair que $x \in N_{L_i/K_{\psi_i}}(M^*(L_i))$.

On déduit alors de [15] (chap. I , § 1,2 et formule (6) , p.21) que $M(K_{\psi_i})^{e_\psi} = \{ x \in M(K_{\psi_i}) , N_{K_{\psi_i}/k}\, x = 1 \text{ pour tout } k, L'_i \subset k \subsetneq K_{\psi_i}\}$

donc $M^*(K_{\psi_i})^{e_\psi} = \{ x \in M^*(K_{\psi_i}) , N_{K_{\psi_i}/k}\, x = 1 , \text{ pour tout } k, L'_i \subset k \subsetneq K_{\psi_i}\}$

(on utilise le fait que les applications $j_{K_{\psi_i}/k}$ sont injectives) . Il résulte de notre définition de M'_χ , que $M^*(K_{\psi_i})^{e_\psi} = M'_{\psi_i}$ pour tout i .

Dans le cas fini, on aura alors : $\prod_{\chi \in \mathfrak{X}_L} |M'_\chi| = \prod_{\psi, i} |M^*(K_{\psi_i})^{e_\psi}| =$

$\prod_{\psi, i} |N^*(L_i)^{e'_\psi}| = \prod_i |N^*(L_i)| = |M^*(L_o)| \prod_{i \geqslant 1} \dfrac{|M(L_i)|}{|M(L_{i-1})|} = |M(L_n)|$.

7) Cas d'une $\mathfrak{G}$ -famille de $\mathbb{Z}_\ell$ -modules . Soit M une $\mathfrak{G}$ -famille . On suppose que les M(K) sont des $\mathbb{Z}_\ell$ -modules , donc des $\mathbb{Z}_\ell[G(K/\mathbb{Q})]$ -modules . On désigne toujours par la lettre ϕ les caractères ℓ -adiques. Etant donné $\chi' \in \mathfrak{X}'$, il éxiste φ' et $\psi' \in \mathfrak{X}'$ uniques tels que $\chi' = \varphi' \psi'$ et tels que φ' soit d' ordre premier à ℓ et ψ' d'ordre une puissance de ℓ . Décomposons G_χ sous la forme $G'_\chi \times H$ (H étant le ℓ - Sylow de G_χ) et posons $g'_\chi = |G'_\chi|$.

On définit $\bar{e}_{\chi'} = \frac{1}{g'_\chi} \sum_{\sigma \in G'_\chi} \varphi'(\sigma^{-1})\sigma$, $\bar{e}_\phi = \frac{1}{g'_\chi} \sum_{\sigma \in G'_\chi} \phi_1(\sigma^{-1})\sigma$,

où ϕ_1 est le caractère ℓ -adique au-dessus de φ' et $\bar{e}_\chi = \frac{1}{g'_\chi} \sum_{\sigma \in G'_\chi} \varphi(\sigma^{-1})\sigma$.

On a donc , en vertu des définitions du § 6 , $\bar{e}_{\chi'} = e_{\varphi'}$, $\bar{e}_\phi = e_{\phi_1}$ et $\bar{e}_\chi = e_\varphi$.

On peut considérer que les $\bar{e}_\phi$ pour $\phi|\chi$ (par exemple) sont les idempotents de l'algèbre $\mathbb{Z}_\ell[G'_\chi]$; ils permettent de décomposer un $\mathbb{Z}_\ell[G_\chi]$-module puisqu'un tel module est canoniquement un $\mathbb{Z}_\ell[G'_\chi]$ -module . L'indiciation $\phi|\chi \longrightarrow \bar{e}_\phi$ est propre .

Nous allons dans le résultat ci-dessous faire le lien avec les définitions antérieures .

Théorème I 2 . Soit M une $\mathfrak{G}$ -famille de $\mathbb{Z}_\ell$ -modules .
Soit $\chi \in \mathfrak{X}$; on a la décomposition : $M_\chi = \bigoplus_{\phi|\chi} M_\phi$. Dans cette décomposition , les sous-modules M_ϕ coïncident avec les sous-modules $M_\chi^{\bar{e}_\phi}$, où $\bar{e}_\phi$ est l'idempotent de $\mathbb{Z}_\ell[G'_\chi]$ associé au caractère $\phi|\chi$.

démonstration

On peut supposer $g_\chi \equiv 0 \bmod \ell$ car sinon on est dans le cas semi-simple et le théorème est alors évident ([17] , partie II) .

Soient deux caractères ℓ -adiques ϕ_1 et ϕ_2 distincts en-dessous de χ ; on pose $P_{\phi_1}(X) = Q_1(X)$, $P_{\phi_2}(X) = Q_2(X)$ (cf. § 4,b pour la définition de P_ϕ) .

Lemme 15 . Il existe U_1 , $U_2 \in \mathbb{Z}_\ell[X]$ tels que $U_1 Q_1 + U_2 Q_2 = 1$.

Comme les polynomes Q_1 et Q_2 sont irréductibles dans $\mathbb{Q}_\ell[X]$, on peut écrire en fait $U_1 Q_1 + U_2 Q_2 = \ell^k$, $k \geqslant 0$, dans $\mathbb{Z}_\ell[X]$ en choisissant U_1 (resp. U_2) de degré inférieur au degré de Q_2 (resp. Q_1) (ceci est toujours possible Q_1 et Q_2 étant unitaires) ; on suppose ensuite les coefficients de U_1 et U_2 non tous divisibles par ℓ ; on peut donc par exemple supposer que les coefficients de U_2 ne sont pas tous divisibles par ℓ . Supposons enfin $k \geqslant 1$.

Soit H_1 le groupe de décomposition de ℓ dans $\mathbb{Q}^{(g_\chi)}/\mathbb{Q}$ et soit ζ une racine de Q_1 dans $\mathbb{Z}_\ell^{(g_\chi)}$ (les autres racines de Q_1 sont les $\zeta^{\sigma_a} = \zeta^a$, pour $\sigma_a \in H_1$) ; on a alors dans $\mathbb{Z}^{(g_\chi)}$:

$U_2(\zeta)\, Q_2(\zeta) = \ell^k$; or $Q_2(X) = \prod_{\sigma_a \in H_1} (X - \zeta_1^{\sigma_a})$, où ζ_1 est de la forme ζ^c avec $\sigma_c \notin H_1$; donc $Q_2(\zeta) = \prod_{\sigma_a \in H_1} (\zeta - \zeta_1^{\sigma_a}) = \prod_{\sigma_a \in H_1} (\zeta - \zeta^{ac}) = \prod_{\sigma_a \in H_1} (\zeta(1 - \zeta^{ac-1}))$. Posons $g_\chi = \ell^n g'_\chi$, $(\ell, g'_\chi) = 1$, $n \geqslant 1$. Pour que $1 - \zeta^{ac-1}$ ne soit pas inversible dans $\mathbb{Z}_\ell^{(g_\chi)}$ il faut et il suffit que l'on ait $ac - 1 \equiv 0 \bmod g'_\chi$, soit $ac \equiv 1\ (g'_\chi)$ ce qui entraîne $\sigma_a\, \sigma_c \in H_1$ car $G(\mathbb{Q}^{(g_\chi)}/\mathbb{Q}^{(g'_\chi)}) \subset H_1$ (l'extension $\mathbb{Q}^{(g_\chi)}/\mathbb{Q}^{(g'_\chi)}$ étant totalement ramifiée) mais $\sigma_a \in H_1$ et on aurait $\sigma_c \in H_1$ ce qui est absurde . Donc $Q_2(\zeta)$ est une unité dans $\mathbb{Z}_\ell^{(g_\chi)}$, d'où $U_2(\zeta) \equiv 0 \bmod \ell$ dans $\mathbb{Z}_\ell^{(g_\chi)}$.

Désignons par $\hat{\mathfrak{P}}_\chi$ l'idéal maximal de $\mathbb{Z}_\ell^{(g_\chi)}$ et soit $\bar{k}$ le corps résiduel de $\mathbb{Q}_\ell^{(g_\chi)}$. Si $P \in \mathbb{Z}_\ell[X]$, désignons par $\bar{P}$ l'image canonique de P dans $\mathbb{F}_\ell[X]$ et soit $\bar{\zeta}$ l'image canonique de ζ dans $\bar{k}$. On a $\bar{Q}_1 = \bar{Q}_o^{\,e}$ où $e = \ell^{n-1}(\ell - 1)$ (indice de ramification de ℓ dans $\mathbb{Q}^{(g_\chi)}$) et où $\bar{Q}_o$ est un polynome irréductible de $\mathbb{F}_\ell[X]$ (c'est donc le polynome irréductible de $\bar{\zeta}$ dans $\mathbb{F}_\ell[X]$). Avec ces notations, tout polynome $P \in \mathbb{Z}_\ell[X]$ tel que $P(\zeta) \equiv 0 \bmod \hat{\mathfrak{P}}_\chi$ est tel que $\bar{P} \in \bar{Q}_o\, \mathbb{F}_\ell[X]$; en particulier on a $\bar{U}_2(\bar{\zeta}) = 0$, donc, dans $\mathbb{F}_\ell[X]$ on aura (puisque $\bar{U}_2 \neq 0$ par hypothèse) :

$\bar{U}_2 = \bar{A}\,\bar{Q}_o^{\alpha}$, $\alpha \geqslant 1$, $\bar{A} \neq 0$, $\bar{Q}_o$ ne divisant pas $\bar{A}$; on désigne par A, Q_o des relèvements de $\bar{A}$, $\bar{Q}_o$ dans $\mathbb{Z}_\ell[X]$ en supposant les coefficients dominants non divisibles par ℓ (il suffit de relever en conservant les degrés). On aura donc $U_2 = A\,Q_o^{\alpha} + \ell B$, $B \in \mathbb{Z}_\ell[X]$ soit $U_2(\zeta) = A(\zeta)\,Q_o^{\alpha}(\zeta) + \ell B(\zeta) \equiv 0 \bmod \ell$, soit $A(\zeta)\,Q_o^{\alpha}(\zeta) \equiv 0 \bmod \ell$. Or $A(\zeta)$ est une unité (car on a supposé $\bar{Q}_o \nmid \bar{A}$), d'où $Q_o^{\alpha}(\zeta) \equiv 0 \bmod \ell$. Montrons que l'on a $\alpha \geqslant e$. Le seul cas où l'on puisse avoir $\ell \mid g_\chi$ et $e = 1$ est le cas $\ell = 2$, $n = 1$. Dans ce cas, on a trivialement $\alpha \geqslant e$. On peut supposer $e > 1$.

On a $P_{g'_\chi}(\zeta) = \prod_{a \in (\mathbb{Z}/g'_\chi\mathbb{Z})^*} (\zeta - \zeta^{\ell^n a}) = \prod_a (\zeta(1 - \zeta^{\ell^n a - 1}))$; or $\zeta^{\ell^n a - 1}$ sera d'ordre une puissance de ℓ si et seulement si $\ell^n a - 1 \equiv 0 \bmod g'_\chi$ soit si et seulement si $a\,\ell^n \equiv 1 \bmod g'_\chi$; ceci, compte-tenu du domaine de variation de a, définit une unique valeur a_o et on a $a_o \ell^n \equiv 1 \bmod g'_\chi$ donc $a_o \ell^n \not\equiv 1 \bmod \ell g'_\chi$ et $\zeta^{a_o \ell^n - 1}$ est une racine de l'unité d'ordre ℓ^n, de telle sorte que $1 - \zeta^{\ell^n a_o - 1} \in \hat{\mathfrak{P}}_\chi \setminus \hat{\mathfrak{P}}_\chi^2$ doù le fait que $P_{g'_\chi}(\zeta) \in \hat{\mathfrak{P}}_\chi \setminus \hat{\mathfrak{P}}_\chi^2$; il en résulte que, en écrivant $P_{g'_\chi} = C Q_o^{\beta} + \ell D$, $C, D \in \mathbb{Z}_\ell[X]$, $C(\zeta) \not\equiv 0 \bmod \hat{\mathfrak{P}}_\chi$, on aura $P_{g'_\chi}(\zeta) \equiv C(\zeta)\, Q_o^{\beta}(\zeta) \bmod \hat{\mathfrak{P}}_\chi^{e}$ soit $Q_o^{\beta}(\zeta) \in \hat{\mathfrak{P}}_\chi \setminus \hat{\mathfrak{P}}_\chi^2$ (car $e > 1$). Ceci entraîne d'une part $\beta = 1$ et, d'autre part, $Q_o(\zeta) \in \hat{\mathfrak{P}}_\chi \setminus \hat{\mathfrak{P}}_\chi^2$. La congruence $Q_o^{\alpha}(\zeta) \equiv 0 \bmod \ell$ obtenue plus haut entraîne donc $\alpha \geqslant e$ et $U_2 = A'\, Q_o^{e} + \ell B$ ($A' = A\, Q_o^{\alpha - e}$) ; mais on a aussi $Q_1 = Q_o^{e} + \ell T$, $T \in \mathbb{Z}_\ell[X]$, soit $U_2 = A'(Q_1 - \ell T) + \ell B = A' Q_1 + \ell S$, $S \in \mathbb{Z}_\ell[X]$. Comme A' est non nul et de coefficient dominant non divisible par ℓ, U_2 est, ici, de degré supérieur ou égal à celui de Q_1, ce qui est absurde. On a donc $\bar{U}_2 = 0$, ce qui est contraire à l'hypothèse, d'où le lemme.

fin de la démonstration du théorème .

Notons $\phi_1, \dots, \phi_m$ les caractères ℓ -adiques distincts au-dessous de χ et notons pour simplifier $Q_1, \dots, Q_m$ les polynomes P_{ϕ_i} ; on a donc d'après le lemme : $\mathbb{Z}_\ell[X] \,/\left(\prod_{i=1}^{m} Q_i(X)\right) = \mathbb{Z}_\ell[X] \,/\, (P_\chi(X)) \simeq \prod_{i=1}^{m} \mathbb{Z}_\ell[X] \,/\, (Q_i(X))$. Il existe donc des éléments $e_i(X) \in \mathbb{Z}_\ell[X]$ dont

les images mod P_χ constituent un système exact d'idempotents orthogoaux . Si q_i désigne l'homomorphisme canonique

$\mathbb{Z}_\ell[X] \longrightarrow \mathbb{Z}_\ell[X] \,/\, (Q_i(X))$, alors $q_i(e_j(X)) = 0$, pour $i \neq j$

et $q_i(e_i(X)) = q_i(1)$; on a $1 \equiv \sum_{k=1}^{m} e_k(X) \bmod P_\chi \mathbb{Z}_\ell[X]$,

$e_i(X)\, e_j(X) \equiv 0 \bmod (P_\chi)$ si $i \neq j$ et $e_i^2(X) \equiv e_i(X) \bmod (P_\chi)$; d'où $1 \equiv \sum_k e_k(\sigma_\chi) \bmod P_\chi(\sigma_\chi)\mathbb{Z}_\ell[G_\chi]$, $e_i(\sigma_\chi)\, e_j(\sigma_\chi) \equiv 0 \bmod (P_\chi(\sigma_\chi))$ pour $i \neq j$ et $e_i^2(\sigma_\chi) \equiv e_i(\sigma_\chi) \bmod (P_\chi(\sigma_\chi))$. On aura donc , puisque $M_\chi^{P_\chi(\sigma_\chi)} = 1$, $M_\chi = \bigoplus_{k=1}^{m} M_\chi^{e_k(\sigma_\chi)}$. Il reste alors à vérifier que $M_\chi^{e_k(\sigma_\chi)} = M_{\phi_k}$:

Si $x \in M_\chi^{e_k(\sigma_\chi)}$, $x = y^{e_k(\sigma_\chi)}$, $y \in M_\chi$ et $x^{Q_k(\sigma_\chi)} = y^{e_k Q_k(\sigma_\chi)}$; or $q_i(e_k(X)\, Q_k(X)) = 0$ pour tout i , donc $e_k(X) Q_k(X) \equiv 0 \bmod P_\chi(X)$ d'où $y^{e_k(\sigma_\chi)\, Q_k(\sigma_\chi)} = 1$ puisque $y \in M_\chi$.

Si $x \in M_{\phi_k}$, alors on écrit $x = \prod_{j=1}^{m} x^{e_j(\sigma_\chi)}$; on a $q_k(e_j) = 0$ si $j \neq k$, donc $e_j(X) \equiv 0 \bmod Q_k(X)$ $(j \neq k)$ et $x^{e_j(\sigma_\chi)} = 1$ pour tout $j \neq k$; on a donc $x = x^{e_k(\sigma_\chi)}$.

Dans l'algèbre $\mathbb{Z}_\ell[G_\chi]/(P_\chi(\sigma_\chi))$, on obtient donc deux systèmes d'idempotents irréductibles : à savoir les images des $\bar{e}_{\phi_i}$ et celles des $e_i(\sigma_\chi)$

dans $\mathbb{Z}_\ell[G_\chi]/(P_\chi(\sigma_\chi))$ (avec les notations précédentes) . Pour vérifier que ces idempotents coïncident pour chaque i il suffit de montrer qu'ils correspondent au même facteur simple de l'algèbre .

Pour cela on remarque que l'homomorphisme défini par $\sigma_\chi \to \chi'(\sigma_\chi)$ avec $\chi'|\phi_j$, induit un homomorphisme de $\mathcal{A} = \mathbb{Z}_\ell[G_\chi]/(P_\chi(\sigma_\chi))$ sur $\mathbb{Z}_\ell^{(g_\chi)}$ dont le noyau (qui ne dépend pas du choix de $\chi'|\phi_j$) est égal à $\bigoplus_{i\neq j} \mathcal{A}\, e_i(\sigma_\chi)$.

Pour montrer que $\mathcal{A}\, e_j(\sigma_\chi) = \mathcal{A}\, \bar{e}_{\phi_j}$, il suffit donc de montrer que $\chi'(\bar{e}_{\phi_j}) \neq 1$; or $\bar{e}_{\phi_j}$ est une somme d'idempotents de la forme $e_{\varphi',k} = \frac{1}{g'_\chi} \sum_{\sigma' \in G'_\chi} \varphi'^k(\sigma')\sigma'^{-1}$ où $\varphi'^k | \phi_o$ (ϕ_o caractère ℓ -adique au-dessus de la composante φ' d'ordre premier à ℓ de χ') . On a alors

$$\chi'(e_{\varphi',k}) = \frac{1}{g'_\chi} \sum_{\sigma' \in G'_\chi} \varphi'^k(\sigma')\, \chi'(\sigma')^{-1} = \frac{1}{g'_\chi} \sum_{\sigma' \in G'_\chi} \varphi'^k(\sigma')\, \varphi'(\sigma')^{-1} \quad \text{qui est}$$

nul pour toutes les valeurs prises par k sauf pour k = 1 , où $\chi'(e_{\varphi'}) = 1$. On a bien $\chi'(\bar{e}_{\phi_j}) \neq 0$.

Le théorème est donc démontré : il constitue la généralisation de la "Δ -décomposition" d'Iwasawa ([12] , § 3) .

<u>Remarque</u> I 4 . Soit M_o un $\mathbb{Z}_\ell[G]$ -module annulé par $P_\chi(\sigma_\chi)$. On peut donc poser $M_o = \bigoplus_{\phi|\chi} M_o^{e_\phi(\sigma_\chi)}$. On sait que $M_o^{e_\phi(\sigma_\chi)}$ coïncide avec le sous-module $M_o^{\bar{e}_\phi}$. Compte-tenu des propriétés des $e_\phi(\sigma_\chi)$, on peut écrire que :

$$M_o^{\bar{e}_\phi} = \{ x \in M_o \ , \ P_\phi(\sigma_\chi)\, x = 1 \} .$$

On peut alors poser la définition suivante :

<u>Définition</u> I 3 . Soit M une $\mathfrak{S}'$-famille de $\mathbb{Z}_\ell$ -modules ; on a $M'_\chi = \bigoplus_{\phi|\chi} M'^{\bar{e}_\phi}_\chi$
Nous posons $M'^{\bar{e}_\phi}_\chi = M'_\phi$ (on a donc $M'_\phi = M'_\chi \cap M_\phi$) .

Chap. II

Application à l'étude des classes relatives des extensions abéliennes.

1) Introduction et définitions . Les groupes des classes des corps $K \in \mathcal{K}$ constituent une $\mathfrak{G}'$-famille $\mathbb{H}$ à laquelle nous allons appliquer les résultats précédents . Différentes propriétés pourront être données sur les modules $\mathbb{H}_\chi$, nous commencerons par le cas des caractères impairs , le cas des caractères pairs , exigeant un approfondissement des résultats de Leopoldt ([15]) , sera traité dans le chapitre suivant .

Si $L \in \mathcal{K}$, on note donc $\mathbb{H}(L)$ le groupe des classes au sens ordinaire de L . Si L est imaginaire , on note $\mathbb{H}'(L)^-$ le groupe des classes relatives (i.e. $\mathbb{H}'(L)^- = \{ h \in \mathbb{H}(L) , N_{L/L_+}(h) = 1\}$, L_+ désignant le sous-corps réel maximal de L) et $\mathbb{H}(L)^+$ le groupe des classes réelles (i.e. le groupe des classes de L_+ : $\mathbb{H}(L)^+ = \mathbb{H}(L_+)$) . On rappelle que (cf. [10]) :

$$|\mathbb{H}(L)| = |\mathbb{H}'(L)^-| \; |\mathbb{H}(L)^+| \quad .$$

Pour le nombre premier ℓ fixé on note $\mathcal{H}(L)$ (resp. $\mathcal{H}'(L)^-$ et $\mathcal{H}(L)^+$) le ℓ-Sylow des groupes $\mathbb{H}(L)$ (resp. $\mathbb{H}'(L)^-$ et $\mathbb{H}(L)^+$) . Les familles $\mathbb{H}$ et $\mathcal{H}$ sont des $\mathfrak{G}'$-familles (les applications N et j associées étant bien connues) .

Dans le cas des groupes $\mathcal{H}(K)$, l'anneau A peut être pris égal à $\mathbb{Z}_\ell$, ce qui permet d'introduire les sous-modules $\mathcal{H}_\phi$ et $\mathcal{H}_\phi'$, pour $\phi \in \Phi$, (caractères ℓ-adiques) , les $\mathcal{H}_\phi$ et $\mathcal{H}_\phi'$ sont donc des $\mathbb{Z}_\ell^{(g_\chi)}$-modules (cf. chap. I , § 4 , f et § 7) .

En ce qui concerne les groupes $\mathbb{H}(K)$, on peut définir les groupes $\mathbb{H}_\chi$ et $\mathbb{H}_\chi'$, qui sont des $\mathbb{Z}^{(g_\chi)}$-modules (cf. chap. I,4 , e et f).

Dans le cas relatif (i.e. $\chi \in \mathcal{X}^-$) on a une simplification importante , à savoir que $\mathbb{H}_\chi' = \mathbb{H}_\chi$.

2) Démonstration de l'égalité $\mathbb{H}_\chi = \mathbb{H}'_\chi$, pour $\chi \in \mathcal{X}^-$.

a) Généralités . Pour démontrer l'égalité en question , il suffit de le faire pour les ℓ -Sylow $\mathcal{H}_\chi$ et $\mathcal{H}'_\chi$.

Lemme II 1 . Supposons $\mathcal{H}'_\chi \subsetneq \mathcal{H}_\chi$. Alors il existe une unique sous-extension K_ψ de K_χ telle que $[K_\chi : K_\psi] = \ell$ et il existe $h \in \mathcal{H}_\chi$ telle que $h' = N_{K_\chi/K_\psi} h$ a les propriétés suivantes :

(i) pour tout p premier , $p \mid g_\chi$, $p \neq \ell$, $\nu_{K_\psi/k'_p}(h') = 1$, k'_p désignant l'unique sous-extension de K_ψ telle que $[K_\psi : k'_p] = p$,

(ii) $j_{K_\chi/K_\psi}(h') = 1$,

(iii) h' est une classe d'ordre ℓ dans $\mathcal{H}(K_\psi)$.

En effet , si $[K_\chi : \mathbb{Q}]$ était premier à ℓ , on serait dans le cas semi-simple (relativement à l'algèbre $\mathbb{Z}_\ell[G_\chi]$) et , dans ce cas , les applications j sont injectives et les applications N surjectives , d'où $\mathcal{H}_\chi = \mathcal{H}'_\chi$ dans ce cas (cf. démonstration de la prop. I 5) . D'où l'existence de K_ψ et son unicité .

Soit alors $h \in \mathcal{H}_\chi$, $h \notin \mathcal{H}_\chi'$ et soit $h' = N_{K_\chi/K_\psi} h$. Soit $p \mid g_\chi$, $p \neq \ell$.

(i) Soit k_p l'unique sous-extension de K_χ telle que $[K_\chi : k_p] = p$:

$$\begin{tikzcd} k_p \arrow[r, dash, "p"] \arrow[d, dash] & K_\chi \arrow[d, dash, "\ell"] \\ k'_p \arrow[r, dash, "p"] & K_\psi \end{tikzcd}$$

On a $\nu_{K_\chi/k_p} h = 1$, donc , par application de N_{K_χ/K_ψ} on aura $\nu_{K_\psi/k'_p} h' = 1$.

(ii) On a $j_{K_\chi/K_\psi} h' = \nu_{K_\chi/K_\psi} h = 1$ puisque $h \in \mathcal{H}_\chi$.

(iii) Comme h' est une classe devenant principale dans K_χ , on sait que son ordre est égal à 1 ou ℓ . Il suffit donc de montrer que $h' \neq 1$. Supposons h' = 1 ; on sait que pour tout $p \neq \ell$, $p | g_\chi$, on a $\nu_{K_\chi / k_p} h = 1$, or l'application j_{K_χ / k_p} est injective (car $p \neq \ell$) et par conséquent , on aura $N_{K_\chi / k_p} h = 1$ et en réalité on aurait $h \in \mathcal{H}'_\chi$, ce qui n'est pas .

Remarquons que malgré (i) , h' n'est pas nécessairement un élément de $\mathcal{H}_\psi$, car on suppose $p \neq \ell$.

Lemme II 2 . Soit L/K une extension cyclique de degré ℓ premier quelconque . Soient E(L) et E(K) les groupes des unités de L et K . Soit j l'homomorphisme $j_{L/K} : \mathbb{H}(K) \longrightarrow \mathbb{H}(L)$. On a la suite exacte :

$$1 \rightarrow \operatorname{Ker} j \longrightarrow E(L)^* / E(L)^{\sigma - 1}$$

où $E(L)^* = \{ \varepsilon \in E(L) , N_{L/K} \varepsilon = 1 \}$ et où σ est un générateur de G(L/K) .

Soient A_L et A_K les anneaux d'entiers de L et K . Si $h' \in \operatorname{Ker} j$, on écrit $h' = cl_K(\mathfrak{a})$, avec $\mathfrak{a} A_L = \alpha A_L$, $\alpha \in L$. On aura donc $(\mathfrak{a} A_L)^{\sigma-1} = A_L$ soit $\alpha^{\sigma - 1} = \varepsilon \in E(L)^*$. Montrons qu'à h' on peut associer la classe de ε modulo $E(L)^{\sigma-1}$: si on écrit $h' = cl_K(\mathfrak{b}) = cl_K(\mathfrak{a})$, alors $\mathfrak{b} = (a)\mathfrak{a}$, $a \in K^*$ et $\mathfrak{b} A_L = \beta A_L$, $\beta \in L$; on aura $\beta^{\sigma - 1} = \eta \in E(L)^*$. Donc $\beta A_L = (a) \mathfrak{a} A_L = a \alpha A_L$, soit $\beta = a \alpha u$, $u \in E(L)$ et $\beta^{\sigma - 1} = \alpha^{\sigma-1} u^{\sigma-1}$ d'où $\eta = \varepsilon u^{\sigma - 1}$. On vérifie qu'on a un homomorphisme .

Si h' est telle que $\alpha^{\sigma - 1} = u^{\sigma-1}$, $u \in E(L)$, alors $a = \alpha u^{-1} \in K$ et $\mathfrak{a} A_L = a A_L$, soit $\mathfrak{a} = a A_K$ et h' = 1 .

Remarque II 1 . On remarque que $E(L)^* / E(L)^{\sigma-1}$ est un groupe d'exposant 1 ou ℓ . En effet, d'après [7](p. 30) , on a $1+X+\ldots+X^{\ell-1} = (X-1)^{\ell-1} - \ell A(X)$ avec $A \in \mathbb{Z}[X]$ et $A(1) = -1$, soit

$A(X) = (X-1)B(X) - 1$, $B \in \mathbb{Z}[X]$; d'où l'égalité :
$\nu_{L/K} = (\sigma-1)^{\ell-1} - \ell(\sigma-1)B(\sigma) + \ell$, ce qui fait que si $\varepsilon \in E(L)^*$ (i.e. $\nu_{L/K}(\varepsilon) = 1$) , alors $\varepsilon^{\ell} \in E(L)^{\sigma-1}$.

b) Etude du cas $\ell \neq 2$. On suppose désormais que $L/\mathbb{Q}$ est cyclique et imaginaire . Si L/K est de degré $\ell \neq 2$, K est aussi imaginaire. On introduit alors les sous-corps réels maximaux de L et K ; L_+ et K_+ :

$$\begin{tikzcd} L_+ \arrow[r, dash, "2"] \arrow[d, dash, "\ell"'] & L \arrow[d, dash, "\ell"] \\ K_+ \arrow[r, dash, "2"] & K \end{tikzcd}$$

Lemme II 3 . Soit T_L^* le ℓ-Sylow du groupe de torsion de $E(L)^*$ (T_L^* est donc l'ensemble des racines de l'unité ζ de L d'ordre une puissance de ℓ telles que $N_{L/K}\zeta = 1$) . Alors l'image de $\mathcal{H}(K)^- \cap \operatorname{Ker} j$ (dans la suite exacte du lemme II 2) est contenue dans $q(T_L^*)$, q étant l'homomorphisme canonique $E(L)^* \longrightarrow E(L)^* / E(L)^{\sigma-1}$.

En effet, si $h' \in \mathcal{H}(K)^- \cap \operatorname{Ker} j$, cela signifie que $\nu_{K/K_+} h' = 1$, soit $h'\overline{h'} = 1$, en désignant de façon générale par $\overline{}$ la conjugaison complexe . On a donc , si $h' = cl_K(\mathfrak{a})$, $\mathfrak{a}\overline{\mathfrak{a}} = a A_K$, $a \in K^*$, soit $\mathfrak{a} A_L \overline{\mathfrak{a}} A_L = a A_L$ avec (puisque $h' \in \operatorname{Ker} j$) $\mathfrak{a} A_L = \alpha A_L$ et $\overline{\mathfrak{a}} A_L = \overline{\alpha} A_L$, ce qui donne $a A_L = \alpha\overline{\alpha} A_L$ soit $\alpha\overline{\alpha} = au$, $u \in E(L)$; $\alpha^{\sigma-1}\overline{\alpha}^{\sigma-1} = u^{\sigma-1}$ soit (avec $\alpha^{\sigma-1} = \varepsilon \in E(L)^*$) $\varepsilon\overline{\varepsilon} = u^{\sigma-1}$; on a donc $q(\varepsilon)q(\overline{\varepsilon}) = 1$; or ([10], Satz 24) , on peut décomposer ε en un produit de la forme $\varepsilon_0\zeta$, $\varepsilon_0 \in E(L_+)$ et ζ racine de l'unité ; d'où $q(\overline{\varepsilon}) = q(\varepsilon_0\overline{\zeta})$ mais $\overline{\zeta} = \zeta^{-1}$, d'où $q(\varepsilon\overline{\varepsilon}) = q(\varepsilon_0^2) = 1$, (on a donc $\pm\varepsilon_0 \in E(L)^*$; on peut donc toujours supposer que c'est ε_0) , soit $q(\varepsilon_0) = 1$; on a donc $\varepsilon_0 \in E(L)^{\sigma-1}$ et $\zeta \in E(L)^*$ et $q(\varepsilon) = q(\zeta)$; comme $E(L)^*/E(L)^{\sigma-1}$ est d'exposant ℓ , on a bien $q(\varepsilon) \in q(T_L^*)$. Il suffit alors de déterminer $q(T_L^*)$:

<u>Lemme</u> II 4 . Le groupe $q(T_L^*)$ est d'ordre 1 ou ℓ . Il est d'ordre ℓ si et seulement si $T_L^* = \langle \zeta_1 \rangle$ et $E(L)^{\sigma-1} \cap \langle \zeta_1 \rangle = (1)$ (ζ_1 désignant une racine primitive ℓ^e de l'unité) .

Soit ζ un générateur de T_L^* (ζ est d'ordre une puissance de ℓ et on peut supposer $\zeta \neq 1$, sinon $q(T_L^*) = \mathcal{H}(K)^- \cap \operatorname{Ker} j = (1)$) . On a $q(T_L^*) \simeq T_L^* / E(L)^{\sigma-1} \cap T_L^*$. Si $\zeta \in K$, alors $N_{L/K}\zeta = \zeta^\ell$, donc dans ce cas $\zeta^\ell = 1$ et $\zeta = \zeta_1 \in K$. Si $\zeta \notin K$, c'est que $L = K(\zeta)$; comme $[L:K] = \ell$, cela signifie que $\zeta_1 \in K$ nécessairement et que $\zeta^\ell \in K$; donc L/K est une extension de Kummer , c.-à-d. que $\zeta^\sigma = \zeta_1 \zeta$, soit $N_{L/K}\zeta = \zeta_1^{1+2+\ldots+(\ell-1)}\zeta^\ell$ soit $N_{L/K}\zeta = \zeta^\ell \in K$. On aura donc encore $\zeta^\ell = 1$ soit $\zeta = \zeta_1$, mais alors il y a contradiction avec l'hypothèse $\zeta \notin K$. Finalement $T_L^* = \langle \zeta_1 \rangle$ et par conséquent $E(L)^{\sigma-1} \cap T_L^* = \langle \zeta_1 \rangle$ ou (1) .

<u>Lemme</u> II 5 . Si l'on suppose $\mathcal{H}(K)^- \cap \operatorname{Ker} j \neq (1)$, alors ce groupe est d'ordre ℓ et l'extension L/K est une extension de Kummer de type " classe " (i.e. de la forme $K(\sqrt[\ell]{a})$, $a \in K^*$, $a A_K = \mathfrak{a}^\ell$, $\mathfrak{a}$ non principal ; cete propriété ne dépend alors pas du choix de a) .

En effet , si $\mathcal{H}(K)^- \cap \operatorname{Ker} j \neq (1)$, cela signifie que $q(T_L^*)$ est d'ordre ℓ , donc que $T_L^* = \langle \zeta_1 \rangle$ et $E(L)^{\sigma-1} \cap \langle \zeta_1 \rangle = (1)$ (lemme II 4) . Donc $\zeta_1 \in K$ (car $[L:K] = \ell$) et L/K est bien une extension de Kummer .

Soit h' une classe non triviale de $\mathcal{H}(K)^- \cap \operatorname{Ker} j$; on a $h' = cl_K(\mathfrak{a}) \neq 1$, avec $h'^\ell = 1$ et $\mathfrak{a} A_L = \alpha A_L$, $\alpha \in L$; on a $\alpha^{\sigma-1} = \varepsilon$, $\varepsilon \in E(L)^*$; on sait (lemme II 3) que $q(\varepsilon) = q(\zeta_1^k)$ soit $\varepsilon = \zeta_1^k u^{\sigma-1}$, $u \in E(L)$, d'où $\alpha^{\sigma-1} = \zeta_1^k u^{\sigma-1}$ et , dans l'égalité $\mathfrak{a} A_L = \alpha A_L$, on peut toujours supposer que α est choisi de telle sorte que $\alpha^{\sigma-1} = \zeta_1^k$; de plus , on aura $k \not\equiv 0 \bmod \ell$ car sinon α serait dans K et $\mathfrak{a}$ serait principal . D'où $\alpha^{\sigma-1} = \zeta_1'$, ζ_1' d'ordre ℓ et $\alpha^\ell \in K$, d'où $L = K(\alpha)$ est l'extension de Kummer $K(\sqrt[\ell]{a})$ avec $a = \alpha^{\ell}$; on a bien $a A_L = \mathfrak{a}^{\ell} A_L$ soit, puisque $a \in K$, $a A_K = \mathfrak{a}^{\ell}$.

Remarquons que nous avons en fait démontré le résultat suivant : Si les extensions L, K sont imaginaires et galoisiennes sur $\mathbb{Q}$ et L/K_+ cyclique de degré 2ℓ, $\ell \neq 2$, alors $\mathcal{H}(K)^- \cap \operatorname{Ker} j$ est d'ordre 1 ou ℓ et cet ordre est ℓ si et seulement si L/K est une extension de Kummer de type "classe".

Montrons maintenant que la situation du lemme II 5 est impossible pour une extension $L/\mathbb{Q}$ cyclique.

Comme $L = K(\sqrt[\ell]{a})$, avec $a A_K = \mathfrak{a}^{\ell}$, cela signifie que seuls les idéaux premiers au-dessus de ℓ peuvent se ramifier dans L/K.

Décomposons alors $L/\mathbb{Q}$ de la façon suivante :

$$\begin{tikzcd}
L' \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash, "\ell"] \\
K' \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash] \\
\mathbb{Q} \arrow[r, dash] & L_o
\end{tikzcd}$$

avec L/L_o et $L'/\mathbb{Q}$ cycliques d'ordre une puissance de ℓ, L/L' et $L_o/\mathbb{Q}$ cycliques d'ordre premier à ℓ. Soit p un nombre premier ramifié dans $L'/\mathbb{Q}$; ce nombre premier sera ramifié dans L'/K' donc dans L/K ; ceci implique donc $p = \ell$ et ℓ est totalement ramifié dans $L'/\mathbb{Q}$ et c'est donc le seul.

Ceci permet d'identifier l'extension $L'/\mathbb{Q}$: son conducteur sera une puissance de ℓ (ℓ^{k+1}, $k \geqslant 1$), $L'/\mathbb{Q}$ sera l'unique sous-extension de degré ℓ^k de $\mathbb{Q}^{(\ell^{k+1})}$ et K' l'unique sous-extension de degré ℓ^{k-1} de $\mathbb{Q}^{(\ell^k)}$. Comme $\zeta_1 \in K$, on aura $\mathbb{Q}^{(\ell^k)} \subset K$, $\mathbb{Q}^{(\ell^{k+1})} \subset L$ et $\mathbb{Q}^{(\ell^{k+1})} \not\subset K$, par conséquent $L = K(\zeta)$, avec ζ d'ordre ℓ^{k+1}.

Il suffit alors d'appliquer la théorie de Kummer qui montre que $a = \zeta^{\lambda\ell} b^{\ell}$, $(\lambda, \ell) = 1$, $b \in K^*$, soit $a A_K = b^{\ell} A_K = \mathfrak{a}^{\ell}$, soit $\mathfrak{a}$ principal, ce qui n'est pas. D'où le fait, dans le cas $\ell \neq 2$, pour $L/\mathbb{Q}$ imaginaire cyclique et pour L/K cyclique de degré ℓ, que $\mathcal{H}(K)^- \cap \operatorname{Ker} j = (1)$.

c) <u>Etude du cas</u> $\ell = 2$. L'extension $L/\mathbb{Q}$ étant encore supposée cyclique imaginaire , dans ce cas K est nécessairement égale à L_+ .

D'après Hasse ([10], Satz 24) l'indice des unités Q_L^- est égal à 1 , lorsque $L/\mathbb{Q}$ est cyclique ; donc , on aura pour tout $\varepsilon \in E(L)^*$, $\varepsilon = \varepsilon_o \zeta$, $\varepsilon_o \in K$, ζ racine de l'unité ; $N_{L/K}\,\varepsilon = 1$ donne ici $\varepsilon_o^2 = 1$ soit $\varepsilon_o = \pm 1$ et ε est une racine de l'unité . Comme on peut représenter, dans $E(L)^* / E(L)^{\sigma-1}$, ε par une racine d'ordre une puissance de 2 et que $L/\mathbb{Q}$ est cyclique , on aura $q(\varepsilon) = q(1)$, $q(-1)$, $q(i)$ ou $q(-i)$.

Soit $h' \in \operatorname{Ker} j$; on suppose $h' \neq 1$; on a $h' = cl_K(\mathfrak{a})$ avec $\mathfrak{a} A_L = \alpha A_L$ et $\alpha^{\sigma-1} = \varepsilon \in E(L)^*$. Quitte à modifier α modulo $E(L)$, on peut supposer $\varepsilon \in \{\pm 1 , \pm i\}$:

(i) Supposons $\varepsilon = \pm 1$. Alors $\alpha^{\sigma-1} = -1$ en fait et $\alpha^2 \in K^*$, donc on obtient pour L/K une extension de type " classe " ($L = K(\sqrt{a})$, avec $a = \alpha^2$ et $a A_K = \mathfrak{a}^2$, $\mathfrak{a}$ non principal) .

(ii) Supposons $\varepsilon = \pm i$; alors $\alpha^{\sigma-1} = \pm i$. On a $(\pm i)^{\sigma-1} = -1$ car $i \in L$ et $i \notin K$; donc on peut toujours supposer que $\alpha^{\sigma-1} = i$. On en déduit aussi que $\alpha^2 i^{-1} \in K$. Posons $\alpha^2 = ic$, $c \in K^*$; il en résulte que $\mathfrak{a}^2 A_L = \alpha^2 A_L = c A_L$ soit $\mathfrak{a}^2 = c A_K$. Soit τ un générateur de $G(L/\mathbb{Q})$; on a $\alpha^{2\tau} = i^\tau c^\tau = -i c^\tau = -c^{\tau-1}\alpha^2$, soit $\alpha^{2\tau} = \alpha^2 d$, $d \in K^*$; on aura donc $(\alpha A_L)^{2\tau} = (\alpha A_L)^2\, d\, A_L$ soit $\mathfrak{a}^{2\tau} A_L = \mathfrak{a}^2 A_L\, d\, A_L$ soit $\mathfrak{a}^{2\tau} = \mathfrak{a}^2\, d\, A_K$. Si $d \in K^{*2}$, on aura $d = e^2$, $e \in K^*$ et $\mathfrak{a}^\tau \sim \mathfrak{a}$ soit, que h' est une classe ambige dans $K/\mathbb{Q}$.

Si $d \notin K^{*2}$, la relation $\alpha^{2\tau} = \alpha^2 d$ montre que $d = (\alpha^{\tau-1})^2$, $d \in L^{*2}$; d'après la théorie de Kummer , puisque $L = K(\sqrt{d}) = K(i)$, on aura $\alpha^{\tau-1} = if$, $f \in K^*$, soit $d = -f^2$ et on aura $\mathfrak{a}^{2\tau} = \mathfrak{a}^2 f^2 A_K$ soit encore h' classe ambige dans $K/\mathbb{Q}$. Or L est le composé des extensions linéairement disjointes $K/\mathbb{Q}$ (réelle) et $\mathbb{Q}(i)/\mathbb{Q}$ (imaginaire) , donc $[K:\mathbb{Q}]$ est nécessairement impair et une classe ambige dans $K/\mathbb{Q}$ ne peut être d'ordre pair , d'où une absurdité dans le cas (ii) (on aurait $h' = 1$) .

On est alors ramené au cas (i) . Comme dans le cas $\ell \neq 2$, on décompose L sous la forme suivante :

$$\begin{tikzcd} L' \arrow[r, dash] \arrow[d, dash] & L \arrow[d, dash, "2"] \\ K' \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash] \\ \mathbb{Q} \arrow[r, dash] & L_o \end{tikzcd}$$

avec L/L_o et $L'/\mathbb{Q}$ cycliques d'ordre une puissance de 2 et $L_o/\mathbb{Q}$ et L/L' de degré impair . Comme dans le cas $\ell \neq 2$, on montre que L' est de conducteur une puissance de 2 (soit 2^{k+1} , $k \geqslant 1$) .

L'extension de Kummer L'/K' est de la forme $L' = K'(\sqrt{a})$, $a \in K'$ et comme le conducteur de L' est une puissance de 2 et que 2 est totalement ramifié , on aura $a A_{K'} = \mathfrak{a}^2$ ou $\mathfrak{a}^2 \mathfrak{P}$ ($\mathfrak{P}$ idéal premier au-dessus de 2) ; comme tous les sous-corps de $\mathbb{Q}^{(2^{k+1})}$ sont principaux (au sens ordinaire) , on voit que a sera équivalent soit à une unité soit à une uniformisante (on peut d'ailleurs vérifier que c'est ce dernier (cas) qui a lieu) . Il en sera donc de même pour l'extension L/K ; comme 2 est non ramifié dans K/K', l'extension de Kummer L/K ne peut être de type classe (en effet, si par exemple $a A_{K'} = \mathfrak{P}$ et si on suppose $a A_K = \mathfrak{a}^2$, on a une absurdité) .

On a donc au cours des § b et c démontré le résultat suivant :

<u>Proposition</u> II 1 . Pour toute extension $L/\mathbb{Q}$ imaginaire cyclique et pour L/K cyclique de degré ℓ , on a (où $j_{L/K}$ est relatif à la famille $\mathcal{H}$) :

$$\mathcal{H}(K)^- \cap \operatorname{Ker} j_{L/K} = (1) \text{ si } \ell \neq 2 \text{ et } \operatorname{Ker} j_{L/K} = (1) \text{ si } \ell = 2.$$

<u>Corollaire</u> II 1 . Soit $L/\mathbb{Q}$ cyclique imaginaire et soit L_+ le sous-corps réel maximal de L . Posons $\mathbb{H}'(L)^- = \{ h \in \mathbb{H}(L) , N_{L/L_+}(h) = 1 \}$ et $\mathbb{H}(L)^- = \{ h \in \mathbb{H}(L) , \nu_{L/L_+} h = 1 \}$; alors on a $\mathbb{H}'(L)^- = \mathbb{H}(L)^-$.

C'est la proposition précédente pour $\ell = 2$.

On rappelle que , classiquement , $\mathbb{H}'(L)^-$ s'appelle le groupe des classes relatives de L .

d) <u>Conclusion</u>. On est en mesure de démontrer le résultat annoncé.

<u>Théorème</u> II 1. Pour tout $\chi \in \mathfrak{X}^-$, on a $\mathbb{H}'_\chi = \mathbb{H}_\chi$ et pour tout $\phi \in \Phi^-$, on a $\mathcal{H}'_\phi = \mathcal{H}_\phi$.

<u>démonstration</u>

On rappelle qu'il suffit de le démontrer pour les groupes $\mathcal{H}'_\chi$ et $\mathcal{H}_\chi$. Supposons $\mathcal{H}'_\chi \neq \mathcal{H}_\chi$ et appliquons le lemme II 1 (on aura alors $L = K_\chi$ et $K = K_\psi$) :

Si $\ell \neq 2$, la classe h' du lemme II 1 est une classe relative de K_ψ (dans (i) du lemme II 1, on fait $p = 2$ qui divise effectivement g_χ puisque $\chi \in \mathfrak{X}^-$) et de plus elle vérifie $j_{K_\chi/K_\psi} h' = 1$ donc $h' \in \mathcal{H}(K_\psi)^- \cap \operatorname{Ker} j$, d'où $h' = 1$ (Prop. II 1), ce qui contredit l'hypothèse $\mathcal{H}'_\chi \subsetneq \mathcal{H}_\chi$ (d'après le lemme II 1, (iii)).

Si $\ell = 2$, alors K_ψ est réel et on remarque que $h' \in \operatorname{Ker} j_{K_\chi/K_\psi}$ et on aura $h' = 1$ (Prop. II 1), d'où le théorème.

Signalons que la proposition II 1 est fausse lorsque $L/\mathbb{Q}$ n'est pas cyclique: prenons par exemple $K = \mathbb{Q}(\sqrt{-6})$ et $L = \mathbb{Q}(\sqrt{-6}, \sqrt{2})$; alors l'extension L/K est non ramifiée et L est d'ailleurs le corps de classes de Hilbert de K; la classe (relative) d'ordre 2 de K devient principale dans L.

3) <u>Détermination de</u> $|\mathbb{H}_\chi|$ <u>pour</u> $\chi \in \mathfrak{X}^-$.

<u>Proposition</u> II 2. On suppose l'extension $L/\mathbb{Q}$ cyclique ; alors on a :

$$|\mathbb{H}(L)| = \prod_{\chi \in \mathfrak{X}_L} |\mathbb{H}'_\chi| \,, \quad |\mathbb{H}(L)^+| = \prod_{\chi \in \mathfrak{X}_L^+} |\mathbb{H}'_\chi| \quad \text{et} \quad |\mathbb{H}(L)^-| = \prod_{\chi \in \mathfrak{X}_L^-} |\mathbb{H}_\chi| \,.$$

<u>démonstration</u>

Prouvons que les fonctions normes (norme des classes habituelles) sont surjectives dans toutes les sous-extensions K/k de $L/\mathbb{Q}$. Il suffit encore de le faire relativement aux ℓ -Sylow des groupes de classes . On sait que la surjectivité a lieu dès que toutes les sous-extensions de degré ℓ dans $L/\mathbb{Q}$ sont ramifiées . On considère le schéma ci-dessous :

$$\begin{tikzcd}[arrows=dash]
L' \arrow[r] \arrow[d] & L \arrow[d] \\
L'_1 \arrow[r] \arrow[d, "\ell"'] & L_1 \arrow[d, "\ell"] \\
\mathbb{Q} \arrow[r] & L_o
\end{tikzcd}$$

où L/L_o et $L'/\mathbb{Q}$ sont cycliques de degré une puissance de ℓ et où L/L' et $L_o/\mathbb{Q}$ sont de degré premier à ℓ .

Soit p un nombre premier ramifié dans $L'_1/\mathbb{Q}$ (ce qui existe); p est totalement ramifié dans $L'/\mathbb{Q}$ (car $L'/\mathbb{Q}$ est cyclique de degré une puissance de ℓ) ; p est donc ramifié dans toute sous-extension de degré ℓ de $L/\mathbb{Q}$.

On peut donc appliquer la proposition I 5 , ce qui démontre que $|\mathbb{H}(L)| = \prod_{\chi \in \mathfrak{X}_L} |\mathbb{H}'_\chi|$. Si L est imaginaire , on a $|\mathbb{H}(L)| = |\mathbb{H}(L)^+|\,|\mathbb{H}(L)^-|$; on peut donc encore appliquer la proposition I 5 au sous-corps réel L_+ de L : on aura $|\mathbb{H}(L)^+| = \prod_{\chi \in \mathfrak{X}_{L_+}} |\mathbb{H}'_\chi| = \prod_{\chi \in \mathfrak{X}_L^+} |\mathbb{H}'_\chi|$, d'où l'expression de $|\mathbb{H}(L)^-|$ compte-tenu du fait que $\mathbb{H}'_\chi = \mathbb{H}_\chi$ pour $\chi \in \mathfrak{X}^-$ (th. II 1) .
Pour une extension $L/\mathbb{Q}$ imaginaire quelconque , on sait ([10], p. 12) que $|\mathbb{H}'(L)^-| = Q_L^- \, w_L \prod_{\chi' \in \mathfrak{X}'^-_L} \left(-\frac{1}{2} B_1(\chi'^{-1})\right)$, où w_L est le nombre de racines de l'unité contenues dans L et Q_L^- l'indice des unités . D'après Hasse ([10] , Satz 24) , on a $Q_L^- = 1$ lorsque L est cyclique .

Posons $\alpha_\chi = 1$ ou 0 selon que g_χ est une puissance de 2 ou non et soit w_χ défini de la manière suivante : $w_\chi = 1$ si K_χ n'est pas un corps cyclotomique (imaginaire) ; dans le cas contraire , K_χ est nécessairement de la forme $\mathbb{Q}^{(\ell^n)}$, ℓ premier , $n \geqslant 1$ et alors $w_\chi = \ell$.

Théorème II 2 , Pour tout $\chi \in \mathfrak{X}^-$, on a $|\mathbb{H}'_\chi| = |\mathbb{H}_\chi| = 2^{\alpha_\chi} w_\chi \prod_{\chi'|\chi} \frac{-1}{2} B_1(\chi'^{-1})$,

démonstration

On utilise la proposition III g de [18] (cf. aussi [15], I, §1,4): il suffit de prouver que pour toute extension $L/\mathbb{Q}$ imaginaire cyclique ,

$|\mathbb{H}(L)^-| = \prod_{\chi \in \mathfrak{X}_L^-} \left(2^{\alpha_\chi} w_\chi \prod_{\chi'|\chi} \frac{-1}{2} B_1(\chi'^{-1})\right)$, Compte-tenu de l'égalité

$|\mathbb{H}(L)^-| = \prod_{\chi \in \mathfrak{X}_L^-} |\mathbb{H}_\chi|$ de la proposition II 2 , on en déduira l'égalité annoncée . Il reste donc à vérifier que $\prod_{\chi \in \mathfrak{X}_L^-} (2^{\alpha_\chi} w_\chi) = w_L$.

Calculons $\prod_{\chi \in \mathfrak{X}_L^-} 2^{\alpha_\chi}$. Pour cela on décompose $L/\mathbb{Q}$ de la façon suivante:

$$\begin{tikzcd}
L' \arrow[r, dash] & L \\
L'_+ \arrow[u, dash, "2"] \arrow[r, dash] & L_+ \arrow[u, dash, "2"'] \\
\mathbb{Q} \arrow[u, dash] \arrow[r, dash] & L_0 \arrow[u, dash]
\end{tikzcd}$$

avec L/L_0 de degré une puissance de 2 et L/L' de degré impair .

Comme L'_+ et L_+ sont réels , il est clair que tous les α_χ sont nuls sauf pour l'unique χ_0 correspondant à L' pour lequel $\alpha_\chi = 1$.

D'où $\prod_{\chi \in \mathfrak{X}_L^-} 2^{\alpha_\chi} = 2$.

Si L ne contient aucun corps cyclotomique (autre que $\mathbb{Q}$) c'est que $w_L = 2$, mais par ailleurs tous les w_χ seront égaux à 1 et on a bien l'égalité voulue dans ce cas . Soit $\mathbb{Q}^{(\ell'')}$ le plus grand corps cyclotomique contenu dans L . On a alors les schémas suivants :

$$\begin{tikzcd}
 & L_+ \arrow[r, dash, "2"] & L \\
 & \mathbb{Q}_+^{(\ell'')} \arrow[u, dash] \arrow[r, dash] & \mathbb{Q}^{(\ell'')} \arrow[u, dash] \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Q}_+^{(\ell)} \arrow[u, dash] \arrow[r, dash] & \mathbb{Q}^{(\ell)} \arrow[u, dash]
\end{tikzcd}$$

$\ell \neq 2$

$$\begin{tikzcd}
L_+ \arrow[r, dash, "2"] & L \\
\mathbb{Q} \arrow[u, dash] \arrow[r, dash] & \mathbb{Q}^{(4)} \arrow[u, dash]
\end{tikzcd}$$

$\ell = 2$

Dans le cas $\ell \neq 2$, on aura $\prod_{\chi \in \mathfrak{X}_L^-} w_\chi = \ell^n$ et dans le cas $\ell = 2$, on aura $\prod_{\chi \in \mathfrak{X}_L^-} w_\chi = 2$, d'où le résultat (à rapprocher de [10], chap. III , § 33 , th. 34 et suivants) .

Remarque II 2 . Pour toute extension imaginaire $L \in \mathcal{K}$, on a $|\mathbb{H}'(L)^-| = \frac{Q_L^- w_L^-}{2^{n_L^-}} \prod_{\chi \in \mathfrak{X}_L^-} |\mathbb{H}_\chi|$, où n_L^- est le nombre de sous-extensions imaginaires cycliques de L de degré une puissance de 2 et où w_L^- est la 2-participation à w_L $\left(\text{resp. } \frac{w_L}{2} \right)$ si $\mathbb{Q}^{(4)} \not\subset L$ (resp. $\mathbb{Q}^{(4)} \subset L$) .

En effet , on a , en vertu des définitions et du calcul de $|\mathbb{H}_\chi|$: $|\mathbb{H}'(L)^-| = Q_L^- w_L \prod_{\chi \in \mathfrak{X}_L^-} \left(\frac{|\mathbb{H}_\chi|}{2^{\alpha_\chi} w_\chi} \right)$. Il suffit donc de calculer $\frac{w_L}{\prod_{\chi \in \mathfrak{X}_L^-} (2^{\alpha_\chi} w_\chi)}$

Posons $w_L^+ = \frac{w_L}{w_L^-}$; comme un corps cyclotomique (autre que $\mathbb{Q}$) est cyclique sur $\mathbb{Q}$ si et seulement si il est de la forme $\mathbb{Q}^{(\ell^n)}$ ($n \geqslant 1$ pour $\ell \neq 2$, $n = 2$ pour $\ell = 2$) , il en résulte que $\prod_{\chi \in \mathfrak{X}_L^-} w_\chi = w_L^+$ si $w_L^- = 2$ et est égal à $2\, w_L^+$ si $w_L^- \geqslant 4$. En résumé , on a

$$\frac{w_L}{\prod_{\chi \in \mathfrak{X}_L^-} w_\chi} = w_L^- \quad \left(\text{resp. } \frac{w_L^-}{2} \right) \text{ si } \mathbb{Q}^{(4)} \text{ n'est pas inclus dans } L$$

(resp. est inclus dans L) . Le reste en résulte immédiatement .

On remarque que le coefficient $\frac{Q_L^- w_L^-}{2^{n_L^-}}$ est une puissance de 2 et que $\frac{Q_L^- w_L^-}{2^{n_L^-}}$ est en général une puissance négative ou nulle de 2.

4) Généralisation d'un résultat d'Iwasawa .

a) Généralités sur ce résultat . On rappelle que dans [11], Iwasawa démontre la formule suivante : Lorsque L est le corps $\mathbb{Q}^{(\ell^n)}$, $\ell \neq 2$, $n \geq 1$, alors le nombre de classes relatives de L est donné par l'expression:

$$|\mathbb{H}(L)^-| = |\,\mathbb{Z}[G]^- \;/\; S_L\mathbb{Z}[G] \cap \mathbb{Z}[G]^-|,$$

avec $G = G(\mathbb{Q}^{(\ell^n)}/\mathbb{Q})$, $\mathbb{Z}[G]^- = \{\omega \in \mathbb{Z}[G],\ (1+\tau)\omega = 0\}$, τ étant la conjugaison complexe , et $S_L = \frac{1}{\ell^n} \sum_{\substack{a=1 \\ (a,\ell)=1}}^{\ell^n} a\,\sigma_a^{-1}$ l'élément de Stickelberger relatif à L , σ_a étant le $\mathbb{Q}$-automorphisme élévation des racines ℓ^n e de l'unité à la puissance a .

On peut se convaincre facilement que le résultat ci-dessus ne se généralise pas immédiatement au cas d'une extension abélienne imaginaire quelconque : par exemple , soit L le composé de $\mathbb{Q}_+^{(7)}$ et de $\mathbb{Q}^{(3)}$; calculons $\mathbb{Z}[G]^- \;/\; S_L\mathbb{Z}[G] \cap \mathbb{Z}[G]^-$ avec , cette fois , $G = G(L/\mathbb{Q})$ et S_L l'élément de Stickelberger associé à L . On trouve

$$S_L = \frac{1}{3}(\,2 + \sigma + 2\sigma^2 + 4\sigma^3 + 5\sigma^4 + 4\sigma^5\,),$$

où σ est un générateur convenable de G . On voit que $\mathbb{Z}[G]^- = (\sigma^3-1)\mathbb{Z}[G]$ et que $S_L\mathbb{Z}[G] \cap \mathbb{Z}[G]^- = 3(\sigma-1)\,S_L\mathbb{Z}[G]$; le quotient à étudier est donc $(\sigma^3-1)\mathbb{Z}[G] \;/\; 3(\sigma-1)\,S_L\mathbb{Z}[G]$. Si on utilise l'homomorphisme $N_{L/K} : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[\bar{G}]$, où $K = \mathbb{Q}^{(3)}$ et $\bar{G} = G(K/\mathbb{Q})$, on constate que $N_{L/K}(3(\sigma-1)\,S_L\mathbb{Z}[G]) = (0)$ et que $N_{L/K}((\sigma^3-1)\mathbb{Z}[G]) = (\bar{\sigma}-1)\,\mathbb{Z}[\bar{G}]$ ($\bar{\sigma}$ générateur de $\bar{G}$) , d'où une surjection de $\mathbb{Z}[G]^- \;/\; S_L\mathbb{Z}[G] \cap \mathbb{Z}[G]^-$ sur le groupe infini $(\bar{\sigma}-1)\mathbb{Z}[G]$. Par conséquent , l'analogue pour L , du quotient proposé par Iwasawa pour $\mathbb{Q}^{(\ell^n)}$, est inadapté . Nous allons , dans ce paragraphe , lever cette ambiguité en donnant une définition différente . On constatera que , comme dans le cas de l'interprétation arithmétique du nombre de classes des corps réels par Leopoldt au moyen de χ-unités convenables , l'utilisation de χ -objets conduit à une expression non triviale dans tous les cas .

b) <u>Elément de Stickelberger</u> ([4], [2], [16]) . Soit $K \in \mathcal{K}$.

On rappelle que :

$$S_K = \frac{1}{f_K} \sum_{a=1}^{f_K}{}^{*} a \left(\frac{K}{a}\right)_{f_K}^{-1}$$

est appelé l'élément de Stickelberger pour le corps K . Ici f_K est le conducteur de K , $\left(\frac{K}{a}\right)_{f_K}$ pour $(a, f_K) = 1$, le symbole d'Artin défini comme étant la restriction à K du $\mathbb{Q}$ -automorphisme σ_a de $\mathbb{Q}^{(f_K)}/\mathbb{Q}$ défini sur les racines f_K^{e} de l'unité par l'élévation à la puissance a ; enfin $\sum_{a=1}^{f_K}{}^{*}$ désigne $\sum_{\substack{a=1 \\ (a,f_K)=1}}^{f_K}$.

On aura les deux $\mathfrak{S}$-familles suivantes à étudier : la $\mathfrak{S}'$-famille M , pour laquelle $M(K) = \mathbb{Z}[G(K/\mathbb{Q})]$ et la $\mathfrak{S}$-famille N définie par $N(K) = S_K \mathbb{Z}[G(K/\mathbb{Q})] \cap \mathbb{Z}[G(K/\mathbb{Q})]$, pour tout $K \in \mathcal{K}$ (cf. chap. I , § 3 , c pour la définition des applications $N_{L/K}$ et $j_{L/K}$ relativement à M) .

<u>Lemme</u> II 6 . Pour tout $c \in \mathbb{Z}$, $(c,f_K) = 1$, $\left(\left(\frac{K}{c}\right) - c\right) S_K \in \mathbb{Z}[G(K/\mathbb{Q})]$.

On écrit , pour $1 \leqslant a < f_K$, $(a,f_K) = 1$, $\left(\frac{K}{a}\right)^{-1} = \left(\frac{K}{ac}\right)^{-1}\left(\frac{K}{c}\right)$

on a donc : $c\, S_K = \frac{1}{f_K} \sum_{a=1}^{f_K}{}^{*} c\, a \left(\frac{K}{ac}\right)^{-1}\left(\frac{K}{c}\right) = \left(\frac{K}{c}\right) \frac{1}{f_K} \sum_{a=1}^{f_K}{}^{*} ([ac] + \lambda_a f_K)\left(\frac{K}{ac}\right)^{-1}$,

où $[\ ]$ désigne le reste modulo f_K compris entre 0 et f_K . On a donc

$$c\, S_K \equiv \left(\frac{K}{c}\right) \frac{1}{f_K} \sum_{a=1}^{f_K}{}^{*} [ac] \left(\frac{K}{ac}\right)^{-1} \mod \mathbb{Z}[G(K/\mathbb{Q})] \quad , \quad \text{or}$$

$$\frac{1}{f_K}\sum_{a=1}^{f_K}{}^{*}\,[ac]\left(\frac{K}{ac}\right)^{-1} = \frac{1}{f_K}\sum_{b=1}^{f_K}{}^{*}\; b\left(\frac{K}{b}\right)^{-1} = S_K \;.$$

<u>Définition</u> II 1 . Posons $\mathfrak{U}_K = \{\omega \in \mathbb{Z}[G(K/\mathbb{Q})] \;,\; \omega S_K \in \mathbb{Z}[G(K/\mathbb{Q})]\}$ ($\mathfrak{U}_K$ est un idéal de $\mathbb{Z}[G(K/\mathbb{Q})]$ et on a $N(K) = S_K \mathfrak{U}_K$) . Définissons Λ_K comme étant le plus petit entier positif tel que $\Lambda_K\, S_K \in \mathbb{Z}[G(K/\mathbb{Q})]$ (on a $\Lambda_K | f_K$) ; pour $K = K_\chi$ nous posons $\Lambda_{K_\chi} = \Lambda_\chi$.

<u>Proposition</u> II 3 . L'idéal $\mathfrak{U}_K$ est un $\mathbb{Z}$-module libre dont une $\mathbb{Z}$-base est de la forme $\left(\ldots, \left(\frac{K}{a}\right) - a \;, \ldots \;; \Lambda_K\right)$, où a parcourt un ensemble de résidus mod f_K , $(a, f_K) = 1$, représentant $G(K/\mathbb{Q}) \setminus \{1\}$.

<u>démonstration</u>

D'après le lemme II 6 , $\left(\frac{K}{a}\right) - a \in \mathfrak{U}_K$ pour tout a , $(a, f_K) = 1$ et $\Lambda_K \in \mathfrak{U}_K$ par définition . A la place de la notation $\left(\frac{K}{a}\right) - a$, on peut écrire provisoirement $\sigma - a_\sigma$, $\sigma \in G(K/\mathbb{Q})$, $\sigma \neq 1$, les a_σ étant choisis une fois pour toutes tels que $\left(\frac{K}{a_\sigma}\right) = \sigma$.

Soit $\omega \in \mathfrak{U}_K$, $\omega = \sum_{\sigma \in G(K/\mathbb{Q})} x_\sigma \sigma$, $\omega S_K = \sum_{\sigma \in G(K/\mathbb{Q})} x_\sigma \sigma S_K$

$= \sum_{\substack{\sigma \in G(K/\mathbb{Q}) \\ \sigma \neq 1}} x_\sigma (\sigma - a_\sigma) S_K + x_1 S_K + S_K \sum_{\substack{\sigma \in G(K/\mathbb{Q}) \\ \sigma \neq 1}} x_\sigma a_\sigma$; comme $(\sigma - a_\sigma) S_K \in \mathbb{Z}[G(K/\mathbb{Q})]$, on doit avoir $S_K\left(x_1 + \sum_{\substack{\sigma \in G(K/\mathbb{Q}) \\ \sigma \neq 1}} x_\sigma a_\sigma\right) \in \mathbb{Z}[G(K/\mathbb{Q})]$.

Posons $\Lambda' = x_1 + \sum_{\substack{\sigma \in G(K/\mathbb{Q}) \\ \sigma \neq 1}} x_\sigma a_\sigma$; comme l'ensemble des $\Lambda' \in \mathbb{Z}$ tels que $\Lambda' S_K \in \mathbb{Z}[G(K/\mathbb{Q})]$ est un idéal de $\mathbb{Z}$, il est de la forme $\Lambda_K \mathbb{Z}$ où Λ_K est le nombre défini dans l'énoncé , donc $\Lambda' \in \Lambda_K \mathbb{Z}$ et $\omega \in (\ldots, \sigma - a_\sigma, \ldots \Lambda_K)$. Reste à voir que l'on a une $\mathbb{Z}$-base . Si $\sum_{\sigma \neq 1} x_\sigma(\sigma - a_\sigma) + x_1 \Lambda_K = 0$, alors

$\sum_{\sigma\neq 1} x_\sigma \sigma + x_1 \Lambda_K - \sum_{\sigma\neq 1} x_\sigma a_\sigma = 0$ dans $\mathbb{Z}[G(K/\mathbb{Q})]$, d'où $x_\sigma = 0$ pour tout $\sigma \neq 1$, mais alors $x_1 \Lambda_K = 0$ entraîne $x_1 = 0$. Le fait que Λ_K divise f_K est évident .

Corollaire II 2 . Si K est supposé cyclique sur $\mathbb{Q}$ alors $\mathfrak{U}_K = \left(\left(\frac{K}{a}\right) -a, \Lambda_K\right)$ (idéal de $\mathbb{Z}[G(K/\mathbb{Q})]$) , où a est tel que $\left(\frac{K}{a}\right)$ engendre $G(K/\mathbb{Q})$.

En effet , soit c , $(c, f_K) = 1$; alors $\left(\frac{K}{c}\right) = \left(\frac{K}{a}\right)^n$ pour un certain n , donc il existe $b \in \mathbb{Z}$ tel que $\left(\frac{K}{b}\right) = 1$ et tel que $c \equiv a^n b \bmod f_K$. On aura (d'après le lemme II 6) $\left(\frac{K}{b}\right) - b \in \Lambda_K \mathbb{Z}$ donc $b \equiv 1 \bmod \Lambda_K$ et $\left(\frac{K}{c}\right) - c \equiv \left(\frac{K}{a}\right)^n - a^n b \equiv \left(\frac{K}{a}\right)^n - a^n \bmod \Lambda_K$ soit $\left(\frac{K}{c}\right) - c \equiv \left[\left(\frac{K}{a}\right) - a\right]\left[\left(\frac{K}{a}\right)^{n-1} + \ldots + a^{n-1}\right] \bmod \Lambda_K$ et $\left(\frac{K}{c}\right) - c \in \left(\left(\frac{K}{a}\right) - a , \Lambda_K\right)$.

Définition II 2 . Soit α_σ le coefficient de $\sigma \in G(K/\mathbb{Q})$ dans la sommation $\sum_{a=1}^{f_K} {}^* a \left(\frac{K}{a}\right)^{-1}$ (on a en particulier $\alpha_1 = \sum_{\substack{a=1 \\ \sigma_a \in G(\mathbb{Q}^{(f_K)}/K)}}^{f_K} {}^* a$) .

Lemme II 7 . On a $\alpha_\sigma \equiv c\, \alpha_1 \bmod f_K$ où c est un entier premier à f_K .

On a $\alpha_\sigma = \sum_{\substack{a=1 \\ \sigma_a \in \sigma^{-1} H}}^{f_K} {}^* a$, où $H = G(\mathbb{Q}^{(f_K)}/K)$. En écrivant σ_b , $(b, f_K) = 1$, les éléments de H , on a $\alpha_\sigma = \sum_{\substack{a=1 \\ \sigma_a = \sigma_c \sigma_b}}^{f_K} {}^* a$, où l'on a posé $\sigma^{-1} = \sigma_c$, $(c, f_K) = 1$. On a donc $\alpha_\sigma = \sum_{\substack{b=1 \\ \sigma_b \in H}}^{f_K} {}^* [bc] \equiv \sum_{\substack{b=1 \\ \sigma_b \in H}}^{f_K} {}^* bc \equiv$

$$c \sum_{\substack{b=1 \\ \sigma_b \in H}}^{f_K}{}^{*} b \equiv c\,\alpha_1 \bmod f_K \text{ , d'où le lemme .}$$

Corollaire II 3 . On a $\Lambda_K = \dfrac{f_K}{\operatorname{pgcd}(f_K, \alpha_1)}$.

En effet , Λ_K sera le plus petit entier Λ tel que $\dfrac{\Lambda \alpha_1}{f_K}$ soit dans $\mathbb{Z}$ (compte-tenu du fait que $\Lambda_K S_K \in \mathbb{Z}[G(K/\mathbb{Q})]$ si et seulement si $\dfrac{\Lambda_K \alpha_\sigma}{f_K} \in \mathbb{Z}$ pour tout $\sigma \in G(K/\mathbb{Q})$ donc en fait , d'après le lemme II 7 , pour une seule valeur de σ , $\sigma = 1$ par exemple) .

c) Etude de M_χ et N_χ pour $\chi \in \mathfrak{X}$. On a $M(K_\chi) = \mathbb{Z}[G_\chi]$ et $N(K_\chi) = S_{K_\chi} \mathfrak{U}_{K_\chi}$ ($N(K_\chi)$ est un idéal de $M(K_\chi)$) . On a $M_\chi = \{\omega \in \mathbb{Z}[G_\chi],\ P_\chi\,\omega = 0\}$ et $N_\chi = S_{K_\chi} \mathfrak{U}_{K_\chi} \cap M_\chi$ (M_χ et N_χ sont encore deux idéaux de $M(K_\chi)$) . Considérons l'homomorphisme d'anneau , surjectif, qu'on appelle encore $\chi' : \mathbb{Z}[G_\chi] \longrightarrow \mathbb{Z}^{(g_\chi)}$, défini par $\sigma_\chi \longrightarrow \chi'(\sigma_\chi)$; son noyau est égal à $P_\chi(\sigma_\chi)\mathbb{Z}[G_\chi]$: en effet , on a $\mathbb{Z}[G_\chi] \simeq \mathbb{Z}[X]/(X^{g_\chi} - 1)$; en appelant encore χ' l'homomorphisme défini par $\chi'(X) = \chi'(\sigma_\chi)$, on a le diagramme commutatif :

$$\begin{tikzcd} \mathbb{Z}[X] \arrow[r, "\chi'"] \arrow[d] & \mathbb{Z}^{(g_\chi)} \\ \mathbb{Z}[G_\chi] \arrow[ur, "\chi'"'] & \end{tikzcd} \qquad X \mapsto \chi'(\sigma_\chi),\ \sigma_\chi$$

Lemme II 8 . Le restriction de χ' à M_χ est un isomorphisme de M_χ sur un idéal entier $\mathfrak{a}_\chi$ de $\mathbb{Z}^{(g_\chi)}$ et dans cet isomorphisme , N_χ correspond à un idéal entier $\mathfrak{b}_\chi$ de $\mathbb{Z}^{(g_\chi)}$ multiple de $\mathfrak{a}_\chi$.

Montrons que cette restriction est injective : Soit $\omega \in M_\chi$ tel que $\chi'(\omega) = 0$; si $\omega = \sum_{i=0}^{g_\chi - 1} a_i \sigma_\chi^i$ appelons $\omega(X)$ le représentant

$\sum_{i=0}^{g_\chi -1} a_i X^i$. Alors $\omega(X) = P_\chi(X)\, A(X)$ dans $\mathbb{Z}[X]$ (car $\omega \in P_\chi(\sigma_\chi)\, \mathbb{Z}[G_\chi]$)

et $P_\chi(\sigma_\chi)\omega = 0$ entraîne $P_\chi(X)\, \omega(X) = B(X)(X^{g_\chi} - 1)$ dans $\mathbb{Z}[X]$; il en résulte que $P_\chi^2(X)\, A(X) = B(X)(X^{g_\chi} - 1)$ soit $P_\chi(X)\, A(X) = B(X)\, Q(X)$ avec $Q(X) = \dfrac{X^{g_\chi} - 1}{P_\chi(X)} \in \mathbb{Z}[X]$; P_χ étant irréductible, il va diviser B nécessairement, d'où $B(X) = C(X)\, P_\chi(X)$ et $A(X) = C(X)\, Q(X)$ dans $\mathbb{Z}[X]$, d'où $\omega(X) = P_\chi(X)\, C(X)\, Q(X) = C(X)(X^{g_\chi} - 1)$ et $\omega = 0$ dans $\mathbb{Z}[G_\chi]$, d'où l'injectivité. La restriction de χ' à N_χ sera aussi injective. Cette application établit donc des isomorphismes de M_χ et N_χ sur des idéaux entiers $\mathfrak{a}_\chi$ et $\mathfrak{b}_\chi$ de $\mathbb{Z}^{(g_\chi)}$; comme $N_\chi \subset M_\chi$, on aura $\mathfrak{b}_\chi \subset \mathfrak{a}_\chi$ soit $\mathfrak{a}_\chi \mid \mathfrak{b}_\chi$.

α) <u>Détermination de $\mathfrak{a}_\chi$</u>.

<u>Lemme II 9</u>. L'image de M_χ par χ' est l'idéal $\mathfrak{a}_\chi = \prod_{\substack{p \mid g_\chi \\ p \text{ premier}}} \left(1 - \chi'(\sigma_\chi)^{g_\chi/p}\right) \mathbb{Z}^{(g_\chi)}$.
On a en outre $M_\chi = \left(\prod_{\substack{p \mid g_\chi \\ p \text{ premier}}} (1 - \sigma_\chi^{g_\chi/p}) \right) \mathbb{Z}[G_\chi]$.

Nous appliquons le théorème I 1 à la $\mathfrak{S}$-famille M :

On a $M_\chi = \{\omega \in \mathbb{Z}[G_\chi],\ \nu_{K_\chi/k_p}\, \omega = 0$, pour tout p premier, $p \mid g_\chi\}$.

Ecrivons $\omega = \sum_{i=0}^{g_\chi -1} a_i \sigma_\chi^i \in M_\chi$; écrivons, pour p fixé, $i = \lambda + \mu \dfrac{g_\chi}{p}$, $0 \leq \lambda < g_\chi/p$ et $0 \leq \mu \leq p-1$; $\omega = \sum_{\lambda,\mu} a_{\lambda + \mu g_\chi/p}\, \sigma_\chi^\lambda\, \sigma_\chi^{\mu g_\chi/p} = \sum_{\lambda=0}^{g_\chi/p-1} \sigma_\chi^\lambda \sum_{\mu=0}^{p-1} a_{\lambda+\mu g_\chi/p}\, \sigma_\chi^{\mu g_\chi/p}$. La condition $\nu_{K_\chi/k_p}\, \omega = 0$ conduit à $\sum_{\mu'=0}^{p-1} \sigma_\chi^{\mu' g_\chi/p}\, \omega = 0$ soit $\sum_{\lambda=0}^{g_\chi/p-1} \sigma_\chi^\lambda \sum_{\mu=0}^{p-1} a_{\lambda+\mu g_\chi/p}\, \nu_{K_\chi/k_p} = 0$ soit $\sum_{\mu=0}^{p-1} a_{\lambda+\mu g_\chi/p} = 0$, pour $\lambda = 0, \dots, g_\chi/p - 1$. Calculons alors

l'image de ω par χ' en tenant compte de ces relations : $\chi'(\omega) =$
$$\sum_{\lambda=0}^{g_\chi/p-1} \chi'(\sigma_\chi)^\lambda \sum_{\mu=0}^{p-1} a_{\lambda+\mu g_\chi/p} (\chi'(\sigma_\chi)^{\mu g_\chi/p} -1) \in (1-\chi'(\sigma_\chi)^{g_\chi/p}) \mathbb{Z}^{(g_\chi)}$$

(car $\chi'(\sigma_\chi)^{g_\chi/p}$ est une racine de l'unité d'ordre p) . Comme les idéaux $(1-\chi'(\sigma_\chi)^{g_\chi/p})$ sont , pour les p distincts divisant g_χ , premiers entre eux deux à deux , $\chi'(\omega) \in \mathfrak{a}_\chi$. Réciproquement soit $\omega_0 = \prod_{p|g_\chi} (1-\sigma_\chi^{g_\chi/p})$, il est clair que $\omega_0 \in M_\chi$ et que $\chi'(\omega_0)$ engendre $\mathfrak{a}_\chi$; comme l'homomorphisme $\mathbb{Z}[G_\chi] \xrightarrow{\chi'} \mathbb{Z}^{(g_\chi)}$ est surjectif , il en résulte que $\chi'(\omega_0\, \mathbb{Z}[G_\chi]) = \mathfrak{a}_\chi$ donc que $\mathfrak{a}_\chi = \chi'(M_\chi)$. D'après le lemme II 8 , on en déduit l'égalité $M_\chi = \omega_0\, \mathbb{Z}[G_\chi]$.

β) <u>Détermination de $\mathfrak{b}_\chi$</u> . On a $N_\chi = \{ \omega \in S_{K_\chi} \mathfrak{U}_{K_\chi},\ P_\chi\, \omega = 0 \}$ et , d'après le théorème I 1 , on a $N_\chi = \{\omega \in S_{K_\chi} \mathfrak{U}_{K_\chi},\ \nu_{K_\chi/k_p}\, \omega = 0, p|g_\chi\}$.
On rappelle (corol. II 2) que si $\sigma_\chi = \left(\frac{K_\chi}{a}\right)$ pour un certain a , $(a, f_\chi)=1$, alors $\mathfrak{U}_{K_\chi}$ est l'idéal de $\mathbb{Z}[G_\chi]$ engendré par $\sigma_\chi - a$ et Λ_χ.

Pour étudier N_χ , on a besoin d'étudier les S_{K_χ} et notamment l'action de ν_{K_χ/k_p} sur les S_{K_χ} ou (ce qui revient au même puisque les applications j_{K_χ/k_p} sont injectives) l'action des N_{K_χ/k_p} , ce qui est préférable car on a alors des homomorphismes d'algèbres.

(i) <u>Etude de $N_{L/K}\, S_L$</u> . Soit L/K une extension quelconque $K, L \in \mathcal{K}$. On a $S_L = \frac{1}{f_L} \sum_{a=1}^{f_L}{}^{*}\, a \left(\frac{L}{a}\right)_{f_L}^{-1}$ et
$$S_K = \frac{1}{f_K} \sum_{b=1}^{f_K}{}^{*}\, b\left(\frac{K}{b}\right)_{f_K}^{-1}$$ considérés respectivement dans $\mathbb{Q}[G(L/\mathbb{Q})]$ et $\mathbb{Q}[G(K/\mathbb{Q})]$, où $\left(\frac{L}{a}\right)_{f_L}$ $\left(\text{resp. } \left(\frac{K}{b}\right)_{f_K}\right)$ est la restriction à L (resp. K)

du $\mathbb{Q}$-automorphisme σ_a de $\mathbb{Q}^{(f_L)}$ (resp. σ_b de $\mathbb{Q}^{(f_K)}$) .

On aura $N_{L/K}\, S_L = \frac{1}{f_L} \sum_{a=1}^{f_L}{}^{*}\; a \left(\frac{K}{a}\right)_{f_K}^{-1}$ (car $\left(\frac{K}{a}\right)_{f_L} = \left(\frac{K}{a}\right)_{f_K}$ puisque $f_K \mid f_L$) .

On va , pour simplifier les calculs , utiliser la convention suivante : on fixe le corps K dans tout le § (i) et on pose

$S_f = \frac{1}{f} \sum_{a=1}^{f}{}^{*}\; a \left(\frac{K}{a}\right)_{f_K}^{-1}$, pour tout $f \in \mathbb{N}$ tel que $K \subset \mathbb{Q}^{(f)}$ (on a nécessairement $f \equiv 0 \bmod f_K$) . On pose $d^f = [\mathbb{Q}^{(f)} : K]$ et $\vartheta = \vartheta_{K/\mathbb{Q}}$.

On a alors $S_K = S_{f_K}$ et $N_{L/K}\, S_L = S_{f_L}$.

<u>Lemme II 10</u> . Soit f tel que $K \subset \mathbb{Q}^{(f)}$ et soit p un nombre premier . On suppose que si $p \mid f$, le symbole $\left(\frac{K}{p}\right)_f^{-1}$ est 0 par convention .

Alors on a la relation :

$$S_{pf} = \left(1 - \left(\frac{K}{p}\right)_f^{-1}\right) S_f + \frac{p-1}{2}\, d^f \vartheta \ .$$

On a $S_{pf} = \frac{1}{pf} \sum_{b=1}^{pf}{}^{*}\; b \left(\frac{K}{b}\right)_{f_K}^{-1}$. On distingue deux cas selon que p divise f ou non et l'on pose dans les deux cas :

$b = a + \lambda f$, $b \in \{1, 2, \ldots, pf\}$, $(b, pf) = 1$, $0 \leqslant a < f$ (la condition $(b, pf) = 1$ équivaut donc à $(a, f) = 1$ et $(a + \lambda f, p) = 1$) ; $0 \leqslant \lambda < p$.

<u>Premier cas</u> : $p \mid f$. Dans ce cas , la seule condition $(a, f) = 1$ équivaut à $(a + \lambda f, pf) = 1$; $S_{pf} = \frac{1}{pf} \sum_{a=1}^{f}{}^{*} \sum_{\lambda=0}^{p-1} (a + \lambda f) \left(\frac{K}{a + \lambda f}\right)_{f_K}^{-1} =$

$$= \frac{1}{pf} \sum_{a=1}^{f}{}^{*} \sum_{\lambda=0}^{p-1} a \left(\frac{K}{a}\right)^{-1}_{f_K} + \frac{1}{p} \sum_{a=1}^{f}{}^{*} \sum_{\lambda=0}^{p-1} \lambda \left(\frac{K}{a}\right)^{-1}_{f_K} =$$

$$\frac{1}{f} \sum_{a=1}^{f}{}^{*} a \left(\frac{K}{a}\right)^{-1}_{f_K} + \frac{p-1}{2} \sum_{a=1}^{f}{}^{*} \left(\frac{K}{a}\right)^{-1}_{f_K}$$, d'où le résultat dans ce cas .

<u>Deuxième cas</u> : $p \nmid f$. On a $S_{pf} = \frac{1}{pf} \sum_{a=1}^{f}{}^{*} \sum_{\lambda=0}^{p-1} (a+\lambda f) \left(\frac{K}{a+\lambda f}\right)^{-1}_{f_K}$

$$- \frac{1}{pf} \sum_{a=1}^{f}{}^{*} \sum_{a+\lambda f \equiv 0\ (p)} (a+\lambda f) \left(\frac{K}{a+\lambda f}\right)^{-1}_{f_K}$$. Dans l'intervalle

$0 \leqslant \lambda < p-1$, et pour a fixé , $a+\lambda f$ prend une fois et une seule , une valeur nulle mod p ; si on appelle λ_a la valeur de λ correspondante et si l'on pose $a+\lambda_a f = n_a p$, on a $0 < n_a < f$. Comme $(a,f) = 1$, $a+\lambda_a f$ est premier à f et réciproquement . Donc n_a parcourt l'ensemble des valeurs $0 < n_a < f$, $(n_a, f) = 1$. On aura :

$$S_{pf} = \frac{1}{f} \sum_{a=1}^{f}{}^{*} a \left(\frac{K}{a}\right)^{-1}_{f_K} + \frac{p-1}{2} \sum_{a=1}^{f}{}^{*} \left(\frac{K}{a}\right)^{-1}_{f_K} - \frac{1}{pf} \sum_{a=1}^{f}{}^{*} n_a p \left(\frac{K}{n_a p}\right)^{-1}_{f_K} ;$$

le terme $\frac{1}{pf} \sum_{a=1}^{f}{}^{*} n_a p \left(\frac{K}{n_a p}\right)^{-1}_{f_K}$ s'écrit $\left(\frac{K}{p}\right)^{-1}_{f_K} \frac{1}{f} \sum_{a=1}^{f}{}^{*} n_a \left(\frac{K}{n_a}\right)^{-1}_{f_K}$

et d'après la propriété des n_a, on obtient : $\frac{1}{f} \left(\frac{K}{p}\right)^{-1}_{f_K} \sum_{a=1}^{f}{}^{*} a \left(\frac{K}{a}\right)^{-1}_{f_K}$.

D'où le lemme .

Passons maintenant au cas général : on pose :

$$f_K = p_1^{a_1} \ldots p_r^{a_r} \quad \text{et} \quad f_L = p_1^{b_1} \ldots p_1^{b_r} q_1^{c_1} \ldots q_t^{c_t} , \ 1 \leqslant a_i \leqslant b_i , \ t \geqslant 0 , \ c_j \geqslant 1 .$$

Théorème II 3 . On a :

(i) Si $t = 0$, $N_{L/K} S_L = S_K + \frac{1}{2}(p_1^{b_1-a_1} \dots p_r^{b_r-a_r} - 1)[\mathbb{Q}^{(f_K)} : K]\, \vartheta_{K/\mathbb{Q}}$;

(ii) Si $t \geqslant 1$, $N_{L/K} S_L = \prod_{i=1}^{t} \left(1 - \left(\frac{K}{q_i}\right)^{-1}_{f_K} \right) S_K +$

$$+ \frac{1}{2}\, p_1^{b_1-a_1} \dots p_r^{b_r-a_r} \varphi(q_1^{c_1} \dots q_t^{c_t})[\mathbb{Q}^{(f_K)} : K]\, \vartheta_{K/\mathbb{Q}} ;$$

(iii) Si l'on pose $S'_L = S_L - \frac{1}{2}[\mathbb{Q}^{(f_L)} : L]\, \vartheta_{L/\mathbb{Q}}$ alors , on a dans tous les cas $N_{L/K} S'_L = \prod_{\substack{q \mid f_L \\ q \nmid f_K}} \left(1 - \left(\frac{K}{q}\right)^{-1}_{f_K} \right) S'_K$.

Cas (i) . On a $f_K = p_1^{a_1} \dots p_r^{a_r}$, $f_L = p_1^{b_1} \dots p_r^{b_r}$, $1 \leqslant a_i \leqslant b_i$.
On démontre par récurrence sur $\sum_{i=1}^{r} (b_i - a_i)$:

Si la somme est nulle ($f_K = f_L$) le 2^e terme du membre de droite est bien nul .

Il suffit alors de faire la démonstration en augmentant b_1 par exemple d'une unité. On aura alors : $S_{p_1 f_L} = (1-0)\, S_{f_L} + \frac{p_1 - 1}{2} \sum_{a=1}^{f_L}{}^{*} \left(\frac{K}{a}\right)_{f_L}$

$= S_{f_K} + \frac{1}{2}(p_1^{b_1-a_1} \dots p_r^{b_r-a_r} - 1)\, d^{f_K} \vartheta + \frac{p_1 - 1}{2}\, d^{f_L} \vartheta$ avec les notations du lemme II 10 ; mais $d^{f_L} = d^{f_K} \dfrac{\varphi(f_L)}{\varphi(f_K)}$ et

$$\frac{\varphi(f_L)}{\varphi(f_K)} = \frac{p_1^{b_1-1} \dots p_r^{b_r-1} (p_1-1) \dots (p_r-1)}{p_1^{a_1-1} \dots p_r^{a_r-1} (p_1-1) \dots (p_r-1)} = p_1^{b_1-a_1} \dots p_r^{b_r-a_r} \quad \text{et}$$

$$S_{p_1 f_L} = S_{f_K} + \frac{1}{2}(p_1^{b_1-a_1}\dots p_r^{b_r-a_r}-1)\, d^{f_K}\vartheta + \frac{p_1-1}{2}\, p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\, d^{f_K}\vartheta =$$

$$S_{f_K} + \frac{1}{2}\, d^{f_K}(p_1^{b_1-a_1+1}\dots p_r^{b_r-a_r}-1)\,\vartheta\ .$$

Cas (ii) . Se démontre aussi par récurrence sur $\sum_{j=1}^{t} c_j$.

Si cette somme est égale à 1 , on a $f_K = p_1^{a_1}\dots p_r^{a_r}$ et $f_L = p_1^{b_1}\dots p_r^{b_r}\, q$, $q \notin \{p_1,\dots,p_r\}$; posons $f = p_1^{b_1}\dots p_r^{b_r}$; $S_{f_L} = \left(1-\left(\frac{K}{q}\right)_f^{-1}\right) S_f + \frac{q-1}{2}\, d^f\vartheta$

mais S_f se calcule d'après (i) : $S_f = S_{f_K} + \frac{1}{2}(p_1^{b_1-a_1}\dots p_r^{b_r-a_r}-1)\, d^{f_K}\vartheta$

et $d^f = p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\, d^{f_K}$, d'où $S_{f_L} = \left(1-\left(\frac{K}{q}\right)_{f_K}^{-1}\right) S_{f_K}$ +

$$+ \left(1-\left(\frac{K}{q}\right)_{f_K}^{-1}\right) d^{f_K}\vartheta\ \frac{1}{2}\,(p_1^{b_1-a_1}\dots p_r^{b_r-a_r}-1)$$

$$+ \frac{q-1}{2}\, d^{f_K}\vartheta\ p_1^{b_1-a_1}\dots p_r^{b_r-a_r} \qquad ; \text{mais } \left(1-\left(\frac{K}{q}\right)_{f_K}^{-1}\right)\vartheta = 0$$

car $\left(\frac{K}{q}\right)_{f_K} \neq 0$ et $\left(\frac{K}{q}\right)_{f_K} \in G(K/\mathbb{Q})$. On a donc

$S_{f_L} = \left(1-\left(\frac{K}{q}\right)_{f_K}^{-1}\right) S_{f_K} + \frac{1}{2}\, p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\ \varphi(q)\, d^{f_K}\vartheta$ et le premier pas de la récurrence est démontré .

Supposons la relation démontrée pour $f_L = p_1^{b_1}\dots p_r^{b_r} q_1^{c_1}\dots q_t^{c_t}$. Il y a alors deux cas : on rajoute un nombre premier q distinct des p_i et des q_j ou bien on augmente c_1 par exemple d'une unité . Dans le premier cas on commence par appliquer le premier pas de la récurrence avec en plus $b_i = a_i$ pour $1 \leqslant i \leqslant r$:

$$S_{f_L q} = \left(1-\left(\frac{K}{q}\right)^{-1}_{f_L}\right) S_{f_L} + \frac{q-1}{2}\, d^{f_L}\vartheta =$$

$$= \left(1-\left(\frac{K}{q}\right)^{-1}_{f_K}\right) \prod_{i=1}^{t} \left(1-\left(\frac{K}{q_i}\right)^{-1}_{f_K}\right) S_{f_K} + \frac{q-1}{2}\, d^{f_L}\vartheta \ ,$$

$$(q-1)\, d^{f_L} = \frac{\varphi(f_L)}{\varphi(f_K)}\,(q-1)\, d^{f_K} = \frac{\varphi(p_1^{b_1}\dots p_r^{b_r})}{\varphi(p_1^{a_1}\dots p_r^{a_r})}\,\varphi(q_1^{c_1}\dots q_t^{c_t})(q-1)\, d^{f_K} =$$

$p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\,\varphi(q_1^{c_1}\dots q_t^{c_t}\, q)\, d^{f_K}$ car $q \notin \{ p_1,\dots,p_r ,\ q_1\dots q_t \}$.
D'où le résultat . Dans le second cas on est ramené au cas (i) avec $a_i = b_i$ pour $i \geqslant 2$ et $b_1 - a_1 = 1$: $S_{f_L q_1} = S_{f_L} + \frac{1}{2}(q_1-1)\, d^{f_L}\vartheta =$

$$= \prod_{i=1}^{t}\left(1-\left(\frac{K}{q_i}\right)^{-1}_{f_K}\right) S_{f_K} + \frac{1}{2}\, p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\,\varphi(q_1^{c_1}\dots q_t^{c_t})\, d^{f_K}\vartheta + \frac{1}{2}(q_1-1)$$

$$p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\,\varphi(q_1^{c_1}\dots q_t^{c_t})\, d^{f_K}\vartheta = \prod_{i=1}^{t}\left(1 -\left(\frac{K}{q_i}\right)^{-1}_{f_K}\right) S_{f_K} \ +$$

$\frac{1}{2}\, d^{f_K}\vartheta (p_1^{b_1-a_1}\dots p_r^{b_r-a_r})\,\varphi(q_1^{c_1}\dots q_t^{c_t})\, q_1$; or comme $c_1 \geqslant 1$,

$\varphi(q_1^{c_1}\dots q_t^{c_t})\, q_1 = \varphi(q_1^{c_1+1}\dots q_t^{c_t})$.

Cas (iii) . Posons $S'_K = S_K + a_K\vartheta_{K/\mathbb{Q}}$, pour un corps K quelconque, avec $a_K = -\frac{1}{2}[\mathbb{Q}^{(f_K)} : K]$. Etudions l'action des $N_{L/K}$ sur la famille des S'_L , $L \subset \mathbb{Q}^a_o$.

On a $N_{L/K}\, S'_L = N_{L/K}(S_L + a_L\vartheta_{L/\mathbb{Q}}) = N_{L/K}\, S_L + a_L[L:K]\vartheta_{K/\mathbb{Q}}$

Si $t = 0$, $N_{L/K}\, S'_L = S_K + \frac{1}{2}(p_1^{b_1-a_1}\dots p_r^{b_r-a_r}-1)[\mathbb{Q}^{(f_K)}:K]\vartheta_{K/\mathbb{Q}} + a_L[L:K]\vartheta_{K/\mathbb{Q}}$

$$= S'_K - a_K \vartheta_{K/\mathbb{Q}} + \frac{1}{2}(p_1^{b_1-a_1}\dots p_r^{b_r-a_r}-1)[\mathbb{Q}^{(f_K)}:K]\vartheta_{K/\mathbb{Q}} - \frac{1}{2}[\mathbb{Q}^{(f_L)}:K]\vartheta_{K/\mathbb{Q}};$$

or $[\mathbb{Q}^{(f_L)}:\mathbb{Q}^{(f_K)}] = \dfrac{\varphi(f_L)}{\varphi(f_K)} = p_1^{b_1-a_1}\dots p_r^{b_r-a_r}$ et $N_{L/K} S'_L = S'_K$.

Si $t>0$, $N_{L/K} S'_L = S_K \prod_{i=1}^{t}\left(1-\left(\frac{K}{q_i}\right)_{f_K}^{-1}\right) +$

$$+ \frac{1}{2} p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\varphi(q_1^{c_1}\dots q_t^{c_t})[\mathbb{Q}^{(f_K)}:K]\vartheta_{K/\mathbb{Q}} + a_L[L:K]\vartheta_{K/\mathbb{Q}}$$

$$= \prod_{i=1}^{t}\left(1-\left(\frac{K}{q_i}\right)_{f_K}^{-1}\right)(S'_K - a_K\vartheta_{K/\mathbb{Q}}) + \frac{1}{2}p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\varphi(q_1^{c_1}\dots q_t^{c_t})[\mathbb{Q}^{(f_K)}:K]$$

$$\vartheta_{K/\mathbb{Q}} - \frac{1}{2}[\mathbb{Q}^{(f_L)}:K]\vartheta_{K/\mathbb{Q}} .$$

Or pour tout $\tau \in \mathrm{Gal}(K/\mathbb{Q})$, $(1-\tau)\vartheta_{K/\mathbb{Q}} = 0$, donc, il reste

$N_{L/K} S'_L = S'_K \prod_{i=1}^{t}\left(1-\left(\frac{K}{q_i}\right)_{f_K}^{-1}\right)$, car

$$\frac{1}{2}[\mathbb{Q}^{(f_L)}:K] = \frac{1}{2} p_1^{b_1-a_1}\dots p_r^{b_r-a_r}\varphi(q_1^{c_1}\dots q_t^{c_t})[\mathbb{Q}^{(f_K)}:K] .$$

On a donc obtenu dans tous les cas :

$$N_{L/K} S'_L = \prod_{\substack{q \mid f_L \\ q \nmid f_K}} \left(1-\left(\frac{K}{q}\right)_{f_K}^{-1}\right) S'_K .$$

Il est interessant de constater l'analogie de ce résultat avec celui obtenu par Leopoldt relativement aux nombres θ_χ définissant les unités cyclotomiques dans le cas réel (cf. [15], [18] et chap. III , 2)) .

Signalons aussi que S'_L est l'élément fourni directement au moyen des valeurs en 0 des fonctions ζ_L partielles (cf. [2], § 2,4 et § 3,2) (voir à ce sujet la remarque II 7 ci-après) .

(ii) <u>Etude des nombres $\psi'(S_{K_\chi})$ pour $\psi' \in \mathfrak{X}'_{K_\chi}$</u> . Supposons maintenant que $L = K_\chi$ pour $\chi \in \mathfrak{X}$. Soit ψ' un élément de $\mathfrak{X}'_{K_\chi}$. On considère l'homomorphisme d'algèbres défini par $\sigma_\chi \longrightarrow \psi'(\sigma_\chi)$ de $\mathbb{Q}[G_\chi]$ dans Ω_ℓ et on note encore ψ' cet homomorphisme . On a le diagramme suivant :

$$\begin{tikzcd} \mathbb{Q}[G_\chi] \arrow[r, "\psi'"] \arrow[d, "N_{K_\chi/K_\psi}"'] & \Omega_\ell \\ \mathbb{Q}[G_\psi] \arrow[ur, "\psi'"'] & \end{tikzcd}$$

Ce diagramme est commutatif car pour $\tau \in \mathrm{Gal}(K_\chi/K_\psi)$, on a $\psi'(\tau) = 1$. On en déduit le résultat suivant en utilisant les conventions de [8] (chap. II , § 1) sur les caractères de Dirichlet :

<u>Proposition</u> II 4 . On a , pour tout $\psi' \in \mathfrak{X}'_{K_\chi}$, $\psi' \neq 1$:

$$\psi'(S_{K_\chi}) = \prod_{\substack{q \mid f_\chi \\ q \text{ premier}}} (1 - \underline{\psi}'^{-1}(q))\, B_1(\psi'^{-1}) ,$$

avec $\underline{\psi}' \in X(f_\psi)$, $B_1(\psi'^{-1})$ étant le nombre de Bernoulli primitif correspondant à ψ' .

<u>démonstration</u>

On a $\psi'(S_K) = \psi'(N_{K_\chi/K_\psi} S_{K_\chi})$. Dans le premier cas du théorème II 3 , on a $N_{K_\chi/K_\psi}(S_{K_\chi}) = S_{K_\psi} + \frac{1}{2}(p_1^{b_1-a_1} \cdots p_r^{b_r-a_r} - 1)[\mathbb{Q}^{(f_\psi)}:K_\psi]\nu_{K_\psi/\mathbb{Q}}$

mais $\psi'(\nu_{K_\psi/\mathbb{Q}}) = 0$, car $\psi' \neq 1$; d'où $\psi'(S_{K_\chi}) = \psi'(S_{K_\psi}) =$

$\frac{1}{f_\psi} \sum_{a=1}^{f_\psi} a\, \psi'^{-1}(a) = B_1(\psi'^{-1})$. Dans le deuxième cas , on a encore

$$\psi'(\nu_{K_\psi/\mathbb{Q}}) = 0 \text{ et } \psi'(S_{K_\chi}) = \prod_{\substack{q_i \mid f_\chi \\ q_i \nmid f_\psi}} (1 - \psi'^{-1}(q_i))\, B_1(\psi'^{-1}) ,$$

ce que l'on peut écrire comme indiqué dans l'énoncé dans tous les cas .

Remarque II 3 . Dans le cas $\psi' = 1$, on obtient $\psi'(S_{K_\chi}) = \frac{1}{2}\,\varphi(f_\chi)$ (resp. 1) pour $\chi \neq 1$ (resp. $\chi = 1$) .

Corollaire II 4 . Si ψ' est un caractère pair ($\psi' \neq 1$) alors $\psi'(S_{K_\chi}) = 0$. Si ψ' est impair (ce qui suppose χ' impair) alors $\psi'(S_{K_\chi})$ est nul si et seulement si il existe un diviseur p du conducteur f_χ qui est tel que $\psi'(p) = 1$.

Ceci résulte du fait que l'on sait caractériser la nullité de $B_1(\psi'^{-1})$: si $\psi' \neq 1$ est pair , $B_1(\psi'^{-1}) = 0$ ([8] , chap. II) ; si ψ' est impair alors $B_1(\psi'^{-1}) \neq 0$ (Th. II 2) .

(iii) Détermination de l'image de N_χ . On suppose χ impair .

Définition II 3 . Notons Ψ_χ' l'ensemble des caractères $\psi' \in \mathcal{X}'_{K_\chi}$ tels que $\psi' \nmid \chi$ et $\psi'(S_{K_\chi}) \neq 0$. Cette condition étant stable par $\Gamma_{\mathbb{Q}}$ -conjugaison , on définit $\Psi_\chi \subset \mathcal{X}_{K_\chi}$ de façon évidente . Posons enfin

$$\bar{Q}(X) = \prod_{\psi \in \Psi_\chi} P_\psi(X) .$$

On a à déterminer $N_\chi = \{\omega \in S_{K_\chi}\mathcal{U}_{K_\chi} ,\ P_\chi\,\omega = 0\}$, puis l'image de N_χ par l'homomorphisme χ' . Posons $\mathcal{U}'_{K_\chi} = \{\omega' \in \mathcal{U}_{K_\chi}, S_{K_\chi}\omega' \in N_\chi\}$; $\mathcal{U}'_{K_\chi}$ est un idéal de $\mathbb{Z}[G_\chi]$ car N_χ est un idéal de $M(K_\chi)$; on a $N_\chi = S_{K_\chi}\mathcal{U}'_{K_\chi}$. On a donc $\omega' \in \mathcal{U}'_{K_\chi}$ qui équivaut à $P_\chi S_{K_\chi}\omega' = 0$ soit $P_\chi \bar{S}_{K_\chi}\omega' = 0$ en posant $\bar{S}_{K_\chi} = f_\chi S_{K_\chi} \in \mathbb{Z}[G_\chi]$. Comme précédemment , on représente les éléments de $\mathbb{Z}[G_\chi]$ par des polynomes : Si on a

$$\bar{S}_{K_\chi} = \sum_{i=0}^{g_\chi - 1} a_i\,\sigma_\chi^i \text{ , on pose } \bar{S}_{K_\chi}(X) = \sum_{i=0}^{g_\chi - 1} a_i\,X^i \text{ et on désigne}$$

par $\omega'(X)$ un représentant modulo $X^{g_\chi}-1$ de ω' . On a donc

$P_\chi S_{K_\chi}\omega' = 0$ **si et seulement si** $\bar{S}_{K_\chi}(X)\,P_\chi(X)\,\omega'(X) \in (X^{g_\chi}-1)\,\mathbb{Z}[X]$

donc si et seulement si $\bar{S}_{K_\chi}(X)\,\omega'(X) \in Q(X)\,\mathbb{Z}[X]$, en posant

$Q(X) = \dfrac{X^{g_\chi}-1}{P_\chi(X)}$. Comme , pour $\psi \in \mathfrak{X}_{K_\chi}$, les polynomes P_ψ sont irréductibles , la condition équivaut à la suivante :

Considérons le diagramme commutatif :

$$\begin{tikzcd}
\mathbb{Z}[X] \arrow[r, "\psi'"] \arrow[d, "\chi"] & \mathbb{Z}^{(g_\chi)}_{\psi'(\sigma_\chi)} \\
\underset{\sigma_\chi}{\mathbb{Z}[G_\chi]} \arrow[ur, "\psi'"'] &
\end{tikzcd}$$

en désignant encore par ψ' l'homomorphisme défini par $\psi'(X) = \psi'(\sigma_\chi)$; alors il faut et il suffit que $\psi'(\bar{S}_{K_\chi}(X)\,\omega'(X)) = 0$ pour tout $\psi' \in \mathfrak{X}'_{K_\chi}$, $\psi' \neq \chi$, soit que l'on ait $\psi'(\bar{S}_{K_\chi}(X)) = 0$ ou bien $\psi'(\omega'(X)) = 0$.
Par définition de Ψ'_χ , la condition est : $\psi'(\omega'(X)) = 0$ pour tout $\psi' \in \Psi'_\chi$.

Déterminons l'image de $\mathfrak{U}'_{K_\chi}$ par l'homomorphisme χ' .
On peut écrire $\mathfrak{U}'_{K_\chi} = \{\omega' \in \mathfrak{U}_{K_\chi}$, $\psi'(\omega'(X)) = 0$ pour tout $\psi' \in \Psi'_\chi\} =$
$\{\omega' \in (\sigma_\chi - a, \Lambda_\chi)$, $\psi'(\omega'(X)) = 0$, pour tout $\psi' \in \Psi'_\chi\} =$
$\{\omega' \in \mathbb{Z}[G_\chi]$, $\omega'(X) \in (X-a, \Lambda_\chi)$ et $\psi'(\omega'(X)) = 0$, pour tout $\psi' \in \Psi'_\chi\}$.
Il en résulte facilement que l'image de $\mathfrak{U}'_{K_\chi}$ par χ' est égale à celle de $\{\omega'(X) \in \mathbb{Z}[X]$, $\omega'(X) \in (X-a, \Lambda_\chi)$ et $\psi'(\omega'(X)) = 0$ pour tout $\psi' \in \Psi'_\chi\}$ par l'homomorphisme , noté encore $\chi' : \mathbb{Z}[X] \longrightarrow \mathbb{Z}^{(g_\chi)}$, défini par $\chi'(X) = \chi'(\sigma_\chi)$. Comme $\bar{Q}(X) = \prod_{\psi \in \Psi_\chi} P_\psi$, l'image cherchée est celle de l'idéal $\bar{Q}(X)\,\mathbb{Z}[X] \cap (X-a, \Lambda_\chi)_{\mathbb{Z}[X]}$. Considérons $I = \{R \in \mathbb{Z}[X], \bar{Q}R \in (X-a, \Lambda_\chi)\}$
I est un idéal de $\mathbb{Z}[X]$ et on a $\bar{Q}\,\mathbb{Z}[X] \cap (X-a, \Lambda_\chi) = \bar{Q}I$. On remarque que $R \in I$ si et seulement si $R(a)\,\bar{Q}(a) \equiv 0 \bmod \Lambda_\chi$: en effet, soit $R \in \mathbb{Z}[X]$, $\bar{Q}R = A(X-a) + (\bar{Q}R)(a)$, $A \in \mathbb{Z}[X]$ (division par $X-a$ dans $\mathbb{Z}[X]$) ; si $R \in I$, $\bar{Q}R = A'(X-a) + B\Lambda_\chi$, $A', B \in \mathbb{Z}[X]$ et $\bar{Q}(a)\,R(a) = B(a)\,\Lambda_\chi$ et inversement si $\bar{Q}(a)\,R(a) \equiv 0 \bmod \Lambda_\chi$ alors $\bar{Q}R = A(X-a) + \bar{Q}(a)\,R(a) \in (X-a, \Lambda_\chi)$

<u>Lemme</u> II 11 . On a $I = (X-a, \Lambda'_\chi)_{\mathbb{Z}[X]}$ où $\Lambda'_\chi = \dfrac{\Lambda_\chi}{\text{p.g.c.d.}\,(\bar{Q}(a), \Lambda_\chi)}$.

En effet, on vient de voir que $R \in I$ si et seulement si $\bar{Q}(a)\,R(a) \equiv 0 \bmod \Lambda_\chi$, donc si et seulement si $R(a) \in \Lambda'_\chi \mathbb{Z}$. La détermination de I en résulte immédiatement .

Définition II 4 . On pose $\bar{\Lambda}_\chi = \text{p.g.c.d.}\,(\Lambda'_\chi,\ P_\chi(a))$, où $\Lambda'_\chi = \dfrac{\Lambda_\chi}{\text{p.g.c.d.}(\bar{Q}(a),\Lambda_\chi)}$

$\bar{\Lambda}_\chi$ est donc un diviseur de Λ_χ .

Lemme II 12 . L'image de l'idéal I dans $\mathbb{Z}^{(g_\chi)}$ est un idéal de norme $\bar{\Lambda}_\chi$.

L'image de I est d'après le lemme II 11 l'idéal $(\zeta - a, \Lambda'_\chi)_{\mathbb{Z}^{(g_\chi)}}$, où $\zeta = \chi'(\sigma_\chi)$. On calcule l'ordre du quotient $\mathbb{Z}^{(g_\chi)}/(\zeta - a, \Lambda'_\chi) \simeq$ $\mathbb{Z}[X]/(P_\chi(X), X-a, \Lambda'_\chi) \simeq \mathbb{Z}[X]/(P_\chi(a), \Lambda'_\chi, X-a) \simeq \mathbb{Z}/(P_\chi(a), \Lambda'_\chi)_{\mathbb{Z}} \simeq$ $\mathbb{Z}/\bar{\Lambda}_\chi \mathbb{Z}$; d'où le lemme .

Il reste alors à calculer l'image de $\bar{Q}$ par χ' . On aura alors obtenu l'image de $\mathfrak{U}'_{K_\chi}$, à savoir : $\bar{Q}(\zeta)\,(\zeta - a, \Lambda'_\chi)$.

Définition II 5 . Notons Ψ^*_χ l'ensemble des caractères impairs $\psi \in \mathfrak{X}_{K_\chi}$ tels que pour $\psi'|\psi$, il existe p premier divisant f_χ tel que $\underline{\psi}'(p) = 1$ (cela veut dire (cf. [17] , Prop. IV b) que p est totalement décomposé dans K_ψ) .

On remarque que $\chi \notin \Psi^*_\chi$ car $\underline{\chi}'(p) = 0$ pour tout $p \mid f_\chi$.

On a donc $\Psi_\chi = \{1\} \cup (\mathfrak{X}^-_{K_\chi} \setminus \{\chi, \Psi^*_\chi\})$. On a $X^{g_\chi} - 1 = \prod_{\psi \in \mathfrak{X}_{K_\chi}} P_\psi$; or ψ' est pair si et seulement si ψ' est d'ordre diviseur de $g_\chi/2$ (ceci car G_χ est cyclique) ; donc $\prod_{\psi \in \mathfrak{X}^-_{K_\chi}} P_\psi = \dfrac{X^{g_\chi} - 1}{\prod_{g_\psi | (g_\chi/2)} P_\psi} = \dfrac{X^{g_\chi} - 1}{X^{g_\chi/2} - 1} = X^{g_\chi/2} + 1$,

d'où $\bar{Q}(X) = \dfrac{P_1}{P_\chi}\left(\prod_{\psi \in \mathfrak{X}^-_{K_\chi}} P_\psi\right)\Big/\left(\prod_{\psi \in \Psi^*_\chi} P_\psi\right) = \dfrac{P_1}{P_\chi} \cdot \dfrac{X^{g_\chi/2} + 1}{\prod_{\psi \in \Psi^*_\chi} P_\psi}$. On a $\zeta^{g_\chi/2} = \chi'(\sigma_\chi^{g_\chi/2}) = \chi'(-1) = -1$, car l'élément d'ordre 2 de G_χ est né -

cessairement la conjugaison complexe . Posons $A = \dfrac{X^{g_\chi/2}+1}{P_\chi}$,

alors $X^{g_\chi/2}+1 = A\,P_\chi$, ce qui donne en dérivant

$g_\chi/2\,X^{g_\chi/2-1} = A\,P'_\chi + A'P_\chi$ soit $-\dfrac{g_\chi}{2}\zeta^{-1} = A(\zeta)\,P'_\chi(\zeta)$ soit

$A(\zeta) = -\dfrac{g_\chi}{2}\dfrac{\zeta^{-1}}{P'_\chi(\zeta)} = -\dfrac{g_\chi}{2}\dfrac{\zeta^{-1}}{\prod_{\sigma\neq 1}(\zeta-\zeta^{\sigma})}$, σ parcourant $G(\mathbb{Q}^{(g_\chi)}/\mathbb{Q})\setminus\{1\}$.

On a $\bar{Q}(\zeta) = \dfrac{\zeta-1}{\prod_{\psi\in\Psi^*_\chi}P_\psi(\zeta)}\left(-\dfrac{g_\chi}{2}\dfrac{\zeta^{-1}}{\prod_{\sigma\neq 1}(\zeta-\zeta^{\sigma})}\right)$. Nous nous interes-

sons principalement à la norme de $\bar{Q}(\zeta)$ (dans $\mathbb{Q}^{(g_\chi)}/\mathbb{Q}$) . Cependant ,

on a obtenu l'idéal $\mathfrak{b}_\chi$ image de N_χ : à savoir

$$\mathfrak{b}_\chi = \frac{(\zeta-1)(g_\chi)(\zeta-a,\Lambda'_\chi)}{\prod_{\psi\in\Psi^*_\chi}P_\psi(\zeta)\prod_{\sigma\neq 1}(\zeta-\zeta^{\sigma})}\left(\frac{1}{2}B_1(\chi'^{-1})\right)\mathbb{Z}^{(g_\chi)}$$. On peut en déduire

facilement $\mathfrak{b}_\chi/\mathfrak{a}_\chi$.

On remarque que $N(\zeta-1)$ vaut 1 si g_χ n'est pas la puissance d'un nombre premier (cf. Rem. I 2) . Dans le cas contraire , c'est une puissance d'un nombre premier donc une puissance de 2 (g_χ est pair) , et dans ce cas $N(\zeta-1) = 2$ (cf. Rem. I 2) . La norme de $\prod_{\sigma\neq 1}(\zeta-\zeta^{\sigma})$ est égale à

$\prod_{\tau,\sigma\neq 1}(\zeta^{\tau}-\zeta^{\sigma\tau}) = \prod_{\tau\neq s}(\zeta^{\tau}-\zeta^{s})$ qui est le discriminant de $\mathbb{Q}^{(g_\chi)}/\mathbb{Q}$, à savoir

(cf. Hasse : [9] , § 27 , 3) : $g_\chi^{\varphi(g_\chi)}\Big/\prod_{\substack{p\mid g_\chi\\ p \text{ premier}}} p^{\varphi(g_\chi)/p-1}$.

La norme de $(\zeta-1)\dfrac{g_\chi}{2}\Big/\prod_{\sigma\neq 1}(\zeta-\zeta^{\sigma})$ est donc égale à

$$2^{\alpha_\chi}\left(\frac{g_\chi}{2}\right)^{\varphi(g_\chi)}\frac{\prod_{p\mid g_\chi}p^{\varphi(g_\chi)/p-1}}{g_\chi^{\varphi(g_\chi)}} = \frac{2^{\alpha_\chi}}{2^{\varphi(g_\chi)}}\prod_{p\mid g_\chi}p^{\varphi(g_\chi)/p-1}$$, avec

$\alpha_\chi = 1$ (resp. 0) si g_χ est une puissance de 2 (resp. n'est pas une puissance de 2) .

Examinons maintenant le terme $\prod_{\psi \in \Psi_\chi^*} P_\psi(\zeta)$. Si $\psi \in \Psi_\chi^*$,

c'est qu'il existe un diviseur premier p de f_χ tel que p est décomposé dans K_ψ (K_ψ étant un corps imaginaire) . Donc , pour un tel ψ , tous les caractères $\varphi \in \mathfrak{X}^-_{K_\psi}$ sont aussi dans Ψ_χ^*. On remarque alors que $\prod_{\varphi \in \mathfrak{X}_{K_\psi}} P_\varphi(\zeta) =$ $\zeta^{g_\psi}-1$, donc de la forme $\zeta_d - 1$ où $d = g_\chi / g_\psi$ est l'ordre de ζ_d ; or , la norme absolue de ζ_d-1 est égale à ± 1 lorsque d n'est pas puissance d'un nombre premier ; par conséquent dans ce cas , $P_\psi(\zeta)$ et les $P_\varphi(\zeta)$, pour $\varphi \in \mathfrak{X}^-_{K_\psi}$, sont des unités . On peut donc restreindre le produit aux caractères $\psi \in \Psi_\chi^*$ tels que g_χ / g_ψ soit la puissance d'un nombre premier . On peut supposer cette puissance impaire car sinon pour la puissance de 2, le corps K_ψ correspondant est réel (car $\chi \notin \Psi_\chi^*$, donc $g_\chi \neq g_\psi$) ce qui est absurde puisque K_ψ doit être imaginaire . On considère alors pour $\psi \in \Psi_\chi^*$:

$$\prod_{\varphi \in \mathfrak{X}_\psi^-} P_\varphi(X) = \Big(\prod_{\varphi \in \mathfrak{X}_\psi} P_\varphi(X)\Big) \Big/ \Big(\prod_{\varphi \in \mathfrak{X}_\psi^+} P_\varphi(X)\Big) = \frac{X^{g_\psi}-1}{X^{g_\psi/2}-1} = X^{g_\psi/2}+1 .$$

On a alors $\prod_{\varphi \in \mathfrak{X}_\psi^-} P_\varphi(\zeta) = \zeta^{g_\psi/2}+1$, or ζ^{g_ψ} est une racine d'ordre p^k , $k \geqslant 1$, p premier , $p \neq 2$, $p \mid g_\chi$ et $\zeta^{g_\psi/2}$ est d'ordre $2p^k$; elle est donc de la forme $-\zeta_{p^k}$, d'où , on obtient $\prod_{\varphi \in \mathfrak{X}_\psi^-} P_\varphi(\zeta) = 1-\zeta_{p^k}$ dont la norme dans $\mathbb{Q}^{(g_\chi)}/\mathbb{Q}$ est une puissance de p .

<u>Définition</u> II 6 . Appelons c_χ la norme $N_{\mathbb{Q}^{(g_\chi)}/\mathbb{Q}}\Big(\prod_{\psi \in \Psi_\chi^*} P_\psi(\chi'(\sigma_\chi))\Big)$

(cf. Déf. II 5) .

On en déduit que la norme absolue de $\tilde{Q}(\zeta)$ est égale à

$$\frac{2^{\alpha_\chi}}{c_\chi \, 2^{\varphi(g_\chi)}} \prod_{p \mid g_\chi} p^{\varphi(g_\chi)/p-1} .$$

Remarque II 4 . Les diviseurs premiers de la constante c_χ sont des nombres premiers impairs divisant g_χ .

γ) Calcul de l'indice $(M_\chi : N_\chi)$. Il est maintenant possible de donner la valeur de l'ordre de M_χ / N_χ . L'image de M_χ dans $\mathbb{Z}^{(g_\chi)}$ est l'idéal $\mathfrak{a}_\chi = \prod_{\substack{p \mid g_\chi \\ p \text{ premier}}} (1 - \chi'(\sigma_\chi)^{g_\chi / p})$ (cf. Lemme II 9) ; dans cet isomorphisme l'image de N_χ est égale à l'image de $S_{K_\chi} \mathcal{U}'_{K_\chi}$ et l'image de $\mathcal{U}'_{K_\chi}$ par χ' est égale à celle de $\bar{Q}I$ par l'homomorphisme défini par $X \longrightarrow \chi'(\sigma_\chi)$.

L'image de S_{K_χ} par χ' est égale à $\frac{1}{f_\chi} \sum_{a=1}^{f_\chi}{}^{*} \chi'^{-1}(a)\, a = B_1(\chi'^{-1})$,

celle de N_χ sera donc un idéal $\mathfrak{b}_\chi$ produit de $B_1(\chi'^{-1})$ par l'idéal image de $\bar{Q}I$. L'indice $(M_\chi : N_\chi)$ est donc égal à (N désignant $N_{\mathbb{Q}^{(g_\chi)}/\mathbb{Q}}$) :

$$N\mathfrak{b}_\chi / N\mathfrak{a}_\chi ; \text{ or } N(\bar{Q}(\zeta)) = \frac{2^{\alpha_\chi}}{c_\chi\, 2^{\varphi(g_\chi)}} = \prod_{p \mid g_\chi} p^{\varphi(g_\chi)/p-1} ,$$

$$N(I(\zeta)) = \bar{\Lambda}_\chi \text{ (cf. Lemme II 12) et } N\mathfrak{a}_\chi = \prod_{\substack{p \mid g_\chi \\ p \text{ premier}}} N(1 - \chi'(\sigma_\chi)^{g_\chi / p}) ;$$

$$\text{or } N(1 - \chi'(\sigma_\chi)^{g_\chi/p}) = N(1 - \zeta_p) = p^{\frac{\varphi(g_\chi)}{p-1}} \quad \text{et } N\mathfrak{a}_\chi = \prod_{p \mid g_\chi} p^{\frac{\varphi(g_\chi)}{p-1}} ,$$

$$\text{d'où } N\mathfrak{b}_\chi / N\mathfrak{a}_\chi = \frac{2^{\alpha_\chi} \prod_{p \mid g_\chi} p^{\varphi(g_\chi)/p-1} \quad N B_1(\chi'^{-1}) \bar{\Lambda}_\chi}{c_\chi\, 2^{\varphi(g_\chi)} \prod_{p \mid g_\chi} p^{\varphi(g_\chi)/p-1}} = \frac{2^{\alpha_\chi} \bar{\Lambda}_\chi}{c_\chi\, 2^{\varphi(g_\chi)}} \prod_{\chi' \mid \chi} B_1(\chi'^{-1}).$$

On a donc obtenu :

$$N\mathfrak{b}_\chi / N\mathfrak{a}_\chi = \frac{2^{\alpha_\chi} \bar{\Lambda}_\chi}{c_\chi} \prod_{\chi' \mid \chi} \left(\frac{1}{2} B_1(\chi'^{-1})\right) .$$

On peut vérifier sans difficulté que $\mathfrak{b}_\chi / \mathfrak{a}_\chi$ est l'idéal entier

$$\frac{(\chi'(\sigma_\chi)-1)\ (\chi'(\sigma_\chi)-a,\bar{\Lambda}_\chi)}{\prod_{\psi\in\Psi_\chi^*} P_\psi(\chi'(\sigma_\chi))}\ \frac{1}{2}\ B_1(\chi'^{-1})$$, ce qui donne une propriété d'intégralité intéressante (comparer avec le Cor. II 7 ci-après) .

δ) <u>Calcul de Λ_χ et $\bar{\Lambda}_\chi$</u> . On rappelle (cf. Déf. II 2 et Corol. II 3) que $\Lambda_\chi = \dfrac{f_\chi}{\text{p.g.c.d.}\ (f_\chi, \alpha_1)}$ et que $\bar{\Lambda}_\chi = \text{p.g.c.d.}\left(P_\chi(a), \dfrac{\Lambda_\chi}{\text{p.g.c.d.}(\bar{Q}(a),\Lambda_\chi)}\right)$

(cf. Déf. II 4) . On va effectuer ces calculs localement : on désigne par $(\quad)_\ell$ la ℓ-participation d'un nombre entier . On pose $f_\chi = \ell^n f'_\chi$, $\ell \nmid f'_\chi$. On suppose $n \geqslant 1$ sinon $(\Lambda_\chi)_\ell = (\bar{\Lambda}_\chi)_\ell = 1$. On rappelle aussi que si $2 \mid f_\chi$, alors $4 \mid f_\chi$. On a $\Lambda_\chi = \dfrac{f_\chi}{\text{p.g.c.d.}\ (f_\chi, \alpha_1)}$ où $\alpha_1 = \sum\limits_{\substack{a=1\\ \sigma_a\in H}}^{f_\chi}{}^{*}\ a$, où $H = G(\mathbb{Q}^{(f_\chi)}/K_\chi)$ (cf. Déf. II 2 et Corol. II 3) .

(i) <u>Cas $\ell \neq 2$</u> . On remarque que si $\mathbb{Q}^{(\ell)}$ n'est pas contenu dans K_χ , alors $(\Lambda_\chi)_\ell = 1$: en effet , si $\mathbb{Q}^{(\ell)} \not\subset K_\chi$, soit ξ_χ une racine primitive d'ordre f_χ de l'unité ; $N_{\mathbb{Q}^{(f_\chi)}/K_\chi}\,\xi_\chi = \xi_\chi^{\alpha_1}$ et $\xi_\chi^{\alpha_1}$ sera une racine d'ordre premier à ℓ , donc $\alpha_1 \equiv 0 \bmod \ell^n$ et $(\Lambda_\chi)_\ell = 1$.

Supposons que K_χ contienne $\mathbb{Q}^{(\ell^k)}$, $k \geqslant 1$,et non $\mathbb{Q}^{(\ell^{k+1})}$. On a $k \leqslant n$. On a le schéma ci-dessous :

$$\begin{tikzcd}
 & \mathbb{Q}^{(\ell^n f'_\chi)} \arrow[d, dash] \\
K_\chi \arrow[r, dash] \arrow[d, dash] & K_\chi\mathbb{Q}^{(\ell^n)} = L \arrow[d, dash] \\
\mathbb{Q}^{(\ell^k)} \arrow[r, dash, "\ell^{n-k}"'] & \mathbb{Q}^{(\ell^n)}
\end{tikzcd}$$

Comme $\mathbb{Q}^{(\ell^{k+1})} \not\subset K_\chi$, $K_\chi/\mathbb{Q}^{(\ell^k)}$ et $\mathbb{Q}^{(\ell^n)}/\mathbb{Q}^{(\ell^k)}$ sont linéairement disjointes. Soit L le composé ; posons $\xi_\chi = \xi_{\ell^n}\xi'$, ξ_{ℓ^n} d'ordre ℓ^n, ξ' d'ordre premier à ℓ. On a $\xi_\chi^{\alpha_1} = N\xi_{\ell^n} N\xi'$ où $N = N_{\mathbb{Q}^{(f_\chi)}/K_\chi}$.

Comme $N\xi'$ est d'ordre premier à ℓ, calculons $N\xi_{\ell^n} = N_{L/K_\chi} N_{\mathbb{Q}^{(f_\chi)}/L}(\xi_{\ell^n})$

$= N_{L/K_\chi}\xi_{\ell^n}^{[\mathbb{Q}^{(f_\chi)}:L]}$. On a $N_{L/K_\chi}\xi_{\ell^n} = N_{\mathbb{Q}^{(\ell^n)}/\mathbb{Q}^{(\ell^k)}}\xi_{\ell^n}$.

<u>Lemme</u> II 13. On a $N_{\mathbb{Q}^{(\ell^r)}/\mathbb{Q}^{(\ell^{r-1})}}\xi_{\ell^r} = \xi_{\ell^r}^{\ell} = \xi_{\ell^{r-1}}$, pour tout $r \geqslant 1$.

En effet, le groupe de Galois de $\mathbb{Q}^{(\ell^r)}/\mathbb{Q}^{(\ell^{r-1})}$ est, pour $r \geqslant 2$, constitué des automorphismes $\xi_{\ell^r} \longrightarrow \xi_{\ell^r}^{1+\lambda\ell^{r-1}}$, $\lambda = 1,2,\dots,\ell$ et $N\xi_{\ell^r} = \xi_{\ell^r}^{\ell+\ell^{r-1}(1+2\dots+\ell)} = \xi_{\ell^r}^{\ell} = \xi_{\ell^{r-1}}$; pour $r = 1$, on a $N\xi_\ell = N_{\mathbb{Q}^{(\ell)}/\mathbb{Q}}\xi_\ell = \xi_\ell^{1+2+\dots+\ell-1} = 1$.

On aura donc $N_{L/K_\chi}\xi_{\ell^n}^{[\mathbb{Q}^{(f_\chi)}:L]} = \xi_{\ell^n}^{\ell^{n-k}[\mathbb{Q}^{(f_\chi)}:L]} = \xi_{\ell^n}^{[\mathbb{Q}^{(f_\chi)}:K_\chi]}$.

On obtient donc :

<u>Proposition</u> II 5. Soit ℓ un nombre premier impair divisant f_χ (on pose $f_\chi = \ell^n f'_\chi$, $\ell \nmid f'_\chi$). Si K_χ ne contient pas $\mathbb{Q}^{(\ell)}$ alors $(\Lambda_\chi)_\ell = 1$.
Si K_χ contient $\mathbb{Q}^{(\ell)}$, alors en posant $([\mathbb{Q}^{(f_\chi)}:K_\chi])_\ell = \ell^{n_\chi}$, on a

$$(\Lambda_\chi)_\ell = \frac{\ell^n}{\text{p.g.c.d.}(\ell^{n_\chi}, \ell^n)}.$$

Compte-tenu de la définition de $\bar{\Lambda}_\chi$, le calcul de $(\bar{\Lambda}_\chi)_\ell$ exige l'étude de $P_\chi(a)$ et $P_\psi(a)$ pour certains ψ (cf. Déf. II 3).

Pour cette étude , on peut supposer $\mathbb{Q}^{(\ell)} \subset K_\chi$.

Soit ψ un caractère impair ($\psi \in \mathfrak{X}^-_{K_\chi}$) et soit a , $(a, f_\chi) = 1$, tel que $\left(\dfrac{K_\chi}{a}\right) = \sigma_\chi$; comme l'image de σ_χ dans G_ψ est génératrice ,

$\psi'(\sigma_\chi) = \psi'(a)$ est une racine d'ordre g_ψ de l'unité pour tout $\psi'|\psi$.

On a $P_\psi(a) = \prod_{\psi'|\psi} (a - \psi'(a)) \in \mathbb{Z}$. Comme on cherche la ℓ -participation à

$P_\psi(a)$, il suffit de caractériser les cas où il existe $\psi'|\psi$ tel que $a - \psi'(a)$ soit non premier à ℓ ; comme $P_\psi(a) \in \mathbb{Z}$, on peut raisonner dans Ω_ℓ; on a $a - \psi'(a) = \theta(a)(1 + \gamma_a \ell) - \psi'(a)$ (cf. [8] , I, § 1 , b,β pour $\gamma_a \in \mathbb{Z}_\ell$)

car $(a, \ell) = 1$ puisque $(a, f_\chi) = 1$ et que $\ell \mid f_\chi$; $a - \psi'(a) \equiv \theta(a) - \psi'(a)$ mod ℓ , soit $a - \psi'(a) \equiv \theta(a)(1 - \psi'(a)\theta^{-1}(a))$ mod ℓ . Il suffit de voir à quelle condition $1 - \psi'\theta^{-1}(a)$ est non premier à ℓ . On sait que $1 - \psi'\theta^{-1}(a)$ est non premier à ℓ si et seulement si $\psi'\theta^{-1}(a)$ est une racine de l'unité d'ordre une puissance d'un nombre premier , donc de ℓ ici ; or on a par hypothèse $\theta \in \mathfrak{X}^+_{K_\chi}$ et $\psi' \in \mathfrak{X}^-_{K_\chi}$, donc $\psi'\theta^{-1} \in \mathfrak{X}^-_{K_\chi}$ et comme

$\sigma_\chi = \left(\dfrac{K_\chi}{a}\right)$ engendre G_χ , l'ordre de $\psi'\theta^{-1}(a)$ est égal à l'ordre du

caractère $\psi'\theta^{-1}$; donc la condition est que $\psi'\theta^{-1}$ soit d'ordre une puissance de ℓ . Soit $\varphi' = \psi'\theta^{-1}$; on a le schéma :

$$\begin{tikzcd} K_\varphi \arrow[r, dash] \arrow[d, dash] & K_\psi \arrow[d, dash, "\ell^r"] \\ \mathbb{Q} \arrow[r, dash] & \mathbb{Q}^{(\ell)} \end{tikzcd}$$

<u>Lemme</u> II 14 . Si K_χ n'est pas une extension de degré ℓ^r , $r \geqslant 0$, de $\mathbb{Q}^{(\ell)}$, alors $(\bar{\Lambda}_\chi)_\ell = 1$.

En effet , on rappelle que $\bar{\Lambda}_\chi = \text{p.g.c.d.}\left(\dfrac{\Lambda_\chi}{\text{p.g.c.d.}(\bar{Q}(a), \Lambda_\chi)}, P_\chi(a)\right)$,

or , d'après ce qui précède , on a $P_\chi(a) \equiv 0$ mod ℓ si et seulement si il existe $\chi'_0|\chi$ tel que $\varphi' = \chi'_0\theta^{-1}$ soit un caractère d'ordre ℓ^r , $r \geqslant 0$, soit $g_\chi = (\ell-1)\ell^r$, d'où $[K_\chi : \mathbb{Q}^{(\ell)}] = \ell^r$. On peut donc désormais supposer que $[K_\chi : \mathbb{Q}^{(\ell)}]$ est d'ordre ℓ^r, $r \geqslant 0$.

Le corps K_χ est le composé de deux extensions K_φ et $\mathbb{Q}^{(\ell)}$ (avec $[K_\varphi : \mathbb{Q}] = \ell^r$) linéairement disjointes. Donc on peut poser $\chi'_o = \theta\varphi'$, $\varphi'|\varphi$ et $P_\chi(a) = \prod_{(\lambda, g_\chi)=1} (a - (\varphi'(a)\theta(a))^\lambda)$ puisque $\chi'|\chi$ équivaut à

$\chi' = \chi_o'^{\lambda}$ pour $\chi'_o|\chi$ fixé et $(\lambda, g_\chi) = 1$. On a, dans $\mathbb{Z}_\ell^{(\ell^r)}$,
$a - \varphi'^\lambda(a)\theta^\lambda(a) \equiv \theta(a)(1 - \varphi'^\lambda(a)\theta^{\lambda-1}(a)) \bmod \ell$. Les seuls termes à considérer (non premiers à ℓ) sont obtenus pour $\lambda \equiv 1 \bmod \ell - 1$, soit $\lambda \in \{1, \ldots, 1 + k(\ell-1), \ldots, 1 + (\ell^r-1)(\ell-1)\}$, avec pour $r \geqslant 1$ $(\lambda, \ell) = 1$, ce qui équivaut à $k \not\equiv 1 \bmod \ell$, $0 \leqslant k \leqslant \ell^r - 1$; cet ensemble a donc $\ell^{r-1}(\ell-1)$ valeurs (pour $r \geqslant 1$). Pour $r \geqslant 1$ et $\lambda \equiv 1 \bmod (\ell - 1)$, $a - \varphi'^\lambda(a)\theta^\lambda(a)$ a même valuation ℓ-adique que $1 - \varphi'^\lambda(a)$, car $\varphi'^\lambda(a)$ est une racine d'ordre une puissance de ℓ (ℓ^r, $r \geqslant 1$) et $\ell \neq 2$. Comme $\mathbb{Q}_\ell^{(\ell^r)}/\mathbb{Q}_\ell$ est totalement ramifiée en ℓ, on en déduit que $P_\chi(a)$ est divisible par ℓ et non par ℓ^2. Dans le cas $r = 0$, on a $K_\chi = \mathbb{Q}^{(\ell)}$ et dans ce cas, $\Lambda_\chi = \ell$ et $P_\chi(a) \equiv 0 \bmod \ell$, d'où $\bar{\Lambda}_\chi = \ell$ (dans le cas $K_\chi = \mathbb{Q}^{(\ell)}$, on peut avoir $P_\chi(a) \equiv 0 \bmod \ell^2$).

L'étude de $\bar{Q}(a)$ en résulte aussi : on rappelle que $\bar{Q}(a) = \prod_{\psi \in \Psi_\chi} P_\psi(a)$ (cf. Déf. II 3). On suppose qu'on est dans le cas où $P_\chi(a) \equiv 0$ mod ℓ ; comme le caractère unité appartient à Ψ_χ, il faut déterminer $P_1(a)$: on a $P_1(a) = a-1$; or $a-1 \equiv 0 \bmod \ell$, cela signifie que $\left(\frac{K_\chi}{a}\right) \in G(K_\chi/\mathbb{Q}^{(\ell)})$, ce qui n'est pas possible puisque $\left(\frac{K_\chi}{a}\right)$ doit engendrer G_χ et que $\mathbb{Q}^{(\ell)} \neq \mathbb{Q}$ car $\ell \neq 2$.

En vertu de l'étude faite, les seuls $\psi \in \Psi_\chi$ à considérer sont à prendre parmi ceux qui correspondent à un corps K_ψ intermédiaire entre K_χ et $\mathbb{Q}^{(\ell)}$ (et distinct de K_χ car $\chi \notin \Psi_\chi$).

Proposition II 6 . On suppose $\ell \neq 2$. Si $K_\chi = \mathbb{Q}^{(\ell)}$, alors $\bar{\Lambda}_\chi = \ell$. Si pour $\ell \mid f_\chi$ tel que $\mathbb{Q}^{(\ell)} \subset K_\chi$, $[K_\chi : \mathbb{Q}^{(\ell)}]$ est différent d'une puissance de ℓ , alors $(\bar{\Lambda}_\chi)_\ell = 1$. Si K_χ est une extension de degré ℓ^r , $r \geqslant 1$, de $\mathbb{Q}^{(\ell)}$, alors $(\bar{\Lambda}_\chi)_\ell = 1$ ou ℓ et on a $(\bar{\Lambda}_\chi)_\ell = 1$ si et seulement si $(\Lambda_\chi)_\ell$ divise $\prod_\psi P_\psi(a)$, le produit étant étendu aux caractères ψ tels que $\mathbb{Q}^{(\ell)} \subset K_\psi \subsetneqq K_\chi$ et tels que il existe $q \mid f_\chi$ totalement décomposé dans K_ψ .

(ii) Cas $\ell = 2$. On a donc $f_\chi = 2^n f'_\chi$, f'_χ impair et $n \geqslant 2$.

On suppose que l'on a $\mathbb{Q}^{(2^k)} \subset K_\chi$, $\mathbb{Q}^{(2^{k+1})} \not\subset K_\chi$, $k \geqslant 1$. Alors nécessairement on a $k = 1$ ou 2 .

Lemme II 15 . On a $N_{\mathbb{Q}^{(2^r)}/\mathbb{Q}^{(2^{r-1})}} \xi_{2^r} = -\xi_{2^{r-1}}$, pour tout $r \geqslant 2$.

En effet , les deux automorphismes de $\mathbb{Q}^{(2^r)}/\mathbb{Q}^{(2^{r-1})}$ sont, pour $r \geqslant 2$, l'identité et $\xi_{2^r} \longrightarrow \xi_{2^r}^{1+2^{r-1}}$ et $N\,\xi_{2^r} = \xi_{2^r}^2\,\xi_{2^r}^{2^{r-1}} = -\xi_{2^r}^2$

$= -\xi_{2^{r-1}}$.

Distinguons plusieurs cas :

Si $k = 2$ (i.e. $\mathbb{Q}^{(4)} \subset K_\chi$) on a le schéma ci-dessous :

$$\begin{tikzcd}
K_\psi \arrow[r, dash, "2"] \arrow[d, dash] & K_\chi \arrow[r, dash] \arrow[d, dash] & L = K_\chi \mathbb{Q}^{(2^n)} \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}^{(2^n f'_\chi)} \\
\mathbb{Q} \arrow[r, dash, "2"'] & \mathbb{Q}^{(4)} \arrow[r, dash, "2^{n-2}"'] & \mathbb{Q}^{(2^n)} &
\end{tikzcd}$$

Comme $\mathbb{Q}^{(2^n)}/\mathbb{Q}^{(4)}$ est cyclique , $K_\chi/\mathbb{Q}^{(4)}$ et $\mathbb{Q}^{(2^n)}/\mathbb{Q}^{(4)}$ sont linéairement disjointes . De plus $[K_\chi : \mathbb{Q}^{(4)}]$ est forcément impair . Il existe donc un sous-corps K_ψ de K_χ , tel que $[K_\chi : K_\psi] = 2$. Le corps K_ψ (réel) sera de conducteur impair (d'après la théorie des groupes de ramification , 2 ne peut pas se ramifier dans une extension cyclique de degré impair) et dans ce cas on a nécessairement $n = 2$, soit $f_\chi = 4 f'_\chi$. On a donc

$$N_{\mathbb{Q}^{(f_\chi)}/K_\chi}(\xi_4) = \xi_4^{[\mathbb{Q}^{(f_\chi)}:K_\chi]} = \xi_4^{[\mathbb{Q}^{(f_\chi)}:\ \mathbb{Q}^{(4)}]} = \xi_4^{\varphi(f'_\chi)}$$ et la valeur

de $(\Lambda_\chi)_2$ dépend du reste mod 4 de $\varphi(f'_\chi)$. Si $f'_\chi = 1$ alors $K_\chi = \mathbb{Q}^{(4)}$ et dans ce cas $\Lambda_\chi = 4$. Si $f'_\chi \neq 1$, $\varphi(f'_\chi)$ est pair , donc on aura $(\Lambda_\chi)_2 = 1$ ou 2 selon que $\varphi(f'_\chi) \equiv 0$ ou $2 \bmod 4$.

Si $k = 1$. On distingue encore deux cas : Si $K_\chi/\mathbb{Q}$ est linéairement disjointe de $\mathbb{Q}^{(2^n)}/\mathbb{Q}$, on a le schéma suivant :

$$\begin{tikzcd}
K_\chi \arrow[r, dash] \arrow[d, dash] & L = K_\chi \mathbb{Q}^{(2^n)} \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}^{(2^n f'_\chi)} \\
\mathbb{Q} \arrow[r, dash] & \mathbb{Q}^{(2^n)} &
\end{tikzcd}$$

et $N_{\mathbb{Q}^{(f_\chi)}/K_\chi}\ \xi_{2^n} = \left(N_{\mathbb{Q}^{(2^n)}/\mathbb{Q}}\ \xi_{2^n}\right)^{[\mathbb{Q}^{(f_\chi)}:L]} = 1$ et dans ce cas $\alpha_1 \equiv 0 \bmod 2^n$ soit $(\Lambda_\chi)_2 = 1$. Si $K_\chi/\mathbb{Q}$ n'est pas linéairement disjointe de $\mathbb{Q}^{(2^n)}/\mathbb{Q}$, alors K_χ est une extension de $k_o \subset \mathbb{Q}^{(2^n)}$:

$$\begin{tikzcd}
 & K_\chi \arrow[r, dash] \arrow[d, dash] & L = K_\chi \mathbb{Q}^{(2^n)} \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}^{(f_\chi)} \\
\mathbb{Q} \arrow[r, dash] & k_o \arrow[r, dash] & \mathbb{Q}^{(2^n)} &
\end{tikzcd}$$

Comme les cas $k_o = \mathbb{Q}$ et $k_o = \mathbb{Q}^{(4)}$ ont déjà été examinés , on peut supposer que k_o est l'un des deux corps suivants :

$k_o = \mathbb{Q}_+^{(2^m)}$ ou $k_o = \mathbb{Q}_+^{(2^{m-1})}(\mu_m)$, avec $3 \leqslant m \leqslant n$, $\mathbb{Q}_+^{(2^{m-1})}(\mu_m)$ désignant l'extension quadratique imaginaire de $\mathbb{Q}_+^{(2^{m-1})}$ contenue dans $\mathbb{Q}^{(2^m)}$ et distincte de $\mathbb{Q}^{(2^{m-1})}$. On vérifie facilement que si k_o est de la forme $\mathbb{Q}_+^{(2^m)}$ (k_o est alors réel) , on a $N_{\mathbb{Q}^{(f_\chi)}/K_\chi}\ \xi_{2^n} = 1$ et dans ce cas

$(\Lambda_\chi)_2 = 1$. Enfin, lorsque $k_o = \mathbb{Q}_+^{(2^{m-1})}(\mu_m)$, k_o est imaginaire ainsi que K_χ ; dans ce cas $[K_\chi : k_o]$ est nécessairement impair .

Lemme II 16 . On a , pour tout r , $r \geqslant 3$, $N_{\mathbb{Q}^{(2^r)}/\mathbb{Q}_+^{(2^{r-1})}(\mu_m)}\ \xi_{2^r} = -1.$

En effet , l'extension correspondante est quadratique et l'automorphisme non trivial est défini par $\xi_{2^r} \to \xi_{2^r}^{-1+2^{r-1}}$, d'où $N\xi_{2^r} = \xi_{2^r}^{2^{r-1}} = -1$.

On en déduit que $N_{\mathbb{Q}^{(f_\chi)}/K_\chi}\ \xi_{2^n} = \left(N_{\mathbb{Q}^{(2^n)}/k_o}\ \xi_{2^n}\right)^{[\mathbb{Q}^{(f_\chi)}:L]} =$

$N_{\mathbb{Q}^{(2^m)}/\mathbb{Q}_+^{(2^{m-1})}(\mu_m)}\ (\pm\ \xi_{2^m})^{[\mathbb{Q}^{(f_\chi)}:L]} = (-1)^{[\mathbb{Q}^{(f_\chi)}:L]} = (-1)^{[\mathbb{Q}^{(f_\chi)}:\mathbb{Q}^{(2^n)}]}$

puisque $[L : \mathbb{Q}^{(2^n)}]$ est impair . Or $[\mathbb{Q}^{(f_\chi)} : \mathbb{Q}^{(2^n)}] = \varphi(f'_\chi)$; donc si $f'_\chi \neq 1$, on a $\varphi(f'_\chi) \equiv 0 \bmod 2$ soit , dans ce cas , $(\Lambda_\chi)_2 = 1$. Si $f'_\chi = 1$, cela veut dire que $K_\chi = k_o = \mathbb{Q}_+^{(2^{n-1})}(\mu_m)$ et dans ce cas on a $\Lambda_\chi = 2$.

Proposition II 7 . Supposons $f_\chi = 2^n f'_\chi$, $n \geqslant 2$, f'_χ impair . Soit k_o l'intersection de K_χ avec l'extension $\mathbb{Q}^{(2^n)}$. Si k_o est réel alors $(\Lambda_\chi)_2 = 1$. Si $k_o = \mathbb{Q}^{(4)}$, $K_\chi \neq \mathbb{Q}^{(4)}$ alors $(\Lambda_\chi)_2 = 1$ (resp. 2) si $\varphi(f'_\chi) \equiv 0$ mod 4 (resp. $\varphi(f'_\chi) \equiv 2 \bmod 4$) . Si $k_o = K_\chi = \mathbb{Q}^{(4)}$ alors $\Lambda_\chi = 4$. si $k_o = \mathbb{Q}_+^{(2^{m-1})}(\mu_m)$, $3 \leqslant m \leqslant n$, alors $(\Lambda_\chi)_2 = 1$ (resp. 2) si $K_\chi \neq k_o$ (resp. $K_\chi = k_o$) .

Passons maintenant au calcul de $(\bar{\Lambda}_\chi)_2$. On procède comme pour le cas $\ell \neq 2$.

Soit $\psi \in \mathfrak{X}^-_{K_\chi}$ et soit a , (a, f_χ) = 1 , tel que $\left(\frac{K_\chi}{a}\right) = \sigma_\chi$.

On a $P_\psi(a) = \prod_{\psi'|\psi} (a - \psi'(a))$. Comme pour le cas $\ell \neq 2$, on aura $P_\psi(a) \equiv 0$ mod 2 si et seulement si il existe $\psi'|\psi$ tel que $a - \psi'(a)$ soit non premier à 2 . Or $a - \psi'(a) \equiv 1 - \psi'(a)$ mod 2 ; la condition est donc que $\psi'(a)$ soit d'ordre une puissance de 2 , donc , pour les mêmes raisons que pour $\ell \neq 2$, que ψ' soit d'ordre une puissance de 2 . Dans le cas $\psi = \chi$, $P_\chi(a) \equiv 0$ (2) équivaut à $[K_\chi : \mathbb{Q}]$ est une puissance de 2 . On peut donc supposer que g_χ est d'ordre une puissance de 2 . Dans ce cas , $P_\chi(a) = \prod_{\chi'|\chi} (a - \chi'(a))$ et $a - \chi'(a) \equiv 1 - \chi'(a)$ mod 2 ; on aura $P_\chi(a) \equiv 0$ mod 2 , $P_\chi(a) \not\equiv 0$ mod 4 si $1 - \chi'(a)$ et 2 n'ont pas la même valuation en 2 , donc dès que χ' est d'ordre 4 au moins . Si χ' est d'ordre 2 , $P_\chi(X) = X+1$ mais K_χ est alors un corps quadratique imaginaire de conducteur pair ; on aura donc $a \equiv -1$ mod 4 (σ_χ est la conjugaison complexe dans ce cas) ; or $P_\chi(-1) = 0$, $\bar{Q}(-1) = -2$. Si K_χ n'est pas l'un des deux corps $\mathbb{Q}^{(4)}$, $\mathbb{Q}(\sqrt{-2})$ alors $(\Lambda_\chi)_2 = 1$ (Prop. II 7) et $(\bar{\Lambda}_\chi)_2 = 1$.

Si $K_\chi = \mathbb{Q}^{(4)}$ alors (Prop. II 7) , on aura $(\bar{\Lambda}_\chi)_2 = 2$; enfin si $K_\chi = \mathbb{Q}(\sqrt{-2})$, on a (Prop. II 7) $(\Lambda_\chi)_2 = 2$ soit $(\bar{\Lambda}_\chi)_2 = 1$.

On suppose maintenant que g_χ est une puissance de 2 au moins égale à 4 . Alors $P_\chi(a) \equiv 2$ mod 4 ; on aura (cf. Déf. II 5) $\bar{Q}(X) = (X-1)\,\dfrac{(X^{g_\chi/2}+1)}{P_\chi}$ (car K_χ ne contient pas de sous-corps imaginaire strict et Ψ^*_χ est vide ; compte-tenu des résultats de la proposition II 7 , il suffit de connaître $\bar{Q}(a)$ mod 2 (en effet , pour les cas restants , $(\Lambda_\chi)_2 = 1$ ou 2). Donc , puisque $\bar{Q}(a) \equiv 0$ mod 2 , $(\bar{\Lambda}_\chi)_2 = \mathrm{pgcd}\left(\dfrac{(\Lambda_\chi)_2}{(2, (\Lambda_\chi)_2)}, 2\right) = 1$

<u>Proposition</u> II 8 . Soit $\chi \in \mathfrak{X}^-$. On a $(\bar{\Lambda}_\chi)_2 = 1$ sauf si $K_\chi = \mathbb{Q}^{(4)}$, auquel cas on a $\bar{\Lambda}_\chi = 2$.

On sait que si K_χ n'est pas une extension de degré une puissance de ℓ de $\mathbb{Q}^{(\ell)}$, alors $P_\chi(a)$ est premier à ℓ. Lorsque $P_\chi(a) \equiv 0 \bmod \ell$, on a $P_\chi(a) \not\equiv 0 \bmod \ell^2$ sauf peut être dans les cas suivants:

(i) $\ell \neq 2$ et $K_\chi = \mathbb{Q}^{(\ell)}$. Mais dans ce cas $(\Lambda_\chi)_\ell = \ell$ et $\Lambda_\chi^\circ = \ell$;

(ii) $\ell = 2$ et K_χ est un corps quadratique imaginaire. Dans ce cas $(\Lambda_\chi)_2 = 1$ ou 2 sauf dans le seul cas $K_\chi = \mathbb{Q}^{(4)}$ où $(\Lambda_\chi)_2 = 4$ et où $\Lambda_\chi^\circ = 4$.

Supposons que $g_\chi = (\ell-1)\ell^k$, $k \geqslant 0$. On sait que ℓ est totalement décomposé dans $\mathbb{Q}^{(\ell-1)}$ et que ℓ est totalement ramifié dans $\mathbb{Q}^{(\ell^k)}$. Donc si $(\zeta - a, \Lambda_\chi)$ n'est pas l'idéal unité, c'est l'un des $\varphi(\ell-1)$ idéaux premiers au-dessus de ℓ dans $\mathbb{Q}^{((\ell-1)\ell^k)}$.

<u>Théorème</u> II 5. Pour tout $\chi \in \mathfrak{X}^-$, le $\mathbb{Z}^{(g_\chi)}$-module $\mathbb{H}_\chi$ est annulé par l'idéal $B_1(\chi'^{-1})(\chi'(a) - a, \Lambda_\chi)$ de $\mathbb{Z}^{(g_\chi)}$. L'idéal $(\chi'(a) - a, \Lambda_\chi)$ étant l'idéal unité sauf lorsque K_χ est une extension de degré une puissance de ℓ de $\mathbb{Q}^{(\ell)}$ et que $\Lambda_\chi \equiv 0 \bmod \ell$, auquel cas cet idéal est l'un des $\varphi(\ell-1)$ idéaux premiers au-dessus de ℓ dans $\mathbb{Q}^{(g_\chi)}$ (sauf si $K_\chi = \mathbb{Q}^{(4)}$, auquel cas cet idéal est l'idéal (4)).

b) <u>Cas des caractères ℓ-adiques</u>. Soit $\chi \in \mathfrak{X}^-$ et soit $\phi | \chi$ (on a donc $\phi \in \Phi^-$). On rappelle que l'on a défini les $\mathbb{Z}_\ell[G_\chi]$-modules $\mathcal{H}_\phi = \{ h \in \mathcal{H}(K_\chi),\ P_\phi h = 1\}$, pour tout $\phi \in \Phi$ (cf. chap. I, § 4, c). On sait aussi que l'on définit sur $\mathcal{H}_\phi$ une loi de $\mathbb{Z}_\ell^{(g_\chi)}$-module au moyen de l'homomorphisme $\chi' : \mathbb{Z}_\ell[G_\chi] \longrightarrow \mathbb{Z}_\ell^{(g_\chi)}$ défini par $\sigma_\chi \longrightarrow \chi'(\sigma_\chi)$, avec $\chi' | \phi$ (ici, χ' doit diviser ϕ) ; pour les différents $\phi | \chi$, les lois de $\mathbb{Z}_\ell^{(g_\chi)}$-modules sont donc distinctes.

On sait que $\mathcal{H}_\phi$ est annulé par $\mathbb{Z}[G_\chi]S_{K_\chi} \cap \mathbb{Z}[G_\chi]$; c'est donc un $\mathbb{Z}_\ell^{(g_\chi)}$-module annulé par l'image de cet idéal par χ', $\chi' | \phi$. On obtient donc par analogie avec les calculs effectués dans le § a précédent et compte tenu du fait que $(\zeta - a, \Lambda_\chi)_{\mathbb{Z}_\ell^{(g_\chi)}}$ est de norme $(P_\phi(a), \Lambda_\chi)_{\mathbb{Z}}$:

Théorème II 6 . Pour tout $\phi \in \Phi^-$, le $\mathbb{Z}_\ell^{(g_\chi)}$-module $\mathcal{H}_\phi$ est annulé par l'idéal $B_1(\chi'^{-1})(\chi'(a) - a, \Lambda_\chi)$ de $\mathbb{Z}_\ell^{(g_\chi)}$, où χ' est l'un quelconque des diviseurs de ϕ . L'idéal $(\chi'(a) - a, \Lambda_\chi)$ de $\mathbb{Z}_\ell^{(g_\chi)}$ est l'idéal unité sauf lorsque K_χ est une extension de degré une puissance de ℓ de $\mathbb{Q}^{(\ell)}$, que l'on a $\Lambda_\chi \equiv 0 \bmod \ell$ et que la condition supplémentaire suivante est réalisée : en écrivant $\chi' = \theta^\lambda \psi'$, ψ' d'ordre ℓ^r , $1 \leq \lambda \leq \ell - 1$, alors $\lambda = 1$. Dans ce cas $(\chi'(a) - a, \Lambda_\chi)$ est l'unique idéal premier de $\mathbb{Z}_\ell^{(g_\chi)}$ divisant ℓ (sauf dans le cas $K_\chi = \mathbb{Q}^{(4)}$ où cet idéal est l'idéal (4)).

Remarque II 5 . Dans le cas où g_χ est de la forme $(\ell - 1)\ell^k$, il y a exactement $\varphi(\ell - 1)$ caractères ℓ-adiques divisant χ , il est donc normal que l'idéal $(\chi'(a) - a, \Lambda_\chi)$ puisse être l'idéal premier de $\mathbb{Z}_\ell^{(g_\chi)}$ pour un unique caractère ϕ_0 bien déterminé (celui qui est au-dessus de $\chi'_0 = \theta\psi'$) . Il est normal aussi de constater que le nombre λ ne dépend que du caractère ϕ au-dessus de χ' (à rapprocher du " cas spécial " défini dans [8] , Déf. III 4) .

Avant de faire certaines remarques sur le théorème de Stickelberger (cf. Remarques II 6 et II 7 , ci-après) nous allons proposer certaines définitions .

6) Définition d'invariants . Dans [8] (chap. I , § 2 , e) nous avions défini des invariants " classes " $m_\chi(\mathcal{H})$ et $m_\phi(\mathcal{H})$ et des invariants "analytiques " $m_\chi(h)$ et $m_\phi(h)$ pour les caractères rationnels et ℓ-adiques tels que g_χ soit premier à ℓ (cas semi-simple) . Nous nous proposons ici d'étendre cette définition au cas général .

(i) Invariants " classes " . Soit $\mathfrak{P}_\chi$ l'idéal premier de $\mathbb{Q}^{(g_\chi)}$ au-dessus de ℓ associé au plongement $\overline{\mathbb{Q}} \longrightarrow \hat{\Omega}_\ell$ et soit $\hat{\mathfrak{P}}_\chi$ sa fermeture dans $\mathbb{Z}_\ell^{(g_\chi)}$ (cf. [8] , chap. I , § 2 , e) . Soit $\phi \in \Phi$. En tant que $\mathbb{Z}_\ell^{(g_\chi)}$-module , $\mathcal{H}_\phi$ est isomorphe à un produit de la forme $\prod_{i \geq 1} \mathbb{Z}_\ell^{(g_\chi)} / \hat{\mathfrak{P}}_\chi^{\,n_{\phi,i}(\mathcal{H})}$,

les $n_{\phi,i}(\mathcal{H})$ étant supposés décroissants et nuls à partir d'un certain rang (ceci assure leur unicité) .

On a de même pour $\mathcal{H}'_\phi$ (cf. Déf. I 3) : $\mathcal{H}'_\phi \simeq \prod_{i\geqslant 1} \mathbb{Z}_\ell^{(g_\chi)} / \hat{\gamma}_\chi^{\,n_{\phi,i}(\mathcal{H}')}$:

<u>Définition</u> II 7 . On pose $m_\phi(\mathcal{H}) = \sum_{i\geqslant 1} n_{\phi,i}(\mathcal{H})$ et $m_\chi(\mathcal{H}) = \sum_{\phi|\chi} m_\phi(\mathcal{H})$;

on pose $m_\phi(\mathcal{H}') = \sum_{i\geqslant 1} n_{\phi,i}(\mathcal{H}')$ et $m_\chi(\mathcal{H}') = \sum_{\phi|\chi} m_\phi(\mathcal{H}')$, $\phi \in \Phi$, $\chi \in \mathcal{X}$.

(ii) <u>Invariants " analytiques " dans le cas impair</u> . Nous supposons maintenant $\chi \in \mathcal{X}^-$; le cas $\chi \in \mathcal{X}^+$ sera abordé dans le chapitre suivant .

Compte tenu des différentes interprétations obtenues pour l'ordre des groupes $\mathbb{H}_\chi$ ($\chi \in \mathcal{X}^-$) , nous proposons la suivante qui généralise celle de [8], qui tient compte du fait que $\mathcal{H}'_\chi = \mathcal{H}_\chi = \bigoplus_{\phi|\chi} \mathcal{H}_\phi$ (th. I 2) et qui va être particulièrement adaptée à certains résultats de Hasse concernant l'intégralité des nombres $\frac{1}{2} B_1(\chi'^{-1})$. On rappelle que

$$|\mathbb{H}_\chi| = 2^{\alpha_\chi} w_\chi \prod_{\chi'|\chi} \left(\frac{1}{2} B_1(\chi'^{-1})\right) .$$

<u>Définition</u> II 8 . On définit $m_\phi(h) = m_\phi(h')$, pour $\phi \in \Phi^-$, de la façon suivante :

(α) Cas $\ell \neq 2$.

$(\alpha)_1$ K_χ n'est pas de la forme $\mathbb{Q}^{(\ell^n)}$, $n \geqslant 1$;

on pose $\left(\frac{1}{2} B_1(\chi'^{-1})\right)\mathbb{Z}_\ell^{(g_\chi)} = \hat{\gamma}_\chi^{\,m_\phi(h)}$ $\quad (\chi'|\phi)$.

$(\alpha)_2$ $K_\chi = \mathbb{Q}^{(\ell^n)}$, $n \geqslant 1$; on a $g_\chi = (\ell-1)\ell^{\,n-1}$ et on peut écrire de façon unique $\chi' = \theta^\lambda \psi'$, ψ' d'ordre $\ell^{\,n-1}$, $(\lambda, \ell-1) = 1$. On rappelle que λ ne dépend que de ϕ au-dessus de χ' . On pose :

$$\left(\frac{1}{2} B_1(\chi'^{-1})\right)\mathbb{Z}_\ell^{(g_\chi)} = \hat{\gamma}_\chi^{\,m_\phi(h)} \quad , \text{ pour } \lambda \neq 1 \quad (\chi'|\phi) ,$$

$$m_\phi(h) = 0 \quad , \quad \text{pour } \lambda = 1 .$$

(β) Cas $\ell = 2$.

(β)$_1$ g_χ n'est pas une puissance de 2 , on pose :

$$\left(\frac{1}{2}\,B_1(\chi'^{-1})\right)\mathbb{Z}_\ell^{(g_\chi)} = \hat{\gamma}_\chi^{\,m_\phi(h)} \qquad (\chi'|\,\phi\,) .$$

(β)$_2$ Si g_χ est une puissance de 2 ; alors on a $\phi = \chi$ et on pose :

$$m_\phi(h) = 0 \quad \text{si } K_\chi = \mathbb{Q}^{(4)} ,$$

$$\left(\frac{1}{2}\,B_1(\chi'^{-1})\right)\mathbb{Z}_\ell^{(g_\chi)} = \hat{\gamma}_\chi^{\,m_\phi(h)-1} \qquad \text{si } K_\chi \neq \mathbb{Q}^{(4)} .$$

On pose ensuite dans tous les cas $m_\chi(h) = \sum\limits_{\phi|\chi} m_\phi(h)$.

<u>Proposition</u> II 10 . Les nombres $m_\phi(h)$ ainsi définis , pour tout $\phi \in \Phi^-$, sont positifs ou nuls .

<u>démonstration</u>

Rappelons un certain nombre de résultats de Hasse ([10] , chap. III) :

<u>Lemme</u> II 17 . Soit χ' un caractère impair et soit $\frac{1}{2}\,B_1(\chi'^{-1}) = \frac{1}{2\,f_\chi}\sum\limits_{a=1}^{f_{\chi^*}} \chi'^{-1}(a)\,a$.

(i) Si f_χ est divisible par au moins deux nombres premiers distincts, alors $\frac{1}{2}\,B_1(\chi'^{-1})$ est un entier algébrique ([10] , formule (3), p. 82) .

(ii) Si f_χ est de la forme ℓ^n , $\ell \neq 2$.

(ii)$_1$ Si g_χ n'est pas une puissance de 2 et si $K_\chi \neq \mathbb{Q}^{(\ell^n)}$ alors $\frac{1}{2}\,B_1(\chi'^{-1})$ est un entier algébrique ([10] , formule (7) , p. 91 et (13) , p. 92) .

(ii)$_2$ Si g_χ est puissance de 2 , $K_\chi \neq \mathbb{Q}^{(\ell^n)}$, alors

$(\chi'(\sigma_\chi) - 1)\frac{1}{2} B_1(\chi'^{-1})$ est entier (ici $(\chi'(\sigma_\chi) - 1)\mathbb{Z}^{(g_\chi)}$ est l'unique idéal premier au-dessus de 2 dans $\mathbb{Q}^{(g_\chi)}/\mathbb{Q}$) et $\frac{1}{2} B_1(\chi'^{-1})$ n'est pas 2-entier ([10], formule (6), p. 91).

$(ii)_3$ Si g_χ n'est pas puissance de 2 et si $K_\chi = \mathbb{Q}^{(\ell^n)}$ alors l'idéal $(\chi'(a) - a, \ell)\ \frac{1}{2} B_1(\chi'^{-1})$ de $\mathbb{Z}^{(g_\chi)}$ est un idéal entier ($(\chi'(a)-a,\ell)$ est alors un idéal premier au-dessus de ℓ dans $\mathbb{Q}^{(g_\chi)} = \mathbb{Q}^{((\ell-1)\ell^{n-1})}$) et $\frac{1}{2} B_1(\chi'^{-1})$ n'est pas ℓ-entier ([10], formule (12), p. 92).

$(ii)_4$ Le seul cas où g_χ est puissance de 2 et $K_\chi = \mathbb{Q}^{(\ell^n)}$, $\ell \neq 2$, est le cas $K = \mathbb{Q}^{(3)}$ et $\frac{1}{2} B_1(\chi'^{-1}) = -\frac{1}{6}$.

(iii) Si f_χ est de la forme 2^n, $n \geqslant 2$.

$(iii)_1$ Si $n = 2$, alors $K_\chi = \mathbb{Q}^{(4)}$ et $\frac{1}{2} B_1(\chi'^{-1}) = -\frac{1}{4}$.

$(iii)_2$ Si $n>2$, K_χ est alors l'unique sous-extension imaginaire cyclique de $\mathbb{Q}^{(2^n)}$, à savoir $\mathbb{Q}_+^{(2^{n-1})}(\mu_n)$, $g_\chi = 2^{n-2}$; alors $(\chi'(\sigma_\chi)-1)\ \frac{1}{2} B_1(\chi'^{-1})$ est entier (ici $\chi'(\sigma_\chi)-1$ engendre l'unique idéal premier au-dessus de 2 dans $\mathbb{Q}^{(2^{n-2})}$) et $\frac{1}{2} B_1(\chi'^{-1})$ n'est pas 2-entier ([10], formule (6), p. 94) .

Etudions alors les différents cas proposés dans la définition:

Cas (α). Comme $\ell \neq 2$, les seuls cas possibles de non intégralité en ℓ sont les cas $(ii)_3$ et $(ii)_4$ du lemme II 17 pour lesquels $K_\chi = \mathbb{Q}^{(\ell^n)}$. On a donc résolu le cas $(\alpha)_1$. Dans le cas $(\alpha)_2$, il suffit de déterminer l'idéal $(\chi'(a)-a,\ell)$ de $\mathbb{Z}_\ell^{(g_\chi)}$. Or $\chi'(a)-a = \psi'(a)\,\theta^\lambda(a) - a \equiv \theta(a)\,(\psi'\theta^{\lambda-1}(a)-1)$ mod ℓ ; donc $\psi'\theta^{\lambda-1}(a)-1$ est une unité de $\mathbb{Z}_\ell^{(g_\chi)}$ si $\lambda \not\equiv 1 \bmod (\ell-1)$. Dans le seul cas $\lambda \equiv 1 \bmod (\ell-1)$, l'idéal $(\chi'(a)-a,\ell)$ est égal à $\hat{\mathfrak{F}}_\chi$. D'où $(\alpha)_2$.

Cas (β) . On a $\ell = 2$ et les seuls cas à envisager sont les cas (ii $)_2$, (ii $)_4$ et (iii) (dans ces cas, g_χ est une puissance de 2 , par conséquent le cas ($\beta)_1$ est résolu) . Les derniers cas restants sont alors immédiats.

Proposition II 11. On a $m_\chi(h) = m_\chi(\mathcal{H})$ pour tout $\chi \in \mathfrak{X}^-$.

démonstration

On a $\mathcal{H}_\chi = \bigoplus_{\phi|\chi} \mathcal{H}_\phi$; par conséquent $|\mathcal{H}_\chi| = \prod_{\phi|\chi} |\mathcal{H}_\phi|$; or $|\mathcal{H}_\phi| = \ell^{\gamma m_\phi(\mathcal{H})}$ (l'anneau $\mathbb{Z}_\ell^{(g_\chi)}/\hat{\mathfrak{P}}_\chi^n$ a $\ell^{\gamma n}$ éléments , γ étant le degré résiduel de ℓ dans $\mathbb{Q}_\ell^{(g_\chi)}$.

On a ensuite $|\mathcal{H}_\chi| = (2^{\alpha_\chi} w_\chi)_\ell \prod_{\phi|\chi}\left(\prod_{\chi'|\phi} \frac{-1}{2} B_1(\chi'^{-1})\right)_\ell$ =

$(2^{\alpha_\chi} w_\chi)_\ell \prod_{\phi|\chi}\left(N_{\mathbb{Q}_\ell^{(g_\chi)}/\mathbb{Q}_\ell}\left(\frac{-1}{2} B_1(\chi'^{-1})\right)\right)_\ell$. On vérifie que le produit de normes ci-dessus est égal à $\ell^{\gamma\sum_{\phi|\chi} m_\phi(h)}$ dans les deux cas $K_\chi \neq \mathbb{Q}^{(\ell^n)}$, $\ell \neq 2$ et g_χ non puissance de 2 , $\ell = 2$; or dans ce cas , $(2^{\alpha_\chi} w_\chi)_\ell = 1$.
Il est égal à $\frac{\ell}{\ell}^{\gamma\sum m_\phi(h)}$ dans les cas $K_\chi = \mathbb{Q}^{(\ell^n)}$, $\ell \neq 2$ (le cas $\lambda = 1$ se produisant une fois et une seule lorsque $\phi|\chi$) et g_χ est une puissance de 2 ($K_\chi \neq \mathbb{Q}^{(4)}$) pour $\ell = 2$. Dans ces deux cas $(2^{\alpha_\chi} w_\chi)_\ell = \ell$.

Remarque II 6 . Il semble que le théorème de Stickelberger (sous forme du th. II 6 par exemple) soit insuffisant en 2 et même en ℓ dans certains cas : pour s'en convaincre considérons l'exemple déjà utilisé dans le § 4,a: $K_\chi = \mathbb{Q}_+^{(7)}\mathbb{Q}^{(3)}$ où l'on obtient les résultats suivants :

(i) $S_{K_\chi} = \frac{1}{3}(2 + 4\sigma + 5\sigma^2 + 4\sigma^3 + 2\sigma^4 + \sigma^5)$, avec $\sigma = \left(\frac{K_\chi}{2}\right)$;

(ii) $B_1(\chi'^{-1})\mathbb{Z}^{(g_\chi)} = (2)$;

(iii) $|\mathbb{H}_\chi| = 1$ (Th. II 2) ;

(iv) $(\chi'(a)-a,\Lambda_\chi) = (\chi'(\sigma)-2,\ 3) = (1-\chi'(\sigma)) = \mathfrak{P}_\chi$;

(v) $(\chi'(a)-a,\Lambda_\chi)\ B_1(\chi'^{-1})\ \mathbb{Z}^{(g_\chi)} = 2\ \mathfrak{P}_\chi$.

Si l'on compare (iii) et (v) on constate que " l'annulateur " trouvé est mauvais . On peut alors proposer plusieurs conjectures tendant à améliorer " l'annulateur " déduit du théorème de Stickelberger . Nous proposons la suivante : Pour tout $\phi\in\Phi^-$, l'idéal $\hat{\mathfrak{P}}_\chi^{\ m_\phi(h)}$ annule le $\mathbb{Z}_\ell^{(g_\chi)}$-module $\mathcal{H}_\phi$.

Remarque II 7 . Dans [2] (Th. 3.1) , le théorème de Stickelberger est énoncé sous la forme suivante (avec nos notations) : Si $L/\mathbb{Q}$ est abélienne alors l'idéal I' engendré par les éléments de $\mathbb{Z}[G(L/\mathbb{Q})]$: $\left(c - \left(\frac{L}{c}\right)\right) S'_L$

où c parcourt l'ensemble des entiers impairs premiers à f_L (pour S'_L , cf. Th. II 3) . L'idéal proposé par Coates est moins bon que l'idéal de Stickelberger $I = \mathfrak{U}_L\ S_L$ que nous avons calculé : Pour s'en convaincre , il suffit , par exemple , de comparer les deux idéaux $(I,\ \nu_{L/\mathbb{Q}})$ et $(I',\nu_{L/\mathbb{Q}})$: On vérifie facilement que $(I',\ \nu_{L/\mathbb{Q}}) = \left(\ldots,\ c - \left(\frac{L}{c}\right)\ ,\ldots\right) S_L\ + (\nu_{L/\mathbb{Q}})$

$(c\in\mathbb{Z},\ (c,\ 2\,f_L) = 1)$. Donnons alors un exemple numérique :

Soit L le composé de $\mathbb{Q}^{(3)}$ avec le sous-corps cubique de $\mathbb{Q}^{(19)}$; on vérifie facilement que $(I,\ \nu_{L/\mathbb{Q}}) = (S_L) + (\nu_{L/\mathbb{Q}})$; le calcul de $(I',\nu_{L/\mathbb{Q}})$ donne alors :

$(I',\nu_{L/\mathbb{Q}}) = \left(\ldots,\ c - \left(\frac{L}{c}\right)\ ,\ldots\right) S_L + (\nu_{L/\mathbb{Q}}) = \left(\ldots, c-\left(\frac{L}{c}\right)\ ,\ldots;\ 2\,f_L\right)S_L + (\nu_{L/\mathbb{Q}})$; or si on considère des c tels que $\left(\frac{L}{c}\right) = 1$ $((c,\ 2\,f_L) = 1)$, on vérifie facilement que les $c - \left(\frac{L}{c}\right)$ correspondants engendrent l'idéal (6), d'où $(I',\ \nu_{L/\mathbb{Q}}) = \left(\ldots,\ c - \left(\frac{L}{c}\right)\ ,\ldots;\ 6\right) S_L + (\nu_{L/\mathbb{Q}})$. Soit alors c_o

impair tel que $\left(\frac{L}{c_o}\right)$ engendre $G(L/\mathbb{Q})$. On vérifie (comme pour la proposition II 3) que $(I', \mathfrak{d}_{L/\mathbb{Q}}) = (c_o - \left(\frac{L}{c_o}\right) ; 6) S_L + (\mathfrak{d}_{L/\mathbb{Q}})$;

on peut prendre $c_o = f_L + 2$; on a alors :

$$(I', \mathfrak{d}_{L/\mathbb{Q}}) = (5 - \left(\frac{L}{2}\right) ; 6) S_L + (\mathfrak{d}_{L/\mathbb{Q}}) ,$$

$$(I, \mathfrak{d}_{L/\mathbb{Q}}) = (S_L) + (\mathfrak{d}_{L/\mathbb{Q}}) .$$

Soit alors χ' le caractère de L défini par $\chi'(2) = -j$; alors $\chi'(I', \mathfrak{d}_{L/\mathbb{Q}}) = \chi'(I') = (1-j)\chi'(S_L) = 2(1-j)^2$ et $\chi'(I, \mathfrak{d}_{L/\mathbb{Q}}) = \chi'(I) = 2(1-j)$ (car $\chi'(5 - \left(\frac{L}{2}\right) ; 6) = (1-j)$ et $\chi'(S_L) = -4_j - 2$).

Ce qui illustre notre remarque .

Chap. III

Application à l'étude des classes réelles des extensions abéliennes

On désigne par $\mathbb{E}$ la $\mathfrak{S}'$-famille des groupes des valeurs absolues des unités des sous-corps de $\mathbb{Q}^a$ (la loi de module étant définie par $|\varepsilon|^{\sigma} = |\varepsilon^{\sigma}|$, pour tout $\sigma \in \mathfrak{S}$) . Les $\mathbb{E}(K)$ sont donc des $\mathbb{Z}$-modules libres (on a donc $\mathbb{E}(K) = |E(K)|$ si l'on désigne par $E(K)$ le groupe des unités de K) .

On a $\mathbb{E}_\chi = \{|\varepsilon| \in \mathbb{E}(K_\chi) , P_\chi(\sigma_\chi)|\varepsilon| = 1\} = \{|\varepsilon| \in \mathbb{E}(K_\chi) , \nu_{K_\chi/K}|\varepsilon| = 1 , \text{ pour tout } K \subsetneq K_\chi\}$.

Désignons par $\mathbb{E}^o$ la $\mathfrak{S}$-famille pour laquelle $\mathbb{E}^o(K)$ est le sous-groupe de $\mathbb{E}(K)$ engendré par les $\mathbb{E}(k)$ pour $k \subsetneq K$.

1) Interprétation des coefficients $Q(K)$ et $q(K)$.

Lemme III 1 . On a $\mathbb{E}^o(K_\chi)\mathbb{E}_\chi = \mathbb{E}^o(K_\chi) \oplus \mathbb{E}_\chi$, pour tout $\chi \in \mathfrak{X}^+$.

On sait que $\bigoplus_{\psi \in \mathfrak{X}_K} \mathbb{E}_\psi$ est d'indice fini dans $\mathbb{E}(K)$ quel que soit K réel (cf. 15 , § 5, 4) . Soit $|\varepsilon| \in \mathbb{E}^o(K_\chi) \cap \mathbb{E}_\chi$; il existe donc des sous-corps stricts $K_1, \dots, K_t$ de K_χ tels que $|\varepsilon| = |\varepsilon_1| \dots |\varepsilon_t|$, $|\varepsilon_i| \in \mathbb{E}(K_i)$ et il existe une puissance de $|\varepsilon|$, $|\varepsilon|^n$, telle que $|\varepsilon_i^n| \in \bigoplus_{\psi \in \mathfrak{X}_{K_i}} \mathbb{E}_\psi$, pour tout i ; on a donc $|\varepsilon|^n \in \Big(\bigoplus_{\substack{\psi \in \mathfrak{X}_{K_\chi} \\ \psi \neq \chi}} \mathbb{E}_\psi\Big) \cap \mathbb{E}_\chi$, ce qui entraîne $|\varepsilon|^n = 1$; mais alors $|\varepsilon| = 1$.

Définition III 1 . On pose pour tout χ pair : $Q_\chi = (\mathbb{E}(K_\chi) : \mathbb{E}^o(K_\chi) \oplus \mathbb{E}_\chi)$; on pose $Q(L) = (\mathbb{E}(L) : \bigoplus_{\psi \in \mathfrak{X}_L} \mathbb{E}_\psi)$, pour tout L réel .

Proposition III 1 . On a pour toute extension cyclique réelle $L/\mathbb{Q}$:

$$Q(L) = \prod_{\chi \in \mathfrak{X}_L} Q_\chi \ .$$

démonstration

On va effectuer ce calcul localement : Soit donc ℓ un nombre premier fixé .

Pour tout corps K posons $\mathcal{E}(K) = \mathbb{E}(K) \otimes \mathbb{Z}_\ell$ (considéré canoniquement comme $\mathfrak{S}$-module) et pour tout χ posons $\mathcal{E}_\chi = \mathbb{E}_\chi \otimes \mathbb{Z}_\ell$ et $\mathcal{E}^o(K_\chi) = \mathbb{E}^o(K_\chi) \otimes \mathbb{Z}_\ell$. Comme $\mathbb{E}_\chi$ est le noyau de l'homomorphisme qui à $|\varepsilon| \in \mathbb{E}(K_\chi)$ associe $|\varepsilon|^{P_\chi(\sigma_\chi)}$ et que $\mathbb{Z}_\ell$ est plat alors $\mathcal{E}_\chi$ est égal au noyau de ce même homomorphisme étendu à $\mathcal{E}(K_\chi)$ (la notation $\mathcal{E}_\chi$ est donc cohérente avec celle qu'on obtient en considérant la $\mathfrak{S}'$-famille $\mathcal{E}$) .
On a aussi que $\mathcal{E}^o(K_\chi)$ est engendré par les $\mathcal{E}(k)$, k $\subsetneq K_\chi$.

On a alors : $(Q_\chi)_\ell = (\mathcal{E}(K_\chi) : \mathcal{E}^o(K_\chi) \oplus \mathcal{E}_\chi)$,

$$(Q(L))_\ell = (\mathcal{E}(L) : \bigoplus_{\psi \in \mathfrak{X}_L} \mathcal{E}_\psi) \ .$$

Considérons le schéma suivant (cf. chap. I , § 6) :

$$\begin{tikzcd}
L'_n \arrow[r, dash] \arrow[d, dash] & K_{\psi_n} \arrow[r, dash] \arrow[d, dash] & L_n = L \arrow[d, dash] \\
L'_i \arrow[r, dash] \arrow[d, dash] & K_{\psi_i} \arrow[r, dash] \arrow[d, dash] & L_i = K_{\varphi_i} \arrow[d, dash] \\
L' = \mathbb{Q} \arrow[r, dash] & K_{\psi_0} = K_\psi \arrow[r, dash] & L_o
\end{tikzcd}$$

où L/L_o est cyclique de degré ℓ^n , L/L'_n est cyclique de degré premier à ℓ .

Ici ψ parcourt l'ensemble $\mathfrak{X}_{L_o}$. Pour simplifier , on appellera φ_i le caractère défini par $K_{\varphi_i} = L_i$ pour $0 \leqslant i \leqslant n$ (Si $L = K_\chi$, on a donc $\varphi_n = \chi$).

Pour la définition des familles d'idempotents e'_ψ et e_ψ , $\psi \in \mathfrak{X}_{L_o}$, cf. chap. I , § 6 .

On posera $\mathcal{E}^*(K_{\psi_i}) = \{ |\varepsilon| \in \mathcal{E}(K_{\psi_i}) \ , \ N_{K_{\psi_i}/K_{\psi_{i-1}}} |\varepsilon| = 1 \}$, pour tout ψ et tout $i \geqslant 1$ et $\mathcal{E}^*(K_{\psi_o}) = \mathcal{E}(K_{\psi_o})$ (on a

$\mathcal{E}^*(K_{\psi_i}) = \mathbb{E}^*(K_{\psi_i}) \otimes \mathbb{Z}_\ell$, en définissant $\mathbb{E}^*(K_{\psi_i})$ de façon analogue) .

Remarquons d'abord que $\mathcal{E}^*(L_i) = \bigoplus_\psi \mathcal{E}^*(L_i)^{e'_\psi}$ et que , d'après la propriété des e_ψ lorsque les applications j et N sont respectivement injectives et surjectives dans les sous-extensions de $L/\mathbb{Q}$ de degré premier à ℓ (cf. chap. I , § 6) , on a $\mathcal{E}^*(L_i)^{e'_\psi} = \mathcal{E}^*(K_{\psi_i})^{e_\psi} = \mathcal{E}_{\psi_i}$.

<u>Lemme</u> III 2 . On a $(\mathcal{E}(L_i) : \mathcal{E}(L_{i-1}) \oplus \mathcal{E}^*(L_i))$ =

$$= \prod_{\psi \in \mathcal{X}_{L_o}} (\mathcal{E}(K_{\psi_i})^{e_\psi} : \mathcal{E}(K_{\psi_{i-1}})^{e_\psi} \oplus \mathcal{E}_{\psi_i}) ,$$

pour $i \geqslant 1$.

On a $\mathcal{E}(L_i) / \mathcal{E}(L_{i-1}) \oplus \mathcal{E}^*(L_i) = \bigoplus_\psi \mathcal{E}(L_i)^{e'_\psi} / \bigoplus_\psi (\mathcal{E}(L_{i-1}) \overset{'}{\oplus} \mathcal{E}_{\psi_i}) =$

$\bigoplus_\psi \mathcal{E}(K_{\psi_i})^{e_\psi} / \bigoplus_\psi (\mathcal{E}(K_{\psi_{i-1}})^{e_\psi} \oplus \mathcal{E}_{\psi_i})$; or $\mathcal{E}(K_{\psi_{i-1}})^{e_\psi} \oplus \mathcal{E}_{\psi_i}$ est un sous-module de $\mathcal{E}(K_{\psi_i})^{e_\psi}$ puisque $\mathcal{E}_{\psi_i} = \mathcal{E}^*(K_{\psi_i})^{e_\psi}$. On a donc un quotient

isomorphe à :

$$\bigoplus_\psi (\mathcal{E}(K_{\psi_i})^{e_\psi} / \mathcal{E}(K_{\psi_{i-1}})^{e_\psi} \oplus \mathcal{E}_{\psi_i}) \text{ , d'où le résultat .}$$

Considérons maintenant , pour $i \geqslant 1$, le quotient (fini) :

$\mathcal{E}(L_i) / \mathcal{E}^o(L_i) \oplus \mathcal{E}_{\varphi_i} \simeq \bigoplus_\psi (\mathcal{E}(K_{\psi_i})^{e_\psi} / (\mathcal{E}^o(L_i) \oplus \mathcal{E}_{\varphi_i})^{e'_\psi})$; on a

$$\mathcal{E}^o(L_i)^{e'_\psi} = \prod_{K \subsetneqq L_i} \mathcal{E}(K)^{e'_\psi} \text{ . Or } \Big(\prod_{K \subsetneqq L_i} \mathcal{E}(K)\Big)^{e'_\psi} =$$

$$= \xi(L_{i-1})^{e'_\psi} \prod_{\substack{\mu \neq \varphi \\ \mu \in \mathfrak{X}_{L_0}}} \xi(K_{\mu_i})^{e'_\psi} \quad ; \text{ on a } \quad \xi(L_{i-1})^{e'_\psi} = \xi(K_{\psi_{i-1}})^{e_\psi} .$$

Calculons maintenant $\xi(K_{\mu_i})^{e'_\psi}$ pour $\mu \neq \varphi$: $\xi(K_{\mu_i}) =$

$$\bigoplus_{\rho \in \mathfrak{X}_{K_\mu}} \xi(K_{\mu_i})^{e'_\rho} = \bigoplus_{\rho \in \mathfrak{X}_{K_\mu}} \xi(K_{\rho_i})^{e_\rho} \quad \text{et} \quad \xi(K_{\mu_i})^{e'_\psi} = \bigoplus_{\rho \in \mathfrak{X}_{K_\mu}} \xi(K_{\rho_i})^{e_\rho e'_\psi} =$$

$\xi(K_{\psi_i})^{e_\psi}$ (resp. 1) si $\psi \in \mathfrak{X}_{K_\mu}$(resp. $\psi \notin \mathfrak{X}_{K_\mu}$) .

On a donc $\prod_{\substack{\mu \neq \varphi \\ \mu \in \mathfrak{X}_{L_0}}} \xi(K_{\mu_i})^{e'_\psi} = \prod_{\substack{\mu \neq \varphi \\ \psi \in \mathfrak{X}_{K_\mu}}} \xi(K_{\psi_i})^{e_\psi} = \prod_{\substack{\mu \neq \varphi \\ K_\mu \supset K_\psi}} \xi(K_{\psi_i})^{e_\psi}$;
ce produit est donc égal à $\xi(K_{\psi_i})^{e_\psi}$ (resp.(1)) si $\psi \neq \varphi$ (resp. $\psi = \varphi$).
D'où :

$$\xi^o(L_i)^{e'_\psi} = \xi(K_{\psi_{i-1}})^{e_\psi} \xi(K_{\psi_i})^{e_\psi} = \xi(K_{\psi_i})^{e_\psi} \quad \text{si } \psi \neq \varphi \text{ et}$$

$$\xi^o(L_i)^{e'_\varphi} = \xi(K_{\varphi_{i-1}})^{e_\varphi} .$$

Enfin $(\xi^o(L_i) \oplus \xi_{\varphi_i})^{e'_\psi} = \xi(K_{\psi_i})^{e_\psi}$ pour $\psi \neq \varphi$ (car

$\xi_{\varphi_i}^{e'_\psi} = (1)$ et $(\xi^o(L_i) \oplus \xi_{\varphi_i})^{e'_\varphi} = \xi(K_{\varphi_{i-1}})^{e_\varphi} \oplus \xi_{\varphi_i}$.

Le quotient $\xi(K_{\psi_i})^{e_\psi} / (\xi^o(L_i) \oplus \xi_{\varphi_i})^{e'_\psi}$ est donc égal à

(1) si $\psi \neq \varphi$ et égal à $\xi(K_{\varphi_i})^{e_\varphi} / \xi(K_{\varphi_{i-1}})^{e_\varphi} \oplus \xi_{\varphi_i}$, pour $\psi = \varphi$.

On a donc démontré :

$$\xi(L_i) / \xi^o(L_i) \oplus \xi_{\varphi_i} \simeq \xi(K_{\varphi_i})^{e_\varphi} / \xi(K_{\varphi_{i-1}})^{e_\varphi} \oplus \xi_{\varphi_i}) \quad , \text{ pour } i \geqslant 1 .$$

On en déduit , en remplaçant L_i par un corps K_{ψ_i} , $i \geqslant 1$:

Lemme III 3 . Pour tout $\psi \in \mathfrak{X}_{L_o}$ et pour $i \geq 1$, on a :

$$\mathcal{E}(K_{\psi_i})/\mathcal{E}^o(K_{\psi_i}) \oplus \mathcal{E}_{\psi_i} \simeq \mathcal{E}(K_{\psi_i})^{e_\psi} / \mathcal{E}(K_{\psi_{i-1}})^{e_\psi} \oplus \mathcal{E}_{\psi_i}$$ et en conséquence

on a $(Q_{\psi_i})_\ell = (\mathcal{E}(K_{\psi_i})^{e_\psi} : \mathcal{E}(K_{\psi_{i-1}})^{e_\psi} \oplus \mathcal{E}_{\psi_i})$.

Considérons maintenant $(Q(L_n))_\ell = (\mathcal{E}(L_n) : \bigoplus_{\psi, i\geq 0} \mathcal{E}_{\psi_i})$;

on a $\bigoplus_{\psi, i\geq 0} \mathcal{E}_{\psi_i} = \bigoplus_{i\geq 0} \mathcal{E}^*(L_i)$ car $\mathcal{E}_{\psi_i} = \mathcal{E}^*(K_{\psi_i})^{e_\psi} = \mathcal{E}^*(L_i)^{e'_\psi}$;

$$(Q(L_n))_\ell = (\mathcal{E}(L_n) : \bigoplus_{i\geq 0} \mathcal{E}^*(L_i)) = (\mathcal{E}(L_n) : \mathcal{E}^*(L_n) \oplus \mathcal{E}(L_{n-1}))$$

$$(\mathcal{E}^*(L_n) \oplus \mathcal{E}(L_{n-1}) : \mathcal{E}^*(L_n) \oplus \mathcal{E}^*(L_{n-1}) \oplus \mathcal{E}(L_{n-2})) \ldots$$

$$(\mathcal{E}^*(L_n) \oplus \ldots \oplus \mathcal{E}^*(L_2) \oplus \mathcal{E}(L_1) : \mathcal{E}^*(L_n) \oplus \ldots \oplus \mathcal{E}^*(L_2) \oplus \mathcal{E}^*(L_1) \oplus \mathcal{E}(L_o))$$

$$= (\mathcal{E}(L_n) : \mathcal{E}^*(L_n) \oplus \mathcal{E}(L_{n-1}))\,(\mathcal{E}(L_{n-1}) : \mathcal{E}^*(L_{n-1}) \oplus \mathcal{E}(L_{n-2})) \ldots$$
$$(\mathcal{E}(L_1) : \mathcal{E}^*(L_1) \oplus \mathcal{E}(L_o)) \; ;$$

or on avait calculé (lemme III 2) $(\mathcal{E}(L_i) : \mathcal{E}(L_{i-1}) \oplus \mathcal{E}^*(L_i))$; d'où

$$(Q(L_n))_\ell = \prod_{i=1}^{n} (\mathcal{E}(L_i) : \mathcal{E}^*(L_i) \oplus \mathcal{E}(L_{i-1})) =$$

$$\prod_{i=1}^{n} \prod_{\psi \in \mathfrak{X}_{L_o}} (\mathcal{E}(K_{\psi_i})^{e_\psi} : \mathcal{E}(K_{\psi_{i-1}})^{e_\psi} \oplus \mathcal{E}_{\psi_i}) = \prod_{i=1}^{n} \prod_{\psi \in \mathfrak{X}_{L_o}} (Q_{\psi_i})_\ell$$

(lemme III 3) ; comme $(Q_{\psi_o})_\ell = 1$ pour tout ψ , on a donc vérifié la propriété localement pour tout ℓ et la proposition en résulte .

Définition III 2 . Pour tout χ pair , on pose :

$$q_\chi = \prod_{p \mid g_\chi} p^{\frac{\varphi(g_\chi)}{p-1}}$$, si g_χ n'est pas la puissance d'un nombre premier ;

$$q_\chi = p^{\frac{\varphi(g_\chi)}{p-1}-1}$$, si $g_\chi \neq 1$ est puissance du nombre premier p ,

$q_1 = 1$;

Soit alors L une extension abélienne réelle de $\mathbb{Q}$ et soit $[L:\mathbb{Q}] = g$;

on pose $q(L) = \left(\dfrac{g^{g-2}}{\prod_{\chi \in \mathfrak{X}_L} d_\chi} \right)^{1/2}$, où d_χ est le discriminant du corps $\mathbb{Q}^{(g_\chi)}$.

On a le résultat suivant :

<u>Proposition</u> III 2 . Si L est une extension cyclique réelle de $\mathbb{Q}$ alors :

$$q(L) = \prod_{\chi \in \mathfrak{X}_L} q_\chi \quad .$$

démontrons d'abord le lemme suivant :

<u>Lemme</u> III 4 . Soit $L/\mathbb{Q}$ cyclique . Posons $q'(L) = \left(\dfrac{g^g}{\prod_{\chi \in \mathfrak{X}_L} d_\chi} \right)^{1/2}$ et

$q'_\chi = \prod_{p \mid g_\chi} p^{\frac{\varphi(g_\chi)}{p-1}}$. On a $\prod_{\chi \in \mathfrak{X}_L} q'_\chi = \left(\dfrac{g^g}{\prod_{\chi \in \mathfrak{X}_L} d_\chi} \right)^{1/2} = q'(L)$.

D'après Hasse ([10] , § 15 , p. 34 et suivantes) , le nombre $\dfrac{g^g \prod_\chi d_\chi}{\prod_\chi g_\chi^{2\varphi(g_\chi)}}$ (formule (2) , p. 35 de [10]) est égal à 1 dans le cas cyclique (Satz 8) . Donc , on aura $g^g \prod_\chi d_\chi = \prod_\chi g_\chi^{2\varphi(g_\chi)}$ soit

$$\frac{g^g}{\prod_\chi d_\chi} = \left(\frac{\prod_\chi g_\chi^{\varphi(g_\chi)}}{\prod_\chi d_\chi} \right)^2 \text{ ; or } \frac{g_\chi^{\varphi(g_\chi)}}{d_\chi} = \frac{g_\chi^{\varphi(g_\chi)}}{g_\chi^{\varphi(g_\chi)} \Big/ \prod_{p \mid g_\chi} p^{\frac{\varphi(g_\chi)}{p-1}}}$$

$= q'_\chi$, d'où le lemme .

Lemme III 5 . Posons $u_\chi = p$ (resp. 1) si $g_\chi \neq 1$ est puissance d'un nombre premier p (resp. n'est pas) et $u_1 = 1$. Alors pour toute extension cyclique $L/\mathbb{Q}$, on a $\prod_{\chi \in \mathcal{X}_L} u_\chi = [L : \mathbb{Q}]$.

La proposition résulte des lemmes précédents .

2) Rappels sur les unités cyclotomiques de Leopoldt ([15] ; cf. [17]).

Soit $\theta_\chi = \prod_{a \in \mathfrak{A}_\chi} (\zeta_{2f_\chi}^{a} - \zeta_{2f_\chi}^{-a})$, $\mathfrak{A}_\chi$ désignant un " demi-système" de représentants dans $(\mathbb{Z}/f_\chi\mathbb{Z})^*$ de Gal $(\mathbb{Q}^{(f_\chi)}/K_\chi)$ (cf. [15] , § 8 , 1) et $\zeta_{2f_\chi} = \exp(\frac{i\pi}{f_\chi})$. On sait que $\theta_\chi^2 \in K_\chi$ et que pour tout conjugué θ'_χ de θ_χ dans $\mathbb{Q}^a/\mathbb{Q}$, $\frac{\theta'_\chi}{\theta_\chi}$ est une unité de K_χ ([15] , § 8 , 1) ; les nombres θ_χ^2 et $\frac{\theta'_\chi}{\theta_\chi}$ ne dépendent pas du choix de $\mathfrak{A}_\chi$ tandis que θ_χ en dépend (par le signe uniquement) .

Définition III 3 . Soit K réel et soit $\Theta'(K)$ le sous-groupe de $\mathbb{Q}^{a*}$ engendré par les θ_ψ et leurs conjugués , pour $\psi \in \mathcal{X}_K$. Compte tenu des propriétés des θ_ψ (définis au signe près) , on considère le groupe $\Theta(K) = |\Theta'(K)|$. On pose ensuite $\mathbb{F}(K) = \Theta(K) \cap \mathbb{E}(K)$ (on a donc $\mathbb{F}(K) = |\Theta'(K) \cap E(K)|$) . Enfin soit $\mathcal{F}(K) = \mathbb{F}(K) \otimes \mathbb{Z}_\ell$.

Lemme III 6 . Le groupe $\Theta(K)$ est canoniquement un $\mathfrak{G}$ -module sans $\mathbb{Z}$-torsion . La famille des $\Theta(K)$ constitue une $\mathfrak{G}'$-famille . Il en est de même pour les familles $\mathbb{F}$ et $\mathcal{F}$.

Le fait que $\Theta(K)$ soit un $\mathfrak{G}$ -module provient du fait que pour $\sigma \in G(K/\mathbb{Q})$ et $\theta \in \Theta'(K)$, $\theta^{2\sigma}$ est défini et si $\bar{\sigma}$ est un prolongement de

σ à $K(\theta)$, alors $\theta^{\bar\sigma}$ est défini au signe près (car $[K(\theta) : K] = 1$ ou 2) , alors $|\theta^{\bar\sigma}|$ ne dépend pas du choix de $\bar\sigma$ et on peut poser $|\theta|^{\sigma} = |\theta^{\bar\sigma}|$.

Les résultats de [15] (chap. 3 , § 8 , 2) montrent que Θ est une $\mathfrak{G}'$-famille relativement aux normes habituelles $N_{L/K}$ et aux injections canoniques $j_{L/K} : K \longrightarrow L$; en effet , on a pour tout χ , $\psi \in \mathfrak{X}^+$ et tels que $K_\psi \subset K_\chi$: $N_{K_\chi/K_\psi}(|\theta_\chi|) = |\theta_\psi|^{\omega}$ avec $\omega = \prod_{q \mid f_\chi} \left(1 - \left(\frac{K_\psi}{q}\right)^{-1}\right)$ et le cas général en résulte facilement .

3) <u>Détermination de $|\mathbb{H}'_\chi|$, χ pair</u> . En utilisant la formule de Leopoldt ([15] , Satz 21 , les propositions III 1 et III 2) , on obtient , en désignant par $\overline{\mathbb{F}}_\chi$ le sous-groupe de $\mathbb{E}_\chi$ engendré par l'unité $|\theta_\chi|^{D_\chi}$, $D_\chi = \prod_{p \mid g_\chi} (1 - \sigma_\chi^{g_\chi/p})$ ([15], § 8 , 4) :

<u>Théorème</u> III 1 . Pour tout $\chi \in \mathfrak{X}^+$, on a :

$$|\mathbb{H}'_\chi| = \frac{Q_\chi}{q_\chi} \; (\mathbb{E}_\chi : \overline{\mathbb{F}}_\chi) \; .$$

<u>Corollaire</u> III 1 . On a $|\mathbb{H}'_\chi| = \dfrac{(\mathbb{E}(K_\chi) : \mathbb{E}^{\circ}(K_\chi) \oplus \overline{\mathbb{F}}_\chi)}{q_\chi}$.

En effet , on écrit que $(\mathbb{E}(K_\chi) : \mathbb{E}^{\circ}(K_\chi) \oplus \overline{\mathbb{F}}_\chi) = (\mathbb{E}(K_\chi) : \mathbb{E}^{\circ}(K_\chi) \oplus \mathbb{E}_\chi)\,(\mathbb{E}^{\circ}(K_\chi) \oplus \mathbb{E}_\chi : \mathbb{E}^{\circ}(K_\chi) \oplus \overline{\mathbb{F}}_\chi)$.

On a donc ainsi interprété le coefficient Q_χ (cf. Déf. III 1) .

Pour interpréter le coefficient q_χ nous allons remplacer le groupe des unités cyclotomiques de Leopoldt par un groupe d'unités plus gros : nous allons utiliser $\mathbb{F}(K_\chi)$.

Nous nous proposons de calculer l'indice suivant pour $\chi \in \mathfrak{X}^+$: $(\mathbb{E}(K_\chi) : \mathbb{E}^{\circ}(K_\chi)\, \mathbb{F}(K_\chi))$.

On a $\left|\mathbb{H}'_\chi\right| = \frac{1}{q_\chi}\,(\,\mathbb{E}(K_\chi) : \mathbb{E}^o(K_\chi) \oplus \overline{\mathbb{F}}_\chi\,) =$

$(\,\mathbb{E}(K_\chi) : \mathbb{E}^o(K_\chi)\,\mathbb{F}(K_\chi))\,(\,\mathbb{E}^o(K_\chi)\,\mathbb{F}(K_\chi) : \mathbb{E}^o(K_\chi) \oplus \overline{\mathbb{F}}_\chi)\,\frac{1}{q_\chi}$;

on a alors l'égalité $(\,\mathbb{E}^o(K_\chi)\,\mathbb{F}(K_\chi) : \mathbb{E}^o(K_\chi) \oplus \overline{\mathbb{F}}_\chi) =$

$= (\,\mathbb{F}(K_\chi) : (\,\mathbb{E}^o(K_\chi) \oplus \overline{\mathbb{F}}_\chi) \cap \mathbb{F}(K_\chi)\,))$.

Nous allons calculer cet indice localement .

Soit ℓ premier fixé ; on utilise le schéma habituel en effectuant le changement de notations correspondant (L_n remplace K_χ , $\chi = \varphi_n$, cf. chap. I , § 6 et démonstration de la proposition III 1) .

Si n est nul alors , l'indice considéré est premier à ℓ (supposons $n \geqslant 1$) . Ecrivons $(\mathbb{F}(L_n) : (\mathbb{E}^o(L_n) \oplus \overline{\mathbb{F}}_{\varphi_n}) \cap \mathbb{F}(L_n)) =$ $(\,\mathbb{F}(L_n) : (\mathbb{E}^o(L_n) \cap \mathbb{F}(L_n)) \oplus \overline{\mathbb{F}}_{\varphi_n})$ et posons $\overline{\mathcal{F}}_{\varphi_n} = \overline{\mathbb{F}}_{\varphi_n} \otimes \mathbb{Z}_\ell$.

De par la platitude de $\mathbb{Z}_\ell$, on vérifie que le ℓ -Sylow de $\mathbb{F}(L_n)/(\mathbb{E}^o(L_n) \cap \mathbb{F}(L_n)) \oplus \overline{\mathbb{F}}_{\varphi_n}$ s'identifie à $\mathcal{F}(L_n)/(\mathcal{E}^o(L_n) \cap \mathcal{F}(L_n)) \oplus \overline{\mathcal{F}}_{\varphi_n} =$

$$\prod_{\psi \in \mathfrak{X}_{L_o}} \mathcal{F}(L_n)^{e'_\psi} / (\,\mathcal{E}^o(L_n)^{e'_\psi} \cap \mathcal{F}(L_n)^{e'_\psi}) \oplus \overline{\mathcal{F}}_{\varphi_n}^{e'_\psi} .$$

On a déjà calculé $\mathcal{E}^o(L_n)^{e'_\psi}$ (cf. démonstration du lemme III 2) :

$\mathcal{E}^o(L_n)^{e'_\psi} = \mathcal{E}(K_{\psi_n})^{e_\psi}$ si $\psi \neq \varphi$, $\mathcal{E}^o(L_n)^{e'_\varphi} = \mathcal{E}(K_{\varphi_{n-1}})^{e_\varphi} = \mathcal{E}(K_{\varphi_{n-1}})^{\bar{e}_\chi}$

(cf. définition de $\bar{e}_\chi$, chap. I , § 7) .

Calculons $\overline{\mathcal{F}}_{\varphi_n}^{e'_\psi}$: On a $\overline{\mathcal{F}}_{\varphi_n} \subset \mathcal{E}_{\varphi_n}$; or $\mathcal{E}_{\varphi_n} = \mathcal{E}^*(L_n)^{\bar{e}_\chi}$ d'où

$\mathcal{E}_{\varphi_n}^{e'_\psi} = (1)$ si $\psi \neq \varphi$ et $\overline{\mathcal{F}}_{\varphi_n}^{e'_\psi} = (1)$ pour $\psi \neq \varphi$.

Si $\psi = \varphi$, $\overline{\mathcal{F}}_{\varphi_n}^{\bar{e}_\chi} = \overline{\mathcal{F}}_{\varphi_n}$ (en effet , $\mathcal{E}_{\varphi_n}^{\bar{e}_\chi} = \mathcal{E}^*(L_n)^{\bar{e}_\chi} = \mathcal{E}_{\varphi_n}$) .

Pour $\psi \neq \varphi$, on a $\mathcal{F}(L_n)^{e'_\psi} / (\mathcal{E}^o(L_n)^{e'_\psi} \cap \mathcal{F}(L_n)^{e'_\psi}) \oplus \overline{\mathcal{F}}_{\varphi_n}^{e'_\psi} =$

$\mathcal{F}(L_n)^{e'_\psi} / (\mathcal{E}(K_{\psi_n})^{e_\psi} \cap \mathcal{F}(L_n)^{e'_\psi})$; mais $\mathcal{F}(L_n)^{e'_\psi} \subset \mathcal{E}(L_n)^{e'_\psi} = \mathcal{E}(K_{\psi_n})^{e_\psi}$ et

le quotient est trivial . Il reste donc le quotient :

$$\mathcal{F}(L_n)^{\bar{e}_\chi} / (\mathcal{E}^o(L_n)^{\bar{e}_\chi} \cap \mathcal{F}(L_n)^{\bar{e}_\chi}) \oplus \overline{\mathcal{F}}_{\varphi_n}^{\bar{e}_\chi} =$$

$$= \mathcal{F}(L_n)^{\bar{e}_\chi} / (\mathcal{E}(K_{\varphi_{n-1}})^{\bar{e}_\chi} \cap \mathcal{F}(L_n)^{\bar{e}_\chi}) \oplus \overline{\mathcal{F}}_{\varphi_n} .$$

On doit calculer $\mathcal{F}(L_n)^{\bar{e}_\chi} / (\mathcal{E}(K_{\varphi_{n-1}})^{\bar{e}_\chi} \cap \mathcal{F}(L_n)^{\bar{e}_\chi}) \oplus \overline{\mathcal{F}}_{\varphi_n}$.

$$\text{On a } D_\chi = \prod_{p \mid g_\chi} (1 - \sigma_\chi^{g_\chi/p}) = (1 - \sigma_\chi^{g_\chi/\ell}) D'_\chi , \quad D'_\chi \in \mathbb{Z}[G_\chi] .$$

<u>Lemme</u> III 7 . On a $D'_\chi \bar{e}_\phi$ inversible dans $\mathbb{Z}_\ell[G_\chi]\bar{e}_\phi$, pour tout caractère ℓ-adique $\phi|\chi$ (cf. notations définies dans le chap. I , § 7) .

On a $\mathbb{Z}_\ell[G_\chi]\bar{e}_\phi = \mathbb{Z}_\ell[G'_\chi]\bar{e}_\phi[H]$; où $H = G(L_n/L_o)$ et $G'_\chi = G(L_n/L'_n)$; on a $\mathbb{Z}_\ell[G'_\chi]\bar{e}_\phi \simeq \mathbb{Z}_\ell^{(g'_\chi)}$ où $g'_\chi = g_\chi/\ell^n$. On a donc $\mathbb{Z}_\ell[G_\chi]\bar{e}_\phi \simeq \mathbb{Z}_\ell^{(g'_\chi)}[H]$. Cette identification s'obtient de la façon suivante : à $\sigma_\chi \bar{e}_\phi$ on associe $\zeta \sigma_\chi^{g'_\chi} \in \mathbb{Z}_\ell^{(g'_\chi)}[H]$ (où ζ est une racine primitive g'_χ ème de l'unité) . Pour $p \mid g_\chi$, $p \neq \ell$, l'image de $(\sigma_\chi^{g_\chi/p} - 1)\bar{e}_\phi$ est égale à $(\zeta^{g_\chi/p} \sigma_\chi^{g'_\chi g_\chi/p} - 1) = \zeta_1 - 1$ où ζ_1 est d'ordre p . Donc $\zeta_1 - 1$ est bien inversible dans $\mathbb{Z}_\ell^{(g'_\chi)}$.

<u>Remarque</u> III 1 . On a la suite exacte de $\mathbb{Z}_\ell^{(g_\chi)}$-modules :

$$1 \longrightarrow \overline{\mathcal{F}}_\phi \longrightarrow \mathcal{F}(K_\chi)^{\bar{e}_\phi} / \mathcal{E}^o(K_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K_\chi)^{\bar{e}_\phi} \longrightarrow \mathcal{F}(K_\chi)^{\bar{e}_\phi} / (\mathcal{E}^o(K_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K_\chi)^{\bar{e}_\phi}) \oplus \overline{\mathcal{F}}_\phi \longrightarrow 1,$$

où $\overline{\mathcal{F}}_\phi = \overline{\mathcal{F}}_\chi^{\bar{e}_\phi}$ est la composante en ϕ de $\overline{\mathcal{F}}_\chi$ (cf. Th. I 2) .

Ici $\mathcal{F}(K_\chi)^{\bar{e}_\phi} / \mathcal{E}^{\circ}(K_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K_\chi)^{\bar{e}_\phi}$ est un $\mathbb{Z}_\ell^{(g'_\chi)}[H]$-module

(cf. démonstration du lemme III 7) annulé par $\nu = 1+\sigma+\ldots+\sigma^{\ell-1}$

$(\sigma = \sigma_\chi^{g_\chi/\ell})$; on a donc un module sur $\mathbb{Z}_\ell^{(g'_\chi)}[H] / (\nu) \simeq \mathbb{Z}_\ell^{(g_\chi)}$.

Il est clair que $\bar{\mathcal{F}}_\phi$ est un sous-$\mathbb{Z}_\ell^{(g_\chi)}$-module de $\mathcal{F}(K_\chi)^{\bar{e}_\phi}/\mathcal{E}^{\circ}(K_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K_\chi)^{\bar{e}_\phi}$.

<u>Lemme</u> III 8 . Si g_χ n'est pas une puissance de ℓ alors

$\mathcal{F}(K_\chi)^{\bar{e}_\phi} / \mathcal{E}(K'_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K_\chi)^{\bar{e}_\phi} \simeq \langle |\theta_\chi|^{\bar{e}_\phi} \rangle / \mathcal{E}(K'_\chi)^{\bar{e}_\phi} \cap \langle |\theta_\chi|^{\bar{e}_\phi} \rangle$,

où K'_χ est le sous-corps de K_χ défini par $[K_\chi : K'_\chi] = \ell$ ($\langle\alpha\rangle$ désignant le $\mathbb{Z}_\ell[G_\chi]$-module engendré par α).

Considérons l'homomorphisme :

$$\langle |\theta_\chi| \rangle^{\bar{e}_\phi} \xrightarrow{D'_\chi} \langle |\theta_\chi|^{D'_\chi} \rangle^{\bar{e}_\phi} \; ;$$

on a $|\theta_\chi|^{D'_\chi} \in \mathbb{E}(K_\chi)$, car D'_χ contient au moins un facteur $\sigma_\chi^{g_\chi/p} - 1$, $p \neq \ell$, donc $|\theta_\chi|^{D'_\chi} \in \mathcal{F}(K_\chi)$. On obtient donc un homomorphisme injectif de $\langle|\theta_\chi|^{\bar{e}_\phi}\rangle / \mathcal{E}(K'_\chi)^{\bar{e}_\phi} \cap \langle|\theta_\chi|^{\bar{e}_\phi}\rangle$ dans $\mathcal{F}(K_\chi)^{\bar{e}_\phi}/\mathcal{E}(K'_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K\ )^{\bar{e}_\phi}$, car $D'_\chi\, \bar{e}_\phi$ est inversible dans $\mathbb{Z}_\ell[G_\chi]\bar{e}_\phi$. Vérifions la surjectivité :

Soit $|\varepsilon| \in \mathbb{F}(K_\chi)$, $|\varepsilon| \in \Theta(K_\chi) \cap \mathbb{E}(K_\chi)$; on peut donc écrire

$|\varepsilon|^{\bar{e}_\phi} = |\theta_\chi|^{\omega_\chi \bar{e}_\phi} \prod_{\substack{\psi \in \mathcal{X}_{K_\chi} \\ \psi \neq \chi}} |\theta_\psi|^{\omega_\psi \bar{e}_\phi}$, par définition de $\Theta(K_\chi)$, $\omega_\chi, \omega_\psi \in \mathbb{Z}[G_\chi]$;

$|\varepsilon|^{\bar{e}_\phi D'_\chi} = |\theta_\chi|^{\omega_\chi \bar{e}_\phi D'_\chi} \prod_{\psi \neq \chi} |\theta_\psi|^{\omega_\psi \bar{e}_\phi D'_\chi}$; les $\theta_\psi^{\omega_\psi D'_\chi}$ sont des unités appartenant aux corps K_ψ pour $\psi \neq \chi$, donc appartenant à $\mathcal{E}^{\circ}(K_\chi)$ et la classe de $|\varepsilon|^{\bar{e}_\phi D'_\chi}$ modulo $\mathcal{E}^{\circ}(K_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K_\chi)^{\bar{e}_\phi}$ est égale à celle de $|\theta_\chi|^{\omega_\chi \bar{e}_\phi D'_\chi}$, d'où le résultat puisque $\bar{e}_\phi\, D'_\chi$ est inversible .

D'après la Rem. III 1 , $\langle|\theta_\chi|^{\bar{e}_\phi}\rangle / \mathcal{E}(K'_\chi)^{\bar{e}_\phi} \cap \langle|\theta_\chi|\rangle^{\bar{e}_\phi}$ est un module de type fini sur $A = \mathbb{Z}_\ell^{(g_\chi)}$; un tel module est isomorphe à un produit de la forme : $A^{r_\chi} \prod_i A / \hat{\mathfrak{P}}_\chi^{n_i}$, $r \geqslant 0$, $n_i \geqslant 1$, $\hat{\mathfrak{P}}_\chi$ étant l'idéal maximal de $\mathbb{Z}_\ell^{(g_\chi)}$. Comme le module considéré est monogène , il en résulte que ou bien il est isomorphe à A ou bien il est isomorphe à $A / \hat{\mathfrak{P}}_\chi^{\,m}$, $m \geqslant 0$. Montrons que ce module est sans torsion et non trivial : il suffit de vérifier qu'il n'est annulé par aucune puissance de ℓ : si $|\theta_\chi|^{\bar{e}_\phi a} \in \mathcal{E}(K'_\chi)^{\bar{e}_\phi}$, $a = \ell^k$, alors en particulier l'unité de Leopoldt $\theta_\chi^{D_\chi}$ vérifie $|\theta_\chi|^{D_\chi a \bar{e}_\phi} = 1$ soit $|\theta_\chi|^{D_\chi \bar{e}_\phi} = 1$, or $|\theta_\chi|^{D_\chi}$ engendre un sous-module d'indice fini dans $\mathbb{E}_\chi$ par conséquent ceci est absurde .

Dans un tel isomorphisme , $\overline{\mathcal{F}}_\chi^{\,\bar{e}_\phi} = \langle |\theta_\chi|^{\sigma-1} \rangle^{\bar{e}_\phi}$ a pour image l'idéal $(w_1 - 1) A$ (w_1 , racine de l'unité d'ordre ℓ) puisque $\sigma = \sigma_\chi^{g_\chi/\ell}$.

Il résulte de la suite exacte de la Remarque III 1 que

$\langle |\theta_\chi|^{\bar{e}_\phi} \rangle / \mathcal{E}^{\circ}(K_\chi)^{\bar{e}_\phi} \cap \langle |\theta_\chi| \rangle^{\bar{e}_\phi} \oplus \langle |\theta_\chi|^{\sigma-1} \rangle^{\bar{e}_\phi}$ est isomorphe à $A/(w_1 - 1)A$.

L'ordre de ce quotient est égal à $\ell^{\mu \ell^{n-1}}$, où μ est le degré résiduel de ℓ dans $\mathbb{Q}_\ell^{(g'_\chi)} / \mathbb{Q}_\ell$.

Corollaire III 2 . Soit ℓ un nombre premier quelconque : si g_χ n'est pas égal à une puissance de ℓ , alors

$(\mathbb{F}(K_\chi) : \mathbb{E}'(K_\chi) \cap \mathbb{F}(K_\chi) \oplus \overline{\mathbb{F}}_\chi)_\ell = (q_\chi)_\ell$.

En effet , il suffit d'écrire que $\mathcal{F}(K_\chi) / \mathcal{E}^{\circ}(K_\chi) \cap \mathcal{F}(K_\chi) \oplus \overline{\mathcal{F}}_\chi \simeq \bigoplus_{\phi | \chi} \mathcal{F}(K_\chi)^{\bar{e}_\phi} / \mathcal{E}^{\circ}(K_\chi)^{\bar{e}_\phi} \cap \mathcal{F}(K_\chi)^{\bar{e}_\phi} \oplus \overline{\mathcal{F}}_\phi$ (th. I 2) et de constater que $\sum_{\phi | \chi} \mu = \varphi(g'_\chi)$.

Passons maintenant au cas $g_\chi = \ell^n$.

a) <u>Cas $\ell \neq 2$</u>. On a à considérer (ici $\bar{e}_\chi = \bar{e}_\phi = 1$) :

$\mathcal{F}(K_\chi) / \mathcal{E}(K'_\chi) \cap \mathcal{F}(K_\chi)$ et $\bar{\mathcal{F}}_\chi$.

(α) f_χ <u>strictement composé</u>. Alors θ_χ^2 est une unité de K_χ ; par conséquent on aura $\Theta^2(K_\chi) = \langle |\theta_\chi|^2, \dots, |\theta_\psi|^2, \dots \rangle$ et $\Theta^2(K_\chi) \cap \mathbb{E}(K_\chi) = \langle |\theta_\chi|^2, \dots, |u_\psi|, \dots \rangle$, les u_ψ étant pour $\psi \neq \chi$ des unités de K_ψ puisque $\theta_\psi^2 \in K_\psi$ (θ_ψ^2 n'est pas nécessairement une unité de K_ψ) et que θ_χ^2 est une unité de K_χ ; par conséquent notre quotient s'identifie encore à $\langle |\theta_\chi| \rangle / \mathcal{E}(K'_\chi) \cap \langle |\theta_\chi| \rangle \simeq A$; l'ordre du quotient cherché est égal à

$$\ell^{\frac{\varphi(g_\chi)}{\ell - 1}} = \ell^{(q_\chi)_\ell}$$ par définition de $(q_\chi)_\ell$ dans ce cas.

(β) $f_\chi = p^a$, p <u>premier</u>. Dans ce cas, θ_χ n'est pas une unité ni les θ_ψ pour tout $\psi \neq 1$. Alors, ou bien $p = \ell$, et dans ce cas K_χ est la sous-extension de degré ℓ^n de la Γ-extension cyclotomique de $\mathbb{Q}$ pour ℓ, ou bien $p \neq \ell$ et alors $a = 1$. On sait ([15], § 8, 1) que θ_χ^2 est une uniformisante dans K_χ et θ_ψ^2 une uniformisante dans K_ψ (au-dessus de p) pour tout $\psi \neq 1$. Montrons que $\mathbb{F}(K_\chi)$, modulo les unités de K'_χ, est engendré par $|\theta_\chi|^{(\sigma_\chi - 1)}$.

D'après Leopoldt ([15], chap. III, § 8, 2), on a pour tout $\psi \in \mathfrak{X}_{K_\chi}$, $\psi \neq 1$, $\nu_{K_\chi/K_\psi} \theta_\chi^2 = \theta_\psi^2$ (en remarquant que f_χ et f_ψ sont par hypothèse une puissance non triviale du nombre premier p). On en déduit $\nu_{K_\chi/K_\psi} |\theta_\chi| = |\theta_\psi|$.

Soit donc $|\varepsilon| \in \mathbb{F}(K_\chi)$; on aura $|\varepsilon| = \prod_\psi |\theta_\psi|^{\omega_\psi}$, $\omega_\psi \in \mathbb{Z}[G_\chi]$, d'où $|\varepsilon| = |\theta_\chi|^{\omega_\chi} \prod_{\psi \neq \chi} |\theta_\chi|^{\nu_{K_\chi/K_\psi} \omega_\psi} = |\theta_\chi|^{\Omega}$, $\Omega \in \mathbb{Z}[G_\chi]$.

Comme θ_χ n'est pas une unité, il est facile de voir que Ω doit être dans l'idéal d'augmentation de $\mathbb{Z}[G_\chi]$, donc $\Omega = (\sigma_\chi - 1)\Omega'$ et $|\varepsilon| = |\theta_\chi|^{(\sigma_\chi - 1)\Omega'}$, d'où le résultat.

Remarquons que dans ce dernier cas, l'hypothèse $\ell \neq 2$ n'est pas nécessaire, ce qui résoud une partie du cas $\ell = 2$.

On peut donc engendrer $\mathbb{F}(K_\chi)$ par $|\eta_\chi| = |\theta_\chi|^{\sigma_\chi - 1} \in \mathbb{F}(K_\chi)$; le quotient à calculer sera donc égal à

$$\langle |\theta_\chi|^{\sigma_\chi - 1} \rangle / \mathcal{E}(K'_\chi) \cap \langle |\theta_\chi|^{\sigma_\chi - 1} \rangle \oplus \langle |\theta_\chi|^{\sigma - 1} \rangle .$$

On vérifie que $\langle |\theta_\chi|^{\sigma_\chi - 1} \rangle / \mathcal{E}(K'_\chi) \cap \langle |\theta_\chi|^{\sigma_\chi - 1} \rangle$ est isomorphe à A .
On procède alors de la même manière que précédemment en utilisant la suite exacte de la Remarque III 1 et on obtient un indice égal à $\ell^{\frac{\varphi(g_\chi)}{\ell - 1} - 1} = (q_\chi)_\ell$ puisque $g_\chi = \ell^n$.

b) <u>Cas $\ell = 2$</u> . On va encore distinguer deux cas :

(α) $f_\chi = p^a$, p <u>premier</u> . Cas résolu (cf. fin du § β précédent); on a un indice égal à $(q_\chi)_2$.

(β) <u>Cas</u> f_χ <u>strictement composé</u> . On rappelle que $g_\chi = 2^n$, $n \geqslant 1$.

Dans ce cas , les θ_χ sont des unités mais pas nécessairement dans K_χ (les θ_ψ , pour $\psi \neq \chi$, pouvant par contre ne pas être des unités).

On distingue deux cas :

(i) <u>$\theta_\chi \in K_\chi$</u> . Considérons $\alpha = \prod_{\psi \neq \chi} \theta_\psi^{\omega_\psi}$, $\omega_\psi \in \mathbb{Z}[G_\chi]$,

et supposons $|\alpha| \in \mathbb{F}(K_\chi)$. Si $|\alpha| \notin \mathbb{F}(K'_\chi)$, il en résulte qu'il existe x défini mod 4 , tel que $K_\chi = K'_\chi(i^x \alpha)$ est de degré 2 sur K'_χ ; or $(i^x\alpha)^2 \in K'_\chi$; donc K_χ / K'_χ serait une extension de Kummer ramifiée en 2 uniquement , ce qui est absurde , donc $|\alpha| \in \mathbb{F}(K'_\chi)$ et $\mathcal{F}(K_\chi)/\mathcal{E}(K'_\chi) \cap \mathcal{F}(K_\chi)$ est bien engendré par l'image de $|\theta_\chi|$.

(ii) <u>$\theta_\chi \notin K_\chi$</u> . Soit $|u| = \prod_\psi |\theta_\psi|^{\omega_\psi} \in \mathbb{F}(K_\chi)$; si $\prod_{\psi \neq \chi} |\theta_\psi|^{\omega_\psi} \in \mathbb{F}(K_\chi)$, le même raisonnement que ci-dessus (β) , (i)) s'applique et $\prod_{\psi \neq \chi} |\theta_\psi|^{\omega_\psi} \in \mathbb{F}(K'_\chi)$ et $|\theta_\chi|^{\omega_\chi} \in \mathbb{F}(K_\chi)$. On peut alors écrire $\omega_\chi = (\sigma_\chi - 1)\omega' + a$, $a \in \mathbb{Z}$, $\omega' \in \mathbb{Z}[G_\chi]$ et $|\theta_\chi|^{\omega_\chi} = |\eta_\chi|^{\omega'} |\theta_\chi|^a$ ($\eta_\chi = \theta_\chi^{\sigma_\chi - 1}$) ; ce qui entraîne $a \equiv 0 \bmod 2$. On peut écrire $2 = (\xi - 1)^{2^{n-1}} \mathcal{E}(\xi)$, avec

ξ racine de l'unité d'ordre 2^n , $\varepsilon(\xi)$ unité . On aura donc

$2 = (\sigma_\chi - 1)^{2^{n-1}} \varepsilon(\sigma_\chi) + (\sigma + 1)\omega''$, $\sigma = \sigma_\chi^{g_\chi/2}$; $|\theta_\chi|^2 = |\eta_\chi|^{\Omega} |\theta'|$ avec $\Omega \in \mathbb{Z}[G_\chi]$, $\theta' \in K'_\chi$; dans ce cas , l'image de $|u|$ dans $\mathcal{E}(K_\chi) / \mathcal{E}(K'_\chi) \cap \mathcal{F}(K_\chi)$ s'exprime à partir de celle de $|\eta_\chi|$.

Si maintenant $|\theta| = \prod_{\psi \neq \chi} |\theta_\psi|^{\omega_\psi} \notin \mathbb{F}(K_\chi)$, on a $|u| = |\theta_\chi|^{\omega_\chi} |\theta| \in \mathbb{F}(K_\chi)$ et $|\theta| \notin \mathbb{F}(K_\chi)$. On peut écrire $\omega_\chi = (\sigma_\chi - 1)\omega' + a$ et cette fois a est impair et on peut écrire $|u| = |\eta_\chi|^{\Omega} |\theta_\chi| |\theta'|$, $|\theta'|$ étant dans $\langle \ldots, |\theta_\psi|, \ldots \rangle$, $\psi \neq \chi$ (compte tenu du fait que d'après [10] , $|\theta_\chi|^{1+\sigma}$ est dans ce sous-groupe) . Ce dernier cas montre que l'image de $|\eta_\chi|$ ne suffit pas nécessairement à engendrer $\mathcal{F}(K_\chi) / \mathcal{E}(K'_\chi) \cap \mathcal{F}(K_\chi)$. Appelons $\mathcal{F}_o(K_\chi)$ le sous-module engendré par $|\eta_\chi|$; alors $\mathcal{F}_o(K_\chi) / \mathcal{E}(K'_\chi) \cap \mathcal{F}_o(K_\chi)$ s'identifie à un sous-module de $\mathcal{F}(K_\chi) / \mathcal{E}(K'_\chi) \cap \mathcal{F}(K_\chi)$ d'indice 2 au plus .

En résumé , on obtient les valeurs suivantes pour l'indice $\mathcal{F}(K_\chi) / \mathcal{E}(K'_\chi) \cap \mathcal{F}(K_\chi)$ (dans le cas f_χ strictement composé) :

$2(q_\chi)_2$ si $\theta_\chi \in K_\chi$,

$(q_\chi)_2$ ou $2(q_\chi)_2$ si $\theta_\chi \notin K_\chi$.

<u>Théorème</u> III 2 . On a pour tout $\chi \in \mathcal{X}^+$:

$|\mathbb{H}'_\chi| = \ell_\chi(\mathbb{E}(K_\chi) : \mathbb{E}^o(K_\chi)\,\mathbb{F}(K_\chi))$, où ℓ_χ prend les valeurs suivantes :

(i) Si g_χ n'est pas puissance d'un nombre premier alors $\ell_\chi = 1$;

(ii) Si $g_\chi = \ell^n$, ℓ premier , $\ell \neq 2$, $n \geqslant 1$, alors :

$(ii)_1$ si $f_\chi = p^k$, p premier , $k \geqslant 1$, alors $\ell_\chi = 1$;

$(ii)_2$ si f_χ est strictement composé , alors $\ell_\chi = \ell$;

(iii) Si $g_\chi = 2^n$ alors :

$(iii)_1$ si $f_\chi = p^k$, p premier , $k \geqslant 1$, alors $\ell_\chi = 1$;

$(iii)_2$ si f_χ est strictement composé alors $\ell_\chi = 1$ ou 2 .

4) Invariants analytiques dans le cas réel . Définitions , propriétés .

Il est naturel de définir dans le cas général des invariants analytiques complétant comme dans le cas relatif la définition donnée dans [8] dans le cas semi-simple :

Soit ℓ premier fixé . On considère le quotient : $\widetilde{\mathcal{E}}_\chi = \mathcal{E}(K_\chi) / \mathcal{E}^{o}(K_\chi)\ \mathcal{F}(K_\chi)$, pour $\chi \in \mathcal{X}^+$; c'est un $\mathbb{Z}_\ell[G_\chi]$-module annulé par $P_\chi(\sigma_\chi)$ (car annulé par les $\nu_{K_\chi/k}$, $k \subsetneq K_\chi$) .

D'après des résultats précédents (Rem. I 6 et Déf. I 3) on a $\widetilde{\mathcal{E}}_\chi = \bigoplus_{\phi|\chi} \widetilde{\mathcal{E}}_\phi$, avec $\widetilde{\mathcal{E}}_\phi = \{ q(|\varepsilon|) \in \widetilde{\mathcal{E}}_\chi \ , \ P_\phi(\sigma_\chi)\, q(|\varepsilon|) = 1 \}$.
On peut aussi écrire $\widetilde{\mathcal{E}}_\phi = \widetilde{\mathcal{E}}_\chi^{\,\bar{e}_\phi}$. Les $\widetilde{\mathcal{E}}_\phi$ sont alors des $\mathbb{Z}_\ell^{(g_\chi)}$-modules (chap. I , 4 , f) .

On peut prouver facilement que $\widetilde{\mathcal{E}}_\chi$ est monogène (cf. Lemme IV 1 , comme justification) ; ce qui fait que $\widetilde{\mathcal{E}}_\phi$ est isomorphe à un module de la forme $\mathbb{Z}_\ell^{(g_\chi)} / \hat{\gamma}_\chi^{\,m'_\phi(h')}$, $m'_\phi(h') \geqslant 0$. Comme les seuls cas $\ell_\chi = \ell \neq 1$ ne peuvent se produire que lorsque g_χ est une puissance de ℓ , ℓ est totalement ramifié dans $\mathbb{Q}^{(g_\chi)}$ et dans ce cas $\phi = \chi$; on est alors conduit à poser :

$$(\mathcal{E}(K_\chi) : \mathcal{E}^{o}(K_\chi)\ \mathcal{F}(K_\chi))\, \mathbb{Z}_\ell^{(g_\chi)} = \hat{\gamma}_\chi^{\,m_\phi(h')} .$$

Dans le cas $\ell_\chi = 1$, on pose $m_\phi(h') = m'_\phi(h')$.

En résumé :

Définition III4 . On pose $\widetilde{\mathcal{E}}_\phi \simeq \mathbb{Z}_\ell^{(g_\chi)} / \hat{\gamma}_\chi^{\,m_\phi(h')}$ (resp. $\mathbb{Z}_\ell^{(g_\chi)} / \hat{\gamma}_\chi^{\,m_\phi(h')-1}$) si $\ell_\chi = 1$ (resp. $\ell_\chi = \ell$) , pour tout $\phi \in \Phi^+$.

Remarque III 2 . Nous avons donc donné une définition générale des invariants $m_\phi(\mathcal{H})$ et $m_\phi(\mathcal{H}')$ (cf. Déf. II 7)et des invariants $m_\phi(h')$ (cf. Déf. II 8 et III 4) , pour tout ℓ premier et tout caractère ℓ -adique ϕ ; ils sont tels que $\sum_{\phi|\chi} m_\phi(\mathcal{H}') = \sum_{\phi|\chi} m_\phi(h')$, pour tout $\chi \in \mathcal{X}$. On peut alors étendre au cas général les conjectures précisées seulement pour le cas " semi-simple" dans [8] (chap. V) . Nous conjecturons que $m_\phi(\mathcal{H}') = m_\phi(h')$, pour tout ℓ et tout caractère ℓ-adique $\phi \in \Phi$.

Remarque III 3 . Nous ne savons pas comment définir des invariants analytiques $m_\phi(h)$ (ϕ pair) qui correspondraient aux invariants $m_\phi(\mathcal{H})$. On peut imaginer , par exemple , de définir les invariants $m_\phi(h)$ à partir d'un quotient de la forme $\mathcal{E}(K_\chi)/\mathcal{E}_1(K_\chi)\,\mathcal{F}(K_\chi)$, où $\mathcal{E}_1(K_\chi)$ serait le sous-groupe de $\mathcal{E}^o(K_\chi)$ engendré par les $N_{K_\chi/K}\,\mathcal{E}(K_\chi)$, pour tout $K \subsetneqq K_\chi$. Mais auparavant , une étude arithmétique des classes devenant principales dans une extension est nécessaire .

Note . Après la rédaction de cet article, nous avons reçu de R. Greenberg un preprint où il est démontré que , dans le cas semi-simple , les conjectures énoncées par Coates et Lichtembaum dans [3] entraînent la nôtre.

Chap. IV

Lien avec les résultats d'Iwasawa dans le cas des Γ-extensions cyclotomiques

1) Introduction . Nous allons montrer que le point de vue adopté dans cette étude permet d'aborder le calcul des invariants bien connus λ , μ et ν relatifs aux Γ-extensions d'un corps de nombres . Nous nous limitons bien entendu aux seules Γ-extensions contenues dans $\mathbb{Q}^a$, à savoir les Γ-extensions cyclotomiques .

On choisit un nombre premier ℓ et on désigne par $\mathbb{Q}_i$ la sous-extension de la Γ-extension cyclotomique de $\mathbb{Q}$ définie par $[\mathbb{Q}_i : \mathbb{Q}] = \ell^i$, $i \geqslant 0$; pour tout corps $K \subset \mathbb{Q}^a$, on pose $K_i = K\mathbb{Q}_i$ et on pose $K_\infty = \bigcup_{i \geqslant 0} K_i$.
On rappelle que pour n assez grand , le nombre de ℓ-classes d'idéaux de K_n est de la forme ([12], [13]) : $|\mathcal{H}(K_n)| = \ell^{\lambda n + \mu \ell^n + \nu}$, $\lambda, \mu, \nu \in \mathbb{Z}$, $\lambda, \mu \geqslant 0$ indépendants de n .

Il est conjecturé que dans le cas des Γ-extensions cyclotomiques , le coefficient μ est nul (cf. [14]) . Nous verrons comment on peut interpreter cette condition ; nous donnerons en même temps une méthode de calcul des invariants qui nous semble généraliser et simplifier les méthodes exposées jusqu'ici (par exemple , Gold ([5] et [6]) pour les corps quadratiques imaginaires) . Enfin l'étude du rang n_o à partir duquel la formule d'Iwasawa est valable sera précisé .

Remarque IV 1 . En vertu d'un résultat d'Iwasawa ([14] , th. 2 et 3) , on peut , pour l'étude de μ , se limiter à étudier la Γ-extension cyclotomique d'une extension cyclique de $\mathbb{Q}$ de degré premier à ℓ . C'est le cadre dans lequel nous allons nous placer dans la suite .

2) Cas de la Γ-extension cyclotomique d'un corps réel . Nous commençons par appliquer les résultats des chapitres précédents au cas d'une extension L cyclique réelle sur $\mathbb{Q}$ dont le degré est de la forme $g = g'\ell^n$, $n \geqslant 2$, g' premier à ℓ :

On considère les sous-corps K et k de L tels que $[L:K] = [K:k] = \ell$. On suppose que $L = K_\chi$. On considère $\tilde{\mathcal{E}}_\chi = \mathcal{E}(L)^{\bar{e}_\chi} / \mathcal{E}^o(L)^{\bar{e}_\chi} \mathcal{F}(L)^{\bar{e}_\chi}$ et on rappelle (chap. III , § 1) que $\mathcal{E}^o(L)^{\bar{e}_\chi} = \mathcal{E}(K)^{\bar{e}_\chi}$. On sait que $\mathcal{E}(L)^{\bar{e}_\chi} / \mathcal{E}(K)^{\bar{e}_\chi} \mathcal{F}(L)^{\bar{e}_\chi}$ peut alors se décomposer en une somme directe sur les caractères ℓ-adiques $\phi|\chi$ dont les termes s'identifient de façon évidente à (Th. I 2 et Rem. I 4) :

$$\tilde{\mathcal{E}}_\phi = \mathcal{E}(L)^{\bar{e}_\phi} / \mathcal{E}(K)^{\bar{e}_\phi} \mathcal{F}(L)^{\bar{e}_\phi}$$

et qui sont des $\mathbb{Z}_\ell^{(g_\chi)}$-modules (cf. Remarque III 1) .

On a l'isomorphisme :

$$\mathcal{E}(L)^{\bar{e}_\phi} / \mathcal{E}(K)^{\bar{e}_\phi} \mathcal{F}(L)^{\bar{e}_\phi} \simeq (\mathcal{E}(L)^{\bar{e}_\phi} / \mathcal{E}(K)^{\bar{e}_\phi}) / (\mathcal{F}(L)^{\bar{e}_\phi} / \mathcal{F}(L)^{\bar{e}_\phi} \cap \mathcal{E}(K)^{\bar{e}_\phi}) .$$

Lemme IV 1 . $\mathcal{E}(L)^{\bar{e}_\phi} / \mathcal{E}(K)^{\bar{e}_\phi}$ est un $\mathbb{Z}_\ell^{(g_\chi)}$-module sans torsion de rang 1 .

C'est un $\mathbb{Z}_\ell^{(g_\chi)}$-module de façon évidente (réalisé au moyen de l'homomorphisme défini par $\sigma_\chi \to \chi'(\sigma_\chi)$, $\chi'|\phi$) . Vérifions qu'il est sans torsion (son rang sera alors évident) . Il suffit de montrer que $\mathbb{E}(L) / \mathbb{E}(K)$ est sans $\mathbb{Z}$-torsion ; en effet , si cela est montré , $\mathcal{E}(L)/\mathcal{E}(K)$ sera sans $\mathbb{Z}_\ell$-torsion (car alors il existe $\mathbb{E}_1$ sans $\mathbb{Z}$-torsion tel que $\mathbb{E}(L) = \mathbb{E}(K) \oplus \mathbb{E}_1$ et $\mathbb{E}(L) / \mathbb{E}(K) \simeq \mathbb{E}_1$, d'où $\mathcal{E}(L) = \mathcal{E}(K) \oplus \mathcal{E}_1$, $\mathcal{E}_1$ sans $\mathbb{Z}_\ell$-torsion) . Les sous-modules $\mathcal{E}(L)^{\bar{e}_\phi} / \mathcal{E}(K)^{\bar{e}_\phi}$ seront sans $\mathbb{Z}_\ell$-torsion donc sans $\mathbb{Z}_\ell^{(g_\chi)}$-torsion : Si on a $|\varepsilon| \in \mathbb{E}(L)$, $|\varepsilon| \notin \mathbb{E}(K)$ avec $|\varepsilon|^a \in \mathbb{E}(K)$, alors on a la même situation avec ε : $\varepsilon \notin E(K)$ et $\varepsilon^a \in E(K)$; d'après la théorie de Kummer , comme L est réelle , on a nécessairement $\varepsilon^2 \in E(K)$, ce qui ne peut se produire que pour $\ell = 2$, auquel cas L/K n'est ramifiée qu'en 2 . On a alors le schéma suivant :

$$\begin{tikzcd} L' \arrow[r, dash] \arrow[d, dash, "2"'] & L \arrow[d, dash] \\ K' \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash, "2^n"] \\ \mathbb{Q} \arrow[r, dash] & L_o \end{tikzcd}$$

où $[L:L']$ est impair et L'/K' est sous-extension de $\mathbb{Q}_\infty$(pour $\ell = 2$) .

On sait alors que $L' = K'(\sqrt{\pi})$ où π est une uniformisante convenable de K' . Si on avait $\sqrt{\pi} = \varepsilon\alpha$, $\alpha \in K$, dans L/K , on aurait $(\sqrt{\pi})A_L = \alpha A_L$, ce qui n'est pas possible compte tenu des valuations (2 étant totalement ramifié dans L/L_o et non ramifié dans $L_o/\mathbb{Q}$. D'où le lemme .

D'après l'étude du chap. III , § 3 , $\mathcal{F}(L)/\mathcal{F}(L) \cap \mathcal{E}(K)$ est connu et c'est aussi l'image de $\mathcal{F}(L)$ dans $\mathcal{E}(L) / \mathcal{E}(K)$. Désignons par $|\bar{\varepsilon}|$ les éléments de $\mathcal{E}(L) / \mathcal{E}(K)$ et soit $|\bar{\varepsilon}_L|$ une $\mathbb{Z}_\ell^{(g_\chi)}$-base de $\mathcal{E}(L)^{\bar{e}_\phi} / \mathcal{E}(K)^{\bar{e}_\phi}$. On peut alors écrire (en termes de $\mathbb{Z}_\ell^{(g_\chi)}$-modules)

$$\mathcal{F}(L)^{\bar{e}_\phi} / \mathcal{F}(L)^{\bar{e}_\phi} \cap \mathcal{E}(K)^{\bar{e}_\phi} = \langle |\bar{\varepsilon}_L|^{(w_n - 1)^A} \rangle$$

, $A \geqslant 0$, où w_n est une racine primitive ℓ^n ème de l'unité (image de $\sigma'_\chi = \sigma_\chi^{g'_\chi}$) .

De la même manière , on peut écrire $\mathcal{F}(K)^{\bar{e}_\phi} / \mathcal{F}(K)^{\bar{e}_\phi} \cap \mathcal{E}(k)^{\bar{e}_\phi} = \langle |\bar{\bar{\varepsilon}}_K|^{(w_{n-1} - 1)^a} \rangle$, $a \geqslant 0$, où $|\bar{\bar{\varepsilon}}_K|$ désigne dans $\mathcal{E}(K)^{\bar{e}_\phi} / \mathcal{E}(k)^{\bar{e}_\phi}$ une $\mathbb{Z}_\ell^{(g_\chi/\ell)}$-base (w_{n-1} est alors l'image de $\bar{\sigma}'_\chi \in G(K/\mathbb{Q})$, $\bar{\sigma}'_\chi$ image canonique de σ'_χ) .

Supposons qu'on soit dans le cas où $\mathcal{F}(L)^{\bar{e}_\phi}$ modulo $\mathcal{E}(K)^{\bar{e}_\phi}$ est engendré par $|\eta_L|$ et $\mathcal{F}(K)^{\bar{e}_\phi}$ modulo $\mathcal{E}(K)^{\bar{e}_\phi}$ par $|\eta_K|$ telles que $|\eta_K| = N_{L/K}|\eta_L|$. On aura donc (Lemme IV 1) : $|\bar{\eta}_L| = |\bar{\varepsilon}_L|^{(w_n - 1)^A u}$, u unité de $\mathbb{Z}_\ell^{(g_\chi)}$, et $|\bar{\bar{\eta}}_K| = |\bar{\bar{\varepsilon}}_K|^{(w_{n-1} - 1)^a v}$, v unité dans $\mathbb{Z}_\ell^{(g_\chi/\ell)}$.

On peut écrire $|\eta_L| = |\varepsilon_L|^{(\sigma'_\chi - 1)^A u(\sigma_\chi)} |\varepsilon_1|$, $|\varepsilon_1| \in \mathcal{E}(K)^{\bar{e}_\phi}$;

$|\eta_K| = |\varepsilon_K|^{(\bar{\sigma}_\chi'-1)^a\, v(\bar{\sigma}_\chi)}\, |\varepsilon_2|$, $|\varepsilon_2| \in \mathcal{E}(k)^{\bar{e}_\phi}$. Considérons $N_{L/K}|\eta_L| = (N_{L/K}|\varepsilon_L|)^{(\sigma_\chi'-1)^A\, u(\sigma_\chi)}\, |\varepsilon_1^\ell| = |\eta_K|$ et considérons l'image dans $\mathcal{E}(K)^{\bar{e}_\phi} / \mathcal{E}(k)^{\bar{e}_\phi}$: on a $|\bar{\bar{\varepsilon}}_K|^{(\bar{\sigma}_\chi'-1)^a\, v(\bar{\sigma}_\chi)} = \overline{\overline{(N_{L/K}|\varepsilon_L|)}}^{(\sigma_\chi'-1)^A\, u(\sigma_\chi)}\, \overline{\overline{|\varepsilon_1|}}^{\ell}$.

On peut poser $\overline{\overline{N_{L/K}|\varepsilon_L|}} = |\bar{\bar{\varepsilon}}_K|^{(w_{n-1}-1)^x\, w}$, $x \geqslant 0$, w unité , d'où

$|\bar{\bar{\varepsilon}}_K|^{(w_{n-1}-1)^a\, v} = |\bar{\bar{\varepsilon}}_K|^{(w_{n-1}-1)^{x+A}\, uw}\, |\bar{\bar{\varepsilon}}_1|^{\ell}$. On en déduit la congruence

$(w_{n-1} - 1)^a\, v \equiv (w_{n-1}-1)^{x+A}\, uw \mod \ell$. D'où :

Proposition IV 1 . Soit $\chi \in \mathcal{X}^+$ tel que $g_\chi \equiv 0 \mod \ell^n$, $n \geqslant 2$. Soient K'_χ et k définis par $[K_\chi : K'_\chi] = [K'_\chi : k] = \ell$. On suppose que $N_{K_\chi/K'_\chi}\mathcal{F}(K_\chi) = \mathcal{F}(K'_\chi)$. Dans l'isomorphisme $\mathcal{E}(K_\chi)^{\bar{e}_\phi} / \mathcal{E}(K'_\chi)^{\bar{e}_\phi} \simeq \mathbb{Z}_\ell^{(g_\chi)}$, posons $\mathcal{F}(K_\chi)^{\bar{e}_\phi} / \mathcal{F}(K_\chi)^{\bar{e}_\phi} \cap \mathcal{E}(K'_\chi)^{\bar{e}_\phi} \simeq \hat{\mathfrak{P}}_\chi^{A}$ et dans l'isomorphisme

$\mathcal{E}(K'_\chi)^{\bar{e}_\phi} / \mathcal{E}(k)^{\bar{e}_\phi} \simeq \mathbb{Z}_\ell^{(g_\chi/\ell)}$, posons $\mathcal{F}(K'_\chi)^{\bar{e}_\phi} / \mathcal{F}(K'_\chi)^{\bar{e}_\phi} \cap \mathcal{E}(k)^{\bar{e}_\phi} \simeq \hat{\mathfrak{P}}_\chi^{a\ell}$ et

$N_{K_\chi/K'_\chi}\mathcal{E}(K_\chi)^{\bar{e}_\phi} / \mathcal{E}(k)^{\bar{e}_\phi} \cap N_{K_\chi/K'_\chi}\mathcal{E}(K_\chi)^{\bar{e}_\phi} \simeq \hat{\mathfrak{P}}_\chi^{\ell x}$. Alors :

(i) Si $a < \ell^{n-2}(\ell-1)$, alors $A = a - x$,

(ii) Si $a \geqslant \ell^{n-2}(\ell-1)$, alors $A \geqslant \ell^{n-2}(\ell-1) - x$.

Passons maintenant au cas d'une Γ-extension : Soit ℓ premier fixé et soit $K = K_o$ une extension cyclique réelle de $\mathbb{Q}$ de degré premier à ℓ . On considère K_∞:

$$\begin{tikzcd}
\mathbb{Q}_\infty \arrow[d, dotted, dash] & K_\infty \arrow[d, dotted, dash] & \\
\mathbb{Q}_n \arrow[r, dash] \arrow[d, dotted, dash] & K_n \arrow[r, dash] \arrow[d, dotted, dash] & \mathbb{Q}^{(f_n)} \arrow[d, dotted, dash] \\
\mathbb{Q}_1 \arrow[r, dash] \arrow[d, dash] & K_1 \arrow[r, dash] \arrow[d, dash] & \mathbb{Q}^{(f_1)} \\
\mathbb{Q} \arrow[r, dash] & K_o \arrow[r, dash] & \mathbb{Q}^{(f_o)} \arrow[u, dash]
\end{tikzcd}$$

Il est clair que seul le nombre premier ℓ est ramifié dans K_∞/K_o (et totalement) . Si f_i est le conducteur de K_i , f_o,au plus divisible par ℓ , peut être premier à ℓ , tandis que f_i pour $i \geqslant 1$ sera divisible exactement par ℓ^{i+1} (en fait $f_i = f_o\,\ell^{i+1}$ pour $i \geqslant 1$) .
Par conséquent , l'hypothèse que les f_i ont les mêmes diviseurs premiers peut n'être vérifiée que pour $i \geqslant 1$.

Utilisons le schéma suivant (où ψ parcourt $\mathfrak{X}_{K_o}$) :

$$\begin{array}{ccccc}
\vdots & & \vdots & & \vdots \\
\mathbb{Q}_i & — & K_{\psi_i} & — & K_{\varphi_i} \\
\vdots & & \vdots & & \vdots \\
\mathbb{Q}_2 & — & K_{\psi_2} & — & K_{\varphi_2} \\
| & & | & & | \\
\mathbb{Q}_1 & — & K_{\psi_1} & — & K_{\varphi_1} \\
| & & | & & | \\
\mathbb{Q} & — & K_{\psi_0} & — & K_{\varphi_0} = K_0
\end{array}$$

D'après le lemme III 8 et [15] (§ 8 , 2) l'hypothèse

$N_{K_{\psi_{i+1}}/K_{\psi_i}}(\mathcal{F}(K_{\psi_{i+1}})) = \mathcal{F}(K_{\psi_i})$ est vérifiée pour tout $i \geqslant 1$ et pour tout $\psi \neq 1$; or on sait que les $\mathbb{Q}_i$ ont un nombre de classes premier à ℓ ; par conséquent , pour $\psi \neq 1$, $|\mathcal{H}'_{\psi_i}| = (\mathcal{E}(K_{\psi_i}) : \mathcal{E}'(K_{\psi_i})\mathcal{F}(K_{\psi_i}))$ car $\ell_{\psi_i} = 1$ (cf. Th. III 2 (i)) . Adoptons les notations suivantes : soit $\psi \in \mathfrak{X}_{K_o}$; on appelle ϕ_o un caractère ℓ-adique en-dessous de ψ ; on pose provisoirement , pour tout $i \geqslant 0$, $m_i = m_{\phi_i}(h')$, ϕ_i désignant le caractère ℓ-adique en-dessous de ψ_i associé (de façon évidente) au caractère $\phi_o|\psi$.
Faisons l'hypothèse suivante :

$H(\mu)^+$: " Pour tout $\psi \in \mathfrak{X}_{K_o}$ et tout $\phi_o|\psi$, il existe $i_o \geqslant 1$ tel que $m_{i_o} < \ell^{i_o - 1}(\ell - 1)$ " .

Alors d'après la prop. IV 1 et cette hypothèse , il existe

$i_o \geqslant 1$ (choisi minimum) tel que $m_{i+1} + x_i = m_i$ pour tout $i \geqslant i_o$ (avec $x_i \geqslant 0$):

En effet , si pour $i = i_o$, $m_i < \ell^{i-1}(\ell-1)$, alors $m_{i+1}+x_i = m_i < \ell^{i-1}(\ell-1)$ entraîne bien $m_{i+1} < \ell^i(\ell-1)$, ce qui permet de voir que l'on a

$m_{i_o} = m_{i_o+1} + x_{i_o} = \dots = m_{i_o+k} + \sum_{j=1}^{k-1} x_{i_o+j}$, pour tout $k \geqslant 0$.

Ceci entraîne que la suite x_{i_o+j} est la suite nulle à partir d'un certain rang; par conséquent la suite m_i est constante à partir d'un certain rang n_o .

De plus , comme la suite $\sum_{j=0}^{k-1} x_{i_o+j}$ est croissante au sens large , la suite m_{i_o+k} est décroissante (au sens large et pour $k \geqslant 0$) . Par consé - quent , si l'hypothèse $H(\mu)$ est vérifiée , on obtient facilement que $|\mathcal{H}'_{\psi_n}|$ est , pour tout $\psi \in \mathfrak{X}_{K_o}$, une suite stationnaire pour n assez grand .

D'après la Prop. II 2 , on a , pour $n \geqslant n_o$, $|\mathcal{H}(K_n)| = \prod_{\psi,i} |\mathcal{H}'_{\psi_i}|$ qui est de la forme $\prod_{\psi} \prod_{i=0}^{n_o-1} |\mathcal{H}'_{\psi_i}| \prod_{\psi} \prod_{i=n_o}^{n} \ell^{\lambda_\psi}$ (λ_ψ indépendant de n) , soit $|\mathcal{H}(K_n)| = \ell^{\alpha} \ell^{\lambda^+(n-n_o+1)} = \ell^{\lambda^+ n + \nu^+}$ avec $\lambda^+ = \sum_\psi \lambda_\psi$ et ν^+ entier.

On a donc prouvé :

Théorème IV 1 . Soit K une extension cyclique réelle de $\mathbb{Q}$ de degré pre- mier à ℓ . Supposons l'hypothèse $H(\mu)^+$ vérifiée pour le corps K . Alors il existe λ^+, ν^+, indépendants de n , tels que pour n assez grand $|\mathcal{H}(K_n)| = \ell^{\lambda^+ n + \nu^+}$; en outre , pour n assez grand on a $\mathcal{E}(K_n) = N_{K_{n+1}/K_n} \mathcal{E}(K_{n+1}) \mathcal{E}(K_{n-1})$; enfin le rang n_o minimum à partir duquel cette formule est valable ne dépend que des unités des corps K_i .

Remarque IV 2 . On retrouve ainsi de façon élémentaire une partie des résultats d'Iwasawa . Signalons que l'hypothèse $H(\mu)^+$ équivaut à celle de la nullité de l'invariant μ d'Iwasawa ([13]) . La méthode employée permet d'étudier le problème théorique de la détermination du n_0 minimum à partir duquel la formule d'Iwasawa est valable . Pour le moment , la détermination numérique de λ^+ et ν^+ ne semble pas être effective parceque nous ignorons le comportement de la suite des x_i .

3) Cas de la Γ-extension cyclotomique d'un corps imaginaire .

Soit $L/\mathbb{Q}$ une extension cyclique imaginaire dont le degré est de la forme $g = g'\ell^n$, $n \geqslant 2$, g' premier à ℓ et $\ell \neq 2$. On considère les sous-corps K et k de L tels que $[L:K] = [K:k] = \ell$. On pose $L = K_\chi$, $K = K'_\chi$.

On suppose être dans le cas où L et K ont des conducteurs possédant les mêmes diviseurs premiers ; on suppose S_L et S_K ℓ-entiers.

Supposons $B_1(\chi'^{-1}) = (w_n - 1)^A \alpha$ dans $\mathbb{Z}_\ell^{(g_\chi)}$, avec $\chi' | \phi$ (complétion en γ_χ) , α premier à ℓ . A partir de la suite exacte :

$$1 \longrightarrow (P_\phi(\sigma_\chi)) \longrightarrow \mathbb{Z}_\ell[G(L/\mathbb{Q})] \longrightarrow \mathbb{Z}_\ell^{(g_\chi)} \longrightarrow 1$$

on peut écrire $S_L = (\sigma_\chi^{g'} - 1)^A \alpha(\sigma_\chi) + \beta(\sigma_\chi)\, P_\phi(\sigma_\chi)$;

$N_{L/K}\, S_L = (\bar{\sigma}_\chi^{g'} - 1)^A \alpha(\bar{\sigma}_\chi) + \beta(\bar{\sigma}_\chi)\, P_\phi(\bar{\sigma}_\chi)$, ce qui donne par l'homomorphisme χ'^ℓ et par le fait que $N_{L/K}\, S_L \equiv S_K \mod \nu_{K/\mathbb{Q}}$ (cf. Th. III 3) :

$$\chi'^\ell(S_K) = (w_{n-1} - 1)^A \alpha(\xi) + \beta(\xi)\, P_\phi(\xi) \quad \text{avec } \xi = \chi'^\ell(\bar{\sigma}_\chi) .$$

On a $P_\phi(\xi) = \prod_a (\xi - \zeta^a)$, où $\zeta = \chi'(\sigma_\chi)$, $\xi = \chi'^\ell(\sigma_\chi) = \zeta^\ell$ et a parcourant les résidus mod g_χ correspondant à $G(\mathbb{Q}_\ell^{(g_\chi)} / \mathbb{Q}_\ell)$.

On a $P_\phi(\xi) = \prod_a (\zeta^\ell - \zeta^a) = \prod_a (1 - \zeta^{a-\ell})\zeta^\ell$; or $\zeta^{a-\ell} - 1$ est non premier à ℓ si et seulement si $\zeta^{a-\ell}$ est d'ordre puissance de ℓ, donc si et seulement si $a \equiv \ell \mod g'$. On remarque que alors $a \not\equiv \ell \mod g'\ell$, donc $\zeta^{a-\ell}$ est d'ordre ℓ^n ; posons $a = \ell + \lambda g'$, $\lambda \not\equiv 0 \mod \ell$ (ce qui suffit à assurer que $(a, g\ ) = 1$) ; il faut ensuite prendre des a correspondant au groupe de décomposition de ℓ dans $\mathbb{Q}^{(g\ )}/\mathbb{Q}$; or modulo g' on a $a \equiv \ell \mod g'$ et le résidu mod g' de a appartient au groupe de décomposition de ℓ dans $\mathbb{Q}^{(g')}/\mathbb{Q}$ ce qui prouve que tous les a, $a\ = \ell + \lambda g'$ $0 \leqslant \lambda < \ell^n$, $(\lambda, \ell) = 1$ conviennent. On trouve alors $P_\phi(\xi) = \ell\gamma$, γ premier à ℓ.

On a donc obtenu :

$$B_1(\chi'^{-\ell}) = (w_{n-1}-1)^A \alpha(\xi) + \beta'(\xi)\ell \quad \text{dans } \mathbb{Z}_\ell^{(g\ /\ell)} .$$

Vérifions que $\alpha(\xi)$ est premier à ℓ : s'il en était autrement, on aurait $\alpha(\xi) = (w_{n-1} - 1)\ \alpha'(\xi)$ soit $\chi'^{\ell}(\alpha) =$ $\chi'^{\ell}(\bar{\sigma}_\chi^{\ g'} - 1)\ \chi'^{\ell}(\alpha')$ soit $\alpha(\bar{\sigma}_\chi) \equiv (\bar{\sigma}_\chi^{\ g'} - 1)\ \alpha' \mod P_{\phi'}(\bar{\sigma}_\chi)$ où ϕ' désigne le caractère ℓ-adique au-dessus de χ'^{ℓ}. On aurait finalement $\alpha(\sigma_\chi) \equiv (\sigma_\chi^{\ g'} - 1)\ \alpha'(\sigma_\chi) \mod (P_{\phi'}(\sigma_\chi), \sigma_\chi^{\ g\ /\ell} - 1)$ soit, en considérant l'image des 2 membres de cette congruence par χ' (où $\zeta = \chi'(\sigma_\chi)$) : $\alpha(\zeta) \equiv (w_n - 1)\,\alpha'(\zeta) \mod (P_{\phi'}(\zeta), w_1 - 1)$. Il suffit de prouver que $P_{\phi'}(\zeta)$ n'est pas premier à ℓ pour trouver une contradiction :

$P_{\phi'}(\zeta) = \prod_b (\zeta - \xi^b)$ avec $\xi = \zeta^\ell$, b parcourant un système de résidus correspondant à $G(\mathbb{Q}_\ell^{(g\ /\ell)}/\mathbb{Q}_\ell)$; $P_{\phi'}(\zeta) = \prod_b (\zeta - \zeta^{\ell b})$;

comme $g\ /\ell$ est encore divisible par ℓ, on aura $(b, \ell) = 1$ et $P_{\phi'}(\zeta) = \prod_b (\zeta^b - \zeta^\ell)$ non premier à ℓ d'après le calcul effectué plus haut.

Si on pose maintenant $B_1(\chi'^{-\ell}) = (w_{n-1} - 1)^a\ \alpha'$, α' premier à ℓ, alors on a la congruence :

$(w_{n-1}-1)^a \alpha' \equiv (w_{n-1}-1)^A \alpha$ modulo ℓ , α , α' premiers à ℓ .
D'où :

Proposition IV 2 . Soit $\chi \in \mathfrak{X}^-$ tel que $g_\chi \equiv 0 \bmod \ell^n$ ($n \geqslant 2$) . Soit K'_χ défini par $[K_\chi : K'_\chi] = \ell$. On suppose S_{K_χ} et $S_{K'_\chi}$ ℓ-entiers vérifiant $S_{K'_\chi} \equiv N_{K_\chi/K'_\chi} S_{K_\chi} \bmod \mathcal{V}_{K'_\chi/\mathbb{Q}}$. On pose (pour $\chi' | \phi$) :
$B_1(\chi'^{-1}) \mathbb{Z}_\ell^{(g_\chi)} = \hat{\mathcal{P}}_\chi^A$ et $B_1(\chi'^{-\ell}) \mathbb{Z}_\ell^{(g_\chi/\ell)} = \hat{\mathcal{P}}_\chi^{\ell a}$.
Alors :

(i) Si $a < \ell^{n-2}(\ell-1)$, alors $A = a$;

(ii) Si $a \geqslant \ell^{n-2}(\ell-1)$, alors $A \geqslant \ell^{n-2}(\ell-1)$.

Remarque IV 3 . Si pour un corps k , S_k n'est pas ℓ-entier , c'est que k est extension de degré une puissance de ℓ de $\mathbb{Q}^{(\ell)}$. Dans ce cas , on peut remplacer S_k par $\left(\left(\frac{K}{a}\right) - a\right) S_k$ qui est entier ; par χ' on obtient $(\chi'(a) - a) B_1(\chi'^{-1})$; or $\chi'(a) - a$ sera premier à ℓ dès que χ' n'est pas de la forme $\theta\psi'$ (ψ' d'ordre puissance de ℓ) . La proposition IV 2 est donc valable (même si S_L et S_K ne sont pas ℓ-entiers) pour tous les caractères ϕ sauf peut être pour celui au-dessus de $\theta\psi'$ pour lequel il faut adapter le calcul (à moins que l'on sache que $\mathcal{H}_\phi = (1)$ pour ce caractère , comme c'est le cas des corps $\mathbb{Q}^{(\ell^n)}$) .

Soit $K = K_o$ une extension cyclique imaginaire de $\mathbb{Q}$ de degré premier à ℓ . On considère K_∞ ; du point de vue des conducteurs des corps K_i on est dans la même situation que dans le § 2 .

Utilisons le même schéma et les mêmes notations que pour le cas réel : on a (Th. II 2) , en supposant $w_{\psi_i} = 1$:

$$\left| \mathcal{H}_{\psi_i} \right| = \prod_{\psi'_i | \psi_i} \left(\frac{1}{2} B_1(\psi_i'^{-1}) \right)_\ell .$$

On peut définir les nombres m_i (pour ϕ_o fixé impair) comme dans le cas pair et faire l'hypothèse suivante :

$H(\mu)^-$: " Pour tout ψ impair et pour tout $\phi_o | \psi$, il existe $i_o \geqslant 1$ tel que $m_{i_o} < \ell^{i_o - 1}(\ell - 1)$ " .

Compte tenu de la proposition IV 2 , du fait que l'hypothèse $N_{K_{\psi_{i+1}}/K_{\psi_i}} S_{K_{\psi_{i+1}}} \equiv S_{K_{\psi_i}} \bmod \nu_{K_{\psi_i}/\mathbb{Q}}$ est vérifiée pour tout $i \geqslant 1$ et tout $\psi \in \mathfrak{X}_K^-$ et du fait que l'hypothèse $S_{K_{\psi_i}}$ ℓ-entier n'est pas nécesssaire dans le cas des Γ-extensions considérées (cf. Remarque IV 3) , on a :

Théorème IV 2 . Soit K une extension cyclique imaginaire de $\mathbb{Q}$ ne contenant pas $\mathbb{Q}^{(\ell)}$, de degré premier à ℓ ($\ell \neq 2$) . Supposons l'hypothèse $H(\mu)^-$ vérifiée pour le corps K . Alors il existe λ^- , ν^- , indépendants de n , tels que pour n assez grand $|\mathcal{H}(K_n)^-| = \ell^{\lambda^- n + \nu^-}$; en outre, le rang n_o minimum à partir duquel la formule est valable est effectivement calculable et ne dépend que des valuations des nombres de Bernoulli $B_1(\chi'^{-1})$, $\chi' \in \mathfrak{X}'_{K_i}$.

La proposition IV 2 permet de déterminer facilement les invariants λ^- et μ^- sous les hypothèses du théorème IV 2 (nous laissons au lecteur le soin d'écrire lui-même l'énoncé relatif à la Γ-extension cyclotomique de $\mathbb{Q}^{(\ell)}$ ($K_i = \mathbb{Q}^{(\ell^{i+1})}$, $i \geqslant 0$) qui nous semble particulièrement intéressant) .

Citons par exemple ce que l'on obtient dans le cas des corps quadratiques imaginaires (retrouvant et améliorant les résultats de Gold, [5] et [6]) :

Proposition IV 3 . Soit $K = \mathbb{Q}(\sqrt{-m})$ un corps quadratique imaginaire quelconque ; soit $\ell \neq 2$ un nombre premier (si $\ell = 3$, on suppose $K \neq \mathbb{Q}^{(3)}$).

Soit K_∞ la Γ-extension cyclotomique de K relativement à ℓ . Posons $K_i = K_{\varphi_i}$, pour $i \geqslant 0$, et soit m_i l'invariant analytique associé à φ_i ($|\mathcal{H}_{\varphi_i}| = \ell^{m_i}$, pour $i \geqslant 0$) . Alors s'il existe $i_o \geqslant 1$ tel que $m_{i_o} < \ell^{i_o - 1}(\ell - 1)$, on a $\mu = 0$, $\lambda = m_{i_o}$ et $\nu = m_o + \ldots + m_{i_o - 1} - \lambda(i_o - 1)$.

En effet , d'après la proposition II 5 , les S_{K_i} sont ℓ-entiers, pour tout $i \geqslant 0$ et on a $N_{K_{i+1}/K_i} S_{K_{i+1}} \equiv S_{K_i} \mod \nu_{K_i/\mathbb{Q}}$, pour tout $i \geqslant 1$ (Th. II 3) . On peut donc appliquer la proposition IV 2 et notre résultat découle du th. II 2 .

Remarque IV 4 . Revenons aux hypothèses et notations du th. IV 2 . Notons r_{ψ_i} le ℓ-rang de $\mathcal{H}_{\psi_i}$, pour tout $\psi \in \mathcal{X}_K^-$ et tout $i \geqslant 0$. On remarque que

$$j_{K_{\psi_{i+1}}/K_{\psi_i}} \{ h \in \mathcal{H}_{\psi_i} , h^\ell = 1 \} \subset \mathcal{H}_{\psi_{i+1}}$$

, pour tout $i \geqslant 0$; or la restriction à $\mathcal{H}_{\psi_i}$ de $j_{K_{\psi_{i+1}}/K_{\psi_i}}$ est injective (Prop. II 1) , donc on aura $r_{\psi_i} \leqslant r_{\psi_{i+1}}$. La suite r_{ψ_i} ($i \geqslant 0$, ψ fixé) est croissante . Si $\mu = 0$, elle est nécessairement bornée : on a donc $r_{\psi_i} = r$ pour i assez grand dans ce cas .

Remarque IV 5 . L'étude précédente (notamment les propositions I V 1 et IV 2) peut s'appliquer dès que l'on a une extension cyclique de degré ℓ^n du corps K , qui n'est pas nécessairement contenue dans la Γ-extension K_∞; on peut donc , dans certains cas , établir des formules du type : $|\mathcal{H}(K_i)| = \ell^{\lambda i + \nu}$, pour $n_o \leqslant i \leqslant n$.

Bibliographie

[1] Brumer (A.), Travaux récents d'Iwasawa et de Leopoldt , Sém.Bourbaki, 325 (1967) .

[2] Coates (J.) , p-adic L-functions and Iwasawa's theory , Durham symposium in algebraic number theory , Sept. 1975 .

[3] Coates (J.) and Lichtenbaum (S.) , On ℓ-adic Zeta functions , Ann.of Math., 98 (1973) , 498 - 550 .

[4] Gillard (R.) , Relation de Stickelberger , Sém. de théorie des Nombres , Grenoble (1974) .

[5] Gold (R.) , Exemples of Iwasawa invariants , Acta Arith., XXVI (1974).

[6] Gold (R.) , Exemples of Iwasawa invariants , II , Acta Arith., XXVI (1975).

[7] Gras (G.) , Sur les ℓ-classes d'idéaux dans les extensions cycliques relatives de degré premier ℓ , Ann. Inst. Fourier , 23 , 3 (1973) , 1-48 .

[8] Gras (G.) , Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés , à paraître dans Ann. Inst.Fourier (1977) (fasc. 1 , t. 27) .

[9] Hasse (H.) , Zahlentheorie , Berlin (1963) .

[10] Hasse (H.) , Über die Klassenzahl abelscher Zahlkörper , Berlin (1952).

[11] Iwasawa (K.) , A class number formula for cyclotomic fields , Ann. of Math., 76 (1962) , 171-179 .

[12] Iwasawa (K.) , On the theory of cyclotomic fields , Ann. of Math., 70 3 (1959) .

[13] Iwasawa (K.) , On Γ-extensions of algebraic number fields , Bul. Amer. Math. Soc., 65 (1959) , 183-226 .

[14] Iwasawa (K.) , On the μ-invariants of $\mathbb{Z}_\ell$-extensions , Number Theory, Algebraic Geometry and Commutative Algebra , in honor of Y. Akizuki , Kinokuniya , Tokyo , (1973) , 1-11 .

[15] Leopoldt (H.W.) , Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper , Abh. Deutsche Akad. Wiss. Berlin , Math., 2 (1954) .

[16] Leopoldt (H.W.) , Zur Arithmetik in abelschen Zahlkörpern , Jour. für die reine und ang. Math., 209 (1962) , 54-71 .

[17] Oriat (B.) , Quelques caractères utiles à l'arithmétique , Publ. Math. de l'Univ. de Besançon (Théorie des Nombres) (1974-1975) .

[18] Oriat (B.) , Exposé sur l'article : Über Einheitengruppe und Klassen - zahl reeller abelscher Zahlkörper " de Leopoldt , Publ. Math. de l'Univ. de Besançon (Théorie des Nombres) (1974-1975).

[19] Serre (J.P.) , Représentations linéaires des groupes finis , Hermann (1971) .

Note : Les résultats obtenus dans cet article ont été exposés dans une conférence aux Journées arithmétiques de Caen (8 Mai 1976) (résumé à paraître dans les Comptes - rendus de ces Journées) .