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] .

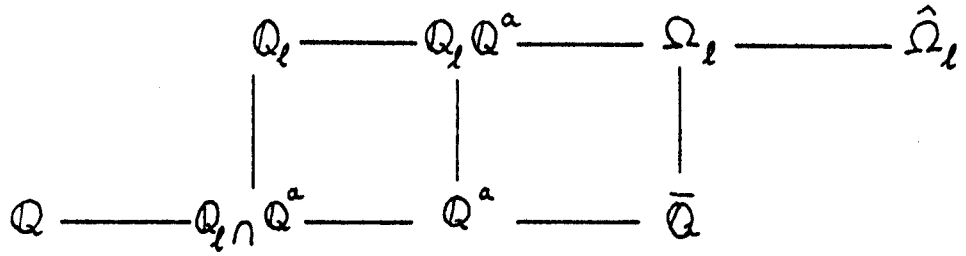
Chap. I

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 $\bar{\mathbb{Q}}$ 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) :



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 $\mathfrak{X}$ la famille des extensions finies de $\mathbb{Q}$ contenues dans

$\mathbb{Q}^a$. On suppose donné une famille M de $\mathbb{Z}[\mathfrak{S}]$ -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 $\sigma\in\mathfrak{S}$, on note σ_K l'image de σ dans $\mathrm{Gal}(K/\mathbb{Q}) = \mathfrak{S}/\mathrm{Gal}(\mathbb{Q}^a/K)$. Pour une extension L/K , L , $K\in\mathcal{X}$, on pose $G(L/K) = \mathrm{Gal}(L/K)$ et on pose $\vartheta_{L/K} = \sum_{s\in G(L/K)} s \in \mathbb{Z}[G(L/K)]$.

a) Hypothèses sur les familles $(M(K))_{K\in\mathcal{X}}$, $(N_{L/K})$ 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 $\sigma\in\mathfrak{S}$, 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 $\mathfrak{S}$ -modules de M(L) dans M(K) , $j_{L/K}$ est un homomorphisme de $\mathfrak{S}$ -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 :

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

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

Définition I 1 . Si $M = (M(K))_{K\in\mathcal{X}}$ vérifie la condition (i) , nous dirons que cette famille est une $\mathfrak{S}$ -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 $\mathfrak{S}$'-famille (les homomorphismes $N_{L/K}$ et $j_{L/K}$ étant supposés associés à M sans ambiguité) .

b) Propriétés immédiates des $\mathfrak{S}$'-familles .

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 $j_{K/K} \circ N_{K/K} = id$; $N_{K/K}^2 = N_{K/K}$ et $j_{K/K}^2 = j_{K/K}$ (d'après (ii)) entraînent $j_{K/K} \circ N_{K/K}^2 = N_{K/K} = j_{K/K} \circ N_{K/K} = id$ et $j_{K/K}^2 \circ N_{K/K} = j_{K/K} = j_{K/K} \circ N_{K/K} = id$.

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^e_χ 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^e_χ 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 $\mathfrak{S}$ 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 $\mathfrak{S}$-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 $P'_\varphi(\sigma_\chi^a) = \prod_{\chi'|\varphi} (\sigma_\chi - \chi'(\sigma_\chi))\,(\sigma_\chi^{a-1} + \ldots \pm \chi'^{a-1}(\sigma_\chi))$ et de la même manière, on aura $P_\varphi(\sigma_\chi) = \prod_{\chi'|\varphi} (\sigma_\chi^a - \chi'^a(\sigma_\chi))\,(\sigma_\chi^{a(a^*-1)} + \ldots \pm \chi'^{a(a^*-1)}(\sigma_\chi))$, 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 :

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

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 :

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

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

Trois lemmes préliminaires sont nécessaires .

Lemme 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 .

Remarque 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 $P_{n_o p^k}$.

Lemme 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

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

Lemme 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 :

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

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 $n > 1$.

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

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 ,

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

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

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 $N_{g_\chi,p}(\sigma_\chi) = \sqrt{}_{K_\chi/k_p}$, 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 .

Remarque 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) Application à la définition de 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) Les M_φ comme $A^{(g_\chi)}$-modules . 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 $\prod_{\substack{p \mid g_\chi \\ p \text{ premier}}} p$.

5) Un calcul d'indice dans un cas particulier . Soit M une $\mathfrak{S}$-famille . On suppose donné une autre $\mathfrak{S}$-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-$A[G(K/\mathfrak{Q})]$-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 $\mathfrak{U}$ de $A^{(g_\chi)}$ et dans cet isomorphisme , N_φ a pour image un idéal $\mathfrak{A}$ multiple de $\mathfrak{U}$. Il en résulte que $M_\varphi / N_\varphi \simeq A^{(g_\chi)} / (\mathfrak{A}/\mathfrak{U})$. On a alors , en posant $\mathfrak{A}/\mathfrak{U} = \mathfrak{C}$ (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 :

Proposition I 4 . Soient M et N deux $\mathfrak{S}$-familles de $A[\mathfrak{S}]$-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 $M_\varphi \longrightarrow \mathfrak{U}$ un isomorphisme de M_φ sur un idéal entier de $A^{(g_\chi)}$ et soit $\mathfrak{A}$ l'image de N_φ par cet isomorphisme , alors $\mathfrak{C} = \mathfrak{A}/\mathfrak{U}$.

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

Proposition I 5 . 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 $\chi \in \mathcal{X}_L$) et on a :

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

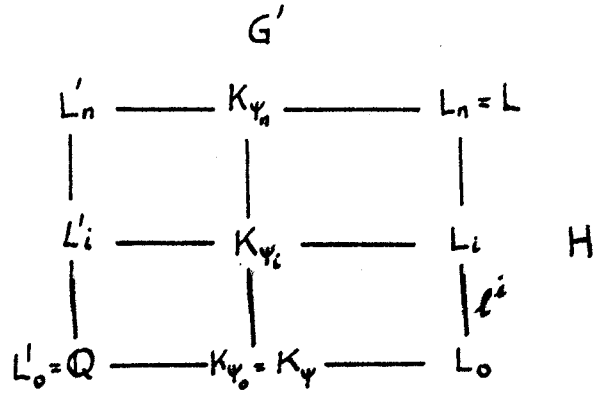
démonstration

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 surjectives . Lorsque les $M(K)$ sont des ℓ -groupes , on a le résultat suivant:

Lemme I 4 . 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. I 2) 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 :



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 $\mathfrak{S}$ '-familles constituées de ℓ -groupes non nécessairement finis :

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

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 di-

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

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

(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 : $\prod_{\chi \in \mathcal{X}_L} |M'_\chi| = \prod_{\psi,i} |M^*(K_{\psi_i})^{e_\psi}| =$

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

7) Cas d'une $\mathfrak{S}$ -famille de $\mathbb{Z}_\ell$ -modules . Soit M une $\mathfrak{S}$ -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 existe 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 $\mathfrak{S}$ -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 I 5 . Il existe U_1 , $U_2 \in \mathbb{Z}_\ell[X]$ tels que $U_1Q_1 + U_2Q_2 = 1$.

Comme les polynomes Q_1 et Q_2 sont irréductibles dans $\mathbb{Q}_\ell[X]$, on peut écrire en fait $U_1Q_1 + U_2Q_2 = \ell^k$, $k \geqslant 0$, 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 $c = 1$ 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 $\phi_1, \ldots, \phi_m$ les caractères ℓ-adiques distincts au-dessous de χ et notons pour simplifier $Q_1, \ldots, Q_m$ les polynomes P_{ϕ_i} ; on a donc d'après le lemme : $\mathbb{Z}_\ell[X] \Big/ \left(\prod_{i=1}^{m} Q_i(X)\right) = \mathbb{Z}_\ell[X] / (P_\chi(X)) \simeq \prod_{i=1}^{m} \mathbb{Z}_\ell[X] / (Q_i(X))$. 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 orthogonaux . 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 $\varphi'^k \mid \phi_o$ (ϕ_o caractère ℓ-adique au-dessus de la composante φ' d'ordre premier à ℓ de χ') . On a alors

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

Remarque 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 :

Définition I 3 . Soit M une $\mathcal{G}'$-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 $K \in \mathfrak{K}$ constituent une $\mathfrak{S}'$-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 $L \in \mathfrak{K}$, 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. $\mathbb{H}'(L)^- = \left\{ h \in \mathbb{H}(L) , N_{L/L_+}(h) = 1 \right\}$, 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 $\mathfrak{K}$ sont des $\mathfrak{S}'$-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. $\chi \in \mathfrak{X}^-$) 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 $[K_\chi : k_p] = p$:

$$\begin{array}{ccc} k_p & \overset{p}{\text{———}} & K_\chi \\ \Big| & & \Big| \ell \\ k'_p & \underset{p}{\text{———}} & K_\psi \end{array}$$

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 $p \neq \ell$, $p \mid g_\chi$, 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 :

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

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 $\mathfrak{a}A_L = aA_L$, soit $\mathfrak{a} = aA_K$ 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_+ :

$$\begin{array}{ccc} L_+ & \overset{2}{\text{—}} & L \\ \ell \,\big|\, & & \big|\, \ell \\ K_+ & \overset{2}{\text{—}} & K \end{array}$$

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 $\mathcal{H}(K)^- \cap$ 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 $h' \in \mathcal{H}(K)^- \cap$ 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 $h' \in$ 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 $q(T_L^*)$:

Lemme 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 $q(T_L^*) = \mathcal{H}(K)^- \cap$ 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) .

Lemme II 5 . Si l'on suppose $\mathcal{H}(K)^- \cap$ 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 $\mathcal{H}(K)^- \cap$ 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 $\mathcal{H}(K)^- \cap$ 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

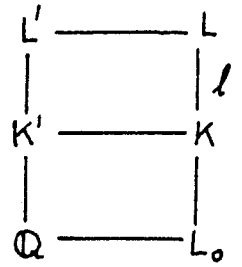
l'extension de Kummer $K(\sqrt[\ell]{a})$ avec $a = \alpha^\ell$; on a bien $a A_L = \mathfrak{a}^\ell A_L$ soit, puisque $a \in K$, $a A_K = \mathfrak{a}^\ell$.

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 :



avec L/L_0 et $L'/\mathbb{Q}$ cycliques d'ordre une puissance de ℓ , L/L' et $L_0/\mathbb{Q}$ 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 $\mathcal{H}(K)^- \cap \operatorname{Ker} j = (1)$.**