

Séminaire de Théorie des Nombres .

- Besançon -

Année 1975-1976

DECOMPOSITION DES IDEAUX DANS UNE EXTENSION
DE KUMMER CYCLIQUE

Danièle CHATELAIN
Faculté des Sciences . Mathématiques
25030 BESANCON CEDEX

DECOMPOSITION DES IDEAUX DANS UNE EXTENSION

DE KUMMER CYCLIQUE

par

D. CHATELAIN

I Introduction .

Cet exposé résulte d'un travail fait en commun avec A. Kerkour sur l'étude de la décomposition des idéaux dans une extension de Kummer, cyclique de degré N . On étudie la généralisation des critères de Hecke ([1], § 39, Satz 118-119), au cas où le degré N n'est pas premier.

1°) Notations .

Soit K un corps, corps de fractions d'un anneau de Dedekind A_K , de caractéristique 0 , et contenant les racines N^{eme} de 1 .

On considère une extension cyclique L de K , de degré N ; (de telles extensions sont dites de "Kummer"; pour leur construction, voir [2] page 218 par exemple).

Soit \mathfrak{p} un idéal premier de A_K ; soit $g_{\mathfrak{p}}(L)$ le nombre d'idéaux premiers de l'anneau des entiers A_L de L au-dessus de \mathfrak{p} . On note $e_{\mathfrak{p}}(L)$ et $f_{\mathfrak{p}}(L)$, l'indice de ramification et le degré résiduel de \mathfrak{p} dans l'extension L/K , (avec : $e_{\mathfrak{p}}(L).f_{\mathfrak{p}}(L).g_{\mathfrak{p}}(L) = N$).

Soit $(\widehat{K}_{\mathfrak{p}}, \sigma_{\mathfrak{p}})$ une complétion de K pour la valuation additive discrète $v_{\mathfrak{p}}$ de K associée à \mathfrak{p} . \mathfrak{p} étant fixé, on identifie K à un sous-corps de $\widehat{K}_{\mathfrak{p}}$, à l'aide du plongement $\sigma_{\mathfrak{p}}$ de K dans $\widehat{K}_{\mathfrak{p}}$. On sait ([2], page 218) qu'il existe $\alpha \in K$ tel que L soit égal à $K(\sqrt[N]{\alpha})$. On a alors $\alpha \in \widehat{K}_{\mathfrak{p}}$, et le corps $\widehat{K}_{\mathfrak{p}}(\sqrt[N]{\alpha})$ est un complété $\widehat{L}_{\mathfrak{p}}$ de L , pour la valuation $v_{\mathfrak{p}}$ de L associée à un idéal premier \mathfrak{P} de A_L au-dessus de \mathfrak{p} .

On note $\overline{K}_{\mathfrak{p}}$ et $\overline{L}_{\mathfrak{p}}$, les corps résiduels de $\widehat{K}_{\mathfrak{p}}$ et $\widehat{L}_{\mathfrak{p}}$. On suppose que $\overline{K}_{\mathfrak{p}}$ est de caractéristique $p \neq 0$. On a besoin, pour la

détermination de $e_p(L)$, de supposer l'extension résiduelle $\overline{L}_p / \overline{K}_p$ séparable. Dans les exemples, K sera une extension finie de \mathbb{Q} ou du corps \mathbb{Q}_p ; le corps résiduel \overline{K}_p est alors fini et l'extension résiduelle $\overline{L}_p / \overline{K}_p$ est toujours séparable.

2°) Réduction à une étude locale.

Soit N'' le plus grand des diviseurs m de N tels que l'on ait $\alpha \in (\widehat{K}_p)^m$. On pose $\alpha = \beta^{N''}$ et $N = N' \cdot N''$. La décomposition du polynôme $X^N - \alpha$ en facteurs irréductibles dans $\widehat{K}_p[X]$ est :

$$X^N - \alpha = \prod_{i=0}^{N''-1} (X^{N'} - \zeta^i \beta) \quad , \quad \text{où } \zeta \text{ est une racine primitive } (N'')^{\text{eme}}$$

de 1. On a donc : $g_p(L) = N''$.

On donne au § II, un critère de calcul de $g_p(L)$ basé sur des résolutions de congruences.

Les nombres $e_p(L)$ et $f_p(L)$ représentent aussi l'indice de ramification et le degré résiduel de l'extension locale $\widehat{L}_p / \widehat{K}_p$. On donne au § III, un critère d'étude de la ramification dans une extension locale, et on en déduit un critère pour l'étude de l'indice de ramification dans l'extension $K(\sqrt[N]{\alpha})$.

3°) Réduction au cas $N = l^n$ (l premier).

Soit $N = \prod_i l_i^{n_i}$, la décomposition de N en nombres premiers.

L est le produit des extensions $K(\sqrt[l_i^{n_i}]{\alpha})$ qui sont deux à deux linéairement disjointes.

On déduit des propriétés classiques des nombres de décomposition que l'on a :

$$e_p(K(\sqrt[N]{\alpha})) = \prod_i e_p(K(\sqrt[l_i^{n_i}]{\alpha}))$$

$$g_p(K(\sqrt[N]{\alpha})) = \prod_i g_p(K(\sqrt[l_i^{n_i}]{\alpha}))$$

On pourra donc, lorsque cela simplifie les démonstrations, étudier la décomposition de p dans une extension cyclique de K de degré l^n (l premier).

II Détermination du nombre $g_p(L)$ d'idéaux premiers de L au-dessus de p .

1°) Effet de l'application $x \mapsto x^m$ sur la filtration du groupe des unités d'un corps k , complet pour une valuation discrète.

Rappelons le résultat suivant ([3], page 219 et [4], page 6).

Proposition II.1.

Soit k un corps de caractéristique 0 , complet pour une valuation discrète v ; on suppose que son corps résiduel est de caractéristique $p \neq 0$. On note pour $i \in \mathbb{N} - \{0\}$, $U^{(i)} = \{x \in k; v(x-1) \geq i\}$.

(1) Pour $i > \frac{v(p)}{p-1}$, l'application $x \mapsto x^p$ est un isomorphisme de $U^{(i)}$ sur $U^{(i+v(p))}$.

(2) Pour m premier avec p et pour $i > 0$, l'application $x \mapsto x^m$ est un automorphisme de $U^{(i)}$.

Corollaire II.2.

Soit $m \in \mathbb{N} - \{0\}$. Posons $a(m) = 0$ si $v(m) = 0$; $a(m) = \left[\frac{v(p)}{p-1} \right] + v(m)$ si $v(m) \neq 0$. ($\left[\frac{v(p)}{p-1} \right]$ est la partie entière de $\frac{v(p)}{p-1}$).

(1) L'application $x \mapsto x^m$ est un isomorphisme de $U^{(i-v(m))}$ sur $U^{(i)}$ pour tout $i > a(m)$.

(2) Si $\frac{v(p)}{p-1}$ est entier, on a :

$$\left[U^{(i - \frac{v(p)}{p-1})} \right]^m \subset U^{(i - \frac{v(p)}{p-1} + v(m))}$$

Démonstration :

(1) est une conséquence immédiate de la proposition précédente (on écrit $m = m' \cdot p^n$ et $x^m = (((x^{m'})^p) \cdots)^p$).

En reprenant la démonstration de la proposition II.1 , on peut vérifier , que pour $i \leq \frac{v(p)}{p-1}$, l'application $x \mapsto x^p$ est un homomorphisme (en général ni injectif , ni surjectif) de $U^{(i)}$ dans $U^{(i \cdot p)}$

On en déduit que si $\frac{v(p)}{p-1}$ est entier , on a

$$\left[U^{(\frac{v(p)}{p-1})} \right]^p \subset U^{(p \cdot \frac{v(p)}{p-1})} = U^{(\frac{v(p)}{p-1} + v(p))}$$

On en déduit alors la relation (2) (utilisée au § III) .

Dans ce qui suit , les notations sont toujours celles de la proposition II.1 .

Corollaire II.3.

Soit $\alpha \in k$ tel que $v(\alpha) \geq 0$ et m un entier naturel non nul . On note π_k une uniformisante de k . Les propositions suivantes sont équivalentes :

- (1) L'équation : $X^m = \alpha$, a une solution dans k .
- (2) Les congruences : $X^m \equiv \alpha \pmod{\pi_k^\lambda}$, ont des solutions dans k pour tout $\lambda \in \mathbb{N}$.
- (3) La congruence : $X^m \equiv \alpha \pmod{\pi_k^{v(\alpha) + a(m) + 1}}$, a une solution $y \in k$ (le nombre $a(m)$ est défini dans le corollaire II.2) .

Démonstration :

Il est clair que (1) implique (2) et que (2) implique (3) .
 Montrons que (3) implique (1) .
 On suppose qu'il existe $y \in k$ et y' entier de k ($v(y') \geq 0$) tel que :

$$\alpha = y^m + y' \cdot \pi_k^{v(\alpha) + a(m) + 1} .$$

On a : $v(\alpha) + a(m) + 1 > v(\alpha)$.

On en déduit : $v(y^m) = v(\alpha) = m \cdot v(y)$.

Posons : $y = \delta \cdot \pi_k^{v(y)}$ avec $\delta \in k$, tel que $v(\delta) = 0$

$$\alpha = \varepsilon \cdot \pi_k^{v(\alpha)} = \varepsilon \cdot \pi_k^{m \cdot v(y)}$$

avec $\xi \in k$, tel que $v(\xi) = 0$.

On en déduit :

$$\xi = \delta^m \left[1 + \frac{y'}{\delta^m} \cdot \prod_k^{a(m)+1} \right].$$

L'élément $1 + \frac{y'}{\delta^m} \cdot \prod_k^{a(m)+1}$ appartient à $U^{(a(m)+1)}$.

D'après le corollaire II.2, il est donc de la forme u^m (avec $u \in U^{(a(m)+1 - v(m))}$) on en déduit

$$= \left[u \cdot \delta \cdot \prod_k^{v(y)} \right]^m \text{ avec } u \cdot \delta \cdot \prod_k^{v(y)} \in k.$$

2°) Détermination de $g_p(L)$.

On reprend les notations du § I.

a) critère : Rappelons que p désigne la caractéristique (non nulle) du corps résiduel de K pour l'idéal \mathfrak{p} (on a : $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$).

Proposition II.4.

Soit L une extension cyclique de K de degré N , et soit $\alpha \in K$ tel que $v_p(\alpha) \geq 0$ et $L = K(\sqrt[N]{\alpha})$.

Le nombre $g_p(L)$ d'idéaux premiers de A_L au-dessus de \mathfrak{p} , est égal au plus grand des diviseurs m du PGCD de $v_p(\alpha)$ et de N tels que la congruence :

$$\alpha \equiv X^m \pmod{\mathfrak{p}^{v_p(\alpha) + a(m) + 1}}$$

ait une solution dans K .

Remarque : Les nombres $a(m)$ sont ceux définis dans le corollaire II.2, en prenant $k = \widehat{K}_p$ et $v = v_p$. Précisons que si l'on a $v(m) > 0$, alors p divise m donc N ; K contient les racines N^{eme} de 1 donc contient une racine primitive ζ , p^{eme} de 1; $\frac{v(p)}{p-1}$ étant égal à la valuation de

$1 - \zeta$ est donc entier et on a pour $v(m) > 0$:

$$a(m) = \frac{v_p(p)}{p-1} + v_p(m).$$

Démonstration :

$g_p(L)$ est tel que l'on ait : $\alpha \in (\widehat{K}_p)^{g_p(L)}$; c'est donc un diviseur de $v_p(\alpha)$; en utilisant la remarque du § I.2°), $g_p(L)$ est donc le plus grand des diviseurs m du PGCD de $v_p(\alpha)$ et de N tels que l'on ait $\alpha \in (\widehat{K}_p)^m$. La proposition est alors une conséquence immédiate du corollaire II.3.

Remarque : Puisque l'on a $\alpha \in (\widehat{K}_p)^{g_p(L)}$, la congruence :

$\alpha \equiv X^{g_p(L)} \pmod{p^{v_p(\alpha) + a(N) + 1}}$ a aussi une solution β dans \widehat{K}_p que l'on peut calculer. On a donc :

$$\alpha = \beta^{g_p(L)} \cdot u$$

avec $u = 1 + \lambda \cdot \prod_k^{v_p(\alpha) + a(N) + 1} (\pi_k \text{ est une uniformisante de } \widehat{K}_p)$.

On déduit du corollaire II.2 que $u = u' \cdot N$.

Posons $N' = \frac{N}{g_p(L)}$.

On a alors : $\widehat{L}_p = \widehat{K}_p(\sqrt[N]{\alpha}) = \widehat{K}_p(\sqrt[N']{\beta})$

avec $N' = [\widehat{K}_p(\sqrt[N']{\beta}) : \widehat{K}_p]$.

b) choix de $\alpha \in K$ tel que $L = K(\sqrt[N]{\alpha})$.

Dans l'application numérique de la proposition précédente, on a intérêt à choisir α tel que $v_p(\alpha)$ soit minimum.

Lemme II.5.

Soit Δ l'ensemble des $\gamma \in K$ tels que $L = K(\sqrt[N]{\gamma})$.

Soit $\alpha \in \Delta$ tel que $v_p(\alpha)$ soit égal à la valeur minimum d des entiers $|v_p(\gamma)|$ lorsque $\gamma \in \Delta$.

(1) Si $d = 0$, on a $v_p(\gamma) \equiv 0 \pmod{N}$, pour tout $\gamma \in \Delta$ et s'il existe $\gamma \in \Delta$ tel que $v_p(\gamma) \equiv 0 \pmod{N}$, on a $d = 0$.

.../...

(2) Si $d \neq 0$, d est le PGCD de N et de $v_p(\gamma)$ pour tout $\gamma \in \Delta$.

Démonstration :

On sait que l'on a $\gamma \in \Delta$ si et seulement si on a : $\gamma = x^N \cdot \alpha^i$ avec $\alpha \in \Delta$, $x \in K$ et $(i, N) = 1$.

On en déduit que si $v_p(\alpha) = d = 0$ on a pour tout $\gamma \in \Delta$, $v_p(\gamma) \equiv 0 \pmod N$.

Inversement supposons que pour un $\gamma \in \Delta$, on ait $v_p(\gamma) = \lambda \cdot N$.

Soit $\prod_K \in K$ tel que $v_p(\prod_K) = 1$. Posons $\alpha' = \prod_K^{-\lambda \cdot N} \cdot \gamma$ on a $\alpha' \in \Delta$ et $v_p(\alpha') = 0$ donc $d = 0$.

Supposons maintenant $d \neq 0$.

On a $\alpha = x^N \cdot \gamma^j$ et $\gamma = x^N \cdot \alpha^i$. On en déduit que le PGCD d' de $v_p(\gamma)$ et de N est égal au PGCD de $v_p(\alpha)$ et de N . d étant non nul on a donc $d' \leq d$.

Montrons alors qu'il existe $\alpha' \in \Delta$ tel que $v_p(\alpha') = d'$, on en déduira (d étant minimum) que l'on a bien : $d = d'$.

Posons : $N = d'N'$ et $v_p(\gamma) = d'd''$ avec $(N', d'') = 1$.

Il existe u_0 et $v_0 \in \mathbb{Z}$ tels que $u_0 N' + v_0 d'' = 1$.

Construisons des coefficients de Bezout, $u = u_0 + \lambda \cdot d''$ et $v = v_0 - \lambda N'$, tels que v et N soient premiers entre eux.

On prend pour λ , le produit des nombres premiers divisant N mais ne divisant ni v_0 ni N' . On vérifie que N et v sont premiers entre eux.

On pose alors : $\alpha' = \prod_K^{u \cdot N} \cdot \gamma^v$.

On a bien : $\alpha' \in \Delta$ (car $(v, N) = 1$)

et $v_p(\alpha') = u \cdot N + v \cdot v_p(\gamma) = d'$.

3°) Etude d'un exemple.

a) " généralités " .

Soit p un nombre premier fixé. On désigne par Ω_p une clôture algébrique de \mathbb{Q}_p et par v_p la valuation de Ω_p prolongeant la valuation p -adique de \mathbb{Q}_p .

On peut identifier \mathbb{Q} à un sous-corps de \mathbb{Q}_p . Soit K une extension galoisienne de \mathbb{Q} . Elle est alors contenue dans Ω_p et de la forme $K = \mathbb{Q}(\theta)$ avec $\theta \in \Omega_p$.

Soit $f(X)$ le polynome irréductible de $\mathbb{Q}[X]$ dont θ est racine. On sait que sa décomposition en polynomes irréductibles de $\mathbb{Q}_p[X]$ est de la forme $f_1(X) \cdot f_2(X) \cdot \dots \cdot f_g(X)$ (f_i , polynomes irréductibles distincts). On choisit pour tout $i \in \{1, \dots, g\}$, une racine θ_i de $f_i(X)$ et on note σ_i , le \mathbb{Q} -homomorphisme de K dans Ω_p défini par $\sigma_i(\theta) = \theta_i$. On sait alors, que les g prolongements distincts de la valuation p -adique v_p de \mathbb{Q} à K , sont les $v_p \circ \sigma_i$. Posons $\hat{K} = \mathbb{Q}_p(\theta_i)$ (Si K est galoisienne, K ne dépend pas de $i \in \{1, \dots, g\}$). Soit \hat{p} l'unique idéal premier de l'anneau des entiers de \hat{K} .

Les g idéaux premiers de K au-dessus de p sont les idéaux $\mathfrak{p}_i = \sigma_i^{-1}(\hat{p})$ et les g complétions de K pour les valuations $v_p \circ \sigma_i$ associées aux idéaux \mathfrak{p}_i sont les (\hat{K}, σ_i) .

Il est alors facile de vérifier que la congruence :

$$\alpha \equiv X^m \pmod{\mathfrak{p}_i^\lambda}$$

a une solution X dans K si et seulement si la congruence :

$$\sigma_i(\alpha) \equiv X^m \pmod{\hat{p}^\lambda}$$

a une solution X dans \hat{K} .

b) l'exemple.

On prend : $K = \mathbb{Q}(\sqrt{113}, \sqrt{2}, \sqrt{i})$, contenant les racines 8^{eme} de 1,

$$L = K(\sqrt[8]{\alpha}) \text{ avec } \alpha = \sqrt{113} + 4\sqrt{2}.$$

On vérifie que $\alpha \notin K^2$ (en utilisant une base des entiers de K).

On a donc bien $[L : K] = 8$.

On remarque que $(\sqrt{113} + 4\sqrt{2}) \cdot (\sqrt{113} - 4\sqrt{2}) = 3^4$.

On a donc $v_p(\alpha) = 0$ pour p non diviseur de 3.

1^{er} cas : $p = 2$.

Les symboles $\sqrt{113}, \sqrt{2}, i$, désignent ici des racines carrées,

fixées une fois pour toutes, de $\sqrt{113}$, $\sqrt{2}$ et i , dans Ω_2 , clôture algébrique de \mathbb{Q}_2 . On a $\sqrt{113} \equiv 1 \pmod{8}$. D'après un résultat classique qui est d'ailleurs une conséquence immédiate du corollaire II.1, on en déduit que $\sqrt{113} \in \mathbb{Q}_2$. On a alors : $\hat{K} = \mathbb{Q}_2(\sqrt{113}, \sqrt{2}, i) = \mathbb{Q}_2(\sqrt{2}, i)$, ($[\hat{K} : \mathbb{Q}_2] = 4$).

Prenons $\theta = \sqrt{113} + \sqrt{2} + i$ ($K = \mathbb{Q}(\theta)$).

Les 8 conjugués de θ par rapport à \mathbb{Q} sont conjugués 4 à 4 par rapport à \mathbb{Q}_2 , de la manière suivante :

$$\left\{ \begin{array}{l} \sqrt{113} + \sqrt{2} + i ; \sqrt{113} - \sqrt{2} - i ; \sqrt{113} + \sqrt{2} - i ; \sqrt{113} - \sqrt{2} + i \\ -\sqrt{113} + \sqrt{2} + i ; -\sqrt{113} - \sqrt{2} - i ; -\sqrt{113} + \sqrt{2} - i ; -\sqrt{113} - \sqrt{2} + i \end{array} \right\}.$$

Il y a donc 2 idéaux \mathfrak{p}_1 et \mathfrak{p}_2 de K au-dessus de 2 . Les complétions de K correspondants sont (\hat{K}, σ_1) et (\hat{K}, σ_2) définies par le choix suivant des plongements :

$$\sigma_1 : \begin{cases} \sqrt{113} \rightarrow \sqrt{113} \\ \sqrt{2} \rightarrow \sqrt{2} \\ i \rightarrow i \end{cases} ; \quad \sigma_2 : \begin{cases} \sqrt{113} \rightarrow -\sqrt{113} \\ \sqrt{2} \rightarrow \sqrt{2} \\ i \rightarrow i \end{cases}$$

ou encore : $\sigma_1(\theta) = \theta_1 = \theta$ et $\sigma_2(\theta) = \theta_2 = -\sqrt{113} + \sqrt{2} + i$.

Soit ζ une racine primitive 8^{ème} de 1 dans $\mathbb{Q}_2(\sqrt{2}, i) = \hat{K}$.

On pose $\pi = 1 - \zeta$; π est alors une uniformisante de \hat{K} ($\mathfrak{p} = (\pi)$).

On a ici $v_{\mathfrak{p}_i}(2) = 4$ et $v_{\mathfrak{p}_i}(\alpha) = 0$ ($i = 1, 2$).

D'après la proposition II.2, $\mathfrak{g}_{\mathfrak{p}_i}(L)$ est le plus grand des diviseurs 2^h

de 8 tels que :

$$\sigma_i(\alpha) \equiv X^{2^h} \pmod{\pi^{5+4h}}$$

avec $\sigma_1(\alpha) = \sqrt{113} + 4\sqrt{2}$ et $\sigma_2(\alpha) = -\sqrt{113} + 4\sqrt{2}$.

Développement π -adique de $\sqrt{113}$ et $4\sqrt{2} \pmod{\pi^{17}}$:

Les éléments entiers de \hat{K} s'écrivent de manière unique, $\sum_{i \in \mathbb{N}} s_i \pi^i$

avec $s_i \in \{0, 1\}$.

Posons $2 = \varepsilon \cdot \pi^4 = \varepsilon(1 - \zeta)^4$.

ζ est racine de $X^4 + 1$, on en déduit par approximations successives :

$$\xi \equiv 1 + \pi^2 + \pi^5 + \pi^6 + \pi^8 + \pi^9 + \pi^{11} + \pi^{12} \pmod{\pi^{13}} .$$

D'autre part, $\frac{1+i}{\sqrt{2}}$ est une racine primitive 8^{eme} de 1 que l'on peut

supposer égale à ζ . On en déduit :

$$\sqrt{2} = \zeta - \zeta^3 = (1 - \pi) - (1 - \pi)^3 = \pi^2 + \pi^3 + \pi^5 - \pi^2 \pi^{10}$$

$$\text{d'où : } 4\sqrt{2} \equiv \pi^{10} + \pi^{11} + \pi^{13} + \pi^{14} + \pi^{16} \pmod{\pi^{17}} .$$

Posons : $\sqrt{113} = u + k\pi^{17}$.

On a :

$$(\sqrt{113} - u)(\sqrt{113} + u) = 113 - u^2 = k' \cdot \pi^{21} .$$

On a :

$$113 = 1 + \pi^{16} + \pi^{20} \pmod{\pi^{21}} .$$

On trouve deux choix possibles pour $u \pmod{\pi^{17}}$, correspondant aux deux racines carrées de 113, en résolvant la congruence :

$$u^2 \equiv \left[1 + \sum_{i=1}^{16} s_i \pi^i \right]^2 \equiv 1 + \pi^{16} + \pi^{20} \pmod{\pi^{21}} .$$

On choisit la plus simple des solutions :

$$\sqrt{113} \equiv 1 + \pi^{12} + \pi^{14} \pmod{\pi^{17}} .$$

On a alors :

$$\alpha = \sigma_1(\alpha) \equiv 1 + \pi^{10} + \pi^{11} + \pi^{12} + \pi^{13} + \pi^{16} \pmod{\pi^{17}}$$

$$\sigma_2(\alpha) = -\sqrt{113} + 4\sqrt{2} = -\alpha + 8\sqrt{2} = \zeta^4 \alpha + 8\sqrt{2} .$$

$$\text{Soit : } \sigma_2(\alpha) \equiv \zeta^4 \alpha \pmod{\pi^{17}} .$$

On en déduit que les congruences : $\sigma_i(\alpha) \equiv X^2 \pmod{\pi^9}$ sont solubles (pour $i = 1, 2$) avec $X = 1$.

On vérifie que $\alpha \equiv X^4 \pmod{\pi^{12}}$ est soluble avec :

$$X = 1 + s\pi^2 + \pi^3 + \lambda \cdot \pi^4 \quad (s = 0 \text{ ou } 1, \lambda \text{ entier de } \hat{K}_p) .$$

On en déduit que la congruence $\alpha \equiv X^4 \pmod{\pi^{13}}$ est insoluble, ainsi que la congruence $\sigma_2(\alpha) \equiv X^4 \pmod{\pi^{13}}$. On a donc :

$$g_{p_1}(L) = g_{p_2}(L) = 2 .$$

Le calcul d'un élément $\beta \in K$ tel que $\hat{L}_p = \hat{K}_p(\sqrt[4]{\beta})$ n'est en fait

pas utile ici pour la détermination de $e_p(L)$.

On peut cependant vérifier que l'élément :

$$\beta = 1 + \pi^6 + \pi^7 + \pi^8 + \pi^{11} + \pi^{12}$$

est tel que :

$$\alpha \equiv \beta^2 \pmod{\pi^{17}} .$$

On a donc : $\widehat{L}_p = \widehat{K}_p(\sqrt[4]{\beta})$ avec $[\widehat{L}_p : \widehat{K}_p] = 4$.

2^e cas : $p = 3$.

On prend ici $\widehat{K} = \mathbb{Q}_3(\sqrt{113}, \sqrt{2}, i)$.

Dans ce cas et dans les cas suivants , p est impair . Pour d premier avec p on utilisera , pour déterminer si d est , ou non , reste quadratique mod p les règles de calcul du symbole de Legendre (défini par :

$$\left(\frac{d}{p}\right) = +1 \text{ si } d \text{ est reste quadratique modulo } p \text{ et par } \left(\frac{d}{p}\right) = -1 \text{ sinon} .$$

D'après des résultats classiques , ou encore d'après le corollaire II.1 , on en déduit que \sqrt{d} est ou non un élément de \mathbb{Q}_p .

$$\text{Pour } p = 3 , \text{ on a : } \left(\frac{-1}{3}\right) = \left(\frac{2}{3}\right) = \left(\frac{113}{3}\right) = -1$$

$$\text{d'où : } \left(\frac{-2}{3}\right) = \left(\frac{-113}{3}\right) = 1 .$$

On a donc : $i \notin \mathbb{Q}_3$; $i\sqrt{2} \in \mathbb{Q}_3$; $i\sqrt{113} \in \mathbb{Q}_3$

et : $\widehat{K} = \mathbb{Q}_3(i)$.

L'élément $\theta = \sqrt{113} + \sqrt{2} + i$ est donc de degré 2 sur \mathbb{Q}_3 .

Les 8 conjugués de θ par rapport à \mathbb{Q} sont deux à deux conjugués par rapport à \mathbb{Q}_3 . Il y a donc 4 idéaux de K au-dessus de 3 , et les 4 complétions (\widehat{K}, σ_i) de K correspondantes peuvent être définies par les plongements

σ_i ci-dessous :

$$\sigma_1: \begin{cases} \sqrt{113} \rightarrow \sqrt{113} \\ \sqrt{2} \rightarrow \sqrt{2} \\ i \rightarrow i \end{cases} \quad \sigma_2: \begin{cases} \sqrt{113} \rightarrow -\sqrt{113} \\ \sqrt{2} \rightarrow -\sqrt{2} \\ i \rightarrow i \end{cases} \quad \sigma_3: \begin{cases} \sqrt{113} \rightarrow \sqrt{113} \\ \sqrt{2} \rightarrow -\sqrt{2} \\ i \rightarrow i \end{cases} \quad \sigma_4: \begin{cases} \sqrt{113} \rightarrow -\sqrt{113} \\ \sqrt{2} \rightarrow \sqrt{2} \\ i \rightarrow i \end{cases}$$

D'autre part , 3 est uniformisante de $\mathbb{Q}_3(i)$; le corps rési-

duel de $\mathbb{Q}_3(i)$ ayant 9 éléments, $\mathbb{Q}_3(i)$ contient les racines 8^{eme} de 1 (Soit ζ une racine primitive 8^{eme} de 1 dans $\mathbb{Q}_3(i)$). Les entiers de $\mathbb{Q}_3(i)$ s'écrivent de manière unique $\sum_{i \in \mathbb{N}} s_i 3^i$ avec $s_i = 0$ ou s_i racine 8^{eme} de 1. (développement 3-adique).

On vérifie que l'on peut prendre $i = \zeta^2$
 $2 = -1 + 3$, d'où $\sqrt{2} \equiv \zeta^2 \pmod{3}$ et $4\sqrt{2} \equiv \zeta^2 \pmod{3}$
 $113 = -1 + 3 \cdot 38$, d'où $\sqrt{113} \equiv \zeta^2 \pmod{3}$.
 D'où $\alpha = \sigma_1(\alpha) = -\sigma_2(\alpha) \equiv \zeta^6 \pmod{3}$
 $\sigma_3(\alpha) = -\sigma_4(\alpha) \equiv 0 \pmod{3}$.

Un calcul plus précis des développements 3-adiques de $\sqrt{2}$ et $\sqrt{113}$ montre que l'on a :

$$\sigma_3(\alpha) = -\sigma_4(\alpha) \equiv \zeta^2 \cdot 3^4 \pmod{3^5}.$$

+ Pour \mathfrak{p}_1 et \mathfrak{p}_2 , idéaux de K associés à σ_1 et σ_2 ($\sigma_i^{-1}((3)) = \mathfrak{p}_i$) on a :

$$v_{\mathfrak{p}_i}(\alpha) = 0, \quad v_{\mathfrak{p}_i}(2) = 0 \quad \text{pour } i = 1, 2.$$

D'après la proposition II.2, $g_{\mathfrak{p}_i}(L)$ est le plus grand des diviseurs m de 8 tels que l'on ait :

$$(1) \quad \sigma_i(\alpha) \equiv X^m \pmod{\hat{\mathfrak{p}} = (3)}.$$

Les éléments ζ^6 et $-\zeta^6 = \zeta^2$ sont des carrés de \hat{K} , mais ne sont pas congrus modulo 3, à des puissances 4^{eme} de K . Les congruences (1) sont donc solubles pour $m = 2$ et insolubles pour $m = 4$.

On a donc :

$$g_{\mathfrak{p}_1}(L) = g_{\mathfrak{p}_2}(L) = 2.$$

+ Pour les idéaux \mathfrak{p}_3 et \mathfrak{p}_4 de K , associés à σ_3 et σ_4 , on a :

$$v_{\mathfrak{p}_i}(\alpha) = 4, \quad v_{\mathfrak{p}_i}(2) = 0 \quad (i = 3, 4).$$

D'après la proposition II.2, $g_{\mathfrak{p}_i}(L)$ est donc le plus grand des diviseurs

m de 8 tels que l'on ait :

$$(2) \quad \sigma_i(\alpha) \equiv X^m \pmod{3^5} .$$

Les congruences :

$$\zeta^2 \cdot 3^4 \equiv X^m \pmod{3^5}$$

$$\zeta^6 \cdot 3 \equiv X^m \pmod{3^5}$$

sont solubles pour $m = 2$ et insolubles pour $m = 4$.

On a donc encore :

$$g_{p_3}(L) = g_{p_4}(L) = 2 .$$

3^e cas : $p \neq 2$ et $p \neq 3$.

Dans ce cas on a toujours $v_p(\alpha) = 0$ (car $\alpha \cdot (\sqrt{113} - 4\sqrt{2}) = 3^4$) et $v_p(2) = 0$, donc $g_p(L)$ est le plus grand des diviseurs de m de 8 tels que l'on ait :

$$\alpha \equiv X^m \pmod{p} .$$

Par des méthodes analogues aux précédentes on détermine les plongements $\sigma_i(\alpha)$ de α dans $\widehat{K} = \mathbb{Q}_p(\sqrt{113}, \sqrt{2}, i)$, modulo \widehat{p} .

Pour $p \neq 113$ on a $\widehat{p} = (p)$

Pour $p = 113$ on a $\widehat{p} = (\sqrt{113})$.

Donnons des exemples de résultats :

+ pour $p = 113$, il y a 4 idéaux de K au-dessus de 113 et on a $g_p(L) = 2$ pour chacun d'eux .

+ pour $p = 5$, il y a encore 4 idéaux de K au-dessus de 5 et on a pour chacun d'eux $g_p(L) = 1$.

+ pour $p = 41$, il y a 8 idéaux de K au-dessus de 41 et on a pour chacun d'eux $g_p(L) = 1$.

III Détermination de l'indice de ramification .

1°) La ramification de \mathfrak{p} dans $K(\sqrt[N]{\alpha})$ lorsque \mathfrak{p} ne divise pas $N.A_K$, ou lorsque $v_{\mathfrak{p}}(\alpha) \not\equiv 0 \pmod{N}$.

Ces cas se traitent directement - sans passer à l'extension locale et sans supposer N de la forme l^n avec l premier - Les deux propositions suivantes reprennent les résultats de [4] page 92 - (La Proposition III.2 est cependant plus précise) .

Proposition III.1 .

Si $\mathfrak{p} \nmid N.A_K$ et si $v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod{N}$, \mathfrak{p} est non ramifié dans $L = K(\sqrt[N]{\alpha})$.

Démonstration :

D'après le lemme II.5 on peut supposer que l'on a $v_{\mathfrak{p}}(\alpha) = 0$, le discriminant de L/K divise le discriminant $N^N \cdot \alpha^{N-1}$ des nombres $\{1, \sqrt[N]{\alpha}, \dots, \sqrt[N]{\alpha}^{N-1}\}$; il est donc premier avec \mathfrak{p} ($v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(N) = 0$) .

Proposition III.2 .

Soit d le PGCD positif de $v_{\mathfrak{p}}(\alpha)$ et de N ; $e_{\mathfrak{p}}(L)$ est le produit de $\frac{N}{d}$ par l'indice de ramification de \mathfrak{p} dans $K(\sqrt[d]{\alpha})$.

En particulier , $e_{\mathfrak{p}}(L) = \frac{N}{d}$ si $\mathfrak{p} \nmid d.A_K$.

Démonstration :

D'après le lemme II.5 on peut supposer que l'on a : soit $v_{\mathfrak{p}}(\alpha) = d$ si $d \neq N$, soit $v_{\mathfrak{p}}(\alpha) = 0$ si $d = N$. Dans ce dernier cas la proposition est triviale .

Supposons donc $v_{\mathfrak{p}}(\alpha) = d$ avec d diviseur strict de N .

Soit θ une racine N^{eme} de α dans $L = K(\sqrt[N]{\alpha})$ et $v_{\mathfrak{p}}$ une valuation de L prolongeant $v_{\mathfrak{p}}$. On a :

$$N \cdot v_{\mathfrak{p}}(\Theta) = v_{\mathfrak{p}}(\alpha) = e_{\mathfrak{p}}(L) \cdot v_{\mathfrak{p}}(\alpha) = e_{\mathfrak{p}}(L) \cdot d$$

D'où :

$$e_{\mathfrak{p}}(L) = \frac{N}{d} v_{\mathfrak{p}}(\Theta) > 1 \quad \text{car} \quad \frac{N}{d} \in \mathbb{N} \quad \text{et} \quad \frac{N}{d} > 1.$$

D'autre part, soit $K_{\mathfrak{T}}$ le corps d'inertie de \mathfrak{p} dans L/K ;
 L/K étant cyclique, $K_{\mathfrak{T}}$ est l'unique sous-corps de L de degré $n = \frac{N}{e_{\mathfrak{p}}(L)}$

par rapport à K ; on a donc

$$K_{\mathfrak{T}} = K(\sqrt[n]{\alpha}).$$

D'après ce qui précède n divise d ; on a donc :

$$\underbrace{K \subset K_{\mathfrak{T}}}_{\text{non ramifié}} \subset \underbrace{K(\sqrt[d]{\alpha})}_{\text{totalement ramifié}} \subset L$$

L'extension $L / K(\sqrt[d]{\alpha})$ est donc totalement ramifiée en tout idéal au-dessus de \mathfrak{p} , d'où le résultat énoncé.

Dans le cas particulier où $\mathfrak{p} \nmid d \cdot A_K$, on applique la proposition III.1 à l'extension $K(\sqrt[d]{\alpha})$. On a donc bien $e_{\mathfrak{p}}(L) = \frac{N}{d}$.

Remarque : Les deux propositions précédentes permettent de se ramener à l'étude de la ramification de \mathfrak{p} dans $K(\sqrt[d]{\alpha})$ avec \mathfrak{p} divisant $d \cdot A_K$ et $v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod{d}$. De plus d'après les remarques faites au § I.3°, et d'après la proposition III.1, l'indice de ramification de \mathfrak{p} dans $K(\sqrt[d]{\alpha})$ est égal à l'indice de ramification de \mathfrak{p} dans $K(\sqrt[p^m]{\alpha})$ avec p nombre premier de \mathbb{N} au-dessous de \mathfrak{p} et $d = p^m \cdot d'$ (avec $(d', p) = 1$).

2°) La ramification de \mathfrak{p} dans $K(\sqrt[p^m]{\alpha})$ lorsque \mathfrak{p} divise $p \cdot A_K$ et $v_{\mathfrak{p}}(\alpha) \equiv 0 \pmod{p^m}$.

a) cas local :

On considère ici un corps k , complet pour une valuation discrète v , dont le corps résiduel est de caractéristique $p \neq 0$. On suppose que k contient les racines $(p^n)^{\text{eme}}$ de 1. Dans la suite on prendra pour k , le complété $\widehat{K}_{\mathfrak{p}}$ de K (si K lui-même n'est pas complet).

Soit ζ_h une racine $(p^h)^{\text{eme}}$ de 1 (contenue dans k pour $1 \leq h \leq n$). On rappelle que l'on a :

$$v(1 - \zeta_h) = \frac{v(p)}{\varphi(p^h)} = \frac{v(p)}{p^{h-1}(p-1)}$$

(φ est la fonction d'Euler).

Soit k_n une extension cyclique de k de degré p^n .

On note v_n la valuation de k_n prolongeant v , \mathfrak{p}_n et \mathfrak{p} les idéaux premiers (uniques) de l'anneau de valuation de k_n et de k (on a ici $g_{\mathfrak{p}}(k_n) = 1$).

On suppose que l'extension résiduelle \bar{k}_n / \bar{k} est séparable.

Soit Δ l'ensemble des $\gamma \in k$ tels que l'on ait :

$$k_n = k(\sqrt[p^n]{\gamma}) . \text{ On suppose que l'on a pour } \gamma \in \Delta, \quad v(\gamma) \equiv 0 \pmod{p^n} .$$

D'après le lemme II.5, il existe $\gamma \in \Delta$ tel que l'on ait $v(\gamma) = 0$.

D'autre part, γ n'appartient pas à k^p (car $[k(\sqrt[p^n]{\gamma}) : k] = p^n$).

On déduit donc du corollaire II.3 que pour les éléments γ de Δ tels que $v(\gamma) = 0$, la congruence :

$$\gamma \equiv X^p \pmod{\mathfrak{p}^{1+a_1}}$$

n'a pas de solution dans k ,

$$\text{avec } a_1 = a(p) = \frac{v(p)}{p-1} + v(p) = p \cdot \frac{v(p)}{p-1} .$$

Le lemme suivant précise le choix de $\gamma \in \Delta$ tel que $k_n = k(\sqrt[p^n]{\gamma})$.

Lemme III.1.

Soit Δ_0 l'ensemble des $\gamma \in k$ tels que $v(\gamma) = 0$ et $k_n = k(\sqrt[p^n]{\gamma})$. Soit λ_n le sup des $v(\gamma - 1)$ pour $\gamma \in \Delta_0$.

(1) On a $\lambda_n \leq a_1$, et il existe $\beta \in \Delta_0$ tel que l'on ait : $\beta \equiv 1 \pmod{\mathfrak{p}^{\lambda_n}}$.

(2) Quel que soit $\gamma \in \Delta_0$, λ_n est le sup des λ tels que la con-

.../...

.../...

gruence $\gamma \equiv X^{p^n} \pmod{p^\lambda}$ ait une solution dans k .

(3) On a $\lambda_n \geq 1$.

Démonstration :

+ On a vu que la congruence :

$$\gamma \equiv X^p \pmod{p^{1+a_1}}$$

n'a pas de solution pour $\gamma \in \Delta_0$, on a donc bien $\lambda_n \leq a_1$ et λ_n est fini. Il existe donc $\beta \in \Delta_0$ tel que :

$$v(\beta - 1) = \lambda_n.$$

+ Soit $\gamma \in \Delta_0$, il existe $x' \in k$ tel que :

$$\gamma = x'^{p^n} \cdot \beta^i \quad \text{avec } (p, i) = 1.$$

D'après le choix de β , β appartient à $U^{(\lambda_n)} = 1 + (p)^{\lambda_n}$.

On déduit de la proposition II.1 que l'on a aussi $\beta^i \in U^{(\lambda_n)}$ d'où :

$$\gamma \equiv x'^{p^n} \pmod{p^{\lambda_n}}.$$

+ Si l'on avait : $\gamma \equiv y^{p^n} \pmod{p^{1+\lambda_n}}$, on aurait :

$$v(y) = 0 \text{ et } \gamma = y^{p^n} \cdot \xi \quad \text{avec } \xi \in U^{(1+\lambda_n)}.$$

On aurait alors $\xi \in \Delta_0$ et $v(\xi - 1) > \lambda_n$, ce qui est en contradiction avec la définition de λ_n .

+ Vérifions que l'on a $\lambda_n \geq 1$. Cela est une conséquence de la séparabilité de l'extension \bar{k}_n / \bar{k} . En effet, si la congruence

$$\gamma \equiv X^{p^n} \pmod{p}$$

était insoluble (avec $\gamma \in \Delta_0$) le polynome $X^{p^n} - \gamma$ n'aurait pas de racines dans \bar{k} et l'extension $\bar{k}(\sqrt[p^n]{\gamma}) / \bar{k}$ (qui est contenue dans l'extension \bar{k}_n / \bar{k}) serait purement inséparable.

Le lemme suivant précise le lien entre la valuation de $x-1$ et celle de $(\sqrt[p^n]{x} - 1)$ pour certains x de k .

Lemme III.2 .

Soit $x \in k$ tel que $v(x-1) \leq a_1$ et tel que les racines de $X^{p^n} - x$ soient dans k_n ($x \neq 1$).

(1) pour tout $\theta \in k_n$ tel que $\theta^{p^n} = x$, on a :

$$v(x-1) = p^n \cdot v_n(\theta-1)$$

(2) Soit $y \in k_n$ tel que $v_n(y-1) > v_n(\theta-1)$, on a alors :

$$v_n(y^{p^n}-1) > v_n(x-1) .$$

Démonstration :

Soit ζ_n une racine primitive $(p^n)^{\text{eme}}$ de 1 .

$$\text{On a : } x-1 = \theta^{p^n}-1 = \prod_{i=0}^{p^n-1} (\theta - \zeta_n^i) = \prod_{i=0}^{p^n-1} [(\theta-1) + (1 - \zeta_n^i)]$$

$$v_n [(\theta-1) + (1 - \zeta_n^i)] \begin{cases} = \inf [v_n(\theta-1), v_n(1 - \zeta_n^i)] ; & \text{si } v_n(\theta-1) \neq v_n(1 - \zeta_n^i) \\ \geq \inf [v_n(\theta-1), v_n(1 - \zeta_n^i)] ; & \text{si } v_n(\theta-1) = v_n(1 - \zeta_n^i) \end{cases}$$

L'hypothèse $v(x-1) \leq a_1$ implique :

$$v_n(\theta-1) \leq \frac{v_n(p)}{\varphi(p^n)} \leq v_n(1 - \zeta_n^i) .$$

On en déduit alors (en distinguant les cas $v_n(\theta-1) < \frac{v_n(p)}{\varphi(p^n)}$ et

$$v_n(\theta-1) = \frac{v_n(p)}{\varphi(p^n)}) \text{ que la relation (1) est vraie .}$$

Soit alors $y \in k_n$ tel que $v_n(y-1) > v_n(\theta-1)$.

Soit $v_n(y-1) < \frac{v_n(p)}{\varphi(p^n)}$, on a alors, d'après (1) :

$$v_n(y^{p^n}-1) = p^n \cdot v_n(y-1) > v_n(x-1) .$$

Si $v_n(y-1) > \frac{v_n(p)}{\varphi(p^n)}$, on a alors en reprenant le calcul initial :

$$v_n(y^{p^n}-1) > p \cdot \frac{v_n(p)}{p-1} \geq v_n(x-1) .$$

Remarque : une étude plus générale de $v_n(\theta^{p^n}-1)$ en fonction de $v_n(\theta-1)$ peut être faite par des méthodes analogues mais n'est pas utile ici .

Lemme III.3 .

Soit $\beta \in k$ tel que $k_n = k(\sqrt[p^n]{\beta})$ et tel que $v(\beta-1) = \lambda_n$,
 (λ_n est défini dans le lemme III.1) .

Soit θ une racine de $X^{p^n} - \beta$ dans k_n et $e = e_p(k_n)$,
 l'indice de ramification de p dans k_n . Si $v_n(\theta-1)$ est multiple de e ,
 ($v_n(\theta-1) = e \cdot \mu'$) et si π_0 est une uniformisante de k , on a :
 $\theta = 1 + \eta \pi_0^{\mu'}$. Alors $\bar{\eta}$ n'appartient pas à \bar{k} et le degré résiduel $f_p(k_n)$
 est multiple de p .

Démonstration :

Soient π_0 et π_n des uniformisantes de k et de k_n .

On a : $\pi_0 = \varepsilon \cdot \pi_n^e$ avec ε unité de k_n .

Si $v_n(\theta-1) = e \cdot \mu'$, on a :

$$\theta = 1 + \eta' \pi_n^{e\mu'} = 1 + \eta' (\varepsilon^{-1} \pi_0)^{\mu'}$$

c'est-à-dire : $\theta = 1 + \eta \pi_0^{\mu'}$ avec η unité de k_n .

Supposons que l'on ait : $\bar{\eta} \in \bar{k}$; alors il existe une unité a de k et un
 entier b de k_n tel que l'on ait :

$$\eta = a + b \pi_0 .$$

D'où : $\theta = [1 + a \pi_0^{\mu'}] \cdot [1 + \frac{b}{1 + a \pi_0^{\mu'}} \cdot \pi_0^{1+\mu'}]$.

Posons : $x = 1 + a \pi_0^{\mu'}$.

On a $x \in k$ et $v(x) = 0$.

Posons : $\theta' = 1 + \frac{b}{1 + a\pi_0^{\mu'}} \cdot \prod_0^{1+\mu'}$.

On a $v_n(\theta') = 0$ et $\beta = \theta^{p^n} = x^{p^n} \cdot \theta'^{p^n}$.

Donc $\beta' = \theta'^{p^n}$ appartient à k avec $v(\beta') = 0$ et

$$k_n = k(\sqrt[p^n]{\beta'}) .$$

On a :

$$v_n(\theta' - 1) \geq e \cdot (\mu' + 1) > e \cdot \mu' = v_n(\theta - 1) .$$

D'après le lemme III.2 (partie 2), on a donc :

$$v(\beta' - 1) > v(\beta - 1) .$$

Ceci est en contradiction avec le choix de β (lemme III.1).

On a donc $\bar{\eta} \notin \bar{k}$ donc $f_p(k_n) = [\bar{k}_n : \bar{k}] > 1$.

Lemme III.4 .

Les hypothèses et les notations sont celles du lemme III.1 .

Si k_n/k est non ramifié de degré p^n , on a nécessairement : $\lambda_n = a_1$.

Démonstration :

Soit $\beta \in k$ tel que $k_n = k(\sqrt[p^n]{\beta})$ avec $v(\beta - 1) = \lambda_n$.

Soit θ une racine $(p^n)^{\text{ème}}$ de β . Si k_n/k est non ramifié,

le lemme III.3 s'applique et on a :

$$\theta = 1 + \eta \pi_0^\mu \text{ avec } \bar{\eta} \notin \bar{k} , \pi_0 = \pi_n .$$

D'autre part, d'après le lemme III.2, on a :

$$v_n(\beta - 1) = p^n \cdot v_n(\theta - 1) = p^n \cdot \mu .$$

Comme $v(\beta - 1) = \lambda_n$, on a $\lambda_n = p^n \cdot \mu$.

Nous allons montrer que, pour $\lambda_n < a_1$, $\bar{\eta}$ est racine d'un polynôme de la forme $X^{p^n} - \bar{\xi}$ (avec $\bar{\xi} \neq 0$), alors que pour $\lambda_n = a_1$, $\bar{\eta}$ est

racine d'un polynome de la forme $X^{p^n} + \bar{C}_{p^{n-1}} X^{p^{n-1}} + \bar{\varepsilon}$ (avec $\bar{C}_{p^{n-1}}$ et $\bar{\varepsilon}$ non nuls). La première éventualité est incompatible avec le fait que $\bar{k}(\bar{\eta})/\bar{k}$, sous-extension de degré $\neq 1$ de \bar{k}_n/\bar{k} , soit séparable. On a donc nécessairement $\lambda_n = a_1$.

Posons : $\beta = 1 + \varepsilon \pi_0^{\lambda_n}$ (avec ε unité de k).

η est racine de l'équation :

$$1 + \varepsilon \pi_0^{\lambda_n} = (1 + \eta \pi_0^\mu)^{p^n}$$

ou encore :

$$(1) \quad \varepsilon \pi_0^{\lambda_n} = \sum_{i=1}^{p^n} C_{p^n}^i \cdot (\eta \pi_0^\mu)^i$$

Posons, pour $i \in \{1, \dots, p^n\}$, $i = p^t \cdot i'$ (avec $(p, i') = 1$).

On vérifie que le coefficient binomial $C_{p^n}^i$ est alors divisible "exactement" par p^{n-t} . On peut donc poser :

$$C_{p^n}^i = C_i \cdot \pi_0^{(n-t) \cdot v(p)} \quad \text{avec } C_i \text{ unité de } k.$$

D'où :

$$\sum_{i=1}^{p^n} C_{p^n}^i \cdot (\eta \pi_0^\mu)^i = \left\{ \sum_{t=0}^{n-1} \left[\sum_{\substack{p^t/i \\ p^{t+1}/i}} \pi_0^{(n-t)v(p)} \cdot C_i \cdot (\eta \pi_0^\mu)^i \right] \right\} + (\eta \pi_0^\mu)^{p^n}.$$

On remarque que $\sqrt[p^t]{p}$ est le plus petit des entiers i tels que l'on ait : p^t/i et $p \nmid i$.

On a donc :

$$(1') \quad \varepsilon \pi_0^{p \cdot \mu} = \left\{ \sum_{t=0}^{n-1} \pi_0^{(n-t) \cdot v(p) + p^t \cdot \mu} \cdot \left[C_{p^t} \cdot \eta^{p^t} + \eta \pi_0^\mu \cdot f_t(\eta \pi_0^\mu) \right] \right\} + (\eta \pi_0^\mu)^{p^n}$$

avec, f_t , polynome dont les coefficients sont des unités de k

$$f_t(X) = \sum_{\substack{i \geq 1+p^t \\ p^t/i \text{ et } p^{t+1}/i}} C_i \cdot X^{i-p^t-1} .$$

On vérifie que pour $\lambda_n < a_1$, c'est-à-dire $\mu < \frac{v(p)}{\varphi(p^n)}$, on a :

pour tout $t \in \{0, \dots, n-1\}$, $(n-t)v(p) + p^t\mu > p^n \cdot \mu$.

La relation (1') se réduit alors, après simplification par $\pi_0^{p^n \cdot \mu}$ à :

$$\xi \equiv \eta^{p^n} \pmod{\pi_0} .$$

(On utilise le fait que l'on a $\mu \neq 0$ car $\lambda_n \neq 0$ - lemme III.1) .

On a donc montré que pour $\lambda_n < a_1$, $\bar{\eta}$ est racine de $X^{p^n} - \bar{\xi}$.

Supposons maintenant $\lambda_n = a_1$, c'est-à-dire $\mu = \frac{v(p)}{\varphi(p^n)}$. On a :

pour $t = n-1$, $v(p) + p^{n-1} \cdot \mu = a_1 = p^n \cdot \mu$

pour $t \in \{0, \dots, n-2\}$, $(n-t) \cdot v(p) + p^t \cdot \mu > p^n \cdot \mu$.

Après simplification, la relation (1') se réduit donc à :

$$\xi \equiv \eta^{p^n} + C_{p^{n-1}} \cdot \eta^{p^{n-1}} \pmod{\pi_0}$$

ce qui prouve que, pour $\lambda_n = a_1$, $\bar{\eta}$ est racine du polynome $X^{p^n} + \bar{C}_{p^{n-1}} X^{p^{n-1}} - \bar{\xi}$ (avec $\bar{C}_{p^{n-1}}$ et $\bar{\xi}$ non nuls) .

Proposition III.5 .

Soit k un corps de caractéristique 0, complet pour une valuation discrète v . Soit \mathfrak{p} l'idéal premier de l'anneau des entiers de k pour v . On suppose que le corps résiduel \bar{k} est de caractéristique $p \neq 0$ et que k contient les racines $(p^n)^{\text{eme}}$ de 1. Soit $\beta \in k$ tel que $v(\beta) = 0$.

Soit $k_n = k(\sqrt[p^n]{\beta})$. On suppose l'extension résiduelle \bar{k}_n/\bar{k} séparable.

On pose $a_1 = p \cdot \frac{v(p)}{p-1}$.

(1) k_n/k est de degré p^n si et seulement si la congruence

$$\beta \equiv X^p \pmod{p^{1+a_1}}$$

est insoluble dans k .

(2) $k(\sqrt[p]{\beta})/k$ est une extension non ramifiée si et seulement si la congruence :

$$\beta \equiv X^p \pmod{p^{a_1}}$$

a une solution dans k .

(3) Soit s le plus grand des $h \in \{0, \dots, n\}$ tels que la congruence :

$$\beta \equiv X^{p^h} \pmod{p^{a_1}}$$

ait une solution dans k ; alors, l'indice de ramification $e_p(k_n)$ de l'extension k_n/k est le produit de p^{n-s} par l'indice de ramification de l'extension $k(\sqrt[p^s]{\beta})/k$.

Pour $s \geq 1$, $f_p(k_n)$ est multiple de p .

Remarques :

+ Cette proposition permet de déterminer complètement la ramification de l'extension k_n/k dans les cas $s = 0$ ou $s = 1$ seulement. Pour $s > 1$, des exemples numériques peuvent montrer que $e_p(k_n)$ peut varier de p^{n-s} à p^{n-1} .

+ Les parties (1) et (2) de cette proposition correspondent au théorème de Hecke ([1] § 39 Satz 119).

Démonstration :

La partie (1) reprend les résultats du § II.

Partie (2) : Supposons que la congruence :

$$\beta \equiv X^p \pmod{p^\lambda}$$

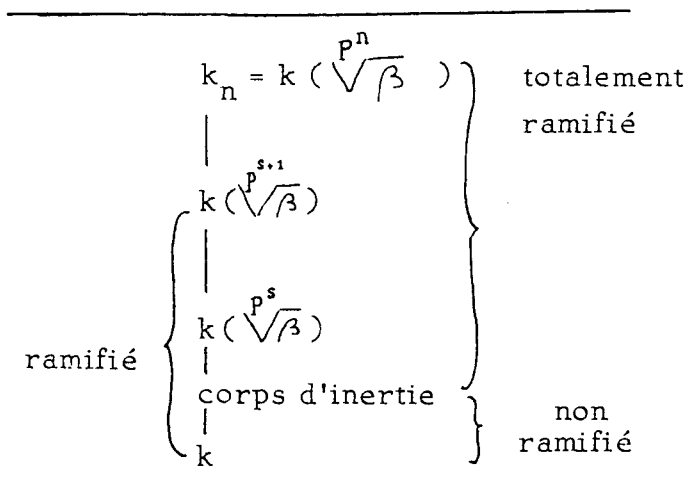
soit soluble dans k , pour $\lambda = a_1$; si elle est aussi soluble pour $\lambda = 1+a_1$, on a alors $k = k(\sqrt[p]{\beta})$ (l'extension $k(\sqrt[p]{\beta})/k$ est trivialement non ramifiée !). Supposons donc la congruence insoluble pour $\lambda = 1+a_1$ alors le

nombre λ_1 relatif à l'extension $k(\sqrt[p]{\beta})$ (défini dans le lemme III.1) est égal à a_1 et on peut supposer β choisi tel que : $v(\beta - 1) = a_1$. On a alors, pour toute racine $p^{\text{eme}} \theta$ de β , dans k_1 (lemme III.2) :

$$v_1(\theta - 1) = \frac{1}{p} \cdot v_1(\beta - 1) = \frac{v_1(p)}{p - 1} = e_p(k_1) \cdot \frac{v(p)}{p - 1} .$$

Le nombre $v_1(\theta - 1)$ est donc multiple de $e_p(k_1)$, et d'après le lemme III.3 , $f_p(k_1)$ est multiple de p . On a donc bien $e_p(k_1) = 1$ ($e_p(k_1) \cdot f_p(k_1) = p$) .

Partie (3) : Si le nombre s défini dans (3) vaut n , la proposition est triviale . Supposons donc $s < n$ ($s+1 \leq n$) ; le nombre λ_{s+1} relatif à l'extension $k(\sqrt[p^{s+1}]{\beta})$ est strictement inférieur à a_1 ($\beta \not\equiv X^{p^{s+1}} \pmod{p^{a_1}}$) .



On déduit alors du lemme III.4 que l'extension $k(\sqrt[p^{s+1}]{\beta})/k$ est ramifiée . L'extension k_n/k étant cyclique de degré p^s , son corps d'inertie est inclus dans $k(\sqrt[p^s]{\beta})$. L'extension $k(\sqrt[p^n]{\beta})/k(\sqrt[p^s]{\beta})$ est donc totalement ramifiée , et

$e_p(k_n)$ est bien le produit de p^{n-s} par l'indice de ramification de l'extension $k(\sqrt[p^s]{\beta})/k$.

D'autre part , pour $s \geq 1$, on déduit de la partie (2) que $k(\sqrt[p]{\beta})/k$ est non ramifié ; $f_p(k_n)$ est alors multiple de p .

b) cas " global " :

On reprend les notations et les hypothèses du § I , avec $N = p^m$ (p premier) , et \mathfrak{p} idéal premier de A_K au-dessus de p . On suppose que

l'on a $L = K(\sqrt[p^m]{\alpha})$ avec $v_p(\alpha) \equiv 0 \pmod{p^m}$, et $[L:K] = p^m$.

On a vu au § II le rôle joué par les nombres $a(m)$ pour la détermination de $g_p(L)$. Ici les diviseurs de p^m sont de la forme p^h ($h \in \{0, \dots, m\}$).

On pose alors :

$$a_h = a(p^h) = \frac{v_p(p)}{p-1} + h \cdot v_p(p).$$

On déduit alors des résultats du § II et de la proposition III.5, la proposition suivante qui résume tous les résultats obtenus, concernant la détermination de $e_p(L)$, $f_p(L)$, $g_p(L)$.

Proposition III.6 . Critère de détermination de $e_p(L)$, $f_p(L)$, $g_p(L)$.

Soit L une extension cyclique de K de degré p^m et \mathfrak{p} un idéal premier de A_K divisant p . On suppose que l'on a $L = K(\sqrt[p^m]{\alpha})$ avec $v_p(\alpha) = 0$.

Soit r le plus grand des $h \in \{0, \dots, m\}$ tels que la congruence :

$$\alpha \equiv X^{p^h} \pmod{\mathfrak{p}^{1+a_h}}$$

ait une solution $x \in K$ (avec $a_h = \frac{v_p(p)}{p-1} + h \cdot v_p(p)$).

(1) On a $g_p(L) = p^r$; et si $r = m$, $e_p(L) = f_p(L) = 1$.

(2) Si $r < m$ et si la congruence

$$\alpha \equiv X^{p^{1+r}} \pmod{\mathfrak{p}^{a_{1+r}}}$$

n'a pas de solution dans K , alors $e_p(L) = p^{m-r}$ et $f_p(L) = 1$.

(3) Si $r < m$ et si les congruences :

$$\alpha \equiv X^{p^h} \pmod{\mathfrak{p}^{a_{1+r}}}$$

ont une solution dans K pour $h \in \{r+1, \dots, r+s\}$, mais pas de solution pour $h > r+s$, alors $f_p(L)$ est multiple de p , et $e_p(L)$ est le produit de p^{m-r-s} par l'indice de ramification de \mathfrak{p} dans $K(\sqrt[p^{r+s}]{\alpha})$.

... / ...

En particulier si la congruence : $\alpha \equiv X^{p^m} \pmod{\mathfrak{p}^{a_1+r}}$ n'a pas de solution, on est sûr que \mathfrak{p} est ramifié, sinon on ne peut pas conclure sauf dans le cas $s = 1$ où l'on a $e_{\mathfrak{p}}(L) = p^{m-r-1}$ et $f_{\mathfrak{p}}(L) = p$.

Démonstration :

La partie (1) est l'expression de la proposition II.4 dans le cas étudié.

Partie (2) et (3) : il existe $\beta \in \widehat{K}_{\mathfrak{p}}$ tel que

$$\alpha = \beta^{p^r}.$$

D'après la définition de r , on a :

$$[\widehat{L}_{\mathfrak{p}} : \widehat{K}_{\mathfrak{p}}] = p^{m-r} \quad \text{et} \quad \widehat{L}_{\mathfrak{p}} = \widehat{K}_{\mathfrak{p}}(\sqrt[p^m]{\alpha}) = \widehat{K}_{\mathfrak{p}}(\sqrt[p^{m-r}]{\beta}).$$

$$\text{Posons : } p^n = p^{m-r} ; k = \widehat{K}_{\mathfrak{p}}, \widehat{L}_{\mathfrak{p}} = k_n.$$

On notera ici $\widehat{\mathfrak{p}}$ l'unique idéal premier de l'anneau de valuation de $\widehat{K}_{\mathfrak{p}}$.
(On a $e_{\widehat{\mathfrak{p}}}(k_n) = e_{\mathfrak{p}}(L)$, $f_{\widehat{\mathfrak{p}}}(k_n) = f_{\mathfrak{p}}(L)$).

On se place dans le cas $m > r$, c'est-à-dire $n \geq 1$, et on applique la proposition III.5 à l'extension k_n/k , en utilisant le lemme suivant :

Lemme .

Soit $h \geq 1$ tel que la congruence

$$\alpha \equiv X^{p^{h+r}} \pmod{\mathfrak{p}^{a_1+r}}$$

n'ait pas de solution dans K , alors la congruence

$$\beta \equiv X^{p^h} \pmod{\widehat{\mathfrak{p}}^{a_1}}$$

est insoluble dans k .

En effet si la congruence $\beta \equiv X^{p^h} \pmod{\widehat{\mathfrak{p}}^{a_1}}$ avait une solution dans k , elle ^{en}aurait aussi une dans K , et on aurait :

$$\beta = x^{p^h} \cdot y \quad \text{avec } y \in K, y \in 1 + (\widehat{\mathfrak{p}})^{a_1} = U^{(a_1)}$$

d'où :

$$\alpha = x^{p^{h+r}} \cdot y^{p^r} \text{ avec } y^{p^r} \in [U^{(a_1)}]^{p^r} \cap K .$$

D'après le corollaire II.2 (partie (2)), on a :

$$[U^{(a_1)}]^{p^r} \subset U^{(a_1 + r \cdot v(p))} .$$

D'autre part, on a : $a_{1+r} = a_1 + r \cdot v(p)$. On a donc :

$$y^{p^r} \equiv 1 \pmod{\mathfrak{p}^{a_{1+r}}} \text{ et } \alpha \equiv x^{p^{h+r}} \pmod{\mathfrak{p}^{a_{1+r}}} \text{ ce qui est absurde .}$$

Reprenons l'hypothèse de la partie (2) . D'après le lemme précédent et de la proposition III.5((2)), $k(\sqrt[p]{\beta})/k$ est ramifiée ; k_n/k est alors totalement ramifié, d'où :

$$e_{\mathfrak{p}}(L) = e_{\hat{\mathfrak{p}}}(k_n) = p^n = p^{m-r}$$

$$f_{\mathfrak{p}}(L) = f_{\hat{\mathfrak{p}}}(k_n) = 1 .$$

Dans la partie (3), on suppose qu'il existe $s \geq 1$ tel que la congruence :

$$\alpha \equiv X^{p^{h+r}} \pmod{\mathfrak{p}^{a_{1+r}}}$$

soit soluble pour $1 \leq h \leq s$, et insoluble pour $h > s$.

Si $r + s = m$, la propriété énoncée est triviale .

On suppose donc $m > r + s$. D'après le lemme (appliqué à $h = s + 1$), la congruence :

$$\beta \equiv X^{p^{s+1}} \pmod{\hat{\mathfrak{p}}^{a_1}}$$

est insoluble .

Montrons que la congruence : $\beta \equiv X^{p^s} \pmod{\hat{\mathfrak{p}}^{a_1}}$, est soluble .

$$\text{On a : } \alpha = x^{p^{s+r}} \cdot y, \text{ avec } y \equiv 1 \pmod{\mathfrak{p}^{a_{1+r}}} .$$

$$\text{Donc } y \in U^{(a_{1+r})} = 1 + \hat{\mathfrak{p}}^{a_{1+r}} .$$

On a : $a_{1+r} > a_r = a(p^r)$; on déduit du corollaire II.2 que l'on a :

$$U^{(a_{1+r})} = U^{(a_1 + r \cdot v(p))} = [U^{(a_1)}]^{p^r} .$$

Donc il existe $y' \in U^{(a_1)}$ tel que $y = y'^{p^r}$, d'où :

$$\alpha = \beta^{p^r} = (x^{p^s})^{p^r} \cdot y^{p^r}$$

d'où : $\beta \equiv X^{p^s} \pmod{\hat{p}^{a_1}}$.

D'après la partie (3) de la proposition III.5, l'indice de ramification $e_{\hat{p}}(k_n) = e_{\hat{p}}(L)$ est égal au produit de p^{n-s} ($= p^{m-r-s}$) par l'indice de ramification de l'extension $k(\sqrt[p^s]{\beta})/k$, c'est-à-dire par l'indice de ramification de \hat{p} dans $K(\sqrt[p^{s+r}]{\alpha})$. D'autre part on a supposé $s \geq 1$, on a donc bien $f_{\hat{p}}(k_n)$ (ou encore $f_{\hat{p}}(L)$), multiple de p .

Conclusion :

Il reste à déterminer l'indice de ramification $e_{\hat{p}}(k_s)$ de l'extension k_s/k avec k corps local et :

$$k_s = k(\sqrt[p^s]{\beta})$$

$$\beta \not\equiv X^p \pmod{\hat{p}^{1+a_1}}$$

$$\beta \equiv X^{p^s} \pmod{\hat{p}^{a_1}} \quad (s > 1)$$

La méthode consiste à étudier, en utilisant la proposition III.5 (partie (2)) la ramification des extensions intermédiaires de degré p $k(\sqrt[p^{h-1}]{\beta})/k(\sqrt[p^h]{\beta})$. On peut cependant éviter de faire des calculs dans les extensions intermédiaires si on connaît par ailleurs le développement π -adique d'un nombre p^s -primaire de k (éléments $\beta_s \in k$ tels que $k(\sqrt[p^s]{\beta_s})/k$ soit non ramifiée et de degré p^s).

En effet, on a supposé que le corps résiduel k admettait une extension cyclique séparable de degré p^n , (donc a fortiori de degré p^s avec $s \leq n$). On en déduit ([3] page 63), que k admet dans une clôture algébrique fixée, une et une seule extension k_s^{NR} non ramifiée et de degré p^s . (Lorsque \bar{k} est fini, et a p^f éléments, elle s'obtient en adjoignant à k les racines $(p^{sf} - 1)^{\text{eme}}$ de 1). Puisque k contient les racines $(p^s)^{\text{eme}}$ de 1, cette extension est de la forme $k(\sqrt[p^s]{\beta_s})$.

Considérons une sous-extension $k(\sqrt[p^h]{\beta})/k$ de l'extension k_s/k ($1 \leq h \leq s$). Pour qu'elle soit non ramifiée il faut et il suffit, (en vertu de l'unicité de l'extension non ramifiée de degré p^h du corps local k) que l'on ait :

$$k(\sqrt[p^h]{\beta}) = k(\sqrt[p^h]{\beta_s})$$

et le degré résiduel $f_p(k_s)$ est alors le plus grand des diviseurs p^h de p^s tels que l'on ait :

$$k(\sqrt[p^h]{\beta}) = k(\sqrt[p^h]{\beta_s}) .$$

D'un point de vue pratique, il faut vérifier par des résolutions de congruences (cf. corollaire II.3) que l'on a $\beta \cdot \beta_s^i \in (k)^{p^h}$ pour $i < p^h$, $(i, p) = 1$.

Dans le cas où \bar{k} est fini (avec p^f éléments) on peut prendre :

$$\beta_s = \langle \Theta, \chi \rangle^{p^s}$$

où Θ est une racine primitive $(p^{f \cdot p^s} - 1)^{\text{eme}}$ de 1 et χ un caractère complexe ($\neq 1$) du groupe de Galois G de k_s^{NR}/k (cyclique) et $\langle \Theta, \chi \rangle$ la résolvante de Lagrange associée ($\langle \Theta, \chi \rangle = \sum_{\sigma \in G} \chi(\sigma^{-1}) \Theta^\sigma$).

De manière générale les nombres p^n -primaires sont définis à partir des fonctions de Hasse- Chafarevitch ([5], [6]). Dans le cas où le corps de base est le corps obtenu en adjoignant à \mathbb{Q}_p , les racines $(p^n)^{\text{eme}}$ de 1, l'expression des nombres p^n primaires est relativement plus facile à obtenir, soit par des calculs directs, soit par [7].

2°) Exemple de détermination de l'indice de ramification.

On reprend l'exemple du § II, $K = \mathbb{Q}(\sqrt{113}, \sqrt{2}, i)$, $\alpha = \sqrt{113} + 4\sqrt{2}$, $L = K(\sqrt[8]{\alpha})$.

a) si p ne divise pas $6 A_K$: on a $v_p(\alpha) = 0$.

D'après la proposition III.1 on a donc $e_p(L) = 1$.

b) si p divise $3 A_K$: on a vu qu'il y a 4 idéaux premiers de A_K divisant 3 , et que l'on a :

$$v_{\mathfrak{p}_1}(\alpha) = v_{\mathfrak{p}_2}(\alpha) = 0 ; \quad v_{\mathfrak{p}_3}(\alpha) = v_{\mathfrak{p}_4}(\alpha) = 4 .$$

D'après la proposition III.1 , \mathfrak{p}_1 et \mathfrak{p}_2 sont non ramifiés dans L .

D'après la proposition III.2 \mathfrak{p}_3 et \mathfrak{p}_4 sont ramifiés dans L (et non ramifiés dans $K(\sqrt[4]{\alpha})$. On a donc $e_{\mathfrak{p}_3}(L) = e_{\mathfrak{p}_4}(L) = 2$.

c) si p divise $2 A_K$: on utilise la proposition III.6 .

On a vu (§ II) qu'il y avait 2 idéaux premiers \mathfrak{p}_1 et \mathfrak{p}_2 de A_K divisant 2 . On a considéré K comme un sous-corps de $\mathbb{Q}_2(\sqrt{2}, i) = K$ et on a pris comme uniformisante de K l'élément :

$$\pi = 1 - \frac{i+1}{2}$$

qui est aussi dans K .

On a vérifié que l'on a :

$$\alpha \equiv 1 + \pi^{10} + \pi^{11} + \pi^{12} + \pi^{13} + \pi^{16} \pmod{\pi^{17}} .$$

D'autre part les congruences

$$\begin{aligned} \alpha &\equiv X^{2^h} \pmod{\mathfrak{p}_1^\lambda} \\ \alpha &\equiv X^{2^h} \pmod{\mathfrak{p}_2^\lambda} \end{aligned}$$

sont équivalentes à :

$$\begin{aligned} \alpha = \sigma_1(\alpha) &\equiv X^{2^h} \pmod{\pi^\lambda} \\ \sigma_2(\alpha) &\equiv X^{2^h} \pmod{\pi^\lambda} \end{aligned}$$

avec $\sigma_2(\alpha) = -\sqrt{13} + 4\sqrt{2} \equiv 3^4 \pmod{\pi^{17}} .$

On a vérifié que l'on a :

$$(1) \quad \alpha \equiv x^4 \pmod{\pi^{a_2}} \quad \text{avec} \quad a_2 = 12$$

$$\text{et } x \equiv 1 + s\pi^2 + \pi^3 \pmod{\pi^4}$$

$$s = 0 \text{ ou } 1$$

$$(2) \quad \alpha \not\equiv X^4 \pmod{\pi^{1+a_2}}$$

d'où $g_{\mathfrak{p}_i}(L) = 2$.

On vérifie immédiatement que $1+s\pi^2 + \pi^3 + \pi^4$ ne peut être congru à un carré modulo π^{12} on a donc :

$$\alpha \not\equiv X^8 \pmod{\pi^{a_2}} \text{ d'où } \alpha \equiv X^8 \pmod{\mathfrak{p}_i^{a_2}} \quad (i = 1, 2) .$$

On est dans le cas où la proposition III.6 permet de conclure . On a donc $e_{\mathfrak{p}_i}(L) = f_{\mathfrak{p}_i}(L) = g_{\mathfrak{p}_i}(L) = 2$ (pour $i = 1, 2$) .

Remarque : L'extension $K(\sqrt[4]{\alpha}) / K$ est non ramifiée pour tous les idéaux, l'extension $K(\sqrt[8]{\alpha}) / K$ n'est ramifiée que pour les deux idéaux de A_K divisant 2 .

Références :

- [1] Hecke : Vorlesungen über die Theorie der Algebraischen Zahlen (Akademische Verlag , Leipzig , 1923) .
- [2] Lang S. : Algebra (Addison-Wesley 1965) .
- [3] Serre J.P. : Corps locaux (Hermann 1962) .
- [4] Cassels-Fröhlich : Algebraic Number Theory (Academic Press 1967) .
- [5] Hasse H. : Die Gruppe der p^n -primären Zahlen für einen Primteiler von p (Journal de Crelle 176 1936) .
- [6] Hasse H. : Zur Arbeit von I.R. Safarevic über das allgemeine Reziprozitätsgesetz (Math. Nachr., Berlin 5 , 301-327 1951) .
- [7] Ullom S. : Integral representations afforded by ambiguous ideals in some abelian extensions . (Journal of Number Theory 6 32-49 1974) .