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 $(\hat{K}_{\mathfrak{p}}, \sigma_{\mathfrak{p}})$ 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 $\hat{K}_{\mathfrak{p}}$, à l'aide du plongement $\sigma_{\mathfrak{p}}$ de K dans $\hat{K}_{\mathfrak{p}}$. On sait ([2] , page 218) qu'il existe $\alpha \in K$ tel que L soit égal à $K(\sqrt[N]{\alpha})$.
On a alors $\alpha \in \hat{K}_{\mathfrak{p}}$, et le corps $\hat{K}_{\mathfrak{p}}(\sqrt[N]{\alpha})$ est un complété $\hat{L}_{\mathfrak{P}}$ 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 $\bar{K}_{\mathfrak{p}}$ et $\bar{L}_{\mathfrak{P}}$, les corps résiduels de $\hat{K}_{\mathfrak{p}}$ et $\hat{L}_{\mathfrak{P}}$.
On suppose que $\bar{K}_{\mathfrak{p}}$ est de caractéristique $p \neq 0$. On a besoin , pour la

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

2°) Réduction à une étude locale .

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

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

de 1 . On a donc : $g_{\mathfrak{p}}(L) = N''$.

On donne au § II , un critère de calcul de $g_{\mathfrak{p}}(L)$ basé sur des résolutions de congruences .

Les nombres $e_{\mathfrak{p}}(L)$ et $f_{\mathfrak{p}}(L)$ représentent aussi l'indice de ramification et le degré résiduel de l'extension locale $\hat{L}_{\mathfrak{P}} / \hat{K}_{\mathfrak{p}}$. 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 linéaire - ment disjointes .

On déduit des propriétés classiques des nombres de décom - position que l'on a :

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

$$g_{\mathfrak{p}}(K(\sqrt[N]{\alpha})) = \prod_i g_{\mathfrak{p}}(K(\sqrt[l_i^{n_i}]{\alpha})) \quad .$$

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

II Détermination du nombre $g_{\mathfrak{p}}(L)$ d'idéaux premiers de L au-dessus de $\mathfrak{p}$.

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 $i \in \mathbb{N} - \{0\}$, $U^{(i)} = \{ x \in k ; v(x-1) \geqslant i \}$.

(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 :

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

Démonstration :

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

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

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

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

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 $v(\alpha) \geqslant 0$ 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 : $X^m \equiv \alpha \bmod \pi_k^{\lambda}$, ont des solutions dans k pour tout $\lambda \in \mathbb{N}$.

(3) La congruence : $X^m \equiv \alpha \bmod \pi_k^{v(\alpha)+a(m)+1}$, 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 ($v(y') \geqslant 0$) tel que :

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

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

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

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

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

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

On en déduit :

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

L'élément $1 + \frac{y'}{m} . \Pi_k^{a(m)+1}$ 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

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

2°) Détermination de $g_{\mathfrak{p}}(L)$.

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 $v_{\mathfrak{p}}(\alpha) \geqslant 0$ et $L = K(\sqrt[N]{\alpha})$.

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

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

ait une solution dans K .

Remarque : Les nombres a(m) sont ceux définis dans le corollaire II.2 , en prenant $k = \hat{K}_{\mathfrak{p}}$ et $v = v_{\mathfrak{p}}$. 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 $v(m) > 0$:

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

Démonstration :

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

Remarque : Puisque l'on a $\alpha \in (\hat{K}_{\mathfrak{p}})^{g_{\mathfrak{p}}(L)}$, la congruence :

$\alpha \equiv X^{g_{\mathfrak{p}}(L)} \bmod \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)+a(N)+1}$ a aussi une solution β dans $\hat{K}_{\mathfrak{p}}$ que l'on peut calculer . On a donc :

$$\alpha = \beta^{g_{\mathfrak{p}}(L)} . u$$

avec $u = 1 + \lambda . \Pi_k^{v_{\mathfrak{p}}(\alpha)+a(N)+1}$ (Π_k est une uniformisante de $\hat{K}_{\mathfrak{p}}$) .

On déduit du corollaire II.2 que $u = u'^{N}$.

Posons $N' = \dfrac{N}{g_{\mathfrak{p}}(L)}$.

On a alors : $\hat{L}_{\mathfrak{P}} = \hat{K}_{\mathfrak{p}}(\sqrt[N]{\alpha}) = \hat{K}_{\mathfrak{p}}(\sqrt[N']{\beta})$

avec $N' = \left[\hat{K}_{\mathfrak{p}}(\sqrt[N']{\beta}) : \hat{K}_{\mathfrak{p}}\right]$.

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 $v_{\mathfrak{p}}(\alpha)$ 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 $v_{\mathfrak{p}}(\alpha)$ soit égal à la valeur minimum d des entiers $|v_{\mathfrak{p}}(\gamma)|$ lorsque $\gamma \in \Delta$.

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

.../...

(2) Si $d \neq 0$, d est le PGCD de N et de $v_{\mathfrak{p}}(\gamma)$ pour tout $\gamma \in \Delta$.

Démonstration :

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

On en déduit que si $v_{\mathfrak{p}}(\alpha) = d = 0$ on a pour tout $\gamma \in \Delta$, $v_{\mathfrak{p}}(\gamma) \equiv 0 \mod N$.

Inversement supposons que pour un $\gamma \in \Delta$, on ait $v_{\mathfrak{p}}(\gamma) = \lambda . N$.

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

Supposons maintenant $d \neq 0$.

On a $\alpha = x'^N . \gamma^j$ et $\gamma = x^N . \alpha^i$. On en déduit que le PGCD d' de $v_{\mathfrak{p}}(\gamma)$ et de N est égal au PGCD de $v_{\mathfrak{p}}(\alpha)$ et de N .

d étant non nul on a donc $d' \leqslant d$.

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

Posons : $N = d'N'$ et $v_{\mathfrak{p}}(\gamma) = d'd''$ avec $(N', d'') = 1$.

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

Construisons des coefficients de Bezout , $u = u_o + \lambda . d''$ et $v = v_o - \lambda N'$, 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_o ni N' . On vérifie que N et v sont premiers entre eux .

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

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

et $v_{\mathfrak{p}}(\alpha') = u.N + v . v_{\mathfrak{p}}(\gamma) = d'$.

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 $f_1(X) \cdot f_2(X) \cdot \ldots \cdot f_g(X)$ (f_i , polynomes irréductibles distincts) . On choisit pour tout $i \in \{1, \ldots, g\}$, 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 $i \in \{1, \ldots, g\}$) . Soit $\hat{\mathfrak{p}}$ 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 $\mathfrak{p}_i = \sigma_i^{-1}(\hat{\mathfrak{p}})$ et les g complétions de K pour les valuations $v_p \circ \sigma_i$ associées aux idéaux $\mathfrak{p}_i$ sont les $(\hat{K}, \sigma_i)$.

Il est alors facile de vérifier que la congruence :

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

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

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

a une solution X dans $\hat{K}$.

b) <u>l'exemple</u> .

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

$L = K(\sqrt[8]{\alpha})$ 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 $v_{\mathfrak{p}}(\alpha) = 0$ pour $\mathfrak{p}$ non diviseur de 3 .

<u>1^{er} cas</u> : $p = 2$.

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

fixées une fois pour toutes , de 113 , 2 et -1 , dans Ω_2 , clôture algébrique de $\mathbb{Q}_2$. On a $113 \equiv 1 \bmod 8$. 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 :

$$\{ \sqrt{113} + \sqrt{2} + i \; ; \; \sqrt{113} - \sqrt{2} - i \; ; \; \sqrt{113} + \sqrt{2} - i \; ; \; \sqrt{113} - \sqrt{2} + i \}$$

$$\{ -\sqrt{113} + \sqrt{2} + i \; ; \; -\sqrt{113} - \sqrt{2} - i \; ; \; -\sqrt{113} + \sqrt{2} - i \; ; \; -\sqrt{113} - \sqrt{2} + i \}.$$

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 $(\hat{K}, \sigma_1)$ et $(\hat{K}, \sigma_2)$ définies par le choix suivant des plongements :

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

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^{eme} 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 , $g_{\mathfrak{p}_i}(L)$ est le plus grand des diviseurs 2^h de 8 tels que :

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

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 $4\sqrt{2}$ mod π^{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 $2 = \varepsilon . \pi^4 = \varepsilon(1 - \zeta)^4$.

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

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

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 :

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

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

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

On a :

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

On a :

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

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

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

On choisit la plus simple des solutions :

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

On a alors :

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

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

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

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

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

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

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

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

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

pas utile ici pour la détermination de $e_{\mathfrak{p}}(L)$.

On peut cependant vérifier que l'élément :

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

est tel que :

$$\alpha \equiv \beta^2 \mod \Pi^{17} \quad .$$

On a donc : $\hat{L}_{\mathfrak{P}} = \hat{K}_{\mathfrak{p}}(\sqrt[4]{\beta})$ avec $[\hat{L}_{\mathfrak{P}} : \hat{K}_{\mathfrak{p}}] = 4$.

<u>2e cas</u> : $p = 3$.

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

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 :

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

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

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

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 $(\hat{K}, \sigma_i)$ de K correspondantes peuvent être définies par les plongements σ_i ci-dessous :

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

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

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 $\sqrt{2} \equiv \zeta^2 \bmod 3$ et $4\sqrt{2} \equiv \zeta^2 \bmod 3$

$113 = -1 + 3.38$, d'où $\sqrt{113} \equiv \zeta^2 \bmod 3$.

D'où $\alpha = \sigma_1(\alpha) = -\sigma_2(\alpha) \equiv \zeta^6 \bmod 3$

$\sigma_3(\alpha) = -\sigma_4(\alpha) \equiv 0 \bmod 3$.

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

$$\sigma_3(\alpha) = -\sigma_4(\alpha) \equiv \zeta^2 . 3^4 \bmod 3^5 .$$

+ 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 :

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

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) $\qquad \sigma_i(\alpha) \equiv X^m \bmod \hat{\mathfrak{p}} = (3)$.

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 :

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

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 :

$$(2) \qquad \sigma_i(\alpha) \equiv X^m \mod 3^5 .$$

Les congruences :

$$\zeta^2 . 3^4 \equiv X^m \mod 3^5$$
$$\zeta^6 . 3 \equiv X^m \mod 3^5$$

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

On a donc encore :

$$g_{\mathfrak{p}_3}(L) = g_{\mathfrak{p}_4}(L) = 2 .$$

<u>3e cas</u> : $p \neq 2$ et $p \neq 3$.

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

$$\alpha \equiv X^m \mod \mathfrak{p} .$$

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

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

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

Donnons des exemples de résultats :

+ pour $p = 113$, il y a 4 idéaux de K au-dessus de 113 et on a $g_{\mathfrak{p}}(L) = 2$ 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 $g_{\mathfrak{p}}(L) = 1$.

+ pour $p = 41$, il y a 8 odéaux de K au-dessus de 41 et on a pour chacun d'eux $g_{\mathfrak{p}}(L) = 1$.

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 $v_{\mathfrak{p}}(\alpha) \not\equiv 0 \bmod N$.

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 $\mathfrak{p} \nmid NA_K$ et si $v_{\mathfrak{p}}(\alpha) \equiv 0 \bmod N$, $\mathfrak{p}$ 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 $N^N . \alpha^{N-1}$ des nombres $\{1, \sqrt[N]{\alpha}, \ldots, \sqrt[N]{\alpha}^{N-1}\}$; 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 :

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

D'où :

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

D'autre part, soit K_T le corps d'inertie de $\mathfrak{p}$ dans L/K ; L/K étant cyclique, K_T est l'unique sous-corps de L de degré $n = \dfrac{N}{e_{\mathfrak{p}}(L)}$ par rapport à K ; on a donc

$$K_T = K(\sqrt[n]{\alpha}) .$$

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

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

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

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 $d.A_K$ et $v_{\mathfrak{p}}(\alpha) \equiv 0 \bmod d$. 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 $d = p^m.\, d'$ (avec $(d', p) = 1$).

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

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 $\hat{K}_{\mathfrak{p}}$ de K (si K lui-même n'est pas complet).

Soit ζ_h une racine $(p^h)^{eme}$ de 1 (contenue dans k pour $1 \leqslant h \leqslant n$) . 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 :

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

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 $\left[k(\sqrt[p^n]{\gamma}) : k\right] = p^n$) . On déduit donc du corollaire II.3 que pour les éléments γ de Δ tels que $v(\gamma) = 0$, la congruence :

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

n'a pas de solution dans k ,

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_o 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 $\gamma \in \Delta_o$.

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

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

.../...

.../...

gruence $\gamma \equiv X^{p^n} \bmod \mathfrak{p}^{\lambda}$ ait une solution dans K .

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

Démonstration :

+ On a vu que la congruence :

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

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

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

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

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

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

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

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

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

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

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

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

$$\gamma \equiv X^{p^n} \bmod \mathfrak{p}$$

était insoluble (avec $\gamma \in \Delta_o$) le polynome $X^{p^n} - \bar{\gamma}$ n'aurait pas de racines dans $\bar{k}$ et l'extension $\bar{k}(\sqrt[p^n]{\bar{\gamma}}) / \bar{k}$ (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 $v(x-1) \leqslant a_1$ 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 $(p^n)^{eme}$ de 1 .

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

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

L'hypothèse $v(x-1) \leqslant a_1$ 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 $v_n(\theta-1) = \frac{v_n(p)}{\varphi(p^n)}$) que la relation (1) est vraie .

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

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

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

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

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

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 $e = e_{\mathfrak{p}}(k_n)$, l'indice de ramification de $\mathfrak{p}$ dans k_n . Si $v_n(\theta-1)$ est multiple de e , ($v_n(\theta-1) = e.\mu'$) et si π_o est une uniformisante de k , on a : $\theta = 1 + \eta \pi_o^{\mu'}$. Alors $\bar{\eta}$ n'appartient pas à $\bar{k}$ et le degré résiduel $f_{\mathfrak{p}}(k_n)$ est multiple de p .

Démonstration :

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

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

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

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

c'est-à-dire : $\theta = 1 + \eta \pi_o^{\mu'}$ 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 :

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

D'où : $\theta = \left[1 + a\pi_o^{\mu'}\right] \cdot \left[1 + \dfrac{b}{1 + a\pi_o^{\mu'}} \cdot \pi_o^{1+\mu'} \right]$.

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

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

Posons : $\theta' = 1 + \dfrac{b}{1 + a\Pi_o^{\mu'}} . \Pi_o^{1+\mu'}$.

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

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

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

On a :

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

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 $k_n = k\left(\sqrt[p^n]{\beta}\right)$ avec $v(\beta-1) = \lambda_n$.

Soit θ une racine $(p^n)^{eme}$ de β . Si k_n/k est non ramifié, le lemme III.3 s'applique et on a :

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

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

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

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

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

racine d'un polynome de la forme $X^{p^n} + \bar{C}_{p^{n-1}} X^{p^{n-1}} + \bar{\mathcal{E}}$ (avec $\bar{C}_{p^{n-1}}$ et $\bar{\mathcal{E}}$ 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 : $\beta = 1 + \mathcal{E}\, \Pi_o^{\lambda_n}$ (avec $\mathcal{E}$ unité de k) .

η est racine de l'équation :

$$1 + \mathcal{E}.\Pi_o^{\lambda_n} = (1 + \eta \Pi_o^{\mu})^{p^n}$$

ou encore :

$$(1) \qquad \mathcal{E}.\Pi_o^{\lambda_n} = \sum_{i=1}^{p^n} C_{p^n}^{i} \cdot (\eta.\Pi_o^{\mu})^{i} \quad .$$

Posons , pour $i \in \{ 1, \ldots, p^n \}$, $i = p^t.i'$ (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 :

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

D où :

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

On remarque que p^t est le plus petit des entiers i tels que l'on ait : p^t/i et $p^{1+t} \not/ i$.

On a donc :

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

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

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

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

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

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

$$\varepsilon \equiv \eta^{p^n} \mod \pi_o .$$

(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 $X^{p^n} - \bar{\varepsilon}$.

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

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

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

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

$$\varepsilon \equiv \eta^{p^n} + C_{p^{n-1}} \cdot \eta^{p^{n-1}} \mod \pi_o$$

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

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

est insoluble dans k .

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

$$\beta \equiv X^p \mod \mathfrak{p}^{a_1}$$

a une solution dans k .

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

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

ait une solution dans k ; alors , l'indice de ramification $e_{\mathfrak{p}}(k_n)$ 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 $s \geqslant 1$, $f_{\mathfrak{p}}(k_n)$ 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 $e_{\mathfrak{p}}(k_n)$ 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 :

$$\beta \equiv X^p \mod \mathfrak{p}^{\lambda}$$

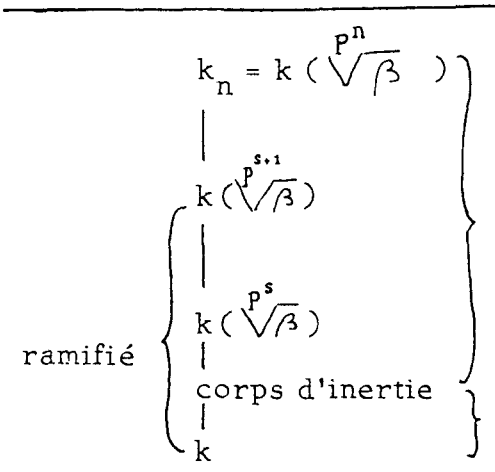
soit soluble dans k , pour $\lambda = a_1$; si elle est aussi soluble pour $\lambda = 1+a_1$, on a alors $k = k(\sqrt[p]{\beta})$ (l'extension $k(\sqrt[p]{\beta})/k$ est trivialement non ramifiée !) . Supposons donc la congruence insoluble pour $\lambda = 1+a_1$ alors le

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^{eme} θ de β , dans k_1 (lemme III.2) :

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

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

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



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 $e_{\mathfrak{p}}(k_n)$ 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 $s \geqslant 1$, on déduit de la partie (2) que $k(\sqrt[p]{\beta}) / k$ est non ramifié ; $f_{\mathfrak{p}}(k_n)$ est alors multiple de p .

b) <u>cas " global "</u> :

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 $v_{\mathfrak{p}}(\alpha) \equiv 0 \mod p^m$, et $[L:K] = p^m$.

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

On pose alors :

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

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 $e_{\mathfrak{p}}(L)$, $f_{\mathfrak{p}}(L)$, $g_{\mathfrak{p}}(L)$.

Proposition III.6 . Critère de détermination de $e_{\mathfrak{p}}(L)$, $f_{\mathfrak{p}}(L)$, $g_{\mathfrak{p}}(L)$.

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 $v_{\mathfrak{p}}(\alpha) = 0$.

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

$$\alpha \equiv x^{p^h} \mod \mathfrak{p}^{1+a_h}$$

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

(1) On a $g_{\mathfrak{p}}(L) = p^r$; et si $r = m$, $e_{\mathfrak{p}}(L) = f_{\mathfrak{p}}(L) = 1$.

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

$$\alpha \equiv x^{p^{1+r}} \mod \mathfrak{p}^{a_{1+r}}$$

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

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

$$\alpha \equiv x^{p^h} \mod \mathfrak{p}^{a_{1+r}}$$

ont une solution dans K pour $h \in \{r+1, \ldots, r+s\}$, mais pas de solution pour $h > r+s$, alors $f_{\mathfrak{p}}(L)$ est multiple de p , et $e_{\mathfrak{p}}(L)$ 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 : $\alpha \equiv X^{p^m} \bmod \mathfrak{P}^{a_{1+r}}$ 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 $\beta \in \hat{K}_{\mathfrak{p}}$ tel que

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

D'après la définition de r , on a :

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

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

On notera ici $\hat{\mathfrak{P}}$ l'unique idéal premier de l'anneau de valuation de $\hat{K}_{\mathfrak{p}}$.

(On a $e_{\hat{\mathfrak{P}}}(k_n) = e_{\mathfrak{p}}(L)$, $f_{\hat{\mathfrak{P}}}(k_n) = f_{\mathfrak{p}}(L)$) .

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

Lemme .

Soit $h \geqslant 1$ tel que la congruence

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

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

$$\beta \equiv X^{p^h} \bmod \hat{\mathfrak{P}}^{a_1}$$

est insoluble dans k .

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

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

d'où :

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

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

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

D'autre part , on a : $a_{1+r} = a_1 + r . v(p)$. On a donc :
$y^{p^r} \equiv 1 \mod \mathfrak{p}^{a_{1+r}}$ et $\alpha \equiv x^{p^{h+r}} \mod \mathfrak{p}^{a_{1+r}}$ 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 :

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

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

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

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

soit soluble pour $1 \leqslant h \leqslant s$, 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 :

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

est insoluble .

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

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

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 :

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

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 : $\beta \equiv X^{p^s} \mod \hat{\mathfrak{p}}^{a_1}$.

D'après la partie (3) de la proposition III.5 , l'indice de ramification $e_{\hat{\mathfrak{p}}}(k_n) = e_{\mathfrak{p}}(L)$ 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 $\mathfrak{p}$ dans $K(\sqrt[p^{s+r}]{\alpha})$. D'autre part on a supposé $s \geqslant 1$, on a donc bien $f_{\hat{\mathfrak{p}}}(k_n)$ (ou encore $f_{\mathfrak{p}}(L)$) , multiple de p .

Conclusion :

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

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

$$\beta \not\equiv X^p \mod \mathfrak{p}^{1+a_1}$$

$$\beta \equiv X^{p^s} \mod \mathfrak{p}^{a_1} \qquad (s > 1)$$

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 $k(\sqrt[p^s]{\beta}) / k$ 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 à fortiori de degré p^s avec $s \leqslant n$) . 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 $(p^{sf}-1)^{eme}$ de 1) . Puisque k contient les racines $(p^s)^{eme}$ 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 $f_{\mathfrak{p}}(k_s)$ 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 $\left(\langle \Theta, \chi \rangle = \sum_{\sigma \in G} \chi(\sigma^{-1}) \Theta^{\sigma} \right)$.

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 $\mathfrak{p}$ ne divise pas $6A_K$: on a $v_{\mathfrak{p}}(\alpha) = 0$.

D'après la proposition III.1 on a donc $e_{\mathfrak{p}}(L) = 1$.

b) si $\mathfrak{p}$ 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 $\mathfrak{p}$ 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 :

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

D'autre part les congruences

$$\alpha \equiv x^{2^h} \mod \mathfrak{p}_1^{\lambda}$$
$$\alpha \equiv x^{2^h} \mod \mathfrak{p}_2^{\lambda}$$

sont équivalentes à :

$$\alpha = \sigma_1(\alpha) \equiv x^{2^h} \mod \pi^{\lambda}$$
$$\sigma_2(\alpha) \equiv x^{2^h} \mod \pi^{\lambda}$$

avec $\sigma_2(\alpha) = -\sqrt{113 + 4\sqrt{2}} \equiv \zeta^4 \mod \pi^{17}$.

On a vérifié que l'on a :

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

et $x \equiv 1 + s\pi^2 + \pi^3 \mod \pi^4$

$s = 0$ ou 1

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

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 :

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

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 Primteilen von p (Journal de Crelle 176 1936) .

[6] Hasse H. : Zur Arbeit von I.R. Safarevic über das allgemeine Reciprozitätsgesetz (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) .