

**ACADEMIE DE LIMOGES**

**UNIVERSITE DE LIMOGES**

# **THESE**

**pour l'obtention du Grade de**

**DOCTEUR DE L' UNIVERSITE DE LIMOGES**

**MENTION : MATHEMATIQUES**

**Soutenue publiquement le 23 novembre 1999 par**

**Mohamed ZAHIDI**

**Co-directeurs de thèse : F. LAUBIE et A. MOVAHHEDI**

XXXXXXXXXXXXXXXXXXXX

## **SYMBOLES DES RESTES QUADRATIQUES ET DISCRIMINANTS**

XXXXXXXXXXXXXXXXXXXX

### **Composition du jury**

V. ABRASHKIN	Université de Moscou	<b>Rapporteur</b>
F. DIAZ Y DIAZ	Université de Bordeaux	<b>Rapporteur</b>
M.J. BERTIN	Université de Paris VI	<b>Examinatrice</b>
F. LAUBIE	Université de Limoges	<b>Examineur</b>
A. MOVAHHEDI	Université de Limoges	<b>Examineur</b>
A. SALINIER	Université de Limoges	<b>Examineur</b>



## REMERCIEMENTS

Je tiens à remercier mes co-directeurs de thèse

- François LAUBIE qui a bien voulu me proposer un thème de recherche et il a accepté de diriger ma thèse avec les conseils qu'il m'a donné durant ces années de travail,

- A. Chazad MOVAHHEDI pour l'attention qu'il a porté sur ce travail durant toutes ces années, ainsi que la disponibilité dont il a su faire part malgré un emploi du temps chargé, et pour les discussions enrichissantes que nous avons eues durant toute la durée de ma thèse qui m'ont apportés énormément d'aides pour la réalisation de ce travail.

Je remercie également Victor ABRASHKIN et Francisco DIAZ Y DIAZ pour avoir accepté d'être rapporteurs.

J'exprime ma reconnaissance à Marie-josé BERTIN et Alain SALINIER pour leur aimable participation à ce jury.

Pierre BARRUCAND était l'initiateur du problème étudié dans cette thèse. Qu'il soit remercié à cette occasion.

Je remercie Nadine Tchéfranoff pour avoir voulu assurer la frappe de ma thèse ainsi que pour sa disponibilité et sa sympathie.

# Table des matières

Introduction

Chapitre I. Symbole des restes quadratiques dans les corps des nombres

Symbole de Jacobi généralisé

Symbole des restes quadratiques

Chapitre II. Symboles des restes quadratiques et discriminants (Cas des indices de ramification impairs)

Généralisation du théorème de Pellet, Stickelberger et Voronoi

Études locales

Globalisation

Chapitre III. Symboles des restes quadratiques et discriminants (Cas des indices de ramification quelconques)

Généralisation de la formule de [1].

Études locales

Le cas galoisien

Formule de transitivité pour  $\epsilon$

Quelques exemples de calcul de  $\epsilon_{L/K}(\mathfrak{p})$

## Chapitre IV. Applications

Loi de réciprocité quadratique

Application aux corps ayant un nombre de classes impair

Annexes

Liste des symboles

Références

## Introduction

Soit  $L$  un corps de nombres de degré  $n$  sur le corps  $\mathbf{Q}$  des nombres rationnels de discriminant  $D = D_{L/\mathbf{Q}}$ . Si l'entier  $D$  n'est pas un carré, on note  $d$  le discriminant du corps quadratique  $\mathbf{Q}(\sqrt{D})$ , sinon on pose  $d = 1$ . Soit  $p$  un nombre premier non-ramifié dans  $L$  de sorte que le symbole des restes quadratiques  $\left(\frac{D}{p}\right)$  soit non-nul. Un théorème déjà ancien dû à A. Pellet ([4, page 245]), L. Stickelberger et G. Voronoi montre que la parité du nombre  $g$  d'idéaux premiers de  $L$  au-dessus de  $p$  est déterminée par ce symbole  $\left(\frac{D}{p}\right)$ . En effet, nous avons :  $\left(\frac{D}{p}\right) = (-1)^{n-g}$ .

Plus généralement, même si  $p$  est ramifié dans  $L$ , on aimerait pouvoir relier le symbole  $\left(\frac{d}{p}\right)$  à la décomposition  $(p) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$  de  $p$  en produit d'idéaux premiers  $\mathfrak{P}_i$  de  $L$ .

Supposons que  $p$  n'est pas sauvagement ramifié dans  $L$ . Si  $f_i$  désigne le degré résiduel de  $\mathfrak{P}_i$  dans l'extension  $L/\mathbf{Q}$ , alors la valuation  $p$ -adique du discriminant  $D$  est donnée par  $v_p(D) = \sum_{i=1}^g (e_i - 1)f_i$  [14, Chap.3, prop.13]. Donc le symbole  $\left(\frac{d}{p}\right)$  est non-nul dès que tous les indices de ramification  $e_i$  sont impairs. Dans ce dernier cas, généralisant une série de résultats (Wahlin [16], Hasse [7], Böhler [2], Dribin [5], Kientega [9], ...), P. Barrucand et F. Laubie ont établi la formule suivante (également valable dans le cas relatif) [1] :

$$\left(\frac{d}{p}\right) = (-1)^F \left(\frac{p}{E}\right) \quad \text{avec} \quad E = \prod_{2|f_i} e_i \quad \text{et} \quad F = \sum_{2|f_i} 1.$$

Notre but est de donner une formule analogue sans aucune hypothèse sur la parité des indices de ramification  $e_i$ . Ce travail s'inscrit donc comme une suite logique de [1] et en est largement inspiré.

Soient  $K$  un corps de nombres et  $L$  une extension finie de  $K$  de degré  $n$ . Soit  $\{b_1, \dots, b_n\}$  une base du  $K$ -espace vectoriel  $L$ . Le discriminant  $D = D_{L/K} = \det(T_{r_{L/K}}(b_i b_j))$  est un élément non-nul de  $K$  :  $D \in K$ . La classe  $\delta = \delta_{L/K}$  de  $D$  modulo les carrés  $K^2$  est indépendante du choix de la base, c'est donc un invariant de l'extension  $L/K$  ; elle détermine une extension quadratique (ou triviale)  $K(\sqrt{\delta})$ .

Soit  $\mathfrak{p}$  un idéal premier de  $K$ . On va s'intéresser au symbole des restes quadratique  $\left(\frac{\delta}{\mathfrak{p}}\right)$ . Soit  $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$  la décomposition de l'idéal  $\mathfrak{p}$  en produit d'idéaux premiers deux à deux distincts  $\mathfrak{P}_i$  de  $L$ . On note  $f_i$  le degré résiduel de  $\mathfrak{P}_i$  de sorte que  $n = e_1 f_1 + \cdots + e_g f_g$ . On désigne par  $\pi$  une uniformisante du corps local  $K_{\mathfrak{p}}$ .

**Proposition 1** *On suppose que l'idéal premier  $\mathfrak{p}$  de  $K$  est non 2-adique.*

*Si  $\sum_{2|e_i} f_i$  est un entier pair, alors le produit  $\prod_{2|e_i} \left(\frac{\pi}{\mathfrak{P}_i}\right)$  est non-nul et est indépendant du choix de l'uniformisante  $\pi$ .*

Cette proposition suggère

**Définition 2** Pour tout idéal premier non 2-adique  $\mathfrak{p}$  du corps de nombres  $K$ , on pose

$$\epsilon(\mathfrak{p}) = \epsilon_{L/K}(\mathfrak{p}) = \begin{cases} 0 & \text{si } \sum_{2|e_i} f_i \text{ est impair} \\ \prod_{2|e_i} \left( \frac{\pi}{\mathfrak{P}_i} \right) & \text{sinon} \end{cases}$$

où  $\pi$  désigne une uniformisante quelconque du corps local  $K_{\mathfrak{p}}$ . Si tous les  $e_i$  sont impairs, on convient que  $\epsilon(\mathfrak{p}) = 1$ . En particulier  $\epsilon(\mathfrak{p}) = 1$  dès que l'idéal premier  $\mathfrak{p}$  est non-ramifié dans  $L$ .

**Remarque 3** Le symbole  $\epsilon$  peut être interprété par l'application de réciprocité d'Artin de la manière suivante. Notons  $\mathfrak{A}$  l'idéal  $\prod_{2|e_i} \mathfrak{P}_i$  de  $L$ . Soit  $(\mathfrak{A}, L(\sqrt{\pi})/L)$  l'élément du groupe de Galois  $G(L(\sqrt{\pi})/L)$  défini par le symbole d'Artin. Lorsque  $\epsilon_{L/K}(\mathfrak{p})$  est non-nul, il est égal à 1 si et seulement si le symbole d'Artin  $(\mathfrak{A}, L(\sqrt{\pi})/L)$  est l'identité [13, Chap.IV, §8]. Nous utiliserons fréquemment cette caractérisation de  $\epsilon_{L/K}(\mathfrak{p})$ .

À l'aide des propriétés fonctorielles du symbole d'Artin, nous pouvons établir une formule de transitivité pour  $\epsilon$  :

**Proposition 4** Soit  $K \subset M \subset L$  une tour d'extensions de corps de nombres. Soit  $\mathfrak{p}$  un idéal premier de  $K$ . Supposons que  $\epsilon_{L/K}(\mathfrak{p})$ ,  $\epsilon_{M/K}(\mathfrak{p})$  ainsi que les  $\epsilon_{L/M}(\mathcal{P})$  pour  $\mathcal{P} \mid \mathfrak{p}$  sont non-nuls, alors nous avons

$$\epsilon_{L/K}(\mathfrak{p}) = \epsilon_{M/K}(\mathfrak{p})^{[L:M]} \prod_{\substack{\mathcal{P} \mid \mathfrak{p} \\ 2 \nmid e(\mathcal{P}/\mathfrak{p})}} \epsilon_{L/M}(\mathcal{P}).$$

Le théorème suivant est le résultat principal de cette thèse qui relie les deux symboles  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$  et  $\epsilon_{L/K}(\mathfrak{p})$ .

**Théorème 5** *Soit  $\mathfrak{p}$  un idéal premier non 2-adique du corps de nombres  $K$ .*

*On suppose que  $\mathfrak{p}$  n'est pas sauvagement ramifié dans  $L$ . Alors les symboles  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$  et  $\epsilon_{L/K}(\mathfrak{p})$  sont reliés par la formule*

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^{F + \frac{q-1}{2}G} \left(\frac{q}{E}\right) \epsilon_{L/K}(\mathfrak{p})$$

*où  $q$  est la norme absolue de  $\mathfrak{p}$  et les trois entiers  $E, F$  et  $G$  sont définis par*

$$E = \prod_{2 \nmid e_i f_i} e_i, \quad F = \sum_{\substack{2 \mid f_i \\ 2 \nmid e_i}} 1 \quad \text{et} \quad G = \sum_{\substack{4 \mid e_i \\ 2 \nmid f_i}} 1.$$

La démonstration de ce théorème se fait essentiellement en trois étapes : complétion, dévissage et globalisation.

**Remarque 6** (i) *Lorsque tous les indices de ramification  $e_i$  sont impairs, alors  $G = 0$ ,  $\epsilon_{L/K}(\mathfrak{p}) = 1$  et on retrouve le théorème principal de Barrucand-Laubie [1, Théorème 2].*

(ii) *Pour les idéaux premiers 2-adiques  $\mathfrak{p}$  qui ne sont pas sauvagement ramifiés dans  $L$ , nous avons encore*

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^F \left(\frac{q}{E}\right).$$

*Néanmoins, ils ont été exclus de l'énoncé du théorème précédent car pour ces idéaux  $\epsilon$  n'est pas défini.*

Supposons maintenant que l'extension  $L/K$  est galoisienne de groupe de Galois  $G$ . Soit, comme d'habitude,

$e =$  l'indice de ramification de  $\mathfrak{p}$  dans  $L/K$ ,

$f =$  le degré résiduel de  $\mathfrak{p}$  dans  $L/K$ ,

$g =$  le nombre d'idéaux premiers de  $L$  au-dessus de  $\mathfrak{p}$ .

Alors pour chaque uniformisante  $\pi \in \mathfrak{p} - \mathfrak{p}^2$ , le symbole  $\rho := \left( \frac{\pi}{\mathfrak{P}} \right)$  est indépendant du choix de la place  $\mathfrak{P}$  au-dessus de  $\mathfrak{p}$  de sorte que  $\epsilon_{L/K}(\mathfrak{p}) = \rho^g$  est une puissance  $g$ -ième.

Avec les notations ci-dessus, le théorème 5 montre facilement que la valeur du symbole  $\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right)$  est donnée par

**Corollaire 7** *Supposons que  $L$  est une extension galoisienne de  $K$ . Pour tout idéal premier  $\mathfrak{p}$  de  $K$  qui n'est pas sauvagement ramifié dans  $L$ , nous avons*

$$\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right) = \begin{cases} 0 & \text{si } 2|e \quad \text{et } 2 \nmid fg \\ \rho^g & \text{si } 2|e \quad \text{et } 2|fg \\ (-1)^g & \text{si } 2 \nmid e \quad \text{et } 2|fg \\ \left( \frac{g}{e} \right) & \text{si } 2 \nmid n. \end{cases}$$

Dans la situation de ce dernier corollaire, le cas où  $2|e$ ,  $2|f$  et  $2 \nmid g$  est le seul où la connaissance des entiers  $e$ ,  $f$  et  $g$  ne suffit pas pour déterminer la valeur de  $\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right)$ . Dans ce dernier cas, nous avons  $\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right) = \epsilon_{L/K}(\mathfrak{p}) = \left( \frac{\pi}{\mathfrak{P}} \right) \neq 0$ . La valeur de  $\rho = \left( \frac{\pi}{\mathfrak{P}} \right)$  est alors liée à la structure du groupe

de décomposition  $D = D(\mathfrak{P}/\mathfrak{p})$  de la place  $\mathfrak{P}$  dans l'extension  $L/K$ . Plus précisément, nous avons

**Proposition 8** *Soit  $L/K$  une extension galoisienne de corps de nombres. Soient  $\mathfrak{p}$  un idéal premier non 2-adique de  $K$  et  $\mathfrak{P}$  un idéal premier de  $L$  au-dessus de  $\mathfrak{p}$ . Supposons que le degré résiduel  $f$  de  $\mathfrak{p}$  dans  $L/K$  est pair. Soit  $\pi$  une uniformisante de  $K_{\mathfrak{p}}$ . Alors  $\left(\frac{\pi}{\mathfrak{P}}\right) = 1$  si et seulement si le 2-sous-groupe de Sylow du groupe de décomposition  $D(\mathfrak{P}/\mathfrak{p})$  n'est pas cyclique.*

Nous verrons dans le chapitre III que dans une même extension  $L/K$ , il est possible que  $\epsilon$  prenne les trois valeurs -1, 0 et 1 en trois places ramifiées.

Comme conséquence immédiate du corollaire 7, citons la proposition suivante qui est à rapprocher au théorème de Pellet-Stickelberger-Voronoi.

**Proposition 9** *Soit  $K$  un corps de nombres,  $L$  une extension galoisienne de  $K$  et  $\mathfrak{p}$  un idéal premier de  $K$  qui n'est pas sauvagement ramifié dans  $L$ . Si  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) \neq 1$ , alors le nombre d'idéaux premiers de  $L$  au-dessus de  $\mathfrak{p}$  est impair.*

Il n'est pas difficile de voir que la réciproque de la proposition précédente est inexacte : en effet, il suffit de prendre  $K = \mathbf{Q}$ ,  $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$  et  $\mathfrak{p} = 3\mathbf{Z}$ . Alors  $\mathfrak{p} = \mathfrak{P}^2$  dans  $L$  et nous avons  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = 1$ .

# Chapitre I

## Symbole des restes quadratiques dans les corps des nombres.

Dans ce chapitre, on se propose de rappeler brièvement les différentes propriétés des symboles quadratiques bien connus dans la littérature, notamment ceux de Jacobi, Kronecker, ainsi que le symbole des restes quadratiques dans les corps des nombres que l'on utilisera souvent dans le chapitre suivant. La référence principale étant [3]

**Résumé.** Soit  $K$  un corps de nombres,  $A$  l'anneau des entiers de  $K$ ,  $\mathfrak{a}$  un idéal de  $A$  de norme absolue impaire, soit  $x$  un élément de  $A$  tel que l'idéal principal  $xA$  est premier à  $\mathfrak{a}$ . Le symbole de Legendre-Jacobi généralisé est défini par la signature de la permutation de  $A/\mathfrak{a}$  par la multiplication par  $\bar{x} = x \bmod \mathfrak{a}$  et est notée par  $\left( \frac{x}{\mathfrak{a}} \right)$ . Nous commencerons par rappeler quelques propriétés de ce symbole. Puis lorsque  $K = \mathbb{Q}$ ,  $A = \mathbb{Z}$  et  $\mathfrak{a} = n\mathbb{Z}$  où  $n$  est un entier pair, même si le symbol  $\left( \frac{\cdot}{\mathfrak{a}} \right)$  n'est pas défini, on se propose dans ce chapitre de calculer la signature de la permutation de  $\mathbb{Z}/n\mathbb{Z}$  induite par la multiplication par la classe de  $a$  où  $a$  est un entier premier à  $n$ . Ce résultat n'est pas en fait traité dans [3] mais nous en aurons besoin au chapitre III.

### Symbole de Jacobi généralisé:

Soient  $K$  un corps de nombres,  $A$  l'anneau des entiers de  $K$ .

Étant donné un idéal  $\mathfrak{a}$  de  $K$  dont la norme absolue  $N(\mathfrak{a})$  est impaire et un élément  $x$  de  $A$ , on dit que  $x$  est étranger à  $\mathfrak{a}$  si l'on a  $A = Ax + \mathfrak{a}$  c'est-à-dire la classe  $\bar{x}$  de  $x$  modulo  $\mathfrak{a}$  est un élément inversible de l'anneau  $A/\mathfrak{a}$ . S'il en est ainsi, la multiplication par  $\bar{x}$  définit une permutation de l'ensemble fini  $A/\mathfrak{a}$ , dont la signature sera notée  $\left(\frac{x}{\mathfrak{a}}\right)$  (voir [3]). Ainsi, on a les propriétés suivantes :

$$\left(\frac{xy}{\mathfrak{a}}\right) = \left(\frac{x}{\mathfrak{a}}\right) \cdot \left(\frac{y}{\mathfrak{a}}\right). \quad (1.1)$$

$$\left(\frac{x}{\mathcal{P}}\right) = x^{\frac{1}{2}(N(\mathcal{P})-1)} \bmod \mathcal{P}. \quad (1.2)$$

$$\left(\frac{x}{\mathcal{P}}\right) = \begin{cases} 1 & \text{si } x \text{ est congru à un carré modulo } \mathcal{P} \\ -1 & \text{sinon} \end{cases} \quad (1.3)$$

$\mathcal{P}$  étant un idéal premier de  $A$ .

La propriété (1.1) découle de la multiplicativité de la signature.

**Preuve de (1.2)**

Notons  $k := A/\mathcal{P}$  le corps résiduel relatif à  $\mathcal{P}$ . Soit  $u_{\bar{x}}$  l'automorphisme de  $k$  qui est la multiplication par  $\bar{x}$ .

On sait que  $\left( \begin{smallmatrix} x \\ \mathcal{P} \end{smallmatrix} \right) = \left( \begin{smallmatrix} \det u_{\bar{x}} \\ \mathbb{F}_p \end{smallmatrix} \right)$  [3, page 41 formule 20] où  $\mathbb{F}_p$  est le sous-corps premier de  $k$ . De plus

$$\left( \begin{smallmatrix} \det u_{\bar{x}} \\ \mathbb{F}_p \end{smallmatrix} \right) = \left( \begin{smallmatrix} N_{k/\mathbb{F}_p}(\bar{x}) \\ \mathbb{F}_p \end{smallmatrix} \right)$$

où  $N_{k/\mathbb{F}_p}(\bar{x}) = \bar{x}^{\frac{N(\mathcal{P})-1}{p-1}}$  est la norme de l'extension  $k/\mathbb{F}_p$ . Comme :

$$\left( \begin{smallmatrix} N_{k/\mathbb{F}_p}(\bar{x}) \\ \mathbb{F}_p \end{smallmatrix} \right) = N_{k/\mathbb{F}_p}(\bar{x})^{\frac{p-1}{2}}.$$

[3, page 40, formule 19], on a  $\left( \begin{smallmatrix} x \\ \mathcal{P} \end{smallmatrix} \right) = \bar{x}^{\frac{N(\mathcal{P})-1}{2}}$  c'est-à-dire

$$\left( \begin{smallmatrix} x \\ \mathcal{P} \end{smallmatrix} \right) = x^{\frac{N(\mathcal{P})-1}{2}} \pmod{\mathcal{P}}.$$

### **preuve de (1.3)**

Soit  $g$  un générateur du groupe multiplicatif  $k^* = (A/\mathcal{P})^*$ . Il existe un entier  $r$  tel que  $\bar{x} = g^r$ .

Premier cas - Si  $x$  est congru à un carré modulo  $\mathcal{P}$ , alors forcément  $r$  est pair, et par conséquent

$$\left( \begin{smallmatrix} x \\ \mathcal{P} \end{smallmatrix} \right) = g^{\frac{r}{2}(N(\mathcal{P})-1)} = 1.$$

Deuxième cas - Si  $x$  n'est pas congru à un carré modulo  $\mathcal{P}$ , il existe un entier  $s$  tel que

$$\left( \begin{smallmatrix} x \\ \mathcal{P} \end{smallmatrix} \right) = g^{(2s+1)\frac{(N(\mathcal{P})-1)}{2}} = g^{s(N(\mathcal{P})-1)} \cdot g^{\frac{N(\mathcal{P})-1}{2}} = 1 \cdot (-1) = -1.$$

**Remarque 1.1** Si  $N(\mathfrak{a})$  est pair, le symbole de Jacobi  $\left(\frac{\cdot}{\mathfrak{a}}\right)$  n'est pas a priori défini par la signature, cependant, lorsque  $A = \mathbb{Z}$  et  $\mathfrak{a} = n\mathbb{Z}$  où  $n$  est un entier pair, nous allons calculer la signature de la multiplication par  $a$  :

$$m_a : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ b & \rightarrow & ab \end{array}$$

pour tout  $a$  premier à  $n$ . Ce résultat nous servira au chapitre III.

**Proposition 1.2** Soit  $n$  un entier pair positif. Soit  $a$  un entier positif premier à  $n$ . La signature de la permutation :

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \rightarrow & \mathbb{Z}/n\mathbb{Z} \\ b & \rightarrow & ab \end{array}$$

est donnée par :  $(-1)^{\binom{n}{2}+1}\binom{a-1}{2}$ .

Pour montrer la proposition , on aura besoin de deux lemmes.

**Lemme 1.3** Soit  $k$  un entier supérieur ou égal à 2, et  $a$  un entier positif impair, la signature de la permutation

$$m_a : \begin{array}{ccc} \mathbb{Z}/2^k\mathbb{Z} & \rightarrow & \mathbb{Z}/2^k\mathbb{Z} \\ b & \rightarrow & ab \end{array}$$

est donnée par  $sg(m_a) = (-1)^{\frac{a-1}{2}}$ .

**Preuve** - Traitons le cas où  $k \geq 3$ , le cas  $k = 2$  étant trivial. Les deux membres de l'égalité à démontrer sont multiplicatifs en  $a \in (\mathbb{Z}/2^k\mathbb{Z})^*$ . Il suffit

donc de montrer le résultat pour un système de générateurs de  $(\mathbb{Z}/2^k\mathbb{Z})^*$ , à savoir 5 et  $-1$  où 5 est d'ordre  $2^{k-2}$ .

Premier cas :  $a = -1$

La permutation  $m_{-1}$  est un produit de transpositions dont les points fixes sont exactement 0 et  $2^{k-1}$ . Donc

$$sg(m_{-1}) = (-1)^{\frac{2^k-2}{2}} = -1.$$

deuxième cas  $a = 5$

Soit  $x$  un élément non-nul de  $\mathbb{Z}/2^k\mathbb{Z}$  et  $\tilde{x} \in \mathbb{Z}$  un représentant de  $x$ . Alors la valuation 2-adique de  $\tilde{x}$  ne dépend pas du représentant choisi et on pose  $v_2(x) = v_2(\tilde{x})$ .

On introduit pour chaque entier  $r$  entre 0 et  $k$  :

$$X_r := \{x \in \mathbb{Z}/2^k\mathbb{Z} ; v_2(x) = r\}.$$

On a pour tout  $r$  entre 0 et  $k-2$  :

$$X_r = \{\pm 2^r 5, \pm 2^r 5^2, \dots, \pm 2^r 5^{2^{k-r-2}}\},$$

et pour  $r = k-1$  et  $k$  ; on a

$$X_{k-1} = \{2^{k-1}\} \quad \text{et} \quad X_k = \{2^k = 0\}.$$

Les  $X_r$  sont stables par  $m_5$  :  $m_5(X_r) = X_r$ . En outre, pour  $r \in \{0, 1, \dots, k-3\}$  l'action de  $m_5$  sur  $X_r$  est le produit de deux cycles de même longueur

$2^{k-r-2}$  :

$$(2^r 5, 2^r 5^2, \dots, 2^r 5^{2^{k-r-2}} = 2^r)(-2^r 5^2, \dots, -2^r 5^{2^{k-r-2}} = -2^r).$$

Tandis que pour  $r \geq k - 2$ ,  $m_5$  agit sur  $X_r$  comme l'identité. Par suite  $m_5$  est une permutation paire.

**Lemme 1.4** *Soient  $X'$  et  $X''$  deux ensembles finis,  $\sigma'$  une permutation de  $X'$  et  $\sigma''$  une permutation de  $X''$ . On pose  $X = X' \times X''$ , et on note  $\sigma$  la permutation de  $X' \times X''$  :*

$$(x', x'') \rightarrow (\sigma'(x'), \sigma''(x'')).$$

*Si  $\epsilon$  (resp.  $\epsilon', \epsilon''$ ) est la signature de  $\sigma$  (resp.  $\sigma', \sigma''$ ), on a :*

$$\epsilon = \epsilon'^{|X''|} \cdot \epsilon''^{|X'|}.$$

**Preuve** - On munit  $X$  de l'ordre lexicographique, on note  $I$  l'ensemble des inversions de  $\sigma$ , c'est-à-dire l'ensemble des couples  $(a, b)$  d'éléments de  $X$  tels que  $a$  est strictement plus petit que  $b$  mais  $\sigma(a)$  est plus grand que  $\sigma(b)$ . Il est alors facile de voir que  $|I|$  est  $|X''|^2 |I'| + |X'| |I''|$  où  $I'$  (resp.  $I''$ ) est le nombre d'inversions de  $\sigma'$  (resp.  $\sigma''$ ). Sachant que  $(-1)^{|I|}$  (resp.  $(-1)^{|I'|}$ ,  $(-1)^{|I''|}$ ) est la signature de  $\sigma$  (resp.  $\sigma', \sigma''$ ) d'après l'une des définitions usuelles de la signature, on a immédiatement le résultat.

**Preuve du lemme 1.1** - Si  $n = 2^k m$  où  $m$  est impair, on prend  $X' = \mathbb{Z}/2^k\mathbb{Z}$  et  $X'' = \mathbb{Z}/m\mathbb{Z}$  de sorte que  $\mathbb{Z}/n\mathbb{Z}$  soit identifié à  $X' \times X''$ . Maintenant d'après le lemme 1.3, la signature de la permutation de  $\mathbb{Z}/n\mathbb{Z}$  qui est la multiplication par  $a$  est donnée par

$$(-1)^{\left(\frac{n}{2}+1\right)\left(\frac{a-1}{2}\right)}.$$

### Symboles des restes quadratiques:

Soit  $K$  un corps de nombres ou un corps de fonctions sur un corps fini.

Le symbole des restes quadratiques est classiquement défini de la façon suivante : soit  $\mathcal{P}$  un idéal premier de l'anneau des entiers de  $K$ . Pour tout  $x \in K$ .

$$\left(\frac{x}{\mathcal{P}}\right) := \begin{cases} 1 & \text{si } x \in K^{\cdot 2} \text{ ou si } \mathcal{P} \text{ se décompose dans } K(\sqrt{x}) \\ -1 & \text{si } x \notin K^{\cdot 2} \text{ et } \mathcal{P} \text{ est inerte dans } K(\sqrt{x}) \\ 0 & \text{si } x \notin K^{\cdot 2} \text{ et } \mathcal{P} \text{ se ramifie dans } K(\sqrt{x}) \end{cases}$$

Il est possible pour n'importe quel corps local  $E$  à corps résiduel fini de définir le symbole des restes quadratiques de la façon suivante :

pour tout  $x \in E$ , si  $\mathcal{P}_E$  désigne l'idéal maximal de  $E$ ,

$$\left(\frac{x}{\mathcal{P}_E}\right) := \begin{cases} 1 & \text{si } x \in E^{\cdot 2} \\ -1 & \text{si } E(\sqrt{x})/E \text{ est quadratique non ramifiée} \\ 0 & \text{si } E(\sqrt{x})/E \text{ est ramifiée.} \end{cases}$$

**Proposition 1.5** Si  $\left(\frac{x}{\mathcal{P}_E}\right)$  et  $\left(\frac{y}{\mathcal{P}_E}\right)$  sont non nuls, alors

$$\left(\frac{xy}{\mathcal{P}_E}\right) = \left(\frac{x}{\mathcal{P}_E}\right) \cdot \left(\frac{y}{\mathcal{P}_E}\right).$$

**Preuve** - Par hypothèse  $E(\sqrt{x}, \sqrt{y})/E$  est une extension non-ramifiée donc  $E(\sqrt{xy})/E$  est aussi non-ramifiée.

Si l'extension  $E(\sqrt{xy})/E$  est triviale, alors les deux corps  $E(\sqrt{x})$  et  $E(\sqrt{y})$  coïncident de sorte que

$$1 = \left(\frac{xy}{\mathcal{P}_E}\right) = \left(\frac{x}{\mathcal{P}_E}\right) \cdot \left(\frac{y}{\mathcal{P}_E}\right).$$

Si l'extension  $E(\sqrt{xy})/E$  est quadratique, comme il n'y a qu'une seule extension quadratique non-ramifiée d'un corps local, l'une des extensions  $E(\sqrt{x})/E$  et  $E(\sqrt{y})/E$  est triviale tandis que l'autre est quadratique non-ramifié. On a alors

$$-1 = \left(\frac{xy}{\mathcal{P}_E}\right) = \left(\frac{x}{\mathcal{P}_E}\right) \cdot \left(\frac{y}{\mathcal{P}_E}\right).$$

**Remarque 1.6** Soit  $K$  un corps de nombres, soit  $\mathcal{P}$  un idéal premier de l'anneau des entiers de  $K$ . Soit  $x$  un élément de l'anneau des entiers  $A_K$  de  $K$  qui est premier à  $\mathcal{P}$ . Il est très important de souligner que le symbole de Jacobi généralisé coïncide avec le symbole des restes quadratiques, c'est-à-dire  $\left(\frac{x}{\mathcal{P}}\right) = \left(\frac{x}{\mathcal{P}}\right)$ . En effet, soit  $A_{K_{\mathcal{P}}}$  l'anneau de valuation du complété  $K_{\mathcal{P}}$ . D'après (1.3), l'égalité  $\left(\frac{x}{\mathcal{P}}\right) = 1$  signifie que  $x$  est un carré modulo

$\mathcal{P}$ , ce qui, d'après le lemme de Hensel, revient à dire que l'unité  $\mathcal{P}$ -adique  $x$  est un carré de  $A_{K_{\mathcal{P}}}$ . Autrement dit  $\left(\frac{x}{\mathcal{P}}\right) = 1$ .

Afin de donner une interprétation du symbole des restes quadratiques  $\left(\frac{x}{\mathcal{P}}\right)$  par le biais du symbole d'Artin, rappelons la définition classique du symbole d'Artin:

Soit  $L/K$  une extension abélienne de degré fini de groupe de Galois  $G$ . Soit  $\mathcal{P}$  un idéal premier de  $K$  non-ramifié dans  $L$  de corps résiduel fini,  $\mathfrak{P}$  un idéal premier de  $L$  au-dessus de  $\mathcal{P}$ . Le groupe de décomposition  $D_{\mathfrak{P}}(L/K)$  de  $\mathfrak{P}$  ne dépend que de  $\mathcal{P}$  et est isomorphe au groupe de Galois de l'extension des corps résiduels  $\bar{L}/\bar{K}$  qui est cyclique engendré par l'automorphisme de Frobenius relatif

$$x \mapsto x^{N_K(\mathcal{P})}$$

où  $N_K(\mathcal{P})$  est la norme absolue de  $\mathcal{P}$ .

Soit  $s_{\mathcal{P}}$  l'élément de  $D_{\mathfrak{P}}(L/K)$  correspondant au générateur  $x \mapsto x^{N_K(\mathcal{P})}$ , il est caractérisé par la propriété suivante:

$$s_{\mathcal{P}}(b) \equiv b^{N_K(\mathcal{P})} \pmod{\mathcal{P}}$$

pour tout  $b$  appartenant à l'anneau des entiers de  $L$ .  $s_{\mathcal{P}}$  ne dépend que de  $\mathcal{P}$ , est noté par  $(\mathcal{P}, L/K)$  et est appelé le symbole d'Artin de  $\mathcal{P}$  dans  $G$ . On étend l'application  $\mathcal{P} \rightarrow (\mathcal{P}, L/K)$  par multiplicativité au groupe des idéaux fractionnaires de  $K$  qui sont premiers avec le discriminant de l'extension

$L/K$ .

Si  $\mathfrak{a} = \prod_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}}$ , alors  $(\mathfrak{a}, L/K) = \prod_{\mathcal{P}} (\mathcal{P}, L/K)^{e_{\mathcal{P}}}$ .

Le symbole d'Artin satisfait à la propriété fonctorielle suivante [14] qu'on utilisera fréquemment:

soit  $L/K$  une extension abélienne et  $E/K$  une extension finie. Soit  $\mathcal{P}$  un idéal premier de  $K$  non-ramifié dans  $L$  et  $\mathfrak{q}$  un idéal premier de  $E$  au-dessus de  $\mathcal{P}$ . On a alors :

$$res_L(\mathfrak{q}, LE/E) = (N_{E/K}(\mathfrak{q}), L/K)$$

Où  $res_L$  désigne la restriction à  $L$ .

Le symbole  $\left(\frac{x}{\mathcal{P}}\right)$  peut être lié au symbole d'Artin dans le cas où  $\left(\frac{x}{\mathcal{P}}\right) \neq 0$  et cela de la manière suivante:

On pose  $L := K(\sqrt{x})$ , alors  $(\mathcal{P}, L/K)(\sqrt{x})/\sqrt{x}$  est égal à 1 ou  $-1$  suivant que  $\mathcal{P}$  est totalement décomposé ou inerte dans  $L$ . On a donc:

$$(\mathcal{P}, K(\sqrt{x})/K)(\sqrt{x}) = \left(\frac{x}{\mathcal{P}}\right) (\sqrt{x}).$$

Nous concluons ce chapitre par une proposition qui sera utile pour la suite.

Soit  $F/E$  une extension de corps locaux à corps résiduel fini et de caractéristique résiduelle différente de 2. Notons  $e$  l'indice de ramification de  $F/E$  et  $N_{F/E}$  l'application norme de  $F/E$ . Nous avons alors [8, Chap. 4,

§3.1].

**Proposition 1.7** *Pour toute unité  $u$  de  $F$ , on a*

$$\left( \frac{N_{F/E}(u)}{\mathcal{P}_E} \right) = \left( \frac{u}{\mathcal{P}_F} \right)^e.$$

**Preuve** - Soit  $\pi_E$  une uniformisante de  $E$  et  $\pi_F$  une uniformisante de  $F$ .

Rappelons que le symbole de Hilbert est défini de la façon suivante : si  $v_{\mathcal{P}_E}$  est la valuation  $\mathcal{P}_E$ -adique de  $E$ , on a : pour tout  $a$  et  $b$ ,  $a = a_0\pi_E^{v_{\mathcal{P}_E}(a)}$  et  $b = b_0\pi_E^{v_{\mathcal{P}_E}(b)}$  où  $a_0$  et  $b_0$  sont des unités de  $E$ . On a :

$$\left( \frac{a, b}{\mathcal{P}_E} \right) = \left( \frac{-1}{\mathcal{P}_E} \right)^{v_{\mathcal{P}_E}(a)v_{\mathcal{P}_E}(b)} \left( \frac{a_0}{\mathcal{P}_E} \right)^{-v_{\mathcal{P}_E}(b)} \left( \frac{b_0}{\mathcal{P}_E} \right)^{v_{\mathcal{P}_E}(a)}.$$

$$\left( \frac{N_{F/E}(u)}{\mathcal{P}_E} \right) = \left( \frac{N_{F/E}(u), \pi_E}{\mathcal{P}_E} \right) = \left( \frac{u, \pi_E}{\mathcal{P}_F} \right) [8, \text{Chap. 4, §3.1, lemme 1].$$

Sachant que  $\pi_E = \pi_F^e \epsilon$  où  $\epsilon$  est une unité de  $F$ , on a bien:

$$\left( \frac{N_{F/E}(u)}{\mathcal{P}_E} \right) = \left( \frac{u, \pi_F^e \epsilon}{\mathcal{P}_F} \right) = \left( \frac{u, \pi_F}{\mathcal{P}_F} \right)^e = \left( \frac{u}{\mathcal{P}_F} \right)^e.$$

## Chapitre II

### Symboles des restes quadratiques et discriminants (Cas des indices de ramification impairs)

Soit  $L$  un corps de nombres de degré  $n$  sur le corps  $Q$  des nombres rationnels de discriminant  $D = D_{L/Q}$ .

Si  $D$  n'est pas un carré, on note  $d$  le discriminant du corps quadratique  $Q(\sqrt{D})$ , sinon on pose  $d = 1$ .

Soit  $p$  un nombre premier non ramifié dans  $L$  de sorte que le symbole  $\left(\frac{D}{p}\right)$  soit non nul. Un théorème déjà ancien dû à A. Pellet, L. Stickelberger et G. Voronoi ([4, page 245]) montre que la parité du nombre  $g$  d'idéaux de  $L$  au-dessus de  $p$  est déterminé par ce symbole  $\left(\frac{D}{p}\right)$  : En effet, nous avons  $\left(\frac{D}{p}\right) = (-1)^{n-g}$ . Supposons que  $p$  n'est pas sauvagement ramifié dans  $L$ .

Soit  $(p) = \prod_{i=1}^g \mathfrak{P}_i^{e_i}$  la décomposition de  $p$  en produit d'idéaux premiers  $\mathfrak{P}_i$  de  $L$ . Si  $f_i$  désigne le degré résiduel de  $\mathfrak{P}_i$  dans l'extension  $L/Q$ , alors la valuation  $p$ -adique du discriminant  $D$  est donnée par

$$v_p(D) = \sum_{i=1}^g (e_i - 1)f_i.$$

Donc le symbole  $\left(\frac{d}{p}\right)$  est non nul dès que tous les indices de ramifications  $e_i$  sont impairs. Dans ce dernier cas, généralisant une série de résultats (Wahlin ([16], Hasse [7], Bühler [2]) P. Barrucand et F. Laubie ont établi la formule

suivante (également valable dans le cas relatif) [1]:

$$\left(\frac{d}{p}\right) = (-1)^F \left(\frac{p}{E}\right)$$

avec  $E = \prod_{2 \nmid f_i} e_i$  et  $F = \sum_{2 \mid f_i} 1$ .

Nous reprenons dans ce chapitre la preuve de la formule précédente en donnant une démonstration qui est différente en ce sens que le lemme principal à savoir le lemme 2 de [1] est démontré de façon beaucoup plus simple.

**Résumé.** Dans la preuve de la formule principale de [1] dans le cas relatif, on est amené à faire une étude en trois étapes basée sur la complétion, le dévissage et la globalisation. Soit  $F/E$  une extension de corps  $\mathcal{P}$ -adiques de degré  $n$ , on note  $\mathcal{P}_E$  l'idéal de valuation de  $E$  et  $q_E$  le cardinal de son corps résiduel. Soit  $\delta_{F/E}$  la classe du discriminant de  $F/E$  modulo les carrés. Lorsque  $F/E$  une extension totalement modérément ramifiée de degré impair  $n$ , alors on établit d'abord l'égalité  $\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{q_E}{n}\right)$ . Puis par dévissage, on obtient  $\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = (-1)^{1+f} \left(\frac{q_E}{e}\right)^f$  lorsque le degré résiduel  $f > 1$ . Enfin, la globalisation nous permet d'énoncer la formule de [1] dans le cas relatif. Soit  $K$  un corps de nombres et  $L/K$  une extension de degré  $n$ . Soit  $\delta = \delta_{L/K}$  la classe du discriminant d'une  $K$ -base de  $L$  modulo les carrés. C'est un invariant de  $L/K$  qui définit une extension quadratique ou triviale  $K(\sqrt{\delta})/K$ . Soit  $\mathfrak{p}$  un idéal premier de  $K$  qui n'est pas sauvagement ramifié dans  $L$  et soit  $\mathfrak{p} = \mathfrak{P}^{e_1} \cdots \mathfrak{P}_g^{e_g}$  la décomposition de  $\mathfrak{p}$  en produit d'idéaux premiers deux à deux distincts  $\mathfrak{P}_i$  de  $L$  avec  $f_i$  le degré résiduel de  $\mathfrak{P}_i$ . Si tous les indices de

ramification  $e_i$  sont impairs, on a alors :

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \prod_{i=1}^g (-1)^{1+f_i} \left(\frac{q}{e_i}\right)^{f_i} = (-1)^F \left(\frac{q}{E}\right)$$

où  $q$  est la norme absolue de  $\mathfrak{p}$ ,  $F = \sum_{2|f_i} 1$  et  $E = \prod_{2 \nmid f_i} e_i$ .

### Généralisation du théorème de Pellet, Stickelberger et Voronoi:

Soit  $K$  un corps de nombres et  $L$  une extension finie de  $K$  de degré  $n$ . Soit  $\{b_1, \dots, b_n\}$  une base du  $K$ -espace vectoriel  $L$ . Le discriminant  $D = D_{L/K} = \det(\text{Tr}_{L/K}(b_i b_j))$  est un élément non nul de  $K$  :  $D \in K$  la classe  $\delta = \delta_{L/K}$  de  $D$  modulo  $K^2$  est indépendante du choix de la base. C'est donc un invariant de  $L/K$  qui définit une extension quadratique ou triviale  $K(\sqrt{\delta})/K$ .

Soit  $\mathfrak{p}$  un idéal premier de  $K$  et soit  $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$  la décomposition de l'idéal  $\mathfrak{p}$  en produit d'idéaux premiers deux à deux distincts  $\mathfrak{P}_i$  de  $L$ . On note  $f_i$  le degré résiduel de  $\mathfrak{P}_i$  de sorte que  $n = e_1 f_1 + \cdots + e_g f_g$ .

**Théorème 2.1** *Supposons que  $\mathfrak{p}$  n'est pas sauvagement ramifié dans  $L$  et que tous les indices de ramification  $e_i$  soient impairs, on a alors*

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \prod_{i=1}^g (-1)^{1+f_i} \left(\frac{q}{e_i}\right)^{f_i} = (-1)^F \left(\frac{q}{E}\right)$$

où  $q$  est la norme absolue de  $\mathfrak{p}$ ,  $F = \sum_{2|f_i} 1$  et  $E = \prod_{2 \nmid f_i} e_i$ .

Pour démontrer le théorème 2.1, on a besoin de certains résultats locaux.

### Études locales:

Tous les corps locaux qu'on considère sont des corps  $\mathcal{P}$ -adiques de caractéristique résiduelle  $p$ .

Pour tout corps local  $E$ , on note  $\mathcal{P}_E$  son idéal de valuation et  $q_E$  le cardinal de son corps résiduel. Soit  $E$  un corps local, et  $F$  une extension finie de  $E$  de degré  $n$ . Soit  $x$  un élément primitif de  $F$  sur  $E$ . Soit  $x_1 = x, x_2, \dots, x_n$  les conjugués de  $x$  dans une clôture algébrique de  $F$ .

Soit  $X = \prod_{i < j} (x_i - x_j)$ ,  $X^2$  est le discriminant de la base  $(1, x, \dots, x^{n-1})$  de  $F$  sur  $E$  et  $\delta_{F/E}$  est l'image de  $X^2$  dans  $E^\cdot/E^{\cdot 2}$ .

**Lemme 2.2** *Si l'extension  $F/E$  est non ramifiée, alors on a :*

$$\left( \frac{\delta_{F/E}}{\mathcal{P}_E} \right) = (-1)^{1+n}.$$

**Preuve** - Si l'extension  $F/E$  est non ramifiée alors elle est cyclique et on a

$$\left( \frac{\delta_{F/E}}{\mathcal{P}_E} \right) \neq 0.$$

Soit  $\sigma$  un générateur de son groupe de Galois. Il est clair que  $\left( \frac{\delta_{F/E}}{\mathcal{P}_E} \right) = 1$  si et seulement si  $X^2$  est un carré dans  $E$  ou encore si et seulement si  $\sigma$

est une permutation paire de l'ensemble  $\{x_1, \dots, x_n\}$  ; donc  $\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right)$  n'est autre que la signature de cette permutation ; or  $\sigma$  permute circulairement les congugués de  $x$  ; donc on a bien

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = (-1)^{1+n}.$$

**Lemme 2.3** *Supposons que l'extension  $F/E$  soit non ramifiée et désignons par  $N_{F/E}$  l'application norme de l'extension  $F/E$ . Soit  $x \in F/F^2$ . Alors on a*

$$\left(\frac{x}{\mathcal{P}_F}\right) = \left(\frac{N_{F/E}(x)}{\mathcal{P}_E}\right)$$

dans les deux cas suivants :

(i) Si  $x = 1$ ;

(ii) Si  $\left(\frac{x}{\mathcal{P}_F}\right) \neq 0$  et si  $n$  est impair.

**Preuve** - Le premier cas étant évident, traitons le second. Posons  $u = N_{F/E}(x) \in E/E^2$ . Rappelons que le choix d'une uniformisante de  $E$  (resp. de  $F$ ) permet d'identifier  $E$  (resp.  $F$ ) à  $\mathbb{Z} \times U_E$  (resp.  $\mathbb{Z} \times U_F$ ) où  $U_E$  (resp.  $U_F$ ) désigne le groupe des unités de  $E$  (resp. de  $F$ ). On a donc des isomorphismes

$$E/E^2 \simeq \mathbb{Z}/2\mathbb{Z} \times U_E/U_E^2, F/F^2 \simeq \mathbb{Z}/2\mathbb{Z} \times U_F/U_F^2$$

et l'hypothèse  $\left(\frac{x}{\mathcal{P}_F}\right) \neq 0$  signifie alors que  $x \in U_F/U_F^2$ .

Maintenant, tout  $E$ -automorphisme  $\sigma$  de  $F$  induit un automorphisme du groupe  $U_F/U_F^2$  et on a

$$\left(\frac{\sigma(x)}{\mathcal{P}_F}\right) = \left(\frac{x}{\mathcal{P}_F}\right).$$

Donc

$$\left(\frac{N_{F/E}(x)}{\mathcal{P}_F}\right) = \left(\frac{x}{\mathcal{P}_F}\right)^n.$$

Enfin, si  $n$  est impair, on a  $U_F^2 \cap U_E = U_E^2$  de sorte que

$$\left(\frac{N_{F/E}(x)}{\mathcal{P}_E}\right) = \left(\frac{N_{F/E}(x)}{\mathcal{P}_F}\right) = \left(\frac{x}{\mathcal{P}_F}\right)^n = \left(\frac{x}{\mathcal{P}_F}\right).$$

**Lemme 2.4** *On suppose que  $n$  est impair et que l'extension  $F/E$  est totalement et modérément ramifiée ; on a alors*

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{q_E}{n}\right).$$

Nous donnons pour ce lemme deux preuves, la première est celle faite dans [1], et la seconde est une démonstration plus directe.

**1ère preuve** - Si l'extension  $F/E$  est totalement et modérément ramifiée alors il existe une uniformisante  $\pi$  de  $E$  telle que  $x := \pi^{1/n}$  est une uniformisante de  $F$  avec  $F = E(x)$  [17, Chap. 3, Prop. 3.4.3]. Il en résulte que la clôture normale  $N$  de  $F$  s'obtient en adjoignant à  $F$  une racine primitive  $n$ -ième de l'unité  $\zeta_n$ . Comme  $p \nmid n$ , l'extension  $E(\zeta_n)$  est non ramifiée, le

corps d'inertie de  $N/E$  est  $E(\zeta_n)$  et  $N$  est l'extension composée des deux extensions linéairement disjointes  $F$  et  $E(\zeta_n)$  sur  $E$ . [14, Chap.4, § 4]. De plus le groupe de Galois de  $N$  sur  $E$  possède deux générateurs  $\sigma$  qui engendrent son sous-groupe d'inertie et  $\tau$  dont le corps des invariants est  $F$  et qui vérifie  $\tau(\zeta_n) = \zeta_n^{q_E}$  [14, Chap. 4, § 4].

On a tout d'abord  $\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) \neq 0$  parce que, l'indice de ramification  $[N : E(\zeta_n)] = n$  de  $N/E$  étant impair, il n'existe pas de sous extension quadratique ramifiée de  $N/E$ . En outre  $X = \prod_{1 \leq i < j \leq n} (x_i - x_j)$  est un élément de  $E(\zeta_n)$ .

On en déduit, comme dans la démonstration du lemme 2.2, que  $\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right)$  n'est autre que la signature de  $\tau$  considéré comme une permutation de l'ensemble des conjugués de  $x$  sur  $E$ . Or les conjugués de  $x$  sur  $E$  sont  $\zeta_n^k x$  pour  $k = 0, 1, \dots, n-1$ . Donc si on identifie le groupe des racines  $n$ -ième de l'unité de  $E(\zeta_n)$  à  $\mathbb{Z}/n\mathbb{Z}$ ,  $\tau$  devient la multiplication par  $q_E$  qui est une permutation de  $\mathbb{Z}/n\mathbb{Z}$  de signature  $\left(\frac{q_E}{n}\right)$  [3]. Il en résulte que

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{q_E}{n}\right).$$

Nous allons maintenant donner une deuxième démonstration de ce lemme basée sur la connaissance explicite du discriminant numérique de l'extension  $F/E$ .

**2ème preuve** - Si  $F/E$  est totalement et modérément ramifiée alors  $F =$

$E(\sqrt[n]{\pi})$  où  $\pi$  désigne une uniformisante de  $E$  [17, Chap. 3, Prop. 3.4.3]. Le discriminant du polynôme  $X^n - \pi$  est égal à  $(-1)^{\frac{n(n-1)}{2}} n^n \pi^{n-1}$ . Comme  $n$  est impair,

$$\delta_{F/E} = (-1)^{\frac{n(n-1)}{2}} n \pmod{E^2}.$$

Remarquons tout d'abord que  $\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) \neq 0$  car l'extension  $E(\sqrt{\delta_{F/E}})/E$  est égale à l'extension  $E(\sqrt{(-1)^{\frac{n-1}{2}} n})/E$  qui est non ramifiée [12, Cor. p. 222].

Si  $p$  est la caractéristique résiduelle de  $E$ ,  $q_E = p^f$  où  $f$  est le degré résiduel de  $E/Q_p$ .

Soit  $E_0$  le corps d'inertie de  $E/Q_p$ . Pour la même raison que précédemment  $E_0(\sqrt{\delta_{F/E}})/E_0$  est non ramifiée et donc,

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{\delta_{F/E}}{\mathcal{P}_{E_0}}\right).$$

Si  $f$  est impair et  $p \neq 2$ , d'après le lemme 2.3 du chapitre II

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{(-1)^{\frac{n-1}{2}} n}{\mathcal{P}_{E_0}}\right) = \left(\frac{(-1)^{\frac{n-1}{2}} n}{p}\right)^f = \left(\frac{(-1)^{\frac{n-1}{2}} n}{q_E}\right),$$

et d'après la loi de réciprocité quadratique de Gauss,

$$\left(\frac{(-1)^{\frac{n-1}{2}} n}{q_E}\right) = \left(\frac{q_E}{n}\right),$$

d'où

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{q_E}{n}\right).$$

Si  $f$  est impair et  $p = 2$ , comme précédemment et d'après le lemme 2.3 du

chapitre II :

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{\delta_{F/E}}{\mathcal{P}_{E_0}}\right) = \left(\frac{(-1)^{\frac{n-1}{2}}n}{\mathcal{P}_{E_0}}\right) = \left(\frac{(-1)^{\frac{n-1}{2}}n}{2}\right).$$

De plus :

$$\left(\frac{(-1)^{\frac{n-1}{2}}n}{2}\right) = (-1)^{\frac{n^2-1}{8}} = \left(\frac{2}{n}\right) = \left(\frac{q_E}{n}\right)$$

d'où  $\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{q_E}{n}\right)$ .

Enfin, traitons le cas où  $f$  est pair:

Remarquons d'abord que  $Q_p(\sqrt{(-1)^{\frac{n-1}{2}}n})/Q_p$  est une extension non ramifiée [12, Cor. p. 222]. De plus  $f$  étant pair,  $E_0$  contient l'unique extension quadratique non ramifiée de  $Q_p$ , par suite l'extension  $Q_p(\sqrt{(-1)^{\frac{n-1}{2}}n})/Q_p$  est soit triviale ou incluse dans  $E_0$ . On a donc :

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = \left(\frac{(-1)^{\frac{n-1}{2}}n}{\mathcal{P}_{E_0}}\right) = 1 = \left(\frac{q_E}{n}\right).$$

**Lemme 2.5** *On suppose maintenant que l'indice de ramification  $e$  de  $F/E$  est impair. Soit  $f$  le degré résiduel de  $F/E$  ; alors on a*

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = (-1)^{1+f} \left(\frac{q_E}{e}\right)^f.$$

**Preuve** - Soit  $E'$  le corps d'inertie de  $F/E$  ; on a  $[F : E'] = e$  et  $[E' : E] = f$ .

D'après la formule de transitivité des discriminants [12, Chap.5, § 1, Prop. 5.7 iii], on a

$$\delta_{F/E} = \delta_{E'/E}^e N_{E'/E}(\delta_{F/E}) \in U_E/U_E^2,$$

et les égalités suivantes résultant alors immédiatement des lemmes 2.2, 2.3

et 2.4 :

$$\begin{aligned} \left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) &= \left(\frac{\delta_{E'/E}}{\mathcal{P}_E}\right)^e \cdot \left(\frac{N_{E'/E}(\delta_{F/E'})}{\mathcal{P}_E}\right) . \\ \left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) &= \left(\frac{\delta_{E'/E}}{\mathcal{P}_E}\right)^e \cdot \left(\frac{\delta_{F/E'}}{\mathcal{P}}\right) \\ \left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) &= (-1)^{1+f} \left(\frac{q_E}{e}\right)^f . \end{aligned}$$

D'où le lemme.

### **Globalisation:**

Nous pouvons maintenant achever la démonstration du théorème 2.1. Nous reprenons les hypothèses et les notations de son énoncé.

Soit  $\hat{K}$  le complété du corps de nombres  $K$  en la place  $\mathfrak{p}$  et  $\hat{\mathfrak{p}}$  l'idéal de valuations de  $\hat{K}$ . Pour tout  $i = 1, \dots, g$ , soit  $\hat{L}_i$  le complété du corps  $L$  en la place  $\mathfrak{P}_i$  ;  $\hat{L}_i$  est une extension de  $\hat{K}$  de degré  $e_i f_i$ , on pose  $\delta_i = \delta_{\hat{L}_i/\hat{K}}$ .

Compte-tenu du lemme 2.5, il nous suffit de prouver que :

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \prod_{i=1}^g \left(\frac{\delta_i}{\hat{\mathfrak{p}}}\right) .$$

Pour tout  $i = 1, \dots, g$  désignons par  $Tr_i$  l'application trace de l'extension  $\hat{L}_i/\hat{K}$ . On sait que les  $\hat{K}$ -algèbres  $L \otimes_K \hat{K}$  et  $\prod_{i=1}^g \hat{L}_i$  sont canoniquement isomorphes et que, pour tout  $x \in L$ , on a

$$Tr_{L/K}(x) = \sum_{i=1}^g Tr_i(x) .$$

Soit  $Tr(xy)$  la forme  $Tr_{L/K}(xy)$  sur  $L$  par extension des scalaires ;  $Tr(xy)$  est somme directe des formes bilinéaires  $Tr_i(xy)$  sur les  $\hat{L}_i$ . Par suite, si, pour tout  $i = 1, \dots, g$  on se donne une base  $\beta_i$  de  $\hat{L}_i$  sur  $\hat{K}$ ,  $\beta := \cup \beta_i$  est alors une base de  $L \otimes_K \hat{K}$  sur  $\hat{K}$  dont le discriminant par rapport à  $Tr(xy)$  est  $\prod_{i=1}^g D_{\hat{L}_i/\hat{K}}(\beta_i)$ . On en déduit aussitôt que :

$$\delta_{L/K} = \prod_{i=1}^g \delta_i$$

ce qui achève la démonstration.

**Théorème 2.6** *Supposons que  $p$  ne soit pas sauvagement ramifié dans  $L$  et que tous les indices de ramification  $e_i$  soient impairs ; on a alors*

$$\left(\frac{d}{p}\right) = \prod_{i=1}^g (-1)^{1+f_i} \left(\frac{p}{e_i}\right)^{f_i} = (-1)^F \cdot \left(\frac{p}{E}\right)$$

avec  $E = \prod_{2 \nmid f_i} e_i$  et  $F = \sum_{2 \nmid f_i} 1$ .

**Preuve** - Le théorème 2.6 est un cas particulier du théorème 2.1. En effet dans le cas où  $K = Q$ , on a  $\mathfrak{p} = p\mathbb{Z}$  et  $\delta_{L/K}$  est l'image du discriminant absolu  $D$  de  $L$  dans  $Q'/Q'^2$  parce qu'en écrivant  $D = d'a^2$  où  $a$  désigne le plus grand entier tel que  $a^2$  divise  $D$ , on a

- $d = d'$  si  $d' \equiv 1 \pmod{4}$  et
- $d = 4d'$  si  $d' \equiv 2$  ou  $3 \pmod{4}$ .

On en déduit aussitôt que

$$\left(\frac{\delta_{L/Q}}{\mathfrak{p}}\right) = \left(\frac{d'}{p}\right) = \left(\frac{d}{p}\right) \text{ si } p \neq 2.$$

Dans le cas où  $p = 2$ , 2 est modérément ramifié dans  $L$  donc aussi dans la clôture normale  $N$  de  $L$  ; or  $Q(\sqrt{D}) \subseteq N$ , donc 2 est modérément ramifié dans  $Q(\sqrt{D})$  ce qui n'est possible que si 2 est non ramifié dans  $Q(\sqrt{D})$ , il s'ensuit que  $d = d'$  et donc que

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \left(\frac{d}{2}\right) = (-1)^{(d^2-1)/8}.$$

## Chapitre III

### Symboles des restes quadratiques et discriminants (Cas des indices de ramification quelconques)

Notre but dans ce chapitre est de donner une formule analogue à la formule de [1] sans aucune hypothèse sur la parité des indices de ramification.

Soit  $K$  un corps de nombres et  $L$  une extension finie de degré  $n$ . Soit  $\mathfrak{p}$  un idéal premier de  $K$  et soit  $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$  la décomposition de l'idéal  $\mathfrak{p}$  en produits d'idéaux premiers deux à deux distincts  $\mathfrak{P}_i$  de  $L$ . On note  $f_i$  le degré résiduel de  $\mathfrak{P}_i$  de sorte que  $n = e_1 f_1 + \cdots + e_g f_g$ . On désigne par  $\pi$  une uniformisante du complété de  $K$  en  $\mathfrak{p}$ .

**Résumé.** Dans la généralisation de la formule du Théorème 2.1 du chapitre II, au cas où les indices de ramification sont quelconques, on est ramené à introduire le produit  $\prod_{2|e_i} \left( \frac{\pi}{\mathfrak{P}_i} \right)$  où  $\pi$  désigne une uniformisante de  $K_{\mathfrak{p}}$ . Ce produit s'avère être indépendant du choix de l'uniformisante  $\pi$  lorsque  $\sum_{2|e_i} f_i$  est pair, dans ce dernier cas, on définit  $\epsilon_{L/K}(\mathfrak{p})$  comme étant égale au produit  $\prod_{2|e_i} \left( \frac{\pi}{\mathfrak{P}_i} \right)$  et lorsque  $\sum_{2|e_i} f_i$  est impair, on pose  $\epsilon_{L/K}(\mathfrak{p}) = 0$ . On exprime alors  $\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right)$  à l'aide de  $\epsilon_{L/K}(\mathfrak{p})$  dans le cas où la ramification de  $\mathfrak{p}$  dans  $L$  est modérée, c'est en effet le théorème principal du chapitre III

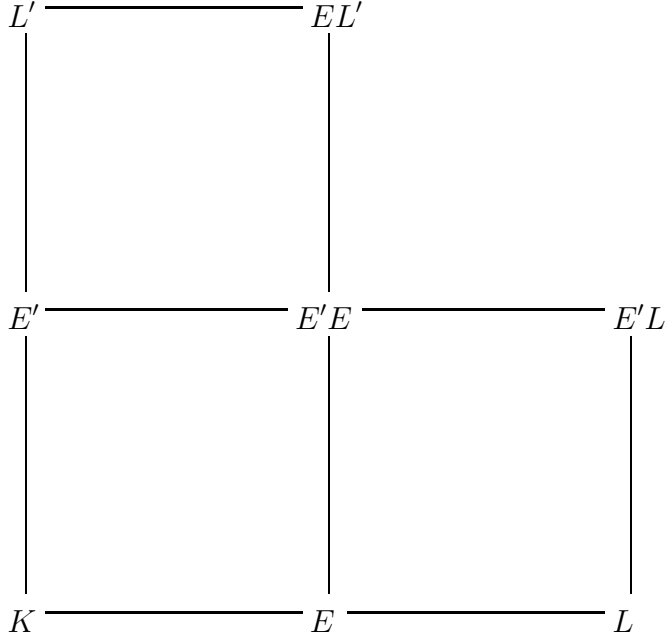
qu'on obtient grâce à certains résultats locaux. Nous établissons ensuite une formule de transitivité pour  $\epsilon_{L/K}(\mathfrak{p})$ , c'est-à-dire si  $K \subseteq M \subseteq L$  est une tour d'extensions de corps de nombres et  $\mathfrak{p}$  un idéal premier de  $K$  et si  $\epsilon_{L/K}(\mathfrak{p})$ ,  $\epsilon_{M/K}(\mathfrak{p})$  ainsi que les  $\epsilon_{L/M}(\mathcal{P})$  pour  $\mathcal{P}|\mathfrak{p}$  sont non nuls, on établit la formule suivante :  $\epsilon_{L/K}(\mathfrak{p}) = \epsilon_{M/K}(\mathfrak{p}) \prod_{2|e(\mathcal{P}/\mathfrak{p})} \epsilon_{L/M}(\mathcal{P})$ . Lorsque  $L/K$  est galoisienne et  $\pi$  désigne une uniformisante de  $K$  en  $\mathfrak{p}$ , le symbole  $\left(\frac{\pi}{\mathfrak{P}_i}\right)$  est indépendant du choix de la place  $\mathfrak{P}_i$  et est égale à  $\rho$  qui ne dépend que de la structure du 2-groupe de Sylow du groupe de décomposition de  $\mathfrak{P}_i$  dans  $L/K$ . De plus on a  $\epsilon_{L/K}(\mathfrak{p}) = \rho^g$  si  $\epsilon_{L/K}(\mathfrak{p}) \neq 0$ . Enfin, nous fournirons à la fin de ce chapitre des familles d'exemples pour lesquels  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$  se lit sur la décomposition de  $\mathfrak{p}$  dans  $L$ .

### Généralisation de la formule de [1]:

Nous commençons par énoncer le lemme d'Abhyankar qui sera utilisé fréquemment

**Lemme (Abhyankar)** - Soit  $K$  un corps local et soient  $L$  et  $L'$  deux extensions finies de  $K$  telles que  $L/K$  est modérément ramifiée et l'indice de ramification  $e = e(L/K)$  divise  $e' = e(L'/K)$ . Alors  $L'L/L'$  est non ramifiée.

**Preuve** - Soit  $E'$  (resp.  $E$ ) le corps d'inertie de  $L'$  (resp. de  $L$ ). On a le diagramme suivant :



En prenant  $K = EE'$ ,  $L = E'L$  et  $L' = EL'$ , on se ramène au cas où  $L/K$  et  $L'/K$  sont totalement ramifiées. Par hypothèse  $L/K$  est modérée, donc il existe une uniformisante  $\pi$  de  $K$  telle que  $L = K(\sqrt[e]{\pi})$ . Soit  $\omega$  une uniformisante de  $L'$ , on a  $\pi = \omega^{e'}u$  où  $u$  est une unité de  $L'$ . Ainsi  $LL' = L'(\sqrt[e]{u})$  car  $e$  divise  $e'$ . Comme  $L/K$  est modérée, la caractéristique résiduelle de  $K$  ne divise pas  $e$ .  $L'(\sqrt[e]{u})/L'$  est une extension non ramifiée [13, Chap. 3, § 5, lemme 5.3], d'où  $LL'/L'$  est non ramifiée.

**Proposition 3.1** *On suppose que l'idéal premier  $\mathfrak{p}$  de  $K$  n'est pas au-dessus de 2. Si  $\sum_{2|e_i} f_i$  est un entier pair, alors  $\prod_{2|e_i} \left( \frac{\pi}{\mathfrak{P}_i} \right)$  est non nul et est indépendant du choix de l'uniformisante  $\pi$ .*

**Preuve** - Soient  $\pi$  et  $\pi'$  deux uniformisantes du complété de  $K$  en  $\mathfrak{p}$ . Posons  $u = \pi/\pi'$ .

Soient  $\mathfrak{P}_i$  une des places de  $L$  au-dessus de  $\mathfrak{p}$ . Désignons par  $K_{\mathfrak{p}}$  et  $L_{\mathfrak{P}_i}$  les complétés de  $K$  et  $L$  en les places  $\mathfrak{p}$  et  $\mathfrak{P}_i$  respectivement.

L'idéal  $\mathfrak{p}$  étant non au-dessus de 2, l'extension  $K_{\mathfrak{p}}(\sqrt{u})/K_{\mathfrak{p}}$  est alors non-ramifiée [12, Cor. p. 222]. On en déduit aussitôt que si le degré résiduel  $f_i$  est pair, alors  $K_{\mathfrak{p}}(\sqrt{u})$  est contenu dans  $L_{\mathfrak{P}_i}$  de sorte que  $\left(\frac{u}{\mathfrak{P}_i}\right) = 1$  ; et que si au contraire  $f_i$  est impair, alors  $[K_{\mathfrak{p}}(\sqrt{u}) : K_{\mathfrak{p}}] = [L_{\mathfrak{P}_i}(\sqrt{u}) : L_{\mathfrak{P}_i}]$  de sorte que  $\left(\frac{u}{\mathfrak{p}}\right) = \left(\frac{u}{\mathfrak{P}_i}\right)$ .

On s'intéresse dans cette proposition qu'aux idéaux premiers  $\mathfrak{P}_i$  avec  $e_i$  pair. Pour un tel idéal premiers  $\mathfrak{P}_i$ , le lemme d'Abhyankar [12, Chap.5, § 2, Cor.4] garantit la non-nullité de  $\left(\frac{\pi}{\mathfrak{P}_i}\right)$  puisqu'il affirme que l'extension  $L_{\mathfrak{P}_i}(\sqrt{\pi})/L_{\mathfrak{P}_i}$  est non-ramifiée.

Supposons maintenant qu'il y a un nombre pair d'idéaux  $\mathfrak{P}_i$  avec  $e_i$  pair et  $f_i$  impair. Alors d'après ce qui précède :

$$\prod_{2|e_i} \left(\frac{u}{\mathfrak{P}_i}\right) = \prod_{\substack{2|e_i \\ 2 \nmid f_i}} \left(\frac{u}{\mathfrak{P}_i}\right) = \prod_{\substack{2|e_i \\ 2 \nmid f_i}} \left(\frac{u}{\mathfrak{p}}\right) = 1.$$

**Définition 3.2** Pour tout idéal premier  $\mathfrak{p}$  de  $K$  non au-dessus de 2, on pose

$$\epsilon_{L/K}(\mathfrak{p}) = \begin{cases} 0 & \text{si } \sum_{2|e_i} f_i \text{ est impair} \\ \prod_{2|e_i} \left( \frac{\pi}{\mathfrak{P}_i} \right) & \text{sinon} \end{cases}$$

On est en mesure maintenant d'énoncer le théorème principal du chapitre III.

**Théorème 3.3** Soit  $\mathfrak{p}$  un idéal premier de  $K$  non au-dessus de 2. On suppose que  $\mathfrak{p}$  n'est pas sauvagement ramifié dans  $L$ . Alors le symbole  $\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right)$  est relié à  $\epsilon_{L/K}(\mathfrak{p})$  par la formule suivante :

$$\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right) = (-1)^{F + \frac{q-1}{2}G} \left( \frac{q}{E} \right) \epsilon_{L/K}(\mathfrak{p}).$$

où  $q$  est la norme absolue de  $\mathfrak{p}$  et les trois entiers  $E$ ,  $F$  et  $G$  sont définis par

$$E = \prod_{\substack{2|e_i \\ 2|f_i}} e_i, \quad F = \sum_{\substack{2|e_i \\ 2|f_i}} 1 \quad \text{et} \quad G = \sum_{\substack{4|e_i \\ 2|f_i}} 1.$$

Pour démontrer le théorème 3.3, on a besoin de certains résultats locaux.

### Études locales:

Tous les corps locaux qu'on considère, sont des corps  $\mathcal{P}$ -adiques de caractéristique résiduelle  $p$ .

Pour tout corps local  $E$ , on note  $\mathcal{P}_E$  son idéal de valuation et  $q_E$  le cardinal de son corps résiduel.

Soit  $E$  un corps local, et  $F$  une extension finie de  $E$  de degré  $n$ . Soit  $x$  un élément primitif de  $F$  sur  $E$ . Soit  $x_1 = x, x_2, \dots, x_n$  les conjugués de  $x$  dans une clôture algébrique de  $F$ . Soit  $X = \prod_{i < j} (x_i - x_j)$ ,  $X^2$  est le discriminant de la base  $(1, x, \dots, x^{n-1})$  de  $F$  sur  $E$  et  $\delta_{F/E}$  l'image de  $X^2$  dans  $E/E^2$ .

**Lemme 3.4** *Soit  $F/E$  une extension de corps locaux. Alors pour chaque uniformisante  $\pi$  de  $E$ , il existe une unité  $u_\pi$  de  $E$  telle que*

$$\delta_{F/E} = \pi^\ell u_\pi \pmod{E^2},$$

où  $\ell$  est la valuation  $\mathcal{P}_E$ -adique de l'idéal discriminant de l'extension  $F/E$ .

**Preuve** - Il suffit de remarquer que l'idéal discriminant est engendré par le discriminant de n'importe quelle base entière de l'anneau de valuation de  $F$  sur celui de  $E$ .

**Remarque** - Supposons que  $F/E$  est une extension modérément ramifiée d'indice de ramification  $e$ . Si l'on suppose que  $e$  est pair, alors l'extension  $F(\sqrt{\pi})/F$  est non-ramifiée de sorte que  $\left(\frac{\pi}{\mathfrak{p}_F}\right) \neq 0$  bien que  $\left(\frac{\pi}{\mathfrak{p}_E}\right) = 0$ .

**Lemme 3.5** *On suppose que l'extension  $F/E$  étant totalement modérément ramifiée de degré  $e$  pair. Alors pour toute uniformisante  $\pi$  de  $E$ , il existe une unité  $u_\pi$  de  $E$  telle que*

$$(i) \delta_{F/E} = \pi u_\pi \pmod{E^2}$$

$$(ii) \left( \frac{u_\pi}{\mathcal{P}_E} \right) = \left( \frac{-1}{q_E} \right)^{\left(\frac{e}{2}+1\right)} \left( \frac{\pi}{\mathcal{P}_F} \right).$$

**Preuve** - L'extension  $F/E$  est totalement et modérément ramifiée, alors on peut choisir  $x = \omega^{1/e}$  comme un élément primitif de  $F$  sur  $E$  où  $\omega$  est une uniformisante de  $E$  [17, Chap. 3, Prop.3.4.3]. Il en résulte que la clôture normale  $N$  de  $F$  s'obtient en adjoignant à  $F$  une racine primitive  $e$ -ième de l'unité  $\zeta_e$ . Comme la caractéristique résiduelle  $p$  de  $E$  ne divise pas  $e$ , l'extension  $E(\zeta_e)/E$  est non-ramifiée, le corps d'inertie de  $N/E$  est  $E(\zeta_e)$  et  $N$  est le composé des deux extensions linéairement disjointes  $F$  et  $E(\zeta_e)$  [14, Chap.4, §4]. De plus d'après le lemme d'Abhyankar [12, Chap.5, §2, cor. 4],  $F(\sqrt{\pi})/F$  est non-ramifiée, et donc l'extension  $N(\sqrt{\pi})/F$  est cyclique puisque c'est la composée de deux extensions non-ramifiées, à savoir  $N/F$  et  $F(\sqrt{\pi})/F$ . Soit  $\tau$  un générateur du groupe de Galois de  $N/F$  vérifiant  $\tau(\zeta_e) = \zeta_e^{q_E}$  [14, Chap.4, § 4], et  $\tilde{\tau}$  un générateur du groupe de Galois de  $N(\sqrt{\pi})/F$  dont la restriction à  $N$  est  $\tau$ . D'après le lemme 3.4, et puisque la valuation  $\mathcal{P}_E$ -adique du discriminant de  $F/E$  dans le cas modéré est  $e - 1$ , on en déduit que pour une uniformisante  $\pi$  de  $E$ , il existe une unité  $u_\pi$  de  $E$  telle que

$$\delta_{F/E} = \pi u_\pi = X^2 \pmod{E^2}$$

$$\text{où } X = \prod_{0 \leq i < j < e} \omega^{1/e} (\zeta_e^i - \zeta_e^j).$$

Nous allons évaluer le symbole  $\left(\frac{u_\pi}{\mathcal{P}_E}\right)$ . Tout d'abord les deux symboles  $\left(\frac{u_\pi}{\mathcal{P}_E}\right)$  et  $\left(\frac{\omega\pi^{-1}}{\mathcal{P}_E}\right)$  sont non-nuls car les deux extensions  $E(\sqrt{u_\pi})/E$  et  $E(\sqrt{\omega\pi^{-1}})/E$  sont non ramifiées (la caractéristique résiduelle de  $E$  est différente de 2) [12, Cor. P. 222].

Par ailleurs

$$\left(\frac{u_\pi}{\mathcal{P}_E}\right) = 1 \Leftrightarrow \frac{X^2}{\pi} \in E(\zeta_e)^2 \quad \text{et} \quad \frac{X^2}{\pi} \in F^{\cdot 2}$$

car  $F \cap E(\zeta_e) = E$ . Or d'une part  $\frac{X^2}{\pi} \in E(\zeta_e)^2$  revient à dire que  $\left(\frac{\omega\pi^{-1}}{\mathcal{P}_E}\right)^f = 1$  où  $f$  est le degré résiduel de  $N/E$ , car

$$\left(\frac{X^2\pi^{-1}}{\mathcal{P}_{E(\zeta_e)}}\right) = \left(\frac{\omega\pi^{-1}}{\mathcal{P}_{E(\zeta_e)}}\right)$$

et d'autre part

$$\left(\frac{\omega\pi^{-1}}{\mathcal{P}_{E(\zeta_e)}}\right) = \left(\frac{\omega\pi^{-1}}{\mathcal{P}_E}\right)^f$$

d'après la proposition 1.7 du chapitre I et d'autre part la condition  $\frac{X^2}{\pi} \in F^{\cdot 2}$  est équivalente à  $\tilde{\tau}\left(\frac{X}{\sqrt{\pi}}\right) = \frac{X}{\sqrt{\pi}}$  ou encore à  $\frac{\tau(X)}{X} = \left(\frac{\pi}{\mathcal{P}_F}\right)$ . Comme les conjugués de  $x$  sur  $E$  sont  $\zeta_e^k x$  pour  $k = 0, \dots, e-1$ ,  $\frac{\tau(X)}{X}$  est la signature de  $\tau$  considérée comme une permutation de  $\mathbb{Z}/e\mathbb{Z}$  induite par la multiplication par  $q_E$ , on a  $\frac{\tau(X)}{X} = \left(\frac{-1}{q_E}\right)^{\left(\frac{e}{2}+1\right)}$  d'après la proposition 1.2 du chapitre I. On déduit de ce qui précède que

$$\left(\frac{u_\pi}{\mathcal{P}_E}\right) = 1 \Leftrightarrow \left(\frac{\omega\pi^{-1}}{\mathcal{P}_E}\right)^f = 1 \quad \text{et} \quad \left(\frac{-1}{q_E}\right)^{\left(\frac{e}{2}+1\right)} \cdot \left(\frac{\pi}{\mathcal{P}_F}\right) = 1.$$

$F/E$  est totalement ramifiée,  $E(\sqrt{\omega\pi^{-1}})/E$  non-ramifiée, donc  $F$  et  $E(\sqrt{\omega\pi^{-1}})$

sont linéairement disjointes sur  $E$  et on a  $\left(\frac{\omega\pi^{-1}}{\mathcal{P}_E}\right) = \left(\frac{\omega\pi^{-1}}{\mathcal{P}_F}\right) = \left(\frac{\pi}{\mathcal{P}_F}\right)$ .

Sachant que  $\left(\frac{-1}{q_E}\right)^{f(\frac{e}{2}+1)} = 1$  puisque  $q_E^f \equiv 1 \pmod{e}$  [14, Chap.5, § 4,

Cor. 1] alors  $\left(\frac{-1}{q_E}\right)^{(\frac{e}{2}+1)} \left(\frac{\pi}{\mathcal{P}_F}\right) = 1$  entraîne que  $\left(\frac{\omega\pi^{-1}}{\mathcal{P}_E}\right)^f = \left(\frac{\pi}{\mathcal{P}_F}\right)^f = 1$ ,

par suite

$$\left(\frac{u_\pi}{\mathcal{P}_E}\right) = \left(\frac{-1}{q_E}\right)^{(\frac{e}{2}+1)} \left(\frac{\pi}{\mathcal{P}_F}\right).$$

**Remarque 3.6** *Il est possible de donner une démonstration beaucoup plus directe du lemme précédent, sans utiliser la notion de signature de permutations, que nous proposons dans la suite.*

**Preuve** - La valuation  $\mathcal{P}_E$ -adique de l'idéal discriminant de l'extension est égale à  $e - 1$  puisque  $F/E$  est modérément ramifiée. Comme  $e$  est pair, on sait, d'après le lemme 3.4, qu'il existe une unité  $u_\pi$  de  $E$  telle que

$$\delta_{F/E} = \pi u_\pi \pmod{E^2}.$$

L'extension  $F/E$  étant totalement modérément ramifiée, il existe une uniformisante  $\pi'$  de  $E$  telle que  $F = E(\sqrt[e]{\pi'})$  [17, Chap. 3, Prop. 3.4.3]. L'entier  $e$  étant pair, on en déduit en particulier que  $\pi'$  est un carré dans  $F$ .

Le discriminant du polynôme  $X^e - \pi'$  étant

$$(-1)^{\frac{e(e-1)}{2}} e^e (-\pi')^{e-1} = (-1)^{(\frac{e}{2}+1)} e^e \pi'^{e-1},$$

On voit que

$$\delta_{F/E} = (-1)^{\left(\frac{e}{2}+1\right)} \pi' \pmod{E^2}.$$

Il en résulte que

$$\left(\frac{u_\pi}{\mathcal{P}_E}\right) = \left(\frac{\delta_{F/E}\pi^{-1}}{\mathcal{P}_E}\right) = \left(\frac{(-1)^{\left(\frac{e}{2}+1\right)}\pi'\pi^{-1}}{\mathcal{P}_E}\right) = \left(\frac{(-1)^{\left(\frac{e}{2}+1\right)}}{\mathcal{P}_E}\right) \left(\frac{\pi'\pi^{-1}}{\mathcal{P}_E}\right).$$

Comme  $F/E$  est totalement ramifiée, les deux extensions non ramifiées  $E(\sqrt{\pi'\pi^{-1}})/E$  et  $F(\sqrt{\pi'\pi^{-1}})/F$  sont de même degré et nous avons

$$\left(\frac{\pi'\pi^{-1}}{\mathcal{P}_E}\right) = \left(\frac{\pi'\pi^{-1}}{\mathcal{P}_F}\right).$$

Or  $\pi'$  est un carré dans  $F$ , donc

$$\left(\frac{\pi'\pi^{-1}}{\mathcal{P}_F}\right) = \left(\frac{\pi}{\mathcal{P}_F}\right).$$

D'où le lemme.

**Lemme 3.7** *On suppose que l'extension  $F/E$  est modérément ramifiée d'indice de ramification pair  $e$  et de degré résiduel  $f$ . Pour toute uniformisante  $\pi$  de  $E$ , il existe une unité  $u_\pi$  de  $E$  telle que :*

$$(i) \quad \delta_{F/E} = \pi^f u_\pi \pmod{E^2}$$

$$(ii) \quad \left(\frac{u_\pi}{\mathcal{P}_E}\right) = \left(\frac{-1}{q_E}\right)^{f\left(\frac{e}{2}+1\right)} \cdot \left(\frac{\pi}{\mathcal{P}_F}\right).$$

**Preuve** - Soit  $E'$  le corps d'inertie de l'extension  $F/E$ . Par la formule de transitivité des discriminants [12, Chap. 5, §1, Prop. 5.7 iii], nous avons :

$$\delta_{F/E} = \delta_{E'/E}^e N_{E'/E}(\delta_{F/E'}).$$

Donc modulo les carrés

$$\delta_{F/E} = N_{E'/E}(\delta_{F/E'}).$$

L'extension  $E'/E$  étant non-ramifiée,  $\pi$  reste une uniformisante de  $E'$ , donc d'après le lemme précédent, il existe une unité  $u'_\pi$  de  $E'$  telle que  $\delta_{F/E'} = \pi u'_\pi$  modulo  $E'^2$  et

$$\left(\frac{u'_\pi}{\mathcal{P}_{E'}}\right) = \left(\frac{-1^{(\frac{e}{2}+1)}}{q_{E'}}\right) \left(\frac{\pi}{\mathcal{P}_F}\right) = \left(\frac{-1}{q_E}\right)^{f(\frac{e}{2}+1)} \left(\frac{\pi}{\mathcal{P}_F}\right).$$

Par ailleurs,  $\left(\frac{u'_\pi}{\mathcal{P}_{E'}}\right) = \left(\frac{N_{E'/E}(u'_\pi)}{\mathcal{P}_E}\right)$  d'après la proposition 1.7. du chapitre I. Maintenant si on pose  $u_\pi = N_{E'/E}(u'_\pi)$ , on obtient à la fois les deux propriétés (i) et (ii) de l'énoncé.

**Lemme 3.8** *On suppose que l'indice de ramification  $e$  de  $F/E$  est impair. Soit  $f$  le degré résiduel de  $F/E$ . Si  $F/E$  n'est pas sauvagement ramifiée, alors*

$$\left(\frac{\delta_{F/E}}{\mathcal{P}_E}\right) = (-1)^{1+f} \left(\frac{q_E}{e}\right)^f.$$

**Preuve** - Voir le lemme 2.5 chapitre II.

Il nous reste plus qu'à démontrer le théorème 3.3. L'idéal  $\mathfrak{p}$  n'est pas sauvagement ramifié dans  $L$ , la valuation  $\mathfrak{p}$ -adique du discriminant  $\delta_{L/K}$  satisfait à la congruence :

$$v_{\mathfrak{p}}(\delta_{L/K}) = \sum_{i=1}^g (e_i - 1)f_i \pmod{2}.$$

$$v_{\mathfrak{p}}(\delta_{L/K}) = \sum_{2|e_i} f_i \pmod{2}$$

Donc si  $\sum_{2|e_i} f_i$  est impair, alors le symbole  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$  est nul tout comme l'est  $\epsilon_{L/K}(\mathfrak{p})$ .

Plaçons-nous désormais dans la situation où  $\sum_{2|e_i} f_i$  est pair. Pour tout  $i = 1, 2, \dots, g$  notons  $\delta_i = \delta_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}$ . Fixons nous une uniformisante  $\pi$  de  $K_{\mathfrak{p}}$ . Pour chaque  $i$  tel que  $e_i$  est pair, notons  $u_i$  l'unité  $u_{\pi}$  de  $K_{\mathfrak{p}}$  intervenant dans le lemme 3.7, Alors, modulo les carrés dans  $K_{\mathfrak{p}}$ , nous avons

$$\delta_{L/K} = \prod_{i=1}^g \delta_i = \prod_{2 \nmid e_i} \delta_i \prod_{2|e_i} \delta_i = \prod_{2 \nmid e_i} \delta_i \prod_{2|e_i} u_i$$

de sorte que :

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \prod_{2 \nmid e_i} (-1)^{1+f_i} \left(\frac{q}{e_i}\right)^{f_i} \prod_{2|e_i} \left(\frac{-1}{q}\right)^{f_i(\frac{e_i}{2}+1)} \prod_{2|e_i} \left(\frac{\pi}{\mathfrak{P}_i}\right)$$

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^F \left(\frac{q}{E}\right) (-1)^{\frac{q-1}{2} \sum_{2|e_i} f_i(\frac{e_i}{2}+1)} \epsilon_{L/K}(\mathfrak{p})$$

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^F \left(\frac{q}{E}\right) (-1)^{\frac{q-1}{2}G} \epsilon_{L/K}(\mathfrak{p}).$$

Le cas galoisien:

Supposons maintenant que l'extension  $L/K$  est galoisienne de groupe de Galois  $G$ . Soit, comme d'habitude;

$e :=$  l'indice de ramification de  $\mathfrak{p}$  dans  $L$

$f :=$  le degré résiduel de  $\mathfrak{p}$  dans  $L$

$g :=$  le nombre d'idéaux premiers de  $L$  au-dessus de  $\mathfrak{p}$ .

Alors pour chaque uniformisante  $\pi \in \mathfrak{p} - \mathfrak{p}^2$  de  $K$  en  $\mathfrak{p}$ , le symbole  $\rho := \left( \frac{\pi}{\mathfrak{P}} \right)$  est indépendant du choix de la place  $\mathfrak{P}$  au-dessus de  $\mathfrak{p}$  de sorte que  $\epsilon_{L/K}(\mathfrak{p})$  est une puissance  $g$ -ième.

**Corollaire 3.9** *Supposons que  $L$  est une extension galoisienne de  $K$ . Pour tout idéal premier  $\mathfrak{p}$  de  $K$  qui n'est pas sauvagement ramifié dans  $L$ , nous avons*

$$\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right) = \begin{cases} 0 & \text{si } 2|e \quad \text{et } 2 \nmid fg \\ \rho^g & \text{si } 2|e \quad \text{et } 2|fg \\ (-1)^g & \text{si } 2 \nmid e \quad \text{et } 2|fg \\ \left( \frac{q}{e} \right) & \text{si } 2 \nmid n \end{cases}$$

**Preuve** - Les deux premiers cas découlent immédiatement du théorème 3.3.

Lorsque  $e$  est impair, puisque  $L/K$  est une extension galoisienne, nous avons, toujours d'après le théorème 3.3,  $\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right) = (-1)^{fg+g} \left( \frac{q}{e} \right)^{fg}$  et donc

- si  $2|fg$ , alors  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^g$ ,
- si  $2 \nmid fg$ , alors  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \left(\frac{g}{e}\right)$ .

Comme conséquence immédiate du corollaire précédent on a la proposition suivante qui est à rapprocher au théorème de Pellet-Stickelberger-Voronoi.

**Proposition 3.10** *Soit  $K$  un corps de nombres,  $L$  une extension galoisienne de  $K$  et  $\mathfrak{p}$  un idéal premier de  $K$  qui n'est pas sauvagement ramifié dans  $L$ . Si  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) \neq 1$ , alors le nombre  $g$  d'idéaux premiers de  $L$  au-dessus de  $\mathfrak{p}$  est impair.*

**Preuve** - Le corollaire 3.10 est une conséquence immédiate du corollaire 3.9.

Il n'est pas difficile de voir que la réciproque de la proposition précédente est inexacte : en effet, il suffit de prendre  $K = \mathbf{Q}$ ,  $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$  et  $\mathfrak{p} = 3\mathbf{Z}$ . Alors  $\mathfrak{p} = \mathfrak{P}^2$  dans  $L$  et nous avons  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = 1$ .

**Proposition 3.11** *Soit  $L/K$  une extension galoisienne de corps de nombres. Soit  $\mathfrak{p}$  un idéal premier de  $K$  non au-dessus de 2 et  $\mathfrak{P}$  un idéal premier de  $L$  au-dessus de  $\mathfrak{p}$ . Supposons que le degré résiduel  $f$  de  $\mathfrak{p}$  dans  $L$  est pair. Soit  $\pi \in \mathfrak{p} - \mathfrak{p}^2$  une uniformisante de  $K$  en  $\mathfrak{p}$ . Alors  $\left(\frac{\pi}{\mathfrak{P}}\right) = 1$  si et seulement si le 2-groupe de Sylow du groupe de décomposition  $D_{\mathfrak{P}}(L/K)$  de  $\mathfrak{P}$  n'est pas cyclique.*

**Preuve** - Soient  $K_{\mathfrak{p}}$  et  $L_{\mathfrak{P}}$  les complétés de  $K$  et  $L$  en les places  $\mathfrak{p}$  et  $\mathfrak{P}$  respectivement. Notons  $E$  le sous-corps de  $L_{\mathfrak{P}}$  laissé fixe par le 2-groupe de Sylow de  $G(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \simeq D_{\mathfrak{P}}(L/K)$ . Comme  $f$  est supposé pair, l'extension quadratique non ramifiée  $M$  est contenue dans  $L_{\mathfrak{P}}$ . Puisque le degré  $[E : K_{\mathfrak{p}}]$  est impair, l'extension  $M(\sqrt{\pi})/E$  est galoisienne de groupe de Galois  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Ceci étant, si  $\left(\frac{\pi}{\mathfrak{P}}\right) = 1$ , alors  $M(\sqrt{\pi}) \subseteq L_{\mathfrak{P}}$  et le groupe de Galois  $G(L_{\mathfrak{P}}/E)$  se surjecte dans  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Il n'est donc pas cyclique.

Réciproquement, si le 2-groupe de Sylow  $G(L_{\mathfrak{P}}/E)$  n'est pas cyclique, alors il existe deux sous-groupes de  $G(L_{\mathfrak{P}}/E)$  d'indice 2 [6, Chap.12, §5, Th. 12.5.3], donc il existe deux extensions quadratiques de  $E$  contenues dans  $L_{\mathfrak{P}}$ . Comme  $E$  n'est pas une extension du corps des nombres 2-adiques  $Q_2$ , alors toutes les extensions quadratiques de  $E$  sont contenues dans  $L_{\mathfrak{P}}$ , en particulier  $E(\sqrt{\pi}) \subset L_{\mathfrak{P}}$ , autrement dit  $\left(\frac{\pi}{\mathfrak{P}}\right) = 1$ .

Remarquons que la parité du degré résiduel  $f$  n'est en fait utilisée que dans un sens de l'équivalence de la proposition. En effet, lorsque le 2-sous-groupe de Sylow du groupe de décomposition  $D_{\mathfrak{P}}(L/K)$  n'est pas cyclique alors, comme on vient de le voir au cours de la démonstration précédente,  $\left(\frac{\pi}{\mathfrak{P}}\right) = 1$  sans aucune hypothèse sur  $f$ .

**Remarque 3.12** *D'après le chapitre I, le symbole  $\epsilon$  peut-être interprété par l'application de réciprocité d'Artin de la manière suivante. Soit  $\pi \in \mathfrak{p}-\mathfrak{p}^2$  une*

uniformisante de  $K$  en  $\mathfrak{p}$ . Notons  $\mathfrak{a}$  l'idéal  $\prod_{2|e_i} \mathfrak{P}_i$  de  $L$ . Soit  $(\mathfrak{a}, L(\sqrt{\pi})/L)$  l'élément du groupe de Galois  $G(L(\sqrt{\pi})/L)$  défini par le symbole d'Artin. Lorsque  $\epsilon_{L/K}(\mathfrak{p})$  est non nul il est égal à 1 si et seulement si le symbole d'Artin  $(\mathfrak{a}, L(\sqrt{\pi})/L)$  est l'identité [13, Chap.IV, §8]. Nous utiliserons fréquemment cette caractérisation de  $\epsilon_{L/K}(\mathfrak{p})$ .

### Formule de transitivité pour $\epsilon$ :

À l'aide des propriétés fonctorielles du symbole d'Artin, nous pouvons établir une formule de transitivité pour  $\epsilon$  :

**Proposition 3.13** *Soit  $K \subseteq M \subseteq L$  une tour d'extensions de corps de nombres. Soit  $\mathfrak{p}$  un idéal premier de  $K$ . Supposons que  $\epsilon_{L/K}(\mathfrak{p})$ ,  $\epsilon_{M/K}(\mathfrak{p})$  ainsi que les  $\epsilon_{L/M}(\mathcal{P})$  pour  $\mathcal{P}|\mathfrak{p}$  sont non-nuls, alors nous avons*

$$\epsilon_{L/K}(\mathfrak{p}) = \epsilon_{M/K}(\mathfrak{p})^{[L:M]} \prod_{\substack{\mathcal{P}|\mathfrak{p} \\ 2 \nmid e(\mathcal{P}/\mathfrak{p})}} \epsilon_{L/M}(\mathcal{P}).$$

**Preuve** - Fixons provisoirement un idéal premier  $\mathcal{P}$  de  $M$  au-dessus de  $\mathfrak{p}$ .

Notons  $e = e(\mathcal{P}/\mathfrak{p})$  l'indice de ramification de  $\mathcal{P}$  dans l'extension  $M/K$ .

Choisissons une uniformisante  $\pi \in \mathfrak{p} - \mathfrak{p}^2$  du corps local  $K_{\mathfrak{p}}$ . Nous allons

évaluer le produit de symboles d'Artin :

$$\prod_{\substack{\mathfrak{P}|\mathfrak{p} \\ 2|e(\mathfrak{P}/\mathfrak{p})}} (\mathfrak{P}, L(\sqrt{\pi})/L)$$

suivant la parité de  $e$  :

Si  $e$  est pair, alors  $M(\sqrt{\pi})/M$  est non-ramifiée en  $\mathcal{P}$  et nous avons :

$$\begin{aligned} \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} (\mathfrak{P}, L(\sqrt{\pi})/L) &= \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} (\mathcal{P}^{f(\mathfrak{P}/\mathcal{P})}, M(\sqrt{\pi})/M) \\ &= (\mathcal{P}, M(\sqrt{\pi})/M)^{\sum_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} f(\mathfrak{P}/\mathcal{P})} \end{aligned}$$

Comme par hypothèse  $\epsilon_{L/M}(\mathcal{P})$  est non nul, la somme  $\sum_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} f(\mathfrak{P}/\mathcal{P})$  est paire de sorte que :

$$\prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} (\mathfrak{P}, L(\sqrt{\pi})/L) = 1.$$

Supposons maintenant que l'indice de ramification  $e$  est impair. Soit  $\omega \in \mathcal{P} - \mathcal{P}^2$  une uniformisante de  $M_{\mathcal{P}}$ . Il existe une unité  $u$  de  $M_{\mathcal{P}}$  telle que  $\pi = \omega^e u$ . Puisque  $\sum_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} f(\mathfrak{P}/\mathcal{P})$  est pair, nous voyons comme dans la démonstration de la proposition 3.1 du chapitre III que

$$\prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} \left( \frac{u}{\mathfrak{P}} \right) = 1$$

de sorte que

$$\prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} (\mathfrak{P}, L(\sqrt{\pi})/L) = \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} \left( \frac{\pi}{\mathfrak{P}} \right) = \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} \left( \frac{\omega}{\mathfrak{P}} \right) = \epsilon_{L/M}(\mathcal{P})$$

Ainsi lorsque  $\mathcal{P}$  parcourt les idéaux premiers de  $M$  au-dessus de  $\mathfrak{p}$ , on a

$$\prod_{\mathcal{P}|\mathfrak{p}} \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2|e(\mathfrak{P}/\mathcal{P})}} (\mathfrak{P}, L(\sqrt{\pi})/L) = \prod_{\substack{\mathcal{P}|\mathfrak{p} \\ 2|e(\mathcal{P}/\mathfrak{p})}} \epsilon_{L/M}(\mathcal{P}).$$

Pour obtenir la formule de la proposition, il nous faut également calculer le produit

$$\prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2 \nmid e(\mathfrak{P}/\mathcal{P})}} (\mathfrak{P}, L(\sqrt{\pi})/L).$$

pour chaque idéal  $\mathcal{P}$  de  $M$  tel que l'indice de ramification  $e = e(\mathcal{P}/\mathfrak{p})$  est pair. Comme précédemment, puisque  $M(\sqrt{\pi})/M$  est non-ramifiée en  $\mathcal{P}$ , nous avons

$$\begin{aligned} \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2 \nmid e(\mathfrak{P}/\mathcal{P})}} (\mathfrak{P}, L(\sqrt{\pi})/L) &= \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2 \nmid e(\mathfrak{P}/\mathcal{P})}} (\mathcal{P}^{f(\mathfrak{P}/\mathcal{P})}, M(\sqrt{\pi})/M) \\ &= (\mathcal{P}, M(\sqrt{\pi})/M)^{\sum_{\substack{\mathfrak{P}|\mathcal{P} \\ 2 \nmid e(\mathfrak{P}/\mathcal{P})}} f(\mathfrak{P}/\mathcal{P})} \\ &= (\mathcal{P}, M(\sqrt{\pi})/M)^{\sum_{\mathfrak{P}|\mathcal{P}} e(\mathfrak{P}/\mathcal{P})f(\mathfrak{P}/\mathcal{P})} \\ &= (\mathcal{P}, M(\sqrt{\pi})/M)^{[L:M]} \end{aligned}$$

et ensuite

$$\prod_{\substack{\mathcal{P}|\mathfrak{p} \\ 2 \nmid e(\mathcal{P}/\mathfrak{p})}} \prod_{\substack{\mathfrak{P}|\mathcal{P} \\ 2 \nmid e(\mathfrak{P}/\mathcal{P})}} (\mathfrak{P}, L(\sqrt{\pi})/L) = \epsilon_{M/K}(\mathfrak{p})^{[L:M]}.$$

La formule de la proposition se déduit alors sans difficulté des considérations précédentes.

**Remarque 3.14** *Notons que dans la même extension  $L/K$ , il est possible que  $\epsilon$  prenne les trois valeurs  $-1$ ,  $0$  et  $1$  en trois places ramifiées : Prenons, par exemple,  $K = \mathbf{Q}$  et soit  $L := \mathbf{Q}(\sqrt{210 + 21\sqrt{10}})$ . Alors  $L/\mathbf{Q}$  est une extension cyclique de degré 4 car*

$$210^2 - 10(21)^2 = 10(63)^2$$

[15, Théorème 1.2.1 du chapitre 1]. Dans  $L$ , à part 2, se ramifient uniquement les nombres premiers 3, 5 et 7. Plus précisément, le discriminant de  $L$

est donné par  $D = 2^{11} \cdot 3^2 \cdot 5^3 \cdot 7^2$ . Puisque 3 est décomposé dans  $\mathbf{Q}(\sqrt{10})$ , il se décompose dans  $L$  sous la forme :  $3 = \mathfrak{P}_1^2 \mathfrak{P}_2^2$ , donc d'après le corollaire 3.9 on a  $\epsilon_{L/\mathbf{Q}}(3) = 1$ . Vu la valuation 5-adique du discriminant, 5 se ramifie totalement dans  $L$  donc toujours d'après le corollaire 3.9 on a  $\epsilon_{L/\mathbf{Q}}(5) = 0$ . Quant au premier 7, puisqu'il est inerte dans  $\mathbf{Q}(\sqrt{10})$ , on a dans  $L$  :  $7 = \mathfrak{P}^2$ , donc  $\epsilon_{L/\mathbf{Q}}(7) = -1$  grâce au corollaire 3.9 et la proposition 3.11.

### Quelques exemples de calcul de $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$ :

Nous terminons ce chapitre avec deux familles d'exemples où  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$  se lit sur la décomposition de  $\mathfrak{p}$  en idéaux premiers de  $L$ . Rappelons qu'on est toujours dans le cas où la ramification est modérée.

1. Plaçons-nous dans la situation où il existe un corps intermédiaire  $M$  entre  $K$  et  $L$ , et où l'idéal premier  $\mathfrak{p}$  de  $K$  ne se décompose pas dans  $M$ . Notons  $\mathcal{P}$  l'idéal premier de  $M$  au-dessus de  $\mathfrak{p}$ , alors  $\mathfrak{p} = \mathcal{P}^{e(\mathcal{P}/\mathfrak{p})}$ . Supposons que l'indice de ramification  $e = e(\mathcal{P}/\mathfrak{p})$  est pair tandis que le degré résiduel  $f = f(\mathcal{P}/\mathfrak{p})$  est impair ; autrement dit  $\epsilon_{M/K}(\mathfrak{p}) = 0$ . Soient  $\mathfrak{P}_1, \dots, \mathfrak{P}_g$  les idéaux de  $L$  au-dessus de  $\mathfrak{p}$ ,  $f_1, \dots, f_g$  leurs degrés résiduels respectifs.

Si  $\sum_{i=1}^g f_i$  est impair, alors  $\epsilon_{L/K}(\mathfrak{p}) = \left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = 0$ .

Si au contraire  $\sum_{i=1}^g f_i$  est pair, alors  $\epsilon_{L/K}(\mathfrak{p}) = 1$  et  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^{\frac{g-1}{2}G}$  où  $G = \sum_{\substack{4|e_i \\ 2|f_i}} 1$ .

En effet, soit  $\pi \in \mathfrak{p} - \mathfrak{p}^2$  une uniformisante de  $K_{\mathfrak{p}}$ . Par le lemme d'Abhyankar [12, Chap.5, § 2, Cor. 4] l'extension  $M(\sqrt{\pi})/M$  est non ramifiée en  $\mathcal{P}$  de sorte que le symbole d'Artin  $(\mathcal{P}, M(\sqrt{\pi})/M)$  est bien défini. Comme  $f$  est supposé impair, nous avons aussi  $\sum_{i=1}^g f(\mathfrak{P}_i/\mathcal{P})$  est pair, d'où

$$(\mathcal{P}, M(\sqrt{\pi})/M)^{\sum_{i=1}^g f(\mathfrak{P}_i/\mathcal{P})} = Id.$$

On en déduit, par fonctorialité du symbole d'Artin, que la restriction à  $M(\sqrt{\pi})$  de  $\prod_{i=1}^g (\mathfrak{P}_i, L(\sqrt{\pi})/L)$  est l'identité :

$$\prod_{i=1}^g (\mathfrak{P}_i, L(\sqrt{\pi})/L) = Id.$$

Ce qui signifie bien que  $\epsilon_{L/K}(\mathfrak{p}) = 1$ . La formule  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^{\frac{g-1}{2}G}$  en est alors une conséquence immédiate.

2. Plaçons-nous dans la situation où il existe une extension cyclique  $M$  de  $K$  contenue dans  $L$ , et que l'idéal  $\mathfrak{p}$  de  $K$  ne se décompose pas dans  $M$ . Notons  $\mathcal{P}$  l'idéal premier de  $M$  au-dessus de  $\mathfrak{p}$ , alors  $\mathfrak{p} = \mathcal{P}^{e(\mathcal{P}/\mathfrak{p})}$ .

Supposons que l'indice de ramification  $e = e(\mathcal{P}/\mathfrak{p})$  et le degré résiduel  $f = f(\mathcal{P}/\mathfrak{p})$  sont pairs. Soient  $\mathfrak{P}_1, \dots, \mathfrak{P}_g$  les idéaux premiers de  $L$  au-dessus de  $\mathfrak{p}$  et  $f_1, \dots, f_g$  leurs degrés résiduels respectifs. Si maintenant

la somme des degrés résiduels  $\sum_{i=1}^g f(\mathfrak{P}_i/\mathcal{P})$  est impaire, alors

$$\epsilon_{L/K}(\mathfrak{p}) = \left( \frac{\delta_{L/K}}{\mathfrak{p}} \right) = -1.$$

En effet, soit  $\pi \in \mathfrak{p} - \mathfrak{p}^2$  une uniformisante de  $K_{\mathfrak{p}}$ .

D'après la proposition 3.11 du chapitre III, nous avons

$$\epsilon_{M/K}(\mathfrak{p}) = \left( \frac{\pi}{\mathcal{P}} \right) = -1;$$

autrement dit l'image de  $\mathcal{P}$  par le symbole d'Artin  $(\cdot, M(\sqrt{\pi})/M)$  n'est pas l'identité :

$$(\mathcal{P}, M(\sqrt{\pi})/M) \neq Id.$$

Comme  $\sum_{i=1}^g f(\mathfrak{P}_i/\mathcal{P})$  est impair, nous avons également

$$(\mathcal{P}, M(\sqrt{\pi})/M)^{\sum_{i=1}^g f(\mathfrak{P}_i/\mathcal{P})} \neq Id.$$

Toujours par la functorialité du symbole d'Artin, ceci entraîne

$$\text{Res}_{M(\sqrt{\pi})} \left( \prod_{i=1}^g \mathfrak{P}_i, L(\sqrt{\pi})/L \right) \neq Id.$$

D'où évidemment  $\left( \prod_{i=1}^g \mathfrak{P}_i, L(\sqrt{\pi})/L \right) \neq Id.$

Ce qui signifie bien que  $\epsilon_{L/K}(\mathfrak{p}) = -1$ , l'égalité  $\left( \frac{\delta_{L/K}}{\mathfrak{p}} \right) = -1$  est alors une conséquence immédiate.

## Chapitre IV

### Applications

On se propose de donner ici quelques applications directes des résultats des chapitres précédents.

**Résumé.** Nous commençons ce chapitre par une démonstration de la loi de réciprocité quadratique de Gauss comme conséquence directe du calcul de  $\epsilon_{L/Q}$  par deux méthodes différentes où  $L$  est le corps  $Q(\sqrt[4]{-p^2q}) = Q(\sqrt{p\sqrt{-q}})$  de degré 4. Ici  $p$  et  $q$  sont deux nombres premiers impairs distincts. Par ailleurs, lorsque  $L/K$  est une extension cyclique de degré une puissance de 2, on montre sous certaines conditions que  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$  ne peut pas prendre la valeur -1.

#### Loi de réciprocité quadratique:

Soient  $p$  et  $q$  deux nombres premiers impairs distincts. Soit  $L$  le corps de nombres suivant  $Q(\sqrt[4]{-p^2q}) = Q(\sqrt{p\sqrt{-q}})$ . Posons  $x = \sqrt{p\sqrt{-q}}$ . Alors  $q$  est totalement modérément ramifié dans  $L$ , car  $x$  est solution d'un polynôme d'Eisenstein en  $q$ . Soit  $A_L$  l'anneau des entiers de  $L$ ,  $\mathcal{P}$  un idéal premier de  $L$  au-dessus de  $p$ ,  $L_{\mathcal{P}} = Q_{\mathcal{P}}(\sqrt{p\sqrt{-q}})$  le complété de  $L$  en  $\mathcal{P}$ .  $L_{\mathcal{P}}$  est une extension quadratique ramifiée de  $Q_{\mathcal{P}}(\sqrt{-q})$  qui est une extension non

ramifiée de  $Q_p$ , ce qui veut dire que l'indice de ramification de  $\mathcal{P}$  dans  $L$  est 2, ainsi la décomposition de  $p$  dans  $L$  est  $pA_L = I^2$  où  $I$  est soit un idéal premier de  $L$  ou produit de deux idéaux premiers de  $L$ . Evaluons  $\epsilon_{L/Q}(p) = (I, L(\sqrt{p})/L)$  par deux méthodes différentes. Remarquons tout d'abord que d'après la proposition 3.1 du chapitre III, on a

$$\epsilon_{L/Q}(p) = (I, L(\sqrt{(-1)^{\frac{p-1}{2}}p})/L).$$

Notons  $\mathfrak{q}$  l'idéal premier de  $L$  au-dessus de  $q$ , on a  $qA_L = \mathfrak{q}^4$ , et donc

$$(xA_L)^4 = (pA_L)^2(qA_L) = (I\mathfrak{q})^4.$$

Puisque  $A_L$  est un anneau de Dedekind, cela entraîne que  $xA_L = I\mathfrak{q}$ .

Afin qu'on ait l'égalité

$$\epsilon_{L/Q}(p) = (\mathfrak{q}, L(\sqrt{(-1)^{\frac{p-1}{2}}p})/L),$$

il suffirait que  $xA_L$  soit dans le noyau de la représentation d'Artin suivante

$$\cdot \mapsto (\cdot, L(\sqrt{(-1)^{\frac{p-1}{2}}p})/L).$$

Or  $L(\sqrt{(-1)^{\frac{p-1}{2}}p})/L$  est une extension non ramifiée en toutes les places finies, en effet le discriminant de l'extension  $L(\sqrt{(-1)^{\frac{p-1}{2}}p})/L$  divise l'idéal  $4pA_L$ , donc les places finies de  $L$  susceptibles d'être ramifiées dans  $L(\sqrt{(-1)^{\frac{p-1}{2}}p})$  sont les places de  $L$  au-dessus de  $p$  et 2. Toute place de  $L$  au-dessus de  $p$  est non ramifiée dans  $L(\sqrt{(-1)^{\frac{p-1}{2}}p})$  d'après le lemme d'Abhyankar [12, Chap.5, § 2, Cor. 4], et toute place de  $L$  au-dessus de 2 est non ramifiée

dans  $L(\sqrt{(-1)^{\frac{p-1}{2}}p})$  [12, Cor. p. 222]. Par suite, puisqu'il n'y a pas de plongements réels de  $L$ , on a

$$(xA_L, L(\sqrt{(-1)^{\frac{p-1}{2}}p})/L) = 1$$

d'après la loi de réciprocité d'Artin.

On en conclut que

$$\epsilon_{L/Q}(p) = (\mathfrak{q}, L(\sqrt{(-1)^{\frac{p-1}{2}}p})/L) = (q, Q(\sqrt{(-1)^{\frac{p-1}{2}}p})/Q)$$

et donc

$$\epsilon_{L/Q}(p) = (q, Q(\sqrt{(-1)^{\frac{p-1}{2}}p})/Q) = \left( \frac{(-1)^{\frac{p-1}{2}}p}{q} \right).$$

Cela étant, d'après le théorème 3.3 du chapitre III, on a

$$\epsilon_{L/Q}(p) = \left( \frac{\delta_{L/Q}}{p} \right) = \left( \frac{q}{p} \right).$$

On en déduit aussitôt que :

$$\left( \frac{(-1)^{\frac{p-1}{2}}p}{q} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left( \frac{p}{q} \right) = \left( \frac{q}{p} \right).$$

### Application aux corps ayant un nombre de classes impair:

**Proposition 4.1** *Soit  $K$  un corps de nombres et  $h_K$  le nombre de classes d'idéaux de  $K$  qu'on suppose impair.  $L/K$  une extension cyclique de degré  $2^r$  où  $r \geq 2$ . On suppose que le nombre de classes d'idéaux  $h_L$  de  $L$  est impair.*

Soit  $\mathfrak{p}$  un idéal premier de  $K$  modérément ramifié dans  $L$ . Si  $\left(\frac{u}{\mathfrak{p}}\right) = 1$  pour toute unité  $u$  de  $K$ , alors

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = 0 \text{ ou } 1.$$

**Preuve** - Supposons par l'absurde que  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = -1$ , le nombre  $g$  d'idéaux de  $L$  au-dessus de  $\mathfrak{p}$  est donc impair d'après le corollaire 3.10 du chapitre III. Par suite il n'existe qu'une place  $\mathfrak{P}$  de  $L$  au-dessus de  $\mathfrak{p}$  car  $g$  divise  $2^r$ . De plus, d'après le corollaire 3.9 du chapitre III, l'indice de ramification  $e$  et le degré résiduel  $f$  de  $\mathfrak{P}$  sont pairs car  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \epsilon_{L/K}(\mathfrak{p})$  est non nul.

Soit  $\gamma \in L$  tel que  $\gamma A_L = \mathfrak{P}^{h_L}$  où  $A_L$  est l'anneau des entiers de  $L$ .

Posons  $M := L(\sqrt{\gamma})$ ,  $\mathfrak{P}$  est totalement ramifié dans  $M$  car la valuation  $\mathfrak{P}$ -adique de  $\gamma$  est  $h_L$  qui est impair. Soit  $\mathcal{L}$  l'unique place de  $M$  au-dessus de  $\mathfrak{P}$ , et  $\pi \in \mathfrak{p} - \mathfrak{p}^2$  une uniformisante de  $K$  en  $\mathfrak{p}$ .

$$\text{res}_{L(\sqrt{\pi})}(\mathcal{L}, M(\sqrt{\pi})/M) = (\mathfrak{P}, L(\sqrt{\pi})/L) = \left(\frac{\pi}{\mathfrak{P}}\right).$$

Or, puisque  $L/K$  est cyclique, d'après la Proposition 3.11 du chapitre III,  $(\mathfrak{P}, L(\sqrt{\pi})/L) \neq Id$ . On en conclut que

$$\epsilon_{M/K}(\mathfrak{p}) = \left(\frac{\pi}{\mathcal{L}}\right) = (\mathcal{L}, M(\sqrt{\pi})/M) = \left(\frac{\pi}{\mathfrak{P}}\right) = -1.$$

On sait que  $N_{L/K}(\gamma A_L) = N_{L/K}(\gamma) A_K$  où  $A_K$  est l'anneau des entiers de  $K$  [14, Chap.1, § 5, Prop.14].

Sachant que  $\gamma A_L = \mathfrak{P}^{h_L}$ , on a  $N_{L/K}(\gamma A_L) = \mathfrak{p}^{fh_L} = (\mathfrak{p}^{h_L})^f$ . En outre puisque  $h_K$  est impair,  $[L : K] = 2^r$ , alors  $h_K$  divise  $h_L$  [12, Chap. 4, §3, Cor. de Prop. 4.23], d'où  $\mathfrak{p}^{h_L}$  est principal engendré par  $\alpha \in A_K$ . On a donc :

$$\alpha^f A_K = N_{L/K}(\gamma) A_K.$$

C'est-à-dire que  $N_{L/K}(\gamma) = \alpha^f u$  où  $u$  est une unité de  $K$ .

Evaluons  $\left(\frac{u}{\mathfrak{p}}\right)$  : La transitivité du discriminant nous donne :

$$\delta_{M/K} = \delta_{L/K}^2 N_{L/K}(\delta_{M/L}) = N_{L/K}(\gamma) \pmod{K^2}.$$

Par suite,

$$\left(\frac{u}{\mathfrak{p}}\right) = \left(\frac{N_{L/K}(\gamma)}{\mathfrak{p}}\right) = \left(\frac{\delta_{M/K}}{\mathfrak{p}}\right).$$

Ceci étant, d'après le théorème 3.3 du chapitre III, on a

$$\left(\frac{\delta_{M/K}}{\mathfrak{p}}\right) = \epsilon_{M/K}(\mathfrak{p}).$$

Comme  $\epsilon_{M/K}(\mathfrak{p}) = -1$  d'après ce qui précède,  $\left(\frac{u}{\mathfrak{p}}\right) = -1$ , ce qui est contradictoire avec les hypothèses.

**Corollaire 4.2** *Soit  $K$  un corps de nombres n'admettant pas de plongements réels et de nombre de classes d'idéaux impair. Soit  $\mathfrak{p}$  un idéal premier de  $K$  principal engendré par  $x$  tel que  $x \equiv 1 \pmod{4A_K}$  où  $A_K$  est l'anneau des entiers de  $K$ . Soit  $L/K$  une extension cyclique de degré  $2^r$  où  $r \geq 2$ . On suppose que le nombre de classes d'idéaux de  $L$  est impair. Si  $\mathfrak{p}$  est modérément ramifié dans  $L$ , alors soit il est totalement ramifié dans  $L$  ou le nombre  $g$  d'idéaux de  $L$  au-dessus de  $\mathfrak{p}$  est pair.*

**Preuve** - Supposons que  $\mathfrak{p}$  n'est pas totalement ramifié dans  $L$ . Soit  $u$  une unité de  $K$ . Alors l'extension  $K(\sqrt{u})/K$  est non-ramifiée en les places non-dyadiques et il n'est pas difficile de voir que son conducteur  $\mathfrak{f}$  divise l'idéal principal  $4A_K$ . Par ailleurs, le corps  $K$  n'admet pas de plongement réel et de plus  $x$  étant congru à 1 modulo  $4A_K$ , donc congru à 1 modulo  $\mathfrak{f}$ , on a d'après la réciprocité d'Artin

$$(xA_K, K(\sqrt{u})/K) = Id$$

c'est-à-dire

$$\left(\frac{u}{\mathfrak{p}}\right) = \left(\frac{u}{xA_K}\right) = 1.$$

On peut alors affirmer que

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \left(\frac{\delta_{L/K}}{xA_K}\right) = 1$$

d'après la proposition précédente car  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) \neq 0$  puisque  $\mathfrak{p}$  n'est pas totalement ramifié dans  $L$  (Corollaire 3.9 du chapitre III). Comme  $L/K$  est cyclique, d'après le corollaire 3.9 et la proposition 3.11 du chapitre III,

$$\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^g.$$

On en déduit, puisque  $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = 1$ , que  $g$  est pair.

## Liste des symboles

$\mathfrak{p}$	un idéal premier de $K$
$\mathfrak{P}_i$	un idéal premier de $L$ au-dessus de $\mathfrak{p}$ .
$e_i$	indice de ramification de $\mathfrak{P}_i$ dans l'extension $L/K$ .
$f_i$	degré résiduel de $\mathfrak{P}_i$ dans l'extension $L/K$ .
$K_{\mathfrak{p}}$ ou $\hat{K}$	le complété de $K$ en $\mathfrak{p}$ .
$L_{\mathfrak{P}_i}$ ou $\hat{L}_i$	le complété de $L$ en $\mathfrak{P}_i$
$D_{\mathfrak{P}}(L/K)$	groupe de décomposition de $\mathfrak{P}$ dans $L/K$ .
$G(L_{\mathfrak{P}}/K_{\mathfrak{p}})$	groupe de Galois de l'extension de corps locaux $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ .
$\mathcal{P}_E$	idéal maximal du corps local $E$ .
$U_E$	groupe des unités d'un corps local $E$ .
$\left(\frac{a}{\mathcal{P}_E}\right)$	symbole des restes quadratiques local.
$\delta_{F/E}$	classe modulo les carrés du discriminant de l'extension $F/E$ .
$\delta_{L/K}$	classe modulo les carrés du discriminant d'une base de $L/K$ .
$\left(\frac{a}{\mathfrak{P}}\right)$	symbole des restes quadratiques.
$(\mathcal{P}, L/K)$	symbole d'Artin.
$(\mathbb{Z}/2^k\mathbb{Z})^*$	groupe des éléments inversibles de $\mathbb{Z}/2^k\mathbb{Z}$ .
$L \otimes_K \hat{K}$	produit tensoriel des $K$ -algèbres $L$ et $\hat{K}$ .
$\prod_{i=1}^g \hat{L}_i$	produit direct des $\hat{L}_i$ .
$N_{F/E}$	application norme de l'extension $F/E$ .
$\left(\frac{a, b}{\mathcal{P}_E}\right)$	symbole de Hilbert.
$Tr_{L/K}$	application trace de l'extension $L/K$ .

## References

- [1] **P. Barrucand et F. Laubie**, *Sur les symboles des restes quadratiques des discriminants*, Acta Arith., 48 (1987), p. 81-88.
- [2] **J.-P. B uhler**, *Icosahedral Galois Representation*, Lecture notes in math. 654, Springer Verlag, 1978.
- [3] **P. Cartier**, *Sur une g eneralisation des symboles de Legendre-Jacobi*, l'enseignement math ematique, IIe s erie, tome XVI, fasc. 1 (1970), p. 31-48.
- [4] **L.E. Dickson**, *History of the Theory of Numbers, volume I*, reprinted by Chelsea, 1952.
- [5] **D.M. Dribin**, *Permutation Groups*, Annals of Math., **38**(3) (1937), p. 739-749.
- [6] **Marshall Hall, Jr**, *The theory of groups*, 2nd ed. (English) New York, N.Y.: Chelsea Publishing Company. XIII.
- [7] **H. Hasse**, *Arithmetische Theorie der kubischen Zahlk orper auf klassenk orpertheoretischen Grundlage*, Math. Z., **31** (1930), p. 565-582.
- [8] **Iyanaga, S.**, *The theory of numbers*, North-Holland Mathematical Library. Vol. 8. Amsterdam - Oxford: North- Holland Publishing Company; New York: American Elsevier Publishing Company
- [9] **G. Kientega**, *Sur les corps alg ebriques du quatri eme degr e*, Th ese de troisi eme cycle, Publications de l'universit e de Paris VI(1980).

- [10] **S. Lang**, *Algebraic number theory*, 2nd ed. (English) Graduate Texts in Mathematics. 110. New York: Springer-Verlag. 1994
- [11] **A. Movahhedi et M. Zahidi**, *Symboles des restes quadratiques des discriminants dans les extensions modérément ramifiées*, Acta Arithmetica, à paraître.
- [12] **W. Narkiewicz**, *Elementary and Analytic Theory of Algebraic Numbers*, Second edition. Springer-Verlag, Berlin ; PWN-Polish Scientific Publishers, Warsaw, 1990.
- [13] **Jürgen Neukirch**, *Class Field Theory*, Springer-Verlag **280**, 1986.
- [14] **J-P. Serre**, *Corps locaux*, troisième édition, Hermann, Paris 1968.
- [15] **J-P. Serre**, *Topics in Galois theory*, Notes written by Henri Darmon. Research Notes in Mathematics. 1. Boston, MA etc. Jones and Bartlett Publishers, 1992.
- [16] **G.E. Wahlin**, *The factorisation of the rational primes in a cubic domain*, Amer. J. Math. **44** (1922), p. 191-203.
- [17] **E. Weiss**, *Algebraic Number Theory*, reprinted by Chelsea, 1963.