ACTA ARITHMETICA
XCII.3 (2000)

Symboles des restes quadratiques des discriminants dans les extensions modérément ramifiées

par

A. Movahhedi et M. Zahidi (Limoges)

1. Introduction. Soit L un corps de nombres de degré n sur le corps $\mathbb{Q}$ des nombres rationnels de discriminant $D = D_{L/\mathbb{Q}}$. Si l'entier D n'est pas un carré, on note d le discriminant du corps quadratique $\mathbb{Q}(\sqrt{D})$, 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 ([3, page 245]), L. Stickelberger et G. Voronoï 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 $(p) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ 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 $L/\mathbb{Q}$, alors la valuation p-adique du discriminant D est donnée par $v_p(D) = \sum_{i=1}^{g}(e_i - 1)f_i$ [9, 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 [10], Hasse [5], Buhler [2], Dribin [4], Kientega [6], ...), P. Barrucand et F. Laubie ont établi la formule suivante (également valable dans le cas relatif) [1] :

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

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

2. Énoncés des résultats. 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

2000 *Mathematics Subject Classification*: 11A15, 11R29, 11S15.

vectoriel L. Le discriminant $D = D_{L/K} = \det(\mathrm{Tr}_{L/K}(b_i\, b_j))$ est un élément non-nul de K : $D \in K^{\cdot}$. La classe $\delta = \delta_{L/K}$ de D modulo les carrés $K^{\cdot 2}$ 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. Notons $K_{\mathfrak{p}}$ le complété de K en la place $\mathfrak{p}$. On va s'intéresser au symbole des restes quadratique $\left(\frac{\delta}{\mathfrak{p}}\right)$: étant donné $a \in K_{\mathfrak{p}}^{\cdot}$, le symbole des restes quadratiques $\left(\frac{a}{\mathfrak{p}}\right)$ est défini par

$$\left(\frac{a}{\mathfrak{p}}\right) = \begin{cases} 1 & \text{si } K_{\mathfrak{p}}(\sqrt{a}) = K_{\mathfrak{p}}, \\ -1 & \text{si } K_{\mathfrak{p}}(\sqrt{a})/K_{\mathfrak{p}} \text{ est une extension quadratique non-ramifiée}, \\ 0 & \text{si } K_{\mathfrak{p}}(\sqrt{a})/K_{\mathfrak{p}} \text{ est une extension quadratique ramifiée}. \end{cases}$$

En particulier $\left(\frac{a}{\mathfrak{p}}\right)$ ne dépend que de la classe de a modulo les carrés. Soit $\mathfrak{p} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ 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 $n = e_1 f_1 + \ldots + e_g f_g$. On désigne par $\pi \in \mathfrak{p}$ une uniformisante du corps local $K_{\mathfrak{p}}$.

Proposition 2.1. *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 π.*

Cette proposition suggère

Définition 2.2. Pour tout idéal premier non 2-adique $\mathfrak{p}$ du corps de nombres K, on pose

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

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

Remarque 2.3. Le symbole ε 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 $\varepsilon_{L/K}(\mathfrak{p})$ 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 [8, Chap. IV, §8]. Nous utiliserons fréquemment cette caractérisation de $\varepsilon_{L/K}(\mathfrak{p})$.

A l'aide des propriétés fonctorielles du symbole d'Artin, nous pouvons établir une formule de transitivité pour ε :

PROPOSITION 2.4. *Soit $K \subset M \subset L$ une tour d'extensions de corps de nombres. Soit $\mathfrak{p}$ un idéal premier de K. Supposons que $\varepsilon_{L/K}(\mathfrak{p})$, $\varepsilon_{M/K}(\mathfrak{p})$ ainsi que les $\varepsilon_{L/M}(\mathcal{P})$ pour $\mathcal{P} \mid \mathfrak{p}$ sont non-nuls. Alors nous avons*

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

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

THÉORÈME 2.5. *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 $\varepsilon_{L/K}(\mathfrak{p})$ sont reliés par la formule*

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

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

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

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

REMARQUE 2.6. (i) Lorsque tous les indices de ramification e_i sont impairs, alors $G = 0$, $\varepsilon_{L/K}(\mathfrak{p}) = 1$ 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 exclu de l'énoncé du théorème précédent car pour ces idéaux ε 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 $\varrho := \left(\frac{\pi}{\mathfrak{P}}\right)$ est indépendant du choix de la place $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ de sorte que $\varepsilon_{L/K}(\mathfrak{p}) = \varrho^g$ est une puissance g-ième.

Avec les notations ci-dessus, le théorème 2.5 montre facilement que la valeur du symbole $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right)$ est donnée par

Corollaire 2.7. *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*

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

Dans la situation de ce dernier corollaire, le cas où $2 \mid e$, $2 \mid f$ 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 $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = \varepsilon_{L/K}(\mathfrak{p}) = \left(\frac{\pi}{\mathfrak{P}}\right) \neq 0$. La valeur de $\varrho = \left(\frac{\pi}{\mathfrak{P}}\right)$ 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 2.8. *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 π 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.*

Notons que dans la même extension L/K, il est possible que ε prenne les trois valeurs -1, 0 et 1 en trois places ramifiées : Prenons, par exemple, $K = \mathbb{Q}$ et soit $L := \mathbb{Q}(\sqrt{210 + 21\sqrt{10}})$. Alors $L/\mathbb{Q}$ est une extension cyclique de degré 4 où 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 $\mathbb{Q}(\sqrt{10})$, il se décompose dans L sous la forme $3 = \mathfrak{p}_1^2\mathfrak{p}_2^2$, donc d'après le corollaire 2.7 on a $\varepsilon_{L/\mathbb{Q}}(3) = 1$. Vu la valuation 5-adique du discriminant, 5 se ramifie totalement dans L, donc toujours d'après le corollaire 2.7 on a $\varepsilon_{L/\mathbb{Q}}(5) = 0$. Quant au premier 7, puisqu'il est inerte dans $\mathbb{Q}(\sqrt{10})$, on a dans L : $7 = \mathfrak{p}^2$, donc $\varepsilon_{L/\mathbb{Q}}(7) = -1$ grâce au corollaire 2.7 et la proposition 2.8.

Comme conséquence immédiate du corollaire 2.7, citons la proposition suivante qui est à rapprocher au théorème de Pellet–Stickelberger–Voronoï.

Proposition 2.9. *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 $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ et $\mathfrak{p} = 3\mathbb{Z}$. Alors $\mathfrak{p} = \mathfrak{P}^2$ dans L et nous avons $\left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = 1$.

3. Étude locale. Dans cette section, nous ne considérons que des corps locaux, c'est-à-dire complets pour une valuation discrète et ayant un corps résiduel fini. Étant donné un corps local E, nous notons

$\pi_E = \pi =$ une uniformisante de E;
$A_E =$ l'anneau de valuation de E;
$\mathfrak{p}_E = \pi A_E$ l'idéal de valuation de E;
$q = q_E =$ le cardinal du corps résiduel $A_E/\mathfrak{p}_E$.

Lorsque F est une extension finie séparable du corps local E, on désignera comme dans le cas global $\delta_{F/E}$ la classe modulo les carrés du discriminant d'une E-base de F.

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 3.1. *On suppose que l'extension locale F/E est totalement et modérément ramifiée de degré pair e. Alors pour toute uniformisante π de E, il existe une unité u_π de E telle que*

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

(ii) $\left(\dfrac{u_\pi}{\mathfrak{p}_E}\right) = \left(\dfrac{-1}{q_E}\right)^{e/2+1} \left(\dfrac{\pi}{\mathfrak{p}_F}\right)$.

Démonstration. La valuation $\mathfrak{p}_E$-adique de l'idéal discriminant de l'extension F/E est égale à $(e-1)$. Comme e est supposé pair, on en déduit qu'il existe une unité u_π de E telle que $\delta_{F/E} = u_\pi \pi \bmod E^{\cdot 2}$.

L'extension F/E étant modérée, il existe une uniformisante π' de E telle que $F = E(\sqrt[e]{\pi'})$ [11, Chap. 3, Prop. 3.4.3]. En particulier π' est un carré dans F.

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

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

on voit que $\delta_{F/E} = (-1)^{e/2+1}\pi' \bmod E^{\cdot 2}$. Il en résulte que

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

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

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

Or π' est un carré de F, donc

$$\left(\frac{\pi'\pi^{-1}}{\mathfrak{p}_E}\right) = \left(\frac{\pi^{-1}}{\mathfrak{p}_F}\right) = \left(\frac{\pi}{\mathfrak{p}_F}\right)$$

d'où le lemme. ∎

Lorsque l'extension locale F/E n'est pas totalement ramifiée, par un dévissage on peut généraliser le lemme précédent de la façon suivante :

LEMME 3.2. *On suppose que l'extension locale F/E est modérément ramifiée d'indice de ramification pair e et de degré résiduel f. Pour toute uniformisante π de E, il existe une unité u_π de E telle que*

(i) $\delta_{F/E} = \pi^f u_\pi \bmod E^{\cdot 2}$;

(ii) $\left(\dfrac{u_\pi}{\mathfrak{p}_E}\right) = \left(\dfrac{-1}{q_E}\right)^{f(e/2+1)} \left(\dfrac{\pi}{\mathfrak{p}_F}\right)$.

Démonstration. La démonstration imite celle du lemme 4 de [1]. Soit E' le corps d'inertie de l'extension F/E. Par la formule de transitivité des discriminants [9, Chap. 3, Prop. 8], nous avons

$$\delta_{F/E} = \delta_{E'/E}^e N_{E'/E}(\delta_{F/E'}) \bmod E^{\cdot 2} = N_{E'/E}(\delta_{F/E'}) \bmod E^{\cdot 2}.$$

L'extension E'/E étant non-ramifiée, π reste une uniformisante de E', donc d'après le lemme précédent il existe une unité u'_π de E' telle que

$$\delta_{F/E'} = \pi u'_\pi \bmod E'^{\cdot 2}$$

et

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

Par ailleurs, $\left(\frac{u'_\pi}{\mathfrak{p}_{E'}}\right)$ peut être vu comme le symbole de Hilbert $\left(\frac{\pi, u'_\pi}{\mathfrak{p}_{E'}}\right)$ [8, Chap. III, §5], d'où

$$\begin{aligned}\left(\frac{u'_\pi}{\mathfrak{p}_{E'}}\right) &= (u'_\pi, E'(\sqrt{\pi})/E')(\sqrt{\pi})/\sqrt{\pi} \\ &= (N_{E'/E}(u'_\pi), E(\sqrt{\pi})/E)(\sqrt{\pi})/\sqrt{\pi} \\ &\qquad\qquad \text{(fonctorialité du symbole d'Artin)} \\ &= \left(\frac{\pi, N_{E'/E}(u'_\pi)}{\mathfrak{p}_E}\right) = \left(\frac{N_{E'/E}(u'_\pi)}{\mathfrak{p}_E}\right).\end{aligned}$$

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. ∎

Le cas où l'indice de ramification e de l'extension locale F/E est impair a été traité dans [1] :

LEMME 3.3. *On suppose que l'indice de ramification e de F/E est impair. Soit f le degré résiduel de F/E. Alors nous avons*

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

Démonstration. C'est le lemme 4 de [1]. ∎

4. Globalisation

Démonstration de la proposition 2.1. Soient π et π' deux uniformisantes de $K_\mathfrak{p}$. Posons $u = \pi/\pi'$.

Soit $\mathfrak{P}_i$ 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 premier $\mathfrak{p}$ étant supposé non 2-adique, l'extension $K_\mathfrak{p}(\sqrt{u})/K_\mathfrak{p}$ est non-ramifiée. On en déduit aussitôt que si le degré résiduel correspondant 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 ne s'intéresse dans cette proposition qu'aux idéaux premiers $\mathfrak{P}_i$ avec e_i pair. Pour un tel idéal premier $\mathfrak{P}_i$, le lemme d'Abhyankar [7, Chap. 5, §2, Cor. 4 au Th. 5.11] garantit la non-nullité de $\left(\frac{\pi}{\mathfrak{P}_i}\right)$ puisqu'il affirme que l'extension $K_{\mathfrak{P}_i}(\sqrt{\pi})/K_{\mathfrak{P}_i}$ 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

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

de sorte que

$$\prod_{2|e_i}\left(\frac{\pi}{\mathfrak{P}_i}\right) = \prod_{2|e_i}\left(\frac{\pi'}{\mathfrak{P}_i}\right).$$

La proposition est donc démontrée. ∎

Démonstration de la proposition 2.4. Fixons-nous 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 π du

corps local $K_{\mathfrak{p}}$ appartenant à K. Nous allons évaluer le produit de symboles d'Artin

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

suivant la parité de e.

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

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

Comme par hypothèse $\varepsilon_{L/M}(\mathcal{P})$ est non-nul, la somme en exposant est paire de sorte que

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

Supposons maintenant que l'indice de ramification e est impair. Soit w une uniformisante de $M_{\mathcal{P}}$. Il existe une unité de $M_{\mathcal{P}}$ telle que $\pi = w^e u$. Puisque $\sum_{\mathfrak{P}|\mathcal{P},\, 2|e(\mathfrak{P}/\mathcal{P})} f(\mathfrak{P}/\mathcal{P})$ est pair, nous voyons, comme dans la démonstration de la proposition précédente (prop. 2.1), que

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

de sorte que

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

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

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

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 premier $\mathcal{P}$ 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-ramifié en $\mathcal{P}$, nous avons

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

et ensuite

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

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

Tous les ingrédients sont maintenant réunis pour obtenir le théorème principal. Nous utiliserons les résultats locaux établis dans la section précédente, en remplaçant E et F par les corps locaux $K_{\mathfrak{p}}$ et $L_{\mathfrak{P}_i}$ respectivement.

Démonstration du théorème 2.5. L'idéal premier $\mathfrak{p}$ étant modérément ramifié dans L, la valuation $\mathfrak{p}$-adique du discriminant $\delta_{L/K}$ satisfait à la congruence

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

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

Plaçons-nous désormais dans la situation où $\sum_{2|e_i} f_i$ est pair : Pour tout $i = 1, \ldots, g$, notons $\delta_i = \delta_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}$. Fixons-nous une uniformisante π de $K_{\mathfrak{p}}$. Pour chaque i tel que e_i est pair, notons u_i l'unité u_π de $K_{\mathfrak{p}}$ intervenant dans le lemme 3.2. Alors, modulo les carrés de $K_{\mathfrak{p}}^{\cdot}$, 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

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

Démonstration de la proposition 2.8. 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-sous-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 de E est contenue dans $L_\mathfrak{P}$. Puisque $[E : K_\mathfrak{p}]$ est un entier impair, l'extension $E(\sqrt{\pi})/E$ est non-triviale et ramifiée de sorte que 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 $M(\sqrt{\pi}) \subset L_\mathfrak{P}$ 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 $G(L_\mathfrak{P}/E)$ n'est pas cyclique, alors il existe un corps F entre E et $L_\mathfrak{P}$ qui possède deux extensions quadratiques distinctes contenues dans $L_\mathfrak{P}$. Comme le corps local F n'est pas 2-adique, cela entraîne que toutes les extensions quadratiques de F sont contenues dans $L_\mathfrak{P}$. En particulier, l'uniformisante $\pi \in K_\mathfrak{p} \subseteq F$ est un carré dans $L_\mathfrak{P}$, autrement dit $\left(\frac{\pi}{\mathfrak{P}}\right) = 1$. ∎

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

5. Exemples. Nous terminons avec deux familles d'exemples. 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 $\varepsilon_{M/K}(\mathfrak{p}) = 0$. Soient $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ les idéaux premiers de L au-dessus de $\mathfrak{p}$ et $f_1, \ldots, f_g$ leurs degrés résiduels respectifs.

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

$$\varepsilon_{L/K}(\mathfrak{p}) = 1 \quad \text{et} \quad \left(\frac{\delta_{L/K}}{\mathfrak{p}}\right) = (-1)^{(q-1)G/2} \quad \text{où } G = \sum_{\substack{4 \mid e_i \\ 2 \nmid f_i}} 1.$$

En effet, soit $\pi \in \mathfrak{p}$ une uniformisante de $K_\mathfrak{p}$. Par le lemme d'Abhyankar, 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 également $\sum_{i=1}^g f(\mathfrak{P}_i/\mathcal{P})$ est pair. D'où

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

On en déduit, par la 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. Donc

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

ce qui signifie bien que $\varepsilon_{L/K}(\mathfrak{p}) = 1$. La formule $\big(\frac{\delta_{L/K}}{\mathfrak{p}}\big) = (-1)^{(q-1)G/2}$ 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 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 $e = e(\mathcal{P}/\mathfrak{p})$ et le degré résiduel $f = f(\mathcal{P}/\mathfrak{p})$ sont pairs. Soient $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ les idéaux premiers de L au-dessus de $\mathfrak{p}$ et $f_1, \ldots, f_g$ leurs degrés résiduels respectifs. Si maintenant la somme des degrés résiduels $\sum_{i=1}^{g} f(\mathfrak{P}_i/\mathcal{P})$ est impaire, alors

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

En effet, soit $\pi \in \mathfrak{p}$ une uniformisante de $K_{\mathfrak{p}}$. D'après la proposition 2.8, nous avons $\varepsilon_{M/K}(\mathfrak{p}) = \big(\frac{\pi}{\mathcal{P}}\big) = -1$; autrement dit l'image de $\mathcal{P}$ par le symbole d'Artin $(\quad, M(\sqrt{\pi})/M)$ n'est pas l'identité : $(\mathcal{P}, M(\sqrt{\pi})/M) \neq \mathrm{Id}$. Comme $\sum_{i=1}^{g} f(\mathfrak{P}_i/\mathcal{P})$ est impair, nous avons également

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

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

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

D'où évidemment $(\prod_{i=1}^{g}\mathfrak{P}_i, L(\sqrt{\pi})/L) \neq \mathrm{Id}$, ce qui signifie bien que $\varepsilon_{L/K}(\mathfrak{p}) = -1$. L'égalité $\big(\frac{\delta_{L/K}}{\mathfrak{p}}\big) = -1$ en est alors une conséquence immédiate.

Remerciement. Les auteurs tiennent à remercier le professeur Francisco Diaz y Diaz qui leur a fourni des exemples de calcul de $\varepsilon_{L/K}(\mathfrak{p})$.

Bibliographie

[1] P. Barrucand et F. Laubie, *Sur les symboles des restes quadratiques des discriminants*, Acta Arith. 48 (1987), 81–88.

[2] J. P. Buhler, *Icosahedral Galois Representations*, Lecture Notes in Math. 654, Springer, 1978.

[3] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, reprinted by Chelsea, 1952.

[4] D. M. Dribin, *Permutation groups*, Ann. of Math. 38 (1937), 739–749.

[5] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischen Grundlage*, Math. Z. 31 (1930), 565–582.
[6] G. Kientega, *Sur les corps algébriques du quatrième degré*, thèse de troisième cycle, Publ. Univ. Paris VI, 1980.
[7] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd ed., Springer, Berlin; PWN–Polish Sci. Publ., Warszawa, 1990.
[8] J. Neukirch, *Class Field Theory*, Grundlehren Math. Wiss. 280, Springer, 1986.
[9] J.-P. Serre, *Corps locaux*, troisième édition, Hermann, Paris, 1968.
[10] G. E. Wahlin, *The factorisation of the rational primes in a cubic domain*, Amer. J. Math. 44 (1922), 191–203.
[11] E. Weiss, *Algebraic Number Theory*, reprinted by Chelsea, 1963.

LACO (UPRESA 6090 CNRS)
Département de mathématiques
Université de Limoges
123 Avenue Albert Thomas
87060 Limoges Cedex, France
E-mail: mova@unilim.fr
zahidi@unilim.fr

Reçu le 26.2.1999
et révisé le 6.9.1999 (3562)