Math. Nachr. **188** (1997), 109 – 140

Interprétation et Calcul du Groupe de Défaut d'un Principe de Hasse

By GEORGES GRAS and ANNE CORTELLA of Besançon

(Received April 26, 1995)

Abstract. Nous reprenons, dans le cadre de la théorie normique explicite du corps de classes, l'étude du groupe de défaut du principe de Hasse pour les similitudes de formes bilinéaires, effectuée par ANNE CORTELLA dans sa thèse ; nous en donnons une interprétation galoisienne concrète puis nous obtenons de nouveaux cas de validité de ce principe ainsi qu'une famille infinie de contre-exemples pour la structure $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

0. Introduction

0.1. Position du problème

Soit k un corps de nombres et soit V un k-espace vectoriel de dimension finie. Si l'on considère une forme k-bilinéaire b sur V, le principe de Hasse pour b est le fait que toute forme k-bilinéaire b' sur V, similaire à b sur tous les complétés k_v de k, est similaire à b sur k. Dans le cas où la k-algèbre à involution R associée à b (au sens d'E. BAYER [B]) est un corps de nombres L, le principe de Hasse pour b est équivalent à la propriété suivante, pour l'extension quadratique L/K (où K est le corps fixe de l'involution):

"L'ensemble $\mathcal{L}$ des $x \in K^\times$ tels que, pour toute place v de k il existe $a_v \in k_v^\times$ tel que xa_v^{-1} soit norme locale dans L/K, en toute place w de K au-dessus de v, est égal à $\mathcal{G} = k^\times N_{L/K} L^\times$."

Dans sa thèse (cf. [C2]), A. CORTELLA a étudié ce problème, lorsque L/k est galoisienne, au moyen de la cohomologie des tores; elle a montré l'exactitude de ce principe de Hasse dans de nombreux cas et trouvé, avec $k = \mathbb{Q}$ et $\mathrm{Gal}(L/\mathbb{Q}) \simeq H_8$, le premier contre-exemple (cf. [C1]).

1991 *Mathematics Subject Classification.* Primary.

Keywords and phrases. Formes bilinéaires, principe de Hasse, similitudes, corps de classes, cohomologie de tores.

Son étude montre que le groupe de défaut $\mathcal{L}/\mathcal{G}$ de ce principe de Hasse dépend d'abord, de façon essentielle, de la nature de $\mathrm{Gal}(L/k)$, et, lorsque l'obstruction galoisienne subsiste, d'un invariant arithmétique associé à la ramification dans L/k.

On se propose ici d'étudier le groupe de défaut $\mathcal{L}/\mathcal{G}$ pour $k = \mathbb{Q}$, pour $L/\mathbb{Q}$ non nécessairement galoisienne, et dans le cadre des voies explicites du corps de classes (caractérisées, comme l'on sait, par l'usage du symbole de restes normiques); par rapport au travail d'A. CORTELLA, le résultat essentiel de cet article est l'interprétation suivante du groupe $\mathcal{L}/\mathcal{G}$ (cf. §4, §5, §6):

Posons $L = K(\sqrt{\delta})$, $E = \mathbb{Q}(\sqrt{d})$, où $d = N_{K/\mathbb{Q}}(\delta)$, et soit $\widehat{L}$ la clôture galoisienne de $L/\mathbb{Q}$; alors il existe une 2-extension abélienne élémentaire explicite F de $\mathbb{Q}$, contenant E, pour laquelle on a $\mathcal{L}/\mathcal{G} \simeq \mathrm{Gal}(E'/E)$, $\mathrm{Gal}(F/E')$ étant de la forme $I''\langle\psi(R')\rangle$, où le groupe I'' est un invariant galoisien, se lisant sur le schéma $\widehat{L}/\widehat{L}\cap F/\mathbb{Q}$, et où $\langle\psi(R')\rangle$ dépend simplement de symboles de Hilbert explicites liés à l'ensemble R des places de $\mathbb{Q}$ ramifiées dans $\widehat{L}/\mathbb{Q}$. L'existence de l'invariant I'' fait que l'on peut avoir $\mathcal{L}/\mathcal{G} = 1$ universellement pour certains groupes $\mathrm{Gal}(\widehat{L}/\mathbb{Q})$, comme cela a été obtenu dans [C2, III 6] par la considération du groupe $Ш_c(k,T)$ qui contient le groupe $\mathcal{L}/\mathcal{G}$ vu comme groupe de Schafarevich-Tate, $Ш(k,T)$, associé à un tore algébrique convenable.

On donne alors un certain nombre de résultats généraux (par exemple (34)) et on obtient une famille infinie de contre-exemples avec $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (cf. (32)).

Enfin, en complément (cf. §8, §9), A. CORTELLA calcule le groupe $Ш_c(k,T)$ pour $\mathrm{Gal}(L/k) = D_8$ et H_{16}, confirme, via les techniques cohomologiques évoquées, le résultat (32), et obtient numériquement une paire de formes bilinéaires illustrant ces contre-exemples.

0.2. Notations générales

D'une manière générale, pour un corps de nombres K, on désigne par $P\ell_K$ l'ensemble des places de K, réunion de $P\ell_K^0$ (l'ensemble des places finies) et de $P\ell_K^\infty$ (celui des places archimédiennes); on confond place et valuation sous-jacente, selon les définitions suivantes:

(i) si $w \in P\ell_K^0$, $w : K^\times \twoheadrightarrow \mathbb{Z}$ est la valuation normalisée usuelle ;

(ii) si $w \in P\ell_K^\infty$ est réelle, $w : K^\times \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ est définie par $(-1)^{w(x)} = \mathrm{signe}(\sigma_w(x))$ pour le plongement réel σ_w associé;

(iii) si w est complexe, la valuation associée est nulle.

Pour toute place $w \in P\ell_K$, on désigne par K_w le complété de K en w.

On désigne ensuite par v les éléments de $P\ell_{\mathbb{Q}}$, par p_v la caractéristique résiduelle correspondante pour $v \in P\ell_{\mathbb{Q}}^0$, et on pose $p_v = -1$ si $v = \infty$ (l'unique place archimédienne de $\mathbb{Q}$). On pose

$$P = \{p_v, v \in P\ell_{\mathbb{Q}}\},$$

de sorte que $\mathbb{Q}^\times = \langle P\rangle$.

On désigne enfin par U_v le groupe des unités de $\mathbb{Q}_v$ (on a $U_v = \mathbb{Z}_{p_v}^*$ si $v \in P\ell_{\mathbb{Q}}^0$, $U_v = \mathbb{R}^{\times+}$ si $v = \infty$).

Soit donc K un corps de nombres, et soit L une extension quadratique de K.

On utilisera les algèbres étales suivantes, pour $v \in P\ell_{\mathbb{Q}}$:

$$K_v = \bigoplus_{\substack{w \in P\ell_K \\ w|v}} K_w,$$

$$L_v = \bigoplus_{\substack{w \in P\ell_K \\ w|v}} L_w, \quad \text{où} \quad L_w = \bigoplus_{\substack{w' \in P\ell_L \\ w'|w}} L_{w'},$$

pour lesquelles la norme

$$N_v : L_v \longrightarrow K_v$$

est définie comme le produit des normes locales correspondantes (ou, ce qui revient au même, comme le prolongement par continuité de la norme usuelle $N_{L/K} : L^\times \to K^\times$).

L'invariant étudié (cf. [C2, II.3]) est alors $\mathcal{L}_{L/K}/\mathcal{G}_{L/K}$, où:

$$\begin{aligned} \mathcal{L}_{L/K} &= \mathcal{L} \\ &= \left\{x \in K^\times,\ x = a_v N_v \alpha_v,\ a_v \in \mathbb{Q}_v^\times,\ \alpha_v \in L_v^\times,\ \text{pour tout } v \in P\ell_{\mathbb{Q}}\right\}, \\ \mathcal{G}_{L/K} &= \mathcal{G} = \mathbb{Q}^\times N_{L/K} L^\times. \end{aligned} \tag{0.1}$$

1. Première réduction pour le calcul de $\mathcal{L}/\mathcal{G}$

On pose

$$\Sigma = \left\{v \in P\ell_{\mathbb{Q}}^0, v \text{ est ramifiée dans } L/K\right\}. \tag{1.1}$$

Remark 1.1. Pour les places à l'infini on ne parle pas de ramification mais d'inertie (degré résiduel égal à 2); ceci revient à se placer dans le cadre "divisoriel" du corps de classes (cf. [J], Chap. III, p. 168). Dans ce cadre, si $w \in P\ell_K^\infty$, le frobenius $\left(\frac{L/K}{w}\right)$ est la conjugaison complexe dans $L_{w'}/K_w = L_{w'}/\mathbb{R}$, $w'|w$.

Lemma 1.2. *Tout élément de $\mathcal{L}/\mathcal{G}$ est représenté par un $y \in K^\times$ tel que $y = u_v N_v \beta_v$, $u_v \in U_v$, $\beta_v \in L_v^\times$, pour tout $v \in P\ell_{\mathbb{Q}}$.*

Proof. Tout élément de $K^\times$ étant norme locale en v, dans L/K, pour presque toute place $v \in P\ell_{\mathbb{Q}}$, on peut supposer que, pour $x \in \mathcal{L}$, la famille $(a_v)_v$ est un idèle de $\mathbb{Q}$ (cf. (0.1)); comme le groupe des classes au sens restreint de $\mathbb{Q}$ est trivial, ceci est équivalent à l'isomorphisme

$$J_{\mathbb{Q}}/\mathbb{Q}^\times \simeq U_{\mathbb{Q}} = \prod_{v \in P\ell_{\mathbb{Q}}} U_v,$$

le groupe des idèles unités de $\mathbb{Q}$. Il existe donc $c \in \mathbb{Q}^\times$ tel que $a_v = c u_v$, $u_v \in U_v$, pour tout $v \in P\ell_{\mathbb{Q}}$; alors $y = c^{-1}x$ convient. □

Ceci amène à définir les groupes $\mathcal{L}'$ et $\mathbb{Q}'$ suivants:

Definition 1.3. On pose successivement

$$\mathcal{L}' = \{x \in K^\times,\ x = u_v N_v \alpha_v,\ \alpha_v \in L_v^\times,\ u_v \in U_v,\ \text{pour tout } v \in P\ell_{\mathbb{Q}}\},$$
$$\mathbb{Q}' = \mathcal{L}'_\cap \mathbb{Q}^\times.$$

Comme $\mathcal{L}'/\mathcal{L}'_\cap \mathcal{G} = \mathcal{L}'/\mathcal{L}'_\cap(\mathbb{Q}^\times N_{L/K} L^\times) = \mathcal{L}'/(\mathcal{L}'_\cap \mathbb{Q}^\times) N_{L/K} L^\times$, on obtient le fait suivant, point de départ de l'étude normique des paragraphes suivants:

Corollary 1.4. *Le groupe de défaut $\mathcal{L}/\mathcal{G}$ est canoniquement isomorphe à $\mathcal{L}'/\mathbb{Q}' N_{L/K} L^\times$.*

2. Symboles de restes normiques

La seconde étape consiste à interpréter $\mathcal{L}'/\mathbb{Q}' N_{L/K} L^\times$ à l'aide de la théorie normique du corps de classes.

Soit $v \in P\ell_{\mathbb{Q}}$, et pour tout $w \in P\ell_K$, $w|v$, soit

$$\left(\frac{,L/K}{w}\right) : K_w^\times \longrightarrow \mathrm{Gal}(L_{w'}/K_w) \hookrightarrow \mathrm{Gal}(L/K), \quad w'|w,$$

le symbole de restes normiques attaché à w, où la flèche de gauche est l'isomorphisme de réciprocité du corps de classes local, et celle de droite résultant de l'isomorphisme canonique du groupe de Galois local avec le groupe de décomposition de w dans L/K; soit alors

$$J_w = \left\{\left(\frac{u_v, L/K}{w}\right),\ u_v \in U_v\right\} \subseteq \mathrm{Gal}(L/K)$$

l'image de U_v par le symbole $\left(\frac{,L/K}{w}\right)$; elle est contenue dans le groupe d'inertie de w dans L/K, et on a donc $J_w = 1$ pour toute place w de K non ramifiée dans L/K.

Definition 2.1. (i) Pour tout $v \in P\ell_{\mathbb{Q}}$, on désigne par

$$J_v = \left\{\left(\left(\frac{u_v, L/K}{w}\right)\right)_{w|v},\ u_v \in U_v\right\} \subseteq \bigoplus_{w|v} J_w$$

l'image diagonale de U_v par le symbole $\bigoplus_{w|v}\left(\frac{,L/K}{w}\right)$.

(ii) On pose

$$J = \bigoplus_{v \in P\ell_{\mathbb{Q}}} J_v \subseteq \bigoplus_{w \in P\ell_K} J_w,$$

puis on désigne par

$$I = \widetilde{\bigoplus_{v \in P\ell_{\mathbb{Q}}}} J_v$$

le sous-groupe de J formé des éléments satisfaisant à la formule du produit dans $\bigoplus_{w\in P\ell_K} J_w$. D'après la remarque précédente, le support $S = \{v \in P\ell_{\mathbb{Q}},\ J_v \neq (1)\}$ est contenu dans Σ, et on a donc $J = \bigoplus_{v\in S} J_v$.

(iii) Pour tout $x \in \mathcal{L}'$ (cf. Déf. (1.3)), on pose

$$\psi(x) = \bigoplus_{v\in P\ell_{\mathbb{Q}}} \left(\left(\frac{x, L/K}{w}\right)\right)_{w|v}.$$

(iv) Enfin on pose (cf. Déf. (1.3))

$$I' = \psi(\mathbb{Q}').$$

Remark 2.2. Par définition de $\mathcal{L}'$, on a, pour tout $x \in \mathcal{L}'$ et tout $v \in P\ell_{\mathbb{Q}}$,

$$\left(\left(\frac{x, L/K}{w}\right)\right)_{w|v} = \left(\left(\frac{u_v, L/K}{w}\right)\right)_{w|v}, \quad u_v \in U_v;$$

donc $\left(\left(\frac{x,L/K}{w}\right)\right)_{w|v} \in J_v$ pour tout $v \in P\ell_{\mathbb{Q}}$, et, comme x est "global", on a

$$\prod_{w\in P\ell_K} \left(\frac{x, L/K}{w}\right) = 1,$$

d'où $\psi(x) \in I$.

On peut alors énoncer:

Lemma 2.3. *L'application ψ induit un isomorphisme canonique de $\mathcal{L}'/\mathbb{Q}'\, N_{L/K} L^\times$ sur I/I'.*

Proof. Soit $(\sigma_w)_w \in I$ vu dans $\bigoplus^{\sim}_{w\in P\ell_K} J_w$; la réciproque de la formule du produit donne l'existence de $x \in K^\times$ tel que

$$\left(\frac{x, L/K}{w}\right) = \sigma_w, \quad \text{pour tout} \quad w \in P\ell_K.$$

Par définition, $x \in \mathcal{L}'$, ce qui prouve la surjectivité de ψ.

Si pour $x \in \mathcal{L}'$, $\left(\left(\frac{x,L/K}{w}\right)\right)_w \in I'$, il existe $c \in \mathbb{Q}'$ tel que

$$\left(\frac{x, L/K}{w}\right) = \left(\frac{c, L/K}{w}\right), \quad \text{pour tout} \quad w \in P\ell_K,$$

ce qui équivaut à $xc^{-1} \in N_{L/K}L^\times$, puisque le principe de Hasse usuel vaut dans l'extension cyclique L/K; d'où $x \in \mathbb{Q}' N_{L/K} L^\times$. □

Remark 2.4. L'isomorphisme canonique $\mathcal{L}/\mathcal{G} \simeq I/I'$ nous ramène à calculer, d'une part, les images diagonales par $\bigoplus_{w|v}\left(\frac{\cdot, L/K}{w}\right)$ des groupes $U_v, v \in S$ (pour la détermination de J puis I), et, d'autre part, l'image par ψ de $\mathbb{Q}'$. Ceci suppose d'établir des

formules explicites pour les symboles de restes normiques dans L/K (ce sera l'objet du §3).

En ce qui concerne $\mathbb{Q}'$, il est en partie élucidé par les propriétés suivantes (Prop. (2.5) et (2.6)):

Proposition 2.5. *Soit*

$$P' = \left\{ p_v \in P, \left(\left(\frac{p_v, L/K}{w} \right) \right)_{w|v} \in J_v \right\};$$

alors on a $\mathbb{Q}' = \langle P' \rangle \mathbb{Q}^{\times 2}$.

Proof. Soit $c \in \mathbb{Q}'$; on a donc $\left(\left(\frac{c, L/K}{w} \right) \right)_{w|v} \in J_v$ pour toute place $v \in P\ell_{\mathbb{Q}}$. Fixons $v \in P\ell_{\mathbb{Q}}$ telle que $v(c) \equiv 1 \bmod 2$, et posons $c = c_v c'_v$, $c_v = p_v^{v(c)}$, $c'_v \in U_v$ (si $v = \infty$, on rappelle que l'on a $p_v = -1$, $c'_v \in \mathbb{R}^{\times +}$) ; on a donc:

$$\left(\left(\frac{c, L/K}{w} \right) \right)_{w|v} = \left(\left(\frac{c_v, L/K}{w} \right) \right)_{w|v} \cdot \left(\left(\frac{c'_v, L/K}{w} \right) \right)_{w|v},$$

mais par hypothèse $c'_v \in U_v$, d'où $\left(\left(\frac{c'_v, L/K}{w} \right) \right)_{w|v} \in J_v$, et finalement

$$\left(\left(\frac{c_v, L/K}{w} \right) \right)_{w|v} = \left(\left(\frac{p_v, L/K}{w} \right) \right)_{w|v} \in J_v ;$$

d'où $p_v \in P'$ et $c \in \langle P' \rangle \mathbb{Q}^{\times 2}$.

L'autre inclusion résulte du fait que pour $v' \neq v$, on a $\left(\left(\frac{p_v, L/K}{w'} \right) \right)_{w'|v'} \in J_{v'}$ car $p_v \in U_{v'}$ dans ce cas. □

Proposition 2.6. *Soit* $v \in P\ell_{\mathbb{Q}} - \Sigma$; *alors les conditions suivantes sont équivalentes:*

(i) $p_v \in P'$;

(ii) *pour tout* $w|v$ *la condition suivante est vérifiée:* w *est décomposée dans* L/K *ou l'indice de ramification* e_w *de* w *dans* $K/\mathbb{Q}$ *est pair.*

Proof. Comme $J_v = 1$ pour $v \notin \Sigma$, on a, d'après la Prop. (2.5), $p_v \in P'$ si et seulement si $\left(\left(\frac{p_v, L/K}{w} \right) \right)_{w|v} = (1)$. Soit π_w une uniformisante de K_w (on rappelle que $\pi_w = -1$, si $w \in P\ell_K^{\infty}$, et qu'alors $e_w = 1$); on a donc

$$\left(\frac{p_v, L/K}{w} \right) = \left(\frac{\pi_w, L/K}{w} \right)^{e_w},$$

car toute unité de K_w est norme dans l'extension non ramifiée L_w/K_w; d'où la proposition puisque $\left(\frac{\pi_w, L/K}{w} \right)$ est le frobenius qui engendre le groupe de décomposition de

w dans L/K. □

Ce second résultat permet de lire facilement la condition $p_v \in P'$, pour $v \notin \Sigma$; le cas général résultera des calculs explicites que nous allons effectuer au §3.

3. Calculs explicites des symboles de restes normiques

Posons

$$L = K(\sqrt{\delta}), \quad \delta \in K^\times, \quad \delta \text{ défini modulo } K^{\times 2}.$$

Soit $c \in \mathbb{Q}_v^\times$ et soit $w \in P\ell_K$, $w|v$; on a donc, en termes de symboles de Hilbert sur K:

$$\left(\frac{c, L/K}{w}\right)\sqrt{\delta} = (c,\delta)_w\sqrt{\delta},$$

et de même, en posant $M = K(\sqrt{c})$, on a aussi

$$\left(\frac{\delta, M/K}{w}\right)\sqrt{c} = (\delta, c)_w\sqrt{c} = (c,\delta)_w\sqrt{c}.$$

Ce second symbole de restes normiques peut se voir dans $\mathrm{Gal}(M_{w'}/K_w)$, où $w'|w$ dans M/K. Soit alors $M_{w'}^{ab}$ l'extension abélienne maximale de $\mathbb{Q}_v$ dans $M_{w'}$; si $\sqrt{c} \notin K_w$, $M_{w'}$ est le composé direct, sur $\mathbb{Q}_v$, de K_w et de l'extension quadratique $\mathbb{Q}_v(\sqrt{c})$, et on a les inclusions

$$\mathbb{Q}_v(\sqrt{c}) \subseteq M_{w'}^{ab} \subseteq M_{w'}.$$

Les propriétés fonctionnelles du symbole de restes normiques (cf. [S, XIII, 4]) montrent que dans l'application canonique (ici injective)

$$\mathrm{Gal}(M_{w'}/K_w) \hookrightarrow \mathrm{Gal}(M_{w'}^{ab}/\mathbb{Q}_v),$$

le symbole $\left(\frac{\delta, M_{w'}/K_w}{w}\right)$ a pour image le symbole $\left(\frac{N_{K_w/\mathbb{Q}_v}\delta, M_{w'}^{ab}/\mathbb{Q}_v}{v}\right)$ qui appartient à $\mathrm{Gal}(M_{w'}^{ab}/M_{w'}^{ab} \cap K_w)$, et que la restriction

$$\mathrm{Gal}(M_{w'}^{ab}/\mathbb{Q}_v) \longrightarrow \mathrm{Gal}(\mathbb{Q}_v(\sqrt{c})/\mathbb{Q}_v)$$

induit l'isomorphisme $\mathrm{Gal}(M_{w'}^{ab}/M_{w'}^{ab} \cap K_w) \simeq \mathrm{Gal}(\mathbb{Q}_v(\sqrt{c})/\mathbb{Q}_v)$ dans lequel le symbole précédent a pour image le symbole $\left(N_{K_w/\mathbb{Q}_v}\delta, \mathbb{Q}_v(\sqrt{c})/\mathbb{Q}_v v\right)$; on vérifie que cette expression vaut également lorsque $\sqrt{c} \in K_w$, ce qui conduit à la relation suivante, pour toute place $v \in P\ell_{\mathbb{Q}}$ et tout $c \in \mathbb{Q}_v^\times$:

$$(3.1) \qquad (c,\delta)_w = (c,\delta_w)_v, \quad \text{avec} \quad \delta_w = N_{K_w/\mathbb{Q}_v}\delta.$$

Ainsi, connaissant les normes locales δ_w, on se ramène à des calculs de symboles de restes quadratiques sur $\mathbb{Q}$ selon le processus suivant:

Definition 3.1. (i) On considère la décomposition usuelle de $\mathbb{Q}_v^\times$ modulo $\mathbb{Q}_v^{\times 2}$:

a) Si $v \in P\ell_{\mathbb{Q}}^0$ est impaire: $\mathbb{Q}_v^\times = p_v^{\mathbb{Z}/2\mathbb{Z}} \times \zeta_v^{\mathbb{Z}/2\mathbb{Z}} \times \mathbb{Q}_v^{\times 2}$, où ζ_v est une racine de l'unité d'ordre $p_v - 1$;

b) si $v \in P\ell_{\mathbb{Q}}^0$ est paire: $\mathbb{Q}_v^\times = 2^{\mathbb{Z}/2\mathbb{Z}} \times (-1)^{\mathbb{Z}/2\mathbb{Z}} \times 5^{\mathbb{Z}/2\mathbb{Z}} \times \mathbb{Q}_v^{\times 2}$;

c) si $v = \infty$: $\mathbb{Q}_v^\times = (-1)^{\mathbb{Z}/2\mathbb{Z}} \times \mathbb{Q}_v^{\times 2}$.

(ii) Pour toute place w de K, soit f_w le degré résiduel de w dans $K/\mathbb{Q}$; comme $N_{K_w/\mathbb{Q}_v}(K_w^\times) \subseteq p_v^{f_w\mathbb{Z}} U_v$, on peut poser:

a) Si $v \in P\ell_{\mathbb{Q}}^0$ est impaire: $\delta_w \equiv p_v^{d_w f_w} \zeta_v^{d'_w} \bmod \mathbb{Q}_v^{\times 2}$, $d_w, d'_w \in \mathbb{Z}/2\mathbb{Z}$;

b) si $v \in P\ell_{\mathbb{Q}}^0$ est paire: $\delta_w \equiv 2^{d_w f_w}(-1)^{d'_w} 5^{d''_w} \bmod \mathbb{Q}_v^{\times 2}$, $d_w, d'_w, d''_w \in \mathbb{Z}/2\mathbb{Z}$;

c) si $v = \infty$: $\delta_w \equiv (-1)^{d_w f_w} \bmod \mathbb{Q}_v^{\times 2}$, $d_w \in \mathbb{Z}/2\mathbb{Z}$.

On notera que l'on a dans tous les cas $d_w \equiv w(\delta) \bmod 2$.

(iii) Pour tout $p = p_v \in P$, on définit le symbole de restes quadratiques généralisé

$$\left(\frac{-}{p}\right) : \mathbb{Q}_v^\times \longrightarrow \{\pm 1\},$$

par $\left(\frac{a}{p}\right) = 1$ si et seulement si $a \in \mathbb{Q}_v^{\times 2}$ (en particulier, $\left(\frac{a}{-1}\right)$ est le signe de a et $\left(\frac{a}{2}\right) = 1$ si et seulement si $a \in 4^{\mathbb{Z}}(1 + 8\mathbb{Z}_2)$).

Lemma 3.2. *Soit $v \in P\ell_{\mathbb{Q}}$ et soit $w \in P\ell_K$, $w|v$; alors on a les formules suivantes:*

(i) *v finie impaire:*

$$(\ell, \delta_w)_v = \left(\frac{(-1)^{\frac{p_v-1}{2}} p_v}{\ell}\right)^{d_w f_w}, \quad \textit{pour tout} \quad \ell \in P, \quad \ell \neq p_v,$$

$$(p_v, \delta_w)_v = (-1)^{\frac{p_v-1}{2} d_w f_w + d'_w};$$

(ii) *v paire:*

$$(\ell, \delta_w)_v = \left(\frac{2}{\ell}\right)^{d_w f_w} \left(\frac{-1}{\ell}\right)^{d'_w}, \quad \textit{pour tout} \quad \ell \in P, \ \ell \neq 2,$$

$$(2, \delta_w)_v = (-1)^{d''_w}$$

(iii) $v = \infty$:

$$(\ell, \delta_w)_v = 1, \quad \textit{pour tout} \quad \ell \in P, \ \ell \neq -1,$$

$$(-1, \delta_w)_v = (-1)^{d_w f_w}.$$

Proof. Compte tenu de la forme de δ_w, il suffit de donner la liste des symboles de base, à savoir:

(α) v finie impaire, $\ell \in P$, $\ell \neq p_v$ (resp. $\ell = p_v$) :

$$(\ell, p_v)_v = \left(\frac{\ell}{p_v}\right), \qquad (\ell, \zeta_v)_v = 1,$$

$$(p_v, p_v)_v = (-1)^{\frac{p_v-1}{2}}, \quad (p_v, \zeta_v)_v = -1;$$

(β) v paire, $\ell \in P$, $\ell \neq 2$ (resp. $\ell = 2$) :

$$(\ell, 2)_v = \left(\frac{2}{\ell}\right), \quad (\ell, -1)_v = \left(\frac{-1}{\ell}\right), \quad (\ell, 5)_v = 1,$$

$$(2,2)_v = 1, \quad (2,-1)_v = 1, \quad (2,5)_v = -1;$$

(γ) $v = \infty$, $\ell \in P$, $\ell \neq -1$ (resp. $\ell = -1$) :

$$(\ell, -1)_v = 1,$$
$$(-1,-1)_v = -1;$$

pour cela on a utilisé les formules explicites classiques suivantes, pour $a, b \in \mathbb{Q}_v^\times$, où $a' = ap_v^{-v(a)}$, $b' = bp_v^{-v(b)}$:

$$(a,b)_v = \left(\frac{(-1)^{v(a)v(b)} a'^{v(b)} b'^{-v(a)}}{p_v}\right), \quad \text{pour } v \text{ impaire}$$

(au sens de la Déf. (3.1), iii);

$$(a,b)_v = (-1)^{\frac{a'-1}{2}\cdot\frac{b'-1}{2}} \left(\frac{2}{a'^{v(b)} b'^{-v(a)}}\right), \quad \text{pour } v \text{ paire},$$

où l'on a posé $\left(\frac{2}{x}\right) = (-1)^{\frac{x^2-1}{8}}$, pour $x \equiv 1 \bmod 2\mathbb{Z}_2$.

(i) Pour v finie impaire, $\ell \in P$, $\ell \neq p_v$, on a donc (cf. Déf. (3.1), (ii), a):

$$\begin{aligned}(\ell, \delta_w)_v &= \left(\ell, p_v^{d_w f_w} \zeta_v^{d'_w}\right)_v \\ &= (\ell, p_v)_v^{d_w f_w} \\ &= \left(\frac{\ell}{p_v}\right)^{d_w f_w};\end{aligned}$$

or la loi de réciprocité quadratique donne, pour $\ell \neq p_v$, et en posant $\varepsilon_v = (-1)^{\frac{p_v-1}{2}}$:

$$\left(\frac{\varepsilon_v p_v}{\ell}\right)\left(\frac{\ell}{p_v}\right) = \left(\frac{\varepsilon_v}{\ell}\right)\left(\frac{p_v}{\ell}\right)\left(\frac{\ell}{p_v}\right) = \left((-1)^{\frac{\ell-1}{2}}\right)^{\frac{p_v-1}{2}} (-1)^{\frac{\ell-1}{2}\cdot\frac{p_v-1}{2}} = 1$$

(on vérifie séparément les cas $\ell \neq -1$ et $\ell = -1$) ; d'où $(\ell, \delta_w)_v = \left(\frac{\varepsilon_v p_v}{\ell}\right)^{d_w f_w}$ dans ce cas.

On a ensuite, pour $\ell = p_v$:

$$\begin{aligned}(p_v, \delta_w)_v &= (p_v, p_v)_v^{d_w f_w} (p_v, \zeta_v)_v^{d'_w} \\ &= (-1)^{\frac{p_v-1}{2} d_w f_w} (-1)^{d'_w} \\ &= (-1)^{\frac{p_v-1}{2} d_w f_w + d'_w},\end{aligned}$$

ce qui établit le point (i) du lemme.

(ii) Pour v paire, $\ell \in P$, $\ell \neq 2$, il vient (cf. Déf. (3.1), (ii), b):

$$\begin{aligned}(\ell, \delta_w)_v &= \left(\ell, 2^{d_w f_w}(-1)^{d'_w} 5^{d''_w}\right)_v \\ &= (\ell, 2)_v^{d_w f_w} (\ell, -1)_v^{d'_w} (\ell, 5)_v^{d''_w} \\ &= \left(\frac{2}{\ell}\right)^{d_w f_w} \left(\frac{-1}{\ell}\right)^{d'_w};\end{aligned}$$

on a, pour $\ell = 2$:

$$(2, \delta_w)_v = (2, 2)_v^{d_w f_w} (2, -1)_v^{d'_w} (2, 5)_v^{d''_w} = (-1)^{d''_w},$$

ce qui établit le second point.

(iii) Enfin pour $v = \infty$, $\ell \in P$, $\ell \neq -1$, on obtient

$$(\ell, \delta_w)_v = 1$$

puis, pour $\ell = -1$

$$(-1, \delta_w)_v = (-1)^{d_w f_w},$$

ce qui achève la preuve du lemme. □

Puisque les symboles de Hilbert et ceux de restes quadratiques, à valeurs dans $\{\pm 1\}$, caractérisent les symboles de restes normiques, à valeurs dans $\mathrm{Gal}(L/K)$, il est commode de considérer l'application (cf. Déf. (2.1))

$$\psi : \mathbb{Q}' \longrightarrow I'$$

qui à c associe $\bigoplus_{v \in P\ell_{\mathbb{Q}}} \left(\left(\frac{c, L/K}{w}\right)\right)_{w|v}$, comme étant à valeurs dans $\bigoplus_{v \in P\ell_{\mathbb{Q}}} \{\pm 1\}$ et donnée par:

$$\psi(c) = \bigoplus_{v \in P\ell_{\mathbb{Q}}} \left((c, \delta_w)_v\right)_{w|v}, \quad \text{pour tout} \quad c \in \mathbb{Q}'.$$

Les formules du Lemme (3.2) permettent donc d'expliciter le groupe $J = \bigoplus_{v \in P\ell_{\mathbb{Q}}} J_v$ (vu désormais comme sous-groupe de $\bigoplus_{v \in P\ell_{\mathbb{Q}}} \{\pm 1\}$) :

Proposition 3.3. *Dans l'identification précédente, on a:*

(i) *si $v \in P\ell_{\mathbb{Q}}^0$ est impaire*

$$J_v = \langle \eta_v \rangle, \quad \text{où} \quad \eta_v = \left((-1)^{d_w f_w}\right)_{w|v};$$

(ii) *si $v \in P\ell_{\mathbb{Q}}^0$ est paire*

$$J_v = \langle \eta_{v,2}, \eta_{v,-1} \rangle, \quad \text{où} \quad \eta_{v,2} = \left((-1)^{d_w f_w}\right)_{w|v}, \quad \eta_{v,-1} = \left((-1)^{d'_w}\right)_{w|v};$$

(iii) *si $v = \infty$, on a $J_v = \{(1)\}$.*

Proof. Par définition, on a

$$J_v \;=\; \langle((u_v,\delta_w)_v)_{w|v},\ u_v\in U_v\rangle\,.$$

Dans le premier cas, J_v est engendré par l'image de ζ_v, soit

$$((\zeta_v,\delta_w)_v)_{w|v} \;=\; \left(\left(\frac{\zeta_v}{p_v}\right)^{d_w f_w}\right)_{w|v} \;=\; \left((-1)^{d_w f_w}\right)_{w|v}.$$

Dans le second cas, J_v est engendré par les images de -1 et 5, soit $((-1,\delta_w)_v)_{w|v} = \left((-1)^{d'_w}\right)_{w|v}$ et $((5,\delta_w)_v)_{w|v} = \left((-1)^{d_w f_w}\right)_{w|v}$. Le dernier cas résulte du fait que $U_v = \mathbb{R}^{\times +} = \mathbb{Q}_v^{\times 2}$. □

Corollary 3.4. *Le sous-ensemble $S = \{v\in P\ell_{\mathbb{Q}}, J_v\neq(1)\}$ est formé des $v\in\Sigma$ pour lesquelles il existe $w|v$ telle que $d_w f_w\neq 0$ (resp. $d_w f_w\neq 0$ ou $d'_w\neq 0$) si v est impaire (resp. paire).*

En revenant à la définition (cf. Prop. (2.5)), on en déduit une caractérisation explicite de P', qui complète le résultat de la Prop. (2.6):

Proposition 3.5. *Soit $v\in P\ell_{\mathbb{Q}}$; on a $p_v\in P'$ si et seulement si la condition suivante est réalisée:*

(i) *Si v est impaire: il existe $\lambda_v\in\mathbb{Z}/2\,\mathbb{Z}$ tel que*

$$d'_w \;=\; \lambda_v\, d_w f_w,\quad \textit{pour tout}\quad w|v\,;$$

(ii) *si v est paire: il existe $\lambda_v,\mu_v\in\mathbb{Z}/2\,\mathbb{Z}$ tels que*

$$d''_w \;=\; \lambda_v\, d_w f_w \,+\, \mu_v\, d'_w,\quad \textit{pour tout}\quad w|v\,;$$

(iii) *si $v=\infty$:*

$$d_w f_w \;=\; 0,\quad \textit{pour tout}\quad w|v\,.$$

Proof. Ceci résulte de la Proposition (3.3) précédente et des formules du Lemme (3.2) donnant $(p_v,\delta_w)_v$, $w|v$. On notera que pour $v\notin S$, ces conditions sont équivalentes à
$\delta_w\in\mathbb{Q}_v^{\times 2}$, pour tout $w|v$. □

4. Interprétation de J comme groupe de Galois

Cette étape va consister à définir une extension $F/\mathbb{Q}$, dépendant simplement de S, dont le groupe de Galois est un 2-groupe abélien élémentaire canoniquement isomorphe à J, et qui permettra l'interprétation galoisienne de $\mathcal{L}/\mathcal{G}$ que nous avons en vue.

Definition 4.1. (i) Soit R l'ensemble des nombres premiers dont l'indice de ramification dans la clôture galoisienne de $L/\mathbb{Q}$ est pair, soit $R' = R_{\cap}P'$ (cf. Prop. (2.5)

et Prop. (3.5)) et soit $\langle P - R\rangle$ le groupe des rationnels étrangers à R. On étend la définition de $\psi : \mathbb{Q}' \to I'$ (cf. Déf. (2.1)) à $\langle P - R\rangle \cup \langle R'\rangle$, en posant

$$\psi(c) = \bigoplus_{v\in S}((c,\delta_w)_v)_{w|v}, \quad \text{pour tout} \quad c \in \langle P - R\rangle \cup \langle R'\rangle;$$

si $c \in \langle P - R\rangle, \psi(c)$ est encore un élément de J, car $c \in U_v$ pour tout $v \in S$, mais non nécessairement de I car on peut avoir $(c,\delta_w)_v = -1$ pour $w|v$, $v \notin S$.

(ii) On désigne par I'' l'image de $\langle P' - R'\rangle$ par ψ.

Remark 4.2. (i) Il est clair que l'on a les inclusions

$$I'' \subseteq I' \subseteq I \subseteq J;$$

(ii) La notation I'' sera justifiée plus loin (cf. §5) par le fait que ce sous-groupe de I' ne dépend pas des valeurs prises par R, mais seulement du "schéma galoisien" qui résulte des données L/K, R (en un sens à préciser);

(iii) comme $\langle P'\rangle/\langle P' - R'\rangle \simeq \langle R'\rangle$, on a la relation

$$I' = I''\langle\psi(R')\rangle,$$

qui montre que, si I'' est identifié, I' s'en déduit au moyen d'un invariant arithmétique élémentaire $(\psi(R'))$ qui dépend alors numériquement de R.

On a alors, d'après le Lemme (3.2), et pour tout $\ell \in P - R$, l'expression suivante de $\psi(\ell)$ sur $J = \bigoplus_{v\in S} J_v$:

$$\psi(\ell) = \left(\ldots, \left(\left(\frac{\varepsilon_v p_v}{\ell}\right)^{d_w f_w}\right)_{w|v}, \ldots; \left(\left(\frac{2}{\ell}\right)^{d_w f_w}\left(\frac{-1}{\ell}\right)^{d'_w}\right)_{w|v}\right),$$

ou

$$\psi(\ell) = \left(\ldots, \left(\left(\frac{\varepsilon_v p_v}{\ell}\right)^{d_w f_w}\right)_{w|v}, \ldots\right),$$

selon que $2 \in S$ ou non.

Cette expression montre qu'il faut réindexer la base $(\eta_v)_{v\in S}$ de J, en la base $(\eta_q)_{q\in Q}$, où l'ensemble Q est ainsi défini:

Definition 4.3. Soit Q l'ensemble des nombres q suivants:

(i) $q = \varepsilon_v p_v$ pour toute place impaire $v \in S$, où $\varepsilon_v = (-1)^{\frac{p_v-1}{2}}$;

(ii) si la place paire est dans S, on considère de façon non exclusive

$$q = 2 \quad \text{si} \quad \eta_{v,-1} = (1) \quad (\text{i.e.} \quad d'_w = 0, \quad \text{pour tout } w|v),$$
$$q = -1 \quad \text{si} \quad \eta_{v,2} = (1) \quad (\text{i.e.} \quad d_w f_w = 0, \quad \text{pour tout } w|v),$$
$$q = -2 \quad \text{si} \quad \eta_{v,-1} = \eta_{v,2} \quad (\text{i.e.} \quad d'_w = d_w f_w, \quad \text{pour tout } w|v).$$

On identifie désormais J à $\{\pm 1\}^Q$ et l'on désigne par $(\eta_q)_{q\in Q}$ la base canonique de $\{\pm 1\}^Q$.

Dans le cadre de ces notations, on obtient immédiatement (en comparant avec l'expression précédente de $\psi(\ell)$) :

$$\psi(\ell) = \left(\left(\frac{q}{\ell}\right)\right)_{q\in Q}, \quad \text{pour tout} \quad \ell \in P - R, \tag{4.1}$$

et en définissant le symbole

$$\left(\frac{q}{\cdot}\right) : \langle P - R\rangle \longrightarrow \{\pm 1\},$$

par multiplicativité, on obtient:

$$\psi(c) = \left(\left(\frac{q}{c}\right)\right)_{q\in Q}, \quad \text{pour tout} \quad c \in \langle P - R\rangle. \tag{4.2}$$

L'interprétation galoisienne que nous avons en vue va être réalisée au moyen de l'extension kummerienne suivante :

Definition 4.4. On désigne par F la 2-extension abélienne élémentaire $\mathbb{Q}\left(\sqrt{\langle Q\rangle}\right)$ de $\mathbb{Q}$.

Considérons alors le symbole d'Artin usuel $\left(\frac{F/\mathbb{Q}}{\cdot}\right)$ à valeurs dans $\mathrm{Gal}(F/\mathbb{Q})$; il est défini en particulier sur $\langle P - R\rangle$ et est caractérisé par ses restrictions aux sous-corps $\mathbb{Q}\left(\sqrt{q}\right)$, $q \in Q$, car F est le composé direct sur $\mathbb{Q}$ de ces corps quadratiques; or on a, pour $\ell \in P - R$, $\ell \neq -1$:

$$\left(\frac{F/\mathbb{Q}}{\ell}\right)\sqrt{q} = \left(\frac{\mathbb{Q}\left(\sqrt{q}\right)/\mathbb{Q}}{\ell}\right)\sqrt{q},$$

égal à $\sqrt{q}$ si et seulement si ℓ est décomposé dans $\mathbb{Q}\left(\sqrt{q}\right)$ (i.e., $\left(\frac{q}{\ell}\right) = 1$); de même, comme $\left(\frac{F/\mathbb{Q}}{-1}\right)$ est la conjugaison complexe sur F, on a:

$$\left(\frac{F/\mathbb{Q}}{-1}\right)\sqrt{q} = \left(\frac{\mathbb{Q}\left(\sqrt{q}\right)/\mathbb{Q}}{-1}\right)\sqrt{q},$$

égal à $\sqrt{q}$ si et seulement si $q > 0$ $\left(\text{i.e., } \left(\frac{q}{-1}\right) = 1\right)$.

Il en résulte, par multiplicativité, l'identité suivante:

$$\left(\frac{F/\mathbb{Q}}{a}\right)\sqrt{q} = \left(\frac{q}{a}\right)\sqrt{q}, \quad \text{pour tout} \quad a \in \langle P - R\rangle, \quad \text{pour tout} \quad q \in Q.$$

Compte tenu de la surjection (car R est fini):

$$\left(\frac{F/\mathbb{Q}}{\cdot}\right) : \langle P - R\rangle \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(F/\mathbb{Q}),$$

et des formules (4.2), on obtient l'isomorphisme fondamental θ avec lequel nous travaillerons désormais.

Proposition 4.5. *L'application θ qui à $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ associe $\left(\sigma\sqrt{q}/\sqrt{q}\right)_{q\in Q}$ est un isomorphisme de $\mathrm{Gal}(F/\mathbb{Q})$ sur $\{\pm 1\}^Q \simeq J$, dans lequel l'image de $\left(\frac{F/\mathbb{Q}}{a}\right)$ est égale à $\psi(a)$ pour tout $a \in \langle P - R\rangle$.*

Remark 4.6. Il est clair que $I'' = \psi(\langle P' - R'\rangle)$ est l'image de $\left\langle\left(\frac{F/\mathbb{Q}}{P'-R'}\right)\right\rangle$ dans l'isomorphisme θ.

Terminons ce paragraphe par un résultat qui permet de voir facilement l'indice (égal à 1 ou 2) de I dans J:

Proposition 4.7. *Soit $d = N_{K/\mathbb{Q}}\delta \in \mathbb{Q}^\times$. Alors on a $d \in \langle Q\rangle\, \mathbb{Q}^{\times 2}$, et*

$$(J : I) = \left(d\mathbb{Q}^{\times 2} : \mathbb{Q}^{\times 2}\right).$$

Proof. Soit $v \in P\ell^0_{\mathbb{Q}}$; la norme globale étant le produit des normes locales, on a $d = \prod_{w|v} \delta_w$; d'après les formules de la Déf. (3.1), (ii), il vient :

$$v(d) \bmod 2\mathbb{Z} = \sum_{w|v} v(\delta_w) \bmod 2\mathbb{Z} = \sum_{w|v} d_w f_w .$$

(i) Si $v \notin S$ (cf. Déf. (2.1), (ii)), on a, d'après la Prop. (3.3), $d_w f_w = 0$, pour tout $w|v$, d'où $v(d) \equiv 0 \bmod 2$, ce qui montre (cf. Déf. (4.3)) que d est de la forme

$$d \equiv \varepsilon \prod_{\substack{q\in Q\\ q\neq -1}} q^{t_q} \bmod \mathbb{Q}^{\times 2}, \quad \varepsilon \in \{\pm 1\}, \quad t_q \in \mathbb{Z}/2\mathbb{Z}. \tag{4.3}$$

(ii) Si $v \in S$, on a donc, pour le nombre $q \neq -1$ correspondant ($q = \varepsilon_v p_v$ ou $q = 2$ ou $q = -2$)

$$t_q = \sum_{w|v} d_w f_w .$$

(iii) On considère maintenant la place paire v (indépendamment du fait que $v \in S$ ou non) et on pose $U' = 1 + 4\mathbb{Z}_2$; il vient (cf. Déf. (3.1), (ii), b) :

$$d = \prod_{w|v} \delta_w \equiv 2^{\sum_{w|v} d_w f_w} (-1)^{\sum_{w|v} d'_w} 5^{\sum_{w|v} d''_w} \bmod \mathbb{Q}_2^{\times 2},$$

soit, en tenant compte de (4.3)

$$\varepsilon \equiv \prod_{\substack{q\in Q\\ q\neq -1}} q^{t_q}\, 2^{\sum_{w|v} d_w f_w} (-1)^{\sum_{w|v} d'_w} \bmod U'\,\mathbb{Q}_2^{\times 2}. \tag{4.4}$$

On utilise la définition de la partie paire de Q (cf. Déf. (4.3), (ii)), en remarquant que $Q - \{2, -1, -2\} \subset U'$:

a) Si $Q \cap \{2, -1, -2\} = \emptyset$, c'est que $d_w f_w = d'_w = 0$, pour tout $w|v$; d'où

$$\varepsilon \in \langle Q\rangle U'\mathbb{Q}_2^{\times 2} \subset U'\mathbb{Q}_2^{\times 2},$$

ce qui conduit à $\varepsilon = 1$.

b) Si $Q \cap \{2, -1, -2, \} = \{2\}$, c'est que $d'_w = 0$, pour tout $w|v$; d'où

$$\varepsilon \in \langle Q \rangle U' \mathbb{Q}_2^{\times 2} \subset 2^{\mathbb{Z}/2\mathbb{Z}}\, U'\, \mathbb{Q}_2^{\times 2},$$

et $\varepsilon = 1$.

c) Si $Q \cap \{2, -1, -2\} = \{-1\}$, c'est que $d_w f_w = 0$, pour tout $w|v$; d'où

$$\varepsilon \equiv (-1)^{\sum_{w|v} d'_w} \bmod U' \mathbb{Q}_2^{\times 2},$$

soit $\varepsilon = (-1)^{t_{-1}}$ avec $t_{-1} = \sum_{w|v} d'_w$.

d) Si $Q \cap \{2, -1, -2\} = \{-2\}$, c'est que $d'_w = d_w f_w$, $w|v$; donc

$$\varepsilon \equiv \prod_{q \in Q} q^{t_q} (-2)^{\sum_{w|v} d'_w} \bmod U' \mathbb{Q}_2^{\times 2},$$

ce qui conduit à $\varepsilon = 1$.

e) Enfin si Q contient $\{-1, 2\}$, on obtient $\varepsilon = (-1)^{t_{-1}}$, avec $t_{-1} = \sum_{w|v} d'_w$.

On a donc, d'après (4.3) et (4.4),

$$(4.5) \qquad d \equiv \prod_{q \in Q} q^{t_q} \bmod \mathbb{Q}^{\times 2}, \quad t_q = \sum_{w|v} d_w f_w \quad \left(\text{resp. } \sum_{w|v} d'_w \right)$$

si $q \neq -1$ (resp. $q = -1$).

On remarque que $I = J$ si et seulement si chaque $\eta_q \in J$, $q \in Q$, satisfait à la formule du produit dans $\bigoplus_{w \in P\ell_K} J_w$; comme

$$\eta_q = \left((-1)^{d_w f_w}\right)_{w|v} \quad \left(\text{resp. } \left((-1)^{d'_w}\right)_{w|v}\right)$$

si $q \neq -1$ (resp. $q = -1$), où v est la place correspondante, on a $I = J$ si et seulement si:

$$\sum_{w|v} d_w f_w = 0 \quad \left(\text{resp. } \sum_{w|v} d'_w = 0 \right)$$

si $q \neq -1$ (resp. $q = -1$), ce qui est équivalent à

$$t_q = 0, \quad \text{pour tout} \quad q \in Q \quad (\text{i.e., } d \in \mathbb{Q}^{\times 2}). \qquad \square$$

Remark 4.8. Si $d \notin \mathbb{Q}^{\times 2}$, la formule du produit ne concerne que le sous-groupe

$$\bigoplus_{q \in Q_0} \langle \eta_q \rangle,$$

où $Q_0 = \{q \in Q, t_q = 1\}$; autrement dit, on a

$$I = \left(\widetilde{\bigoplus_{q \in Q_0}} \langle \eta_q \rangle \right) \bigoplus \left(\bigoplus_{q \in Q - Q_0} \langle \eta_q \rangle \right),$$

où

$$\widetilde{\bigoplus_{q\in Q_0}}\langle\eta_q\rangle \;=\; \left\{ \left(\eta_q^{\lambda_q}\right)_{q\in Q_0}, \lambda_q \in \mathbb{Z}/2\,\mathbb{Z}, \sum_{q\in Q_0}\lambda_q = 0 \right\}.$$

5. Interprétation galoisienne de $\theta^{-1}(I'')$

Soit $\widehat{L}$ la clôture galoisienne de $L/\mathbb{Q}$. Le but de ce §5 est d'établir le résultat fondamental concernant la structure de I', à savoir que son sous-groupe

$$I'' \;=\; \langle\psi(P'-R')\rangle$$

est un invariant galoisien lié essentiellement à la structure de $\mathrm{Gal}(\widehat{L}/\mathbb{Q})$ (en un sens qui sera précisé dans la remarque (5.4)), ramenant ainsi, grâce à la relation $I' = I''\langle\psi(R')\rangle$, le calcul de I', puis de $\mathcal{L}/\mathcal{G} \simeq I/I'$, à celui des symboles de Hilbert $(p,\delta_w)_v$, $w|v$, $v\in S$, $p\in R'$, donnés numériquement par le Lemme (3.2).

En réalité cette étude se fait au niveau des images $\theta^{-1}(I')$, $\theta^{-1}(I'')$ (sous-groupes de $\theta^{-1}(J) = \mathrm{Gal}(F/\mathbb{Q})$) (cf. Prop. (4.5)) qui permettent seules l'interprétation galoisienne en question.

Definition 5.1. (i) Soit $\mathcal{D}_{L/K} = \mathcal{D}$ l'ensemble des 2-sous-groupes cycliques D de $G = \mathrm{Gal}(\widehat{L}/\mathbb{Q})$ ayant la propriété suivante: Pour tout conjugué D' de D on a $D'_{\cap}\,\mathrm{Gal}(\widehat{L}/K) \subseteq \mathrm{Gal}(\widehat{L}/L)$.

(ii) Soit $A = \mathrm{Gal}(\widehat{L}/\widehat{L}_{\cap}F)$. Pour tout $D\in\mathcal{D}$, on désigne par $\overline{D} = DA/A$ l'image canonique de D dans $\mathrm{Gal}(\widehat{L}_{\cap}F/\mathbb{Q})$ (elle ne dépend que de la classe de conjugaison de D) et on appelle E'' le sous-corps de $\widehat{L}_{\cap}F$ fixe par le sous-groupe de G/A engendré par les $\overline{D}$, $D\in\mathcal{D}$.

On peut alors énoncer:

Theorem 5.2. *Le sous-groupe* $\mathrm{Gal}(F/E'')$ *est égal à l'image de* $\langle P'-R'\rangle$ *par le symbole d'Artin* $\left(\frac{F/\mathbb{Q}}{\cdot}\right)$; *par conséquent,* $I'' = \theta(\mathrm{Gal}(F/E''))$.

Proof.(i) Inclusion $\left\langle\left(\frac{F/\mathbb{Q}}{P'-R'}\right)\right\rangle \subseteq \mathrm{Gal}(F/E'')$.

Montrons que si $\ell = p_v \in P'-R'$ alors $\left(\frac{F/\mathbb{Q}}{\ell}\right) \in \mathrm{Gal}(F/E'')$. Puisque $E''\subseteq \widehat{L}_{\cap}F$, il revient au même de montrer que

$$\left(\frac{\widehat{L}_{\cap}F/\mathbb{Q}}{\ell}\right) \in \mathrm{Gal}(\widehat{L}_{\cap}F/E'')\,.$$

Soit Δ le groupe de décomposition, dans $\widehat{L}/\mathbb{Q}$, d'une place $\widehat{w}$ de $\widehat{L}$ au-dessus de v; comme l'indice de ramification de $\widehat{w}$ est impair, il existe un sous-groupe normal Ω de Δ, d'ordre impair, contenant le sous-groupe d'inertie de $\widehat{w}$, et tel que Δ/Ω soit

un 2-groupe cyclique; si D est un 2-Sylow quelconque de Δ, alors D est cyclique et on a $\Delta = \Omega \rtimes D$. Soient N_0 et N les sous-corps de $\widehat{L}$ fixes par Δ et Ω; alors $\mathrm{Gal}(N/N_0) \simeq \Delta/\Omega$ est engendré par le Frobenius $\left(\frac{N/N_0}{\widehat{w}}\right)$, et comme $\widehat{L}\cap F \subseteq N$, la restriction de $\left(\frac{N/N_0}{\widehat{w}}\right)$ à $\widehat{L}\cap F$ est

$$\left(\frac{\widehat{L}\cap F/N_0\cap F}{\widehat{w}}\right) = \left(\frac{\widehat{L}\cap F/\mathbb{Q}}{\widehat{w}}\right)$$

puisque $\widehat{w}$ est totalement décomposée dans $N_0/\mathbb{Q}$; mais

$$\left(\frac{\widehat{L}\cap F/\mathbb{Q}}{\widehat{w}}\right) = \left(\frac{\widehat{L}\cap F/\mathbb{Q}}{v}\right)$$

qui n'est autre que le symbole d'Artin $\left(\frac{\widehat{L}\cap F/\mathbb{Q}}{\ell}\right)$. Enfin comme $\Omega \subseteq A$, on a

$$\overline{D} = DA/A = \Omega DA/A = \Delta A/A \simeq \mathrm{Gal}(\widehat{L}\cap F/N_0\cap F)$$

engendré par $\left(\frac{\widehat{L}\cap F/\mathbb{Q}}{\ell}\right)$.

Si l'on montre que $D \in \mathcal{D}$ (cf. Déf. (5.1), (i)), on aura montré que $\left(\frac{\widehat{L}\cap F/\mathbb{Q}}{\ell}\right) \in \overline{D} = DA/A$, et donc que $\left(\frac{F/\mathbb{Q}}{\ell}\right) \in \mathrm{Gal}(F/E'')$ par définition de E'' (cf. Déf. (5.1), (ii)). Or puisque $\ell = p_v \in P' - R'$, la place v est totalement décomposée dans L/K (cf. Prop. (2.6)); comme l'ensemble des groupes de décomposition des places de $\widehat{L}$ au-dessus de v est l'ensemble des conjugués Δ' de Δ, la condition de décomposition est équivalente à $\Delta'_\cap \mathrm{Gal}(\widehat{L}/K) \subseteq \mathrm{Gal}(\widehat{L}/L)$ quel que soit Δ'; ceci implique en particulier

$$D'_\cap \mathrm{Gal}(\widehat{L}/K) \subseteq \mathrm{Gal}(\widehat{L}/L)$$

pour tout conjugué D' de D, ce qui signifie bien $D \in \mathcal{D}$.

(ii) Inclusion $\mathrm{Gal}\,(F/E'') \subseteq \left\langle \left(\frac{F/\mathbb{Q}}{P'-R'}\right)\right\rangle$.

Pour démontrer l'inclusion opposée, il suffit de montrer que:

Pour tout $\overline{\tau} \in \mathrm{Gal}(\widehat{L}\cap F/E'')$, tel que $\langle\overline{\tau}\rangle = \overline{D}$ pour un $D \in \mathcal{D}$, et pour tout relèvement τ_1 de $\overline{\tau}$ dans $\mathrm{Gal}(F/\mathbb{Q})$, il existe $\ell \in P' - R'$ tel que $\left(\frac{F/\mathbb{Q}}{\ell}\right) = \tau_1$.

(α) Cas où $\overline{\tau} = 1$. Dans ce cas on peut prendre $D = 1$, et ici τ_1 est un élément de $\mathrm{Gal}(F/\widehat{L}\cap F)$. Relevons τ_1 en $\tau'_1 \in \mathrm{Gal}(\widehat{L}F/\widehat{L}) \simeq \mathrm{Gal}(F/\widehat{L}\cap F)$; alors il existe une place $\widehat{w}$ de $\widehat{L}F$, que l'on peut choisir au-dessus d'une place v de $\mathbb{Q}$ non ramifiée dans $\widehat{L}F/\mathbb{Q}$, telle que l'on ait $\left(\frac{\widehat{L}F/\mathbb{Q}}{\widehat{w}}\right) = \tau'_1$. Comme τ'_1 fixe $\widehat{L}$, il en est de même pour ses conjugués dans $\mathrm{Gal}(\widehat{L}F/\mathbb{Q})$ $\left(\text{i.e., pour les frobenius } \left(\frac{\widehat{L}F/\mathbb{Q}}{\widehat{w}'}\right), \widehat{w}'|v\right)$, et v est totalement décomposée dans $\widehat{L}/\mathbb{Q}$, donc dans L/K; d'où $\ell = p_v \in P' - R'$ (cf. Prop. (2.6)) et, par restriction à F, $\left(\frac{\widehat{L}F/\mathbb{Q}}{\widehat{w}}\right)$ a pour image $\left(\frac{F/\mathbb{Q}}{v}\right) = \left(\frac{F/\mathbb{Q}}{\ell}\right) = \tau_1$.

(β) Cas où $\overline{\tau} \neq 1$. Soit N le sous-corps de $\widehat{L}$ fixe par $D \in \mathcal{D}$ tel que $\overline{D} = \langle \overline{\tau} \rangle$, et soit M le sous-corps de $\widehat{L} \cap F$ fixe par $\overline{\tau}$; on a $AD = \mathrm{Gal}(\widehat{L}/M)$. Soit τ_1 un relèvement de $\overline{\tau}$ dans $\mathrm{Gal}(F/\mathbb{Q})$ et soit M_1 le corps qu'il fixe; on remarque que $M_1 \cap \widehat{L} = M$. En effet, $M_1 \cap \widehat{L}$ est contenu dans $\widehat{L}$ et dans F, donc dans $\widehat{L} \cap F$; de plus $M_1 \cap \widehat{L}$ est fixe par τ_1, donc par $\overline{\tau}$, et on a $M_1 \cap \widehat{L} \subseteq M$, d'où l'égalité, l'autre inclusion étant triviale. On a donc $\mathrm{Gal}(\widehat{L}F/M_1) \simeq \mathrm{Gal}(\widehat{L}/M)$.

Soit alors N_1 le composé $M_1 N$; on a donc l'isomorphisme:

$$D_1 \;=\; \mathrm{Gal}(\widehat{L}F/N_1) \;\simeq\; \mathrm{Gal}(\widehat{L}/N) \;=\; D\,.$$

Par conséquent, D_1 est 2-cyclique et il existe une place $\widehat{w}$ de $\widehat{L}F$, au-dessus d'une place v de $\mathbb{Q}$ non ramifiée dans $\widehat{L}F/\mathbb{Q}$, telle que $\left(\frac{\widehat{L}F/\mathbb{Q}}{\widehat{w}}\right)$ engendre D_1.

Dans la projection $\mathrm{Gal}(\widehat{L}F/\mathbb{Q}) \to \mathrm{Gal}(\widehat{L}/\mathbb{Q})$, l'image d'un conjugué D_1' de D_1 est un conjugué D' de D pour lequel on sait que $D' \cap \mathrm{Gal}(\widehat{L}/K) \subseteq \mathrm{Gal}(\widehat{L}/L)$; or ceci est précisément équivalentà la décomposition de v dans L/K. Par ailleurs la restriction de $\left(\frac{\widehat{L}F/\mathbb{Q}}{\widehat{w}}\right)$ à F est $\left(\frac{F/\mathbb{Q}}{v}\right) = \left(\frac{F/\mathbb{Q}}{\ell}\right) = \tau_1$; on a donc encore $\ell = p_v \in P' - R'$.

D'où le théorème. □

Remark 5.3. (i) On peut montrer assez facilement que si l'on a $L \subseteq KF$, alors E'' est un sous-corps de $L \cap F$.

(ii) La construction que nous faisons, en termes de frobenius, se justifie par le fait que l'on dispose du théorème de densité de Čebotarev qui permet de dire que tout sous-groupe cyclique de G est, d'une infinité de façons, groupe de décomposition dans $\widehat{L}/\mathbb{Q}$ d'une place de $\widehat{L}$, ceci ne voulant pas dire que tout élément de I'' soit de la forme $\psi(\ell)$ $\left($ou, de façon équivalente, tout élément de $\mathrm{Gal}(F/E'')$ de la forme $\left(\frac{F/\mathbb{Q}}{\ell}\right)\right)$ pour $\ell \in P'$. L'exemple des extensions galoisiennes $\widehat{L}/\mathbb{Q}$ à groupe de Galois isomorphe à D_8, est instructif à ce sujet: Soit $\widehat{L}$ une extension galoisienne de $\mathbb{Q}$ telle que $G = \mathrm{Gal}(\widehat{L}/\mathbb{Q}) \simeq D_8$. Désignons par K_0 le sous-corps biquadratique de $\widehat{L}$ et par (K_1, K_1'), (K_2, K_2') les deux paires de corps non galoisiens conjugués, de degré 4. On a $K_1 \cap K_1' = k_1$, $K_2 \cap K_2' = k_2$, où k_1 et k_2 sont deux des sous-corps quadratiques de K_0; le troisième sous-corps quadratique k_0 est fixé par l'unique sous-groupe cyclique d'ordre 4 de G. On désigne successivement par D_1, D_1', D_2, D_2' les groupes de Galois de $\widehat{L}/K_1$, $\widehat{L}/K_1'$, $\widehat{L}/K_2$, $\widehat{L}/K_2'$.

Supposons que $L = \widehat{L}$, $K = K_0$ et que $\widehat{L} \cap F = K_0$; on a $\mathcal{D}_{L/K} = \{D_1, D_1', D_2, D_2'\}$ et les DA/A, qui sont les $\mathrm{Gal}(K/k_i)$, $i = 1, 2$, engendrent $\mathrm{Gal}(K/\mathbb{Q})$ sans que tous les sous-groupes de ce groupe soient de la forme DA/A: le générateur de $\mathrm{Gal}(K/k_0)$ n'est pas le frobenius d'une place de $\mathbb{Q}$ (non ramifiée dans $\widehat{L}/\mathbb{Q}$) décomposée dans L/K.

Remark 5.4. La définition de E'' fait référence à l'intersection $\widehat{L} \cap F$ qui peut varier en fonction de F (donc de l'arithmétique de $L/K/\mathbb{Q}$) par l'intermédiaire de l'ensemble Q; cependant, à G fixé comme groupe abstrait, le groupe $\mathrm{Gal}(E''/\mathbb{Q}) \simeq J/I''$ ne peut prendre qu'un nombre fini de valeurs dépendant seulement de $G/G^2[G,G]$, le quotient

abélien 2-élémentaire maximal de G. On perçoit donc maintenant mieux les "degrés de liberté" de l'invariant $\mathcal{L}/\mathcal{G} \simeq I/I'$, lorsque G est fixé. Le cas limite, qui élimine toute référence à l'arithmétique, est le suivant:

Corollary 5.5. *Soit L/K une extension quadratique de corps de nombres, et soit G le groupe de Galois de la clôture galoisienne $\widehat{L}$ de L sur $\mathbb{Q}$. Soit $\Gamma = G^2[G,G]$; si les images $D\Gamma/\Gamma$ des sous-groupes $D \in \mathcal{D}_{L/K}$ engendrent G/Γ, alors on a $\mathcal{L}_{L/K}/\mathcal{G}_{L/K} = 1$.*

En effet, puisque $\widehat{L}_\cap F/\mathbb{Q}$ est une 2-extension abélienne élémentaire,

$$A \;=\; \mathrm{Gal}\big(\widehat{L}/\widehat{L}_\cap F\big) \supset \Gamma\,;$$

comme les DA/A sont les images des $D\Gamma/\Gamma$ dans la projection $G/\Gamma \to G/A$, il est clair que les DA/A engendrent G/A et donc que $E'' = \mathbb{Q}$, ce qui implique $I'' = I' = I = J$, soit $\mathcal{L}_{L/K}/\mathcal{G}_{L/K} = 1$.

Remark 5.6. En utilisant l'exemple précédent de D_8, on vérifie facilement que le Corollaire (5.5) s'applique pour toutes les extensions quadratiques L/K pour lesquelles la clôture galoisienne de L est $\widehat{L}$ ($\widehat{L}/K_0$, puis $\widehat{L}/K_1, K_1/k_1$ et leurs analogues); le cas de $L/K = \widehat{L}/K_1$ illustre le Théorème (7.3) démontré plus loin et est repris au §8, b; enfin le cas de $L/K = \widehat{L}/K_0$ a été démontré par A. Cortella [C2].

6. Interprétation et calcul de $\mathcal{L}/\mathcal{G}$

Dans l'isomorphisme canonique

$$\theta^{-1} \;:\; J \;\longrightarrow\; \mathrm{Gal}(F/\mathbb{Q}) \quad \text{(cf. Prop. (4.5))}\,,$$

les inclusions

$$I'' \subseteq I' \subseteq I \subseteq J\,,$$

correspondent aux inclusions

$$E'' \supseteq E' \supseteq E \supseteq \mathbb{Q}\,,$$

de sous-corps de $\widehat{L}_\cap F$ pour lesquels on a

$$\mathcal{L}/\mathcal{G} \;\simeq\; I/I' \;\simeq\; \mathrm{Gal}(E'/E)\,.$$

Le corps $E'' \subseteq F = \mathbb{Q}\big(\sqrt{\langle Q\rangle}\big)$ étant connu de façon galoisienne (cf. Déf. (5.1), (ii)), écrivons-le sous la forme kummerienne

$$E'' \;=\; \mathbb{Q}\big(\sqrt{\wedge''}\big)\,, \quad \wedge'' \subseteq \langle Q\rangle\,,$$

avec

$$\wedge'' \;=\; \langle d_1, \ldots, d_t\rangle\,, \quad d_i \;=\; \prod_{q\in Q} q^{n_{q,i}}\,. \tag{6.1}$$

Dans l'isomorphisme

$$\theta \,:\, \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow J\,,$$

la base $(\eta_q)_{q\in Q}$ de J (cf. Déf. (4.3)) correspond à la base canonique $(\sigma_q)_{q\in Q}$ de $\mathrm{Gal}(F/\mathbb{Q})$ caractérisée par les conditions suivantes

$$\sigma_q\big(\sqrt{q'}\big) \;=\; \sqrt{q'}\,, \quad \text{pour tout} \quad q' \in Q - \{q\} \quad \text{et} \quad \sigma_q\big(\sqrt{q}\big) \;=\; -\sqrt{q}\,. \tag{6.2}$$

Posons alors, pour tout $p \in R'$,

$$\psi(p) \;=\; \Big((-1)^{y_q^p}\Big)_{q\in Q}, \quad y_q^p \in \mathbb{Z}/2\mathbb{Z}\,, \tag{6.3}$$

et

$$\tau_p \;=\; \prod_{q\in Q} \sigma_q^{y_q^p}\,.$$

On a par définition $\tau_p = \theta^{-1}(\psi(p))$, et le sous-groupe engendré par $\mathrm{Gal}(F/E'')$ et les τ_p, $p \in R'$, fixe par définition le sous-corps E' cherché. De façon précise, posons $E' = \mathbb{Q}\big(\sqrt{\Lambda'}\big)$, $\Lambda' \subseteq \Lambda''$; trouver E' équivaut à caractériser les $d' \in \langle d_1, \ldots, d_t\rangle$ tels que $\sqrt{d'} \in E'$:

Posons $d' = \prod_{i=1}^t d_i^{m_i}$, $m_i \in \mathbb{Z}/2\,\mathbb{Z}$; alors $\sqrt{d'} \in E'$ si et seulement si $\sqrt{d'}$ est fixe par tous les τ_p, $p \in R'$, ce qui s'écrit

$$\Big(\prod_{q\in Q} \sigma_q^{y_q^p}\Big)\big(\sqrt{d'}\big) = \sqrt{d'}\,, \quad \text{pour tout} \quad p \in R'\,,$$

$$\Longleftrightarrow$$

$$\Big(\prod_{q\in Q} \sigma_q^{y_q^p}\Big)\Big(\prod_{i=1}^t \sqrt{d_i}^{\,m_i}\Big) = \prod_{i=1}^t \sqrt{d_i}^{\,m_i}\,, \quad \text{pour tout} \quad p \in R'\,,$$

$$\Longleftrightarrow$$

$$\sum_{q,i} y_q^p m_i n_{q,i} \;=\; 0\,, \quad \text{pour tout} \quad p \in R'\,, \qquad \text{(cf. (6.1))}$$

$$\Longleftrightarrow$$

$$\sum_{i=1}^t \Big(\sum_{q\in Q} y_q^p n_{q,i}\Big)\, m_i \;=\; 0\,, \quad \text{pour tout} \quad p \in R';$$

posons

$$\alpha_i^p \;=\; \sum_{q\in Q} y_q^p n_{q,i}\,, \quad \text{pour tout} \quad p \in R'\,, \quad \text{pour tout} \quad i \in \{1, \ldots, t\}\,, \tag{6.4}$$

alors toute base de solutions du système

$$\sum_{i=1}^t \alpha_i^p m_i \;=\; 0\,, \quad p \in R'\,, \tag{6.5}$$

donne une base du radical de $E'/\mathbb{Q}$.

Il ne reste plus qu'à identifier le corps E; comme on peut s'y attendre, il est lié au nombre d introduit à la Prop. (4.7) pour caractériser l'indice $(J : I)$:

Lemma 6.1. *On a* $E = \mathbb{Q}(\sqrt{d})$, *où* $d = N_{K/\mathbb{Q}}\delta$.

Proof. Posons $E = \mathbb{Q}(\sqrt{d_0})$; comme E est un sous-corps de $F = \mathbb{Q}(\sqrt{\langle Q \rangle})$, on peut poser $d_0 = \prod_{q \in Q} q^{n_q}$; d_0 est caractérisé par les conditions suivantes (cf. Rem. (4.8)):

$$\prod_{q \in Q} \sigma_q^{\lambda_q}(\sqrt{d_0}) = \sqrt{d_0},$$

quels que soient les $\lambda_q \in \mathbb{Z}/2\mathbb{Z}$, $q \in Q$, tels que $\sum_{q \in Q_0} \lambda_q = 0$. On a

$$\prod_{q \in Q} \sigma_q^{\lambda_q}(\sqrt{d_0}) = (-1)^{\sum_q \lambda_q n_q} \sqrt{d_0};$$

par conséquent, les n_q doivent vérifier

$$\sum_{q \in Q} \lambda_q n_q = 0, \text{ pour tout } (\lambda_q)_{q \in Q} \text{ tel que } \sum_{q \in Q_0} \lambda_q = 0;$$

on vérifie facilement que l'unique solution non triviale est donnée par

$$n_q = 0, \quad \text{pour tout} \quad q \notin Q_0, \quad n_q = 1, \quad \text{pour tout} \quad q \in Q_0;$$

d'où le lemme compte-tenu de la définition de d. □

Corollary 6.2. *On a* $|\mathcal{L}/\mathcal{G}| = 2^{t-rg(M)}$ *(resp.* $2^{t-rg(M)-1}$*) si* $d \in \mathbb{Q}^{\times 2}$ *(resp.* $d \notin \mathbb{Q}^{\times 2}$*), où* M *est la matrice* (α_i^p), $p \in R'$, $i = 1, \ldots, t$ *(cf.* (6.4), (6.1), (6.3)).

7. Considérations pratiques et exemple

Par commodité nous résumons ici les différentes étapes permettant la détermination effective de $\mathcal{L}/\mathcal{G}$ pour $L = K(\sqrt{\delta})$, de clôture galoisienne $\widehat{L}$:

(i) On détermine l'ensemble

$$\Sigma = \{v \in P\ell_{\mathbb{Q}}, v \text{ ramifiée dans } L/K\}.$$

(ii) On calcule les normes locales

$$\delta_w = N_{K_w/\mathbb{Q}_v}\delta, \quad v \in \Sigma, \quad w|v,$$

et on pose (cf. Déf. (3.1)), pour $v \in \sum$, $w|v$:

$$\delta_w \equiv p_v^{d_w f_w} \zeta_v^{d'_w} \bmod \mathbb{Q}_v^{\times 2}, \qquad \text{pour } v \text{ impaire},$$
$$\delta_w \equiv 2^{d_w f_w}(-1)^{d'_w} 5^{d''_w} \bmod \mathbb{Q}_v^{\times 2}, \quad \text{pour } v \text{ paire},$$

où f_w est le degré résiduel de w dans $K/\mathbb{Q}$ et d_w, d'_w, $d''_w \in \mathbb{Z}/2\mathbb{Z}$.

(iii) On détermine l'ensemble

$$Q = \left\{(-1)^{\frac{p_v-1}{2}} p_v, v \in \Sigma, v \text{ impaire}, (d_w f_w)_{w|v} \neq (0)\right\} \bigcup \begin{cases} \{2,-1\}, \\ \text{ou } \{2\}, \\ \text{ou } \{-1\}, \\ \text{ou } \{-2\}, \\ \text{ou } \emptyset, \end{cases}$$

selon que la place paire v est telle que

$$\begin{aligned} &\langle (d_w f_w)_{w|v}, (d'_w)_{w|v}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \\ &(d'_w)_{w|v} = (0) \quad \text{et} \quad (d_w f_w)_{w|v} \neq (0), \\ &(d_w f_w)_{w|v} = (0) \quad \text{et} \quad (d'_w)_{w|v} \neq (0), \\ &(d_w f_w)_{w|v} = (d'_w)_{w|v} \neq (0), \\ &(d_w f_w)_{w|v} = (d'_w)_{w|v} = (0). \end{aligned}$$

On obtient alors

$$F = \mathbb{Q}\left(\sqrt{\langle Q\rangle}\right),$$

puis (cf. Lemme (6.1))

$$E = \mathbb{Q}\left(\sqrt{d}\right), \quad d = N_{K/\mathbb{Q}}\delta \in \langle Q\rangle \mathbb{Q}^{\times 2}.$$

(iv) On considère le corps $\widehat{L}_\cap F$ et on pose

$$A = \mathrm{Gal}\left(\widehat{L}/\widehat{L}_\cap F\right);$$

on détermine le sous-corps E'' de $\widehat{L}_\cap F$ fixe par le sous-groupe de $\mathrm{Gal}\left(\widehat{L}_\cap F/\mathbb{Q}\right)$ engendré par les DA/A, pour les 2-sous-groupes cycliques D de $\mathrm{Gal}\left(\widehat{L}/\mathbb{Q}\right)$ tels que $D'_\cap \mathrm{Gal}\left(\widehat{L}/K\right) \subseteq \mathrm{Gal}\left(\widehat{L}/L\right)$ pour tout conjugué D' de D. Si $E'' = E$, on a $\mathcal{L}/\mathcal{G} = 1$.

Supposons $[E'' : E] > 1$.

(v) On détermine l'ensemble R des nombres premiers dont l'indice de ramification dans $\widehat{L}/\mathbb{Q}$ est pair, puis $R' = R_\cap P'$ qui, d'après la Prop. (3.5), est donné par

$$\begin{aligned} R' = \{&p_v \in R, \text{ il existe } \lambda_v \in \mathbb{Z}/2\mathbb{Z} \text{ (resp. il existe } \lambda_v, \mu_v \in \mathbb{Z}/2\mathbb{Z}) \text{ tels que} \\ &d'_w = \lambda_v d_w f_w, \text{ pour tout } w|v, \text{ pour } v \text{ impaire} \\ &(\text{resp. } d''_w = \lambda_v d_w f_w + \mu_v d'_w, \text{ pour tout } w|v, \text{ pour } v \text{ paire}\}. \end{aligned}$$

On remarquera que pour les $p_v \in R$ tels que $v \notin \Sigma$, il est plus rapide d'utiliser la Prop. (2.6) puisque dans ce cas les δ_w ne sont pas calculés.

(vi) On calcule les

$$\psi(p) = \left((-1)^{y_q^p}\right)_{q \in Q}, \quad p \in R',$$

au moyen des formules explicites suivantes (cf. Lemme (3.2) et Prop. (3.5)):

(α) Si $q \notin \{2,-1,-2\}$ $\left(\text{i.e., } q = (-1)^{\frac{p_v-1}{2}} p_v\right)$:

$$\begin{aligned}(-1)^{v_q^p} &= \left(\frac{q}{p}\right) && \text{si } p \neq p_v\,,\\ &= (-1)^{\frac{p-1}{2}+\lambda_v} && \text{si } p = p_v\,;\end{aligned}$$

(β) si $q \in \{2,-1,-2\}$ (i.e., $p_v = 2$) :

$$\begin{aligned}(-1)^{v_2^p} &= \left(\frac{2}{p}\right) && \text{si } p \neq 2,\\ &= (-1)^{\lambda_v} && \text{si } p = 2;\\ (-1)^{v_{-1}^p} &= \left(\frac{-1}{p}\right) && \text{si } p \neq 2,\\ &= (-1)^{\mu_v} && \text{si } p = 2;\\ (-1)^{v_{-2}^p} &= \left(\frac{-2}{p}\right) && \text{si } p \neq 2,\\ &= (-1)^{\lambda_v+\mu_v} && \text{si } p = 2.\end{aligned}$$

(vii) On calcule une base $(d_1, \ldots, d_t)$ du radical de l'extension $E''/\mathbb{Q}$ caractérisée au point (iv), et l'on écrit

$$d_i = \prod_{q \in Q} q^{n_{q,i}}, \quad i = 1, \ldots, t, \quad n_{q,i} \in \mathbb{Z}/2\mathbb{Z};$$

on forme enfin la matrice

$$M = (\alpha_i^p), \quad p \in R', \quad i = 1, \ldots, t,$$

où

$$\alpha_i^p = \sum_{q \in Q} y_q^p n_{q,i}, \quad p \in R', \quad i = 1, \ldots, t,$$

et on obtient

$$|\mathcal{L}/\mathcal{G}| = \frac{2^{t-\mathrm{rg}\,(M)}}{[E : \mathbb{Q}]}.$$

A titre d'illustration, démontrons le résultat suivant, donnant pour la structure $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, une famille infinie de contre-exemples.

Theorem 7.1. *Soit* $k = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Q}^\times - \mathbb{Q}^{\times 2}$, $m \equiv \pm 1 \bmod 5$. *Soit* $L = k(\mu_5)$, *et soit* $K = \mathbb{Q}(\sqrt{m}, \sqrt{5})$. *Alors, pour l'extension quadratique* L/K, *on a* $|\mathcal{L}/\mathcal{G}| = 2$ *si et seulement si tout diviseur premier du discriminant de* k *est congru à* ± 1 *modulo* 5.

Proof. Comme $\mathbb{Q}(\mu_5) = \mathbb{Q}(\sqrt{5})\left(\sqrt{\frac{-5+\sqrt{5}}{2}}\right)$, on a $L = K(\sqrt{\delta})$ pour $\delta = \frac{-5+\sqrt{5}}{2}$.

(i) On a $\Sigma = \{v\}$, où $p_v = 5$, et $\{w \in P\ell_K, w|v\} = \{w', w''\}$ puisque $\left(\frac{m}{5}\right) = 1$.

(ii) Comme le corps de décomposition de v dans $L/\mathbb{Q}$ est k, on a, pour $w \in \{w', w''\}$,

$$\delta_w = N_{K/k}\delta = N_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}\left(\frac{-5+\sqrt{5}}{2}\right) = 5,$$

d'où $d_w f_w = d_w = 1$ et $d'_w = 0$, pour $w \in \{w', w''\}$.

(iii) On a immédiatement

$$Q = \{5\}, \quad N_{K/\mathbb{Q}}\,\delta = 5^2, \quad F = \mathbb{Q}(\sqrt{5}), \quad E = \mathbb{Q}.$$

(iv) On a $A = \mathrm{Gal}(L/\mathbb{Q}(\sqrt{5}))$ et

$$\mathcal{D}_{L/K} = \{\mathrm{Gal}(L/\mathbb{Q}(\mu_5),\ \mathrm{Gal}(L/L')\},$$

où L' est l'extension cyclique de degré 4 distincte de $\mathbb{Q}(\mu_5)$; comme ces sous-groupes D se projettent sur 1 dans G/A, on a $E'' = F = \mathbb{Q}(\sqrt{5})$. Donc ici $[E'' : E] = 2$.

(v) On a $R = \{5, p_1, \ldots, p_r\}$, où les p_i sont les nombres premiers ramifiés dans $k/\mathbb{Q}$. Comme $\delta_w = 5 \equiv 5^1\ \zeta_v^0 \bmod \mathbb{Q}_v^{\times 2}$, pour tout $w \in \{w', w''\}$, on a $5 \in R'$ car $\lambda_v = 0$ convient; comme l'indice de ramification des p_i dans $K/\mathbb{Q}$ est pair, on a $p_i \in R'$ pour tout i, d'où $R' = R$.

(vi) On a successivement, pour $p \in R$ $(p \neq 5)$,

$$\psi(p) = \left(\frac{5}{p}\right),$$

et, de même

$$\psi(5) = (-1)^{\frac{5-1}{2} + \lambda_v} = 1;$$

on a donc $t = 1$ et $|\mathcal{L}/\mathcal{G}| = 2^{t - rg(M)}$, où M est la matrice colonne formée des y_5^p, $p \in R$, pour lesquels

$$(-1)^{y_5^{p_i}} = \left(\frac{5}{p_i}\right) = \left(\frac{p_i}{5}\right), \quad i = 1, \ldots, r, \quad \text{et} \quad y_5^5 = 0;$$

d'où

$$(7.1) \qquad |\mathcal{L}/\mathcal{G}| = 2 \text{ si et seulement si } \left(\frac{p}{5}\right) = 1, \quad \text{pour tout} \quad p \in R - \{5\},$$

ce qui fournit, pour cette structure, une infinité de contre-exemples au principe de Hasse étudié (le corps L de conducteur minimum conduisant à un tel contre-exemple est obtenu pour $m = -11$). Remarquons que la condition ci-dessus suppose $m \equiv 1 \bmod 4$, car $\left(\frac{2}{5}\right) = -1$; elle est alors compatible avec la condition de décomposition $\left(\frac{m}{5}\right) = 1$. Pour $m \equiv 1 \bmod 4$, on aura $\mathcal{L}/\mathcal{G} = 1$ dès qu'il existe un nombre pair non nul de p_i tels que $\left(\frac{p_i}{5}\right) = -1$. Enfin si $\left(\frac{m}{5}\right) = -1$, on a, pour l'unique place w de K au-dessus de 5,

$$\delta_w = N_{K_w/\mathbb{Q}_w}(\delta) = N_{K/\mathbb{Q}}(\delta) = 5^2,$$

soit $Q = \emptyset$, $F = \mathbb{Q}$ et $\mathcal{L}/\mathcal{G} = 1$. □

Remark 7.2. Lorsque K est imaginaire (i.e., $m < 0$) et que $\mathcal{L}/\mathcal{G} \simeq \mathbb{Z}/2\mathbb{Z}$ (i.e., $\left(\frac{p}{5}\right) = 1$ pour tout p ramifié dans $k/\mathbb{Q}$), alors $\varepsilon = \frac{1+\sqrt{5}}{2}$ est un représentant de la classe non triviale de $\mathcal{L}/\mathcal{G}$ (et même de $\mathcal{L}'/\mathbb{Q}'N_{L/K}L^\times$):

(i) L'unité ε est norme locale dans L/K en toute place de K ne divisant pas 5 (ceci est en défaut pour les places à l'infini de K lorsque celui-ci est réel car ε n'est pas totalement positive). Comme $\varepsilon \equiv \frac{1}{2} \bmod \left(\sqrt{5}\right)$, on a bien $\varepsilon = u_v N_v \alpha_v$, $\alpha_v \in L_v$, pour $p_v = 5$, en prenant $u_v = \frac{1}{2}$ (cf. Déf. (1.3)).

(ii) Supposons que $\varepsilon = a\ N_{L/K}\alpha$, $a \in \mathbb{Q}'$, $\alpha \in L^\times$. Puisque $5 = N_{L/K}\left(\sqrt{5}\right)$, on peut toujours supposer que a est de la forme

$$a = \ell_1 \dots \ell_r,\ \ell_i \in P' - \{5\},\quad \ell_i \text{ distincts}.$$

On a donc en particulier $(\varepsilon a^{-1}, \delta)_w = 1$ pour $w \in \{w', w''\}$, soit, puisque $(\varepsilon, \delta)_w = \left(\frac{\varepsilon}{w}\right) = \left(\frac{1/2}{w}\right) = -1$,

$$\left(\frac{a}{5}\right) = -1.$$

D'après la Prop. (2.6), les ℓ_i sont soit décomposés dans L/K, soit ramifiés dans $K/\mathbb{Q}$; dans le premier cas, on vérifie que ℓ_i est nécessairement décomposé dans $\mathbb{Q}\left(\sqrt{5}\right)/\mathbb{Q}$, d'où $\left(\frac{\ell_i}{5}\right) = 1$; dans le second, ℓ_i est alors l'un des p ramifiés dans $k/\mathbb{Q}$ pour lesquels on a par hypothèse $\left(\frac{p}{5}\right) = 1$. On obtient donc $\left(\frac{a}{5}\right) = \prod_{i=1}^{r}\left(\frac{\ell_i}{5}\right) = 1$, ce qui est absurde.

Le cas $\mathrm{Gal}(\widehat{L}/\mathbb{Q}) \simeq D_8$ ayant été résolu dans la Rem. (5.3), donnons le résultat général suivant qui correspond au cas où L/K est "décomposée":

Theorem 7.3. *On suppose que $L = KL_1$, où L_1 est une extension quadratique de $\mathbb{Q}$ non contenue dans K.*

(i) *Si $[K : \mathbb{Q}]$ est impair alors $\mathcal{L}/\mathcal{G} = 1$.*

(ii) *Si K contient un sous-corps quadratique, alors $\mathcal{L}/\mathcal{G} = 1$.*

Proof. On peut prendre pour δ le rationnel qui est tel que $L_1 = \mathbb{Q}\left(\sqrt{\delta}\right)$, auquel cas on a

$$d = N_{K/\mathbb{Q}}\delta = \delta^{[K:\mathbb{Q}]}.$$

Dans le cas (i), comme $[K : \mathbb{Q}] \equiv 1 \bmod 2$, $d \notin \mathbb{Q}^{\times 2}$ et on obtient $E = L_1$; dans le cas (ii), on a au contraire $E = \mathbb{Q}$. Nous allons montrer que dans tous les cas le Corollaire (5.5) s'applique ici. Désignons par L_2 la sous-extension de $\widehat{L}$ fixe par $G^2[G,G]$ et posons $M = L_2 \cap K$ et $M_1 = ML_1 = L_2 \cap L$; on a $[M_1 : M] = 2$. Convenons du fait que pour tout $\overline{\tau} \in \mathrm{Gal}(L_2/\mathbb{Q})$, τ désigne un relèvement de $\overline{\tau}$ dans G, d'ordre puissance de 2 $\left(\text{c'est toujours possible puisque } \overline{\tau^\lambda} = \overline{\tau}^\lambda \text{ pour tout } \lambda \text{ impair}\right)$. Soit enfin $s \in \mathrm{Gal}\left(\widehat{L}/K\right)$ tel que sa restriction à L engendre $\mathrm{Gal}(L/K)$.

Soit $\bar{\sigma} \in \mathrm{Gal}(L_2/\mathbb{Q})$ tel que les restrictions $\bar{\sigma}_{M_1}$ et $\bar{s}_{M_1}$ de $\bar{\sigma}$ et $\bar{s}$ à M_1 soient distinctes; alors on a $\langle\sigma\rangle \in \mathcal{D}$ pour $\sigma \in G$ relevant $\bar{\sigma}$: dans le cas contraire il existe

$\tau \in G$ tel que $\langle \tau\sigma\tau^{-1}\rangle \cap \mathrm{Gal}(\widehat{L}/K) \not\subseteq \mathrm{Gal}(\widehat{L}/L)$, donc il existe $t \in \mathrm{Gal}(\widehat{L}/K)$, de la forme $t = \tau\sigma^i\tau^{-1}$, $i \in \mathbb{Z}$, tel que $t \notin \mathrm{Gal}(\widehat{L}/L)$, ce qui équivaut à $t = st'$, $t' \in \mathrm{Gal}(\widehat{L}/L)$, et on a donc

$$st' = \tau\sigma^i\tau^{-1},$$

qui conduit à

$$\bar{s}\bar{t}' = \bar{\tau}\bar{\sigma}^i\bar{\tau}^{-1} = \bar{\sigma}^i \text{ puisque } \mathrm{Gal}(L_2/\mathbb{Q}) \text{ est abélien};$$

comme $t' \in \mathrm{Gal}(\widehat{L}/L)$, $\bar{t}' \in \mathrm{Gal}(L_2/M_1)$ et par conséquent, $\bar{s}_{M_1} = \bar{\sigma}^i_{M_1}$, ce qui est absurde car si $i \equiv 0\ (2)$, on obtient $\bar{s}_{M_1} = \bar{1}$ ce qui est contraire au choix de s, et si $i \equiv 1\ (2)$, c'est contraire au choix de $\bar{\sigma}$; d'où l'assertion.

Posons $\mathcal{D}' = \{D = \langle\sigma\rangle,\ \bar{\sigma}_{M_1} \neq \bar{s}_{M_1}\} \subseteq \mathcal{D}$, et vérifions que $\{\overline{D} = \langle\bar{\sigma}\rangle, D \in \mathcal{D}'\}$ engendre $\mathrm{Gal}(L_2/E)$.

Dans le cas (i), puisque $E = L_1$, le résultat est clair car

$$M_1 = L_1 \quad \text{et} \quad \mathcal{D}' = \{\langle\sigma\rangle, \bar{\sigma} \in \mathrm{Gal}(L_2/L_1)\}.$$

Dans le cas (ii), il faut engendrer $\mathrm{Gal}(L_2/\mathbb{Q})$. Soit $\bar{\tau} \in \mathrm{Gal}(L_2/\mathbb{Q})$; si $\bar{\tau}_{M_1} \neq \bar{s}_{M_1}$ alors $\langle\bar{\tau}\rangle = \overline{D}$ avec $D = \langle\tau\rangle \in \mathcal{D}'$; supposons alors que $\bar{\tau}_{M_1} = \bar{s}_{M_1}$; comme par hypothèse K contient un sous-corps quadratique, on a $[M_1 : L_1] \geq 2$, ce qui fait qu'il existe $\bar{\sigma}_0 \in \mathrm{Gal}(L_2/L_1)$ tel que $\bar{\sigma}_{0M_1} \neq \bar{1}$, et on a $\overline{\tau\sigma_0}_{M_1} = \bar{\tau}_{M_1}\bar{\sigma}_{0M_1} = \bar{s}_{M_1}\bar{\sigma}_{0M_1} \neq \bar{s}_{M_1}$, d'où l'existence de λ impair tel que $\langle(\tau\sigma_0)^\lambda\rangle \in \mathcal{D}'$; de même, $\bar{\sigma}_{0M_1} \neq \bar{s}_{M_1}$ car $\mathrm{Gal}(M_1/L_1) \cap \mathrm{Gal}(M_1/M) = 1$, et $\langle\sigma_0\rangle \in \mathcal{D}'$. D'où le résultat puisque $\bar{\tau} = (\overline{\tau\sigma_0})\,\bar{\sigma}_0 = (\overline{\tau\sigma_0})^\lambda\bar{\sigma}_0 = \overline{(\tau\sigma_0)^\lambda}\bar{\sigma}_0$. □

8. Compléments (d'après les techniques de [C2])

Au plan cohomologie des tores, il vient donc

$$\mathcal{L}/\mathcal{G} \simeq Ш\,(k,T) = Ш\,(T),$$

où $Ш\,(k,T)$ est le groupe de Schafarevich-Tate,

$$\ker\left(H^1(k,T) \longrightarrow \prod_{v\in P\ell_k} H^1(k_v,T)\right),$$

d'un tore T convenable associé à l'extension $L/K/k$ (cf. [C2, III 1]), où le corps de base k est ici un corps de nombres quelconque, mais L/k galoisienne de groupe de Galois G.

Considérons le diagramme ci-dessous, dans lequel $H = \mathrm{Gal}(L/K)$, et Ω est l'ensemble (fini) des sous-groupes de G qui coïncident avec le groupe de décomposition G_v, dans L/k, d'une place de L au-dessus d'une place v de k,

$$\begin{array}{ccc} H & \xleftarrow{\mu} & G^{ab} \\ \uparrow & & \uparrow\delta \\ \prod\limits_{v\in\Omega}\left(\bigoplus\limits_{i=1}^{r_v} H_i^v\right) & \xleftarrow{\eta} & \prod\limits_{v\in\Omega} G_v^{ab} \end{array} \tag{8.1}$$

les applications μ et η_v sont respectivement les transferts ver_H^G et $\mathrm{ver}_{H_i^v}^{G_v}$, où

$$H_i^v = G_v \cap x_i^v H (x_i^v)^{-1},$$

les x_i^v décrivant un système de représentants des r_v doubles classes $G_v \backslash G / H$ (cf. [C2, III 4, b]), l'application δ étant canonique.

Ce diagramme conduit à l'isomorphisme suivant permettant le calcul de $Ш(T)$ (cf. [C2, III 4, d]):

$$Ш(T) \simeq \mathrm{Ker}\,\mu / \delta(\mathrm{Ker}\,\eta). \tag{8.2}$$

Si l'on remplace Ω par l'ensemble $\mathcal{C}$ des sous-groupes cycliques de G, le schéma (8.1) devient

$$\begin{array}{ccc} H & \xleftarrow{\mu} & G^{ab} \\ \uparrow & & \uparrow \delta' \\ \prod\limits_{c \in \mathcal{C}} \left(\bigoplus\limits_{i=1}^{r_c} H_i^c \right) & \xleftarrow{\eta'} & \prod\limits_{c \in \mathcal{C}} c \end{array} \tag{8.3}$$

et le groupe

$$Ш_c(k,T) = Ш_c(T) = \ker\left(H^1(k,T) \longrightarrow \prod_{G_v \in \mathcal{C}} H^1(k_v,T)\right),$$

qui contient trivialement $Ш(k,T)$, est tel que

$$Ш_c(T) \simeq \mathrm{Ker}\,\mu / \delta'(\ker \eta'). \tag{8.4}$$

a) Etude de la famille du Théorème (7.1).

Désignons par s (resp. t) un générateur de $\mathrm{Gal}\big(L/\mathbb{Q}(\sqrt{m})\big)$ (resp. $L/\mathbb{Q}(\mu_5)$), et calculons ver_H^G au moyen de la section (cf. [Se, Prop. 7, p. 129])

$$\theta : G/H \longrightarrow G,$$

définie par

$$\begin{aligned} \theta(\bar{1}) &= \theta(\bar{s}^2) = 1, \\ \theta(\bar{t}) &= \theta(\bar{t}\,\bar{s}^2) = t, \\ \theta(\bar{s}) &= \theta(\bar{s}^3) = s, \\ \theta(\bar{t}\,\bar{s}) &= \theta(\bar{t}\,\bar{s}^3) = ts; \end{aligned}$$

alors les $x_{\bar{a},b} = \theta(\bar{a}) b \theta(\bar{a}\,\bar{b})^{-1}$, $\bar{a} \in G/H$, $b \in \{s,t\}$, sont les suivants:

$$\begin{aligned} x_{\bar{1},s} &= \theta(\bar{1}) s \theta(\bar{s})^{-1} = 1, & x_{\bar{1},t} &= \theta(\bar{1}) t \theta(\bar{t})^{-1} = 1, \\ x_{\bar{t},s} &= \theta(\bar{t}) s \theta(\bar{t}\,\bar{s})^{-1} = 1, & x_{\bar{t},t} &= \theta(\bar{t}) t \theta(\bar{1})^{-1} = 1, \\ x_{\bar{s},s} &= \theta(\bar{s}) s \theta(\bar{s}^2)^{-1} = s^2, & x_{\bar{s},t} &= \theta(\bar{s}) t \theta(\bar{s}\bar{t})^{-1} = 1, \\ x_{\bar{t}\bar{s},s} &= \theta(\bar{t}\bar{s}) s \theta(\bar{t}\bar{s}^2)^{-1} = s^2, & x_{\bar{s}\bar{t},t} &= \theta(\bar{t}\bar{s}) t \theta(\bar{s})^{-1} = 1, \end{aligned}$$

et $\mathrm{ver}_H^G : G^{ab} = G \to H$ est caractérisé par

$$\mathrm{ver}_H^G(s) = \prod_{\bar{a} \in G/H} x_{\bar{a},s} = 1, \qquad \mathrm{ver}_H^G(t) = \prod_{\bar{a} \in G/H} x_{\bar{a},t} = 1;$$

d'où $\mathrm{Ker}\,\mathrm{ver}_H^G = \mathrm{Ker}\,\mu = G$.

De même, les calculs de transferts

$$\mathrm{ver}_{H\cap C}^C : C \longrightarrow C_{\cap} H,$$

pour les sous-groupes cycliques C de G, donnent

$$\begin{aligned} \mathrm{Ker}\big(\mathrm{ver}_{H\cap C}^C(C)\big) &= C, && \text{pour } C = \langle t\rangle \text{ ou } \langle ts^2\rangle, \\ \mathrm{Ker}\big(\mathrm{ver}_{H\cap C}^C(C)\big) &= \langle 1\rangle, && \text{pour } C = \langle s^2\rangle, \\ \mathrm{Ker}\big(\mathrm{ver}_{H\cap C}^C(C)\big) &= \mathrm{Ker}\big(\mathrm{ver}_H^C(C)\big) = \langle s^2\rangle, && \text{pour } C = \langle s\rangle \text{ ou } \langle t\,s\rangle \end{aligned}$$

(cf. [C2, III 7, e]).

D'où (cf. (8.3), (8.4))

$$\begin{aligned} Ш_c(T) &= G/\delta'\big(\langle t\rangle \times \langle ts^2\rangle \times \langle 1\rangle \times \langle s^2\rangle \times \langle s^2\rangle\big) \\ &= G/\langle t, s^2\rangle \\ &\simeq \mathbb{Z}/2\mathbb{Z}; \end{aligned} \tag{8.5}$$

on est bien dans un cas où l'obstruction galoisienne ne suffit pas.

Pour le calcul de $Ш(T)$, il reste uniquement à regarder les morphismes de transferts

$$\mathrm{ver}_{G_v\cap H}^{G_v},$$

pour les groupes de décomposition G_v associés aux places v ramifiées dans $L/\mathbb{Q}$, avec G_v non cyclique, les seules possibilités étant ici $G_v = \langle t, s\rangle$, $\langle t, s^2\rangle$.

Il suffit même de se limiter aux cas où G_v contient le générateur s (dont la classe mod $\langle t, s^2\rangle$ engendre $Ш_c(T)$), ce qui équivaut à supposer $G_v = G$. Or, par définition, les ramifiés dans $L/\mathbb{Q}$ sont 5 et les p_i ramifiés dans $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$; donc $G_v = G$ ne peut se produire que pour certains des p_i puisque, par hypothèse, 5 est décomposé dans $\mathbb{Q}(\sqrt{m})/\mathbb{Q}$, donc s'il existe p_i tel que $\left(\frac{p_i}{5}\right) = -1$ (i.e. p_i totalement inerte dans $\mathbb{Q}(\mu_5)/\mathbb{Q}$), auquel cas $Ш(T) = 1$. On retrouve bien le fait que

$$Ш(T) = Ш_c(T) \simeq \mathbb{Z}/2\mathbb{Z}$$

si et seulement si $\left(\frac{p_i}{5}\right) = 1$ pour tout i (cf. (7.1)).

b) Etude du cas de D_8 avec H non normal.

Comparons avec les résultats obtenus (Rem. (5.6) et Th. (7.3)).

On pose $G = \langle t, s\rangle$, avec $t^2 = s^4 = 1$ et $tst^{-1} = s^{-1}$; on a

$$G^{ab} = G/\langle s^2\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z};$$

on considère le cas où $H = \langle t\rangle$.

En prenant les représentants de $H\backslash G$ dans $\langle s\rangle$ (i.e., $\theta(\bar{1}) = \theta(\bar{t}) = 1$, $\theta(\bar{s}) = \theta(\bar{t}\bar{s}) = s$, $\theta(\bar{s}^2) = \theta(\bar{t}\,\bar{s}^2) = s^2$, $\theta(\bar{s}^3) = \theta(\bar{t}\bar{s}^3) = s^3$), il vient:

$$\begin{aligned}
x_{\bar{1},t} &= \theta(\bar{1})t\theta(\bar{t})^{-1} = t, & x_{\bar{1},s} &= \theta(\bar{1})s\theta(\bar{s})^{-1} = 1,\\
x_{\bar{s},t} &= \theta(\bar{s})t\theta(\bar{s}\bar{t})^{-1} = sts = t, & x_{\bar{s},s} &= \theta(\bar{s})s\theta(\bar{s}^2)^{-1} = 1,\\
x_{\bar{s}^2,t} &= \theta(\bar{s}^2)t\theta(\bar{s}^2\bar{t})^{-1} = s^2ts^2 = t, & x_{\bar{s}^2,s} &= \theta(\bar{s}^2)s\theta(\bar{s}^3)^{-1} = 1,\\
x_{\bar{s}^3,t} &= \theta(\bar{s}^3)t\theta(\bar{s}^3\bar{t})^{-1} = s^3ts^{-1} = t, & x_{\bar{s}^3,s} &= \theta(\bar{s}^3)s\theta(\bar{1})^{-1} = 1;
\end{aligned}$$

d'où $\mathrm{ver}_H^G(t) = t^4 = 1$ et $\mathrm{ver}_H^G(s) = 1$, soit

$$\mathrm{Ker}(\mathrm{ver}_H^G) = G^{ab}.$$

Ensuite, pour un sous-groupe cyclique C de G, il faut faire l'intersection de C avec les H_i^c, c'est-à-dire trouver les conjugués de H qui sont dans C (les autres donnant un transfert nul).

Ces conjugués sont les $\langle s^i\, t\, s^{-i}\rangle = \langle t\, s^{2i}\rangle$; d'où

$$H = \langle t\rangle \quad \text{et} \quad H' = \langle t\, s^2\rangle.$$

Examinons les différents $C \in \mathcal{C}$.

(i) $C = H$ ou H' : $\mathrm{ver}_C^C = \mathrm{id}$, de noyau $\langle 1\rangle$;
(ii) $C = \langle s^2\rangle$: $H_\cap C = H'_\cap C = \{1\}$;
(iii) $C = \langle t\, s\rangle$ ou $\langle t\, s^3\rangle$: $H_\cap C = H'_\cap C = \{1\}$;
(iv) $C = \langle s\rangle$ $H_\cap C = H'_\cap C = \{1\}$;

d'où

$$\ker\eta = \langle s^2\rangle \times \langle t\, s\rangle \times \langle t\, s^3\rangle \times \langle s\rangle$$

et

$$\delta(\ker\eta) \equiv \langle s, ts\rangle \bmod \langle s^2\rangle = G^{ab},$$

soit, comme attendu (cf. Rem. (5.6)):

$$\text{(8.6)} \qquad \text{Ш}\,(T) = \text{Ш}_C\,(T) = 1.$$

c) Etude du cas de $G = H_{16}$.

Alors H est nécessairement l'unique sous-groupe d'ordre 2 de G. On pose

$$G = \langle s, t\rangle, \quad \text{avec} \quad s^8 = t^4 = 1,\ s^4 = t^2,\ tst^{-1} = s^{-1};$$

on a alors

$$H = \langle t^2\rangle = \langle s^4\rangle.$$

On a $G^{ab} = G/\langle s^2\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On peut prendre le système de représentants de $H\backslash G$ défini par

$$\begin{aligned}
\theta(\bar{s}^i) &= \theta(\bar{s}^{i+4}) = s^i, \quad \text{si } 0 \le i \le 3,\\
\theta(\bar{s}^i\bar{t}) &= \theta(\bar{s}^{i+4}\bar{t}) = s^it, \quad \text{si } 0 \le i \le 3;
\end{aligned}$$

alors, pour $0 \le i \le 3$ et $0 \le j \le 1$, on a :

$$x_{\bar{s}^i\bar{t}^j,t} = \theta(\bar{s}^i\bar{t}^j)t\theta(\bar{s}^i\bar{t}^{j+1})^{-1} = s^it^jt(s^it^{1-j})^{-1} = s^it^{2j}s^{-i} = t^{2j},$$

donc

$$\mathrm{ver}_H^G(t) = \prod_{i,j}^{3} x_{\bar{s}^i\bar{t}^j,t} = \prod_{i=0}^{3}\prod_{j=0}^{1} t^{2j} = t^8 = 1;$$

$$\begin{aligned} x_{\bar{s}^i\bar{t}^j,s} &= \theta(\bar{s}^i\bar{t}^j)s\theta(\bar{s}^i\bar{t}^j\,\bar{s})^{-1} \\ &= s^{i+1}(s^{i+1})^{-1} && = 1, && \text{si } j = 0,\ 0 \le i \le 2, \\ &= s^4 && = t^2, && \text{si } j = 0,\ i = 3, \\ &= s^{i-1}t(s^{i-1}t)^{-1} && = 1, && \text{si } j = 1,\ 1 \le i \le 3, \\ &= s^{-1}t(s^3t)^{-1} && = s^{-4} = s^4 = t^2, && \text{si } j = 1,\ i = 0. \end{aligned}$$

Donc

$$\mathrm{ver}_H^G(s) = \prod_{i,j} x_{\bar{s}^i\bar{t}^j,s} = t^4 = 1, \quad \text{et} \quad \ker(\mathrm{ver}_H^G) = G^{ab}.$$

Pour les sous-groupes cycliques, il vient (H étant normal):

(i) $C = H$: $\mathrm{ver}_H^H = \mathrm{id}$;

(ii) $C = \langle t\rangle$, $\langle s^2t\rangle$, $\langle st\rangle$ ou $\langle s^3t\rangle$: $H \cap C = H$, et $\ker \mathrm{ver}_H^C = H$ ([C2, III 7, e]);

(iii) $C = \langle s^2\rangle$: $H \cap C = H$ et $\ker(\mathrm{ver}_H^C) = H$;

(iv) $C = \langle s\rangle$: le calcul de ver_H^C: $\langle s\rangle \simeq \mathbb{Z}/8\mathbb{Z} \to \langle s^4\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ donne facilement $\ker(\mathrm{ver}_H^C) = \langle s^2\rangle$.

D'où

$$(8.7) \qquad Ш_C(T) \simeq G^{ab} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z};$$

on retrouve le même groupe que dans le cas de H_8 (cf. [C2, III 7, d]) ce qui peut conduire au même type de contre-exemple que celui de [C1].

9. Calcul explicite d'un nouveau contre-exemple

On va exhiber des formes $\mathbb{Q}$-bilinéaires ne satisfaisant pas au principe de Hasse, à partir de la structure $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, étudiée au Th. (7.1) et au §8, a, avec $m = -11$.

D'après la Rem. (7.2), $\varepsilon = \frac{1+\sqrt{5}}{2}$ est un représentant de la classe non triviale de $\mathcal{L}/\mathcal{G}$ pour l'extension $L/K = K(\sqrt{\delta})/K$ avec $K = \mathbb{Q}(\sqrt{5}, \sqrt{-11})$.

On vérifie enfin que $\alpha = \frac{2\zeta+1+\sqrt{-11}}{2\zeta^{-1}+1-\sqrt{-11}}$ (où $\zeta = \exp(2i\pi/5)$) est un élément primitif de $L/\mathbb{Q}$ de norme 1 dans L/K.

On trouve (en utilisant PARI):

$$\begin{aligned} P &= \mathrm{Irr}(\alpha, \mathbb{Q}) \\ &= X^8 - 10X^7 + \frac{471}{11}X^6 - \frac{1090}{11}X^5 + 131X^4 - \frac{1090}{11}X^3 + \frac{471}{11}X^2 - 10X + 1. \end{aligned}$$

Le polynôme $U(X)$, défini modulo P et tel que $U(\alpha) = \varepsilon = \frac{1+\sqrt{5}}{2}$, est le suivant:

$$U = \frac{55}{6}X^7 - \frac{539}{6}X^6 + \frac{2245}{6}X^5 - \frac{4979}{6}X^4 + \frac{6115}{6}X^3 - 670X^2 + 220X - 29.$$

Les formes bilinéaires b et β, correspondant respectivement aux formes hermitiennes $\langle 1\rangle$ et $\langle a\rangle$ de L, ont les coefficients suivants (cf. [C2, IV 5, b] pour les formules):

$$b_5 = -9 \qquad \beta_1 = 0 \qquad \beta_5 = -50$$
$$b_6 = \frac{-519}{11} \qquad \beta_2 = \frac{-11}{6} \qquad \beta_6 = \frac{-1160}{11}$$
$$b_7 = \frac{-2041}{11} \qquad \beta_3 = \frac{-22}{3} \qquad \beta_7 = \frac{-13015}{66}$$
$$b_8 = \frac{72120}{121} \qquad \beta_4 = \frac{-125}{6} \qquad \beta_8 = \frac{-119842}{363}$$

et les matrices correspondantes sont données par:

$$\begin{pmatrix} 0 & 0 & 0 & -1 & b_5 & b_6 & b_7 & b_8 \\ 0 & 0 & 0 & 0 & -1 & b_5 & b_6 & b_7 \\ 0 & 0 & 0 & 0 & 0 & -1 & b_5 & b_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & b_5 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ b_5 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ b_6 & b_5 & -1 & 0 & 0 & 0 & 0 & 0 \\ b_7 & b_6 & b_5 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 & \beta_8 \\ \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 & \beta_7 \\ \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 & \beta_6 \\ \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 & \beta_5 \\ \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 & \beta_3 \\ \beta_6 & \beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 & \beta_2 \\ \beta_7 & \beta_6 & \beta_5 & \beta_4 & \beta_3 & \beta_2 & \beta_1 & \beta_1 \end{pmatrix}$$

References

[B] BAYER-FLUCKIGER, E.: Principe de Hasse pour les Systèmes de Formes Quadratiques, J. reine angew. Math. **378** (1987), 55-59

[C1] CORTELLA, A.: Un Contre-Exemple au Principe de Hasse pour les Similitudes de Formes Bilinéaires, C. R. Acad. Sci. Paris T. **317**, Série I (1993), 707-710

[C2] CORTELLA, A.: Le Principe de Hasse pour les Similitudes de Formes Bilinéaires (Thèse), Besançon, (1993)

[J] JAULENT, J.-F.: L'Arithmétique des ℓ-Extensions (Thèse), Publ. Math. Fac. Sci. Besançon (Théorie des Nombres), Années 1984/85-1985/86, Fasc. 1 (1986)

[S] SERRE, J.-P.: Corps Locaux, Hermann, Paris, 1968

UFR Sciences
Equipe de Mathématiques
URA CNRS 741
F-25030 Besançon Cedex
France