

Sur la norme du groupe des unités d'extensions quadratiques relatives

par

GEORGES GRAS (Besançon)

0. Introduction. Récemment, plusieurs articles ont traité de la question de la norme de l'unité fondamentale d'un corps quadratique réel, ceci par des méthodes variées:

- (α) M. Hikita (cf. [H, corollary, p. 87]);
- (β) R. Pioui (cf. [P, corollaire (4.9)]);
- (γ) A. Costa and R. Kingan (cf. [C-K, propositions 1.2, 1.2' et corollaries 1.1, 1.2, 1.3, 1.3']);
- (δ) J. Hurrelbrink (cf. [Hu, proposition 1.1, theorem 1.6, proposition 2.1]).

L'un des résultats typiques énoncés dans les articles ci-dessus est le suivant (ou lui est équivalent) :

(0.1) PROPOSITION. Soient $K = \mathbb{Q}(\sqrt{d})$, $K' = \mathbb{Q}(\sqrt{-d})$, $d > 0$ pair sans facteur carré et sans diviseurs premiers congrus à 3 modulo 4; soient $\mathcal{H}_K^{\text{ord}}$, $\mathcal{H}_{K'}^{\text{ord}}$ les 2-Sylow du groupe des classes au sens ordinaire de K , K' , et soit ε l'unité fondamentale de K . Alors les conditions suivantes sont équivalentes :

- (i) $\mathcal{H}_K^{\text{ord}}$ est élémentaire et $N_{K/\mathbb{Q}} \varepsilon = -1$;
- (ii) $\mathcal{H}_{K'}^{\text{ord}}$ est élémentaire ⁽¹⁾.

On peut aussi énoncer ce résultat en termes de cardinalités h , h' des \mathcal{H}^{ord} , car si t est le nombre de diviseurs premiers de d (y compris 2), les conditions (i), (ii) sont respectivement équivalentes à :

- (i)' $h = 2^{t-1}$ et $N_{K/\mathbb{Q}} \varepsilon = -1$;
- (ii)' $h' = 2^{t-1}$.

Dans (α) (resp. (β)), ce résultat est obtenu par des congruences à partir des fonctions L -complexes (resp. 2-adiques); dans (γ), il s'agit de techniques

⁽¹⁾ Un 2-groupe fini est dit élémentaire s'il est annulé par 2.

utilisant des formes modulaires ainsi que leurs liens avec les fonctions L , et, dans (δ) , le résultat est obtenu de façon classique à partir de [C-H].

En fait, un tel résultat est une application immédiate de principes généraux que nous avons donnés dans [G1,2] pour interpréter et systématiser d'anciens résultats de Rédei [R1,2], Scholtz [S], Inaba [I], Fröhlich [F] et d'autres, et pour les étendre au cas des extensions relatives.

Nous avons obtenu le résultat principal (2.1) qui donne une classe naturelle d'extensions quadratiques K/k pour lesquelles une unité de k est norme d'unité si et seulement si elle est norme dans K/k ; voir également le résultat (3.2) qui généralise (0.1) même lorsque $k = \mathbb{Q}$ (cf. (3.4)).

(0.2) HYPOTHÈSE. On fixe un corps de base k totalement réel et 2-principal au sens restreint (i.e. $\mathcal{H}_k^{\text{res}} = 1$ (cf. (0.3))).

(0.3) NOTATIONS. (i) On désigne par $\mathcal{H}_L^{\text{ord}}$ (resp. $\mathcal{H}_L^{\text{res}}$) le 2-groupe des classes au sens ordinaire (resp. restreint) d'un corps de nombres L , par E_L son groupe des unités. On appelle I_L , P_L^{ord} (resp. P_L^{res}) le groupe des idéaux de L , le sous-groupe des idéaux principaux au sens ordinaire (resp. restreint); $\mathcal{H}_L^{\text{ord}}$ et $\mathcal{H}_L^{\text{res}}$ sont donc les 2-Sylow des groupes I_L/P_L^{ord} et I_L/P_L^{res} .

Si $\sigma_1, \dots, \sigma_{r_L}$ sont les r_L plongements réels de L , et si $s_L: L^\times \rightarrow \{\pm 1\}^{r_L}$ est l'homomorphisme de signature, défini par

$$s_L(x) = (\text{signe}(\sigma_i(x)))_{i=1, \dots, r_L},$$

alors on a $P_L^{\text{res}} = \{(x) : x \in L^\times, s_L(x) = 1\}$ ainsi que les suites exactes suivantes qui relient sens ordinaire et sens restreint :

$$\begin{aligned} 1 &\rightarrow P_L^{\text{ord}}/P_L^{\text{res}} \rightarrow \mathcal{H}_L^{\text{res}} \rightarrow \mathcal{H}_L^{\text{ord}} \rightarrow 1, \\ 1 &\rightarrow E_L/E_L^+ \rightarrow L^\times/L^{\times+} \rightarrow P_L^{\text{ord}}/P_L^{\text{res}} \rightarrow 1, \end{aligned}$$

où $L^{\times+} = \text{Ker}(s_L)$ et $E_L^+ = E_L \cap \text{Ker}(s_L)$.

(ii) Soit K une extension quadratique de k , $K = k(\sqrt{\delta})$, $\delta \in k^\times - k^{\times 2}$; soit $G = \langle \tau \rangle = \text{Gal}(K/k)$ et soit $N = N_{K/k}$. On désigne par $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ les idéaux premiers de k ramifiés dans K/k (d'après (0.2) et le corps de classes, on a $t \geq 1$), et on désigne par $\infty_1, \dots, \infty_{t_\infty}$, $t_\infty \geq 0$, les places à l'infini réelles de k ramifiées dans K/k . Si l'on pose $[k : \mathbb{Q}] = m$, le nombre r_K de plongements réels de K est donné par $r_K = 2\varrho$, où $\varrho = m - t_\infty$. Si $\sigma_1, \dots, \sigma_\varrho$ (resp. $\sigma_{\varrho+1}, \dots, \sigma_{\varrho+t_\infty}$) sont les plongements de k dont les prolongements à K sont réels (resp. complexes), on désigne ceux de K sous la forme suivante (par abus de notation) :

$$\sigma_1, \sigma_1\tau, \dots, \sigma_\varrho, \sigma_\varrho\tau \quad (\text{resp. } \sigma_{\varrho+1}, \sigma_{\varrho+1}\tau, \dots, \sigma_{\varrho+t_\infty}, \sigma_{\varrho+t_\infty}\tau).$$

Les t_∞ places à l'infini ∞_j de k , ramifiées dans K/k , correspondent donc aux $\sigma_{\varrho+j}$, $j = 1, \dots, t_\infty$, pour lesquels on a précisément $\sigma_{\varrho+j}(\delta) < 0$.

(iii) On note par $(a, b)_\mathfrak{p}$ le symbole de Hilbert usuel, à valeurs dans $\{\pm 1\}$, où $a, b \in k^\times$ et où \mathfrak{p} est une place arbitraire de k , et on pose $(a, b)_\mathfrak{p} =$

$(-1)^{[a,b]_{\mathfrak{p}}}$ (on dira par abus que $[a,b]_{\mathfrak{p}} \in \mathbb{F}_2$ est le symbole de Hilbert en notation additive). Pour $j \in \{1, \dots, t_\infty\}$, on a $(\delta, a)_{\infty_j} = -1$ si et seulement si $\sigma_{\varrho+j}(a) < 0$.

(0.3.1) Remarque. L'hypothèse (0.2) implique $s_k(E_k) = s_k(k^\times) = \{\pm 1\}^m$, soit $(E_k : E_k^+) = 2^m = (E_k : E_k^2)$, d'où $E_k^+ = E_k^2$.

(0.3.2) Remarque. Le corps k étant seulement supposé 2-principal au sens restreint, pour tout idéal \mathfrak{a} de k , il existe $q \in 1 + 2\mathbb{Z}$ tel que $\mathfrak{a}^q = (a)$ avec $a \in k^{\times+}$; par commodité on désignera par $\tilde{\mathfrak{a}}$ une telle puissance de \mathfrak{a} (q est par exemple le nombre de classes du corps k). En particulier, en ce qui concerne le nombre δ dans (0.3)(ii), on peut toujours supposer que $(\delta) = \tilde{\mathfrak{p}}_1 \dots \tilde{\mathfrak{p}}_{t_0}$, $t_0 \leq t$, quitte à remplacer δ par une puissance impaire, puis choisir un représentant convenable modulo $k^{\times 2}$.

La méthodologie développée dans [G1,2] peut se résumer en l'énoncé suivant (sous l'hypothèse (0.2) et avec les notations (0.3) précédentes relativement à l'extension quadratique K/k):

(0.4) THÉORÈME ([G1, th. (4.3), p. 41; corol. (4.4), p. 42]). Soit \mathcal{H} un sous- G -module de $\mathcal{H}_K^{\text{res}}$ et soit $\tilde{\mathcal{H}} = \{h \in \mathcal{H}_K^{\text{res}} : h^{1-\tau} \in \mathcal{H}\}$; alors $|\tilde{\mathcal{H}}/\mathcal{H}| = 2^{t-1-r}$, où $r \leq t-1$ est le \mathbb{F}_2 -rang de la matrice suivante de symboles de Hilbert en notation additive :

$$M(a_1, \dots, a_n) = ([\delta, a_i]_{\mathfrak{p}_j})_{i=1, \dots, n, j=1, \dots, t}$$

où les a_i sont déterminés ainsi : Soit $\mathcal{I} = \langle \mathfrak{A}_1, \dots, \mathfrak{A}_n \rangle$ un sous- G -module de I_K tel que $\mathcal{I}P_K^{\text{res}}/P_K^{\text{res}} = \mathcal{H}$; soit Λ l'image réciproque de $N\mathcal{I} = \langle N\mathfrak{A}_1, \dots, N\mathfrak{A}_n \rangle \subset P_k^{\text{res}}$ par l'application canonique $\psi : k^{\times+} \rightarrow P_k^{\text{res}}$; on pose alors $\Lambda = \langle a_1, \dots, a_n \rangle E_k^2$.

(0.5) Remarque. Pour le calcul de $r = r(\Lambda)$, on peut remplacer Λ par tout groupe Λ' tel que $\Lambda'NK^\times = \Lambda NK^\times$: en effet, si $a' \in \Lambda'$, il vient $a' \in aNK^\times$, $a \in \Lambda$, soit $(\delta, a')_{\mathfrak{p}} = (\delta, a)_{\mathfrak{p}}$ pour toute place \mathfrak{p} de k ; ceci exprime que $r(\Lambda') \leq r(\Lambda)$, d'où l'égalité par symétrie. On écrit alors $\Lambda' \sim \Lambda$.

1. Caractérisation des $\mathcal{H}_K^{\text{res}}$ élémentaires. On a $(\mathcal{H}_K^{\text{res}})^2 = 1$ si et seulement si $\mathcal{H}_K^{\text{res}} = (\mathcal{H}_K^{\text{res}})^G$, car, puisque $\mathcal{H}_k^{\text{res}} = 1$, pour tout $h \in \mathcal{H}_K^{\text{res}}$ on a $h^2 = h^{1-\tau}h^{1+\tau} = h^{1-\tau}$. Par un argument élémentaire (i.e. le fait que $\tilde{\mathcal{H}} = \mathcal{H}$ équivaut à $\mathcal{H} = \mathcal{H}_K^{\text{res}}$), il suffit de traduire, à partir de (0.4), que $r = t-1$ relativement à $\mathcal{H} = (\mathcal{H}_K^{\text{res}})^G$ (ce qui fait l'objet de l'énoncé (1.6)).

(1.1) LEMME. Le groupe $(\mathcal{H}_K^{\text{res}})^G$ est d'ordre 2^{t-1} et est engendré par les classes (au sens restreint) des éléments de P_K^{ord} et des idéaux $\tilde{\mathfrak{P}}_j$ où \mathfrak{P}_j est au-dessus de \mathfrak{p}_j , $j = 1, \dots, t$ (cf. (0.3), (0.3.2)).

Soit $\mathfrak{A} \in I_K$ tel que $\mathfrak{A}^{1-\tau} = (\alpha)$, $\alpha \in K^{\times+}$; on a donc $N\alpha = \varepsilon \in E_k^+$, mais d'après (0.3.1), $E_k^+ = E_k^2$. On a alors $N\alpha = \eta^2$, $\eta \in E_k$, d'où $\alpha = \eta\beta^{1-\tau}$, $\beta \in K^\times$, d'où $\mathfrak{A}^{1-\tau} = (\beta)^{1-\tau}$, et il existe $\mathfrak{b} \in I_k$, $\mathfrak{B} \in \langle \mathfrak{P}_1, \dots, \mathfrak{P}_t \rangle$, où $N\mathfrak{P}_j = \mathfrak{p}_j$, tels que $\mathfrak{A} = (\beta)(\mathfrak{b})\mathfrak{B}$; comme $\mathfrak{b} \in I_k = P_k^{\text{res}}$, la seconde partie du lemme en résulte. Quant au nombre de classes au sens restreint, invariantes, il a été donné dans [G1, th. (4.1), p. 26].

Soit $\mathcal{P} = \langle (\beta_1), \dots, (\beta_u) \rangle$, $\beta_i \in K^\times$, tels que $\mathcal{P}P_K^{\text{res}} = P_K^{\text{ord}}$; alors on pose $\mathcal{I} = \mathcal{P}\langle \tilde{\mathfrak{P}}_1, \dots, \tilde{\mathfrak{P}}_t \rangle$; d'où $N\mathcal{I} = \langle (N\beta_1), \dots, (N\beta_u), \tilde{\mathfrak{p}}_1, \dots, \tilde{\mathfrak{p}}_t \rangle \subset P_k^{\text{res}}$.

Il existe des $b_i \in k^{\times+}$ et des $\eta_i \in E_k$ tels que

$$(1.1.1) \quad \eta_i N\beta_i = b_i, \quad i = 1, \dots, u;$$

de même il existe des $\pi_j \in k^{\times+}$ tels que $\tilde{\mathfrak{p}}_j = (\pi_j)$, $j = 1, \dots, t$; d'où par ψ^{-1} ,

$$\Lambda = E_k^+ \langle b_1, \dots, b_u, \pi_1, \dots, \pi_t \rangle = E_k^2 \langle b_1, \dots, b_u, \pi_1, \dots, \pi_t \rangle.$$

(1.2) LEMME. On a $\Lambda \sim \Lambda' = F\langle \pi_1, \dots, \pi_t \rangle$ (cf. (0.5)), où $F = \{\eta \in E_k : (\delta, \eta)_{\infty_j} = 1, \text{ pour } j = 1, \dots, t_\infty\}$ (cf. (0.3)(iii)).

D'après (1.1.1), on a $\eta_i \in F$, $i = 1, \dots, u$; d'où $\Lambda \subset \Lambda'NK^\times$. Inversement, si $\eta \in E_k$ est norme locale en les places à l'infini ∞_j , $j = 1, \dots, t_\infty$, η est norme locale en toutes les places à l'infini de k car $(\delta, \eta)_\infty = 1$ si ∞ est non ramifiée dans K/k , donc il existe $\beta \in K^\times$ tel que $b = \eta N\beta \in k^{\times+}$; comme $(\beta) \in \mathcal{P}P_K^{\text{res}} \subset \mathcal{I}P_K^{\text{res}}$, $N(\beta) \in N\mathcal{I}N(P_K^{\text{res}})$, d'où $(b) \in N\mathcal{I}N(P_K^{\text{res}})$ et $b \in \Lambda NK^{\times+}$; d'où $\eta \in \Lambda NK^\times$. D'où le lemme.

(1.3) LEMME. On a $(F : E_k^2) = 2^\rho$ (cf. (0.3)(ii)).

En effet, on a la suite exacte

$$1 \rightarrow F \rightarrow E_k \xrightarrow{f} \{\pm 1\}^{t_\infty} \rightarrow 1,$$

où $f(\varepsilon) = (\text{signe } \sigma_{\varrho+j}(\varepsilon))_{j=1, \dots, t_\infty}$, la surjectivité résultant de l'égalité $s_k(E_k) = s_k(k^\times)$; on a

$$\begin{aligned} \text{Ker } f &= \{\eta \in E_k : \sigma_{\varrho+j}(\eta) > 0, j = 1, \dots, t_\infty\} \\ &= \{\eta \in E_k : (\delta, \eta)_{\infty_j} = 1, \text{ pour } j = 1, \dots, t_\infty\} = F. \end{aligned}$$

D'où $(E_k : F) = 2^{t_\infty}$, soit $(F : E_k^2) = 2^\rho$.

(1.4) Remarque. Si K est totalement réel (resp. totalement imaginaire), alors on a $\Lambda \sim E_k \langle \pi_1, \dots, \pi_t \rangle$ (resp. $\Lambda \sim \langle \pi_1, \dots, \pi_t \rangle$).

(1.5) Notations. On rappelle que $\pi_1, \dots, \pi_t \in k^{\times+}$ sont des générateurs de puissances impaires convenables des idéaux $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ de k ramifiés dans K/k ; on désigne par $\eta_1, \dots, \eta_\varrho$ des unités de k telles que $\langle \eta_1, \dots, \eta_\varrho \rangle E_k^2 = F$ (cf. (1.2), (1.3)). On pose alors

$$(a_1, \dots, a_n) = (\eta_1, \dots, \eta_\varrho, \pi_1, \dots, \pi_t), \quad n = \varrho + t = m - t_\infty + t,$$

et on considère la matrice à coefficients dans \mathbb{F}_2 :

$$M(a_1, \dots, a_n) = M(\eta_1, \dots, \eta_\varrho, \pi_1, \dots, \pi_t) = ([\delta, a_i]_{\mathfrak{p}_j})_{i=1, \dots, n, j=1, \dots, t}.$$

En résumé, on a obtenu sous (0.2), et pour K/k quadratique :

(1.6) THÉORÈME. On a $|\mathcal{H}_K^{\text{res}}| = 2^{t-1}$ (i.e. $\mathcal{H}_K^{\text{res}}$ est élémentaire) si et seulement si $M(\eta_1, \dots, \eta_\varrho, \pi_1, \dots, \pi_t)$ est de rang $t - 1$ (cf. (1.5)).

(1.7) Remarque. Ce résultat peut être considéré comme la généralisation du critère de Rédei pour les extensions quadratiques de \mathbb{Q} , car dire que $\mathcal{H}_K^{\text{res}}$ est élémentaire revient à dire que le 4-rang de ce groupe est nul; or comme $(\mathcal{H}_K^{\text{res}})^{1+\sigma} = 1$, $1 - \sigma$ opère comme 2 et il en résulte que ce 4-rang est égal à $t - 1 - r$.

Ceci achève l'application de (0.4) pour $\mathcal{H} = (\mathcal{H}_K^{\text{res}})^G$. Nous allons voir dans le §2 ce qu'implique une telle situation au niveau du groupe NE_K .

2. Résultat principal. Nous faisons intervenir maintenant le groupe $\mathcal{H}_K^{\text{ord}}$. Le résultat principal est le suivant :

(2.1) THÉORÈME. Soit $K = k(\sqrt{\delta})$ une extension quadratique d'un corps k totalement réel et 2-principal au sens restreint. Alors les conditions suivantes sont équivalentes (cf. Notations (0.3) et (1.5)) :

- (i) $|\mathcal{H}_K^{\text{ord}}| = 2^{t-1+t_\infty} / (E_k : E_k \cap NK^\times)$ (i.e. $\mathcal{H}_K^{\text{ord}}$ est élémentaire) et $NE_K = E_k \cap NK^\times$;
- (ii) $M(\eta_1, \dots, \eta_\varrho, \pi_1, \dots, \pi_t)$ est de rang $t - 1$ (i.e. $\mathcal{H}_K^{\text{res}}$ est élémentaire).

(2.2) COROLLAIRE. Les conditions suivantes sont équivalentes:

- (i) $|\mathcal{H}_K^{\text{ord}}| = 2^{t-1}$ et $(E_k : NE_K) = 2^{t_\infty}$;
- (ii) $|\mathcal{H}_K^{\text{ord}}| = 2^{t-1}$ et $(E_k : E_k \cap NK^\times) = 2^{t_\infty}$ et $NE_K = E_k \cap NK^\times$;
- (iii) $(E_k : E_k \cap NK^\times) = 2^{t_\infty}$ et $M(\pi_1, \dots, \pi_t)$ est de rang $t - 1$.

Démonstrations. Définissons, dans $s_k(k^\times) = \{\pm 1\}^m$:

$$S_{\mathbb{R}} = \{(\dots, \text{signe}(\sigma_i(a)), \dots; \dots, 1, \dots) : a \in k^\times, \sigma_i(\delta) > 0, i = 1, \dots, \varrho\},$$

$$S_{\mathbb{C}} = \{(\dots, 1, \dots; \dots, \text{signe}(\sigma_{\varrho+j}(a)), \dots) : a \in k^\times, \sigma_{\varrho+j}(\delta) < 0,$$

$$j = 1, \dots, t_\infty\},$$

de telle sorte que $s_k(k^\times) = S_{\mathbb{R}} \oplus S_{\mathbb{C}}$.

On a, sur $s_K(K^\times)$, une norme (notée encore N) telle que

$$N(s_1, s'_1, \dots, s_\varrho, s'_\varrho) = (s_1 s'_1, \dots, s_\varrho s'_\varrho),$$

où $s_i = \text{signe}(\sigma_i(\alpha))$, $s'_i = \text{signe}(\sigma_i \tau(\alpha))$, $\alpha \in K^\times$, pour les 2ϱ plongements

réels $\sigma_i, \sigma_i\tau, i = 1, \dots, \varrho$, de K ; on a le diagramme commutatif suivant :

$$\begin{array}{ccc} K^\times & \xrightarrow{s_K} & s_K(K^\times) \simeq \{\pm 1\}^{2\varrho} \\ N \downarrow & & \downarrow N \\ k^\times & \xrightarrow{s_k} & s_k(k^\times) \simeq \{\pm 1\}^{\varrho+t_\infty} \end{array}$$

On vérifie que $N \circ s_K(K^\times) \simeq S_{\mathbb{R}}$.

(2.3) LEMME. *On a $2^\varrho(NE_K : E_k^2) = |s_K(E_K)|$.*

Soit S_0 le noyau de N dans $s_K(K^\times)$; on a $s_K(E_k) \subseteq S_0$ car pour $\varepsilon_0 \in E_k$, $N \circ s_K(\varepsilon_0) = s_k(N\varepsilon_0) = s_k(\varepsilon_0^2) = 1$. Comme $S_0 = \{(s_1, s_1, \dots, s_\varrho, s_\varrho) : s_i = \pm 1\}$, et comme $s_k(E_k) = s_k(k^\times)$, on en déduit l'égalité $S_0 = s_K(E_k)$. Soit alors S_1 un supplémentaire de S_0 dans $s_K(E_K)$; on a $s_K(E_K) = S_0 \oplus S_1$, d'où, par N qui est injective sur S_1 , $S_1 \simeq NS_1 = N(s_K(E_K)) = s_k \circ N(E_K)$; par conséquent la suite exacte

$$1 \rightarrow E_k^2 \rightarrow NE_K \xrightarrow{s_k} s_k \circ N(E_K) \rightarrow 1$$

conduit à $(NE_K : E_k^2) = |S_1| = |s_K(E_K)|/|S_0|$; d'où le lemme puisque $|S_0| = 2^\varrho$.

Montrons l'implication (i) \Rightarrow (ii) du théorème : L'égalité $NE_K = E_k \cap NK^\times$ implique, via (2.3),

$$|s_K(E_K)| = 2^\varrho(E_k \cap NK^\times : E_k^2) = 2^{\varrho+m}/(E_k : E_k \cap NK^\times),$$

soit (cf. (0.3)(i))

$$|\mathcal{H}_K^{\text{res}}||\mathcal{H}_K^{\text{ord}}|^{-1} = 2^{2\varrho}(E_k : E_k \cap NK^\times)/2^{\varrho+m} = (E_k : E_k \cap NK^\times)/2^{t_\infty};$$

d'après l'expression classique de $|(\mathcal{H}_K^{\text{ord}})^G|$ (cf. [G1, p. 25]), la première condition de (2.1)(i) signifie bien que $\mathcal{H}_K^{\text{ord}}$ est élémentaire, d'où

$$|\mathcal{H}_K^{\text{res}}| = |\mathcal{H}_K^{\text{ord}}|(E_k : E_k \cap NK^\times)/2^{t_\infty} = 2^{t-1};$$

comme $|(\mathcal{H}_K^{\text{res}})^G| = 2^{t-1}$ (cf. (1.1)), $\mathcal{H}_K^{\text{res}}$ est aussi élémentaire, ce qui donne (ii) grâce à (1.6).

Montrons ensuite l'implication (ii) \Rightarrow (i) : Si $\mathcal{H}_K^{\text{res}}$ est élémentaire, $\mathcal{H}_K^{\text{ord}}$, qui en est un quotient, est élémentaire et on a donc $|\mathcal{H}_K^{\text{ord}}| = 2^{t-1+t_\infty}/(E_k : E_k \cap NK^\times)$ (première condition de (i)). On a également $|\mathcal{H}_K^{\text{res}}| = 2^{t-1}$; d'où

$$|\mathcal{H}_K^{\text{res}}||\mathcal{H}_K^{\text{ord}}|^{-1} = (E_k : E_k \cap NK^\times)/2^{t_\infty}.$$

Comme

$$|\mathcal{H}_K^{\text{res}}||\mathcal{H}_K^{\text{ord}}|^{-1} = |s_K(K^\times)|/|s_K(E_K)| = 2^{2\varrho}/|s_K(E_K)| = 2^\varrho/(NE_K : E_k^2)$$

(d'après (2.3)), il vient $(E_k : E_k \cap NK^\times)/2^{t_\infty} = 2^\varrho/(NE_K : E_k^2)$, soit $(E_k : E_k \cap NK^\times)(NE_K : E_k^2) = 2^m$, ce qui implique $E_k \cap NK^\times = NE_K$.

Etablissons enfin (2.2) : Si on a (i), on a

$$|(\mathcal{H}_K^{\text{ord}})^G| = 2^{t-1}2^{t_\infty}/(E_k : E_k \cap NK^\times) \leq 2^{t-1},$$

soit $(E_k : E_k \cap NK^\times) \geq 2^{t_\infty}$; mais $(E_k : E_k \cap NK^\times)$ divise $(E_k : NE_K) = 2^{t_\infty}$, et nécessairement $(E_k : E_k \cap NK^\times) = 2^{t_\infty}$, d'où (ii).

Ensuite, (ii) n'est autre que le point (i) de (2.1) avec la condition supplémentaire $(E_k : E_k \cap NK^\times) = 2^{t_\infty}$, ce qui conduit au point (iii) de (2.2) avec la matrice $M(\eta_1, \dots, \eta_\rho, \pi_1, \dots, \pi_t)$ au lieu de $M(\pi_1, \dots, \pi_t)$; mais on a $E_k \cap NK^\times \subseteq F$ (cf. (1.2)) et

$$(F : E_k \cap NK^\times) = (F : E_k^2)/(E_k \cap NK^\times : E_k^2) = 2^e/2^{m-t_\infty} = 1$$

(cf. (1.3)), d'où $E_k \cap NK^\times = F$, auquel cas $\langle \eta_1, \dots, \eta_\rho, \pi_1, \dots, \pi_t \rangle \sim \langle \pi_1, \dots, \pi_t \rangle$.

Enfin, si le rang de $M(\pi_1, \dots, \pi_t)$ est $t - 1$, celui de $M(\eta_1, \dots, \eta_\rho, \pi_1, \dots, \pi_t)$ est a fortiori $t - 1$, ce qui est le point (ii) de (2.1), d'où (i) de (2.1) qui, compte-tenu de l'égalité $(E_k : E_k \cap NK^\times) = 2^{t_\infty}$, donne (i) de (2.2).

(2.4) COROLLAIRE. Si K est totalement réel et si $E_k \subset NK^\times$, alors les conditions suivantes sont équivalentes :

- (i) $|\mathcal{H}_K^{\text{ord}}| = 2^{t-1}$ et $NE_K = E_k$;
- (ii) $M(\pi_1, \dots, \pi_t)$ est de rang $t - 1$.

En particulier, si K est totalement réel et si $t = 1$, alors $|\mathcal{H}_K^{\text{ord}}| = 1$ et $NE_K = E_k$.

3. Application à la généralisation de (0.1). Le principe est de considérer deux corps quadratiques $K = k(\sqrt{\delta})$ et $K' = k(\sqrt{\delta'})$, $\delta, \delta' \in k^\times - k^{\times 2}$, pour lesquels les conditions du théorème (2.1) (ou du corollaire (2.2)) pour K soient équivalentes aux conditions analogues pour K' , de telle sorte que, lorsqu'elles ont lieu, l'on puisse écrire

$$|\mathcal{H}_K^{\text{ord}}| = 2^{t-1} \text{ et } (E_k : NE_K) = 2^{t_\infty} \\ \Leftrightarrow |\mathcal{H}_{K'}^{\text{ord}}| = 2^{t'-1} \text{ et } (E_k : N'E_{K'}) = 2^{t'_\infty}.$$

Une façon simple de réaliser cette situation est de prendre $K = k(\sqrt{\delta})$, $K' = k(\sqrt{-\delta})$ avec $\delta \in k^{\times+}$ (donc K est totalement réel et K' totalement imaginaire) et de faire les hypothèses suivantes :

- (α) $E_k \subset NK^\times$;
- (β) le nombre premier 2 est non décomposé dans k/\mathbb{Q} .

On remarque alors que $|t' - t| \leq 1$, et si $t' \neq t$, il s'agit de l'idéal premier au-dessus de 2 qui se ramifie dans une seule des deux extensions quadratiques (auquel cas δ peut être supposé "impair").

On remarque enfin que $E_k \cap N'K'^{\times} = E_k^+ = E_k^2 = N'E_{K'}$ puisque $N'K'^{\times} \subset k^{\times+}$. On a alors $t_{\infty} = 0$, $t'_{\infty} = m$, et les conditions (i), (ii) (resp. (i)', (ii)') de (2.1) relatives à K (resp. K') deviennent ici (compté-tenu de (α) , (β) , et avec des notations évidentes):

- (i) $|\mathcal{H}_K^{\text{ord}}| = 2^{t-1}$ et $NE_K = E_k$;
- (ii) $M(\pi_1, \dots, \pi_t) = ([\delta, \pi_i]_{\mathfrak{p}_j})_{i,j=1,\dots,t}$ est de rang $t - 1$;
- (i)' $|\mathcal{H}_{K'}^{\text{ord}}| = 2^{t'-1}$;
- (ii)' $M' = M(\pi'_1, \dots, \pi'_{t'}) = ([-\delta, \pi'_i]_{\mathfrak{p}'_j})_{i,j=1,\dots,t'}$ est de rang $t' - 1$.

(3.1) LEMME. On a $(-\delta, \pi'_i)_{\mathfrak{p}'_j} = (\delta, \pi'_i)_{\mathfrak{p}'_j}$ pour tout $i, j = 1, \dots, t'$, et, de même, $(\delta, \pi_i)_{\mathfrak{p}_j} = (-\delta, \pi_i)_{\mathfrak{p}_j}$ pour tout $i, j = 1, \dots, t$.

Calculons $(-1, \pi'_i)_{\mathfrak{p}'_j}$. Si \mathfrak{p}'_j ne divise pas 2 alors il divise (δ) et est donc égal à un \mathfrak{p}_j ramifié dans K/k ; comme -1 est norme dans K/k , on a $(\delta, -1)_{\mathfrak{p}_j} = 1$; or $(\delta, -1)_{\mathfrak{p}_j} = (-1/\mathfrak{p}_j)$ (symbole de reste quadratique), et on a donc $(-1/\mathfrak{p}_j) = 1$; mais $(-1, \pi'_i)_{\mathfrak{p}_j} = 1$ pour $i \neq j$ et est donné par $(-1/\mathfrak{p}_j)$ sinon, d'où $(-1, \pi'_i)_{\mathfrak{p}'_j} = 1$ dans ce cas. Si \mathfrak{p}'_j divise 2, ce qui en vertu de (β) se produit au plus une fois, la formule du produit $\prod_{\mathfrak{p}'} (-1, \pi'_i)_{\mathfrak{p}'} = 1$, \mathfrak{p}' parcourant l'ensemble des places de k , conduit au résultat car $(-1, \pi'_i)_{\infty} = 1$ pour les places à l'infini de k ($\pi'_i \in k^{\times+}$).

La seconde partie du lemme est analogue.

On a alors essentiellement 2 cas :

- (i) $t' = t$, qui conduit à $M' = M$ d'après (3.1);
- (ii) $t' = t + 1$, qui conduit, en vertu de (3.1), à

$$M' = \left(\begin{array}{ccc|c} & & & [\delta, \pi_1]_{\mathfrak{p}_0} \\ & & & \vdots \\ & M & & [\delta, \pi_t]_{\mathfrak{p}_0} \\ \hline [\delta, \pi_0]_{\mathfrak{p}_1} & \dots & [\delta, \pi_0]_{\mathfrak{p}_t} & [\delta, \pi_0]_{\mathfrak{p}_0} \end{array} \right)$$

(ou *vice versa*, par échange de M et M' et de t et t' , lorsque $t = t' + 1$), où l'on a posé $\mathfrak{p}'_j = \mathfrak{p}_j$, pour $j = 1, \dots, \text{Min}(t, t')$, et où $\pi_0 \in k^{\times+}$ engendre une puissance impaire convenable de l'idéal premier \mathfrak{p}_0 de k au-dessus de 2.

Examinons le cas (ii) sous la forme ci-dessus ($t' = t + 1$); par addition des colonnes de M' à sa dernière colonne, la formule du produit $\prod_{j=0}^t (\delta, \cdot)_{\mathfrak{p}_j} = 1$, appliquée aux π_i , $0 \leq i \leq t$, conduit à la matrice

$$\left(\begin{array}{ccc|c} & & & 0 \\ & & & \vdots \\ & M & & 0 \\ \hline [\delta, \pi_0]_{\mathfrak{p}_1} & \dots & [\delta, \pi_0]_{\mathfrak{p}_t} & 0 \end{array} \right)$$

puis, par addition des t premières colonnes, la formule du produit $\prod_{j=1}^t (\delta, \cdot)_{\mathfrak{p}_j} = 1$, appliquée aux π_i , $1 \leq i \leq t$, conduit à la matrice

$$\left(\begin{array}{ccc|cc} & & & 0 & 0 \\ & & & \vdots & \vdots \\ & & & 0 & 0 \\ \hline & M_1 & & u & 0 \\ \hline [\delta, \pi_0]_{\mathfrak{p}_1} & \dots & [\delta, \pi_0]_{\mathfrak{p}_{t-1}} & & \end{array} \right)$$

où M_1 est à t lignes et $t - 1$ colonnes, et de même rang que M , et où $u = [\delta, \pi_0]_{\mathfrak{p}_0}$ (en effet, comme $\prod_{j=0}^t (\delta, \pi_0)_{\mathfrak{p}_j} = 1$, on a $\sum_{j=1}^t [\delta, \pi_0]_{\mathfrak{p}_j} = [\delta, \pi_0]_{\mathfrak{p}_0} = u$).

Par conséquent, l'équivalence

$$\text{rang}(M) = t - 1 \Leftrightarrow \text{rang}(M') = t' - 1$$

est vraie si et seulement si $u \neq 0$ (i.e. $(\delta, \pi_0)_{\mathfrak{p}_0} = -1$).

D'où l'énoncé généralisant (0.1) :

(3.2) THÉORÈME. Soit k un corps de nombres totalement réel, 2-principal au sens restreint, et dans lequel 2 ne se décompose pas. Soient $K = k(\sqrt{\delta})$, $K' = k(\sqrt{-\delta})$, $\delta \in k^{\times+} - k^{\times 2}$; on suppose que $E_k \subseteq NK^{\times}$. Soit $\pi_0 \in k^{\times+}$ un générateur d'une puissance impaire convenable de l'idéal premier de k au-dessus de 2, soient t, t' les nombres d'idéaux premiers ramifiés dans K, K' , et soient h, h' les 2-nombres de classes au sens ordinaire de K, K' . Alors on a les résultats suivants :

(i) Si $t' = t$, alors on a $h = 2^{t-1}$ et $NE_K = E_k$ si et seulement si $h' = 2^{t-1}$;

(ii) si $t' \neq t$, supposons en outre que $(\delta, \pi_0)_{\mathfrak{p}_0} = -1$; alors on a $h = 2^{t-1}$ et $NE_K = E_k$ si et seulement si $h' = 2^{t'-1}$.

Enonçons des corollaires relatifs au cas $k = \mathbb{Q}$:

(3.3) COROLLAIRE. Soit $\delta = 2p_1 \dots p_{t-1}$, $t \geq 1$, où les p_i sont des nombres premiers impairs distincts congrus à 1 modulo 4; alors $h = 2^{t-1}$ et $N\varepsilon = -1$ si et seulement si $h' = 2^{t-1}$.

(3.4) COROLLAIRE. Soit $\delta = p_1 \dots p_t$, $t \geq 1$, où les p_i sont comme dans (3.3) et tels que $(\delta, 2)_2 = -1$ (i.e. $\delta \equiv 5 \pmod{8}$); alors $h = 2^{t-1}$ et $N\varepsilon = -1$ si et seulement si $h' = 2^t$.

On notera que (3.3) n'est autre que (0.1).

(3.5) Remarques conclusives. (i) Si, dans (3.2)(ii), on a $(\delta, \pi_0)_{\mathfrak{p}_0} = 1$, alors (en supposant $t' = t + 1$ pour fixer les idées) la matrice M' est de rang $\leq t - 1$, auquel cas $\mathcal{H}_{K'}$ n'est jamais élémentaire (autrement dit, on a $h' \equiv 0 \pmod{2^{t+1}}$; mais on peut avoir $h = 2^{t-1}$ et $N\varepsilon = -1$).

(ii) L'application pratique du théorème (2.1) se fait comme suit : ayant vérifié que le rang de la matrice $M(\eta_1, \dots, \eta_\varrho, \pi_1, \dots, \pi_t)$ est $t-1$ (cf. (1.5)), on dispose de la sous-matrice $M(\eta_1, \dots, \eta_\varrho)$ qui permet de trouver NE_K comme étant défini par $E_k \cap NK^\times = F \cap NK^\times = \{\eta = \prod_{i=1}^\varrho \eta^{x_i} : x_i \in \mathbb{F}_2, \sum_{i=1}^\varrho x_i [\delta, \eta_i]_{p_j} = 0, \text{ pour } j = 1, \dots, t\} E_k^2$.

(iii) De nombreuses situations, non abordées ici, peuvent être traitées selon notre résultat général (0.4), sur un plan théorique ou sur un plan numérique (à ce sujet on pourra se référer à [G2, V, C] pour les problèmes de 4-rangs des corps quadratiques, à [G2, VI, A, B] pour l'aspect numérique).

(iv) Soit $d > 0$ sans facteurs carrés et sans diviseurs premiers congrus à 3 modulo 4; les exemples numériques suivants ($k = \mathbb{Q}$) montrent que les seules considérations locales ne suffisent plus à déterminer $N_{K/\mathbb{Q}\varepsilon}$ si l'on n'est plus dans le cadre des corollaires (3.3) et (3.4), autrement dit si l'on est dans l'un des 3 cas suivants:

- (a) d pair et $\mathcal{H}_{K'}^{\text{ord}}$ non élémentaire;
- (b) d impair, $d \equiv 5 \pmod{8}$ et $\mathcal{H}_{K'}^{\text{ord}}$ non élémentaire;
- (c) d impair, $d \equiv 1 \pmod{8}$.

On donne alors successivement d , $\mathcal{H}_{K'}^{\text{ord}}$, $\mathcal{H}_K^{\text{ord}}$, $N_{K/\mathbb{Q}\varepsilon}$:

(a)	$34 = 2 \cdot 17$	C_4	C_2	$+ 1$
	$82 = 2 \cdot 41$	C_4	C_4	$- 1$
(b)	$205 = 5 \cdot 41$	$C_2 \times C_4$	C_2	$+ 1$
	$445 = 5 \cdot 89$	$C_2 \times C_4$	C_4	$- 1$
(c)	$65 = 5 \cdot 13$	$C_2 \times C_4$	C_2	$- 1$
	$305 = 5 \cdot 61$	$C_2 \times C_8$	C_2	$+ 1$.

Nous remercions le Rapporteur de nous avoir indiqué les travaux de P. Morton où sont prouvés des résultats de densité confirmant précisément l'impossibilité de prévoir de façon locale la norme de l'unité fondamentale d'un corps quadratique réel sur \mathbb{Q} lorsque le 2-groupe des classes au sens restreint n'est pas élémentaire (cf. [M]).

Bibliographie

- [C-H] P. Conner and J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. 8, World Sci., Singapore 1988.
- [C-K] A. Costa and R. Kingan, *On the norms of units for real quadratic extensions of number fields*, preprint.
- [F] A. Fröhlich, *The generalization of a theorem of L. Rédei's*, Quart. J. Math. Oxford Ser. (2) 5 (1954), 130–140.
- [G1,2] G. Gras, *Sur les l -classes d'idéaux dans les extensions cycliques relatives de degré premier l* , Ann. Inst. Fourier (Grenoble) 23 (3) (1973), 1–48; 23 (4) (1973), 1–44.

- [H] M. Hikita, *On the congruences for the class numbers of the quadratic fields whose discriminants are divisible by 8*, J. Number Theory 23 (1) (1986), 86–101.
- [Hu] J. Hurrelbrink, *On the norm of the fundamental unit*, preprint.
- [I] E. Inaba, *Über die Struktur der l -Klassengruppe zyklischer Zahlkörper von Primzahlgrad l* , J. Fac. Sci. Univ. Tokyo Sect. I 4 (1940), 61–115.
- [M] P. Morton, *On the non-existence of abelian conditions governing solvability of the -1 Pell equation*, J. Reine Angew. Math. 405 (1990), 147–155.
- [P] R. Pioui, *Mesures de Haar p -adiques et interprétation arithmétique de $(1/2)L_2(\chi, s) - (1/2)L_2(\chi, t)$, $s, t \in \mathbb{Z}_2$ (χ quadratique)*, Thèse, Univ. Besançon, 1990.
- [R1] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. 171 (1934), 55–61.
- [R2] —, *Über die Grundeinheit und die durch acht teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, *ibid.*, 131–148.
- [S] A. Scholtz, *Über die Lösbarkeit der Gleichung $t^2 - Du^2 = -4$* , Math. Z. 39 (1934), 95–111.

FACULTÉ DES SCIENCES
LABORATOIRE DE MATHÉMATIQUES
U.A.741 au C.N.R.S.
F-25030 BESANÇON CEDEX, FRANCE

Reçu le 2.1.1991

(2110)