In closing, the author would like to thank Jacki Pitts for organizing and writing up a good deal of this material as part of a requirement for her M.S. degree at the University of South Carolina. The author further thanks Carl Pomerance for suggesting using reference [14] as in the final part of this paper. In addition, the author is greatly indebted to David Richman for several helpful comments and suggestions including the proof of Lemma 7. Finally, the author is grateful to Emil Grosswald for his constant encouragements through the years knowing well that they will remain with this author in the years to come.

References

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, Orlando 1966.
[2] N. G. de Bruijn, *On the number of positive integers $\leqslant x$ and free of prime factors $> y$*, Nederl. Akad. Wetensch. Proc. Ser. A 54 (= Indag. Math. 13) (1951), 50–60.
[3] N. Chebotarev (N. Tschebotarëw), *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. 95 (1926), 191–228.
[4] P. Erdös, *A theorem of Sylvester and Schur*, J. London Math. Soc. 9 (1934), 282–288.
[5] M. Filaseta, *The irreducibility of almost all Bessel Polynomials*, J. Number Theory 27 (1987), 22–32.
[6] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Sympos. Pure Math. 24, Amer. Math. Soc., Providence, RI, 1973, 91–101.
[7] E. Grosswald, *Bessel Polynomials*, Lecture Notes in Math. 698, Springer-Verlag, Berlin 1978.
[8] –, *On some algebraic properties of the Bessel Polynomials*, Trans. Amer. Math. Soc. 71 (1951), 197–210.
[9] –, *On some algebraic properties of the Bessel Polynomials*, Addendum, ibid. 144 (1969), 569–570.
[10] –, private communication.
[11] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev Density Theorem*, Proceedings of the 1975 Durham Symposium, Academic Press, London and New York 1977, 409–464.
[12] K. K. Norton, *Numbers with small prime factors, and the least k-th power non-residue*, Mem. Amer. Math. Soc. 106 (1971), 1–106.
[13] I. Schur, *Einige Sätze über Primzahlen mit Anwendungen auf Irreduzibilitätsfragen, I*, Sitzungsber. Preuss. Akad. Wiss. (1929), 125–136; also in *Issai Schur Gesammelte Abhandlungen*, Bd. III, edited by A. Brauer and H. Rohrbach, Springer-Verlag, New York 1973.
[14] A. Selberg, *On the normal density of primes in small intervals, and the difference between consecutive primes*, Arch. Math. Naturvid., no. 6, 47 (1943), 87–105.
[15] H. M. Stark, *Some effective cases of the Brauer–Siegel theorem*, Invent. Math. 23 (1974), 135–152.
[16] J. Sylvester, *On arithmetical series*, Messenger of Math. 21 (1892), 1–19, 87–120.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SOUTH CAROLINA
Columbia, S.C. 29208
U.S.A.

Received on 6.10.1989
and in revised form on 18.4.1990 (1976)

ACTA ARITHMETICA
LVIII.3 (1991)

Norme relative de l'unité fondamentale et 2-rang du groupe des classes d'idéaux de certains corps biquadratiques

par

STÉPHANE LOUBOUTIN (Caen)

Notations. k désigne un corps quadratique imaginaire de nombre de classes d'idéaux $h(k)$ impair, de discriminant $D_{k/Q}$ donc égal à -4, -8 ou égal à p, $p \equiv 1 \pmod 4$ premier, d'anneau des entiers R_k, de groupe des classes d'idéaux $H(k)$ et de groupe (fini) des unités (i.e. de ses racines de l'unité) U_k.

K est une extension quadratique de k, R_K son anneau des entiers, $h(K)$ son nombre de classes d'idéaux et $H(K)$ son groupe des classes d'idéaux (remarquons que K étant totalement complexe, les notions de classe stricte et large coïncident). Nous notons $j_{K/k}$ l'homomorphisme canonique de $H(k)$ dans $H(K)$. Le nombre de classes de k étant supposé impair, cet homomorphisme est ici injectif (car $N_{K/k} \circ j_{K/k}$ n'est autre que l'élévation au carré). Nous notons $D_{K/Q}$ le discriminant absolu de K/Q, $\delta_{K/k}$ l'idéal de R_k égal au discriminant relatif de l'extension K/k et $D_{k/Q}$ le discriminant absolu de k/Q. Nous avons donc $D_{K/Q} = N_{k/Q}(\delta_{K/k})(D_{k/Q})^2$. K étant totalement complexe et de degré quatre, son groupe des unités U_K est de rang 1 et nous notons η_K une unité fondamentale. La norme relative $N_{K/k}(\eta_K)$ de η_K étant une unité de k, elle est une racine de l'unité de k et est égale à ± 1 pour $k \neq Q(i), Q(j)$, elle est égale à $\pm 1, \pm i$ pour $k = Q(i)$, et est finalement égale à $\pm 1, \pm j, \pm j^2$, pour $k = Q(j)$. Il est aisé de voir que pour $k = Q(i)$ on peut se ramener après multiplication éventuelle par i au cas où $N_{K/k}(\eta_K) = +1$ ou i, et que pour $k = Q(j)$ on peut se ramener après multiplication éventuelle par j ou j^2 au cas où $N_{K/k}(\eta_K) = +1$ ou -1. Finalement, nous posons $\varepsilon_k = -1$ lorsque $k \neq Q(i)$, et $\varepsilon_k = i$ lorsque $k = Q(i)$, de sorte que U_k est inclus dans $N_{K/k}(U_K)$ si et seulement si ε_k appartient à $N_{K/k}(U_K)$.

Introduction. Nous déterminons premièrement le 2-rang du groupe des classes d'idéaux de K. L'imparité du nombre de classes de certains de ces corps biquadratiques nous permet de secondement donner au corollaire 6 une preuve rapide, dans notre cas particulier, de la loi de réciprocité établie, par E. Hecke, et au corollaire 11 une preuve de la loi de réciprocité établie par P. G. L. Dirichlet. Nous développons finalement aux propositions 13 et 14 des moyens de calcul de la norme relative de l'unité fondamentale de K. Nous nous astreignons, délibérément, à n'utiliser que les fondements de la théorie

algébrique des nombres: idéaux, groupe des classes,..., sans recourir à des outils plus élaborés (symboles de normes résiduelles, symboles locaux,...), les réservant à un seul paragraphe. Expliquons succintement les restrictions que nous nous imposons quant au cadre de cet article, et leur lien avec son plan. Dans [11] nous développons une technique analytique d'évaluation des nombres de classes des extensions quadratiques K/k d'un corps quadratique imaginaire principal k. Pour ce faire, il nous faut construire le caractère de cette extension K/k. Semblablement au cas des corps quadratiques réels, sa construction repose sur les lois de réciprocité (pour les symboles $[-]$ que nous introduisons au corollaire 6). Dans le souci de rassembler en ces deux articles une approche autonome de l'arithmétique de ces extensions quadratiques, nous nous efforçons ici d'intriquer dans le cadre particulier des extensions quadratiques d'un corps quadratique imaginaire principal les résultats de C. Chevalley sur l'ordre du groupe des classes ambiges et ceux de E. Hecke sur les lois de réciprocité quadratiques pour les faire tous deux découler d'une approche unitaire. La restriction k principal étant essentielle pour notre approche analytique, nous en eussions ici également fait l'assomption si celle plus générale de la seule imparité du nombre de classes de ce corps quadratique imaginaire n'eût pas été plus éclairante pour notre propos.

Une seconde raison pour nous restreindre au cas d'un corps biquadratique K totalement complexe contenant un sous corps quadratique (ici de plus supposé quadratique imaginaire) est que nous désirons que le rang des unités de K vale 1 (afin d'obtenir des résultats précis et explicites) et que la norme de l'unité fondamentale de K ne soit pas toujours égale à $+1$, ce qui nous contraint à parler de la norme relative de cette unité (la norme absolue d'une unité d'un corps totalement complexe étant égale à $+1$), i.e. à disposer d'un sous corps quadratique dans K. Notre proposition 14 est, ce nous semble, la première généralisation du fait que l'algorithme des fractions continues donne dans le cas des corps quadratiques réels le signe de la norme de l'unité fondamentale.

Rappelons préalablement les résultats bien connus sur le 2-rang du groupe des classes dans le cas des extensions quadratiques k/Q du corps des rationnels Q de discriminant $D_{k/Q}$ ayant t facteurs premiers distincts.

(a) Pour $D_{k/Q} < 0$ les 2-rangs des groupes des classes aux sens strict et large valent $t-1$.

(b) Pour $D_{k/Q} > 0$ le 2-rang du groupe des classes au sens large vaut $t-1$ si les diviseurs premiers impairs de $D_{k/Q}$ sont congrus à 1 modulo 4; sinon, il vaut $t-2$.

Dans ces deux cas, le 2-rang du groupe des classes au sens strict vaut $t-1$.

Le sous-groupe des classes régulières. Nous notons t le nombre d'idéaux premiers de k ramifiés dans K/k et appelons *invariant* un idéal entier I de K tel que $I^\sigma = I$, où σ est le k-isomorphisme non trivial de K/k. Un tel idéal est de la forme $I = j_{K/k}(N)P_{i_1}\dots P_{i_r}$ où N est un idéal entier de k, où $0 \leqslant r \leqslant t$ et où

$P_{i_1},\dots,P_{i_r}$ sont r des t idéaux premiers ramifiés dans K/k. Une classe d'idéaux C de K est dite *ambige* si elle reste invariante sous l'action de σ, elle de plus dite *régulière* si elle contient un idéal invariant. Nous notons $H_{\mathrm{reg}}(K)$ et $H_{\mathrm{amb}}(K)$ ces sous-groupes respectifs des classes régulières et des classes ambiges. Lorsque k est principal, il y a équivalence entre être une classe ambige et être une classe d'ordre 2.

THÉORÈME 1. *Le sous-groupe des classes régulières est d'ordre* $h(k)2^{t-2}$ *pour* $N_{K/k}(\eta_K) = +1$, *et d'ordre* $h(k)2^{t-1}$ *sinon.*

Preuve. Soient $U_K^{(1)}$ le groupe des unités de K de norme $+1$, G le groupe dont les éléments sont les parties de l'ensemble à t éléments formé par les idéaux premiers ramifiés muni de la loi de la différence symétrique, ϕ et ψ les morphismes définis de la façon suivante:

ψ: $G \to H_{\mathrm{reg}}(K)/j_{K/k}(H(k))$ défini par $\psi(\{P_{i_1},\dots,P_{i_r}\}) \overset{\mathrm{def}}{=}$ classe de $P_{i_1}\dots P_{i_r}$;

ϕ: $U_K^{(1)} \to G$ défini par $\phi(\varepsilon) \overset{\mathrm{def}}{=} \{P;\ P$ idéal premier ramifié tel que $v_P(x)$ est impaire$\}$, où $x \in R_K$ est quelconque tel que $\varepsilon = \sigma(x)/x$.

ϕ est bien défini, premièrement parce que si ε appartient à $U_K^{(1)}$ il existe au moins un x tel que $\varepsilon = \sigma(x)/x$ (à savoir $x = 1+\sigma(\varepsilon)$), secondement parce que $\phi(\varepsilon)$ ne dépend pas du x choisi. En effet, si $\varepsilon = \sigma(x)/x = \sigma(y)/y$, alors $z = x\sigma(y)$ est un entier de R_K invariant par σ, donc un entier de R_k. Si P est un idéal premier ramifié dans K/k, $v_P(z)$ est donc paire et $v_P(x) \equiv v_P(y) \pmod 2$.

De l'immédiate surjectivité de ψ, nous déduisons l'exactitude de la suite:

$$U_K^{(1)} \xrightarrow{\phi} G \xrightarrow{\psi} H_{\mathrm{reg}}(K)/j_{K/k}(H(k)) \to 1.$$

D'où:

$$|H_{\mathrm{reg}}(K)|/h(k) = \frac{|G|}{|\mathrm{Ker}(\psi)|} = \frac{2^t}{|\mathrm{Im}(\phi)|} = \frac{2^t}{(U_K^{(1)}:\ \mathrm{Ker}(\phi))}.$$

Reste à déterminer ce dernier indice.

Si ε est dans le noyau de ϕ, alors $\varepsilon = \sigma(x)/x$ pour un entier x de K tel que l'idéal $I = (x)$ soit invariant par σ et tel que P premier ramifié divise I implique $v_P(x)$ paire, donc tel que $(x) = j_{K/k}(N)$, avec N un idéal entier de k. Mais alors $(x^{h(k)}) = (\alpha)$, soit $x^{h(k)} = \eta\alpha$ pour α un entier de k et η une unité de K. Puisque $\varepsilon^2 = \sigma(x)/x$ pour $x = \sigma(\varepsilon)$ lorsque $\varepsilon \in U_K^{(1)}$, il en résulte que $\mathrm{Ker}(\phi) = \{\sigma(\eta)/\eta,\ \eta \in U_K\}$. Le calcul de l'indice s'en déduit par une étude exhaustive des cas possibles, i.e. en considérant séparément les trois cas: $k = Q(i)$, $k = Q(j)$ et $k \neq Q(i), Q(j)$.

Le sous-groupe des classes ambiges.

LEMME a. K/k *une extension quadratique et* $j_{K/k}$ *le morphisme canonique du groupe des classes de* k *dans celui de* K. *Soit* I *un idéal entier de* K *tel que* $N_{K/k}(I) = M^2$ *pour un idéal entier* M *de* k. *Alors, il existe un idéal entier* N *de* k *divisant* M *et un idéal entier* J *de* K *tels que* $I = j_{K/k}(N)J^2$.

Preuve. Par multiplicativité il suffit de voir le résultat lorsque M est une puissance d'un idéal premier de k. En distinguant les trois cas correspondant à un idéal premier inerte, ramifié ou totalement décomposé dans l'extension quadratique K/k, on construit explicitement les idéaux répondant à la question.

LEMME b. *Soit K/k une extension quadratique d'un corps quadratique imaginaire telle que $N_{K/k}(\eta_K) = +1$. Si ε_k appartient à $N_{K/k}(K^*)$ et si $(Z, m) \in R_K \times R_k$ est tel que $N_{K/k}(Z) = \varepsilon_k m^2$, alors il existe un idéal entier N de k divisant (m) et un idéal entier J de K tels que $(Z) = j_{K/k}(N)J^2$ et $N_{K/k}(J) = (m)/N$. La classe de l'idéal J est alors ambige mais n'est pas régulière.*

Preuve. La première assertion découle du lemme précédent. Pour la seconde, on remarque que

$$(Z)J^\sigma = j_{K/k}(N)JJJ^\sigma = j_{K/k}(N)j_{K/k}(N_{K/k}(J))J$$

$$= j_{K/k}(N)j_{K/k}\left(\frac{(m)}{N}\right)J = (m)J.$$

La classe de J est donc ambige.

Supposons qu'elle soit régulière et contienne donc un idéal invariant A. Il existe alors x et y entiers de K tels que $(x)J = (y)A$. Si $z = x\sigma(y)$, alors $(z)J$ est invariant et nous avons $(\sigma(z))JJ^\sigma = (z)J^2$, soit

$$(\sigma(z))j_{K/k}(N_{K/k}(J)) = \frac{(zZ)}{j_{K/k}(N)},$$

soit

$$(\sigma(z))\frac{(m)}{j_{K/k}(N)} = \frac{(zZ)}{j_{K/k}(N)},$$

soit finalement $(m\sigma(z)) = (zZ)$. Il existe donc une unité η de K telle que $m\sigma(z) = \eta zZ$. En prenant les normes relatives dans cette égalité, nous obtenons $N_{K/k}(\eta) = \varepsilon_k$, ce qui contredit $N_{K/k}(\eta_K) = +1$.

THÉORÈME 2. *K/k une extension quadratique (d'un corps quadratique imaginaire k de nombre de classes impair) d'unité fondamentale η_K de norme relative $+1$ ou -1, ou de norme relative $+1$ ou i pour le cas de $k = Q(i)$. Alors,*

(a) *Si $N_{K/k}(\eta_K) \neq +1$, alors toute classe ambige est régulière et*

$$|H_{amb}(K)| = |H_{reg}(K)| = h(k)2^{t-1}.$$

(b) *Si $N_{K/k}(\eta_K) = +1$ et $\varepsilon_k \notin N_{K/k}(K^*)$, alors toute classe ambige est régulière et*

$$|H_{amb}(K)| = |H_{reg}(K)| = h(k)2^{t-2}.$$

(c) *Si $N_{K/k}(\eta_K) = +1$ et $\varepsilon_k \in N_{K/k}(K^*)$, alors $H_{reg}(K)$ est d'indice 2 dans $H_{amb}(K)$ et donc*

$$|H_{amb}(K)| = h(k)2^{t-1}.$$

Preuve. (a), (b) Soit C une classe ambige et I un idéal de C. Il existe donc x et y entiers de K tel que $(x)I = (y)I^\sigma$. Nous avons donc $N_{K/k}(x) = \varepsilon N_{K/k}(y)$ où ε est une unité de K. Si cette unité peut être choisie égale à $+1$ (changer y en $y\eta$ avec $\eta \in U_K$ changeant ε en $\varepsilon N_{K/k}(\eta)$, ceci est possible dans le cas (a), et l'est également dans le cas(b)), alors x/y est de la forme $z/\sigma(z)$ pour un entier z de K ($z = yy^\sigma + xy^\sigma$ convient). Mais alors l'idéal $(z)I$ est invariant sous l'action de σ et la classe C contient donc bien un idéal invariant. Le théorème 1 donne alors le résultat.

(c) Soient C_1 et C_2 deux classes ambiges non régulières et I et J deux idéaux entiers de ces classes. Semblablement à ce qui précède, il existe w, x, y et z entiers de K tels que $(w)I = (x)I^\sigma$, $(y)J = (z)J^\sigma$ avec $N_{K/k}(w) = \varepsilon_k N_{K/k}(x)$ et $N_{K/k}(y) = \varepsilon_k N_{K/k}(z)$. Mais alors $(wy)IJ = (xz)(IJ)^\sigma$ et $N_{K/k}(wy) = \varepsilon' N_{K/k}(xz)$ avec $\varepsilon' = +1$ pour $k \neq Q(i)$ et $\varepsilon' = -1$ pour $k = Q(i)$. Semblablement au (a), (b), la classe de IJ contient un idéal invariant.

Si il existe une classe ambige non régulière C_0 et si $C_1, \ldots, C_r$ sont les classes régulières, alors $C_0C_1, \ldots, C_0C_r$ sont des classes ambiges non régulières, et si une classe ambige C ne contient pas d'idéal invariant, c'est une de celles-ci. En effet, CC_0^{-1} étant régulière est une des classes C_i, et $C = C_0C_i$.

H_{reg} est donc d'indice 1 ou 2 dans H_{amb}. D'après le lemme b, il est d'indice 2.

2-rang du groupe des classes et norme relative de l'unité fondamentale.

THÉORÈME 3. *Soit K/k une extension quadratique (d'un corps quadratique imaginaire k de nombre de classes impair). Le 2-rang du groupe des classes de K vaut $t-1-\varepsilon$, où t est le nombre d'idéaux premiers ramifiés dans K/k et où $\varepsilon = 0$ ou 1 suivant que U_k est ou n'est pas inclus dans $N_{K/k}(K^*)$.*

Preuve. $H_{amb}(K)/j_{K/k}(H(k))$ est un groupe d'ordre $2^{t-1-\varepsilon}$. Soit $H_2(K)$ le groupe des classes d'ordre 2 dans K et 2^r son cardinal, de sorte que r est le 2-rang du groupe des classes. Si une classe C est d'ordre 2, alors $Cj_{K/k}(N_{K/k}(C)) = CCC^\sigma = C^\sigma$ et $C^{h(k)}$ est donc ambige. Réciproquement, si C est ambige, alors $C^2 = CC^\sigma = j_{K/k}(N_{K/k}(C))$ et $C^{h(k)}$ est d'ordre 2. Puisque l'élévation à la puissance $h(k)$ trivialise les éléments de $j_{K/k}(H(k))$, nous pouvons donc définir deux morphismes de groupes:

$$f: H_2(K) \to H_{amb}(K)/j_{K/k}(H(k))$$

et

$$g: H_{amb}(K)/j_{K/k}(H(k)) \to H_2(K)$$

par $f(C) = C^{h(k)}$, et $g(C) = C^{h(k)}$. Puisque $f \circ g$ et $g \circ f$ sont injectives (car $h(k)^2$ est impair et donc premier à 2), f et g le sont également et ces deux groupes sont donc de même ordre. D'où le résultat.

COROLLAIRE 4. *Soit K/k une extension quadratique de discriminant relatif $\delta_{K/k}$ un idéal premier dans l'anneau des entiers d'un corps quadratique imaginaire k de nombre de classes impair, alors la norme relative de l'unité fondamentale de K n'est pas égale à $+1$ et le nombre de classes de K est impair.*

Preuve. D'après le théorème 1, $N_{K/k}(\eta_K) \neq +1$; d'après le théorème 3 le 2-rang du groupe des classes est alors nul.

Cas d'un corps quadratique imaginaire principal. Dans tout ce paragraphe nous supposons k principal et levons par des moyens élémentaires l'indétermination du théorème 3. Notons que $\delta_{K/k}$ n'est déterminé qu'aux carrés des racines de l'unité de k près.

DÉFINITION. Un entier de k est dit *impair* lorsque sa norme absolue sur Q est un entier impair; un entier de k est dit *primaire* si il est congru à un carré modulo l'idéal principal $(4) = 4R_k$. Lorsque $k = Q(i)$, nous appelons *faiblement primaire* un entier de k congru à un carré modulo l'idéal (2).

PROPOSITION 5. *Soit K/k une extension quadratique d'un corps quadratique imaginaire principal k de discriminant relatif $\delta_{K/k}$. Alors, $\delta_{K/k}$ est primaire et l'anneau des entiers de K est le R_k-module libre de R_k-base $\{1, (P_0+\sqrt{\delta_{K/k}})/2\}$, dès que P_0 dans R_k est tel que 4 divise $P_0^2-\delta_{K/k}$. Si $K = k(\sqrt{d})$ avec d libre de carrés dans R_k, alors d divise $\delta_{K/k}$ et $\delta_{K/k}$ divise $4d$. En particulier, $\delta_{K/k}$ n'est jamais divisible par le carré d'un élément premier de R_k au dessus de p premier impair. Si d est primaire, alors $\delta_{K/k} = d$ pour $k \neq Q(i)$ et $\delta_{K/k} = \pm d$ pour $k = Q(i)$ où le signe n'est pas déterminé.*

Lorsque $k = Q(i)$ et d est faiblement primaire mais n'est pas primaire, alors $\delta_{K/k} = \pm 2id$ où le signe n'est pas déterminé.

Preuve. R_k étant principal, R_K admet une R_k-base $\{\alpha, \beta\}$. Puisque $1 \in R_K$, R_K admet même une R_k-base $\{1, \gamma\}$. Mais alors,

$$\delta_{K/k} = \begin{vmatrix} 1 & \gamma \\ 1 & \gamma^\sigma \end{vmatrix}^2 = (\gamma^\sigma - \gamma)^2$$

est dans R_k et $\delta_{K/k} = b^2 d/c^2$, si $\gamma = (a+b\sqrt{d})/2c$. Puisque d est libre de carrés dans R_k, c divise b; puisque $\gamma \in R_K$, $N_{K/k}(\gamma) = (a^2-db^2)/4c^2 \in R_k$ et donc c divise également a. Nous pouvons donc écrire $\gamma = (P_0+b\sqrt{d})/2$ avec $b^2 d = \delta_{K/k}$, et donc d divise $\delta_{K/k}$ et $\gamma = (P_0+\sqrt{\delta_{K/k}})/2$. Puisque $N_{K/k}(\gamma) \in R_k$, 4 divise bien $P_0^2-\delta_{K/k}$. Finalement, $\sqrt{d}$ appartenant à R_K, on peut écrire $\sqrt{d} = a + b(P_0+\sqrt{\delta_{K/k}})/2$ avec a et b dans R_k. On en déduit que $4d = b^2\delta_{K/k}$ et que $\delta_{K/k}$ divise bien $4d$.

Si d est primaire et congru à P^2 modulo (4), alors $(P+\sqrt{d})/2$ est un élément de K de trace et norme relatives sur k appartenant à R_k. Il est donc entier sur R_k et donc dans R_K. On en déduit, comme précédemment, qu'il existe b dans R_k tel que $d = b^2\delta_{K/k}$. Puisqu'on sait déjà que d divise $\delta_{K/k}$, il en résulte que b est une unité, et donc que $b^2 = 1$ pour $k \neq Q(i)$, et que $b^2 = \pm 1$ pour $k = Q(i)$.

Si $k = Q(i)$ et d est faiblement primaire mais n'est pas primaire et si d est congru à P^2 modulo (2), alors $(P+\sqrt{d})/(1+i)$ appartient à R_K et il existe donc b dans R_k tel que $-2id = b^2\delta_{K/k}$. Puisqu'on sait déjà que d divise $\delta_{K/k}$, on a $b^2 = \pm 1$ ou $b^2 = \pm 2i$, soit $\delta_{K/k} = \pm 2id$ ou $\delta_{K/k} = \pm d$. Mais $\delta_{K/k} = \pm 2id$ étant primaire cette dernière occurrence ne saurait avoir lieu et nous avons le résultat.

COROLLAIRE 6. Loi de réciprocité: *Soit k un corps quadratique imaginaire principal et π_1 et π_2 deux irréductibles impairs distincts de l'anneau des entiers R_k de k dont l'un d'entre eux au moins est primaire; alors,*

$$\left[\frac{\pi_1}{(\pi_2)}\right] = \left[\frac{\pi_2}{(\pi_1)}\right],$$

où pour P idéal premier de k et $z \notin P$ le symbole $\left[\frac{z}{P}\right]$ est défini comme valant $+1$ ou -1 suivant que la congruence $X^2 \equiv z \pmod{P}$ admet ou n'admet pas de solution dans R_k.

Preuve. Elle découle des corollaire 4 et proposition 5 et suit celle de la preuve de la loi de réciprocité quadratique pour les symboles de Legendre telle que la donne H. Cohn [4], Ch. XI, pp. 190–193; l'important étant d'être assuré de l'imparité du nombre de classes des extensions quadratiques K/k qui apparaissent au cours de cette preuve, et de ce que la norme relative de l'unité fondamentale n'étant pas égale à $+1$, les normes relatives des éléments de K peuvent être ajustées par multiplication par ± 1 pour $k \neq Q(i)$, et par multiplication par ± 1, $\pm i$ pour $k = Q(i)$. Voir notre preuve du corollaire 11 pour l'esprit de cette démonstration. Nous retrouvons ainsi, dans un cas particulier, le résultat de E. Hecke, Th. 165 de [10].

COROLLAIRE 7. *Soient π_1 et π_2 deux irréductibles primaires impairs distincts tels que $\left[\frac{\pi_1}{\pi_2}\right] = -1$; alors la norme relative de l'unité fondamentale du corps biquadratique $K = k(\sqrt{\pi_1\pi_2})$ n'est pas égale à $+1$ et le nombre de classes de K est pair (plus précisément, le groupe des classes est de 2-rang valant 1).*

Preuve. Supposons la de norme $+1$. Puisque $\pi_1\pi_2$ est primaire, nous avons $\delta_{K/k} = \pi_1\pi_2$, $t = 2$ et l'idéal premier ramifié de K au dessus de (π_1) est principal (théorème 1). L'équation $X^2 - \pi_1\pi_2 Y^2 = \pm 4\pi_1$ est donc résoluble dans R_k, ainsi donc que $\pi_1 X^2 - \pi_2 Y^2 = \pm 4$. En passant modulo (π_2) nous en

déduisons $\left[\frac{\pm\pi_1}{\pi_2}\right] = +1$, puis $\left[\frac{\pi_1}{\pi_2}\right] = +1$ en remarquant que $\left[\frac{-1}{\pi_2}\right] = +1$ (et ce parce que $\left[\frac{-1}{\pi_2}\right] = (-1)^{(N_{k/Q}(\pi_2)-1)/2} = (-1)^{(|\pi_2|^2-1)/2}$ et que si $\pi_2 \equiv \alpha^2 \pmod 4$, alors $|\pi_2|^2 \equiv (|\alpha|^2)^2 \pmod 4 \equiv 1 \pmod 4$ puisque $|\alpha|^2 = N_{k/Q}(\alpha)$ est un entier de N).

THÉORÈME 8. *Supposons que $N_{K/k}(\eta_K) = +1$. Alors, le 2-rang du groupe des classes au sens large vaut $t-2$ dès que $D = |\delta_{K/k}|^2$ admet un diviseur premier p non inerte dans k/Q tel que $p \equiv 3 \pmod 4$ pour $k \neq Q(i)$, et tel que $p \equiv 5 \pmod 8$ pour $k = Q(i)$; il vaut $t-1$ sinon.*

Preuve. Supposons que le 2-rang vale $t-1$. D'après le théorème 3, il existe x et y dans R_K tels que $N_{K/k}(x) = \varepsilon_k N_{K/k}(y)$. Nous avons alors $N_{K/k}(xy) = \varepsilon_k m^2$ avec $m = N_{K/k}(y) \in R_k$. Les entiers de K s'écrivant sous la forme $(X + Y\sqrt{\delta_{K/k}})/2$ avec $X, Y \in R_k$, l'équation $X^2 - \delta_{K/k} Y^2 = 4\varepsilon_k m^2$ est résoluble dans R_k.

Soit π un diviseur premier de $\delta_{K/k}$ dans le corps principal k, π au dessus de p premier impair. Si il divise m, il divise X, puis, son carré ne divisant pas $\delta_{K/k}$, il divise Y. Nous pouvons donc supposer, après d'éventuelles simplifications, qu'il ne divise pas m qui est alors inversible dans le corps fini $R_k/(\pi)$ à $N_{k/Q}(\pi) = |\pi|^2$ éléments. La congruence $X^2 \equiv \varepsilon_k \pmod \pi$ est donc résoluble, et nous avons

$$\varepsilon_k^{(|\pi|^2-1)/2} \equiv (X^2)^{(|\pi|^2-1)/2} = X^{|\pi|^2-1} \equiv 1 \pmod \pi,$$

ou encore $\varepsilon_k^{(|\pi|^2-1)/2} = 1$.

Pour $\varepsilon_k = -1$, nous devons donc avoir $|\pi|^2 \equiv 1 \pmod 4$. Si $|\pi|^2 = p$ nous imposons bien $p \equiv 1 \pmod 4$; si $|\pi|^2 = p^2$, cette congruence est automatiquement satisfaite. Pour $\varepsilon_k = i$, nous devons donc avoir $|\pi|^2 \equiv 1 \pmod 8$. Si $|\pi|^2 = p$ nous imposons bien $p \equiv 1 \pmod 8$; si $|\pi|^2 = p^2$, cette congruence est automatiquement satisfaite.

Réciproquement, pour $k \neq Q(i)$ et $|\pi|^2 \equiv 1 \pmod 4$, il existe un élément d'ordre 4 dans le groupe multiplicatif cyclique $(R_k/(\pi))^*$ à $|\pi|^2 - 1$ éléments, donc -1 est un carré dans ce corps et $X^2 \equiv \varepsilon_k \pmod \pi$ est résoluble. De même, pour $k = Q(i)$, on prouve que $X^2 \equiv \varepsilon_k \pmod \pi$ est résoluble. Mais dire que ces congruences admettent des solutions, c'est dire que $R_L/\pi R_L$ n'est pas un corps, donc dire que πR_k n'est pas inerte dans L, où nous notons L le corps biquadratique $L = k(\sqrt{\varepsilon_k})$. Remarquons que $L = Q(\zeta_8)$ lorsque $k = Q(i)$, $Q(\sqrt{-2})$. Puisque L est principal (voir H. Cohn [4], théorème 19.8, page 253), il existe z_π entier de L tel que $\pi = N_{L/k}(z_\pi)$. De même, pour π premier de R_k au dessus de 2 divisant $\delta_{K/k}$, montrons qu'il existe z_π entier de L tel que $\pi = N_{L/k}(z_\pi)$. Si $k = Q(i)$ ou $k = Q(\sqrt{-2})$, alors $L = Q(\zeta_8)$ avec $\zeta_8 = (1+i)/\sqrt{2}$.

Puisque $\sqrt{-2} = N_{L/Q(\sqrt{-2})}(1+\zeta_8)$ et $1+i = N_{L/Q(i)}(1-\zeta_8)$, nous avons le résultat dans ces deux cas. Pour $k \neq Q(i), Q(\sqrt{-2})$, 2 étant inerte dans k/Q, donc premier dans k, et 2 étant ramifié dans $Q(i)/Q$, l'idéal $2R_k$ est ramifié dans L/k. L étant principal, il existe bien un z_π dans R_L tel que $2 = N_{L/k}(z_\pi)$ (à priori, nous avons seulement $2\varepsilon = N_{L/k}(z_\pi)$ pour ε une unité de k. Mais i appartenant à L, nous pouvons ajuster z_π de telle sorte que $\varepsilon = 1$). Finalement, $\delta_{K/k} = N_{L/k}(Z)$ pour un entier Z de R_L, ou encore, $4\delta_{K/k} = X^2 - \varepsilon_k Y^2$, soit $X^2 - 4\delta_{K/k} = \varepsilon_k Y^2$ pour un certain (X, Y) dans R_k. (Si $Z = (X + Y\sqrt{\varepsilon_k})/2 \in R_L$, alors sa trace relative X et sa norme relative $(X^2 - \varepsilon_k Y^2)/4$ sur L/k sont dans R_k, donc également X et Y.)

Mais alors, ε_k appartient à $N_{K/k}(K^*)$ et le 2-rang vaut donc bien $t-1$.

THÉORÈME 9. *Le 2-rang du groupe des classes d'un corps K, extension quadratique K/k d'un corps quadratique imaginaire principal k, de discriminant relatif $\delta_{K/k}$ ayant t facteurs premiers distincts dans k vaut $t-1$ si les diviseurs premiers impairs de $D = |\delta_{K/k}|^2$ qui ne sont pas inertes dans k/Q sont congrus à 1 modulo 8 pour $k = Q(i)$, et congrus à 1 modulo 4 pour $k \neq Q(i)$; sinon, il vaut $t-2$.*

Preuve. Si $N_{K/k}(\eta_K) = \varepsilon_k$, alors $x^2 - \delta_{K/k} y^2 = 4\varepsilon_k$ est résoluble dans R_k. Si π est premier au dessus de p non inerte dans k/Q et divise $\delta_{K/k}$, alors ε_k est donc un carré dans le groupe fini à $p-1$ éléments $(R_k/(\pi))^*$, donc ce groupe admet un élément d'ordre 4 pour $k \neq Q(i)$, et 4 divise $p-1$ (respectivement 8 divise $p-1$ pour $k = Q(i)$). ∎

COROLLAIRE 10. *Nous explicitons le résultat précédent dans les trois cas suivants: $k = Q(\sqrt{-1}) = Q(i)$, $k = Q(\sqrt{-2})$ et $k = Q(\sqrt{-3}) = Q(j)$:*

(a) *Pour $K/Q(i)$ une extension quadratique, le groupe des classes de K est de 2-rang $t-1$ si $D_{K/Q}$ n'a pas de diviseur premier p tel que $p \equiv 5 \pmod 8$; sinon, il est de 2-rang $t-2$.*

(b) *Pour $K/Q(\sqrt{-2})$ une extension quadratique, le groupe des classes de K est de 2-rang $t-1$ si $D_{K/Q}$ n'a pas de diviseur premier p tel que $p \equiv 3 \pmod 8$; sinon, il est de 2-rang $t-2$.*

(c) *Pour $K/Q(j)$ une extension quadratique, le groupe des classes de K est de 2-rang $t-1$ si $D_{K/Q}$ n'a pas de diviseur premier p tel que $p \equiv 7 \pmod{12}$; sinon, il est de 2-rang $t-2$.*

Un exemple numérique. Nous montrons sur un exemple numérique que, dans le cas $k = Q(i)$, les résultats de ce corollaire sont bien en accord avec ceux qu'implique la connaissance des nombre de classes. Nous considérons les extensions quadratiques de $Q(i)$ de discriminants relatifs $\delta_{K/Q(i)}$ tels que $\delta_{K/Q(i)} \equiv \pm 1 \pmod{(4)}$, tels que $D = |\delta_{K/Q(i)}|^2 \leqslant 10000$ et tels que $\delta_{K/Q(i)}$ soit de la forme $\delta_{K/Q(i)} = m^2 + 4\varepsilon$ avec $\varepsilon = \pm 1$ et $m = a + ib$. Pour ces corps, nous avons $\eta_K = (m - \sqrt{\delta_{K/Q(i)}})/2$, et l'unité fondamentale est donc de norme relative

± 1 et on espère que t n'est pas trop faible, et ce parce que nous avons déjà la factorisation $\delta_{K/Q(i)} = (m-2i)(m+2i)$ pour $\varepsilon = +1$, et la factorisation $\delta_{K/Q(i)} = (m-2)(m+2)$ pour $\varepsilon = -1$. Les nombres de classes ont été calculés à l'aide de la méthode exposée dans S. Louboutin [11].

a	b	ε	D	2-rang	h
2	1	-1	17	0	1
2	1	$+1$	$65 = 5\times 13$	0	1
3	2	-1	$145 = 5\times 29$	0	1
4	1	-1	$185 = 5\times 37$	0	1
4	3	-1	$585 = 3^2\times 5\times 13$	1	2
5	2	-1	$689 = 13\times 53$	0	1
4	3	$+1$	$697 = 17\times 41$	1	2
6	1	-1	$1105 = 5\times 13\times 17$	1	2
6	1	$+1$	$1665 = 3^2\times 5\times 37$	1	2
5	4	$+1$	$1769 = 29\times 61$	0	1
6	3	$+1$	$2257 = 37\times 61$	0	3
7	2	-1	$2465 = 5\times 17\times 29$	1	2
7	2	$+1$	$3185 = 5\times 7^2\times 13$	1	2
6	5	-1	$3649 = 41\times 89$	1	2
8	1	-1	$3737 = 37\times 101$	0	3
7	4	-1	$3977 = 41\times 97$	1	4
7	4	$+1$	$4505 = 5\times 17\times 53$	1	4
8	1	$+1$	$4745 = 5\times 13\times 73$	1	4
8	3	-1	$4905 = 3^2\times 5\times 109$	1	2
8	3	$+1$	$5785 = 5\times 13\times 89$	1	4
7	6	-1	$7137 = 3^2\times 13\times 61$	1	4
7	6	$+1$	$7345 = 5\times 13\times 113$	1	6
8	5	$+1$	$8249 = 73\times 113$	1	2
9	4	-1	$8905 = 5\times 13\times 137$	1	4
9	4	$+1$	$9945 = 3^2\times 5\times 13\times 17$	2	4

Nous amendons maintenant, dans les cas de $k = Q(i)$, la loi de réciprocité établie au corollaire 6, obtenant ainsi une démonstration différente de celle de P. G. L. Dirichlet de sa loi de réciprocité quadratique. Remarquons préalablement qu'un entier impair x de $Q(i)$ est primaire si et seulement si $x \equiv \pm 1 \pmod{(4)}$, et est faiblement primaire si et seulement si $x \equiv 1 \pmod{(2)}$, i.e. si et seulement si $x = a+ib$ avec a impair et b pair. En particulier, x ou ix est faiblement primaire.

COROLLAIRE 11. *Pour $k = Q(i)$ la loi de réciprocité énoncée au corollaire 6 reste valable en supposant seulement les deux irréductibles π_1 et π_2 faiblement primaires.*

Preuve. Les deux symboles $\left[\frac{\pi_1}{(\pi_2)}\right]$ et $\left[\frac{\pi_2}{(\pi_1)}\right]$ valant ± 1, il suffit de montrer que

$$\left[\frac{\pi_1}{(\pi_2)}\right] = +1 \Leftrightarrow \left[\frac{\pi_2}{(\pi_1)}\right] = +1,$$

puis par symétrie que

$$\left[\frac{\pi_1}{(\pi_2)}\right] = +1 \Rightarrow \left[\frac{\pi_2}{(\pi_1)}\right] = +1.$$

Nous supposons π_1 et π_2 (au dessus de p_1 et p_2) faiblement primaires mais non primaires, sans quoi le corollaire 6 nous donne le résultat. Ils sont alors tous deux congrus à $\pm 1+2i$ modulo l'idéal (4), et p_1 et p_2 sont congrus à 5 modulo 8. Soit $K = Q(i, \sqrt{\pi_1})$ et $k = Q(i)$. Alors $\delta_{K/k} = \pm 2i\pi_1$ et $\omega_0 = (P_0+\sqrt{\pi_1})/(1+i)$ est un R_k-générateur de l'anneau des entiers de K, où $\pi_1 \equiv P_0^2 \pmod{(2)}$. Puisque $\left[\frac{\pi_1}{(\pi_2)}\right] = +1$, l'équation $X^2 \equiv \pi_1 \pmod{(\pi_2)}$ est résoluble dans R_k et l'idéal (π_2) n'est donc pas inerte dans K/k (car l'anneau $R_K/(\pi_2)$ n'est pas un intègre), donc est totalement décomposé en disons $(\pi_2) = PP'$. D'après le corollaire 10, le nombre de classes $h(K)$ est impair (car $t = 2$ et $p_1 \equiv 5 \pmod 8$), et $P^{h(K)}$ est principal. Prenons les normes relatives, il existe donc $(\varepsilon', x, y) \in U_k \times R_k \times R_k$ tel que $\varepsilon'\pi_2^{h(K)} = (x^2-\pi_1 y^2)/(-2i)$, donc $(\varepsilon, x, y) \in U_k \times R_k \times R_k$ tel que $2\varepsilon\pi_2^{h(K)} = x^2-\pi_1 y^2$. Si $\varepsilon = \pm 1$, alors en passant modulo l'idéal (4) et tenant compte de $\pi_1, \pi_2 \equiv \pm 1+2i \pmod{(4)}$, nous obtenons $2\varepsilon\pi_2^{h(K)} \equiv \pm 2 \pmod{(4)}$ et $x^2-\pi_1 y^2 \equiv x^2-(\pm 1+2i)y^2 \pmod{(4)}$. Si x et y sont impairs, alors $x^2 \equiv y^2 \equiv \pm 1 \pmod{(4)}$ ce qui contredit $2\varepsilon\pi_2^{h(K)} \equiv x^2-\pi_1 y^2 \pmod{(4)}$. Si x ou y est pair, alors x et y sont pairs, c'est à dire divisibles par $1-i$, et en posant $x = (1-i)x'$ et $y = (1-i)y'$ nous avons: $x'^2-\pi_1 y'^2 = i\varepsilon\pi_2^{h(K)}$. En passant modulo l'idéal (2) nous obtenons $x'^2-y'^2 \equiv \pm i \pmod{(2)}$, ce qui n'est pas possible puisque $x'^2, y'^2 \equiv 0, 1 \pmod{(2)}$. Finalement, $\varepsilon = \pm i$ et $2\varepsilon = \pm(1+i)^2$. Nous avons donc $\pm\left((1-i)\pi_2^{(h(K)-1)/2}\right)^2\pi_2 = x^2-\pi_1 y^2$, et π_2 est un carré modulo l'idéal (π_1), i.e. $\left[\frac{\pi_2}{(\pi_1)}\right] = +1$. ∎

Cas d'un corps quadratique imaginaire de nombre de classes impair. La référence principale de ce dernier paragraphe est [2]. K/k étant cyclique (de degré 2) et non ramifiée aux places infinies, ε_k est une norme relative globale si et seulement elle est une norme relative locale en toute place P, P un idéal premier de k. D'après la formule du produit pour les symboles de Hilbert, on peut même ne pas tenir compte d'une place. Puisque nous avons déjà traité le cas des corps $Q(i)$, $Q(j)$ et $Q(\sqrt{-2})$, nous pouvons supposer que 2 est inerte dans k/Q et que $\varepsilon_k = -1$. Nous avons ainsi que $\varepsilon_k = -1$ est une norme relative globale si et seulement elle est une norme relative locale en toute place P, P un idéal premier de k au dessus de p premier impair.

Soient alors d dans R_k tel que $K = k(\sqrt{d})$. Des propriétés satisfaites par les symboles de Hilbert, nous déduisons que -1 appartient à $N_{K/k}(K^*)$ si et seulement si

$$\left(\frac{-1, d}{P}\right) = \left(\frac{-1}{P}\right)^{v_P(d)} = +1$$

pour tout idéal premier P de k de norme absolue impaire. Utilisons alors le résultat particulier suivant de la théorie de Kummer:

LEMME. *K/k une extension quadratique, d dans k tel que $K = k(\sqrt{d})$ et P un idéal premier de k de norme absolue impaire. Alors, P est ramifié dans K/k si et seulement si la P-valuation $v_P(d)$ de d est impaire.*

Nous en déduisons que -1 appartient à $N_{K/k}(K^*)$ si et seulement si

$$\left(\frac{-1}{P}\right) = (-1)^{(N_{k/Q}(P)-1)/2} = +1$$

pour tout idéal premier P de k ramifié dans K/k et de norme absolue impaire. Nous avons donc le résultat final suivant qui lève l'ambiguïté du théorème 3:

THÉORÈME 12. *Soit k un corps quadratique imaginaire non principal de nombre de classes impair et soit K/k une extension quadratique de k de discriminant relatif $\delta_{K/k}$. Alors, -1 appartient à $N_{K/k}(K^*)$ si et seulement si les diviseurs premiers impairs non inertes dans k/Q de $N_{k/Q}(\delta_{K/k})$ sont congrus à 1 modulo 4.*

Détermination de la norme relative de l'unité fondamentale. K/Q désigne une extension biquadratique contenant un corps quadratique imaginaire k, de sorte que K/Q est totalement complexe et donc de rang de groupe des unités valant 1. Nous voulons déterminer la norme relative $N_{K/k}(\eta_K)$ de l'unité fondamentale η_K de K, et ce pour connaître l'ordre du sous groupe des classes régulières (théorème 1).

1er cas: *K/Q est galoisienne*: Etant de degré 4, elle est abélienne et la conjugaison complexe est un Q-isomorphisme non trivial de K qui admet donc un unique sous-corps quadratique réel, ici noté k_+, sous corps dont nous notons ε_+ l'unité fondamentale. Nous notons comme précédemment σ le k-isomorphisme non trivial de K. Puisque σ restreint à k_+ n'est pas trivial, c'est le Q-isomorphisme non trivial de k_+. Notons que nous n'avons nul besoin de supposer k de nombre de classes impair pour ce qui suit.

PROPOSITION 13. *Supposons K distinct de $Q(\zeta_n)$, $n = 8$, 10 ou 12. Alors,*

(a) *Si $Q(i) \subseteq K$ et $k = Q(i)$ on a $\eta_K = \varepsilon_+$ et $N_{K/k}(\eta_K) = +1$, excepté lorsque l'idéal (2) est ramifié en $(2) = P^2$ dans k_+/Q avec P principal, auquel cas $\eta_K = \sqrt{-i\varepsilon_+}$ et $N_{K/k}(\eta_K) = i$.*

(b) *Si $Q(i) \subseteq K$ et $k \neq Q(i)$ on a $\eta_K = \varepsilon_+$ et $N_{K/k}(\eta_K) = N_{k_+/Q}(\varepsilon_+)$, excepté lorsque l'idéal (2) est ramifié en $(2) = P^2$ dans k_+/Q avec P principal, auquel cas $\eta_K = \sqrt{-i\varepsilon_+}$ et $N_{K/k}(\eta_K) = +1$ si P est principal au sens strict, alors que $N_{K/k}(\eta_K) = -1$ si P est principal au sens large mais ne l'est pas au sens strict.*

(c) *Si $Q(i) \not\subseteq K$ et $k = Q(\sqrt{-d})$ avec $d \in N^*$ libre de carrés, on a $\eta_K = \varepsilon_+$ et $N_{K/k}(\eta_K) = N_{k_+/Q}(\varepsilon_+)$, excepté lorsque l'idéal (d) est ramifié en $(d) = I^2$ dans k_+/Q avec I principal, auquel cas $\eta_K = \sqrt{-\varepsilon_+}$, et $N_{K/k}(\eta_K) = -1$ si I est principal au sens strict, alors que $N_{K/k}(\eta_K) = +1$ si I est principal au sens large mais ne l'est pas au sens strict.*

(d) *Si on est dans la seconde alternative du* (c), *alors $N_{k_+/Q}(\varepsilon_+) = +1$.*

(e) *Ces différentes possibilités sont discriminées en développant en fractions continues le générateur habituel ω_0 de l'anneau des entiers de k_+* (voir Louboutin [12]).

EXEMPLES.

(α) $k = Q(\sqrt{-3})$, $k_+ = Q(\sqrt{21})$ et $K = Q(\sqrt{-3}, \sqrt{7})$. Ici $\varepsilon_+ = (5+\sqrt{21})/2$, $\sqrt{-\varepsilon_+} = (\sqrt{-3}-\sqrt{-7})/2 = (-3-\sqrt{21})/2\sqrt{-3}$ et donc $N_{K/k}(\eta_K) = (3^2-21)/(-12) = +1$.

(β) $k = Q(\sqrt{-3})$, $k_+ = Q(\sqrt{33})$ et $K = Q(\sqrt{-3}, \sqrt{11})$. Ici $\varepsilon_+ = 23+4\sqrt{33}$, $\sqrt{-\varepsilon_+} = 2\sqrt{-3}-\sqrt{-11} = (-6-\sqrt{33})/\sqrt{-3}$ et donc $N_{K/k}(\eta_K) = (6^2-33)/(-3) = -1$.

Ces résultats sont conformes aux prédictions de notre proposition 13(c) puisque dans le premier cas $\omega_0 = (1+\sqrt{21})/2$ est de longueur de période de développement en fractions continues valant 2 et que, avec les notations de Louboutin [12], $Q_1(R_{k_+}) = 3$, et que donc I est principal au sens large mais pas au sens strict; alors que dans le second cas $\omega_0 = (1+\sqrt{33})/2$ est de longueur de période de développement en fractions continues valant 4 et que $Q_2(R_{k_+}) = 3$, et que donc I est principal au sens strict.

Remarque. Si $k_+ = Q(\sqrt{d_+})$ avec $d_+ \in N^*$ libre de carrés, alors $k' = Q(\sqrt{-d'})$ est le dernier sous-corps quadratique de K (où d' est libre de carrés et défini par $dd_+ = n^2 d'$) et il est quadratique imaginaire. Il en résulte que si $(d) = I^2$ dans k_+, alors $(d') = J^2$ où J est l'idéal ramifié dual de I. En particulier, I et J sont simultanément principaux ou non principaux et, si ils sont principaux, un seul d'entre eux est principal au sens strict. Nous avons donc $N_{K/k}(\eta_K) = -N_{K/k'}(\eta_K)$ lorsqu'on se trouve dans la seconde alternative de la proposition 13(c).

Preuve de la proposition 13. L'extension K/Q étant abélienne, si nous notons $\bar{\eta}_K$ le conjugué complexe de η_K, alors $\dfrac{\bar{\eta}_K}{\eta_K}$ est de module 1 ainsi que tous ses conjugués par le groupe de Galois de K/Q. C'est donc une racine de l'unité de K.

LEMME. *K/Q de degré 4. Alors $K = Q(\zeta_n)$ avec $n = 8$, 10 ou 12 et alors $h(K) = 1$, ou bien le groupe $\mu(K)$ des racines de l'unité de K est $\{\pm 1\}$, $\{\pm 1, \pm i\}$ ou $\{\pm 1, \pm j, \pm j^2\}$ (cas exclusifs).*

La preuve en est aisée et résulte de ce que si ζ_n est une racine primitive n-ième de K, alors $\phi(n)$ divise 4. Notre but étant de déterminer l'ordre du

groupe des classes régulières, nous exclusons les trois corps principaux $Q(\zeta_n)$ avec $n = 8$, 10 ou 12 pour lesquels l'ordre des classes régulières vaut évidemment 1.

En multipliant au besoin η_K par une racine de l'unité de K, nous pouvons supposer que $\bar{\eta}_K/\eta_K = \pm 1$ pour $Q(i) \notin K$, et que $\bar{\eta}_K/\eta_K = +1$ ou i pour $Q(i) \subseteq K$.

(α) Si $\bar{\eta}_K/\eta_K = +1$ alors η_K appartient à k_+ et il existe donc $m \in Z$ tel que $\eta_K = \pm(\varepsilon_+)^m$. D'un autre côté, ε_+ est une unité de K et il existe donc $n \in Z$ et $\varepsilon \in \mu(K)$ tels que $\varepsilon_+ = \varepsilon(\eta_K)^n$. Il en résulte que $m = \pm 1$ et que nous pouvons supposer que $\eta_K = \varepsilon_+$. Réciproquement, si $\eta_K = \varepsilon_+$, alors $\bar{\eta}_K/\eta_K = +1$. Maintenant, nous avons alors $N_{K/k}(\eta_K) = N_{K/k}(\varepsilon_+) = \varepsilon_+ \sigma(\varepsilon_+) = N_{k_+/Q}(\varepsilon_+)$ d'après la remarque précédant notre proposition 13.

(β) Si $\bar{\eta}_K/\eta_K \neq +1$. Comme précédemment, il existe (m, n) dans Z et ε dans $\mu(K)$ tels que $\bar{\eta}_K \eta_K = (\varepsilon_+)^m$ et $\varepsilon_+ = \varepsilon(\eta_K)^n$. D'où en passant aux modules: $mn = 2$. Si $n = \pm 1$, alors $\bar{\eta}_K/\eta_K = \bar{\varepsilon}/\varepsilon = \varepsilon^{-2}$ ne peut valoir -1 pour $\mu(K) \neq \{\pm 1, \pm i\}$, et ne peut valoir i pour $\mu(K) = \{\pm 1, \pm i\}$. Nous avons donc $n = \pm 2$ et on peut même supposer que $n = 2$. D'où $m = 1$ et

$$\bar{\eta}_K \eta_K = \varepsilon_+ = (\eta_K)^2 \frac{\bar{\eta}_K}{\eta_K},$$

et donc $(\eta_K)^2 = -\varepsilon_+$ pour $Q(i) \notin K$, et $(\eta_K)^2 = -i\varepsilon_+$ pour $Q(i) \subseteq K$.

Nous avons donc les premières parties de nos énoncés (a), (b) et (c).

Pour les secondes parties, nous distinguons les cas $Q(i) \subseteq K$ et $Q(i) \notin K$.

(i) $(\eta_K)^2 = -i\varepsilon_+$ et $Q(i) \subseteq K$. Soit $\alpha = (1+i)\eta_K$. Alors $\bar{\alpha} = \alpha$ et α appartient donc à k_+. De plus, $\alpha^2 = 2\varepsilon_+$ appartient à $2R_{k_+}$. L'idéal $P = (\alpha)$ est donc premier et principal dans k_+ et tel que $P^2 = (2)$. Réciproquement, si $(2) = P^2$ avec $P = (\alpha)$ principal, alors $\eta = \alpha/(1+i)$ est de trace relative α sur k_+ et de norme relative $\alpha^2/2$ sur k_+ toutes deux dans R_{k_+}, l'anneau des entiers de k_+. Il en résulte que η_K est une unité de K telle que $\bar{\eta}/\eta = (1+i)/(1-i) = i$, et il en est conséquemment de même de η_K. Finalement,

$$N_{K/k}(\eta_K) = N_{K/k}\left(\frac{\alpha}{1+i}\right) = \frac{N_{k_+/Q}(\alpha)}{N_{K/k}(1+i)} = \frac{\pm 2}{N_{K/k}(1+i)}$$

est égale à $\mp i$ pour $i \in k$, et égale à $+1$ pour $i \notin k$ et P principal au sens strict, et égale à -1 pour $i \notin k$ et P principal au sens large mais pas au sens strict.

(ii) $(\eta_K)^2 = -\varepsilon_+$ et $Q(i) \notin K$. La preuve suit la précédente mais en considérant $\alpha = \sqrt{-d}\eta_K$.

Le (d) résulte de ce que si $k_+ = Q(\sqrt{d_+})$ avec $d_+ \in N^*$ libre de carrés, alors $Q(i) \notin K$ implique $d \neq d_+$, et de ce que si $N_{k_+/Q}(\varepsilon_+) = -1$, alors les deux seuls idéaux primitifs ramifiés principaux de k_+ sont $(1) = R_{k_+}$ et $(\sqrt{d_+})$.

2ème cas: *K/Q n'est pas galoisienne et k est quadratique imaginaire principal.* Il est bien connu que la norme de l'unité fondamentale d'un corps quadratique réel vaut $+1$ ou -1 suivant que la période primitive du développement en fractions continues du générateur habituel ω_0 de l'anneau des entiers est paire ou impaire. L'algorithme de développement en fractions continues étant aisément implémentable sur microordinateur, on dispose ainsi d'un moyen numérique de test de la norme de l'unité fondamentale (la connaissance exacte de cette unité est elle en général hors de portée puisqu'elle peut être de grandeur telle qu'elle ne soit pas représentable par la machine, bien que le régulateur de ce corps quadratique lui soit aisément calculable à toute précision (suffisante pour en déduire le nombre de classes par la formule analytique du nombre de classes) par cet algorithme des fractions continues). Dans le cas d'un corps de nombres quelconque, si on ne dispose plus de cet outil, on dispose néanmoins de son prolongement: la théorie des cycles d'idéaux réduits. Nous montrons ici que la longueur du cycle des idéaux réduits de l'anneau des entiers de K contient de même des informations sur la norme relative de l'unite fondamentale, généralisant ainsi ce test fourni par l'algorithme des fractions continues. Nous supposons k principal et assumons la théorie des cycles d'idéaux développée par H. Amara [1] dans ce cadre.

PROPOSITION 14. *Si le cycle des idéaux réduits de l'idéal R_K est de longueur paire, alors la norme relative $N_{K/k}(\eta_K)$ de l'unité fondamentale de K vaut $+1$.*

Pour ce faire, nous admettons ici les résultats suivants sur les cycles d'idéaux réduits (dont nous donnerons ailleurs la démonstration):

Un idéal I de K est dit *réduit* lorsqu'il est entier, non nul et tel que $z \in I$ et $z \neq 0$ impliquent $\max(|z|, |z^\sigma|) \geqslant |N_{K/k}(I)|$. Si I_0 est un idéal réduit de K, il existe à multiplication par une unité de k près un unique $h_0(I_0)$ non nul et dans I_0 tel que $|h_0(I_0)| < |N_{K/k}(I)|$ et tel que $z \in I_0$, $z \neq 0$ et $|z| < |N_{K/k}(I_0)|$ impliquent $|z^\sigma| \geqslant |h_0^\sigma(I_0)|$. Cet élément est appelé *l'élément de conversion* de l'idéal I_0. Si I_1 est l'idéal de K défini par

$$I_1 = \left(\frac{h_0^\sigma(I_0)}{N_{K/k}(I_0)}\right) I_0,$$

alors I_1 est un idéal réduit appelé *le successeur* de l'idéal I_0. L'ensemble des idéaux réduits de K est fini, toute classe d'idéaux contient un idéal réduit et les idéaux réduits d'une même classe d'idéaux sont ordonnés en cycle par l'application successeur. Autrement dit, on peut indicer ces disons L idéaux réduits d'une classe quelconque en $\{I_i, 0 \leqslant i \leqslant L-1\}$ de telle sorte que I_{i+1} soit de successeur de I_i pour $0 \leqslant i \leqslant L-2$, et tel que I_0 soit le successeur de I_{L-1}. On peut alors pour $i \in Z$ définir I_i par $I_i = I_{\bar{i}}$ où $\bar{i} \equiv i \pmod{L}$ avec $0 \leqslant \bar{i} \leqslant L-1$. Si I est réduit, il en est de même de son conjugué I^σ et $(I_i)^\sigma = (I^\sigma)_{-i}$, cela résultant de ce que $h_0((I_1)^\sigma) = h_0(I_0)$.

Prenons $I_0 = I = R_K$ et notons $2L$ la longueur supposée paire du cycle d'idéaux réduits de I_0. Puisque $(I_L)^\sigma = (I^\sigma)_{-L} = I_{-L} = I_L$, I_L est réduit, invariant et distinct de I. L'idéal $(\sqrt{d})$ n'étant pas réduit (où $d \in R_k$ est libre de carré dans R_k et tel que $K = k(\sqrt{d})$), nous avons donc au moins quatre idéaux primitifs ramifiés principaux dans K, à savoir R_K, $(\sqrt{d})$, I_L et l'idéal J dual de ce dernier (défini par J est primitif et $(\sqrt{d})I_L = (m)J$, $m \in R_k$). Le sous-groupe $H_{reg}(K)$ des classes régulières est donc d'ordre au plus 2^{t-2}. Le théorème 1 donne le résultat.

Ce résultat n'est que partiel et nous ne disposons pas encore de sa réciproque (la difficulté résultant de ce que contrairement au cas des corps quadratiques réels, ici les cycles d'idéaux réduits n'ont plus nécessairement même parité de longueur, et il n'est plus vrai qu'un idéal primitif ramifié ou son idéal dual soit réduit). Nous aborderons ailleurs de façon plus détaillée ces considérations.

Bibliographie

[1] H. Amara, *Groupe des classes et unité fondamentale des extensions quadratiques relatives à un corps quadratique imaginaire principal*, Pacific J. Math. 96 (1) (1981), 1–12.

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Thompson, Washington, DC, 1967.

[3] C. Chevalley, *Sur la théorie du corps de classes*, J. Fac. Sci. Tokyo, Sec. 1, 1–2 (1933), 365–476. Plus spécialement, 402–406.

[4] H. Cohn, *Second Course in Number Theory*, Wiley, New York 1962.

[5] — *A Classical Invitation to Algebraic Numbers and Class Fields*, Universitext, Springer, 1978.

[6] Nguyen Quang Do Thong, *Unités de norme −1 d'un corps quadratique réel*, Séminaire Delange–Pisot–Poitou 1975/76, exposé G6.

[7] F. Gerth, *The 4-class ranks of quadratic extensions of certain imaginary quadratic fields*, Illinois J. Math. 33 (1) (1989), 132–142.

[8] G. Gras, *Etude du l-groupe des classes des extensions cycliques de degré l*, Séminaire Delange–Pisot–Poitou 1971/72, exposé 20.

[9] — *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier (Grenoble) 23 (3) (1973), 1–48; ibid. 23 (4) (1973), 1–44.

[10] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Graduate Texts in Math. 77, Springer, 1981.

[11] S. Louboutin, *Nombre de classes d'idéaux des extensions quadratiques du corps de Gauss*, preprint.

[12] — *Le groupe des classes ambiges (au sens strict)*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math. 81, Birkhäuser, Boston 1990, 147–153.

UNIVERSITÉ DE CAEN
U.F.R. SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES
Esplanade de la Paix
14032 Caen Cedex, France

Reçu le 4.1.1990
et révisé le 3.4.1990 (1997)

ACTA ARITHMETICA
LVIII.3 (1991)

On the generalized Ramanujan–Nagell equation $x^2 - D = p^n$

by

MAOHUA LE (Changsha, China)

1. Introduction. Let Z, N, Q be the sets of integers, positive integers and rational numbers respectively. Let $D \in N$, and let p be an odd prime with $p \nmid D$. We denote the number of positive solutions[1] (x, n) of the generalized Ramanujan–Nagell equation

$$x^2 - D = p^n \tag{1}$$

by $N(D, p)$. In [1], Beukers proved that $N(D, p) \leqslant 4$. Simultaneously, he suspected that $N(D, p) \leqslant 3$. In this paper, we prove the following results.

THEOREM 1. *If* $\max(D, p) \geqslant 10^{100}$ *and*

$$p = \begin{cases} 3, \\ 4a^2+1; \end{cases} \qquad D = \begin{cases} \left(\dfrac{3^m+1}{4}\right)^2 - 3^m, & 2 \nmid m, \\ \left(\dfrac{p^m-1}{4a}\right)^2 - p^m, & \end{cases} \qquad a, m \in N,\ m > 1, \tag{2}$$

then $N(D, p) = 3$.

THEOREM 2. *If* $\max(D, p) \geqslant 10^{240}$, *then* $N(D, p) \leqslant 3$.

2. Lemmas. By the proof of Theorem 2 of [1], we see that if D is a square, then $N(D, p) \leqslant 1$. From now on we assume that D is not a square.

LEMMA 1 ([1], Lemma 5). *Let* (x, n), (x', n'), (x'', n'') *be three positive solutions of* (1) *with* $n < n' < n''$. *Then* $n'' \geqslant 2n' + \max(3, n, 2(n'-1)/3)$ *except when* D, p *satisfy* (2) *and* $(n, n', n'') = (1, m, 2m+1)$. ∎

LEMMA 2 ([1], Theorem 1). *Let* (x, n), (x', n') *be two positive solutions of* (1) *with* $n < n'$. *Then* $p^n \leqslant \max(2 \cdot 10^6, 600D^2)$. ∎

LEMMA 3 ([3], Lemma 1). *Let* $u_1 + v_1\sqrt{D}$ *be the fundamental solution of the equation*

$$u^2 - Dv^2 = 1. \tag{3}$$

[1] Throughout this paper "solution" and "positive solution" are the abbreviations for "integer solution" and "positive integer solution" respectively.