J. Math. Soc. Japan
Vol. 25, No. 4, 1973

Divisibilité par 8 du nombr des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique

Par Pierre KAPLAN

(Reçu le 30 sept., 1972)

Introduction.

Soit (C^*) d'ordre $h^*(D)$ le groupe des classes d'idéaux au sens étroit de $\boldsymbol{Q}(\sqrt{D})$. Son 2-sous-groupe de Sylow (C_2) est cyclique d'ordre $h_2(D) \geqq 4$ dans les cas suivants:

$$D=-p \text{ ou } D=\pm 2p, \text{ avec } p\equiv 1 \pmod 8$$

$$D=-2p, \text{ avec } p\equiv -1 \pmod 8$$

$$D=\pm pq, \text{ avec } p\equiv \pm q\equiv 1 \pmod 4 \text{ et } \left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)=1.$$

Récemment, plusieurs auteurs ([1], [3], [9], [10] et [11]) ont étudié le problème de distinguer, parmi ces cas, ceux où $h^*(D)$ est divisible par 8; leurs résultats concernent surtout les cas des corps imaginaires. Il existe aussi des critères plus anciens dans [16] et [20], démontrés à l'aide de la théorie du Corps de Classes.

Le but de ce travail est de traiter ce problème *dans tous les cas* par une méthode uniforme et élémentaire, n'utilisant rien d'autre que la théorie des formes quadratiques binaires. Pour les corps *réels* nous obtenons les résultats nouveaux suivants:

1) *Cas* $\boldsymbol{Q}(\sqrt{2p})$: *Soit* $p=a^2+b^2\equiv 1 \pmod 8$ *où* $b\equiv 0 \pmod 4$.

$h^*(2p)$ *est divisible par* 8 *si, et seulement si,* $a\equiv \pm 1$ *et* $b\equiv 0 \pmod 8$.

Malgré sa simplicité et son élégance ce critère semble ne pas avoir été remarqué jusqu'à présent.

2) *Cas* $\boldsymbol{Q}(\sqrt{pq})$: *Soient* p *et* $q\equiv 1 \pmod 4$, $p=a^2+b^2$, $q=c^2+d^2$, b *et* d *pairs, et* $(p/q)=(q/p)=1$. Une et une seule des équations $t^2-pqu^2=-1, p, q$ a des solutions.

Si $t^2-pqu^2=-1$ *a des solutions:*

$$(-1)^{h^*(pq)/4}=(p/q)_4=(q/p)_4 \text{ et } (ac+bd)/p=(ac+bd)/q=1.$$

Si $t^2-pqu^2=p$ *a des solutions:*

$$(-1)^{h^*(pq)/4}=(ac+bd)/p=(ac+bd)/q=(p/q)_4 \text{ et } (q/p)_4=1.$$

(Le fait que $(q/p)_4=1$ quand $t^2-pqu^2=p$ a des solutions était connu de Dirichlet.)

Des critères 2) on déduit immédiatement:

a) Un critère de L. Redei [**16**] et A. Schalz [**20**] déjà mentionné:

$$h^*(pq)\equiv 0 \pmod 8 \text{ si et seulement si } (p/q)_4=(q/p)_4=1.$$

b) Une démonstration entièrement nouvelle, ne sortant pas du cadre de la théorie des formes quadratiques binaires, de la Loi de Réciprocité Biquadratique Rationnelle de K. Burde [**5**]:

$$\text{Si } p\equiv q\equiv 1 \pmod 4 \text{ et } (p/q)=(q/p)=1,$$
$$\text{alors } (p/q)_4(q/p)_4=((ac+bd)/p)=((ac+bd)/q).$$

Nous redémontrons en passant l'essentiel des critères de [**1**], [**3**], [**9**] et [**10**] concernant les cas des corps imaginaires $\boldsymbol{Q}(\sqrt{-p})$ et $\boldsymbol{Q}(\sqrt{-2p})$, car leurs démonstrations sont, en grande partie, incluses dans celle du critère pour $\boldsymbol{Q}(\sqrt{2p})$, et aussi parce que les critères utilisant la décomposition $p=a^2+b^2$ sont, l'un, à peine formulé et, l'autre, non démontré (Cf. [**1**], formule 6a, et [**10**], note page 232); nous pouvons ainsi prouver le résultat suivant:

Si $p\equiv 1 \pmod 8$, $h^*(2p)$ *est divisible par* 8 *si, et seulement si,* $h^*(-p)$ *et* $h^*(-2p)$ *sont divisibles par* 8.

Ensuite nous montrons comment notre méthode permet de retouver les critères, utilisant les solutions de certaines équations diophantiennes, de [**11**] et de trouver d'autres critères analogues, mais plus simples (Théorème 9).

Enfin, dans un dernier paragraphe, nous comparons la Loi de Réciprocité Biquadratique Rationnelle b) avec la Loi de Réciprocité Biquadratique générale, ce qui nous conduit à formuler une loi de réciprocité biquadratique rationnelle nouvelle dans le cas où $p\equiv q\equiv 1 \pmod 4$ et $(p/q)=(q/p)=-1$ (Théorème 10).

§ 1. Notations et rappels.

p et q désigneront toujours des nombres premiers.

Une forme quadratique binaire $AX^2+2BXY+CY^2$ sera notée $[A, B, C]$, son déterminant B^2-AC noté D. Nous ne considérons que des formes "proprement primitives", où le P. G. C. D. $(A, 2B, C)=1$. Deux formes f et f' sont équivalentes (noté: $f\approx f'$) si l'on passe de l'une à l'autre par une substitution linéaire de déterminant $+1$. Les classes d'équivalence des formes de même déterminant D, positives si $D<0$, forment un groupe (C) pour la "composi-

tion", une forme composée de $[A, B, A'C]$ et $[A', B, AC]$ étant $[AA', B, C]$. Si D n'a pas de diviseur carré, le groupe (C^*) des classes d'idéaux au sens étroit de $\boldsymbol{Q}(\sqrt{D})$ est isomorphe à (C) ou au quotient de (C) par un sous-groupe à 3 éléments, donc leurs 2-composantes (C_2) sont isomorphes.

(C_2) est cyclique non trivial quand il existe, outre la classe unité $\mathcal{I}$ de $[1, 0, -D]$, exactement une autre classe $\mathcal{A}$ "ambiguë" dont le carré est $\mathcal{I}$. Depuis Gauss on sait pour quels D cela est, et on sait trouver des représentants de $\mathcal{A}$: appelons "ambiguë simple" une forme du type $[A, 0, C]$ avec $|A| \leqq |C|$, $(D = -AC)$ ou bien du type $[2B, B, E]$ avec $|B| \leqq |2E-B| = |B'|$ $(D = -BB')$. (Il n'y a de formes du deuxième type que si $D \equiv -1 \pmod 4$.) Alors:

PROPOSITION 0 (Gauss): *Les classes ambiguës sont les classes contenant des formes ambiguës simples. Une classe indéfinie $(D > 0$ non carré$)$ contient exactement deux formes ambiguës simples; une classe définie $(D < 0)$ en contient exactement une. (C_2) est cyclique non trivial quand $D = \pm p \equiv -1 \pmod 4$, ou bien quand $D = \pm 2p$, ou bien quand $D = \pm pq \equiv 1 \pmod 4$.*

Si (C_2) est cyclique non trivial son ordre h_2 est divisible par 4 si et seulement si $\mathcal{A}$ est un carré. La proposition 0 permet facilement de trouver des représentants de $\mathcal{A}$ et, d'autre part, la théorie de Gauss montre aussi que une classe est un carré si et seulement si elle est dans le "genre principal", défini par les caractères génériques qui sont ici:

$$\text{Si } D = \pm p \equiv -1 \pmod 4\text{: } \left(\frac{m}{p}\right) \text{ et } (-1)^{(m-1)/2} = \left(\frac{-1}{m}\right)$$

$$\text{Si } D = \pm pq \equiv 1 \pmod 4\text{: } \left(\frac{m}{q}\right) \text{ et } \left(\frac{m}{q}\right)$$

$$\text{Si } D = \pm 2p \equiv 2 \pmod 8\text{: } \left(\frac{m}{p}\right) \text{ et } (-1)^{(m^2-1)/8} = \left(\frac{2}{m}\right)$$

$$\text{Si } D = \pm 2p \equiv -2 \pmod 8\text{: } \left(\frac{m}{p}\right) \text{ et } (-1)^{(m^2-1)/8+(m-1)/2}.$$

Chaque caractère à la même valeur pour tous les nombres m premiers à $2D$ représentés par une même forme f de déterminant D, et le produit de ces valeurs est 1; f est dans le genre principal si, et seulement si, les deux caractères valent 1, donc si, et seulement si, un des deux vaut 1.

On vérifie ainsi facilement que (C_2) *est cyclique et* $h_2 \equiv 0 \pmod 4$ *dans les cas suivants:*

a) $D = -p$, $p \equiv 1 \pmod 8$;
b) $D = -2p$, $p \equiv \pm 1 \pmod 8$;
c) $D = -pq$, $p \equiv 1$, $q \equiv -1 \pmod 4$, $(p/q) = 1$;
d) $D = 2p$, $p \equiv 1 \pmod 8$;

e) $D=pq$, $p\equiv q\equiv 1 \pmod 4$, $(p/q)=1$.

En effet:

1) Si $D=p$, où $p\equiv -1 \pmod 4$, et si $D=pq$, $p\equiv q\equiv 3 \pmod 4$, la classe ambiguë de $[-1, 0, D]$ n'est pas dans le genre principal, donc $h_2=2$.

2) Si $D=-p$ où $p\equiv 1 \pmod 4$, ou si $D=-2p$, $\mathcal{A}$ a un représentant du type $[2, \cdots, \cdots]$, qui est dans le genre principal si, et seulement si, $(2/p)=1$. Donc $h_2\equiv 0 \pmod 4$ si, et seulement si, $p\equiv 1 \pmod 8$ pour $D=-p$, et si, et seulement si, $p\equiv \pm 1 \pmod 8$ pour $D=-2p$. De même, si $D=-pq$, $\mathcal{A}$ contient $[p, 0, q]$.

3) Si $D=2p$, les formes ambiguës simples sont $[1, 0, -D]$, $[-1, 0, D]$, $[2, 0, -p]$ et $[-2, 0, p]$. Elles sont toutes dans le genre principal si, et seulement si, $p\equiv 1 \pmod 8$.

4) Si $D=pq$, $p\equiv q\equiv 1 \pmod 4$, les formes ambiguës simples sont $[1, 0, -D]$, $[-1, 0, D]$, $[p, 0, -q]$ et $[-p, 0, q]$. Elles sont toutes dans le genre principal si, et seulement si, $(p/q)=(q/p)=1$.

Dans les cas où $h(D)$ est divisible par 4, $h(D)$ est divisible par 8 si, et seulement si, une racine carrée de $\mathcal{A}$ est dans le genre principal.

§2. Racine carrée de $[-1, 0, D]$.

a) Pour que $[A, B, C]$ soit équivalente à $[C, B, A]$ il faut et il suffit que sa classe soit ambiguë. Car $[A, B, C][C, B, A]=[AC, B, 1]\approx[1, 0, -D]$.

b) Pour que $[A, B, C]$ soit équivalente à $[-A, B, -C]$ il faut et il suffit que $t^2-Du^2=-1$ ait des solutions. La démonstration est semblable à celle qui permet de trouver les automorphes d'une forme $[A, B, C]$. Voir [**17**], page 124 ou [**13**], Chapitre 8.

c) Si $D=A^2+B^2$ avec $(A, 2B)=1$, $[A, B, -A]^2=[A^2, B, -1]\approx[-1, 0, D]$. D'autre part toute forme $[A', B', C']$ de la classe de $[A, B, -A]$ est équivalente à $[-C', B', -A']$: si T transforme $[A, B, -A]$ en $[A', B', C']$, ${}^tT^{-1}$ transforme $[A, B, -A]$ en $[-C', B', -A']$.

d) Comme deux des relations: $[A, B, C]\approx[-A, B, -C]$, $[A, B, C]\approx[C, B, A]$ et $[A, B, C]\approx[-C, B, -A]$ entrainent la troisième on voit que:

PROPOSITION 1. *Soit $D=A^2+B^2$ avec $(A, 2B)=1$:*

α) Le carré de la classe de $[A, B, -A]$ est $[-1, 0, D]$.

β) Si $t^2-Du^2=-1$ a des solutions, a classe de $[A, B, -A]$ est ambiguë.

γ) Si $t^2-Du^2=-1$ n'a pas de solution, la classe de $[A, B, -A]$ n'est pas ambiguë.

REMARQUE. La théorie des formes indéfinies réduites permet de montrer la réciproque de c): Si $[A', B', C']$ et $[-C', B', -A']$ sont équivalentes, leur classe contient une forme du type $[A, B, -A]$. Donc si $t^2-Du^2=-1$ a des solutions, toute classe ambiguë contient des formes $[A, B, -A]$ et D est

somme de deux carrés. Remarquant que les formes $[A, B, -A]$ où $B>0$ sont réduites on peut prouver la: (Pour une démonstration complète, voir [13], Chapitre 8.)

PROPOSITION 1′. a) *Si* $t^2-Du^2=-1$ *a des solutions, D est somme de deux carrés premiers entre eux:* $D=A^2+B^2$ *où* $(A, 2B)=1$. *Les classes ambiguës sont les classes contenant des formes* $[A, B, -A]$. *Chaque classe ambiguë contient alors exactement un couple* $[A, B, -A]$, $[-A, B, A]$ *où* $B>0$.

b) *Si* $t^2-Du^2=-1$ *n'a pas de solution, mais si D est somme de deux carrés:* $D=A^2+B^2$ *avec* $(A, 2B)=1$, *les formes du type* $[A, B, -A]$ *où* $B>0$ *se répartissent par couples* $[A, B, -A]$, $[A', B', -A']$ *où* $|A|\neq|A'|$, *dans des classes qui ne sont pas ambiguës.*

c) *Dans les deux cas* a) *et* b), *les classes contenant des formes* $[A, B, -A]$ *où* $(A, 2B)=1$ *sont les racines carrées de la classe de* $[-1, 0, D]$.

§ 3. Cas du déterminant $D=2p$, $p=a^2+b^2\equiv 1 \pmod 8$, $b\equiv 0 \pmod 4$.

Les formes ambiguës simples sont $[1, 0, -2p]$, $[-1, 0, 2p]$, $[2, 0, -p]$ et $[-2, 0, p]$; elles se groupent deux par classe. Celle qui va avec $[1, 0, -2p]$ est celle dont le premier coefficient est représenté par $[1, 0, -2p]$, donc *exactement une des équations* $t^2-2pu^2=-1, 2, -2$ *a des solutions, et les deux formes qui restent définissent* $\mathcal{A}$.

Dirichlet ([3] page 219···) a démontré:

1) *Si* $t^2-2pu^2=2$ *a des solutions,* $a\equiv\pm 1 \pmod 8$.

2) *Si* $t^2-2pu^2=-2$ *a des solutions,* $b\equiv 0 \pmod 8$.

En effet:

1) *Soit* $t^2-2pu^2=2$, $t=2v$, donc $2v^2-pu^2=1$. u est impair, donc $2v^2\equiv 2 \pmod 8$, donc v est impair, donc $2v^2=pu^2+1\equiv 2 \pmod{16}$. 2 est résidu quadratique des facteurs premiers de u, qui sont donc tous $\equiv\pm 1 \pmod 8$. Donc $u^2\equiv 1 \pmod{16}$, donc $p\equiv 1 \pmod{16}$, donc $a\equiv\pm 1 \pmod 8$.

2) *Soit* $t^2-2pu^2=-2$, $t=2v$, donc $2v^2-pu^2=-1$, u est impair, donc $pu^2-1\equiv 0 \pmod 8$, donc v est pair: $v=2^h v'$. p est résidu quadratique des facteurs premiers de v', donc $(p/v')=1$, donc $(v'/p)=1$ et, comme $(2/p)=1$, $(v/p)=1$. Élevant $2v^2-pu^2=-1$ à la puissance $(p-1)/4$ il vient $2^{(p-1)/4}\equiv 1 \pmod p$, donc, utilisant le caractère biquadratique de 2 ([17] page 96): $b\equiv 0 \pmod 8$.

La proposition 1 permet de montrer:

3) *Si* $t^2-2pu^2=-1$ *a des solutions,* $a+b\equiv\pm 1 \pmod 8$.

En effet les classes ambiguës contiennent les formes $[A, B, -A]$, qui sont $[a+b, a-b, -a-b]$ car $2p=(a+b)^2+(a-b)^2$. Mais, comme $p\equiv 1 \pmod 8$, les classes ambiguës sont dans le genre principal, donc $a+b\equiv\pm 1 \pmod 8$.

C. Q. F. D.

En éliminant les cas impossibles on trouve la:

PROPOSITION 2.

α) *Si* $a \equiv \pm 1$ *et* $b \equiv 4 \pmod 8$, t^2-2pu^2 *représente* 2,

β) *Si* $a \equiv \pm 3$ *et* $b \equiv 0 \pmod 8$, t^2-2pu^2 *représente* -2,

γ) *Si* $a \equiv \pm 3$ *et* $b \equiv 4 \pmod 8$, t^2-2pu^2 *représente* -1,

δ) *Si* $a \equiv \pm 1$ *et* $b \equiv 0 \pmod 8$, *on ne peut rien dire.*

Dans les cas α) *et* β), $\mathcal{A}$ contient $[-1, 0, 2p]$, et la proposition 1 montre que le carré de la classe $\mathcal{B}$ de $\varphi = [a+b, a-b, -a-b]$ est $\mathcal{A}$. Dans ces deux cas $a+b \equiv \pm 3 \pmod 8$, donc $\mathcal{B}$ n'est pas un carré, *et* $h_2 \equiv 4 \pmod 8$.

Dans le cas γ) (respectivement: δ)), $\mathcal{A}$ contient (respectivement: peut contenir) $[2, 0, -p]$, dont nous voulons une racine carrée: comme $p \equiv 1 \pmod 8$, $p = 2e^2-d^2$ donc $2p = 4e^2-2d^2$, et la forme $\psi = [d, 2e, 2d]$ de déterminant $2p$ a pour carré $[d^2, 2e, 2]$, équivalente à $[2, 0, -p]$. Il reste à calculer $(-1)^{(d^2-1)/8} = (2/d)$ en fonction de a et b pour savoir si ψ est dans le genre principal: e est impair, donc $2e^2 \equiv 2 \pmod{16}$, d'où $p-1 \equiv 1-d^2 \equiv d^2-1 \pmod{16}$. Donc:

$$\frac{(a+b)^2-1}{8} = \frac{p-1}{8} + a\frac{b}{4} \equiv \frac{p-1}{8} + \frac{b}{4} \equiv \frac{d^2-1}{8} + \frac{b}{4} \pmod 2,$$

donc:

$$\left(\frac{2}{a+b}\right) = \left(\frac{2}{d}\right)(-1)^{b/4}, \quad \text{et} \quad \left(\frac{2}{a}\right) = \left(\frac{2}{d}\right).$$

Si $p \equiv 1 \pmod 8$, nous poserons: $\lambda(p) = (2/(a+b))$.

Dans le cas γ): $a+b \equiv \pm 1 \pmod 8$, mais $b \equiv 4 \pmod 8$, donc $(2/d) = -1$, *et* $h_2 \equiv 4 \pmod 8$.

Dans le cas δ): La racine carrée de $\mathcal{A}$ contient, suivant le nombre p, soit φ soit ψ. Mais $a+b \equiv \pm 1 \pmod 8$ et $b/4$ est pair, donc $(2/(a+b)) = (2/d) = 1$: φ et ψ sont dans le genre principal, *donc* h_2 *est toujours divisible par* 8.

Nous avons donc démontré le:

THÉORÈME 1. *Soit* $p = a^2+b^2 \equiv 1 \pmod 8$, *où* $b \equiv 0 \pmod 4$.

$h(2p)$ *est divisible par* 8 *si, et seulement si,* $a \equiv \pm 1$ *et* $b \equiv 0 \pmod 8$.

§ 4. Cas des déterminants $-p$ et $-2p$ où $p \equiv 1 \pmod 8$.

$p = a^2+b^2 = 2e^2-d^2 = f^2-2g^2$, avec e et $f > 0$ et $g = 2^h g'$, g' impair. $p = 2e^2-d^2$ montre que $(e/p)(2/p)_4 = (d/p) = (p/d) = (2e^2/d) = (2/d)$, donc $(e/p) = (2/d)(-1)^{b/4}$; nous avons utilisé la loi de réciprocité quadratique et le caractère biquadratique de 2. La forme $\psi = [e, d, 2e]$ a pour déterminant $-p$, donc, puisque $e > 0$: $(e/p) = (-1)^{(e-1)/2}$. Le carré de ψ représente 2, donc est dans $\mathcal{A}$, donc, compte tenu des valeurs de $\lambda(p)$ déjà trouvés:

$$\lambda(p) = \left(\frac{2}{a+b}\right) = \left(\frac{a+b}{p}\right) = \left(\frac{2}{d}\right)(-1)^{b/4} = \left(\frac{e}{p}\right) = (-1)^{(e-1)/2} = (-1)^{h(-p)/4}.$$

En particulier:

THÉORÈME 2. *Si* $p\equiv 1 \pmod 8$, $h(-p)\equiv 0 \pmod 8$ *si, et seulement si,* $a+b\equiv \pm 1 \pmod 8$.

$p=f^2-2g^2$ montre que $\left(\frac{f}{p}\right)=\left(\frac{2}{p}\right)_4\left(\frac{g}{p}\right)=(-1)^{b/4}\left(\frac{p}{g'}\right)=(-1)^{b/4}$.

La forme $\chi=[f, 2g, 2f]$ a pour déterminant $-2p$, son carré représente 2, donc son carré est une racine carrée de $\mathcal{A}$. χ est dans le genre principal si et seulement si $(f/p)=1$, donc si $b\equiv 0 \pmod 8$. Donc:

THÉORÈME 3. *Si* $p\equiv 1 \pmod 8$, $h(-2p)\equiv 0 \pmod 8$ *si, et seulement si,* $b\equiv 0 \pmod 8$.

REMARQUE: Le résultat de [**10**] s'obtient en regardant la valeur du deuxième caractère pour f.

COROLLAIRE: *Soit* $p\equiv 1 \pmod 8$. *Pour que* $h(2p)$ *soit divisible par* 8 *il faut et il suffit que* $h(-p)$ *et* $h(-2p)$ *soient divisibles par* 8.

§ 5. Cas du déterminant $D=-2p$, où $p\equiv -1 \pmod 8$.

Le caractère supplémentaire relatif à D est $\varepsilon=(-1)^{(m^2-1)/8}$. Considérant $\chi=[f, 2g, 2f]$ on voit que $h(-2p)\equiv 0 \pmod 8$ si et seulement si $f\equiv \pm 1 \pmod 8$. Ici g est impair, donc $2g^2\equiv 2 \pmod{16}$, donc $p+1\equiv f^2-1 \pmod{16}$, d'où:

THÉORÈME 4. *Si* $p\equiv -1 \pmod 8$, $h(-2p)\equiv 0 \pmod 8$ *si, et seulement si,* $p\equiv -1 \pmod{16}$.

§ 6. Cas d'un déterminant $D=pq$ où $p\equiv q\equiv 1 \pmod 4$, $(p/q)=(q/p)=1$.

Soit $p=a^2+b^2$, $q=c^2+d^2$ où a et c sont impairs; les décompositions de pq en somme de deux carrés sont: $pq=(ac\pm bd)^2+(ad\mp bc)^2$, où $ac\pm bd$ est impair; on vérifie que $ac\pm bd$ et $ad\mp bc$ sont premiers à p et à q. Le symbole de Jacobi $(pq/(ac\pm bd))$ est défini et vaut 1, donc $((ac+bd)/p)=((ac+bd)/q)$, quelque soient les signes de a, b, c et d.

Les formes ambiguës simples de déterminant pq sont (si $p<q$):

$$[1, 0, -pq],\ [-1, 0, pq],\ [p, 0, -q] \text{ et } [-p, 0, q]\approx[q, 0, -p].$$

Elles se groupent deux par classe ambiguë, donc $[1, 0, -pq]$ *représente un et un seul des nombres* $p, q, -1$.

Si $[1, 0, -pq]$ *représente* q: $\mathcal{A}$ contient $[-1, 0, pq]$ et $[p, 0, -q]$. La proposition 1 montre que une racine carrée de $\mathcal{A}$ est $\varphi=[ac+bd, ad-bc, -ac-bd]$ donc $h(pq)\equiv 0$ où $4 \pmod 8$ suivant que $((ac+bd)/p)=1$ où -1.

D'autre part, soit w le premier coefficient, choisi premier à $2pq$, d'une forme racine carrée de $\mathcal{A}$ (ici $ac+bd$ conviendrait). w^2 est représenté par $\mathcal{A}$,

donc $w^2=px^2-qy^2$ où, nécessairement, x est impair, y pair premier à p: $y=2^hz$ et on voit que, si $p\equiv 5 \pmod 8$, $h=1$, d'où résulte: $(2^h/p)=(2/p)=(-1)^{(p-1)/4}$. Calculons (w/p):

$$\left(\frac{w}{p}\right)=(-1)^{(p-1)/4}\left(\frac{2^h}{p}\right)\left(\frac{z}{p}\right)\left(\frac{q}{p}\right)_4=\left(\frac{p}{z}\right)\left(\frac{q}{p}\right)_4=\left(\frac{q}{p}\right)_4.$$

D'autre part, $t^2-pqu^2=q$ a des solutions. Dans ce cas Dirichlet savait déjà que $(p/q)_4=1$: q divise t, d'où $1=qx^2-pu^2$, cas $w=1$ du calcul ci-dessus. Donc:

$$\left(\frac{p}{q}\right)_4=1 \quad et \quad \left(\frac{ac+bd}{p}\right)=(-1)^{h(pq)/4}=\left(\frac{q}{p}\right)_4.$$

Si $[1, 0, -pq]$ *représente* -1: $\mathcal{A}$ contient $[p, 0, -q]$ et $[q, 0, -p]$. La proposition 1 montre que $\varphi=[ac+bd, \cdots, \cdots]$ est dans une classe ambiguë, $\mathcal{T}$ ou $\mathcal{A}$. $\mathcal{T}$ et $\mathcal{A}$ sont dans le genre principal, donc $((ac+bd)/p)=1$.

Soit w, choisi premier à $2pq$, le premier coefficient d'une forme racine carrée de $\mathcal{A}$. Cette fois $w^2=px^2-qy^2=qx'^2-py'^2$, donc, comme plus haut:

$$\left(\frac{w}{p}\right)=\left(\frac{q}{p}\right)_4=\left(\frac{p}{q}\right)_4, \quad \text{et} \quad \left(\frac{w}{p}\right)=(-1)^{h(pq)/4}.$$

Résumons:

Si t^2-pqu^2 représente p: $\left(\frac{q}{p}\right)_4=1$ et $\left(\frac{p}{q}\right)_4=\left(\frac{ac+bd}{p}\right)=(-1)^{h(pq)/4}$
Si t^2-pqu^2 représente q: $\left(\frac{p}{p}\right)_4=1$ et $\left(\frac{q}{p}\right)_4=\left(\frac{ac+bd}{p}\right)=(-1)^{h(pq)/4}$
Si t^2-pqu^2 représente -1: $\left(\frac{p}{q}\right)_4=\left(\frac{q}{p}\right)_4=(-1)^{h(pq)/4}$ et $\left(\frac{ac+bd}{p}\right)=1$

Dans ce tableau, on lit trois théorèmes:

THÉORÈME 5. *$h(pq)$ est divisible par 8 si, et seulement si, $(p/q)_4=(q/p)_4=1$.*

THÉORÈME 6. *$(p/q)_4(q/p)_4=((ac+bd)/p)$.*

THÉORÈME 7. *Si $(p/q)_4=(q/p)_4=-1$, t^2-pqu^2 représente -1.*
Si $(p/q)_4=1$ et $(q/p)_4=-1$, t^2-pqu^2 représente q.
Si $(p/q)_4=-1$ et $(q/p)_4=1$, t^2-pqu^2 représente p.

§7. Cas d'un déterminant $D=-pq$, où $p\equiv -q\equiv 1 \pmod 4$ et $(p/q)=(q/p)=1$.

Comme dans le cas $D=pq$, on voit qu'il existe w, premier à $2pq$, tel que $w^2=px^2+qy^2$, où x est impair, $y=2^hz$, $(2^h/p)=(2/p)$. Alors:

$$\left(\frac{w}{p}\right)=\left(\frac{q}{p}\right)_4\left(\frac{y}{p}\right)=\left(\frac{q}{p}\right)_4\left(\frac{2}{p}\right)\left(\frac{z}{p}\right)=\left(\frac{4q}{p}\right)_4\left(\frac{p}{z}\right)=\left(\frac{4q}{p}\right)_4=\left(\frac{-q}{p}\right)_4$$

car, comme $p \equiv 1 \pmod 4$, $(-1/p)_4 = (-1)^{(p-1)/4} = (2/p) = (4/p)_4$, d'où : $(-4/p)_4 = 1$, donc : $(-1)^{h(-pq)/4} = (-q/p)_4$, c'est à dire :

THÉORÈME 8. *$h(-pq)$ est divisible par 8 si, et seulement si, $(-q/p)_4 = 1$.*

§ 8. Remarques.

a) Les Théorèmes 5 et 8 sont des conséquences d'un résultat de Redei ([**16**], Satz II, page 138). La démonstration de [**16**], beaucoup plus compliquée, utilise la théorie du corps de classes. On peut démontrer une grande partie des résultats de [**16**] par notre méthode. On notera que la démonstration des Théorèmes 5 et 8 est indépendante des considérations concernant $((ac+bd)/p)$, ce qui permet de la généraliser aux cas du Satz II de [**16**].

b) Le Théorème 6 est la " Loi de Réciprocité Biquadratique Rationnelle " de K. Burde [**5**], dont nous avons obtenu ainsi une nouvelle démonstration, indépendante de la loi de Réciprocité Biquadratique. On passe de la formulation de [**5**] : $(p/q)_4(q/p)_4 = (-1)^{(p-1)/4}((ad-bc)/p)$, à la nôtre en remarquant que $a(ac+bd) \equiv b(ad-bc) \pmod p$, et que ab^{-1} est un carré modulo p si, et seulement si, $p \equiv 1 \pmod 8$.

Il résulte du Théorème 6 que $((ac+bd)/p)$ ne dépend pas des signes de a, b, c et d. Pour démontrer ceci directement, il suffit de vérifier que $((a^2c^2-b^2d^2)/p) = 1$. En effet : $a^2c^2-b^2d^2 \equiv a^2c^2+(a^2+b^2)d^2-b^2d^2 = a^2q \pmod p$, et $(q/p) = 1$.

c) Le Théorème 7 est un résultat de E. Brown [**4**]. La démonstration de [**4**] suppose connu le Théorème 6, et utilise un résultat équivalent à " $((ac+bd)/p) = 1$ quand $[1, 0, -pq]$ représente -1 " démontré à l'aide des " Diagrammes de Cantor " (Cf. aussi [**20**]).

d) L'idée d'utiliser systématiquement la Proposition 0 est due à G. Pall [**14**]. On peut déduire notre Proposition 2 des Théorèmes 3 et 4 de [**14**] mais notre démonstration est beaucoup plus simple.

e) G. Gras [**19**] obtient par une autre méthode le critère suivant : *Soit* $p \equiv 1 \pmod 8$, $p = 2e^2-d^2 = u^2+2v^2 = a^2+b^2$. $h(2p) \equiv 0 \pmod 8$ *si et seulement si* $d^2 \equiv u^2 \equiv 1 \pmod{16}$. Vérifions que ce critère est équivalent à notre Théorème 1 : un raisonnement élémentaire (Cf. [**9**], page 168) montre que $(-1)^{(|e|-1)/2} = (-1)^{v/2}$, donc $(2/(a+b)) = (-1)^{v/2}$, et nous avons vu que $(2/a) = (2/d)$. Si $a \equiv \pm 1$ et $b \equiv 0 \pmod 8$, alors $p \equiv d^2 \equiv 1 \pmod{16}$ et $v^2 \equiv 0 \pmod{16}$, donc $u^2 \equiv 1 \pmod{16}$. Inversement, si $d^2 \equiv u^2 \equiv 1 \pmod{16}$, alors $a \equiv \pm 1 \pmod 8$ donc $p \equiv 1 \pmod{16}$, d'où $2v^2 \equiv 0 \pmod{16}$ et $v \equiv 0 \pmod 4$, donc $a+b \equiv \pm 1 \pmod 8$ et $b \equiv 0 \pmod 8$.

f) EXEMPLES. Le plus petit p tel que $h(2p)$ soit divisible par 8 est $113 = 7^2+8^2$, et $h(226) = 8$. Il y a 41 valeurs de $2p < 10000$ telles que $h(2p) \equiv 0 \pmod 8$ et parmi les 31 telles que $2p < 8191$, $h(2p) = 16$ pour $p = 1217$, 2593, 3089, 3313, et 3361, $h(2p) = 24$ pour $4049 = 55^2+32^2$, $h(2p) = 8$ pour les autres.

Il y a 35 nombres $pq<10000$ tels que $p\equiv q\equiv 1 \pmod 4$, $(p/q)=1$, $h(pq)\equiv 0 \pmod 8$. Le plus petit est $pq=505$. Parmi les 26 de ces nombres $pq<8191$, $h(pq)=16$ pour $5249=29.181$ et $5513=37.149$, $h(pq)=8$ pour les autres.

Ces résultats sont tirés de la table de L. Bouvier [**18**] et d'une table de $h(D)$ pour $1<D\leqq 8191$ communiquée par H. Wada.

§ 9. Complément.

Dans les cas $D=\pm pq$, nous avons vu que certains des nombres w premiers à $2pq$, solution, suivant le cas, de $w^2=px^2-qy^2$, ou $w^2=qx'^2-py'^2$, ou $w^2=px^2+qy^2$, déterminent la divisibilité par 8 de $h(D)$ par: $(-1)^{h(D)/4}=(w/p)$; ces w sont ceux qui sont premier coefficient d'une racine carré de $\mathcal{A}$.

Réciproquement, tout w solution de l'équation convenable vérifie $(-1)^{h(D)/4}=(w/p)$ car *si* $w^2=px^2\pm qy^2$ *avec* $(x, y)=1$ *alors* w *est premier coefficient d'un racine carrée de* $[p, 0, \mp q]$.

En effet, comme $(w, 2p)=(x, y)=1$, $(x, w)=(y, w)=1$, et la forme $\varphi=[w, px, pw]$ est proprement primitive, a pour déterminant $(px)^2-pw^2=\pm pqy^2$, et $\varphi^2=[w^2, px, p]\approx[p, 0, \mp qy^2]$. Comme $(y, w)=1$, il existe B telque $By\equiv px \pmod w$ si bien que φ est équivalente à une forme $[w, By, Cy^2]$. Or il existe un homomorphisme du groupe des classes (proprement primitives) de déterminant Dy^2 sur celui, (C), des classes de déterminant D, dans lequel l'image de $[w, By, Cy^2]$ est $[w, B, C]$, et, celle de $[p, 0, \mp qy^2]$ est $[p, 0, \mp q]$ (Cf. [**13**] Chapitre, 6, § 7 ou [**15**], page 26). Donc $[w, B, C]^2\approx[p, 0, \mp q]$.

C. Q. F. D.

Ainsi nous obtenons le:

THÉORÈME 9. *Soit* $D=\pm pq$, $p\equiv\pm q\equiv 1 \pmod 4$ *et* $(p/q)=(q/p)=1$, *et soit* (w, x, y) *une solution où* w *est premier à* $2pq$ *de:*

a) $w^2=px^2+qy^2$, *si* $D=-pq$ $(q\equiv -1 \pmod 4)$.

b) $w^2=px^2-qy^2$, *si* $D=pq$ *et si* $t^2-pqu^2=q$ *a des solutions.*

c) $w^2=px^2-qy^2$ *ou* $w^2=qx'^2-py'^2$, *si* $D=pq$ *et si* $t^2-pqu^2=-1$ *a des solutions.*

Alors: $(-1)^{h(D)/4}=(w/p)=(p/w)$.

Ce critère, et sa démonstration, est analogue au critère de H. Hasse [**11**]. Pour obtenir exactement le critère de (11) il suffit de raisonner dans le groupe des classes de formes "improprement primitives" de déterminant D (formes $[A, B, C]$ où $(A, B, C)=1$ et $(A, 2B, C)=2$), ce qui est normal, car c'est ce groupe qui, quand $D\equiv 1 \pmod 4$, est isomorphe au groupe des classes de $\boldsymbol{Q}(\sqrt{D})$. Vérifions-le dans le cas où $D=-pq$: $\mathcal{A}$ contient $[2p, p, (q+p)/2]$, et, si $2v$, où $(v, 2pq)=1$, est le premier coefficient d'une racine carrée de $\mathcal{A}$: $2v^2=2px^2+2pxy+((p+q)/2)y^2$, donc: $4pv^2=X^2-Dy^2$, avec $X=2px+py$: c'est

l'équation (11) de [11]. On voit ensuite, comme plus haut, que pour tout v solution de cette équation, $(-1)^{h(D)/4}=(v/p)$.

§ 10. Comparaison des Lois de Réciprocité Biquadratique Rationnelle et Complexe.

Soient p et q deux nombres premiers, $p\equiv q\equiv 1 \pmod 4$, $p=a^2+b^2$, $q=c^2+d^2$ avec $a\equiv c\equiv 1 \pmod 4$, ce qui détermine les signes de a et c. Soit $m=a+bi$, $n=c+di$, $m'=a-bi$, $n'=c-di$. Le symbole biquadratique complexe $(x/m)_4$ est une puissance de i, définie par $x^{(p-1)/4}\equiv(x/m)_4 \pmod m$.

Soit un nombre premier $r\equiv -1 \pmod 4$. Le symbole biquadratique complexe $(x/r)_4$ est la puissance de i définie par $x^{(r^2-1)/4}\equiv(x/r)_4 \pmod r$.

La loi de réciprocité biquadratique consiste essentiellement en les deux formules:

$$(1):\ \left(\frac{m}{n}\right)_4\left(\frac{m}{n'}\right)_4=\left(\frac{q}{m}\right)_4 \qquad \text{et} \qquad (2):\ \left(\frac{m}{r}\right)_4=\left(\frac{-r}{m}\right)_4.$$

La formule plus connue

$$(3):\ \left(\frac{m}{n}\right)_4\left(\frac{n}{m}\right)_4=(-1)^{((p-1)/4)((q-1)/4)}$$

se démontre à partir de (1) et (2) par des calculs formels faciles (Cf. [8], page 65 et [12], page 134 et 143).

1) *Supposons* $(p/q)=(q/p)=1$. Comme toute classe modulo m a un représentant réel, le symbole biquadratique réel $(p/q)_4$ est égal à $(p/n)_4$. Le Théorème 6 s'écrit donc:

$$(4):\ \left(\frac{ac+bd}{p}\right)=\left(\frac{q}{m}\right)_4\left(\frac{m}{n}\right)_4\left(\frac{m'}{n}\right)_4.$$

$(m'/n)_4$ et $(m/n')_4$ sont conjugués, donc égaux ou opposés suivant que leurs carrés valent 1 ou -1. Or le carré de $(m/n')_4$ est le symbole quadratique complexe $[m/n']$ de Dirichlet, qui vaut $((ac-bd)/p)$, ce qui est très facile à prouver (Cf. [6], page 554). Comme $(p/q)=(q/p)=1$ nous savons que $((ac-bd)/p)=((ac+bd)/p)$, et donc, portant dans (4) on trouve la formule (1). Ce raisonnement peut se faire en sens inverse, donc *la Loi de Réciprocité Biquadratique Rationnelle* (Théorème 6) *est équivalente au cas* $(p/q)=(q/p)=1$ *de la formule* (1).

2) *Supposons* $(p/q)=(q/p)=-1$. Le raisonnement précédent montre que $(m/n')_4=((ac-bd)/p)(m'/n)_4$, donc, remplaçant dans la formule (1) on trouve ici:

$$\left(\frac{q}{m}\right)_4\left(\frac{p}{n}\right)_4=-\left(\frac{ac-bd}{p}\right)=\left(\frac{ac+bd}{p}\right).$$

Rappelons que les classes biquadratiques modulo p de "numéro k", définies

pour les entiers réels x d'une part par $x^{(p-1)/4} \equiv i^k \pmod m$, et d'autre part par $x^{(p-1)/4} \equiv f^k \pmod p$, coïncident si f est la racine carrée de -1 modulo p définie par $a+bf \equiv 0 \pmod p$ (car, alors, $f \equiv i \pmod m$). On obtient donc, avec les conventions précédentes:

THÉORÈME 10. *Si* $(p/q)=(q/p)=-1$, *les numéros* (1 ou 3) *des classes biquadratiques de p modulo q et de q modulo p sont égaux ou diffèrent de* 2 *suivant que* $((ac-bd)/p)$ *vaut* 1 *ou* -1, *ou encore, suivant que* $ac-bd$ *est ou non représenté par* $[1, 0, -pq]$.

3) Pour conclure, remarquons que la formule (2) donne le critère suivant: *Soit* $D=-pr$, $p \equiv -r \equiv 1 \pmod 4$. *Alors:* $(-1)^{h(D)/4}=(-r/p)_4=(m/r)_4$.

Bibliographie

[1] P. Barrucand et H. Cohn, Note on primes of type x^2+32y^2, class number, and residuacity, J. reine angew. Math., **238** (1969), 67-70.

[2] E. Brown, Representations of Discriminantal Divisors by Binary Quadratic Forms, J. Number Theory, **3** (1791), 213-225.

[3] E. Brown, The class number of $\boldsymbol{Q}(\sqrt{-p})$, for $p \equiv 1 \pmod 8$ a prime, Proc. Amer. Math. Soc., **31** (1972), 381-383.

[4] E. Brown, Binary Quadratic Forms of Determinant $-pq$, J. Number Theory, **4** (1972), 408-410.

[5] K. Burde, Ein rationales biquadratisches Reziprozitätsgesetz, J. reine und angew. Math., **235** (1969), 175-184.

[6] P. G. L. Dirichlet, Werke I, (Chelsea).

[7] C. F. Gauss, Disquisitiones Arithmeticae.

[8] C. F. Gauss, Werke, Tome 10_1.

[9] H. Hasse, Über die Klassenzahl des Körpers $\boldsymbol{P}(\sqrt{-p})$ mit einer Primzahl $p \equiv 1 \bmod 2^3$, Aequationes Math., **3** (1969), 165-169.

[10] H. Hasse, Über die Klassenzahl des Körpers $\boldsymbol{P}(\sqrt{-2p})$ mit einer Primzahl $p \neq 2$, J. Number Theory, **1** (1969), 231-234.

[11] H. Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, Math. Nachrichten, **46** (1970), 61-70.

[12] P. Kaplan, Démonstration des lois de réciprocité quadratique et biquadratique, J. Fac. Sc. Univ. Tokyo, **16** (1969), 115-145.

[13] P. Kaplan, Cours d'Arithmétique, U. E. R. de Mathématiques, Nancy (1972).

[14] G. Pall, Discriminantal Divisors of Binary Quadratic Forms, J. Number Theory, **1** (1969), 525-533.

[15] H. S. Butts et G. Pall, Modules and binary quadratic forms, Acta Arithmetica, **15** (1968), 23-44.

[16] L. Redei, Über die Grundeinheit und die durch 8 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. reine und angew. Math., **171** (1934), 131-148.

[17] A. Scholz et B. Schöneberg, Einführung in die Zahlentheorie, Sammlung Göschen 1131 (1966).

[18] L. Bouvier, Table des 2-rang, 4-rang et 8-rang du 2-groupe des classes d'idéaux

au sens restreint de $\boldsymbol{Q}(\sqrt{m})$, Institut de Mathématiques pures, Grenoble (1971).
[19] G. Gras, Problèmes de 1-classes d'idéaux dans les extensions cycliques relatives de degré premier l, Thèse, Grenoble (1972).
[20] A. Scholz, Über die Lösbarkeit der Gleichung $t^2-Du^2=-4$, Math. Zeitschrift, **39** (1935), 95-111.

Pierre KAPLAN
9, rue des Soeurs Macarons
54000-Nancy
France