Sur les nombres de classes de certains corps quadratiques.

Autor(en): **Humbert, Pierre**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **12 (1939-1940)**

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-12805

Sur les nombres de classes de certains corps quadratiques

Par Pierre Humbert, Lausanne

Le but de ce travail est de montrer comment on peut construire une infinité de corps quadratiques imaginaires dans lesquels le groupe des classes d'idéaux contient un élément d'ordre donné g. La méthode employée s'inspire de la théorie classique des corps de nombres algébriques, telle qu'on la trouve exposée par exemple dans le livre de Hecke[1]).

§ 1. Densité des nombres sans diviseurs carrés

Soient x un nombre réel positif, et Q un entier rationnel. Nous allons déterminer le nombre $N(x, Q)$ des entiers sans diviseurs carrés, ne dépassant pas x et premiers à Q.

Supposons d'abord $Q = 1$. Il s'agit de déterminer le nombre $N(x, 1) = N(x)$ des entiers $n \leqslant x$ sans diviseurs carrés. La même méthode permettra ensuite de trouver $N(x, Q)$.

Si m est un entier quelconque, il est clair que $\left[\frac{x}{m^2}\right]$ représente le nombre des $n \leqslant x$ divisibles par m^2. Soit $a_n^{(1)}$ le nombre des différents p^2, p premier, par lesquels n est divisible. On a

$$\sum_p \left[\frac{x}{p^2}\right] = \sum_{n \leq x} a_n^{(1)}$$

car la somme $\sum_p \left[\frac{x}{p^2}\right]$ étendue à tous les p premiers est le nombre des $n \leqslant x$ divisibles par un p^2, chaque n étant compté $a_n^{(1)}$ fois.

Si $n = \Pi p_i^{g_i}$ est la décomposition de n en facteurs premiers, on a

$$a_n^{(1)} = r(n) = \text{nombre de } g_i \geqslant 2 .$$

De même

$$\sum_{p_i \neq p_j} \left[\frac{x}{p_i^2 \, p_j^2}\right] = \sum_{n \leq x} a_n^{(2)}$$

où $a_n^{(2)}$ est le nombre des différents facteurs $p_i^2 \cdot p_j^2$, $p_i \neq p_j$ premiers, par lesquels n est divisible. D'une façon générale on a

[1]) *E. Hecke:* Vorlesungen über die Theorie der algebraischen Zahlen. Leipzig, 1923.

$$\sum_{p_1,\dots,p_k}\left[\frac{x}{p_1^2\cdots p_k^2}\right]=\sum_{n\le x}a_n^{(k)}$$

où $a_n^{(k)}$ est le nombre des différents facteurs de la forme $p_1^2\dots p_k^2$, $p_i\neq p_j$ premiers, par lesquels n est divisible. On a évidemment

$$a_n^{(k)}=\binom{r}{k}$$

où $r=r(n)=$ nombre de facteurs premiers entrant dans n à une puissance supérieure à la première.

Considérons alors l'expression

$$[x]-\sum_p\left[\frac{x}{p^2}\right]+\sum_{p_1\neq p_2}\left[\frac{x}{p_1^2p_2^2}\right]-\sum_{p_1,p_2,p_3}\left[\frac{x}{p_1^2p_2^2p_3^2}\right]+\cdots=$$

$$=\sum_{n\le x}\left(1-a_n^{(1)}+a_n^{(2)}-a_n^{(3)}+\cdots\right).$$

Dans le 2ème membre, la somme

$$\nu(n)=1-a_n^{(1)}+a_n^{(2)}-a_n^{(3)}+\cdots=1-\binom{r}{1}+\binom{r}{2}-\binom{r}{3}+\cdots$$

est égale à 0 si $r>0$ et à 1 si $r=0$, c'est-à-dire si n est sans diviseurs carrés. La somme $\sum_{n\le x}\nu(n)$ représente le nombre $N(x)$ des $n\leqslant x$ sans diviseurs carrés. On a donc

$$N(x)=[x]-\sum_p\left[\frac{x}{p^2}\right]+\sum_{p_1\neq p_2}\left[\frac{x}{p_1^2p_2^2}\right]-\cdots. \tag{1}$$

Le nombre des termes non nuls de cette somme est au plus égal au nombre des carrés $\leqslant x$, car à chaque terme $\left[\frac{x}{p_1^2\cdots p_k^2}\right]>0$ correspond un carré $p_1^2\dots p_k^2\leqslant x$ bien déterminé, et à 2 termes différents correspondent 2 carrés différents. Le nombre de ces termes non nuls est donc $\leqslant\sqrt{x}$.

Comparons $N(x)$ avec la somme infinie et convergente

$$x-\sum_p\frac{x}{p^2}+\sum_{p_1\neq p_2}\frac{x}{p_1^2p_2^2}-\cdots=x\prod_p\left(1-\frac{1}{p^2}\right)=\frac{x}{\zeta(2)}. \tag{2}$$

L'erreur que l'on commet en prenant $\frac{x}{\zeta(2)}$ pour valeur de $N(x)$ provient de 2 causes:

1° Du fait que l'on a remplacé les termes $\left[\frac{x}{p_1^2\cdots p_k^2}\right]>0$ par $\frac{x}{p_1^2\cdots p_k^2}$;

l'erreur ainsi commise ne dépasse pas 1 pour chacun de ces termes, et leur nombre est au plus $\sqrt{x}$; on a ainsi une erreur $\theta\sqrt{x}$, $|\theta| \leqslant 1$.

2° Du fait que la somme (2) contient une infinité de termes qui se réduisent à 0 dans (1), tous ceux pour lesquels $\frac{x}{p_1^2 \cdots p_k^2} < 1$. Soit $\varrho(x)$ l'erreur ainsi commise. En valeur absolue cette erreur ne dépasse pas $2\sqrt{x}$ pour $x \geqslant 4$, car

$$|\varrho(x)| \leqslant \sum_{p^2>x} \frac{x}{p^2} + \sum_{p_1^2 p_2^2 > x} \frac{x}{p_1^2 p_2^2} + \cdots < x \sum_{n^2>x} \frac{1}{n^2} < x \int_{\sqrt{x}-1}^{\infty} \frac{dt}{t^2} < 2\sqrt{x} \text{ si } x \geqslant 4.$$

On peut donc écrire

$$N(x) = \frac{x}{\zeta(2)} + \theta_1 \sqrt{x} \quad \text{avec} \quad |\theta_1| \leqslant 3 . \tag{3}$$

(Pour $x < 4$ on vérifie numériquement la validité de la formule (3) sachant que $\zeta(2) = \frac{\pi^2}{6}$) .

Supposons maintenant $Q > 1$:

$$Q = q_1 q_2 \cdots q_t \quad , \quad q_i \text{ premier}, \ q_i \neq q_j .$$

Evaluons d'abord le nombre $Q(x)$ des entiers premiers à Q et ne dépassant pas x. Posons $\gamma = \frac{\varphi(Q)}{Q}$. Si x est un multiple entier de Q, on aura

$$Q(x) = \gamma x .$$

Si x est quelconque, on voit par des considérations identiques à celles qui ont conduit à la formule (1) que

$$Q(x) = [x] - \sum_{q/Q} \left[\frac{x}{q}\right] + \sum_{q_1 q_2/Q} \left[\frac{x}{q_1 q_2}\right] - \cdots . \tag{4}$$

(La notation q/Q signifie q *divise* Q.)

En supprimant les crochets, on obtient $x \prod_{q/Q} \left(1 - \frac{1}{q}\right) = x\gamma$ dans le 2ème membre de (4); l'erreur commise est au plus égale au nombre des termes entre crochets de ce 2ème membre, donc à 2^t, où t = nombre de facteurs premiers de Q. Donc

$$Q(x) = \gamma x + \theta \qquad \text{avec} \qquad |\theta| \leqslant 2^t . \tag{5}$$

Nous sommes alors en mesure d'évaluer le nombre $N(x, Q)$ des entiers sans diviseurs carrés, premiers à Q et $\leqslant x$.

Le nombre des entiers premiers à Q, divisibles par $p_1^2 \ldots p_k^2$, $(p_1 \ldots p_k, Q) = 1$, et ne dépassant pas x est égal au nombre des n tels que

$$n p_1^2 \ldots p_k^2 \leqslant x \qquad (n, Q) = 1$$

donc au nombre

$$Q\left(\frac{x}{p_1^2 \ldots p_k^2}\right) .$$

Si $A_n^{(k)}$ représente le nombre des facteurs $p_1^2 \ldots p_k^2$, $(p_1 \ldots p_k, Q) = 1$, par lesquels n est divisible, on aura comme précédemment

$$\sum_{\substack{(p_1 \ldots p_k, Q)=1 \\ p_1^2 \ldots p_k^2 \leq x}} Q\left(\frac{x}{p_1^2 \ldots p_k^2}\right) = \sum_{\substack{(n, Q)=1 \\ n \leq x}} A_n^{(k)} \qquad A_n^{(k)} = \binom{A_n^{(1)}}{k} .$$

Formons alors l'expression

$$Q(x) - \sum_{\substack{(p, Q)=1 \\ p^2 \leq x}} Q\left(\frac{x}{p^2}\right) + \sum_{\substack{(p_1 p_2, Q)=1 \\ p_1^2 p_2^2 \leq x}} Q\left(\frac{x}{p_1^2 p_2^2}\right) - \cdots = \sum_{\substack{(n, Q)=1 \\ n \leq x}} (1 - A_n^{(1)} + A_n^{(2)} - \cdots) \tag{6}$$

La somme alternée $1 - A_n^{(1)} + A_n^{(2)} - \cdots$ est égale à 1 si $A_n^{(1)} = 0$ et à 0 si $A_n^{(1)} > 0$. L'expression (6) représente donc le nombre cherché $N(x, Q)$. En remplaçant les $Q(y)$ par leurs valeurs (5), on obtient

$$N(x, Q) = \gamma x - \gamma \sum_{\substack{(p, Q)=1 \\ p^2 \leq x}} \frac{x}{p^2} + \gamma \sum_{\substack{(p_1 p_2, Q)=1 \\ p_1^2 p_2^2 \leq x}} \frac{x}{p_1^2 p_2^2} - \cdots + \varrho(x, Q) . \tag{7}$$

L'erreur $\varrho(x, Q)$ est en valeur absolue au plus égale à 2^t multiplié par le nombre des termes $Q(y)$ dans (6), nombre inférieur, on l'a vu, à $\sqrt{x}$:

$$|\varrho(x, Q)| \leqslant 2^t \sqrt{x} .$$

En sommant dans le second membre de (7) sur tous les p premiers à Q, on commet une nouvelle erreur inférieure en valeur absolue au reste de la série $\gamma \Sigma \frac{x}{n^2}$ pour $n^2 > x$, donc inférieure à $2\sqrt{x}$ pour $x \geqslant 4$. On obtient ainsi en définitive

$$N(x, Q) = \gamma x \prod_{(p, Q)=1} \left(1 - \frac{1}{p^2}\right) + \psi(x, Q) \quad |\psi(x, Q)| \leqslant (2^t + 2)\sqrt{x} . \tag{8}$$

La densité des nombres sans diviseurs carrés et premiers à Q, c'est-à-dire la limite de $\frac{N(x,Q)}{x}$ pour $x\to\infty$ est

$$\lim_{x\to\infty}\frac{N(x,Q)}{x}=\gamma\prod_{(p,Q)=1}\left(1-\frac{1}{p^2}\right)=\frac{1}{\zeta(2)\prod_{p/Q}\left(1+\frac{1}{p}\right)}\qquad \zeta(2)=\frac{\pi^2}{6}.$$

Rappelons qu'on avait posé $\gamma=\frac{\varphi(Q)}{Q}=\prod_{p/Q}\left(1-\frac{1}{p}\right)$. Par exemple, la densité des nombres impairs sans diviseurs carrés est $\frac{4}{\pi^2}$. On voit que parmi les nombres sans diviseurs carrés il y a 2 fois plus de nombres impairs que pairs, ce qu'on peut d'ailleurs prévoir a priori en supposant l'existence de densités pour ces nombres.

§ 2. Construction de corps quadratiques imaginaires dont le nombre des classes h est divisible par un nombre donné g

Un nombre D est discriminant d'un corps quadratique dans l'un des deux cas suivants:

$D\equiv 1\pmod 4$ et D sans diviseurs carrés.

$D\equiv 0\pmod 4$, $\frac{D}{4}\equiv 2,3\pmod 4$ et $\frac{D}{4}$ sans diviseurs carrés.

Un nombre $A\equiv 0,1\ (mod\ 4)$ se met d'une façon unique sous la forme $A=a^2D$, où $D=$ discriminant d'un corps quadratique. En effet mettons A sous la forme $A=a^2d$, d sans diviseurs carrés, donc $d\equiv 1,2,3\pmod 4$. Si $d\equiv 1\pmod 4$ le discriminant cherché est $D=d$. Si $d\equiv 2,3\pmod 4$, le nombre a est pair, car sinon on aurait $a^2\equiv 1\pmod 4$ d'où $A\equiv 2,3\pmod 4$, ce qui n'est pas. Alors $A=4b^2d$ et le discriminant est $D=4d$.

Les nombres entiers du corps $K=R(\sqrt{D})$, obtenu en adjoignant au corps des nombres rationnels R la quantité $\sqrt{D}$, sont de la forme

$$\frac{x+y\sqrt{D}}{2}\qquad x,y=\text{entiers rationnels.}$$

Réciproquement un nombre de la forme $\frac{x+y\sqrt{D}}{2}$ n'est entier que si $x\equiv y\pmod 2$ dans le cas $D\equiv 1\pmod 4$, et si $x\equiv 0\pmod 2$ dans le cas $D\equiv 0\pmod 4$.

Cela rappelé, nous démontrons le

Théorème 1. Soit $g > 0$ un entier donné, q son plus petit facteur premier. a et $P > 1$ étant 2 nombres premiers entre eux, considérons le discriminant D de corps quadratique défini par

$$a^2 - 4P^g = b^2 D \ . \tag{9}$$

Si $D \leqslant -4P^{\frac{g}{q}}$ le nombre des classes du corps $K = R(\sqrt{D})$ est divisible par g.

D'après les lois de décomposition dans le corps K, et à cause de (9), on voit que chacun des facteurs premiers p_i de P se décompose dans K en deux facteurs idéaux premiers différents.

On a

$$P^g = \frac{a + b\sqrt{D}}{2} \cdot \frac{a - b\sqrt{D}}{2} \ .$$

Décomposons dans K l'idéal principal et entier $\left(\frac{a + b\sqrt{D}}{2}\right)$ en ses facteurs premiers:

$$\left(\frac{a + b\sqrt{D}}{2}\right) = \Pi \mathfrak{p}_i^{m_i} \ . \tag{10}$$

L'accent désignant l'idéal conjugué, on a

$$\mathfrak{p}_i \neq \mathfrak{p}_j' \ .$$

Pour $i = j$ c'est vrai car $\mathfrak{p}_i | P$. Pour $i \neq j$, c'est vrai également, car sinon l'idéal $\left(\frac{a + b\sqrt{D}}{2}\right)$ serait divisible par un facteur $\mathfrak{p}\mathfrak{p}' = (p)$. Le nombre $\alpha = \frac{a + b\sqrt{D}}{2p}$ devrait être entier. Pour $p > 2$ cela est impossible, car on a $(a, b) \leqslant 2$ puisque $(a, P) = 1$. Pour $p = 2$ c'est aussi impossible; en effet on aurait alors $2 | P$, donc $a \equiv 1 \pmod 2$ à cause de $(a, P) = 1$, et le nombre $\alpha = \frac{a + b\sqrt{D}}{4}$ de trace $\frac{a}{2}$ ne serait pas entier. En prenant les normes dans (10) on obtient

$$P^g = \Pi N \mathfrak{p}_i^{m_i} = \Pi p_i^{m_i} \ .$$

On a $p_i = N\mathfrak{p}_i \neq N\mathfrak{p}_j = p_j$ si $i \neq j$ puisque $\mathfrak{p}_i \neq \mathfrak{p}_j'$. Les p_i sont les facteurs premiers de $P = \Pi p_i^{n_i}$. D'où

$$m_i = g n_i \ .$$

Considérons l'idéal $\mathfrak{a} = \Pi \mathfrak{p}_i^{n_i}$ de norme $N\mathfrak{a} = P$. L'idéal $\mathfrak{a}^g = \left(\frac{a + b\sqrt{D}}{2}\right)$ est principal. Montrons que $\mathfrak{a}^k$ n'est pas principal si $k \leqslant \frac{g}{q}$. En effet, supposons $\mathfrak{a}^k$ principal:

$$\mathfrak{a}^k = \left(\frac{x + y\sqrt{D}}{2}\right) \quad x,\ y \text{ entiers rationnels.}$$

$x \neq 0$ car $(\mathfrak{a}, D) = 1$, ce qui résulte de $(P, D) = (P, a) = 1$. $y \neq 0$ car on a vu que $\mathfrak{a}$ n'est divisible par aucun entier rationnel, donc $\mathfrak{a}^k$ non plus; en outre $\mathfrak{a} \neq (1)$ puisque $N\mathfrak{a} = P > 1$.

En prenant les normes, on trouve

$$P^k = \frac{x^2 - y^2 D}{4} .$$

Or par hypothèse $-\frac{D}{4} \geqslant P^{\frac{g}{q}}$; on en déduit, à cause de $x \neq 0$, $|y| \geqslant 1$:

$$P^k > P^{\frac{g}{q}} \quad \text{donc} \quad k > \frac{g}{q} .$$

Il s'ensuit que *l'ordre de* $\mathfrak{a}$ *dans le groupe des classes est égal à* g. Car $\mathfrak{a}^g$ étant principal, cet ordre est un diviseur de g; or le plus grand diviseur de g (différent de g) est $\frac{g}{q}$, et $\mathfrak{a}^k$ n'est pas principal pour $k \leqslant \frac{g}{q}$. c.q.f.d.

Remarques. La condition $(a, P) = 1$ est essentielle, comme on le voit avec l'exemple suivant:

$$g = 3, \quad a = 10, \quad P = 4, \quad \text{donc } (a, P) = 2 .$$

On trouve $D = -39 < -4P$. Or le corps $R(\sqrt{-39})$ a un nombre de classes $h = 4$ non divisible par 3. Le théorème 1 montre d'ailleurs que $4|h$, car pour $g = 4$, $a = 5$, $P = 2$ on a

$$D = 5^2 - 4 \cdot 2^4 = -39 < -4 \cdot 2^2 .$$

De même l'exemple $g = 5$, $a = 11$, $P = 2$ montre la nécessité de la condition $D \leqslant -4P^{\frac{g}{q}}$, car on trouve ici $D = -7 > -8$, et $h = 1$ dans $R(\sqrt{-7})$.

Application: Construction d'une infinité de corps quadratiques imaginaires dans lesquels le nombre h des classes est divisible par un nombre premier $q > 2$ *donné.*

Appliquons le théorème 1 avec $a = 2$ si $q \equiv 3\ (4)$, $a = 2^{q+1}$ si $q \equiv 1\,(4)$. Le discriminant D est défini par

$$4\,(1 - P^q) = b^2 D, \quad P \text{ impair, si } q \equiv 3\ (4)$$
$$4\,(4^q - P^q) = b^2 D, \quad P \text{ impair, si } q \equiv 1\ (4)\ .$$

Si D est au moins égal à $4P$ en valeur absolue, on aura q/h dans le corps $R(\sqrt{D})$.

Choisissons P de sorte que les conditions suivantes soient remplies:

$P - 1$ sans diviseurs carrés; $P \not\equiv 1\ (q)$ et $P \not\equiv 7\ (8)$ si $q \equiv 3\ (4)$
$P - 4$ sans diviseurs carrés; $P \not\equiv 4\ (q)$ et $P \equiv 1\ (4)$ si $q \equiv 1\ (4)$.

Cela est possible d'une infinité de façons. Montrons que la condition $|D| \geqslant 4P$ est satisfaite. Pour cela raisonnons sur le premier cas où $q \equiv 3\ (4)$, la démonstration se fait de façon analogue dans le cas où $q \equiv 1\ (4)$. On a

$$4\,(1 - P)\ (1 + P + \cdots + P^{q-1}) = b^2 D\ .$$

Le nombre $A = 1 + P + \cdots + P^{q-1}$ est impair car P et q le sont. D'autre part A est premier à $P - 1$ car

$$(P - 1, A) = (P - 1, q) = 1\ .$$

Si A n'est pas carré, sa contribution à D est $\geqslant 3$, et l'on aura bien

$$|D| \geqslant 3 \cdot 4\,(P - 1) > 4P\ .$$

Or tout carré impair est $\equiv 1\ (8)$, et l'on a

$$A = (1+P)\ (1+P^2+\cdots+P^{2\frac{q-3}{2}}) + P^{q-1} \equiv (1+P)\,\frac{q-1}{2} + 1 \equiv 5 \qquad (8)$$

à cause de $P \equiv 3\ (8)$ et $q \equiv 3\ (4)$.

Ayant ainsi construit un corps $R(\sqrt{D})$ dans lequel $q|h$, on en construira un deuxième à l'aide d'un nombre $P_1 > \frac{|D|}{4}$ satisfaisant aux conditions énoncées; le discriminant D_1 obtenu au moyen de P_1 est tel que

$$|D_1| \geqslant 4P_1 > |D| \qquad |D_1| > |D|\ .$$

Les corps $R(\sqrt{D_1})$ et $R(\sqrt{D})$ sont différents, et en continuant de la sorte on obtient une infinité de corps $R(\sqrt{D})$ de discriminants croissants (en valeur absolue) et dans lesquels $q|h$. D'une manière plus générale, démontrons le

Théorème 2. Il existe une infinité de corps quadratiques imaginaires dont le nombre de classes h est divisible par g, g étant un nombre naturel donné quelconque.

Définissons le discriminant D par

$$4\,(a^2 - P^{2g}) = Db^2 \qquad (2\,a,\, P) = 1\ .$$

Si $D \leqslant -4\,P^g$, le nombre des classes du corps $R(\sqrt{D})$ est divisible par $2\,g$ d'après le théorème 1. Prenant pour a un nombre pair, on aura

$$\frac{Db^2}{4} = a^2 - P^{2g} \equiv 3(4)\ .$$

Le discriminant D est alors égal à $D = 4\,d$, où d est le nombre sans diviseurs carrés défini par

$$(a + P^g)\ (a - P^g) = b^2\,d\ .$$

Si le nombre impair P est assez grand, $P > C$, il existe au moins un nombre $a + P^g$ sans diviseurs carrés compris entre P^g et $2\,P^g$, impair et premier à P. En effet nous avons vu au § 1 que la densité des nombres n sans diviseurs carrés tels que

$$(n,\, 2P) = 1$$

est finie et vaut $\kappa = \dfrac{4}{\pi^2} \prod\limits_{p/P} \dfrac{p}{p+1}$.

Plus précisément, la formule (8) montre que le nombre de ces n compris entre P^g et $2\,P^g$ est

$$N = \kappa P^g + \omega \qquad \text{avec} \qquad |\omega| \leqslant (2^{t+1} + 2)\,(1 + \sqrt{2})\,P^{\frac{g}{2}}$$

t = nombre de facteurs premiers de P.

Or N tend vers l'infini en même temps que P si $g \geqslant 2$. En effet chacun des facteurs premiers de P étant au moins égal à 3, on a $t \leqslant \dfrac{\log P}{\log 3}$, et dans l'expression de $\kappa = \dfrac{4}{\pi^2} \prod\limits_{p/P} \dfrac{p}{p+1}$, les facteurs $\dfrac{p}{p+1}$ sont au moins égaux à $\dfrac{3}{4}$, ce qui donne

$$\kappa \geqslant \frac{4}{\pi^2}\,P^{1 - \frac{\log 4}{\log 3}}$$

donc

$$N \geqslant \frac{4}{\pi^2}\,P^{g+1-\frac{\log 4}{\log 3}} - 2(1+\sqrt{2})\,(P^{\frac{\log 2}{\log 3}} + 1)\,P^{\frac{g}{2}}\ .$$

Comme on a $g+1-\frac{\log 4}{\log 3} > \frac{g}{2}+\frac{\log 2}{\log 3}$ dès que $g \geqslant 2$, on voit que $N \to \infty$ si $P \to \infty$.

Il existe donc un nombre pair $a < P^g$ tel que $P^g + a$ soit sans diviseurs carrés et premier à $2P$.

Les 2 nombres $P^g + a$ et $P^g - a$ sont premiers entre eux, par conséquent $|d|$ est au moins égal à $P^g + a$, et l'on a

$$|D| = 4|d| > 4P^g .$$

Supposons qu'on ait obtenu de cette façon un corps quadratique imaginaire $R(\sqrt{D})$ dans lequel $2g/h$. A l'aide d'un nombre $P_1 > C$ tel que $4P_1^g > |D|$, on obtiendra au moins un autre corps $R(\sqrt{D_1})$, avec $2g/h_1$; ce corps est différent du précédent car

$$|D_1| > 4P_1^g > |D| .$$

En poursuivant de la sorte, on obtient bien une infinité de corps $R(\sqrt{D})$ dans lesquels $2g/h$.

§ 3. Corps quadratiques réels dans lesquels g/h

Des considérations analogues à celles du § 2 permettent de construire des corps quadratiques réels dont le nombre de classes est divisible par un nombre donné g; malheureusement l'existence effective de tels corps paraît difficile à établir ainsi.

Théorème 3. Un corps quadratique réel ayant son discriminant D défini par

$$a^2 D = 4P^{2g} + 1 , \quad P > 1 , \quad \text{avec} \quad 0 < a < P^{g\frac{q-1}{2q}} \tag{11}$$

a son nombre de classes divisible par g.

Il est clair d'après les lois de décomposition dans $R(\sqrt{D})$ et à cause de (11) que tous les facteurs premiers p de P se décomposent en 2 facteurs idéaux premiers distincts: $p = \mathfrak{p}\mathfrak{p}'$.

Considérons le nombre entier de $R(\sqrt{D})$

$$\alpha = \frac{2P^g + 1 + a\sqrt{D}}{2}$$

dont la norme est $N\alpha = P^g$.

L'idéal principal engendré par ce nombre se décompose de la façon suivante en facteurs idéaux premiers:

$$(\alpha) = \Pi\, \mathfrak{p}_i^{m_i} \quad \mathfrak{p}_i \neq \mathfrak{p}_j \quad \text{si} \quad i \neq j\,. \tag{12}$$

Il est visible que $N\mathfrak{p}_i \neq N\mathfrak{p}_j$ si $i \neq j$, car α n'est divisible par aucun entier rationnel.

En prenant les normes dans (12) on obtient

$$P^g = \Pi\, N\mathfrak{p}_i^{m_i} = \Pi\, p_i^{m_i} \quad p_i = N\mathfrak{p}_i \quad p_i \neq p_j\,.$$

Soit $P = \Pi p_i^{n_i}$ la décomposition de P en ses facteurs premiers entiers rationnels. On aura $m_i = g n_i$.

L'idéal entier $\mathfrak{a} = \Pi \mathfrak{p}_i^{n_i}$ a pour norme $N\mathfrak{a} = P$. La $g^{\text{ième}}$ puissance de $\mathfrak{a}$ est l'idéal (α) qui est principal: $\mathfrak{a}^g = \Pi \mathfrak{p}_i^{g n_i} = (\alpha)$. Nous allons voir que l'idéal $\mathfrak{a}^k$ ne peut pas être principal pour $k \leqslant \frac{g}{q}$, q étant le plus petit facteur premier de g; le théorème 3 s'en suit. Supposons donc que $\mathfrak{a}^k$ soit principal:

$$\mathfrak{a}^k = (\xi)\,.$$

Soit $\varepsilon > 1$ une unité de norme -1 du corps $R(\sqrt{D})$. En remplaçant ξ par un associé convenable, on aura, si l'accent désigne le conjugué:

$$1 \leqslant \left| \frac{\xi}{\xi'} \right| \leqslant \varepsilon^2\,.$$

On peut encore supposer $N\xi = -P^k$; car si $N\xi = P^k$, on prendra $\varepsilon\xi'$ au lieu de ξ, ce qui revient à changer $\mathfrak{a}$ en $\mathfrak{a}'$ c'est-à-dire α en α', et tous les raisonnements précédents subsistent. De même en prenant éventuellement $-\xi$ au lieu de ξ, on aura $\xi > 0$, donc $\xi' < 0$.

Soient

$$\xi = \frac{x + y\sqrt{D}}{2}\,, \qquad \xi' = \frac{x - y\sqrt{D}}{2}\,.$$

L'inégalité $|\xi| \leqslant \varepsilon^2 |\xi'|$ avec $|\xi\xi'| = P^k$ donne $|\xi| \leqslant \varepsilon P^{\frac{k}{2}}$.

L'inégalité $|\xi'| \leqslant |\xi|$ avec $|\xi\xi'| = P^k$ donne $|\xi'| \leqslant P^{\frac{k}{2}}$.

Donc

$$0 < \frac{x + y\sqrt{D}}{2} \leqslant \varepsilon P^{\frac{k}{2}}$$

$$0 < \frac{-x + y\sqrt{D}}{2} \leqslant P^{\frac{k}{2}}\,.$$

D'où par addition

$$0 < y\sqrt{D} \leqslant (\varepsilon + 1)\, P^{\frac{k}{2}}.$$

Or $\varepsilon = 2P^g + a\sqrt{D} > 1$ est une unité de norme -1 du corps $R(\sqrt{D})$.

On a alors

$$y \leqslant \frac{\varepsilon + 1}{\sqrt{D}} P^{\frac{k}{2}} = a(2 + \varrho) P^{\frac{k}{2}} .$$

On vérifie aisément que $0 < \varrho < \frac{1}{2}$.

L'égalité $N\xi = -P^k$ s'écrit, si l'on tient compte de $\xi = \frac{x + y\sqrt{D}}{2}$:

$$a^2 x^2 = (2yP^g)^2 + (y^2 - 4a^2 P^k) . \qquad (13)$$

La quantité $A = y^2 - 4a^2 P^k$ ne peut être nulle, car si elle l'était on aurait $x = \pm \frac{2yP^g}{a}$ et

$$\xi = \frac{x + y\sqrt{D}}{2} = \frac{y}{2a}\varepsilon \text{ ou } \xi = -\frac{y}{2a}\varepsilon' .$$

L'idéal (ξ) serait entier rationnel, ce qui est impossible, car on a $(\xi) = \mathfrak{a}^k$, $\mathfrak{a} \neq (1)$ puisque $N\mathfrak{a} = P > 1$, et deux facteurs idéaux premiers différents de $\mathfrak{a}$ ne peuvent être conjugués.

L'égalité (13) montre alors que la quantité A est au moins égale en valeur absolue à la différence entre $(2yP^g)^2$ et le carré immédiatement supérieur ou inférieur suivant que A est positif ou négatif.

1er *cas*. $A > 0$. Alors

$$y^2 - 4a^2 P^k \geqslant 4yP^g + 1 .$$

Comme $1 \leqslant y \leqslant a(2 + \varrho) P^{\frac{k}{2}}$ on en déduit

$$P^k > \frac{4}{4 + \varrho} \cdot \frac{1}{\varrho} \frac{P^g}{a^2} .$$

Or on a vu que $0 < \varrho < \frac{1}{2}$, par conséquent

$$P^k > \frac{P^g}{a^2}$$

2ème *cas*. $A < 0$. Alors

$$4a^2 P^k - y^2 \geqslant 4yP^g - 1 .$$

Comme $y \geqslant 1$ on en tire

$$P^k \geqslant \frac{P^g}{a^2} .$$

On a donc dans les 2 cas $P^k \geqslant \frac{P^g}{a^2}$; or par hypothèse $a < P^{g\frac{q-1}{2q}}$; il en découle

$$P^k > P^{\frac{g}{q}} \quad \text{c'est-à-dire} \quad k > \frac{g}{q},$$

et le théorème est démontré.

Pour $g = 2$ on obtient la curieuse conséquence:

Aucun des nombres $4P^4 + 1$ *n'est premier pour* $P > 1$.

En effet, supposons $4P^4 + 1 = p$ premier; on aurait $D = p$, $a = 1$, et la condition $a < P^{g\frac{q-1}{2q}} = \sqrt{P}$ serait satisfaite; le nombre des classes du corps $R(\sqrt{p})$ serait d'après le théorème 3 divisible par 2. Or, cela est impossible, car dans le groupe des classes restreintes d'idéaux de $R(\sqrt{D})$, le nombre d'éléments de base dont l'ordre est une puissance de 2 est égal à $t - 1$, t étant le nombre des facteurs premiers distincts de D. Si $D = p$ on a $t = 1$, et l'ordre h_0 du groupe des classes restreintes est impair, et a fortiori l'ordre h du groupe des classes, puisque $h_0 = h$ ou $h_0 = 2h$.

Si $P \not\equiv 0$ (5), on a $P^4 \equiv 1$ (5) et les nombres $4P^4 + 1$ sont tous divisibles par 5. Donc seul le cas $P = 5 \cdot Q$ mérite d'être signalé:

Aucun des nombres $2500\,Q^4 + 1$ *n'est premier.*

Et pourtant il n'existe aucun nombre premier fixe p qui divise tous ces nombres, car la congruence $2500\,Q^4 + 1 \equiv 0\,(p)$ admet au plus quatre solutions (mod p), et comme $p \geqslant 13$, il existe des Q pour lesquels $2500\,Q^4 + 1 \not\equiv 0\,(p)$.

(Reçu le 9 décembre 1939.)