4.3. Le cas l > 3

THÉORÈME 4.2.2. *Une condition nécessaire et suffisante pour que le nombre de classes d'un corps quadratique soit divisible par* 3 *est que ce corps soit de la forme* $\mathbf{Q}(\sqrt{-3\,(x^2\text{-}4z^3)})$ *où* x *et* z *sont deux entiers rationnels non nuls, tels que les p.g.c.d.* $(z, 2l)$ *et* (x, z) *sont égaux à* 1, *que* $x^2 - 4z^3$ *est divisible par* 27 *et n'est pas un carré et que le polynôme* $X^3 - 3zX-$ *n'a pas de racines rationnelles.*

Démonstration. Soit L un corps quadratique. Le nombre de classe de L est divisible par 3 si et seulement si L possède des extensions abéliennes non ramifiées de degré 3. Comme on l'a remarqué ci-dessus, une telle extension est la clôture galoisienne d'un corps tchébychévien. Supposons donc que L possède une telle extension et notons T le corps tchébychévien dont elle est la clôture galoisienne. Désignons par d l'entier sans carré tel que $L = \mathbf{Q}\,(\sqrt{-3d})$ (d existe puisque $L \neq \mathbf{Q}\,(\sqrt{-3})$). Le théorème 4.1.1. affirme l'existence d'un entier ξ de $\mathbf{Q}\,(\sqrt{d})$ dont la norme est le cube d'un rationnel impair M, qui définit T et qui vérifie les conditions 1), 2) et 3) de cette proposition. Ecrivons $\xi = \frac{1}{2}\,(a+b\sqrt{d})$ et posons $x = a$ et $z = M$; on vérifie facilement que $L = \mathbf{Q}\,(\sqrt{-3\,(x^2-4z^3})$ et que x et z vérifient toutes les conditions de notre proposition, Réciproquement, soient x et z vérifiant toutes les conditions de notre proposition; nous posons $x^2 - 4z^3 = b^2 d$ avec d sans carré. L'entier quadratique $\xi = \frac{1}{2}\,(x+b\sqrt{d})$ vérifie les conditions 1), 2) et 3) du théorème 4.1.1 donc la clôture galoisienne du corps tchébychévien associé à ξ est une extension abélienne non ramifiée de degré 3 de $\mathbf{Q}\,(\sqrt{-3d})$ i.e de $Q\,(\sqrt{-3\,(x^2-4z^3})$; le nombre de classe de ce corps quadratique est donc divisible par 3 ce qui achève la démonstration.

4.3. *Le cas* $l > 3$

On rappelle que ω est $\cos\frac{2\pi}{l}$. Le corps L est le corps $\mathbf{Q}\,(\omega, \sqrt{d\,(\omega^2-1)})$; c'est une extension quadratique du sous-corps réel maximal du corps des racines l-ième de l'unité. On n'a pas dans ce cas de résultat aussi précis que celui du théorème 4.2.2, mais le théorème 4.1.1 permet de démontrer le résultat suivant:

THÉORÈME 4.3.1. *Soient* x *et* z *deux entiers rationnels non nuls tels que* $(z, 2l) = (x, z) = 1$, *que* $x^2 - 4z^l$ *est divisible par* l^3 *et n'est pas un carré et que le polynôme* $P_l(X; z) - x$ *n'a pas de racines rationnelles, alors* l *divise le nombre de classe du corps* $\mathbf{Q}\left(\omega, \sqrt{(x^2-4z^l)(\omega^2-1)}\right)$.

Démonstration. Analogue à la partie correspondante (dans le cas $l = 3$) du théorème 4.2.2.

Terminons ce travail par une illustration numérique. Prenons $l = 5$; le corps L est alors $\mathbf{Q}\left(\sqrt{\left(\frac{-5+\sqrt{5}}{2}\right) d}\right)$ et l^3 est 125. — Soit p un nombre premier congru à 1 modulo 5. — Nous prenons $z = \pm p$. — Dans les deux cas z est un carré modulo 5, donc aussi modulo 125, et $4z^5$ est un carré modulo 125. — Choisissons alors x tel que, d'une part, x^2 soit congru à $4z^5$ modulo 125 et que, d'autre part, x ne soit pas une puissance 5-ième modulo p (de tels x existent puisque 125 et p sont premiers entre eux). — Le polynôme $P_5(X; z)$ est $X^5 - 5zX^3 + 5z^2X$; en réduisant modulo p, on voit que l'équation $P_5(X; z) - x$ n'a pas de racines rationnelles. — En conséquence, pour un tel x et un tel z, le nombre de classes du corps $\mathbf{Q}\left(\sqrt{\left(\frac{-5+\sqrt{5}}{2}\right)(x^2 - 4z^5)}\right)$ est divisible par 5 dès que $x^2 - 4z^5$ n'est pas un carré.

En se servant, comme le fait Honda [3], d'un théorème de Mordell (ou de celui de Thue [9], chap. 28, qui est suffisant), on peut voir qu'il y a une infinité de corps réels et une infinité de corps imaginaires du type $\mathbf{Q}\left(\sqrt{\left(\frac{-5+\sqrt{5}}{2}\right)(x^2 - 4z^5)}\right)$ dont le nombre de classes est divisible par 5. — En effet il suffit pour le voir de remarquer que, si l'on pose $x^2 - 4z^5 = y^2\delta$ avec δ sans carré, alors, en faisant varier x et z assujettis aux conditions décrites ci-dessus, on obtient une infinité de δ positifs et une infinité de δ négatifs (δ positif correspond à un corps imaginaire et δ négatif à un corps réel puisque $\frac{-5+\sqrt{5}}{2}$ est négatif). — En fait on fixe un x qui n'est pas une puissance 5-ième et on montre que l'on obtient déjà l'infinité de δ cherchée avec cette valeur de x. — Désignons par ζ une racine 25-ième de l'unité et considérons l'extension $M = \mathbf{Q}(\zeta, \sqrt[5]{x})$. — C'est une extension galoisienne de degré 100 sur $\mathbf{Q}$; l'extension $M/\mathbf{Q}(\zeta)$ est de degré 5 et l'ensemble des 4 automorphismes non triviaux de $M/\mathbf{Q}(\zeta)$ est une classe de conjugaison de Gal (M/Q); notons la C. — D'après le théorème de Tchebotarev, il existe une infinité de nombres premiers dont le Frobenius est cette classe de conjugaison. — Soit p un tel nombre premier; il est totalement décomposé dans $\mathbf{Q}(\zeta)$ donc congru à 1 modulo 25, et il n'est pas totalement décomposé dans M donc x n'est pas une puissance 5-ième modulo p. — En conséquence, si $z = \pm p$, le nombre de classes du corps $\mathbf{Q}\left(\sqrt{\left(\frac{-5+\sqrt{5}}{2}\right)(x^2-4z^5)}\right)$ est divisible par 5 dès que $x^2 - 4z^5$ est divisible par 125. — Prenons $x = 2$ et $z = p$ alors $x^2 - 4z^5 = 4 - 4p^5 = y^2\delta$ est divisible par 125. — Pour un δ fixé l'équation $4 - 4p^5 = y^2\delta$ n'a, d'après le théorème de Thue, qu'un nombre fini de solutions; une infinité de p étant permis, on obtient donc l'infinité de δ cherchée et ces δ sont clairement négatifs. — De même, en prenant $x = 11$ et $z = -p$, on obtient l'infinité de δ positifs cherchée. —

Remarque. On peut montrer qu'en fait, dans le cas $l = 5$, les conditions nécessaires à la divisibilité par 5 du nombre de classes de $\mathbf{Q}\left(\sqrt{\left(\frac{-5+\sqrt{5}}{2}\right)(x^2-4z^5)}\right)$ énoncées dans le théorème 4.3.1. sont suffisantes. —

BIBLIOGRAPHIE

[1] GUT, Max. Relativquadratische Zahlkörper, deren Klassenzahl durch eine vorgegebene ungerade Primzahl teilbar ist. *Comment. Math. Helv. 2.* (1954), pp.270-277.

[2] NEUMANN, Olaf. Relativquadratische Zahlkorper, deren Klassenzahlen durch 3 teilbar sind. *Math. Machrichten 56* (1973), pp. 281--306.

[3] HONDA, Taira. On real quadratic fields whose class numbers are multiples of 3. *J. Reine Angew. Math. 233* (1968), pp. 101-102.

[4] GRAS, Georges. Extensions abéliennes non ramifiées de degré premier d'un corps quadratique. *Bull. Soc. Math. France 100* (1972), pp. 177-193.