Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 25 (1979)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: CORPS RÉSOLUBLES ET DIVISIBILITÉ DE NOMBRES DE CLASSES D'IDÉAUX
Autor: Satgé, Ph.
Kapitel: 4) Applications
DOI: https://doi.org/10.5169/seals-50376

donc $a_{\frac{p-1}{l}}/2$ est une puissance l-ième modulo p et donc ξ, qui est congru à $a_{\frac{p-1}{l}}/2$ modulo p, est une puissance l-ième modulo $\mathfrak{p}$. On conclut en remarquant que, s'il existe un k divisant $\frac{p-1}{l}$ tel que p divise b_k, alors p divise $b_{\frac{p-1}{l}}$. Pour terminer notre démonstration il ne reste plus que le cas $(\frac{d}{p}) = -1$ et $p \equiv -1 \bmod l$. Dans ce cas, il y a un seul idéal premier de K au-dessus de p, notons le $\mathfrak{p}$. Si ξ est une puissance l-ième modulo $\mathfrak{p}$, alors $\xi^{\frac{p+1}{l}}$ est congru à un rationnel modulo $\mathfrak{p}$; mais $\sqrt{d}$ n'est pas congrue à un rationnel modulo $\mathfrak{p}$, donc p divise $b_{\frac{p+1}{l}}$. Réciproquement, si p divise $b_{\frac{p+1}{l}}$, alors $\xi^{\frac{p+1}{l}}$ est congru à un rationnel modulo $\mathfrak{p}$, donc $\xi^{\frac{p+1}{l}(p-1)}$ est congru à 1 modulo $\mathfrak{p}$ ce qui implique que ξ est une puissance l-ième modulo $\mathfrak{p}$. Enfin, on conclut comme précédemment en remarquant que, si il existe un k divisant $\frac{p+1}{l}$ tel que p divise b_k, alors p divise $b^{\frac{p+1}{l}}$.

4) Applications

4.1. *Corps tchébychéviens non ramifiés*

Nous allons étudier les corps tchébychéviens dont la clôture galoisienne N est non ramifiée sur L. L'existence de tels corps implique la divisibilité par l du nombre de classes du corps L; nous reviendrons sur cet aspect aux paragraphes 4.2 et 4.3. On a le théorème suivant:

Théorème 4.1.1. *Soit* $\xi = \frac{1}{2}(a+b\sqrt{d})$ *un entier du corps* K *dont la norme est la puissance* l-ième *d'un entier rationnel impair* M. *Si les trois conditions suivantes sont vérifiées:* 1) *le polynôme* $P_l(X; M) - a$ *n'a pas*

de racines rationnelles ; 2) l^2 *divise le produit* bd, *3) le p.g.c.d de* a *et* b *est* 1 *ou* 2, *alors* ξ *définit un corps tchébychévien* T *dont la clôture galoisienne* N *est non ramifiée sur* L. *Réciproquement, si* T *est un corps tchébychévien dont la clôture galoisienne est non ramifiée sur* L, *alors il existe un entier quadratique* $\xi = \frac{1}{2}(a+b\sqrt{d})$ *de norme* M^l *avec* M *impair qui définit* T *et qui vérifie les conditions* 1), 2) *et* 3) *énoncées ci-dessus.*

Démonstration. Supposons 1), 2) et 3) vérifiées. Le lemme 1.1.2 et la condition 1) montrent que ξ n'est pas une puissance l-ième dans K, donc que ξ définit un corps tchébychévien T. Les conditions 2) et 3) montrent que l divise b mais ne divise pas a; en conséquence l ne divise pas M et donc l'idéal engendré par ξ est premier à l. L'entier quadratique ξ vérifie donc la condition imposée au début de la partie 2) de ce travail et nous pouvons employer les résultats de cette partie. La condition 3) signifie que ξ n'est divisible par aucun nombre rationnel différent de ± 1, donc la proposition 2.2.6 montre que seuls les idéaux premiers de L qui divisent l peuvent se ramifier dans la clôture galoisienne N de T. Le lemme 2.1.1 et la proposition 2.2.1 montrent que ξ est l-primaire, ce qui implique que les idéaux premiers de L au-dessus de l ne sont pas ramifiés dans N/L. Enfin, l'extension N/L étant de degré impair, les places à l'infini de L ne peuvent pas se ramifier dans N, donc N/L est non ramifiée. Réciproquement, soit T un corps tchébychévien dont la clôture galoisienne N est non ramifiée sur L. Soit $\eta = \frac{1}{2}(\alpha+\beta\sqrt{d})$ un entier quadratique définissant T; comme on l'a vu au début de la partie 2) de ce travail, on peut supposer que l'idéal principal (η) n'est divisible par la puissance l-ième d'aucun idéal premier de K qui divise l. L'extension N/L étant non ramifiée, l'idéal principal (η) engendré par η dans K est la puissance l-ième d'un idéal, donc η et l sont premiers entre eux et η est l-primaire; de plus, quitte à multiplier η par une puissance l-ième, on peut supposer que η est premier à 2. En vertu du lemme 2.1.1 et de la proposition 2.2.1 on peut, en remplaçant éventuellement η par une de ses puissances premières à l (ce qui, d'après la proposition 1.2.5, ne change pas le corps tchébychévien associé) supposer que l^2 divise βd. Ecrivons alors $\eta = c_1 c_2^l \xi$ où c_1 et c_2 sont des entiers rationnels, ou c_1 est sans puissance l-ième et où $\xi = \frac{1}{2}(a+b\sqrt{d})$ est un entier de K qui n'est divisible par aucun entier rationnel différent de ± 1. La norme de η étant

une puissance l-ième, on peut, en remplaçant éventuellement η par son carré (ce qui ne change pas le corps tchébychévien associé) supposer que les nombres premiers qui divisent c_1 sont décomposés dans le corps K. La proposition 2.2.6 montre qu'aucun nombre premier différent de l ne divise c_1; comme de plus l et η sont premiers entre eux, l ne divise pas c_1 et donc $c_1 = 1$. L'entier quadratique ξ définit donc le corps tchébychévien T. D'autre part l^2 divisant βd divise aussi bd puisque l ne divise pas $c_1 c_2^l$. Enfin, ξ définissant le corps tchébychévien T, il n'est pas une puissance l-ième dans K et le lemme 1.1.2 montre que $P_l(X; M) - a$ n'a pas de racines rationnelles. L'élément ξ répond donc à notre question.

4.2. Rappelons le lemme suivant:

LEMME 4.2.1. *Soit L un corps quadratique et M une 3-extension abélienne non ramifiée de L, alors M est galoisienne sur* $\mathbf{Q}$.

Démonstration. Soit H le groupe de Galois de la 3-extension abélienne maximale non ramifiée de L. Cette extension maximale étant galoisienne sur $\mathbf{Q}$, le groupe Gal $(L/\mathbf{Q})$ agit par conjugaison sur H. Soit H_1 le sous-groupe de H formé des éléments invariant par Gal $(L/\mathbf{Q})$ et H_2 celui formé des éléments qui, par l'action de l'élément non trivial de Gal $(L/\mathbf{Q})$, se transforment en leur inverse. Les sous-groupes H_1 et H_2 sont stables par Gal $(L/\mathbf{Q})$ et leur produit direct est isomorphe à H. En conséquence, le corps des invariants M_2 de H_2 est galoisien sur $\mathbf{Q}$ et Gal $(L/\mathbf{Q})$ agit trivialement sur Gal (M_2/L). Les ordres de Gal (M_2/L) et de Gal $(L/\mathbf{Q})$ étant premier entre eux, le corps M_2 est le composé de L et d'une 3-extension non ramifiée de $\mathbf{Q}$. Le corps $\mathbf{Q}$ n'ayant pas d'extension non ramifiée, on a $M_2 = L$ i.e $H_2 = H$ et donc tous les sous-groupes de H sont stables par l'action de Gal $(L/\mathbf{Q})$ ce qui implique l'assertion de notre lemme.

Il résulte de ce lemme que toute extension abélienne non ramifiée de degré 3 d'un corps quadratique (nécessairement différent de $\mathbf{Q}(\sqrt{-3})$) est la clôture galoisienne d'un corps tchébychévien: en effet, ce lemme montre qu'une telle extension est galoisienne sur $\mathbf{Q}$; elle n'est pas abélienne sur $\mathbf{Q}$ puisque $\mathbf{Q}$ ne possède pas d'extension non ramifiée, c'est donc la clôture galoisienne d'un corps cubique non galoisien; ce corps n'est pas pur puisque le corps quadratique K contenu dans sa clôture galoisienne n'est pas le corps $\mathbf{Q}(\sqrt{-3})$, donc (remarque 1.1.6) c'est un corps tchébychévien. On peut maintenant donner une caractérisation des corps quadratiques dont le nombre de classes est divisible par 3; on a:

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* $\mathbf{Q}(\sqrt{-3\,(x^2-4z^3)})$ *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 $x^2 - 4z^3 = b^2d$ 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 consi-

dérons 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.