Astérisque

PHILIPPE SATGÉ

Divisibilité du nombre de classes de certains corps cycliques

Astérisque, tome 61 (1979), p. 193-203

<http://www.numdam.org/item?id=AST_1979__61__193_0>

Société Mathématique de France
Astérisque 61 (1979) p. 193-203

DIVISIBILITÉ DU NOMBRE DE CLASSES DE CERTAINS CORPS CYCLIQUES

par

Philippe SATGÉ

-:-:-:-

Soient ℓ un nombre premier impair et $n = \ell^r$ une puissance de ℓ ; φ étant l'indicateur d'Euler, nous considérons les extensions cycliques de $\mathbb{Q}$ de degré $\varphi(n)$ qui contiennent le sous-corps réel maximal du n-ème corps cyclotomique. Nous montrons essentiellement qu'il existe une infinité de tels corps (aussi bien réels qu'imaginaires) dont le groupe des classes possède un élément d'ordre n. Dans les cas $n = 3$ et $n = 5$, nous donnons même une caractérisation de tous les corps de ce type dont le nombre de classes est divisible par n. Nous obtenons ces résultats en construisant des extensions non ramifiées.

§ .I. - Construction de corps

I.1. - Notations et définition des ψ-corps

Dans tout cet article, ℓ est un nombre premier impair et $n = \ell^r$ est une puissance de ℓ. On désigne par L un corps cyclique sur $\mathbb{Q}$ dont le degré divise $\varphi(n)$ (φ = indicateur d'Euler), par ζ une racine de l'unité d'ordre n, par L' et N' les corps $N(\zeta)$ et $L(\zeta)$, par ψ un homomorphisme de $\mathrm{Gal}(L'/\mathbb{Q})$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles modulo n dont le noyau est $\mathrm{Gal}(L'/L)$ et par ω l'homomorphisme de $\mathrm{Gal}(L'/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ défini, pour tout σ de $\mathrm{Gal}(L'/\mathbb{Q})$, par $\sigma(\zeta) = \zeta^{\omega(\sigma)}$. On pose $\bar{\psi} = \omega\,\psi^{-1}$, on note K le corps des invariants du noyau de $\bar{\psi}$ et $V(\bar{\psi})$ le sous-groupe de K^* formé des x tels que, pour tout σ de $\mathrm{Gal}(L'/\mathbb{Q})$, le produit $\sigma(x)\,x^{-\bar{\psi}(\sigma)}$ est

une puissance n-ème dans K (ce qui a un sens bien que $\bar{\psi}(\sigma)$ ne soit défini que modulo n). Nous définissons les ψ-corps de la manière suivante :

DÉFINITION I.1.1.- Un corps N est un ψ-corps si N/L est une extension cyclique de degré n , si N est galoisien sur $\mathbb{Q}$ et si l'action par conjugaison de $Gal(L/\mathbb{Q})$ sur $Gal(N/L)$ est l'élévation à la puissance $\psi(\sigma)$.

I.2.- Construction des ψ-corps

Les ψ-corps ont été étudiés dans [1] ; nous donnons ici sans démonstration les résultats de [1] dont nous avons besoin dans la suite.

PROPOSITION I.2.1.- Soit N un ψ-corps ; le corps N' est obtenu en adjoignant à L' la racine n-ème d'un élément x de $V(\bar{\psi})$; de plus, si l'intersection $N \cap L'$ est réduite à L, cet élément n'est pas la puissance ℓ-ème d'un élément de K .

Sous l'hypothèse restrictive que le corps K ne contient pas de racine de l'unité d'ordre ℓ , la proposition précédente admet la réciproque suivante :

PROPOSITION I.2.2.- Si K ne contient pas de racine de l'unité d'ordre ℓ et si x est un élément de $V(\bar{\psi})$ qui n'est pas une puissance ℓ-ème, alors il existe un ψ-corps et un seul N tel que $N' = L'(\sqrt[n]{x})$.

On dira que N est le ψ-corps associé à l'élément x de $V(\bar{\psi})$ ou que x est un élément de $V(\bar{\psi})$ associé à N ; on a la proposition suivante :

PROPOSITION I.2.3.- On suppose toujours que K ne contient pas de racine de l'unité d'ordre ℓ . Soient x_1 et x_2 deux éléments de $V(\bar{\psi})$ qui ne sont pas des puissances ℓ-èmes dans K et soient N_1 et N_2 les ψ-corps associés. On a $N_1 = N_2$ si et seulement si il existe un entier a premier à ℓ et un x de K tels que $x_1 = x_2^a x^n$.

§ .2.- Conditions de non ramification

On conserve les notations introduites en I.1 et l'on suppose que K ne contient pas de racine de l'unité d'ordre ℓ . Comme au § .I, nous donnons ici sans dé-

monstration les résultats de [1] dont nous avons besoin dans la suite.

II.1. - Les ψ-corps non ramifiés

DÉFINITION II.1.1. - Nous dirons que le ψ corps N est non ramifié si l'extension N/L est non ramifiée.

Nous aurons besoin de séparer du cas général un cas spécial que nous définissons ainsi :

DÉFINITION II.1.2. - Le cas spécial est le cas où ℓ est totalement décomposé dans le plus grand sous-corps de L de degré premier à ℓ .

Nous étudions les ψ-corps non ramifiés sous l'une ou l'autre des hypothèses suivantes :

a) ℓ ne divise pas le degré $[L' : L]$ de L'/L ;

b) on n'est pas dans le cas spécial.

II.2. - Générateurs des ψ-corps non ramifiés

DÉFINITION II.2.1. - Soit x un élément de K ; nous disons que x est n-primaire si l'extension $K(\zeta, \sqrt[n]{x})/K(\zeta)$ est non ramifiée.

PROPOSITION II.2.2. - Soit x un élément de $V(\bar{\psi})$; on a :

1) si x est une puissance n-ème dans un complété de K en une place au-dessus de ℓ, alors x est n-primaire ;

2) si b) est vérifiée et si x est n-primaire, alors x est une puissance n-ème dans un complété de K en une place au-dessus de ℓ ; dans ce cas x est une puissance n-ème dans tous les complétés de K au-dessus de ℓ .

PROPOSITION II.2.3. - On suppose a) ou b) vérifiée. Si x est un élément de $V(\bar{\psi})$ qui n'est pas une puissance ℓ-ème et si N est le ψ-corps qui lui est associé, alors les deux assertions suivantes sont équivalentes :

1) N est un ψ-corps non ramifié ;

2) l'idéal principal engendré par x dans K est une puissance n-ème et x est n primaire.

§. III. - Applications

III. 1. - Le cas $K = \mathbb{Q}$

Nous partons de $L = \mathbb{Q}(\zeta)$ et de $\psi = \omega$; on a alors $\bar{\psi} = 1$, donc $K = \mathbb{Q}$ et $V(\psi) = \mathbb{Q}^*$. La proposition II.2.2. montre qu'il n'y a pas de ω-corps non ramifié. En particulier, en prenant $n = \ell$, on retrouve le fait que la partie du ℓ-groupe des classes du ℓ-ème corps cyclotomique associée au caractère ω est triviale.

III. 2. - Le cas K quadratique

On pose $\theta = \cos \frac{2\pi}{n}$ et $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2 - 1)})$ où d est un entier sans facteur carré. Si $d \neq (-1)^{(\ell-1)/2} \ell$, le corps L est une extension quadratique de $\mathbb{Q}(\theta)$ différente de $\mathbb{Q}(\zeta)$ et $L/\mathbb{Q}$ est cyclique de degré $\varphi(n)$ sur $\mathbb{Q}$. Le corps L' est le corps $\mathbb{Q}(\sqrt{d}, \zeta)$ et il y a une injection et une seule de $\mathrm{Gal}(L'/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ telle que $\bar{\psi}$ est l'homomorphisme d'ordre 2 de $\mathrm{Gal}(L'/\mathbb{Q})$ dans $(\mathbb{Z}/n\mathbb{Z})^*$, de noyau $\mathrm{Gal}(L'/\mathbb{Q}(\sqrt{d}))$. Pour ces choix de L et de ψ, on a donc $K = \mathbb{Q}(\sqrt{d})$. Dans toute la suite nous nous plaçons dans cette situation ; le cas spécial est alors le cas $\ell = 3$ et $d \equiv -3 \bmod 9$. La démonstration du lemme suivant est évidente.

LEMME III.2.1. - *Un élément de K^* est dans $V(\bar{\psi})$ si et seulement si sa norme sur $\mathbb{Q}$ est la puissance n-ème d'un rationnel.*

Montrons maintenant la proposition suivante :

PROPOSITION III.2.2. - *Soit N un ψ-corps ; une condition suffisante pour que le ψ-corps N soit non ramifié est qu'il existe, dans l'ensemble des éléments de $V(\bar{\psi})$ associé à N, un x vérifiant les trois conditions suivantes :*

1) *x est un entier de K qui n'est divisible par aucun entier rationnel différent de ± 1 ;*

2) *la norme de x sur $\mathbb{Q}$ est la puissance n-ème d'un entier rationnel premier à 2ℓ ;*

3) *x n'est pas une puissance ℓ-ème dans K mais est une puissance ℓ-ème dans un complété de K en une place divisant ℓ.*

De plus, si l'on n'est pas dans le cas spécial, cette condition suffisante est nécessaire.

Démonstration. - Si $\mathfrak{a}$ est un idéal entier de K, nous convenons de noter

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i} \prod_j \mathfrak{q}_j^{m_j} \prod_k \mathfrak{r}_k^{s_k} \tilde{\mathfrak{r}}_k^{\tilde{s}_k}$$

la décomposition de $\mathfrak{a}$ en produit de puissance d'idéaux premiers, les $\mathfrak{p}_i$ étant inertes, les $\mathfrak{q}_j$ ramifiés, les $\mathfrak{r}_k$ décomposés et les $\tilde{\mathfrak{r}}_k$ étant les conjugués des $\mathfrak{r}_k$; de plus, on suppose $s_k \geq \tilde{s}_k$ et l'on note p_i, q_j et r_k les nombres premiers contenus respectivement dans $\mathfrak{p}_i$, $\mathfrak{q}_j$ et $\mathfrak{r}_k$. Soit alors x un élément de $V(\bar{\psi})$ vérifiant 1), 2) et 3) et soit N le ψ-corps associé ; pour prouver la première partie de la proposition, il suffit, compte tenu des propositions II.2.2 et II.2.3, de voir que l'idéal $(x)_K$ engendré par x dans K est la puissance n-ème d'un idéal de K. La condition 1) implique que $(x)_K$ est de la forme :

$$\prod_j \mathfrak{q}_j^{m_j} \prod_k \mathfrak{r}_k^{s_k} .$$

La condition 2) montre alors que les m_j et les s_k sont divisibles par n l'idéal $(x)_K$ est donc une puissance n-ème.

Pour prouver la deuxième partie de la proposition, nous supposons que nous ne sommes pas dans le cas spécial. Soient N un ψ-corps non ramifié et y un élément de $V(\bar{\psi})$ qui lui est associé. D'après la proposition II.2.3, l'idéal $(y)_K$ engendré par y dans K est la puissance n-ème d'un idéal et y est n-primaire. Le lemme d'approximation montre qu'il existe un α dans K tel que $z = y\alpha^n$ est un entier de K premier à 2ℓ. Soit $(z)_K$ l'idéal de K engendré par z ; si

$$(z)_K = \prod_i \mathfrak{p}_i^{n_i} \prod_j \mathfrak{q}_j^{m_j} \prod_k \mathfrak{r}_k^{s_k} \tilde{\mathfrak{r}}_k^{\tilde{s}_k} ,$$

on a :

$$z^2 = x \prod_i p_i^{2n_i} \prod_j \mathfrak{q}_j^{m_j} \prod_k r_k^{2s_k}$$

où x est un entier de K qui n'est divisible par aucun entier rationnel différent de ± 1. D'autre part, $(z)_K$ est la puissance n-ème d'un idéal, donc n divise les n_i, les m_j et les $\tilde{s}_k$ et donc (proposition I.2.3) x est associé à N et vérifie 1) et 2). Enfin la proposition II.2.2. montre que y, donc z, donc x est une puissance n-ème dans un complété de K en une place au-dessus de ℓ, c'est-à-dire que x vérifie 3) ; cela achève la démonstration.

Rappelons les résultats suivants :

LEMME III.2.3.- Soit $K = \mathbb{Q}(\sqrt{d})$ avec d sans facteur carré et soit x un entier de K. Il existe a et b dans $\mathbb{Z}$ tel que $x = \frac{1}{2}(a+b\sqrt{d})$ et on a l'équivalence :

1) $(a,b) = 1$ ou $(a,b) = 2$ et $d \not\equiv 1 \mod 4$;

2) x n'est divisible par aucun entier rationnel différent de ± 1.

LEMME III.2.4.- Soit x un entier de K ; pour tout entier naturel i on pose $x^i = \frac{1}{2}(a_i+b_i\sqrt{d})$ avec a_i et b_i dans $\mathbb{Z}$. Si la norme de x est première à ℓ, il existe un entier i premier à ℓ tel que ℓ divise $b_i d$ et l'on peut toujours trouver un tel i divisant $\ell - (\frac{d}{\ell})$.

Démonstration.- Si ℓ divise d, c'est clair. Sinon, la norme de l'entier x étant première à ℓ, x lui-même est premier à ℓ ; en conséquence $x^{\ell-(d/\ell)}$ est congru à un rationnel modulo ℓ, ce qui implique le lemme.

On rappelle que $n = \ell^r$; alors :

PROPOSITION III.2.5.- On reprend les notations du lemme III.2.4 et l'on suppose de plus que la norme de x est la puissance n-ème d'un rationnel premier à ℓ. Si i est un entier naturel premier à ℓ tel que ℓ divise $b_i d$, alors x est une puissance n-ème dans un complété de K au-dessus de ℓ si et seulement si :

1) ℓ^{r+1} divise $b_i d$ si l'on n'est pas dans le cas spécial

2) et ℓ^{r+2} divise $b_i d$ si l'on est dans le cas spécial.

Démonstration.- Désignons par $\mathfrak{l}$ un idéal premier de K au-dessus de ℓ, par e son indice de ramification, par $\hat{K}$ le complété de K en ℓ et, pour un entier naturel j, par U^j le groupe des unités de $\hat{K}$ congrues à 1 modulo la puissance j-ème de l'idéal maximal de $\hat{K}$. Le cas spécial correspond à $\hat{K} = \mathbb{Q}_3(\sqrt{-3})$.

LEMME III.2.6.- Un élément u de U^1 est une puissance n-ème si et seulement si :

1) u est dans U^{1+er} si l'on n'est pas dans le cas spécial,

2) u est dans U^{2+er} si l'on est dans le cas spécial.

Revenons à la démonstration de notre proposition. Soit $x^i = \frac{1}{2}(a_i + b_i\sqrt{d})$ de norme m^n avec m entier rationnel premier à ℓ ; on suppose que ℓ divise $b_i d$ et l'on note ℓ^α la plus grande puissance de ℓ qui divise $b_i d$. Supposons tout d'abord que ℓ ne divise pas d ; alors ℓ^α divise b_i et l'égalité $m^n = (a_i^2/4) + (b_i^2 d/4)$ montre que $(a_i/2)$ est une puissance n-ème modulo $l^{2\alpha}$. D'autre part m étant premier à ℓ, a_i est premier à ℓ ; l'égalité $x^i = (a_i/2)(1 + b_i\sqrt{d}/a_i)$ et le lemme III.2.6 montrent alors que x^i, donc x, est une puissance n-ème si et seulement si $\alpha \geq r+1$. Dans le cas où ℓ divise d on conclut à l'aide d'un raisonnement similaire.

Rappelons enfin le résultat suivant démontré dans [2] : soit m un rationnel ; on définit une famille de polynômes en posant $P_o(X;m) = 2$, $P_1(X;m) = X$ et $P_k(X;m) = X P_{k-1}(X;m) - m P_{k-2}(X;m)$; on a alors :

PROPOSITION III.2.7. - Soit x un élément de K dont la norme est m^n avec m rationnel ; x est une puissance ℓ-ème dans K si et seulement si le polynôme $P_\ell(X; m^{n/\ell}) - \mathrm{tr}(x)$ où $\mathrm{tr}(x)$ est la trace de x n'a pas de racine rationnelle.

Les propositions III.2.2, III.2.5, III.2.7 et le lemme III.2.3 se résument dans le théorème suivant :

THÉORÈME III.2.8. - On pose $n = \ell^r$; le corps L et le caractère ψ sont ceux définis au début de ce paragraphe III.2. Alors :

1) si l'on n'est pas dans le cas spécial, l'existence d'un ψ-corps non ramifié est équivalente à l'existence de deux entiers rationnels a et b vérifiant les trois conditions suivantes :

i) $(a,b) = 1$ ou 2 et ℓ^{r+1} divise bd ;

ii) $a^2 - db^2 = 4m^n$ pour un entier rationnel m premier à 2ℓ ;

iii) $P_\ell(X; m^{n/\ell}) - a$ n'a pas de racine rationnelle ;

2) si l'on est dans le cas spécial, alors l'existence de deux entiers rationnels a et b vérifiant, d'une part la condition

i_s) $(a,b) = 1$ et ℓ^{r+2} divise bd

et d'autre part les conditions ii) et iii) de 1) impliquent l'existence d'un ψ-corps non ramifié.

COROLLAIRE III.2.9.- Soient a et m deux entiers rationnels tels que :

1) $(m, 2\ell) = (a, m) = 1$;

2) $a^2 - 4m^n$ n'est pas un carré, est divisible par ℓ^{2r+1} si $\ell \neq 3$ et par 3^{2r+2} si $\ell = 3$;

3) le polynôme $P_\ell(X; m^{n/\ell})$ - a n'a pas de racine rationnelle.

Alors, le groupe des classes du corps $L = \mathbb{Q}(\theta, \sqrt{(a^2-4m^n)(\theta^2-1)})$ possède un élément d'ordre n .

Démonstration.- L'existence d'un ψ-corps non ramifié implique l'existence d'un quotient cyclique d'ordre n du groupe des classes de L ; si un tel quotient existe, alors il existe une classe d'ordre n .

Remarque III.2.10.- Si $\ell \equiv 3 \mod 4$, alors $L = \mathbb{Q}(\theta, \sqrt{-3(a^2-4m^n)})$. La classe d'ordre n dont le corollaire III.2.9 assure l'existence ne provient pas d'une classe d'ordre n du corps quadratique $\mathbb{Q}(\sqrt{-3(a^2-4m^n)})$: en effet, $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{-3(a^2-4m^n)}))$ agit non trivialement sur les groupes de Galois des ψ-corps, donc agit non trivialement sur les classes d'ordre n associées aux ψ-corps non ramifiés.

En s'inspirant d'un raisonnement de Honda ([3]), on peut maintenant montrer le résultat suivant :

PROPOSITION III.2.11.- Il existe une infinité de corps réels et une infinité de corps imaginaires cycliques de degré $\varphi(n)$ sur $\mathbb{Q}$ et contenant le sous-corps réel maximal de $\mathbb{Q}(\zeta)$ qui possèdent une classe d'ordre n .

Démonstration.- Posons $\alpha = 2r+2$ ou $2r+1$ suivant que $\ell = 3$ ou $\ell \neq 3$. Choisissons un entier naturel a qui n'est pas une puissance ℓ-ème et qui est congru à 2 modulo ℓ^α . Considérons le corps $M = \mathbb{Q}(\mu, \sqrt[\ell]{a})$ où μ est une racine de l'unité d'ordre ℓ^α ; M est galoisien sur $\mathbb{Q}$ et les $(\ell-1)$ éléments non triviaux de $\mathrm{Gal}(M/\mathbb{Q}(\mu))$ forment une classe de conjugaison de $\mathrm{Gal}(M/\mathbb{Q})$; nous notons S l'ensemble des nombres premiers dont le Frobenius tombe dans cette classe ; S est infini. Les nombres premiers de S sont congrus à 1 mod ℓ^α et a n'est pas une puissance ℓ-ème modulo ces nombres premiers. Prenons m dans S . Alors $a^2 - 4m^n$ est divisible par ℓ^α ; de plus, $P_\ell(X; m^{n/\ell})$ est

congru à X^ℓ modulo ℓ, donc le polynôme $P_\ell(X; m^{n/\ell})$ n'a pas de racine rationnelle. En conséquence (corollaire III.2.9), le corps $L = \mathbb{Q}(\theta, \sqrt{(a^2-4m^n)(\theta^2-1)})$ possède une classe d'ordre n si a^2-4m^n n'est pas un carré. Posons $a^2 - 4m^n = y^2\, d(m)$ où $d(m)$ est un entier sans carré. On sait (théorème de Thue) que l'équation $a^2 - 4X^m = Y^2 d$, où X et Y sont les inconnues et a et d sont des constantes entières, n'a qu'un nombre fini de solutions entières. On en déduit que, lorsque m décrit l'ensemble infini S, on obtient une infinité d'entiers $d(m)$; les m étant positifs, presque tous les $d(m)$ sont négatifs, donc on a une infinité de corps $L = \mathbb{Q}(\theta, \sqrt{(a^2-4m^n)(\theta^2-1)})$ réels et ils possèdent une classe d'ordre n.

En reprenant le même raisonnement avec a congru à -2 modulo ℓ^α et en faisant décrire à m les opposés des éléments de S (i.e. $-m$ est dans S), on trouve une infinité de $d(m)$ positifs, donc une infinité de corps imaginaires L qui possèdent une classe d'ordre n, C.Q.F.D.

Terminons ce travail par quelques exemples particuliers.

Le cas $n = 3$ a été étudié en détail dans [2] ; on y montre qu'il n'y a pas lieu de séparer le cas spécial, i.e. que la partie 1 du théorème III.2.8 est valable sans restriction.

Le cas $n = 5$. Soit d un entier rationnel sans facteur carré et non divisible par 5, soit $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2-1)})$ et soit ψ l'injection de $\mathrm{Gal}(L/\mathbb{Q})$ dans $(\mathbb{Z}/5\mathbb{Z})^*$ telle que $\bar{\psi}$ est l'homomorphisme d'ordre 2 dont le noyau est $\mathrm{Gal}(L'/\mathbb{Q}(\sqrt{d}))$. Le corps $\mathbb{Q}(\theta)$ étant le corps $\mathbb{Q}(\sqrt{5})$, les corps $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2-1)})$ et $\mathbb{Q}(\theta, \sqrt{5d(\theta^2-1)})$ coïncident ; il y a donc une injection ψ^* de $\mathrm{Gal}(L/\mathbb{Q})$ dans $(\mathbb{Z}/5\mathbb{Z})^*$ telle que $\bar{\psi}^*$ est l'homomorphisme d'ordre 2 dont le noyau est $\mathrm{Gal}(L'/\mathbb{Q}(\sqrt{5d}))$. Soit maintenant H le sous-groupe du groupe des classes de L formé des éléments annulés par 5 ; ce groupe est un $\mathbb{F}_5[\mathrm{Gal}(L/\mathbb{Q})]$- module semi-simple et donc se décompose en une somme $H_1 \oplus H_2 \oplus H_\psi \oplus H_{\psi^*}$ où H_1, H_2, H_ψ et H_{ψ^*} sont les sous-groupes de H correspondant respectivement au caractère unité, au caractère d'ordre 2, à ψ et à ψ^*. Les groupes H_1 et H_2 sont triviaux puisque les nombres de classes de $\mathbb{Q}$ et de $\mathbb{Q}(\sqrt{5})$ sont égaux à 1. La non-trivialité de H_ψ (resp. de H_{ψ^*}) est équivalente à l'existence d'un ψ-corps (resp. d'un ψ^*-corps) non ramifié. Enfin, lorsque d décrit les entiers sans facteur carré non divisibles par 5, les corps $L = \mathbb{Q}(\theta, \sqrt{d(\theta^2-1)})$ décrivent toutes les extensions cycliques de degré 4 de $\mathbb{Q}$ qui contiennent $\mathbb{Q}(\sqrt{5})$; les

résultats établis précédemment donnent donc le critère suivant : un corps cyclique du degré 4 contenant $\mathbb{Q}(\sqrt{5})$ a un nombre de classes divisible par 5 si et seulement si il est de la forme $\mathbb{Q}(\theta, \sqrt{(a^2-4m^5)(\theta^2-1)})$ où a et m sont deux entiers rationnels vérifiant :

1) $(m, 10) = (a, m) = 1$;

2) $a^2 - 4m^5$ est divisible par 125 et n'est pas un carré ;

3) le polynôme $X^5 - 5mX^3 + 5m^2X - a$ n'a pas de racine rationnelle.

On peut remarquer que $\mathbb{Q}(\theta, \sqrt{(a^2-4m^5)(\theta^2-1)}) = \mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(a^2-4m^5)})$ qui est la forme donnée dans [2].

Exemple numérique. - Prenons $m = 11$, alors $4m^5 = 644\,204$ et $644\,204 \equiv (52)^2$ mod. 125 ; par conséquent, si l'on prend $a \equiv \pm 52$ mod 125, alors $a^2 - 4m^5$ est divisible par 125. De plus, si l'on prend $a \not\equiv 0, 1, -1$ mod. 11, on voit, en réduisant modulo 11, que les conditions 1) et 3) sont vérifiées. En prenant $a = 677, 698, 823, 927$ on trouve que les deux corps réels $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(-1487)})$ et $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(-314)})$ et les deux corps imaginaires $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(1721)}$ et $\mathbb{Q}(\sqrt{\frac{-5+\sqrt{5}}{2}(53)})$ ont un nombre de classes divisible par 5 .

Le cas $n = 9$. Soient d un entier sans facteur carré, et $L = \mathbb{Q}(\theta, \sqrt{(\theta^2-1)})$; on vérifie que $L = \mathbb{Q}(\theta, \sqrt{-3d})$. Le corollaire III.2.8 entraîne donc le résultat suivant : s'il existe deux entiers rationnels a et m tels que :

1) $(m, 6) = (a, m) = 1$,

2) $a^2 - 4m^9$ est divisible par $3^6 = 729$ et n'est pas un carré,

3) et $X^3 - 3m^3X - a$ n'a pas de racine rationnelle, alors le groupe des classes de $\mathbb{Q}(\theta, \sqrt{-3(a^2-4m^9)})$ a un élément d'ordre 9 .

Exemple numérique. - Prenons $m = 7$, alors $4m^9 = 161\,414\,428$ et $161\,414\,428 \equiv 706$ mod 3^6 ; d'autre part, $706 \equiv (187)^2$ mod 3^6 ; en conséquence, si l'on prend $a \equiv \pm 187$ mod 3^6, alors $a^2 - 4m^9$ est divisible par 3^6 . De plus, si l'on prend $a \not\equiv 0, 1, -1$ mod 7 on voit, en réduisant modulo 7 que 1) et 3) sont vérifiées. En prenant $a = 10\,393, 12\,206$ on trouve que les deux corps réels $\mathbb{Q}(\theta, \sqrt{2\,713})$, $\mathbb{Q}(\theta, \sqrt{12\,786})$ possèdent une classe d'ordre 9 .

-:-:-:-

BIBLIOGRAPHIE

[1] Ph. SATGÉ, Construction de corps résolubles non ramifiés, Séminaire de l'Université de Caen (1977).

[2] Ph. SATGÉ, Corps résolubles et divisibilité de nombre de classes d'idéaux, l'Enseignement Mathématique, à paraître.

[3] T. HONDA, On real quadratic fields whose class numbers are multiples of 3 , J. reine angew. Math. 233 (1968), 101-102.

[4] O. NEUMANN, Relativ-quadratische Zahlkörper, deren Klassenzahlen durch 3 teilbar sind, Math. Nachrichten 56 (1973), 281-306.

-:-:-:-

Philippe SATGÉ
U.E.R. Sciences
Université de Caen
14032 CAEN CEDEX