CORPS RÉSOLUBLES ET DIVISIBILITÉ DE NOMBRES DE CLASSES D'IDÉAUX

Autor(en): **Satgé, Ph.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **25 (1979)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-50376

CORPS RÉSOLUBLES ET DIVISIBILITÉ DE NOMBRES DE CLASSES D'IDÉAUX

par Ph. SATGÉ

Plusieurs auteurs se sont attachés à construire des corps quadratiques dont le nombre de classes est divisible par 3 (par exemple [1], [2], [3], [4], [5]). Cependant, c'est seulement en 1968 que Taira Honda [3] a démontré l'existence d'une infinité de corps quadratiques réels dont le nombre de classes est divisible par 3. Nous complétons ici ce résultat de Honda en donnant une caractérisation de tous les corps quadratiques dont le nombre de classes est divisible par 3 (Th. 4.2.2). En fait, cette caractérisation apparaît ici comme cas particulier d'un critère plus général qui affirme la divisibilité par un nombre premier impair l du nombre des classes de certains corps cycliques de degré $l - 1$ (Th. 4.3.1). — Ce critère permet de montrer l'existence d'une infinité de corps imaginaires et d'une infinité de corps réels, cycliques de degré $l - 1$, dont le nombre de classes est divisible par l. Pour cela, nous sommes amenés à étudier les corps obtenus en adjoignant au corps $\mathbf{Q}$ des rationnels la somme des racines l-ièmes de deux éléments conjugués d'un corps quadratique. Sous certaines conditions, nous obtenons ainsi des corps, généralement non galoisiens, que nous appelons « Tchebycheviens » (en raison du lien qui unit le polynôme minimal de leurs générateurs et les polynômes classiques de Tchebychev). Ces corps sont une généralisation naturelle des corps cubiques: en effet, les formules de Cardan montrent que tout corps cubique est obtenu en adjoignant à $\mathbf{Q}$ la somme des racines cubiques de deux éléments conjugués d'un corps quadratique. Les corps ainsi obtenus possèdent certaines propriétés remarquables que nous développons pour elles-mêmes dans les trois premiers paragraphes de ce travail.

Dans le premier paragraphe, nous définissons et étudions les propriétés générales de ces corps (dans cette partie il n'est pas nécessaire de supposer l premier et nous remplaçons l par un entier n impair quelconque).

Dans le second paragraphe, nous calculons leurs discriminants par la méthode des représentations d'Artin.

Dans le troisième paragraphe, nous donnons la loi de décomposition des nombres premiers dans ces corps non galoisiens.

Enfin, dans le quatrième paragraphe, nous établissons les propriétés de divisibilité des nombres de classes annoncées au début en construisant des corps tchébychéviens dont les clôtures galoisiennes sont des extensions abéliennes non ramifiées de degré l de certains corps cycliques de degré $l - 1$. Les paragraphes 2, 3 et 4 sont essentiellement indépendants; seuls quelques lemmes établis au paragraphe 2 servent dans les paragraphes 3 et 4.

L'idée d'étudier les corps tchébychéviens m'a été donnée par Pierre Barrucand; les trois premiers paragraphes de ce travail ont été élaborés avec lui; je tiens à le remercier ici.

0) Notations

Nous désignons par n un nombre positif impair (dans les parties 2), 3) et 4) ce n sera supposé premier, nous poserons alors $n = l$), par K le corps quadratique $\mathbf{Q}(\sqrt{d})$ où d est sans carré, par δ le discriminant de K et par ξ et $\bar{\xi}$ deux entiers conjugués (non rationnels) de K tels que $\xi\bar{\xi} = M^n$ où M est un entier rationnel. Nous choisissons une racine n-ième de ξ que nous notons $\sqrt[n]{\xi}$ et nous posons $\sqrt[n]{\bar{\xi}} = M/\sqrt[n]{\xi}$, $\zeta = \exp\left(\frac{2\pi i}{n}\right)$, $\omega = \cos\left(\frac{2\pi}{n}\right)$ et $L = \mathbf{Q}\left(\omega, \sqrt{d(\omega^2 - 1)}\right)$. Pour tout entier positif k, nous posons

$$t_k = (\sqrt[n]{\xi})^k + (\sqrt[n]{\bar{\xi}})^k, \quad t^{(k)} = \zeta^k \sqrt[n]{\xi} + \zeta^{-k} \sqrt[n]{\bar{\xi}},$$

$T^{(k)} = \mathbf{Q}(t^{(k)})$, $t = t^{(0)}$ et $T = T^{(0)}$. Nous désignons par N la clôture galoisienne de T. Enfin, si A est un anneau, A^n est le semi-groupe des puissanceses n-ièmes des élémentsde A et A^* est le groupe des éléments inversibles de A.

1) Etude générale

1.1. *Une famille de polynômes*

Pour tout entier positif k, nous désignons par $T_k(X)$ le polynôme vérifiant $T_k(e^z + e^{-z}) = e^{kz} + e^{-kz}$ (c'est-à-dire, à une légère modification

près, le k-ième polynôme de Tchébychev de 1ère espèce). On a $T_0(X) = 2$, $T_1(X) = X$ et $T_k(X) = XT_{k-1}(X) - T_{k-2}(X)$.

Posons $P_k(X; M) = M^{k/2} T_k(X/\sqrt{M})$. On vérifie que, pour $k > 0$, les $P_k(X; M)$ sont des polynômes unitaires de degré k à coefficients entiers, que $P_0(X; M) = 2$, que $P_1(X; M) = X$ et que $P_k(X; M) = XP_{k-1}(X; M) - MP_{k-2}(X; M)$.

LEMME 1.1.1. *Pour tout entier positif k, on a $P_k(t; M) = t_k$.*

Démonstration. Soit z un nombre complexe tel que $e^z = \sqrt[n]{\xi}/\sqrt{M}$, alors $e^z + e^{-z} = t/\sqrt{M}$ et donc $P_k(t; M) = M^{k/2} T_k(t/\sqrt{M}) = M^{k/2}(e^{kz} + e^{-kz}) = t_k$.

Soit $tr(\xi) = \xi + \bar{\xi}$; le lemme précédent appliqué avec $k = n$ montre que $P_n(t, M) - tr(\xi) = 0$. De même, pour tout j on a $P_n(t^{(j)}; M) - tr(\xi) = 0$. On voit facilement que les $t^{(j)}$ sont distincts deux à deux (car ξ n'est pas rationnel), ce sont donc les n racines de $P_n(X; M) - tr(\xi)$. De cela on déduit le lemme suivant:

LEMME 1.1.2. *ξ est une puissance n-ième dans K si et seulement si le polynôme $P_n(X; M) - \mathrm{tr}(\xi)$ admet une racine rationnelle* qui permet très simplement de savoir si ξ est une puissance n-ième dans K. Enfin on a le critère d'irréductibilité suivant:

PROPOSITION 1.1.3. *Le polynôme $P_n(X; M) - \mathrm{tr}(\xi)$ est irréductible si et seulement si, pour aucun diviseur premier l de n, le polynôme $P_l(X; M^{n/l}) - \mathrm{tr}(\xi)$ n'a de racines rationnelles.*

Démonstration. Notre polynôme est irréductible si et seulement si le corps $T = \mathbf{Q}(t)$ est de degré n sur $\mathbf{Q}$. Mais, n étant impair, T est de degré n sur $\mathbf{Q}$ si et seulement si $K(\sqrt[n]{\xi})$ est une extension de degré n sur K. Cela équivaut à ce que, pour aucun diviseur premier l de n, le nombre ξ n'est une puissance l-ième dans K; on conclut à l'aide du lemme précédent.

1. 2. *Les corps tchebycheviens*

DÉFINITION 1. 2. 1. Le corps T obtenu par le procédé précédent est dit tchebychevien si il est de degré n sur $\mathbf{Q}$. Dans ce cas on dira que T est le corps tchebychevien associé à ξ ou que ξ est un entier quadratique définissant le corps tchebychevien T.

Dans toute la suite, nous supposons que T est tchebychevien. Les $T^{(j)}$ sont donc les conjugués de T; le corps T est totalement réel si $d < 0$ et simplement réel (i.e. un et un seul conjugué réel) si $d > 0$. De plus, pour tout diviseur m de n, le corps $\mathbf{Q}(t_m)$ est un sous-corps de T qui est tchebychevien de degré n/m sur $\mathbf{Q}$; en conséquence, si $n = \pi_j l_j^{v_j}$ est la décomposition canonique de n et si $n_j = n/l_j^{v_j}$, alors T est le composé des corps tchebycheviens $\mathbf{Q}(t_{n_j})$.

Nous allons maintenant déterminer la clôture galoisienne N du corps tchebychevien T. Pour cela nous aurons besoin d'un lemme:

LEMME 1.2.2. *Le nombre* $t^* = \sqrt{d}\,(\sqrt[n]{\xi} - \sqrt[n]{\bar{\xi}})$ *appartient à* T.

Démonstration. On a $(\sqrt[n]{\xi})^2 - t(\sqrt[n]{\xi}) + M = 0$ donc $K(\sqrt[n]{\xi}) = T(\sqrt[n]{\xi}) = T(\sqrt{t^2-4M})$. D'autre part $K(\sqrt[n]{\xi})$ contient $T(\sqrt{d})$; ces deux corps ayant même degré sur $\mathbf{Q}$ sont égaux. En conséquence, l'automorphisme non trivial de $K(\sqrt[n]{\xi})/T$ envoie $\sqrt{d}$ sur $-\sqrt{d}$ et $\sqrt{t^2-4M}$ sur $-\sqrt{t^2-4M}$ donc laisse invariant $\sqrt{d}\sqrt{t^2-4M}$; cet élément est donc dans T. On conclut en remarquant que les deux racines de l'équation $X^2 - tX + M = 0$ sont $\sqrt[n]{\xi}$ et $\sqrt[n]{\bar{\xi}}$ donc que $\sqrt[n]{\xi} - \sqrt[n]{\bar{\xi}} = \sqrt{t^2-4M}$ (au signe près).

On peut maintenant démontrer la proposition suivante:

PROPOSITION 1.2.3. *La clôture galoisienne* N *de* T *est le corps* $\mathbf{Q}(t, \omega, \sqrt{d(\omega^2-1)})$ *c'est-à-dire le composé* TL *de* T *et* L.

Démonstration. Les conjugués de t étant les $t^{(j)}$, on a $N = \mathbf{Q}(t=t^{(0)}, t^{(1)}, \ldots, t^{(n-1)})$. On a $t^{(1)} + t^{(n-1)} = 2\omega t$ et $t^{(1)} - t^{(n-1)} = +2i \sin \frac{2\pi}{n}(\sqrt[n]{\xi} - \sqrt[n]{\bar{\xi}})$, soit $t^{(1)} - t^{(n-1)} = +2\sqrt{d(\omega^2-1)}\frac{t^*}{d}$ (où t^* est défini dans le lemme précédent). En conséquence $\mathbf{Q}(t, \omega, \sqrt{d(\omega^2-1)})$ est inclus dans N. D'autre part, pour tout j on a $t^{(j)} = 2t\cos\left(j\frac{2\pi}{n}\right) +$

$$2i\frac{t^*}{\sqrt{d}}\sin\left(j\frac{2\pi}{n}\right) = 2t\cos\left(j\frac{2\pi}{n}\right) + 2\sqrt{d(\omega^2-1)}\,\frac{\sin\left(j\frac{2\pi}{n}\right)}{\sin\left(\frac{2\pi}{n}\right)}\,\frac{t^*}{d}.$$

Mais $\cos\left(j\frac{2\pi}{n}\right)$ et $\dfrac{\sin\left(j\frac{2\pi}{n}\right)}{\sin\left(\frac{2\pi}{n}\right)}$ sont dans $\mathbf{Q}(\omega)$ et t^* est dans $\mathbf{Q}(t)$, donc $t^{(j)}$ est dans $\mathbf{Q}(t, \omega, \sqrt{d(\omega^2-1)}$ et donc N est inclus dans $\mathbf{Q}(t, \omega, \sqrt{d(\omega^2-1)})$, ce qui achève la démonstration.

Le corps $L = \mathbf{Q}(\omega, \sqrt{d(\omega^2-1)})$ est une extension cyclique de $\mathbf{Q}$ de degré $\varphi(n)$ (φ est l'indicateur d'Euler) sauf si K est un sous-corps imaginaire de $\mathbf{Q}(\zeta)$ auquel cas ce degré est $\frac{\varphi(n)}{2}$. Si n est premier, on montre facilement la proposition suivante:

PROPOSITION 1.2.4. *Si n est premier et si K n'est pas un sous-corps imaginaire de $\mathbf{Q}(\zeta)$, alors* Gal $(N/\mathbf{Q})$ *est isomorphe au groupe métacyclique* (c'est-à-dire au groupe multiplicatif des matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ où a et b sont dans le corps à n éléments et $a \neq 0$).

Démonstration. N est la clôture galoisienne d'un corps résoluble de degré premier. Le groupe Gal $(N/\mathbf{Q})$ est donc isomorphe à un sous-groupe du groupe métacyclique. Mais Gal $(L/\mathbf{Q})$ est un quotient d'ordre $\varphi(n)$ de Gal $(N/\mathbf{Q})$, ce dernier est donc le groupe métacyclique tout entier.

Le nombre n étant toujours supposé premier, le cas où K est un sous-corps imaginaire de $\mathbf{Q}(\zeta)$ se traite de la même manière. Si $K \neq \mathbf{Q}\sqrt{-3}$ ou si $n \neq 3$, on trouve que Gal $(N/\mathbf{Q})$ est isomorphe au sous-groupe d'indice 2 du groupe métacyclique formé des matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ où a est un carré non nul dans le corps à n éléments. Si $K = \mathbf{Q}(\sqrt{-3})$ et $n = 3$, alors $L = \mathbf{Q}$ donc $N = T$ est une extension cyclique d'ordre 3 de $\mathbf{Q}$.

Remarque. Dans le cas général (i.e. n non premier) on a un résultat analogue: si K n'est pas un sous-corps imaginaire de $\mathbf{Q}(\zeta)$, le groupe Gal $(N/\mathbf{Q})$ est isomorphe au sous-groupe du groupe multiplicatif de l'anneau $M_2(\mathbf{Z}/n\mathbf{Z})$ des matrices 2×2 sur l'anneau $\mathbf{Z}/n\mathbf{Z}$ formé des matrices du type $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ où a est inversible. Si K est un sous-corps imaginaire de $\mathbf{Q}(\zeta)$

différent de $\mathbf{Q}(\sqrt{-3})$ où si 3 ne divise pas n, alors Gal $(N/\mathbf{Q})$ est un sous-groupe d'indice 2 du groupe précédent.

Enfin, si ξ_1 et ξ_2 sont deux entiers de K dont les normes sont les puissances n-ièmes de rationnels mais qui, pour aucun diviseur premier l de n, ne sont des puissances l-ièmes dans K, on a la proposition suivante:

PROPOSITION 1.2.5. *Les corps* T_1 et T_2 *coïncident si et seulement si* $\xi_1 = \xi_2^k \eta^n$ *où* k *est un entier premier à* n *et où* η *est un élément de* K.

Démonstration. Si $T_1 = T_2$, on voit facilement que $K(\zeta, \sqrt[n]{\xi_1}) = K(\zeta, \sqrt[n]{\xi_2})$ et donc (théorie de Kummer) $\xi_1 = \xi_2^k \psi^n$ où k est un entier premier à n et où ψ est un élément de $K(\zeta)$. On sait ([6] par exemple) que cela implique une égalité $\xi_1 = \xi_2^k \eta^n$ avec η dans K. Réciproquement, si $\xi_1 = \xi_2^k \eta^n$, on a $\sqrt[n]{\xi_1} + \sqrt[n]{\bar{\xi}_1} = \eta^n \sqrt[n]{\xi_2^k} + \bar{\eta}^n \sqrt[n]{\bar{\xi}_2^k}$. Posons $\eta = \alpha + \beta\sqrt{d}$, il vient $\sqrt[n]{\xi_1} + \sqrt[n]{\bar{\xi}_1} = \alpha(\sqrt[n]{\xi_2^k} + \sqrt[n]{\bar{\xi}_2^k}) + \beta\sqrt{d}\,(\sqrt[n]{\xi_2^k} - \sqrt[n]{\bar{\xi}_2^k})$. Les lemmes 1.1.1 et 1.2.2 montrent que $\sqrt[n]{\xi_2^k} + \sqrt[n]{\bar{\xi}_2^k}$ et $\sqrt{d}\,(\sqrt[n]{\xi_2} - \sqrt[n]{\bar{\xi}_2^k})$ sont dans T_2, donc que T_1 est inclus dans T_2; ces corps ayant même degré, on a $T_1 = T_2$. C.Q.F.D.

REMARQUE 1.2.6. Si $n = 3$, les formules de Cardan montrent que les corps tchebycheviens coïncident avec les corps cubiques non purs (un corps pur étant un corps du type $\mathbf{Q}(\sqrt[3]{m})$ avec m rationnel).

2) LE CALCUL DU DISCRIMINANT

Nous supposons maintenant que n est premier (impair); pour souligner cette hypothèse nous posons $n = l$. Nous allons calculer le discriminant Δ du corps T. Comme on pourra le constater sur la formule, ce discriminant n'est pas, en général, le discriminant du polynôme définissant T. La formule est donnée dans le premier paragraphe.

2.1. *La formule*

Nous supposerons dans toute cette partie que l'entier quadratique ξ n'est divisible par la puissance l-ième d'aucun idéal premier de K qui divise l;

tous les corps tchebycheviens sont obtenus à l'aide de tels entiers (en effet, l'idéal principal engendré par ξ s'écrit $a^l b$ où a et b sont des idéaux entiers et où b n'est divisible par la puissance l-ième d'aucun idéal premier; choisissons dans la classe de a un idéal c premier à l et désignons par α un générateur de $a^{-1}c$; le nombre $\xi\alpha^l$ est un entier de K qui n'est divisible par la puissance l-ième d'aucun idéal premier contenant l et le corps tchebychevien défini par cet entier est celui défini par ξ). Pour énoncer la formule du discriminant, nous aurons besoin de quelques préliminaires. Pour tout entier i, on définit les entiers rationnels a_i et b_i par l'égalité $\xi^i = \frac{1}{2}(a_i + b_i\sqrt{d})$; on a alors le lemme suivant:

LEMME 2.1.1. *On suppose que l ne divise pas la norme de ξ, alors*

I) *il existe un entier τ premier à l tel que l divise le produit $b_\tau d$ (et on peut toujours trouver un tel τ divisant $l - (\frac{d}{l})$)*

II) *si, pour un entier τ premier à l, le produit $b_\tau d$ est divisible par l^2, alors pour tout entier i premier à l, le produit $b_i d$ est divisible par l^2 dès qu'il est divisible par l.*

Démonstration

I) Si l divise d, c'est clair. Si $(\frac{d}{l}) = 1$, alors ξ^{l-1} est congru à 1 modulo l i.e. $\xi^{l-1} = 1 + l\,\frac{\alpha + \beta\sqrt{d}}{2}$ avec α et β entiers rationnels. On a donc $b_{l-1} = l\beta$ c'est-à-dire que l divise b_{l-1}. De même si $(\frac{d}{l}) = -1$, alors ξ^{l+1} est congru à un entier rationnel modulo l et le même raisonnement montre que l divise b_{l+1}.

II) Soit τ un entier premier à l tel que l divise $b_\tau d$. Il est facile de voir que l^2 divise $b_\tau d$ si et seulement si ξ^τ est congru à un entier rationnel modulo le carré d'un idéal premier de K au-dessus de l. On conclut en remarquant qu'alors, pour tout entier i premier à l tel que ξ^i est congru à un rationnel modulo l, cet entier quadratique ξ^i est congru à un rationnel modulo l^2.

On définit j de la manière suivante: on pose $j = 1$ si l ne divise pas la norme de ξ et si, pour les entiers i premiers à l, le produit $b_i d$ est divisible par l^2 dès qu'il est divisible par l et on pose $j = 0$ sinon. De plus si c est le plus grand entier naturel divisant ξ et si $c = c_1 c_2^l$ où c_1 est sans puissance l-ième, on pose $g = \prod_{\substack{p \mid c_1 \\ (\frac{d}{p}) = 1}} p$. Enfin on pose $\lambda = \frac{l-1}{2}$ ou $\frac{l+1}{2}$ suivant que l est congru à 1 ou à 3 modulo 4 et on désigne par (l, d) le p.g.c.d de l et de d. Le discriminant Δ de T est alors donné par la formule suivante:

$$|\Delta| = \frac{l^{l-2j} \, |\delta|^{(l-1)/2} \, g^{l-1}}{(l, d)^{j\lambda}} \tag{2.1.2}$$

(On rappelle que δ est le discriminant du corps $K = \mathbf{Q}(\sqrt{d})$.

2.2. *Démonstration de la formule*

Rappelons qu'un élément ξ de K est dit l primaire si il est étranger à l et si l'extension de Kummer $K(\zeta, \sqrt[l]{\xi})/K(\zeta)$ est non ramifiée au-dessus de l. On a alors la proposition suivante:

PROPOSITION 2.2.1. *L'entier j étant celui défini au paragraphe précédent, on a $j = 1$ ou 0 suivant que ξ est ou n'est pas l-primaire.*

Démonstration. Pour plus de concision, nous supposerons dans cette démonstration que le corps K n'est pas inclus dans $\mathbf{Q}(\zeta)$; le cas où K est inclus dans $\mathbf{Q}(\zeta)$ se traite de façon analogue. Nous désignons par $\mathfrak{L}$ un idéal premier de $K(\zeta)$ au dessus de l et par $\mathfrak{l}$ l'intersection de $\mathfrak{L}$ et de K. On vérifie que l'indice de ramification de $\mathfrak{L}$ sur $\mathbf{Q}$ est $l - 1$, donc ([7], § 39, satz 118-119; [8]) ξ est l-primaire si et seulement si il existe dans $K(\zeta)$ un élément x tel que l'on ait la congruence suivante:

$$(*) \qquad \xi \equiv x^l \pmod{\mathfrak{L}^l}.$$

Montrons que (*) est équivalente à la congruence suivante:

(**) $\xi \equiv y^l \pmod{\mathfrak{I}^2}$ avec y dans K.

Si $\mathfrak{L}$ est le seul idéal premier de $K(\zeta)$ au dessus de $\mathfrak{I}$, alors en prenant les normes dans l'extension $K(\zeta)/K$, la congruence (*) implique $N_{K(\zeta)/K}(\xi) \equiv (N_{K(\zeta)/K}(x))^l \pmod{\mathfrak{L}^l}$ d'où $\xi^{l-1} \equiv z^l \pmod{l^2}$ avec z dans K ce qui implique (**). Sinon, soit K_1 le corps de décomposition de $\mathfrak{I}$ dans $K(\zeta)/K$ et $\mathfrak{I}_1$ l'intersection de $\mathfrak{L}$ et de K_1. L'idéal $\mathfrak{L}$ étant le seul idéal de $K(\zeta)$ au dessus de $\mathfrak{I}_1$ et le degré de $K(\zeta)/K$, étant $\dfrac{l-1}{2}$ un raisonnement analogue à celui que l'on vient de faire montre que (*) implique l'existence d'un z_1 dans K_1 vérifiant la congruence $\xi^{\frac{l-1}{2}} \equiv z_1^l \pmod{\mathfrak{I}_1^2}$; l'idéal $\mathfrak{I}$ étant totalement décomposé dans K/K_1 cela implique l'existence d'un z dans K tel que $\xi^{\frac{l-1}{2}} \equiv z^l \pmod{\mathfrak{I}^2}$ ce qui entraîne (**). Réciproquement, si $\mathfrak{I}$ est totalement ramifié dans $K(\zeta)/K$, alors (**) implique $\xi \equiv y^l \pmod{\mathfrak{L}^{2(l-1)}}$ ce qui donne (*). Sinon, l est ramifié dans K; désignons alors par A l'anneau des entiers K. Le noyau de la surjection canonique de $(A/\mathfrak{I}^3)^*$ sur $(A/\mathfrak{I}^2)^*$ est le sous groupe de $(A/\mathfrak{I}^3)^*$ formé des classes des $1 + kl$ où $k = 0, \ldots, l-1$. La congruence (**) implique donc l'existence d'un entier k compris entre 0 et $l-1$ tel que $\xi \equiv (1+kl)\, y^l \pmod{\mathfrak{I}^3}$. En prenant la norme sur $\mathbf{Q}$, il vient $M^l \equiv (1+kl)^2 \left(N_{K/Q}(y)\right)^l \pmod{l^2}$ et donc $1 + kl$ est une puissance l-ième modulo l^2 i.e. modulo l'idéal $\mathfrak{I}^4$. On a donc $\xi \equiv x^l \pmod{\mathfrak{I}^3}$ d'ou $\xi \equiv x^l \pmod{\mathfrak{L}^{3(l-1)/2}}$ ce qui implique (*) et achève la démonstration de l'équivalence de (*) et (**).

Soit maintenant i un entier tel que l divise $b_i d$. On a $N_{K/\mathbf{Q}}(\xi^i) = M^{il} = \frac{1}{4}(a_i^2 + b_i^2 d)$. D'autre part $b_i^2 d/4$ est dans l'idéal $\mathfrak{I}^2$ (en effet, si l ne divise pas d, alors l divise b_i donc l^2 divise b_i^2 et, si l divise d, alors l est dans $\mathfrak{I}^2$). Le rationnel $a_i^2/4$ est donc une $\mathfrak{I}$-unité qui est une puissance l-ième modulo $\mathfrak{I}^2$; il en est donc de même de $2/a_i$. En conséquence ξ^i est une puissance l-ième modulo $\mathfrak{I}^2$ si et seulement si $(2/a_i)\,\xi^i = 1 + b_i a_i^{-1} \sqrt{d}$ en est une. Si l^2 ne divise pas $b_i d$, alors $1 + b_i a_i^{-1} \sqrt{d}$ est congru à 1 modulo $\mathfrak{I}$ mais pas modulo $\mathfrak{I}^2$ donc n'est pas une puissance l-ième modulo $\mathfrak{I}^2$. Si l^2 divise $b_i d$ et si l ne divise pas d alors $1 + b_i a_i^{-1} \sqrt{d}$ est congru à 1 modulo $\mathfrak{I}^2$ donc est une puissance l-ième modulo l^2. Si l^2 divise $b_i d$ et si l divise d, alors $1 + b_i a_i^{-1} \sqrt{d}$ est congru à 1 modulo $\mathfrak{I}^3$ donc est une puissance l-ième modulo $\mathfrak{I}^2$ ce qui achève la démonstration.

Venons-en maintenant à la démonstration de la formule 2.1.2. Pour alléger la rédaction, nous supposerons encore que K n'est pas inclus dans $\mathbf{Q}(\zeta)$; le cas ou K est inclus dans $\mathbf{Q}(\zeta)$ se traite de manière analogue. Cette démonstration repose essentiellement sur les méthodes décrites dans [8], nous adopterons donc pour l'essentiel les notations et la terminologie de cet ouvrage.

On sait ([8], chap. IV, prop. 6, cor. 1) que le discriminant Δ de T est le conducteur d'Artin de la représentation de Gal $(N/\mathbf{Q})$ induite par la représentation triviale de Gal (N/T). Pour calculer ce conducteur désignons par $(\chi_k)_{k=1,\ldots,l-1}$ les $l-1$ représentations non triviales de degré 1 de Gal (N/L), par $1_{N/\mathbf{Q}}$ et $1_{N/T}$ les représentations triviales de Gal $(N/\mathbf{Q})$ et de Gal (N/T) et, pour toute représentation ρ d'un sous-groupe de Gal $(N/\mathbf{Q})$ par ρ^* la représentation induite par ρ sur Gal $(N/\mathbf{Q})$. On a alors l'égalité $(l-1)\,1^*_{N/T} = (l-1)\,1_{N/\mathbf{Q}} + \sum_{k=1}^{l-1} \chi_k^*$ comme on le vérifie en calculant le caractère de chacun des deux membres. De cette égalité on tire, en prenant les conducteurs d'Artin, l'égalité

$$\Delta^{l-1} = \prod_{k=1}^{l-1} f(\chi_k^*) \tag{2.2.2}$$

où $f(\chi_k^*)$ est le conducteur d'Artin de χ_k^*.

Le conducteur d'Artin de χ_k^* est le produit du discriminant d_L du corps L par la norme sur $\mathbf{Q}$ du conducteur d'Artin de χ_k. Ce dernier étant le conducteur de l'extension abélienne N/L, la formule 2.2.2 donne

$$\Delta = d_L\, N_{L/\mathbf{Q}}(\mathfrak{f}) \tag{2.2.3}$$

où $\mathfrak{f}$ est le conducteur de l'extension abélienne N/L.

Le calcul de d_L ne pose pas de difficulté, on trouve:

$$d_L = \begin{cases} l^{l-2}\left[\dfrac{\delta}{(l,d)}\right]^{(l-1)/2} & \text{si} \quad l \equiv 1 \bmod 4 \\ \dfrac{l^{l-2}}{(l,d)}\left[\dfrac{\delta}{(l,d)}\right]^{(l-1)/2} & \text{si} \quad l \equiv 3 \bmod 4 \end{cases} \tag{2.2.4}$$

Le calcul de Δ est donc ramené à celui du conducteur $\mathfrak{f}$ de l'extension N/L. Cette extension étant cyclique de degré l et le corps N étant galoisien sur $\mathbf{Q}$, l'idéal $\mathfrak{f}$ est de la forme

$$\mathfrak{f} = \left(\prod_{\mathfrak{L}} \mathfrak{L}\right)^x \times (\Pi\, \mathfrak{p}) \tag{2.2.5}$$

où x est un entier naturel, où $\mathfrak{L}$ décrit les idéaux premiers de L qui contiennent l et où $\mathfrak{p}$ décrit les idéaux premiers de L étrangers à l et ramifiés dans N. Avec les notations introduites dans 2.1, on a la proposition suivante:

PROPOSITION 2.2.6. *Soit p un nombre premier différent de l. Les idéaux premiers de L contenant p se ramifient dans N si et seulement si p divise c_1 et $\left(\frac{d}{p}\right) = 1$ (on convient que $\left(\frac{d}{2}\right) = 1$ si et seulement si 2 est décomposé dans K).*

Démonstration. Soit $\mathfrak{p}'$ un idéal premier de $K(\zeta)$ au dessus de p. Posons $\mathfrak{P} = \mathfrak{p}' \cap K$ et $\mathfrak{p} = \mathfrak{p}' \cap L$. Le comportement de $\mathfrak{p}$ dans N/L est identique à celui de $\mathfrak{p}'$ dans $N(\zeta)/K(\zeta)$. Mais $N(\zeta) = K(\zeta, \sqrt[l]{\xi})$ donc $\mathfrak{p}'$ se ramifie dans $N(\zeta)/K(\zeta)$ si et seulement si son exposant dans l'idéal de $K(\zeta)$ engendré par ξ est premier à l. Le degré de $K(\zeta)/K$ étant premier a l, ceci est équivalent à ce que l'exposant de $\mathfrak{p}$ dans l'idéal de K engendré par ξ est lui même premier à l. La norme de ξ étant une puissance l-ième, cela implique que p se décompose dans K i.e. que $\left(\frac{d}{p}\right) = +1$. Dans ce cas, en remplaçant éventuellement $\mathfrak{P}$ par son conjugué, l'idéal de K engendré par ξ est de la forme $(p)^{x_1}\,\mathfrak{p}^{x_2}\,\mathfrak{a}$ où (p) est l'idéal principal de K engendré par p, où x_1 et x_2 sont deux entiers naturels et où $\mathfrak{a}$ est un idéal de K étranger à p. Il résulte de la définition de c_1 que p divise c_1 si et seulement si l ne divise pas x_1. Mais $2x_1 + x_2$ est l'exposant de p dans la norme de ξ donc est divisible par l. En conséquence $x_1 + x_2$ qui est l'exposant de $\mathfrak{p}$ dans l'idéal engendré de K engendré par ξ est divisible par l si et seulement si l divise x_1 et donc si et seulement si p ne divise pas c_1 ce qui achève la démonstration.

Il reste à calculer le x de la formule 2.2.5. Pour celà, on choisit un idéal premier $\mathfrak{L}'$ de $K(\zeta)$ au dessus de l et on pose $\mathfrak{l} = \mathfrak{L}' \cap K$ et $\mathfrak{L} = \mathfrak{L}' \cap L$. On désigne respectivement par s et s' les plus grands entiers tels que les groupes de ramifications d'indice inférieur s et s' de $\mathfrak{L}$ et $\mathfrak{L}'$ dans N/L et $N(\zeta)/K(\zeta)$ sont non triviaux (s et s' sont donc des entiers relatifs supérieurs ou égaux à -1). L'extension N/L étant cyclique de degré l, on sait que $x = s + 1$. On sait aussi que $s = -1$ est équivalent à la non ramification de $\mathfrak{L}$ dans N/L donc à $s' = -1$. Si $s \neq -1$, les valeurs de s et s' sont liées par le lemme suivant:

LEMME 2.2.7. *On suppose* $s' \neq -1$. *On a alors* $s = s'/2$ *ou* $s = s'$ *suivant que* $\mathfrak{L}$ *est ou n'est pas ramifié dans* $K(\zeta)/L$.

Démonstration. On désigne respectivement par $\hat{L}$, $\hat{N}$, $\hat{K}(\zeta)$ et $\hat{N}(\zeta)$ les complétés de L, N, $K(\zeta)$ et $N(\zeta)$ au dessus de l. Le degré de $K(\zeta)/L$ étant premier à l, les groupes de ramifications d'indice strictement positif de $\mathfrak{L}$ dans N/L sont identiques à ceux de ce même $\mathfrak{L}$ dans $N(\zeta)/L$ et à ceux de $\mathfrak{L}'$ dans $N(\zeta)/K(\zeta)$. Posons $G = \mathrm{Gal}\,(N(\zeta)/L)$ et $H = \mathrm{Gal}\,(N(\zeta)/N)$. Alors toujours avec les notations de [8], chap. IV), v défini par $v = \varphi_{\hat{N}(\xi)/\hat{N}}(s')$ est le plus grand réel tel que G^v est non trivial. Mais G^v est cyclique d'ordre l et H est d'ordre 2, donc v est le plus grand réel tel que $G^v H/H$ est non trivial. D'autre part $G^v H/H = (G/H)^v$ et $G/H = \mathrm{Gal}\,(\hat{N}/\hat{L})$ donc $\psi_{\hat{N}/\hat{L}}(v)$ est le plus grand réel tel que $\mathrm{Gal}\,(\hat{N}/\hat{L})_{\psi_{\hat{N}/\hat{L}}(v)}$ est non trivial ce qui signifie que $s = \psi_{\hat{N}/\hat{L}}(v)$. Enfin $\psi_{\hat{N}/\hat{L}}(v) = \psi_{\hat{N}/\hat{L}} \circ \psi_{\hat{N}(\zeta)/\hat{L}}(s') = \psi_{\hat{N}(\zeta)/\hat{N}}(s')$; on achève la démonstration en remarquant que $\psi_{\hat{N}(\xi)/\hat{N}}$ est la multiplication par 1/2 où l'identité suivant que $\mathfrak{L}$ est ou n'est pas ramifié dans $K(\zeta)/L$.

In ne nous reste donc plus qu'à calculer s'; c'est l'objet de la proposition suivante:

PROPOSITION 2.2.8. *Si* l *divise* c_1 *on a* $s' = l$. *Sinon, si* $j = 1$ *on a* $s' = -1$; *si* $j = 0$ *on a* $s' = \dfrac{l+1}{2}$ *ou* 1 *suivant que* l *divise ou ne divise pas* d.

Démonstration. Si l divise c_1 alors I divise ξ. Par hypothèse I^l ne divise pas ξ, donc l'exposant de I dans l'idéal principal engendré par ξ est premier à l. Le degré de $K(\zeta)/K$ étant premier à l, il en est de même de l'exposant de $\mathfrak{L}'$ dans l'idéal de $K(\zeta)$ engendré par ξ et donc ([7]) on a $s' = l$.

Si l ne divise pas c_1, il résulte des hypothèses faites sur ξ que I ne divise pas ξ. Si $j = 1$, alors ξ est l-primaire donc $\mathfrak{L}'$ est non ramifiée dans $N(\zeta)/K(\zeta)$ donc $s' = -1$. Si $j = 0$, on désigne par Y le plus grand entier tel que ξ est, dans $K(\zeta)$, une puissance l-ième modulo $\mathfrak{L}'^Y$. On sait ([7]) que $Y \leqslant l$ et que $s' = l - Y$. Il ne reste donc plus qu'à calculer Y. On a vu dans la démonstration de la proposition 2.2.1 que $j = 0$ est équivalent à ce que ξ est, dans K, congru à une puissance l-ième modulo I mais pas modulo l^2. Si l divise d, l'indice de ramification de $K(\zeta)/K$ est $\dfrac{l-1}{2}$ et

donc ξ est, dans $K(\zeta)$, congru à une puissance l-ième modulo $\mathfrak{L}'^{(l-1)/2}$ mais pas modulo $\mathfrak{L}'^{1+(l-1)/2}$; on a donc $s' = l - (l-1)/2 = (l+1)/2$. Si l ne divise pas d, l'indice de ramification de $K(\zeta)/K$ est $l-1$ et donc ξ est, dans $K(\zeta)$, congru à une puissance l-ième modulo $\mathfrak{L}'^{l-1}$ mais pas modulo $\mathfrak{L}'^{l}$; on a donc $s' = l - (l-1) = 1$, C.Q.F.D.

En regroupant tous ces résultats, on obtient la formule 2.1.2.

3) Décomposition des nombres premiers dans T

On désigne toujours par T un corps tchébychévien de degré premier l, par ξ un entier quadratique définissant T et assujetti à la condition imposée au début de la partie 2 de ce travail, par N la clôture galoisienne de T et par L le sous-corps d'indice l de N. De plus, si p est un nombre premier, on note $(p)_L$ et $(p)_T$ les idéaux principaux de L et T engendrés par p. Enfin, pour alléger la rédaction, on suppose dans toute cette partie que le degré de $N/\mathbf{Q}$ est $l(l-1)$.

On a la proposition suivante:

Proposition 3.1. *Soit p un nombre premier et $\mathfrak{p}$ un idéal premier de N au dessus de p; on note $\mathfrak{p}_L$ l'intersection de $\mathfrak{p}$ et de L.*

a) *Si $\mathfrak{p}_L$ est inerte dans N/L, alors p est inerte dans T (c'est-à-dire $(p)_T$ est un idéal premier de T).*

b) *Si $\mathfrak{p}_L$ est ramifié dans N/L, alors p est totalement ramifié dans T (i.e. l'idéal $(p)_T$ est la puissance l-ième d'un idéal premier de T).*

c) *Si $\mathfrak{p}_L$ est décomposé dans N/L et si $(p)_L = (\mathfrak{q}_1 \ldots \mathfrak{q}_{g_p})^{e_p}$ où $\mathfrak{q}_1, \ldots, \mathfrak{q}_{g_p}$ sont des idéaux premiers de L distincts deux à deux et de degré résiduel f_p, on a $(p)_T = \mathfrak{P}(\mathfrak{P}_1 \ldots \mathfrak{P}_{g_p})^{e_p}$ où $\mathfrak{P}, \mathfrak{P}_1, \ldots, \mathfrak{P}_{g_p}$ sont des idéaux premiers de T distincts deux à deux, le degré résiduel de $\mathfrak{P}$ étant 1 et les degrés résiduels des $\mathfrak{P}_i$ étant f_p.*

Démonstration.

a) L'hypothèse implique que le degré résiduel de $\mathfrak{p}$ dans N/Q est divisible par l. Posons $\mathfrak{p}_T = \mathfrak{p} \cap T$. Ce degré résiduel est le produit du degré résiduel de $\mathfrak{p}_T$ dans $T/\mathbf{Q}$ par le degré résiduel de $\mathfrak{p}$ dans N/T. L'extension N/T étant galoisienne, ce dernier doit diviser le degré de l'extension N/T; il est donc premier à l. En conséquence l divise le degré résiduel de $\mathfrak{p}_T$ dans $T/\mathbf{Q}$. Le degré de $T/\mathbf{Q}$ étant l, on a le résultat cherché.

b) Même démonstration qu'au a) en remplaçant « degré résiduel » par « indice de ramification ».

c) Notons $\sigma_1, \sigma_2, \ldots, \sigma_l$ les l automorphismes de l'extension N/L en convenant que σ_1 est l'identité. Pour $i = 1, \ldots, l$ on pose $\mathfrak{p}_i = \sigma_i(\mathfrak{p})$ (donc $\mathfrak{p}_1 = \mathfrak{p}$); par hypothèse les $\mathfrak{p}_i$ sont distincts deux à deux.

On désigne par $G_{-1}(\mathfrak{p}_i)$ le groupe de décomposition de $\mathfrak{p}_i$; l'ordre de $G_{-1}(\mathfrak{p}_i)$ est $e_p f_p$ qui est premier à l, donc le corps des invariants de $G_{-1}(\mathfrak{p}_i)$ contient au moins un conjugué de T; quitte à remplacer T par un de ses conjugués, on peut donc supposer que T est inclus dans $G_{-1}(\mathfrak{p}_1)$. On pose $\mathfrak{p}_{i,T} = \mathfrak{p}_i \cap T$ et $T^{(i)} = \sigma_i^{-1}(T)$. De plus on note $\hat{N}$ le complété de N en $\mathfrak{p}_1$ et $\hat{T}^{(i)}$ l'adhérence de $T^{(i)}$ dans $\hat{N}$. Avec nos choix des indices, on a $T^{(1)} = T$ et $\hat{T}$ est le corps $\mathbf{Q}_p$ des nombres p-adiques, ce qui signifie que $\mathfrak{p}_{1,T}$ est non ramifié et de degré résiduel 1 dans $T/\mathbf{Q}$. D'autre part, si $i > 1$, le composé $T.T^{(i)}$ est N, donc le composé $\hat{T}.\hat{T}^{(i)}$ est $\hat{N}$ et donc $\hat{T}^{(i)} = \hat{N}$. Cela signifie que le degré résiduel et l'indice de ramification de $\mathfrak{p}_1$ dans $N/\mathbf{Q}$, qui sont respectivement égaux à e_p et f_p, sont égaux à ceux de $\mathfrak{p}_1 \cap T^{(i)}$ dans $T^{(i)}/\mathbf{Q}$. Mais (toujours par le choix de nos indices) ceux-ci sont égaux à ceux de $\mathfrak{p}_i \cap T = \mathfrak{p}_{i,T}$ dans $T/\mathbf{Q}$. Enfin, l'extension N/T étant galoisienne, si $\mathfrak{p}_{k,T} = \mathfrak{p}_{l,T}$ alors il existe un τ dans Gal (N/T) tel que $\tau(\mathfrak{p}_k) = \mathfrak{p}_l$. Mais $\mathfrak{p}_k \cap L = \mathfrak{p}_l \cap L = \mathfrak{p}_L$, donc la restriction de τ à L est dans le groupe de décomposition de $\mathfrak{p}_L$ dans $L/\mathbf{Q}$. Ce groupe est d'ordre $e_p f_p = \dfrac{l-1}{g_p}$, donc τ est dans le sous-groupe de Gal (N/T) d'ordre $\dfrac{l-1}{g_p}$. En conséquence, parmi les $l-1$ idéaux $\mathfrak{p}_{2,T}, \ldots, \mathfrak{p}_{l,T}$ il y en a au moins g_p distincts. On a donc trouvé, dans T, au dessus de p, un idéal premier non ramifié de degré résiduel 1 dans $T/\mathbf{Q}$ et une collection d'au moins g_p idéaux premiers d'indice de ramification e_p et de degré résiduel f_p dans $T/\mathbf{Q}$. Comme $[T:\mathbf{Q}] = l = 1 + g_p e_p f_p$, cette collection d'idéaux premiers est constituée d'exactement g_p éléments et on a trouvé tous les idéaux premiers de T au dessus de p; celà achève la démonstration.

On rappelle (voir 2.1) que $j = 1$ ou 0 suivant que ξ est ou n'est pas l-primaire et que, si c est le plus grand entier rationnel divisant ξ, on a posé $c = c_1 c_2^l$ avec c_1 sans puissance l-ième et $g = \prod_{p \mid c_1} p$. En plus,

$$\left(\frac{d}{p}\right) = 1$$

pour tout nombre premier p, on pose $(p)_L = (\mathfrak{q}_1 \dots \mathfrak{q}_{g_p})^{e_p}$ où les $\mathfrak{q}_i$ sont des idéaux premiers de L distincts deux à deux de degré résiduel f_p dans $L/\mathbf{Q}$. L'extension $L/\mathbf{Q}$ étant cyclique, le calcul de e_p, f_p et g_p est simple.

Avec ces notations, on a:

THÉORÈME 3.2. La décomposition d'un nombre premier p dans T est donnée par les règles suivantes:

1) Si $p = l$ et si $j = 0$ on a $(l)_T = \mathfrak{l}^l$ où $\mathfrak{l}$ est un idéal premier de T. Si $j = 1$ on a $(l)_T = \mathfrak{l}(\mathfrak{l}_1, \dots \mathfrak{l}_{g_l})^{e_l}$ où $\mathfrak{l}, \mathfrak{l}_1 \dots, \mathfrak{l}_{g_l}$ sont des idéaux premiers de L distincts deux à deux, le degré résiduel de $\mathfrak{l}$ étant 1 et les degrés résiduels des $\mathfrak{l}_i$ étant f_l, sauf si $l = 3$, $d \equiv 6 \pmod 9$ et si $\xi = \frac{1}{2}(a+b\sqrt{d})$ avec b non divisible par 9 auquel cas 3 est inerte dans T (i.e. $(3)_T$ est premier).

2) Si p divise g, alors $(p)_T = \mathfrak{P}^l$ où $\mathfrak{P}$ est un idéal premier de T (si l divise g et $(\frac{d}{l}) = 1$, alors $j = 0$ et on retrouve un cas de 1)).

3) Si $p \neq l$ et si p ne divise pas g, alors en supposant ξ premier à p (ce à quoi on peut toujours se ramener quitte à changer le ξ définissant T), on a deux cas

a) Si ξ est, modulo un idéal premier de K au-dessus de p, une puissance l-ième, alors $(p)_T = \mathfrak{P}(\mathfrak{P}_1 \dots \mathfrak{P}_{g_p})^{e_p}$ où $\mathfrak{P}, \mathfrak{P}_1, \dots, \mathfrak{P}_{g_p}$ sont des idéaux premiers de T distincts deux à deux, le degré résiduel de $\mathfrak{P}$ étant 1 et les degrés résiduels des $\mathfrak{P}_i$ étant f_p.

b) Si ξ n'est pas, modulo un idéal premier de K au-dessus de p, une puissance l-ième, alors p est inerte dans T (i.e $(p)_T$ est un idéal premier).

De plus, si $p \not\equiv (\frac{d}{p}) \bmod l$, on est toujours dans le cas a). Sinon, pour tout entier k, posons $\xi^k = \frac{1}{2}(a_k + b_k\sqrt{d})$; on est dans les cas a) ou b) suivant qu'il existe ou qu'il n'existe pas de k divisant $\frac{1}{l}(p - (\frac{d}{p}))$ tel que p divise b_k.

Démonstration. Nous aurons besoin du lemme suivant:

LEMME 3.3. Soit p un nombre premier; si les idéaux premiers de L qui contiennent p sont inertes dans N/L, alors p est totalement décomposé dans L.

Démonstration du lemme. Soit $\mathfrak{p}$ un idéal premier de N contenant p et $\mathfrak{p}_L$ l'intersection de $\mathfrak{p}$ et de L. Supposons $\mathfrak{p}_L$ inerte dans N/L et désignons par G_{-1} et G_0 les groupes de décomposition et d'inertie de $\mathfrak{p}$ dans $N/\mathbf{Q}$, par N_{-1} et N_0 les corps des invariants de G_{-1} et de G_0, par $\hat{N}$ le complété de N en $\mathfrak{p}$ et par $\hat{N}_{-1}$, $\hat{N}_0$ et $\hat{L}$ les adhérences de N_{-1}, N_0 et L dans $\hat{N}$. Le corps $\hat{N}_{-1}$ est le corps $\mathbf{Q}_p$ des nombres p-adiques. L'extension $\hat{N}_0/\hat{N}_{-1}$ est cyclique non ramifiée et son degré est égal au degré résiduel de $\mathfrak{p}$ dans $N/\mathbf{Q}$ donc est divisible par l. Enfin, l'extension $\hat{L}/\mathbf{Q}_p$ est cyclique et son indice de ramification est e_p. Ce e_p est aussi l'indice de ramification de $\mathfrak{p}$ dans $N/\mathbf{Q}$; le composé $\hat{L}.\hat{N}_0$ est donc une extension abélienne de $\mathbf{Q}_p$ dont l'indice de ramification et le degré résiduel sont égaux à l'indice de ramification et au degré résiduel de $\mathfrak{p}$ dans $N/\mathbf{Q}$. En conséquence $\hat{N}$ est le composé $\hat{L}\hat{N}_0$, donc est abélien sur $\mathbf{Q}_p$ et donc G_{-1} est un groupe abélien. Mais, $\mathfrak{p}_L$ étant inerte dans N/L, l'ordre de G_{-1} est divisible par l. Le seul sous-groupe abélien de Gal $(N/\mathbf{Q})$ dont l'ordre divise l est Gal (N/L), donc G_{-1} est Gal (N/L) ce qui implique que p est totalement décomposé dans L, C.Q.F.D.

Revenons à la démonstration du théorème:

1) Soit $\mathfrak{L}$ un idéal premier de N au-dessus de l et $\mathfrak{L}_L$ l'intersection de $\mathfrak{L}$ et L. Si $j = 0$, alors $\mathfrak{L}_L$ est ramifié dans N/L et on conclut avec la proposition 3.1. Si $j = 1$, $\mathfrak{L}_L$ est non ramifié dans N/L, donc est décomposé ou inerte. Si $\mathfrak{L}_L$ est inerte, alors, d'après le lemme 3.3, l est totalement décomposé dans L. Le corps L étant une extension quadratique du sous-corps réel maximal du corps des racines l-ièmes de l'unité, on a nécessairement $l = 3$. Le corps L est alors $\mathbf{Q}(\sqrt{-3d})$ donc il faut $d \equiv 6 \pmod 9$ pour que 3 soit totalement décomposé dans L, ce qui démontre la première partie de notre assertion. Enfin, ξ étant 3-primaire, la proposition 2.2.1 montre que 3 divise b. On tire alors de [8], par des arguments analogues à ceux employés dans la démonstration de la proposition 2.2.1, que dans N/L, l'idéal $\mathfrak{L}_L$ est inerte si l ne divise pas b et décomposé si l divise b. Notre résultat est donc conséquence de la proposition 3.1.

2) Si $p \neq l$, la proposition 2.2.6 montre que les idéaux premiers de L au-dessus de p sont ramifiés dans N/L. Si $p = l$, alors $j = 0$ et on a le même résultat. On conclut alors à l'aide de la proposition 3.1.

3) La proposition 2.2.6 montre que les idéaux premiers de L au-dessus de p sont non ramifiés dans N/L; en conséquence, ils sont inertes ou décomposés. Ils sont décomposés si et seulement si les idéaux premiers de $\mathbf{Q}(\zeta)$ au-dessus de p sont décomposés dans $K(\zeta, \sqrt[l]{\xi})$ i.e si et seulement si ξ est une puissance l-ième dans les complétés de $K(\zeta)$ en les idéaux premiers qui divisent p. On sait (par exemple [4]) qu'il en est ainsi si et seulement si ξ est une puissance l-ième dans les complétés de K en les idéaux premiers qui divisent p. D'après le lemme de Hensel, il en est ainsi si et seulement si ξ est une puissance l-ième modulo les idéaux premiers de K qui divisent p. Comme de plus $\xi\bar{\xi}$ est une puissance l-ième, il en est ainsi si et seulement si ξ est une puissance l-ième modulo un des idéaux premiers de K qui divisent p; nos assertions a) et b) résultent donc de la proposition 3.1.

De plus, on vérifie facilement que si $p \not\equiv \left(\frac{d}{p}\right) \bmod l$, alors p n'est pas totalement décomposé dans L; on déduit donc du lemme 3.3 et de la proposition 3.1 que l'on est dans le cas a). Enfin, si $p \equiv \left(\frac{d}{p}\right) \bmod l$, alors $\left(\frac{d}{p}\right) \neq 0$. Si $\left(\frac{d}{p}\right) = 1$ (et donc $p \equiv 1 \bmod l$) alors p se décompose dans K en le produit de deux idéaux premiers $\mathfrak{p}$ et $\bar{\mathfrak{p}}$. Si ξ est une puissance l-ième modulo $\mathfrak{p}$, alors $\xi^{\frac{p-1}{l}}$ est congru à 1 modulo $\mathfrak{p}$. Mais $\xi\bar{\xi} = M^l$, donc $(\xi\bar{\xi})^{\frac{p-1}{l}} = M^{p-1}$ est congru à 1 modulo p. Il en résulte que $\bar{\xi}^{\frac{p-1}{l}}$ est aussi congru à 1 modulo $\mathfrak{p}$. Par conjugaison, on en déduit que $\xi^{\frac{p-1}{l}}$ est congru à 1 modulo $\bar{\mathfrak{p}}$, donc $\xi^{\frac{p-1}{l}}$ est congru à 1 modulo p, donc $b_{\frac{p-1}{l}}$ est divisible par p. Réciproquement, si p divise $b_{\frac{p-1}{l}}$, alors $\xi^{\frac{p-1}{l}}$ est congru à $a_{\frac{p-1}{l}}/2$ modulo p. En conséquence, $(\xi\bar{\xi})^{\frac{p-1}{l}} = M^{p-1}$ est congru à $(a_{\frac{p-1}{l}}/2)^2$ modulo p. Mais M^{p-1} est congru à 1 modulo p,

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.

[5] UCHIDA, Kenkichi. Unramifield extensions of quadratic number fields I. *Tôhoku Math. J. 22*:1 (1970), pp. 138-141.

[6] CHEVALLEY, Claude. Sur deux théorèmes d'arithmétiques. *J. of the Math. Soc. of Japan, 3* (1951), pp. 36-44.

[7] HECKE, E. *Vorlesungen über die Theorie der Algebraischen Zahlen.* Academic Verlag, Leipzig, 1923.

[8] SERRE, J. P. *Corps locaux.* Hermann. Paris.

[9] MORDELL, L. J. *Diophantine Equations.* Academic Press New York.

(Reçu le 24 mai 1978)

Philippe Satgé

Université de Caen
Département de Mathématiques
14032 Caen CEDEX.

NOTE.

Ce travail est un travail commun avec Pierre BARRUCAND. Seules des divergences sur la manière de présenter et de rédiger les résultats ont conduit à les publier sous le seul nom du rédacteur.