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: 1) Etude générale
DOI: https://doi.org/10.5169/seals-50376

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;