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: 2.2. Démonstration de la formule

DOI: https://doi.org/10.5169/seals-50376

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 $g = \prod\limits_{\substack{p \mid c_1 \\ \left(\frac{d}{p}\right) = 1}} p$. 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 audessus 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:

$$\xi \equiv x^l \pmod{\mathfrak{L}^l}. \tag{*}$$

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

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

Si $\mathfrak{L}$ est le seul idéal premier de $K(\zeta)$ au dessus de $\mathfrak{l}$, 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 $\mathfrak{l}$ dans $K(\zeta)/K$ et $\mathfrak{l}_1$ l'intersection de $\mathfrak{L}$ et de K_1. L'idéal $\mathfrak{L}$ étant le seul idéal de $K(\zeta)$ au dessus de $\mathfrak{l}_1$ 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 $\xi^{\frac{l-1}{2}} \equiv z_1^l \pmod{\mathfrak{l}_1^2}$; l'idéal $\mathfrak{l}$ étant totalement décomposé dans K/K_1 cela implique l'existence d'un z dans K tel que $\xi^{\frac{l-1}{2}} \equiv z^l \pmod{\mathfrak{l}^2}$ ce qui entraîne (**). Réciproquement, si $\mathfrak{l}$ 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 $(A/\mathfrak{l}^3)^*$ sur $(A/\mathfrak{l}^2)^*$ est le sous groupe de $(A/\mathfrak{l}^3)^*$ 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 $\xi \equiv (1+kl)\, y^l \pmod{\mathfrak{l}^3}$. En prenant la norme sur $\mathbf{Q}$, il vient $M^l \equiv (1+kl)^2 (N_{K/\mathbf{Q}}(y))^l \pmod{l^2}$ et donc $1 + kl$ est une puissance l-ième modulo l^2 i.e. modulo l'idéal $\mathfrak{l}^4$. On a donc $\xi \equiv x^l \pmod{\mathfrak{l}^3}$ 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 $\mathfrak{l}^2$ (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 $\mathfrak{l}^2$). Le rationnel $a_i^2/4$ est donc une $\mathfrak{l}$-unité qui est une puissance l-ième modulo $\mathfrak{l}^2$; il en est donc de même de $2/a_i$. En conséquence ξ^i est une puissance l-ième modulo $\mathfrak{l}^2$ 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 $\mathfrak{l}$ mais pas modulo $\mathfrak{l}^2$ donc n'est pas une puissance l-ième modulo $\mathfrak{l}^2$. 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 $\mathfrak{l}^2$ 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 $\mathfrak{l}^3$ donc est une puissance l-ième modulo $\mathfrak{l}^2$ 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:

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

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 $\mathfrak{l}$ divise ξ. Par hypothèse $\mathfrak{l}^l$ ne divise pas ξ, donc l'exposant de $\mathfrak{l}$ 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 $\mathfrak{l}$ 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 $\mathfrak{l}$ 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.