3) DÉCOMPOSITION DES NOMBRES PREMIERS DANS T

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **11.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

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*