IV. Bases entières d'une extension quadratique.

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **18 (1972)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Comme $[L_n:K_n]$ divise $p - 1$, pour que $\mathfrak{q}$ soit totalement décomposé dans K_n/k, il faut et il suffit qu'il le soit dans L_n/k. Et l'on obtient que le corps de décomposition de $\mathfrak{q}$ dans K/k est de degré fini sur k.

$$\begin{tikzcd} & K = k\Gamma \arrow[dl, dash] \arrow[dr, dash] & \\ \Gamma \arrow[dr, dash] & & k \arrow[dl, dash] \\ & \mathbf{Q} & \end{tikzcd}$$

. Supposons maintenant que $\mathcal{P}$ divise p, et soit Γ la Γ-extension cyclotomique de $\mathbf{Q}$ associée à p. On sait que p est totalement ramifié dans $\Gamma/\mathbf{Q}$. En utilisant la branche $\mathbf{Q}\,.\,k\,.\,K$ du diagramme, on obtient encore que le corps de décomposition de $\mathcal{P}$ est de degré fini sur k.

Remarque: On pourrait chercher à généraliser la proposition 4 au cas d'une Γ-extension quelconque d'un corps de nombres. En fait, ce résultat est faux. Montrons-le à partir d'un exemple dû à Hasse et décrit par B. Martel dans [10]. Soit $k = \mathbf{Q}(\sqrt{-m})$ un corps quadratique imaginaire. Définissons le groupe de congruences H_n modulo p^{n+1} comme groupe des idéaux principaux (x) de k, premiers à p, et tels qu'il existe un rationnel r vérifiant $x \equiv r$ modulo p^{n+1}. Si L_n est le corps de classes sur k associé à H_n, et K_n la p-extension maximale de k dans L_n, $K = \bigcup_n K_n$ est une Γ-extension de k linéairement disjointe sur k de la Γ-extension cyclotomique. F. Bertrandias nous a fait remarquer que si q est un nombre premier rationnel inerte dans $k/\mathbf{Q}$, et distinct de p, l'idéal (q) de k appartient à H_n quel que soit n. Donc (q) est totalement décomposé dans K/k.

Plus généralement, tout corps de nombres qui contient une extension quadratique imaginaire de $\mathbf{Q}$ admet une Γ-extension qui n'est pas de type J.

IV. Bases entières d'une extension quadratique.

1. *Critère d'existence d'une base entière.*

H. B. Mann précise dans [9] le critère d'Artin, lorsque L/K est une extension quadratique du corps des quotients K d'un anneau de Dedekind. Il énonce les deux théorèmes suivants:

THÉORÈME 4 (Mann).

Soit L une extension quadratique d'un corps K de caractéristique différente de 2. Pour que B soit A-libre, il faut et il suffit que l'idéal $\Delta_{L/K}$ soit principal, et engendré par D tel que $L = K(D^{1/2})$.

THÉORÈME 5 (Mann).

Soit $L = K(a^{1/2})$ *une extension quadratique d'idéal discriminant* Δ. *Posons* $(a) = \mathfrak{a}^2\mathfrak{c}$ *et* $\Delta = \delta^2\mathfrak{c}'$, *ou* $\mathfrak{c}$ *et* $\mathfrak{c}'$ *sont des idéaux entiers sans facteur carré. L'extension L/K admet une base entière si et seulement si* $\mathfrak{c} = \mathfrak{c}'$ *et* $\mathfrak{a} \sim \delta$ *(modulo les idéaux principaux).*

Le théorème 4 se généralise facilement au cas où K est une extension infinie du corps des quotients d'un anneau de Dedekind, de caractéristique différente de 2. Reprenons les notations du début. Supposons que L soit une extension quadratique de K, de discriminant un idéal principal engendré par l'entier D_1. Il existe un indice α_0 tel que pour tout $\alpha \geqq \alpha_0$. D_1 appartienne *à* A_α.

Supposons que L/K admette une base entière $\{\lambda, \mu\}$. Considérons un indice $\alpha \geqq \alpha_0$, tel que B_α contienne λ et μ : $\{\lambda, \mu\}$ est une base entière de L_α/K_α, et le théorème 4 donne $L_\alpha = K_\alpha(D^{1/2})$, D étant un générateur du discriminant. D'où $L = K(D^{1/2})$.

Inversement, si $L = K(D_1^{1/2})$, $L_\alpha = K_\alpha(D_1^{1/2})$. En appliquant le théorème 4 aux extensions L_α/K_α telles que $\alpha \geqq \alpha_0$, on obtient que L/K admet une base entière.

Pour généraliser le théorème 5, il nous faut une théorie de la divisibilité. *C'est pourquoi nous supposerons, pour le reste de ce paragraphe, que K est un corps de type J.*

Lemme.

Soient p un entier, et $\mathfrak{a}$ *un idéal de K.* $\mathfrak{a}$ *se décompose de manière unique en produit*

$$\mathfrak{a} = \mathfrak{b}^p \mathfrak{c}\mathfrak{c}'$$

$\mathfrak{b}$: *idéal fractionnaire dont toutes les composantes non triviales sont dans des stries finies.*

$\mathfrak{c}$: *idéal entier sans facteur puissance p-ième, dont toutes les composantes non-triviales sont dans des stries finies.*

$\mathfrak{c}'$: *idéal dont toutes les composantes non triviales sont dans des stries non finies.*

L'idéal $\mathfrak{a}$ se décompose de manière unique en produit d'idéaux $\mathfrak{a}_i$:

$$\mathfrak{a} = \mathfrak{a}_1 \times \mathfrak{a}_2 \times \ldots \times \mathfrak{a}_l$$

chaque $\mathfrak{a}_i$ appartenant à une strie maximale. Notons $\mathfrak{m}_i$ l'idéal maximal équivalent à $\mathfrak{a}_i$, et ordonnons les indices de manière que $\mathfrak{m}_1, \ldots, \mathfrak{m}_j$ soient de type fini, et que $\mathfrak{m}_{j+1}, \ldots, \mathfrak{m}_l$ ne le soient pas. Posons $\mathfrak{m}_i \cap k = \mathscr{P}_i$.

Puisque K est de type J, il n'existe dans K qu'un nombre fini d'idéaux premiers au-dessus de $\mathscr{P}_i$. Lorsque $1 \leqq i \leqq j$, on peut donc trouver un indice α_i tel que l'idéal $\mathscr{P}_i$ reste inerte dans K/K_{α_i}. Posons alors $\chi = K_{\alpha 1} \ldots K_{\alpha_j}$; c'est une extension finie de k. Et dans χ, l'idéal $\left(\prod_{i=1}^{j} \mathfrak{a}_i\right) \cap \chi$ se décompose de manière unique en:

$$\left(\prod_{i=1}^{j} \mathfrak{a}_i\right) \cap \chi = \mathfrak{b}_1{}^p \mathfrak{c}_1$$

$\mathfrak{c}_1$ idéal entier sans facteur puissance p-ième. L'idéal $\mathfrak{c}_1$ reste inerte dans K/χ, donc son étendu est sans facteur puissance p-ième.

On peut choisir alors comme idéaux $\mathfrak{b}$, $\mathfrak{c}$ et $\mathfrak{c}'$: $\mathfrak{b} = \mathfrak{b}_1 A$, $\mathfrak{c} = \mathfrak{c}_1 A$ et $\mathfrak{c}' = \mathfrak{a}_{j+1} \times \ldots \times \mathfrak{a}_l$.

L'unicité de cette décomposition provient de l'unicité de la décomposition en produit d'idéaux appartenant à des stries maximales.

Nous pouvons maintenant énoncer un résultat analogue au théorème 5:

Proposition 5.

Soient K un corps de type J, de caractéristique différente de 2, et $L = K(a^{1/2})$ une extension quadratique d'idéal discriminant Δ. Utilisons le lemme pour écrire

$$(a) = \mathfrak{a}^2 \mathfrak{b}\mathfrak{b}', \qquad \Delta = \mathfrak{c}^2 \delta\delta'.$$

Le A-module B est libre si et seulement si l'on peut trouver $\alpha \in K^*$ tel que

$$\mathfrak{c}^2 \delta' = (\alpha^2)\, \mathfrak{a}^2 \mathfrak{b}' \qquad \text{et} \qquad \mathfrak{b} = \delta.$$

En effet, si $\mathfrak{b} = \delta$ et $\mathfrak{c}^2 \delta' = (\alpha^2)\, \mathfrak{a}^2 \mathfrak{b}'$, $\Delta = (\alpha^2)\, \mathfrak{a}^2 \mathfrak{b}' \mathfrak{b} = (a\alpha^2)$. Le discriminant de l'extension L/K est principal, de générateur $a\alpha^2$, et $L = K((a\alpha^2)^{1/2})$. La généralisation du théorème 4 permet de conclure que B est A-libre.

Inversement, si B est A-libre, l'idéal Δ est principal; en vertu du même théorème, il est engendré par D tel que $L = K(D^{1/2})$. Donc

$$a^{1/2} = x + yD^{1/2} \quad (x \text{ et } y \text{ éléments de } K).$$

Elevons au carré:

$$a = x^2 + y^2D + 2xyD^{1/2}.$$

Nécessairement $x = 0$ et $a = y^2D$.

$$\mathfrak{a}^2\mathfrak{b}\mathfrak{b}'. = y^2\mathfrak{c}^2\delta\delta'.$$

D'après le lemme

$$\mathfrak{b} = \delta \qquad \text{et} \qquad \mathfrak{a}^2\mathfrak{b}' = (y^2)\mathfrak{c}^2\delta'.$$

2. *Détermination explicite d'une base entière.*

Plaçons-nous dans le cas particulier où K est une extension infinie de $\mathbf{Q}$: $K = \bigcup_{n \in \mathrm{N}} K_n$, avec $[K_n:\mathbf{Q}] < \infty$. Soit $L = K(\sqrt{a})$ une extension quadratique de K. Supposons qu'elle admette une base entière $\{\lambda, \mu\}$: il existe alors un indice n_0 tel que pour $n \geqq n_0$, $\{\lambda, \mu\}$ soit une base entière de $L_n = K_n(\sqrt{a})/K_n$. Nous sommes donc ramenés à la recherche d'une base entière d'une extension quadratique d'un corps de nombres.

Ce problème a été résolu par Fröhlich (Discriminants of algebraic number fields [5]). Il montre que lorsqu'on connait l'existence d'une base entière, on peut trouver un générateur d de l'idéal discriminant, et un entier β tel que

$$d - \beta^2 \equiv 0 \text{ modulo } 4.$$

Comme base entière, on trouve alors $\{1, \dfrac{\beta + \sqrt{d}}{2}\}$.

3. *Une condition suffisante d'existence d'une base normale.*

Proposition 6.

Soit L une extension quadratique d'un corps de nombres K. Pour que l'anneau des entiers B de L admette une A-base normale, il suffit que B soit A-libre, que B/A soit modérément ramifiée, et que 2 soit totalement décomposé dans $K/\mathbf{Q}$.

Il est évidemment nécessaire qu'il existe une base entière. On sait aussi que la condition « être modérément ramifiée » est nécessaire pour toute extension finie d'un corps de nombres. (cf. J. Martinet [11]).

Supposons donc que L/K admette une base entière; d'après le paragraphe précédent, nous pouvons la prendre de la forme $\{1, \frac{\beta + \sqrt{d}}{2}\}$, où d est un générateur de l'idéal discriminant, et β un entier tel que $\beta^2 - d \equiv 0$ (4).

Une condition nécessaire et suffisante pour que L/K admette une base normale est qu'il existe deux éléments x et y de A tels que:

$$\left(\begin{vmatrix} x + y\dfrac{\beta + \sqrt{d}}{2} & x + y\dfrac{\beta - \sqrt{d}}{2} \\ x + y\dfrac{\beta - \sqrt{d}}{2} & x + y\dfrac{\beta + \sqrt{d}}{2} \end{vmatrix}^2 \right) = (d)$$

$$\left(y^2\, d\, (2x + y\beta)^2\right) = (d)\,.$$

Comme x, y, d et β sont des entiers, il faut et il suffit que y et $2x + y\beta$ soient des unités de A.

En particulier, $2x + y\beta$ doit être une unité $\mathcal{P}$-adique pour tout idéal $\mathcal{P}$ divisant 2. Donc β doit être une unité $\mathcal{P}$-adique. Comme $d \equiv \beta^2$ (4), on obtient que d doit être une unité $\mathcal{P}$-adique pour tout $\mathcal{P} \mid 2$. Cela équivaut à la ramification modérée de B/A.

Supposons maintenant 2 totalement décomposé dans $K/\mathbf{Q}$. Si $\mathcal{P}$ est un idéal premier de A divisant 2, $A/\mathcal{P}$ est un corps à deux éléments. Choissons un élément π dans $\mathcal{P} \backslash \mathcal{P}^2$. Tout élément de $A/\mathcal{P}^2$ peut-être représenté par

$$m = \varepsilon_1 + \varepsilon_2 \pi \qquad \varepsilon_1, \varepsilon_2 \in \{0, 1\}\,.$$

Si m est une unité $\mathcal{P}$-adique, $\varepsilon_1 = 1$. Alors

$$m^2 = 1 + 2\varepsilon_2 \pi + \varepsilon_2^2 \pi^2 \equiv 1 \mod \mathcal{P}^2\,.$$

Tous les carrés d'unités $\mathcal{P}$-adiques sont congrus à 1 mod $\mathcal{P}^2$. En particulier

$$\beta^2 \equiv 1 \text{ modulo } 4.$$

Comme valeur de β, on peut choisir 1. Prenons alors $x = 0$, $y = 1$: B admet une A-base normale engendrée par $\dfrac{1 + \sqrt{d}}{2}$.

Corallaire.

Soit $L = K(a^{1/2})$ *une extension quadratique d'une extension infinie* K *de* $\mathbf{Q}$, *de type J. Pour que l'anneau des entiers* B *de* L *admette une A-base normale, il suffit que*

. B *soit* A-libre

. B/A *soit modérément ramifiée*

. *il existe dans* K *une extension finie* k *de* $\mathbf{Q}$ *telle que* $[k\ a^{1/2}):k] = 2$,

que le discriminant de L/K *soit l'étendu du discriminant de* $k(a^{1/2})/k$, *et que* 2 *soit totalement décomposé dans* $k/\mathbf{Q}$.

Pour démontrer ce corollaire, il suffit de voir que k vérifie les hypothèses de la proposition 6. L'extension $k(a^{1/2})/k$ admet une base entière, grâce à la proposition 5. Elle est modérément ramifiée: son discriminant est premier à 2, comme celui de L/K. Enfin 2 est totalement décomposé dans $k/\mathbf{Q}$.

Exemple: Considérons le corps $K = \bigcup_{n \in \mathbf{N}} \mathbf{Q}(\sqrt{-7}, \zeta_n)$ où ζ_n est une racine primitive 3^n-ième de l'unité. Si $\theta = 1 + 4\sqrt{-7}$, $L = K(\theta^{1/2})$ est une extension quadratique de K.

Déterminons le discriminant de $\mathbf{Q}(\theta^{1/2})/\mathbf{Q}(\sqrt{-7})$. L'idéal premier $(1+4\sqrt{-7})$ se ramifie dans l'extension considérée; il figure donc avec l'exposant 1 dans le discriminant. Les seuls idéaux distincts de $(1+4\sqrt{-7})$ qui peuvent se ramifier dans $\mathbf{Q}(\theta^{1/2})/\mathbf{Q}(\sqrt{-7})$ sont les idéaux au-dessus de 2. Or, dans $\mathbf{Q}(\sqrt{-7})$,

$$(2) = \left(\frac{1+\sqrt{-7}}{2}\right)\left(\frac{1-\sqrt{-7}}{2}\right).$$

D'autre part

$$1 + 4\sqrt{-7} \equiv \left(\frac{1+3\sqrt{-7}}{2}\right)^2 \bmod \left(\frac{1+\sqrt{-7}}{2}\right)^2$$

et

$$1 + 4\sqrt{-7} \equiv \left(\frac{1+\sqrt{-7}}{2}\right)^2 \bmod \left(\frac{1-\sqrt{-7}}{2}\right)^2.$$

D'après la théorie de Kummer, les idéaux au-dessus de 2 sont non ramifiés dans l'extension $\mathbf{Q}(\theta^{1/2})/\mathbf{Q}(\sqrt{-7})$; le discriminant de cette extension vaut exactement $(1+4\sqrt{-7})$. Le théorème 5 permet d'affirmer que $\mathbf{Q}(\theta^{1/2})/\mathbf{Q}(\sqrt{-7})$ vérifie toutes les hypothèses de la proposition 6: cette extension admet donc une base normale entière, engendrée par $\dfrac{1+\sqrt{1+4\sqrt{-7}}}{2}$.

On vérifie aisément que le discriminant de L/K est l'étendu de celui de $\mathbf{Q}(\theta^{1/2})/\mathbf{Q}(\sqrt{-7})$. Donc L/K admet aussi une base normale entière engendrée par $\dfrac{1+\sqrt{1+4\sqrt{-7}}}{2}$.

BIBLIOGRAPHIE

[1] Artin, E. Questions de base minimale dans la théorie des nombres algébriques. *Coll. Int. CNRS*, vol. 24 (1950), pp. 19-20.
[2] Bourbaki, N. *Algèbre commutative*. Chap. 7, Hermann, Paris.
[3] —— *Algèbre commutative*. Chap. 6, Hermann, Paris.
[4] Chevalley, C. Sur la théorie du corps de classes dans les corps finis et les corps locaux. *Journal of the Fac. of Science*, Tokyo, vol. 2, part. 9 (1933).
[5] Fröhlich, A. Discriminants of algebric number fields. *Math. Zeitschr. 74*, pp. 18-28 (1960).
[6] Hecke, E. *Vorlesungen über die Theorie der algebraischen Zahlen*. Leipzig (1923). Réimpression: New York (1948).
[7] Jaffard, P. Théorie arithmétique des anneaux du type de Dedekind. *Bull. Soc. Math. de France*, vol. 80 (1952), pp. 61-94.
[8] Kaplansky, J. Modules over Dedekind rings and valuation rings. *Trans. AMS*, vol. 72 (1952), pp. 327-340.
[9] Mann, H. B. On integral bases. *Proc. AMS*, vol. 9 (1958), pp. 167-172.
[10] Martel, B. *Γ-extensions d'un corps quadratique imaginaire*. Séminaire Th. Nb, Grenoble, fév. 1971.
[11] Martinet, J. Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre $2p$. *Ann. Inst. Fourier*, tome 19, fasc. 1 (1969), pp. 1-79.
[12] Samuel, P. *Théorie algébrique des nombres*. Hermann, Paris 1967.
[13] Serre, J.-P. *Corps locaux*. Hermann, Paris 1968.

Reçu le 10 décembre 1971

Nicole Moser
Institut de Mathématiques Pures
B.P. 116
38 — St-Martin-d'Hères, France