Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 18 (1972)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ARITHMÉTIQUE DANS DES EXTENSIONS FINIES DU CORPS DES QUOTIENTS DE CERTAINS ANNEAUX DE PRÜFER

Autor: Moser, Nicole

DOI: https://doi.org/10.5169/seals-45366

ARITHMÉTIQUE DANS DES EXTENSIONS FINIES DU CORPS DES QUOTIENTS DE CERTAINS ANNEAUX DE PRÜFER

par Nicole MOSER

Dans cet article, nous cherchons à généraliser des résultats arithmétiques connus pour les anneaux de Dedekind à certains anneaux de Prüfer. On pourra trouver dans Bourbaki ([2], § 2, exercice 12) la définition des anneaux de Prüfer. Donnons ici les deux caractérisations que nous utiliserons:

soit A un anneau intègre; c'est un anneau de Prüfer s'il vérifie l'une des deux propriétés équivalentes suivantes:

a — Pour tout idéal premier $\mathfrak{P}$, l'anneau local $A_{\mathfrak{P}}$ est un anneau de valuation.

b — Tout idéal non nul et de type fini dans A est inversible.

Nous nous intéresserons par la suite à l'anneau des entiers A d'une extension algébrique infinie K du corps des quotients d'un anneau de Dedekind; c'est un anneau de Prüfer, (caractérisation b), mais en général ce n'est pas un anneau de Dedekind. Soit L une extension finie séparable de K, d'anneau des entiers B.

Dans une première partie (§ I et II), nous généralisons le critère d'Artin ([1]), qui donne une condition nécessaire et suffisante pour que B soit un A-module libre. Ensuite (§ IV), nous supposons que L/K est une extension quadratique telle que A soit un anneau de Prüfer uniforme du type de Dedekind (cf. Jaffard [7] et § III). D'après un article de Mann ([9]), nous précisons le critère d'Artin. Puis, lorsque celui-ci est vérifié, nous obtenons une condition suffisante d'existence d'une base normale entière.

Dans la plupart des démonstrations, nous travaillerons sur des sous-corps de K qui sont corps des quotients d'un anneau de Dedekind. Nous aurons donc besoin des quelques résultats classiques que nous rappelons ci-dessous.

Soient D un anneau de Dedekind, de corps des quotients M, et N une extension finie séparable de M; notons D' la fermeture intégrale de D dans N. Comme P. Samuel [12], choisissons pour définition du discriminant la caracterisation suivante:

Définition.

On appelle discriminant de D' sur D l'idéal de D engendré par les discriminants des bases de N/M qui sont contenues dans D'.

On démontre alors la

Proposition.

Pour qu'un idéal premier $\mathfrak{P}$ de D se ramifie dans D', il faut et il suffit qu'il contienne l'idéal discriminant $\Delta_{D'/D}$. (cf. [12]).

Le discriminant est déterminé par sa décomposition en idéaux premiers de D; on peut étudier séparément la participation de chaque idéal premier, grâce à deux résultats que l'on trouve dans « Corps locaux » de J.-P. Serre ([13]).

Proposition.

Soit S une partie multiplicative de D; localisons en S; alors

$$S^{-1}\Delta_{D'/D} = \Delta_{S^{-1}D'/S^{-1}D}.$$

Proposition.

Soit $\mathfrak{p}$ un idéal premier de D', et soit $\mathfrak{P} = \mathfrak{p} \cap D$. Soit $\hat{\Delta}_{\mathfrak{P}}$ l'idéal du complété $\hat{D}_{\mathfrak{P}}$ engendré par le discriminant $\Delta_{D'/D}$, et soit $\Delta_{\mathfrak{p}}$ le discriminant de $\hat{D}'_{\mathfrak{p}}$ par rapport à $\hat{D}_{\mathfrak{P}}$. On a:

$$\hat{\Delta}_{\mathfrak{P}} = \prod_{\mathfrak{p}|\mathfrak{P}} \Delta\mathfrak{p}.$$

Grâce aux groupes de ramification, E. Hecke dans [6] (chap. 5) détermine complètement le discriminant lorsque M contient les racines p-ièmes de l'unité, et lorsque $[N:M] = p$, pour un nombre premier p. Alors M contient une racine primitive p-ième de l'unité, ω, et N s'écrit $N = M(\alpha^{1/p})$, α élément de $M \backslash M^p$. Il obtient les résultats suivants:

THÉORÈME.

Soit $\mathfrak{P}$ un idéal maximal de D, ne divisant pas pD, et soit $\mathfrak{P}^n$ la plus haute puissance de $\mathfrak{P}$ divisant α. Alors N/M est ramifiée en $\mathfrak{P}$ si et seulement si p ne divise pas n. L'exposant de $\mathfrak{P}$ dans $\Delta_{D'/D}$ vaut alors $p - 1$.

THÉORÈME.

Soient $\mathfrak{P}$ un idéal maximal de D, divisant pD, a l'exposant de $\mathfrak{P}$ dans $(1-\omega)\,D$, n l'exposant de $\mathfrak{P}$ dans αD :

1) *Si $p \nmid n$, N/M est ramifiée en $\mathfrak{P}$, et l'exposant de $\mathfrak{P}$ dans $\Delta_{D'/D}$ vaut $(p-1)\,(ap+1)$.*

Si $p \mid n$, on se ramène à $n = 0$.

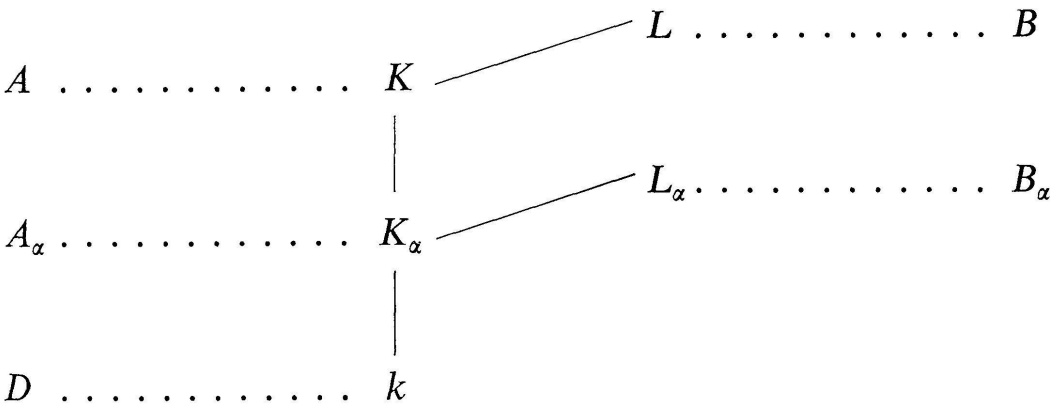
2) *Si la congruence $\alpha \equiv \xi^p \bmod \mathfrak{P}^{ap}$ est possible avec un $\xi \in D$, alors N/M est non ramifiée en $\mathfrak{P}$.*

3) *Si la congruence $\alpha \equiv \xi^p \bmod \mathfrak{P}^{ap}$ est impossible avec un $\xi \in D$, soit m le plus grand entier tel que la congruence $\alpha \equiv \xi^p \bmod \mathfrak{P}^m$ soit possible avec un $\xi \in D$. Posons $m = pu + v$, avec $0 \leq v \leq p-1$, et $0 \leq u \leq a-1$.*

. Si $v = 0$, l'extension résiduelle $(D'/\mathfrak{P}D')\,/\,(D/\mathfrak{P})$ est purement inséparable, et l'exposant de $\mathfrak{P}$ dans $\Delta_{D'/D}$ est $p\,(p-1)\,(a-u)$.

. Si $v \neq 0$, $\mathfrak{P}$ se ramifie dans D', et son exposant dans $\Delta_{D'/D}$ vaut $(p-1)\,[p\,(a-u) + 1 - v]$.

Notations.



Soit D un anneau de Dedekind, de corps des quotients k. Considérons une extension algébrique infinie K de k, et la famille $\{K_\alpha\}_{\alpha \in \mathfrak{F}}$ des extensions finies de k contenues dans K. Munissons l'ensemble d'indices $\mathfrak{F}$ de la relation d'ordre

$$\alpha \geq \beta \Leftrightarrow K_\alpha \supset K_\beta\,.$$

Nous désignerons par I un sous-ensemble de $\mathfrak{F}$ possédant les propriétés suivantes:

(1) $\begin{cases} . \ K = \bigcup\limits_{\alpha \in I} K_\alpha . \\ . \ \text{Si } \alpha \text{ et } \beta \text{ appartiennent à } I, \text{ le corps composé } K_\alpha . K_\beta \text{ appartient} \\ \quad \text{à l'ensemble } \{K_\gamma\}_{\gamma \in I}. \end{cases}$

Il existe toujours au moins un sous-ensemble I, $\mathscr{F}$ lui-même. Lorsque D est dénombrable, nous pouvons prendre $\mathbf{N}$ comme sous-ensemble I:

$$K = \bigcup_{n \in \mathbf{N}} K_n$$

les corps K_n étant emboîtés.

Soit L une extension finie séparable de K. Si θ est un générateur de L/K, posons $L_\alpha = K_\alpha(\theta)$. *Nous ne considèrerons par la suite que les indices* α *pour lesquels* $[L_\alpha : K_\alpha] = [L : K] = n$.

Enfin les anneaux d'entiers de K, L, K_α et L_α seront notés respectivement A, B, A_α et B_α.

I. Discriminant et ramification.

1. *Discriminant.*

Définition 1.

Nous appellerons discriminant de l'extension L/K *l'idéal* Δ *de* A *engendré par les discriminants des bases de* L/K *à éléments dans* B.

Puisque L/K est séparable, Δ est un idéal entier non nul de A.

Proposition 1.

Soit I *un sous-ensemble de* $\mathscr{F}$ *possédant la propriété* (1). *Notons* Δ *le discriminant de* L/K, *et* Δ_α *celui de* L_α/K_α. *Alors*

$$\Delta = \bigcup_{\alpha \in I} \Delta_\alpha .$$

En effet, un élément de Δ est combinaison linéaire finie, à coefficients dans A, de discriminants de bases de L/K à éléments dans B: c'est donc un élément d'un Δ_α.

Inversement, puisque $[L_\alpha : K_\alpha] = [L : K]$, toute base de L_α/K_α à coefficients dans B_α est une base de L/K à coefficients dans B, et Δ contient $\bigcup\limits_{\alpha \in I} \Delta_\alpha$.

2. *Ramification.*

Remarquons que dans l'anneau A, tout idéal premier $\mathscr{P}$ est maximal. Le localisé $A_{\mathscr{P}}$ est un anneau de valuation, donc, à $\mathscr{P}$, on peut associer une valuation v sur K, de groupe des valeurs Γ_v. Comme l'extension L/K est finie, il n'existe dans B qu'un nombre fini d'idéaux premiers au-dessus de $\mathscr{P}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ (cf. Bourbaki [3] § 8). A chaque $\mathfrak{p}_i$ est associée une valuation v_i de L qui prolonge v; le groupe Γ_{v_i} des valeurs de v_i admet Γ comme sous-groupe.

Définition 2.

Soit $\mathscr{P}$ un idéal premier de A. Nous dirons que $\mathscr{P}$ se ramifie dans l'extension L/K si l'un des indices $e_i = (\Gamma_{v_i}:\Gamma_v)$ est strictement supérieur à 1.

Remarque: si $f_i = [B/\mathfrak{p}_i:A/\mathscr{P}]$, l'inégalité $\sum_{i=1}^{l} e_i f_i \leq n$ est encore vraie. (cf. Bourbaki [3]).

Proposition 2.

Pour qu'un idéal premier $\mathscr{P}$ de A se ramifie dans l'extension L/K, il faut et il suffit qu'il contienne l'idéal discriminant Δ.

La démonstration de cette proposition repose sur le principe bien connu de la propagation de la non-ramification vers le haut. On peut énoncer ce principe de la manière suivante:

soient k le corps des quotients d'un anneau de Dedekind, M et N deux extensions algébriques finies séparables de k, linéairement disjointes sur k. Si $\mathscr{P}$ est un idéal premier de k non ramifié dans l'extension M/k, tout idéal premier $\mathfrak{p}$ de N qui divise $\mathscr{P}$ est non ramifié dans l'extension $M \cdot N/N$.

Posons $\mathscr{P}_\alpha = \mathscr{P} \cap A_\alpha$, et notons v^α (resp v_i^α) la restriction de v (resp v_i) à K_α (resp L_α).

Supposons $\mathscr{P}$ ramifié dans L/K: il existe un indice $i \in [1, l]$ tel que $(\Gamma_{v_i}:\Gamma_v) > 1$. On ne peut trouver $\alpha_0 \in I$ tel que $(\Gamma_{v_i^{\alpha_0}}:\Gamma_{v^{\alpha_0}}) = 1$; sinon, la « propagation de la non-ramification vers le haut », et l'égalité $K = \bigcup_{\substack{\beta \in I \\ \beta \geq \alpha_0}} K_\beta$ permettraient de conclure que $(\Gamma_{v_i}:\Gamma_v) = 1$. Donc pour tout $\alpha \in I$, $\mathscr{P}_\alpha$ est ramifié dans L_α/K_α : $\mathscr{P}_\alpha$ contient le discriminant Δ_α de L_α/K_α, et $\mathscr{P}$ contient $\Delta = \bigcup \Delta_\alpha$.

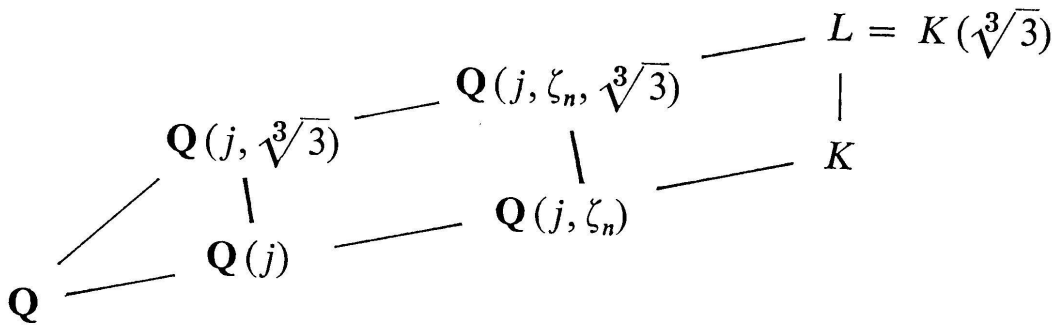
Inversement, si $\mathscr{P}$ contient Δ, pour tout $\alpha \in I$, on a les inclusions:

$$\mathscr{P}_\alpha \supset \Delta \cap A_\alpha \supset \Delta_\alpha .$$

Donc $\mathscr{P}_\alpha$ se ramifie dans L_α/K_α. Par « propagation de la non-ramification vers le haut », il existe au moins un indice i tel que pour tout α, $(\Gamma_{v_i}\alpha:\Gamma_v\alpha) > 1$. Pour cette valeur de i, $(\Gamma_{v_i}:\Gamma_v) > 1$, et $\mathscr{P}$ est ramifié dans L/K.

II. Bases entières.

1. *Exemple*



Soit K le corps obtenu en adjoignant à $\mathbf{Q}$, j et toutes les racines 5^n-ièmes de l'unité; soit ζ_n une racine primitive 5^n-ième de l'unité. Le corps K, extension cyclotomique de $\mathbf{Q}$, est une extension abélienne de $\mathbf{Q}$. Mais $\mathbf{Q}(j, \sqrt[3]{3})/\mathbf{Q}$ n'est pas abélienne; donc $L = K(\sqrt[3]{3})$ est une extension de degré 3 de K.

Les extensions $\mathbf{Q}(j, \sqrt[3]{3}, \zeta_n)/\mathbf{Q}(j, \zeta_n)$ sont des extensions de Kummer. Les seuls idéaux qui peuvent se ramifier sont ceux qui divisent 3. La théorie de Kummer (cf. Hecke [6]) permet de calculer leur participation au discriminant de L_n/K_n; on obtient: $\Delta_n = 3^4 A_n$. Mais comme $Z[j]$ est principal, $\mathbf{Q}(j, \sqrt[3]{3})/\mathbf{Q}(j)$ admet une base entière, $\{\lambda, \mu, \nu\}$, de discriminant 3^4. Donc L/K admet $\{\lambda, \mu, \nu\}$ comme base entière.

2. *Caractérisation des A-modules B de type fini.*

Proposition 3.

A et B étant définis au paragraphe précédent, les propositions suivantes sont équivalentes :

a — B est un A-module de type fini.

b — Il existe une famille finie $\{\lambda_1, ..., \lambda_l\}$ *d'éléments de B, et un indice* $\alpha_0 \in I$, *tels que pour tout* $\beta \geqq \alpha_0$, $\{\lambda_1, ..., \lambda_l\}$ *soit un système de générateurs du* A_β*-module* B_β.

c — L'idéal discriminant Δ *de L/K est de type fini.*

$a \Rightarrow b$ — Choisissons un système fini de générateurs de B, $\{\lambda_1, ..., \lambda_l\}$. D'après la condition (1), il existe un indice $\alpha_0 \in I$ tel que les λ_i appartiennent tous à B_{α_0}. Pour $\beta \geqq \alpha_0$, considérons le A_β-module $M_\beta = A_\beta\lambda_1 + ... + A_\beta\lambda_l$, et montrons que $M_\beta = B_\beta$.

Le module M_β est sans torsion, de rang n, sur l'anneau de Dedekind A_β. Utilisons un résultat démontré par Artin dans ([1]): étant donnés n éléments l_i de M_β linéairement indépendants sur K_β, on peut trouver n idéaux fractionnaires $\mathfrak{a}_i$ de A_β tels que

$$M_\beta = \mathfrak{a}_1 l_1 \oplus ... \oplus \mathfrak{a}_n l_n .$$

Cette écriture permet de vérifier l'égalité, pour $\gamma \geqq \beta$:

$$M_\gamma \cap B_\beta = M_\beta .$$

On peut alors définir une injection de B_β/M_β dans B_γ/M_γ. La famille $\{B_\alpha/M_\alpha\}_{\alpha \geqq \alpha_0}$ constitue un système inductif, de limite inductive 0. Donc, pour $\alpha \geqq \alpha_0$,

$$B_\alpha = M_\alpha = A_\alpha\lambda_1 + ... + A_\alpha\lambda_l .$$

$b \Rightarrow c$ — Supposons B de type fini. Soit encore α_0 l'indice intervenant dans la démonstration de $a \Rightarrow b$. Choisissons un idéal premier $\mathfrak{P}$ de A_{α_0}, et localisons en $\mathfrak{P}$. (Nous surlignerons les localisés). Pour $\alpha \geqq \alpha_0$, B_α et B_{α_0} possèdent un système de générateurs commun, donc $\overline{B_\alpha}$ et $\overline{B_{\alpha_0}}$ ont une base commune respectivement sur $\overline{A_\alpha}$ et $\overline{A_{\alpha_0}}$. Et

$$\overline{\Delta_\alpha} = \overline{\Delta_{\alpha_0}}\,\overline{A_\alpha} .$$

Ceci étant vrai pour tout idéal premier $\mathfrak{P}$ de A_{α_0},

$$\Delta_\alpha = \Delta_{\alpha_0} A_\alpha .$$

Comme on obtient une nouvelle famille d'indices vérifiant les conditions (1) en ne considérant que les indices de I supérieurs à α_0, on peut conclure que

$$\Delta = \Delta_{\alpha_0} A .$$

$c \Rightarrow b \Rightarrow a$ — Soit $\{\delta_1, ..., \delta_l\}$ un système de générateurs de Δ. Considérons un indice α_0 tel que A_{α_o} contienne tous les δ_i, et, pour $\alpha \geqq \alpha_0$, posons

$$\mathfrak{a}_\alpha = \delta_1 A_\alpha + ... + \delta_l A_\alpha .$$

Comme $\mathfrak{a}_\alpha A_\beta = \mathfrak{a}_\beta$ lorsque $\beta \geqq \alpha$, on a

$$\mathfrak{a}_\beta \cap \Delta_\alpha = \mathfrak{a}_\alpha .$$

La limite inductive du système inductif $\{\Delta_\alpha/\mathfrak{a}_\alpha\}_{\alpha \geqq \alpha_o}$ est nulle, donc pour $\alpha \geqq \alpha_0$, $\Delta_\alpha = \mathfrak{a}_\alpha = \Delta_{\alpha_o} A_\alpha$.

Si $\{l_1, ..., l_p\}$ est un système de générateurs du A_{α_o}-module B_{α_o}, considérons pour $\alpha \geqq \alpha_0$

$$M_\alpha = A_\alpha l_1 + ... + A_\alpha l_p .$$

Grâce à l'hypothèse $\Delta_\alpha = \Delta_{\alpha_o} A_\alpha$, on montre par localisation que $M_\alpha = B_\alpha$. Comme $K = \bigcup_{\substack{\alpha \in I \\ \alpha \geqq \alpha_o}} K_\alpha$, on peut donc conclure que B est un A-module de type fini.

Cette caractérisation va nous permettre de construire une extension L/K ou B n'est pas un A-module de type fini.

Considérons le corps $K_n = \mathbf{Q}(\sqrt[3^n]{2})$; c'est une extension de degré 3^n de $\mathbf{Q}$, dans laquelle 2 est totalement ramifié. Le corps $K = \cup K_n$ est une extension réelle de $\mathbf{Q}$, donc $L = K(i)$ est une extension de degré 2 de K.

$$\begin{array}{ccccccc}
\mathbf{Q}(i) & \text{———} & \mathbf{Q}(i, \sqrt[3]{2}) & \text{———} & \mathbf{Q}(i, \sqrt[3^n]{2}) & \text{———} & L \\
| & & | & & | & & | \\
\mathbf{Q} & \text{———} & \mathbf{Q}(\sqrt[3]{2}) & \text{———} & \mathbf{Q}(\sqrt[3^n]{2}) & \text{———} & K
\end{array}$$

L'indice de ramification de 2 dans $\mathbf{Q}(i)/\mathbf{Q}$ vaut 2; dans $\mathbf{Q}(\sqrt[3^n]{2})/\mathbf{Q}$, il vaut 3^n. Donc $\mathfrak{P}_n = (\sqrt[3^n]{2})$ est ramifié dans $\mathbf{Q}(i, \sqrt[3^n]{2})/\mathbf{Q}(\sqrt[3^n]{2})$. On voit que l'entier maximum x_n tel que la congruence

$$-1 \equiv \xi_n^2 \bmod \mathfrak{P}_n^{x_n}$$

admette une solution dans A_n est 3^n. La théorie de Kummer (cf. [6]) nous donne donc comme valeur du discriminant Δ_n de $\mathbf{Q}(i, \sqrt[3^n]{2})/\mathbf{Q}(\sqrt[3^n]{2})$

$$\Delta_n = \mathfrak{P}_n^{3n+1}.$$

Soit m un indice supérieur à n.

$$\mathscr{P}_n A_m = \mathscr{P}_m^{3m-n}.$$

$$\Delta_n A_m = \mathscr{P}_m^{3m+3m-n}$$

$$\Delta_m = \mathscr{P}_m^{3m+1}.$$

Donc dès que m diffère de n, Δ_m contient strictement $\Delta_n A_m$, et Δ_m n'est jamais l'étendu d'un discriminant d'indice inférieur. La proposition 3 permet de conclure que B n'est pas un A-module de type fini.

3. *Critère d'Artin.*

Pour généraliser le critère d'Artin, nous utiliserons un théorème démontré en 1952 par Kaplansky ([8]).

THÉORÈME 1 (Kaplansky)

Soit R un domaine d'intégrité vérifiant les deux conditions suivantes :

. tout idéal de type fini est inversible.

. si $\mathfrak{a}$ est un idéal non nul de type fini de R, $R/\mathfrak{a}$ est un anneau dans lequel tout idéal de type fini est principal.

Alors si M est un R-module sans torsion de type fini

a — M se représente comme somme directe d'idéaux de type fini, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$.

b — Le rang n de M, et la classe du produit $\mathfrak{a}_1 \times \ldots \times \mathfrak{a}_n$ dans une représentation de M comme somme directe d'idéaux constituent un système complet d'invariants pour M.

On voit facilement que les anneaux A qui nous intéressent vérifient les hypothèses du théorème 1. Si l'on suppose que B est de type fini sur A, on peut trouver des idéaux $\mathfrak{a}_i$ de A tels que

$$B = \mathfrak{a}_1 \oplus \ldots \oplus \mathfrak{a}_n .$$

On peut donc conclure que pour que B soit un A-module libre, il faut et il suffit que l'idéal $\mathfrak{a}_1 \times \ldots \times \mathfrak{a}_n$ soit principal.

Critère d'Artin.

Soit D le discriminant d'une base $\{\xi_i\}$ de L/K, et soit Δ l'idéal discriminant de L/K. Les deux assertions suivantes sont équivalentes :

a — B est un A-module libre.

b — $\Delta/(D)$ est le carré d'un idéal principal.

Soit $\{\xi_i\}$ une base de L/K. Supposons B de type fini sur A; d'après le théorème 1, on peut écrire

$$B = \mathfrak{a}_1\xi_1 \oplus \ldots \oplus \mathfrak{a}_n\xi_n$$

où les $\mathfrak{a}_i$ sont des idéaux de type fini de A. Posons

$$\mathfrak{a}_i^\alpha = \mathfrak{a}_i \cap A_\alpha .$$

$$B_\alpha = \mathfrak{a}_1^\alpha\xi_1 \oplus \ldots \oplus \mathfrak{a}_n^\alpha\xi_n$$

pour tout indice α tel que L_α contienne les ξ_i. Utilisons les résultats d'Artin ([1]) pour L_α/K_α:

$$\Delta_\alpha = (\mathfrak{a}_1^\alpha)^2 \times \ldots \times (\mathfrak{a}_n^\alpha)^2 D .$$

Comme $\Delta = \bigcup_{\alpha\in I} \Delta_\alpha$, $\Delta = (\mathfrak{a}_1 \times \ldots \times \mathfrak{a}_n)^2\, D$, et le critère est une conséquence immédiate du théorème 1.

III. Arithmétique dans certains anneaux de Prüfer.

1. *Anneaux et corps de type J.*

Dans un article de 1952, P. Jaffard ([7]) construit une théorie de la divisibilité pour des anneaux plus généraux que les anneaux de Dedekind. Il procède de la manière suivante: soient A un anneau commutatif unitaire, et J l'ensemble de ses idéaux. On peut munir J d'une relation d'équivalence:

les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont équivalents, si tout idéal de J, étranger à l'un, est étranger à l'autre.

On appelle « strie » une classe d'équivalence de J pour cette relation; une strie maximale est une strie qui contient un idéal maximal; celui-ci est d'ailleurs unique.

Théorème 2 (Jaffard).

Soit A un anneau commutatif unitaire, vérifiant les deux conditions suivantes :

* *L'intersection d'une infinité d'idéaux maximaux distincts se réduit à l'idéal* $\{0\}$.

* *tout idéal premier non nul et différent de A appartient à une strie maximale.*

Alors tout idéal $\mathfrak{a}$ *de A se décompose de manière unique en un produit d'idéaux,* $\mathfrak{a}_1 \times \ldots \times \mathfrak{a}_n$, *chaque* $\mathfrak{a}_i$ *appartenant à une strie maximale.*

Définition 3.

Soient A un anneau vérifiant les hypothèses du théorème 2, et $\mathfrak{m}$ un idéal maximal de A. Etant donné un idéal $\mathfrak{a}$ de A, nous appellerons *composante de* $\mathfrak{a}$ *relativement à* $\mathfrak{m}$ l'idéal de la strie de $\mathfrak{m}$ qui intervient dans la décomposition de $\mathfrak{a}$.

Nous dirons qu'une *strie maximale est finie* si l'idéal maximal qu'elle contient est de type fini; tout idéal d'une strie finie est de type fini. Dans le cas contraire, nous dirons qu'une strie maximale est non finie.

Pour être complètement renseigné sur la divisibilité des idéaux, il faut supposer de plus que A est un anneau de Prüfer uniforme (c'est-à-dire un anneau de Prüfer où deux idéaux premiers de J, différents de $\{0\}$, sont toujours premiers entre eux). Pour ces anneaux, on peut définir une décomposition des idéaux fractionnaires suivant les stries maximales, et démontrer le

THÉORÈME 3 (Jaffard).

Soit A un anneau de Prüfer uniforme, satisfaisant aux hypothèses du théorème 2. *Si* $\mathfrak{a}$ *et* $\mathfrak{b}$ *sont deux idéaux fractionnaires de A, les assertions suivantes sont équivalentes :*

a — il existe un idéal $\mathfrak{c}$ *tel que* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

b — pour tout idéal maximal $\mathfrak{m}$ *de A tel que la composante de* $\mathfrak{a}$ *relative à* $\mathfrak{m}$ *soit finie, la composante de* $\mathfrak{b}$ *relative à* $\mathfrak{m}$ *est également finie.*

Définition 4.

Soient D un anneau de Dedekind, et A la clôture intégrale de D dans une extension algébrique infinie du corps des quotients de D. Nous dirons que *A est un anneau de type J* si l'ensemble des idéaux premiers de A au-dessus d'un idéal premier $\mathscr{P}$ de D est fini.

Il est clair qu'un anneau de type J est un anneau de Prüfer uniforme, qui vérifie les hypothèses du théorème 2.

Un corps K *est un corps de type* J s'il est corps des quotients d'un anneau de type J.

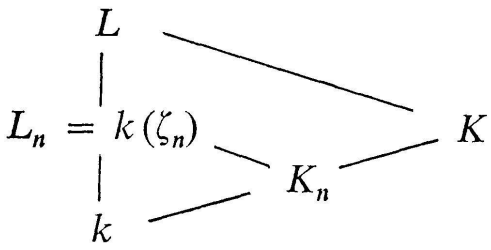
2. *Exemple de corps de type J.*

Soit k un corps de nombres. On dit que K est une Γ-extension de k si K/k est galoisienne, et si Gal (K/k) est isomorphe à $\mathbf{Z}_p$. Les extensions intermédiaires d'une Γ-extension K/k sont donc des extensions cycliques de degré p^n de k. Soit alors $\mathfrak{P}$ un idéal premier de k; son corps de décomposition est soit K, soit un corps de nombres.

Proposition 4.

Toute Γ-extension cyclotomique d'un corps de nombres est un corps de type J.

Soit ζ_n une racine primitive p^n-ième de l'unité. Notons L_n le corps $k(\zeta_n)$. Par définition, la Γ-extension cyclotomique K d'un corps de nombres k, associée au nombre premier p est la Γ-extension contenue dans $L = \bigcup_n^{\infty} L_n$. Si k contient les racines p-ièmes de l'unité, alors $K = L$. Sinon, $K = \bigcup_{n=2}^{\infty} K_n$, K_n étant la sous-extension de degré p^{n-1} de L_n, et $[L_n:K_n]$ divise $p - 1$.



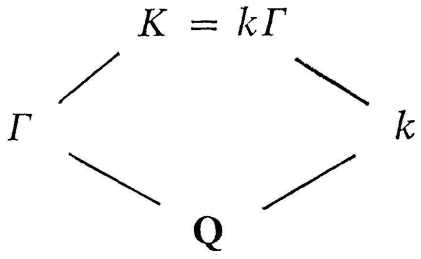
. Soit $\mathfrak{q}$ un idéal premier de k ne divisant pas p. La théorie du corps de classes [4] nous dit que $\mathfrak{q}$ se décompose totalement dans l'extension L_n/k si et seulement si $\mathfrak{q}$ appartient au groupe d'Artin H_n de L_n/k. L'image de $\mathfrak{q}$ par l'automorphisme de Frobenius est l'élément σ de Gal (L_n/k) défini par:

$$\sigma\zeta_n = \zeta_n^{N(\mathfrak{q})}.$$

Donc $\mathfrak{q}$ est totalement décomposé dans L_n/k si et seulement si

$$N(\mathfrak{q}) \equiv 1 \mod p^n.$$

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.



. Supposons maintenant que $\mathscr{P}$ 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 $\mathscr{P}$ 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 $1 \leq i \leq j$, 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 $(\prod_{i=1}^{j} \mathfrak{a}_i) \cap \chi$ se décompose de manière unique en:

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

$\mathfrak{c}_1$ 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

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

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

Plaçons-nous dans le cas particulier où K est une extension infinie de $\mathbf{Q}$: $K = \bigcup_{n\in\mathbf{N}} K_n$, 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:

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

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

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

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

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

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

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

Tous les carrés d'unités $\mathfrak{P}$-adiques sont congrus à 1 mod $\mathfrak{P}^2$. 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 $\frac{1 + \sqrt{d}}{2}$.

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