

SÉMINAIRE DELANGE-PISOT-POITOU. THÉORIE DES NOMBRES

DONALD L. MCQUILLAN

Réseaux sur les anneaux d'entiers algébriques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 2 (1972-1973),
exp. n° 25, p. 1-5

http://www.numdam.org/item?id=SDPP_1972-1973__14_2_A9_0

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1972-1973, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

RÉSEAUX SUR LES ANNEAUX D'ENTRIERS ALGÈBRIQUES

par Donald L. McQUILLAN

1. Soit σ l'anneau d'entiers d'un corps de nombres algébriques k . Soit $V = V_n$ l'espace vectoriel (sur k) des polynômes $f(x)$ dont le degré est majoré par n . Nous considèrerons l'ensemble \mathcal{L} des réseaux dans V , c'est-à-dire l'ensemble des sous- σ -modules L de V tels que L est de type fini et de rang $n+1$, la dimension de V . De plus, dans tout ce qui suit, nous allons ajouter la condition spéciale suivante :

Si $f(x) \in L$, alors on a $f(0) \in L$. Cette condition revient à dire que

$$L = L_0 \oplus L_1,$$

où L_0 est l'ensemble des éléments constants de L , et L_1 est l'ensemble des éléments $f(x)$ de L tels que $f(0) = 0$.

Le but de cet exposé est d'étudier l'opération de certains groupes naturels sur \mathcal{L} et sur quelques sous-ensembles de \mathcal{L} . Nous n'allons donner qu'une esquisse des résultats. Les démonstrations paraîtront ailleurs. Ces recherches ont été faites en collaboration avec mon collègue H. GUNJI.

Nos études proviennent des articles de POLYA [5], de CAHEN [1] et d'OSTROWSKI [4]. Tous les trois se sont occupés de l'étude du réseau des polynômes $f(x) \in V$ tels que $f(\theta) \in \theta$. On utilisera quelques résultats qui se trouvent dans [2]. Enfin, la plupart de nos résultats permettra de généraliser au cas où σ est un anneau de Dedekind.

2. On note I le groupe des idéaux fractionnaires non nuls de σ , et I^+ l'ensemble des idéaux entiers non nuls. Si $L \in \mathcal{L}$ et $a \in k^x$, on note L^a l'ensemble des polynômes $f(x/a)$, où $f(x) \in L$. Il est clair que $L^a \in \mathcal{L}$.

DÉFINITION 1. - Soit $L \in \mathcal{L}$, et soit $\alpha \in I$. On pose $L^\alpha = \bigcap_a L^a$, où a parcourt les éléments non nuls de α .

THÉORÈME 1. - Si $L \in \mathcal{L}$ et $\alpha \in I$, alors on a $L^\alpha \in \mathcal{L}$. De plus, on a

(i) $L^a + L^b = L^{[a,b]}$,

(ii) $L^a \cap L^b = L^{(a,b)}$

(iii) $(L^a)^b = L^{ab}$.

Étant donné $L \in \mathcal{L}$, on démontre sans peine qu'il existe $\alpha \in I^+$ tel que $L \subset L^\alpha$.

DÉFINITION 2. - Soit $a \in I^+$. On note $\mathcal{L}(a)$ l'ensemble des réseaux L tels que $L \subset L^a$.

On peut démontrer le lemme suivant.

LEMME 1. - L'application $a \mapsto \mathcal{L}(a)$ est une application de I^+ dans l'ensemble des sous-ensembles non vides de \mathcal{L} . Elle est injective. En effet, si $a \neq b$, alors on a $\mathcal{L}(a) \not\subset \mathcal{L}(b)$. De plus, on a $\mathcal{L} = \bigcup_{a \in I^+} \mathcal{L}(a)$.

Remarque. - Soient a et b deux éléments de I . Le réseau $M(a, b)$ des polynômes $f(x) \in V$, tels que $f(a) \subset b$, appartient à $\mathcal{L}(a)$, et généralise d'une façon naturelle le réseau étudié par POLYA. Une certaine suite d'idéaux entiers, notés $\mathfrak{S}_0, \mathfrak{S}_1, \dots, \mathfrak{S}_r, \dots$ (trouvée par POLYA [5] et retrouvée par nous [2]) joue un rôle capital en ce qui concerne la structure de $M(a, b)$. On a le théorème suivant.

THÉORÈME 2. - Il existe des polynômes unitaires $f_0(x), f_1(x), \dots, f_n(x) \in k[x]$ de degré $0, 1, \dots, n$ qui ne dépendent que de a tels que

$$(i) \quad f_i(x) \in \mathfrak{o}[x] \quad \text{si} \quad a \in I^+,$$

$$(ii) \quad M(a, b) = \sum_{i=0}^n \frac{b}{a^i \mathfrak{S}_i} f_i(x).$$

3. Soit $G = k^x \times k^x \times \dots \times k^x$ ($n+1$ fois), et définissons une opération du groupe multiplicatif G sur \mathcal{L} . D'abord, si $f(x) = \sum_{i=0}^n a_i x^i \in V$, et $g = (g_0, g_1, \dots, g_n) \in G$, on note $f^g(x)$ le polynôme

$$\sum_{i=0}^n g_i a_i x^i.$$

Alors, si $L \in \mathcal{L}$, posons :

$$L^g = \{f^g(x) ; f(x) \in L\}.$$

Il est clair que $L^g \in \mathcal{L}$ et, de plus, si $L \in \mathcal{L}(a)$, alors on a $L^g \in \mathcal{L}(a)$. De cette façon G opère sur \mathcal{L} et sur tous les $\mathcal{L}(a)$. Quand $n = 0$ ou 1 , on a $|\mathcal{L}/G| = h^{n+1}$, où h note le nombre de classes de k . Au contraire quand $n \geq 2$, la cardinalité de \mathcal{L}/G est infinie. En effet, si p désigne un entier rationnel premier, posons

$$L(p) = \mathfrak{o} + p\mathfrak{o}x + \mathfrak{o}(x + x^2) + \sum_{i=3}^n \mathfrak{o}x^i.$$

On démontre facilement que $L(p_1)$ et $L(p_2)$ n'appartiennent pas à la même orbite si $p_1 \neq p_2$. Pourtant on a le résultat suivant.

THÉORÈME 3. - Soit $a \in I^+$. Alors l'ensemble $\mathcal{L}(a)/G$ est fini.

La démonstration provient du fait qu'on peut identifier l'espace \mathcal{L} avec l'espace homogène U/H , où H est le produit restreint des groupes $GL_{n+1}(k_p)$ par rapport aux groupes unimodulaires $U_{n+1}(\mathfrak{o}_p)$ et $U = \prod_p U_{n+1}(\mathfrak{o}_p)$. De cette façon, on

peut faire opérer le groupe $G^1 = J^1 \times \dots \times J^1$ ($n + 1$ fois) sur \mathcal{L} , où J^1 note les idèles de k dont le volume est égal à 1. Ensuite, on démontre que l'ensemble $\mathcal{L}(\alpha)/G^1$ est fini en utilisant [2]. Enfin, le groupe G^1/G est compact, et on s'en sert pour achever la démonstration.

4. Il résulte du théorème 1 (ii) qu'étant donné $L \in \mathcal{L}$, il existe un idéal $f(L) = f \in I^+$ tel que

- (i) $L \subset L^f$,
- (ii) Si $L \subset L^a$, alors on a $a \subset f$.

DÉFINITION 3. - Soit $L \in \mathcal{L}$. L'idéal $f(L)$ est dit le conducteur de L .

Notation. - On note $\mathcal{L}_1(f)$ l'ensemble de réseaux L dont le conducteur est égal à f . Le lemme 2 montre que $\mathcal{L}_1(f) \neq \emptyset$ quel que soit l'idéal $f \in I^+$ et que $\mathcal{L} = \bigcup_{f \in I^+} \mathcal{L}_1(f)$.

Nous allons d'abord étudier l'ensemble $\mathcal{L}(\mathfrak{o})$.

THÉORÈME 4. - Le groupe $I^2 = I \times I$ opère sur l'ensemble $\mathcal{L}(\mathfrak{o})$. Si $X = \mathcal{L}(\mathfrak{o})/I^2$, alors il existe une application $\phi : X \rightarrow I^+$ telle que la cardinalité de l'ensemble $\phi^{-1}(\alpha)$ est finie pour tout $\alpha \in I^+$.

En effet, si $L \in \mathcal{L}(\mathfrak{o})$, alors on a $L \subset L^0 \subset L$, c'est-à-dire $L = L^0$, et il suit sans peine que l'application $(\alpha, b, L) \mapsto bL^\alpha$ de $I^2 \times \mathcal{L}(\mathfrak{o})$ dans $\mathcal{L}(\mathfrak{o})$ définit une opération du groupe I^2 sur $\mathcal{L}(\mathfrak{o})$.

Pour définir l'application ϕ du théorème, on a besoin d'associer quelques idéaux avec un réseau L . D'abord, notons $b(L)$ (resp. $c(L)$) l'ensemble des éléments constants de L (resp. des coefficients de x^n dans les polynômes de L). La définition d'un troisième idéal $\alpha(L)$ se trouve dans le lemme suivant.

LEMME 2. - Soit $L \in \mathcal{L}$. Alors il existe $\alpha(L) \in I$ possédant les propriétés suivantes :

- (i) Si $a \in \alpha(L)$, alors $f(x + a) \in L$ pour tout $f(x) \in L$,
- (ii) Si $\alpha \in I$ est un idéal quelconque vérifiant la propriété (i), alors

$$\alpha \subset \alpha(L).$$

LEMME 3. - Soit $L \in \mathcal{L}$. Alors l'idéal $M(L) = \alpha(L)^n c(L) \mathfrak{F}_n / b(L)$ est entier. De plus, si $L_1 = bL^\alpha$, alors on a $M(L) = M(L_1)$.

Maintenant la définition de l'application $\phi : X \rightarrow I^+$ se fait de la manière suivante : Si $\xi \in X$ et $L \in \xi$, soit $\phi(\xi) = M(L)$.

Notation. - On note $\nu(\alpha)$ la cardinalité de $\phi^{-1}(\alpha)$, où $\alpha \in I^+$.

THÉOREME 5.

(i) Si x est réel et positif, on a

$$\sum_{Np \leq x} v(p) \sim c_n(x/\log x)$$

où c_n est un entier positif qui ne dépend que de n et de k .

(ii) La série de Dirichlet $F_n(s) = \sum_a (v(a)/Na^s)$, $s \in \mathbb{C}$, est convergente dans un demi-plan $\text{Re}(s) > \rho$. $F_n(s)$ se prolonge analytiquement au demi-plan $\text{Re}(s) > 0$, et on a

$$F_n(s) = H_n(s) \zeta_k(s)^n / \zeta_k(ns),$$

où $\zeta_k(s)$ est la fonction ζ de k , et $H_n(s)$ est une fonction analytique dans $\text{Re}(s) > 0$, qui ne dépend que des idéaux premiers de \mathfrak{o} qui divisent $n!$

Enfin, regardons les ensembles $\mathcal{L}_1(f)$. Nous allons généraliser les résultats ci-dessus. Notons $I(f)$ l'ensemble des idéaux qui sont premiers à f , et $J(f)$ l'ensemble des idéaux engendrés par les idéaux premiers qui divisent f . On peut définir une opération du groupe $I(f)$ sur $\mathcal{L}(f)$, $(\mathfrak{a}, L) \mapsto \mathfrak{a} \circ L$, en précisant que

$$(\mathfrak{a} \circ L)_p = \begin{cases} L_p^{\mathfrak{a}} & \text{si } (p, f) = 1 \\ L_p & \text{sinon} \end{cases}$$

pour tout idéal premier p de \mathfrak{o} .

Ensuite $I(f) \times I$ opère sur $\mathcal{L}(f)$ selon la définition $(\mathfrak{a}, b, L) \mapsto b(\mathfrak{a} \circ L)$. Toute classe de $I/I(f)$ peut s'écrire comme $f_1 \cdot I(f)$, où $f_1 \in J(f)$ et f_1 est unique. Notons alors $\mathcal{L}(f, f_1)$ l'ensemble des $L \in \mathcal{L}(f)$ tels que $\mathfrak{a}(L) \in f_1 \cdot I(f)$. Le groupe $I(f) \times I$ opère aussi sur $\mathcal{L}(f, f_1)$, et, dans le cas où $f = \mathfrak{o}$, on a $f_1 = \mathfrak{o}$ et $\mathcal{L}(\mathfrak{o}, \mathfrak{o}) = \mathcal{L}(\mathfrak{o})$. Soit

$$X(f, f_1) = \mathcal{L}(f, f_1) / I(f) \times I.$$

On peut démontrer deux théorèmes concernant l'espace $X(f, f_1)$ qui généralisent les théorèmes 4 et 5 ci-dessus.

BIBLIOGRAPHIE

- [1] CAHEN (P.-J.). - Polynômes à valeurs entières, *Canad. J. math.*, t. 24, 1972, p. 747-754.
- [2] GUNJI (H.) and McQUILLAN (D. L.). - On a class of ideals in an algebraic number field, *J. Number Theory*, t. 2, 1970, p. 207-222.
- [3] O'MEARA (O. T.). - Introduction to quadratic forms. - Berlin, Springer-Verlag, 1963 (*Grundlehren der mathematischen Wissenschaften*, 117).
- [4] OSTROWSKI (A.). - Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. für reine und angew. math.*, t. 149, 1919, p. 117-124.

- [5] POLYA (G.). - Über ganzzahlige Polynome in algebraischen Zahlkörpern, J. für reine und angew. math., t. 149, 1919, p. 97-116.

(Texte reçu le 12 octobre 1973)

Donald L. McQUILLAN
Department of Mathematics
University of Wisconsin
MADISON, Wisc. 53706 (Etats-Unis)
