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)
14e année, 1972/73, n° 25, 5 p.

28 mai 1973

RÉSEAUX SUR LES ANNEAUX D'ENTIERS ALGÉBRIQUES

par Donald L. McQUILLAN

1. Soit o 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 $\mathfrak{L}$ des réseaux dans V, c'est-à-dire l'ensemble des sous-o-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 $\mathfrak{L}$ et sur quelques sous-ensembles de $\mathfrak{L}$. 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 $f(\theta) \subset \theta$. On utilisera quelques résultats qui se trouvent dans [2]. Enfin, la plupart de nos résultats permettra de généraliser au cas où o est un anneau de Dedekind.

2. On note I le groupe des idéaux fractionnaires non nuls de o, et I^+ l'ensemble des idéaux entiers non nuls. Si $L \in \mathfrak{L}$ 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 $L^a \in \mathfrak{L}$.

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

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

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

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

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

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

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

On peut démontrer le lemme suivant.

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

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

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

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

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

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

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

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

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

Il est clair que $L^g \in \mathfrak{L}$ et, de plus, si $L \in \mathfrak{L}(\mathfrak{a})$, alors on a $L^g \in \mathfrak{L}(\mathfrak{a})$. De cette façon G opère sur $\mathfrak{L}$ et sur tous les $\mathfrak{L}(\mathfrak{a})$. Quand $n = 0$ ou 1 , on a $|\mathfrak{L}/G| = h^{n+1}$, où h note le nombre de classes de k . Au contraire quand $n \geq 2$, la cardinalité de $\mathfrak{L}/G$ 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 $\mathfrak{a} \in I^+$. Alors l'ensemble $\mathfrak{L}(\mathfrak{a})/G$ est fini.

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

peut faire opérer le groupe $G^1 = J^1 \times \ldots \times J^1$ ($n+1$ fois) sur $\mathfrak{L}$, où J^1 note les idèles de k dont le volume est égal à 1. Ensuite, on démontre que l'ensemble $\mathfrak{L}(\mathfrak{a})/G^1$ 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 $L \in \mathfrak{L}$, il existe un idéal $f(L) = f \in I^+$ tel que

(i) $L \subset L^f$,

(ii) Si $L \subset L^{\mathfrak{a}}$, alors on a $\mathfrak{a} \subset f$.

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

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

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

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

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

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

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

(i) Si $a \in \mathfrak{a}(L)$, alors $f(x+a) \in L$ pour tout $f(x) \in L$,

(ii) Si $\mathfrak{a} \in I$ est un idéal quelconque vérifiant la propriété (i), alors

$$\mathfrak{a} \subset \mathfrak{a}(L).$$

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

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

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

THÉORÈME 5.

(i) Si x est réel et positif, on a

$$\Sigma_{N\mathfrak{p}\leq x} \nu(\mathfrak{p}) \sim c_n(x/\log x)$$

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

(ii) La série de Dirichlet $F_n(s) = \Sigma_{\mathfrak{a}} (\nu(\mathfrak{a})/N\mathfrak{a}^s)$, $s \in \underset{\sim}{C}$, est convergente dans un demi-plan $\mathrm{Re}(s) > \rho$. $F_n(s)$ se prolonge analytiquement au demi-plan $\mathrm{Re}(s)>0$, 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 $\mathrm{Re}(s) > 0$, qui ne dépend que des idéaux premiers de o qui divisent $n!$

Enfin, regardons les ensembles $\mathfrak{L}_1(f)$. 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 $\mathfrak{L}(f)$, $(\mathfrak{a}, L) \longmapsto \mathfrak{a} \circ L$, en précisant que

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

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

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

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

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 gan wertige 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)