

QUASI-MONOGÉNÉITÉ DE L'ANNEAU DES ENTIERS

OUAFAR LAHLOU ET MOHAMED ELHASSANI CHARKANI

RÉSUMÉ. Il est bien connu que la propriété de la monogénéité d'un corps de nombres de degré fini sur $\mathbb{Q}$ est rarement satisfaite. On définit alors une notion de *quasi-monogénéité* pour l'anneau des entiers d'une famille plus large de corps de nombres et on détermine une base pour l'anneau des entiers algébriques de ces corps. Ensuite, on donne un critère pratique caractérisant la quasi-monogénéité de l'anneau des entiers de ces corps. Enfin, on caractérise la monogénéité des corps de nombres de degré fini sur $\mathbb{Q}$ au moyen d'équations diophantiennes.

ABSTRACT. It is well known that the property of monogeneity of a number field of finite degree over $\mathbb{Q}$ occurs only rarely. We define a notion of *quasi-monogeneity* which is satisfied by the ring of integers of a larger family of number fields and which allows to determine an integral basis. We also give a practical criterion for characterizing the quasi-monogeneity of the ring of integers of a number field. Finally, we characterize the monogeneity of quasi-monogeneous number fields of finite degree over $\mathbb{Q}$ by a diophantine equation.

1. Introduction. Le but de cet article est de définir un nouveau procédé de recherche de bases de l'anneau des entiers O_K d'un corps de nombres $K = \mathbb{Q}(\alpha)$ de degré n . Le principe consiste à déterminer le plus grand entier positif non nul λ_i tel que $\alpha^i/\lambda_i \in O_K$, pour $i = 1, \dots, n-1$, et ainsi $\{1, \alpha/\lambda_1, \dots, \alpha^{n-1}/\lambda_{n-1}\}$ devient une base de O_K si et seulement si $\text{Ind}(\alpha) = \prod_{i=1}^{n-1} \lambda_i$. Ces anneaux d'entiers sont alors dits *quasi-monogènes*. On donne ainsi un critère pratique caractérisant la quasi-monogénéité de l'anneau des entiers. Un autre résultat de cet article est une caractérisation de la monogénéité des corps de nombres de degré n quasi-monogènes par des équations diophantiennes.

2. Quasi-monogénéité de l'anneau des entiers. Soient $K = \mathbb{Q}(\alpha)$ un corps de nombres de degré n , O_K l'anneau des entiers de K , $P(X) \in \mathbb{Z}[X]$ le polynôme minimal de α et $\sigma_1, \dots, \sigma_n$ les n -plongements distincts de K dans $\mathbb{C}$. Soient $\Delta_0(X_1, \dots, X_n) = 1$ et

$$\Delta_j(X_1, \dots, X_n) = \sum_{1 \leq i_1 < i_2 < \dots < i_j \leq n} X_{i_1} \dots X_{i_j},$$

pour $j = 1, \dots, n$, les polynômes symétriques élémentaires et $S_j(x) = \Delta_j(\sigma_1(x), \dots, \sigma_n(x))$ la j -ième fonction symétrique de $x \in K$.

Reçu le 10 septembre 2003 et, sous forme définitive, le 17 février 2005.

Proposition 2.1. [3] Les assertions suivantes sont équivalentes :

- (1) L'élément $\frac{x}{\lambda} \in O_K$ avec $x \in K$ et $\lambda \in \mathbb{Q}^*$;
- (2) Pour tout $j = 1, \dots, n$, on a $S_j(x) \in \lambda^j \mathbb{Z}$.

Lemme 2.2. [2] Les $S_k(x)$, pour $x \in K$ et $k = 0, \dots, n$, se calculent à l'aide des formules (analogues aux formules de Newton)

$$\begin{cases} \rho_k(x) - \rho_{k-1}(x)S_1(x) + \dots + (-1)^n \rho_{k-n}(x)S_n(x) = 0 & \text{si } k \geq n, \\ \rho_k(x) - \rho_{k-1}(x)S_1(x) + \dots + (-1)^k k S_k(x) = 0 & \text{si } k \leq n, \end{cases}$$

où $\rho_k(x) = S_1(x^k)$, et aussi à l'aide de la formule

$$S_k(x) = \frac{1}{k!} \det \begin{pmatrix} \rho_1(x) & 1 & 0 & 0 & \dots & 0 \\ \rho_2(x) & \rho_1(x) & 2 & 0 & \dots & 0 \\ \rho_3(x) & \rho_2(x) & \rho_1(x) & 3 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ \rho_{k-1}(x) & \rho_{k-2}(x) & \rho_{k-3}(x) & \rho_{k-4}(x) & \dots & k-1 \\ \rho_k(x) & \rho_{k-1}(x) & \rho_{k-2}(x) & \rho_{k-3}(x) & \dots & \rho_1(x) \end{pmatrix}.$$

Définition 2.3. Soit $x \in O_K$. On appelle K -contenu de x le plus grand entier positif non nul λ tel que $\frac{x}{\lambda} \in O_K$. On le notera $C_K(x)$. Un élément x de O_K est dit admissible si $C_K(x) = 1$.

Proposition 2.4. [3] Soient $x = \sum_{j=1}^n a_j x_j \in O_K = \bigoplus_{i=1}^n \mathbb{Z} x_i$ et $\lambda = C_K(x)$. Alors $\lambda = \text{pgcd}(a_j, j = 1, \dots, n)$.

Remarque 2.5. Soit $x \in O_K$. Pour que x soit un élément d'une base d'entiers il faut que x soit admissible.

Proposition 2.6. [3] Pour $i = 1, \dots, n-1$, soit $\lambda_i \in \mathbb{N}^*$ tel que $\frac{\alpha^i}{\lambda_i} \in O_K$. On a :

$$(1) D\left(1, \frac{\alpha}{\lambda_1}, \dots, \frac{\alpha^{n-1}}{\lambda_{n-1}}\right) = \frac{[O_K : \mathbb{Z}[\alpha]]^2 d_K}{\left(\prod_{i=1}^{n-1} \lambda_i\right)^2};$$

(2) Soient $M = \mathbb{Z} \oplus \mathbb{Z} \frac{\alpha}{\lambda_1} \oplus \dots \oplus \mathbb{Z} \frac{\alpha^{n-1}}{\lambda_{n-1}}$ et e l'exposant de $O_K/\mathbb{Z}[\alpha]$. Alors

(i) $[M : \mathbb{Z}[\alpha]] = \prod_{i=1}^{n-1} \lambda_i$,

(ii) $\prod_{i=1}^{n-1} \lambda_i$ divise $\text{Ind}(\alpha)$ et e^n ,

(iii) Si $M = O_K$ alors e divise $\prod_{i=1}^{n-1} \lambda_i$;

(3) De plus, $\left\{1, \frac{\alpha}{\lambda_1}, \dots, \frac{\alpha^{n-1}}{\lambda_{n-1}}\right\}$ est une base de O_K si et seulement si $\text{Ind}(\alpha) = \prod_{i=1}^{n-1} \lambda_i$.

Définition 2.7. Pour $i = 1, \dots, n-1$, soit $\lambda_i = C_K(\theta^i)$ pour un certain $\theta \in O_K$. On dit que O_K est quasi-monogène si et seulement si $\left\{1, \frac{\theta}{\lambda_1}, \dots, \frac{\theta^{n-1}}{\lambda_{n-1}}\right\}$ est une base de O_K . Par abus de langage, on dit que K est quasi-monogène.

Proposition 2.8. Pour $i = 1, \dots, n-1$, soit $\lambda_i = C_K(\alpha^i)$.

- (1) On a l'égalité $\lambda_i = \prod_{p \in P} p^c$ avec $c = \inf_{1 \leq j \leq n} \left(\left\lceil \frac{v_p(S_j(\alpha^i))}{j} \right\rceil \right)$ où $[x]$ désigne la partie entière du réel x , $v_p(x)$ est le plus grand entier m tel que $p^m \mid x$ et P est l'ensemble des nombres premiers.
- (2) De plus,

$$v_p(d_K) \leq v_p(\text{Disc}(P)) - 2v_p \left(\prod_{i=1}^{n-1} \lambda_i \right)$$

où d_K (resp. $\text{Disc}(P)$) désigne le discriminant de K (resp. du polynôme $P(X)$).

Démonstration. La partie (1) résulte de la proposition 2.1, de la définition 2.3 et de la définition du pgcd. La partie (2) résulte de la proposition 2.6 et du fait que $\text{Disc}(P) = (\text{Ind}(\alpha))^2 d_K$ (voir la proposition 4.4.4 en page 166 de [2]). $\square$

3. Critères de quasi-monogénéité et de monogénéité.

Lemme 3.1. [2] Soient $K = \mathbb{Q}(\alpha)$ un corps de nombres de degré n , $P(X) \in \mathbb{Z}[X]$ le polynôme minimal de α , O_K l'anneau des entiers de K et p un nombre premier. Soit

$$\overline{P}(X) = \prod_{i=1}^r \overline{P}_i^{e_i}(X)$$

la factorisation de $P(X)$ modulo p en facteurs irréductibles dans $\mathbb{F}_p[X]$ avec $P_i(X) \in \mathbb{Z}[X]$ unitaire, image réciproque de $\overline{P}_i(X)$ et soit

$$T(X) = \frac{1}{p} \left(P(X) - \prod_{i=1}^r P_i^{e_i}(X) \right) \in \mathbb{Z}[X].$$

- (1) Si p ne divise pas $\text{Ind}(\alpha)$, alors

$$pO_K = \prod_{i=1}^r \beta_i^{e_i}$$

avec $\beta_i = pO_K + P_i(\alpha)O_K$. De plus, le degré résiduel f_i est égal au degré de P_i .

- (2) Le premier p ne divise pas $\text{Ind}(\alpha)$ si et seulement si $(\overline{P}_i, \overline{T}) = 1$ dans $\mathbb{F}_p[X]$ pour tout i tel que $e_i \geq 2$.

Proposition 3.2. En reprenant les notations du lemme 3.1 on a que p ne divise pas $\text{Ind}(\alpha)$ si et seulement si $v_p(\text{Res}(P_i, P)) = \deg(P_i)$ pour tout i tel que $e_i \geq 2$.

Démonstration. Résulte du lemme 3.1, du corollaire 2, p. 73 de [1] et des propriétés du résultant de [2]. $\square$

Théorème 3.3. (CRITÈRE) *En reprenant les notation ci-dessus, on a l'équivalence des affirmations suivantes :*

- (1) $O_K = \bigoplus_{i=0}^{n-1} \mathbb{Z} \frac{\alpha^i}{\lambda_i}$, c'est-à-dire O_K est quasi-monogène;
- (2) Pour tout nombre premier p tel que $v_p(\text{Disc}(P)) \geq 2$, on a :
 - (i) Si $v_p\left(\prod_{i=1}^{n-1} \lambda_i\right) \geq 1$, alors $v_p(\text{Ind}(\alpha)) = v_p\left(\prod_{i=1}^{n-1} \lambda_i\right)$,
 - (ii) Si $v_p\left(\prod_{i=1}^{n-1} \lambda_i\right) = 0$, alors $v_p(\text{Res}(P_i, P)) = \deg(P_i)$ pour tout i tel que $e_i \geq 2$.

Démonstration. D'après la proposition 2.6, d'une part, on a $O_K = \bigoplus_{i=0}^{n-1} \mathbb{Z} \frac{\alpha^i}{\lambda_i}$ si et seulement si $\text{Ind}(\alpha)$ divise $\prod_{i=1}^{n-1} \lambda_i$. D'autre part, $\text{Disc}(P) = (\text{Ind}(\alpha))^2 d_K$. Ainsi, le résultat s'obtient à l'aide de la proposition 3.2. $\square$

Corollaire 3.4. (CRITÈRE) $O_K = \mathbb{Z}[\alpha]$ si et seulement si pour tout nombre premier p tel que $v_p(\text{Disc}(P)) \geq 2$, on a $v_p(\text{Res}(P_i, P)) = \deg(P_i)$ pour tout i tel que $e_i \geq 2$.

4. Sur la monogénéité des corps de nombres quasi-monogènes. Si $P(X) = \sum_{i=0}^n t_i X^i$, avec $t_i \in \mathbb{Z}$ pour tout i et $t_n = 1$, on a $\alpha^n = \sum_{i=0}^{n-1} (-t_i) \alpha^i$. Si on pose $\alpha^{n+k} = \sum_{i=0}^{n-1} r_{i,k} \alpha^i$, alors la représentation standard de α^{n+k} est $(r_{0,k}, \dots, r_{n-1,k}, 1)$ et les $r_{i,k}$ se calculent par induction à l'aide des formules suivantes :

$$r_{i,0} = -t_i \quad \text{et} \quad r_{i,k+1} = \begin{cases} r_{i-1,k} - t_i r_{n-1,k} & \text{si } i \geq 1; \\ -t_0 r_{n-1,k} & \text{si } i = 0. \end{cases}$$

Posons

$$\beta^i = \sum_{j=0}^{n-1} a_{i,j} \alpha^j, \quad A = (a_{i,j})_{0 \leq i, j \leq n-1} \quad \text{et} \quad b_{l,k} = \sum_{i+j=k} a'_{1,i} a'_{l-1,j}$$

avec $a_{i,j} = \frac{a'_{i,j}}{d_i}$, $d_i > 0$, $a'_{i,j} \in \mathbb{Z}$ et $\text{pgcd}(a'_{i,0}, \dots, a'_{i,n-1}, d_i) = 1$.

Proposition 4.1. *On a :*

- (1) $d_i = d_1 d_{i-1}$ et $a'_{i,j} = b_{i,j} + \sum_{k=0}^{n-2} r_{j,k} b_{i,n+k}$ pour $2 \leq i \leq n-1$ et $0 \leq j \leq n-1$.
- (2) Si $\beta \in O_K$ alors $\text{Ind}(\beta) = |\det A| \text{Ind}(\alpha)$.

Démonstration. On a que $(a'_{1,0}, \dots, a'_{1,n-1}, d_1)$ et $(a'_{i-1,0}, \dots, a'_{i-1,n-1}, d_{i-1})$ sont les représentations standards de β et β^{i-1} . Donc la partie (1) résulte de la propriété multiplicative de β et β^{i-1} (voir [2], p. 160). La partie (2) résulte du fait que pour $x \in O_K$,

$$D(1, x, \dots, x^{n-1}) = (\text{Ind}(x))^2 d_K = (\det(\sigma_i(x^{j-1}))_{1 \leq i, j \leq n})^2. \quad \square$$

Théorème 4.2. *Si O_K est quasi-monogène, alors les assertions suivantes sont équivalentes :*

- (1) K est monogène;
- (2) L'équation diophantienne

$$\det \begin{pmatrix} x_1 & x_2 & \dots & x_{n-1} \\ \lambda_1 a_{2,1} & \lambda_2 a_{2,2} & \dots & \lambda_{n-1} a_{2,n-1} \\ \vdots & \vdots & & \vdots \\ \lambda_1 a_{n-1,1} & \lambda_2 a_{n-1,2} & \dots & \lambda_{n-1} a_{n-1,n-1} \end{pmatrix} = \pm 1$$

admet des solutions en $x_1, \dots, x_{n-1} \in \mathbb{Z}$.

Démonstration. Si $O_K = \bigoplus_{i=0}^{n-1} \mathbb{Z} \frac{\alpha^i}{\lambda_i}$, alors K est monogène si et seulement si il existe $\beta = \sum_{i=0}^{n-1} x_i \frac{\alpha^i}{\lambda_i} \in O_K$ tel que $\text{Ind}(\beta) = 1$. Or d'après les propositions 2.6 et 4.1, on a

$$\text{Ind}(\alpha) = \prod_{i=1}^{n-1} \lambda_i \quad \text{et} \quad \text{Ind}(\beta) = |\det A| \text{Ind}(\alpha).$$

Donc K est monogène si et seulement si il existe $\beta = \sum_{i=0}^{n-1} x_i \frac{\alpha^i}{\lambda_i} \in O_K$ tel que $\det(a_{i,j} \lambda_j)_{0 \leq i,j \leq n-1} = \pm 1$, avec $\lambda_0 = a_{0,0} = 1$, $a_{0,j} = 0$ pour $j = 1, \dots, n-1$ et $a_{1,j} = \frac{x_j}{\lambda_j}$ pour $j = 0, \dots, n-1$. $\square$

Corollaire 4.3. *Soit K est un corps de nombres cubique quasi-monogène. Alors K est monogène si et seulement si l'équation diophantienne*

$$x_1 \lambda_2 \left(\frac{x_1}{\lambda_1} - t_2 \frac{x_2}{\lambda_2} \right)^2 + t_1 \left(\frac{x_1 x_2^2}{\lambda_2} - t_2 \frac{\lambda_1 x_2^3}{\lambda_2^2} \right) + \frac{t_0 \lambda_1 x_2^3}{\lambda_2^2} = \pm 1$$

admet des solutions en $x_1, x_2 \in \mathbb{Z}$.

Donc on retrouve le résultat donné dans le théorème 3.1 de [3].

English extended abstract. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n over $\mathbb{Q}$, O_K its ring of integers, and let $P(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α .

Definitions. (1) Let $x \in O_K$. The largest positive integer λ such that $\frac{x}{\lambda} \in O_K$ is called the K -content of x and is denoted by $C_K(x)$. If $C_K(x) = 1$ for some algebraic integer x in O_K , then the element x is said to be *admissible*.

(2) For $i = 1, \dots, n-1$, let $\lambda_i = C_K(\theta^i)$ for some $\theta \in O_K$. We say that O_K is *quasi-monogeneous* if and only if $\{1, \frac{\theta}{\lambda_1}, \dots, \frac{\theta^{n-1}}{\lambda_{n-1}}\}$ is a basis of O_K .

We have the following criterion.

Theorem 1. (CRITERION) *Under the assumptions of Lemma 3.1, the following statements are equivalent:*

- (1) $O_K = \bigoplus_{i=0}^{n-1} \mathbb{Z} \frac{\alpha^i}{\lambda_i}$, with $\lambda_i = C_K(\alpha^i)$ for $i = 1, \dots, n-1$.
- (2) For every prime number p such that $v_p(\text{Disc}(P)) \geq 2$ we have:
 - (i) If $v_p \left(\prod_{i=1}^{n-1} \lambda_i \right) \geq 1$, then $v_p(\text{Ind}(\alpha)) = v_p \left(\prod_{i=1}^{n-1} \lambda_i \right)$.

- (ii) If $v_p\left(\prod_{i=1}^{n-1} \lambda_i\right) = 0$, then $v_p(\text{Res}(P_i, P)) = \deg(P_i)$ for every i such that $e_i \geq 2$.

Corollary 1. (CRITERION) *The following statements are equivalent:*

- (1) $O_K = \mathbb{Z}[\alpha]$.
- (2) For every prime number p such that $v_p(\text{Disc}(P)) \geq 2$, we have $v_p(\text{Res}(P_i, P)) = \deg(P_i)$ for every i such that $e_i \geq 2$.

Under the assumptions of Section 4, and from Propositions 2.3 and 4.1, we obtain the following Theorem.

Theorem 2. *If $O_K = \bigoplus_{i=0}^{n-1} \mathbb{Z} \frac{\alpha^i}{\lambda_i}$, with $\lambda_i = C_K(\alpha^i)$ for $i = 1, \dots, n-1$, then the following statements are equivalent:*

- (1) O_K is monogeneous.
- (2) The diophantine equation

$$\det \begin{pmatrix} x_1 & x_2 & \dots & x_{n-1} \\ \lambda_1 a_{2,1} & \lambda_2 a_{2,2} & \dots & \lambda_{n-1} a_{2,n-1} \\ \vdots & \vdots & & \vdots \\ \lambda_1 a_{n-1,1} & \lambda_2 a_{n-1,2} & \vdots & \lambda_{n-1} a_{n-1,n-1} \end{pmatrix} = \pm 1$$

has the solutions $x_1, \dots, x_{n-1} \in \mathbb{Z}$.

Corollary 2. *Suppose that $P(X) = X^2 + t_1 X + t_2$ is the minimum polynomial of α . Assume that we have*

$$O_K = \bigoplus_{i=0}^2 \mathbb{Z} \frac{\alpha^i}{\lambda_i} \quad \text{with } \lambda_i = C_K(\alpha^i).$$

Then O_K is monogeneous if and only if the diophantine equation

$$x_1 \lambda_2 \left(\frac{x_1}{\lambda_1} - t_2 \frac{x_2}{\lambda_2} \right)^2 + t_1 \left(\frac{x_1 x_2^2}{\lambda_2} - t_2 \frac{\lambda_1 x_2^3}{\lambda_2^2} \right) + \frac{t_0 \lambda_1 x_2^3}{\lambda_2^2} = \pm 1$$

has solutions $x_1, x_2 \in \mathbb{Z}$.

BIBLIOGRAPHIE

1. N. Bourbaki, *Algèbre, Chapitres 4 à 7*, Masson, Paris, 1981.
2. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, New York, 1993.
3. M. E. Charkani et O. Lahlou, *Quasi-monogénéité de l'anneau des entiers*; À paraître.

O. LAHLOU ET M. E. CHARKANI
DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ SIDI MOHAMED BEB ABDELLAH
FACULTÉ DES SCIENCES DHAR-MAHRAZ
B. P. 1796, FÈS, MAROC
COURRIEL : l.ouafae@caramail.com
mcharkani@fsdmfes.ac.ma