ACTA ARITHMETICA
117.2 (2005)

Valeurs entières de fractions rationnelles

par

Laurent Denis et Sophie Dion (Lille)

1. Introduction. Soient $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et $f \in \overline{\mathbb{Q}}(X)$ une fraction rationnelle à une indéterminée. Si f prend des valeurs entières en un nombre infini d'entiers relatifs, alors f est un polynôme (on peut le voir en prenant le résultant du dénominateur et du numérateur de f). Ce résultat ne tient évidemment plus si f est à plusieurs variables. Cependant, si l'ensemble des points entiers en lesquels f prend des valeurs entières est suffisamment « grand », on pourra affirmer que f est un polynôme. L'un des premiers résultats en ce sens est celui de M. Yasumoto [Y]. Avant de l'énoncer, on donne une définition.

Soient k un entier non nul et E un sous-ensemble de $\mathbb{Z}^k$. Pour tout entier positif M, on définit

$$E(M) = \{(n_1, \dots, n_k) \in E : \forall i \in \{1, \dots, k\},\ |n_i| \le M\}.$$

Théorème (M. Yasumoto). *Soit $E \subset \mathbb{Z}^k$ un ensemble vérifiant*

$$(*) \qquad \limsup_{M \to +\infty} \frac{\operatorname{card}(E(M))}{(2M+1)^k} > 0.$$

Soit $f \in \overline{\mathbb{Q}}(X_1, \dots, X_k)$ une fraction rationnelle. Si pour tout $(n_1, \dots, n_k)$ dans E, $f(n_1, \dots, n_k)$ est entier sur $\mathbb{Z}$ ou n'est pas défini, alors f est un élément de $\overline{\mathbb{Q}}[X_1, \dots, X_k]$.

Dans le cas de deux variables, une première amélioration de ce résultat a été démontrée par J. C. Masseron ([M]) qui obtient la même conclusion en remplaçant la condition $(*)$ par la suivante :

$$\limsup_{M \to +\infty} \frac{\operatorname{card}(E(M))}{(2M+1)^{3/2+\varepsilon}} > 0,$$

où $\varepsilon > 0$ peut être choisi aussi petit que l'on veut. Il conjectura de plus que l'exposant $3/2 + \varepsilon$ pouvait être remplacé par $1 + \varepsilon$. Les résultats démontrés ici donneront une réponse positive à cette conjecture.

2000 *Mathematics Subject Classification*: Primary 11C08; Secondary 11J72.

On s'intéresse ici au problème plus général suivant : soit K un corps de nombres et $\mathcal{O}$ son anneau d'entiers. Que peut-on dire si, dans l'énoncé précédent, on prend pour E un sous-ensemble de $\mathcal{O}^k$? L'un des problèmes qui apparaît est le fait que l'ensemble des unités $\mathcal{U}$ de $\mathcal{O}$ peut être infini.

On note $\overline{\mathbb{Z}}$ l'ensemble des éléments de $\overline{\mathbb{Q}}$ qui sont entiers sur $\mathbb{Z}$. On désigne par N la norme associée à l'extension K de $\mathbb{Q}$. Ainsi, on a l'égalité

$$\mathcal{U} = \{z \in \mathcal{O} : |N(z)| = 1\}.$$

Soit $M \geq 1$ un entier et E un sous-ensemble de $\mathcal{O}^k$. On définit

$$E(M) = \{(z_1, \dots, z_k) \in E : \forall i \in \{1, \dots, k\},\ |N(z_i)| \leq M\}.$$

En particulier, l'ensemble $\mathcal{O}^k(M)$ n'est pas toujours fini. Il l'est uniquement quand $K = \mathbb{Q}$ ou quand K est une extension quadratique imaginaire de $\mathbb{Q}$. Ainsi, si $K = \mathbb{Q}$ on a $\operatorname{card}(\mathcal{O}^1(M)) = 2M + 1$, et si K est une extension quadratique imaginaire de $\mathbb{Q}$, alors on dispose d'une majoration du type $\operatorname{card}(\mathcal{O}^1(M)) \leq cM$, où c est une constante ne dépendant que de K. Avec ces notations, on a le théorème suivant.

Théorème 1. *Soit K un corps qui est soit celui des rationnels, soit une extension quadratique imaginaire de ce dernier. Soit $f \in \overline{\mathbb{Q}}(X_1, \dots, X_k)$ une fraction rationnelle. Alors, il existe des constantes $\kappa > 0$, $\chi > 0$ et $M_0 > 0$, dépendant de K et de f, pour lesquelles pour tout sous-ensemble E de $\mathcal{O}^k$ vérifiant*

$$(**) \qquad \exists M > M_0, \quad \operatorname{card}(E(M)) > \kappa M^{k-1+\chi/\log\log(M)},$$

on a l'implication suivante :

$$\forall z \in E,\ f(z) \in \overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z \ \Rightarrow\ f \in \overline{\mathbb{Q}}[X_1, \dots, X_k].$$

Dans le cas d'une seule variable, la condition $(**)$ peut être remplacée par « l'ensemble E est infini ». Dans le cas de deux variables et quand K est le corps des rationnels, on peut améliorer la condition $(**)$ par la suivante :

$$\exists M > M_0, \quad \operatorname{card}(E(M)) > \kappa M \log(M)^{\chi},$$

en utilisant des résultats de J. G. van der Corput (voir [VDC]) concernant des moyennes de nombres de diviseurs d'entiers. Ce résultat sera développé en annexe.

On donne maintenant un corollaire direct dont l'énoncé est indépendant de la fraction f. Pour toute application $g : \mathbb{N} \to \mathbb{R}^+$ vérifiant les propositions suivantes :

$$(\mathrm{P}_1) \qquad \lim_{M \to +\infty} g(M) = 0,$$

$$(\mathrm{P}_2) \qquad \lim_{M \to +\infty} g(M) \log\log(M) = +\infty,$$

on a le corollaire suivant, qui améliore le résultat de M. Yasumoto.

COROLLAIRE 2. *Soit K un corps qui est soit celui des rationnels, soit une extension quadratique imaginaire de ce dernier. Soit E un sous-ensemble de $\mathcal{O}^k$ vérifiant*

$$\limsup_{M\to+\infty} \frac{\operatorname{card}(E(M))}{M^{k-1+g(M)}} > 0.$$

Si f est une fraction rationnelle de $\overline{\mathbb{Q}}(X_1,\dots,X_k)$ vérifiant

$$\forall z \in E, \quad f(z) \in \overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z,$$

alors f est un polynôme de $\overline{\mathbb{Q}}[X_1,\dots,X_k]$.

On s'intéresse ensuite au problème de Yasumoto généralisé pour des fractions rationnelles en une variable, et pour tous les corps de nombres K. Avant d'énoncer le résultat obtenu, on donne quelques notations.

Soit K un corps de nombres et $\mathcal{O}$ son anneau des entiers. On note n son degré sur $\mathbb{Q}$. On désigne encore par s le nombre d'isomorphismes réels de K dans $\mathbb{C}$, et par t celui des isomorphismes complexes. On a clairement $n = s + 2t$. On pose alors

$$r(K) = s + t - 1.$$

Le théorème démontré dans la partie 4 est le suivant.

THÉORÈME 3. *Soit K un corps dont on note $\mathcal{O}$ l'anneau des entiers. Soit $f \in \overline{\mathbb{Q}}(X)$ une fraction rationnelle dont le dénominateur n'est pas un monôme. Alors, il existe deux constantes $\kappa > 0$ et $M_0 > 0$, dépendant de K et de f, pour lesquelles pour tout sous-ensemble E de $\mathcal{O}$ vérifiant*

$$\exists M > M_0, \quad \operatorname{card}(E(M)) > \kappa \log(M)^{r(K)},$$

on a l'implication suivante :

$$\forall z \in E,\ f(z) \in \overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z \ \Rightarrow\ f \in \overline{\mathbb{Q}}[X].$$

De plus, l'exposant $r(K)$ est optimal.

On remarque que si f est de la forme $f(X) = 1/X^d$, alors f prend des valeurs entières sur l'ensemble des unités. Ainsi, si $r(K)$ est non nul (c'est-à-dire si K n'est ni le corps des rationnels, ni une extension quadratique imaginaire de ce dernier), il existe un nombre infini de z de norme égale à 1 pour lesquels $f(z)$ est entier. L'hypothèse faite sur la fraction f dans l'énoncé du théorème 3 n'est donc pas superflue.

Le corollaire suivant est une version du résultat précédent, où l'énoncé ne dépend plus de la fraction f choisie.

COROLLAIRE 4. *Soit E un sous-ensemble de $\mathcal{O}$ vérifiant*

$$\limsup_{M\to+\infty} \frac{\operatorname{card}(E(M))}{\log(M)^{r(K)}} = +\infty.$$

Pour toute fraction rationnelle $f \in \overline{\mathbb{Q}}(X)$ dont le dénominateur n'est pas un monôme, on a l'implication suivante :

$$\forall z \in E,\ f(z) \in \overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z \ \Rightarrow\ f \in \overline{\mathbb{Q}}[X].$$

On s'intéresse enfin au cas le plus général, où la fraction f est à plusieurs variables et à coefficients dans un corps de nombres quelconque. Ici, le fait que l'ensemble $\mathcal{U}$ puisse être infini constitue un véritable obstacle. On ne parvient pas à écarter une famille de fractions pour obtenir un résultat intéressant.

On considère par exemple les fractions

$$f_1(X,Y) = \frac{2}{X+Y} \quad \text{et} \quad f_2(X,Y) = \frac{X+1}{Y+1},$$

et l'ensemble $E = \{(u,u) : u \in \mathcal{U}\}$. Il est clair que f_1 et f_2 prennent des valeurs entières sur E, et que $E(1)$ est infini, dès que $r(K)$ est non nul.

On peut cependant obtenir un résultat convenable en n'utilisant non pas la norme d'un nombre algébrique $z \in K$, mais sa hauteur relative à K, définie comme suit :

$$H_K(z) = e^{[K:\mathbb{Q}]h(z)},$$

où $h(z)$ désigne la hauteur logarithmique absolue de Weil de z. Cette fois, le nombre d'éléments de K de hauteur bornée est fini. Soit E un sous-ensemble de $\mathcal{O}^k$; on note

$$E\langle M\rangle = \{(z_1,\dots,z_k) \in E : \forall i \in \{1,\dots,k\},\ H_K(z_i) \le M\}.$$

On remarque que cette définition prolonge encore celle de M. Yasumoto, car dans le cas où K est le corps des rationnels, si z est un entier, alors on a

$$|N(z)| = H_K(z) = |z|.$$

Avec ces notations, on a le théorème suivant, qui prolonge le théorème 1, uniquement quand K est le corps des rationnels.

Théorème 5. *Soit $f \in \overline{\mathbb{Q}}(X_1,\dots,X_k)$ une fraction rationnelle. Alors, il existe des constantes $\kappa > 0$, $\chi > 0$ et $M_0 > 0$, dépendant de K et de f, pour lesquelles pour tout sous-ensemble E de $\mathcal{O}^k$ vérifiant*

$$\exists M > M_0, \quad \operatorname{card}(E\langle M\rangle) > \kappa M^{k-1+\chi/\log\log(M)},$$

on a l'implication suivante :

$$\forall z \in E,\ f(z) \in \overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z \ \Rightarrow\ f \in \overline{\mathbb{Q}}[X_1,\dots,X_k].$$

Pour toute fonction $g : \mathbb{N} \to \mathbb{R}^+$ vérifiant les propriétés (P_1) et (P_2), on a le corollaire suivant.

Corollaire 6. *Soit K un corps de nombres. Soit E un sous-ensemble de $\mathcal{O}^k$ vérifiant*

$$\limsup_{M\to+\infty} \frac{\operatorname{card}(E\langle M\rangle)}{M^{k-1+g(M)}} > 0.$$

Si f est une fraction rationnelle de $\overline{\mathbb{Q}}(X_1,\dots,X_k)$ vérifiant

$$\forall z \in E, \quad f(z) \in \overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z,$$

alors f est un polynôme de $\overline{\mathbb{Q}}[X_1,\dots,X_k]$.

Les démonstrations des théorèmes 3 et 5 sont beaucoup moins directes que celle du théorème 1. Néanmoins, contrairement à celle de M. Yasumoto, aucune d'elles ne fait appel à l'axiome du choix. Avant de les commencer, on détermine une majoration du nombre de diviseurs d'un élément de l'anneau $\mathcal{O}$, où K est quelconque.

2. Majoration du nombre de classes de diviseurs. Soit K un corps de nombres de degré $n \in \mathbb{N}$ sur $\mathbb{Q}$, et $\mathcal{O}$ son anneau des entiers. Soit z un élément de l'anneau $\mathcal{O}$. Le but de ce paragraphe est de majorer le nombre de diviseurs $\delta(z)$ (ou de classes de diviseurs modulo les unités $\overline{\delta}(z)$) de z dans $\mathcal{O}$. L'anneau $\mathcal{O}$ n'étant pas toujours factoriel, on est amené à considérer les décompositions d'idéaux en produits d'idéaux premiers. D'après le théorème 3 page 60 de [S], tout idéal $\mathcal{I}$ de $\mathcal{O}$ a une décomposition unique en produit d'idéaux premiers. On a donc

$$\mathcal{I} = \prod_{\wp\in\mathcal{P}} \wp^{m_\wp(\mathcal{I})} \quad (m_\wp(\mathcal{I}) \in \mathbb{N}),$$

où $\mathcal{P}$ désigne l'ensemble des idéaux premiers de $\mathcal{O}$, et où les $m_\wp(z)$ sont nuls sauf un nombre fini. On écrit également ce produit pour l'idéal $(z) = z\mathcal{O}$:

$$(z) = \prod_{\wp\in\mathcal{P}} \wp^{m_\wp(z)} \quad (m_\wp(z) \in \mathbb{N}).$$

Soit $a \in \mathcal{O}$ un diviseur de z. Alors,

$$(z) \subset (a).$$

D'après l'assertion 8 page 62 de [S], pour tout $\wp \in \mathcal{P}$, on a $m_\wp(a) \le m_\wp(z)$. Par conséquent, il y a au plus $\widetilde{\delta}(z)$ idéaux (a) possibles, où

$$\widetilde{\delta}(z) = \prod_{\wp\in\mathcal{P}} (1 + m_\wp(z)).$$

On a toujours $\overline{\delta}(z) \le \widetilde{\delta}(z)$. Par analogie, si $\mathcal{I}$ est un idéal de $\mathcal{O}$, on pose

$$\widetilde{\delta}(\mathcal{I}) = \prod_{\wp\in\mathcal{P}} (1 + m_\wp(\mathcal{I})).$$

On cherche maintenant une majoration de $\widetilde{\delta}(z)$ à la manière de G. Tenenbaum, qui obtient dans [T, Chap. I.5, paragraphe 5.2] un ordre maximal de

la fonction $\log(\tau(m))$, où $\tau(m)$ désigne le nombre de diviseurs d'un entier relatif m. Plus précisément, on démontre la proposition suivante.

PROPOSITION 7. *Il existe une constante $\alpha(n) > 0$ pour laquelle, pour tout $z \in \mathcal{O}$ vérifiant $|N(z)| > e^e$, on a la majoration suivante :*

$$\log(\widetilde{\delta}(z)) \leq \frac{\log(2)\log|N(z)|}{\log\log|N(z)|}\left(1+\alpha(n)\,\frac{\log\log\log|N(z)|}{\log\log|N(z)|}\right).$$

On rappelle que N désigne la norme associée à l'extension K de $\mathbb{Q}$. La proposition 1 page 62 de [S] donne alors

$$|N(z)| = \operatorname{card}(\mathcal{O}/(z)).$$

Pour tout idéal $\mathcal{I}$ de $\mathcal{O}$, on introduit de façon analogue la notation

$$|N(\mathcal{I})| = \operatorname{card}(\mathcal{O}/\mathcal{I}).$$

Si $\mathcal{I}$ et $\mathcal{J}$ sont des idéaux de $\mathcal{O}$, on a $|N(\mathcal{I}\mathcal{J})| = |N(\mathcal{I})|\,|N(\mathcal{J})|$ (proposition 2 page 63 de [S]). Soit $t > 0$ un entier. On désigne par $c(t)$ le nombre d'idéaux premiers de $\mathcal{O}$ de norme inférieure ou égale à t. Le lemme suivant donne une majoration de $c(t)$.

LEMME 8. *Pour tout entier $t > 0$ on a la majoration*

$$c(t) \leq n\psi(t),$$

où $\psi(t)$ désigne le nombre de nombres premiers inférieurs ou égaux à t.

Preuve. Soit $\wp$ un idéal premier de $\mathcal{O}$ vérifiant

$$|N(\wp)| = R \leq t.$$

L'ordre de 1 dans $\mathcal{O}/\wp$ est un diviseur de $R = \operatorname{card}(\mathcal{O}/\wp)$. Ainsi, R est un élément de $\wp$. Comme l'idéal $\wp$ est premier, il existe un nombre premier $p \leq t$ contenu dans $\wp$. Par suite, l'idéal $p\mathcal{O}$ est inclus dans $\wp$, et donc $\wp$ est l'un des idéaux premiers définissant $p\mathcal{O}$.

Soient $\wp_1, \ldots, \wp_q$ les idéaux premiers définissant $p\mathcal{O}$. Pour tout $i = 1, \ldots, q$ on note f_i le degré résiduel de $\wp_i$ sur $\mathbb{Z}$, c'est-à-dire la dimension du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\mathcal{O}/\wp_i$. On a alors (voir par exemple [S, §5.2, théorème 1])

$$\sum_{i=1}^{q} m_{\wp_i}(p\mathcal{O}) \cdot f_i = n.$$

Il existe donc au plus n idéaux premiers définissant $p\mathcal{O}$, d'où le lemme. ∎

Preuve de la proposition 7. On se donne un réel $t > 0$, que l'on fixera dans la suite. Soit z un élément de $\mathcal{O}$. On pose $N = |N(z)|$, et on suppose que $N > e^e$. On a, d'une part, les majorations

$$\begin{aligned}\prod_{|N(\wp)|>t}(1+m_\wp(z)) &\le \prod_{|N(\wp)|>t} 2^{m_\wp(z)}\\ &\le \Big(\prod_{|N(\wp)|>t}|N(\wp)|^{m_\wp(z)}\Big)^{\log(2)/\log(t)}\\ &\le \Big|\prod_{\wp\in\mathcal{P}} N(\wp)^{m_\wp(z)}\Big|^{\log(2)/\log(t)} \le N^{\log(2)/\log(t)}.\end{aligned}$$

D'autre part, pour tout idéal premier $\wp$, on a aussi $N = |N(z)| \ge 2^{m_\wp(z)}$. Grâce au lemme 8, on obtient

$$\prod_{|N(\wp)|\le t}(1+m_\wp(z)) \le \prod_{|N(\wp)|\le t}\left(1+\frac{\log(N)}{\log(2)}\right) \le \left(1+\frac{\log(N)}{\log(2)}\right)^{n\psi(t)}.$$

On termine la preuve de la proposition 7. On pose

$$t = \frac{\log(N)}{(\log\log(N))^3};$$

on obtient alors

$$\begin{aligned}\log(\widetilde{\delta}(z)) &\le nt\log\left(1+\frac{\log(N)}{\log(2)}\right)+\frac{\log(2)\log(N)}{\log(t)}\\ &\le 2nt\log(1+\log(N))+\frac{\log(2)\log(N)}{\log(t)}\\ &\le \frac{2n\log(N)\log(1+\log(N))}{(\log\log(N))^3}+\frac{\log(2)\log(N)}{\log\log(N)-3\log\log\log(N)}\\ &\le \frac{\log(2)\log(N)}{\log\log(N)}\left(1+\alpha(n)\,\frac{\log\log\log(N)}{\log\log(N)}\right),\end{aligned}$$

d'où la proposition. ∎

Les corollaires suivants en découlent facilement.

Corollaire 9. *Soit K un corps de nombres de degré n sur $\mathbb{Q}$. Il existe une constante $\alpha(n) > 0$ pour laquelle, pour tout $z \in \mathcal{O}$ vérifiant $|N(z)| > e^e$, on a la majoration suivante* :

$$\log(\overline{\delta}(z)) \le \frac{\log(2)\log|N(z)|}{\log\log|N(z)|}\left(1+\alpha(n)\,\frac{\log\log\log|N(z)|}{\log\log|N(z)|}\right).$$

Corollaire 10. *Si K est le corps des rationnels, ou une extension quadratique imaginaire de ce dernier, alors pour tout $z \in \mathcal{O}$ vérifiant $|N(z)| > e^e$, on a la majoration suivante* :

$$\log(\delta(z)) \le \frac{\log(2)\log|N(z)|}{\log\log|N(z)|}\left(1+\alpha\,\frac{\log\log\log|N(z)|}{\log\log|N(z)|}\right)+\log(6).$$

3. Démonstration du théorème 1. On suppose dans cette partie que K est soit le corps des rationnels, soit une extension quadratique imaginaire de $\mathbb{Q}$, et que la fraction $f \in \overline{\mathbb{Q}}(X_1, \dots, X_k)$ dépend effectivement de deux variables au moins. Le cas particulier où $k = 1$ est en effet élémentaire, il sera néanmoins abordé au paragraphe suivant dans le cas de corps de nombres quelconque.

On montre dans un premier temps le théorème 1 pour une fraction à coefficients dans K. On verra à la fin de ce paragraphe comment se ramener à ce cas quand f est à coefficients dans $\overline{\mathbb{Q}}$.

On se donne donc une fraction rationnelle $f = P/Q$, et l'on suppose que Q n'est pas un polynôme constant. On peut donc choisir P et Q dans $K[X_1, \dots, X_l, Y]$, où l'on a noté $l = k-1$, et où le polynôme Q dépend effectivement de la variable Y. Quitte à multiplier P et Q par un dénominateur, et à les diviser par leurs facteurs communs, on peut supposer qu'ils sont à coefficients dans $\mathcal{O}$, et que leur résultant $R \in \mathcal{O}[X_1, \dots, X_l]$ en la variable Y est non nul. On considère l'ensemble

$$E_0 = \left\{(x_1, \dots, x_l, y) \in \mathcal{O}^{l+1} : Q(x_1, \dots, x_l, y) = 0 \text{ ou } \frac{P(x_1, \dots, x_l, y)}{Q(x_1, \dots, x_l, y)} \in \mathcal{O}\right\}.$$

Puisque R est combinaison linéaire à coefficients dans $\mathcal{O}[X_1, \dots, X_l]$ de P et de Q, on a clairement l'inclusion $E_0 \subseteq F_0$, où

$$F_0 = \left\{(x_1, \dots, x_l, y) \in \mathcal{O}^{l+1} : Q(x_1, \dots, x_l, y) = 0 \text{ ou } \frac{R(x_1, \dots, x_l)}{Q(x_1, \dots, x_l, y)} \in \mathcal{O}\right\}.$$

Soit $M \geq 1$ un entier. Dans la suite, on détermine une majoration du cardinal de $F_0(M)$. Pour cela, on fixe tout d'abord $(x_1, \dots, x_l)$ dans $\mathcal{O}^l(M)$. Si le polynôme $Q(x_1, \dots, x_l, Y)$ n'est pas nul, on a

$$\operatorname{card}\{y \in \mathcal{O}(M) : Q(x_1, \dots, x_l, y) = 0\} \leq \deg_Y Q,$$

$$\operatorname{card}\left\{y \in \mathcal{O}(M) : \frac{R(x_1, \dots, x_l)}{Q(x_1, \dots, x_l, y)} \in \mathcal{O}\right\} \leq \deg_Y Q \cdot \delta(R(x_1, \dots, x_l)).$$

On majore maintenant le cardinal de l'ensemble $\mathcal{G}_Q(M)$ composé des points $(x_1, \dots, x_l) \in \mathcal{O}^l(M)$ pour lesquels le polynôme $Q(x_1, \dots, x_l, Y)$ est nul. Soit $(x_1, \dots, x_l) \in \mathcal{O}^l(M)$. Puisque Q dépend réellement de la variable Y, il existe un polynôme $Q_0 \in \mathcal{O}[X_1, \dots, X_l]$ non nul (l'un des coefficients de Q vu comme polynôme en Y), et dont les degrés en X_i sont respectivement inférieurs ou égaux à ceux de Q, pour lequel

$$Q_0(x_1, \dots, x_l) = 0.$$

Soit Q_0 est une constante non nulle et dans ce cas l'ensemble $\mathcal{G}_Q(M)$ est vide, soit le polynôme Q_0 dépend au moins d'une variable. On a alors

$$\begin{aligned}\operatorname{card}(\mathcal{G}_Q(M)) &\leq \operatorname{card}\{(x_1, \dots, x_l) \in \mathcal{O}^l(M) : Q_0(x_1, \dots, x_l) = 0\} \\ &\leq \deg(Q_0) \operatorname{card}(\mathcal{O}^{l-1}(M)).\end{aligned}$$

On obtient alors

$$\operatorname{card}(F_0(M)) \leq 2\deg Q\Big(\operatorname{card}(\mathcal{O}^l(M)) + \sum_{\substack{\mathbf{x}\in\mathcal{O}^l(M)\setminus\mathcal{G}_Q(M)\\ \mathbf{x}=(x_1,\ldots,x_l)}} \delta(R(x_1,\ldots,x_l))\Big).$$

Si R est un polynôme constant, alors on peut trouver une constante C_0 ne dépendant que de K, P et Q, et pour laquelle

$$\operatorname{card}(F_0(M)) \leq C_0 \operatorname{card}(\mathcal{O}^l(M)).$$

On suppose désormais que le résultant R n'est pas constant, et on note ϱ son degré total. Par choix de K, la norme associée à l'extension K de $\mathbb{Q}$ vérifie l'inégalité triangulaire. Ainsi, il existe une constante $C_1 > 0$ pour laquelle si $M > e^e$, on a

$$\forall (x_1,\ldots,x_l) \in \mathcal{O}^l(M), \qquad N(R(x_1,\ldots,x_l)) \leq C_1(M^\varrho + 1).$$

De plus, d'après le corollaire 10, pour tout $z \in \mathcal{O}$ vérifiant $|N(z)| > e^e$, on a la majoration

$$\log(\delta(z)) \leq \frac{\log(2)\log|N(z)|}{\log\log|N(z)|}\left(1 + \alpha\,\frac{\log\log\log|N(z)|}{\log\log|N(z)|}\right) + \log(6).$$

En particulier, avec $z = R(x_1,\ldots,x_l)$, où $(x_1,\ldots,x_l) \in \mathcal{O}^l(M)$, on obtient l'existence d'une constante $C_2 > 0$ pour laquelle

$$\log(\delta(R(x_1,\ldots,x_l))) \leq C_2\left(\frac{\log(M)}{\log\log(M)} + 1\right).$$

Ainsi, il existe une constante $C_3 > 0$, ne dépendant que de K et de f, et vérifiant

$$\delta(R(x_1,\ldots,x_l)) \leq C_3 M^{C_2/\log\log(M)}.$$

On obtient finalement l'existence d'une constante $C_4 > 0$, pour laquelle

$$\begin{aligned}\operatorname{card}(F_0(M)) &\leq 2\deg Q\Big(\operatorname{card}(\mathcal{O}^l(M)) + \sum_{\substack{\mathbf{x}\in\mathcal{O}^l(M)\setminus\mathcal{G}_Q(M)\\ \mathbf{x}=(x_1,\ldots,x_l)}} C_3 M^{C_2/\log\log(M)}\Big),\\ &\leq C_4(M^{l+C_2/\log\log(M)} + 1).\end{aligned}$$

On a donc démontré que si $f \in K(X_1,\ldots,X_k)$ est une fraction rationnelle, il existe des constantes $\chi > 0$, $\kappa > 0$ et $M_0 > 0$ pour lesquelles si f n'est pas définie ou prend des valeurs entières sur $\mathbb{Z}$ sur un ensemble E vérifiant

$$\exists M > M_0, \qquad \operatorname{card}(E(M)) > \kappa M^{k-1+\chi/\log\log(M)},$$

alors nécessairement f est un polynôme.

On se place désormais dans les conditions du théorème 1, et on utilise le résultat précédent. La fraction f est donc à coefficients dans $\overline{\mathbb{Q}}$, et pour chaque point z de E, soit $f(z)$ n'existe pas, soit $f(z)$ est entier sur $\mathbb{Z}$. Soit K_1 l'extension engendrée sur K par tous les coefficients de la fraction f, et

$g_1, \dots, g_\mu$ les K-isomorphismes du corps K_1. On pose $X = (X_1, \dots, X_k)$ et on considère le polynôme

$$G(Y) = \prod_{i=1}^{\mu} (Y - g_i(f(X))) = \sum_{i=0}^{\mu} G_i(X) Y^i \in K(X)[Y].$$

Pour tout $z \in \mathcal{O}$ et pour tout $i \in \{1, \dots, \mu\}$, on a l'implication suivante :

$$f(z) \text{ entier sur } \mathbb{Z} \ \Rightarrow \ G_i(z) \in \mathcal{O}.$$

Ainsi, d'après le résultat intermédiaire précédent, à condition de choisir des constantes χ, κ et M_0 suffisamment grandes, les G_i sont des polynômes. Par suite, $G(Y)$ est un élément de $(K[X])[Y]$. Or, il est unitaire et s'annule en $f(X)$. Par conséquent, $f(X) \in \overline{\mathbb{Q}}(X)$ est entière sur $\mathbb{Q}[X]$, c'est donc un polynôme : $f(X) \in \overline{\mathbb{Q}}[X]$. ∎

4. Fractions rationnelles en une variable. Il est clair que si K est le corps des rationnels ou une extension quadratique imaginaire de ce dernier, et si $f \in \overline{\mathbb{Q}}[X]$ n'est pas définie ou prend des valeurs entières sur un sous-ensemble E de $\mathcal{O}$, il suffit de savoir que E est infini pour conclure que f est un polynôme. Dans le cas d'un corps de nombres quelconque, ce fait n'a plus lieu. Avant de commencer la démonstration du théorème 3, on donne quelques définitions et notations.

On note $r = r(K) = s + t - 1$, et $\sigma_1, \dots, \sigma_s, \sigma_{s+1}, \overline{\sigma}_{s+1}, \dots, \sigma_{s+t}, \overline{\sigma}_{s+t}$ les isomorphismes de K dans $\mathbb{C}$. Le théorème de Dirichlet (voir [BS, chap. II, §4.3]) donne alors l'existence d'un r-uplet $(\varepsilon_1, \dots, \varepsilon_r)$ d'unités de $\mathcal{O}$, appelé *système d'unités fondamentales* de $\mathcal{U}$, tel que toute unité $\varepsilon \in \mathcal{U}$ s'écrive de manière unique sous la forme

$$\varepsilon = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r},$$

où ζ est une racine de l'unité appartenant au corps K, et où $(n_1, \dots, n_r)$ est un r-uplet d'entiers relatifs. On fixe désormais un système d'unités fondamentales $(\varepsilon_1, \dots, \varepsilon_r)$ de $\mathcal{U}$. Soit $\varepsilon = \zeta \varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$ un élément de $\mathcal{U}$; on pose

$$\varrho(\varepsilon) = \max\{|n_i| : i = 1, \dots, r\}.$$

On s'intéresse maintenant au théorème 3. De la même manière que dans la preuve du théorème 1, on peut se ramener au cas où la fraction f est à coefficients dans K. De plus, quitte à prendre le résultant du numérateur et du dénominateur de f, on peut supposer qu'elle s'écrit de la façon suivante :

$$f(X) = \frac{a}{X^\nu P(X)} = \frac{a}{X^\nu (a(d) X^d + \cdots + a(1) X + a(0))},$$

où les nombres $a, a(d), \dots, a(0)$ sont des éléments de $\mathcal{O}$, et où $d, a(0)$ et $a(d)$ sont non nuls. On se donne enfin un ensemble $D(a) \subset \mathcal{O}$ formé de la famille

des diviseurs de a, non associés deux à deux :

$$D(a) = \{\delta_1, \dots, \delta_J\},$$

où $(\delta_1, \dots, \delta_J)$ est un système de représentants des classes de diviseurs de a modulo la relation d'équivalence $\sim$ définie comme suit :

$$\delta \sim \delta' \ (\delta \text{ et } \delta' \text{ sont } \textit{associés}) \ \Leftrightarrow \ \exists \varepsilon \in \mathcal{U},\ \delta = \varepsilon\delta'.$$

Si $a(0)$ est un diviseur de a, alors on le choisit comme représentant de sa classe modulo les unités. Ainsi, si $a(0)$ divise a alors c'est un élément de $D(a)$. On définit enfin

$$E_0 = \{z \in \mathcal{O} : z^\nu P(z) \,|\, a\}.$$

La démonstration du théorème 3 comporte trois étapes, dont les résultats seront regroupés dans une brève conclusion. On verra aussi que dans le cas particulier où ν est non nul, l'ensemble E_0 est fini. On donnera enfin un exemple illustrant le caractère optimal de l'exposant $r(K)$.

Première étape : Recherche de k pour lequel $|\sigma_k(\varepsilon)|$ est « grand ». Dans ce paragraphe, on montre le lemme général suivant.

Lemme 11. *Il existe une constante $\xi > 0$ dépendant de $(\varepsilon_1, \dots, \varepsilon_r)$ telle que pour toute unité ε de K, on puisse trouver un indice $k \in \{1, \dots, s+t\}$ vérifiant la minoration*

$$|\sigma_k(\varepsilon)| > e^{\xi \varrho(\varepsilon)}.$$

Preuve. Puisque ε est une unité, il s'écrit $\varepsilon = \zeta\varepsilon_1^{n_1} \cdots \varepsilon_r^{n_r}$, où ζ est une racine de l'unité de K, et où $(n_1, \dots, n_r)$ est un r-uplet d'entiers relatifs. On définit encore les objets suivants. Si λ est un élément de K, on note

$$\begin{aligned}\ell(\lambda) &= (\log|\sigma_1(\lambda)|, \dots, \log|\sigma_s(\lambda)|, \log|\sigma_{s+1}(\lambda)|^2, \dots, \log|\sigma_{s+t}(\lambda)|^2) \\ &= (\ell_1(\lambda), \dots, \ell_{s+t}(\lambda)).\end{aligned}$$

C'est un résultat classique que l'ensemble $\Lambda = \{\ell(\lambda) : \lambda \in \mathcal{U}\} \subset \mathbb{R}^{s+t}$ est un réseau de rang $r = s + t - 1$. Puisque pour tout indice i, on a l'égalité

$$|\sigma_i(\varepsilon)| = |\sigma_i(\varepsilon_1)|^{n_1} \cdots |\sigma_i(\varepsilon_r)|^{n_r},$$

on a aussi

$$\ell_i(\varepsilon) = \sum_{j=1}^{r} n_j \ell_i(\varepsilon_j).$$

Ainsi, si l'on note $A(\varepsilon_1, \dots, \varepsilon_r)$ la matrice $[\ell_i(\varepsilon_j)]_{\substack{i=1,\dots,s+t \\ j=1,\dots,r}}$, on a l'égalité

$$A(\varepsilon_1, \dots, \varepsilon_r) \cdot \begin{pmatrix} n_1 \\ \vdots \\ n_r \end{pmatrix} = \begin{pmatrix} \ell_1(\varepsilon) \\ \vdots \\ \ell_r(\varepsilon) \end{pmatrix}.$$

La matrice $A(\varepsilon_1,\dots,\varepsilon_r)$ est de rang r, et tous ses mineurs d'ordre r sont égaux à un même nombre $\mathcal{R}$ ([BS, chap. II, §4.4]), qui ne dépend pas du système $(\varepsilon_1,\dots,\varepsilon_r)$ d'unités fondamentales choisi. Ce nombre $\mathcal{R}$ est appelé *régulateur* du corps K. On peut inverser le système linéaire précédent, et obtenir des relations du type suivant :

$$\forall p \in \{1,\dots r\}, \quad n_p = \frac{1}{\mathcal{R}} \sum_{q=1}^{s+t} \beta_{p,q}(\varepsilon_1,\dots,\varepsilon_r)\ell_q(\varepsilon),$$

où les $\beta_{p,q}(\varepsilon_1,\dots,\varepsilon_r)$ sont des polynômes homogènes de degré $r-1$ en les $\ell_i(\varepsilon_j)$. On peut donc trouver une constante $C_0 > 0$ ne dépendant que de $(\varepsilon_1,\dots,\varepsilon_r)$ vérifiant

$$\varrho(\varepsilon) \le C_0 \max\{|\ell_q(\varepsilon)| : q = 1,\dots,s+t\}.$$

Soit $j \in \{1,\dots,s+t\}$ pour lequel $|\ell_j(\varepsilon)| = \max\{|\ell_q(\varepsilon)| : q = 1,\dots,s+t\}$.

Si $\ell_j(\varepsilon) > 0$, alors en prenant $k = j$ le lemme est clairement démontré.

Si $\ell_j(\varepsilon) < 0$, alors on a $\varrho(\varepsilon) \le -C_0\ell_j(\varepsilon)$. Puisque ε est de norme 1, on a $\sum_{q=1}^{s+t} \ell_q(\varepsilon) = 0$, ainsi

$$\sum_{\substack{q=1\\ q\neq j}}^{s+t} \ell_q(\varepsilon) = -\ell_j(\varepsilon) \ge \frac{1}{C_0}\,\varrho(\varepsilon).$$

Par conséquent, il existe un indice $q \in \{1,\dots,s+t\}$ pour lequel

$$\ell_q(\varepsilon) \ge \frac{1}{rC_0}\,\varrho(\varepsilon).$$

Le lemme 11 est donc établi en choisissant $k = q$. ∎

Deuxième étape : Minoration de $|\sigma_k(z)|$. Soit z un élément de E_0. Ainsi, $P(z)$ divise a dans l'anneau $\mathcal{O}$. Par définition de $D(a)$, il existe donc un unique $\delta \in D(a)$ pour lequel $\varepsilon = \mathcal{P}(z)/\delta$ est une unité de $\mathcal{O}$. On rappelle que le polynôme P s'écrit de la façon suivante :

$$P(X) = a(d)X^d + \cdots + a(1)X + a(0).$$

On définit alors la *maison* de P par

$$\overline{|P|} = \max\{|\sigma_i(a(j))| : i = 1,\dots,s+t \text{ et } j = 0,\dots,d\}.$$

D'une part, on a les majorations

$$\forall i \in \{1,\dots,s+t\},\ \forall x \in \mathbb{C}, \quad |\sigma_i(P)(x)| \le (d+1)\overline{|P|}(|x|^d + 1).$$

D'autre part, ε est une unité, donc, d'après le lemme précédent, on peut trouver un indice $k \in \{1,\dots,s+t\}$ vérifiant $|\sigma_k(\varepsilon)| \ge e^{\xi\varrho(\varepsilon)}$. Par conséquent,

$$e^{\xi\varrho(\varepsilon)} \le \left|\frac{\sigma_k(P)(\sigma_k(z))}{\sigma_k(\delta)}\right| \le \frac{(d+1)\overline{|P|}}{|\sigma_k(\delta)|}\,(|\sigma_k(z)|^d + 1),$$

et donc, on obtient une minoration de $|\sigma_k(z)|^d$:

$$|\sigma_k(z)|^d \geq C_1 e^{\xi\varrho(\varepsilon)} - 1 \geq \frac{C_1}{2}\, e^{\xi\varrho(\varepsilon)},$$

où la constante

$$C_1 = \frac{\min\{|\sigma_i(\delta)| : \delta \in D(a),\, i \in \{1,\dots,s+t\}\}}{(d+1)\overline{|P|}}$$

ne dépend que de P et de a, et où la deuxième minoration a lieu pour $\varrho(\varepsilon)$ suffisamment grand.

Finalement, on a démontré qu'il existe k pour lequel, si $\varrho(\varepsilon)$ est suffisamment grand, on a

$$|\sigma_k(z)| \geq \frac{C_1^{1/d}}{2}\, e^{C_2\varrho(\varepsilon)},$$

où $C_2 = \xi/d$ est une constante dépendant de K et de d.

Troisième étape : Minoration des autres $|\sigma_i(z)|$. C'est dans cette partie qu'intervient l'hypothèse faite sur f. On rappelle qu'on a choisi $z \in E$ et $\delta \in D(a)$ tels que $\varepsilon = P(z)/\delta$ soit une unité. On a décomposé cette unité dans le système d'unités fondamentales choisi,

$$\varepsilon = \zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r},$$

où $\zeta \in K$ est une racine de l'unité, et où $(n_1,\dots,n_r) \in \mathbb{Z}^r$. On a donc

$$P(z) = a(d)z^d + \cdots + a(1)z + a(0) = \delta\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}.$$

Comme d et $a(d)$ ne sont pas nuls, on peut écrire cette relation sous la forme

$$zA(z) = \delta\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r} - a(0),$$

où $A(z) = a(d)z^{d-1} + \cdots + a(1)$. Si $|\sigma_i(z)|$ est supérieur à 1, alors on en a une bonne minoration. Sinon, $|\sigma_i(z)| < 1$, et donc

$$|\sigma_i(A)(\sigma_i(z))| \leq d\overline{|P|}.$$

On obtient alors

$$\begin{aligned}
|\sigma_i(z)| &= \frac{|\sigma_i(\delta\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r} - a(0))|}{|\sigma_i(A)(\sigma_i(z))|} \\
&\geq \frac{|\sigma_i(a(0))|}{d\overline{|P|}}\left|\sigma_i\left(\frac{\delta}{a(0)}\,\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}\right) - 1\right| \\
&\geq C_3\left|\sigma_i\left(\frac{\delta}{a(0)}\,\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}\right) - 1\right|.
\end{aligned}$$

Il reste donc à minorer

$$\left|\sigma_i\left(\frac{\delta}{a(0)}\,\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}\right) - 1\right|.$$

On utilise pour cela un résultat de P. Philippon et de M. Waldschmidt (voir [PW]), et on distingue deux cas.

Premier cas : $\delta = a(0)$. On doit trouver une bonne minoration de $|\sigma_i(\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r})-1|$. Par unicité de l'écriture de $\varepsilon=\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}$, ce nombre est non nul, on peut donc utiliser le théorème 1.2 de [PW]. Si ϱ est supérieur ou égal à e, on a

$$\varrho(\varepsilon)\le\varrho \;\Rightarrow\; |\sigma_i(\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r})-1|>e^{-C_4\log(\varrho)},$$

où $C_4>0$ ne dépend que de K et du système d'unités fondamentales choisi. On obtient donc le résultat suivant :

$\forall\varrho>\varrho_1$, $\forall i\in\{1,\dots,s+t\}$, $\forall z\in E_0$, si $P(z)=\varepsilon\delta$ avec $\delta\in D(a)$ et $\varepsilon\in\mathcal{U}$:

$$\varrho(\varepsilon)\le\varrho \;\Rightarrow\; |\sigma_i(z)|\ge e^{-C_5\log(\varrho)},$$

où ϱ_1 et C_5 sont des constantes dépendant de K et du système d'unités fondamentales choisi.

Deuxième cas : $\delta\ne a(0)$. Par choix de $D(a)$, δ et $a(0)$ ne sont pas associés, ce qui signifie que le quotient $\delta/a(0)$ n'est pas une unité. Comme précédemment, on détermine une minoration du nombre non nul

$$\left|\sigma_i\left(\frac{\delta}{a(0)}\,\zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}\right)-1\right|.$$

On applique comme dans le cas précédent le théorème 1.2 de [PW]. On obtient donc, de la même manière, une minoration de $|\sigma_i(z)|$, à ceci près que les constantes ϱ_1 et C_5 dépendent maintenant de K, δ (donc a) et $a(0)$.

Conclusion. Soit $z\in\mathcal{O}$ tel que $f(z)$ soit un élément de $\mathcal{O}$. D'après la deuxième étape, il existe un indice $k\in\{1,\dots,s+t\}$ pour lequel $|\sigma_k(z)|>e^{C_6\varrho(\varepsilon)}$ (si $\varrho(\varepsilon)$ est assez grand), où ε est uniquement déterminé par l'égalité

$$P(z)=\varepsilon\delta\quad(\delta\in D(a)).$$

La troisième étape donne une minoration pour tous les autres $|\sigma_i(z)|$. Si $\varrho(\varepsilon)$ est suffisamment grand, on a

$$\forall i\in\{1,\dots,s+t\},\quad |\sigma_i(z)|>e^{-C_5\log(\varrho(\varepsilon))}.$$

En multipliant ces inégalités, on obtient

$$\varrho(\varepsilon)>\varrho_2 \;\Rightarrow\; |N(z)|>e^{C_7\varrho(\varepsilon)},$$

où $\varrho_2>0$ et $C_7>0$ sont des constantes dépendant de K et de f. Ainsi, si z est un élément de $E(M)$, alors $\varrho(\varepsilon)$ est plus petit que

$$\max\left(\varrho_2,\frac{1}{C_7}\log(M)\right)\le C_8\log(M).$$

On désigne par $c(K)$ le cardinal du groupe fini des racines de l'unité de $\mathcal{U}$; il y a alors au plus

$$c(K)(2C_8\log(M)+1)^r$$

choix possibles pour $\varepsilon = \zeta\varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r}$. De plus, à chaque ε et à chaque $\delta \in D(a)$, il y a au plus $\deg(P)$ valeurs possibles pour z. Ainsi, on a les majorations suivantes, qui achèvent la démonstration du théorème 3 :

$$\begin{aligned}\operatorname{card}(E_0(M)) &\le c(K)\deg(P)\operatorname{card}(D(a))(2C_8\log(M)+1)^r\\ &\le C_9(\log(M)^r+1),\end{aligned}$$

où C_9 est une constante dépendant de K, a et P.

Cas particulier : $\nu \ge 1$. Dans ce cas, si z est un élément de $\mathcal{O}$ tel que $f(z)$ est entier sur $\mathbb{Z}$, alors z divise a dans $\mathcal{O}$, et donc

$$|N(z)| \le |N(a)|.$$

Par conséquent, l'ensemble $E_0(|N(a)|)$ est l'ensemble E_0 tout entier, ce dernier est donc fini.

Optimalité. On se donne la fraction f définie par

$$f(X) = \frac{1}{X-1},$$

et l'on considère l'ensemble E formé des entiers de la forme

$$z(n_1,\dots,n_r) = \varepsilon_1^{n_1}\cdots\varepsilon_r^{n_r} + 1.$$

Par unicité de l'écriture d'une unité dans la base fondamentale $(\varepsilon_1,\dots,\varepsilon_r)$, les $z(n_1,\dots,n_r)$ sont distincts. Il existe de plus une constante $C>0$ pour laquelle, pour tout $z = z(n_1,\dots,n_r) \in E$, on a

$$\begin{aligned}|N(z)| &= \prod_{i=1}^{s}|\sigma_i(z)| \prod_{i=s+1}^{s+t}|\sigma_i(z)|^2\\ &\le \prod_{i=1}^{s}(|\sigma_i(\varepsilon_1^{n_1})\cdots\sigma_i(\varepsilon_r^{n_r})|+1)\prod_{i=s+1}^{s+t}(|\sigma_i(\varepsilon_1^{n_1})\cdots\sigma_i(\varepsilon_r^{n_r})|+1)^2\\ &\le e^{C\max\{|n_1|,\dots,|n_r|\}}.\end{aligned}$$

Ainsi, dès que $\max\{|n_1|,\dots,|n_r|\}$ est plus petit que $(1/C)\log(M)$, l'entier $z(n_1,\dots,n_r)$ est un élément de $E(M)$. Par conséquent,

$$\operatorname{card}(E(M)) \ge \frac{1}{C^r}\log(M)^r,$$

ce qui montre bien que l'exposant $r = r(K)$ est optimal.

5. Cas général. Dans cette partie, K est un corps de nombres quelconque. On se donne une fraction $f \in \overline{\mathbb{Q}}(X_1,\dots,X_k)$ dépendant de $k \ge 2$ variables au moins. Comme précédemment, on peut se ramener au cas où f est à coefficients dans K. On considère R et Q dans $K[X_1,\dots,X_l,Y]$, où $l = k-1$. On suppose que le polynôme Q n'est pas constant, et qu'il

dépend effectivement de la variable Y. Quitte à faire les mêmes manipulations algébriques élémentaires que dans les parties précédentes, on peut supposer que R ne dépend pas de Y, et que les polynômes R et Q sont à coefficients dans $\mathcal{O}$. La démonstration qui suit est une combinaison des deux précédentes. On considère l'ensemble

$$F_0 = \left\{(x_1, \dots, x_l, y) \in \mathcal{O}^l : Q(x_1, \dots, x_l, y) = 0 \text{ ou } \frac{R(x_1, \dots, x_l)}{Q(x_1, \dots, x_l, y)} \in \mathcal{O}\right\}.$$

On détermine une majoration du cardinal de $F_0\langle M\rangle$.

On fixe désormais un système d'unités fondamentales $(\varepsilon_1, \dots, \varepsilon_r)$ de $\mathcal{U}$. On définit tout d'abord la notion d'entier réduit modulo le système $(\varepsilon_1, \dots, \varepsilon_r)$. Soit $\lambda \in K$; on pose $N = |N(\lambda)|$. On rappelle que l'on a noté

$$\begin{aligned}\ell(\lambda) &= (\log|\sigma_1(\lambda)|, \dots, \log|\sigma_s(\lambda)|, \log|\sigma_{s+1}(\lambda)|^2, \dots, \log|\sigma_{s+t}(\lambda)|^2)\\ &= (\ell_1(\lambda), \dots, \ell_{s+t}(\lambda)).\end{aligned}$$

Ainsi, $\ell(\lambda)$ appartient à l'hyperplan affine d'équation

$$(\mathcal{H}(N)) \qquad \sum_{i=1}^{s+t} X_i = \log(N),$$

qui est parallèle à celui engendré par les unités de K, et d'équation

$$(\mathcal{H}(1)) \qquad \sum_{i=1}^{s+t} X_i = 0.$$

L'ensemble $\Lambda = \{\ell(\varepsilon) : \varepsilon \in \mathcal{U}\}$ est un réseau de $(\mathcal{H}(1))$, par conséquent

$$\Lambda_N = \Lambda + (\log(N), 0, \dots, 0)$$

est un translaté de Λ dans $(\mathcal{H}(N))$. Ainsi, tout parallélogramme fondamental dans $(\mathcal{H}(N))$ contient un et un seul entier associé à λ. On considère le parallélogramme fondamental suivant :

$$\Pi(N) = \{(\log(N), 0, \dots, 0) + x_1\ell(\varepsilon_1) + \cdots + x_r\ell(\varepsilon_r) : x_1, \dots, x_r \in [0, 1[\}.$$

On dira alors que λ est *réduit modulo* $(\varepsilon_1, \dots, \varepsilon_r)$, s'il appartient au parallélogramme $\Pi(|N(\lambda)|)$. L'intérêt des entiers réduits est que leurs conjugués ne « s'éloignent » pas trop de leur norme. En effet, si λ est réduit modulo $(\varepsilon_1, \dots, \varepsilon_r)$, alors on a

$$\ell(\lambda) = (\log(N), 0, \dots, 0) + x_1\ell(\varepsilon_1) + \cdots + x_r\ell(\varepsilon_r)$$

avec $0 \le x_i < 1$ pour $i = 1, \dots, s+t$. Par conséquent, on a les encadrements suivants :

$$\log(N) - \sum_{j=1}^{r} |\ell_1(\varepsilon_j)| \le \ell_1(\lambda) \le \log(N) + \sum_{j=1}^{r} |\ell_1(\varepsilon_j)|,$$

$$|\ell_i(\lambda)| \le \sum_{j=1}^{r} |\ell_i(\varepsilon_j)| \quad (i = 2, \dots, r).$$

Ainsi, on a le lemme qui suit.

LEMME 12. *Soit* $(\varepsilon_1, \dots, \varepsilon_r)$ *un système d'unités fondamentales de* $\mathcal{U}$. *Alors, il existe* $\eta_1 > 0$ *et* $\eta_2 > 1$ *pour lesquelles pour tout entier* λ *réduit modulo* $(\varepsilon_1, \dots, \varepsilon_r)$ *on a les encadrements suivants* :

$$\eta_1 < |\sigma_1(\lambda)| < \eta_2 |N(\lambda)| \quad \textit{et} \quad \eta_1 < |\sigma_i(\lambda)| < \eta_2 \quad \textit{pour } i = 2, \dots, r.$$

On rappelle le résultat suivant (voir [L, théorème 2.4, p. 57, chap. II]) :

$$\exists C > 0, \quad \operatorname{card}(\mathcal{O}\langle M\rangle) = CM \log(M)^r + O(M \log(M)^{r-1}).$$

Comme dans la démonstration du théorème 1, on peut majorer convenablement le nombre de points $(x_1, \dots, x_l) \in \mathcal{O}^l\langle M\rangle$ qui rendent identiquement nul le polynôme $Q(x_1, \dots, x_l, Y)$. Ainsi, grâce à l'assertion précédente,

$$\operatorname{card}\{(x_1, \dots, x_l) \in \mathcal{O}^l\langle M\rangle : Q(x_1, \dots, x_l, Y) = 0\} \le \gamma_0 (M \log(M)^r + 1)^{l-1},$$

où $\gamma_0 > 0$ est une constante dépendant de Q et de K.

On fixe désormais $(x_1, \dots, x_l) \in \mathcal{O}^l\langle M\rangle$ pour lequel

$$Q(x_1, \dots, x_l, Y) \neq 0.$$

On suit la démonstration du théorème 1. On majore donc le cardinal de l'ensemble $E_0^{(x_1,\dots,x_l)}\langle M\rangle$, où

$$E_0^{(x_1,\dots,x_l)} = \{y \in \mathcal{O} : Q(x_1, \dots, x_l, y) \,|\, R(x_1, \dots, x_l)\}.$$

On pose dans la suite de la démonstration

$$a = R(x_1, \dots, x_l).$$

On note encore

$$D(a) = \{d_1, \dots, d_J\} \quad (J = J(x_1, \dots, x_l)),$$

la famille des diviseurs de a non-associés deux à deux, et qui sont réduits modulo la base $(\varepsilon_1, \dots, \varepsilon_r)$.

On rappelle les propriétés élémentaires suivantes. Soient α et β des éléments du corps de nombres K. En notant $n = [K : \mathbb{Q}]$, la définition de la hauteur logarithmique de Weil et les propriétés (3.3) du chapitre 3 de [W] ont pour conséquences les inégalités suivantes :

$$\begin{aligned} |N(\alpha)| &\le H_K(\alpha)^n, \\ H_K(\alpha + \beta) &\le 2^n H_K(\alpha) H_K(\beta), \\ H_K(\alpha\beta) &\le H_K(\alpha) H_K(\beta), \\ H_K(\alpha/\beta) &\le H_K(\alpha) H_K(\beta). \end{aligned}$$

Par conséquent, on peut trouver des constantes $\gamma_1 > 0$ et $\gamma_2 > 0$, ne dépendant que de n, Q et R, pour lesquelles on a l'implication suivante :

$$\left.\begin{array}{r}\max\limits_{i=1,\dots,l}\{H_K(x_i)\} \le M \\ H_K(y) \le M\end{array}\right\} \Rightarrow \left\{\begin{array}{l}H_K(Q(x_1,\dots,x_l,y)) \le \gamma_1(M^{\gamma_2}+1),\\ H_K(R(x_1,\dots,x_l)) \le \gamma_1(M^{\gamma_2}+1).\end{array}\right.$$

Soit $y \in E_0^{(x_1,\dots,x_l)}$; alors $Q(x_1,\dots,x_l,y)$ divise $a = R(x_1,\dots,x_l)$. Par conséquent, il existe un unique $\delta \in D(a)$ et un unique $\varepsilon \in \mathcal{U}$ pour lesquels

$$Q(x_1,\dots,x_l,y) = \delta\varepsilon.$$

On rappelle encore, pour tout élément α de $\mathcal{O}$, les encadrements suivants :

$$\max_{i=1,\dots,s+t}\{|\sigma_i(\alpha)|\} \le H_K(\alpha) \le (\max_{i=1,\dots,s+t}\{|\sigma_i(\alpha)|\})^n.$$

Puisque δ divise a, et puisqu'il est réduit modulo $(\varepsilon_1,\dots,\varepsilon_r)$, en vertu du lemme 12, on a les majorations successives suivantes :

$$\begin{aligned}H_K(\delta) &\le (\max_{i=1,\dots,s+t}\{|\sigma_i(\delta)|\})^n \le (\eta_2|N(\delta)|)^n\\ &\le (\eta_2|N(a)|)^n \le \eta_2^n H_K(a)^{n^2}\\ &\le \gamma_1^{n^2}\eta_2^n(M^{\gamma_2}+1)^{n^2}.\end{aligned}$$

D'autre part, en appliquant le lemme 11, on obtient les minorations

$$H_K(\varepsilon) \ge \max_{i=1,\dots,s+t}\{|\sigma_i(\varepsilon)|\} \ge e^{\xi\varrho(\varepsilon)}.$$

Finalement,

$$e^{\xi\varrho(\varepsilon)} \le H_K(\varepsilon) \le H_K(Q(x_1,\dots,x_l,y))H_K(\delta).$$

Donc, il existe des constantes $\gamma_3 > 0$ et $\gamma_4 > 0$, ne dépendant que de n, P, Q et du système $(\varepsilon_1,\dots,\varepsilon_r)$, pour lesquelles

$$e^{\xi\varrho(\varepsilon)} \le \gamma_3(M^{\gamma_4}+1).$$

On peut ainsi trouver une constante $\gamma_5 > 0$ vérifiant

$$\varrho(\varepsilon) \le \gamma_5(\log(M)+1).$$

Cette majoration permet d'évaluer le nombre maximal de ε possibles, et donc de majorer le cardinal de $E_0^{(x_1,\dots,x_l)}\langle M\rangle$. Comme dans la conclusion de la démonstration du théorème 3, on a

$$\begin{aligned}\operatorname{card}(E_0^{(x_1,\dots,x_l)}\langle M\rangle) &\le c(K)\deg_Y(Q)(2\gamma_5(\log(M)+1)+1)^r \operatorname{card}(D(a))\\ &\le \gamma_6(\log(M)^r \operatorname{card}(D(a))+1),\end{aligned}$$

où γ_6 est une constante positive. Il reste donc, pour conclure, à majorer convenablement le cardinal de l'ensemble $D(a)$. On utilise à cet effet les résultats de la partie 2, et plus précisément le corollaire 10. On connaît les majorations

$$|N(a)| \le H_K(a)^n \le \gamma_1^n(M^{\gamma_2}+1)^n.$$

Ainsi, il existe $\gamma_7 > 0$ et $\gamma_8 > 0$ vérifiant

$$\operatorname{card}(D(a)) \leq \gamma_7 M^{\gamma_8/\log\log(M)}.$$

Finalement, grâce à la majoration de $\operatorname{card}(\mathcal{O}\langle M\rangle)$ citée précédemment, on conclut comme dans la partie 3 :

$$\operatorname{card}(F_0^{(x_1,\ldots,x_l)}\langle M\rangle) \leq \gamma_9 M^{l+\gamma_8/\log\log(M)},$$

ce qui achève la démonstration du théorème 5. ∎

6. Annexe. On traite dans cette annexe le cas particulier des fractions rationnelles à deux variables et on suppose que K est le corps des rationnels. Comme précédemment, il suffit de traiter le cas des fractions rationnelles s'écrivant sous la forme

$$f(X,Y) = \frac{R(X)}{Q(X,Y)},$$

où R et Q sont des polynômes à coefficients dans $\mathbb{Z}$. On reprend globalement la démonstration du théorème 1, mais au lieu de majorer brutalement $\delta(R(x))$, on utilise une majoration de la moyenne des $\delta(R(x))$ dûe à J. G. van der Corput. Il démontre en effet le résultat suivant (voir [VDC, proposition 3]). Il existe un nombre $\Omega > 0$, dépendant de R, tel que pour tout entier $M \geq 3$ on ait

$$\sum_{\substack{x=1,\ldots,M\\ R(x)\neq 0}} \delta(R(x)) \leq M\log(M)^{\Omega}.$$

Quitte à considérer le polynôme $R(-X)$ on a aussi la majoration

$$\sum_{\substack{|x|\leq M\\ R(x)\neq 0}} \delta(R(x)) \leq 2M\log(M)^{\Omega} + \delta(R(0)).$$

On a tout d'abord la majoration

$$\operatorname{card}\{(x,y)\in\mathbb{Z}^2(M) : R(x)=0 \text{ ou } Q(x,Y)=0\} \leq (2M+1)(\deg R + \deg Q).$$

On considère désormais les $x \in \mathbb{Z}(M)$ pour lesquels $R(x)$ est non nul et $Q(x,Y)$ n'est pas le polynôme nul. D'une part, pour un tel x on a

$$\operatorname{card}\{y\in\mathbb{Z}(M) : Q(x,y)=0\} \leq \deg_Y Q.$$

D'autre part, on a aussi

$$\operatorname{card}\{y\in\mathbb{Z}(M) : Q(x,y) \mid R(x)\} \leq (\deg_Y Q)\delta(R(x)).$$

Finalement,

$$\begin{aligned}\operatorname{card}\{(x,y)\in\mathbb{Z}^2(M) : Q(x,y)=0 \text{ ou } Q(x,y)\mid R(x)\}\\ \le C_1M+\deg_Y(Q)\sum_{\substack{|x|\le M\\ R(x)\neq 0}}\delta(R(x))\le C_2(M\log(M)^{\Omega}+1),\end{aligned}$$

où $C_2>0$ est une constante dépendant des polynômes R et Q, et $\Omega>0$ un nombre dépendant de R. Ainsi, on a démontré le théorème suivant.

THÉORÈME 13. *Soit $f\in\overline{\mathbb{Q}}(X,Y)$ une fraction rationnelle. Alors, il existe des constantes $C_0>0, \Omega>0$ et $M_0>0$, dépendant de f, pour lesquelles pour tout sous-ensemble E de $\mathbb{Z}^2$ vérifiant*

$$\exists M>M_0,\quad \operatorname{card}(E(M))>C_0M\log(M)^{\Omega},$$

on a l'implication suivante :

$$\forall z\in E,\ f(z)\in\overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z \ \Rightarrow\ f\in\overline{\mathbb{Q}}[X,Y].$$

L'exemple qui suit montre qu'on ne peut pas espérer supprimer le terme $\log(M)$. On considère la fraction

$$f(X,Y)=\frac{X}{Y}\in\mathbb{Q}[X,Y]$$

et l'ensemble $E=\{(ax,x) : (a,x)\in\mathbb{Z}^2\}$. C'est un exercice facile que de calculer le cardinal de $E(M)$. En particulier, on en a l'équivalent suivant :

$$\operatorname{card}(E(M))\simeq 2M\log(M).$$

La fraction f prend des valeurs entières en chaque point de l'ensemble E et n'est pas un polynôme, ce qui montre bien la nécessité d'un terme $\log(M)$. On peut alors raisonnablement conjecturer l'énoncé suivant.

CONJECTURE 14. *Soit $f\in\overline{\mathbb{Q}}(X_1,\dots,X_k)$ une fraction rationnelle. Alors, il existe des constantes $C_0>0$, $\Omega>0$ et $M_0>0$, dépendant de f, pour lesquelles pour tout sous-ensemble E de $\mathbb{Z}^k$ vérifiant*

$$\exists M>M_0,\quad \operatorname{card}(E(M))>C_0M^{k-1}\log(M)^{\Omega},$$

on a l'implication suivante :

$$\forall z\in E,\ f(z)\in\overline{\mathbb{Z}} \text{ ou } f \text{ n'est pas définie en } z \ \Rightarrow\ f\in\overline{\mathbb{Q}}[X_1,\dots,X_k].$$

Références

[BS] Z. I. Borevitch et I. R. Shafarevitch, *Théorie des nombres*, Gauthier-Villars, 1967.
[L] S. Lang, *Number Theory III*, Encyclopaedia Math. Sci. 60, Springer, 1991.
[M] J. C. Masseron, *Propriétés arithmétiques de fractions rationnelles à coefficients algébriques*, Michigan Math. J. 47 (2000), 57–78.

[PW] P. Philippon and M. Waldschmidt, *Lower bounds for linear forms in logarithms*, dans : New Advances in Transcendence Theory, Cambridge Univ. Press, 1988, 280–312.

[S] P. Samuel, *Théorie algébrique des nombres*, 2ème éd., Hermann, 1971.

[T] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Cours Spécialisés 1, Soc. Math. de France, Paris, 1995.

[VDC] J. G. van der Corput, *Une inégalité relative au nombre de diviseurs*, Nederl. Akad. Wetensch. Proc. 42 (1939), 547–553.

[W] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Grundlehren Math. Wiss. 326, Springer, 2000.

[Y] M. Yasumoto, *Arithmetically independent integers and values of rational functions*, Manuscripta Math. 85 (1994), 1–10.

U.F.R. de mathématiques pures et appliquées
Université des Sciences et Technologies de Lille
59655 Villeneuve d'Ascq Cedex, France
E-mail: Laurent.Denis@math.univ-lille1.fr
Sophie.Dion@math.univ-lille1.fr

Reçu le 2.6.2004
et révisé le 14.10.2004 (4779)