Journal of Number Theory

MINORATION EFFECTIVE DE LA DISTANCE P-ADIQUE ENTRE PUISSANCES DE NOMBRES ALGÉBRIQUES.

par Y. Bugeaud (*) **et M. Laurent** (**) .

Abstract — We use the new tool of interpolation determinants to get precise lower bounds for the p-adic distance between two integral powers of algebraic numbers. This work is the p-adic analogue of the two papers [4] and [5] on which it is based, although several new specific p-adic ideas are introduced here.

1. Introduction.

On se propose d'adapter au cadre p-adique les résultats de [4] et de [5]. Rappelons qu'il s'agissait alors de minorer la valeur absolue usuelle d'une combinaison linéaire à coefficients entiers de deux logarithmes de nombres algébriques. A cet effet, on réexaminait la construction de Schneider dans le contexte des déterminants d'interpolation. Une première traduction p-adique de cette étude a été entreprise par Y. Bugeaud, *cf.* [2]. Nous introduisons dans cet article de nouveaux ingrédients plus spécifiquement p-adiques et améliorons ainsi les minorations obtenues dans [2]. Par exemple, pour ce qui concerne la dépendance en p des résultats, nous substituons le terme $p^f - 1$ à son carré ; voir le Corollaire 1 ci-dessous pour un énoncé précis. D'autre part, nous divisons essentiellement les constantes numériques par un facteur 20. De plus, grâce à l'introduction d'un paramètre g, nous pouvons regrouper dans un même énoncé les résultats du cas général avec ceux obtenus par Dong Ping Ping pour des unités principales, *cf.* [3].

La difficulté principale du cas p-adique réside dans le fait que les points considérés naturellement dans la construction ne sont plus nécessairement situés dans le domaine de convergence p-adique de la série exponentielle. On est donc amené à se placer dans ce domaine par un artifice. Pour ce faire, l'argument le plus simple consiste à élever les deux nombres algébriques considérés α_1 et α_2 à des puissances "suffisantes". Nous utilisons ici une construction plus sophistiquée. Comme l'on considère des produits de puissances $\alpha_1^r \alpha_2^s$, il suffit d'imposer une seule relation de congruence à une certaine forme linéaire en r et s,

(*) Université Louis Pasteur, Strasbourg.

(**) Laboratoire de Mathématiques discrètes, CNRS, Marseille.

au lieu de deux congruences portant respectivement sur chacun des exposants r et s ; d'où provient le gain du carré. Il devient alors nécessaire de reprendre le lemme de zéros ainsi que les résultats combinatoires de [5]. On notera que la construction utilisée est l'exacte duale (au sens de M. Waldschmidt, *cf.* [7] ou le paragraphe XII.2 de [8]) de celle considérée par Yu Kun Rui. Il n'est donc pas étonnant de trouver la même dépendance en p que dans les travaux de Yu Kun Rui, *cf.* [9],[10],[11].

Nous introduirons également un autre ingrédient tout à fait spécifique aux déterminants d'interpolation. Pour majorer de tels déterminants, on peut soit utiliser le principe du maximum, soit étudier leurs développements en série de Taylor qui font intervenir des valeurs particulières de polynômes de Schur. Cette démarche vaut aussi bien dans le cadre archimédien que p-adique. Dans le cas archimédien, une évaluation précise semble assez délicate à obtenir, et il est plus simple d'utiliser le principe du maximum comme dans [4] et [5]. Comme les coefficients des polynômes de Schur sont des entiers rationnels, donc contenus dans la boule unité de $\mathbf{Z}_p$, les évaluations p-adiques sont par contre très simples à effectuer, de même que celles de discriminants (voir le Lemme 2 ci-dessous). Nous obtenons ainsi de bien meilleures majorations analytiques que celles déduites du principe du maximum. En fait, bien que le rayon de convergence de la série exponentielle p-adique soit égal à $p^{-1/(p-1)}$, on notera que lors de la majoration de déterminants d'interpolation de fonctions exponentielles-polynômes p-adiques, tout se passe au niveau des estimations comme si ce rayon de convergence se trouvait être égal à 1.

Les auteurs remercient Dong Ping Ping pour ses remarques et suggestions lors de la vérification de cet article.

2. Énoncé des résultats.

Soit p un nombre premier. On désignera par $\overline{\mathbf{Q}}_p$ une clôture algébrique du corps $\mathbf{Q}_p$ des nombres p-adiques. Le corps $\overline{\mathbf{Q}}_p$ est muni de la valeur absolue ultramétrique $|x|_p = p^{-v(x)}$, où v désigne l'unique prolongement à $\overline{\mathbf{Q}}_p$ de la valuation p-adique standard sur $\mathbf{Q}_p$ normalisée par $v(p) = 1$. Soient α_1, α_2 deux nombres algébriques sur $\mathbf{Q}$, vus comme éléments du corps $\overline{\mathbf{Q}}_p$. On se propose de minorer la valeur absolue de l'écart

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2},$$

où b_1 et b_2 désignent des entiers rationnels positifs. Comme dans le cas complexe, *cf.* [4] et [5], on notera par $h(\alpha)$ la hauteur logarithmique absolue d'un nombre algébrique α.

Nos résultats dépendent, entre autres choses, de certaines quantités attachées au corps $\mathbf{K}_v = \mathbf{Q}_p(\alpha_1, \alpha_2)$. On désignera notamment par e l'indice de ramification du groupe de valuation dans l'extension de $\mathbf{Q}_p$ à $\mathbf{K}_v$, par f le degré résiduel de cette extension, par U_v le groupe multiplicatif des unités de $\mathbf{K}_v^*$ (formé des $x \in \mathbf{K}_v$ avec $v(x) = 0$), par U_v^1 le sous-groupe des unités principales (celles pour lesquelles $v(x-1) > 0$), et enfin par t l'entier ≥ 0 déterminé par l'encadrement

$$p^{t-1} \leq \frac{e}{p-1} < p^t.$$

Posons

$$D = \frac{[\mathbf{Q}(\alpha_1, \alpha_2) : \mathbf{Q}]}{f}.$$

Nous supposerons dans toute la suite que α_1 et α_2 appartiennent à U_v. Soit g le plus petit entier positif tel que

$$\alpha_i^g \in U_v^1, \ (i = 1, 2).$$

Fixons dans $\overline{\mathbf{Q}}_p$ une racine de l'unité ζ d'ordre exactement g. Le Lemme 4 ci-dessous montre que ζ appartient en fait au sous-corps $\mathbf{K}_v$, que g divise $p^f - 1$, et que les nombres α_1 et α_2 se décomposent uniquement sous la forme

$$\alpha_i = \zeta^{m_i}\theta_i\,,\ \theta_i \in U_v^1\ ,(i = 1, 2),$$

avec des entiers m_1, m_2 déterminés modulo g. Notre résultat principal s'énonce ainsi.

Théorème 1. *Soient K un entier ≥ 3, L un entier ≥ 2, R_1, R_2, S_1, S_2 des entiers > 0. Notons*

$$R = R_1 + R_2 - 1, S = S_1 + S_2 - 1, N = KL,$$
$$\gamma_1 = \frac{R+g-1}{2R} - \frac{gN}{6R(S+g-1)}, \quad \gamma_2 = \frac{S+g-1}{2S} - \frac{gN}{6S(R+g-1)}.$$

Pour tout couple d'entiers positifs (b_1, b_2), désignons par p^u la plus grande puissance de p divisant simultanément b_1 et b_2. On notera

$$b = \frac{(R-1)b_2 + (S-1)b_1}{2} \left(\prod_{k=1}^{K-1} k! \right)^{-2/(K^2-K)}.$$

Supposons qu'il existe deux classes c_1 et c_2 d'entiers modulo g, telles que :

$$(1)\quad \begin{aligned} &\mathrm{Card}\left\{\alpha_1^{p^t r}\,\alpha_2^{p^t s};\, 0 \leq r < R_1,\, 0 \leq s < S_1,\, m_1 r + m_2 s \;\equiv\; c_1 \,\mathrm{modulo}\, g\right\} \geq L,\\ &\mathrm{Card}\left\{r b_2 + s b_1;\, 0 \leq r < R_2,\, 0 \leq s < S_2,\, m_1 r + m_2 s \;\equiv\; c_2 \,\mathrm{modulo}\, g\right\} > (K-1)L. \end{aligned}$$

On supposera aussi que

$$(2)\quad \begin{aligned} &K(L-1)p^t \log p - (D+2e)\log N - D(K-1)\log b\\ &\qquad\qquad - \gamma_1 p^t DLRh(\alpha_1) - \gamma_2 p^t DLSh(\alpha_2) \;>\; 0. \end{aligned}$$

Alors

$$|\Lambda|_p \geq p^{-\frac{p^t}{e}(KL - \frac{1}{2}) - u} \geq p^{-\frac{p}{p-1}(KL - \frac{1}{2}) - u}.$$

Voici quelques corollaires simples du Théorème 1. Soient $A_1 > 1, A_2 > 1$ deux nombres réels, tels que

$$\log A_i \geq \max \left\{ h(\alpha_i), \frac{\log p}{D} \right\}, \ (i = 1, 2).$$

Comme dans le cas archimédien, notons alors

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

Commençons par un résultat asymptotique (c'est à dire valable lorsque b_1 ou b_2 est suffisamment grand) qui, bien que sans utilité pratique, nous indique le meilleur résultat numérique qui puisse être déduit du Théorème 1.

Théorème 2. *Supposons que α_1, α_2 soient multiplicativement indépendants. Pour tout réel $c > \frac{64}{9}$, il existe alors un réel effectivement calculable $b(c, p)$, tel que*

$$v(\Lambda) \leq \frac{cpg}{(p-1)(\log p)^4} D^4 \left(\log b' \right)^2 \log A_1 \log A_2,$$

dès que $b' \geq b(c, p)$.

La fonction $b(c, p)$ est bien sûr effectivement calculable comme dans le cas archimédien. Voici quelques exemples de résultats totalement explicites.

Théorème 3. *Supposons que α_1, α_2 soient multiplicativement indépendants. On a la majoration*

$$v(\Lambda) \leq \frac{24pg}{(p-1)(\log p)^4} D^4 \left(\max \left\{ \log b' + \log \log p + 0.4, \frac{10 \log p}{D}, 10 \right\} \right)^2 \log A_1 \log A_2.$$

Majorant $g \leq p^f - 1$, il vient immédiatement le

Corollaire 1. *Avec les hypothèses et notations du Théorème 3, on a*

$$v(\Lambda) \leq \frac{24p(p^f-1)}{(p-1)(\log p)^4} D^4 \left(\max \left\{ \log b' + \log \log p + 0.4, \frac{10 \log p}{D}, 10 \right\} \right)^2 \log A_1 \log A_2.$$

Considérons maintenant dans le cas particulier où $g = 1$, spécialement étudié par Dong Ping Ping, *cf.* [3]. On obtient immédiatement le

Corollaire 2. *Avec les hypothèses et notations du Théorème 3, supposons de plus que α_1 et α_2 appartiennent à U_v^1. Alors*

$$v(\Lambda) \le \frac{24p}{(p-1)(\log p)^4} D^4 \left(\max\left\{\log b' + \log\log p + 0.4, \frac{10\log p}{D}, 10\right\}\right)^2 \log A_1 \log A_2$$
$$\le 208 D^4 \left(\max\left\{\log b' + \log\log p + 0.4, \frac{10\log p}{D}, 10\right\}\right)^2 \log A_1 \log A_2.$$

Le nombre 10 apparait deux fois dans les formules ci-dessus comme coefficient des termes $\log p/D$ et 1 respectivement. Si nous désignons plus généralement ces deux coefficients par μ et ν, il est possible de choisir arbitrairement leurs deux valeurs, en remplaçant le facteur numérique 24 par une fonction $c(\mu,\nu)$ adéquate. Le Théorème 4 ci-dessous fournit une table de valeurs de cette fonction c. Le lecteur intéressé par d'autres valeurs des paramètres μ et ν, trouvera dans le paragraphe 5.4 une description de la méthode de calcul employée.

Théorème 4. *Pour tout couple (μ,ν) appartenant au produit $\{4,6,8,10,15\}\times\{5,10\}$, définissons $c(\mu,\nu)$ par le tableau*

	$\mu=4$	$\mu=6$	$\mu=8$	$\mu=10$	$\mu=15$
$\nu=5$	53.8	36.1	28.1	24	18.6
$\nu=10$	51.7	34.8	27.3	23.2	18

Supposons que α_1,α_2 soient multiplicativement indépendants. On a alors la majoration

$$v(\Lambda) \le c(\mu,\nu)\frac{pg}{(p-1)(\log p)^4} D^4 \left(\max\left\{\log b' + \log\log p + 0.4, \frac{\mu\log p}{D}, \nu\right\}\right)^2 \log A_1 \log A_2$$

pour tout $(\mu,\nu)\in\{4,6,8,10,15\}\times\{5,10\}$.

Remarque. Dans certaines applications, on ne dispose pas de la valeur exacte de D ; toutefois les résultats ci-dessus subsistent généralement en remplaçant D par un majorant.

3. Préliminaires d'analyse p-adique.

Les lemmes techniques contenus dans ce paragraphe nous serviront à majorer finement la valeur absolue p-adique de déterminants d'interpolation de fonctions exponentielles-polynômes.

Lemme 1. *Pour tout entier n positif, on a l'estimation*

$$\frac{n}{p-1} - \frac{\log(1+n)}{\log p} \le v(n!) \le \frac{n}{p-1}.$$

Preuve — On sait (*cf.* [1] Lemme 3.5.6) que si

$$n = c_0 + \cdots + c_k p^k, 0 \leq c_j \leq p-1, 0 \leq j \leq k,$$

désigne l'écriture de l'entier n dans la base p, on a l'égalité

$$v(n!) = \frac{n - c_0 - \cdots - c_k}{p-1}.$$

Il s'agit donc de montrer que

$$c_0 + \cdots + c_k \leq \frac{p-1}{\log p} \log\left(1 + c_0 + \cdots + c_k p^k\right).$$

Si l'on fixe $c_0 + \ldots + c_k$, on constate immédiatement que le minimum de $c_0 + \cdots + c_k p^k$ est atteint pour un $(k+1)$-uplet d'entiers (c_j) de la forme

$$(c_0, \ldots, c_k) = (p-1, \ldots, p-1, c, 0, \ldots, 0).$$

Il suffit donc de vérifier que pour tout $j \geq 0, 0 \leq c \leq p-1$, on a

$$j(p-1) + c \leq \frac{p-1}{\log p} \log\left(1 + p^j - 1 + cp^j\right) = \frac{p-1}{\log p} \log\left((c+1)p^j\right),$$

autrement dit que

$$\frac{c}{\log(1+c)} \leq \frac{p-1}{\log p},\ 0 \leq c \leq p-1;$$

cette dernière inégalité exprimant simplement la croissance de la fonction $x \mapsto \frac{x}{\log(1+x)}$ pour $x \geq 0$. $\square$

On déduit immédiatement du Lemme 1 le

Corollaire. *Pour tout entier positif n, on a la minoration*

$$v\left(\prod_{\nu=1}^{n-1} \nu!\right) \geq \frac{n^2 - n}{2(p-1)} - \frac{n \log n}{\log p}.$$

Lemme 2. *Soient $z_1, \ldots, z_n$ des éléments de $\mathbf{Z}_p$, on a la minoration*

$$v\left(\prod_{1 \leq i < j \leq n} (z_i - z_j)\right) \geq v\left(\prod_{\nu=1}^{n-1} \nu!\right).$$

Preuve — D'après la formule de Vandermonde

$$\prod_{1 \leq i < j \leq n} (z_j - z_i) = \det\left(z_i^{j-1}\right),$$

on a

$$\frac{\prod_{1\le i<j\le n}(z_j-z_i)}{\prod_{\nu=1}^{n-1}\nu!}=\det\left(\frac{z_i^{j-1}}{(j-1)!}\right)=\det\left(\binom{z_i}{j-1}\right),$$

par multilinéarité du déterminant. Or, pour tout élément $z\in\mathbf{Z}_p$, le coefficient binomial $\binom{z}{k}=\frac{z(z-1)\cdots(z-k+1)}{k!}$ appartient à $\mathbf{Z}_p$, puisqu'il en est ainsi sur le sous-ensemble dense des entiers rationnels. □

Lemme 3. *Soit θ un élément de $\overline{\mathbf{Q}}_p$ tel que $v(\theta-1)>0$. Alors*

$$v\left(\theta^p-1\right)=pv(\theta-1)\quad si\quad v(\theta-1)<\frac{1}{p-1},$$
$$v\left(\theta^p-1\right)=v(\theta-1)+1\quad si\quad v(\theta-1)>\frac{1}{p-1},$$
$$v\left(\theta^p-1\right)\ge\frac{p}{p-1}=\frac{1}{p-1}+1\quad si\quad v(\theta-1)=\frac{1}{p-1}.$$

Preuve — La formule du binôme écrite sous la forme

$$x^p-1=(x-1)^p+\sum_{j=1}^{p-1}\frac{p}{j}\binom{p-1}{j-1}(x-1)^j$$

montre que

$$v\left(\theta^p-1\right)\ge\min\left\{pv(\theta-1),1+v(\theta-1)\right\}.$$

Les deux termes du minimum deviennent égaux pour la valeur critique $v(\theta-1)=\frac{1}{p-1}$. La transformation $x\mapsto x^p$ multiplie donc par p la valuation $v(x-1)$ en deçà de cette valeur critique, et ajoute 1 au delà, d'où le résultat. □

La série exponentielle p-adique est convergente dans le disque ouvert centré à l'origine de rayon $p^{-1/(p-1)}$. Le corollaire suivant, dans lequel on utilise les notations du paragraphe 2, nous permettra de nous amener dans cette boule par élévation à la puissance p^t.

Corollaire. *Soit θ une unité principale dans $\mathbf{K}_v$. Alors*

$$v\left(\theta^{p^t}-1\right)\ge\frac{p^t}{e}>\frac{1}{p-1}.$$

Preuve — On rappelle que t désigne le plus grand entier h tel que $\frac{p^{h-1}}{e}\le\frac{1}{p-1}$. On montre par récurrence sur $h=0,\ldots,t$ que $v\left(\theta^{p^h}-1\right)\ge\frac{p^h}{e}$. L'assertion est triviale pour $h=0$ et le Lemme 3 permet de passer de h à $h+1$. □

Remarque. L'argument ci-dessus est dû à Yu Kun Rui. On notera qu'il doit utiliser des puissances p^h-ièmes avec $h = t+1$ ou $h = t$, selon que l'écart $\frac{p^t}{e} - \frac{1}{p-1}$, à priori compris entre 0 et 1, se trouve être proche de l'origine ou non. Grâce à une analyse p-adique plus précise, spécifique à la considération de déterminants d'interpolation, nous pourrons nous restreindre à l'exposant minimal $h = t$; c'est essentiellement de là que provient le gain d'un facteur $\left(2 + \dfrac{1}{p-1}\right)^4$ dans les constantes.

Nous devrons utiliser quelques propriétés classiques des corps cyclotomiques pour lesquelles le lecteur pourra consulter les ouvrages [1] et [6].

Lemme 4. *Le groupe quotient U_v/U_v^1 est cyclique de cardinal $p^f - 1$, canoniquement isomorphe au groupe multiplicatif des éléments non nuls du corps résiduel de $\mathbf{K}_v$. De plus, chaque classe contient une unique racine (p^f-1)-ième de l'unité.*

Preuve — Proposition 8 du chapitre 2 de [6].

Lemme 5. *Soit ξ une racine de l'unité dans $\overline{\mathbf{Q}}_p$ d'ordre exact p^u. L'extension de corps $\mathbf{Q}_p(\xi)/\mathbf{Q}_p$ est totalement ramifiée de degré $p^{u-1}(p-1)$. Pour tout entier naturel m de la forme $m = m'p^u$, avec m' premier à p, on a la formule*

$$\sum_{\substack{\zeta^m=1\\ \zeta\neq 1}} v(\zeta - 1) = u.$$

Preuve — Proposition 17 du chapitre 4 de [6].

Pour achever ces préliminaires, signalons aussi la version suivante du

Lemme de Krasner. *Soient ξ et σ deux éléments de $\overline{\mathbf{Q}}_p$. Soient $\xi_1 = \xi, \xi_2, \ldots, \xi_d$ les conjugués de ξ sur $\mathbf{Q}_p$. On suppose que*

$$v(\sigma - \xi) > v(\sigma - \xi_i), \quad (2 \le i \le d).$$

Alors ξ appartient au corps $\mathbf{Q}_p(\sigma)$.

Preuve — Voir le Théorème 2.7.1 de [1].

4. Un lemme de zéros.

Nous aurons également besoin de généraliser le lemme de zéros utilisé dans le cas complexe, *cf.* [5]. En fait, les arguments développés au cours de la démonstration de la proposition 1 de [5] contiennent implicitement l'énoncé suivant.

Lemme 6. *Soient a_1, a_2, b_1, b_2, des éléments d'un corps commutatif $\mathbf{K}$, avec $a_1 \neq 0, a_2 \neq 0$. Soient K et L des entiers positifs, et soient $\mathcal{E}_1, \mathcal{E}_2$ deux sous-ensembles finis de $\mathbf{Z}^2$. Soit enfin $P \in \mathbf{K}[X,Y]$ un polynôme non nul, de degré partiel $\le K-1$ en X et $\le L-1$ en Y. Supposons que*

$$\mathrm{Card}\left\{a_1^r\, a_2^s \,;\, (r,s) \in \mathcal{E}_1\right\} \ge L,$$

et que

$$\mathrm{Card}\left\{b_2r+b_1s\,;\ (r,s)\in\mathcal{E}_2\right\}>(K-1)\,L.$$

Alors, l'un au moins des nombres

$$P(b_2r+b_1s,a_1^r\,a_2^s),\quad (r,s)\in\mathcal{E}_1+\mathcal{E}_2,$$

est non nul.

Preuve— Supposons que tous les nombres $P(b_2r+b_1s,a_1^r\,a_2^s),(r,s)\in\mathcal{E}_1+\mathcal{E}_2$, sont nuls et éliminons la variable Y entre les polynômes translatés $P_{r,s}(X,Y):=P(X+b_2r+b_1s,a_1^ra_2^sY)$ lorsque (r,s) décrit $\mathcal{E}_1$. Pour cela, on écrit P comme un polynôme en Y à coefficients dans $\mathbf{K}[X]$:

$$P(X,Y)=\sum_{\ell\in\mathcal{L}}Q_\ell(X)Y^\ell\,,\ Q_\ell\neq 0\,,\ \ell\in\mathcal{L}.$$

Par hypothèse, chacun des polynômes

$$P_{r',s'}(X,Y)=\sum_{\ell\in\mathcal{L}}Q_\ell(X+b_2r'+b_1s')(a_1^{r'}a_2^{s'})^\ell Y^\ell,\ (r',s')\in\mathcal{E}_1,$$

s'annule au point $(b_2r''+b_1s'',a_1^{r''}a_2^{s''})$ lorsque $(r'',s'')\in\mathcal{E}_2$. Grâce au Lemme 1 de [5], fixons un sous-ensemble $\mathcal{E}_1'\subseteq\mathcal{E}_1$, de même cardinal que $\mathcal{L}$, tel que

$$\delta=\det\Big(\big(a_1^{r'}a_2^{s'}\big)^\ell\Big)_{\substack{\ell\in\mathcal{L}\\(r',s')\in\mathcal{E}_1'}}\neq 0,$$

et posons

$$\Delta(X)=\det\Big(Q_\ell(X+b_2r'+b_1s').\big(a_1^{r'}a_2^{s'}\big)^\ell\Big)_{\substack{\ell\in\mathcal{L}\\(r',s')\in\mathcal{E}_1'}}.$$

Fixons maintenant un point (u,v) de la forme $(b_2r''+b_1s'',a_1^{r''}a_2^{s''})$ avec $(r'',s'')\in\mathcal{E}_2$. Regardant les égalités $P_{r',s'}(u,v)=0\,,\ (r',s')\in\mathcal{E}_1'$, comme un système de $n=:\mathrm{Card}\,\mathcal{L}=\mathrm{Card}\,\mathcal{E}_1'$ équations linéaires en les n variables $v^\ell\,,\ (\ell\in\mathcal{L})$, il est clair que le déterminant $\Delta(u)$ de ce système linéaire s'annule. D'autre part, si $Q_\ell(X)=q_\ell X^{k_\ell}+\cdots$, alors $\Delta(X)=q_1\cdots q_n\delta X^{k_1+\cdots+k_n}+\cdots$ est un polynôme de degré $k_1+\cdots+k_n\leq n(K-1)\leq L(K-1)$. D'où la contradiction lorsque (r'',s'') décrit $\mathcal{E}_2$. $\square$

4. Preuve du Théorème 1.

Soient K,L,R_1,R_2,S_1,S_2 des paramètres entiers satisfaisant les conditions (1) et (2) du théorème. On raisonne par l'absurde et on suppose donc que

$$|\Lambda|_p<p^{-\frac{p^t}{e}\left(N-\frac{1}{2}\right)-u}. \tag{3}$$

Rappelons que α_1 et α_2 se décomposent uniquement sous la forme

$$\alpha_i = \zeta^{m_i}\theta_i \ , (i = 1, 2),$$

avec des entiers m_1, m_2 déterminés modulo g. On notera que, par définition de g, les nombres m_1, m_2, g sont premiers entre eux.

Les étapes de la démonstration sont alors parallèles à celles du cas complexe, *cf.* [4] et [5].

4.1. Construction d'une matrice $\mathcal{M}$.

Nous allons extraire une matrice $\mathcal{M}$ de la matrice $\mathbf{M}$ de format $N \times RS$ dont les coefficients sont les nombres

$$\binom{rb_2 + sb_1}{k} {\alpha_1}^{p^t \ell r} {\alpha_2}^{p^t \ell s},$$

où (k, ℓ) $(0 \le k < K, 0 \le \ell < L)$ désigne l'indice de ligne et (r, s) $(0 \le r < R, 0 \le s < S)$ désigne celui de colonnes. La numérotation choisie des lignes et des colonnes est ici sans importance.

Lemme 7. *Fixons des entiers c_1 et c_2 vérifiant la condition* (1) *du Théorème* 1 *et notons $c = c_1 + c_2$. Alors la matrice extraite $\mathcal{M}$, formée des colonnes de* $\mathbf{M}$ *d'indice (r, s) vérifiant $m_1 r + m_2 s \equiv c$ modulo g, est de rang maximal, égal au nombre N de ses lignes.*

Preuve— L'hypothèse (1) signifient que les sous-ensembles de $\mathbf{Z}^2$

$$\mathcal{E}_1 = \{(r, s); 0 \le r < R_1, 0 \le s < S_1, m_1 r + m_2 s \equiv c_1 \bmod g\}$$
$$\mathcal{E}_2 = \{(r, s); 0 \le r < R_2, 0 \le s < S_2, m_1 r + m_2 s \equiv c_2 \bmod g\}$$

vérifient les deux conditions

$$\mathrm{Card}\left\{\alpha_1^{p^t r}\alpha_2^{p^t s}; (r, s) \in \mathcal{E}_1\right\} \ge L$$
$$\mathrm{Card}\,\{b_2 r + b_1 s; (r, s) \in \mathcal{E}_2\} > (K - 1)L$$

requises par le Lemme 6. Remarquons que

$$\mathcal{E}_1 + \mathcal{E}_2 \subseteq \{(r, s); 0 \le r < R, 0 \le s < S, m_1 r + m_2 s \equiv c \bmod g\}.$$

Une relation linéaire non triviale entre les lignes de la matrice $\mathcal{M}$ se traduit alors par l'existence d'un polynôme $P(X, Y)$, non nul, de degrés partiels en X et Y respectivement majorés par $K - 1$ et $L - 1$, et s'annulant aux points

$$\left(b_2 r + b_1 s, \alpha_1^{p^t r}\alpha_2^{p^t s}\right), \ (r, s) \in \mathcal{E}_1 + \mathcal{E}_2,$$

contrairement à la conclusion du Lemme 6. □

4.2. Majoration analytique des mineurs de $\mathcal{M}$.

Soit Δ un mineur d'ordre $N \times N$ extrait de la matrice $\mathcal{M}$. Nous nous proposons d'établir la majoration suivante de $|\Delta|_p$, lorsque $|\Lambda|_p$ est petit.

Lemme 8. *Supposons que*

$$v(\Lambda) \geq \frac{p^t}{e}\left(N - \frac{1}{2}\right) + u$$

alors

$$v(\Delta) \geq \frac{p^t NK(L-1)}{2e} - \frac{N \log N}{\log p}.$$

Preuve— Après avoir numéroté les lignes et les colonnes de la matrice extraite, écrivons

$$\Delta = \det\left(\binom{r_j b_2 + s_j b_1}{k_i} {\alpha_1}^{p^t \ell_i r_j} {\alpha_2}^{p^t \ell_i s_j},\right)_{1 \leq i,j \leq N}.$$

Comme

$$m_1 r_j + m_2 s_j \equiv c \bmod g, \ (j = 1, \ldots, N),$$

en substituant $\alpha_1 = \zeta^{m_1}\theta_1, \alpha_2 = \zeta^{m_2}\theta_2$, il vient la formule

$$\Delta = \zeta^{cp^t(\sum \ell_i)} \Delta',$$

avec

$$\Delta' = \det\left(\binom{r_j b_2 + s_j b_1}{k_i} {\theta_1}^{p^t \ell_i r_j} {\theta_2}^{p^t \ell_i s_j}\right)_{1 \leq i,j \leq N}.$$

Il s'ensuit en particulier que $v(\Delta) = v(\Delta')$. D'autre part, d'après (3), puisque

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2} = \zeta^{m_1 b_1}\theta_1^{b_1} - \zeta^{m_2 b_2}\theta_2^{b_2}$$

est de valuation positive, $m_1 b_1$ et $m_2 b_2$ sont nécessairement dans la même classe modulo g. Si l'on pose

$$\tilde{\Lambda} = \theta_1^{b_1} - \theta_2^{b_2}$$

il est alors clair que $v(\Lambda) = v(\tilde{\Lambda})$. En d'autres termes, il suffit de démontrer le lemme lorsque $\alpha_1 = \theta_1$ et $\alpha_2 = \theta_2$ sont des unités principales.

Rappelons que u désigne l'entier tel que p^u divise exactement $\operatorname{pgcd}(b_1, b_2)$. Une difficulté supplémentaire apparaît si $u > 0$; posons alors

$$b_1' = \frac{b_1}{p^u}, \ b_2' = \frac{b_2}{p^u}, \ \sigma = \frac{\theta_1^{b_1'}}{\theta_2^{b_2'}}$$

et montrons l'existence d'une racine p^t-ième de l'unité ξ_1 dans $\mathbf{K}_v$, telle que

$$v(\theta_1^{b_1'} - \xi_1\theta_2^{b_2'}) \geq \frac{p^t}{e}\left(N - \frac{1}{2}\right).$$

A cet effet, remarquons que

$$v\left(\sigma^{p^u}-1\right)=v\left(\frac{\tilde{\Lambda}}{\theta_2^{b_2}}\right)=v(\Lambda)\geq\frac{p^t}{e}\left(N-\frac{1}{2}\right)+u>\frac{1}{p-1}+u,$$

par hypothèse ; autrement dit

$$\sum_{\xi}v(\sigma-\xi)=v(\Lambda)\geq\frac{p^t}{e}\left(N-\frac{1}{2}\right)+u>\frac{1}{p-1}+u,$$

où l'indice de sommation ξ décrit l'ensemble des racines p^u-ièmes de l'unité dans $\overline{\mathbf{Q}}_p$. On utilise alors un argument standard pour montrer que σ est proche d'une, et d'une seule, de ces racines de l'unité. De façon précise, classons les racines p^u-ièmes de l'unité de telle sorte que

$$v(\sigma-\xi_1)\geq\cdots\geq v(\sigma-\xi_{p^u}).$$

Par l'inégalité ultramétrique, on a

$$v\left(\frac{\xi_\nu}{\xi_1}-1\right)=v\left(\xi_\nu-\xi_1\right)\geq v\left(\sigma-\xi_\nu\right),\quad(\nu=2,\ldots,p^u).$$

Il vient donc

$$v(\sigma-\xi_1)+\sum_{\substack{\xi^{p^u}=1\\ \xi\neq1}}v(\xi-1)\geq\frac{p^t}{e}\left(N-\frac{1}{2}\right)+u>\frac{1}{p-1}+u.$$

D'après le Lemme 5, la somme ci-dessus est égale à u. Il s'ensuit tout d'abord que $v(\sigma-\xi_1)>\frac{1}{p-1}$, puis que $v(\sigma-\xi_1)>v(\sigma-\xi_2)$. En effet, en cas d'égalité $v(\sigma-\xi_1)=v(\sigma-\xi_2)$, et toujours grâce à l'inégalité ultramétrique, on aurait

$$\frac{1}{p^{w-1}(p-1)}=v\left(\frac{\xi_2}{\xi_1}-1\right)=v(\xi_2-\xi_1)>\frac{1}{p-1},$$

où p^w désigne l'ordre exact de la racine de l'unité $\frac{\xi_2}{\xi_1}\neq1$; d'où la contradiction. Le Lemme de Krasner montre alors que ξ_1 appartient au corps $\mathbf{Q}_p(\sigma)\subseteq\mathbf{K}_v$. Il s'ensuit que $\xi_1^{p^t}=1$. En effet, désignant maintenant par p^w l'ordre de la racine de l'unité ξ_1, on a

$$p^{w-1}(p-1)\leq e<p^t(p-1),$$

puisque l'indice de ramification de l'extension $\mathbf{Q}_p(\xi_1)/\mathbf{Q}_p$ est égal à $p^{w-1}(p-1)$. Il vient ainsi $w\leq t$. Posons

$$\Lambda'=\theta_1^{b_1'}-\xi_1\theta_2^{b_2'}.$$

Comme $\xi_1^{p^u} = 1$, le Lemme 3 montre alors que

$$v(\Lambda) = v(\tilde{\Lambda}) = v\left(\sigma^{p^u} - 1\right) = v\left(\left(\frac{\sigma}{\xi_1}\right)^{p^u} - 1\right) = v(\sigma - \xi_1) + u = v(\Lambda') + u.$$

De manière alternative, on notera que l'égalité $v(\Lambda) = v(\Lambda') + u$ résulte aussi directement des inégalités ultramétriques ci-dessus. Grâce à (3), on a donc bien la minoration annoncée:

$$v(\Lambda') = v(\Lambda) - u \geq \frac{p^t}{e}\left(N - \frac{1}{2}\right).$$

On peut supposer sans restriction que p ne divise pas b'_2. Notons alors $\beta = \frac{b_1}{b_2} = \frac{b'_1}{b'_2}$. A partir de la relation

$$\theta_2^{b'_2} = \frac{\theta_1^{b'_1} - \Lambda'}{\xi_1} = \frac{\theta_1^{b'_1}(1 - \theta_1^{-b'_1}\Lambda')}{\xi_1},$$

en remarquant que $\xi_1^{p^t} = 1$, on obtient la formule

$$\theta_2^{b'_2 p^t \ell_i s_j} = \theta_1^{b'_1 p^t \ell_i s_j}\left(1 - \theta_1^{-b'_1}\Lambda'\right)^{p^t \ell_i s_j}, \quad (1 \leq i, j \leq N).$$

Notons que, pour tout $b \in \mathbf{Z}_p$, l'application $a \mapsto a^b := \exp_p(b \log_p a)$ réalise un homomorphisme de groupe injectif du disque $\left\{a \in \overline{\mathbf{Q}}_p; v(a-1) > \frac{1}{p-1}\right\}$ dans lui-même. D'après le corollaire du Lemme 3, on a

$$v\left(\theta_i^{p^t} - 1\right) \geq \frac{p^t}{e} > \frac{1}{p-1}, \quad (i = 1, 2),$$

et d'autre part,

$$v(\Lambda') \geq \frac{p^t}{e}(N - \frac{1}{2}) > \frac{1}{p-1},$$

comme on vient de le voir. Elevant alors les deux membres de l'égalité ci-dessus à la puissance $1/b'_2$, il vient

$$\begin{aligned} \theta_2^{p^t \ell_i s_j} =& (\theta_1^{p^t})^{\beta \ell_i s_j}\left(1 - \theta_1^{-b'_1}\Lambda'\right)^{p^t \ell_i s_j / b'_2} \\ =& (\theta_1^{p^t})^{\beta \ell_i s_j}(1 + \sigma_{i,j}\Lambda'), \quad (1 \leq i, j \leq N), \end{aligned}$$

avec $\sigma_{i,j} \in \overline{\mathbf{Q}}_p$. De plus, comme $\ell_i s_j / b'_2 \in \mathbf{Z}_p$, on déduit du Lemme 3 que $|\sigma_{i,j}|_p \leq p^{-t} \leq 1$.

Substituons maintenant les expressions ci-dessus dans le déterminant Δ'. Par multilinéarité du déterminant, il vient

$$\begin{aligned} \Delta' &= \det\left(\frac{(r_j b_2 + s_j b_1)^{k_i}}{k_i!}\theta_1^{p^t \ell_i (r_j + s_j \beta)}(1 + \sigma_{i,j}\Lambda')\right)_{1 \leq i,j \leq N} \\ &= b_2^{\sum k_i} \times \det\left(\frac{(r_j + s_j \beta)^{k_i}}{k_i!}\theta_1^{p^t \ell_i (r_j + s_j \beta)}(1 + \sigma_{i,j}\Lambda')\right)_{1 \leq i,j \leq N} \qquad (4) \\ &= b_2^{\sum k_i} \times \sum_{I \subseteq \{1, \ldots, N\}} (\Lambda')^{N - |I|}\Delta'_I \end{aligned}$$

où, pour tout sous-ensemble de lignes I, on a noté

$$\Delta'_I = \det \begin{pmatrix} \varphi_i(z_1) & ,\dots, & \varphi_i(z_N) \\ \\ \sigma_{i,1}\varphi_i(z_1) & ,\dots, & \sigma_{i,N}\varphi_i(z_N) \end{pmatrix} \begin{matrix} \} & i \in I \\ \\ \} & i \notin I \end{matrix} \tag{5}$$

avec

$$\varphi_i(z) = \frac{z^{k_i}}{k_i!}\theta_1^{p^t \ell_i z}, z_j = r_j + \beta s_j, \quad (1 \le i, j \le N).$$

Développons ensuite le déterminant Δ'_I grâce à la formule de Laplace:

$$\Delta'_I = \sum_{\substack{J \subseteq \{1,\dots,N\} \\ \mathrm{Card}(J) = \mathrm{Card}(I)}} \epsilon_J \Delta'_{I,J} \Delta'_{\overline{I},\overline{J}} \tag{6}$$

où $\epsilon_J = \pm 1$, et

$$\Delta'_{I,J} = \det \Big(\varphi_i(z_j)\Big)_{\substack{i \in I \\ j \in J}} \quad , \quad \Delta'_{\overline{I},\overline{J}} = \det \Big(\sigma_{i,j}\varphi_i(z_j)\Big)_{\substack{i \notin I \\ j \notin J}}.$$

Puisque les z_j appartiennent à $\mathbf{Z}_p$, on minore trivialement

$$v\left(\Delta'_{\overline{I},\overline{J}}\right) \ge -v\left(\prod_{i \notin I} k_i!\right) \ge -\frac{1}{p-1}(\sum_{i \notin I} k_i), \tag{7}$$

grâce au Lemme 2. Notons

$$\omega := \log_p\left(\theta_1^{p^t}\right) = \sum_{k=1}^{+\infty}(-1)^{k-1}\frac{(\theta_1^{p^t} - 1)^k}{k}.$$

Or, par inégalité ultramétrique,

$$v(\omega) = v\left(\log_p \theta_1^{p^t}\right) = v\left(\theta_1^{p^t} - 1\right) \ge \frac{p^t}{e} > \frac{1}{p-1}.$$

Les fonctions φ_i sont donc analytiques dans une boule ouverte centrée à l'origine de rayon > 1, et s'y développent en série de Taylor:

$$\varphi_i(z) = \sum_{\nu \ge k_i} \frac{\nu(\nu-1)\cdots(\nu-k_i+1)}{\nu! k_i!}(\ell_i\omega)^{\nu-k_i} z^\nu = \sum_{\nu \in \mathbf{N}} \binom{\nu}{k_i}(\ell_i\omega)^{\nu-k_i}\frac{z^\nu}{\nu!}.$$

Reportons maintenant cette formule dans le déterminant d'interpolation $\Delta'_{I,J}$. Pour simplifier l'écriture, posons $n = \mathrm{Card}\, I = \mathrm{Card}\, J$, et supposons que $J = \{1,\dots,n\}$. Par multilinéarité du déterminant sur les colonnes, il vient alors

$$\begin{aligned} \Delta'_{I,J} &= \sum_{(\nu_1,\dots,\nu_n) \in \mathbf{N}^n} \left(\prod_{j=1}^n \frac{z_j^{\nu_j}}{\nu_j!}\right) \det\left(\binom{\nu_j}{k_i}(\ell_i\omega)^{\nu_j - k_i}\right)_{\substack{i \in I \\ 1 \le j \le n}} \\ &= \sum_{\substack{0 \le \nu_1 < \cdots < \nu_n \\ \sum \nu_j \ge \sum k_i}} \frac{\det\left(z_i^{\nu_j}\right) \times \det\left(\binom{\nu_j}{k_i}\ell_i^{\nu_j - k_i}\right)}{\nu_1! \times \cdots \times \nu_n!}\omega^{(\sum \nu_j - \sum k_i)}, \end{aligned} \tag{8}$$

cette dernière égalité provenant du fait que les déterminants dans le membre de droite de la première ligne changent de signe, lorsque l'on permute deux indices de sommation ν_{j_1} et ν_{j_2}. Remarquons maintenant que le quotient

$$\frac{\det\left(z_i^{\nu_j}\right)}{\prod_{1\le i<j\le n}(z_i-z_j)}$$

n'est autre que la valeur d'un polynôme de Schur évalué en des points $z_j\in\mathbf{Z}_p$. D'après les Lemmes 1 et 2, on a donc

$$v\Big(\det\left(z_i^{\nu_j}\right)\Big)\ge v\left(\prod_{1\le i<j\le n}(z_i-z_j)\right)\ge v\left(\prod_{\nu=1}^{n-1}\nu!\right)\ge\frac{n^2-n}{2(p-1)}-\frac{n\log n}{\log p},$$

et d'autre part

$$v\Big(\nu_1!\times\cdots\times\nu_n!\Big)\le\frac{\nu_1+\cdots+\nu_n}{p-1}.$$

Il vient donc

$$v(\Delta'_{I,J})\ge\min\left\{\Big(v(\omega)-\frac{1}{p-1}\Big)(\nu_1+\cdots+\nu_n)\right\}-v(\omega)\Big(\sum_{i\in I}k_i\Big)+\frac{n^2-n}{2(p-1)}-\frac{n\log n}{\log p},$$

où le minimum est pris sur les n-uplets d'entiers $(\nu_1,\dots,\nu_n)$ vérifiant $0\le\nu_1<\cdots<\nu_n$ et $\sum_{j=1}^n\nu_j\ge\sum_{i\in I}k_i$. Comme

$$v(\omega)\ge\frac{p^t}{e}>\frac{1}{p-1},$$

il s'ensuit que

$$\begin{aligned}v(\Delta'_{I,J})\ge\left(v(\omega)-\frac{1}{p-1}\right)\max\left\{\frac{n^2-n}{2},\sum_{i\in I}k_i\right\}-v(\omega)\left(\sum_{i\in I}k_i\right)+\frac{n^2-n}{2(p-1)}-\frac{n\log n}{\log p}=\\ \max\left\{v(\omega)\left(\frac{n^2-n}{2}-\sum_{i\in I}k_i\right),\frac{1}{p-1}\left(\frac{n^2-n}{2}-\sum_{i\in I}k_i\right)\right\}-\frac{n\log n}{\log p}\\ \ge\frac{p^t}{e}\left(\frac{n^2-n}{2}-\sum_{i\in I}k_i\right)-\frac{n\log n}{\log p}.\end{aligned}$$

Reportant dans (6), il vient grâce à (7) et à la minoration $\frac{p^t}{e}>\frac{1}{p-1}$

$$\begin{aligned}v(\Delta'_I)&\ge\frac{p^t}{e}\left(\frac{n^2-n}{2}-\sum_{i=1}^{N}k_i\right)-\frac{n\log n}{\log p}\\&\ge\frac{p^t}{e}\left(\frac{n^2-n}{2}-\frac{N(K-1)}{2}\right)-\frac{N\log N}{\log p}.\end{aligned}$$

La formule (4) montre alors que

$$\begin{aligned} v(\Delta) = v(\Delta') \geq & \min_{0\leq n\leq N} \left\{ (N-n)v(\Lambda') + \frac{p^t(n^2-n)}{2e} \right\} - \frac{p^tN(K-1)}{2e} - \frac{N\log N}{\log p} \\ \geq & \frac{p^t}{e} \min_{0\leq n\leq N} \left\{ (N-n)(N-\frac{1}{2}) + \frac{n^2-n}{2} \right\} - \frac{p^tN(K-1)}{2e} - \frac{N\log N}{\log p} \\ = & \frac{p^t(N^2-N)}{2e} - \frac{p^tN(K-1)}{2e} - \frac{N\log N}{\log p}, \end{aligned}$$

d'où s'ensuit le lemme. □

4.3. Minoration arithmétique de $|\Delta|_p$.

Nous commençons par un résultat combinatoire qui joue le rôle du Lemme 4 de [5] dont nous rappelons ici l'énoncé.

Lemme 9. *Soient K, L, R et S des entiers ≥ 1. Posons $N = KL$ et $\ell_\nu = [(\nu-1)/K]$, $(1 \leq \nu \leq N)$. Pour chaque suite d'entiers $(r_1, \dots, r_N)$ compris entre 0 et $R-1$, et telle qu'aucun entier ne soit répété plus de S fois dans la suite, on a l'encadrement*

$$M - G \leq \sum_{\nu=1}^{N} \ell_\nu r_\nu \leq M + G,$$

où

$$M = \frac{(L-1)(r_1+\cdots+r_N)}{2}, \quad G = \frac{NLR}{2}\left(\frac{1}{4} - \frac{N}{12RS}\right).$$

Le résultat suivant coincide avec le Lemme 9 lorsque $g = 1$.

Lemme 10. *Soit K, L, R, S, g des entiers ≥ 1, m_1, m_2, c, des entiers rationnels. On suppose que les entiers m_1, m_2, g sont premiers entre eux. Notons $N = KL$ et $\ell_\nu = [(\nu-1)/K]$ $(1 \leq \nu \leq N)$. Soit $(r_1, s_1), \dots, (r_N, s_N)$ une suite de N couples d'entiers, deux à deux distincts, et vérifiant les conditions*

$$(*) \qquad 0 \leq r_\nu \leq R-1\,,\ 0 \leq s_\nu \leq S-1\,,\ m_1 r_\nu + m_2 s_\nu \equiv c \,\mathrm{modulo}\, g,$$

pour tout $\nu = 1, \dots, N$. On a alors les encadrements

$$M_1 - G_1 \leq \sum_{\nu=1}^{N} \ell_\nu r_\nu \leq M_1 + G_1,$$

$$M_2 - G_2 \leq \sum_{\nu=1}^{N} \ell_\nu s_\nu \leq M_2 + G_2.$$

avec

$$M_1 = \frac{(L-1)(r_1 + \cdots + r_N)}{2}, \quad G_1 = \frac{NL(R+g-1)}{8} - \frac{gN^2L}{24(S+g-1)},$$
$$M_2 = \frac{(L-1)(s_1 + \cdots + s_N)}{2}, \quad G_2 = \frac{NL(S+g-1)}{8} - \frac{gN^2L}{24(R+g-1)}.$$

Preuve — Montrons le premier encadrement ; le deuxième s'en déduisant par permutation de R et S. Notons

$$g' = \mathrm{pgcd}(m_2, g), \;\; g'' = g/g'.$$

En particulier m_1 et g' sont premiers entre eux. Soit c' l'entier compris entre 0 et $g'-1$ tel que $m_1 c' \equiv c \bmod g'$. Les relations $m_1 r_\nu + m_2 s_\nu \equiv c \bmod g$ pour $\nu = 1, \ldots, N$, montrent alors que les r_ν sont congrus à c' modulo g'. Ecrivons donc

$$r_\nu = c' + g' r'_\nu, 0 \le r'_\nu \le R' := \left[\frac{R-1}{g'}\right], (\nu = 1, \ldots, N).$$

D'autre part, la même congruence $m_1 r + m_2 s \equiv c \bmod g$ montre que pour r fixé , la classe de s modulo g'' est uniquement déterminée. Il y a donc au plus $S' = \left[\frac{S-1}{g''}\right] + 1$ couples d'entiers (r, s) vérifiant $(*)$ pour lesquels la première coordonnée r est fixée. Le Lemme 9 ci-dessus appliqué à la suite d'entiers $(r'_1, \ldots, r'_N)$ nous fournit alors l'encadrement

$$M'_1 - G'_1 \le \sum_{\nu=1}^{N} \ell_\nu r'_\nu \le M'_1 + G'_1,$$

avec

$$M'_1 = \frac{(L-1)(r'_1 + \cdots + r'_N)}{2}, \quad G'_1 = \frac{NL(R'+1)}{8} - \frac{N^2 L}{24 S'}.$$

Notant que $\sum_{\nu=1}^{N} \ell_\nu = \frac{(L-1)N}{2}$, il s'ensuit que

$$M_1 - g' G'_1 \le \sum_{\nu=1}^{N} \ell_\nu r_\nu \le M_1 + g' G'_1.$$

Majorant alors trivialement

$$R' + 1 \le \frac{R + g' - 1}{g'}, S' \le \frac{S + g'' - 1}{g''},$$

il vient

$$g' G'_1 \le \frac{NL(R + g' - 1)}{8} - \frac{N^2 Lg}{24(S + g'' - 1)} \le G_1. \;\; \square$$

Rappelons que nous avons défini

$$b = \frac{(R-1)b_2 + (S-1)b_1}{2} \left(\prod_{k=1}^{K-1} k! \right)^{-2/(K^2-K)},$$

$$\gamma_1 = \frac{R+g-1}{2R} - \frac{gN}{6R(S+g-1)} = \frac{4G_1}{NLR}, \quad \gamma_2 = \frac{S+g-1}{2S} - \frac{gN}{6S(R+g-1)} = \frac{4G_2N}{NLS}.$$

Lemme 11. *Soit Δ un mineur non nul d'ordre maximal $N \times N$ extrait de $\mathcal{M}$. On a alors la minoration:*

$$\log |\Delta|_p \geq -\frac{DN}{2e}\Big(\log N + (K-1)\log b + \gamma_1 p^t LRh(\alpha_1) + \gamma_2 p^t LSh(\alpha_2)\Big).$$

Preuve— Ce lemme correspond à la Proposition 3 de [2] : il s'agit de l'analogue p-adique du Lemme 6 de [5]. On utilise ici la version suivante de l'inégalité de Liouville: pour tout polynôme $P(X,Y)$, à coefficients entiers, et pour tous nombres algébriques ξ et ζ contenus dans $\overline{\mathbf{Q}}_p$, tels que $P(\xi,\zeta) \neq 0$, on a la minoration

$$\log |P(\xi,\zeta)|_p \geq -\frac{[\mathbf{Q}(\xi,\zeta):\mathbf{Q}]}{ef}\Big\{ \log |P| + (\deg_X P)h(\xi) + (\deg_Y P)h(\zeta)\Big\},$$

où e et f désignent comme précédemment l'indice de ramification et le degré résiduel de l'extension de corps $\mathbf{Q}_p(\xi,\zeta)/\mathbf{Q}_p$, et où

$$|P| = \max\{|P(x,y)|; x \in \mathbf{C}, y \in \mathbf{C}, |x| = |y| = 1\}$$

désigne la "norme sup" du polynôme P. Cette version de l'inégalité de Liouville résulte par exemple du Lemme 3.5 et de l'exercice 2 du chapitre 3 de [8].

Considérons le polynôme

$$P(X,Y) = \sum_\sigma \mathrm{sg}(\sigma) \prod_{i=1}^N \binom{r_{\sigma(i)}b_2 + s_{\sigma(i)}b_1}{k_i} X^{\sum_{i=1}^N \ell_i r_{\sigma(i)}} Y^{\sum_{i=1}^N \ell_i s_{\sigma(i)}},$$

où σ décrit le groupe symétrique $\mathcal{S}_N$, et où $\mathrm{sg}(\sigma)$ désigne la signature de la substitution σ. Il est clair que $\Delta = P(\alpha_1^{p^t}, \alpha_2^{p^t})$. D'autre part, la majoration

$$|P| \leq N^{N/2} \left(\frac{(R-1)b_2 + (S-1)b_1}{2} \right)^{(K-1)N/2} \left(\prod_{i=1}^N k_i! \right)^{-1} = N^{N/2}\, b^{(K-1)N/2},$$

a été établie dans le Lemme 6 de [5]. La preuvese pousuit alors comme dans le cas archimédien. Le Lemme 10 nous fournit maintenant les estimations

$$M_1 - G_1 \leq \sum \ell_i r_{\sigma(i)} \leq M_1 + G_1,$$

$$M_2 - G_2 \leq \sum \ell_i s_{\sigma(i)} \leq M_2 + G_2,$$

avec

$$G_1 = \frac{NL(R+g-1)}{8} - \frac{gN^2L}{24(S+g-1)} = \frac{\gamma_1 LRN}{4}$$
$$G_2 = \frac{NL(S+g-1)}{8} - \frac{gN^2L}{24(R+g-1)} = \frac{\gamma_2 LSN}{4}.$$

Désignons par V_1 (resp. V_2) la partie entière de M_1+G_1 (resp. M_2+G_2), et par U_1 (resp. U_2) le plus petit entier $\geq M_1 - G_1$ (resp. $M_2 - G_2$). On a alors la formule

$$\Delta = P(\alpha_1^{p^t}, \alpha_2^{p^t}) = \alpha_1^{p^tV_1}\alpha_2^{p^tV_2}\tilde{P}\left(\frac{1}{\alpha_1^{p^t}}, \frac{1}{\alpha_2^{p^t}}\right),$$

où $\tilde{P}(X,Y)$ est un polynôme à coefficients entiers, dont la norme $|\tilde{P}|$ est égale à $|P|$, et dont les degrés en X et en Y sont respectivement majorés par V_1-U_1 et par V_2-U_2. Appliquant l'inégalité de Liouville ci-dessus au polynôme $\tilde{P}$ et sachant que $h(\alpha_i^{p^t}) = p^t h(\alpha_i)$, on obtient la minoration

$$\log|\tilde{P}\left(\alpha_1^{p^t}, \alpha_2^{p^t}\right)|_p \geq -\frac{D}{e}\left\{\log|\tilde{P}| + p^t(V_1-U_1)h(\alpha_1) + p^t(V_2-U_2)h(\alpha_2)\right\}.$$

Puisque $|\alpha_1|_p = |\alpha_2|_p = 1$ et que $U_i - V_i \leq 2G_i$ pour $i=1,2$, il vient

$$\log|\Delta|_p \geq -\frac{D}{e}\left\{\log|P| + 2G_1p^th(\alpha_1) + 2G_2p^th(\alpha_2)\right\}.$$

On obtient alors le lemme en utilisant la majoration ci-dessus de $|P|$ et en substituant aux G_i leurs valeurs. $\square$

4.3. Démonstration du Théorème 1.

Sous réserve de la majoration (3), les Lemmes 8 et 11 fournissent l'encadrement suivant de $\log|\Delta|_p$:

$$-\frac{p^t\log p}{2e}NK(L-1) + N\log N \geq \log|\Delta|_p \geq -\frac{DN}{2e}\Big(\log N + (K-1)\log b$$
$$+\gamma_1p^tLRh(\alpha_1) + \gamma_2p^tLSh(\alpha_2)\Big).$$

Après multiplication par $2e/N$, on aboutit à l'opposé de (2).

5. Mode d'emploi du Théorème 1.

Simplifions tout d'abord l'hypothèse (2) en la remplaçant par une inégalité plus forte. Plaçons nous maintenant dans le contexte du Théorème 2 et posons:

$$D' = \frac{D}{\log p}, \quad a_i = \frac{D \log A_i}{\log p} \geq \max\left\{ \frac{Dh(\alpha_i)}{\log p}, 1 \right\}, \ (i = 1, 2).$$

Soit d'autre part

$$B \geq D' \log b = \frac{D \log b}{\log p},$$

un nombre réel ≥ 0 que l'on fixera ultérieurement. Comme $t \geq 0$ et que $e \leq D$, la condition

$$(2)' \qquad K(L-1) > 3D' \log N + (K-1)B + \gamma_1 LRa_1 + \gamma_2 LSa_2.$$

implique alors (2).

5.1. Choix des paramètres et estimations.

Soient k et ℓ deux constantes > 0. On fixe alors

$$L = [\ell B] + 2, \quad K = [kgLa_1a_2] + 1$$
$$R_1 = \left[\sqrt{gLa_2/a_1}\right] + 1, \quad S_1 = \left[\sqrt{gLa_1/a_2}\right] + 1$$
$$R_2 = \left[\sqrt{g(K-1)La_2/a_1}\right] + 1, \quad S_2 = \left[\sqrt{g(K-1)La_1/a_2}\right] + 1.$$

Par définition même des quantités R_1, S_1, R_2, S_2, on a les minorations

$$(1)' \qquad \begin{aligned} R_1S_1 &\geq gL \\ R_2S_2 &> g(K-1)L. \end{aligned}$$

Nous allons maintenant majorer les termes $\gamma_1 LRa_1, \gamma_2 LSa_2$ et $(K-1)B$, qui interviennent dans le membre de droite de $(2)'$. On notera que les estimations obtenues sont tout à fait analogues à celles des Lemmes 7 et 8 de [5], qui coincident essentiellement avec les deux lemmes suivants lorsque $g = 1$.

Lemme 12. *On a la majoration*

$$\gamma_1 Ra_1 \leq \frac{1}{3}\sqrt{g(K-1)La_1a_2} + \frac{2}{3}\sqrt{gLa_1a_2} + \frac{ga_1}{2} + \frac{ga_2}{6}$$
$$\gamma_2 Sa_2 \leq \frac{1}{3}\sqrt{g(K-1)La_1a_2} + \frac{2}{3}\sqrt{gLa_1a_2} + \frac{ga_2}{2} + \frac{ga_1}{6}.$$

Preuve — Montrons la première majoration ; la deuxième s'en déduisant en permutant a_1 et a_2. On part de la formule

$$\gamma_1 Ra_1 = \frac{(R+g-1)a_1}{2} - \frac{gKLa_1}{6(S+g-1)}.$$

Comme dans le Lemme 9 de [5], utilisons les estimations

$$\begin{gathered}
R+g-1=R_1+g-1+R_2-1 \le R_1+g-1+\sqrt{g(K-1)La_2/a_1} \\
S+g-1=S_1+g-1+S_2-1 \le S_1+g-1+\sqrt{g(K-1)La_1/a_2} \\
\sqrt{gLa_2/a_1} \le R_1 < 1+\sqrt{gLa_2/a_1}, \quad \sqrt{gLa_1/a_2} \le S_1 < 1+\sqrt{gLa_1/a_2}, \\
\frac{1}{S+g-1} \ge \frac{1}{S_1+g-1+\sqrt{g(K-1)La_1/a_2}} \ge \frac{1}{\sqrt{g(K-1)La_1/a_2}} - \frac{S_1+g-1}{g(K-1)La_1/a_2}.
\end{gathered}$$

Cette dernière minoration montre que

$$\begin{aligned}
\frac{gKLa_1}{6(S+g-1)} \ge \frac{g(K-1)La_1}{6(S+g-1)} &\ge \frac{\sqrt{g(K-1)La_1a_2}}{6} - \frac{(S_1+g-1)a_2}{6} \\
&\ge \frac{\sqrt{g(K-1)La_1a_2}}{6} - \frac{\sqrt{gLa_1a_2}}{6} - \frac{ga_2}{6}.
\end{aligned}$$

D'autre part, on majore

$$\frac{(R+g-1)a_1}{2} \le \frac{ga_1+\sqrt{gLa_1a_2}+\sqrt{g(K-1)La_1a_2}}{2}.$$

Regroupant les diverses estimations, on trouve la majoration annoncée. $\Box$

Nous pouvons maintenant reformuler la condition $(2)'$ en une relation numérique simple entre les paramètres k, ℓ, B, a_1, a_2. Posons $\lambda = \ell + \frac{2}{B}$, de telle sorte que

$$\ell B < L-1 < L \le \ell B + 2 = \lambda B.$$

On minore

$$K(L-1) > kgLa_1a_2 \times \ell B > k\ell^2 gB^2 a_1a_2,$$

tandis que l'on majore

$$(K-1)B \le kgLa_1a_2 \times B \le kgBa_1a_2(\ell B+2) = k\ell gB^2a_1a_2 + 2kgBa_1a_2.$$

D'autre part, le Lemme 12 nous fournit la majoration

$$\begin{aligned}
\gamma_1 LRa_1 \le& \frac{1}{3}\sqrt{k}gL^2a_1a_2 + \frac{2}{3}L^{3/2}\sqrt{ga_1a_2} + \frac{gLa_1}{2} + \frac{gLa_2}{6} \\
\le& \frac{1}{3}\sqrt{k}\lambda^2 gB^2a_1a_2 + \frac{2}{3}\lambda^{3/2}B^{3/2}\sqrt{ga_1a_2} + \frac{g\lambda Ba_1}{2} + \frac{g\lambda Ba_2}{6} \\
\le& gB^2a_1a_2\left(\frac{\sqrt{k}\lambda^2}{3} + \frac{2}{3}\frac{\lambda^{3/2}}{\sqrt{B}} + \frac{2}{3}\frac{\lambda}{B}\right),
\end{aligned}$$

en tenant compte des minorations $g \ge 1, a_1 \ge 1, a_2 \ge 1$. Par symétrie, la même majoration vaut pour $\gamma_2 LSa_2$. On majore enfin

$$N = KL \le kgL^2a_1a_2 + L \le k\lambda^2 gB^2a_1a_2 + \lambda B.$$

Remplaçant les termes intervenant dans $(2)'$ par les diverses estimations ci-dessus et divisant par $gB^2a_1a_2$, il s'ensuit que la relation

$$(2)'' \qquad k\ell^2 - k\ell - \frac{2}{3}\sqrt{k}\lambda^2 \geq \frac{2k}{B} + \frac{4}{3}\frac{\lambda^{3/2}}{\sqrt{B}} + \frac{4}{3}\frac{\lambda}{B} + \frac{3D'\log\left(k\lambda^2 gB^2a_1a_2 + \lambda B\right)}{gB^2a_1a_2},$$

où le membre de droite tend vers 0 quand B tend vers l'infini, implique l'inégalité $(2)'$.

Il nous reste maintenant à comparer $B \geq D'\log b$ avec b', comme dans le Lemme 8 de [5]. Rappelons que nous avons posé

$$b' = \frac{b_1}{D\log A_2} + \frac{b_2}{D\log A_1} = \frac{1}{\log p}\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right)$$

$$b = \frac{(R-1)b_2 + (S-1)b_1}{2}\left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)}.$$

Lemme 13. *On a la majoration*

$$\log b \leq \log b' + \log\log p - \frac{1}{2}\log k - \log 2 + \frac{3}{2} + \epsilon(K),$$

où ϵ désigne la fonction décroissante de la variable réelle $x > 1$:

$$\epsilon(x) = \log\frac{\left(1+\sqrt{x-1}\right)\sqrt{x}}{(x-1)}.$$

Preuve — Il a été établi dans le Lemme 8 de [5] que

$$\left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)} \leq \exp\left\{-\log(K-1) + \frac{3}{2} - \frac{\log\left(2\pi(K-1)/\sqrt{e}\right)}{K-1} + \frac{\log K}{6K(K-1)}\right\}.$$

Négligeant le terme négatif $-\frac{\log\left(2\pi(K-1)/\sqrt{e}\right)}{K-1} + \frac{\log K}{6K(K-1)}$, il vient

$$\begin{aligned}
b &\leq \frac{(R-1)b_2 + (S-1)b_1}{2(K-1)}e^{3/2} \\
&\leq \frac{\left(1+\sqrt{K-1}\right)\sqrt{gLa_1a_2}}{2(K-1)}\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right)e^{3/2} \\
&\leq \frac{\left(1+\sqrt{K-1}\right)\sqrt{K}}{2(K-1)\sqrt{k}}\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right)e^{3/2}.
\end{aligned}$$

On obtient ainsi

$$\log b \leq \log b' + \log\log p - \log\sqrt{k} - \log 2 + \frac{3}{2} + \log\frac{\left(1+\sqrt{K-1}\right)\sqrt{K}}{(K-1)}. \quad \square$$

5.2. Preuve du Théorème 2.

On s'intéresse à la valeur asymptotique de la constante c, de telle sorte que seuls les termes de plus haut degré en B sont à considérer. Soit η un réel > 1. Fixons $B = \eta D' \log b'$. Comme le terme reste ϵ du Lemme 13 tend vers 0 quand K tend vers l'infini, il est clair d'après ce même lemme que $D' \log b \leq B$ lorsque b' est suffisamment grand. La démonstration se scinde en deux alternatives analogues à celles rencontrées dans le cadre archimédien.

Supposons tout d'abord que pour toute classe c modulo g, on ait

$$\mathrm{Card}\left\{b_2 r + b_1 s\,;\, 0 \leq r < R_2, 0 \leq s < S_2,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\} = \mathrm{Card}\left\{(r,s)\,;\, 0 \leq r < R_2, 0 \leq s < S_2,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\}.$$

Puisque α_1, α_2 sont multiplicativement indépendants, on a de même

$$\mathrm{Card}\left\{\alpha_1^{p^t r}\alpha_2^{p^t s}\,;\, 0 \leq r < R_1, 0 \leq s < S_1,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\} = \mathrm{Card}\left\{(r,s)\,;\, 0 \leq r < R_1, 0 \leq s < S_1,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\}.$$

D'après $(1)'$, on a alors

$$\sum_{c=1}^{g} \mathrm{Card}\left\{\alpha_1^{p^t r}\alpha_2^{p^t s}\,;\, 0 \leq r < R_1, 0 \leq s < S_1,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\} = R_1 S_1 \geq gL$$

$$\sum_{c=1}^{g} \mathrm{Card}\left\{b_2 r + b_1 s\,;\, 0 \leq r < R_2, 0 \leq s < S_2,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\} = R_2 S_2 > g(K-1)L.$$

Le principe des tiroirs nous fournit alors des entiers c_1, c_2 tels que la condition (1) du Théorème 1 soit vérifiée. D'autre part, la condition $(2)''$ se réduit asymptotiquement à l'inégalité

$$k\ell^2 - k\ell - \frac{2}{3}\sqrt{k}\ell^2 > 0$$

lorsque B est grand. On choisit alors les paramètres k et ℓ très proches par valeurs supérieures des valeurs limites $k = \frac{16}{9}, \ell = 2$, pour lesquelles la quantité $k\ell^2$ est minimale et vaut $\frac{64}{9}$. Majorant trivialement $u \leq \log \min\{b_1, b_2\}/\log p$, le Théorème 1 nous fournit la majoration

$$v(\Lambda) \leq \frac{p}{p-1} KL + u \leq \frac{c' p g}{(p-1)(\log p)^4} D^4 (\log b')^2 \log A_1 \log A_2$$

pour b' suffisamment grand, dès lors que la constante c' est $> 64/9$.

Supposons maintenant qu'il existe une classe c modulo g telle que

$$\mathrm{Card}\left\{b_2 r + b_1 s\,;\, 0 \leq r < R_2, 0 \leq s < S_2,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\} < \mathrm{Card}\left\{(r,s)\,;\, 0 \leq r < R_2, 0 \leq s < S_2,\ m_1 r + m_2 s \ \equiv\ c \text{ modulo } g\right\}.$$

Dans cette situation, nous allons établir la majoration plus fine

$$v(\Lambda) \leq gD' \log 2 + 2\sqrt{k}\lambda gBa_1a_2 + u \leq \frac{c''g}{(\log p)^3} D^3 \log b' \log A_1 \log A_2$$

pour b' suffisamment grand, lorsque la constante c'' est $> 19/3$.

Le principe des tiroirs montre alors qu'il existe un couple d'entiers $(r, s) \neq (0, 0)$ vérifiant

$$|r| < R_2, |s| < S_2, b_2r + b_1s = 0, \, m_1r + m_2s \equiv 0 \text{ modulo } g.$$

Posons

$$r' = \frac{r}{\mathrm{pgcd}(r,s)}, \quad s' = \frac{s}{\mathrm{pgcd}(r,s)},$$

de telle sorte que

$$b_1 = nr', \quad b_2 = -ns'.$$

On écrit alors

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2} = \alpha_1^{nr'} - \alpha_2^{-ns'} = \prod_{\xi^n=1} \left(\alpha_1^{r'} - \xi\alpha_2^{-s'}\right).$$

Comme $n = \mathrm{pgcd}(b_1, b_2) = n'p^u$ avec n' premier à p, le Lemme 5 montre que

$$\sum_{\substack{\xi^n=1 \\ \xi\neq 1}} v(\xi - 1) = u.$$

Procédant comme dans la preuve du Lemme 8, il existe une unique racine n-ième de l'unité μ telle que

$$v(\alpha_1^{r'} - \mu\alpha_2^{-s'}) \geq v(\Lambda) - u,$$
$$v(\alpha_1^{r'} - \mu\alpha_2^{-s'}) > v(\alpha_1^{r'} - \xi\alpha_2^{-s'}), \quad (\xi^n = 1, \xi \neq \mu),$$

dès lors que $v(\Lambda) > \frac{1}{p-1} + u$. Le Lemme de Krasner nous montre maintenant que μ appartient au corps $\mathbf{Q}_p(\alpha_1^{r'}\alpha_2^{s'}) \subseteq \mathbf{K}_v$. On peut donc écrire μ sous la forme $\mu = \zeta^m\xi$ avec $\xi^{p^t} = 1$, puisque la classe dans U_v/U_v^1 de la composante de μ d'ordre premier à p est engendrée par les classes de α_1 et α_2, et que l'ordre de la composante p-primaire de μ divise p^t par l'argument de ramification déjà utilisé dans la preuve du Lemme 8. Comme $\xi \in U_v^1$ et que $\alpha_1^{r'} - \mu\alpha_2^{-s'}$ est de valuation positive, la réduction modulo U_v^1 entraîne de plus la congruence d'entiers

$$m_1r' \equiv -m_2s' + m \text{ modulo } g.$$

Il s'ensuit que

$$m \times \mathrm{pgcd}(r, s) \equiv m_1r + m_2s \equiv 0 \text{ modulo } g.$$

Posons alors $g' = g/\mathrm{pgcd}(m, g)$. La congruence ci-dessus montre que $\mathrm{pgcd}(r, s)$ est divisible par g'. On obtient ainsi les majorations

$$|r'| \leq \frac{R_2 - 1}{g'}, |s'| \leq \frac{S_2 - 1}{g'}.$$

Appliquons maintenant l'inégalité de Liouville au polynôme $X - Y$. Il vient

$$\begin{aligned}\log\left|\alpha_1^{r'} - \mu\alpha_2^{-s'}\right|_p &\geq -\frac{[\mathbf{Q}(\alpha_1,\alpha_2,\mu):\mathbf{Q}]}{[\mathbf{Q}_p(\alpha_1,\alpha_2,\mu):\mathbf{Q}_p]}\left(\log 2 + \frac{R_2-1}{g'}h(\alpha_1) + \frac{S_2-1}{g'}h(\alpha_2)\right)\\ &\geq -\frac{[\mathbf{Q}(\alpha_1,\alpha_2,\mu):\mathbf{Q}]}{ef}\left(\log 2 + \frac{R_2-1}{g'}h(\alpha_1) + \frac{S_2-1}{g'}h(\alpha_2)\right).\end{aligned}$$

D'autre part, ζ^m est une racine de l'unité d'ordre exactement g'. On majore alors

$$\begin{aligned}\frac{[\mathbf{Q}(\alpha_1,\alpha_2,\mu):\mathbf{Q}]}{ef} &\leq \frac{[\mathbf{Q}(\alpha_1,\alpha_2):\mathbf{Q}]\times[\mathbf{Q}(\zeta^m):\mathbf{Q}]\times[\mathbf{Q}(\xi):\mathbf{Q}]}{ef}\\ &\leq \frac{Dg'p^{t-1}(p-1)}{e} \leq Dg'.\end{aligned}$$

La majoration annoncée se déduit alors immédiatement des estimations

$$\begin{aligned}D'(R_2-1)h(\alpha_1) &\leq \sqrt{k}gLa_1a_2 \leq \sqrt{k}\lambda gBa_1a_2\\ D'(S_2-1)h(\alpha_2) &\leq \sqrt{k}gLa_1a_2 \leq \sqrt{k}\lambda gBa_1a_2.\end{aligned}$$

5.3. Preuve du Théorème 3.

Elle consiste à rendre effectives les estimations asymptotiques précédentes. On choisit maintenant

$$k = 3, \quad \ell = 2.6, \quad B = D'\max\left\{\log b' + \log\log p + 0.4\,,\ \frac{10}{D'}\,,\ 10\right\}.$$

Vérifions tout d'abord que l'on a bien

$$B \geq D'\log b.$$

Puisque $B \geq 10$, on a $L \geq 28$, et $K \geq 85$. Le Lemme 13 nous fournit la minoration requise en majorant trivialement

$$-\frac{1}{2}\log k - \log 2 + \frac{3}{2} + \epsilon(85) \leq 0.4.$$

Majorant alors $\lambda \leq 2.8$, et minorant $B \geq \max\{10D', 10\}, a_1 \geq 1, a_2 \geq 1$, on constate que le membre de droite de $(2)''$ est

$$\leq 0.6 + \frac{4\times(2.8)^{3/2}}{3\times\sqrt{10}} + \frac{4\times 2.8}{3\times 10} + \frac{3\log\left(3\times(2.8)^2\times 100 + 2.8\times 10\right)}{10\times 10} \leq 3.2;$$

tandis que le membre de gauche est ≥ 3.4. La relation $(2)''$ est donc satisfaite pour notre choix de paramètres. Dans ces conditions, il a été établi dans le paragraphe 5.2 que l'on a la majoration

$$v(\Lambda) \leq \max\left\{\frac{p}{p-1}KL\,,\, gD'\log 2 + 2\sqrt{k}\lambda g B a_1 a_2\right\} + u,$$

le maximum correspondant aux deux alternatives évoquées ci-dessus. Montrons maintenant que

$$u \leq \frac{a_2}{\log p}\max\left\{\log b' + \log\log p, 1\right\} \leq B a_1 a_2.$$

A cet effet, remarquons que

$$\log b' + \log\log p = \log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) \geq \log\left(\frac{b_1}{a_2}\right).$$

D'autre part, on a $u \leq \log b_1/\log p$ puisque p^u divise b_1. Il suffit donc de vérifier que l'inégalité

$$\log b_1 \leq a_2 \max\left\{\log\frac{b_1}{a_2}, 1\right\}$$

vaut pour tout réel $b_1 \geq 1$ et $a_2 \geq 1$: lorsque $b_1 \leq ea_2$, on a bien $\log b_1 \leq 1 + \log a_2 \leq a_2$, et lorsque $b_1 \geq ea_2$, on a encore $\log b_1 \leq a_2 \log(b_1/a_2)$, puisque

$$(\log b_1)(a_2 - 1) \geq (1 + \log a_2)(a_2 - 1) \geq a_2 \log a_2.$$

Ici, e désigne bien sûr la base du logarithme néperien et non plus l'indice de ramification ! On majore alors

$$N = KL \leq gB^2 a_1 a_2\left(k\lambda^2 + \frac{\lambda}{B}\right) \leq 23.8 g B^2 a_1 a_2,$$
$$D' \leq \frac{B}{10}.$$

Substituant les estimations effectuées, il vient imédiatement

$$v(\Lambda) \leq \frac{24pg}{p-1}B^2 a_1 a_2. \quad \square$$

5.4. Preuve du Théorème 4.

On choisit

$$B = D' \max\left\{\log b' + \log\log p + 0.4\,,\ \frac{\mu}{D'}\,,\ \nu\right\}$$

de telle sorte que $B \geq \max\{\mu, \nu D'\}$. Notant alors

$$\tilde{\lambda} := \ell + \frac{2}{\mu} \geq \ell + \frac{2}{B} = \lambda,$$

il suffit de satisfaire l'inéquation

$$(2)''' \qquad k\ell^2 - k\ell - \frac{2}{3}\sqrt{k}\tilde{\lambda}^2 \geq \frac{2k}{\mu} + \frac{4}{3}\frac{\tilde{\lambda}^{3/2}}{\sqrt{\mu}} + \frac{4}{3}\frac{\tilde{\lambda}}{\mu} + \frac{3\log\left(k\tilde{\lambda}^2\mu^2 + \tilde{\lambda}\mu\right)}{\mu\nu},$$

liant les paramètres k, ℓ, μ, ν pour que la relation $(2)''$ soit vérifiée ; pourvu que

$$\log(k\ell^2\mu^2 + 4k\ell\mu + \ell\mu + 4k + 2) \geq 2,$$

auquel cas le dernier terme du membre de droite de $(2)'''$ est une fonction décroissante de la variable μ au point considéré. On notera que ces conditions sont satisfaites par les quadruplets $\Big(k(\mu,\nu), \ell(\mu,\nu), \mu, \nu\Big)$ avec $(\mu,\nu) \in \{4,6,8,10,15\} \times \{5,10\}$, où $k(\mu,\nu)$ et $\ell(\mu,\nu)$ sont déterminés respectivement par les deux tableaux suivants:

	$\mu=4$	$\mu=6$	$\mu=8$	$\mu=10$	$\mu=15$
$\nu=5$	4.3	3.6	3.4	3.0	3.1
$\nu=10$	3.9	3.7	3.3	2.9	3.0

	$\mu=4$	$\mu=6$	$\mu=8$	$\mu=10$	$\mu=15$
$\nu=5$	3.0	2.8	2.6	2.6	2.3
$\nu=10$	3.1	2.7	2.6	2.6	2.3

Comme $K \geq K_0 := [k[\ell\mu + 2] + 1]$, le tableau des minorants K_0 s'écrit alors:

	$\mu=4$	$\mu=6$	$\mu=8$	$\mu=10$	$\mu=15$
$\nu=5$	61	65	75	85	114
$\nu=10$	55	67	73	82	109

Il s'ensuit que la quantité

$$-\frac{1}{2}\log k(\mu,\nu) - \log 2 + \frac{3}{2} + \epsilon(K_0)$$

est toujours ≤ 0.4. On peut bien sûr raffiner l'énoncé du théorème 4 en remplaçant la constante 0.4 par la quantité ci-dessus dont voici la liste des valeurs numériques

	$\mu=4$	$\mu=6$	$\mu=8$	$\mu=10$	$\mu=15$
$\nu=5$	0.21	0.30	0.32	0.37	0.34
$\nu=10$	0.27	0.28	0.33	0.39	0.36

Le Lemme 13 montre alors que la condition requise $B \geq D' \log b$ est bien satisfaite par le choix de B effectué. Il nous suffit de reprendre les estimations du paragraphe 5.3. Majorons maintenant

$$D' \leq \frac{B}{\nu}, \quad u \leq Ba_1a_2 \leq \frac{B^2a_1a_2}{\mu}.$$

Il vient alors

$$\begin{aligned} v(\Lambda) &\leq \max\left\{\frac{p}{p-1}KL\,,\, gD'\log 2 + 2\sqrt{k}\tilde{\lambda}gBa_1a_2\right\} + u \\ &\leq \max\left\{\frac{p}{p-1}\left(k\tilde{\lambda}^2 + \frac{\tilde{\lambda}}{\mu}\right)gB^2a_1a_2\,,\, \frac{\log 2}{\nu}gB + 2\sqrt{k}\tilde{\lambda}gBa_1a_2\right\} + \frac{B^2a_1a_2}{\mu} \\ &\leq c(\mu,\nu)\frac{p}{p-1}gB^2a_1a_2, \end{aligned}$$

avec

$$c(\mu,\nu) = \max\left\{k\tilde{\lambda}^2 + \frac{\tilde{\lambda}}{\mu}, \frac{\log 2}{\mu\nu} + \frac{2\sqrt{k}\tilde{\lambda}}{\mu}\right\} + \frac{1}{\mu}.$$

Substituant alors les valeurs numériques des paramètres k et l, indiquées ci-dessus pour chacun des couples (μ,ν) considérés, on obtient immédiatement le tableau du Théorème 4. □

BIBLIOGRAPHIE

[1] Y. Amice : Les nombres p-adiques, Presses Universitaires de France (1975).

[2] Y. Bugeaud : Minoration effective de formes linéaires en deux logarithmes p-adiques, à paraître dans les publications de l'IRMA (Strasbourg).

[3] Dong Ping Ping : Minoration de combinaisons linéaires de deux logarithmes p-adiques, *Annales de la Faculté des Sciences de Toulouse* **12** (1991), 177-236 .

[4] M. Laurent : Linear forms in two logarithms and interpolation determinants, *Acta Arithmetica* **LXVI.2** (1994), 181-199.

[5] M. Laurent, M. Mignotte, Y. Nesterenko : Formes linéaires en deux logarithmes et déterminants d'interpolation, *Journal of Number theory* (à paraître).

[6] J.-P. Serre : Corps locaux, Hermann (1968).

[7] M. Waldschmidt : Fonctions auxiliaires et fonctionnelles analytiques, *J. Analyse Math.* **56** (1991), 231-279.

[8] M. Waldschmidt : Linear independence of logarithms of algebraic numbers, The Institute of Mathematical Sciences, IMSc. Report **116** (1992).

[9] Yu Kun Rui : Linear forms in p-adic logarithms, *Acta Arithmetica* **53** (1989), 107-189.

[10] Yu Kun Rui : Linear forms in p-adic logarithms II, *Compositio Math.* **74** (1990), 15-113.

[11] Yu Kun Rui : Linear forms in p-adic logarithms III, *Compositio Math.* **91** (1994), 241-276.

Yann BUGEAUD
Université Louis Pasteur
Institut de mathématiques
7 rue René Descartes
67084 STRASBOURG France

Michel LAURENT
Laboratoire de Mathématiques discrètes,
163 Avenue de Luminy, Case 930.
13288 MARSEILLE Cédex 9 France