Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Gérard Rauzy

Équations de la forme $\lambda\alpha^x - \mu\beta^y = \nu$ aux inconnues x, y $(entiers \geqslant 0)$

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 4 (1962-1963), exp. n° 9, p. 1-13

<http://www.numdam.org/item?id=SDPP_1962-1963__4__A8_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
4e année, 1962/63, n° 9

21 janvier 1963

ÉQUATIONS DE LA FORME $\lambda\alpha^x - \mu\beta^y = \nu$ AUX INCONNUES x , y (entiers $\geqslant 0$)

par Gérard RAUZY

1. Forme générale.

Soient α , β , λ , μ , ν des entiers algébriques donnés non nuls. Soit K un corps algébrique de degré fini sur $\mathbb{Q}$ corps des rationnels, contenant les entiers α , β , λ , μ , ν . Nous noterons $\mathfrak{a}$, $\mathfrak{b}$, ... les idéaux de l'anneau des entiers de K , $\mathfrak{p}$, $\mathfrak{q}$, ... les idéaux premiers et $[\alpha]$ l'idéal principal engendré par les multiples de l'entier α . Nous appellerons $\mathfrak{o}$ l'idéal unité, c'est-à-dire l'ensemble de tous les entiers de K . Enfin nous désignerons par $(\mathfrak{a} , \mathfrak{b})$ le p. g. c. d. des idéaux $\mathfrak{a}$ et $\mathfrak{b}$.

Nous écartons dans la suite le cas où α ou β sont des racines de l'unité. Si alors n est le degré de K et $\alpha_1 , \dots , \alpha_n , \beta_1 , \dots , \beta_n , \lambda_1 , \dots , \lambda_n , \mu_1 , \dots , \mu_n , \nu_1 , \dots , \nu_n$ les conjugués respectivement de $\alpha , \beta , \lambda , \mu , \nu$ on a alors :

$$\lambda\alpha^x - \mu\beta^y = \nu \iff \forall\ i = 1 , \dots , n , \ \lambda_i \alpha_i^x - \mu_i \beta_i^y = \nu_i .$$

Comme α n'est pas racine de l'unité, on ne peut avoir $|\alpha_i| = 1$, $\forall$ i . Mais $\Pi|\alpha_i| = |N_\alpha| \geqslant 1$, donc $\exists$ i tel que $|\alpha_i| > 1$.

Si nous supposons alors $|\beta_i| \leqslant 1$, pour toute solution (x , y) de l'équation $\lambda\alpha^x - \mu\beta^y = \nu$, on a :

$$|\lambda_i| \ |\alpha_i|^x \leqslant |\nu_i| + |\mu_i| \ |\beta_i|^y \leqslant |\nu_i| + |\mu_i| ,$$

d'où, comme $|\alpha_i| > 1$,

$$x \leqslant \frac{\operatorname{Log} \frac{|\nu_i| + |\mu_i|}{|\lambda_i|}}{\operatorname{Log}|\alpha_i|} .$$

D'autre part si (x_1 , y_1) , (x_2 , y_2) sont solutions de l'équation

$x_1 = y_1 \implies \beta^{y_1} = \beta^{y_2}$ et comme β n'est pas racine de l'unité

$$y_1 = y_2 .$$

Dans ce cas, l'équation n'admet donc qu'un nombre fini de solutions et l'on peut donner une borne pour la plus haute solution en x .

Nous supposerons donc dans la suite que ce cas est écarté et nous poserons (en prenant $\alpha = \alpha_i$, $\beta_i = \beta$)

$$|\alpha| > 1 \quad \text{et} \quad |\beta| > 1 .$$

D'autre part si $([\alpha] , [\beta]) \neq 0$, $\exists$ p premier $p|([\alpha] , [\beta])$ et comme $\nu \neq 0$, $\exists$ c tel que $p^c \not| \nu$.

Par conséquent l'équation $\lambda\alpha^x - \mu\beta^y = \nu$ ne peut avoir de solution avec $\min(x , y) \geqslant c$.

Dans ce cas l'équation n'admet encore qu'un nombre fini de solution et nous pouvons donner une borne pour $\min(x , y)$. Nous supposerons donc dans la suite que $([\alpha] , [\beta]) = 0$.

Alors $\exists$ (x_0 , y_0) tel que :

$$([\lambda\alpha^x] , [\mu\beta^y]) = ([\lambda\alpha^{x_0}] , [\mu\beta^{y_0}]) \quad \forall \ (x , y) , \ x \geqslant x_0 , \ y \geqslant y_0$$

en effet si

$$[\alpha] = p_1^{a_1} \cdots p_A^{a_A} , \ a_i \geqslant 1 , \quad \lambda = p_1^{c_1} \cdots p_A^{c_A} q_1^{c'_1} \cdots q_B^{c'_B} \ell , \ c_i \geqslant 0 , \ c'_i \geqslant 0$$

$$[\beta] = q_1^{b_1} \cdots q_B^{b_B} , \ b_i \geqslant 1 , \quad \mu = p_1^{d_1} \cdots p_A^{d_A} q_1^{d'_1} \cdots q_B^{d'_B} m , \ d_i \geqslant 0 , \ d'_i \geqslant 0$$

$$p_i \neq q_j , \ \forall \ i , j , \ p_i \not| \ell , \ p_i \not| m , \ q_j \not| \ell , \ q_j \not| m$$

si $\left.\begin{cases} x_0 = \max\limits_{i=1,\ldots,A} d_i \\ y_0 = \max\limits_{j=1,\ldots,B} c'_j \end{cases}\right\}$ alors $x \geqslant x_0 , \ y \geqslant y_0 \implies (\lambda\alpha^x , \mu\beta^y)$

$$= (\ell , m) \prod_{i=1}^{A} p_i^{d_i} \prod_{j=1}^{B} q_j^{c'_j}$$

qui est indépendant de (x , y) .

En posant $\lambda' = \lambda\alpha^{x_0}$, $\mu' = \mu\beta^{y_0}$ pour résoudre $\lambda\alpha^x - \mu\beta^y = \nu$ on sera ramené (sauf pour un nombre fini de solutions pour lesquelles on peut donner une borne pour x ou pour y) à résoudre $\lambda'\alpha^u - \mu'\beta^v = \nu$ et

$$([\lambda'\alpha^x] , [\mu'\beta^y]) = (\lambda' , \mu') , \ \forall \ x , y \geqslant 0 .$$

Finalement nous considérerons dans toute la suite des équations du type :

$$\lambda\alpha^x - \mu\beta^y = \nu$$

avec $|\alpha| > 1$, $|\beta| > 1$

$\delta = ([\lambda] , [\mu])$

$= ([\lambda\alpha^x] , [\mu\beta^y])$, $\forall \ x \geqslant 0$, $y \geqslant 0$ (ce qui entraîne $([\alpha] , [\beta]) = 0$).

Nous poserons

$$[\lambda] = \mathfrak{d}\alpha\ ,\quad [\mu] = \mathfrak{d}\mathfrak{b}\ ,\quad \text{donc}\quad ([\alpha^x]\ \alpha\ ,\ [\beta^y]\ \mathfrak{h}) = \mathfrak{o}\ .$$

Nous dirons que les équations $\mathcal{E}$: $\lambda\alpha^x - \mu\beta^y = \nu$ et $\mathcal{E}'$: $\lambda'\alpha'^x - \mu'\beta'^y = \nu'$ sont associées si $\alpha = \alpha'$, $\beta = \beta'$, et λ/λ' et μ/μ' sont des **unités**, c'est-à-dire $[\lambda'] = [\lambda]$ et $[\mu'] = [\mu]$, si $\mathcal{E}$ vérifie les conditions précédemment imposées, il en est alors de même de $\mathcal{E}'$.

2. Groupe des classes premières avec α mod α .

Un nombre α est dit premier avec α si $([\alpha]\ ,\ \alpha) = \mathfrak{o}$.

α premier avec α , β premier avec α $\Longrightarrow$ $\alpha\beta$ premier avec α , car si $\mathfrak{p}|\alpha$ et $\mathfrak{p}|[\alpha\beta]$, $\mathfrak{p}|[\alpha]\ [\beta]$, d'où $\mathfrak{p}|[\alpha]$ ou $\mathfrak{p}|[\beta]$ ce qui est contraire à l'hypothèse

α premier avec α , $\beta = \alpha \pmod{\alpha}$ $\Longrightarrow$ β premier avec α , car si $\mathfrak{p}|\alpha$, $\mathfrak{p}|[\beta]$, comme $\alpha|[\beta - \alpha]$, $\beta - \alpha \in \alpha \subseteq \mathfrak{p}$ $\Longrightarrow$ $\alpha \in \mathfrak{p}$ $\Longrightarrow$ $\mathfrak{p}|[\alpha]$ contraire à l'hypothèse.

Une classe mod α sera dite première avec α $\Longleftrightarrow$ tous ses éléments sont premiers avec α .

α premier avec α $\Longleftrightarrow$ $\exists\ \beta$, $\alpha\beta = 1 \pmod{\alpha}$.

En effet : $([\alpha]\ ,\ \alpha) = \mathfrak{o}$ $\Longrightarrow$ $\exists\ \lambda \in [\alpha]$, $\mu \in \alpha$, $\lambda + \mu = 1$, mais $\lambda \in [\alpha]$ $\Longleftrightarrow$ $\lambda = \beta\alpha$, β entier, donc $\beta\alpha = 1 - \mu$ $\Longrightarrow$ $\beta\alpha = 1 \pmod{\alpha}$.

Réciproquement si $\alpha\beta = 1 \pmod{\alpha}$, $\alpha\beta = 1 + \mu$, $\mu \in \alpha$ $\Longrightarrow$ $1 \in ([\alpha]\ ,\ \alpha)$ $\Longrightarrow$ $([\alpha]\ ,\ \alpha) = [1] = \mathfrak{o}$.

Il résulte de ce qui précède que les classes mod α premières avec α forment un groupe multiplicatif $\mathfrak{G}_\alpha$.

On montre aisément que l'ordre $\varphi(\alpha)$ du groupe $\mathfrak{G}_\alpha$ est égal à :

$$\varphi(\alpha) = N\alpha \prod_{\mathfrak{p}|\alpha} (1 - 1/N\mathfrak{p})\ .$$

(Pour cela il suffit d'établir la formule de récurrence

$$N\alpha = \sum_{\mathfrak{d}|\alpha} \varphi(\mathfrak{d})$$

mais si l'on considère le nombre de classes mod α telles que $([\alpha]\ ,\ \alpha) = \mathfrak{d}$ où $\mathfrak{d}|\alpha$ et où α est un représentant quelconque de la classe, on voit que leur nombre est précisément $\varphi(\frac{\alpha}{\mathfrak{d}})$ et réciproquement à tout α correspond un idéal $\mathfrak{d}|\alpha$.)

3. Ordre d'un élément de $\mathcal{S}_\alpha$, fonction $I(\alpha, \alpha)$.

Nous appelons ordre d'un élément A de $\mathcal{S}_\alpha$ l'ordre du groupe cyclique engendré par les puissances successives de A. Cet ordre divise donc $\varphi(\alpha)$.

Nous définissons alors une fonction $I(\alpha, \alpha)$ de l'idéal α et de l'entier α.

$I(\alpha, \alpha) = 0$ si α n'est pas premier avec α

$=$ Ordre de A dans $\mathcal{S}_\alpha$, si α est premier avec α et appartient à la classe A de $\mathcal{S}_\alpha$.

On a alors :

$\alpha^k = 1 \pmod{\alpha} \iff \exists\ h$ entier ≥ 0, $k = hI(\alpha, \alpha)$.

En effet, si $\alpha^k = 1 \pmod{\alpha}$ et si $k = 0$, on a bien $k = 0 \times I(\alpha, \alpha)$; si $k > 0$, $\alpha \times \alpha^{k-1} = 1 \pmod{\alpha} \Rightarrow \alpha$ premier avec $\alpha \Rightarrow I(\alpha, \alpha) > 0$; mais si $\alpha \in A$ classe de $\mathcal{S}_\alpha$; $\alpha^k \in A^k$ et par conséquent $1 \in A^k$, A^k est la classe unité de $\mathcal{S}_\alpha$, on a bien alors $k = h \times I(\alpha, \alpha)$, $h \geq 0$.

Réciproquement si $k = hI(\alpha, \alpha)$ ou bien $I(\alpha, \alpha) = 0 \Rightarrow k = 0$, $\alpha^0 = 1 \Rightarrow \alpha^k = 1 \pmod{\alpha}$, ou bien $I(\alpha, \alpha) > 0$ et α premier avec α si A est la classe de α, $\alpha^k \in A^k = (A^{I(\alpha,\alpha)})^h$ classe unité donc $\alpha^k = 1 \pmod{\alpha}$.

4. Calcul de $I(\alpha, \alpha)$.

Il suffit de le faire pour les idéaux α de la forme p^k, k entier positif, en effet :

si $(\alpha, b) = \mathfrak{d}$ alors : $I(\alpha b, \alpha) = I(\alpha, \alpha) \wedge I(b, \alpha)$ (le signe $\wedge$ désignant le p. p. c. m.) et plus généralement $\forall\ \alpha$ et b, $I(\alpha \cap b) = I(\alpha, \alpha) \wedge I(b, \alpha)$.

a. Soit δ un entier algébrique alors $\delta \in \alpha \cap b \iff \delta \in \alpha$ et $\delta \in b$.

b. Soit k un entier quelconque ≥ 0, posons $\delta = \alpha^k - 1$, alors :
$\delta \in \alpha \cap b \iff \alpha^k = 1 \pmod{\alpha \cap b} \iff \exists\ h$ entier ≥ 0, $k = hI(\alpha \cap b, \alpha)$.

De même

$\delta \in \alpha$

$\iff \exists\ h_1$, $k = h_1 I(\alpha, \alpha)$

$\delta \in b$

et $\exists\ h_2$, $k = h_2 I(b, \alpha) \iff \exists\ h'$, $k = h' I(\alpha, \alpha) \wedge I(b, \alpha)$,

Finalement tout multiple de $I(\alpha \cap b, \alpha)$ est multiple de $I(\alpha, \alpha) \wedge I(b, \alpha)$ et réciproquement, on a donc bien égalité entre ces deux nombres.

Nous sommes donc ramenés au calcul, pour $k \geq 1$, de $I(p^k, \alpha)$ nous supposons que $(p^k, [\alpha]) = \mathfrak{o}$, i.e. que $\mathfrak{p} \nmid \alpha$.

Nous posons $Np = p^f$, $[p] = \mathfrak{p}^g \mathfrak{q}$, $\mathfrak{p} \nmid \mathfrak{q}$ ($g = 1$, si $\mathfrak{p} \nmid \Delta$ le discriminant du corps).

On a : $1 \leq fg \leq n$ (n degré de l'extension K).

a. Soit ξ tel que $p^k | \xi$, $k \geq 1$, alors $(1 + \xi)^s = 1 + s\xi \pmod{p^{k+1}}$

en effet :

$$(1 + \xi)^s = 1 + s\xi + \sum_{\sigma=2}^{s} C_s^\sigma \xi^\sigma$$

or

$$p^k | \xi \implies p^{2k} | \xi^\sigma, \ \forall\ \sigma \geq 2 \text{ et } k \geq 1 \implies k + 1 \leq 2k \implies p^{k+1} | p^{2k} .$$

b. Soit ξ tel que $p^k | \xi$, $k \geq 1$.

Supposons soit $p > g + 1$, soit $k > g$ ($p > g + 1$ sera vrai pour tout p sauf pour un nombre fini) alors $(1 + \xi)^p = 1 + p\xi \pmod{p^{k+g+1}}$.

En effet si $p > g$,

$$(1 + \xi)^p = \sum_{\sigma=0}^{g+1} C_p^\sigma \xi^\sigma + \sum_{\sigma > g+1} C_p^\sigma \xi^\sigma$$

$$p^{k+g+1} | p^{k(g+2)} \ | \xi^{g+2} | \xi^\sigma , \ \forall\ \sigma > g + 1$$

car : $k + g + 1 \leq k(g + 2)$, donc :

$$(1 + \xi)^p = \sum_{\sigma=0}^{g+1} C_p^\sigma \xi^\sigma \pmod{p^{k+g+1}}$$

mais $C_p^\sigma = \dfrac{p(p-1) \cdots (p-\sigma+1)}{\sigma!}$ si $\sigma = 2, \cdots, g+1$, $\sigma!$ est premier avec p, donc

$$\sigma! \mid (p-1) \cdots (p-\sigma+1) \implies p | C_p^\sigma \implies p\xi^2 | C_p^\sigma \xi^\sigma \implies p^{k+1+g} | p^{2k+g} | C_p^\sigma \xi^\sigma .$$

C. Q. F. D.

Si maintenant $k > g$, alors

$$(1 + \xi)^p = 1 + p\xi + \xi^2 \times \text{ entier et } p^{k+g+1} | p^{2k} | \xi^2 .$$

C. Q. F. D.

c. Si nous supposons alors $p > g + 1$, posons $k(p, \alpha) = \max k$ tels que $p^k | \alpha^{I(p,\alpha)} - 1$ (en supposant que α n'est pas racine de l'unité).

On a alors :

$$I(p^k, \alpha) = p^{\max\left(0,\, 1 + \left[\frac{k - k(p,\alpha) - 1}{g}\right]\right)} I(p, \alpha) .$$

En effet, on a : $\alpha^{I(p,\alpha)} = 1 + \xi$ avec $p^{k(p,\alpha)} | \xi$, $p^{1+k(p,\alpha)} \nmid \xi$. Si $K = 1 + k(p , \alpha)$, $I(p^K , \alpha)$ est donc différent de $I(p^{K-1} , \alpha) = I(p , \alpha)$. Mais

$$\alpha^h = 1 \pmod{p^K} \implies \alpha^h = 1 \pmod{p^{K-1}}$$

donc : $I(p^K , \alpha) = sI(p^{K-1} , \alpha)$ où s est un entier > 1 (car $p \nmid \alpha$).

Pour que $(1 + \xi)^s = 1 \pmod{p^K}$, $s\xi = 0 \pmod{p^K}$ d'après (a)

$$\iff p|s \implies Np|Ns \implies p^f|s^n \implies p|s$$

on a donc nécessairement $I(p^K , \alpha) = tpI(p^{K-1} , \alpha)$ mais nous devons prendre t minimum. Or pour $t = 1$ en vertu de (a)

$$p\xi = 0 \pmod{p^K} \implies (1 + \xi)^p = 1 \pmod{p^K} .$$

Donc on a $I(p^K , \alpha) = pI(p^{K-1} , \alpha)$.

Mais comme d'après (b)

$$(1 + \xi)^p = 1 + p\xi \pmod{p^{K+g}}$$

et que :

$$p^{K-1+g} | p\xi \quad \text{et} \quad p^{K+g} \nmid p\xi$$

on aura :

$$I(p^{K+g-1} , \alpha) = I(p^K , \alpha) = pI(p , \alpha) \quad \text{et} \quad I(p^{K+g} , \alpha) \neq I(p^K , \alpha) .$$

De manière générale si $I(p^{K+tg} , \alpha) \neq I(p^{K+tg-1} , \alpha)$, on montrerait de la même manière que : $I(p^k , \alpha) = pI(p^{K+tg-1} , \alpha)$ si $K + tg \leqslant k < K + (t + 1) g$, et que $I(p^{K+(t+1)g} , \alpha) \neq pI(p^{K+tg-1} , \alpha)$.

On a donc, si $t \geqslant 0$ et $K + tg \leqslant k < K + (t + 1) g$, $I(p^k , \alpha) = p^{(t+1)} I(p , \alpha)$ mais alors :

$$(t + 1) \leqslant \frac{k + g - K}{g} < (t + 1) + 1$$

d'où la formule annoncée.

d. Si $p \leqslant g + 1$ nous pourrons faire un raisonnement analogue si $k(p , \alpha) > g$. Mais de manière générale :

Si nous posons $k_1(p , \alpha) = \max k$ tels que $p^k | \alpha^{I(p^{g+1},\alpha)} - 1$ (en supposant toujours que α n'est pas racine de l'unité) on aura $k_1(p , \alpha) > g$, donc, $\forall\ k \geqslant g + 1$,

$$I(p^k , \alpha) = p^{\max(0,\, 1+[\frac{k-k_1(p,\alpha)}{g}])} I(p^{g+1} , \alpha)$$

et par ailleurs

$$I(p^{g+1} , \alpha) = p^h I(p , \alpha) \quad \text{avec} \quad 0 \leqslant h \leqslant g .$$

e. Si α est racine de l'unité et $p \nmid \alpha$ alors évidemment dès que k est assez grand on a : $I(p^k , \alpha) = m$ si α est racine primitive m-ième de l'unité.

5. Théorèmes sur les équations associées.

1° THÉORÈME. - Soit une équation ε : $\lambda\alpha^x - \mu\beta^y = \nu$ avec les hypothèses faites dans le paragraphe 1. Soient (x_0 , y_0) un couple d'entiers ≥ 0.

Nous considérons l'ensemble des couples (x , y) avec $x > x_0$, $y > y_0$ tels qu'il existe une équation ε' associée à ε admettant (x_0 , y_0) et (x , y) comme solution, cet ensemble sera noté $E(\lambda , \mu , \alpha , \beta)$ (il ne dépend évidemment pas de ν).

Alors ou bien $E(\lambda , \mu , \alpha , \beta)$ est vide

ou bien $\exists\ (x_1 , y_1) \in E(\lambda , \mu , \alpha , \beta)$ tel que

$$\forall\ (x , y) \in E(\lambda , \mu , \alpha , \beta) \begin{cases} x_1 - x_0 \mid x - x_0 \\ y_1 - y_0 \mid y - y_0 \end{cases}$$

2° COROLLAIRE. - Si L , M , A , B , N sont des nombres entiers > 0, $(A , B) = 1$ et si (x_1 , y_1) , (x_2 , y_2) , (x_3 , y_3) sont trois solutions consécutives (c'est-à-dire telles que $x_1 < x_2 < x_3$, d'où $y_1 < y_2 < y_3$ et telles qu'il n'existe pas de solution avec $x_1 < x < x_2$ ou $x_2 < x < x_3$), de l'équation $LA^x - MB^y = N$, on a alors : $x_2 - x_1 \mid x_3 - x_1$ et $y_2 - y_1 \mid y_3 - y_1$.

En effet nous prenons $K = Q$, les équations associées à $LA^x - MB^y = N$ admettant la solution (x_1 , y_1) sont de la forme $\pm LA^x \pm MB^y = \pm LA^{x_1} \pm MB^{y_1}$ (car $\pm$ sont les seules unités de Q) soit $LA^x + MB^y = LA^{x_1} + MB^{y_1}$ et $LA^x - MB^y = LA^{x_1} - MB^{y_1}$ $(= N)$.

Mais si $x > x_1$, $y > y_1$, $LA^x + MB^y > LA^{x_1} + MB^{y_1}$.

Dans ce cas, l'ensemble $E(L , M , A , B)$ est réduit aux seules solutions de l'équation donnée. Le corollaire suit alors immédiatement.

En fait, il fallait supposer $(LA^x , MB^y) = (L , M)$, $\forall\ x \geq 0$, $y \geq 0$, mais l'équation a la forme

$$LA^x - MB^y = LA^{x_1} - MB^{y_1}$$

d'où si $x > x_1$, $y > y_1$

$$LA^{x_1}(A^{x-x_1} - 1) = MB^{y_1}(B^{y-y_1} - 1)$$

et en posant

$$L' = \frac{LA^{x_1}}{(LA^{x_1}, MB^{y_1})} \qquad M' = \frac{MB^{y_1}}{(LA^{x_1}, MB^{y_1})}$$

les solutions (x , y) de $\mathcal{E}$ avec $x \geqslant x_1$, $y \geqslant y_1$ correspondent biunivoquement aux solutions (u , v) avec $u \geqslant 0$, $v \geqslant 0$ de $\mathcal{E}'$, $L'A^u - M'B^v = L' - M'$ par la correspondance $x = x_1 + u$, $y = y_1 + v$. Il suffit donc de montrer que l'on peut appliquer le théorème à $\mathcal{E}'$.

Or si $x_2 - x_1 = u_1$, $y_2 - y_1 = v_1$, $L'(A^{u_1} - 1) = M'(B^{v_1} - 1)$ si $p | (L'A^x , M'B^y)$, alors $p|A$ et M' ou $p|L'$ et B puisque $(A , B) = (L' , M') = 1$, mais $p|M' \implies p|L'(A^{u_1} - 1) \implies p|A^{u_1} - 1$ incompatible avec $p|A$.

La démonstration s'applique donc bien à $\mathcal{E}'$ puisque $(L'A^x , M'B^y) = (L' , M') = 1$, $\forall \quad x \geqslant 0$, $y \geqslant 0$.

3° Démonstration du théorème. - Nous posons : $(\lambda , \mu) = \mathfrak{d}$ et $[\lambda] = \mathfrak{a}\mathfrak{d}$, $[\mu] = \mathfrak{b}\mathfrak{d}$,

$$\mathfrak{a}' = \mathfrak{a}[\alpha^{x_0}] , \quad \mathfrak{b}' = \mathfrak{b}[\beta^{y_0}] .$$

Alors : $(\mathfrak{a}' , \mathfrak{b}') = \mathfrak{o}$ puisque $(\mathfrak{a}'\mathfrak{b} , \mathfrak{b}'\mathfrak{b}) = (\lambda\alpha^{x_0} , \mu\beta^{y_0}) = (\lambda , \mu) = \mathfrak{b}$.

Pour toute équation associée à $\mathcal{E}$ on aura $[\lambda'] = [\lambda]$, $[\mu'] = [\mu]$.

a. $(x_1 , y_1) \in E(\lambda , \mu , \alpha , \beta)$

$$\iff \exists \text{ un idéal } \mathfrak{c} \text{ tel que } \begin{cases} \mathfrak{c}\mathfrak{b}' = [\alpha^{x_1 - x_0} - 1] , & x_1 > x_0 \\ \mathfrak{c}\mathfrak{a}' = [\beta^{y_1 - y_0} - 1] , & y_1 > y_0 \end{cases}$$

En effet s'il existe une équation $\mathcal{E}'$: $\lambda'\alpha^x - \mu'\beta^y = \nu'$ associée à $\mathcal{E}$ admettant (x_0 , y_0) , (x_1 , y_1) pour solution avec $x_1 > x_0$, $y_1 > y_0$, on a :

$$\lambda'\alpha^{x_1} - \mu'\beta^{y_1} = \lambda'\alpha^{x_0} - \mu'\beta^{y_0}$$

soit

$$\lambda'\alpha^{x_0}(\alpha^{x_1 - x_0} - 1) = \mu'\beta^{y_0}(\beta^{y_1 - y_0} - 1) = \xi$$

soit

$$\mathfrak{a}'\mathfrak{b}[\alpha^{x_1 - x_0} - 1] = \mathfrak{b}'\mathfrak{b}[\beta^{y_1 - y_0} - 1] = [\xi]$$

alors $\mathfrak{b} | [\xi]$, $[\xi] = \mathfrak{A}\mathfrak{b}$, mais alors $\mathfrak{A} = \mathfrak{a}'[\alpha^{x_1 - x_0} - 1] \implies \mathfrak{a}' | \mathfrak{A}$.

De même $\mathfrak{b}' | \mathfrak{A}$, mais $(\mathfrak{a}' , \mathfrak{b}') = 1 \implies \mathfrak{a}'\mathfrak{b}' | \mathfrak{A}$ soit

$$\mathfrak{A} = \mathfrak{c}\mathfrak{a}'\mathfrak{b}' \text{ alors } \begin{cases} \mathfrak{c}\mathfrak{b}' = [\alpha^{x_1 - x_0} - 1] \\ \mathfrak{c}\mathfrak{a}' = [\beta^{y_1 - y_0} - 1] \end{cases}$$

C. Q. F. D.

Réciproquement si $\exists$ c tel que $\begin{cases} c\mathfrak{b}' = [\alpha^{x_1-x_0} - 1] \\ c\alpha' = [\beta^{y_1-y_0} - 1] \end{cases}$

on aura :

$$\mathfrak{b}c\alpha'\mathfrak{b}' = \mathfrak{b}\alpha'[\alpha^{x_1-x_0} - 1] = [\lambda(\alpha^{x_1} - \alpha^{x_0})]$$

et de même

$$\mathfrak{b}c\alpha'\mathfrak{b}' = [\mu(\beta^{y_1} - \beta^{y_0})] \quad .$$

D'où

$$[\lambda(\alpha^{x_1} - \alpha^{x_0})] = [\mu(\beta^{y_1} - \beta^{y_0})] \implies \lambda(\alpha^{x_1} - \alpha^{x_0}) = \varepsilon\mu(\beta^{y_1} - \beta^{y_0})$$

où ε est une unité.

Soit $\lambda\alpha^{x_1} = \varepsilon\mu\beta^{y_1} = \lambda\alpha^{x_0} - \varepsilon\mu\beta^{y_0} = \nu'$. L'équation $\lambda\alpha^{x} - \varepsilon\mu\beta^{y} = \nu'$ admet les solutions (x_0 , y_0) , (x_1 , y_1) et est associée à l'équation $\mathcal{E}$.

C. Q. F. D.

b. Si $\exists$ c tel que $\begin{cases} c\mathfrak{b}' = [\alpha^{u} - 1] \\ c\alpha' = [\beta^{v} - 1] \end{cases}$ alors il existe des suites infinies d'idéaux α_n et $\mathfrak{b}_n$ non nuls tels que :

$$\begin{cases} \alpha_n | c , \mathfrak{b}_n | c , \alpha_0 = \mathfrak{o} \\ \alpha'\mathfrak{b}_n = [\beta^{I(\alpha'\alpha_n, \beta)} - 1] \\ \mathfrak{b}'\alpha_{n+1} = [\alpha^{I(\mathfrak{b}'\mathfrak{b}_n, \alpha)} - 1] \end{cases}$$

En effet appelons

H_n l'hypothèse : $\alpha_0 , \mathfrak{b}_0 , \cdots , \alpha_{n-1} , \mathfrak{b}_{n-1} , \alpha_n$ existent, sont non nuls et $\alpha_n | c$.

K_n l'hypothèse : $\alpha_0 , \mathfrak{b}_0 , \cdots , \alpha_n , \mathfrak{b}_n$ existent sont non nuls et $\mathfrak{b}_n | c$.

Evidemment H_0 est vérifiée.

Montrons que $H_n \implies K_n \implies H_{n+1}$.

En effet si H_n est vraie :

$$\alpha_n | c \implies \alpha_n \alpha' | c\alpha' = [\beta^{v} - 1] \implies \beta^{v} = 1 \pmod{\alpha_n \alpha'}$$

comme $v > 0$, $([\beta] , \alpha_n \alpha') = \mathfrak{o}$.

Donc $I(\alpha_n \alpha' , \beta) > 0$ et $v = hI(\alpha_n \alpha' , \beta)$, $\beta^{I(\alpha_n\alpha', \beta)} - 1 \neq 0$ car $I(\alpha_n \alpha' , \beta) > 0$ et β n'est pas racine de l'unité.

De plus

$$\beta^{V} - 1 = \beta^{hI(\alpha_n\alpha',\beta)} - 1 = (\beta^{I(\alpha_n\alpha',\beta)} - 1)(\beta^{(h-1)I(\alpha_n\alpha',\beta)} + \dots 1)$$

donc

$$\beta^{I(\alpha_n\alpha',\beta)} - 1 \mid \beta^{V} - 1 \ .$$

D'autre part

$$\alpha' \mid [\beta^{I(\alpha_n\alpha',\beta)} - 1] \implies [\beta^{I(\alpha_n\alpha',\beta)} - 1] = b_n \alpha'$$

avec b_n non nul et

$$b_n \alpha' \mid [\beta^{V} - 1] = c\alpha' \implies b_n \mid c \implies K_n \ .$$

On montrerait de même que $K_n \implies H_{n+1}$.

c. Réciproquement s'il existe des suites α_n , b_n non nulles et un idéal e tels que :

$$\begin{cases} \alpha' b_n = [\beta^{I(\alpha'\alpha_n,\beta)} - 1] \\ b'\alpha_n = [\alpha^{I(b'b_n,\alpha)} - 1] \\ \\ \alpha_n \mid e \quad \text{et} \quad b_n \mid e \end{cases}$$

alors $\exists\ c \mid e$ tel que $\begin{cases} \alpha' c = [\beta^{I(\alpha' c,\beta)} - 1] \ , \quad I(\alpha' c \ , \ \beta) > 0 \\ b' c = [\alpha^{I(b' c,\alpha)} - 1] \ , \quad I(b' c \ , \ \alpha) > 0 \end{cases}$

En effet : $\alpha' b_n$ n'est pas nul, donc

$$\beta^{I(\alpha'\alpha_n,\beta)} - 1 \neq 0 \implies I(\alpha'\alpha_n \ , \ \beta) \neq 0 \implies \alpha'\alpha_n \text{ est premier avec } \beta$$

et

$$\beta^{I(\alpha'\alpha_n,\beta)} = 1 \pmod{\alpha'\alpha_n} \implies \alpha'\alpha_n \mid [\beta^{I(\alpha'\alpha_n,\beta)} - 1] = \alpha' b_n \implies \alpha_n \mid b_n$$

de même $b_n \mid \alpha_{n+1}$.

On a donc $\alpha_0 \mid \alpha_1 \mid \dots \mid \alpha_n \mid \dots \mid e$.

La suite α_n est donc constante à partir d'un certain rang : i. e. $\alpha_n = \alpha_{n_0}$ $\forall\ n \geqslant n_0$.

Si $c = \alpha_{n_0}$, comme $c = \alpha_{n_0} \mid b_{n_0} \mid \alpha_{n_0+1} = c$, $b_{n_0} = c$.

D'où

$$\begin{cases} \alpha' c = [\beta^{I(\alpha' c, \beta)} - 1] \\ b' c = [\alpha^{I(b' c, \alpha)} - 1] \end{cases} \quad \text{et} \quad c | c$$

C. Q. F. D.

d. Démonstration. - S'il existe une solution $(x_1 , y_1) \in E(\lambda , \mu , \alpha , \beta)$, alors $\exists\ \varepsilon_1$ telle que ε_1, associée à ε, ε_1, admet une solution, alors les suites α_n et b_n existent, et $\alpha_n | c_1$, $b_n | c_1$ (c_1 correspondant à ε_1) d'après (b) et (a).

Mais alors $\exists\ c_2 | c_1$ tel que $\begin{cases} \alpha' c_2 = [\beta^{I(\alpha' c_2, \beta)} - 1] \\ b' c_2 = [\alpha^{I(b' c_2, \alpha)} - 1] \end{cases}$ d'après (c).

Donc d'après (a), $\exists\ \varepsilon_2$ correspondant à c_2 de solution (x_2 , y_2) avec

$$\begin{cases} x_2 - x_0 = I(\alpha' c_2 , \beta) \\ y_2 - y_0 = I(b' c_2 , \alpha) \end{cases}$$

Mais alors

$$c_2 | c_1 \implies \alpha' c_2 | \alpha c_1 \implies I(\alpha' c_2 , \beta) | I(\alpha' c_1 , \beta)$$

(car $\beta^{I(\alpha' c_1, \beta)} = 1 \pmod{\alpha' c_1} \implies \beta^{I(\alpha' c_1, \beta)} = 1 \pmod{\alpha' c_2}$).

D'autre part comme $[\beta^{x_1 - x_0} - 1] = \alpha' c_1$,

$$\beta^{x_1 - x_0} = 1 \pmod{\alpha' c_1} \implies I(\alpha' c_1 , \beta) | x_1 - x_0$$

et finalement

$$x_2 - x_0 | x_1 - x_0$$

C. Q. F. D.

(Car c_2 est indépendant de l'équation ε_1 dont on est parti, puisque, les α_n , b_n le sont par leur procédé de construction.)

De même

$$y_2 - y_0 | y_1 - y_0 .$$

6. Cas particuliers où λ et ν sont racines de l'unité.

THÉORÈME. - Si λ et ν sont racines de l'unité, l'équation $\lambda \alpha^x - \mu \beta^y = \nu$ n'a pas de solution (x , y) avec $y \geq C(\alpha , \beta , \lambda , \mu , \nu)$ où C est calculable effectivement

En effet posons $[\beta] = p_1^{b_1} \cdots p_r^{b_r}$, $b_i \geqslant 1$

$$Np_i = p_i^{f_i} \qquad [p_i]\ p_i^{g_i}\ q_i \qquad (p_i \nmid q_i)$$

λ et ν étant racines de l'unité, $\exists$ m_1 et m_2 , $\lambda^{m_1} = 1$, $\nu^{m_2} = 1$, soit $m = m_1 \wedge m_2$.

Si $\lambda\alpha^x - \mu\beta^y = \nu$, on a :

$$\lambda\alpha^x = \nu \pmod{[\beta^y]}$$

soit encore

$$\alpha^{mx} = 1 \pmod{[\beta^y]} .$$

D'où

$$mx = hI([\beta^y] , \alpha) , \quad h \text{ entier } \geqslant 0$$

- ou bien $x = 0$, d'où

$$\mu\beta^y = \lambda - \nu \implies y \leqslant y_0 \frac{\operatorname{Log}\left|\frac{\lambda - \nu}{\mu}\right|}{\operatorname{Log}|\beta|} = \text{Cte effectivement calculable}$$

- ou bien $x \neq 0 \implies x \geqslant \frac{1}{m} I([\beta^y] , \alpha)$.

Or :

$$I([\beta^y] , \alpha) = \bigwedge_{i=1}^{r} I(p_i^{yb_i} , \alpha) .$$

Dès que $y \geqslant g_i + 1$, $yb_i \geqslant g_{i+1}$.

Donc

$$I([\beta^y] , \alpha) = \bigwedge_{i=1}^{r} p_i^{\max(0,\, 1+[(yb_i - k_1(p_i,\alpha)-1)/g_i])}\, I(p_i^{g_i+1} , \alpha) .$$

D'où

$$I([\beta^y] , \alpha) \geqslant \max p_i^{\max(0,\, 1+[(yb_i - k_1(p_i,\alpha)-1/g_i])}$$

p_i étant premier $p_i \geqslant 2$, $\forall$ i , $b_i \geqslant 1$.

Si $g = \min g_i$, on a donc :

$$I([\beta^y] , \alpha) \geqslant 2^{\max(0,\, 1+[(y - k_1(p_{i_0})\alpha)-1)/g_i]}$$

or

$$1 + \left[\frac{y - k_1 - 1}{g}\right] > \frac{y - k_1 - 1}{g}$$

On peut donc écrire finalement $x \geqslant \frac{C_1}{m} 2^{y/g}$ où C_1 est une constante effectivement calculable en fonction de α , β

$$C_1 = \min_i 2^{-(k_1(p_i,\alpha)-1)/\min_i g_i}$$

$C_2 = C_1/m$ est calculable à partir de α , β , λ , ν et $x \geqslant C_2\, 2^{y/g}$.

Mais on a $|\alpha| > 1$, $|\beta| > 1$

$$|\lambda\alpha^x| = |\alpha|^x \geqslant |\alpha|^{C_2 2^{y/g}}$$

or

$$|\lambda\alpha^x| = |\mu\beta^y + \nu| \leqslant |\mu|\ |\beta|^y + .1 \quad .$$

Mais $|\mu|\ |\beta|^y \to \infty$ quand $y \to \infty$, donc $y > y_1$ (calculable à partir de μ et β , $y_1 = -\frac{\mathrm{Log}|\mu|}{\mathrm{Log}|\beta|}$) $\Longrightarrow$ $|\mu|\ |\beta|^y > 1 \Longrightarrow |\mu|\ |\beta|^y + 1 < 2|\mu|\ |\beta|^y$.

D'où $|\alpha|^{C_2 2^{y/g}} < 2|\mu|\ |\beta|^y$ si $y > \max(y_0 , y_1)$,

$$C_2 \times 2^{y/g} < y\,\frac{\mathrm{Log}|\beta|}{\mathrm{Log}|\alpha|} + \frac{\mathrm{Log}\, 2|\mu|}{\mathrm{Log}|\alpha|}$$

quand $y \to \infty$, $2^{y/g}/y \to \infty$, donc dès que

$$y > y_2 \Longrightarrow C_2 \times 2^{y/g} \geqslant y\frac{\mathrm{Log}|\beta|}{\mathrm{Log}|\alpha|} + \frac{\mathrm{Log}\, 2|\mu|}{\mathrm{Log}|\alpha|}$$

et y_2 est calculable.

Finalement si $C = \max(y_0 , y_1 , y_2)$, $y < C$, et C est calculable.

Remarque. - Les résultats de GEL'FAND ou, dans le cas des nombres entiers, de MAHLER sont plus généraux, mais ils ne prouvent pas que la constante $C(\alpha , \beta , \lambda , \mu , \nu)$ soit calculable.