Astérisque

PIERRE LIARDET

Sur une conjecture de Serge Lang

Astérisque, tome 24-25 (1975), p. 187-210

<http://www.numdam.org/item?id=AST_1975__24-25__187_0>

Société Mathématique de France
Astérisque 24-25 (1975)

SUR UNE CONJECTURE DE SERGE LANG

par

Pierre LIARDET

-:-:-:-

Le but de ce qui suit est de démontrer le théorème suivant conjecturé par S. Lang [4] :

THÉORÈME 1. - Soit Γ_o un sous-groupe de type fini du groupe multiplicatif du corps des nombres comples $\mathbb{C}$. Soit Γ le groupe multiplicatif des nombres complexes dont une puissance entière non nulle est dans Γ_o . Si $P(X, Y)$ est un polynôme de deux variables à coefficients complexes et si pour une infinité de α et β dans Γ on a $P(\alpha, \beta) = 0$, alors il existe des entiers (rationnels) non nuls u, v, des éléments a, b de Γ tels que identiquement on ait :

$$P(ax^u , bx^v) \equiv_x 0 \quad .$$

La première partie est consacrée à la démonstration de ce théorème en distinguant plusieurs cas ; la seconde partie donne quelques conséquences.

Supposons $\Gamma_o \subset K^*$ et $P(X,Y)$ dans $K[X,Y]$, où K est une extension de type fini de $\mathbb{Q}$ (dans $\mathbb{C}$) et posons $\Gamma(K) = \Gamma \cap K$. Pour tout $\alpha \in \Gamma$, $M(\alpha)$ désignera le plus petit entier $M > 0$ tel que $\alpha^M \in \Gamma(K)$. Il est clair que si n est un entier tel que $\alpha^n \in \Gamma(K)$, alors n est un multiple de $M(\alpha)$. Pour tout $a \in K$ et tout entier $m > 0$, nous poserons :

$$D_K(a,m) = \text{Mini}\{[K(\alpha):K],\ \alpha^m = a\}$$

et pour tout $\alpha \in \Gamma$, nous poserons pour simplifier :

$$D_K(\alpha) = D_K(\alpha^{M(\alpha)},\ M(\alpha)).$$

Enfin, pour θ algébrique sur K, $d_K(\theta) = [K(\theta) : K]$. Par ailleurs Γ_o étant supposé de type fini, il en est de même de $\Gamma(K)$. En effet, lorsque K est un corps de nombres, cela résulte du théorème de Dirichlet, sinon cela résulte par exemple du lemme 3 ci-dessous et d'une récurrence sur le degré de transcendance de K sur $\mathbb{Q}$. Alors, pour tout entier $N > 0$, il est loisible de déterminer une extension algébrique finie L de K telle que :

$$(1) \qquad (\forall \gamma)\ (\gamma \in \Gamma \text{ et } \gamma^N \in \Gamma(K) \Rightarrow \gamma \in \Gamma(L)).$$

Nous noterons $K_{(N)}$ la plus petite extension L de K vérifiant (1).

Soit alors $\mathcal{A}$ (resp. $\mathcal{B}$) l'ensemble des $\alpha \in \Gamma$ (resp. $\beta \in \Gamma$) pour lesquels il existe $\beta \in \Gamma$ (resp. $\alpha \in \Gamma$) tels que $P(\alpha,\beta) = 0$ avec $P(\alpha,Y) \neq 0$ (resp. $P(X,\beta) \neq 0$). Par hypothèse $\mathcal{A}$ et $\mathcal{B}$ sont infinis (si l'un de ces ensembles est fini, l'autre étant infini, l'identité du théorème 1 est évidente avec l'un des entier u, v nul) ; P est donc de degré non nul en X et Y, degrés que nous noterons respectivement n_X et n_Y. Dans la suite, nous identifierons K avec un sous-corps de $\mathbb{C}$ et désignerons par $\mathbf{U}$ le sous-groupe de $\mathbb{C}^*$ des racines de l'unité.

La démonstration du théorème 1 pour $\Gamma_o \subset K$ et $P(X,Y)$ dans $K[X,Y]$ se décompose ainsi :

1) Si $d_K(\mathcal{A})$ est borné, par le lemme 1, on déduira $M(\mathcal{A})$ et $M(\mathcal{B})$ bornés et l'on se ramène au théorème de S. Lang [3] à savoir :

THÉORÈME 2. - Avec les notations du théorème 1, si pour une infinité de α et β dans Γ_o on a $P(\alpha,\beta) = 0$, alors $P(ax^u, bx^v) \equiv_x 0$ pour des entiers non nuls u, v et des éléments a, b de Γ_o.

Pour démontrer ce théorème, S. Lang utilise le théorème diophantien de C. Siegel sur les courbes ayant une infinité de points définis dans un anneau de type fini sur $\mathbb{Z}$; nous donnerons ici une autre démonstration en faisant directement usage du théorème de Thue-Siegel-Roth par les développements de Puiseux.

2) Si $\Gamma_o = \{1\}$; alors $\Gamma = \mathbf{U}$; on montrera alors le théorème 3, qui assure les conclusions du théorème 1 lorsque $P(\alpha,\beta) = 0$, α, β dans $\mathbf{U}$, avec $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq C$, la constante C ne dépendant que du corps K, et des degrés n_X, n_Y de P en X et Y ; cette dépendance de C joue un rôle essentiel dans les autres cas.

3) Si $D_K(\mathcal{A})$ borné ; on montre que le théorème 1 se ramène au cas où $\mathcal{A} \subset K\mathbf{U}$, quitte à remplacer K par une extension algébrique finie ; le lemme 4 sur les degrés montre alors que $\mathcal{B}^{c_o} \subset K\mathbf{U}$ pour un entier c_o, et l'on se ramène au cas 2.

4) Si $D_K(\mathcal{A})$ non borné ; pour tout $\alpha \in \mathcal{A}$ et tout $\beta \in \mathcal{B}$ tels que $P(\alpha, \beta) = 0$, on adjoint à K les racines $M(\alpha)\,M(\beta)$-ièmes de l'unité ; soit E le corps ainsi obtenu. Si $E(\alpha) \cap E(\beta) = H$ est de degré d sur E, la théorie de Kummer permet d'établir une relation :

$$\alpha^v = \theta \beta^u ,$$

pour des entiers u, v dans $0(\sqrt{d})$ avec $\theta \in E$. Si H reste de degré borné sur E, le lemme 4 permet de montrer que $\mathcal{A} \cup \mathcal{B} \subset F\mathbf{U}$ pour une extension algébrique finie F de K et l'on se ramène au théorème 3 ; dans le cas contraire, la conclusion du théorème 1 résulte alors du théorème de Bezout sur le nombre de points dans l'intersection de deux courbes algébriques.

I. - DÉMONSTRATION DU THÉORÈME 1. - Nous supposons $\Gamma_o \subset K^*$ et $P(X, Y)$ à coefficients dans K pour une extension K de $\mathbb{Q}$, de type fini.

1) Supposons $d_K(\mathcal{A})$ borné ; il en est de même de $M(\mathcal{A})$. En fait, si $\alpha \in \Gamma$ est de degré s sur K, alors

$$N(\alpha) = \zeta \alpha^s$$

où $N(\alpha)$ désigne la norme de α sur K et ζ une racine de l'unité dans $K(\alpha)$, de degré au plus s sur K. Soit :

$$\psi_K(s) = \text{p. p. c. m. } \{M(\omega),\ \omega \text{ racine de l'unité et } [K(\omega) : K] \leq s\}.$$

$\psi_K(s)$ est évidemment finie et

$$[N(\alpha)]^{\psi_K(s)} = \zeta^{\psi_K(s)}\, \alpha^{s\,\psi_K(s)} \in K ,$$

avec $\zeta^{\psi_K(s)} \in K$ ce qui assure le

LEMME 1. - Si α est un élément de Γ de degré s sur K, $s\,\psi_K(s)$ est multiple (entier) de $M(\alpha)$.

$M(\mathfrak{A})$ est donc borné, de même $M(\mathfrak{B})$ est borné. Il existe alors une borne multiplicative de ces ensembles i. e. il existe un entier $N>0$, tel que

$$\mathfrak{A}^N \cup \mathfrak{B}^N \subset \Gamma(K) \ .$$

On est ainsi ramené à la démonstration du théorème 1 lorsque $\mathfrak{A}$ et $\mathfrak{B}$ sont dans Γ_o en remplaçant K par $K_{(N)}$, Γ_o par $\Gamma(K_{(N)})$. Ce cas est couvert par le théorème 2 de S. Lang.

Démonstration du théorème 2. - Nous dirons que le théorème est vrai pour un corps K s'il est vrai lorsqu'on suppose $\Gamma_o \subset K^*$ et $P(X,Y)$ à coefficients dans K.

a) Démontrons le théorème pour un corps de nombres K. Soit $\mathfrak{M}$ un ensemble de valeurs absolues sur K vérifiant la formule du produit :

$$x \in K^* \Rightarrow \overline{\prod_{v \in \mathfrak{M}}} |x|_v^{n_v} = 1 \ .$$

Nous poserons $\|x\|_v = |x|_v^{n_v}$ et désignerons par h la hauteur absolue sur K, définie comme dans [3] ; en particulier, lorsque $x \in K$, on a

$$h(x) = \overline{\prod_{v \in \mathfrak{M}}} \operatorname{Max}\{1, \|x\|_v\} \ .$$

Γ_o étant de type fini, il existe une partie finie non vide S de $\mathfrak{M}$ telle que pour tout $\gamma \in \Gamma_o$ et toute valeur absolue $v \in \mathfrak{M}-S$, on ait $|\gamma|_v = 1$. Soit alors $(\alpha_\nu)_{\nu \in \mathbb{N}}$ une suite d'éléments tous distincts de $\mathfrak{A}$ et $(\beta_\nu)_{\nu \in \mathbb{N}}$ une suite de $\mathfrak{B}$ telle que $P(\alpha_\nu, \beta_\nu) = 0$ pour tout entier ν. On peut alors trouver une partie

non vide T de S et des constantes $A_w > 0$ pour chaque $w \in S-T$ telles que

(i) $\forall v \in T$, $\lim_{\nu \to \infty} |\alpha_\nu|_v = +\infty$;

(ii) $\forall w \in S-T$, $\forall \nu \in \mathbb{N}$, $|\alpha_\nu|_w \leq A_w$.

Nous pouvons supposer, sans nuire à la généralité, que $P(X,Y)$ est absolument irréductible à coefficients dans K , quitte à remplacer $P(X,Y)$ par un de ses facteurs absolument irréductibles convenable à coefficients dans une extension algébrique finie de K . D'après le théorème de Puiseux [2], quitte à remplacer $(\alpha_\nu)_\nu$ par une suite extraite, on peut supposer qu'il existe une extension algébrique finie L de K , une racine e-ième de α_ν notée $\alpha_\nu^{1/e}$, (e entier $\leq n_Y$) , une suite $(a_\mu)_\mu$ d'éléments de L et une constante $C_v > 0$ pour chaque $v \in S$ que l'on prolongera à L d'une manière quelconque, tels que

$$|\alpha_\nu|_v > C_v^e \Rightarrow \beta_\nu = \sum_{\mu \geq r}^{\infty} a_\mu \alpha_\nu^{-\mu/e} ,$$

la série étant convergente au sens de la topologie définie par $|\ |_v$. Nous supposerons $a_r \neq 0$. Pour deux applications réelles φ, ψ définies sur un ensemble E nous utiliserons la notation standard $\varphi(\nu) \ll \psi(\nu)$ qui assure l'existence d'une constante $C > 0$ telle que $\varphi(\nu) \leq C\, \psi(\nu)$ pour tout $\nu \in E$. On a alors pour tout $v \in T$:

$$|\beta_\nu - a_r \alpha_\nu^{-r/e}|_v \ll |\alpha_\nu|_v^{-\frac{r+1}{e}} ,$$

d'où :

$$|\alpha_\nu^r \beta_\nu^e - a_r^e|_v \ll |\alpha\ |_v^{-1/e} .$$

Posons $a = a_r^e$, $\theta_\nu = \alpha_\nu^r \beta_\nu^e$; on obtient :

$$\prod_{v\in S} \mathrm{Mini}\{1, \|\theta_\nu - a\|_v\} \leq \prod_{v\in T} \mathrm{Mini}\{1, \|\theta_\nu - a\|_v\}$$

$$\ll \Big(\prod_{\nu\in T} \mathrm{Max}\{1, \|\alpha_\nu\|_v\}\Big)^{-\frac{1}{e}} \leq \Big(\prod_{w\in S-T} A_w\Big).(h(\alpha_\nu))^{-\frac{1}{e}}.$$

Par ailleurs, d'après la théorie de la hauteur, on a le :

LEMME 2. - *Soit* $f(X) = d_o X^n + \ldots + d_n$ *un polynôme à coefficients dans* K, $d_o \neq 0$, $\theta_1, \ldots, \theta_n$ *les racines (distinctes ou pas) de* f. *Alors* :

$$\prod_{i=1}^{n} h(\theta_i) \leq C_K^n\, h(f) ,$$

où C_K *est une constante ne dépendant que de* $\mathcal{M}$ *et*

$$h(f) = \prod_{v\in\mathcal{M}} \mathrm{Max}\{\|d_o\|_v, \ldots, \|d_n\|_v\} .$$

Ce lemme est un simple corollaire de [3] prop. 3, ch. III, §. 2. Alors si $P(\alpha_\nu, Y) = d_o(\alpha_\nu)\, Y^n + \ldots + d_n(\alpha_\nu)$ on obtient :

$$h(\beta_\nu) \leq C_K^n \cdot \prod_{v\in\mathcal{M}} \mathrm{Max}_{i=1,\ldots,n} \mathrm{Max}\{1, \|d_i(\alpha_\nu)\|_v\} ,$$

les d_i étant des polynômes de degré au plus $m = n_X$, d'où l'existence de constantes D_v $(v \in \mathcal{M})$, toutes égales à 1 sauf pour un nombre fini d'entre elles, telles que :

$$\mathrm{Max}\{1, \|d_i(\alpha_\nu)\|_v\} \leq D_v . \mathrm{Max}\{1, \|\alpha_\nu\|_v^m\} ;$$

majorations qui assurent $h(\beta_\nu) \ll (h(\alpha_\nu))^m$, d'où

$$h(\theta_\nu) \ll (h(\alpha_\nu))^{me+r}$$

et par suite

$$(*) \qquad \prod_{v\in S} \mathrm{Mini}\{1, \|\theta_\nu - a\|_v\} \ll (h(\theta_\nu))^{-\frac{1}{e(me+r)}} .$$

Soit alors un entier $N>0$; s'il existe une infinité de θ_ν, Γ_o/Γ_o^N étant fini, il existe $g\in\Gamma_o$ tel qu'une infinité de θ_ν soit de la forme

$$\theta_\nu = g\,\gamma_\nu^N \quad , \qquad (\gamma_\nu\in\Gamma_o) \quad ;.$$

Il existe donc une racine N-ième de a/g, disons b, telle que pour une infinité d'entiers ν,

$$|\gamma_\nu - b|_v \ll |\gamma_\nu^N - a/g|_v \quad , \quad (v\in S) \quad ;$$

la majoration (*) devient alors :

$$(**) \qquad \overline{\prod_{v\in S}}\ \mathrm{Mini}\{1, \|\gamma_\nu - b\|_v\} \ll (h(\gamma_\nu))^{-\frac{N}{e(me+r)}} \quad .$$

choisissons $N > 2e\,(me+r)$, le théorème de Thue-Siegel-Roth [3] montre que l'ensemble des γ_ν vérifiant (**) est de hauteur bornée, donc est fini, ce qui contredit l'hypothèse faite sur les θ_ν et par suite, pour une infinité de α_ν et β_ν on a $\alpha_\nu^r \beta_\nu^e = a$. On en déduit que $P(X,Y)$ est, à un facteur multiplicatif près, de la forme $X^rY^e - a$ ou $Y^e - aX^{-r}$ suivant le signe de r.

b) Supposons maintenant $\Gamma_o \subset K^*$ et $P(X,Y)$ dans $K[X,Y]$ où K est un corps de fonctions algébriques d'une variable, de corps des constantes E. Sans nuire à la généralité, nous pouvons supposer que $P(X,Y)$ est absolument irréductible. D'après un lemme de G. Shimura ([6] lemme 3) on a :

(***) Pour presque toute place φ de K sur E (i. e. toutes sauf un nombre fini) le polynôme image $P_\varphi(X,Y)$ de $P(X,Y)$ par φ reste absolument irréductible.

Par ailleurs, il est loisible de choisir une infinité de places φ injectives sur Γ_o. En fait, E étant de type fini sur $\mathbb{Q}$ donc hilbertien (au sens de Lang), on a le lemme suivant, conséquence de [3], ch. VIII, §. 6 :

LEMME 3. - Soit K un corps de fonctions algébriques d'une variable sur un corps de constantes E, Γ_o un sous-groupe de type fini de K^*. Supposons E hilbertien, alors il existe une infinité de places de K sur E injectives sur Γ_o.

Alors pour une infinité de places φ, il existe une infinité d'éléments α_φ, β_φ de $\varphi(\Gamma_o)$ tels que $P_\varphi(\alpha_\varphi, \beta_\varphi) = 0$. Supposons le théorème 2 vrai pour tout corps dont le degré de transcendance sur $\mathbb{Q}$ est strictement plus petit que celui de K. P_φ est défini sur le corps des restes K_φ de K en φ et $\varphi(\Gamma_o) \subset K_\varphi^*$. Par hypothèse il existe des entiers $u = u_\varphi$, $v = v_\varphi$, des éléments a, b dans Γ_o tels que :

$$P_\varphi(\varphi(a)\, x^u,\ \varphi(b)\, x^v) \equiv_x 0 .$$

Il est loisible de choisir u et v premiers entre eux ; P_φ, étant absolument irréductible, est égal à un facteur constant près à $X^v - c_\varphi Y^u$ si $u > 0$ ou $X^v Y^{-u} - c_\varphi$ si $u < 0$, pour un élément $c_\varphi \in \varphi(\Gamma_o)$; il est alors possible de choisir φ ni zéro, ni pôle des coefficients de P qui est donc, à un facteur constant près, de la forme $X^u - c\, Y^v$ ou $X^u Y^{-v} - c$ pour un $c \in \Gamma_o$. Le théorème 2 est alors démontré pour les extensions K de type fini de $\mathbb{Q}$ en raisonnant par récurrence sur le degré de transcendance de K sur $\mathbb{Q}$.

2) Supposons $\Gamma_o = \{1\}$. - Le théorème 1 est démontré dans ce cas par S. Lang [5] mais nous aurons besoin d'amélioration (théorème 3) dû à la nature arithmétique du problème qu'il pose. Commençons par établir la

PROPOSITION 1. - Soit L une extension de type fini de $\mathbb{Q}$, L_o la clôture algébrique de $\mathbb{Q}$ dans L et $\delta_L = [L : \mathbb{Q}]$. Soit α une racine primitive ℓ-ième de l'unité et soit β une racine de l'unité telle que $[L(\alpha, \beta) : L(\alpha)] \leq n$. Alors

il existe une racine de l'unité ζ , des entiers u , v tels que l'on ait :

$$\beta^u = \zeta \alpha^v \quad \text{avec} \quad d_{\mathbb{Q}}(\zeta) \leq n\,\delta_L \ ,$$

$$|v| < 2\sqrt{\ell} \quad \text{et} \quad 0 < u \leq (n\,\delta_L / d_{\mathbb{Q}}(\zeta))\sqrt{\ell} \ .$$

Démonstration : Par un plongement convenable de $L(\alpha)$ dans $\mathbb{C}$, nous pouvons supposer que $\alpha = e(\frac{1}{\ell})$ (où l'on note $e(x) = \exp(2i\pi x)$ pour tout $x \in \mathbb{C}$). Posons $\beta = e(\frac{a}{b})$ avec a, b premiers entre eux (b = 1 si a = 0) et soit $k = p.p.c.m\{\ell, b\}$.

On a alors $\mathbb{Q}(\lambda) = \mathbb{Q}(\alpha, \beta)$ pour $\lambda = e(\frac{1}{k})$. D'autre part, pour tout x algébrique sur L_o , L et $L_o(x)$ sont linéairement disjoints sur L_o et $[L_o(x) : L_o] = [L(x) : L]$ d'où :

$$[\mathbb{Q}(\lambda) : \mathbb{Q}(\alpha)] \leq [\, L_o(\alpha, \beta) : \mathbb{Q}(\alpha)\,] \leq n\,\delta_L \ .$$

a) Soit $h = (\ell, b)$ $(= p.g.c.d.\ \{\ell, b\})$ et considérons les décompositions $\ell = h\ell_o\ell'$, $b = hb_o b'$; les facteurs premiers de $\ell_o b_o$ étant facteurs de h mais non facteurs de $\ell' b'$.

On a $k = \ell b' b_o$ et $[\mathbb{Q}(\lambda) : \mathbb{Q}(\alpha)] = \dfrac{\varphi(k)}{\varphi(\ell)} = \dfrac{\varphi(\ell b_o)\,\varphi(b')}{\varphi(\ell)} = b_o\,\varphi(b')$ où φ désigne la fonction d'Euler ; on obtient ainsi l'inégalité

$$(2) \qquad b_o\,\varphi(b') \leq n\,\delta_L \ .$$

b) Relations entre α et β . - Posons $\theta = e(\frac{1}{\ell b_o})$. Il existe une racine b'-ième de l'unité ζ_1 et un entier rationnel v_1 tels que

$$(3) \qquad \lambda = \zeta_1\,\theta^{v_1} \ .$$

En effet, $(\ell b_o, b') = 1$; il existe donc u_1 et v_1 dans $\mathbb{Z}$ tels que $u_1 \ell b_o + v_1 b' = 1$ d'où (3) avec $\zeta_1 = e(\frac{u_1}{b'})$. Par ailleurs $\theta^{b_o} = \alpha$ et $\beta = \lambda^{a\ell'\ell_o}$;

en tenant compte de (3) on obtient $\beta^{b_o} = \zeta_2 \alpha^{v_2 \ell_o}$, où ζ_2 est une racine b'-ième de l'unité. On a ainsi établi entre racines de l'unité, la relation

$$\beta^{b_o} = \zeta_2 \alpha^s \tag{4}$$

pour un entier $s \in \{0, \dots, \ell-1\}$ avec

$$b_o d_{\mathbb{Q}}(\zeta_2) \leq n \delta_L \ . \tag{5}$$

Choisissons maintenant un entier N tel que $0 < N \leq \ell$ et considérons les $N+1$ expressions $\nu s - \ell[\frac{\nu s}{\ell}]$ pour $\nu = 0, 1, \dots, N$, où $[x]$ désigne la partie entière d'un réel x. Par le "principe des tiroirs", il existe $\mu \in \{1, \dots, N\}$ et $\sigma \in \mathbb{Z}$ tels que l'on ait $|\mu s - \ell \sigma| < \frac{\ell}{N}$. On tire alors de (4) la relation

$$\beta^{\mu b_o} = \zeta_3 \alpha^t \ , \tag{6}$$

où ζ_3 est une racine de l'unité, t et μ entiers, satisfaisant aux inégalités

$$|t| < \ell / N \ , \quad 0 < \mu \leq N \ , \quad b_o d_{\mathbb{Q}}(\zeta_3) \leq n \delta_L \ .$$

Pour obtenir les inégalités de la proposition 1, il suffit de choisir $N = [\sqrt{\ell}]$.

C. Q. F. D.

THÉORÈME 3. - Soit $P(X, Y)$ un polynôme à coefficients complexes, de degré m en X et n en Y avec $mn \neq 0$, de corps de définition L. Il existe une constante C $(= 81\, \delta_L^8\, n^4\, (m+n)^4)$ telle que si $P(\alpha, \beta) = 0$ pour des racines de l'unité α, β, avec α racine primitive ℓ-ième de l'unité et $\ell \geq C$, alors $P(X, Y)$ admet un facteur irréductible de la forme $\zeta - X^v Y^u$ ou $\zeta X^v - Y^u$ avec u, v entiers, $u \neq 0$ et ζ racine de l'unité.

Démonstration : Quitte à remplacer $P(X, Y)$ par un polynôme associé, on peut supposer les coefficients de $P(X, Y)$ dans L. Soit $P(\alpha, \beta) = 0$ dans les condi-

tions du théorème, alors $[L(\alpha,\beta) : L(\alpha)] \leq n$ si $\varphi(\ell) > m\,\delta_L$. Il existe donc (proposition 1) des entiers u, v $(u>0)$ tels que le point de coordonnées α, β soit commun aux courbes affines planes d'équations respectives

$$P(x,y) = 0 \qquad \text{et} \qquad y^u - \zeta x^v = 0 .$$

L'intersection de ces courbes contient donc au moins autant de points distincts que de conjugués distincts de α sur $L(\zeta)$, or

$$[L(\alpha,\zeta) : L(\zeta)] \geq \frac{\varphi(\ell)}{\delta_L\, d_{\mathbb{Q}}(\zeta)} .$$

D'autre part, ces deux courbes sont de degré projectif

$$\sigma \leq m+n \qquad \text{et} \qquad \tau \leq u + |v|$$

respectivement. D'après le théorème de Bezout, elles auront une composante commune si l'on a :

$$(7) \qquad \sigma\,\tau\,\delta_L\, d_{\mathbb{Q}}(\zeta) < \varphi(\ell) \qquad (\text{et } \varphi(\ell) > m\,\delta_L) .$$

Or par la proposition 1, on peut choisir u et v tels que :

$$u + |v| < 3\frac{n\,\delta_L}{d_{\mathbb{Q}}(\zeta)}\sqrt{\ell} .$$

Enfin, pour tout $\varepsilon > 0$, on sait que $\lim\limits_{\nu\to\infty} \frac{\varphi(\nu)}{\nu^{1-\varepsilon}} = +\infty$. Prenons ici $\varepsilon = 1/4$, on a alors

$$(8) \qquad \varphi(\ell) \geq \ell^{3/4} ,$$

pour ℓ assez grand ; plus précisément, un calcul direct montre que l'inégalité (8) est assurée pour $\ell > 180$. D'où les inégalités (7) assurées pour $\ell^{1/4} \geq 3\delta_L^2\, n(m+n)$ $(\text{et } \ell > 180)$ ou encore lorsque

$$(9) \qquad \ell \geq 81\ \delta_L^8\, n^4 (m+n)^4 .$$

Sous cette condition, quitte à remplacer X par $1/X$, nous pouvons supposer que $P(X,Y)$ et $\zeta X^v - Y^u$ ont sur $\mathbb{C}$ un facteur commun irréductible avec $v \geq 0$. Mais si $w = (u,v)$, $\zeta X^v - Y^u = \prod\limits_{\theta^w = \zeta} (\theta X^{v/w} - Y^{u/w})$ est une décomposition en

facteurs irréductibles sur $\mathbb{C}$; $P(X, Y)$ admet donc un facteur irréductible de la forme requise.

3) Supposons $D_K(\mathcal{A})$ borné. - Soit d_o un entier majorant de $D_K(\mathcal{A})$. Pour tout $\alpha \in \mathcal{A}$, il existe ω, racine $M(\alpha)$-ième de l'unité telle que $[K(\omega\alpha) : K] \leq d_o$ d'où

$$M(\omega\alpha) \leq d_o \, \psi_K(d_o) \ ,$$

d'après le lemme 1. Il existe donc une constante m_o ne dépendant que de d_o et de K telle que pour tout $\alpha \in \mathcal{A}$ on ait $\zeta_\alpha \alpha^{m_o} \in K$ pour une racine de l'unité ζ_α. Envisageons l'extension $K_{(m_o)}$; les racines m_o-ièmes de $\zeta_\alpha \alpha^{m_o}$ sont dans $\Gamma(K_{(m_o)})$ et par suite, pour alléger les notations, nous prendrons $K_{(m_o)}$ pour corps K et supposerons donc que $\mathcal{A}$ satisfait à

$$\mathcal{A} \subset K\mathbf{U} \ .$$

Soit β tel que $P(\alpha, \beta) = 0$ avec $\alpha = \zeta a$, $\alpha \in \mathcal{A}$, $a \in K$, $\zeta \in \mathbf{U}$. Soit ℓ un entier multiple de $M(\beta)$ de telle sorte que $\zeta^\ell = 1$. On a $\beta^\ell = b_1 \in K$ et comme $P(\alpha, Y) \neq 0$:

$$[K(\omega_\ell, \beta) : K(\omega_\ell)] \leq [K(\zeta, \beta) : K(\zeta)] \leq n_Y \ ,$$

où ω_ℓ désigne une racine primitive ℓ-ième de l'unité (et $n_Y \neq 0$ égal au degré de $P(X, Y)$ en la variable Y). Supposons démontré le

LEMME 4. - Soit L une extension de type fini de $\mathbb{Q}$. Il existe une constante $\varkappa = \varkappa(L)$, ne dépendant que de L, telle que pour tout $a \in L$, non racine de l'unité et tout m, m' entiers non nuls, on ait :

$$D_L(a^{\rho(s)\varkappa}, m) \geq 2\varkappa \ \Rightarrow \ D_{L(\omega_{mm'})}(a, m) > s \ ,$$

où $\omega_{mm'}$ est une racine primitive mm'-ième de l'unité et $\rho(s) = \text{p. p. c. m.}\{1, \ldots, s\}$.

Supposons β non racine de l'unité et posons $c_1 = \rho(n_Y)\varkappa$. Alors, d'après le lemme 4, $D_K(b_1^{c_1}, \ell) < 2\varkappa$; il existe donc un entier r tel que $[K(\omega_\ell^r \beta^{c_1}) : K] = D_K(b_1^{c_1}, \ell)$ d'où (lemme 1) :

$$M(\omega_\ell^r \beta^{c_1}) \mid c_2 \quad ,$$

avec $c_2 = \rho(2\varkappa)\, \psi_K(2\varkappa)$, ce qui assure $\beta^{c_1 c_2} \in K\mathbf{U}$ et par suite pour $c_o = c_1 c_2$, $\mathfrak{B}^{c_o} \subset K\mathbf{U}$ d'où :

$$\mathfrak{A} \cup \mathfrak{B} \subset K_{(c_o)}\mathbf{U} \ .$$

Soit C la constante du théorème 3 en posant $m = n_X$, $n = n_Y$, $\delta_L = \delta_{K_{(c_o)}}$. D'après 1) nous pouvons supposer $d_K(\mathfrak{A})$ non borné. Choisissons $\alpha \in \mathfrak{A}$, $\beta \in \mathfrak{B}$ tels que $P(\alpha, \beta) = 0$, $\alpha = \zeta a'$, $\beta = \zeta' b'$, a' et b' dans $K_{(c_o)}$, $\zeta' \in \mathbf{U}$ et ζ racine primitive q-ième de l'unité avec $q \geq C$. D'après le théorème 3 et compte tenu du fait que $\mathfrak{A}$ et $\mathfrak{B}$ sont infinis, il existe a, b éléments de Γ et des entiers non nuls u, v tels que $P(ax^u, bx^v) \equiv_x 0$.

Démonstration du lemme 4 : Remarquons que si E est une extension finie de L, on a $D_E(a, m) \geq \frac{1}{[E:L]} D_L(a, m)$, pour tout $a \in L$. Il sera utile dans la démonstration de supposer i ($i^2 = -1$) dans L ; la constante $\varkappa(L)$ sera définie après cette adjonction. Nous démontrerons donc le lemme en supposant que L contienne ce nombre algébrique, avec la condition $D_L(a^{\rho(s)\varkappa}, m) \geq \varkappa$ au lieu de $D_L(a^{\rho(s)\varkappa}, m) \geq 2\varkappa$. La démonstration repose essentiellement sur la théorie des extensions Kummeriennes ([1], ch. III).

Posons $\varkappa = \prod_{p \text{ premier}} p^{\tau_p}$ où $\tau_p = 0$ si L ne contient pas de racine p-ième de l'unité et $\tau_p = \tau+1$ si L contient les racines p^τ-ièmes de l'unité mais pas les racines $p^{\tau+1}$-ièmes. Notons que τ_p est nul sauf pour un nombre fini de premier p.

Soit β tel que $\beta^m = a$; l'extension $L(\omega_{mm'}, \beta)/L(\omega_{mm'})$ est Kummerienne ; si nous supposons son degré sur $L(\omega_{mm'})$ inférieur à s, i.e. si $D_{L(\omega_{mm'})}(a, m) \leq s$, alors $\beta^{\rho(s)} \in L(\omega_{mm'})$. On a ainsi $(\beta^{\rho(s)\varkappa})^m = a^{\rho(s)\varkappa}$.
Nous poserons désormais

$$a_1 = a^{\rho(s)\varkappa} ,$$

ce qui donne

$$\sqrt[m]{a_1} \in L(\omega_{mm'})$$

où $\sqrt[m]{a_1}$ désigne une quelconque racine m-ième de a_1.

Envisageons maintenant le groupe

$$\mathfrak{U} = \{\gamma \in L , \exists u, v \in \mathbb{Z} , u \neq 0 , \gamma^u = a^v \} ,$$

et notons $\mathbb{U}(L)$ le groupe des racines de l'unité de L. Il est clair que $\mathbb{U}(L) \subset \mathfrak{U}$ et que $\mathfrak{U}/\mathbb{U}(L)$ est cyclique infini. Soit ε un générateur de $\mathfrak{U}$ modulo $\mathbb{U}(L)$. Alors

$$a = \zeta \varepsilon^{n'_1} \qquad \text{avec} \qquad \zeta \in \mathbb{U}(L) ,$$

mais $\zeta^{\varkappa} = 1$, il existe donc $n_1 \in \mathbb{Z}^*$ tel que $a_1 = \varepsilon^{n_1}$. Posons :

$$r_m = (m, n_1) \quad \text{et} \quad a_o = \varepsilon^{n_1/r_m} .$$

De $(m/r_m , n_1/r_m) = 1$, on déduit :

(*) *si* p *premier impair tel que* $p \mid \frac{m}{r_m}$ (*resp. si* $4 \mid \frac{m}{r_m}$), *alors* $a_o \notin L^p$ (*resp.* $a_o \notin -4L^4$ $(= L^4)$).

D'après un théorème classique, (*) assure

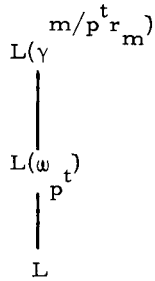
(**) *si* $u \mid \frac{m}{r_m}$, $X^u - a_o$ *est irréductible sur* L.

Si $\gamma^{m/r_m} = a_o$, alors $\gamma^m = (a_o)^{r_m} = a_1$, on a donc :

$$(10) \qquad \frac{m}{r_m} = [L(\gamma) : L] \geq D_L(a_1, m) .$$

Par ailleurs $L(\gamma) \subset L(\omega_{mm'})$; l'extension $L(\gamma)/L$ est donc abélienne ; $L(\gamma)$ contient alors toutes les racines de $X^{m/r_m} - a_o = 0$ et par suite contient les $\frac{m}{r_m}$-ièmes racines de l'unité. Soit $\varkappa_o$ l'ordre de $\mathbf{U}(L)$, on a $\varkappa_o | \varkappa$ et $\varkappa_o \neq \varkappa$. Si $D_L(a_1, m) \geq \varkappa$, alors par (10), $\frac{m}{r_m} \geq \varkappa$ et $\omega_{m/r_m} \notin L$.

Soit p premier tel que $p | \frac{m}{r_m}$. γ^{m/pr_m} est une racine p-ième de a_o, mais $X^p - a_o$ est irréductible sur L, donc $[L(\gamma^{m/pr_m}) : L] = p$; l'extension $L(\gamma^{m/pr_m})/L$ est cyclique et L contient les racines p-ièmes de l'unité. Les diviseurs premiers de m/r_m sont donc diviseurs de $\varkappa$ d'où l'existence d'un premier p et d'un entier $t \geq \tau_p$ tels que $\tau_p \neq 0$ et p^t divise m/r_m exactement (i.e. $p^{t+1} \nmid m/r_m$) lorsque $\frac{m}{r_m} \geq \varkappa$. On met ainsi en évidence une tour d'extensions de trois corps distincts L, $L(\omega_{p^t})$ $L(\gamma^{m/p^t r_m})$, la plus grande étant de degré p^t sur L.



D'autre part, pour $1 \leq t_1 \leq t$, les extensions $L(\omega_{p^{t_1}}) / L(\omega_{p^{t_1}}^p)$ sont Kummeriennes donc de degré 1 ou p (car p premier) ; on peut ainsi, en élevant ω_{p^t} à une puissance convenable, trouver $t' \geq \tau_p$ tel que $L(\omega_{p^{t'}})$ soit cyclique de degré p sur L. Mais $L(\gamma^{m/p^t r_m})$ étant une extension Kummerienne de $L(\omega_{p^t})$, une puissance p^ℓ-ième de $\gamma^{m/p^t r_m}$ est dans $L(\omega_{p^t})$ sans être ici dans L d'après ce qui précède. Il en résulte aussitôt que $L(\gamma^{m/pr_m}) \subset L(\omega_{p^t})$. Par ailleurs, L contenant i, que p soit premier pair ou impair, l'extension $L(\omega_{p^t})/L$ est cyclique ; les sous-groupes d'un groupe cyclique étant caractérisés par leurs ordres, $L(\gamma^{m/pr_m})$ et $L(\omega_{p^{t'}})$ sont corps invariants d'un même sous-groupe de $\mathrm{Gal}(L(\omega_{p^t})/L)$ et donc

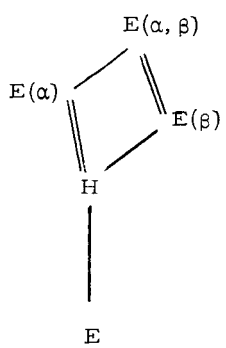
$$L(\sqrt[p]{a_o}) = L(\omega_{p^{t'}}) \quad .$$

D'après la théorie de Kummer, il existe $c \in L$ et un entier r (premier à p) tels que

$$a_o = c^p \, (\omega_{p^{t'}})^{pr} \quad .$$

En particulier $c \in \mathfrak{U}$. Soit $c = \zeta \varepsilon^{\lambda}$ avec $\zeta \in \mathbf{U}(L)$, $\lambda \in \mathbb{Z}^*$. On obtient ainsi : $a_o = \varepsilon^{n_1/r_m} = \varepsilon^{p\lambda}$, donc $p \mid n_1/r_m$, mais $p \mid m/r_m$, ce qui est absurde.
Nous obtenons ainsi, compte tenu de (10), $[L(\omega_{mm'}, \beta) : L(\omega_{mm'})] > s$ lorsque $D_L(a_1, m) \geq \varkappa$.

4) Supposons $D_K(\mathcal{A})$ non borné. - Rappelons que nous avons supposé $P(\alpha, Y) \neq 0$ et $P(X, \beta) \neq 0$ pour tous les $\alpha \in \mathcal{A}$ et $\beta \in \mathcal{B}$. D'après 2) et 3) nous pouvons aussi supposer que $\mathcal{A} \cup \mathcal{B}$ ne contienne pas de racines de l'unité. Soit E le corps obtenu en adjoignant à K une racine primitive $M(\alpha)\,M(\beta)$-ième de l'unité lorsque $\alpha \in \mathcal{A}$, $\beta \in \mathcal{B}$ et $P(\alpha, \beta) = 0$. Soit $H = E(\alpha) \cap E(\beta)$ et $d = [H : E]$. Par la théorie de Kummer, les extensions $E(\alpha)$, $E(\beta)$ et H sont cycliques sur E . D'après la théorie de Galois $[E(\alpha) : H] = v_o \leq n_X$ et $[E(\beta) : H] = u_o \leq n_Y$.



En outre on a :

$$\alpha^s = a' \in E \quad , \quad \beta^t = b' \in E$$

et $E(\alpha) = E(\sqrt[s]{a'})$, $E(\beta) = E(\sqrt[t]{b'})$ en posant $s = [E(\alpha) : E]$ et $t = [E(\beta) : E]$. Alors $E(\sqrt[s]{a'^{v_o}})$ et $E(\sqrt[t]{b'^{u_o}})$ sont de degré $d = s/v_o = t/u_o$ sur E ; ces extensions se confondent donc avec H et

$$H = E(\sqrt{a'}) = E(\sqrt{b'}) \quad .$$

Par la théorie de Kummer, il existe $c \in E$ et r entier tels que $a' = c^d b'^r$.
Mais $a' = \alpha^{v_o d}$, $b' = \beta^{u_o d}$, d'où l'existence d'un $\gamma' \in \Gamma(E)$ et d'un entier

$w \in \{0, 1, \ldots, t\}$ tels que

$$(11) \qquad \alpha^{v_o} = \gamma' \beta^{w} \quad .$$

Notons que $\beta^t \in E$. Donnons nous maintenant un entier N , $0 < N \leq d u_o$. En procédant comme dans 2) prop. 1, b), on détermine un entier $\mu \in \{1, \ldots, N\}$ et un entier $\nu \in \mathbb{Z}$ tels que (11) donne

$$\alpha^{\mu v_o} = \gamma \beta^{\nu}$$

avec $\gamma \in \Gamma(E)$, et $|\nu| < \frac{d u_o}{N}$. Choisissons $N = [\sqrt{d}]$, (α, β) est donc un point sur la courbe d'équation

$$x^v - \gamma y^u = 0$$

avec $u \neq 0$ si $d > 1$ et

$$\gamma \in \Gamma(E) \ , \quad 0 < v \leq v_o \sqrt{d} \ , \quad |u| < 2 u_o \sqrt{d} \ .$$

Par conjugaison sur E on obtient ainsi plus de d points communs aux courbes d'équations $P(x, y) = 0$ et $x^v - \gamma y^u = 0$. Si $d > (n_X + n_Y)(2u_o + v_o)\sqrt{d}$, notamment si

$$d \geq d_o = 4(n_X + n_Y)^4 \quad .$$

Les deux courbes projectives associées à $P(x, y) = 0$ et $x^v - \gamma y^u = 0$ (non nécessairement irréductibles) ont une composante commune d'après le théorème de Bezout, ce qui assure la conclusion du théorème 1 s'il existe $\alpha \in \mathcal{A}$ réalisant $d \geq d_o$; pour cela, il suffit de prendre $\alpha \in \mathcal{A}$ tel que $[E(\alpha) : E] \geq n_Y n_X d_o = s_o$. D'après le lemme 4, cette inégalité est assurée pour $D_K(\alpha^{\rho(s_o)M(\alpha)\varkappa}, M(\alpha)) \geq 2\varkappa$. Si nous supposons un tel choix impossible, alors on a (lemme 4) :

$$\mathcal{A}^{s_1} \subset K \ \mathbf{U} \quad , \quad \text{pour} \quad s_1 = \varkappa \, \rho(s_o) \, \rho(2\varkappa)$$

En raisonnant sur les β comme sur les α on obtient :

$$\mathcal{A} \cup \mathcal{B} \subset K_{(s_1)} \ \mathbf{U} \ ,$$

mais le théorème 1 est déjà démontré dans ce cas par le théorème 3.

C. Q. F. D.

II. - APPLICATIONS

1) Nous pouvons exprimer le théorème 1 sous une forme plus générale, par exemple :

THÉORÈME 4. - *Soit Γ_o un sous-groupe de type fini de $\mathbb{C}^*$ et Γ définit comme dans le théorème 1. Soit $\mathcal{C}$ une courbe irréductible dans l'espace affine $\mathbb{A}^n(\mathbb{C})$, de corps de définition L. Supposons que pour un système donné de coordonnées de $\mathbb{A}^n$, $\mathcal{C}$ admette une infinité de points à coordonnées dans Γ. Alors $\mathcal{C}$ est de genre zéro et de plus admet un point générique sur L de la forme $(\alpha_1 t^{r_1}, \ldots, \alpha_n t^{r_n})$, pour des entiers rationnels r_i et des $\alpha_i \in \Gamma$.*

En effet, soit dans le système donné de coordonnées, $(x_1, \ldots, x_n)$ un point générique de $\mathcal{C}$ sur L. Sans nuire à la généralité, on peut supposer x_1 transcendant sur L et les autres x_i sont alors racines de polynômes irréductibles sur $L(x_1)$. D'après le théorème 1, chaque x_i vérifie une relation du type $x_1^{h_i} = a_i x_i^{m_i}$, avec $m_i \neq 0$. On peut alors choisir une quantité t telle que pour tout $i \in \{1, \ldots, n\}$:

$$x_i = \alpha_i t^{r_i},$$

pour des entiers r_i (que l'on peut prendre premiers entre eux, d'où $t \in E(x_1, \ldots, x_n)$ pour une extension algébrique finie E de L) et des α_i dans Γ.

Nous pouvons également énoncer, en suivant S. Lang [4] le :

THÉORÈME 4 bis. - Soit A une variété en groupe en caractéristique 0 , isomorphe à un produit de groupes multiplicatifs. Soit Γ_o un sous-groupe de A de type fini et Γ le sous-groupe des points $x \in A$ tels qu'il existe un entier $n \neq 0$ tel que $x^n \in \Gamma_o$. Soit V une courbe algébrique irréductible dans A et supposons l'intersection de V avec Γ infinie. Alors V est une translation d'une sous-variété en groupe de A .

2) La démonstration du théorème 1 suggère de généraliser le théorème 3. Avec les notations de I) montrons le

THÉORÈME 5. - Soit K un sous-corps de $\mathbb{C}$ de type fini sur $\mathbb{Q}$. Notons Ω_K le sous-groupe de $\mathbb{C}^*$ des nombres complexes dont une puissance entière non nulle est dans K^* , et soient m, n des entiers > 0 . Il existe une constante effective $B(m, n, K) = B$ ne dépendant que de m, n et K , telle que pour tout polynôme $P(X, Y)$ à coefficients dans K , de degré m en X , n en Y , si $P(\alpha, \beta) = 0$ avec α et β dans Ω_K et $M(\alpha) \geq B$, alors $P(ax^u, bx^v) \equiv_x 0$ pour des entiers u , v , $u \neq 0$ et des éléments a, b de Ω_K .

Démonstration : Soient α et β dans Ω_K tels que $P(\alpha, Y) \neq 0$ et $P(\alpha, \beta) = 0$. Si $P(X, \beta) = 0$ le théorème est démontré ; nous écartons donc ce cas.

Notons Γ_o le sous-groupe de K^* engendré par $\alpha^{M(\alpha)}$ et $\beta^{M(\beta)}$. $\Gamma(K)$ est de rang au plus 2 . Avec les notations de I), pour tout entier $q \geq 1$, d'après la définition de $K_{(q)}$ on a :

$$[K_{(q)} : K] \leq q^3 \quad . \tag{12}$$

Posons $E = K(\omega_{M(\alpha)M(\beta)})$. D'après I-4), si $[E(\alpha) : E]$ ou $[E(\beta) : E] \geq 4mn(m+n)^4$, les conclusions du théorème sont assurées. Supposons donc

$$[E(\alpha) : E] \leq 4mn(m+n)^4 = s_o \quad \text{et} \quad [E(\beta) : E] \leq s_o \ .$$

. Si α ou $\beta \in \mathbf{U}$, I-3) donne $\{\alpha, \beta\} \subset K_{(c_o)}\mathbf{U}$,

. Si α et $\beta \notin \mathbf{U}$, I-4) in fine donne $\{\alpha, \beta\} \subset K_{(s_1)}\mathbf{U}$;

les constantes c_o et s_1 ne dépendant que de m, n et K .

Comme $K_{(c_o)}$ et $K_{(s_1)}$ sont des sous-corps de $K_{(c_o s_1)}$, posons $c_3 = c_o s_1$ et $L = K_{(c_3)}$, on obtient

$$\{\alpha, \beta\} \subset L\mathbf{U} \ .$$

D'autre part on a immédiatement $M_L(\alpha)\, M(\alpha^{M_L(\alpha)}) = M(\alpha)$ où $M_L(\alpha)$ est le plus petit entier N tel que $\alpha^N \in L$. Le lemme 1 donne

$$M(\alpha^{M_L(\alpha)}) \leq [L : K]\, \psi_K([L : K]) \ .$$

Si on suppose

$$M(\alpha) \geq C(m, n, \delta_L)\, [L:K]\, \psi_K([L:K])$$

où $C(m, n, \delta_L)$ est la constante du théorème 3, ce dernier théorème assure les conclusions du théorème à montrer. Il reste donc à majorer convenablement $[L : K]$ (puisque $\delta_L \leq \delta_K [L : K]$) par une constante ne dépendant que de m , n et K , ce qui est fait par (12) .

3) Quelques courbes à points algébriques particuliers

Pour tout $S(X) \in \mathbb{C}[X]$, notons $\mathcal{L}_S$ l'ensemble des nombres complexes z tels que $S(z) \in \mathbf{U}$. Notons également $\mathfrak{T}$ l'ensemble des entiers algébriques

θ dont tous les conjugués sur $\mathbb{Q}$, θ compris, sont réels et de module au plus 2 (entiers de Kronecker). I-2) permet de décrire les courbes algébriques qui admettent, en nombre suffisant, des points à coordonnées dans des ensembles tels que $\mathfrak{L}_S$ ou $\mathfrak{T}$. Enonçons deux propositions à ce sujet :

PROPOSITION 2. - Soient K un sous-corps de $\mathbb{C}$ de type fini sur $\mathbb{Q}$, S et T des polynômes non constants à coefficients dans K, de degré au plus d et soit $\mathcal{C}$ une courbe algébrique plane de degré σ définie sur K. Supposons que dans un système donné de coordonnées, $\mathcal{C}$ admette un point (α, β) tel que $\alpha \in \mathfrak{L}_S$, $\beta \in \mathfrak{L}_T$ et $d_K(\alpha) \geq 81 d^5 (\sigma \delta_K)^8$. Alors $\mathcal{C}$ admet une composante commune avec la courbe d'équation

$$[T(y)]^v - \zeta [S(x)]^u = 0 ,$$

où u et v sont des entiers, $v > 0$ et $\zeta \in \mathbf{U}$.

La démonstration repose sur la proposition 1 et le raisonnement fait dans la démonstration du théorème 3.

PROPOSITION 3. - Soit $\mathcal{C}$ une courbe algébrique plane en caractéristique zéro, de degré σ, irréductible et de corps de définition L. Supposons que dans un système donné de coordonnées, $\mathcal{C}$ admette un point $(\alpha, \beta) \in \mathfrak{T}^2$ tel que $d_L(\alpha) \geq 81 (3\sigma \delta_L)^8$. Alors, il existe des entiers u, v $(v > 0)$ et une racine de l'unité ω tels que $(t^v + 1/t^v , \omega t^u + 1/\omega t^u)$ soit un point générique de $\mathcal{C}$ sur L.

En effet, d'après un théorème de Kronecker, les éléments de $\mathfrak{T}$ sont de la forme $\zeta + 1/\zeta$ où ζ est une racine de l'unité. Si $F(x, y) = 0$ est une équation irréductible de $\mathcal{C}$ dans le système donné de coordonnées, la proposition 3

résulte du théorème 3 appliqué au polynôme

$$P(X, Y) = X^m Y^n F(X+1/X\ ,\ Y+1/Y)$$

avec des entiers convenables m et n. En effet, nous pouvons écarter le cas banal où $\mathcal{C}$ est une droite d'équation $y = \beta$; si $d_L(\alpha) > 1$, on peut alors supposer F de degré non nul en x et y, et P de degré au plus 3σ. Remarquons maintenant que dans le théorème 3 le terme $(m+n)$ dans la constante C provient d'une majoration du degré du polynôme. D'autre part, si $\alpha = \zeta+1/\zeta$ avec $\zeta \in \mathbf{U}$ d'ordre ℓ, on a $\ell > d_L(\alpha)$, d'où notre assertion.

Ainsi, toute courbe algébrique plane réelle qui admet suffisamment de points dans $\mathfrak{X}^2$, est une courbe de Lissajoux.

-:-:-:-

BIBLIOGRAPHIE

[1] CASSELS-FRÖHLICH. - Algebraic number theory. Academic Press, London and New-York, 1967.

[2] EICHLER M. - Introduction to the theory of algebraic numbers and functions. Academic Press, London and New-York, 1966.

[3] LANG S. - Diophantine Geometry. New-York, Interscience Publisher, 1962.

[4] LANG S. - Report on diophantine approximations. Bull. Soc. Math. France, 93, 1965, p. 177 à 192.

[5] LANG S. - Division points on curves. Ann. math. Pura Appl. 1965, p. 229-234.

[6] SHIMURA G. - Reduction of algebraic varieties with respect to a discrete valuation of the basic field. American J. of Math. 77; 134-176.

-:-:-:-

Pierre LIARDET
Université de Provence
Département de Mathématiques
3, place Victor Hugo
13331 MARSEILLE CEDEX 3