SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

F. GAUTHIER

Solving Diophantine Problems Modulo Every Prime

Séminaire de théorie des nombres de Grenoble, tome 1 (1971-1972), p. 9-19

<http://www.numdam.org/item?id=STNG_1971-1972__1__9_0>

SOLVING DIOPHANTINE PROBLEMS MODULO EVERY PRIME

d'après [1]

---

par F. GAUTHIER les 17-24 novembre et 1er décembre 1971

Dans [5], à la fin du chapitre sur le théorème de la progression arithmétique, Serre signale à titre de remarque :

"Soit $\{f_\alpha(X_1,\dots,X_n)\}$ une famille de polynômes à coefficients entiers, et soit P_o l'ensemble des nombres premiers p tels que les réductions des f_α (modulo p) aient un zéro commun dans $(\mathbb{F}_p)^n$. On peut montrer, que P_o a une densité de Dirichlet, que cette densité est un nombre rationnel, et n'est nulle que si P_o est fini".

Dans une première partie nous allons démontrer ce résultat en admettant une proposition et un théorème qui seront démontrés dans une seconde partie.

Nous allons tout d'abord introduire quelques notations.

Si E est un corps, $\tilde{E}$ désigne une clôture algébrique de E. Soit $\mathbb{Q}$ le corps des rationnels ; si M est un sous-corps de $\tilde{\mathbb{Q}}$, $I(M)$ désigne l'anneau des entiers de M, $P(M)$ l'ensemble des idéaux premiers de $I(M)$. Si $\mathfrak{p} \in P(M)$, on note $I(M)_{\mathfrak{p}}$ le localisé de $I(M)$ en $\mathfrak{p}$ et $M(\mathfrak{p})$ l'adhérence de $\mathbb{Q}$ dans M pour la topologie définie par $\mathfrak{p}$ sur M. Remarquons que si M est une extension galoisienne de $\mathbb{Q}$, $M(\mathfrak{p})$ est le corps de décomposition de $\mathfrak{p}$.

Si, pour $1 \le \lambda \le m$, $f_\lambda \in I(M)[X_1,\dots,X_n]$, on note $a_M(f_1,\dots,f_m)$ l'ensemble des $\mathfrak{p} \in P(M)$ tels qu'il existe $x \in \mathbb{Z}^n$ avec :

$$f_\lambda(x) \equiv 0 \quad (\mathfrak{p}) \qquad \text{pour} \quad 1 \le \lambda \le m .$$

Soit $A_n(M)$ l'algèbre de Boole engendrée, dans l'ensemble des parties de $P(M)$, par les $a_M(f_1,\ldots,f_m)$ lorsque m décrit $\mathbb{N}^*$ et $f_\lambda \in I(M)[X_1,\ldots,X_n]$.

Soit d'autre part $A(M)$ l'algèbre de Boole engendrée par les $a_M(f)$ pour $f \in I(M)[X_1]$.

De façon évidente :

- $A(M) \subset A_n(M)$ pour $n \geq 1$
- $A(M)$ contient les parties finies de $P(M)$.

Si $M \subset M'$ et si $a \subset P(M')$ nous noterons $(a|M)$ l'ensemble des $\mathfrak{p} \cap M$ pour $\mathfrak{p} \in a$.

Soit k un corps de nombres ; pour tout $\alpha \in k$, $\alpha \neq 0$ considérons le polynôme minimal de α sur $\mathbb{Q}$:

$$f(X) = X^h + \frac{c_1}{d_1} X^{h-1} + \ldots + \frac{c_i}{d_i} X^{h-i} + \ldots + \frac{c_o}{d_o} \quad ,$$

$c_i \in \mathbb{Z}$, $d_i \in \mathbb{Z}$, $(c_i,d_i) = 1$.

On note $S_k(\alpha)$ l'ensemble des $\mathfrak{p} \in P(k)$ tels que $\mathfrak{p}$ divise l'un des d_i ou $\mathfrak{p}$ divise le discriminant de f. Soit k un corps de nombres, considérons une extension galoisienne L de k et notons G le groupe de Galois de L/k. Soit $\mathcal{K} = \{k_i\}$ une famille de sous-corps de L, nous dirons que $\mathcal{K}$ est L/k normale si $\mathcal{K}$ est stable par G.

Si $\mathcal{K}$ est L/k normale, on désigne par $b_{L/k}(\mathcal{K})$ l'ensemble des $\mathfrak{p} \in P(k)$ tels qu'il existe $\mathfrak{P} \in P(L)$ avec $L(\mathfrak{P}) \in \mathcal{K}$ et $\mathfrak{P}|\mathfrak{p}$.

On note $B(L/k)$ l'ensemble des $b_{L/k}(\mathcal{K})$ pour $\mathcal{K}$ parcourant les familles L/k normales de sous corps de L, et $B'(L/k)$ l'algèbre de Boole engendrée sur $P(k)$ par $B(L/k)$ et les parties finies de $P(k)$.

I. L'ENSEMBLE DES p TELS QUE ... A UNE DENSITE RATIONNELLE.

Soit, pour $1 \leq \alpha \leq m$, $f_\alpha \in \mathbb{Z}[X_1,\ldots,X_n]$.

Soit $P_o = a_{\mathbb{Q}}(f_1,\ldots,f_m)$ l'ensemble des $p \in P(\mathbb{Q})$ pour lesquels il existe $x \in \mathbb{Z}^n$ avec $f_\alpha(x) \equiv 0(p)$ $1 \leq \alpha \leq m$. Alors $P_o \in A_n(\mathbb{Q})$. Nous verrons au II que $A_n(\mathbb{Q}) = A(\mathbb{Q})$ et que $A(\mathbb{Q}) = \cup B'(L/\mathbb{Q})$, l'union portant sur toutes les extensions $L/\mathbb{Q}$ galoisiennes.

Par suite, il existe une extension galoisienne $L/\mathbb{Q}$, une famille $\mathcal{K}$, $L/\mathbb{Q}$ normale, et une partie finie S de $P(\mathbb{Q})$ telles que $P_o \setminus S = b_{L/k}(\mathcal{K}) \setminus S$. Nous supposons que S contient les p qui se ramifient dans $L/\mathbb{Q}$.

Pour $p \in P(\mathbb{Q}) \setminus S$ notons $F[\mathfrak{P}]$ le Frobénius d'un idéal $\mathfrak{P} \in P(L)$ tel que $\mathfrak{P} | p$ et $F(p)$ la classe de conjugaison (dans $Gal(L/\mathbb{Q})$) de $F[\mathfrak{P}]$ (symbole d'Artin).

Considérons les classes $F(p)$ pour $p \in P_o \setminus S$, nous obtenons ainsi un nombre fini de classes c_i $1 \leq i \leq t$.

De plus, si $p \in P(\mathbb{Q}) \setminus S$ et $F(p) = c_i$ avec $1 \leq i \leq t$, il existe $p_o \in P_o \setminus S$ tel que $F(p) = F(p_o)$.

Soit $\begin{cases} \mathfrak{p} \in P(L) \text{ tel que } \mathfrak{p} | p \\ \mathfrak{p}_o \in P(L) \text{ tel que } \mathfrak{p}_o | p_o \end{cases}$ il existe $\tau \in Gal(L/\mathbb{Q})$

tel que $F[\mathfrak{p}] = \tau F[\mathfrak{p}_o]\tau^{-1} = F[\tau \mathfrak{p}_o]$.

Donc les corps de décomposition de $\mathfrak{p}$ et de $\tau\mathfrak{p}_o$ sont les mêmes : $L(\mathfrak{p}) = L(\tau\mathfrak{p}_o)$. $p_o \in P_o \Rightarrow L(\tau\mathfrak{p}_o) \in \mathcal{K}$ donc $L(\mathfrak{p}) \in \mathcal{K}$ par suite $p \in b_{L/k}(\mathcal{K}) \setminus S = P_o \setminus S$.

Le théorème d'Artin-Tchebotareff (voir [2]) nous permet d'affirmer de de l'ensemble des $p \in P(\mathbb{Q})$ non ramifiés dans l'extension $L/\mathbb{Q}$ et tel que $F(p) = c_i$ a une densité analytique et cette densité est

$$\frac{\text{card } (c_i)}{\text{card } (Gal(L/\mathbb{Q}))} \quad .$$

La remarque énoncée par Serre se trouve ainsi démontrée.

II. ETUDE DES ALGEBRES DE BOOLE $A(k)$ ET $A_n(k)$.

Lemme.

Soient $\begin{cases} L \text{ un corps de nombres} \\ \alpha \in L \ , \ \alpha \neq 0 \\ \mathfrak{p} \in P(L) \backslash S_L(\alpha) \end{cases}$

alors $\mathfrak{p} \in a_L(X-\alpha)$ si et seulement si $\alpha \in L(\mathfrak{p})$.

Démonstration :

Soit $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$, on a alors $L(\mathfrak{p}) = L \cap \mathbb{Q}_p$.

Si $\alpha \in L(\mathfrak{p})$, le polynôme minimal de α sur $\mathbb{Q}$ appartient à $\mathbb{Z}_{p\mathbb{Z}}[X]$, puisque $\mathfrak{p} \notin S_L(\alpha)$; par suite $\alpha \in \mathbb{Q}_p$ et α est $\mathfrak{p}$ entier, donc il existe $a \in \mathbb{Z}$ tel que $\alpha \equiv a(\mathfrak{p})$.

Si $\mathfrak{p} \in a_L(X-\alpha)$, il existe $a \in \mathbb{Z}$ avec $a \equiv \alpha(\mathfrak{p})$. Soit $f(X)$ le polynôme minimal de α sur $\mathbb{Q}$. $f(a) \equiv 0(\mathfrak{p})$. Soit $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. $f(X) \in \mathbb{Z}_{p\mathbb{Z}}[X] \subset \mathbb{Z}_p[X]$. Comme $f(a) \equiv 0(p\mathbb{Z}p)$ et $\mathfrak{p} \notin S_L(\alpha)$ le lemme de Hensel nous permet d'affirmer qu'il existe $\alpha' \in \mathbb{Z}_p$, $\alpha' \equiv a(p)$ tel que $f(\alpha') = 0$. Donc pour tout $i \in \mathbb{N}^*$ il existe $a_i \in \mathbb{Z}$ tel que $a_i \equiv \alpha'(p)$ et $f(a_i) \equiv 0(p^i)$. Soit M une extension de L dans laquelle f se factorise complètement : $f(X) = \prod_j (X-\gamma_j)$.

Soit $\mathfrak{P}$ un idéal de M au-dessus de $\mathfrak{p}$; $a_i - \alpha \equiv 0(\mathfrak{P})$ et comme $\mathfrak{p} \notin S_L(\alpha)$ $f(a_i) \equiv 0(\mathfrak{P}^i)$ entraîne $a_i \equiv \alpha(\mathfrak{P}^i)$ et donc $\alpha \in L(\mathfrak{p})$.

Corollaire.

Si $f(X) \in I(L)[X]$ et si f se factorise complètement dans L , il existe une partie finie S de $P(L)$ telle que pour $\mathfrak{p} \in P(L)\backslash S$ on ait :

$$\mathfrak{p} \in a_L(f) \Leftrightarrow f \text{ a une racine dans } L(\mathfrak{p}) .$$

Il suffit de prendre $S = \bigcup_\alpha S_L(\alpha)$, l'union portant sur les racines non nulles de f .

Proposition.

k désignant un corps de nombres $A(k) = \bigcup_L B'(L/k)$.

L'union portant sur les L extensions galoisiennes de k .

Démonstration :

Soit $f \in I(k)[X]$. Considérons une extension galoisienne L de k dans laquelle f se factorise complètement et la famille $\mathcal{K}$ des sous corps de L dans lesquels f a une racine. $\mathcal{K}$ est L/k normale. Il résulte du corollaire du lemme que $a_k(f)$ et $b_{L/k}(\mathcal{K})$ différent par une partie finie. Comme $\bigcup_L B'(L/k)$ est une algèbre de Boole, on a

$$A(k) \subset \bigcup_L B'(L/k) .$$

Pour montrer l'autre inclusion, il suffit de prendre $a \in B(L/k)$ avec L/k galoisienne et de montrer que $a \in A(k)$. Soit $\mathcal{K}$ une famille L/k normale telle que $a = b_{L/k}(\mathcal{K})$. Pour chaque $k_i \in \mathcal{K}$, considérons la trajectoire de k_i , c'est-à-dire l'ensemble des $\sigma(k_i)$ avec $\sigma \in Gal(L/k)$. Les trajectoires sont des familles L/k normales et comme $b_{L/k}(\mathcal{K}) = \cup b_{L/k}(\mathcal{H})$ l'union portant sur les trajectoires $\mathcal{H} \subset \mathcal{K}$ on peut supposer que $\mathcal{K}$ est une trajectoire. Soit $\mathcal{J}$ la famille des sous corps J de L tels que

- il existe $k_i \in \mathcal{K}$ avec $k_i \subset J$
- l'extension J/k_i n'ait pas de corps intermédiaire.

Soit $\mathcal{K}'$(resp $\mathcal{J}'$) l'ensemble des sous corps de L qui contiennent un élément de $\mathcal{K}$(resp $\mathcal{J}$) ; alors $\mathcal{K}'$ et $\mathcal{J}'$ sont des familles L/k normales et $\mathcal{K} = \mathcal{K}' \setminus \mathcal{J}'$; par suite $b_{L/k}(\mathcal{K}) = b_{L/k}(\mathcal{K}') \setminus b_{L/k}(\mathcal{J}')$. Il suffit donc de montrer que si $\mathcal{M}$ est une famille L/k normale et si $\mathcal{M}'$ est la famille L/k normale des sous corps de L contenant un corps de la famille $\mathcal{M}$ on a $b_{L/k}(\mathcal{M}') \in A(k)$:

Pour chaque $m_i \in \mathcal{M}$ considérons θ_i entier sur $\mathbb{Q}$ et tel que $\mathbb{Q}(\theta_i) = m_i$. Soit f_i le polynôme minimal de θ_i sur k , $f_i \in I(k)[X]$. Soit $f = \prod f_i$, alors $f \in I(k)[X]$, f se factorise complètement dans L et la famille $\mathcal{M}'$ est la famille des sous corps de L dans lesquels f a une racine, par suite $b_{L/k}(\mathcal{M}')$ et $a_k(f)$ diffère par une partie finie et

$$\cup B'(L/k) \subset A(k) .$$

Corollaire.

$$\text{Soient} \begin{cases} k & \text{un corps de nombres} \\ h & \text{un sous corps de } k \\ a & \in A(k) \end{cases}$$

Alors, on a : $(a|h) \in A(h)$.

Démonstration :

$a \in A(k) = \cup B'(L/k)$ donc il existe une extension $L/\mathbb{Q}$ galoisienne telle que $k \subset L$ et $a \in B'(L/k)$. Il suffit de montrer que si $\mathcal{K}$ est L/k normale

$$(b_{L/k}(\mathcal{K})|h) \in A(h) .$$

Soit $\mathcal{H}$ la famille des sous corps de L qui sont L/h conjugués des corps de la famille $\mathcal{K}$, on a

$$(b_{L/k}(\mathcal{K})|h) = b_{L/h}(\mathcal{H}) \in A(h) .$$

Soient M un corps de nombres, $\mathfrak{p} \in P(M)$ et $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. Nous associerons à $\mathfrak{p}$ une place de M dans $\tilde{\mathbb{F}}_p \cup \{\infty\}$ (que nous noterons également $\mathfrak{p}$) de la manière suivante :

Soit $x \in I(M)$, soit $\bar{x}$ la classe de x dans $I(M)/\mathfrak{p}$.

$I(M)/\mathfrak{p} \simeq \mathbb{F}_{p^f} \subset \tilde{\mathbb{F}}_p$.

La place $\mathfrak{p}$ est alors définie par

- si $\alpha = \frac{x}{y} \in I(M)_{\mathfrak{p}}$ $\qquad \mathfrak{p}(\alpha) = \frac{\bar{x}}{\bar{y}}$
- si $\alpha \in M \backslash I(M)_{\mathfrak{p}}$ $\qquad \mathfrak{p}(\alpha) = \infty$

On notera également $\mathfrak{p}$ l'application induite sur M^n et celle induite sur $M[X]$.

Théorème.

Soit k un corps de nombres, pour tout $n \geq 1$:

$$A_n(k) = A(k)$$

Démonstration :

Il suffit de montrer que si pour $1 \leq \lambda \leq m$, $g_\lambda \in I(k)[X_1,\dots,X_n]$ on a $a_k(g_1,\dots,g_m) \in A(k)$.

Remarquons tout d'abord que $\mathfrak{p} \in a_k(g_1,\dots,g_m)$ équivaut à "les polynômes $\mathfrak{p}(g_\lambda)$, $1 \leq \lambda \leq m$, ont un zéro commun dans $(\mathbb{F}_p)^n$ ".

Soit d'autre part V l'ensemble algébrique défini par les g_λ , $1 \leq \lambda \leq m$. Nous allons procéder par récurrence sur la dimension d de V (sur k).

1) Si V ne contient qu'un nombre fini de points. Soit $V = \{x^{(1)},\dots,x^{(\ell)}\}$. Il existe une extension galoisienne N de k telle que $x^{(\mu)} \in N^n$ pour $1 \leq \mu \leq \ell$.

D'après le corollaire de la proposition il suffit de montrer que $a_N(g_1,\dots,g_m) \in A(N)$.

Or, on peut montrer (voir [6] chap.III § 12) que pour $\mathfrak{P} \in P(N)$:

- l'ensemble des $(\xi) \in (\tilde{\mathbb{F}}_p)^n$ tels que pour tout λ , $1 \leq \lambda \leq m$ $\mathfrak{P}(g_\lambda)(\xi) = 0$,
- et l'ensemble $\mathfrak{P}(V)$ des $(\xi) \in (\tilde{\mathbb{F}}_p)^n$ tels qu'il existe une place $\mathfrak{P}'$ au-dessus de $\mathfrak{P}$ et un $(x) \in V$ avec $\mathfrak{P}'(x) = (\xi)$,

sont égaux sauf pour $\mathfrak{P}$ appartenant à une partie finie S' de $P(N)$.

Par suite, pour tout $\mathfrak{P} \in P(N)\backslash S'$ les solutions dans $(\tilde{\mathbb{F}}_p)^n$ du système $\mathfrak{P}(g_\lambda) = 0$, $1 \leq \lambda \leq m$ sont $\mathfrak{P}(x^{(\mu)})$ $1 \leq \mu \leq \ell$.

Donc, pour $\mathfrak{P} \in P(N)\backslash S'$, $\mathfrak{P} \in a_N(g_1,\dots,g_m)$ équivaut à "il existe μ , $1 \leq \mu \leq \ell$, tel que $\mathfrak{P}(x^{(\mu)}) \in (\mathbb{F}_p)^n$."

Soit $S'' = (\bigcup_\gamma S_N(\gamma)) \cup S'$, l'union étant prise sur les γ , coordonnées non nulles des $x^{(\mu)}$; S'' est un ensemble fini et pour $\mathfrak{P} \in P(N)\backslash S''$:

$\mathfrak{P} \in a_N(g_1,\dots,g_m)$ équivaut à "il existe μ , $1 \leq \mu \leq \ell$ avec $x^{(\mu)} \in (N(\mathfrak{P}))^n$."

Soit b l'ensemble des $\mathfrak{P} \in P(N)$ tel qu'il existe μ , $1 \leq \mu \leq \ell$ avec $x^{(\mu)} \in (N(\mathfrak{P}))^n$.

La famille de corps $N(\mathfrak{P})$, $\mathfrak{P} \in b$, est N/N normale, $a_N(g_1,\dots,g_m)$ et b ne différent que par un ensemble fini, et par suite $a_N(g_1,\dots,g_m) \in A(N)$.

La propriété est donc vraie si $d = -1$ $(V=\phi)$ et $d=0$.

2) Si $d \geq 1$:

Supposons la propriété établie pour toutes les dimensions strictement inférieures à d .

Il existe une extension $N/\mathbb{Q}$ galoisienne, $N \supset k$, et des variétés V_τ absolument irréductibles sur N , telles que :

$$V = \bigcup_{\tau=1}^{t} V_\tau \ .$$

Soit $\{g_{\tau,1}, g_{\tau,2},\dots,g_{\tau,b}\} \subset I(N)[X_1,\dots,X_n]$ une famille de polynômes définissant V_τ . Pour $\mathfrak{P} \in P(N)$, $\mathfrak{P}(V) = \bigcup_{\tau=1}^{t} \mathfrak{P}(V_\tau)$, et par suite il existe une partie finie T de $P(N)$ telle que pour $\mathfrak{P} \in P(N)\backslash T$:

$$\{(\xi) \in (\tilde{\mathbb{F}}_p)^n / \mathfrak{P}(g_\mu)(\xi) = 0 \ , \ 1 \leq \mu \leq m\} = \bigcup_{\tau=1}^{t} \{(\xi) \in (\tilde{\mathbb{F}}_p)^n / \mathfrak{P}(g_{\tau,\beta})(\xi) = 0 \ , \ 1 \leq \beta \leq b\} \ ;$$

d'où

$$a_N(g_1,\dots,g_m)\backslash T = \bigcup_{\tau=1}^{t} a_N(g_{\tau,1},\dots,g_{\tau,b})\backslash T \ .$$

Comme $\begin{cases} (a_N(g_1,\dots,g_m)\,|\,k) = a_k(g_1,\dots,g_m) \ , \\ A(k) \text{ est clos pour l'union et contient les parties finies.} \end{cases}$

On voit qu'il suffit de montrer que $a_N(g_{\tau,1},\dots,g_{\tau,b}) \in A(N)$ et par suite on peut supposer V absolument irréductible, et $k/\mathbb{Q}$ galoisienne. Pour chaque sous corps k' de k , $\{k'\}$ est une famille k/k normale, $b_{k/k}(\{k'\})$ désigne alors l'ensemble des $\mathfrak{p} \in P(k)$ tels que $k(\mathfrak{p}) = k'$. Comme $a_k(g_1,\dots,g_m) = \bigcup_{k' \subset k} [a_k(g_1,\dots,g_m) \cap b_{k/k}(\{k'\})]$ nous sommes ramenés à montrer que si k' est un sous corps de k , $a_k(g_1,\dots,g_m) \cap b_{k/k}(\{k'\}) \in A(k)$.

En fait il suffit de montrer que :

$$a_k(g_1,\dots,g_m) \cap [b_{k/k}(\{k'\})\backslash S] \in A(k)$$

S désignant une partie finie de $P(k)$.

Nous supposerons que S contient les $\mathfrak{p} \in P(k)$ tels que $\mathfrak{p}\,|\,p$ avec p ramifié dans $k/\mathbb{Q}$.

Si $\mathfrak{p} \in b_{k/k}(\{k'\})\backslash S$, $k(\mathfrak{p}) = k'$ est le corps de décomposition de $\mathfrak{p}$ et par suite

$$[k:k'] = f(\mathfrak{p}/p) = f \quad .$$

Soit pour $1 \leq \varphi \leq f$, $\omega_\varphi \in I(k)$ tels que $\{\omega_1, \ldots, \omega_f\}$ forme une base de k sur k' . Chaque g_μ $(1 \leq \mu \leq m)$ s'écrit de manière unique :

$$g_\mu = \sum_{\varphi=1}^{f} g_{\mu,\varphi}\omega\varphi$$

avec $g_{\mu,\varphi} \in k'[X_1, \ldots, X_n]$. Il existe $\omega \in I(k')$ tel que $\omega g_{\mu,\varphi} \in I(k')[X_1, \ldots, X_n]$ pour $1 \leq \mu \leq m$ et $1 \leq \varphi \leq f$.

Nous supposerons que S contient les $\mathfrak{p} \in P(k)$ tels que $\mathfrak{p} \mid \omega$ ou $\mathfrak{p} \mid \omega_\varphi$, $1 \leq \varphi \leq f$; on peut donc supposer que

$$g_{\mu,\varphi} \in I(k')[X_1, \ldots, X_n]$$

pour $1 \leq \mu \leq m$ et $1 \leq \varphi \leq f$.

Si $\mathfrak{p} \in b_{k/k}(\{k'\})\backslash S$ on a :

$$\mathfrak{p}(g_\mu) = \sum_{\varphi=1}^{f} \mathfrak{p}(g_{\mu,\varphi})\mathfrak{p}(\omega_\varphi) \quad ,$$

$$\mathfrak{p}(g_{\mu,\varphi}) \in \mathbb{F}_p[X_1, \ldots, X_n] \quad \text{et}$$

$\{\mathfrak{p}(\omega_\varphi) \ , 1 \leq \varphi \leq f\}$ est une base de $I(k)/\mathfrak{p}$ sur $\mathbb{F}_p$; par suite $\mathfrak{p} \in a_k(g_1, \ldots, g_m)$ équivaut à $\mathfrak{p} \in a_k(g_{1,1}, \ldots, g_{m,f})$. Il suffit donc de montrer que :

$$a_k(g_{1,1}, \ldots, g_{m,f}) \cap ([b_{k/k}(\{k'\})]\backslash S) \in A(k) \ .$$

Soit W l'ensemble algébrique défini sur k' par $g_{1,1}, \ldots, g_{m,f}$; on a $W \subset V$. Si $W \subsetneq V$, V étant absolument irréductible $\dim W < \dim V$ et l'hypothèse de récurrence permet de conclure.

Si $W = V$, V est alors une variété absolument irréductible définie sur k' .

Il suffirait de montrer qu'il existe une partie finie Ω de $P(k)$ telle que :

$$b_{k/k}(\{k'\})\backslash\Omega \subset a_k(g_{1,1}, \ldots, g_{m,f}) \ ,$$

et pour cela que pour tout $\mathfrak{p} \in b_{k/k}(\{k'\})$ sauf peut-être un nombre fini, les polynômes :

$$\mathfrak{p}(g_{\mu,\varphi}) \quad \text{avec} \quad 1 \leq \mu \leq m \quad \text{et} \quad 1 \leq \varphi \leq f \ ,$$

ont un zéro commun dans $(\mathbb{F}_p)^n$.

Si $\mathfrak{p} \in b_{k/k}(\{k'\})$

on a $k(\mathfrak{p}) = k'$; notons $\mathfrak{p}' = \mathfrak{p} \cap k'$, alors $\mathfrak{p}(g_{\mu,\varphi}) = \mathfrak{p}'(g_{\mu,\varphi}) \in \mathbb{F}_p[X]$. Pour tout $\mathfrak{p}$ sauf un nombre fini, l'ensemble algébrique $\mathfrak{p}(V)$ défini sur $\mathbb{F}_p$ par les polynômes $\mathfrak{p}(g_{\mu,\varphi})$ est une variété non vide de même dimension d que la variété V , (voir [6] et [7]).

Soit $g^*_{\mu,\varphi}$ le polynôme obtenu à partir de $\mathfrak{p}(g_{\mu,\varphi})$ par homogénéisation :

si s est le degré total de $\mathfrak{p}(g_{\mu,\varphi})$

$$g^*_{\mu,\varphi}(X_o, X_1, \ldots, X_n) = X_o^s\, \mathfrak{p}[g_{\mu,\varphi}(\frac{X_1}{X_o}, \ldots, \frac{X_n}{X_o})] \quad .$$

Nous obtenons ainsi une variété projective V^* ; nous voulons montrer que pour tout $\mathfrak{p}$ (sauf un nombre fini) :

V^* contient au moins un point rationnel sur $\mathbb{F}_p$ et tel que $x_o \neq 0$ (point à distance finie).

Soit N le nombre de points de V^* , rationnels sur $\mathbb{F}_p$, on sait que :

$$|N - p^d| \leq \delta . p^{d-\frac{1}{2}} + A p^{d-1} \quad ;$$

δ et A désignant deux constantes indépendantes de p (voir [3]).

Par suite pour p assez grand $N > \frac{1}{2} p^d$. Soit H_o l'hyperplan d'équation $X_o = 0$; V^* n'est pas incluse dans H_o , sinon $\mathfrak{p}(V)$ serait vide.

Désignons par :

- τ le degré de $\mathfrak{p}(V)$
- N_o le nombre de points rationnels de $V^* \cap H_o$
- N_a le nombre de points à distance finie de V^*

$V^* \cap H_o$ est un cycle de degré τ et de dimension $d-1$ donc il existe une constante $B(n, \tau, d)$ telle que :

$$N_o \leq B(n, \tau, d) p^{d-1}$$

(voir [3], lemme 1).

Il en résulte que pour p assez grand $N_a = N - N_o > 0$.

BIBLIOGRAPHIE

[1] - J. AX - Solving diophantine problems modulo every prime (Ann. of Math. vol. 85, 1967, p. 161-171).

[2] - J.R. JOLY - Théorème d'Artin-Tchebotareff (Séminaire de Théorie des Nombres, Grenoble, 20.1.71).

[3] - S. LANG et A. WEIL - Number of points of varietes in finite fields. (Amer. J. Math. 76, 1954, p. 819-827).

[4] - S. LANG - Introduction to Algebraic Geometry.

[5] - J.P. SERRE - Cours d'Arithmétique.

[6] - G. SHIMURA and Y. TANIYAMA - Complex multiplication of abelian varietes and its applications to Number Theory.

[7] - G. SHIMURA - Reduction of algebraic varietes with respect to a discrete valuation of the basic field (Amer. J. Math. 77, 1955, p. 134-176).

[8] - B.L. VAN DER WAERDEN - Einführung in die Algebraische Geometrie.

[9] - B.L. VAN DER WAERDEN - Modern Algebra (vol. II).
