Sur la dimension diophantienne des corps

Cours pour l'Ecole Polytechnique Fédérale de Lausanne

Bruno Deschamps

Lausanne — 2002
(Caen — 2016)

Table des matières

1 Dimension diophantienne

1.1 Le théorème initial

L'histoire commence par le

Théorème 1.– (Chevalley-Warning) *Soient q une puissance non nulle d'un nombre premier p, n un entier non nul, I un ensemble fini d'indices et pour tout $i \in I$, $f_i(X_1, \cdots, X_n) \in \mathbb{F}_q[X_1, \cdots, X_n]$ un polynôme à n indéterminées sans terme constant. Si $\sum_{i\in I} \mathrm{d}^\circ f_i < n$ alors les f_i possèdent un zéro non trivial en commun dans $\mathbb{F}_q^n$.*

Preuve : On note $V \subset \mathbb{F}_q^n$ l'ensemble des zéros communs au f_i et l'on pose

$$P(X_1, \cdots, X_n) = \prod_{i\in I}(1 - f_i^{q-1}(X_1, \cdots, X_n))$$

Le polynôme P est alors la fonction caractéristique de V. Si, pour tout $f \in \mathbb{F}_q[X_1, \cdots, X_n]$, on pose

$$S(f) = \sum_{(x_1,\cdots,x_n)\in\mathbb{F}_q^n} f(x_1, \cdots, x_n)$$

on a alors $S(P) = \sum_{(x_1,\cdots,x_n)\in V} 1 = \sharp V.1$, ce qui assure que $\sharp V \equiv S(P)[p]$.

Considérons un entier k et évaluons la somme $\sum_{x\in\mathbb{F}_q} x^k = 0$:

• Si k est divisible par $q-1$, alors $k = l(q-1)$ et donc si $x \neq 0$, alors $x^k = x^{(q-1)l} = 1^l = 1$. Comme $0^k = 0$ on en déduit que $\sum_{x\in\mathbb{F}_q} x^k = (q-1).1 = -1$.
• Si k n'est pas divisible par $(q-1)$ alors il existe $y \in \mathbb{F}_q^*$ tel que $y^k \neq 1$. Dans ces conditions, on a

$$\sum_{x\in\mathbb{F}_q} x^k = \sum_{x\in\mathbb{F}_q^*} x^k = \sum_{x\in\mathbb{F}_q^*} y^k x^k = y^k \sum_{x\in\mathbb{F}_q^*} x^k$$

(les deux dernières égalités ont lieu puisque $u \longmapsto y^k u$ est un automorphisme de $\mathbb{F}_q^*$) et donc $(1 - y^k)\sum_{x\in\mathbb{F}_q} x^k = 0$. Par conséquent $\sum_{x\in\mathbb{F}_q} x^k = 0$.

Comme $\sum_{i\in I} \mathrm{d}^\circ f_i < n$, il s'ensuit que $\mathrm{d}^\circ P < (q-1)n$. Le polynôme P s'écrit formellement

$$P(X_1, \cdots, X_n) = \sum_{k_1,\cdots,k_n} \alpha_{k_1,\cdots,k_n} X_1^{k_1} \cdots X_n^{k_n}$$

L'hypothèse faite sur le degré implique que pour les n-uplets d'entiers $(k_1, \cdots, k_n)$ considérés dans la somme précédente, on ait $k_1 + \cdots + k_n < (q-1)n$. Maintenant,

$$S(P) = \sum_{k_1,\cdots,k_n} \alpha_{k_1,\cdots,k_n} S(X_1^{k_1} \cdots X_n^{k_n})$$

Nous allons montrer que pour tout choix de n-uplet $(k_1, \cdots, k_n)$ tel que $k_1 + \cdots + k_n < (q-1)n$, nous avons $S(X_1^{k_1} \cdots X_n^{k_n}) = 0$. Constatons tout d'abord que

$$S(X_1^{k_1} \cdots X_n^{k_n}) = \sum_{x_1\in\mathbb{F}_q} \cdots \sum_{x_n\in\mathbb{F}_q} x_1^{k_1} \cdots x_n^{k_n}$$

Par conséquent, si l'un des k_i est nul, par exemple k_n, on a:

$$S(X_1^{k_1} \cdots X_n^{k_n}) = \sum_{x_1\in\mathbb{F}_q} \cdots \sum_{x_{n-1}\in\mathbb{F}_q} x_1^{k_1} \cdots x_{n-1}^{k_{n-1}} \sum_{x_n\in\mathbb{F}_q} x_n^0$$

(en convenant bien sûr que $0^0 = 1$)
Alors $\sum_{x_n \in \mathbb{F}_q} x_n^0 = 0$ et donc $S(X_1^{k_1} \cdots X_n^{k_n}) = 0$.
Supposons maintenant qu'aucun des k_i ne soit nul. On a:

$$S(X_1^{k_1} \cdots X_n^{k_n}) = \prod_{i=1}^{n} S(X_i^{k_i})$$

Par hypothèse, $\mathrm{d}^\circ P < (q-1)n$, donc il existe $j \in I$ tel que $k_i < (q-1)$, d'après ce qui précède, $S(X_j^{k_j}) = 0$ et donc $S(X_1^{k_1} \cdots X_n^{k_n}) = 0$.
□

Corollaire 2.– *Tout polynôme homogène en n variables de degré $d < n$ à coefficients dans un corps finis possède un zéro non trivial.*

L'idée de la dimension diophantienne et de la notion corps de classe C_i est lié à une volonté de donner un équivalent de ce théorème pour les autres corps. Historiquement, il semble que cette idée apparaisse dans la thèse de Lang (où il parle de corps de classe C_2).

1.2 Définitions

Suivant le vieil usage non appelerons *forme* sur un corps K, tout polynôme homogène à coefficients dans K.

Définition 3.– *Soit d un entier non nul et i un réel positif. Un corps K est dit de classe $\mathrm{C}_i(d)$ si toute forme sur K de degré d en $n > d^i$ variables possède un zéro non trivial. Un corps K sera dit de classe C_i s'il est de classe $\mathrm{C}_i(d)$ pour tout d. On définit alors la dimension diophantienne d'un corps K comme étant l'élément*

$$\mathrm{dd}(K) = \inf\{i \in \mathbb{R}^+ / \ K \text{ est de classe } \mathrm{C}_i\}$$

et si l'ensemble considéré est vide, on posera $\mathrm{dd}(K) = +\infty$.

De même, si d désigne un entier non nul, on définit la d-dimension diophantienne d'un corps K comme étant l'élément

$$\mathrm{dd}_d(K) = \inf\{i \in \mathbb{R}^+ / \ K \text{ est de classe } \mathrm{C}_i(d)\}$$

et si l'ensemble considéré est vide, on posera $\mathrm{dd}_d(K) = +\infty$. *Ainsi, on a :*

$$\mathrm{dd}(K) = \sup_d \mathrm{dd}_d(K)$$

Lemme 4.– *Soit K un corps. L'ensemble des réels i tel que K soit de classe C_i est exactement l'intervalle fermé* $[\mathrm{dd}(K), +\infty[$.

Preuve : Il est clair que si K est C_i alors K est C_j pour tout $j > i$. Le point est donc de montrer qu'un corps K est toujours de classe C_α avec $\alpha = \mathrm{dd}(K)$.

Si P désigne une forme en n variables de degré d vérifiant $n > d^\alpha$, par continuité de la fonction $x \mapsto d^x$, il existe un réel $i > \alpha$ tel que $n > d^i > d^\alpha$. Comme K est de classe C_i (par définition de la borne inférieure et par la remarque précédente), P possède un zéro non trivial et par suite K est bien de classe C_α.
□

1.3 Sur la nature arithmétique d'une dimension diophantienne

Tous les réels positifs n'ont pas la chance d'être la dimension diophantienne d'un corps. En effet :

Proposition 5.– *Soit K un corps. Les propriétés suivantes sont équivalentes*

i) K est algébriquement clos,

ii) $\mathrm{dd}(K) = 0$,

iii) $\mathrm{dd}(K) < 1$.

Preuve : *i)* $\Rightarrow$ *ii)* Montrer que $\mathrm{dd}(K) = 0$ équivaut à montrer que K est C_0, c'est-à-dire à prouver que tout forme sur K en plus de deux variables possède un zéro non trivial. Soit donc $P(X_1, \cdots, X_n)$ une telle forme. On peut écrire

$$P(X_1, \cdots, X_n) = \sum_{h=0}^{d} Q_h(X_1, \cdots, X_{n-1}) X_n^h$$

avec $Q_h(X_1, \cdots, X_{n-1}) \in K[X_1, \cdots, X_{n-1}]$ pour tout h. Il est clair qu'il existe un $h_0 > 0$ tel que Q_{h_0} soit non nul. Maintenant, le corps K, étant supposé algébriquement clos, ne peut pas être fini. Il s'ensuit qu'il existe une infinité de $n-1$-uplets $(x_1, \cdots, x_{n-1})$ tels que $Q_{h_0}(x_1, \cdots, x_{n-1}) \neq 0$, donc en particulier, il existe un uplet $(x_1, \cdots, x_{n-1}) \neq (0, \cdots, 0)$ tel que

$$Q_{h_0}(x_1, \cdots, x_{n-1}) \neq 0$$

Le polynôme

$$P(x_1, \cdots, x_{n-1}, X_n) = \sum_{h=0}^{d} Q_h(x_1, \cdots, x_{n-1}) X_n^h$$

est alors non constant et comme K est algébriquement clos, possède une racine x_n. Le n-uplet $(x_1, \cdots, x_n)$ est donc un zéro non trivial de la forme P.

ii) $\Rightarrow$ *i)* Soit $P(X) = a_d X^d + \cdots + a_0 \in K[X]$ un polynôme de degré $d > 0$. Le polynôme homogénéisé $\tilde{P}(X, Y) = a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_0 Y^d$ est une forme en $n = 2$ variable de degré d. Comme $\mathrm{dd}(K) = 0$, K est de classe C_0 et comme $n > d^0$, $\tilde{P}$ possède un zéro non trivial (a, b). Si $b = 0$, alors $a = 0$ ce qui est absurde. Comme $P(a/b) = \tilde{P}(a, b) = 0$; on en déduit que K est bien algébriquement clos.

ii) $\Rightarrow$ *iii)* !

non *i)* $\Rightarrow$ non *iii)* Soit L/K une extension algébrique finie de degré $n > 1$. Soit $(e_1, \cdots, e_n)$ une K-base de L. Le polynôme

$$P(X_1, \cdots, X_n) = \mathrm{N}_{L/K}(X_1 e_1 + \cdots + X_n e_n)$$

est une forme sur K en n variables de degré n. Si l'on avait $\mathrm{dd}(K) = \alpha < 1$ alors le corps K serait C_α et par suite, comme $n > n^\alpha$, le polynôme P possèderait un zéro non trivial. Ceci étant absurde, on en déduit bien que $\alpha \geq 1$.

□

Corollaire 6.– *Si F désigne un corps fini alors* $\mathrm{dd}(F) = 1$.

Preuve : Le théorème de Chevalley montre que F est de classe C_1, la proposition précédente, compte tenu du fait que F n'est pas algébriquement clos, montre que $\mathrm{dd}(F) = 1$.

□

Il a y donc un "trou" dans la droite diophantienne : aucun élément de l'intervalle $]0,1[$ n'est la dimension diophantienne d'un corps. Il est difficile de prévoir la nature arithmétique d'une dimension diophantienne d'un corps. On peut toutefois remarquer que

Proposition 7.– *Soit K un corps et d un entier non nul. Le réel $d^{\mathrm{dd}_d(K)}$ est un entier. En conséquence de quoi, le réel $\mathrm{dd}_d(K)$ est soit rationnel, soit transcendant.*

Preuve : Soit $\alpha = \mathrm{dd}_d(K)$, supposons que le réel d^α ne soit pas entier. En prenant $m = [d^\alpha]$ on a alors $m < d^\alpha < m+1$. La fonction $x \mapsto d^x$ étant strictement croissante et continue, il existe donc un réel $i < \alpha$ tel que $m < d^i < d^\alpha < m+1$. Soit P une forme en n variable de degré d telle que $n > d^i$. Comme n est entier, on a $n \geq m+1$ et par suite, P possède un zéro non trivial. Ainsi K est de classe $\mathrm{C}_i(d)$ ce qui est contraire aux hypothèses.

Ainsi, $\alpha = \log(h)/\log(d)$ avec $h \in \mathbb{N}^*$, et le théorème de Gelfon'd-Scheinder[1] assure alors le résultat annoncé.

□

Cette proposition ne permet pas de déduire quelque chose sur $\mathrm{dd}(K)$, puisque l'ensemble des réels de la forme $\log(h)/\log(d)$ avec h et d entiers est dense.

Problème 8.– *La dimension diophantienne d'un corps est-elle toujours un nombre entier?*

1.4 Théorèmes de transition.

1.4.1 Comment évolue la dimension diophantienne dans une extension ?

Théorème 9.– (Nagata) *Soit K un corps de classe C_i et $f_1, \cdots, f_r$ des formes de degré d en n variables. Si $n > rd^i$ alors il existe un zéro non trivial dans K commun aux formes $f_1, \cdots, f_r$.*

Preuve : • si $d = 1$ c'est un théorème d'algèbre linéaire bien connu. Si K est algébriquement clos, alors on peut supposer $i = 0$ et $n > r$. Le théorème de Bézout sur l'intersection d'hypersurfaces assure alors le théorème. On suppose donc que $d \geq 2$ et que $K \neq \overline{K}$.

• Soit $x \in \overline{K} - K$ et

$$f(X) = X^s + \alpha_1 X^{s-1} \cdots + \alpha_s$$

son polynôme minimal sur K. On pose

$$\begin{array}{lcl} g^{(0)}(X,Y) & = & Y^s f\left(\dfrac{X}{Y}\right) \\ g^{(1)}(X_1,X_2,X_3,X_4) & = & g^{(0)}(g^{(0)}(X_1,X_2), g^{(0)}(X_3,X_4)) \\ & \vdots & \\ g^{(l)}(X_1,\cdots,X_{2^{l+1}}) & = & g^{(0)}(g^{(l-1)}(X_1,\cdots,X_{2^l}), g^{(l-1)}(X_{2^l+1},\cdots,X_{2^{l+1}})) \end{array}$$

Par récurrence immédiate, le polynôme $g^{(l)}$ est une forme sur K en 2^{l+1} variables, de degré s^{l+1} et ne possédant que le zéro trivial sur K. On choisit l tel que $2^{l+1} \geq r$ et on pose $g = g^{(l)}$, $\nu = 2^{l+1}$ et $\delta = s^{l+1}$.

• On pose $h_0 = g$, $\delta_0 = \delta$ et $\nu_0 = \nu$. On définit alors, par récurrence, une suite de polynôme $(h_n)_n$. Soit $\nu_0 = a_0 r + b_0$ la division euclidienne de ν_0 par r. On pose :

$$\begin{array}{lcl} h_1 & = & h_0(f_1(X_1^1,\cdots,X_n^1),\cdots,f_r(X_1^1,\cdots,X_n^1), \\ & & f_1(X_1^2,\cdots,X_n^2),\cdots,f_r(X_1^2,\cdots,X_n^2), \\ & & \cdots \\ & & f_1(X_1^{a_0},\cdots,X_n^{a_0}),\cdots,f_r(X_1^{a_0},\cdots,X_n^{a_0}), \\ & & 0,0,\cdots,0) \quad (b_0 \text{ zéros}) \end{array}$$

[1] Ce théorème affirme que si a et b sont deux nombres algébriques avec b non rationnel, alors le nombre a^b est transcendant.

Le polynôme h_1 est alors une forme sur K de degré $\delta_1 = d\delta_0$ à $\nu_1 = a_0 n$ variables. De même, soit $\nu_1 = a_1 r + b_1$ la division euclidienne de ν_1 par r. On pose :

$$\begin{aligned} h_2 \quad = \quad & h_1(f_1(X_1^1, \cdots, X_n^1), \cdots, f_r(X_1^1, \cdots, X_n^1), \\ & f_1(X_1^2, \cdots, X_n^2), \cdots, f_r(X_1^2, \cdots, X_n^2), \\ & \cdots \\ & f_1(X_1^{a_1}, \cdots, X_n^{a_1}), \cdots, f_r(X_1^{a_1}, \cdots, X_n^{a_1}), \\ & 0, 0, \cdots, 0) \quad (b_1 \text{ zéros}) \end{aligned}$$

Le polynôme h_2 est alors une forme sur K de degré $\delta_2 = d\delta_1$ à $\nu_1 = a_1 n$ variables. Par récurrence, on construit ainsi une forme h_j sur K de degré $\delta_j = d\delta_{j-1}$ en $a_j = a_{j-1} n$ variables.

Le point est alors de remarquer que si j est un indice tel que h_j ait un zéro non-trivial et tel que h_{j-1} n'en ait pas, alors les formes $f_1, \cdots f_r$ ont un zéro non trivial en commun. En effet soit j un tel indice et $x_1^1, \cdots, x_n^{a_{j-1}}, 0, \cdots, 0)$ un zéro non-trivial de h_j. Il existe deux indices k, l tel que $x_l^k \neq 0$ et par ailleurs, comme h_{j-1} ne possède que le zéro trivial, on a

$$f_1(x_1^k, \cdots, x_n^k) = \cdots f_r(x_1^k, \cdots, x_n^k) = 0$$

et donc $(x_1^k, \cdots, x_n^k)$ est un zéro non trivial aux formes $f_1, \cdots, f_r$.

• Comme h_0 ne possède que le zéro trivial, tout revient donc à montrer qu'il existe un j assez grand tel que h_j possède un zéro non-trivial. Mais comme K est de classe C_i, il suffit juste de montrer qu'il existe j tel que $\nu_j > \delta_j^i$. Un récurrence montre déjà que pour tout $j \geq 1$, on a

$$\nu_j > r(d^{ji} - d^{(j-1)i} - \cdots d^i) = \frac{d^{(j+1)i} - 2d^{ji} + d^i}{d^i - 1}$$

et comme $d \geq 2$ et $i \geq 1$, on en déduit donc que

$$\lim_j \nu_j = +\infty$$

Soit maintenant $c > 0$ tel que $n = rd^i + c$. On a

$$\nu_j = \left[\frac{\nu_{j-1}}{r}\right] n \geq \left(\frac{\nu_{j-1}}{r} - 1\right)(rd^i + c) = \nu_{j-1}\left(d^i + \frac{c}{r}\right) - n$$

Il s'ensuit que

$$\frac{\nu_j}{\nu_{j-1}} \geq d^i + \frac{c}{r} - \frac{n}{\nu_{j-1}}$$

Considérons un réel λ tel que $0 < \lambda < c/2r$. Comme $\lim_j \nu_j = +\infty$, il existe un indice j_0 tel que pour tout $j \geq j_0$, on ait $0 < \frac{n}{\nu_{j-1}} < \lambda$. Pour tout $j \geq j_0$, on a alors

$$\frac{\nu_j}{\nu_{j-1}} \geq d^i + \frac{c}{r} - \lambda > d^i + \lambda$$

et ainsi, on a

$$\nu_j \geq \nu_{j_0}(d^i + \lambda)^{j-j_0} \geq rd^{i(j-j_0)} \frac{d^{i(j_0+1)} - 2d^{j_0 i} + d^i}{d^i - 1} \left(1 + \frac{\lambda}{d^i}\right)^{j-j_0}$$

Pour j suffisament grand, on a

$$\frac{d^{i(j_0+1)} - 2d^{j_0 i} + d^i}{d^{ij_0}(d^i - 1)} \left(1 + \frac{\lambda}{d^i}\right)^{j-j_0} > \frac{\delta^i}{r}$$

et donc $\nu_j > (d^j \delta)^i = \delta_j^i$.

□

Théorème 10.– *Soit L/K une extension de degré de transcendance j fini. Si K est de classe C_i alors L est de classe C_{i+j}. En conséquence de quoi, on a l'inégalité*

$$\mathrm{dd}(L) \leq \mathrm{dd}(K) + \mathrm{degtr}(L/K)$$

Preuve : On est ramené à montrer la proposition dans le cas d'une extension algébrique et dans le cas d'une extension transcendante pure (et par récurrence immédiate, dans le cas d'une extension transcendante pure de degré 1).

1er cas : L/K **algébrique.** On suppose donc K de classe C_i. Soit f une forme à coefficients dans L de degré d en n variable telle que $n > d^i$. Nous devons montrer que f possède un zéro non trivial dans L.

Considérons le sous-corps F de L engendré sur K par les coefficients de f. Comme l'extension L/K est algébrique et que les coefficients de f sont en nombre fini, on a $[F : K] = m < +\infty$. Soit alors $\{y_1, \cdots, y_m\}$ une K-base de F. On pose

$$\begin{aligned} g(X_{11}, \cdots, X_{nm}) &= f\left(\sum_{r=1}^{m} y_r X_{1r}, \cdots, \sum_{r=1}^{m} y_r X_{nr}\right) \\ &= \sum_{r=1}^{m} g_r(X_{11}, \cdots, X_{nm}) y_r \end{aligned}$$

où chaque g_r est une forme sur K, de degré d, en nm variables. Puisque $nm > md^i$, il résulte du théorème 9 qu'il existe un zéro commun non trivial $(x_{11}, \cdots, x_{nm}) \in K^{nm}$ aux formes g_r. Puisque $\{y_1, \cdots, y_m\}$ est une base, le n-uplet

$$\left(\sum_{r=1}^{m} y_r x_{1r}, \cdots, \sum_{r=1}^{m} y_r x_{nr}\right) \in F^n$$

est non trivial et est un zéro de f dans L. Donc L est bien de classe C_i.

2ème cas : $L = K(t)$. On suppose donc K de classe C_i. Soit f une forme à coefficients dans L de degré d en n variable telle que $n > d^{i+1}$. Nous devons montrer que f possède un zéro non trivial dans L. En chassant les dénominateurs, on peut supposer que f est à coefficients dans $K[t]$

Si s désigne un entier, on pose :

$$\begin{aligned} g(X_{11}, \cdots, X_{ns}) &= f\left(\sum_{k=1}^{s} X_{1k} t^k, \cdots, \sum_{k=1}^{s} X_{nk} t^k\right) \\ &= \sum_{k=1}^{r+ds} g_k(X_{11}, \cdots, X_{ns}) t^k \end{aligned}$$

où g_k est une forme à coefficients dans K de degré d en ns variables. Si r désigne le maximum des degrés des polynômes-coefficients non nuls de f, on choisit un entier s tel que

$$s(n - d^{i+1}) > rd^i \text{ c'est-à-dire } ns > (r + ds)d^i$$

Le théorème 9 assure l'existence d'un zéro non-trivial $(x_{11}, \cdots, x_{ns}) \in K^{ns}$ de K, commun aux formes g_k. Le n-uplet

$$\left(\sum_{k=1}^{s} x_{1r} t^k, \cdots, \sum_{k=1}^{s} x_{nr} t^k\right)$$

est non trivial et est un zéro de f dans $K[t]$. Donc L est bien de classe C_{i+1}.

□

Théorème 11.– (Lang-Tsen) *Soit K un corps. On a :*

$$\mathrm{dd}(K(T)) = \mathrm{dd}(K) + 1$$

Preuve : On sait déjà, par le théorème 10, que $\mathrm{dd}(K(T)) \leq \mathrm{dd}(K) + 1$. Le corps $K(T)$ est un corps valué pour la valuation normalisée usuelle, v, associée aux polyômes.

Soit $d \geq 2$ un entier et $i < \mathrm{dd}_d(K)$. Par hypothèse, il existe une forme g sur K de degré d en n variables tels que $n > d^i$ ne possédant que le zéro trivial sur K. Posons

$$f(X_{11}, \cdots, X_{nd}) = \sum_{j=1}^{d} g(X_{1j}, \cdots, X_{nj}) T^{j-1}$$

Supposons que f possède un zéro non trivial $(x_{11}, \cdots, x_{nd})$ dans $K(T)$. Pour tout $j = 1, \cdots, d$, notons a_j le ppcm des dénominateurs des fractions rationnelles $(x_{1j}, \cdots, x_{nj})$, de sorte que l'on peut écrire

$$\begin{array}{rcl} 0 & = & f(x_{11}, \cdots, x_{nd}) \\ & = & \sum_{j=1}^{d} g(x_{1j}, \cdots, x_{nj}) t^{j-1} \\ & = & \sum_{j=1}^{d} a_j^{-d} g(y_{1j}, \cdots, y_{nj}) t^{j-1} \end{array}$$

avec $y_{lk} \in K[T]$ et pour tout $j = 1, \cdots, d$, soit $(x_{1j}, \cdots, x_{nj})$ est nul, soit il existe un indice l tel que $v(x_{1l}) = 0$. Il s'ensuit, pour ce dernier cas, que $v(g(y_{1j}, \cdots, y_{nj})) = 0$, puisque la réduction à K du polynôme $g(y_{1j}, \cdots, y_{nj})$ ne peut être nul par hypothèse sur K et sur g. Ainsi, on en déduit qu'il existe deux indices i et j distincts tels que

$$v(a_i^{-d} g(y_{1i}, \cdots, y_{ni}) t^{i-1}) = v(a_j^{-d} g(y_{1j}, \cdots, y_{nj}) t^{j-1}) \neq +\infty$$

et donc $i - j \in d\mathbb{Z}$ ce qui est impossible.

Il existe donc une forme sur $K(T)$ en nd variables de degré d avec $n > d^i$ qui ne possède que le zéro trivial. Donc $\mathrm{dd}_d(K(T)) \geq i + 1$ et par suite $\mathrm{dd}_d(K(T)) \geq \mathrm{dd}_d(K) + 1$. Ainsi $\mathrm{dd}(K(T)) \geq \mathrm{dd}(K) + 1$.

□

Corollaire 12.– *Pour tout corps K, le corps $\overline{K}(T)$ est projectif.*

Preuve : D'après le théorème 11, $\overline{K}(T)$ est un corps C_1 et nous verrons plus loin que les corps C_1 sont toujours projectifs.

□

1.4.2 Le cas des corps valués.

La preuve du théorème 11 utilise une remarque sur les corps valués. On peut apporter quelques précisions à ce sujet. Dans ce qui suit, les valuations considérées auront pour groupe un groupe abélien totalement ordonné. Si v désigne une valuation sur un corps K de corps résiduel k, alors on notera A_v (resp. P_v) l'anneau (resp. l'idéal) de la valuation v. Pour $x \in A_v$, on notera $\overline{x}$ l'image de x dans k. On considérera aussi une section $\varphi : k \longrightarrow A_v$ de l'application $x \longmapsto \overline{x}$.

Théorème 13.– *Soit (K, v) un corps valué (v n'est pas forcément supposée réelle) de corps résiduel k. On a l'inégalité :*

$$\mathrm{dd}(k) \leq \mathrm{dd}(K)$$

Preuve: Montrons que si une forme P à coefficients dans k ne possède que le zéro trivial sur k, alors $\varphi(P)$ ne possède que le zéro trivial sur K.

Considérons une forme $P \in k[X_1, \cdots, X_n]$ de degré d ne possédant que le zéro trivial sur k. Soit $(a_1, \cdots, a_n) \in K^n$ un zéro non trivial de $\varphi(P)$ (que nous noterons abusivement P) dans K. Il existe un indice j tel que $v(a_j)$ soit minimal. Posons, pour tout $i = 1, \cdots, n$, $b_i = a_i/a_j$. On a alors $v(b_i) \geq 0$ et

$$P(a_1, \cdots, a_n) = a_j^d P(b_1, \cdots, b_n)$$

et par suite

$$P(b_1, \cdots, b_n) = 0$$

Maintenant, comme $\overline{P(b_1, \cdots, b_n)} = P(\overline{b_1}, \cdots, \overline{b_n}) = 0$, on en déduit, par hypothèse, que $\overline{b_i} = 0$ pour tout $i = 1, \cdots, n$, ce qui est absurde puisque $b_j = 1$.

Soit $i \geq 0$ un réel tel que k ne soit pas C_i, il existe donc une forme P sur k en n variable de degré d telle que $n > d^i$ et telle que P n'admette que le zéro trivial sur k. D'après ce qui précède, $\varphi(P)$ est une forme en n variables de degré d avec $d < n^i$ qui n'admet que le zéro trivial sur K. Ainsi K n'est pas C_i et donc $\mathrm{dd}(k) \leq \mathrm{dd}(K)$.

□

Si l'on est en mesure de controler l'indice des sous-groupe $dv(K)$ de $v(K)$ pour d entiers, alors on peut affiner encore les choses :

Proposition 14.– *Soit K un corps et v une valuation (non nécessairement réelle) sur K et notons k le corps résiduel de K pour v. Pour tout entier $d \geq 2$ telle $[v(K) : dv(K)] < +\infty$, on a*

$$\mathrm{dd}_d(K) \geq \mathrm{dd}_d(k) + \log_d[v(K) : dv(K)]$$

Preuve : Soit $d \geq 1$ un entier. Considérons un réel $i < \mathrm{dd}_d(k)$ et montrons que $i + \log_d[v(K) : dv(K)] \leq \mathrm{dd}_d(K)$, ceci prouvera la proposition. Il suffit donc de trouver une forme f, à coefficients dans K, de degré d, à $n.[v(K) : dv(K)]$ inderterminée, où $n > d^i$ et possédant seulement le zéro trivial dans K.

Par hypothèse, il existe une forme h à coefficients dans k de degré d à $n > d^i$ indéterminées et possédant seulement le zéro trivial dans k. Il existe donc une forme g à coefficients dans l'anneau de la valuation A_v de degré d en n variables telle que $\overline{g} = h$.

On pose $\delta = [v(K) : dv(K)]$ et l'on se donne $t_1, \cdots, t_\delta \in K$ tels que $\{v(t_1), \cdots, v(t_\delta)\}$ soit une classe de représentants de $v(K)$ modulo $dv(K)$.

Considérons alors la forme $f = \sum_{j=1}^{\delta} g(X_{1j}, \cdots, X_{nj}) t_j$ qui est à coefficients dans K, de degré d et en $n\delta$ variables, et $(x_{11}, \cdots, x_{n\delta})$ un zéro de f dans K. Quitte à permuter les variables, on peut supposer qu'il existe un indice $\delta' \leq \delta$ tel que $x_{ij} = 0$ pour tout $i \leq n$ et tout $j > \delta'$ et que pour $j \leq \delta'$ il existe $i \leq n$ tel que $x_{ij} \neq 0$. Nous allons montrer que $\delta' = 0$.

Supposons que $\delta' \geq 1$, alors pour tout $j = 1, \cdots, \delta'$, considérons un élément $a_j \in K$ tel que $v(a_j) = \min_{1 \leq i \leq n} v(x_{ij})$. Par hypothèse, $a_j \neq 0$ et l'on peut écrire $x_{ij} = a_j y_{ij}$ où $y_{ij} \in A_v$. On a

$$0 = f(x_{11}, \cdots, x_{n\delta}) = \sum_{j=1}^{\delta'} g(x_{1j}, \cdots, x_{nj}) t_j = \sum_{j=1}^{\delta'} g(y_{1j}, \cdots, y_{nj}) a_j^d t_j$$

Puisque $\min_{1 \leq i \leq n} v(y_{ij}) = 0$, il existe un indice i tel que $\overline{y_{ij}} \neq 0$ et donc l'image de $g(y_{1j}, \cdots, y_{nj})$ dans k (qui vaut $h(\overline{y_{1j}}, \cdots, \overline{y_{nj}})$) ne peut pas être nulle car h ne possède que le zéro trivial dans k. Ainsi, il existe au moins deux indices $j_0 \neq j_1$ tels que $v(g(y_{1j_0}, \cdots, y_{nj_0}) a_{j_0}^d t_{j_0}) = v(g(y_{1j_1}, \cdots, y_{nj_1}) a_{j_1}^d t_{j_1}) = 0$. On a alors

$$v(g(y_{1j_0}, \cdots, y_{nj_0})) + dv(a_{j_0}) + v(t_{j_0}) = v(g(y_{1j_1}, \cdots, y_{nj_1})) + dv(a_{j_1}) + v(t_{j_1})$$

et ainsi, $v(t_{j_1}) - v(t_{j_0}) \in dv(K)$, ce qui est absurde. Donc $\delta' = 0$ et f ne possède par conséquent que le zéro trivial.

□

Corollaire 15.– *Si (K, v) est un corps discrètement valué de corps résiduel k alors* $\mathrm{dd}(K) \geq \mathrm{dd}(k) + 1$.

En particulier, on a $\mathrm{dd}(\mathbb{Q}_p) \geq 2$.

1.4.3 Le cas des corps de séries.

Le cas des corps de séries de Laurent jouit de la même propriété que celui des corps de fractions :

Théorème 16.– (Greenberg) *Soit k un corps. On a*

$$\mathrm{dd}(k((T))) = \mathrm{dd}(k) + 1$$

Preuve : En considérant la valuation usuelle sur $k((T))$, on voit que la proposition précédente assure que $\mathrm{dd}(k((T))) \geq \mathrm{dd}(k) + 1$. On va montrer l'autre inégalité dans le cas où k est un corps fini. Dans ces conditions $\mathrm{dd}(k) = 1$ et l'on a donc $\mathrm{dd}(k((T))) \geq 2$. Ainsi, montrer l'égalité $\mathrm{dd}(k((T))) = 2$ revient à montrer que le corps $k((T))$ est C_2.

Soit h une forme de degré d en $n > d^2$ variables à coefficients dans $k[[T]]$. Pour tout entier $i \geq 1$, on considère l'application $\tau_i : k[[T]] \longrightarrow k[T]$ de troncature au degré i. La forme $\tau_i(h)$ est aussi de degré d en $n > d^2$ variables mais à coefficients dans $k[t]$. Puisque $k(t)$ est C_2, $\tau_i(h)$ possède un zéro non trivial $x^{(i)} = (x_1^{(i)}, \cdots, x_n^{(i)}) \in k[T]^n \subset k[[T]]^n$. Quitte à multiplier par une bonne puissance de t, on peut supposer que $(x_1^{(i)}, \cdots, x_n^{(i)})$ est primitif, c'est-à-dire que $\min_j v(x_i^{(j)}) = 0$.

Puisque k est supposé fini, l'anneau $k[[T]]$ est un espace métrique compact. Ainsi, la suite $(x^{(i)})_i$ possède une valeur d'adhérence $x = (x_1, \cdots, x_n)$ et l'on peut la choisir primitive. En effet, si pour $j = 1, \cdots, n$, on note $A_j = \{i \geq 0 / \ v(x_j^{(i)}) = 0\}$, puisque chaque $x^{(i)}$ est primitif on a $A_1 \cup \cdots \cup A_n = \mathbb{N}$ et donc il existe un indice j_0 tel que A_{j_0} soit infini. On a alors, pour tout $i \in A_{j_0}$, $v(x_{j_0}^{(i)}) = 0$ et la suite $(x^{(i)})_{i \in A_{j_0}}$ possède alors une valeur d'adhérence $x = (x_1, \cdots, x_n)$ qui vérifie $v(x_{j_0}) = 0$.

Le passage à la limite montre que, pour tout entier $q \geq 0$, il existe un indice i_q tel que $v(x_j - x_j^{(i_q)}) \geq q$ pour tout $j = 1, \cdots, n$ et que

$$\tau_q(h(x_1, \cdots, x_n)) = \tau_q(h)(x_1^{(i_q)}, \cdots, x_n^{(i_q)}) = 0$$

Ceci étant valable pour tout entier $q \geq 0$, on en déduit que $(x_1, \cdots, x_n)$ est un zéro non-trivial (car primitif) de h.

□

Remarque : Bien que le corps résiduel de $\mathbb{Q}_p$ soit fini (i.e. $\mathbb{Z}_p$ compact), on ne peut appliquer le même argument que dans le théorème de Greenberg à cette situation. Le passage clé dans la preuve précédente est que le corps $k(T)$ est C_2. L'analogue de $k(T)$ dans $\mathbb{Q}_p$ est le corps $\mathbb{Q}$, qui n'est visiblement pas C_2...

Corollaire 17.– *Soit (K, v) un corps discrètement valué complet de caractéristique égale à celle de son corps résiduel et L/K une extension algébrique (valué par le prolongement unique de v). Si k (resp. l) désigne le corps résiduel de K (resp. L), on a les inégalités :*

$$\mathrm{dd}(l) \leq \mathrm{dd}(L) \leq \mathrm{dd}(k) + 1$$

Preuve : Sous les hypothèses de l'énoncé, on sait que K est isomorphe à $k((X))$ (voir par exemple [Ser2]). Le théorème de Greenberg affirme que $\mathrm{dd}(k((X))) = \mathrm{dd}(k) + 1$. L'extension L/K étant algébrique, le théorème de transition sur la dimension diophantienne, assure que $\mathrm{dd}(L) \leq \mathrm{dd}(K)$, ce qui prouve la deuxième inégalité.

La première inégalité est la proposition précédente.

□

Dans le cas d'un corps de séries de Puiseux[2], on obtient en particulier :

Corollaire 18.– *Soit k un corps et* $\mathrm{Puis}(k)$ *son corps de séries de Puiseux. On a*

$$\mathrm{dd}(k) \leq \mathrm{dd}(\mathrm{Puis}(k)) \leq \mathrm{dd}(k) + 1$$

En conséquence de quoi, si $k = \bar{k}$ est algébriquement clos, on a :

- *si* $\mathrm{car}(\bar{k}) = 0$, *alors* $\mathrm{dd}(\mathrm{Puis}(\bar{k})) = 0$;
- *si* $\mathrm{car}(\bar{k}) \neq 0$, *alors* $\mathrm{dd}(\mathrm{Puis}(\bar{k})) = 1$;

en particulier, le corps $\mathrm{Puis}(\bar{k})$ *est toujours projectif.*

Preuve: $\mathrm{Puis}(k)$ est une extension algébrique de $k((X))$ qui est complet à valuation discrète. La valuation ν d'une série de puiseux est donnée par

$$\nu\left(\sum_{k\geq k_0} a_k X^{k/n}\right) = \frac{\inf_{k\geq k_0}(k/\ a_k \neq 0)}{n}$$

Son corps résiduel est k. Le corollaire précédent donne alors les inégalités annoncées.

Si $\mathrm{car}(\bar{k}) = 0$, il est bien connu que $\mathrm{Puis}(\bar{k})$ est algébriquement clos (cf par exemple [Ser2]) et par suite, $\mathrm{dd}(\mathrm{Puis}(\bar{k})) = 0$. Si $\mathrm{car}(\bar{k}) \neq 0$, le théorème montre que $0 \leq \mathrm{dd}(\mathrm{Puis}(\bar{k})) \leq 1$, c'est-à-dire $\mathrm{dd}(\mathrm{Puis}(\bar{k})) = 0$ ou 1. Dire que $\mathrm{dd}(\mathrm{Puis}(\bar{k})) = 0$ revient à dire que $\mathrm{Puis}(\bar{k})$ est algébriquement clos, ce qui est bien connu pour être faux. Donc $\mathrm{dd}(\mathrm{Puis}(\bar{k})) = 1$.

□

1.5 La dimension diophantienne de $\mathbb{Q}_p$

Le corps $\mathbb{Q}_p$ a une dimension diopantienne ≥ 2. On peut le voir "à la main", mais une façon plus directe de le voir est de remarquer que $\mathbb{Q}_p$ n'est pas un corps projectif (nous établirons au paragraphe suivant que les corps de dimension diophantienne < 2 sont toujours projectifs). Il existe une analogie formelle entre le corps $\mathbb{Q}_p$ et le corps $\mathbb{F}_p((T))$. en effet les éléments de $\mathbb{F}_p((T))$ sont des séries de la forme $\sum_{n\geq n_0} a_i T^i$ avec $a_i \in \mathbb{F}_p$, et les éléments de $\mathbb{Q}_p$ ont un développement de Hensel de la forme $\sum_{n\geq n_0} a_i p^i$ avec $a_i \in \mathbb{F}_p$. Bien sur l'arithmétique sur ces deux corps est différente, puisque déjà $\mathbb{F}_p((T))$ est de caractéristique p alors que $\mathbb{Q}_p$ est de caractéristique zéro. Cette analogie a poussé Artin à conjecturer qu pour tout premier p, $\mathrm{dd}(\mathbb{Q}_p) = 2$. Terjanian a montré qu'en fait il n'en est rien :

Proposition 19.– (Terjanian) *Il existe une forme sur $\mathbb{Q}_2$ de degré 4 en 18 variables, ne possédant pas de zéro non trivial. En conséquence de quoi $\mathbb{Q}_2$ n'est pas* $\mathrm{C}_2(4)$ *et*

$$\mathrm{dd}(\mathbb{Q}_2) \geq \mathrm{dd}_4(\mathbb{Q}_2) \geq \log_4 18 > 2$$

[2] Rappelons que si k désigne un corps, on appelle corps des séries Puiseux sur k le corps noté $\mathrm{Puis}(k)$ et égal à la réunion des corps de séries de Laurent $k((X^{1/n}))$ en la variable $X^{1/n}$ (pour être tout à fait rigoureux, $\mathrm{Puis}(k) = \varinjlim_n k((X_n))$, limite inductive prise sur le système inductif $(k((X_n)), \varphi_{nm})_n$ où $k((X_n))$ est le corps des séries de Laurent et $\varphi_{nm} : k((X_n)) \to k((X_m))$ est donnée pour $n|m$, disons $m = an$, par $\varphi_{nm}(X_n) = X_m^a$).

Preuve : Considérons la forme

$$f = X_1^4 + X_2^4 + X_3^4 - X_1^2X_2^2 - X_1^2X_3^2 - X_2^2X_3^2 - X_1^2X_2X_3 - X_1X_2^2X_3 - X_1X_2X_3^2$$

Soit $(x_1, x_2, x_3) \in \mathbb{Z}_2$. Si $x_1, x_2, x_3 \in 2\mathbb{Z}_2$, alors $f(x_1, x_2, x_3) \equiv 0(2^4\mathbb{Z}_2)$, dans le cas contraire, on a $f(x_1, x_2, x_3) \equiv 1(2^2\mathbb{Z}_2)$, c'est-à-dire

$$f(x_1, x_2, x_3) \equiv 1, 5, 9 \text{ ou } 13(2^4\mathbb{Z}_2)$$

Considérons à présent la forme

$$\begin{aligned} g \quad = \quad & f(X_1, X_2, X_3) + f(Y_1, Y_2, Y_3) + f(Z_1, Z_2, Z_3) \\ & +4\left(f(U_1, U_2, U_3) + f(V_1, V_2, V_3) + f(W_1, W_2, W_3)\right) \end{aligned}$$

de degré 4 en 18 indéterminées à coefficients dans $\mathbb{Z}_2$. Si g possède un zéro non-trivial dans $\mathbb{Q}_p$, alors quitte à multiplier par une bonne puissance de 2, g possède un zéro non-trivial dans $\mathbb{Z}_2$ dont une des composantes est une unité. Soit $(x_1, \cdots, w_3)$ un tel zéro. Toutes les composantes $x_1, \cdots, w_3$ sont dans $2\mathbb{Z}_2$ sinon, en vertu de la remarque du début, on ne pourrait avoir

$$g(x_1, \cdots, w_3) \equiv 0(2^4\mathbb{Z}_2)$$

or ceci est absurde, puisqu'une des composantes est une unité 2-adique.

□

Remarque : On a quand même les résultats suivants : pour tout premier p,

- $\mathbb{Q}_p$ est $C_2(2)$ (Hasse).
- $\mathbb{Q}_p$ est $C_2(3)$ (Lewis).

Théorème 20.– (Ax-Kochen) *Pour tout entier $d \geq 1$, il existe un entier $m(d)$ tel que, pour tout premier $p \geq m(d)$, $\mathbb{Q}_p$ est $C_2(d)$ (i.e. seul un nombre fini de corps $\mathbb{Q}_p$ ne sont pas $C_2(d)$).*

Remarque : Le théorème d'Ax-Kochen n'implique pas que $\mathrm{dd}(\mathbb{Q}_p) = 2$ pour p assez grand.

2 Dimension diophantienne et cohomologie

2.1 Corps de classe C_r et dimension cohomologique

On rappelle que la dimension cohomologique d'un corps K est l'entier $\mathrm{cd}(K)$ défini :

$$\mathrm{cd}(K) = \inf\{n \in \mathbb{N} / \ \forall p > n, \ \forall A \ G_K\text{-module de torsion } H^p(G_K, A) = 0\}$$

Les corps séparablement clos (e.g. algébriquement clos) sont donc de dimension cohomologique nulle. Le fait d'être de dimension cohomologique ≤ 1 équivaut, pour un corps, à être projectif (i.e. tout problème de plongement pour G_K admet une solution faible). Rappellons cette importante caractérisation cohomologique des corps projectif (voir Serre, Cohomologie galoisienne) :

Proposition 21.– *Soit K un corps et les propositions suivantes :*

i) K est projectif,

ii) L'application norme $N_{L/K} : L^* \to N^*$ est surjective pour toute extension L/K finie et séparable et, de manière équivalente, pour toute extension L/K séparable,

iii) Le groupe de Brauer $\mathrm{Br}(L)$ est trivial pour toute extension L/K finie et, de manière équivalente, pour toute extension L/K algébrique.

On a ii) $\Longleftrightarrow$ *iii)* $\Longrightarrow$ *i) et l'on a i)* $\Longrightarrow$ *iii) dés que* $\mathrm{car}(K) = 0$ *ou que* $\mathrm{car}(K) = p$ *et que* $\mathrm{Br}(L)(p) = 0$ *pour toute extension* L/K *algébrique.*

Commencons par le cas des corps de classe C_1 :

Proposition 22.– *Tout corps de classe* C_1 *est projectif.*

Preuve : Soit K un corps de classe C_1 et L/K une extension finie de degré n. Soit $(e_1, \cdots, e_n)$ une K-base de L. Soit $x \in K^*$, considérons la forme

$$P(X_0, \cdots, X_n) = \mathrm{N}_{L/K}(X_1 e_1 + \cdots + X_n e_n) - X_0^n x \in K[X_0, \cdots, X_n]$$

Cette forme est en $n+1$ variables et de degré n, donc, comme K est C_1, elle admet un zéro non trivial $(x_0, \cdots, x_n)$. Comme la norme ne s'annulle qu'en zéro, on a forcément $x_0 \neq 0$. L'élément

$$y = \frac{x_1}{x_0} e_1 + \cdots + \frac{x_n}{x_0} e_n$$

vérifie alors $\mathrm{N}_{L/K}(y) = x$. La norme est donc bien surjective.

□

Corollaire 23.– (Wedderburn) *Tout corps fini est commutatif.*

Preuve : Les corps finis commutatifs sont donc projectifs. Soit F un corps fini (éventuellement gauche), soit $Z(F)$ son centre et soit p sa caractéristique. Comme F est fini, l'extension $F/Z(F)/\mathbb{F}_p$ est donc finie. En vertu de la caractérisation précédente de la projectivité, on a $\mathrm{Br}(Z(F)) = 0$ et donc $F = Z(F)$ est commutatif.

□

Problème 24.– *A-t-on toujours pour un corps* K *et un réel positif* r, $\mathrm{dd}(K) \leq r \Longrightarrow \mathrm{cd}(K) \leq r$*?*

D'importants travaux de Suslin et Merkurjev sur le sujet on permis de conclure pour le cas $r = 2$:

Théorème 25.– (Suslin-Merkurjev) *Tout corps de classe* C_2 *est de dimension cohomologique* ≤ 2.

Dans le cas d'une dimension diophantienne dans $[0, 2[$, on peut préciser un peu plus le résultat :

Proposition 26.– *Si* k *désigne un corps tel que* $\mathrm{dd}(K) < 2$ *alors* k *est projectif.*

Preuve : Soit k un corps commutatif et A une k-algèbre simple centrale. On rappelle que la norme réduite sur A est l'application $\mathrm{Nrd} : A \longrightarrow k$ définie de la manière suivante : si L/k désigne un corps neutralisant de A et $f : A \otimes_k L \longrightarrow \mathscr{M}_n(L)$ un L-isomorphisme, alors on pose, pour tout $\alpha \in A$, $\mathrm{Nrd}(\alpha) = \det(f(\alpha \otimes 1))$. On vérifie que cette définition ne dépendant ni de L ni de f.

Si l'on note $n^2 = [A : k]$, alors une fois choisie une k-base de A, on voit que cette application de norme réduite sur A est une forme en n^2 variables de degré n à coefficients dans k. Si A est un corps, alors la norme réduite ne s'annule qu'en 0. Ainsi, si $\mathrm{Br}(k) \neq 0$, alors le corps k est de dimension diophantienne ≥ 2. En prenant la contraposée de cet énoncé, on a donc que tout corps de dimension diophantienne < 2 a un groupe de Brauer nul. Maintenant, si L/k une extension finie alors le théorème 10 assure que $\mathrm{dd}(L) \leq \mathrm{dd}(k) < 2$ et donc $\mathrm{Br}(L) = 0$. La proposition 21 prouve finalement que k est projectif.

□

Le cas limite de l'application du théorème de Suslin-Merkurjev est donc obtenu par des corps de dimension diophantienne 2, comme par exemple les corps $\mathbb{C}(X, Y)$ et $\mathbb{C}((X))((Y))$.

2.2 Un exemple de corps projectif et de dimension diophantienne infinie

Les corps C_1 sont projectifs, la réciproque de cette proposition est fausse. Ax a donné un exemple de corps projectif qui n'est non seulement pas de classe C_1, mais qui est en fait de dimension diophantienne infinie. Nous allons présenter cet exemple dans ce paragraphe.

On note $\mathcal{P}$ l'ensemble des nombres premiers et on définit alors la suite de corps $(k_p)_{p\in\mathcal{P}}$ de la manière suivante :

$$\begin{aligned} k_2 &= \bigcup_{n/(n,2)=1} \mathbb{C}((t_2^{1/n})) \\ k_3 &= \bigcup_{n/(n,3)=1} k_2((t_3^{1/n})) \\ &\vdots \\ k_q &= \bigcup_{n/(n,q)=1} k_p((t_q^{1/n})) \quad \text{si } q \text{ désigne le successeur premier de } p \end{aligned}$$

On note alors $R = \bigcup_p k_p$. Ce corps est projectif et de dimension diophantienne infinie. Le corps R est projectif, on a même un peu plus précisément :

Proposition 27.– *Le groupe de Galois absolu,* $\mathrm{Gal}(\overline{R}/R)$*, du corps R est isomorphe au groupe* $\widehat{\mathbb{Z}}$*.*

Preuve : • Soit K un corps de caractéristique zéro contenant toutes les racines de l'unité et p un nombre premier. On considère le corps $L = \bigcup_{n/(n,p)=1} K((X^{1/n}))$. Le groupe de Galois absolu de L, $G_L = \mathrm{Gal}(\overline{L}/L)$ est isomorphe au groupe $G_K \times \mathbb{Z}_p$.

En effet, K étant de caractéristique zéro, on a

$$\overline{K((X))} = \bigcup_{M/K \ finie} Puis(M)$$

Si on pose

$$M_0 = \bigcup_n L(X^{1/p^n}),\ M_1 = \bigcup_{M/K \ finie} M.L$$

on a alors $\overline{L} = M_0.M_1$. Par ailleurs $M_0 \cap M_1 = L$ et comme K contient les racines de l'unité, l'extension M_0/L est galoisienne (M_1/L l'est aussi visiblement). Ainsi, $G_L \simeq \mathrm{Gal}(M_0/L) \times \mathrm{Gal}(M_1/L) \simeq \mathbb{Z}_p \times G_K$.

• En appliquant ce qui précède, on déduit donc que $\mathrm{Gal}(\overline{k_q}/k_q) \simeq \prod_{p\ premier\leq q} \mathbb{Z}_p$. On vérifie aisément que pour deux nombres premiers $q_1 \leq q_2$, le diagramme suivant

$$\begin{array}{ccc} \mathrm{Gal}(\overline{k_{q_2}}/k_{q_2}) & \longrightarrow & \prod_{p\leq q_2} \mathbb{Z}_p \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\overline{k_{q_1}}/k_{q_1}) & \longrightarrow & \prod_{p\leq q_1} \mathbb{Z}_p \end{array}$$

commute bien, ce qui assure le "passage à la limite" :

$$\mathrm{Gal}(\overline{R}/R) \simeq \prod_{p\ premier} \mathbb{Z}_p \simeq \widehat{\mathbb{Z}}$$

□

Lemme 28.– *Soit K un corps et m un entier non nul. On considère le corps*

$$L = \bigcup_{n/(n,m)=1} K((X^{1/n}))$$

Soit $P \in K[X_1, \cdots, X_k]$ une forme de degré d. Si P, n'a pas de zéro non trivial dans K, alors elle n'en a pas dans L et pour tout k-uplet $(a_1, \cdots, a_k) \in L^k$, on a

$$\nu(P(a_1, \cdots, a_k)) \in d\mathbb{Z}_{(m)}$$

Preuve : Pour $x \in L$, on note $\bar{x}$ la réduction de x dans K. Soit $(a_1, \cdots, a_k) \in L^k$ non trivial et soit a_i l'élément de ce k-uplet de valuation minimal. On pose pour tout $j = 1, \cdots, k$, $b_j = a_j/a_i$ (ainsi $b_j \leq 0$). On a donc

$$P(a_1, \cdots, a_k) = a_i^d P(b_1, \cdots, b_k)$$

Si $P(a_1, \cdots, a_k) = 0$ alors $P(b_1, \cdots, b_k) = 0$ et par suite puisque

$$\overline{P(b_1, \cdots, b_k)} = P(\overline{b_1}, \cdots, \overline{b_k})$$

le k-uplet $(\overline{b_1}, \cdots, \overline{b_k})$ est un zéro non trivial de P (puisque $\nu(b_i) = 0$ et donc $\overline{b_i} \neq 0$) ce qui est absurde.

Maintenant, on a :

$$\nu(P(a_1, \cdots, a_k)) = d\nu(a_i) + \nu(P(b_1, \cdots, b_k))$$

or $\nu(P(b_1, \cdots, b_k)) = 0$ car sinon on aurait à nouveau $P(\overline{b_1}, \cdots, \overline{b_k}) = 0$, et par ailleurs $\nu(a_i) \in \mathbb{Z}_{(m)}$ par définition de ν.

□

Donnons nous maintenant un entier $a \in]0, 1[$ fixé. Pour $m \in \mathbb{N}$ et $p \in \mathcal{P}$, on dit que p est m-représentable si $m = 0$ ou bien si l'on peut écrire $p = p_1 + p_2 + p_3$ avec p_1, p_2, p_3 des nombres premiers $m-1$-représentables vérifiants $p^a < p_1 < p_2 < p_3$. On note dans la suite

$$\lambda(m, a) = \frac{1 - a^m}{1 - a}$$

Lemme 29.– *Si $p \in \mathcal{P}$ est m-représentable, alors il existe une forme sur k_p de degré p en au moins $p^{\lambda(m,a)}$ variables, ne possédant que le zéro trivial sur k_p.*

Preuve : La preuve se fait par récurrence sur l'entier m. Pour $m = 1$, l'application norme de l'extension $k_p(x^{1/p})/k_p$ fournit la forme recherchée.

Supposons établie la propriété au rang $m - 1 \geq 1$ et considérons un nombre premier p, m-représentable. Posons donc $p = p_1 + p_2 + p_3$ avec p_1, p_2, p_3 des nombres premiers $m-1$-représentables vérifiants $p^a < p_1 < p_2 < p_3$ et notons $\mu = \lambda(m-1, a)$. D'après l'hypothèse de récurrence, il existe pour $i = 1, 2, 3$ une forme $H_i(U_1, \cdots, U_{n_i})$ de degré p_i à coefficients dans k_{p_i} ne possédant que le zéro trivial et vérifiant $n_i \geq p_i^\mu \geq p_1^\mu$. Quitte à mettre des zéros dans les variables en trop, on peut supposer que $n_i = n_1 = n$ pour tout i. Soit alors

$$J(U_1, \cdots, U_n) = \prod_{i=1}^{3} H_i(U_1, \cdots, U_n) \in k_{p_3}[U_1, \cdots, U_n]$$

posons

$$\begin{aligned} H(Z_1, \cdots, Z_{pn}) &= \sum_{i=0}^{p-1} t_p^i J(Z_{in+1}, \cdots, Z_{(i+1)n}) \\ &= J(Z_1, \cdots, Z_n) + t_p J(Z_{n+1}, \cdots, Z_{2n}) + \cdots \end{aligned}$$

Le polynôme H est une forme à coefficients dans k_p en np variables de degré $p_1 + p_2 + p_3 = p$, et

$$pn \geq pp_1^\mu > p(p^a)^\mu = p^{1+a\mu} = p^{\lambda(m,a)}$$

Le lemme 28 montre que pour tout n-uplet non trivial $(z_1, \cdots, z_n) \in k_p^n$, on a

$$\nu(J(z_1, \cdots, z_n)) \in p\mathbb{Z}_{(p)}$$

donc en particulier pour tout couple d'indices $i \neq j$ et pour tout pn-uplet non trivial $(z_1, \cdots, z_{np}) \in k_p^{np}$,

$$v(t_p^i J(z_{in+1}, \cdots, z_{(i+1)n})) \neq v(t_p^j J(z_{jn+1}, \cdots, z_{(j+1)n}))$$

ce qui justifie que $H(z_1, \cdots, z_{np}) \neq 0$.

□

Lemme 30.– *Pour tout entier m, il existe c_m tel que pour tout nombre premier $p \geq c_m$, p soit m-représentable.*

Preuve : Le théorème de Vinogradov affirme que si pour N entier on note

$$\theta(N) = \sharp\left\{(p_1, p_2, p_3) \in \mathcal{P}^3 / \ p_1 \leq p_2 \leq p_3 \ et \ N = p_1 + p_2 + p_3\right\}$$

alors il existe une constante $c \in \mathbb{N}$ telle que pour tout $N \geq c$,

$$\theta(N) \geq \frac{N^2}{(\log N)^4}$$

Pour p premier, posons

$$\psi(p) = \sharp\left\{(p_1, p_2, p_3) \in \mathcal{P}^3 / \ p^a < p_1 < p_2 < p_3 \ et \ p = p_1 + p_2 + p_3\right\}$$

Le nombre d'écriture de $p = n_1 + n_2 + n_3$ avec $n_1 \leq p^a$ est majoré par $p^a p = p^{a+1}$. Le nombre d'écriture de $p = n_1 + 2n_2$ est majoré par p, donc

$$\psi(p) \geq \frac{p^2}{(\log p)^4} - p^{a+1} - p \longrightarrow +\infty$$

La proposition est donc vraie pour $m = 1$. Si on la suppose vraie au rang $m-1$ alors l'inégalité précédente la montre pour m en remarquant que (par hypothèse de récurrence) pour p assez grand $\psi(p)$ est précisément le nombre d'écriture $p = p_1 + p_2 + p_3$ avec p_1, p_2, p_3 $m-1$-représentables et $p^a < p_1 < p_2 < p_3$.

□

Proposition 31.– *La dimension diophantienne du corps R est infinie.*

Preuve : Soit un réel $r \geq 1$. Considérons un réel $a \in]0,1[$ tel que $\frac{1}{1-a} > r$, il existe un entier m tel que $\lambda(m,a) > r$. D'après le lemme 30, il existe un nombre premier p qui est m-représentable. Le lemme 29 montre alors qu'il existe une forme P sur k_p de degré p en au moins $p^{\lambda(m,a)} > p^r$ variables, ne possédant que le zéro trivial sur k_p. Enfin, une récurence immédiate appliquée au lemme 28, montre que P ne possède que le zéro trivial sur k_q pour tout $q \geq p$ et par suite sur R

□

On peut remarquer que les corps k_p ont eux une dimension diophantienne finie et que celle-ci croit en fonction de p. Par ailleurs, chacun des corps k_p est projectif.

3 Dimension diophantienne et géométrie

3.1 Quelques rappels de géométrie algébrique

• Soit K un corps Ω un sur-corps algébriquement clos. Si n désigne un entier non nul, on note $\mathbb{A}^n = \Omega^n$ l'espace affine. A toute famille a_0 de polynômes de $K[\underline{X}] = K[X_1, \cdots X_n]$, on associe l'ensemble algébrique

$$V(a_0) = \left\{\underline{x} \in \mathbb{A}^n / \ f(\underline{x}) = 0 \text{ pour tout } f \in a_0\right\}$$

Les ensembles algébriques de $\mathbb{A}^n$ seront appelés les ensembles K-fermés de $\mathbb{A}^n$.

• Si L/K désigne une extension avec $L \subset \Omega$, et A une partie de $\mathbb{A}^n$ on notera

$$I_L(A) = \left\{ f \in L[\underline{X}] / \ f(\underline{x}) = 0 \text{ pour tout } \underline{x} \in A \right\}$$

• Une partie V de $\mathbb{A}^n$ sera dite irréductible si l'on ne peut pas écrire $V = V_1 \cup V_2$ avec V_1 et V_2 deux ensembles K-fermés distincts. Un ensemble K-fermé irréductible sera alors appelé une K-variété.

• Un K-variété V sera dite absolument irréductible, si V reste irréductible vu comme L-variété pour toute extension L/K.

• Une K-variété absolument irréductible V sera dite définie sur K si l'idéal $I_{\overline{K}}(V)$ est engendré par des polynômes de $K[\underline{X}]$ (i.e. $I_{\overline{K}}(V) = \overline{K}.I_K(V)$). Un résultat de Weil montre que si K est un corps parfait alors toute K-variété absolument irréductible est définie sur K.

3.2 Un résultat de théorie de Galois

L'objet de ce paragraphe est de rappeler un résultat de théorie de Galois moderne du à Moshe Jarden. Soit e un entier non nul et $\underline{\sigma} = (\sigma_1, \cdots, \sigma_e) \in G_K^e$. On note $\overline{K}(\underline{\sigma})$ l'extension maximale purement inséparable de $K^{sep}(\underline{\sigma})$. C'est le corps des invariants de $\overline{K}$ par l'unique relevé de $\underline{\sigma}$ à $\overline{K}$. L'intérêt du corps $\overline{K}(\underline{\sigma})$ est qu'il a le même groupe de Galois absolu que $K^{sep}(\underline{\sigma})$ et que si $K^{sep}(\underline{\sigma})$ est PAC alors $\overline{K}(\underline{\sigma})$ l'est aussi mais lui est en plus parfait...

Théorème 32.– *Soit K un corps hilbertien et dénombrable et e un entier non nul. Pour presque tout $\underline{\sigma} = (\sigma_1, \cdots, \sigma_e) \in G_K^e$, le corps $\overline{K}(\underline{\sigma})$ est e-libre et PAC.*

3.3 Corps faiblement C_i

Définition 33.– *Une extension L/K sera dite primaire si l'extension $L \cap \overline{K}/K$ est purement inséparable (ou de manière équivalente si le corps L est linéairement disjoint du corps K^{sep} sur K).*

Proposition 34.– *(a) Si E/K et F/E sont des extensions primaires, alors F/K en est une.*

(b) Si F/K est primaire alors E/K l'est aussi pour tout corps $K \subset E \subset L$.

(c) Toute extension d'un corps séparablement clos est primaire.

(d) une extension F/K est régulière (i.e. $F \cap \overline{K} = K$) si et seulement si elle est séparable et primaire.

Preuve :
□

Définition 35.– *Un corps K est dit faiblement de classe $C_i(d)$ (i réel positif et d entier non nul) si pour toute forme f à coeeficients dans K de degré d en n variables telle que $n > d^i$, l'ensemble K-fermé $V(f)$ de $\mathbb{P}^n$ contient une sous-variété W qui est K fermée.*

Un corps K est dit faiblement C_i s'il est faiblement $C_i(d)$ pour tout d.

Les corps de classe C_i sont visiblement faiblement de classe C_i. La réciproque se trouve réalisée pour les corps PAC parfait, puisque d'après Weil les K-variétés sont définies sur K dés que K est parfait. Dans cette partie nous établirons deux résultats pour les corps faiblement C_i identiques à ceux que nous avons établis pour les corps C_i.

Lemme 36.– *Soit K un corps i un réel positif et d un entier non nul. Les propositions suivantes sont équivalentes :*

i) K est faiblement $C_i(d)$,

ii) toute forme à coefficients dans K en n variables de degré K, telle que $n > d^i$, *possède un zéro non trivial* $\underline{x}$ *tel que* $K(\underline{x})/K$ *soit une extension primaire.*

Preuve :

□

Lemme 37.– *Soit K un corps non-séparablement clos et* e_0 *un entier. Il existe un entier* $e \geq e_0$ *et une forme* ϕ *à coefficients dans K en e variables de degré e telle que si* $K(y_1, \cdots, y_e)$ *est une extension primaire de K alors*

$$\phi(y_1, \cdots, y_e) = 0 \Rightarrow y_1 = \cdots = y_e = 0$$

Preuve :

□

Proposition 38.– *Soit K un corps faiblement* C_i *et soit* $f_1, \cdots, f_r$ *des formes à coefficients dans K de degré d en n variables. Si* $n > rd^i$, *alors* $f_1, \cdots, f_r$ *ont un zéro non trivial en commun dans une extension primaire L de K.*

Preuve :

□

Corollaire 39.– *Soit* L/K *une extension de degré de tanscendance j. Si K est faiblement* C_i, *alors L est faiblement* C_{i+j}.

Preuve : La preuve de ca corollaire se réduit à examiner les cas où L/K est *transcendante pure de degré* 1, *finie et séparable* et *finie et purement inséparable.*

1/ $L = K(t)$.

2/ L/K finie et séparable.

3/ L/K finie et purement inséparable.

□

3.4 La conjecture d'Ax sur les corps PAC et ses conséquences

Les corps PAC sont réputés être projectifs. Ax pose le problème suivant :

Problème 40.– *Est-ce que tout corps PAC est* C_1*?*

L'objectif de ce paragraphe est de donner une application géométrique à cette conjecture.

Théorème 41.– *Soit K un corps hilbertien dénombrable (e.g.* $K = \mathbb{Q}$*). Les propositions suivantes sont équivalentes :*

i) K est faiblement C_i,

ii) pour tout $e \in \mathbb{N}$ *et pour presque tout* $\underline{\sigma} \in G_K^e$, $\overline{K}(\underline{\sigma})$ *est* C_i.

Preuve :

□

Corollaire 42.– *Si le problème d'Ax admet une réponse positive alors toute forme de degré d en* $d+1$ *variables à coefficients dans* $\mathbb{Q}$ *contient une sous-*$\mathbb{Q}$*-variété.*

Preuve :

□