Ktorphée 10 : Quand p premier tend vers 0

Silvain Rideau-Kikuchi

1er juin 2024

1 Un peu de géométrie algébrique

Un phénomène bien connu des géomètres algébristes est que « la grande caractéristique finie » ressemble à la caractéristique nulle. Par exemple,

Théorème 1. *Soient $P_1 \ldots P_n \in \mathbb{Z}[x_1, \ldots, x_m]$. Sont équivalents :*
(i) les P_i ont un zéro commun dans $\mathbb{C}$;
(ii) les P_i ont un zéro commun dans une infinité de $\mathbb{F}_p$;
(iii) les P_i ont un zéro commun dans tous les $\mathbb{F}_p^{\mathrm{a}}$ à un nombre fini près.

On rappelle que, pour tout p premier, $\mathbb{F}_p$ est le corps $\mathbb{Z}/p\mathbb{Z}$. Pour toute puissance $q = p^n$ de p, $\mathbb{F}_q$ est son unique extension de degré n — c'est l'ensemble des racines de $x^{p^n} - x$. Enfin $\mathbb{F}_p^{\mathrm{a}} = \bigcup_q \mathbb{F}_q$ est la clôture algébrique de tous ces corps.

1.1 Construire des zéros dans $\mathbb{C}$

Concentrons nous tout d'abord sur l'implication (ii) ⇒ (i). Soit X un ensemble infini de premiers tels que que pour tout $p \in X$, il existe $x_p \in \mathbb{F}_p^m$ qui est un zéro commun des P_i. On considère l'anneau $A = \prod_{p \in X} \mathbb{F}_p$, muni des opérations coordonnées par coordonnés. Alors $x = (x_p)_{p \in X} \in A^m$ est un zéro commun des P_i (vu comme des polynômes sur A).

Par contre, A n'est certainement pas un corps. Il n'est même pas réduit (il admet des diviseurs de zéro non triviaux). On veut donc quotienter par un idéal maximal. Mais pas n'importe lequel : pour tout $p \in X$, A se projette sur $\mathbb{F}_p$ et le noyau $\mathfrak{m}_p$ de cette projection est un idéal maximal. C'est l'idéal engendré par l'élément dont toutes les coordonnées sont égales à 1 sauf la p-ième coordonnée qui est 0 — on écrira cet élément $1 - a_p$, où a_p est donc l'élément dont toutes les coordonnées sont 0 sauf la p-ième qui est 1. Ce quotient ne nous intéresse pas parce qu'on récupère un des corps de départ (et un des zéros de départ).

Soit I l'idéal engendré par les a_p, pour tout $p \in X$. Soit $\mathfrak{m}$ un idéal maximal qui contient I. Il est distinct de tous les $\mathfrak{m}_p$ puisqu'il contient $a_p \notin \mathfrak{m}_p$. Il ne contient pas non plus p (qui est dans A la suite constante égale à p) : sinon on aurait $p \cdot (\ldots p^{-1} 0 p^{-1} \ldots) = 1 - a_p \in \mathfrak{m}$... Donc

$$A/\mathfrak{m} \text{ est un corps de caractéristique nulle !}$$

On vérifie aisément qu'il est de cardinalité inférieur à $\mathbb{C}$ (qui est de même cardinalité que $\mathbb{R}$ et donc que de $2^{\mathbb{Z}}$ et $\mathbb{Z}^{\mathbb{Z}}$). Après un choix de base de transcendance, il se plonge dans $\mathbb{C}$ en tant que corps[1].

L'image de x dans $A/\mathfrak{m}$, ainsi que son image dans $\mathbb{C}$ est le zéro commun des P_i recherché.

De manière semblable, en considérant les idéaux maximaux $\mathfrak{m}$ de $\prod_p \mathbb{F}_p^{\mathrm{a}}$, on peut obtenir l'implication (iii) $\Rightarrow$ (i). En fait, dans ce cas là $\prod_p \mathbb{F}_p^{\mathrm{a}}/\mathfrak{m}$ est algébriquement clos et isomorphe à $\mathbb{C}$.

Remarque 2. On a fait un usage immodéré de l'axiome du choix dans cette construction (pour trouver $\mathfrak{m}$ et ensuite pour trouver le plongement dans $\mathbb{C}$), cette construction n'est donc absolument pas constructive et je serais assez embêté pour vous exhiber un zéro explicite.

1.2 Construire des zéros dans $\mathbb{F}_p^{\mathrm{a}}$

On a vu précédemment que l'existence de zéros se transfert des $\mathbb{F}_p$ à A puis à $A/\mathfrak{m}$ (et enfin à $\mathbb{C}$). Mais pourrait-on transférer des propriétés plus compliquées, ou transférer dans l'autre sens pour, par exemple, prouver l'implication (i) $\Rightarrow$ (iii). Répondre à cette question nécessite de comprendre un peu plus finement la construction précédente. Commençons par la réinterpréter en termes plus topologiques.

À tout $c = (c_p)_{p\in X} \in A = \prod_{p\in X} \mathbb{F}_p$ on associe $X_c = \{p \in X : c_p = 0\}$ et à tout idéal maximal $\mathfrak{m}$ de $\prod_{p\in X} \mathbb{F}_p$, on associe $\mathfrak{U}_\mathfrak{m} = \{X_c : c \in \mathfrak{m}\}$. C'est un ultrafiltre sur X[2] :

- $X \in \mathfrak{U}_\mathfrak{m}$;
- si $Y, Z \in \mathfrak{U}_\mathfrak{m}$ alors $Y \cap Z \in \mathfrak{U}_\mathfrak{m}$;
- si $Y \in \mathfrak{U}$ et $Y \subseteq Z$ alors $Z \in \mathfrak{U}$;
- pour tout $Y \subseteq X$, on a soit $Y \in \mathfrak{U}$ soit $X \setminus Y \in \mathfrak{U}$.

On vérifie alors qu'on a la bijection suivante :

$$\begin{array}{ccc} \{\text{Idéaux maximaux de A}\} & \leftrightarrow & \{\text{ultrafiltres sur } X\} \\ \mathfrak{m} & \mapsto & \mathfrak{U}_\mathfrak{m} \\ \mathfrak{m}_\mathfrak{U} = \{c : X_c \in \mathfrak{U}\} & \leftarrow & \mathfrak{U} \end{array}$$

L'idéal $\mathfrak{m}_p$ correspond à l'ultrafiltre $\{Y \subseteq X : p \in Y\}$ qui est dit principal en p. Les ultrafiltres qui nous intéressent sont donc les ultrafiltres non principaux. Ils ne contiennent aucun singleton et donc aucun ensemble fini. Ils contiennent donc tous les ensembles fini co-finis.

Ces deux ensembles d'idéaux maximaux et d'ultrafiltres sont naturellement des espaces topologiques compacts et la bijection ci-dessus est un homéomorphisme :

- les fermés de l'ensemble des idéaux maximaux sont les $\{\mathfrak{m} : I \subseteq \mathfrak{m}\}$ pour tout les idéaux I de A. Cet espace topologique est appelé de le spectre de A, muni de la topologie de Zariski[3] ;

[1] Pour être parfaitement honnête, $A/\mathfrak{m}$ est de même cardinalité que $\mathbb{C}$ est sa clôture algébrique est isomorphe à $\mathbb{C}$.

[2] Je vous laisse vérifier, il est utile de se ramener à des éléments $c \in A$ dont toutes les coordonnées sont 0 ou 1.

[3] Pour ceux qui en savent trop, je vous invite à montrer que tous les idéaux premiers de A sont tous maximaux, et que $\mathrm{Spec} A = \mathrm{Spec}_{\max} A$ est séparé.

- les fermés de l'ensemble des ultrafiltres sont les intersections de $\{\mathfrak{U} : Y \in \mathfrak{U}\}$, pour $Y \subseteq X$. Cet espace est le compactifié de Stone-Čech de X pour la topologie discrète[4].

On a vu plus haut que la construction de l'anneau $A/\mathfrak{m}$ préserve l'existence de racines communes aux polynômes sur $\mathbb{Z}$. Mais elle préserve de nombreuses autres propriétés : elle préserve toutes les propriétés qui sont « exprimables au premier ordre ».

Une formule (du premier ordre, dans langage des anneaux) est soit :

1. une formule de base : $P(x_1, \ldots, x_n) = 0$ où $P \in \mathbb{Z}[x_1, \ldots, x_n]$;
2. une combinaison booléenne de formules plus simples : $\varphi \wedge \psi$, $\varphi \vee \psi$ ou $\neg\varphi$;
3. une quantification sur les éléments de l'anneau d'une formule plus simple : $\forall x\, \varphi$ ou $\exists x\, \varphi$.

Si $\varphi(x)$ est une formule[5], R est un anneau et $r \in R^x$, si φ est vérifiée en r dans R, on écrit

$$R \vDash \varphi(r).$$

On vérifie alors (c'est fastidieux mais la principale difficulté est de gérer les indices) le théorème suivant :

Théorème 3 (Łoś). *Soit $\varphi(x)$ une formule et $a = (a_p)_{p \in X} + \mathfrak{m} \in A/\mathfrak{m}$. Alors*

$$A/\mathfrak{m} \vDash \varphi(a) \text{ si et seulement si } \{p \in X : \mathbb{F}_p \vDash \varphi(a_p)\} \in \mathfrak{U}_{\mathfrak{m}}.$$

Ce théorème s'applique plus généralement si on considère une famille $(A_p)_{p \in X}$ d'anneaux indexés par un ensemble X quelconque. L'implication (i)⇒(iii) en découle : s'il existe un ensemble infini X de premiers tels que les P_i n'ont pas de zéro dans $\mathbb{F}_p^{\mathrm{a}}$, alors pour tout ultrafiltre non principal sur X, on a $\mathbb{C} \simeq \prod_{p \in X} \mathbb{F}_p^{\mathrm{a}}/\mathfrak{m}_{\mathfrak{U}}$ et

$$\prod_{p \in X} \mathbb{F}_p^{\mathrm{a}}/\mathfrak{m}_{\mathfrak{U}} \vDash \forall x_1 \ldots \forall x_m \bigvee_i P_i(x_1, \ldots, x_m) \neq 0.$$

Je laisse au lecteur féru de théorie des nombres algébrique le soin de démontrer que (i) ⇒ (ii) ; cela dépasse le cadre ce cet exposé.

Remarque 4. Petit aparté sur les corps algébriquement clos : pour toute formule φ (sans variables libres), les énoncés suivants sont équivalents.

1. La formule φ est vérifiée dans tout corps algébriquement clos de caractéristique nulle ;
2. La formule φ est vérifiée dans $\mathbb{C}$;
3. La formule φ est vérifiée dans tous les corps algébriquement clos de caractéristique première p, sauf pour un nombre fini de p.

L'équivalence des énoncés 2 et 3 découle d'un raffinement de la preuve que l'on vient de faire. L'équivalence avec nécessite un peu plus d'outils logiques, par exemple le théorème de Lowenheim-Skolem.

On peut en déduire un énoncé surprenant en caractéristique nulle :

[4] Ce compactifié n'est pas entièrement nécessaire pour comprendre ces questions d'existence de points, le compactifié d'Alexandrov, qui n'est autre que $\mathrm{Spec}(\mathbb{Z})$, suffit amplement aux géomètres algébriques munis de schémas.

[5] Sauf précision contraire, x peut être un uplet de variables.

Théorème 5 (Ax-Grothendieck). *Soit $f : \mathbb{C}^n \to \mathbb{C}^n$ une application polynomiale injective, alors elle est surjective.*

Ce résultat est clair pour les corps finis $\mathbb{F}_q$. Puisque la restriction d'une injection reste injective, qu'il est vrai sur $\mathbb{F}_p^{\mathrm{a}} = \bigcup_n \mathbb{F}_{p^n}$. Vu que (en bornant le degré sur les polynômes) c'est un énoncé du premier ordre, il se transfert donc à $\mathbb{C}$. Par la même preuve, cela reste vrai pour tout endomorphisme injectif d'une variété sur $\mathbb{C}$!

2 Au delà de la géométrie algébrique

On voudrait à présent se concentrer sur des corps qui ne sont pas algébriquement clos, voire des questions plus analytiques. Le corps le plus naturel à considérer est $\mathbb{R}$ mais il est ordonné et cela se prête assez mal à l'approximation par des corps de caractéristique positive qui ne peuvent pas être ordonnés.

2.1 Les corps p-adiques

On va donc s'intéresser à d'autres complétions de $\mathbb{Q}$ qui sont des objects naturels de la théorie (algébrique) des nombres : les corps de nombres p-adiques. Soit donc p un nombre premier. Pour tout rationnel non nul $q = p^n \frac{a}{b}$ avec a et b premiers entre eux et premiers à p, on pose $\mathrm{v}_p(q) = n$ (et $v_p(0) = 0$).

La fonction $q \mapsto |q|_p = p^{-\mathrm{v}_p(q)}$ est une norme, dite p-adique sur $\mathbb{Q}$. Elle vérifie une version forte de l'inégalité triangulaire appelée l'inégalité ultramétrique :

$$|q_1 + q_2|_p \leqslant \max\{|q_1|_p, |q_2|_p\}.$$

Ce genre d'inégalité triangulaire forte est aussi vérifiée, par exemple, par le degré sur le corps $k(t)$ des fonctions rationnelles sur t (si l'on décide que le degré de 0 est $-\infty$).

La géométrie de ces normes, dites non-archimédiennes, est contre-intuitive puisque tout triangle est isocèle et tout point d'une boule en est le centre. Il en découle que les boules ouvertes sont des fermés (et inversement) dans la topologie induite par cette norme et donc que les seuls sous-ensembles connexes sont les points !

On peut aussi vérifier que la boule unité fermée est un anneau : en l'occurrence, le localisé $\mathbb{Z}_{(p)}$ de $\mathbb{Z}$ en p dont les éléments sont les rationnels de la forme a/b où b est premier à p. C'est même un anneau local donc l'idéal maximal est la boule unité ouverte.

Néanmoins, ces normes ont un contenu arithmétique évident puisqu'elles mesurent à quel point un rationnel est divisible par p.

Comme souvent, il est plus pratique de travailler avec des espaces complets et on considère donc la complétion $\mathbb{Q}_p$ de $\mathbb{Q}$ pour cette norme $|\cdot|_p$. C'est le corps des nombres p-adiques. Sa boule unité fermée est notée $\mathbb{Z}_p$. Elle peut-être présentée de plusieurs manières différentes :

- C'est la « pro-p-complétion » de $\mathbb{Z}$: on a

$$\mathbb{Z}_p \simeq \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}.$$

- C'est l'ensemble des « développements infinis en base p » : on a

$$\mathbb{Z}_p = \{\sum_i a_i p^i : 0 \leqslant a_i < p\}.$$

Naturellement, on peut vouloir comparer $\mathbb{Z}_p$ aux séries entières sur $\mathbb{F}_p$, l'anneau

$$\mathbb{F}_p[[t]] = \{\sum_i a_i t^i : 0 \leqslant a_i < p\}$$

muni des opérations habituelles sur les séries entières (somme coefficient par coefficient et multiplication de Cauchy); alors que les opérations sur $\mathbb{Z}_p$ étendent celles sur $\mathbb{Z}$ en prenant en compte les retenues.

Remarque 6. L'anneau $\mathbb{F}_p[[t]]$ est aussi un complété, le complété de $\mathbb{F}_p[t]$ pour la norme t-adique définie par $|t^n a| = p^{-n}$ si a et t sont deux à deux premiers entre eux.

Une comparaison possible est donnée par l'énoncé remarquable suivant :

Théorème 7 (Principe d'Ax-Kochen-Ershov)**.** *Pour toute formule φ (sans variable libre, dans le langage des anneaux), il existe un entier N tel que, pour tout premier $p > N$,*

$$\mathbb{Z}_p \vDash \varphi \textit{ si et seulement si } \mathbb{F}_p[[t]] \vDash \varphi.$$

Le principe d'Ax-Kochen-Ershov est un des résultats fondateurs de la « théorie des modèles des corps valués ».

Il découle du fait que, si $\mathfrak{U}$ est un ultrafiltre non principal sur les premiers alors les anneaux $\prod_p \mathbb{F}_p[[t]]/\mathfrak{m}_{\mathfrak{U}}$ et $\prod_p \mathbb{Z}_p/\mathfrak{m}_{\mathfrak{U}}$ vérifient les même formules (sans variables libres). En fait, en supposant l'hypothèse du continu, ils sont isomorphes. Ceci est de loin le résultat le plus difficile que l'on a mentionné jusqu'à présent[6] ! Le principe d'Ax-Kochen-Ershov se déduit alors immédiatement du théorème de Łoś (théorème 3).

Une première application est :

Proposition 8. *Soient $P_1, \ldots, P_n \in \mathbb{Z}[x_1, \ldots, x_m]$ des polynômes. Il existe un entier N tel que, pour tout premier $p > N$, toute solution commune des P_i dans $\mathbb{F}_p$ se relève en une solution commune dans $\mathbb{Z}_p$.*

Le théorème 7 n'est pas vraiment nécessaire pour l'énoncé ci-dessus qui peut se déduire directement du « lemme de Hensel ».

Démonstration. Comme $\mathbb{F}_p$ est un sous-anneau de $\mathbb{F}_p[[t]]$ (on l'identifie aux séries constantes), la proposition ci-dessus est vraie dans $\mathbb{F}_p[[t]]$. Elle est donc aussi vraie pour p suffisamment grand par le théorème 7. □

Un application plus difficile est :

[6] Il en existe de nombreuses preuves dans la littérature. Je vous recommande le texte de M. Hils, *Model theory of valued fields*, Lectures in model theory. European Mathematical Society (EMS). 151–180 (2018); ou encore mes notes de cours sur le sujet : https://www.math.ens.psl.eu/~rideau/teaching/val/vf.pdf.

Théorème 9 (Conjecture d'Artin). *Pour tout entier d, il existe un entier N tel que si $p \geqslant N$, tout polynôme P sur $\mathbb{Z}_p$ homogène de degré d en au moins d^2+1 variables a au moins un zéro non trivial dans $\mathbb{Z}_p$.*

Ce résultat est optimal, on connaît des contre-exemples pour $d \geqslant 4$ et p petit. Le même résultat pour $\mathbb{F}_p[[t]]$ (pour tout p) est du à Lang. On en déduit le cas de $\mathbb{Q}_p$ (pour $p \gg 1$) par le théorème 7 en vérifiant que l'énoncé ci-dessus est bien du premier ordre.

2.2 Intégration motivique

On a pour l'instant surtout considéré des questions d'existence de points, mais les anneaux $\mathbb{Z}_p$ et $\mathbb{F}_p[[t]]$ ont aussi une riche structure analytique. Par exemple, ils sont munis d'une mesure de probabilité μ qui est invariante par translation — elle est appelée la mesure de Haar. C'est l'équivalent de la mesure de Lebesgue (qui est la mesure de Haar de $\mathbb{R}$).

Calculons la mesure de certains ensembles, par exemple la boule ouverte b de rayon 1 centrée en 0 qui est respectivement $p\mathbb{Z}_p$ ou $t\mathbb{F}_p[[t]]$ — et qui est aussi la boule fermée de rayon p^{-1}. L'anneau $\mathcal{O}$ est couvert par p translaté de b — un par élément de $\mathcal{O}/b \simeq \mathbb{F}_p$. Du coup,

$$\mu(b) = p^{-1}.$$

Plus généralement, une boule fermée de rayon p^{-i} est couverte par p boules de rayon $p^{-(i-1)}$ et, par récurrence, elle est donc de mesure p^{-i}.

On peut aussi essayer de calculer la mesure de l'ensemble des carrés (si $p \neq 2$). Un élément x de $\mathbb{Z}_p$ est un carré si et seulement si $|x|_p \in p^{2\mathbb{Z}}$ et $x \cdot |x|_p$ est un carré modulo $p\mathbb{Z}_p$ (c'est encore une conséquence de lemme de Hensel). On a donc

$$\mathbb{Z}_p^{\times 2} = \bigcup_{n \geqslant 0} \{x \in \mathbb{Z}_p : |x|_p = p^{-2n} \text{ et } xp^{-2n} + p\mathbb{Z}_p \in \mathbb{F}_p^{\times 2}\}.$$

Comme il y a $\frac{p-1}{2}$ carrés non nuls dans $\mathbb{F}_p$, on a

$$\begin{aligned} \mu(\mathbb{Z}_p^{\times 2}) &= \sum_{n \geqslant 0} \frac{p-1}{2} \cdot p^{-(2n+1)} \\ &= \frac{p-1}{2p} \sum_{n=0} (p^{-2})^n \\ &= \frac{p-1}{2p} \left(1 - \frac{1}{p^2}\right) \\ &= \frac{(p-1)(p^2-1)}{2p^3}. \end{aligned}$$

Pour faire bonne mesure, calculons aussi une intégrale. La fonction est $|x|_p$ est constante égale à p^n sur $p^n\mathbb{Z}_p \smallsetminus p^{n+1}\mathbb{Z}_p$, qui est couvert par $p-1$ translatés de $p^{n+1}\mathbb{Z}_p$. On a donc :

$$\begin{aligned}\int_{\mathbb{Z}_p} |x|_p^s d\mu(x) &= \sum_{n\geqslant 0} p^{-sn}(p-1)p^{-(n+1)} \\ &= \frac{p-1}{p}\sum_{n\geqslant 0} p^{-(s+1)n} \\ &= \frac{p-1}{p}\left(1-p^{-(s+1)}\right) \\ &= \frac{p-1}{p^2}(p-p^{-s}).\end{aligned}$$

On remarque que les résultats de tous ces calculs ont une forme assez similaire. Et ce n'est pas un hasard[7] :

Théorème 10 (Denef). *Soit $X \subseteq \mathbb{Z}_p^n$ définissable par une formule (dans le langage des anneaux) et soit $f \in \mathbb{Q}_p(x_1, \ldots x_n)$. Alors*

$$\int_X |f(x)|^s dx \in \mathbb{Q}(p^{-s}).$$

De plus la fonction obtenue est « uniforme en p » mais cette uniformité est un peu subtile. Soient $P \in \mathbb{Z}[x_1 \ldots, x_n]$ et $X_p = \{x \in \mathbb{Z}_p^n : |P(x)| < 1\}$. Alors

$$\mu_p(X_p) = \frac{1}{p}\#\{x \in \mathbb{F}_p^n : P(x) = 0\}.$$

qui dépend donc du nombre de point dans $\mathbb{F}_p$ d'une variété algébrique sur $\mathbb{Z}$ (toujours la même !).

Comme on l'a vu précédemment dans les exemples précédents, ce genre d'uniformité en p est expliquée par un objet en caractéristique zéro. Un bon candidat ici est $(\prod_p \mathbb{F}_p/\mathfrak{m}_{\mathfrak{U}})[[t]] = k[[t]]$ où $\mathfrak{U}$ est un ultrafiltre non principal sur les premiers.

Comme k est infini, toute mesure invariante par translation sur $k[[t]]$ est nulle. On n'a pas d'intégrale au sens classique sur ce corps. Mais cela n'arrête pas un algébriste ! À défaut de mesure, on peut construire un « invariant additif universel ».

Notons Var_k l'ensemble des variétés sur k — les plus simples d'entres elles, les variétés affines, sont les lieux de zéros de polynômes sur k, le reste des variétés est obtenu en recollant des variétés affines. On note

$$\mathrm{K}_0(\mathrm{Var}_k) = \bigoplus_{V\in\mathrm{Var}_k} \mathbb{Z}[V]/\langle [V] = [U] + [W] : V \simeq U \sqcup W\rangle$$

le groupe abélien libre engendré par les éléments de Var_k quotienté par la relation d'être isomorphe à l'union disjointe de deux autres variétés. On munit de groupe d'une multiplication par $[V]\cdot[W] = [V \times W]$.

La fonction $[\cdot] : \mathrm{Var}_k \to \mathrm{K}_0(\mathrm{Var}_k)$ est une mesure additive que l'on pourrait rendre σ-additive quitte à compléter $\mathrm{K}_0(\mathrm{Var}_k)$. Son seul défaut est de ne pas être à valeur réelle... Mais

[7] On nage à présent dans des eaux profondes. Les résultats qui suivent reposent tous sur des preuves complexes dont le principe d'Ax-Kochen-Ershov (théorème 7) n'est que la prémisse.

elle est universelle par construction : toute mesure additive sur Var_k se factorise à travers $[\cdot]$. En particulier, on a une fonction $\#_{\mathbb{F}_p} : \mathrm{K}_0(\mathrm{Var}_k) \to \mathbb{Z}$ telle que $\#_{\mathbb{F}_p}([V]) = \#V(\mathbb{F}_p)$.

On peut alors développer une théorie de l'intégration sur $k[[t]]$ pour la « mesure » $[\cdot]$ et les fonction définissables — c'est-à-dire essentiellement les fonctions qui (par morceaux définissables) sont de la forme $v_p(P(x))$ où $P \in \mathbb{Z}[x_1, \dots, x_n]$. On en déduit le résultat d'uniformité promis. On note $\mathbb{L} \in \mathrm{K}_0(\mathrm{Var}_k)$, la classe de la droite affine sur k.

Théorème 11 (Denef-Loeser). *Soit $f : \mathbb{Z}_p^n \to \mathbb{Z}$ (resp. $f : \mathbb{F}_p[[t]]^n \to \mathbb{Z}$) une fonction définissable uniformément en $p \gg 1$. Il existe $F \in \mathrm{K}_0(\mathrm{Var}_k)[\mathbb{L}^{-1}](t)$ tel que, pour tout $p \gg 1$,*

$$\int f(x)dx = \#_{\mathbb{F}_p}(F)(p^{-s}).$$

Ce genre de résultats peut permettre, par exemple, de transférer le lemme fondamental du programme de Langlands — qui s'exprime comme une égalité d'intégrale p-adiques — entre $\mathbb{F}_p[[t]]$ et $\mathbb{Z}_p$, pour $p \gg 1$.