Séminaire BOURBAKI Novembre 2022
74e année, 2022–2023, no 1200, p. 121 à 140
doi : 10.24033/ast.1209

SUR UN THÉORÈME DE LANG–WEIL TORDU
[*d'après* E. Hrushovski, K. V. Shuddhodan et Y. Varshavsky]

par **Silvain Rideau-Kikuchi**

Le fil directeur de cet exposé est la grande uniformité du comportement asymptotique, pour les grandes valeurs de q, du morphisme de Frobenius

$$\begin{array}{rccc} \phi_q : & K & \to & K \\ & x & \mapsto & x^q, \end{array}$$

où K est un corps (algébriquement clos) de caractéristique positive p et q est une puissance de p.

Les estimées de Lang et Weil (1954) en sont un exemple classique : étant donné une variété algébrique [(1)] X de dimension d sur $\overline{\mathbf{F}}_p$, pour toute puissance q de p suffisamment grande, X est définie par des équations à coefficients dans $\mathbf{F}_q$ et le morphisme de Frobenius induit un morphisme $\phi_{q,X} : X \to X$. Le nombre de points fixes de $\phi_{q,X}$ est alors de l'ordre de

$$q^d + O(q^{d-1/2}).$$

De plus, la constante du O ne dépend que de la complexité des équations qui définissent X — mais pas de K ou p.

Dans la mesure où les points fixes de ϕ_q^n ne sont rien d'autre que les éléments du corps fini $\mathbf{F}_{q^n}$, l'énoncé ci-dessus est, en fait, une estimation du nombre de points de X dans le corps $\mathbf{F}_{q^n}$; ce qui est la manière classique de présenter le problème.

Un théorème remarquable de Hrushovski (2004) donne une explication générale à ce comportement asymptotique uniforme, du moins pour ce qui est des propriétés que l'on peut exprimer par une formule du premier ordre. Ici, on considère des formules qui s'écrivent avec des symboles pour l'addition, la soustraction, la multiplication, les éléments 0 et 1 et un endomorphisme σ fixé et où on autorise la quantification uniquement sur les éléments des corps que l'on considère. Par exemple, la formule

$$\forall x \forall y \, \sigma(x+y) = \sigma(x) + \sigma(y) \wedge \sigma(x \cdot y) = \sigma(x) \cdot \sigma(y) \wedge \sigma(1) = 1$$

(1) Dans cet exposé, on ne considèrera que des variétés *irréductibles* sur un corps K algébriquement clos.

qui exprime que σ est un morphisme d'anneaux, ou encore les formules

$$\forall x_0 \dots \forall x_n \, (\bigwedge_{i \leqslant n} \sigma(x_i) = x_i) \to \exists y \, \sigma(y) = y \wedge y^{n+1} + \sum_{i \leqslant n} x_i y^i = 0$$

qui expriment que le corps fixé par σ est algébriquement clos.

La théorie des modèles a une riche histoire de tels résultats asymptotiques. L'un des plus anciens est un principe de transfert entre la grande caractéristique positive et la caractéristique zéro, qui découle immédiatement de la compacité de la logique du premier ordre. Pour toute formule ψ *sans le symbole d'automorphisme*,

$$\text{pour tout } p \text{ grand, la formule } \psi \text{ est vérifiée dans } \overline{\mathbf{F}}_p,$$

si et seulement si

$$\text{la formule } \psi \text{ est vérifiée dans } \mathbf{C}.$$

Le théorème de Hrushovski généralise ce principe en prenant en compte le morphisme de Frobenius ϕ_q. D'après ce théorème, celui-ci se comporte pour les grandes valeurs de q comme un automorphisme de corps générique. Plus précisément, il existe une classe de « corps avec automorphisme générique » dont on peut donner une axiomatisation explicite, habituellement notée ACFA — *cf.* proposition 1.2 pour une liste de ces axiomes. Cette classe est l'équivalent, pour les corps avec automorphisme, des corps algébriquement clos pour les corps sans automorphisme et la section 1 de cet exposé a pour but d'en donner une présentation plus exhaustive

Le résultat précis, que nous démontrerons dans la section 3, énonce alors que pour toute formule ψ,

$$\text{pour tout } q \text{ grand } {}^{(2)}, \text{ la formule } \psi \text{ est vraie de } \overline{\mathbf{F}}_q \text{ et } \phi_q,$$

si et seulement si

$$\text{la formule } \psi \text{ est une conséquence des axiomes ACFA.}$$

Ce résultat repose en grande partie sur deux résultats qui décrivent le comportement du morphisme ϕ_q quand q varie. Le premier est un théorème de théorie algébrique des nombres, le théorème de densité de Chebotarev (voir, par exemple, Fried et Jarden, 2008, théorème 6.3.1), qui décrit les liens entre le morphisme ϕ_q et les extensions cycliques des corps de nombres. Le second est un résultat de géométrie algébrique qui généralise les estimées de Lang–Weil. C'est d'ailleurs un phénomène remarquable en soi que les propriétés asymptotiques au premier ordre du morphisme de Frobenius ne dépendent que de ces deux résultats, profonds, mais qui ne semblent *a priori* couvrir qu'une petite partie des propriétés exprimables par des formules.

(2) On considère bien ici toutes les puissances de tous les nombres premiers.

Comme on l'a vu ci-dessus, on peut voir les estimées de Lang–Weil comme un énoncé de comptage du nombre de points fixes du morphisme de Frobenius. On peut naturellement se demander si ce phénomène d'uniformité reste vrai pour des questions de comptage plus générales impliquant l'automorphisme de Frobenius. Le théorème 2.1 donne une réponse positive à cette question — ainsi que son titre à l'exposé.

Pour toute variété X sur un corps K algébriquement clos, on note $X^{(q)} = X^{\phi_q}$ le changement de base de X le long de l'automorphisme de Frobenius et $\phi_{q,X} : X \to X^{(q)}$ le morphisme induit par ϕ_q. Si $X \subseteq K^n$ est le lieu des zéros des polynômes $P_1, \dots, P_m \in K[x_1, \dots, x_n]$, alors $X^{(q)}$ est le lieu des zéros des polynômes $\phi_q(P_i)$ et $\phi_{q,X}$ est l'action de ϕ_q coordonnée par coordonnée.

Les estimées de Lang–Weil tordues affirment alors que, pour toute variété X de dimension d sur K, tout q suffisamment grand et toute sous-variété $C \subseteq X \times X^{(q)}$ vérifiant certaines hypothèses techniques, l'intersection de C avec le graphe du morphisme de Frobenius $\phi_{q,X}$ contient un nombre de points de l'ordre de

$$cq^d + O(q^{d-1/2}),$$

où c est une constante qui dépend de la géométrie de C, et les différentes bornes ne dépendent que de la complexité des équations qui définissent X et C.

Ce résultat est aussi originellement dû à Hrushovski (2004) et sa preuve repose sur le développement de nouveaux outils, intéressants en eux-mêmes, introduits à cette occasion — dont le développement d'une théorie des schémas aux différences ainsi que la théorie des modèles de certains corps valués avec automorphisme. Nous exposerons, dans la section 2, une preuve récente de Shuddhodan et Varshavsky (2022) qui, pour les citer, est « purement géométrique ».

Enfin, dans la section 4, nous discuterons de certaines applications de ces résultats en dynamique algébrique et en géométrie algébrique aux différences.

Pour conclure cette introduction, je voudrais remercier Élisabeth Bouscaren, Antoine Chambert-Loir et Martin Hils pour nos discussions ainsi que leurs nombreux commentaires dont ce texte a grandement bénéficié.

1. Automorphisme générique

Commençons par introduire la notion d'automorphisme « générique » ainsi que divers outils de théorie des modèles nécessaires à sa définition.

Un objet central de ce texte est l'étude des équations dites « aux différences », c'est-à-dire les équations de la forme (pour le cas en une variable)

$$\sum_{i_j \leqslant d} a_i x^{i_0} \sigma(x)^{i_1} \cdots \sigma^n(x)^{i_n} = 0,$$

où les coefficients a_i sont dans un corps K sur lequel on a choisi un endomorphisme σ — on parle alors de corps aux différences (K, σ). Historiquement, le nom d'équations aux différences est hérité du cas où $K = k(t)$ est un corps de fonctions rationnelles sur un corps k et $\sigma(f) = f(t+1)$. Un autre exemple classique est celui des équations aux q-différences où l'on considère le morphisme $\sigma(f) = f(qt)$. Comme on peut le voir dans ces exemples, leur étude est étroitement liée à celle de la dynamique algébrique.

Pour étudier ces équations, il est utile de disposer de « domaines universels » dans lesquels toutes les équations aux différences ont des solutions — voire suffisamment de solutions pour pouvoir en détecter la structure. La théorie des modèles fournit une notion abstraite d'un tel domaine :

Définition 1.1. Un corps aux différences (K, σ) est dit *existentiellement clos* si tout système d'équations aux différences sur K (en plusieurs variables) qui a une solution dans un corps aux différences (L, τ) qui contient K — et dont l'endomorphisme τ étend σ — a une solution dans K.

En d'autres termes, pour toute formule $\psi(x_1, \ldots, x_n)$ sans quantificateurs à paramètres dans K dans laquelle les variables non quantifiées sont parmi $x_1, \ldots, x_n$, si ψ est vérifiée par des éléments $a_1, \ldots, a_n$ d'une extension de (K, σ), elle est déjà vérifiée par des élément $c_1, \ldots, c_n \in K$.

On dit que l'automorphisme σ est *générique* puisque tout comportement possible d'un automorphisme de corps se retrouve dans le corps aux différences (K, σ).

Si l'on travaille seulement dans le langage des anneaux (c'est-à-dire sans le symbole pour l'endomorphisme σ), un corps est existentiellement clos si et seulement s'il est algébriquement clos — c'est exactement ce qu'énonce le *Nullstellensatz* de Hilbert. Il suffit donc dans ce cas de considérer des équations en une seule variable.

Les corps aux différences existentiellement clos sont, par définition, ceux qui vérifient une forme du *Nullstellensatz* pour les équations aux différences. Mais il est aussi possible, dans ce cas, de caractériser quelles équations aux différences doivent avoir une solution dans un corps aux différences pour qu'il soit existentiellement clos.

Soit X une variété sur un corps aux différences (K, σ) (algébriquement clos). On note X^σ le changement de base de X le long de σ et $\sigma_X : X \to X^\sigma$ le morphisme induit par σ. Comme précédemment, si $X \subseteq K^n$ est le lieu des zéros des polynômes $P_1, \ldots, P_m \in K[x_1, \ldots, x_n]$, alors X^σ est le lieu des zéros des polynômes $\sigma(P_i)$ obtenus en faisant agir σ sur les coefficients et pour tout $(a_1, \ldots, a_n) \in X$, $\sigma_X(a) = (\sigma(a_1), \ldots, \sigma(a_n))$.

Un morphisme $f : X \to Y$ entre variétés est dit *dominant* s'il est d'image dense pour la topologie de Zariski. On peut maintenant énoncer la caractérisation suivante, isolée par Hrushovski (*cf.* Macintyre (1997, p. 172-173)), des corps aux différences existentiellement clos :

Proposition 1.2. *Un corps aux différences (K, σ) est existentiellement clos si et seulement si :*

1. *Le corps K est algébriquement clos ;*
2. *Le morphisme σ est surjectif ;*
3. *Pour toute variété affine X sur K et toute sous-variété $C \subseteq X \times X^\sigma$ telle que les projections vers X et X^σ sont dominantes, l'ensemble des couples $(x, \sigma(x))$, avec $x \in X(K)$, est Zariski dense dans C.*

Ces conditions peuvent s'exprimer par un ensemble (infini) de formules. La principale subtilité est de pouvoir quantifier sur les sous-variétés $C \subseteq X \times X^\sigma$. Pour cela, il faut vérifier que, pour toute sous-variété $X \subseteq \mathbf{A}_K^{n+m}$, l'ensemble des $y \in \mathbf{A}_K^n$ tels que la fibre $X_y \subseteq \mathbf{A}_K^m$ est (géométriquement) irréductible est donné par une formule — en d'autres termes, que le lieu d'irréductibilité (géométrique) de la famille X_y est constructible. Mais cela est bien connu, voir par exemple Grothendieck (1966, théorème 9.7.7) ou van den Dries et Schmidt (1984) pour une approche de cette question par le biais d'algèbres de polynômes non standards. La seconde difficulté est de détecter, par une formule, quand un morphisme est dominant. Mais il suffit, pour cela, de savoir que la dimension d'une fibre est continue pour la topologie constructible — voir, par exemple, Grothendieck (1966, théorème 9.5.5).

La classe des corps aux différences existentiellement clos admet donc une axiomatisation (infinie), qui est habituellement notée ACFA. Cette axiomatisation n'est pas complète, c'est-à-dire qu'il existe des corps aux différences (K, σ) et (L, τ) existentiellement clos qui ne vérifient pas les mêmes formules sans variable non quantifiée — on parle habituellement d'énoncés. Pour qu'ils vérifient les mêmes énoncés, il faudrait évidemment que K et L aient la même caractéristique. Mais il faut également que les restrictions des automorphismes à la clôture algébrique de leur corps premier soient conjuguées. Macintyre (1997, p. 173-174) montre que c'est, en fait, suffisant :

Proposition 1.3. *Soient (K, σ) et (L, τ) des corps aux différences existentiellement clos, $F \leqslant K$ un sous-corps aux différences algébriquement clos et $f : F \to L$ un morphisme de corps aux différences — c'est-à-dire un morphisme de corps tel que $\sigma \circ f = f \circ \tau$. Alors pour toute formule $\psi(x_1, \ldots, x_n)$ et tout $a \in F^n$,*

$$a \text{ réalise } \psi \text{ dans } (K, \sigma) \text{ si et seulement si } f(a) \text{ réalise } \psi \text{ dans } (L, \tau).$$

En particulier, deux corps aux différences existentiellement clos (K, σ) et (L, τ) vérifient les mêmes énoncés si et seulement si :

$$\text{les corps aux différences } (K_0, \sigma|_{K_0}) \text{ et } (L_0, \tau|_{L_0}) \text{ sont isomorphes,}$$

où K_0 (respectivement L_0) est la clôture algébrique du corps premier de K (respectivement L).