JOHN B. GOODE

H. L. M. (Hrushovski-Lang-Mordell)

Astérisque, tome 241 (1997), Séminaire Bourbaki,
exp. nº 811, p. 179-194

<http://www.numdam.org/item?id=SB_1995-1996__38__179_0>

Séminaire BOURBAKI
48ème année, 1995-96, n° 811

Février 1996

H. L. M.
(HRUSHOVSKI–LANG–MORDELL)

par **John B. GOODE**

INTRODUCTION

S'il était encore parmi nous, Dieudonné en avalerait son bourbaki ! J'ai été très marqué dans ma jeunesse par ses conférences sur les mathématiques vides et les mathématiques significatives, où il plaçait la Logique pas bien au-dessus du niveau de la fosse à purin (mais c'était pas le plus bas), tandis que la Géométrie, je veux dire l'algébrique, planait à des hauteurs éthérées où seuls pouvaient s'élever les esprits les plus subtils. Quoi qu'on en ait dit à l'époque, cette classification ne révélait ni intolérance, ni fermeture d'esprit : je me rappelle l'avoir vu très intéressé par une conférence, dans ce même séminaire, sur le modèle de Solovay, où tous les ensembles de réels sont mesurables ; il en tirait joyeusement la conclusion que la Logique était la science qui permettait de prouver n'importe quoi. Je ne peux m'empêcher de me demander quelle aurait été sa réaction aujourd'hui ; aurait-il admis que la Logique se permît de poser ses pattes sales sur la formelle beauté des courbes et des nombres, et dérivât avec insolence, comme simple corollaire, la solution d'un problème ouvert de type mordellien d'un résultat longtemps attendu en Théorie des modèles ?

Car c'est bien là le caractère le plus surprenant de la preuve que je vais présenter aujourd'hui. Son auteur, Ehud Hrushovski, ne s'est pas mis en tête, un jour, de s'atteler à la tâche de prouver la conjecture de Lang ; non, mais quand il en a entendu causer, il a tout de suite vu que ça entrait dans le cadre de la notion de "structure de Zariski" qu'il venait de dégager, en compagnie de Boris Zil'ber. Voir l'unité profonde de questions sans rapports apparents, c'est le propre des mathématiciens qui créent, s'il m'est permis d'user d'une terminologie typiquement dieudonnienne.

À mon (humble) avis, c'est la première fois que la Logique sert vraiment à montrer un résultat impliquant des objets mathématiques classiques. Comme la Logique, en tant que spécialité mathématique, est une discipline plutôt neuve, les logiciens aiment bien pouvoir brandir ce genre d'étendard. Le drapeau précédent, c'était le théorème d'Ax et Kochen, qui résolvait asymptotiquement une conjecture d'Artin ; un beau succès, mais où la Théorie des modèles n'intervenait guère que par un principe de compacité ; et puis, je suis persuadé que le but que s'étaient fixé MM. Ax et Kochen, c'était bien dès le début de résoudre la conjecture d'Artin !

Cela étant dit, précisons ce dont on parle. Considérons l'énoncé suivant :

A. *Soient K un corps, S une variété abélienne définie sur K, X un fermé de Zariski de S, et Γ un sous-groupe de S de type fini ; alors $X \cap \Gamma$, s'il n'est pas vide, s'exprime comme une réunion finie $a_1 + \Gamma_1 \cup \ldots \cup a_n + \Gamma_n$, où les $a_i + \Gamma_i$ sont des cossettes modulo des sous-groupes Γ_i de Γ.*

Explication de texte : "de type fini" signifie que Γ est finiment engendré à division près, mais qu'on ne divise pas par la caractéristique. Autrement dit, il existe un système fini $g_1, \cdots g_m$ d'éléments de S tels que tout x dans Γ satisfasse une relation $n \cdot x = n_1 \cdot g_1 + \cdots n_m \cdot g_m$, à coefficients entiers relatifs, où n est non-nul, et même non-divisible par p si on est en caractéristique p. On remarque que Γ est le seul objet discret, non géométrique, de l'énoncé.

Toute personne siégeant dans cette assemblée éminente a vu le rapport de cet énoncé A avec la conjecture de Mordell, déclarant qu'une courbe de genre au moins deux n'a qu'un nombre fini de points rationnels sur un corps de nombres (ou extension de degré fini du corps des rationnels) ; ce paragraphe n'est destiné qu'au logicien égaré dans la consultation des actes de ce séminaire. Soit X notre courbe ; elle apparaît comme un fermé de sa jacobienne S, qui est une variété abélienne ayant pour dimension le genre de X ; d'après un théorème d'André Weil (voir [WEIL 1948]), les points de S rationnels sur un corps de nombres forment un groupe Γ de type fini ; pour pouvoir assimiler les variétés à leur ensemble de points K–rationnels, nous remplaçons K par sa clôture algébrique ; si nous supposons que $a_i + \Gamma_i$ est infini et contenu dans X, irréductible de dimension un, il en est de même de sa clôture de Zariski $a_i + clz(\Gamma_i)$, et il faut alors que la courbe elle–même soit cette cossette, qu'elle porte une structure de groupe algébrique, donc qu'elle soit de genre un (ou zéro, mais là il n'y a pas de jacobienne !) ; si donc le genre est supérieur à deux, l'énoncé A implique que $X \cap \Gamma$ est fini, c'est-à-dire la conjecture de Mordell.

Je rappelle que cette conjecture a été prouvée par Faltings dans [FALTINGS 1983] ; c'est également Faltings qui a prouvé l'énoncé A en caractéristique nulle ; plus exactement, il a apporté la touche finale à une œuvre collective : voir [LANG 1991] ;

on consultera également [LANG 1995] à propos des évé(è)nements pittoresques qui peuvent se produire dans les milieux académiques. C'est donc un énoncé plus puissant que la conjecture de Mordell en caractéristique nulle ; qu'en est–il en caractéristique p ? Eh bien, il est trop puissant, pour la raison triviale que, si K est la clôture algébrique du corps premier $\mathbf{F}_p$, le groupe S lui–même est de torsion, qu'il lui arrive de ne pas avoir de p-éléments, et qu'il y a pourtant des courbes qui ne sont pas des cossettes ! Il faut donc le modérer par une hypothèse supplémentaire :

B. *Notons k la clôture algébrique du corps premier ($\mathbf{Q}$ ou $\mathbf{F}_p$) ; on suppose en outre que la trace de S sur k est nulle, c'est-à-dire qu'il n'existe pas d'homomorphisme (au sens géométrique) non nul entre une sous–variété abélienne de S et une variété abélienne définie sur k.*

C'est l'énoncé A avec l'hypothèse B qui est prouvé par Hrushovski : cet $A+B$ est connu sous les noms de "conjecture géométrique de Mordell–Lang", ou "conjecture de Mordell–Lang pour les corps de fonctions" ; elle apparaît dans [LANG 1965]. La preuve de [HRUSHOVSKI 199?] est uniforme en caractéristique nulle et en caractéristique p, ne variant que par la structure auxiliaire utilisée ; c'est la première preuve de la conjecture en ce qui concerne la caractéristique p.

Elle procède ainsi : on munit le corps K d'une structure supplémentaire (corps différentiellement clos en caractéristique nulle, corps séparablement clos en caractéristique p) ; pour qu'il puisse porter cette structure, il faut éventuellement l'élargir, mais ça n'a pas d'importance : c'est au corps k qu'il ne faut pas toucher ; on remplace Γ par un groupe G plus grand, mais qui est définissable, c'est-à-dire "géométrique" au sens de cette structure enrichie ; en caractéristique nulle, on utilise pour cela un homomorphisme entre la variété abélienne S et un groupe vectoriel, introduit par Manin ; en caractéristique p, on se débrouille avec le noyau p-divisible de S. L'important, c'est que cette structure enrichie reste maniable, qu'aux objets qui y sont définissables soit associée une notion de dimension analogue à la dimension en Géométrie algébrique. La situation sera contrôlée par ce que tous les ensembles de dimension un seront des "structures de type Zariski" ; l'hypothèse B permettra d'exploiter le fait que k sera le seul corps de dimension finie définissable dans K. Les détails suivent.

Je remercie Françoise DELON, Carlo GASBARRI et Olivier MATHIEU pour les corrections qu'ils ont apportées à la première version de cet exposé.

1. STRUCTURES DE TYPE ZARISKI : LE RÉSULTAT SÉRIEUX

Il aura fallu trois lustres, de Morley à Zil'ber, pour que les théoriciens des modèles se rendent compte qu'ils étudient les mêmes objets que les géomètres algébriques, à savoir ceux qui sont définissables dans un corps algébriquement clos. Je ne fais pas ici l'histoire de cette convergence ; ça serait pourtant bien intéressant, car le plus surprenant dans ce résultat, pour un mathématicien normal, c'est de voir d'où il sort !

Les géomètres et les logiciens n'abordent pas ce corps K de la même façon ; je rappelle qu'un fermé de Zariski est une partie de K^n définie par un système d'équations polynomiales, tandis qu'un constructible est une combinaison booléenne d'un nombre fini de fermés de Zariski. Disons en première approximation que les géomètres travaillent au niveau des fermés de Zariski, tandis que les logiciens vivent dans les constructibles. Mais aussi les logiciens travaillent à un niveau d'abstraction supérieur à celui des géomètres (c'est pas de la provoc) : ces derniers se donnent dès le départ un corps, des anneaux locaux, des dérivations, etc., bref une grande richesse structurelle, tandis que les logiciens n'ont rien, ou presque : seulement une notion abstraite de dimension ! Il faut donc s'attendre à ce que la Théorie des modèles produise des théorèmes plus généraux, donc plus vagues, moins précis que ceux de la Géométrie ; et pourtant elle arrive à quelque chose !

La notion suivante d'"ensemble fortement minimal", formalisant la notion de structure connexe de dimension un, est apparue dans la foulée des travaux de Michael Morley sur la catégoricité en aleph-un.

On se donne un ensemble M infini, et pour chaque entier n une famille de parties de M^n, qu'on appelle les ensembles définissables (avec paramètres) au sens de M ; ils doivent satisfaire aux conditions suivantes :

(i) les parties définissables de M^n forment une algèbre de Boole : si A et B sont définissables, il en est de même de $A \cap B$, $A \cup B$, et du complément de A ;

(ii) le produit cartésien d'une partie définissable A de M^m et d'une partie définissable B de M^n est une partie définissable de M^{m+n} ; les singletons $\{x \,/\, x = a\}$ et les diagonales $\{(x,y) \,/\, x = y\}$ sont définissables ; une permutation des variables transforme un ensemble définissable en un autre ;

(iii) la projection sur M^n d'une partie définissable de M^{n+1} est définissable ;

(iv) M est uniformément (irréductible et) de dimension un, ce qui signifie qu'à toute partie définissable $X(x, \mathbf{y})$ de M^{1+n} est associé un entier e, tel que, pour tout

$\mathbf{a}$ de M^n, ou bien $X(x, \mathbf{a})$ contienne au plus e éléments, ou bien $X(x, \mathbf{a})$ contienne tous les éléments de M sauf au plus e.

Prenons pour ensemble M un corps K algébriquement clos, et considérons les trois exemples suivants, qui satisfont – le lecteur s'en convaincra – à ces quatre conditions :

a) les ensembles définissables sont les combinaisons booléennes de singletons et de diagonales ;

b) les ensembles définissables sont les combinaisons booléennes d'ensembles définis par des équations linéaires $m_1 \cdot x_1 + \cdots + m_n \cdot x_n = a$, à coefficients entiers relatifs, et à second membre dans K ;

c) dans le premier exemple, on n'utilise pas de structure du tout (seulement que K est un ensemble M infini), et dans le deuxième seulement l'addition, c'est-à-dire la structure d'espace vectoriel sur le corps premier ; dans ce troisième exemple, on utilise somme et produit et on prend pour ensembles définissables les parties constructibles de K^n.

Ces trois exemples sont typiques, car ils illustrent une trichotomie établie par Boris Zil'ber dans [ZIL'BER 1984] :

α) *le cas trivial* ; on ne peut alors définir de groupe infini dans M ;

β) *le cas modulaire* ; l'ensemble M, s'il n'est pas lui–même porteur d'une structure de groupe (définissable !), est cependant étroitement associé un groupe fortement minimal ; tous les groupes G qu'on peut alors interpréter (*i.e.* dont l'ensemble sous–jacent est le quotient d'un ensemble définissable par une relation d'équivalence définissable, et dont la loi de groupe est bien sûr définissable) dans M sont modulaires, ce qui signifie que toute partie définissable de G (et de G^n !) est combinaison booléenne de cossettes modulo des sous-groupes définissables ; tous ces groupes sont abéliens par finis, et on ne peut interpréter de corps infinis ($GL_n(K)$ n'est pas abélien par fini !) ; on voit ce qui a fait tilt dans le crâne de Hrushovski à propos de l'énoncé de la conjecture de Mordell–Lang, dans lequel on peut remplacer S par S^n et Γ par Γ^n : il s'agit tout simplement de montrer que la géométrie algébrique n'induit sur Γ qu'une structure modulaire !

γ) *le troisième cas* ; Zil'ber montre qu'on peut alors y définir une structure appelée pseudo–plan, qui ressemble à un plan projectif. Il a conjecturé que, dans ce cas, on devait pouvoir interpréter un corps infini K (qui ne peut qu'être algébriquement clos d'après [MACINTYRE 1971]). À l'origine, cette conjecture n'impliquait pas d'arrière–pensée, mais quand, en 1986, j'ai sommé Zil'ber de préciser, il a admis que ce corps

K ne devait pas porter de structure plus riche que celle d'un corps (algébriquement clos), c'est-à-dire que les parties de K^n définissables au sens de M n'étaient rien d'autres que les constructibles au sens du corps K. Vu sous cet angle, ça devenait une conjecture extrêmement ambitieuse, postulant que tout objet de dimension un était essentiellement connu, étant fortement corrélé à un objet classique.

Eh bien, Hrushovski a montré qu'elle était brutalement fausse, en construisant dans [HRUSHOVSKI 1993], à partir de rien, un ensemble fortement minimal non–trivial qui n'interpète pas de groupe ; dans la foulée, [BALDWIN 1994] en a construit un qui interprète un plan projectif (non arguésien !) et pas de corps, et [BAUDISCH 1995] un autre qui interprète un groupe 2–nilpotent non abélien par fini et pas de corps. Pour ce qui est de la structure supplémentaire, Hrushovski a réussi plus récemment un mélange fantastique : prenant par exemple deux structures de corps algébriquement clos de degré de transcendance dénombrable, l'un de caractéristique deux, l'autre de caractéristique trois, il réussit à les poser simultanément sur le même ensemble M tout en gardant la forte minimalité (voir [HRUSHOVSKI 1992]) !

Quand Shiva a détruit, Vishnu reconstruit. Zil'ber et Hrushovski ont sauvé la trichotomie en introduisant une notion abstraite de fermés de Zariski, et en demandant qu'ils satisfassent le Hauptidealsatz (si on ajoute une équation, on ne peut faire choir la dimension que de un).

Ils appellent *structure de Zariski* la donnée d'un ensemble M, avec une topologie sur chaque M^n , satisfaisant aux conditions suivantes :

(i) les conditions usuelles définissant les topologies ;

(ii) toute application de M^m dans M^n dont les coordonnées sont des projections ou des constantes est continue ; singletons et diagonales sont fermés ;

(iii) la projection d'un fermé de M^{n+1} est un constructible (= combinaison booléenne de fermés) de M^n ;

(iv) M est uniformément (irréductible et) de dimension un, c'est-à-dire qu'à tout fermé $X(x, \mathbf{y})$ de M^{1+n} est associé un entier e, tel que, pour tout $\mathbf{a}$ de M^n , ou bien $X(x, \mathbf{a})$ contienne au plus e éléments, ou bien $X(x, \mathbf{a})$ soit M tout entier ;

(v) si X est un fermé irréductible de dimension d, chaque composante de son intersection avec une diagonale est de dimension au moins $d-1$ (ici, la "dimension" est la dimension topologique ; on voit sans peine que les axiomes imposent aux topologies d'être noethérienne, et que M^n est de dimension n).

Ces axiomes forcent les constructibles de M à former une structure fortement minimale au sens précédent ; nos trois exemples provenaient bien chacun d'une structure de Zariski :

a) prendre pour fermés les combinaisons booléennes positives de diagonales et de singletons ;

b) prendre pour fermés les combinaisons booléennes positives d'ensembles de solutions d'équations linéaires à coefficients entiers ;

c) prendre les fermés de Zariski usuels ; plus généralement, si C est une courbe lisse, les topologies de Zariski sur les C^n forment une structure de Zariski ; ce n'est pas toujours le cas d'une courbe non lisse (cubique à point double, où (v) n'est pas vérifié), mais ça peut arriver (cubique à point de rebroussement, topologiquement équivalente à sa normalisée).

Dans une structure de Zariski, on appellera famille de courbes planes la donnée d'un fermé $X(x, y, \mathbf{z})$ de M^{2+n} tel que, pour chaque $\mathbf{a}$ de M^n, $X(x, y, \mathbf{a})$ soit un fermé irréductible de dimension un de M^2 ; on dit que la structure est ample si elle possède une famille de courbes telle que par deux points p et q du plan en position générique (*i.e.* pour tous p et q d'un ouvert non vide du plan M^2), il passe une courbe de la famille.

C'est ainsi que ni a) ni b) ne sont amples : dans le premier cas, on ne peut guère définir, comme familles de courbes, que les parallèles aux axes $x = a$ ou $y = b$, et dans le deuxième les parallèles $n \cdot x + m \cdot y = a$ à une direction (rationnelle !) donnée ; tandis que c) est ample, puisqu'on peut y définir la famille de toutes les droites $a \cdot x + b \cdot y = c$ du plan.

Le résultat de [HRUSHOVSKI-ZIL'BER 1993 et 199?] est le suivant : si la structure de Zariski n'est pas ample, l'ensemble minimal associé est trivial ou modulaire ; si elle est ample, on peut y interpréter un corps algébriquement clos k, unique à isomorphisme définissable près, et qui n'est rien d'autre qu'un corps : ses parties définissables dans M sont les constructibles au sens des corps. L'article contient en outre une caractérisation des topologies de Zariski des courbes lisses : je n'en parle pas car nous n'en aurons pas besoin ici.

2. NOTE DU CRU DE L'AUTEUR

[HRUSHOVSKI-ZIL'BER 1993] ne résoud pas tous les problèmes à propos de la trichotomie de Zil'ber. Par exemple, on ne sait toujours pas si elle est vraie pour un ensemble fortement minimal interprétable dans un corps algébriquement clos (où les parties définissables de M sont certains constructibles). De plus, c'est une théorie vraiment adaptée à la dimension un ; il serait intéressant de pouvoir caractériser abstraitement la topologie de Zariski d'un groupe algébrique : c'est une de mes obsessions depuis [POIZAT 1984].

Cette obsession mérite quelques explications : étant donnée une variété V, il n'y a pas de sens à chercher à distinguer les fermés, parmi les constructibles, par une propriété particulière, tout simplement parce que les bijections constructibles ne sont pas continues (elles le sont seulement "génériquement"), et ne conservent pas la notion de fermé. Mais cela fait sens si cette variété algébrique est un groupe algébrique G , et qu'on insiste sur la préservation de sa loi de groupe, car tout automorphisme abstrait σ de ce groupe G qui, pour chaque n, envoie les contructibles de G^n sur les constructibles de G^n, envoie aussi ses fermés sur ses fermés. En effet, tout isomorphisme abstrait entre un groupe algébrique G_1 sur un corps algébriquement clos K_1 , et un groupe algébrique G_2 sur un corps algébriquement clos K_2, qui envoie constructible sur constructible, se décompose en une application induite par un isomorphisme des corps de base et un morphisme géométrique : la démonstration est la même que celle du théorème de Borel–Tits donnée dans [POIZAT 1988].

Un groupe G constructible, qui finalement doit être constructiblement isomorphe à un groupe algébrique (voir [POIZAT 1987]), a donc parmi ses constructibles des éléments bien particuliers, ceux qui deviennent fermés de Zariski quand on en fait un groupe algébrique, quelle que soit la manière dont on s'y prend. Ça serait bien d'avoir une autre caractérisation de ces fermés, du genre de celle des constructibles génériques, ceux qui sont d'intérieur non vide, qui sont également ceux dont un nombre fini de translatés recouvrent G : on sait quelles bonnes propriétés ont les génériques, ainsi définis, dans le contexte des groupes stables, un contexte bien plus large que celui des groupes de rang de Morley (= dimension) fini. Le rêve est donc le suivant : trouver une caractérisation des fermés de Zariski faisant sens pour un groupe stable, ou du moins distinguer des groupes stables "avec topologie de Zariski", sans référence à la dimension !

3. LA CARACTÉRISTIQUE NULLE

Comme je l'ai dit, la démonstration est la même en toute caractéristique, sauf qu'on n'emploie pas la même structure auxiliaire, ce qui justifie la séparation en deux sections. Nous traitons ici de la caractéristique zéro.

Comme je l'ai dit également, l'énoncé à prouver n'est pas affecté par une extension du corps K : il importe seulement de ne pas toucher à k. Nous supposons donc que K est algébriquement clos et de degré de transcendance infini sur k ; dans ces conditions, il existe une dérivation de K, dont k est le corps de constantes (éléments de dérivé nul), et qui fait de K un corps différentiellement clos.

Les corps différentiellement clos sont aux corps différentiels (= corps munis d'une dérivation) ce que sont les corps algébriquement clos aux corps ordinaires : ce sont ceux qui satisfont le Théorème des Zéros de Hilbert, à savoir que tout système formé d'un nombre fini d'équations et d'inéquations polynomiales différentielles (*i.e.* des polynômes en les inconnues et leurs dérivées successives), à coefficients dans K, qui a une solution dans une extension de K, en a une dans K.

En caractéristique nulle, la machine fonctionne bien : tout corps différentiel a une "clôture différentielle" uniquement déterminée à l'isomorphie près. Si K est différentiellement clos, on définit les fermés de Zariski différentiels comme étant les ensembles solutions de systèmes d'équations différentielles polynomiales ; ça donne des topologies noethériennes, et on a bien que la projection d'un fermé est un constructible (les logiciens appellent ce phénomène : élimination des quanteurs). La seule différence, c'est que la dimension topologique de K n'est plus un, ni même un nombre fini : c'est l'ordinal oméga, le premier ordinal infini. Il n'y a pas là de quoi se mettre martel en tête : cela signifie simplement que K n'a pas de suite infinie strictement décroissante de fermés (ça, c'est la noethérianité) ; par contre, il a des suites infinies croissantes de fermés irréductibles ; toutefois, un fermé contenant une telle suite ne peut qu'être K tout entier (sinon sa dimension serait plus que oméga). De même, K^n a pour dimension l'ordinal $n \cdot \omega$; ça ne l'empêche pas, bien au contraire, d'avoir des sous-ensembles de dimension finie, et de dimension un en particulier !

Pour un excellent exposé de tous ces trucs élémentaires sur les corps différentiellement clos, consulter [POIZAT 1985, ch. 6].

Comme K est muni de deux structures, celle de corps et celle de corps différentiel, d'où risque de confusion, nous convenons qu'à partir de maintenant les mots fermés de Zariski, constructibles, dimension réfèrent au pur langage des corps ; leurs homologues différentiels seront fermés de Zariski différentiels, ensembles définissables, rang de

Morley.

Une propriété des corps différentiellement clos de caractéristique nulle nouvellement mise en évidence dans [HRUSHOVSKI-SOKOLOVIC 199?], c'est que tout ensemble définissable M de rang de Morley un est une structure de Zariski, et que par conséquent nous sommes dans un cadre où la trichotomie de Zil'ber est valide. On prend pour fermés de Zariski de M, et de ses puissances, les traces des fermés de Zariski différentiels. Il faut éventuellement lui enlever un nombre fini de singularités pour que le Hauptidealsatz soit vérifié.

Il reste encore deux choses à faire avaler au lecteur avant de commencer la preuve.

La première est faite dans [SOKOLOVIC 1992] : tout corps (infini) de rang de Morley fini définissable dans K est définissablement isomorphe à son corps de constantes k, défini par l'équation $x' = 0$.

La deuxième est plus ancienne : elle vient de [MANIN 1958]. La dérivation introduit des corrélations entre des groupes algébriques sans rapports au niveau algébrique pur ; le plus connu est la dérivée logarithmique, qui à x du groupe multiplicatif K^* associe x'/x du groupe additif K^+ ; pour un corps ordinaire, c'est-à-dire un corps de constantes, c'est l'homomorphisme nul, mais si K est différentiellement clos cet homomorphisme est surjectif : ça ne contredit pas la propriété d'additivité des dimensions, car K^* et K^+ sont de rang oméga, tandis que le rang de Morley du noyau est fini ($= 1$). De même, si S est le groupe de la cubique définie par l'équation $y^2 = x \cdot (x-1) \cdot (x-q)$, où q est une constante (*i.e.* $q' = 0$), on voit sans trop de douleur que x'/y définit un homomorphisme de groupe de S dans K^+ ; une façon de faire est de dériver formellement une intégrale elliptique, et de faire taire ses états d'âme sur la signification de ce calcul ; si q n'est pas une constante, il faut dériver deux fois pour éliminer les intégrales elliptiques qui surgissent dans ce calcul, et on obtient un homomorphisme de S dans K^+ qui s'exprime en fonction de x, y et de leurs dérivées premières et secondes. Plus généralement, Yuri Manin définit grâce à la dérivation un homomorphisme μ d'une variété abélienne quelconque $S = S(K)$, de dimension d , dans $(K^+)^d$, qui est surjectif si K est différentiellement clos. Si S est définie sur k, le noyau de μ n'est autre que le groupe algébrique $S(k)$; mais si, à l'opposé, S est de trace nulle sur k, ce noyau $\mathrm{Ker}(\mu)$, qui est de rang de Morley fini par suite d'un simple calcul d'additivité des rangs, est modulaire, comme nous l'allons voir.

Une remarque historique avant de commencer la preuve : ce n'est pas Hrushovski, mais Buium qui a pensé à introduire ce noyau de Manin pour montrer la conjecture de Mordell–Lang ; mais ensuite, Buium fait de l'algèbre, pas de la théorie des modèles (voir [BUIUM 1992]).

Maintenant, on y va. Si Γ est "engendré" par $g_1, \cdots g_m$, $\mu(\Gamma)$ est contenu dans $\mathbf{Q}\cdot g_1+\cdots+\mathbf{Q}\cdot g_m$, donc aussi dans $k\cdot g_1+\cdots+k\cdot g_m$; ce dernier groupe est définissable de rang de Morley m, donc son image réciproque par μ est un sous-groupe définissable G de S, de rang de Morley fini et qui contient Γ. Nous prouvons le théorème avec G à la place de Γ, ce qui est évidemment plus fort.

Nous montrons maintenant que toute partie A de G, définissable de rang de Morley un (et "connexe", c'est-à-dire non-décomposable en deux tels sous-ensembles), est modulaire. Pour cela, nous utilisons une variation due à Zil'ber du théorème classique qui déclare qu'un sous-fermé irréductible A d'un groupe algébrique, et qui contient l'identité, engendre un sous-groupe algébrique connexe (dont chaque élément est produit d'un nombre fixe d'éléments de A) ; Zil'ber a remarqué que ça marchait dans un groupe de rang de Morley fini G, et pour les parties définissables indécomposables, *i.e.* qui ne se répartissaient pas en un nombre fini $\neq 1$ de cossettes modulo un sous-groupe définissable de G. Donc, on enlève à A un nombre fini de points pour le rendre indécomposable, on le translate pour qu'il contienne l'identité, et on est ramené au cas où il engendre un sous groupe définissable H de G ; ça empêche déjà A d'être trivial.

S'il était du troisième type, son corps associé ne pourrait être que k, et on pourrait décomposer H en une tour de groupes finis ou bien connexes et k–internes (voir [POIZAT 1987], p. 66). Quitte à le remplacer par le dernier groupe infini de cette tour, et à quotienter S par un noyau fini, nous pourrions supposer que H lui–même est k–interne, et H serait définissablement isomorphe à un groupe algébrique $I(k)$ sur k (voir [POIZAT 1987, ch. 4]). Autrement dit, on obtiendrait un isomorphisme f, définissable avec l'aide de la dérivation, de H vers $I(k)$; l'isomorphisme réciproque g, par contre, s'exprimerait uniquement avec des opérations rationnelles, puisque x' peut se remplacer par 0 quand il est question d'éléments de k !

Exemple d'une telle situation : $S = K^+$, qui n'est pas tout à fait une variété abélienne ; H est défini par la condition $x'' = 0$: il est de la forme $k + k \cdot a$, où a est une primitive de 1 ($a' = 1$) ; f va de H dans $(k^+)^2$, $f(x) = (x - a \cdot x', x')$; g va de $(k^+)^2$ dans H, $g(u, v) = u + a \cdot v$.

Comme $S = S(K)$ est aussi un groupe algébrique, défini dans le pur langage des corps, g s'étend en un homorphisme (algébrique) γ de $I(K)$ dans la clôture de

Zariski de H. Montrons que γ est injectif (ce n'est pas le cas dans notre exemple). Tout d'abord, $I(K)$ est une variété abélienne : en effet, comme $S(K)$ est abélienne, le plus grand sous–groupe affine de $I(K)$ est contenu dans le noyau de γ ; comme $I(K)$ est défini sur k, il en est de même de sa partie affine : si elle n'était pas nulle, on trouverait des points dans le noyau de g. Ensuite, une propriété importante des variétés abéliennes est leur rigidité : une variété abélienne définie sur k algébriquement clos a tous ses sous-groupes constructibles (qui sont de fait Zariski fermés) définis sur k, on n'en voit pas apparaître de nouveaux quand on étend le corps de base (par contraste, il y a dans $(K^+)^2$ de nouvelles droites dont on ne voit trace dans $(k^+)^2$). Par conséquent, si γ avait un noyau, on lui trouverait des points k–rationnels, c'est-à-dire dans le noyau de g.

En conséquence, γ est bien un isomorphisme entre le groupe algébrique $I(K)$ et la clôture de Zariski de H ; mézalor, comme $I(K)$ est défini sur k, notre hypothèse de trace nulle est contredite.

Pour résumer, le groupe H engendré par A étant modulaire, ce dernier est, à un nombre fini de points près, de la forme $a + J$, où J est un sous-groupe modulaire de G de rang de Morley un.

Ça suffit pour montrer le théorème quand X est une courbe, *i.e.* un fermé de Zariski de dimension (géométrique !) un, que nous prenons irréductible. C'est assez clair quand $X \cap G$ est fini ; sinon il contient un ensemble de rang de Morley un, de la forme $(a+J) - \{b_1, \cdots b_m\}$, si bien que X contient la clôture de Zariski de ce dernier, qui est $a + clz(J)$: X est lui-même cossette d'un groupe algébrique de dimension un.

Pour le cas général, on induit sur la dimension de X. On invoque la complétude de S pour que X reste fermé après passage au quotient.

On considère alors le sous-groupe L de G engendré par tous les sous-groupes définissables de rang de Morley un de G ; L est modulaire, mais G ne l'est pas nécessairement, puisque G/L peut contenir des copies de k^+. Pour des raisons tout à fait générales (voir [HRUSHOVSKI-PILLAY 1987]), un groupe modulaire est aussi rigide, et L ne contient qu'une famille fixe $J_1, \cdots J_n$, ... de sous-groupes de rang de Morley un (la vie serait un peu plus simple s'il n'y en avait qu'un nombre fini !) ; c'est d'ailleurs une information dont le géomètre peut se passer, car ce qui importe, c'est que leurs clôtures de Zariski $clz(J_1), \cdots clz(J_n)$ ... forment une famille fixe, ce qui est garanti par la rigidité de S. Notons X_n la partie de X stable sous l'action de $clz(J_n)$, c'est-à-dire l'ensemble des x tels que la cossette $x + clz(J_n)$ soit contenue dans X, et montrons que $X \cap G$ est contenu dans une réunion finie $X_1 \cup \cdots \cup X_n$. Sinon, quitte à remplacer K par une extension élémentaire saturée (ça augmente k, mais ça n'a plus d'importance), on trouve un type de rang de Morley un dans $X \cap G$, et qui n'est dans aucun des X_i ; ce type est le générique d'une $a + J_i$, si bien que cette cossette, privée d'un nombre fini de ses points est contenue dans $X \cap G$, et qu'en conséquence sa clôture de Zariski $a + clz(J_i)$ est contenue dans X : contradiction. Il suffit donc de démontrer le résultat pour chaque X_n, en se plaçant dans $S/clz(J_n)$, et en utilisant l'induction.

Si ce dernier paragraphe vous semble obscur, c'est que vous n'êtes pas familiers des techniques de base de la Théorie des modèles ; vous avez le choix entre cette familiarisation, ou bien la traduction dans votre propre langage : vous devez y arriver, car il n'y a pratiquement plus de mathématiques là-dedans, que des arguments de bon sens !

4. LA CARACTÉRISTIQUE p

C'est la partie que vous attendez tous, puisque c'est la première preuve de ce cas, et ça va être la plus frustrante : je me contente de vous répéter qu'on fait la même chose, mais avec une autre structure auxiliaire.

Pour enrichir la structure, on n'ajoute pas d'opérations (on pourrait sans doute le faire, car il existe une notion de corps différentiellement clos en caractéristique p, plus difficile à manier qu'en caractéristique nulle). Non, on n'ajoute pas d'opération à la somme et au produit, mais on change la notion de constructible : on prend un corps K séparablement clos, mais non algébriquement clos, tel que l'extension K/K^p soit de dimension finie (K^p désigne ici non pas une puissance cartésienne de K, mais l'image de K par l'homomorphisme ϕ de Frobenius qui à x associe x^p) ; si on fixe une base de cette extension, chaque x de K se décompose en un certain nombre de coordonnées : dans la notion de partie définissable de la puissance cartésienne, on tient non seulement compte des équations vérifiées par $x_1, \cdots x_n$, mais aussi de celles vérifiées par leurs coordonnées, les coordonnées de leurs coordonnées, etc., ce qui permet de garder la condition que la projection d'un définissable est définissable. On fait ça en s'arrageant pour que le corps algébriquement clos k soit l'intersection des $\phi^m(K)$.

Une autre façon de décrire ces "constructibles" d'un corps séparablement clos, c'est d'introduire des dérivations d'ordre supérieur de Hasse : voir [MESSMER-WOOD 1995].

Le contexte modèle–théorique est un petit peu plus élaboré : la théorie est stable, non superstable, ce qui oblige à considérer des ensembles infiniment définissables, comme le corps k, et non plus simplement définissables, mais ce n'est pas sérieusement plus complexe. Le seul corps de rang un est le corps k ([MESSMER 1994]), et les ensembles de rang un sont zariskis ([HRUSHOVSKI 199?] et [DELON 199?]) ; il ne manque plus que l'homomorphisme de Manin. Eh bien, on n'en a pas besoin : ce qu'on montre, c'est que, si S est de trace nulle sur k, le groupe G intersection des $p^n \cdot S$ est (de "dimension" finie et) modulaire, et qu'il peut jouer le rôle dévolu au noyau de Manin. Plus précisément, on suppose comme d'habitude que X est irréductible et que $X \cap \Gamma$ est zariski–dense dans X ; comme Γ se répartit en un nombre fini de cossettes modulo $p^n \cdot S$, l'une de celles-ci a son intersection avec X dense dans X ; on en déduit l'existence d'une cossette de G dont l'intersection avec X est dense dans X, et la conclusion. Comme quoi c'est à la fois plus simple et plus compliqué qu'en caractéristique nulle !

BIBLIOGRAPHIE

[BALDWIN 1994] J.T. BALDWIN - *An almost strongly minimal non–Desarguesian projective plane*, Trans. Am. Math. Soc. **342**, 695–711.

[BAUDISCH 1995] A. BAUDISCH - *Another stable group*, preprint n° A 95-5, Freie Universität Berlin.

[BUIUM 1992] A. BUIUM - *Intersections in jet spaces and a conjecture of S. Lang*, Annals of Mathematics **136**, 557–567.

[DELON 199?] F. DELON - *Separably closed fields*, Model Theory and Algebraic Geometry Workshop, Manchester, Sept. 1994 (Ed. E. Bouscaren & D. Lascar).

[DIEUDONNÉ 1981] J. DIEUDONNÉ - *Mathématiques vides et mathématiques significatives*, Points, série sciences **29**, Seuil, 15–38.

[HRUSHOVSKI 1992] E. HRUSHOVSKI - *Strongly minimal expansions of algebraically closed fields*, Israel J. of Math.**79**, 129–151.

[HRUSHOVSKI 1993] E. HRUSHOVSKI - *A new strongly minimal set*, Ann. Pure Appl. Logic **62**,147–166.

[HRUSHOVSKI 199?] E. HRUSHOVSKI - *The Mordell-Lang conjecture for function fields*, preprint.

[HRUSHOVSKI-PILLAY 1987] E. HRUSHOVSKI & A. PILLAY - *Weakly normal* *groups*, Logic Colloquium **85**, North Holland, 233–244.

[HRUSHOVSKI-SOKOLOVIC 199?] E. HRUSHOVSKI & Z. SOKOLOVIC - *Minimal subsets of differentially closed fields*, preprint.

[HRUSHOVSKI-ZIL'BER 1993] E. HRUSHOVSKI & B. ZIL'BER - *Zariski's geometries*, Bulletin AMS **28**, 315–324.

[HRUSHOVSKI-ZIL'BER 199?] E. HRUSHOVSKI & B. ZIL'BER - *Zariski's geometries*, preprint (plus détaillé que le précédent).

[FALTINGS 1983] G. FALTINGS - *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Math. **73**, 349–366.

[LANG 1965] S. LANG - *Division points on curves*, Ann. Math. Pures et Appl. **4**, 229–234.

[LANG 1991] S. LANG - *Number theory III : Diophantine Geometry*, Encyclopedia of Mathematical Sciences, Springer Verlag.

[LANG 1995] S. LANG - *Mordell's Review, Siegel's letter to Mordell, Diophantine Geometry and 20th Century Mathematics*, Gazette des Mathématiciens **63**, 17–36.

[MACINTYRE 1971] A. MACINTYRE - *On aleph-one categorical theories of fields*, Fundamenta Mathematicae **71**, 1–25.

[MANIN 1958] Y. MANIN - *Courbes algébriques sur un corps avec dérivation* (en russe), Izveztia Akad. Nauk SSSR **22**, 737–756.

[MESSMER 1994] M. MESSMER - *Groups and fields interpretable in separably closed fields*, TAMS **344**, 361–377.

[MESSMER-WOOD 1995] M. MESSMER & C. WOOD - *Separably closed fields with higher derivation I*, The Journal of Symbolic Logic **60**, 898–910.

[POIZAT 1984] B. POIZAT - *La structure géométrique des groupes stables*, Seminarberichte **60**, Humbodt-Universität zu Berlin, 205–217.

[POIZAT 1985] B. POIZAT - *Cours de Théorie des Modèles*, Nur al-Mantiq wal-Ma'rifah (distribué par OFFILIB).

[POIZAT 1987] B. POIZAT - *Groupes stables*, Nur al-Mantiq wal-Ma'rifah (distribué par OFFILIB).

[POIZAT 1987a] B. POIZAT - *À propos de groupes stables*, Logic Colloquium **85**, North Holland, 245–265.

[POIZAT 1988] B. POIZAT - *MM. Borel, Tits, Zil'ber et le Général Nonsense*, The Journal of Symbolic Logic **53**, 124–131.

[SOKOLOVIC 1992] Z. SOKOLOVIC - *Model Theory of Differential Fields*, PhD thesis, Notre Dame.

[WEIL 1948] A. WEIL - *Variétés abéliennes et courbes algébriques*, Hermann.

[ZIL'BER 1984] B.I. ZIL'BER - *The structure of models of uncountably categorical theories*, Proceedings of the ICM–Warsaw 1983, North Holland, 359–368.

John B. GOODE

Qazaqstanyn Memlekettik Universiteti
Qaragandy

et

Institut Girard Desargues
Centre de Mathématiques
URA 746 du CNRS
Bâtiment du Doyen J. Braconnier (101)
43, bld du 11 novembre 1918
F-69622 VILLEURBANNE CEDEX
E–mail : poizat@jonas.univ-lyon1.fr