The Journal of Symbolic Logic
Volume 67, Number 1, March 2002

LA LIMITE DES THEORIES DE COURBES GENERIQUES

OLIVIER CHAPUIS, EHUD HRUSHOVSKI, PASCAL KOIRAN, ET BRUNO POIZAT

Resumo. Ne estas prima orda formulo, kiu definas la Zariskijajn ŝlositojn inter la konstruitoj, malpli ke la konektojn inter la ŝlositoj.

Introduction. Pour paraphraser [SHM 1984] : les questions résolues dans cet article ont été posées par le premier et le troisième auteurs ; pour ce qui est de la solution, la lumière est venue du second ; quant au quatrième, il s'est chargé des détails techniques et de la rédaction, sous l'attention vigilante des trois autres.

Nous parlons ici de la possibilité d'exprimer certaines propriétés par des formules du premier ordre. Voilà ce que ça signifie : on considère une structure M, un entier m, et un énoncé $\varphi(R)$ usuel, c'est-à-dire finitiste et du premier ordre (il ne quantifie que des *éléments* de M), dans le langage de M augmenté d'un symbole R de relation m-aire. Etant donné un ensemble X de parties de M^m, on dit que le sous-ensemble Y de X est défini à l'intérieur de X par l'énoncé $\varphi(R)$ si Y est précisément formé des éléments A de X pour lesquels cet énoncé devient vrai dans M quand on y interprète le symbole R par la relation A.

Par exemple, dans un corps réel-clos K, les parties fermées de K^m sont caractérisées par une propriété évidente du premier ordre. Par contre, nous verrons ici que, si K est algébriquement clos, il est impossible de définir par un énoncé du premier ordre les fermés de Zariski, même parmi les ensembles définissables, dès que $m \geq 2$: c'est la réponse à une question posée dans [CHAPUIS-KOIRAN 1999].

Outre l'intérêt proprement modèle-théorique attaché à la caractérisation des fermés de Zariski parmi les constructibles (c'est-à-dire les ensembles définissables dans un corps algébriquement clos), ce type de questions a des motivations en Complexité algébrique : quand on travaille en Géométrie réelle ou complexe, et qu'on se pose la question de savoir si un ensemble défini par une formule $\rho(\underline{x})$ possède une certaine propriété P, si jamais cette propriété, pour un ensemble définissable, s'exprime au premier ordre par $\varphi(R)$, on obtient un algorithme de décision en substituant ρ à R et en éliminant les quanteurs ! D'ailleurs, cette simplicité algorithmique des propriétés exprimables au premier ordre fait qu'elles ont été intensément étudiées par les spécialistes des bases de données, qui traduiraient nos résultats en termes de bases de données géographiques avec contraintes dans un corps algébriquement

Received November 25, 1999; revised February 14, 2000.
Les recherches du deuxième auteur ont été soutenues par la Fondation Scientifique d'Israel.

0022-4812/02/6701-0002/$2.10

clos : nous renvoyons nos lecteurs intéressés par leur point de vue à [BDLW 1998] et [BALDWIN-BENEDIKT 1999].

Dans le cas des corps algébriquement clos, nous allons voir que bien des propriétés topologiques des ensembles définissables ne peuvent ainsi se caractériser. La seule propriété remarquable qui se définit par un énoncé du premier ordre est la dimension : en effet, une partie constructible A de K^m est de dimension m si et seulement si elle est *générique,* c'est-à-dire si K^m est recouvert par $m+1$ translatés de A (il existe $\underline{a}_0, \ldots, \underline{a}_m$ tels que $K^m = \underline{a}_0 + A \cup \ldots \cup \underline{a}_m + A$) ; elle est de dimension au moins n, $n \leq m$, si et seulement si elle a une projection sur n coordonnées qui est une partie générique de K^n.

Les résultats. Tous les corps que nous considérons ici sont algébriquement clos, d'une caractéristique arbitraire, mais fixée.

Un polynôme $P(x, y)$, en deux variables x et y, à coefficients dans k, de degré total (au plus) d s'écrit $P(x, y) = \sum a_{ij} \cdot x^i y^j$, $i + j \leq d$; nous notons $N+1$ son nombre de monômes, ou de coefficients, qui est facile à calculer, en évaluant le nombre de j possibles pour un i donné, puis en sommant : $N + 1 = (d+1) + d + \ldots + 1 = (d+1)(d+2)/2$.

Nous dirons que P est générique si ses coefficients a_{ij} sont algébriquement indépendants (sur le corps premier) ; il est alors irréductible (Lemme 4), si bien que l'équation $P(x, y) = 0$ définit une courbe plane irréductible, que nous notons $C_{\underline{a}}$. La théorie de cette courbe, c'est l'ensemble des énoncés, dans le langage L des corps augmenté d'un symbole de relation binaire $C(x, y)$, qui deviennent vrais quand C est interprété par $C_{\underline{a}}$. Comme cette théorie s'interprète dans le type de $\underline{a}$, il est clair que toutes les courbes génériques de degré d ont une même théorie T_d.

Nous allons montrer que cette suite est convergente, dans l'espace des théories complètes de langage L, et que sa limite T a la propriété suivante : à partir d'un modèle de T, quel que soit le point (a, b) sur la "courbe" C, on obtient un autre modèle de T en considérant la courbe $C - \{(a, b)\}$ obtenue en enlevant le point (a, b) à C ; autrement dit, quelle que soit la formule φ, T a pour conséquence $(\forall x)(\forall y)\varphi(C) \leftrightarrow \varphi(C - \{(x, y)\})$. Cela implique que, étant donné un énoncé $\varphi(C)$ satisfait par C, il existe un point (c, d) hors de C tel que la courbe augmentée de ce point satisfasse aussi φ ; en effet, la courbe $C - \{(a, b)\}$ satisfait cette dernière condition, donc C aussi.

Il devient alors clair qu'il n'existe pas d'énoncé (du premier ordre) séparant les courbes planes des courbes planes privées d'un point, ni les courbes planes des courbes planes augmentées d'un point ; ni à fortiori d'énoncé qui distingue les fermés de Zariski parmi les constructibles, ou bien les connexes ou les irréductibles parmi les fermés de Zariski. En effet, un tel énoncé devrait être conséquence de T, ainsi que sa négation, dans le cas où le corps algébriquement clos dans lequel on se place est de degré de transcendance infini ; et c'est aussi vrai s'il est de degré de transcendance fini, bien qu'il n'ait pas de courbes génériques de grand degré, car la chose se transmet par restriction élémentaire !

Il est également possible — ce sera un exercice facile pour le lecteur qui sera parvenu à la fin de cet article — de voir que, si on prend pour D_d la réunion de deux courbes génériques et indépendantes, définie par une équation $P(x, y) \cdot Q(x, y) = 0$ où P et Q sont deux polynômes de degré d dont les $2N + 2$ coefficients sont algébriquement indépendants, alors on obtient la même théorie T à la limite. On ne peut donc séparer par une formule une courbe de deux courbes, soit encore caractériser par une formule les fermés irréductibles parmi les fermés connexes. La conclusion est qu'on peut obtenir facilement une pléthore de résultats de ce genre dès que la dimension est supérieure à deux.

Nous notons en passant que [KOIRAN 2000] montre, par une tout autre méthode, des résultats analogues dans les corps réel-clos : il est impossible de caractériser par une formule les variétés irréductibles de R^2 parmi les variétés, ni d'ailleurs les variétés parmi les ensembles semi-algébriques.

L'article est organisé ainsi : dans une première partie, nous décrivons la théorie T ; elle est obtenue par une construction qui a été initiée il y a plus de dix ans par le second auteur, et qui est devenue une vraie usine à produire des exemples de toutes sortes en Théorie des modèles. D'habitude, cette construction fabrique des objets pathologiques : ici, c'est la première fois qu'elle produit une théorie ayant une interprétation naturelle ; c'est pour cela que nous avons particulièrement soigné son axiomatisation. Dans le cas d'espèce, c'est une application plutôt simple de cette méthode, qui ressemble beaucoup à ce qui a été fait dans [POIZAT 1999], auquel nous renvoyons pour certains détails. Dans une deuxième partie, nous montrons que la suite T_d converge bien vers T, c'est-à-dire que chaque axiome de T est vérifié par T_d dès que d est assez grand ; c'est la partie la plus délicate, qui demande un peu de connaissances en Géométrie algébrique, auxquelles nous nous efforcerons de conserver un caractère élémentaire.

Première partie. Construction de T. Nous considérons donc des corps K algébriquement clos d'une caractéristique donnée, muni en outre d'un symbole $C(x,y)$ ajouté au langage des corps, interprétant une partie de K^2, que nous appellerons ici “la courbe C”.

Nous demandons à ces corps de vérifier la propriété suivante : si

$$\{(a_1,b_1),\ldots,(a_n,b_n)\}$$

est un ensemble de points deux-à-deux distincts tous sur la courbe, alors le degré de transcendance (sur le corps premier) du uple $(a_1,b_1,\ldots,a_n,b_n)$ de leurs coordonnées vaut au moins n.

Autrement dit, si k est un sous-corps algébriquement clos de degré de transcendance fini de K, et si on note $\delta(k)$ la différence entre le degré de transcendance de k et le nombre de points de k^2 sur la courbe (qui doit être fini), alors ce $\delta(k)$ est toujours positif ou nul. Nous noterons Θ_0 (et non pas T_0 comme dans [POIZAT 1999]) la classe des corps avec courbe ayant cette propriété, dans laquelle nous travaillons désormais.

On nous aura déjà pardonné un abus de langage naturel : quand nous disons que k est un sous-corps de K, nous voulons dire que c'en est une sous-structure dans le langage L, c'est-à-dire que la courbe de k est formée des points de k^2 qui sont sur la courbe de K.

Si k est un sous-corps (algébriquement clos, de degré de transcendance fini) de K, il est possible qu'on puisse trouver k_1 intermédiaire entre k et K tel que $\delta(k) > \delta(k_1)$. Si cela ne se produit pas, on dit que k est autosuffisant (ou encore ormessien) dans K ; autrement dit, k est autosuffisant dans K si et seulement si, chaque fois que n points distincts sont pris sur la courbe dans $K^2 - k^2$, alors leur degré de transcendance sur k vaut au moins n.

On montrera comme dans [POIZAT 1999] la batterie de lemmes qui suit ; ils ne posent que peu de difficultés par rapport à d'autres versions de cette méthode, car la partie négative de la formule définissant δ n'est qu'une simple cardinalité.

Existence. *k a toujours au moins une extension k_1 de degré de transcendance fini qui soit ormessienne dans K* (prendre k_1 de δ minimal parmi les extensions de k).

Transitivité. *Si k est autosuffisant dans k_1 et k_1 est autosuffisant dans K, alors k est autosuffisant dans K.*

Intersection. *Si k_1 et k_2 sont autosuffisants dans K, il en est de même de leur intersection* (on montrera d'abord que $k_1 \cap k_2$ est autosuffisant dans k_2).

Clôture. *Il existe un plus petit corps (algébriquement clos !) contenant k et autosuffisant dans K, qu'on appelle la clôture autosuffisante de k dans K ; c'est le plus petit corps de δ minimal parmi les sous-corps de K contenant k.*

Limite. *Si $k_0 \ldots , k_i, k_{i+1}, \ldots$ est une suite croissante de corps (dans Θ_0, comme toujours !), chacun étant autosuffisant dans le suivant, alors ils sont tous autosuffisants dans leur limite $K = \cup k_i$.*

Nous définissons maintenant la notion d'amalgame libre, au-dessus de k, de deux extensions K_1 et K_2 de k, que nous notons $K_1 \oplus_k K_2$. Pour en former le corps, nous plaçons K_1 et K_2 de manière indépendante au dessus de k, au sens de la théorie des corps algébriquement clos ; en termes algébriques, cela signifie que K_1 et K_2 sont linéairement disjoints au-dessus de k ; puis nous prenons la clôture algébrique K du corps qu'ils engendrent. Ils reste à définir la courbe de K : nous lui mettons le moins de points possible, c'est-à-dire que c'est la réunion de la courbe de K_1 et de celle de K_2.

On obtient alors sans douleur le :

LEMME D'AMALGAMATION. *Si k est autosuffisant dans K_1, alors l'amalgame libre $K_1 \oplus_k K_2$ est bien dans Θ_0, et K_2 est autosuffisant dans $K_1 \oplus_k K_2$.*

Après qu'on a observé qu'il n'y a, à l'isomorphie près, qu'une famille dénombrable de corps k de degré de transcendance fini dans Θ_0, on met à contribution ce lemme, par une technique routinière depuis les travaux de Fraïssé et de Jonsson, pour construire un corps K, dans Θ_0 bien sûr, dénombrable et ayant la propriété suivante (où les lettres minuscules désignent des corps de degré de transcendance fini) :

Si k est une restriction autosuffisante de K, et si par ailleurs k est autosuffisant dans k', alors il existe un k-plongement de k' dans K, dont l'image est autosuffisante dans K.

Nous dirons qu'un corps est *riche* s'il a cette propriété.

Deux corps riches se correspondent par va-et-vient infini, obtenu en prenant à chaque étape les clôtures autosuffisantes, si bien qu'ils sont élémentairement équivalents (ils sont même équivalents dans $L_{\infty,\omega}$). Pour la même raison, il n'y a à l'isomorphie près qu'un seul corps riche dénombrable. La théorie T qui nous intéresse ici, c'est celle des corps riches ; nous allons l'axiomatiser.

Pour cela, nous exhibons une liste d'axiomes que nous avons voulu la plus simple possible, quitte à obscurcir ses motivations. Nous vérifions que cette liste est consistante, soit encore que les corps riches satisfont ses axiomes : nous faisons cette vérification ici, afin de ne pas embrouiller l'esprit de notre lecteur, bien que cette consistance soit une conséquence de la deuxième partie. Ensuite, il ne reste plus qu'à montrer que ses seuls modèles ω-saturés sont les corps riches.

Nous rassemblons les axiomes en trois groupes :

1. Ceux qui expriment que le corps est algébriquement clos, de la caractéristique voulue.

2. **Les axiomes universels.** Soit $P(u_1, \dots, u_n)$ un polynôme en n variables non identiquement nul, à coefficients dans le corps premier ; on met l'axiome universel suivant :

$$(\forall x_1, y_1, \dots, x_n, y_n) \wedge \bigwedge_{1 \leq i < j \leq n} (x_i, y_i) \neq (x_j, y_j) \wedge \ \wedge \bigwedge_{1 \leq i \leq n} C(x_i, y_i) \\ \rightarrow \dots \vee \bigvee_\varepsilon P(u_{\varepsilon 1}, \dots, u_{\varepsilon n}) \neq 0$$

la disjonction portant sur les 2^n fonctions ε qui choisissent une variable $u_{\varepsilon i}$ dans chaque couple (x_i, y_i).

3. **Les axiomes inductifs (en $\forall\exists$).** Nous considérons une conjonction

$$\varphi(x_1, y_1, \dots, x_n, y_n, \underline{z})$$

d'équations polynomiales à coefficients dans le corps premier. Comme la dimension est définissable, pour chaque fonction ε choisissant une variable $u_{\varepsilon i}$ entre x_i et y_i, il existe une formule $\psi_\varepsilon(\underline{z})$ du langage des corps exprimant que, le paramètre $\underline{z}$ étant fixé, la formule $(\exists u_{\varepsilon 1}, \dots, u_{\varepsilon n})\varphi(\underline{x}, \underline{y}, \underline{z})$ définit une partie (constructible !) de K^n générique, c'est-à-dire de dimension n. Nous notons $\psi(\underline{z})$ la disjonction des ψ_ε, et nous introduisons dans notre liste l'axiome suivant :

$$(\forall \underline{z})(\exists x_1, y_1, \dots, x_n, y_n) \qquad \psi(\underline{z}) \quad \rightarrow \quad \wedge \bigwedge_{1 \leq i \leq n} C(x_i, y_i) \wedge \varphi(\underline{x}, \underline{y}, \underline{z}).$$

Vérifions tout d'abord que ces axiomes sont satisfaits par un corps riche.

Les axiomes universels constituent en fait une axiomatisation de Θ_0, comme le montre le Corollaire 3 ci-dessous ; nous sommes reconnaissants à Frank O. Wagner de nous avoir fait observer qu'il reposait sur un célèbre théorème matrimonial, généralisé à la géométrie des corps (et en fait à n'importe quelle géométrie combinatoire ; cette généralisation est bien connue des spécialistes de la chose : voir [BOLLOBAS 1986, Th. 1, p. 137]).

LEMME 1 (Théorème des mariages). *On considère un ensemble fini de femmes, qui aiment des hommes. On suppose que chaque fois qu'on en prend un certain nombre n, il y a au moins n hommes qui sont aimés d'au moins l'une d'entre elles. Il est alors possible de marier monogamiquement toutes les femmes, chacune à un homme qu'elle aime.*

DÉMONSTRATION. Voir le Lemme 2. ⊢ Fin

LEMME 2 (Théorème des mariages indépendants). *On suppose en outre que les hommes vivent dans une extension de corps K/k, et que, chaque fois qu'on prend n femmes, l'ensemble des hommes qu'elles aiment engendre un corps de degré de transcendance au moins n sur k. Alors il est possible de marier toutes les femmes à des hommes algébriquement indépendants sur k.*

DÉMONSTRATION. On se ramène au cas ou il n'y a qu'un nombre fini d'hommes aimés et on raisonne par récurrence sur leur nombre. La récurrence s'amorce sans difficulté au jardin d' Eden. Pour le pas d'induction, si chaque ensemble non vide de femmes aime des hommes dont le degré de transcendance est strictement supérieur à leur nombre, on conserve l'hypothèse de mariabilité en tuant n'importe quel homme, et l'hypothèse de récurrence permet de marier les femmes aux survivants.

Sinon, nous considérons n (non nul et) minimal tel qu' il existe n femmes $f_1, \ldots, f_n$ dont l'ensemble d'hommes aimés est de degré de transcendance exactement n sur k. Nous commençons par marier la première femme à un homme transcendant h_1. Par hypothèse de minimalité sur n, si on prend m femmes parmi $f_2, \ldots, f_n$, le degré de transcendance des hommes qu'elles aiment vaut au moins $m+1$ sur k, et donc au moins m sur $k(h_1)$. Ces femmes satisfont par conséquent l'hypothèse de mariabilité sur $k(h_1)$, et comme h_1 est maintenant mort (enfin, nous voulons dire marié et algébrique) on peut par hypothèse d'induction marier $f_2, \ldots, f_n$ à des hommes $h_2, \ldots, h_n$ algébriquement indépendants au-dessus de $k(h_1)$.

S'il reste des femmes, on observe qu'elle satisfont l'hypothèse de mariabilité sur $k(h_1, \ldots, h_n)$, et on termine le mariage en s'appuyant également sur l'hypothèse de récurrence. $\vdash$ Fin

COROLLAIRE 3. *La condition de positivité de δ s'exprime également ainsi : étant donnés n points distincts $(a_1, b_1), \ldots, (a_n, b_n)$ sur la courbe, on peut pour chaque $i \leq n$ choisir c_i dans $\{a_i, b_i\}$ de sorte que $c_1, \ldots, c_n$ soient algébriquement indépendants.*

DÉMONSTRATION. Les femmes, ce sont les points sur la courbe, et les hommes qu'elles aiment, leurs coordonnées. $\vdash$ Fin

Nous vérifions maintenant que chaque axiome en $\forall\exists$, de la forme

$$(\forall \underline{z})(\exists x_1, y_1, \ldots, x_n, y_n) \qquad \psi(\underline{z}) \quad \rightarrow \quad \wedge \bigwedge_{1 \leq i \leq n} C(x_i, y_i) \wedge \varphi(\underline{x}, \underline{y}, \underline{z})$$

est satisfait dans un corps riche K.

Soit donc $\underline{d}$ dans K satisfaisant ψ et soit k la clôture autosuffisante du corps engendré par $\underline{d}$. Dans une certaine extension de k, on peut trouver $a_1, b_1, \ldots, a_n, b_n$ satisfaisant $\varphi(\underline{x}, \underline{y}, \underline{d})$, avec $c_1 \in \{a_1, b_1\}, \ldots, c_n \in \{a_n, b_n\}$ algébriquement indépendants au-dessus de k. Nous notons k' la clôture algébrique de $k(a_1, b_1, \ldots, a_n, b_n)$, que nous transformons en corps avec courbe en mettant les (a_i, b_i) sur la courbe, et rien que ceux-là en dehors des points à coordonnées dans k qui y sont déjà. On observe alors que k' est dans Θ_0, et que c'est une extension autosuffisante de k : *c'est vrai même si certains des (a_i, b_i) sont confondus.* La richesse de K permet d'y plonger k', si bien que l'axiome est vérifié.

Notre théorie T est donc consistante, et c'est un fragment de la théorie des corps riches ; pour voir qu'elle est complète, il nous suffit de montrer que tout modèle K de T ω-saturé est riche.

Soit donc k autosuffisant à la fois dans K et dans k' ; nous dirons que l'extension k'/k est minimale s'il n'y a pas de corps intermédiaires autosuffisants dans k' : comme nous parlons de corps algébriquement clos de degré de transcendance fini, toute extension ormessienne se décompose en une tour finie de telles extensions minimales, si bien qu'il nous suffit de montrer la propriété de richesse relativement aux extensions minimales.

Nous supposons donc que k'/k est minimale, et aussi, pour l'instant, que $\delta(k) = \delta(k')$: k' sera donc engendré au-dessus de k par n points distincts sur la courbe et de degré de transcendance n. Il y a de très nombreux exemples de cette situation ; une façon simple d'en produire un est de prendre $c_1, \ldots, c_n$ algébriquement indépendants et de mettre les n points $(c_1, c_2), (c_2, c_3), \ldots, (c_n, c_1)$ sur la courbe. Soient $(a_1, b_1), \ldots, (a_n, b_n)$ les points de la courbe qui sont dans k' sans être dans k, et soit $\varphi(\underline{x}, \underline{y}, \underline{d})$ une conjonction d'équations définissant la variété de $\underline{a} \wedge \underline{b}$ sur k ; nous supposons en outre que le paramètre $\underline{d}$ pris dans k contient toutes les coordonnées des points de k^2 qui sont sur la courbe (il n'y en a qu'un nombre fini).

Comme k est autosuffisant dans k', $\underline{d}$ satisfait la formule ψ associée à φ (Lemme 2), si bien qu'on peut trouver $(\alpha_1, \beta_1), \ldots, (\alpha_n, \beta_n)$ dans K, sur la courbe, et satisfaisant $\varphi(\underline{x}, \underline{y}, \underline{d})$; mais ça ne nous suffit pas, car nous les voudrions aussi deux-à-deux distincts et tous hors de k. Par bonheur, cette dernière condition est impliquée par un axiome du même type associé à une variété définie par une formule $\varphi^*(\underline{x}^*, \underline{y}^*, \underline{z})$ contenant plus de variables. Par exemple, si $a_1 \neq b_2$, nous ajoutons un couple de variables (x_{n+1}, y_{n+1}) et l'équation $(x_1 - y_2) \cdot y_{n+1} = 1$: comme rien n'est exigé de x_{n+1}, $\underline{d}$ satisfait aussi la condition ψ^* associée à φ^* ; de même, si par exemple $b_3 \neq d_1$, on ajoute deux nouvelles variables (x_{n+2}, y_{n+2}) et l'équation $(z_1 - y_3) \cdot y_{n+2} = 1$.

Si donc les n points $(\alpha_1, \beta_1, \ldots, (\alpha_n, \beta_n)$ sont distincts et pas dans k, l'autosuffisance de k dans K les force à être de degré de transcendance au moins n, ce qui implique qu'ils réalisent sur k le générique de la variété irréductible $\varphi(\underline{x}, \underline{y}, \underline{d})$, que les corps $k(a_1, b_1, \ldots, a_n, b_n)$ et $k(\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n)$ sont k-isomorphes. Il en est de même de k' et de la clôture algébrique κ de $k(\alpha_1, \beta_1, \ldots, \alpha_n, \beta_n)$ dans K. Par ailleurs, cette autosuffisance de k implique aussi qu'il n'y a pas d'autre points dans κ sur la courbe autres que ceux que nous connaissons déjà, si bien que k' et κ sont aussi isomorphes en tant que corps avec courbe. Enfin, comme $\delta(k) = \delta(\kappa)$, κ est nécessairement autosuffisant dans K : nous avons bien obtenu un plongement ormessien de k' dans K.

Pour l'instant, nous n'avons pas utilisé la ω-saturation de K, car nous n'avons fait que réaliser des types isolés. Nous en avons besoin pour réaliser la dernière sorte d'extension minimale, correspondant au “générique du corps” : k'/k est de degré de transcendance un et il n'y a pas dans k' de nouveaux points sur la courbe. On obtient ce dernier type comme limite d'une suite de types isolés (parce que k est de degré de transcendance fini !), si bien qu'il doit être lui-aussi réalisé (c'est-à-dire qu'on peut plonger *autosuffisamment* k' dans K) : par exemple, si $c \in K - k$ et (c, c) est sur la courbe, $\text{tp}(c^n/k)$ tend vers le type générique. Si un détail vous échappe, voyez [POIZAT 1999].

REMARQUE. Nous aurions pu reproduire l'axiomatisation de [POIZAT 1999], avec ses blocs de variables ; si celle que nous offrons ici est moins pénible, c'est que nous sommes dans une situation où le Théorème des mariages permet d'approcher économiquement l'autosuffisance !

Il faut enfin faire ce que nous avons promis dans l'introduction, à savoir montrer que si, dans un modèle de T, on enlève un point (a, b) de la courbe, on obtient un autre modèle de T. Il est clair que si on efface des points de la courbe d'un modèle de T, les axiomes universels sont encore vrais (si on en ajoute, ce sont les axiomes inductifs qui restent satisfaits !). Quant aux axiomes inductifs, il faut voir que celui qui est associé à $\varphi(x_1, y_1, \dots, x_n, y_n, \underline{z})$ reste vrai quand on y remplace $C(x, y)$ par $C(x, y) \wedge (x, y) \neq (a, b)$; c'est conséquence de l'axiome associé à la formule Φ définie par la conjonction : $\varphi(x_1, y_1, \dots, x_n, y_n, \underline{z}) \wedge ((x_1 - a)x_{n+1} - 1) \cdot ((y_1 - b)y_{n+1} - 1) = 0 \wedge \dots, \wedge((x_n - a)x_{2n} - 1) \cdot ((y_n - b)y_{2n} - 1) = 0$; en effet, la formule $\psi(\underline{z})$ associée à φ est satisfaite par les mêmes $\underline{z}$ que la formule $\Psi(\underline{z}, a, b)$ associée à Φ. On peut aussi vérifier directement que, si on enlève un point de la courbe d'un corps riche, ça n'en fait pas un prolétaire.

Remarque. Une analyse des types en tous points identique à ce qui est fait dans [POIZAT 1999] montre que T est ω-stable, de rang de Morley ω. Les corps riches peuvent être collapsés sur des corps de rang de Morley un, comportant une "courbe" non définissable dans le langage des corps. Les conditions permettant de définir un collapsé sont faciles à déterminer, mais tous les collapsés ne seront pas saturés, ni oméga-stables, ni même stables. En effet, la théorie T a la dope ; elle a beaucoup de types orthogonaux, ce qui ne l'empêche pas d'être stable car les dimensions associées à ses types isolés sont infinies. Mais dans un collapsé ces dimensions deviennent finies, et on peut faire en sorte qu'une dimension basée sur un paramètre algébrique soit strictement inférieure à celle qui lui correspond sur un paramètre transcendant, et donc définir le corps des nombres algébriques, et en fait interpréter n'importe quelle structure dessus. Pour éviter cela, il faut choisir d'une façon uniforme ces dimensions : c'est ce que [BALDWIN-HOLLAND 2000] ont appelé la condition "finite to one".

Deuxième partie. La suite T_d tend vers T. Nous montrons maintenant que chaque axiome de T est vérifié par les courbes planes génériques de degré d, dès que d est assez grand.

Nous revenons à notre polynôme générique $P(x, y) = \sum a_{ij} \cdot x^i y^j, i + j \leq d$, à $N + 1 = (d + 1)(d + 2)/2$ coefficients algébriquement indépendants, définissant une courbe plane $C_{\underline{a}}$.

Il est clair que, si on multiplie les a_{ij} par un même scalaire non nul, on ne change pas la courbe. Comme $a_{00} \neq 0$, on peut être tenté de normaliser le polynôme en lui imposant d'avoir un coefficient constant égal à 1, c'est-à-dire de remplacer $P(x, y)$ par $Q(x, y) = (1/a_{00}) \cdot P(x, y) = \sum(a_{ij}/a_{00}) \cdot x^i y^j$; c'est utile pour montrer le lemme bien connu qui suit.

Lemme 4. *Un polynôme générique en deux variables est (absolument) irréductible, et définit donc une courbe plane irréductible.*

Démonstration. Si le polynôme Q est réductible, il se décompose comme produit de deux polynômes Q' et Q'', de degrés respectifs d' et d'', avec $d' + d'' = d, 1 \leq d' \leq d'' \leq d - 1$, dont les coefficients constants sont égaux à 1. Les coefficients de Q s'expriment en fonction de ceux de Q' et de Q'', si bien que leur degré de transcendance ne peut excéder $N' + N''$; mézalor, un bête exercice sur les variations de la fonction $t(t + 1)$ montre que $N' + N'' < N$, si bien que les coefficients de Q ne sont pas algébriquement indépendants. ⊢ Fin

Mais il est préférable, et surtout indispensable pour la fin de la section, de considérer le uple $\underline{a}$ de paramètres de la courbe comme un point de l'espace projectif de dimension N. En effet, nous allons utiliser un théorème d'intersection, qui n'est pas valable dans l'espace affine, certains points pouvant fuir à l'infini ; il nous servira à mettre en évidence l'existence d'un point de cet espace projectif, dont il n'est pas évident a priori que sa première coordonnée soit non nulle ; mais ce sera bien vrai a posteriori, quand nous aurons montré que ce point est générique !

Nous rappelons que la donnée d'un point de l'espace projectif de dimension N, c'est un $(N+1)$-uple de coordonnées non toute nulles, considéré à proportionnalité près ; si la première coordonnée de ce uple n'est pas nulle, on obtient un représentant canonique du point en imposant à la première coordonnée de valoir 1, et le degré de transcendance du point ou de son représentant, c'est la même chose (en Théorie des modèles, on dit qu'on élimine un imaginaire) ; sinon il faut prendre une autre coordonnée.

Par un abus de langage naturel, nous qualifierons l'espace projectif de dimension N d' “espace des courbes planes de degré d”, même si la courbe $C_{\underline{a}}$, ensemble des points (x, y) qui satisfont l'équation polynôme ayant $\underline{a}$ pour coefficients, n'est pas irréductible ; il y a même une courbe vide, la “droite de l'infini comptée d fois”, d'équation $1 = 0$; pour lui trouver des points, il faudrait remplacer le plan affine par le plan projectif, ce qui n'est pas utile pour ce que nous allons faire (ça serait même nuisible, car dans la théorie T obtenue à la limite, la notion de “points à l'infini sur la courbe C” n'a plus aucun sens !).

On remarque que, pour une courbe, passer par un point donné se traduit par une condition linéaire non triviale sur les coefficients du polynôme ; cela signifie que les courbes passant par ce point forment une variété projective de dimension $N - 1$. Voici un lemme (bien connu ?) sur l'indépendance de ces différentes conditions :

LEMME 5. *Si $d \geq n - 1$, les courbes planes de degré d qui passent par n points distincts du plan forment une variété de dimension $N - n$.*

DÉMONSTRATION. Nous devons montrer que les équations linéaires, dont les inconnues sont les coefficients de la courbe, exprimant que cette dernière passe par chacun des points en question sont linéairement indépendantes ; elles définiront alors un espace vectoriel de codimension n dans l'espace vectoriel de dimension $N + 1$, et une variété projective de codimension n dans son quotient. (C'est de l'algèbre linéaire élémentaire : ce n'est pas là qu'il est essentiel de raisonner projectivement).

Cela revient à montrer qu'aucune de ces équations n'est conséquence des autres, soit encore qu'on peut trouver une courbe de degré (au plus !) d qui passe par $n - 1$ des points $(a_1, b_1), \ldots, (a_{n-1}, b_{n-1})$, et pas par le dernier (a_n, b_n) ; cette courbe a pour équation :

$$\prod_{i<n, a_i \neq a_n} (x_i - a_i) \times \prod_{j<n, a_i = a_n} (y_i - b_j) = 0 \quad !$$

⊢ Fin

COROLLAIRE 6. *Si $d = n - 1$, et si une courbe générique de degré d passe par n points $(a_1, b_1), \ldots, (a_n, b_n)$ du plan, leur degré de transcendance vaut au moins n.*

DÉMONSTRATION. Les coefficients de la courbe, une fois normalisés, ont un degré de transcendance N sur $\emptyset$; d'après le corollaire précédent, leur degré de transcendance sur $\{a_1, b_1, \ldots, a_n, b_n\}$ est au plus $N - n$; il faut donc que le degré de transcendance de $\{a_1, b_1, \ldots, a_n, b_n\}$ soit au moins n (et si ce degré est n, les a_i et les b_i sont algébriques sur ces coefficients). ⊢ Fin

CONCLUSION. Les axiomes universels sont finalement vérifiés.

Pour les axiomes en $\forall\exists$, c'est plus subtil. Appelons K le corps sur lequel est dessiné la courbe générique $C_{\underline{\alpha}}$, et soit k un de ses sous-corps algébriquement clos engendré par un $\underline{d}$ satisfaisant ψ (qui est une formule du pur langage des corps). Dans une certaine extension de k, on peut trouver $a_1, b_1, \ldots, a_n, b_n$ satisfaisant $\varphi(\underline{x}, \underline{y}, \underline{d})$, avec $c_1 \in \{a_1, b_1\}, \ldots, c_n \in \{a_n, b_n\}$ algébriquement indépendants au-dessus de k. Ce qu'il nous faut montrer, c'est que si d est grand par rapport au degré de transcendance de k et par rapport à n, alors on peut trouver $\underline{a}' \wedge \underline{b}'$ dans une extension (élémentaire !) K' de K, de même type que $\underline{a} \wedge \underline{b}$ sur k, tel que la courbe $C_{\underline{\alpha}}$ passe par tous les points (a_i', b_i').

En fait, nous allons faire le contraire, c'est-à-dire garder $\underline{a} \wedge \underline{b}$ fixé et faire passer une courbe $C_{\underline{\beta}}$ par chacun des (a_i, b_i), et nous montrerons ensuite que $\underline{\beta}$ et $\underline{\alpha}$ ont même type sur k !

Nous considérons donc $\underline{\alpha}$ comme un point de l'espace projectif de dimension N, et nous appelons V la variété projective dont il est le point générique sur k. Comme $\underline{\alpha}$ est de degré de transcendance N sur $\emptyset$, la dimension de V est au moins $N - d°\text{trans}(k)$, et sera supérieure à n si on prend d assez grand.

Par ailleurs, nous considérons la variété projective W, à coefficients dans la clôture algébrique k' de $k(a_1, b_1, \ldots, a_n, b_n)$, définie par la condition que la courbe passe par chacun des (a_i, b_i) ; d'après le Théorème de la dimension, dit encore Hauptidealsatz, l'intersection $V \cap W$ n'est pas vide, et sa codimension dans V est au plus n. C'est là un résultat tout-à-fait fondamental sur la dimension, si bien qu'il est démontré dans un manuel élémentaire de Géométrie comme [DIEUDONNE 1974, p. 96] ; c'est pour qu'on ait ici une intersection non vide qu'il est essentiel que le problème soit de nature projective.

Soit $\underline{\beta}$ un point générique sur k' de $V \cap W$. Nous notons $n + m$ le degré de transcendance de k'/k. Ce qui fait marcher la chose, c'est le lemme suivant (où RM, "Rang de Morley", est une notation modèle-théoriste pour le degré de transcendance) :

Lemme 7. *Si d est assez grand, $\underline{a} \wedge \underline{b}$ est de degré de transcendance au plus m sur $k(\underline{\beta})$.*

Démonstration. Notons P_1 l'ensemble des n_1 points (a_i, b_i) qui sont algébriques sur $k(\underline{\beta})$, et P_2 celui des n_2 autres ; on suppose $n_2 \neq 0$ (sinon la chose est claire !) et on note θ le degré de transcendance de P_2 sur $k(\underline{\beta})$. Par ailleurs, puisque le degré de transcendance de $k(P_1, P_2)/k$ est $n + m = n_1 + n_2 + m$, et celui de $k(P_1)/k$ au moins n_1 par la condition sur les c_i, $\text{RM}(P_2/k(P_1)) \leq n_2 + m$.

On réalise $1 + [d/n_2]$ fois, de manière indépendante sur $k(\underline{\beta})$, le type fort de P_2 sur $k(\underline{\beta})$; on obtient ainsi un ensemble de points $Q = P_1 \cup P_{2,1} \cup \ldots \cup P_{2,i} \cup \ldots$; on observe que la courbe passe par tous les points de Q, et qu'il y en a plus que d, si bien que $\text{RM}(\underline{\beta}/Q) \leq N - d$; on évalue alors le degré de transcendance de $k(\underline{\beta}, Q)$ sur k.

D'une part, $\text{RM}(\underline{\beta} \wedge Q/k) = \text{RM}(\underline{\beta}/k) + \text{RM}(Q/k(\underline{\beta})) = N - r + \theta \cdot (1 + [d/n_2])$, où $r = n + d°\text{trans}(k)$.

D'autre part, $\text{RM}(\underline{\beta} \wedge Q/k) = \text{RM}(Q/k) + \text{RM}(\underline{\beta}/k(Q)) \leq \text{RM}(P_1/k) + (n_2 + m) \cdot (1 + [d/n_2]) + N - d$.

Si on regroupe ce qui est borné, cela donne $N + \theta d/n_2 + O(1) \leq N + md/n_2 + O(1)$, ce qui donne $\theta \leq m$ pour les grandes valeurs de d (à partir d'un seuil facilement calculable, suivant l'expression consacrée, en fonction de n et du degré de transcendance de k, lui-même borné par la longueur de $\underline{z}$ (nous prétendons que ça marche dès que $d \geq n(2n + d^\circ k + 1) - 1$; qui dit mieux ?). $\vdash$ Fin

Pour ces grandes valeurs de d, nous injectons ce lemme dans un dernier calcul de dimension : $\mathrm{RM}(\underline{\beta} \wedge \underline{a} \wedge \underline{b}/k) = \mathrm{RM}(\underline{a} \wedge \underline{b}/k) + \mathrm{RM}(\underline{\beta}/k(\underline{a} \wedge \underline{b})) = n + m + dim(V \cap W) \geq n + m + dim(V) - n = dim(V) + m$ d'une part ; $\mathrm{RM}(\underline{\beta} \wedge \underline{a} \wedge \underline{b}/k) = \mathrm{RM}(\underline{\beta}/k) + \mathrm{RM}(\underline{a} \wedge \underline{b}/k(\underline{\beta})) = \mathrm{RM}(\underline{\beta}/k) + m$ d'autre part. En comparant on voit que $\mathrm{RM}(\underline{\beta}/k) = dim(V)$, c'est-à-dire que $\underline{\beta}$ réalise bien sur k le type générique de V, qu'il a même type que $\underline{\alpha}$ sur k ; nous pouvons donc supposer que $\underline{\beta} = \underline{\alpha}$, si bien qu'il y a une copie de $\underline{a} \wedge \underline{b}$, dans toute extension de K de degré de transcendance suffisant, telle que la courbe C_α passe par tous les points (a_i, b_i), et notre axiome est vérifié (dans K lui-même !).

Remarque. On a en fait égalité dans le Lemme 7 : le degré de transcendance de $\underline{a} \wedge \underline{b}$ sur $k(\underline{\alpha})$ est m. Quand $m = 0$, $\underline{a} \wedge \underline{b}$ est algébrique sur $k(\underline{\alpha})$, mais son nombre de conjugués croît avec d, si bien qu'à la limite, dans la théorie T, il ne définit pas un type algébrique, mais un type de rang un.

RÉFÉRENCES

[BALDWIN-BENEDIKT 1999] John Baldwin and M. Benedikt, *Permutations of indiscernibles and embedded finite models*, prépublication.

[BALDWIN-HOLLAND 2000] John Baldwin and Kitty Holland, *Constructing omega-stable structures : rank 2 fields*, this Journal, vol. 65, pp. 371–391.

[BDLW 1998] M. Benedikt, G. Dong, L. Libkin, and L. Wong, *Relational expressive power of constraint query languages*, ***Journal of the Association for Computing Machinery***, vol. 45, pp. 1–34.

[BOLLOBAS 1986] Béla Bollobas, ***Combinatorics***, Cambridge University Press.

[CHAPUIS-KOIRAN 1999] Olivier Chapuis and Pascal Koiran, *Definability of geometric properties in algebraically closed fields*, ***Mathematical Logic Quaterly***, vol. 45, pp. 533–550.

[DIEUDONNE 1974] Jean Dieudonne, *Cours de Géométrie Algébrique*, t. 2, P.U.F, Paris.

[KOIRAN 2000] Pascal Koiran, *On defining irreducibility*, ***Comptes Rendus de l' Académie des Sciences***, vol. 330, pp. 529–532.

[POIZAT 1999] Bruno Poizat, *Le carré de l'égalité*, this Journal, vol. 64, pp. 1339–1355.

[SHM 1984] Saharon Shelah, Leo Harrington, and Michael Makkai, *A proof of Vaught's conjecture for totally transcendental theories*, ***Israel Journal for Mathematics***, vol. 49, pp. 259–278.

DÉPARTEMENT DE MATHÉMATIQUES
UNIVERSITÉ HÉBRAÏQUE À JÉRUSALEM
91904 JÉRUSALEM, ISRAEL
E-mail: ehud@math.huji.ac.il

LABORATOIRE D'INFORMATIQUE DU PARALLÉLISME
ECOLE NORMALE SUPÉRIEURE DE LYON
46, ALLÉE D'ITALIE, 69364 LYON, FRANCE
E-mail: koiran@ens-lyon.fr

INSTITUT GIRARD DESARGUES
UNIVERSITÉ CLAUDE BERNARD (LYON-1)
MATHÉMATIQUES, BÂTIMENT 101
43, BOULEVARD DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE-CEDEX, FRANCE
E-mail: chapuis@desargues.univ-lyon1.fr
E-mail: poizat@desargues.univ-lyon1.fr