THE JOURNAL OF SYMBOLIC LOGIC
Volume 59, Number 1, March 1994

INDÉCIDABILITÉ DES CORPS DE COURBE RÉELLE

LUC BÉLAIR AND JEAN-LOUIS DURET

Nous dirons qu'un corps (commutatif) K est un *corps de courbe réelle* sur le corps k si et seulement si c'est une extension de k, ordonnable, finiment engendrée et de degré de transcendance 1 sur k, telle que k soit relativement algébriquement clos dans K. Un tel corps est le corps d'une courbe (plane) définie sur k. De plus si k est réel-clos, toute courbe définie sur k dont K est le corps, a un point régulier rationnel sur k; en effet soit $I \subset k[X_0, \ldots, X_n]$ l'idéal d'une telle courbe Γ; on a donc: $K = k[x_0, \ldots, x_n]$ où $x_0, \ldots, x_n$ sont les classes d'équivalence de $X_0, \ldots, X_n$; $(x_0, \ldots, x_n)$ est *un* point régulier de Γ dans la clôture réelle de K, et par modèle-complétude, Γ a un point régulier rationnel sur k.

Notre but est d'étendre les résultats de Raphael Robinson [6] sur l'indécidabilité des corps de fractions rationnelles sur un corps ordonnable (dans le langage des corps). Comme lui, nous donnerons une méthode qui ne s'applique que lorsque le corps de base k est réel-clos, et une seconde méthode générale.

A. Le cas du corps de base réel-clos.

1. PROPOSITION. *Un corps de courbe réelle sur un corps réel-clos R est le corps d'une courbe plane dont la projection sur le premier axe contient* $[0, +\infty[(= \{x \in R; x \geq 0\})$.

DÉMONSTRATION. Soient $K = R(u_0, v_0)$ le corps de courbe réelle considéré et $P_0(X, Y)$ le polynôme minimale de v_0 sur $R(u_0)$ (K est donc le corps de la courbe d'équation $P(x, y) = 0$).

Une projection sur l'un des axes contient un intervalle. En effet, sinon, puisque ces deux projections sont définissables (avec paramètres), ce serait des ensembles finis, et donc la courbe d'équation $P(x, y) = 0$ serait incluse dans un ensemble fini, donc finie, et ne contiendrait aucun point régulier ce qui est contradictoire. Quitte à échanger u_0 et v_0 ($R(u_0, v_0) = R(v_0, u_0)$), c'est à dire à effectuer une symétrie par rapport à la première bissectrice, on peut supposer que c'est la première projection qui contient cet intervalle.

Soit $[a, b]$ un intervalle inclus dans la première projection; soient a' et b' satisfaisant à: $P_0(a, a') = 0$ et $P_0(b, b') = 0$. On a: $R(u_0, v_0) = R(u_1, v_1)$ avec $u_1 = u_0 - a$ et $v_1 = v_0 - a'$ (on effectue une translation qui met (a, a') à l'origine). Donc K est le corps de la courbe d'équation $P_1(x, y) = P_0(x + a, y + a') = 0$, dont la projection sur le premier axe contient $[0, c]$ $(c = b - a)$.

Received March 1, 1993.

0022-4812/94/5901-0006/$01.50

On a: $R(u_1, v_1) = R(u_2, v_2)$ où $u_2 = 1/u_1$ et $v_2 = v_1$ (on envoie $(0,0)$ à l'infini). Donc K est le corps de la courbe d'équation $P_2(x,y) = x^n P_1(\frac{1}{x}, y)$ (où: $n = d_X^0 P_1$) dont la première projection contient $[\frac{1}{c}, +\infty]$.

Enfin, on a: $R(u_2, v_2) = R(u, v)$ avec: $u = u_2 - \frac{1}{c}$ et $v = v_2$ (translation qui amène $(\frac{1}{c}, b' - a')$ à l'orgine). Le corps K est donc le corps de la courbe d'équation $P(x,y) = P_2(x + \frac{1}{c}, y + b' - a') = 0$ dont la première projection contient $[0, +\infty[$. □

Rappelons un résultat de Julia Robinson utilisé par Raphael Robinson [6, §3].

2. PROPOSITION. *Soient $x_0, \ldots, x_n$ des nombres rationnels. Il existe $f(X) \in \mathbf{Q}(X)$ tel qu'on ait*

$$(\forall i = 0, \ldots, n)(\exists z_1, \ldots, z_8 \in \mathbf{Q}(X)) \left((X - x_i)^2 - f(X)^2 = \sum_{i=1}^{8} z_i^2 \right).$$

(8 peut être remplacé par 5 en utilisant le resultat de Pourchet qui améliore le résultat de Landau utilisé.)

3. THÉORÈME. *Un corps de courbe réelle sur un corps réel-clos est indécidable.*

DÉMONSTRATION. Soient K ce corps et R le corps réel-clos. Soit $x \leq_8 y$ la formule $(\exists z_1, \ldots, z_8)(y - x = \sum_{i=1}^{8} z_i^2)$. D'après la proposition 1, il existe des éléments u et v de K tels qu'on ait: $K = R(u,v)$ et $P(u,v) = 0$ si P est le polynôme minimal de v sur $P(u)$ et tels que la première projection de la courbe plane C d'équation $P(x,y) = 0$ contienne $[0, +\infty[$, donc $\mathbf{N}$. Soit $\mathscr{R}(x)$ une formulae définissant R dans K ([1], Corollaire 11). On voit alors que $\mathbf{N}$ est définissable dans K par la formule $\mathscr{N}(x)$ (avec u comme paramètre):

$$\exists f[f \neq 0 \wedge f^2 \leq_8 u^2]$$
$$\wedge \forall h(\mathscr{R}(h) \wedge h \neq x \wedge f^2 \leq_8 (u-h)^2 \rightarrow f^2 \leq_8 (u - h - 1)^2)].$$

Si n est un entier naturel, K satisfait $\mathscr{N}(n)$ d'après la proposition 2 appliquée avec $x_i = i$.

D'autre part, si h est un entier naturel (donc est élément de la première projection de C) et si on a: $f(u,v)^2 \leq_8 (u-h)^2$, soient des éléments de $K, z_1, \ldots, z_8$ satisfaisant à $(u - x_i)^2 - f(u,v)^2 = \sum_{i=1}^{8} z_i^2$. Soit h' tel que (h,h') soit un élément de C. Si (h,h') n'est ni un point isolé de C, ni un pôle de f, sur un voisinage de (h,h') où il n'y a d'autre pôle des z_i éventuellement que (h,h'), on a: $\sum_{i=1}^{8} z_i^2 \geq 0$, et par passage à la limite: $-f(h,h')^2 \geq 0$, donc en définitive: $f(h,h') = 0$. On a donc démontré que, si h est un entier naturel satisfaisant à: $f(u,v)^2 \leq_8 (u-h)^2$, alors (h,h') est un point isolé de C, un zéro de f ou un pôle de f. Or il n'y a qu'un nombre fini de tels points; mais, si x n'est pas un entier naturel et satisfait $\mathscr{N}(x)$, on démontre (par récurrence) que pour tout entier naturel n, on a: $f(u,v)^2 \leq_8 (u-n)^2$, et que, donc, l'ensemble des points isolés de C, des zéros de f, et des pôles de f contient $\mathbf{N}$ ce qui est contradictoire. □

B. Le cas général.

4. PROPOSITION. *Soient K un corps de courbe réelle sur k, u et v des éléments de K tels qu'on ait: $K = k(u,v)$, et P le polynôme minimal de v sur $k(u)$; C la courbe plane (définie sur k) d'équation $P(x,y) = 0$; $\overline{k}$ la clôture réelle de k. S'il existe une*

courbe elliptique plane E définie sur $\overline{k}$, d'équation $y^2 = 4x^3 - g_2x - g_3$, telle qu'on ait:

(1) *il n'existe pas de morphisme fini de C sur E,*

(2) *il existe un point de E, rationnel sur $\overline{k}$, d'ordre infini (pour l'addition de E dont l'élément neutre est le point à l'infini), alors K est indécidable.*

DÉMONSTRATION. Soit k' le sous-corps de $\overline{k}$ engendré sur k par g_2, g_3 et les coordonnées du point d'ordre infini (α, β). Puisque $K' = K \otimes_k k' = k'(u, v)$ est traductible (avec un nombre fini de paramètres) dans K, il suffit de traduire $(\mathbf{N}, +, \cdot)$, ou $(\mathbf{N}^*, +, |)$, dans K' avec comme paramètres u, g_2, g_3, α, et β.

Soit φ une formule (à paramètres) à 6 variables libres $x_1, x_2, y_1, y_2, z_1, z_2$, telle que, si (a_1, a_2) et (b_1, b_2) sont des points de E, K satisfait $\varphi(a_1, \ldots, c_2)$ si et seulement si (c_1, c_2) est le composé (pour la loi de E) de (a_1, a_2) et de (b_1, b_2) (voir [2] chapitre 5, §6). Soit ψ la formule à 4 variables libres x_1, x_2, y_1, y_2:

$$\begin{aligned}\exists f \exists g \{ & f \neq 0 \wedge g \neq 0 \wedge f^2 \leq_8 (u - x_1)^2 \wedge g^2 \leq_8 (u - x_2)^2 \\ & \wedge \forall z_1 \forall z_2 [\langle z_2^2 = 4z_1^3 - g_2 z_1 - g_3 \wedge (z_1 \neq y_1 \vee z_2 \neq y_2) \\ & \qquad \wedge f^2 \leq_8 (u - x_1)^2 \wedge g^2 \leq_8 (u - x_2)^2 \rangle \\ & \rightarrow \forall w_1 \forall w_2 \langle \varphi(z_1, z_2, \alpha, \beta, w_1, w_2) \rightarrow f^2 \leq_8 (u - w_1)^2 \wedge g^2 \leq_8 (u - w_2)^2 \rangle] \}.\end{aligned}$$

On voit, comme précedemment, que, si (a_1, a_2) et (b_1, b_2) sont des points de E, K satisfait $\psi(a_1, a_2, b_1, b_2)$ si et seulement si (b_1, b_2) est un "multiple" de (a_1, a_2).

On traduit alors $\mathbf{N}^*$ par l'ensemble des couples d'éléments de K, (x_1, x_2) qui satisfont la formule:

$$x_2^2 = 4x_1^3 - g_2 x_1 - g_3 \wedge \psi(\alpha, \beta, x_1, x_2).$$

Si a_1 et a_2 sont des points de K satisfaisant à $a_2^2 = 4a_1^3 - g_2 a_1 - g_3$, puisqu'il n'existe pas de morphisme fini de C sur E, a_1 et a_2 sont des éléments de k', et donc la traduction de $\mathbf{N}^*$ est l'ensemble des multiples de (α, β). On traduit alors l'addition par φ et la divisibilité par ψ. □

Nous allons maintenant donner des conditions suffisantes des hypothèses de cette proposition.

5. PROPOSITION. *Si C est une courbe, il existe une courbe elliptique E définie sur $\mathbf{Q}$ telle qu'il n'y ait pas de morphisme fini de C sur E.*[1]

DÉMONSTRATION. Si le genre de C est nul, d'après le théorème de Hurwitz, n'importe quelle courbe elliptique convient.

Supposons donc que le genre de C n'est pas nul, et soit E est une courbe elliptique (d'invariant modulaire j) telle qu'il y ait un morphisme dominant $C \rightarrow E$. De ce morphisme, on déduit un morphisme nontrivial des jacobiennes $\psi: J(E) \rightarrow J(C)$. La variété abélienne $J(C)$ est isogène à un produit fini de sous-variétés abéliennes simples $A_1 \times \cdots \times A_n$, uniques à isogènie près ([4], chapitre I, théorème 11, p. 19). Mais d'après le théorème de réductibilité complète de Poincaré ([4], chapitre I, théorème 9, p. 15), il existe une sous-variété abélienne de $J(C)$, A, telle qu'on ait $J(C) = \operatorname{Im}\psi + A$ et que $\operatorname{Im}\psi \cap A$ soit fini; donc $J(C)$ est isogène à

[1] Merci à Arnaut Beauville, Jean-Yves Mérindol, et les géomètres d'Angers.

$\operatorname{Im}\psi \times A$. Donc $\operatorname{Im}\psi$ est isogène à l'un des A_i, et j est entier sur $\mathbf{Z}[j_i]$ (où j_i est l'invariant modulaire de A_i) ([5], chapitre III, théorème (3.10), p. 201).

Il suffit donc de prendre une courbe elliptique dont l'invariant modulaire j est rationnel et n'est pas entier sur $\mathbf{Z}[j_i]$ pour tout i tel que A_i est de dimension 1. L'existence d'un tel rationnel résulte des lemmes suivants. □

6. LEMME. *Si t est un nombre transcendant sur $\mathbf{Q}$, tout nombre rationnel entier sur $\mathbf{Z}[t]$ est un entier relatif.*

DÉMONSTRATION. Soient x un rationnel entier sur

$$\mathbf{Z}[t], P(T,X) = X^n + \sum_{i=0}^{n-1} A_i(T)X^i \in \mathbf{Z}[T,X]$$

un polynôme tel qu'on ait: $P(t,x) = 0$. Puisque $P(T,x)$ est un polynôme (en T) sur $\mathbf{Q}$ et que t est transcendant sur $\mathbf{Q}$, $P(T,x)$ est nul; le coefficient constant (en T) de $P(T,x)$ est nul, ce qui est une relation de dépendance intégrale de x sur $\mathbf{Z}$. Puisque $\mathbf{Z}$ est intégralement clos, x est élément de $\mathbf{Z}$. □

7. LEMME. *Soient A un anneau intègre, F son corps des fractions, α un élément algébrique sur F, et $P(X) = \Delta X^n + \sum_{i=0}^{n-1} a_i X^i \in A[X]$ un polynôme dont α est racine. Alors $\Delta\alpha$ est entier sur A.*

DÉMONSTRATION. On a en effet:

$$(\Delta\alpha)^n + \sum_{i=0}^{n-1} a_i \Delta^{n-1-i}(\Delta\alpha)^i = (\Delta^{n-1}P)(\alpha) = 0. \qquad \square$$

8. LEMME. *Soient α un nombre algébrique sur $\mathbf{Q}$, $P(X) = \Delta X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbf{Z}[X]$ un polynôme dont α est racine et β un nombre entier sur $\mathbf{Z}[\alpha]$. Il existe un entier naturel m tel que $\Delta^m\beta$ soit entier sur $\mathbf{Z}$.*

DÉMONSTRATION. Soit $Q(T,X) \in \mathbf{Z}[T,X]$ un polynôme unitaire en X satisfaisant à $Q(\alpha,\beta) = 0$. Si m est la plus grande puissance de T dans $Q(T,X)$, d'après le lemme 7, $\Delta^m Q(\alpha,X)$ est un polynôme dont les coefficients sont entiers sur $\mathbf{Z}$ et dont le coefficient dominant en X est Δ^m. D'après le lemme 7, $\Delta^m\beta$ est entier sur l'anneau engendré sur $\mathbf{Z}$ par les coefficients de $\Delta^m Q(\alpha,X)$, anneau qui est entier sur $\mathbf{Z}$. Donc $\Delta^m\beta$ est entier sur $\mathbf{Z}$. □

9. FIN DE LA DÉMONSTRATION DE LA PROPOSITION 5. Soient $B_1,\ldots,B_r$ les sous-variétés A_i de dimension 1 dont les invariants modulaires $j_1,\ldots,j_r$ sont algébriques sur $\mathbf{Q}$, Δ_i le coefficient du terme de plus haut degré du polynôme minimal de j_i, p un entier naturel premier ne divisant aucun des Δ_i. Quel que soit m, Δ_i^m/p est un rationnel qui n'est pas élément de $\mathbf{Z}$, et qui, donc, n'est pas entier sur $\mathbf{Z}$ (puisque $\mathbf{Z}$ est intégralement clos); donc $\frac{1}{p}$ n'est pas entier sur $\mathbf{Z}[j_i]$ (lemme 8). Tenant compte du lemme 6, $\frac{1}{p}$ est le nombre rationnel cherché. □

10. PROPOSITION. *Si E est une courbe elliptique défini sur un corps formellement réel k_0 et k une extension de k_0 réelle-close, alors il existe un point de E rationnel sur k d'ordre infini.*

DÉMONSTRATION. Nous pouvons supposer E sous forme de Weierstrass, c'est à dire d'équation $y^2 = x^3 + ax + b$ (où a et b sont éléments de k_0). Soit j son invariant modulaire.

Supposons k de degré de transcendance au moins 1 sur $\mathbf{Q}(j)$ (corps de définition de E, donc inclus dans k_0). Les coordonnées des points d'ordre fini sont algé-

briques sur k_0 ([3], chapitre 2, §1, p. 24). Un point dont l'ordonnée est transcendante sur k_0, est donc d'ordre infini.

Si k est algébrique sur $\mathbf{Q}(j)$ (donc sous-corps de la clôture réelle de $\mathbf{Q}(j)$), soit A_n le sous-groupe des points dont l'ordre divise n. Si le corps engendré sur $\mathbf{Q}(j)$ par $\bigcup_{n\in\mathbf{N}} A_n$ contenait la clôture réelle de $\mathbf{Q}(j)$, la clôture algébrique de $\mathbf{Q}(j)$ serait $\mathbf{Q}(j)(\bigcup_{n\in\mathbf{N}} A_n)$ ou $\mathbf{Q}(j)(\bigcup_{n\in\mathbf{N}} A_n, i)$. Soit K une extension galoisienne de $\mathbf{Q}(j)$ dont le groupe de Galois est S_m; K est un sous-corps de $\mathbf{Q}(j)(A_N)$ ou de $\mathbf{Q}(j)(A_N, i)$ (pour un certain N), et S_m est donc image homomorphe du groupe de Galois de $\mathbf{Q}(j)(A_N)$ on de $\mathbf{Q}(j)(A_N, i)$ sur $\mathbf{Q}(j)$. D'où une contradiction car le groupe de Galois de $\mathbf{Q}(j)(A_N)$ est un sous-groupe de $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ ([3], chapitre 2, §1). □

Comme corollaire des propositions 4, 5, et 10, on obtient donc:

11. THÉORÈME. *Un corps de courbe réelle est indécidable.*

RÉFÉRENCES

[1] JEAN-LOUIS DURET, *Sur la théorie élémentaire des corps de fonctions*, this JOURNAL, vol. 51 (1968), pp. 948–956.

[2] WILLIAM FULTON, ***Algebraic curves***, Benjamin, New York.

[3] SERGE LANG, ***Elliptic functions***, Addison-Wesley, Reading.

[4] ANDRÉ NÉRON, ***Variétés abéliennes***, Publication Mathématiques d'Orsay, Orsay.

[5] ALAIN ROBERT, ***Elliptic curves***, Lecture Notes in Mathematics, vol. 326, Springer-Verlag, Berlin and New York.

[6] RAPHAEL ROBINSON, *The undecidability of pure transcendental extensions of real fields*, ***Zeitschrift für Matematische Logik und Grundlagen der Mathematik, vol. 10*** (1964), pp. 275–282.

DÉPARTEMENT DE MATHÉMATIQUES ET INFORMATIQUE
UNIVERSITÉ DU QUÉBEC À MONTRÉAL
MONTRÉAL, QUÉBEC, H3C 3P8

E-mail: r31170@uqam.bitnet

U. F. R. STRUCTURES ET MATÉRIAUX
UNIVERSITÉ D'ANGERS
49045 ANGERS CEDEX, FRANCE

E-mail: duret@logique.jussieu.fr