Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 336 (2003) 459–462
COMPTES RENDUS MATHEMATIQUE

Logique

La définissabilité des entiers dans les corps de courbes réelles archimédiens

Definability of the natural numbers in function fields over an Archimedean field

Luc Bélair [a,b]

[a] *Département de mathématiques, Université du Québec, Montréal, Québec, H3C 3P8, Canada*
[b] *Équipe de logique mathématique – CNRS, UFR de mathématiques, Université Denis Diderot – Paris 7, 2, place Jussieu, 75251 Paris cedex 05, France*

Reçu le 4 février 2003 ; accepté le 19 février 2003

Présenté par Jean-Yves Girard

Résumé

On montre que les entiers naturels sont définissables dans les corps de courbes réelles sur un corps ordonnable qui admet au moins un ordre archimédien. Ceci généralise le résultat de Raphael Robinson sur les corps de fonctions rationnelles. ***Pour citer cet article : L. Bélair, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

Abstract

We show that the natural numbers are definable in the function field of a curve over a formally real field which admits at least one Archimedean order. This generalises Raphael Robinson's result on fields of rational functions. ***To cite this article: L. Bélair, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

1. Introduction

Dans son très bel article sur l'indécidabilité des corps de fonctions rationnelles sur les corps ordonnables, Raphael Robinson [2] a aussi montré que l'ensemble des entiers naturels est définissable si le corps de base possède au moins un ordre archimédien. Dans la généralisation aux corps de courbes réelles dans [1], cet aspect a été négligé. On vérifie ci-dessous que ce résultat se généralise aussi aux corps de courbes réelles. La définissabilité des entiers naturels dans un corps de courbe réelle quelconque est toujours ouverte.

Adresse e-mail : belair.luc@uqam.ca (L. Bélair).

1631-073X/03/$ – see front matter
doi:10.1016/S1631-073X(03)00115-8

Soit k un corps ordonnable qui admet au moins un ordre archimédien. Soit K un corps de courbe réelle sur k, c'est-à-dire que K est une extension de k ordonnable, finiment engendrée sur k 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. Notons que, puisque k se plonge dans $\mathbb{R}$ et y est dense, toute courbe sur k dont K est le corps a un point régulier rationnel sur k (voir [1]). Comme dans [1] on a besoin d'une courbe elliptique sur $\mathbb{Q}$ avec un invariant modulaire approprié. Cette fois-ci, on remarque qu'on peut trouver une telle courbe avec un point d'ordre infini explicite, comme Raphael Robinson. Le reste de l'argument se transpose alors sans nouvelle difficulté.

2. Courbes elliptiques avec un point d'ordre infini

On montre dans [1], §B, que l'ensemble des solutions (x, y) de la formule $y^2 = x^3 + ax + b$, dans $K \times K$, est contenu dans $k \times k$ dès que $y^2 = x^3 + ax + b$ est une courbe elliptique définie sur $\mathbb{Q}$ dont l'invariant modulaire est n/p pour un nombre premier p approprié, qui ne divise pas n. Soit la courbe elliptique

$$y^2 = x^3 + 3(p-4)x + (p-4)^2.$$

Son invariant modulaire est

$$J = \frac{27(3(p-4))^3}{4(3(p-4))^3 + 27((p-4)^2)^2} = \frac{27}{4 + (p-4)} = \frac{27}{p}.$$

Elle possède le point rationnel $(0, p-4)$. On vérifie ci-dessous, à la main, que c'est un point d'ordre infini.[1]

On paramètre la courbe à l'aide de la fonction de Weirstrass

$$x = \mathcal{P}(w),$$
$$y = \frac{\mathcal{P}'(w)}{2}.$$

Soit

$$(x_1, y_1) = (0, p-4),\ y_1 = \frac{\mathcal{P}'(v)}{2}.$$

Les multiples de (x_1, y_1) sont

$$(x_n, y_n) = \left(\mathcal{P}(nv), \frac{\mathcal{P}'(nv)}{2}\right)$$

et seront aussi rationnels, pour $n \in \mathbb{Z}$. Soit $m_{ij} = (y_j - y_i)/(x_j - x_i)$. Par la construction géométrique de l'addition sur la courbe, le point (x_{i+j}, y_{i+j}) est donné par le troisième point d'intersection de la corde

$$y - y_i = m_{ij}(x - x_i)$$

avec la courbe. En substituant dans l'équation de la courbe, on obtient

$$x^2 + \left(x_i - m_{ij}^2\right)x + x_i^2 + 3(p-4) + m_{ij}^2 x_i - 2m_{ij} y_i = 0.$$

On sait que

$$x_j = \frac{-x_i + m_{ij}^2 + \alpha}{2},$$
$$x_{i+j} = \frac{-x_i + m_{ij}^2 - \alpha}{2}$$

[1] Le rapporteur note que cela découle aussi du théorème de Lutz–Nagell (voir [3]).

pour un certain α disons. D'où

$$x_{i+j} = -x_i - x_j + m_{ij}^2.$$

Quand $i = j$, on remplace m_{ij} par

$$m_{ii} = \left.\frac{dy}{dx}\right|_{(x_i, y_i)} = \frac{3x_i^2 + 3(p-4)}{2y_i}.$$

Ainsi

$$\begin{aligned} x_{2i} &= -2x_i + \left(\frac{3x_i^2 + 3(p-4)}{2y_i}\right)^2 \\ &= \frac{-8x_i(x_i^3 + 3(p-4)x_i + (p-4)^2) + 9(x_i^2 + p - 4)^2}{4(x_i^3 + 3(p-4)x_i + (p-4)^2)}. \end{aligned}$$

Posons $x_i = a/b$, $a, b \in \mathbb{Z}$, sous forme irréductible. On obtient

$$x_{2i} = \frac{-8a(a^3 + 3(p-4)ab^2 + (p-4)^2b^3) + 9(a^2 + (p-4)b^2)^2}{4b(a^3 + 3(p-4)ab^2 + (p-4)^2b^3)}.$$

Supposons a impair.

Alors $4b$ est premier au numérateur et apparaît donc au dénominateur de x_{2i} exprimé sous forme irréductible.

Or notons que $x_2 = 9/4$.

Ainsi lorsque x_{2^i} est exprimé sous forme irréductible, un facteur 4^i apparaît au dénominateur de sorte que tous les points (x_{2^i}, y_{2^i}) sont des points rationnels distincts.

Ainsi cette courbe possède un nombre infini de points rationnels. En particulier, le point (x_1, y_1) est d'ordre infini.

Il s'ensuit aussi que la valeur du paramètre v qui correspond au point $(x_1, y_1) = (0, p-4)$ n'est pas un multiple rationnel de la période de $\mathcal{P}(w)$. Ainsi *tous* les points (x_n, y_n) sont distincts, et ils sont denses sur la courbe dans le plan réel. En particulier, les ordonnées y_n sont denses dans les nombres rationnels.

On peut utiliser cette courbe pour le cas général dans [1], §B, ce qui simplifie un peu les choses.

3. Définition des entiers naturels

Il suffit maintenant de suivre le procédé de Raphael Robinson pour obtenir une formule $\kappa(x)$ qui puisse définir un sous-ensemble de k qui contienne les entiers naturels. Cela suffit pour obtenir une définition des entiers naturels comme dans [1], §A, qui est une adaptation de la méthode de Julia Robinson (voir [2], §3).

Dans la suite, nous explicitons succinctement la formule $\kappa(x)$.

On fixe une courbe plane C sur k dont K est le corps de fonctions. Disons C d'équation $P(X, Y) = 0$, et $\alpha, \beta \in K \setminus k$ tel que $P(\alpha, \beta) = 0$ et $K = k(\alpha, \beta)$.

Nous allons définir les abscisses puis les ordonnées des points (x_n, y_n) ci-dessus. Rappelons un résultat de Julia Robinson : pour tous nombres rationnels $x_1, \ldots, x_n$ il existe une fonction rationnelle $f(X) \in \mathbb{Q}(X)$, sans pôle réel et dont les seuls zéros sont $x_1, \ldots, x_n$[2] telle que pour chaque $i = 1, \ldots, n$ il existe $z_1, \ldots, z_8 \in \mathbb{Q}(X)$ tel que $(X - x_i)^2 - f(X)^2 = \sum_{i=1}^{8} z_i^2$. Rappelons aussi la notation $x \leqslant_n y$ pour désigner $\exists z_1, \ldots, z_n (y - x = \sum_{i=1}^{n} z_i^2)$.

Les abscisses sont définies par la formule $ABS(a)$, avec α comme paramètre :

[2] Cette propriété, essentielle, a malheureusement disparu du rappel fait dans [1], §A.2.

$$\begin{aligned} a = 0 \vee \exists f \big(& f \neq 0 \wedge f^2 \leqslant_8 (\alpha - 9/4)^2 \\ & \wedge \forall x, y, m (x \neq 9/4 \wedge x \neq a \wedge f^2 \leqslant_8 (\alpha - x)^2 \\ & \wedge y^2 = x^3 + 3(p-4)x + (p-4)^2 \wedge y - (p-4) = mx \\ & \longrightarrow f^2 \leqslant_8 (\alpha + x - m^2)^2 \big). \end{aligned}$$

Remarquons tout d'abord que si $a \neq 0$, la formule assure l'existence d'une fonction non nulle f telle que $f^2 \leqslant_8 (\alpha - x)^2$ est vérifiée quand $x = x_2 = 9/4$, et que si cette inégalité est vérifiée pour $x = x_k$, $x_k \neq 0$ et $x_k \neq a$, alors elle est vérifiée pour $x = x_{k-1}$ et $x = x_{k+1}$ (deux cas à cause de l'ambiguité du signe de y). Voyons que les abscisses $a = x_n$ vérifient la formule $ABS(a)$. En effet, si $a = x_n$, $n \geqslant 2$, alors la fonction de Julia Robinson satisfait la condition requise, car les coordonnées des points sur la courbe elliptique doivent être dans k. Voyons maintenant que seules les abscisses $a = x_n$ vérifient la formule $ABS(a)$. En effet, si a n'est pas un x_n mais vérifie quand même la formule $ABS(a)$, on montre par récurrence que pour tout $n \geqslant 2$ on a $f(\alpha, \beta) \leqslant_8 (\alpha - x_n)^2$. Or on vérifie (voir [1], §A.3) que cela entraîne que (x_n, y_n) est soit un point isolé de C, soit un pôle de f, soit un zéro de f, de sorte que l'ensemble des points isolés de C, des zéros de f et des pôles de f serait infini, ce qui est absurde.

Les ordonnées sont alors définies par la formule $ORD(b)$:

$$\exists a \big(ABS(a) \wedge b^3 = a^3 + 3(p-4)a + (p-4)^2 \big).$$

Soit la formule $\kappa(x)$:

$$\forall y \big(ORD(y) \to x \leqslant_4 y \vee y \leqslant_4 x \big).$$

Tout entier naturel satisfait cette formule. La formule $\kappa(x)$ définit dans K un ensemble de constantes de k. En effet, dans un ordre archimédien sur k, les nombres rationnels, et de là les ordonnées y satisfaisant $ORD(y)$, sont denses dans k. Ainsi, une fonction x qui n'est pas constante doit être parfois plus petite et parfois plus grande qu'au moins une de ces ordonnées, et donc ne peut pas satisfaire $\kappa(x)$.

Les entiers naturels sont alors définis dans K par la formule suivante $NAT(x)$, avec α comme paramètre :

$$\exists f \big[f \neq 0 \wedge f^2 \leqslant_8 \alpha^2 \wedge \forall h \big(\kappa(h) \wedge h \neq x \wedge f^2 \leqslant_8 (\alpha - h)^2 \to f^2 \leqslant_8 (\alpha - h - 1)^2 \big) \big].$$

Julia Robinson indique comment éliminer facilement le paramètre α (voir [2], §3).

Références

[1] L. Bélair, J.-L. Duret, Indécidabilité des corps de courbe réelle, J. Symbolic Logic 59 (1994) 87–91.
[2] R. Robinson, The undecidability of pure transcendental extensions of real fields, Z. Math. Logik Grundlag. Math. 10 (1964) 275–282.
[3] J. Silverman, The Arithmetic of Elliptic Curves, Springer, 1986.