Équivalence élémentaire de corps elliptiques

Xavier VIDAUX

Comptes Rendus de l'Académie des Sciences de Paris, Série I 330 (2000), pp 1-4

Résumé. Il s'agit de démontrer une partie de la conjecture suivante: deux corps elliptiques sur un corps algébriquement clos k sont k -isomorphes si et seulement s'ils sont élémentairement équivalents dans le langage des corps enrichi d'une constante (l'invariant modulaire). C'est une extension des résultats de Duret sur l'équivalence élémentaire des corps de fonctions.

Elementary equivalence of elliptic fields

Abstract. I prove some part of the following conjecture: two elliptic fields over an algebraically closed field k are k -isomorphic if and only if they are elementarily equivalent in the language of fields expanded with a symbol of constant (the modular invariant). This is an extension of Duret's results about elementary equivalence of function fields.

Si ω_1 et ω_2 sont des nombres complexes $\mathbf{R}$ -linéairement indépendants, notons $\langle \omega_1, \omega_2 \rangle$ le réseau de $\mathbf{C}$ ayant pour base (ω_1, ω_2) . Soit τ un nombre complexe algébrique quadratique. Soit $AX^2 + BX + C$ un polynôme dont il est la racine, avec A un entier naturel strictement supérieur à 0, B et C des entiers relatifs vérifiant $A \wedge B \wedge C = 1$ ($a \wedge b$ désignant le pgcd positif de a et de b). Pour tout entier $n \in \mathbf{N}$ non nul, notons Λ_n le réseau $\langle \frac{1}{n}, \tau \rangle$, E_n le quotient $\frac{\mathbf{C}}{\Lambda_n}$, $\text{Hom}(E_1, E_n)$ le sous-groupe de $\mathbf{C} \setminus \{0\}$ $\{\alpha \in \mathbf{C} \mid \alpha \Lambda_1 \subset \Lambda_n\}$, $\text{End}(E_1)$ l'anneau $\text{Hom}(E_1, E_1)$ et δ_n l'entier $A \wedge nB \wedge nC = A \wedge n$. On a, pour tout entier naturel n strictement positif, $\text{End } E_1 \subset \text{Hom}(E_1, E_n)$ et si p est un diviseur de n , alors $\text{Hom}(E_1, E_p) \subset \text{Hom}(E_1, E_n)$.

Proposition 1 Pour tout entier $n \geq 1$, on a : $\text{Hom}(E_1, E_n) = \langle 1, \frac{A}{\delta_n} \bar{\tau} \rangle$

Démonstration : Pour la première inclusion, on a :

$$\langle 1, \frac{A}{\delta_n} \bar{\tau} \rangle \langle 1, \tau \rangle = \langle 1, \tau, \frac{A}{\delta_n} \bar{\tau}, \frac{A}{\delta_n} \bar{\tau} \tau \rangle = \langle 1, \tau, \frac{-B - A\tau}{\delta_n}, \frac{C}{\delta_n} \rangle = \langle 1, \tau, \frac{B}{\delta_n}, \frac{C}{\delta_n} \rangle \subset \langle \frac{1}{n}, \tau \rangle.$$

Il s'ensuit que le réseau $\langle 1, \frac{A}{\delta_n} \bar{\tau} \rangle$ est inclus dans $\text{Hom}(C_1, C_n)$.

Nous montrons l'inclusion réciproque en utilisant un argument analogue à [5, thm. 2, p. 90].

On constate que :

$$\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n} \bar{\tau} \rangle \langle 1, \tau \rangle = \frac{n}{\delta_n} \langle A, A\bar{\tau}, A\tau, A\tau\bar{\tau} \rangle = \frac{n}{\delta_n} \langle A, -B - A\tau, A\tau, C \rangle = \frac{n}{\delta_n} \langle A, B, A\tau, C \rangle.$$

Or $A \wedge B \wedge C$ est égal à 1, donc 1 est élément de $\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n} \bar{\tau} \rangle \langle 1, \tau \rangle$. On constate aussi que :

$$\begin{aligned} \langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n} \bar{\tau} \rangle \langle \frac{1}{n}, \tau \rangle &= \frac{1}{\delta_n} \langle A, nA\tau, A\bar{\tau}, nA\tau\bar{\tau} \rangle = \\ &= \frac{1}{\delta_n} \langle A, n(-B - A\tau), A\bar{\tau}, nC \rangle = \frac{1}{\delta_n} \langle A, nB, A\bar{\tau}, nC \rangle \subset \frac{1}{\delta_n} \langle \delta_n, A\bar{\tau} \rangle \end{aligned}$$

car $A \wedge nB \wedge nC$ est par définition égal à δ_n . Donc on a $\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n} \bar{\tau} \rangle \langle \frac{1}{n}, \tau \rangle \subset \langle 1, \frac{A}{\delta_n} \bar{\tau} \rangle$. Par conséquent, si nous notons Λ le réseau $\langle \frac{nA}{\delta_n}, \frac{nA}{\delta_n} \bar{\tau} \rangle$, les remarques précédentes se traduisent par: $1 \in \Lambda\Lambda_1$ et $\Lambda\Lambda_n \subset \langle 1, \frac{A}{\delta_n} \bar{\tau} \rangle$. Soit α un élément de $\text{Hom}(E_1, E_n)$. On a $\alpha\Lambda_1 \subset \Lambda_n$, donc on a aussi $\alpha\Lambda\Lambda_1 \subset \Lambda\Lambda_n$, mais comme $1 \in \Lambda\Lambda_1$, on a $\alpha \in \Lambda\Lambda_n \subset \langle 1, \frac{A}{\delta_n} \bar{\tau} \rangle$. D'où l'autre inclusion. $\square$

Lemme 2 *Le réseau $\text{Hom}(E_1, E_n)$ est inclus dans le réseau $\text{Hom}(E_1, E_p)$ si et seulement si δ_n divise p .*

Démonstration :

$$\begin{aligned} \text{Hom}(E_1, E_n) \subset \text{Hom}(E_1, E_p) &\iff \langle 1, \frac{A}{\delta_n} \bar{\tau} \rangle \subset \langle 1, \frac{A}{\delta_p} \bar{\tau} \rangle \iff \exists l \in \mathbf{Z}, \frac{A}{\delta_n} \bar{\tau} = \frac{lA}{\delta_p} \bar{\tau} \\ &\iff \exists l \in \mathbf{Z}, \delta_p = l\delta_n \iff A \wedge n \text{ divise } A \wedge p \iff A \wedge n \text{ divise } p. \end{aligned}$$

$\square$

Corollaire 3 *Pour tout entier $n \in \mathbf{N}^*$, on a :*

$$\text{Hom}(E_1, E_n) = \text{Hom}(E_1, E_{\delta_n}).$$

Le plus petit entier naturel p tel que $\text{Hom}(E_1, E_n) = \text{Hom}(E_1, E_p)$ est $p = \delta_n$.

Corollaire 4 *Si p et q divisent A , alors on a l'équivalence suivante :*

$$\text{Hom}(E_1, E_p) = \text{Hom}(E_1, E_q) \iff p = q.$$

Corollaire 5 *L'application*

$$\begin{array}{ccc} \{p \in \mathbf{N}^* \mid p \text{ divise } A\} & \longrightarrow & \{\text{Hom}(E_1, E_p) \mid p \in \mathbf{N}^*\} \\ p & \longmapsto & \text{Hom}(E_1, E_p) \end{array}$$

est une bijection. En particulier, la cardinal de l'ensemble $\{\text{Hom}(E_1, E_p) \mid p \in \mathbf{N}^\}$ est le nombre de diviseurs de A .*

Démonstration : C'est une application injective par 4. Elle est surjective par 3. $\square$

Dorénavant, nous noterons Λ_n^τ le réseau $\langle \frac{1}{n}, \tau \rangle$. Notons $\mathcal{P}_n^\tau$ la fonction de Weierstrass de Λ_n^τ et $g_2^n(\tau)$ et $g_3^n(\tau)$ les nombres complexes tels que $(\mathcal{P}_n^{\tau'})^2 = 4\mathcal{P}_n^{\tau 3} - g_2^n(\tau)\mathcal{P}_n^\tau - g_3^n(\tau)$. Notons $R_n^\tau(X, Y)$ le polynôme $Y^2 - 4X^3 + g_2^n(\tau)X + g_3^n(\tau) \in \mathbf{C}[X, Y]$. Si k est un corps, notons $cl.a.(k)$ sa clôture algébrique.

Nous rappelons que (voir [4, p. 316-336]) pour tout corps de courbe K sur un corps algébriquement clos k , sous-corps de $\mathbf{C}$, d'invariant modulaire j , il existe u et v dans K et des éléments a et b de k tels que $v^2 = 4u^3 - au - b$. Mais j est égal à $1728 \frac{a^3}{a^3 - 27b^2}$ donc j est élément de k . Il s'ensuit que k contient $cl.a.(\mathbf{Q}(j))$. Par la suite, nous noterons j_τ l'invariant modulaire de la courbe elliptique associée à $E_1^\tau = \frac{\mathbf{C}}{\Lambda_1^\tau}$, et Δ_τ le corps $cl.a.(\mathbf{Q}(j_\tau))$. On a l'égalité $cl.a.(\mathbf{Q}(j_\tau)) = cl.a.(\mathbf{Q}(g_2^1(\tau), g_3^1(\tau)))$.

D'après [1, prop. 31, p. 816], $g_2^n(\tau)$ et $g_3^n(\tau)$ sont algébriques sur $\mathbf{Q}(g_2^1(\tau), g_3^1(\tau))$, donc ils sont dans Δ_τ . Nous noterons $\mathcal{E}(\Lambda_n^\tau)$ le corps des fonctions méromorphes ayant pour ensemble de périodes Λ_n^τ . On a $\mathcal{E}(\Lambda_n^\tau) = \mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$. Enfin, nous noterons $\mathcal{L}$ le langage des corps et $\mathcal{L}(j_\tau)$ le langage des corps ayant j_τ comme symbole de constante supplémentaire.

Si k est un sous-corps de $\mathbf{C}$ algébriquement clos contenant Δ , τ un nombre complexe algébrique quadratique et n un entier naturel strictement supérieur à 1, soit $\mathbf{P}_n^\tau(k)$ la propriété: “ $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j_\tau)$ ”. Si K est un corps de courbe de genre 1 sur un corps algébriquement clos k de caractéristique 0, avec multiplication complexe et d’invariant modulaire j , et K' un corps de courbe sur k non isomorphe à K , soit $\mathbf{P}(K, K')$ la propriété: “ K et K' ne sont pas élémentairement équivalents dans le langage $\mathcal{L}(j)$ ”.

Proposition 6 *Si $\mathbf{P}_n^\tau(k)$ est vraie pour tout triplet (k, τ, n) , alors $\mathbf{P}(K, K')$ est vraie pour tout couple (K, K') .*

Démonstration: On trouve tous les arguments dans la première partie de la démonstration de [1, thm. 35, p. 818]. L’auteur démontre d’abord l’équivalence entre les trois propriétés suivantes ($2 \Rightarrow 1$ puis $3 \Rightarrow 2$):

1. La propriété $\mathbf{P}(K, K')$ est vraie pour tout couple (K, K') .
2. La propriété $\mathbf{P}(K, K')$ est vraie pour tout couple (K, K') avec k sous-corps de $\mathbf{C}$.
3. La propriété $\mathbf{P}(K, K')$ est vraie pour tout couple (K, K') avec K' sous-corps de K et k sous-corps de $\mathbf{C}$.

Si k est un sous-corps de $\mathbf{C}$, alors on a $K \otimes_k \mathbf{C} = \mathcal{E}(\Lambda)$ et $K' \otimes_k \mathbf{C} = \mathcal{E}(\Lambda')$ pour des réseaux Λ et Λ' de $\mathbf{C}$; et comme K' est un sous-corps de K , on a $\Lambda \subset \Lambda'$. D’après [3, 63, p. 132], il existe une base (ω_1, ω_2) de Λ et des entiers naturels non nuls m et n tels que $(\frac{\omega_1}{mn}, \frac{\omega_2}{m})$ soit une base de Λ' . Notons τ le quotient $\frac{\omega_2}{\omega_1}$. Comme $\langle \frac{\omega_1}{mn}, \frac{\omega_2}{m} \rangle$ est similaire à $\langle \frac{\omega_1}{n}, \omega_2 \rangle$, et donc à $\langle \frac{1}{n}, \tau \rangle$, et $\langle \omega_1, \omega_2 \rangle$ est similaire à $\langle 1, \tau \rangle$, $\mathcal{E}(\Lambda)$ et $\mathcal{E}(\Lambda')$ sont $\mathbf{C}$ -isomorphes respectivement à $\mathcal{E}(\langle 1, \tau \rangle)$ et à $\mathcal{E}(\langle \frac{1}{n}, \tau \rangle)$. Si nous notons $\mathcal{P}_n^\tau$ la fonction de Weierstrass de $\langle \frac{1}{n}, \tau \rangle$ et $\mathcal{P}_1^\tau$ celle de $\langle 1, \tau \rangle$, $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ sont k -isomorphes respectivement à K' et à K . Donc la propriété $\mathbf{P}(K, K')$ est équivalente à la propriété $\mathbf{P}(k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'}), k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'}))$, ie: $\mathbf{P}_n^\tau(k)$. $\square$

Lemme 7 *Soit n un entier strictement positif et p un diviseur de n . On a alors $\Lambda_p^\tau \subset \Lambda_n^\tau$. Soit k un sous-corps de $\mathbf{C}$, extension de Δ .*

1. Les corps $\Delta(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ sont sous-corps respectivement de $\Delta(\mathcal{P}_p^\tau, \mathcal{P}_p^{\tau'})$ et de $k(\mathcal{P}_p^\tau, \mathcal{P}_p^{\tau'})$.
2. La fonction de Weierstrass $\mathcal{P}_p^\tau$ est élément primitif de $\Delta(\mathcal{P}_p^\tau, \mathcal{P}_p^{\tau'})$ sur $\Delta(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$, de $k(\mathcal{P}_p^\tau, \mathcal{P}_p^{\tau'})$ sur $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et de $\mathbf{C}(\mathcal{P}_p^\tau, \mathcal{P}_p^{\tau'})$ sur $\mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$.
3. Tout polynôme minimal de $\mathcal{P}_p^\tau$ sur $\Delta(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ est polynôme minimal de $\mathcal{P}_p^\tau$ sur $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et sur $\mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$. Il existe donc un polynôme $P_p^\tau(X, Y, Z)$ à coefficients dans Δ , tel que $P_p^\tau(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'}, Z)$ soit polynôme minimal de $\mathcal{P}_p^\tau$ sur $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et sur $\mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$.

Démonstration: On applique [1, prop. 32, p. 817] aux réseaux $\Lambda_p^\tau \subset \Lambda_n^\tau$ en constatant qu’en notant $\omega_1 = \frac{1}{p}$, $\omega_2 = \tau$ et $m = \frac{n}{p}$, on a :

$$\Lambda_p^\tau = \langle \omega_1, \omega_2 \rangle \subset \langle \frac{\omega_1}{m}, \omega_2 \rangle = \Lambda_n^\tau.$$

$\square$

Proposition 8 [Duret] *Pour tout couple (τ, n) , si $\text{Hom}(E_1^\tau, E_n^\tau)$ est égal à $\text{End } E_1^\tau$, alors la propriété $\mathbf{P}_n^\tau(k)$ est vraie pour tout k .*

Démonstration : [1, rem. 37, p. 821 relative au thm. 35, p. 818] $\square$

Théorème 9 *Pour tout couple (τ, n) , s'il existe un entier p tel que $1 \leq p < n$ et $\text{Hom}(E_1^\tau, E_n^\tau)$ est égal à $\text{Hom}(E_1^\tau, E_p^\tau)$, alors la propriété $\mathbf{P}_n^\tau(k)$ est vraie pour tout k .*

Démonstration : D'après la proposition 8, il suffit de le démontrer si p est strictement supérieur à 1, et d'après le corollaire 3, nous pouvons alors choisir $p = n \wedge A$. Soit C une formule définissant k dans $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et dans $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$, et $\mathbf{C}$ dans $\mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ et dans $\mathbf{C}(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ [2, prop. 10, p. 950]. D'après [1, prop. 33, p. 818], il suffit de trouver une formule à coefficients dans Δ_τ . Soit $\Theta_n^\tau(k)$ la formule

$$\exists x, y \left(-C(x) \wedge R_n^\tau(x, y) = 0 \wedge \forall z P_p^\tau(x, y, z) \neq 0 \right)$$

où $P_p^\tau(X, Y, Z) \in \Delta_\tau[X, Y, Z]$ est le polynôme défini dans le lemme 7(3).

Il est clair que $k(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'})$ satisfait la formule $\Theta_n^\tau(k)$. Il suffit de choisir $x = \mathcal{P}_n^\tau$, $y = \mathcal{P}_n^{\tau'}$ et de conclure d'après le lemme 7(3).

Montrons que $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ satisfait la formule $\neg\Theta_n^\tau(k)$. Soit donc u et v des éléments de $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ tels qu'on ait : $u \notin k$ et $R_n^\tau(u, v) = 0$. Nous cherchons $w \in k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ vérifiant $P_p^\tau(u, v, w) = 0$. S'il existe un tel w , il est algébrique sur $\Delta_\tau(u, v) \subset k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$. Mais $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ est algébriquement clos dans $\mathbf{C}(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$, donc il existe un tel w dans $k(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$ si et seulement s'il en existe un dans $\mathbf{C}(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$. Les conditions sur u et v donnent un $\mathbf{C}$ -isomorphisme de corps :

$$\phi_0: \mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'}) \xrightarrow{\sim} \mathbf{C}(u, v)$$

où $\phi_0(\mathcal{P}_n^\tau) = u$ et $\phi_0(\mathcal{P}_n^{\tau'}) = v$. Or on a $\mathbf{C}(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'}) = \mathcal{E}(\Lambda_n^\tau)$, donc il existe un nombre complexe non nul α tel qu'on ait $\mathbf{C}(u, v) = \mathcal{E}(\alpha\Lambda_n^\tau)$ [3, 90, pp. 195-196]. Mais $\mathbf{C}(u, v) \subset \mathbf{C}(\mathcal{P}_1^\tau, \mathcal{P}_1^{\tau'})$, donc on a $\mathcal{E}(\alpha\Lambda_n^\tau) \subset \mathcal{E}(\Lambda_1^\tau)$, ou en termes de réseaux, $\Lambda_1^\tau \subset \alpha\Lambda_n^\tau$, i.e. : $\alpha^{-1} \in \text{Hom}(E_1^\tau, E_n^\tau)$. Donc, et d'après l'hypothèse du théorème, α^{-1} est élément de $\text{Hom}(E_1^\tau, E_p^\tau)$, ce qui implique que Λ_1^τ est inclus dans $\alpha\Lambda_p^\tau$, ou, en termes de corps, $\mathcal{E}(\alpha\Lambda_p^\tau)$ est inclus dans $\mathcal{E}(\Lambda_1^\tau)$. Il s'ensuit que nous pouvons étendre ϕ_0 à un $\mathbf{C}$ -morphisme de corps :

$$\phi: \mathcal{E}(\Lambda_p^\tau) \xrightarrow{\sim} \mathcal{E}(\alpha\Lambda_p^\tau) \subset \mathcal{E}(\Lambda_1^\tau).$$

Choisissons $w = \phi(\mathcal{P}_p^\tau)$. On a bien $P_p^\tau(u, v, w) = \phi(P_p^\tau(\mathcal{P}_n^\tau, \mathcal{P}_n^{\tau'}, \mathcal{P}_p^\tau)) = 0$. $\square$

D'après le corollaire 5, il existe p tel que $1 \leq p < n$ et $\text{Hom}(E_1, E_n) = \text{Hom}(E_1, E_p)$ si et seulement si n ne divise pas A . Pour chaque τ donc, et pour chaque k , il reste à trouver la formule $\Theta_n^\tau(k)$ pour tous les diviseurs n de l'entier A .

Références bibliographiques

- [1] Duret J.-L., Équivalence élémentaire et isomorphisme des corps de courbe sur un corps algébriquement clos, Journ. Symb. Logic, vol.57, n3 (1992) 808-823.
- [2] Duret J.-L., Sur la théorie élémentaire des corps de fonctions, Journ. Symb. Logic, vol. 51, n4 (1986) 948-956.
- [3] Du Val P., Elliptic Functions and elliptic curves, London Math. Society Lect. Note Series, 9, Cambridge University Press, 1973.
- [4] Hartshorne R., Algebraic geometry, Springer-Verlag, New York, 1977.
- [5] Lang S., Elliptic functions, Springer-Verlag, New York, 1987.