

Author: Dimitrios Poulakis

Title: Courbes Elliptiques et 2 – Extensions Abeliennes

Creator: HDML

COURBES ELLIPTIQUES ET 2-EXTENSIONS ABÉLIENNES

Dimitrios Poulakis

Résumé

Soient K une extension de \mathbf{Q} de type fini et E une courbe elliptique sur K . On montre que le \mathbf{Z} -rang du groupe $E(F)$, où $F = K[\sqrt{z} \mid z \in K]$ est infini. On étend ainsi un résultat des Frey et Jarden ([1], §2) en vertu duquel pour toute courbe elliptique sur \mathbf{Q} , le \mathbf{Z} -rang du groupe $E(F)$, où $F = \mathbf{Q}[\sqrt{z} \mid z \in \mathbf{Z}]$ est infini.

Summary

Let K be an extension of finite type over \mathbf{Q} and E an elliptic curve over k . We prove that the \mathbf{Z} -rank of the group $E(F)$, where $F = K[\sqrt{z} \mid z \in K]$, is infinite. We thus extend a result of Frey and Jarden ([1], §2) that states: for any elliptic curve over \mathbf{Q} , the \mathbf{Z} -rank of the group $E(F)$, where $F = \mathbf{Q}[\sqrt{z} \mid z \in \mathbf{Z}]$, is infinite.

1. Introduction

Soient $k = \mathbf{Q}$ ou $k = F_p$ et K/k une extension de k de type fini. Soit A une variété abélienne sur K . D'après le fameux théorème des Mordell-Weil-Néron on a:

$$A(K) \cong \mathbf{Z}^f \oplus T$$

où T est un groupe fini. Si l'extension K/k n'est pas de type fini on a, d'après [1], que en général le \mathbf{Z} -rang du groupe $A(K)$ n'est pas fini.

Soit E une courbe elliptique sur \mathbf{Q} . Dans le §2 de [1] on construit une suite (P_i) de points de E , qui sont \mathbf{Z} -linéairement indépendants et P_i est rationnel sur un corps quadratique; cela entraîne que le \mathbf{Z} -rang du groupe $E(K)$, où $K = \mathbf{Q}[\sqrt{z} \mid z \in \mathbf{Z}]$ est infini.

Soit E une courbe elliptique sur $L = \mathbf{Q}(T_1, \dots, T_n)$, une extension transcendante pure de \mathbf{Q} . Alors il est facile à vérifier, en utilisant le résultat précédent, que le \mathbf{Z} -rang du groupe $E(F)$, où $F = L[\sqrt{z} \mid z \in \mathbf{Z}[T_1, \dots, T_n]]$ est infini.

Dans cette note on établit, sans utiliser les résultats de [1], l'énoncé plus général suivant:

Théorème

Soient K une extension de \mathbf{Q} de type fini et E une courbe elliptique sur K . Alors le \mathbf{Z} -rang du groupe $E(F)$, où $F = k[\sqrt{z} \mid z \in K]$, est infini.

2. Lemmes Auxiliaires

Soit

$$Y^2 = X^3 + aX + b$$

où $a, b \in K$, un modèle de la courbe elliptique E sur K . Soient e_1, e_2, e_3 les racines du polynôme $f(X) = X^3 + aX + b$. On note $\Omega = K(e_1, e_2, e_3)$. Supposons aussi que $K = \mathbf{Q}(T_1, \dots, T_n, y)$, où $n \geq 0$, T_1, \dots, T_n sont des indéterminées sur \mathbf{Q} et y est algébrique sur $\mathbf{Q}(T_1, \dots, T_n)$.

Lemme 1

Il existe un ensemble fini $\Sigma \subseteq \Omega$ tel que pour tout $P = (x, y) \in E(\Omega)$ on a

$$x - e_i = \alpha_i z^{2i} \quad i = 1, 2, 3$$

où $\alpha_i \in \Sigma$ et $z \in \Omega$.

Démonstration

Tout élément premier p de $\mathbf{Z}[T_1, \dots, T_n]$ définit une valuation discrète v_p de K . Si on note A_p l'anneau de valuation associé à v_p on a $A_p \cap \mathbf{Q} = \mathbf{Q}$. Soit W l'ensemble des valuations de Ω qui prolongent les valuations v_p . L'anneau

$$A = \{x \in \Omega \mid v_w(x) \geq 0 \text{ pour tout } w \in W\}$$

est la fermeture intégrale de $\mathbf{Z}[T_1, \dots, T_n]$ dans Ω . Il en résulte que A est un anneau noethérien et un $\mathbf{Z}[T_1, \dots, T_n]$ -module de type fini.

On peut supposer, sans restreindre la généralité, que $e_1, e_2, e_3 \in A$. Soient

$$S = \{w_1, w_2, \dots, w_r\}$$

l'ensemble des valuations de W telles que

$w_1((e_1 - e_2)(e_1 - e_3)(e_2 - e_3)) > 0$ et u_1, \dots, u_k les paramètres locaux correspondants.

Alors le groupe des unités D^* de l'anneau $D = A \left[\frac{1}{u_1}, \dots, \frac{1}{u_k} \right]$ est de type fini ([2],

chap.2, corol. 7.5 ou [3], §1). Si $w \notin S$ on a un des cas suivants:

- i) $w(x - e_j) = 0$ $j = 1, 2, 3$
- ii) $w(x - e_{i_1}) > 0$, $w(x - e_{i_2}) = 0$, $w(x - e_{i_3}) = 0$, où i_1, i_2, i_3 est une permutation des 1, 2, 3.
- iii) $w(x - e_1) < 0$, $w(x - e_2) < 0$, $w(x - e_3) < 0$.

Il en résulte

$$w \left(\frac{x - e_j}{x - e_1} \right) = 2 \alpha_j \quad j = 2, 3$$

Soient

$$z_j = \prod_{w \notin S} u_w^{-\alpha_j} \quad j = 2, 3$$

où u_w est un paramètre local de w . Alors

$$z^2 (x - e_j) (x - e_1)^{-1} \in D^* \quad j = 2, 3.$$

Si $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$ engendrent D^* on a

$$x - e_j = (x - e_1) z_1^{-2} \varepsilon_1^{\alpha_1} \dots \varepsilon_r^{\alpha_r} \quad \text{où } \alpha_k \in \mathbf{Z}, \quad k = 1, 2, \dots, r.$$

On déduit donc que

$$x - e_1 = \varepsilon_1^{\beta_1} \dots \varepsilon_r^{\beta_r} z^2 \quad 0 \leq \beta_k \leq 1, \quad k = 1, 2, \dots, r.$$

De même, on a des relations analogues pour $x - e_2$ et $x - e_3$.

Lemme 2

L'ensemble des points de torsion de E , de degré borné, est fini.

Démonstration

Supposons d'abord que K est un corps de nombres. Soit N un entier positif. Considérons un point de torsion P de E sur une extension L de K de degré $[L:K] \leq N$. Si \hat{h} est l'hauteur des Neron-Tate sur E , on $\hat{h}(P) = 0$ ([4], chap. VIII, théorème 9.3). Aussi, se h_f est l'hauteur sur E associée à une fonction paire $f \in K(E)$, il existe un constant $C > 0$ telle que $|\text{deg } \hat{h} - h_f| \leq C$ ([4], chap. VIII, théorème 9.3). On a donc $h_f(P) \leq C$. Alors le théorème de Northcott ([2], chap. 3, théorème 2.6 ou [5] §2.4) entraîne que l'ensemble

$$\{P \in E(\bar{K}) / h_f(P) \leq C, [K(P):K] \leq N\}$$

est fini.

Supposons maintenant que K n'est pas un corps de nombres. Alors il existe une spécialisation non dégénérée \tilde{E} de E sur un corps de nombres K' telle que l'homomorphisme induit $\sigma: E(K) \rightarrow \tilde{E}(K')$ est un extension L de K de degré $\leq N$. Le monomorphisme σ se prolonge sur L . Donc l'image injection ([2], ch. 9 Corol. 9.3.). Soit P un point de torsion de E sur une \tilde{P} de P est un point de torsion de \tilde{E} sur une extension L de K de degré $\leq N$. Comme il n'existe qu'un nombre fini de nombre fini de points de torsion de E de degré borné on a le résultat.

3. Démonstration du Théorème

On peut que pour tout $\sigma, \tau \in \Sigma$ l'élément $\sigma^{-1} \tau$ n'est pas un carré. Choisissons $\alpha \in \Omega$ tel que

- (i) $\sigma^{-1} \alpha$ n'est pas un carré
- (ii) $x = e_1 + \alpha \in K$, où $\sigma \in \Sigma$.

D'après le lemme 2, on peut aussi avoir que le point $P = (x, \sqrt{f(x)})$ de E n'est pas un point de torsion.

Si $\sqrt{f(x)} \in \Omega$, le lemme 1 et (ii) entraînent que $\alpha = x - e_1 = \sigma_1 z^2$, d'où $\sigma^{-1} \alpha = z^2$, ce qui n'est pas vrai, d'après

- (ii). Donc $\sqrt{f(x)} \notin \Omega$ et P est d'ordre infini et rationnel sur l'extension quadratique $L = K(\sqrt{f(x)})$. Suivant cette méthode on construit une suite de points de E $P_i = (x_i, \sqrt{f(x_i)})$, $i = 1, 2, \dots$ tel que P_i est d'ordre infini et rationnel sur l'extension quadratique de K , $L_i = K(\sqrt{f(x_i)})$.

Solent p un élément premier de $\mathbf{Z}[T_1, \dots, T_n]$, v_p la valuation associée à p et w_p une extension de v_p dans K . Si w_p est non-ramifié au dessus de v_p et l'élément

$$\left(\frac{1}{p} - e_1\right) \sigma^{-1} \tau^{-1} \rho \quad \text{où } \sigma, \tau, \rho \in \Sigma$$

est un carré on a une contradiction.

Comme les v_p qui sont ramifiées dans K sont en nombre fini, on a la sous-suite

$(P_{n(i)})$ de (P_i) où $P_{n(i)} = \left(\frac{1}{p_i} \frac{\sqrt{c_1}}{p_i}\right)$, p_i est un premier de $\mathbf{Z}[T_1, \dots, T_n]$ tel que v_p est non-ramifiée dans K et $c_1 = 1 + ap_i^2 + bp_i^3$.

Supposons qu'ils existent $m_1, \dots, m_r \in \mathbf{Z}$ tels que $m_1 P_{n(1)} + \dots + m_r P_{n(r)} = 0$ et $m_r \neq 0$.

Comme $P_{n(i)}$ est rationnel sur $K_i = K\left(\sqrt{\frac{c_1}{p_i}}\right)$ on a que $m_r P_{n(r)} \in E(K_1 \dots K_{r-1})$.

D'autre part $P_{n(r)} \in E(K_r)$. Il en résulte que $m_r P_{n(r)}$ est rationnel sur $K_1 \dots K_{r-1} \cap K_r = K$.

La courbe elliptique E a bonne réduction presque pour tout p_i ([2], chap. 6 lemme 2.1). On peut donc exclure de la suite $(P_{n(i)})$ les points qui correspondent à des "mauvais" premiers.

Soient $m_r P_{n(r)} = P$ et M_r l'extension de K engendré par les coefficients des points de E d'ordre m_r . Alors si w'_p est une extension sur M_r de la valuation de $\mathbf{Q}(T_1, \dots, T_n)$

associée à p_r , l'extension $M_r\left(\frac{1}{m_r} P\right) / M_r$ est non ramifiée en w'_p ([2], chap. 6, lemme

2.2). Aussi, on a que l'extension M_r/K est non ramifiée en p_r ([4], chap. VII, théorème

7.1). Donc $M_r\left(\frac{1}{m_r} P\right) / \mathbf{Q}(T_1, \dots, T_n)$ est non ramifiée en p_r . Comme $K_r \subseteq M_r\left(\frac{1}{m_r} P\right)$ il

résulte que $K_r/\mathbf{Q}(T_1, \dots, T_n)$ est non ramifié en p_r , ce qui n'est pas le cas. Donc les points $P_{n(1)}, \dots, P_{n(r)}$ sont \mathbf{Z} -linéairement indépendants.

Remerciements

Je tiens à remercier le professeur Daniel Bertrand pour les discussions utiles que j'ai eu avec lui pendant la préparation de cette note.

References

- [1] GERHARD FREY and MOSHE JARDEN, Approximation theory and the rank of abelian varieties over large algebraic fields, Proc. London Math. Soc. (3) 28 (1974) 112-128.
- [2] SERGE LANG, Fundamentals of Diophantine Geometry, Springer-Verlag 1983.
- [3] PIERRE SAMUEL, 'A propos du théorème des unités, Bull. Sc. Math. 90 (1966) 89-96.
- [4] JOSEPH SILVERMAN, The arithmetic of Elliptic curves, Springer-Verlag 1986.
- [5] JEAN-PIERRE SERRE, Lectures on the Mordell-Weil Theorem, Vieweg 1989.

Université de Thessalonique
Département de Mathématique
540 06 Thessalonique, Grèce