

# Conjecture de Zagier pour l'extension des scalaires d'une courbe elliptique (suite)

François Brunault (ÉNS Lyon)  
francois.brunault@ens-lyon.fr

21 juin 2011

On s'intéresse à la conjecture de Zagier pour  $L(E/F, 2)$  où  $E$  est une courbe elliptique définie sur  $\mathbf{Q}$  et  $F$  est un corps de nombres. Soit  $\Sigma$  l'ensemble des plongements de  $F$  dans  $\mathbf{C}$ . On note

$$\begin{aligned}\Sigma_{\mathbf{R}} &= \{\sigma_1, \dots, \sigma_{r_1}\} \\ \Sigma_{\mathbf{C}} &= \{\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \dots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}\} \\ [F : \mathbf{Q}] &= n = r_1 + 2r_2.\end{aligned}$$

Chaque  $\sigma \in \Sigma$  induit  $\mathbf{Z}[E(\overline{\mathbf{Q}})]^{\text{Gal}(\overline{\mathbf{Q}}/F)} \hookrightarrow \mathbf{Z}[E(\mathbf{C})]$ .

On dispose des fonctions dilogarithmes de Bloch  $D_E : E(\mathbf{C}) \rightarrow \mathbf{R}$  et  $J_E : E(\mathbf{C}) \rightarrow \mathbf{R}$ . On a  $D_E(\overline{P}) = D_E(P)$  et  $J_E(\overline{P}) = -J_E(P)$  pour tout  $P \in E(\mathbf{C})$ .

On étend  $D_E$  et  $J_E$  par linéarité à  $\mathbf{Z}[E(\mathbf{C})]$ .

## Définition

On définit  $\vec{D}_E : \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\text{Gal}(\overline{\mathbf{Q}}/F)} \rightarrow \mathbf{R}^n$  par

$$\vec{D}_E = \begin{pmatrix} D_E \circ \sigma_1 \\ \vdots \\ D_E \circ \sigma_{r_1+r_2} \\ J_E \circ \sigma_{r_1+1} \\ \vdots \\ J_E \circ \sigma_{r_1+r_2} \end{pmatrix}$$

## Conjecture

Il existe  $\ell_1, \dots, \ell_n \in \mathcal{A}_{E/F}$  tels que

$$L(E/F, 2) \sim_{\mathbf{Q}^*} \frac{\pi^n}{\mathfrak{I}(\tau)^{r_2}} \det(\vec{D}_E(\ell_1), \dots, \vec{D}_E(\ell_n)).$$

Lorsque  $F/\mathbf{Q}$  n'est pas abélienne, on ne sait démontrer *aucun exemple* de cette conjecture.

On va vérifier numériquement cette conjecture sur un exemple.

*Idée* : soit  $K_m = \mathbf{Q}(E[m])$  avec  $m \geq 1$ .

L'extension  $K_m/\mathbf{Q}$  est galoisienne et en général non abélienne.

Comme  $E[m] \subset E(K_m)$ , on peut espérer utiliser les points de  $E[m]$  pour vérifier la conjecture pour  $L(E/K_m, 2)$ .

Pour  $m = 2$  on a génériquement  $\text{Gal}(\mathbf{Q}(E[2])/\mathbf{Q}) \cong \mathfrak{S}_3$ .

*Problème* :  $D_E$  et  $J_E$  sont impaires donc s'annulent sur  $E[2]$ ...

→ On choisit  $E$  telle que  $E(K_2)$  contient strictement  $E[2]$ .

## Exemple

$$E = X_1(11) : y^2 + y = x^3 - x^2$$

$E(\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$  engendré par  $P = (0, 0)$ .

On note  $(Q_1, Q_2)$  une base de  $E[2]$  telle que  $Q_1 \in E(\mathbf{R})$ .

$$\begin{array}{c}
 K = \mathbf{Q}(E[2]) \\
 \left. \begin{array}{c} \text{---} \\ \text{---} \\ \text{---} \end{array} \right\} \mathfrak{S}_3 \\
 \begin{array}{c} | \\ 2 \\ | \\ F = \mathbf{Q}(Q_1) \\ | \\ 3 \\ | \\ \mathbf{Q} \end{array}
 \end{array}$$

$E(F) \cong \mathbf{Z}/10\mathbf{Z}$  engendré par  $P + Q_1$ .

On vérifie que  $\mathbf{Z}[E(F)] \subset \mathcal{A}_{E/F}$  (cf. Magma).

Par imparité de  $\vec{D}_E$ , il suffit de considérer les diviseurs à support dans  $\{P, 2P, P + Q_1, 2P + Q_1\}$ . De plus  $2\vec{D}_E(2P) = 3\vec{D}_E(P)$ . On prend donc

$$\ell_1 = [P] \quad \ell_2 = [P + Q_1] \quad \ell_3 = [2P + Q_1]$$

$$R := \begin{vmatrix} D_E(P) & D_E(P + Q_1) & D_E(2P + Q_1) \\ D_E(P) & D_E(P + Q_2) & D_E(2P + Q_2) \\ 0 & J_E(P + Q_2) & J_E(2P + Q_2) \end{vmatrix}$$

Numériquement (à 30 décimales)  $L(E/F, 2) \stackrel{?}{=} -\frac{(10\pi)^3}{11^4 \mathfrak{J}(\tau)} \cdot R$ .

## Remarques

1. Comme  $R$  est divisible par  $D_E(P)$  et grâce à la formule  $L(E, 2) = \frac{10\pi}{11} D_E(P)$ , on obtient une expression conjecturale pour  $L(E \otimes \rho, 2)$ , où  $\rho$  est l'unique représentation irréductible de dimension 2 de  $\text{Gal}(K/\mathbf{Q})$ .
2. Il serait intéressant de vérifier numériquement la conjecture sur d'autres exemples (par exemple pour une extension non résoluble de  $\mathbf{Q}$ , ou pour des familles de courbes elliptiques).
3. Un obstacle est le temps de calcul de  $L(E/F, s)$  qui devient rapidement prohibitif lorsque le discriminant de  $F$  augmente.

*Idée* : si  $F/\mathbf{Q}$  est finie galoisienne et  $G = \text{Gal}(F/\mathbf{Q})$ , alors

$$V := \mathbf{Z}[E(F)] \cap \mathcal{A}_{E/F}$$

est un  $\mathbf{Z}[G]$ -module. Soit  $\rho$  une représentation irréductible de  $G$  qui apparaît dans  $V \otimes \overline{\mathbf{Q}}$ . On note  $V_\rho$  la composante  $\rho$ -isotypique de  $V \otimes \overline{\mathbf{Q}}$ . Si  $\vec{D}_E(V_\rho) \neq 0$  alors on peut espérer exprimer  $L(E \otimes \bar{\rho}, 2)$  en termes d'un déterminant de  $\vec{D}_E(V_\rho)$ .

Soit  $E$  une courbe elliptique sur  $\mathbf{Q}$ . On rappelle que  $D_E$  vérifie une relation de *m-distribution* pour tout  $m \in \mathbf{Z} - \{0\}$  :

$$D_E(mP) = m \sum_{Q \in E[m]} D_E(P + Q) \quad (P \in E(\mathbf{C})).$$

Pour  $f, g \in \mathbf{C}(E)^\times$ , posons

$$\operatorname{div}(f) = \sum_i m_i [P_i]$$

$$\operatorname{div}(g) = \sum_j n_j [Q_j]$$

$$\beta(f, g) := \sum_{i,j} m_i n_j [P_i - Q_j] \in \mathbf{Z}[E(\mathbf{C})].$$

L'application  $(f, g) \mapsto \beta(f, g)$  est bilinéaire.

## Théorème (Bloch)

Pour tout  $f \in \mathbf{C}(E) - \{0, 1\}$ , on a

$$D_E(\beta(f, 1 - f)) = 0$$

## Remarques

1. Le théorème de Bloch et le théorème de Matsumoto entraînent que  $D_E \circ \beta$  se factorise par  $K_2(\mathbf{C}(E))$ . Le morphisme  $K_2(\mathbf{C}(E)) \rightarrow \mathbf{R}$  ainsi défini est l'*application régulateur* associée à  $E$ .
2. L'application  $\beta$  est compatible à l'action de Galois. En particulier si  $f \in \mathbf{Q}(E) - \{0, 1\}$  alors  $\beta(f, 1 - f) \in \mathbf{Z}[E(\overline{\mathbf{Q}})]^{\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})}$ .

Le théorème de Bloch permet de montrer des relations de dépendance linéaire entre les valeurs de  $D_E$  en des points algébriques de  $E$ .

Zagier et Gangl ont conjecturé que le noyau de  $D_E : \mathcal{A}_{E/\mathbf{Q}} \rightarrow \mathbf{R}$  est engendré par :

- ▶ les relations de  $m$ -distribution pour  $m \in \{-1, 2\}$  ;
- ▶ les relations de Bloch  $\beta(f, 1 - f)$  pour  $f \in \mathbf{Q}(E) - \{0, 1\}$ .

### Remarque

En notant  $\mathcal{C}_{E/\mathbf{Q}}$  le groupe engendré par ces relations, la conjecture de Zagier prédit que  $\mathcal{A}_{E/\mathbf{Q}}/\mathcal{C}_{E/\mathbf{Q}}$  est de rang 1.

On appelle *relation exotique* une relation de dépendance linéaire entre valeurs de  $D_E$  qui ne provient pas des relations de distribution.

### Exemple

$$E : y^2 + y = x^3 - x^2 \quad P = (0, 0) \quad 2P = (1, -1)$$

On prend  $f = -y$ . Alors

$$\operatorname{div}(f) = \operatorname{div}(y) = 2[P] + [-2P] - 3[0]$$

$$\operatorname{div}(1 - f) = \operatorname{div}(y + 1) = 2[-P] + [2P] - 3[0]$$

$$\beta(f, 1 - f) = -11[P] + 4[2P] + 4[-P] - 6[-2P] + 9[0]$$

$$\Rightarrow -15D_E(P) + 10D_E(2P) = 0$$

$$\Rightarrow 3D_E(P) = 2D_E(2P).$$

Il est facile de détecter numériquement des relations  $D_E(\ell) \stackrel{?}{=} 0$ , au moyen de l'algorithme LLL implémenté dans Pari/GP.

→ Comment démontrer ces relations ?

**Idée de Goncharov et Levin** : on se donne trois droites concourantes  $(d_i)_{i \in \mathbf{Z}/3\mathbf{Z}}$  dans  $\mathbf{P}^2(\mathbf{C})$  et on pose

$$\ell_i := d_i \cap E \in \mathbf{Z}[E(\mathbf{C})] \quad (i \in \mathbf{Z}/3\mathbf{Z}).$$

D'après le théorème de Bézout,  $\ell_i$  est un diviseur de degré 3.

### Proposition

On a  $\sum_{i \in \mathbf{Z}/3\mathbf{Z}} D_E(\beta(\ell_i, \ell_{i+1})) = 0$ .

## Proposition

On a  $\sum_{i \in \mathbb{Z}/3\mathbb{Z}} D_E(\beta(\ell_i, \ell_{i+1})) = 0$ .

## Démonstration.

On peut choisir des équations  $f_i = 0$  des droites  $d_i$  de telle sorte que  $f_3 = f_1 + f_2$ . On pose  $f = \frac{f_1}{f_3}$  et donc  $1 - f = \frac{f_2}{f_3}$ . Grâce à la relation de Bloch  $D_E$  s'annule sur le diviseur

$$\beta\left(\frac{f_1}{f_3}, \frac{f_2}{f_3}\right) = \beta(f_1, f_2) + \beta(f_2, f_3) + \beta(f_3, f_1)$$

par bilinéarité de  $\beta$ . On termine le calcul en utilisant le fait que  $\operatorname{div}(f_i) = \ell_i - 3[0]$ . □

## Remarque

On peut montrer que si les  $d_i$  sont concourantes en un point de  $E$  alors la relation précédente est triviale i.e. est conséquence de l'imparité de  $D_E$ . On cherche donc des droites concourantes en un point situé hors de  $E$ .

On en déduit une méthode pour trouver des relations exotiques.

1. On se donne un ensemble fini de points  $S \subset E(\overline{\mathbf{Q}})$ .
2. On calcule l'ensemble  $\mathcal{D}$  des droites  $d$  telles que  $d \cap E \subset S$ .
3. On calcule l'ensemble  $\mathcal{T}$  des triplets de droites de  $\mathcal{D}$  concourantes en un point non situé sur  $E$ .
4. Pour chaque  $(d_1, d_2, d_3) \in \mathcal{T}$ , on calcule  $\sum_i \beta(l_i, l_{i+1})$ .

## Résultats numériques

- ▶ Pour les courbes elliptiques de conducteur  $\leq 210$ , on trouve numériquement 27 relations exotiques entre valeurs de  $D_E$  en des points de torsion rationnels de  $E$ .
- ▶ La méthode des droites concourantes utilisée avec  $S = E(\mathbf{Q})_{\text{tors}}$  permet de montrer 17 de ces relations.
- ▶ Dans chacun des 10 cas restants, on peut trouver une isogénie  $\varphi : E' \rightarrow E$  telle que la méthode des droites concourantes appliquée à  $(E', \varphi^{-1}(S))$  permette de montrer la relation voulue.
- ▶ Si l'on excepte les courbes elliptiques d'invariant  $j = 0$ , il ne semble pas y avoir d'autre relation exotique entre valeurs de  $D_E$  aux points de torsion rationnels de  $E$ .

Une autre application de la méthode des droites concourantes :

Conjecture de Zagier explicite pour

$$E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$$

$$(*) \quad L(E, 2) \stackrel{?}{=} \frac{4\pi}{55} (2D_E(2P) - D_E(P)) \quad P = (5, 5).$$

- ▶ La méthode de Beilinson ne marche pas pour  $X_0(11)$ .
- ▶ On utilise l'isogénie  $\varphi : X_1(11) = E' \rightarrow E$  pour traduire (\*) en une identité sur  $E'$  (relation de  $\varphi$ -distribution).
- ▶ On sait que  $L(E, 2)$  est proportionnel à une valeur de  $D_{E'}$ .
- ▶ On est ramenés à montrer une relation de dépendance linéaire entre valeurs de  $D_{E'}$ , ce qui peut se faire par la méthode des droites concourantes avec  $S = \varphi^{-1}(E(\mathbf{Q})) \subset E'(\overline{\mathbf{Q}})$ .

En général, pour démontrer une relation de dépendance linéaire entre valeurs de  $D_E$  par la méthode des droites concourantes, on est obligés d'inclure dans  $S$  des points algébriques, ainsi que des points d'ordre infini.

- ▶ On ne sait pas borner a priori la taille de l'ensemble  $S$  ni le corps de nombres engendré par  $S$  (ce problème est essentiellement équivalent à savoir calculer dans  $K_2(E)$ ).
- ▶ Autre question ouverte : peut-on généraliser la méthode des droites concourantes aux courbes de genre  $\geq 2$  ?