La conjecture de Birch et Swinnerton-Dyer

Exposé au séminaire des doctorants en théorie des nombres de Chevaleret

Nicolas Ratazzi et Marusia Rebolledo

20 Juin 2002

Résumé : L'objectif de cet exposé est de parvenir à énoncer la conjecture de Birch et Swinnerton-Dyer sur $\mathbb{Q}$ et à comprendre les termes qui interviennent dedans.

Table des matières

Soit K un corps. Dans toute la suite, on dira que V est une *variété sur* K si V est un K-schéma irréductible géométriquement réduit de type fini. Si L/K est une extension et V une variété sur K, alors, la notation V_L dénote le produit fibré $V \times_{\mathrm{Spec}\ K} \mathrm{Spec}\ L$, et $V(L)$ dénote $\mathrm{Mor}_K(\mathrm{Spec}\ L, V)$. Enfin on appelle *variété abélienne* sur K toute variété en groupes, propre sur K. Une telle variété est automatiquement un K-schéma en groupes, commutatif projectif lisse.

Sauf mention contraire, dans tout l'exposé, A/K sera une variété abélienne de dimension g sur un corps de nombres.

1 Énoncé de BSD1

Pour pouvoir énoncer la conjecture (BSD1), on a besoin de deux objets : la notion de fonction L associée à une variété abélienne et le théorème de Mordell-Weil concernant le groupe des points $A(K)$ d'une variété abélienne A/K.

1.1 Fonction L

On ne fait ici que de brefs rappels concernant les fonctions L. Pour tout p premier, on choisit un premier $l \neq p$, on définit le module de Tate $T_l(A)$ et on tensorise par $\mathbb{Q}_l$ pour obtenir $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$ qui est un $\mathbb{Q}_l$-espace vectoriel de dimension $2g$. De plus on a une action naturelle, par la *représentation l-adique* ρ_l, de $\mathrm{Gal}(\overline{K}/K)$ sur ces objets :

$$\rho_l : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbb{Q}_l}\left(V_l(A)\right) \simeq \mathrm{GL}_{2g}(\mathbb{Q}_l).$$

Soit $\mathfrak{p}$ un premier de O_K, de groupe d'inertie $I_\mathfrak{p}$. On pose

$$Q_\mathfrak{p}(A,T) = \det\left(\mathrm{Id}_{2g} - \left(\rho_l(\mathrm{Frob}_\mathfrak{p}) \mid V_l(A)^{I_\mathfrak{p}}\right) T\right).$$

Notons que ce polynôme est *a priori* à coefficients dans $\mathbb{Q}_l$. En fait (c'est un théorème difficile) le polynôme $Q_\mathfrak{p}(A,T)$ est à coefficients dans $\mathbb{Z}$ et est indépendant de $l \neq p$. On peut maintenant définir la *fonction L* associée à la variété abélienne A :

$$L(A,s) = \prod_\mathfrak{p} \frac{1}{Q_\mathfrak{p}\left(A, \left(N_{\mathbb{Q}}^K \mathfrak{p}\right)^{-s}\right)}.$$

Quand la variété à bonne réduction en $\mathfrak{p}$, l'action de l'inertie est triviale sur $V_l(A)$, et le polynôme $Q_\mathfrak{p}(A,T)$ est de degré $2g$. Dans ce cas, ses racines complexes $\alpha_{i,\mathfrak{p}}$ sont des nombres de Weil, *i.e.*, de valeur absolue $\left(N_{\mathbb{Q}}^K \mathfrak{p}\right)^{\frac{1}{2}}$.

La fonction $L(A,\cdot)$ est définie pour $\mathrm{Re}(s) > \frac{3}{2}$. Conjecturalement elle se prolonge en une fonction entière (holomorphe sur tout le plan complexe). En particulier, elle est conjecturalement définie en $s = 1$. On écrit

$$L(A,1) \underset{s \mapsto 1}{\sim} C\,(s-1)^{r_{an}},$$

et on dit que r_{an} est *le rang analytique*. La conjecture (BSD1) explique qui est r_{an}, et la conjecture (BSD2) raconte ce que vaut la constante C.

1.2 Théorème de Mordell-Weil

Théorème 1.1 (Mordell-Weil) *Soient K un corps de nombres et A/K une variété abélienne. Le groupe $A(K)$ est de type fini.*

Le groupe $A(K)$ étant abélien, il peut s'écrire sous la forme

$$A(K) = A(K)_{\text{tors}} \times \mathbb{Z}^{r_{mw}}.$$

Le théorème précédent nous assure que l'entier r_{mw}, appellé *le rang de Mordell-Weil* de A/K, est fini. On peut maintenant énoncer la conjecture 1 :

Conjecture 1.1 (BSD1) *On a l'égalité $r_{an} = r_{mw}$.*

On va tout de suite énoncer la conjecture (BSD2) puis on définira les symboles qui apparaissent dedans. Pour simplifier, on énonce la conjecture dans le cas d'une variété abélienne $A/\mathbb{Q}$, toutefois, quand travailler avec un corps de nombres K ou avec $\mathbb{Q}$ ne change rien, on définira les termes pour une variété abélienne A/K.

Conjecture 1.2 (BSD2) *On a :*

$$\lim_{s \mapsto 1} \frac{L(A,s)}{(s-1)^{r_{mw}}} = \Omega_A \prod_p c_p \frac{\left|\text{Ш}(A/\mathbb{Q})\right| \left|\text{Reg}(A/\mathbb{Q})\right|}{\left|A(\mathbb{Q})_{\text{tors}}\right| \left|\widehat{A}(\mathbb{Q})_{\text{tors}}\right|}.$$

Si on voulait énoncer la conjecture sur un corps de nombres K, il faudrait remplacer

$\prod_p$	par	$\prod_{\mathfrak{p}}$,
Ш $(A/\mathbb{Q})$	par	Ш(A/K), (groupe de Shafarevitch-Tate),
$\text{Reg}(A/\mathbb{Q})$	par	$\text{Reg}(A/K)$, (régulateur de A),
$A(\mathbb{Q})_{\text{tors}}$	par	$A(K)_{\text{tors}}$,
$\widehat{A}(\mathbb{Q})_{\text{tors}}$	par	$\widehat{A}(K)_{\text{tors}}$.

Toutefois il faudrait également remplacer la période réelle Ω_A par le produit de toutes les périodes réelles et complexes correspondant aux plongements de K dans $\mathbb{C}$ et rajouter un petit facteur supplémentaire faisant intervenir le discriminant du corps $K/\mathbb{Q}$. On va maintenant expliciter les divers objets introduits dans l'énoncé.

2 Groupe de Shafarevitch-Tate

C'est la partie de Marusia. Voir par exemple le très joli exposé de Tate, *Galois cohomology. Arithmetic algebraic geometry (Park City, UT, 1999).*

3 Variété duale, régulateur, facteurs c_p et période Ω_A

3.1 Variété duale $\widehat{A}/K$

Soit A/K une variété abélienne. On note Pic(A) le groupe de Picard de A, *i.e.*, le groupe des diviseurs de A à équivalence linéaire près, ou encore, le groupe des faisceaux inversibles à isomorphismes près. On note t_a l'opérateur de translation par a sur A. Si on se fixe un faisceau inversible $\mathcal{L}$, alors l'application

$$\varphi_{\mathcal{L}} \ : \ A(K) \to \mathrm{Pic}(A), \qquad a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

est un morphisme de groupe (ceci n'est pas trivial, c'est le théorème du carré qui le dit).

Définition 3.1 Soit A/K une variété abélienne. On définit $\mathrm{Pic}^0(A)$ comme étant le sous-groupe de $\mathrm{Pic}(A)$ constitué des classes de diviseurs invariants par translations :

$$\mathrm{Pic}^0(A) = \left\{ \mathcal{L} \in \mathrm{Pic}(A) \ / \ \forall a \in A(\overline{K}) \ \ t_a^*\mathcal{L} \simeq \mathcal{L} \right\}.$$

Remarque 3.1 Si A est une courbe, on peut vérifier que $\mathrm{Pic}^0(A)$ est le groupe des diviseurs de degré 0. Dans le cas général ce n'est plus vrai, il s'agit de ce que l'on appelle *le groupe des diviseurs algébriquement équivalents à zéro.*

Définition-Théorème Il existe une variété abélienne sur K, appelée *variété abélienne duale de* A/K, notée $\widehat{A}$, telle que,

$$\text{pour toute extension de corps } L/K, \quad \widehat{A}(L) = \mathrm{Pic}^0(A_L).$$

Rigoureusement on a la définition et le théorème suivant :

Définition 3.2 Soit A/K une variété abélienne. Une variété abélienne $\widehat{A}$ est *la variété duale* de A, s'il existe un faisceau inversible $\mathcal{P}$ (le *fibré de Poincaré*) sur $A \times \widehat{A}$ vérifiant :

(i) $\mathcal{P}|_{\{0\}\times\widehat{A}}$ est trivial et pour tout $a \in \widehat{A}$, le faisceau $\mathcal{P}|_{A\times\{a\}}$ appartient à $\mathrm{Pic}^0(A_{k(a)})$.

(ii) Pour tout K-schéma T, et pour tout faisceau inversible $\mathcal{L}$ sur $A \times T$ vérifiant la propriété (i), il existe un unique morphisme

$$f \ : \ T \to \widehat{A} \ \text{ tel que } \quad (1 \times f)^* \, \mathcal{P} \simeq \mathcal{L}.$$

Théorème 3.1 *La variété abélienne duale, munie du faisceau de Poincaré, existe et est unique à unique isomorphisme près. De plus, le fibré de Poincaré est symétrique.*

Remarque 3.2 Dans le cas d'une variété abélienne principalement polarisée (c'est à dire telle que $A \simeq \widehat{A}$), (par exemple, toute courbe elliptique ou mieux toute Jacobienne est principalement polarisée), on a une description explicite du fibré de Poincaré. Je vais ici me limiter au cas des courbes elliptiques mais la description vaut de manière générale. On note $s \ : \ E \times E \to E$ l'addition, et p_1 et p_2 les deux projections. En notant Δ_{-1} l'anti-diagonale (la seconde bissectrice) de $E \times E$ et en terme de diviseurs, on a

$$\mathcal{P} = \Delta_{-1} - \{0\} \times E - E \times \{0\}.$$

3.2 Régulateur $\mathrm{Reg}(A/K)$

Il y a deux façons de définir le régulateur :

• étant donné un diviseur ample et symétrique D, on construit la hauteur canonique (également appelée hauteur de Néron-Tate) $\widehat{h}_D$ associée sur $A(\overline{K})$. Elle s'étend en une forme quadratique définie positive sur $A(K)\otimes\mathbb{R}$. On note $\langle\cdot,\cdot\rangle_D$ la forme bilinéaire associée et, si $\{P_1,\dots,P_r\}$ est une base du goupe de Mordell-Weil, on pose

$$\mathrm{Reg}_D(A/K) = \Big|\det\left(\langle P_i,P_j\rangle_{1\leq i,j\leq r}\right)\Big|.$$

Le régulateur est juste le volume d'une maille fondamentale du réseau $A(K)/A(K)_{\mathrm{tors}}$ plongé dans l'espace euclidien $A(K)\otimes\mathbb{R}$ avec la structure euclidienne définie par $\widehat{h}_D$.

Malheureusement, ce régulateur dépend de D (au moins quand D ne définit pas une polarisation principale). On va donc le renormaliser de sorte à enlever cette dépendance. Le diviseur D définit une application φ_D de $A(K)$ dans $\mathrm{Pic}^0(A)$: c'est l'application définie au paragraphe précédent, on vérifie facilement qu'elle est à valeur dans $\mathrm{Pic}^0(A)$. De plus D étant ample, cette application donne une isogénie de A dans $\widehat{A}$ (c'est "bien connu" mais non-trivial). On peut donc poser :

$$\mathrm{Reg}(A/K) = \frac{1}{[\widehat{A}(K):\varphi_D(A(K))]}\mathrm{Reg}_D(A/K).$$

La seconde façon de définir le régulateur nous prouvera bien que ceci est indépendant du choix de D.

• Le seconde définition consiste à définir le régulateur en utilisant le fibré de Poincaré $\mathcal{P}$: on pose

$$\mathrm{Reg}(A/K) = \left|\det\left(\widehat{h}_{\mathcal{P}}\left(P_i,\widehat{P}_j\right)_{1\leq i,j\leq r}\right)\right|,$$

où $\widehat{h}_{\mathcal{P}}$ dénote la hauteur canonique sur $(A\times\widehat{A})(\overline{K})$ relativement au fibré en droites $\mathcal{P}$ et où $\{P_1,\dots,P_r\}$ est une base de $A(K)$ et $\{\widehat{P}_1,\dots,\widehat{P}_r\}$ une base de $\widehat{A}(K)$.

Proposition 3.1 *Les deux définitions du régulateur $Reg(A/K)$ coïncident. De plus si A est principalement polarisée, alors* $\mathrm{Reg}_D(A/K) = \mathrm{Reg}(A/K)$.

Démonstration : La première assertion résulte essentiellement du fait que

$$\widehat{h}_D(P) = \widehat{h}_{\mathcal{P}}(P,\varphi_D(P)).$$

Cette dernière formule découle simplement des multiples propriétés vérifiées par la hauteur de Néron-Tate (quadraticité par rapport aux points, additivité et fonctorialité par rapport aux diviseurs), et de la définition du fibré en droites $\mathcal{P}$.
La seconde assertion est évidente car dans ce cas $[\widehat{A}(K):\varphi_D(A(K))] = 1$. □

3.3 Facteurs $c_\mathfrak{p}$

Ils sont faciles à définir : soient p un nombre premier et $\mathfrak{p}$ un premier de K au-dessus de p. On pose également A/K une variété abélienne de modèle de Néron $\mathcal{A}/O_K$ et on note $\mathcal{A}^0$ la composante connexe de l'identité de $\mathcal{A}$. On note $k_\mathfrak{p}$ le corps résiduel en $\mathfrak{p}$, et $\mathcal{A}_\mathfrak{p} = \mathcal{A} \times_{O_K} k_\mathfrak{p}$ la réduction modulo $\mathfrak{p}$ du modèle de Néron. On définit alors $c_\mathfrak{p}$ par

$$c_\mathfrak{p} = \left| \mathcal{A}_\mathfrak{p}(k_\mathfrak{p}) / \mathcal{A}^0_\mathfrak{p}(k_\mathfrak{p}) \right|.$$

Notons que ce nombre est bien presque tout le temps égal à 1 car il vaut 1 quand A a bonne réduction (*i.e.* quand $\mathcal{A}_\mathfrak{p}/k_\mathfrak{p}$ est une variété abélienne). Le produit $\prod c_\mathfrak{p}$ est donc bien défini.

3.4 Période réelle Ω_A

On considère comme précédemment $A/\mathbb{Q}$ de dimension g, de modèle de Néron $\mathcal{A}/\mathbb{Z}$, et on note $A_\sigma = A \times_\mathbb{Q} \mathbb{R}$. Le schéma $\mathcal{A}/\mathbb{Z}$ est lisse de dimension relative g, donc le faisceau des différientielles relatives $\Omega^1_{\mathcal{A}/\mathbb{Z}}$ est localement libre de rang g. On pose

$$\omega_{\mathcal{A}/\mathbb{Z}} = \bigwedge_{i=1}^{g} \Omega^1_{\mathcal{A}/\mathbb{Z}} \text{ le fibré (faisceau, classe) canonique.}$$

C'est un faisceau inversible *(i.e.* localement libre de rang 1). On considère alors η une g-forme différentielle (dite de Néron) qui engendre $\omega_{\mathcal{A}/\mathbb{Z}}$. Dans une trivialisation affine on peut écrire $\eta = f \mathrm{d}x_1 \wedge \ldots \wedge \mathrm{d}x_g$, avec les bonnes conditions de recollement. Dans le cas particulier d'une courbe elliptique $E/\mathbb{Q}$ donnée par une équation de Weierstrass minimale $E : y^2 + a_1xy + a_3y = x^3 + a_4x + a_6$, on peut prendre $\eta = \frac{dx}{2y+a_1x+a_3}$. On peut maintenant définir la période réelle

$$\Omega_A = \left| A_\sigma(\mathbb{R}) / A_\sigma(\mathbb{R})^0 \right| \cdot \left| \int_{A_\sigma(\mathbb{R})} \eta \right|.$$

4 Résultats connus

On se restreint ici au cas (le seul ou presque pour lequel on sait dire quelque chose) où $A = E$ est une courbe elliptique sur $K = \mathbb{Q}$.

Théorème 4.1 (Shimura années 1960) *Si $E/\mathbb{Q}$ est modulaire, alors $L(E, \cdot)$ est entière.*

Théorème 4.2 (Coates-Wiles 1977) *Si E est à multiplication complexe, alors,*

$$r_{an} = 0 \Rightarrow r_{mw} = 0.$$

Théorème 4.3 (Rubin années 1980) *Si E est à multiplication complexe, alors,*

$$Ш(E/\mathbb{Q}) \text{ est fini.}$$

Théorème 4.4 (Gross-Zagier 1984) *Si E est modulaire, alors,*

$$r_{an} = 1 \Rightarrow r_{mw} \geq 1.$$

Théorème 4.5 (Kolyvagin 1987) *Si E est modulaire et $r_{an} \leq 1$ alors,*

$$Ш(E/\mathbb{Q}) \text{ est fini et } r_{an} = r_{mw}.$$

Théorème 4.6 (Kato 1993) *Si E est modulaire et $r_{an} = 0$, alors $r_{mw} = 0$.*

Remarque 4.1 Ce dernier résultat est déja contenu dans le théorème de Kolyvagin, mais Kato utilise une méthode complètement différente. Ici c'est donc plus la preuve que le résultat qui importe.

Théorème 4.7 (Wiles 1993 ; Taylor-Wiles 1994) *Toute courbe elliptique $E/\mathbb{Q}$ semi-stable est modulaire.*

Théorème 4.8 (Breuil-Conrad-Diamond-Taylor 2000) *Toute courbe elliptique $E/\mathbb{Q}$ est modulaire.*

Théorème 4.9 (Nekovar 2000) *Si $Ш(E/\mathbb{Q})$ est fini, alors,*

$$r_{an} = r_{mw} \bmod 2.$$