
LA CONJECTURE ÉQUIVARIANTE DE TAMAGAWA

par

Werner Bley

Résumé. — Nous donnons une brève introduction à la Conjecture Equivariante des Nombres de Tamagawa (ETNC), formulée par Burns et Flach, généralisant ainsi des travaux de Bloch, Fontaine, Kato et Perrin-Riou. Plutôt que de présenter ETNC en toute généralité nous nous arrêtons sur deux cas spéciaux, le cas du motif de Tate non-twisté et le cas du changement de base d'une courbe elliptique E définie sur \mathbb{Q} .

Dans la dernière partie du manuscrit, nous nous concentrons sur le cas d'une courbe elliptique. En supposant que E satisfait certaines hypothèses nous donnons (sans preuve) des reformulations très explicites de ETNC, ce qui nous permet alors de donner quelques évidences numériques et théoriques en faveur de cette conjecture.

Abstract. — We give a brief introduction to the Equivariant Tamagawa Number Conjecture (ETNC for short) which is formulated by Burns and Flach generalizing seminal work of Bloch, Fontaine, Kato and Perrin-Riou. Rather than discussing the ETNC in full generality we focus on two special cases, namely, the case of the untwisted Tate motive and the base change of an elliptic curve E which is defined over \mathbb{Q} .

In the last part of the manuscript we concentrate on the elliptic curve case. Assuming that E satisfies certain quite strong hypothesis we will describe (without proof) very explicit reformulations of the ETNC. Based on this we briefly discuss both numerical and theoretical evidence in favour of the conjecture.

1. Introduction

Cet article est l'élaboration de deux exposés donnés pour les Premières Journées Arithmétiques de Meknès (Fonctions L et Arithmétique) en Octobre 2010. J'ai essayé de conserver le caractère de ces exposés.

Le but de la première partie de mes exposés a été de donner une introduction informelle à la conjecture équivariante de Tamagawa (brièvement ETNC) accessible aussi pour le non-spécialiste. La ETNC est formulée par Burns et Flach dans [10] en grande généralité dans

Classification mathématique par sujets (2000). — 11R42, 11G40, 14G10 .

Mots clefs. — Equivariant Tamagawa Number conjecture, Birch-Swinnerton-Dyer conjecture.

Je remercie les organisateurs des Journées Arithmétiques de Meknès pour l'invitation et pour la possibilité d'exposer.

la langage des motifs en utilisant la théorie des foncteurs de déterminants. Pour échapper à l'énoncé général, qui est relativement abstrait, nous nous sommes concentrés sur deux exemples particuliers. Cela nous a permis de réduire les préparations générales au minimum. Voici les exemples.

1. Soit K/k une extension galoisienne de corps de nombres, $G = \text{Gal}(K/k)$. Alors nous considérons la ETNC pour le couple $(h^0(\mathbb{Q})_K, \mathbb{Z}[G])$, où $h^0(\mathbb{Q})$ dénote le motif de Tate.
2. Soit E/\mathbb{Q} une courbe elliptique et K/\mathbb{Q} une extension galoisienne de corps de nombres, $G = \text{Gal}(K/\mathbb{Q})$. Alors nous étudions la ETNC pour le couple $(h^1(E_K)(1), \mathbb{Z}[G])$, où E_K désigne la courbe elliptique E vue sur K .

Dans l'exemple 1 la ETNC décrit une version fine et équivariante de la formule analytique du nombre de classes, et dans l'exemple 2 nous obtenons une version fine et équivariante de la conjecture de Birch et Swinnerton-Dyer.

Dans la dernière partie de mes exposés j'ai étudié l'exemple 2 un peu plus en détail. J'ai expliqué quelques résultats numériques et dans des cas très spéciaux j'ai donné aussi quelques résultats théoriques. Ces résultats proviennent de [2, 3, 4].

Nous ne présentons presque pas de démonstration. Il est alors inévitable de lire la littérature originale et nous nous contentons ici de renvoyer le lecteur aux articles [8, 10] de Burns et Flach où l'on trouve beaucoup de références importantes. Les articles sommaires [17, 18] sont aussi fortement recommandés pour une introduction à la conjecture ETNC.

Notations : Nous introduisons quelques notations qui seront utilisées partout dans le texte. Pour une extension d'anneau $R \subseteq S$ et un R -module M nous posons $M_S := M \otimes_R S$. Si M est un \mathbb{Z} -module nous écrivons brièvement M_l pour $M \otimes_{\mathbb{Z}} \mathbb{Z}_l$.

Soit M un \mathbb{Z} -module de type fini. Alors on dénote M_{tors} le sous-module de torsion et on pose $M_{tf} := M/M_{tors}$. On écrit $\text{rk}(M)$ ou $\text{rk}_{\mathbb{Z}}(M)$ pour le rang de M_{tf} . Alors $\text{rk}(M) = \dim_{\mathbb{Q}}(M_{\mathbb{Q}})$.

Soit R un anneau. Alors $\zeta(R)$ dénote le centre de R et R^\times les unités de R . Comme d'habitude, pour un corps de nombres F , notons \mathcal{O}_F pour l'anneau des entiers de F .

2. K -théorie

Les références principales pour cette section sont [23] et [25].

2.1. Définition de K_0 . — Soit Λ un anneau (toujours avec un élément neutre). Tous les modules sur Λ seront pris à gauche. Soit $\text{PMod}(\Lambda)$ la catégorie des Λ -modules projectifs de type fini. Le groupe $K_0(\Lambda)$ est le groupe de Grothendieck de la catégorie $\text{PMod}(\Lambda)$. Il est défini par générateurs et relations comme suit :

- Un générateur $[P]$ pour chaque classe d'isomorphisme de module projectif de type fini.
- Une relation $[P \oplus Q] = [P] + [Q]$ pour tous les $P, Q \in \text{PMod}(\Lambda)$.

On dénote par (P) la classe de $P \in \text{PMod}(\Lambda)$ dans $K_0(\Lambda)$.

Exemple 2.1. — 1) Si Λ est un corps, alors tous les modules de type fini sont isomorphes à Λ^n pour un certain $n \in \mathbb{N}$. Ceci implique que $K_0(\Lambda) \simeq \mathbb{Z}$, où l'isomorphisme est induit par $(\Lambda^n) \mapsto n$.

2) Si Λ est un anneau local, alors $K_0(\Lambda) \simeq \mathbb{Z}$, parce que tout module projectif de type fini sur un anneau local est libre. Alors, comme dans 1), on a une notion de rang qui donne l'isomorphisme (cf. [25, Th. 1.3.11]).

3) Si Λ est un anneau de Dedekind, alors $K_0(\Lambda) \simeq \mathbb{Z} \oplus \text{cl}(\Lambda)$, où $\text{cl}(\Lambda)$ désigne le groupe des classes d'idéaux fractionnaires. Ce résultat est une conséquence du Théorème de Steinitz (cf. [25, Th. 1.4.12]).

2.2. Définition de K_1 . — Soit $\text{Gl}_n(\Lambda)$ le groupe des matrices inversibles. On a un plongement naturel

$$\text{Gl}_n(\Lambda) \hookrightarrow \text{Gl}_{n+1}(\Lambda), \quad A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}.$$

On définit

$$\text{Gl}(\Lambda) := \varinjlim_n \text{Gl}_n(\Lambda)$$

et

$$K_1(\Lambda) := \text{Gl}(\Lambda)/[\text{Gl}(\Lambda), \text{Gl}(\Lambda)],$$

où $[\text{Gl}(\Lambda), \text{Gl}(\Lambda)]$ est le groupe des commutateurs. Par le lemme de Whitehead on sait bien que $[\text{Gl}(\Lambda), \text{Gl}(\Lambda)] = E(\Lambda)$ où $E(\Lambda)$ désigne le groupe des matrices élémentaires.

Supposons Λ commutatif. Alors on a le déterminant

$$\text{Gl}(\Lambda) \xrightarrow{\det} \Lambda^\times.$$

L'application \det est surjective et scindée par

$$(1) \quad \Lambda^\times \longrightarrow \text{Gl}(\Lambda), \quad u \mapsto \begin{pmatrix} u & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \ddots \end{pmatrix}$$

Par conséquent, $K_1(\Lambda) \simeq \Lambda^\times \oplus \text{Sl}(\Lambda)/E(\Lambda)$, où $\text{Sl}(\Lambda)$ est la limite directe de $\text{Sl}_n(\Lambda) := \{A \in \text{Gl}_n(\Lambda) \mid \det(A) = 1\}$. On définit

$$\text{SK}_1(\Lambda) := \text{Sl}(\Lambda)/E(\Lambda).$$

Il existe certains cas intéressants où $\text{SK}_1(\Lambda) = 1$, par exemple, si Λ est un corps, un anneau local ou un anneau euclidien. Si $\Lambda = \mathcal{O}_K$ avec K/\mathbb{Q} un corps de nombres, alors il est démontré dans [1] ou [23, Sec. 16] que $\text{SK}_1(\Lambda) = 1$. En général, pour un anneau de Dedekind quelconque le groupe $\text{SK}_1(\Lambda)$ n'est pas trivial. Typiquement pour l'anneau $\Lambda = \mathbb{R}[x, y]/(x^2 + y^2 - 1)$ des fonctions polynomiales sur le cercle (cf. [1]).

On conclut cette section par un résultat important qui est utilisé dans plusieurs situations, entre autres dans la théorie d'Iwasawa non-commutative (cf. [28]). Rappelons-nous qu'un anneau Λ est semi-local si et seulement si $\Lambda/\text{rad}(\Lambda)$ est artinien (à gauche). Par exemple, si R est un anneau local et Λ une R -algèbre de type fini, alors Λ est semi-local. Par contre, \mathbb{Z} n'est pas semi-local, et plus généralement, tout anneau de Dedekind avec une infinité d'idéaux maximaux ne l'est pas non plus (cf. [14, §5C]).

Théorème 2.2. — *Soit Λ un anneau semi-local, alors l'application naturelle*

$$\Lambda^\times \longrightarrow K_1(\Lambda)$$

est surjective.

Démonstration. — [14, Th. (40.31)]. □

2.3. Le K_0 relatif. — Soit $\varphi: \Lambda \rightarrow \Lambda'$ un homomorphisme d'anneaux. On considère la catégorie suivante :

- Objets : Triplets (P, ϑ, Q) avec $P, Q \in \text{PMod}(\Lambda)$ et $\vartheta: P \otimes \Lambda' \rightarrow Q \otimes \Lambda'$ est un isomorphisme de Λ' -module.
- Morphismes : Un morphisme $(P, \vartheta, Q) \rightarrow (P_1, \vartheta_1, Q_1)$ est la donnée de Λ -homomorphismes $\alpha: P \rightarrow P_1$ et $\beta: Q \rightarrow Q_1$ telle que le diagramme suivant soit commutatif :

$$\begin{array}{ccc} P \otimes \Lambda' & \xrightarrow{\alpha \otimes \Lambda'} & P_1 \otimes \Lambda' \\ \downarrow \vartheta & & \downarrow \vartheta_1 \\ Q \otimes \Lambda' & \xrightarrow{\beta \otimes \Lambda'} & Q_1 \otimes \Lambda' \end{array}$$

Par définition, un morphisme dans cette catégorie est un isomorphisme, si et seulement si α et β sont des isomorphismes de Λ -modules. On dit que

$$(2) \quad 0 \rightarrow (P_1, \vartheta_1, Q_1) \xrightarrow{(\alpha_1, \beta_1)} (P, \vartheta, Q) \xrightarrow{(\alpha_2, \beta_2)} (P_2, \vartheta_2, Q_2) \rightarrow 0$$

est une suite exacte courte dans cette catégorie, si

$$\begin{array}{ccccccc} 0 & \rightarrow & P_1 & \xrightarrow{\alpha_1} & P & \xrightarrow{\alpha_2} & P_2 \rightarrow 0, \\ 0 & \rightarrow & Q_1 & \xrightarrow{\beta_1} & Q & \xrightarrow{\beta_2} & Q_2 \rightarrow 0 \end{array}$$

sont des suites exactes courtes de Λ -modules.

On définit maintenant le groupe $K_0(\Lambda, \varphi)$ par générateurs et relations comme suit :

- Générateurs : $[P, \vartheta, Q]$ pour toutes les classes d'isomorphismes d'objets (P, ϑ, Q) .
- Relations :
 - (i) $[P, \vartheta, Q] = [P_1, \vartheta_1, Q_1] + [P_2, \vartheta_2, Q_2]$ pour toute suite exacte courte comme dans (2).
 - (ii) Si $P, Q, R \in \text{PMod}(\Lambda)$ et $\vartheta_1: P \otimes \Lambda' \xrightarrow{\cong} Q \otimes \Lambda'$, $\vartheta_2: Q \otimes \Lambda' \xrightarrow{\cong} R \otimes \Lambda'$, alors

$$[P, \vartheta_1, Q] + [Q, \vartheta_2, R] = [P, \vartheta_2 \circ \vartheta_1, R].$$

Par abus de notation on dénote la classe de $[P, \vartheta, Q]$ dans $K_0(\Lambda, \varphi)$ par le même symbole.

2.4. La suite exacte de localisation. — La suite exacte qu'on présentera dans cette section joue un rôle important dans plusieurs situations, notamment dans la théorie de la conjecture équivariante de Tamagawa mais aussi dans la théorie d'Iwasawa non-commutative. Nous avons une suite exacte reliant les K -groupes qu'on vient de définir

$$K_1(\Lambda) \xrightarrow{\varphi_*} K_1(\Lambda') \xrightarrow{\partial_1} K_0(\Lambda, \varphi) \xrightarrow{\partial_0} K_0(\Lambda) \xrightarrow{\varphi_*} K_0(\Lambda')$$

où pour une matrice $A \in \text{GL}_n(\Lambda')$ nous avons posé

$$\partial_1(A) := [\Lambda^n, A, \Lambda^n], \quad \partial_0([P, \vartheta, Q]) := (P) - (Q)$$

et où φ_* est induit par φ de façon naturelle.

Nous donnerons deux exemples particuliers. Le premier est important pour la conjecture ETNC, le deuxième pour la conjecture principale de la théorie d'Iwasawa non-commutative.

Exemple 2.3. — Soit G un groupe fini, $\Lambda = \mathbb{Z}[G]$ ou $\Lambda = \mathbb{Z}_l[G]$, où l désigne un nombre premier. On écrit \mathbb{C}_l pour le complété d'une clôture algébrique de \mathbb{Q}_l . On se donne une extension de corps $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{C}$ ou $\mathbb{Q}_l \subseteq \mathbb{E} \subseteq \mathbb{C}_l$ et on pose $\Lambda' := \mathbb{E}[G]$. L'application φ est l'inclusion. Dans ce cas présent nous utiliserons la notation $K_0(\Lambda, \varphi) = K_0(\mathbb{Z}[G], \mathbb{E})$ ou $K_0(\mathbb{Z}_l[G], \mathbb{E})$.

Pour $\mathbb{E} = \mathbb{R}$ nous avons maintenant un diagramme fondamental pour la suite

$$(3) \quad \begin{array}{ccccccc} & & \zeta(\mathbb{R}[G])^\times & & & & \\ & & \uparrow \text{Nrd}_{\mathbb{R}[G]} & \searrow \hat{\partial}_1 & & & \\ K_1(\mathbb{Z}[G]) & \longrightarrow & K_1(\mathbb{R}[G]) & \xrightarrow{\partial_1} & K_0(\mathbb{Z}[G], \mathbb{R}) & \xrightarrow{\partial_0} & K_0(\mathbb{Z}[G]) \\ \uparrow = & & \uparrow & & \uparrow \subseteq & & \uparrow = \\ K_1(\mathbb{Z}[G]) & \longrightarrow & K_1(\mathbb{Q}[G]) & \xrightarrow{\partial_1} & K_0(\mathbb{Z}[G], \mathbb{Q}) & \xrightarrow{\partial_0} & K_0(\mathbb{Z}[G]) \\ & & & & \downarrow \simeq & & \\ & & & & \coprod_l K_0(\mathbb{Z}_l[G], \mathbb{Q}_l) & & \end{array}$$

Ici, l'application $\text{Nrd}_{\mathbb{R}[G]}$ est la norme réduite qui est définie, par exemple, dans [14, §7D]. Rappelons que $\text{Nrd}_{\mathbb{R}[G]}$ induit une application $K_1(\mathbb{R}[G]) \rightarrow \zeta(\mathbb{R}[G])^\times$ qui est injective, mais en général pas surjective. L'image est décrite par le théorème de Hasse-Schilling-Maass ([14, Th. (45.3)]). Cependant on peut définir une application naturelle $\hat{\partial}_1$ telle que $\partial_1 = \hat{\partial}_1 \circ \text{Nrd}_{\mathbb{R}[G]}$ (cf. [7, Lemma 2.2]).

Exemple 2.4. — Soit $S \subseteq \Lambda$ un ensemble multiplicativement fermé contenu dans le centre $\zeta(\Lambda)$ de Λ , ou plus généralement, un ensemble de Ore. C'est-à-dire, un ensemble multiplicativement fermé pour lequel la localisation $S^{-1}\Lambda$ existe. Soit $\varphi: \Lambda \rightarrow S^{-1}\Lambda$ l'application canonique.

Soit \mathcal{T} la catégorie des Λ -modules de type fini qui sont de S -torsion et de dimension projective ≤ 1 . Soit $K_0(\mathcal{T})$ le groupe de Grothendieck de la catégorie \mathcal{T} . Alors

$$(4) \quad K_0(\mathcal{T}) \simeq K_0(\Lambda, \varphi), \quad (C) \mapsto [Q, \alpha, P],$$

si $0 \rightarrow Q \xrightarrow{\alpha} P \rightarrow C \rightarrow 0$ est une résolution projective de C .

2.5. K_0 relatif et idéaux de Fitting. — Dans cette section G désigne un groupe fini abélien. Soit \mathcal{T} la catégorie des $\mathbb{Z}[G]$ -modules finis de dimension projective finie. Autrement dit, \mathcal{T} est la catégorie des $\mathbb{Z}[G]$ -modules finis et cohomologiquement triviaux. Signalons que la dimension projective d'un $\mathbb{Z}[G]$ -module cohomologiquement trivial est ≤ 1 . Soit $I_{\mathbb{Q}}(\mathbb{Z}[G])$ le groupe des $\mathbb{Z}[G]$ -modules $I \subseteq \mathbb{Q}[G]$ inversibles (ou, ce qui revient au même, localement libres). Alors on a

$$\begin{aligned} K_0(\mathcal{T}) &\simeq I_{\mathbb{Q}}(\mathbb{Z}[G]), \\ (C) &\mapsto \text{Fitt}_{\mathbb{Z}[G]}(C), \\ (\mathbb{Z}[G]/I) &\leftarrow I \end{aligned}$$

Ainsi, grâce à l'exemple 2.4, nous avons $K_0(\mathbb{Z}[G], \mathbb{Q}) \simeq K_0(\mathcal{T}) \simeq I_{\mathbb{Q}}(\mathbb{Z}[G])$.

De la même façon, on a $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l) \simeq K_0(\mathcal{T}_l) \simeq I_{\mathbb{Q}_l}(\mathbb{Z}_l[G])$, où \mathcal{T}_l désigne la catégorie des $\mathbb{Z}_l[G]$ -modules finis de dimension projective finie.

2.6. Calculs dans $K_0(\mathbb{Z}[G], \mathbb{Q})$. — On reprend le diagramme fondamental (3). Avec quelques simplifications, les conjectures qu'on veut étudier dans la suite prennent la forme d'une équation

$$(5) \quad \hat{\partial}_1(\mathcal{L}^*) = [P, \vartheta, Q] \text{ avec } \mathcal{L}^* \in \zeta(\mathbb{R}[G])^\times$$

dans le groupe relatif $K_0(\mathbb{Z}[G], \mathbb{R})$. Pour la conjecture ETNC l'élément \mathcal{L}^* est un objet analytique défini comme le terme dominant d'une fonction L motivique.

D'autre part, on dispose d'un élément algébrique qu'on va définir dans des exemples particuliers.

Dans ce qui suit, nous aurons besoin de quelques résultats de la théorie des représentations d'un groupe G fini.

Soit $\text{Irr}(G)$ l'ensemble des caractères absolument irréductibles de G . Par le théorème de Wedderburns nous avons

$$\mathbb{C}[G] \simeq \bigoplus_{\chi \in \text{Irr}(G)} M_{n_\chi}(\mathbb{C}),$$

qui induit un isomorphisme canonique

$$\zeta(\mathbb{C}[G]) \simeq \bigoplus_{\chi \in \text{Irr}(G)} \mathbb{C}.$$

Très souvent nous considérerons cet isomorphisme comme une égalité.

Lemme 2.5. — Soit \mathbb{E} un corps tel que $\mathbb{Q} \subseteq \mathbb{E} \subseteq \mathbb{C}$. Soit $\alpha = (\alpha_\chi)_{\chi \in \text{Irr}(G)} \in \zeta(\mathbb{C}[G])$. Alors on a

$$\alpha \in \zeta(\mathbb{E}[G]) \iff \alpha_{\sigma \circ \chi} = \sigma(\alpha_\chi), \forall \sigma \in \text{Aut}(\mathbb{C}/\mathbb{E}).$$

Démonstration. — [2, Lemma 2.8]. □

Pour un caractère χ nous désignons par $\mathbb{Q}(\chi)$ le corps engendré par les valeurs $\chi(g)$ où g parcourt les éléments du groupe G . L'extension $\mathbb{Q}(\chi)/\mathbb{Q}$ est abélienne et dans le cas important où $\mathbb{E} = \mathbb{Q}$ le lemme 2.5 prend la forme

$$\alpha \in \zeta(\mathbb{Q}[G]) \iff \begin{cases} \alpha_\chi \in \mathbb{Q}(\chi), & \forall \chi \in \text{Irr}(G) \text{ et} \\ \alpha_{\sigma \circ \chi} = \sigma(\alpha_\chi), & \forall \sigma \in \text{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}). \end{cases}$$

Revenons à l'étude de l'égalité (5). Posons

$$T\Omega := \hat{\partial}_1(\mathcal{L}^*) - [P, \vartheta, Q]$$

et considérons d'abord la question $T\Omega \stackrel{?}{\in} K_0(\mathbb{Z}[G], \mathbb{Q})$ que nous appelons conjecture de rationalité. Par un résultat de Swan (cf. [14, Th. (32.11)]), les modules $P_{\mathbb{Q}}$ et $Q_{\mathbb{Q}}$ sont des

$\mathbb{Q}[G]$ -modules libres de même rang, disons r . Choisissons des bases sur $\mathbb{Q}[G]$ de $P_{\mathbb{Q}}$ et $Q_{\mathbb{Q}}$ et représentons l'application ϑ par rapport à ces bases. Cela nous donne une matrice $B \in \mathrm{GL}_r(\mathbb{R}[G])$ (évidemment dépendant du choix des bases). Posons alors

$$u := \frac{\mathcal{L}^*}{\mathrm{Nrd}_{\mathbb{R}[G]}(B)} \in \zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times.$$

Évidemment u est bien défini. Par abus de notation, écrivons aussi u pour tout relèvement de u à $\zeta(\mathbb{R}[G])^\times$. On peut démontrer que (cf. [2, Lemma 2.4 (a)])

$$T\Omega \in K_0(\mathbb{Z}[G], \mathbb{Q}) \iff u \in \zeta(\mathbb{Q}[G])^\times.$$

Dorénavant on suppose la conjecture de rationalité vraie.

Il est maintenant raisonnable, et l'énoncé de ETNC le nécessite, de travailler nombre premier par nombre premier. Fixons alors un premier l et discutons la question $T\Omega_l \stackrel{?}{=} 0$ dans $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$. Soit $\mathrm{Irr}_{\mathbb{Q}}(G)$ un système de représentants de $\mathrm{Irr}(G)$ par l'action du groupe de Galois absolu $G_{\mathbb{Q}}$. On pose

$$C := \zeta(\mathbb{Q}[G]) \simeq \prod_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \mathbb{Q}(\chi).$$

Soit \mathcal{O}_C la clôture intégrale de \mathbb{Z} dans C . Évidemment \mathcal{O}_C s'identifie avec $\prod_{\chi \in \mathrm{Irr}_{\mathbb{Q}}(G)} \mathcal{O}_{\mathbb{Q}(\chi)}$.

Signalons que par le résultat de Swan [14, Th. (32.11)], tout $\mathbb{Z}[G]$ -module projectif est localement libre. Nous choisissons alors des $\mathbb{Z}_l[G]$ -bases de $P \otimes_{\mathbb{Z}} \mathbb{Z}_l$ et $Q \otimes_{\mathbb{Z}} \mathbb{Z}_l$ et représentons ϑ par rapport à ces bases. En fait, il suffit de travailler avec les localisations, et pour éviter encore plus de notations, c'est ce qu'on suppose désormais. Il en résulte une matrice $B \in \mathrm{GL}_r(\mathbb{R}[G])$ et nous posons

$$u_l := \frac{\mathcal{L}^*}{\mathrm{Nrd}_{\mathbb{R}[G]}(B)} \in \zeta(\mathbb{R}[G])^\times / \mathrm{Nrd}_{\mathbb{Q}[G]}(\mathbb{Z}_{(l)}[G]^\times),$$

où $\mathbb{Z}_{(l)} \subseteq \mathbb{Q}$ est la localisation de \mathbb{Z} . Par hypothèse (on rappelle que l'on a supposé vraie la conjecture de rationalité), tout relèvement de u_l (qu'on notera aussi u_l) est contenu dans $\zeta(\mathbb{Q}[G])^\times$. De plus, nous avons la

Proposition 2.6. — *On a $T\Omega_l = 0$ si et seulement si*

- (i) $u_l \in \mathcal{O}_{C,l}^\times$ (c'est-à-dire u_l est une unité l -adique), et
- (ii) $u_l \equiv 1 \pmod{\mathrm{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times)}$.

Supplément : Si $l \nmid |G|$, alors $\mathbb{Z}_l[G]$ est un ordre maximal et on a $\mathrm{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times) = \mathcal{O}_{C,l}^\times$ (cf. [6, Th. 2.2]). Dans ce cas il ne reste que la condition (i).

Par contre, si $l \mid |G|$ la condition (ii) se traduit par des congruences explicites. Donnons en deux exemples.

Exemple 2.7. — 1) Soit $G = \langle g_0 \rangle$ un groupe cyclique d'ordre l . Alors l'isomorphisme $\mathbb{C}[G] \simeq \mathbb{C} \oplus \dots \oplus \mathbb{C}$ correspond aux caractères χ_j définis par $\chi_j(g_0) := \zeta_l^j, \zeta_l = \exp(2\pi i/l), j = 0, \dots, l-1$. On a

$$\alpha = (\alpha_0, \dots, \alpha_{l-1}) \in \mathbb{Q}[G] \iff \begin{cases} \alpha_0 \in \mathbb{Q}, \alpha_1, \dots, \alpha_{l-1} \in \mathbb{Q}(\zeta_l) \text{ et} \\ \sigma_j(\alpha_1) = \alpha_j, j = 1, \dots, l-1. \end{cases}$$

Ici $\sigma_j \in \text{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$ est l'isomorphisme défini par $\sigma_j(\zeta_l) = \zeta_l^j$. Par conséquent, on peut prendre $\text{Irr}_{\mathbb{Q}}(G) = \{\chi_0, \chi_1\}$. De plus, si (α_0, α_1) satisfait (i), alors on a

$$\alpha \in \text{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times) = \mathbb{Z}_l[G]^\times \iff \alpha_0 \equiv \alpha_1 \pmod{1 - \zeta_l}.$$

2) Soit $G = \langle \sigma, \tau : \sigma^l = id = \tau^2, \tau\sigma = \sigma^{-1}\tau \rangle$ le groupe diédral d'ordre $2l$, $l \neq 2$ premier. On dénote χ_0 le caractère trivial et χ_1 le caractère défini par $\chi_1(\sigma) = 1$ et $\chi_1(\tau) = -1$. Ce sont les caractères abéliens. Il y a $m := \frac{l-1}{2}$ caractères de degré 2 de la forme $\psi_j = \text{ind}_H^G(\lambda_j)$, où λ_j parcourt la moitié des caractères non triviaux de $H = \langle \sigma \rangle$. Plus explicite, si λ_j est défini par $\lambda_j(\sigma) = \zeta_l^j$, $j = 0, \dots, l-1$, alors on prend les λ_j pour $j = 1, \dots, m$. Les caractères de degré 2 prennent leurs valeurs dans le corps réel maximal $\mathbb{Q}(\zeta_l)^+$ du corps cyclotomique $\mathbb{Q}(\zeta_l)$ (cf. [14, (10.11)]). On en déduit

$$\mathbb{C}[G] \simeq \mathbb{C} \oplus \mathbb{C} \oplus M_2(\mathbb{C}) \oplus \dots \oplus M_2(\mathbb{C}).$$

Pour un élément $\alpha = (\alpha_{\chi_0}, \alpha_{\chi_1}, \alpha_{\psi_1}, \dots, \alpha_{\psi_m}) \in \zeta(\mathbb{C}[G])$ on a

$$\alpha \in \zeta(\mathbb{Q}[G]) \iff \alpha_{\chi_0}, \alpha_{\chi_1} \in \mathbb{Q} \text{ et } \alpha_{\psi_1}, \dots, \alpha_{\psi_m} \in \mathbb{Q}(\zeta_l)^+ \text{ sont conjugués.}$$

En plus, si $(\alpha_{\chi_0}, \alpha_{\chi_1}, \alpha_{\psi_1})$ satisfait (i), alors on a

$$\alpha \in \text{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times) \iff \alpha_{\chi_0} \alpha_{\chi_1} \equiv \alpha_{\psi_1} \pmod{1 - \zeta_l}.$$

Pour encore plus d'exemples et plus de détails le lecteur est renvoyé à [2, Sec. 2.3] et à [3, Sec. 5].

3. Caractéristique d'Euler attachée aux complexes parfaits

Pour l'énoncé de la conjecture équivariante de Tamagawa il nous faut encore une méthode pour produire des éléments algébriques dans le K_0 relatif à partir d'un complexe parfait et la donnée de certains isomorphismes entre ses groupes de cohomologie.

Pour l'instant, soit Λ un anneau quelconque. Pour un complexe

$$A^\bullet : \dots \longrightarrow A^{i-1} \xrightarrow{\partial^{i-1}} A^i \xrightarrow{\partial^i} A^{i+1} \longrightarrow \dots$$

on désigne, comme d'habitude, par

$$H^i(A^\bullet) := \frac{\ker(\partial^i)}{\text{im}(\partial^{i-1})}$$

les groupes de cohomologie. On dit que A^\bullet est un complexe parfait lorsqu'il existe un complexe

$$(6) \quad P^\bullet : \dots \longrightarrow P^{i-1} \xrightarrow{\partial^{i-1}} P^i \xrightarrow{\partial^i} P^{i+1} \longrightarrow \dots$$

et un morphisme de complexes $\pi : P^\bullet \longrightarrow A^\bullet$ tel que

- P^\bullet est borné, c'est-à-dire, il n'y a qu'un nombre fini de P^i non nul.
- $P^i \in \text{PMod}(\Lambda)$ pour tout i .
- π induit des isomorphismes $H^i(P^\bullet) \xrightarrow{\simeq} H^i(A^\bullet)$ pour tout i . (Dans ce cas on dit que π est un quasi-isomorphisme.)

Soit maintenant $\Lambda = \mathbb{Z}[G]$. Posons

$$H^{pair}(P^\bullet) := \bigoplus_{2|i} H^i(P^\bullet), \quad H^{impair}(P^\bullet) := \bigoplus_{2 \nmid i} H^i(P^\bullet)$$

et supposons qu'on a un isomorphisme

$$\vartheta: H^{pair}(P^\bullet)_{\mathbb{R}} \xrightarrow{\simeq} H^{impair}(P^\bullet)_{\mathbb{R}}.$$

Lorsqu'on pose $Z^i = Z^i(P^\bullet) := \ker(\partial^i)$, $B^i = B^i(P^\bullet) := \text{im}(\partial^{i-1})$ on a par définition les suites exactes courtes tautologiques

$$\begin{aligned} 0 \longrightarrow Z^i \longrightarrow P^i \xrightarrow{\partial^i} B^{i+1} \longrightarrow 0 \\ 0 \longrightarrow B^i \xrightarrow{\subseteq} Z^i \longrightarrow H^i \longrightarrow 0 \end{aligned}$$

En appliquant le foncteur $\otimes_{\mathbb{Z}} \mathbb{R}$, ces suites deviennent scindées (car $\mathbb{R}[G]$ est semi-simple) et on peut définir un isomorphisme $\tilde{\vartheta}$ de $\mathbb{R}[G]$ -modules comme la composée suivante

$$\tilde{\vartheta}: P_{\mathbb{R}}^{pair} \simeq H_{\mathbb{R}}^{pair} \oplus B_{\mathbb{R}}^{all} \xrightarrow{\vartheta \oplus id} H_{\mathbb{R}}^{impair} \oplus B_{\mathbb{R}}^{all} \simeq P_{\mathbb{R}}^{impair},$$

où $B^{all} := \bigoplus_{i \in \mathbb{Z}} B^i$ (pour plus de détails voir [12, Sec. 1]).

Définition 3.1. — Pour un complexe P^\bullet comme dans (6) on définit la caractéristique d'Euler $\chi_{\mathbb{Z}[G], \mathbb{R}}(P^\bullet, \vartheta) \in K_0(\mathbb{Z}[G], \mathbb{R})$ par

$$\chi_{\mathbb{Z}[G], \mathbb{R}}(P^\bullet, \vartheta) := [P^{pair}, \tilde{\vartheta}, P^{impair}].$$

Il est démontré dans [12] que cette caractéristique d'Euler est bien définie et est indépendante du choix des applications scindées.

Avant de donner la définition générale pour un complexe parfait A^\bullet , nous explicitons la construction dans un cas spécial. Si P^\bullet n'a que deux modules non nuls, disons P^0 et P^1 , alors on a un diagramme

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^0 & \longrightarrow & P^0 & \xrightarrow{\partial^0} & P^1 & \xrightarrow{\tau} & H^1 & \longrightarrow & 0 \\ & & & & \searrow & & \nearrow & & & & \\ & & & & & & B^1 & & & & \\ & & & & \swarrow & & \searrow & & & & \\ & & & & 0 & & 0 & & & & \end{array}$$

où toutes les suites courtes sont exactes. Après $\otimes_{\mathbb{Z}} \mathbb{R}$ on peut choisir des applications scindées, dénotées σ et τ dans le diagramme, et on obtient

$$\tilde{\vartheta}: P_{\mathbb{R}}^0 \simeq H_{\mathbb{R}}^0 \oplus B_{\mathbb{R}}^1 \longrightarrow H_{\mathbb{R}}^1 \oplus B_{\mathbb{R}}^1 \simeq P_{\mathbb{R}}^1.$$

Le premier isomorphisme est induit par σ et le dernier par τ . On remarque qu'en général les applications σ et τ n'existent qu'au niveau des $\mathbb{R}[G]$ -modules.

Définition 3.2. — Soit A^\bullet un complexe parfait, $\vartheta: H^{pair}(A^\bullet)_{\mathbb{R}} \xrightarrow{\simeq} H^{impair}(A^\bullet)_{\mathbb{R}}$ un isomorphisme de $\mathbb{R}[G]$ -modules et $\pi: P^\bullet \rightarrow A^\bullet$ un quasi-isomorphisme comme ci-dessus. On définit la caractéristique d'Euler $\chi_{\mathbb{Z}[G], \mathbb{R}}(A^\bullet, \vartheta) \in K_0(\mathbb{Z}[G], \mathbb{R})$ par

$$\chi_{\mathbb{Z}[G], \mathbb{R}}(A^\bullet, \vartheta) := \chi_{\mathbb{Z}[G], \mathbb{R}}(P^\bullet, \pi^{-1}\vartheta\pi).$$

Grâce à un résultat de Burns [12, Sec. 2], la quantité $\chi_{\mathbb{Z}[G], \mathbb{R}}(A^\bullet, \vartheta)$ est bien définie, c'est-à-dire, la définition ne dépend pas des choix qu'on a fait pendant la construction.

Donnons deux exemples qui montrent que cette caractéristique d'Euler généralise des concepts bien connus.

Exemple 3.3. — Soit $G = 1$ et C un groupe abélien fini. Comme d'habitude, écrivons $C[1]$ pour le complexe qui a comme seul module non nul le module C en degré 1. Soit

$$0 \rightarrow \mathbb{Z}^n \xrightarrow{\alpha} \mathbb{Z}^n \rightarrow C \rightarrow 0$$

une présentation de C . Alors le complexe $C[1]$ est parfait comme le montre le diagramme suivant

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\alpha} & \mathbb{Z}^n \\ & & \downarrow \pi \\ & & C \end{array}$$

où les modules sont placés en les degrés 0 et 1. On obtient $\chi_{\mathbb{Z}, \mathbb{R}}(C[1], 0) = [\mathbb{Z}^n, \alpha, \mathbb{Z}^n] \in K_0(\mathbb{Z}, \mathbb{R})$. On déduit de la suite exacte de localisation, ou bien du diagramme (3), que $K_0(\mathbb{Z}, \mathbb{R}) \simeq \mathbb{R}^\times / \pm 1$, l'isomorphisme étant induit par \det . Alors $\chi_{\mathbb{Z}, \mathbb{R}}(C[1], 0) = [\mathbb{Z}^n, \alpha, \mathbb{Z}^n] \mapsto \det(\alpha) \bmod \pm 1$. D'un autre côté, $|\det(\alpha)| = |C|$ et on retrouve ainsi l'ordre d'un \mathbb{Z} -module C fini.

Exemple 3.4. — Soit G abélien et C un $\mathbb{Z}[G]$ -module fini et cohomologiquement trivial. Alors on a une suite exacte

$$0 \rightarrow Q \rightarrow \mathbb{Z}[G]^n \xrightarrow{\pi} C \rightarrow 0$$

avec $n \in \mathbb{N}$ assez grand et $Q = \ker(\pi)$. La suite exacte de cohomologie démontre que Q aussi est cohomologiquement trivial. De plus, Q est sans torsion sur \mathbb{Z} . On rappelle que tout module cohomologiquement trivial et sans \mathbb{Z} -torsion est $\mathbb{Z}[G]$ -projective (cf. [24]). Donc, comme ci-dessus le complexe $C[1]$ est parfait et on arrive à $\chi_{\mathbb{Z}[G], \mathbb{R}}(C[1], 0) = [Q, id, \mathbb{Z}[G]^n] \in K_0(\mathbb{Z}[G], \mathbb{Q})$. Mais d'après le paragraphe 2.5 on a $K_0(\mathbb{Z}[G], \mathbb{Q}) \simeq I_{\mathbb{Q}}(\mathbb{Z}[G])$. Cet isomorphisme applique l'élément $[Q, id, \mathbb{Z}[G]^n]$ à $\text{Fitt}_{\mathbb{Z}[G]}(C)$. Ainsi la caractéristique d'Euler qu'on vient de définir généralise la notion de l'idéal de Fitting.

4. Courbe elliptique, BSD et fonctions L de Hasse-Weil tordues

Le but de ce paragraphe est d'introduire les objets analytiques qui figurent dans ETNC dans un cas particulier, plus précisément, dans le cas où le motif vient d'une courbe elliptique définie sur \mathbb{Q} considérée comme une courbe sur K , où K désigne une extension galoisienne de \mathbb{Q} .

Pour donner un minimum de motivation, nous commençons par la conjecture de Birch et Swinnerton-Dyer (abrégée BSD) qui est conjointement avec la formule analytique du nombre de classes le prototype pour ETNC.

Soit E/\mathbb{Q} une courbe elliptique définie sur \mathbb{Q} . Rappelons rapidement la définition de la fonction L de Hasse-Weil qui est définie par un produit d'Euler. Les facteurs locaux sont donnés par

$$L_p(E/\mathbb{Q}, T) := \begin{cases} 1 - a_p T + pT^2, & \text{bonne réduction en } p, \\ 1 - T, & \text{réduction multiplicative déployée,} \\ 1 + T, & \text{réduction multiplicative non-déployée,} \\ 1 & \text{réduction additive,} \end{cases}$$

où $a_p = p + 1 - |\bar{E}(\mathbb{F}_p)|$. On remarque qu'on a toujours $L_p(E/\mathbb{Q}, \frac{1}{p}) = \frac{|\bar{E}_{ns}(\mathbb{F}_p)|}{p}$, où $\bar{E}_{ns}(\mathbb{F}_p)$ désigne le groupe des points \mathbb{F}_p -rationnels non-singuliers sur la courbe réduite.

Définition 4.1. — On pose

$$L(E/\mathbb{Q}, s) := \prod_p L_p(E/\mathbb{Q}, p^{-s})^{-1},$$

où p parcourt tous les nombres premiers et on l'appelle la fonction L de Hasse-Weil associée à la courbe E .

Remarque 4.2. — 1) Le produit d'Euler converge pour $\text{Re}(s) > \frac{3}{2}$. Comme conséquence du théorème de modularité on sait qu'il existe un prolongement sur tout le plan complexe.

2) La fonction L de Hasse-Weil s'écrit comme série de Dirichlet

$$L(E/\mathbb{Q}, s) = \sum_{n \geq 1} a_n n^{-s}, \quad \text{Re}(s) > \frac{3}{2},$$

où les a_n sont définis à partir des a_p , p premier, par les formules

$$a_{mn} = a_m a_n, \text{ si } (m, n) = 1, \quad a_{p^{\nu+1}} = a_p a_{p^\nu} - p a_{p^{\nu-1}}, \text{ si } \nu \geq 1 \text{ et } a_1 = 1.$$

D'après le théorème de Mordell-Weil le groupe des points de E rationnels sur \mathbb{Q} , noté $E(\mathbb{Q})$, est un groupe abélien de type fini.

Comme d'habitude, $\text{III}(E/\mathbb{Q})$ désigne le groupe de Tate-Shafarevic, Ω_+ la période réelle et c_p les facteurs locaux de Tamagawa. Finalement, Reg est le régulateur elliptique. Nous donnerons sa définition après l'énoncé de la conjecture de Birch et Swinnerton-Dyer.

La conjecture BSD

1) (Conjecture du rang)

$$\text{ord}_{s=1} L(E/\mathbb{Q}, s) \stackrel{?}{=} \text{rg}_{\mathbb{Z}}(E(\mathbb{Q})).$$

2) (Conjecture de rationalité) Posons $r := \text{rg}_{\mathbb{Z}}(E(\mathbb{Q}))$ et

$$L^*(E/\mathbb{Q}, 1) := \lim_{s \rightarrow 1} (s-1)^{-r} L(E/\mathbb{Q}, s).$$

Alors

$$\frac{L^*(E/\mathbb{Q}, 1)}{\Omega_+ \text{Reg}} \stackrel{?}{\in} \mathbb{Q}^\times.$$

3) (Conjecture d'intégralité)

$$\frac{L^*(E/\mathbb{Q}, 1)}{\Omega_+ \text{Reg}} \stackrel{?}{=} \frac{|\text{III}(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\text{tors}}|^2} \cdot \prod_p c_p.$$

Rappelons la définition du régulateur. On fixe une base P_1, \dots, P_r de $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$, alors

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}P_1 \oplus \dots \oplus \mathbb{Z}P_r.$$

On dénote P_1^*, \dots, P_r^* la base duale, c'est-à-dire,

$$P_i^*(P_j) = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Si $\langle _, _ \rangle_{NT}: E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$ désigne l'accouplement de Néron-Tate, on obtient un isomorphisme

$$\begin{aligned} \lambda_{NT}: E(\mathbb{Q})_{\mathbb{R}} &\longrightarrow E(\mathbb{Q})_{\mathbb{R}}^* := \text{Hom}_{\mathbb{R}}(E(\mathbb{Q})_{\mathbb{R}}, \mathbb{R}), \\ P &\mapsto \langle P, _ \rangle_{NT}. \end{aligned}$$

Comme $\langle P_i, _ \rangle_{NT} = \sum_{j=1}^r \langle P_i, P_j \rangle_{NT} P_j^*$ la matrice correspondante à λ_{NT} par notre choix des bases est évidemment $(\langle P_i, P_j \rangle_{NT})_{1 \leq i, j \leq r}$. On définit

$$\text{Reg} := \det (\langle P_i, P_j \rangle_{NT}).$$

En résumé, on note que nous avons choisi des \mathbb{Z} -bases de $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ et de $E(\mathbb{Q})^*$, puis nous avons représenté l'isomorphisme λ_{NT} par une matrice et, finalement, nous en avons pris le déterminant.

Nous ne donnerons pas la définition de Ω_+ mais nous nous contentons de constater que Ω_+ a aussi une interprétation comme le déterminant d'un isomorphisme naturel qu'on appelle isomorphisme de période. Puisque les \mathbb{Z} -modules sont ici de rang 1 cela a peut-être l'air artificiel mais c'est exactement ce point de vue qui se généralise dans le cas équivariant.

Remarque 4.3. — La conjecture ETNC pour le motif $h^1(E)(1)$ est équivalente à la conjecture BSD. La démonstration de ce fait n'est pas évidente, car l'énoncé de ETNC est très technique et très général. Le lecteur peut se reporter aux articles de Kings [21] ou de Venjakob [29].

L'objectif de ce qui suit est le développement d'une conjecture plus fine que BSD dans la situation suivante :

$$\begin{aligned} E/\mathbb{Q} &\text{ est une courbe elliptique sur } \mathbb{Q}, \\ K/\mathbb{Q} &\text{ une extension galoisienne finie,} \\ M_K &= h^1(E_K)(1). \end{aligned}$$

Cette conjecture plus fine doit faire ressortir l'action du groupe $G = \text{Gal}(K/\mathbb{Q})$ sur les objets arithmétiques associés à E/K qui sont, entre autres, le groupe $E(K)$ ou le groupe $\text{III}(E/K)$. Commençons par la définition du côté analytique de la conjecture. Pour tout caractère $\chi \in \text{Irr}(G)$ on peut définir une fonction L de Hasse-Weil tordue qu'on dénote par $L(E/\mathbb{Q}, \chi, s)$.

Nous ne donnerons pas la définition. Il nous suffit, pour avoir une idée, de constater que dans le cas où G est abélien on a

$$L_p(E/\mathbb{Q}, \chi, T) = 1 - \chi(p)a_p T + \chi(p)^2 p T^2$$

pour tout caractère χ abélien et tout premier p où la courbe a bonne réduction. Ou bien,

$$L(E/\mathbb{Q}, \chi, s) = \sum_{n=1}^{\infty} \chi(n) a_n n^{-s}, \quad \operatorname{Re}(s) > \frac{3}{2}.$$

Dans les deux formules on considère χ comme un caractère de Dirichlet par la théorie du corps de classes.

Définition 4.4. — a) La fonction L motivique associée au motif M_K est la fonction ayant les valeurs dans $\zeta(\mathbb{C}[G])$ donnée par

$$L(M_K, s) = (L(E/\mathbb{Q}, \bar{\chi}, s + 1))_{\chi \in \operatorname{Irr}(G)}.$$

b) On pose

$$\mathcal{L}^* := (L^*(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \operatorname{Irr}(G)}.$$

Le lecteur trouvera plus de détails dans [10, Rem. 7] ou dans [2, Sec. 3]. A priori, $\mathcal{L}^* \in \zeta(\mathbb{C}[G])^\times$, mais comme la conjugaison complexe est continue on déduit facilement du lemme 2.5 que $\mathcal{L}^* \in \zeta(\mathbb{R}[G])^\times$.

Remarque 4.5. — Lorsqu'on remplace le motif $h^1(E_K)(1)$ par le motif de Tate $h^0(\mathbb{Q})_K$, les fonctions L de Hasse-Weil tordues sont à remplacer par les fonctions L d'Artin. Dans ce cas on arrive essentiellement à la fonction

$$\theta_S: \mathbb{C} \longrightarrow \mathbb{C}[G] \simeq \bigoplus_{\chi \in \operatorname{Irr}(G)} \mathbb{C}$$

introduite dans l'exposé [20] de Greither (avec quelques modifications à cause de l'ensemble S).

Pour définir le terme de droite dans (5) et pour bien comprendre les problèmes qui se posent en travaillant avec des $\mathbb{Z}[G]$ -modules, il faut avoir une idée de la conjecture ETNC dans le cas général.

5. La conjecture équivariante de Tamagawa : une esquisse

La conjecture équivariante de Tamagawa est une conjecture formulée dans le langage de la théorie des motifs. Nous ne donnerons pas une introduction de cette théorie. Le but de cette section est modeste : on veut obtenir une idée de ETNC dans le cas général et bien comprendre deux cas spéciaux. Ce sont le cas des motifs de Tate en $s = 0$ et le cas de l'extension des scalaires d'une courbe elliptique E/\mathbb{Q} déjà décrit dans la Section 4.

Soit

- A une algèbre semi-simple de type fini sur \mathbb{Q} ,
- M un motif sur \mathbb{Q} , muni d'une A -action.

Une structure motivique pour nous consiste en

- des réalisations l -adiques, de Betti et de deRham,
- des groupes motiviques de cohomologie,
- des isomorphismes de comparaison,
- une suite exacte conjecturale mettant ces objets en relation entre eux.

Dans la suite nous décrirons cette structure pour deux motifs ; ce sont nos exemples principaux.

Exemple 1 : (Motif de Tate) Soit K/\mathbb{Q} une extension finie galoisienne avec groupe G . Alors on a un motif $M = h^0(\mathbb{Q})_K$; c'est l'extension des scalaires du motif de Tate $h^0(\mathbb{Q})$.

Exemple 2 : (Extension des scalaires d'une courbe elliptique) C'est l'exemple qu'on a déjà décrit dans la Section 4. Alors :

$$\begin{aligned} E/\mathbb{Q} & \quad \text{une courbe elliptique ,} \\ K/\mathbb{Q} & \quad \text{une extension finie galoisienne avec groupe } G, \\ M & = h^1(E/K)(1) \end{aligned}$$

Dans nos exemples principaux l'algèbre A est l'algèbre $\mathbb{Q}[G]$.

La réalisation l -adique d'un motif est une représentation A_l -linéaire du groupe de Galois absolu $G_{\mathbb{Q}} = \text{Gal}(\mathbb{Q}^c/\mathbb{Q})$. Pour un corps de nombres F , on pose $\Sigma(F)$ pour l'ensemble des plongements de F dans \mathbb{C} . Nous définissons $H_K := \bigoplus_{\sigma \in \Sigma(K)} \mathbb{Q}$. Les groupes G et $G_{\mathbb{Q}}$ opèrent sur $\Sigma(K)$ et cela fournit bien une action de G et $G_{\mathbb{Q}}$ sur H_K .

Dans l'exemple 1 on a

$$M_l = H_{K,l} = \bigoplus_{\sigma \in \Sigma(K)} \mathbb{Q}_l$$

et dans l'exemple 2

$$M_l = H_{K,l} \otimes_{\mathbb{Q}_l} \text{Hom}(V_l(E), \mathbb{Q}_l)(1),$$

où $T_l(E)$ est le module de Tate, $V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ et $G_{\mathbb{Q}}$ opère bien sur $H_{K,l}$ et $V_l(E)$.

On utilise alors les réalisations l -adiques pour la définition des fonctions L . Supposons pour l'instant que A soit commutative. Pour un premier p on désigne par $Fr_p \in G_{\mathbb{Q}}$ un élément de Frobenius et par I_p le groupe de ramification. On pose

$$\begin{aligned} L_p(M, T) & := \det_{A_l} \left(1 - Fr_p^{-1} \cdot T | M_l^{I_p} \right) \in A_l[T], \\ L(M, s) & := \prod_p L_p(M, p^{-s})^{-1} \end{aligned}$$

Si A est non-commutative, on doit remplacer \det par la norme réduite. Remarquons que ces fonctions L prennent leurs valeurs dans $\zeta(A_{\mathbb{C}})$ (cf. [10, Rem. 7]).

Dans nos exemples on a $A_{\mathbb{C}} = \mathbb{C}[G]$. Rappelons que nous identifions $\zeta(\mathbb{C}[G])$ et $\prod_{\chi \in \text{Irr}(G)} \mathbb{C}$. Dans notre exemple 1 la fonction L motivique est le vecteur des fonctions L d'Artin,

$$L(M, s) = (L(K/\mathbb{Q}, \bar{\chi}, s))_{\chi \in \text{Irr}(G)},$$

et dans l'exemple 2 on obtient, comme on a déjà expliqué, le vecteur des fonctions L de Hasse-Weil tordues,

$$L(M, s) = (L(E/\mathbb{Q}, \bar{\chi}, s + 1))_{\chi \in \text{Irr}(G)}.$$

Continuons avec la description des réalisations M_B de Betti dans nos exemples principaux. En général, M_B est un espace sur A de type fini muni d'une action de la conjugaison complexe. Dans l'exemple 1 on a

$$M_B = H_K = \bigoplus_{\sigma \in \Sigma(K)} \mathbb{Q}.$$

Le groupe G et la conjugaison complexe opèrent sur $\Sigma(K)$ et cela induit des actions naturelles de A et de la conjugaison complexe sur M_B . Dans l'exemple 2 la réalisation de Betti est donnée par

$$M_B = H_K \otimes_{\mathbb{Q}} H^1(E(\mathbb{C}), 2\pi i\mathbb{Q}),$$

où $H^1(E(\mathbb{C}), 2\pi i\mathbb{Q})$ est le groupe de cohomologie singulière avec son action naturelle de la conjugaison complexe. Le groupe G opère sur le premier facteur.

La réalisation M_{dR} de deRham est un espace sur A muni d'une filtration $F^i M_{dR}$ naturelle, la filtration de Hodge. On définit l'espace tangentiel t_M par $M_{dR}/F^0 M_{dR}$. Dans l'exemple 1 on a

$$M_{dR} = K, \quad F^i M_{dR} = \begin{cases} K, & i \leq 0, \\ 0, & i > 0, \end{cases} \quad \text{alors } t_M = 0.$$

Pour l'exemple 2 nous nous contentons de décrire l'espace tangentiel :

$$t_M = K \otimes_{\mathbb{Q}} \text{Hom}(\Omega_{E/\mathbb{Q}}^1, \mathbb{Q})$$

où $\Omega_{E/\mathbb{Q}}^1$ désigne les formes différentielles de E . Le groupe G opère sur le premier facteur K de façon naturelle.

Dans la théorie des motifs, il y a un isomorphisme très important qu'on appelle isomorphisme de périodes,

$$\alpha'_M : M_{B,\mathbb{C}} \xrightarrow{\cong} M_{dR,\mathbb{C}}.$$

Comme d'habitude nous appelons M_B^+ le sous-module de M_B sur lequel la conjugaison complexe opère comme l'identité. Alors l'isomorphisme α'_M induit un homomorphisme de $A_{\mathbb{R}}$ -modules

$$\alpha_M : M_B^+ \otimes_{\mathbb{Q}} \mathbb{R} \longrightarrow t_M \otimes_{\mathbb{Q}} \mathbb{R}.$$

Nous écrirons α_M dans nos exemples principaux.

Pour le motif de Tate (exemple 1) on a

$$M_B^+ \otimes_{\mathbb{Q}} \mathbb{R} = \bigoplus'_{\sigma \in \Sigma(K)} \mathbb{R},$$

où ' indique que les éléments σ ne parcourent qu'un système de représentants de $\Sigma(K)$ pour l'action de la conjugaison complexe (si σ et $\bar{\sigma}$ sont conjugués, on ne prend qu'un seul élément du couple $(\sigma, \bar{\sigma})$). Comme $t_M = 0$, l'application α_M est 0.

Dans le cas des courbes elliptiques (exemple 2), α_M est un isomorphisme qui est essentiellement induit par

$$\begin{aligned} H_1(E(\mathbb{C}), \mathbb{C}) &\longrightarrow \text{Hom}(\Omega_{E/\mathbb{Q}}^1, \mathbb{C}), \\ \gamma &\mapsto \left(\omega \mapsto \int_{\gamma} \omega \right). \end{aligned}$$

On trouve une description plus détaillée de α_M dans [2, Sec. 3].

Dans l'exemple 1, les groupes de cohomologie motivique $H_f^0(M)$ et $H_f^1(M)$ pour un motif M et son dual $M^*(1)$ sont donnés par

$$\begin{aligned} H_f^0(M) &= \mathbb{Q}, & H_f^1(M) &= 0, \\ H_f^0(M^*(1)) &= 0, & H_f^1(M^*(1)) &= \mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{Q}. \end{aligned}$$

Dans l'exemple 2, le motif est auto-dual, c'est-à-dire, $M = M^*(1)$. On a

$$H_f^0(M) = 0, \quad H_f^1(M) = E(K) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Conjecturalement, on a une suite exacte fondamentale reliant les objets qu'on vient de définir (cf. [10, Conjecture 1]). Cette suite exacte est de la forme

$$(7) \quad \begin{array}{ccccccc} 0 & \longrightarrow & H_f^0(M)_{\mathbb{R}} & \xrightarrow{c} & \ker(\alpha_M) & \xrightarrow{r^*} & H_f^1(M^*(1))_{\mathbb{R}}^* \xrightarrow{h} \\ & & & & & & \\ & & H_f^1(M)_{\mathbb{R}} & \xrightarrow{r} & \text{cok}(\alpha_M) & \xrightarrow{c^*} & H_f^0(M^*(1))_{\mathbb{R}}^* \longrightarrow 0, \end{array}$$

où c est une application de classes de cycles, h est induit par une forme bilinéaire de hauteur et r est un régulateur à la Beilinson.

Pour le motif de Tate, la deuxième moitié de la suite est nulle et r est le régulateur de Dirichlet. Plus explicitement, il ne reste que la suite exacte courte

$$0 \longrightarrow \mathbb{R} \longrightarrow \bigoplus'_{\sigma \in \Sigma(K)} \mathbb{R} \xrightarrow{r^*} (\mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{R})^* \longrightarrow 0.$$

Ce n'est autre que le dual de la suite exacte du régulateur de Dirichlet bien connue qui apparaît dans la démonstration du théorème de Dirichlet sur les unités d'un corps de nombres.

Dans le cas des courbes elliptiques α_M est un isomorphisme et h est le dual de l'isomorphisme λ_{NT} . Alors, la suite exacte fondamentale se réduit à

$$0 \longrightarrow E(K)_{\mathbb{R}}^* \xrightarrow{h} E(K)_{\mathbb{R}} \longrightarrow 0.$$

Pour tout motif M la suite exacte fondamentale (7) induit, par choix des applications scindées, un isomorphisme

$$\vartheta : H_f^0(M)_{\mathbb{R}} \oplus H_f^1(M^*(1))_{\mathbb{R}}^* \oplus t_{M, \mathbb{R}} \longrightarrow H_f^1(M)_{\mathbb{R}} \oplus H_f^0(M^*(1))_{\mathbb{R}}^* \oplus M_{B, \mathbb{R}}^+.$$

En principe, nous choisissons des $\mathbb{Q}[G]$ -bases de

$$H_f^0(M) \oplus H_f^1(M^*(1))^* \oplus t_M$$

et de

$$H_f^1(M) \oplus H_f^0(M^*(1))^* \oplus M_B^+$$

et représentons ϑ par rapport à ces bases. Bien sûr, il faut préciser la notion d'une $\mathbb{Q}[G]$ -base parce qu'en général un $\mathbb{Q}[G]$ -module n'est pas libre. Mais la théorie des représentations permet de donner un sens à cette notion. Pour plus de détails voir [2, Rem. 6b)]. Ainsi nous obtenons une matrice $A(\vartheta) \in \text{Gl}_m(\mathbb{R}[G])$ et nous considérons la classe de $\text{Nrd}_{\mathbb{R}[G]}(A(\vartheta))$ dans $\zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times$. Il est vrai que cette classe dépend du choix des bases, mais on peut démontrer qu'elle ne dépend pas du choix de ϑ .

Conjecture 5.1. —

$$\mathcal{L}^* \cdot \text{Nrd}_{\mathbb{R}[G]}(A(\vartheta)) \in \zeta(\mathbb{Q}[G])^\times.$$

On peut démontrer que la conjecture 5.1 est équivalente à la conjecture [10, Conj. 4(iii)]. Dans la suite nous désignons par $\text{Nrd}_{\mathbb{R}[G]}(\vartheta)$ la classe de $\text{Nrd}_{\mathbb{R}[G]}(A(\vartheta))$ dans $\zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times$. Plus explicitement, dans l'exemple 1 le régulateur de Dirichlet induit un isomorphisme de $\mathbb{R}[G]$ -modules

$$\begin{aligned} \lambda_{Dir} : \mathcal{O}_{K,\mathbb{R}}^\times &\longrightarrow X_{\mathbb{R}}, \\ u &\mapsto - \sum_{w \in S_\infty} \log |u|_w w, \end{aligned}$$

où X est le noyau de $\mathbb{Z}S_\infty \longrightarrow \mathbb{Z}, w \mapsto 1$, et nous obtenons un régulateur équivariant

$$R = (R_\chi)_{\chi \in \text{Irr}(G)} := \text{Nrd}_{\mathbb{R}[G]}(\lambda_{Dir}) \in \zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times.$$

Comme $\text{Nrd}_{\mathbb{R}[G]}(\vartheta^*) = \text{Nrd}_{\mathbb{R}[G]}(\vartheta)$ et comme ϑ^* est essentiellement λ_{Dir}^{-1} , la conjecture 5.1 prend la forme

$$\mathcal{L}^*/R \stackrel{?}{\in} \zeta(\mathbb{Q}[G])^\times,$$

où par abus de notation nous désignons par R un relèvement quelconque. On peut aussi démontrer que la conjecture 5.1 est équivalente à la conjecture de Stark comme formulée dans [27]. Pour une démonstration de ce résultat voir [11].

Dans l'exemple 2, il vient l'application $\vartheta = \lambda_{NT}^{-1} \oplus \alpha_M^{-1}$. Si l'on pose

$$\begin{aligned} \text{Reg} &= (\text{Reg}_\chi)_{\chi \in \text{Irr}(G)} := \text{Nrd}_{\mathbb{R}[G]}(\lambda_{NT}) \in \zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times, \\ \Omega &= (\Omega_\chi)_{\chi \in \text{Irr}(G)} := \text{Nrd}_{\mathbb{R}[G]}(\alpha_M) \in \zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times. \end{aligned}$$

la conjecture 5.1 prend la forme

$$\mathcal{L}^*/\text{Reg} \cdot \Omega \stackrel{?}{\in} \zeta(\mathbb{Q}[G])^\times,$$

où on utilise les mêmes conventions de notation que ci-dessus. C'est une forme équivariante de la conjecture de rationalité de BSD. Il y a des expressions très explicites pour le régulateur Reg et la période Ω dans [3, Sec. 4] et dans [2, Prop. 3.1].

L'idée naïve pour formuler une conjecture d'intégralité serait comme suit. On prend des $\mathbb{Z}[G]$ -modules canoniques dans les $\mathbb{Q}[G]$ -espaces, par exemple \mathcal{O}_K^\times dans $\mathcal{O}_K^\times \otimes_{\mathbb{Z}} \mathbb{Q}$ ou $E(K)$ dans $E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$, et on les utilise pour l'énoncé d'une conjecture d'intégralité. Par exemple, dans le cas des motifs de Tate une forme naïve serait peut-être

$$\hat{\delta}_1(\mathcal{L}^*) = [\mathcal{O}_K^\times, \lambda_{Dir}, X].$$

Mais cela ne marche pas parce que les modules ne sont pas projectifs. Par conséquent, l'élément de droite n'existe pas dans $K_0(\mathbb{Z}[G], \mathbb{R})$.

La conjecture ETNC est probablement la façon correcte de résoudre ce problème. Nous fixons un premier l avec le but de formuler une conjecture de l -intégralité (pour laquelle nous utilisons le sigle ETNC_l). En utilisant la théorie de la cohomologie étale on peut définir un complexe parfait

$$R\Gamma_{c,l} = R\Gamma_c(\mathbb{Z}[1/S_l], \mathcal{M}_l)$$

ayant les propriétés suivantes :

- $R\Gamma_{c,l}$ est parfait.
- $R\Gamma_{c,l}$ a les bons groupes de cohomologie.

On retrouve les $\mathbb{Z}[G]$ -modules, ou bien leurs complétés en l , qui sont intéressants d'un point de vue arithmétique (par exemple les unités \mathcal{O}_K^\times ou le groupe de Mordell-Weil $E(K)$), comme les groupes de cohomologie d'un complexe parfait. Malheureusement, la définition de $R\Gamma_{c,l}$ est assez compliquée (cf. [10, Sec. 3.3 - 3.4]), et nous ne la donnerons pas ici.

Notons par \mathbb{C}_l la complétion d'une clôture algébrique de \mathbb{Q}_l et fixons un plongement $j: \mathbb{R} \rightarrow \mathbb{C}_l$. Soit $j_*: \zeta(\mathbb{R}[G])^\times \rightarrow \zeta(\mathbb{C}_l[G])^\times$ induit par j et soit

$$\vartheta_l: H^{\text{pair}}(R\Gamma_{c,l}) \otimes_{\mathbb{Z}_l} \mathbb{C}_l \rightarrow H^{\text{impair}}(R\Gamma_{c,l}) \otimes_{\mathbb{Z}_l} \mathbb{C}_l$$

l'isomorphisme de $\mathbb{C}_l[G]$ -modules induit par ϑ et j . La construction analogue à celle de la Section 3 donne une caractéristique d'Euler

$$\chi_{\mathbb{Z}_l[G], \mathbb{C}_l}(R\Gamma_{c,l}, \vartheta_j) \in K_0(\mathbb{Z}_l[G], \mathbb{C}_l).$$

Soit $\hat{\vartheta}_{1,l}: \zeta(\mathbb{C}_l[G])^\times \rightarrow K_0(\mathbb{Z}_l[G], \mathbb{C}_l)$ l'application analogue à $\hat{\vartheta}_1$ dans (3). Nous pouvons finalement énoncer la conjecture ETNC $_l$.

Conjecture 5.2. — Pour tout premier l , on a

$$\hat{\vartheta}_{1,l}(j_*(\mathcal{L}^*)) = \chi_{\mathbb{Z}_l[G], \mathbb{C}_l}(R\Gamma_{c,l}, \vartheta_j)$$

dans $K_0(\mathbb{Z}_l[G], \mathbb{C}_l)$.

Si nous supposons la conjecture de rationalité, alors pour tout premier l on a une égalité dans $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$.

En général, on ne dispose pas d'une description explicite du complexe $R\Gamma_{c,l}$. Mais pour les motifs de Tate il existe un lien avec les suites de Tate qui rend une construction un peu plus explicite de $R\Gamma_{c,l}$. Rappelons très brièvement les suites de Tate.

Soit K/k une extension galoisienne de corps de nombres et soit $G = \text{Gal}(K/k)$. Pour un ensemble S fini de places de k on note par $S(K)$ l'ensemble des places de K au-dessus des places de S . Soit $\mathcal{O}_{K,S}$ l'anneau des $S(K)$ -entiers de K et soit $\text{cl}_S(K)$ le groupe des classes d'idéaux de $\mathcal{O}_{K,S}$. Soit X_S le noyau de $\mathbb{Z}S(K) \rightarrow \mathbb{Z}$, $w \mapsto 1$.

On dit que S est admissible si $\text{cl}_S(K) = 1$ et si S contient les places archimédiennes ainsi que les places qui se ramifient dans K/k .

Rappelons que Tate a défini une classe dans $\text{Ext}_{\mathbb{Z}[G]}^2(X_S, \mathcal{O}_{K,S}^\times)$, appelée classe canonique de Tate, qui est fournie par la théorie locale et globale du corps de classes.

Théorème 5.3. — (Tate [26]) Soit K/k une extension galoisienne de corps de nombres avec $G = \text{Gal}(K/k)$. Soit S un ensemble de places de k admissible. Alors il existe une suite exacte

$$0 \rightarrow \mathcal{O}_{K,S}^\times \rightarrow A_S \rightarrow B_S \rightarrow X_S \rightarrow 0$$

avec des modules parfaits A_S, B_S représentant la classe canonique de Tate.

Soit T_l^\bullet le complexe $[A_{S,l} \rightarrow B_{S,l}]$ où les modules sont concentrés en les degrés 0 et 1. Alors on a

Théorème 5.4. — (Burns/Flach [9, Prop. 3.5]) Pour les motifs de Tate $M = h^0(\mathbb{Q})_K$ le complexe $R\Gamma_{c,l}$ est quasi-isomorphe à T_l^\bullet .

Par conséquent, on peut utiliser le complexe T_l^\bullet pour la construction de la caractéristique d'Euler $\chi_{\mathbb{Z}_l[G], \mathbb{C}_l}(R\Gamma_{c,l}, \vartheta_j)$. Bien que les suites de Tate ne soient pas suffisamment explicites non plus, on a ici plus d'information que dans le cas des courbes elliptiques. Comme noté par exemple dans l'article [20] cela rend ETNC un peu plus explicite.

6. ETNC dans le cas des courbes elliptiques

Dans ce paragraphe, nous nous proposons de rendre encore plus explicite la conjecture ETNC dans le cas des courbes elliptiques. En utilisant ces résultats on peut calculer des exemples numériques comme celui que nous décrirons dans la Section 6.3. En plus, sous des hypothèses très fortes, on aura dans la Section 6.4 quelques résultats théoriques démontrant ETNC $_l$ pour une infinité de l -extensions K/\mathbb{Q} abéliennes.

6.1. Conjecture de rationalité. — Pour commencer, nous donnons les constructions explicites du régulateur équivariant Reg et de la période équivariante Ω .

D'abord, on décrit la période équivariante. Soit ω_0 une forme différentielle de Néron et soient γ_+ and γ_- des \mathbb{Z} -générateurs de $H_1(E(\mathbb{C}), \mathbb{Z})^+$ et $H_1(E(\mathbb{C}), \mathbb{Z})^-$, respectivement. On définit

$$\Omega_+ := \int_{\gamma_+} \omega_0, \quad \Omega_- := \int_{\gamma_-} \omega_0.$$

Soit $\alpha_0 \in K$ un générateur d'une base normale de K/\mathbb{Q} . Fixons un plongement $\iota : K \hookrightarrow \mathbb{C}$ et définissons $\tau \in G$ par $c \circ \iota = \iota \circ \tau$, où c est la conjugaison complexe. Comme dans la Proposition 3.1 de [2] on pose

$$\lambda_{\alpha_0} := \left(\Omega_+ \frac{1+\tau}{2} + \Omega_- \frac{1-\tau}{2} \right) \left(\sum_{\sigma \in G} (\iota \circ \sigma)(\alpha_0) \sigma^{-1} \right)^{-1}$$

et on définit

$$\Omega := \text{Nrd}_{\mathbb{R}[G]}(\lambda_{\alpha_0}) \in \zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times.$$

Il est facile de démontrer que Ω ne dépend pas du choix de α_0 .

Le régulateur équivariant Reg est défini comme dans [2, Rem. 2.6(b)] avec

$$Y^{ev} = E(K)_{\mathbb{Q}}, \quad Y^{od} = E(K)_{\mathbb{Q}}^* \quad \text{et} \quad \theta_{\mathbb{R}} = \lambda_{NT}.$$

Nous présentons ici une définition équivalente qui est un peu plus constructive. On choisit d'abord une $\mathbb{Q}[G]$ -résolution libre de $E(K)_{\mathbb{Q}}^*$,

$$\mathbb{Q}[G]^{n_0} \xrightarrow{\alpha} \mathbb{Q}[G]^{n_1} \xrightarrow{\pi} E(K)_{\mathbb{Q}}^* \longrightarrow 0$$

et on pose $Z := \ker(\alpha)$. Soit $\varphi : Z \longrightarrow E(K)_{\mathbb{Q}}$ un $\mathbb{Q}[G]$ -homomorphisme quelconque. En augmentant éventuellement n_0 on peut supposer que l'application φ est surjective. Si on pose

$\mathcal{K}_\varphi := \ker(\varphi)$, on obtient le diagramme suivant

$$(8) \quad \begin{array}{ccccccccc} & & \mathcal{K}_\varphi & \xrightarrow{=} & \mathcal{K}_\varphi & & & & \\ & & \downarrow & & \downarrow & & & & \\ 0 & \longrightarrow & Z & \xrightarrow{\iota} & F^0 & \xrightarrow{\alpha} & F^1 & \xrightarrow{\pi} & E(K)_\mathbb{Q}^* \longrightarrow 0 \\ & & \downarrow \varphi & & \searrow & \nearrow & \downarrow = & & \downarrow = \\ & & & & & W & & & \\ & & & & \swarrow & \searrow & \downarrow = & & \downarrow = \\ 0 & \longrightarrow & E(K)_\mathbb{Q} & \longrightarrow & A & \longrightarrow & F^1 & \xrightarrow{\pi} & E(K)_\mathbb{Q}^* \longrightarrow 0 \end{array}$$

où $F^0 := \mathbb{Q}[G]^{n_0}$, $F^1 := \mathbb{Q}[G]^{n_1}$, $W := \ker(\pi)$ et où A désigne le “pushout” le long de ι et φ . Soit maintenant $\lambda_{NT}(\varphi)_{triv}$ le composé

$$(9) \quad \begin{array}{l} F_{\mathbb{R}}^0 \xrightarrow{\sigma_1} Z_{\mathbb{R}} \oplus W_{\mathbb{R}} \xrightarrow{\sigma_2} \mathcal{K}_{\varphi, \mathbb{R}} \oplus E(K)_{\mathbb{R}} \oplus W_{\mathbb{R}} \\ \xrightarrow{\sigma_3} \mathcal{K}_{\varphi, \mathbb{R}} \oplus E(K)_{\mathbb{R}}^* \oplus W_{\mathbb{R}} \xrightarrow{\sigma_4} \mathcal{K}_{\varphi, \mathbb{R}} \oplus F_{\mathbb{R}}^1, \end{array}$$

où $\sigma_1, \sigma_2, \sigma_4$ sont induites par le choix des applications scindées de

$$\begin{array}{l} 0 \longrightarrow Z_{\mathbb{R}} \xrightarrow{\iota} F_{\mathbb{R}}^0 \longrightarrow W_{\mathbb{R}} \longrightarrow 0, \\ 0 \longrightarrow \mathcal{K}_{\varphi, \mathbb{R}} \longrightarrow Z_{\mathbb{R}} \xrightarrow{\varphi} E(K)_{\mathbb{R}} \longrightarrow 0, \\ 0 \longrightarrow W_{\mathbb{R}} \longrightarrow F_{\mathbb{R}}^1 \xrightarrow{\pi} E(K)_{\mathbb{R}}^* \longrightarrow 0, \end{array}$$

respectivement, et où finalement σ_3 est induit par λ_{NT} .

Le $\mathbb{Q}[G]$ -module \mathcal{K}_φ est libre sur $\mathbb{Q}[G]$. Choisissons des $\mathbb{Q}[G]$ -bases de F^0 et $\mathcal{K}_\varphi \oplus F^1$. En représentant $\lambda_{NT}(\varphi)_{triv}$ par rapport à ces bases nous obtenons une matrice $A_\varphi \in \text{Gl}_{n_0}(\mathbb{R}[G])$, et finalement posons

$$\text{Reg} := \text{Nrd}_{\mathbb{R}[G]}(A_\varphi) \cdot \zeta(\mathbb{Q}[G])^\times \in \zeta(\mathbb{R}[G])^\times / \zeta(\mathbb{Q}[G])^\times.$$

On peut démontrer que Reg est bien défini et que cette définition coïncide avec celle de [2, Rem. 2.6(b)].

Par abus de notation écrivons également Reg , respectivement Ω , pour un relèvement quelconque à $\zeta(\mathbb{R}[G])^\times$. Posons $u := \frac{\mathcal{L}^*}{\Omega \text{Reg}} \in \zeta(\mathbb{R}[G])^\times$ et remarquons que u est bien défini modulo $\zeta(\mathbb{Q}[G])^\times$. Si l'on écrit $\text{ETNC}_\mathbb{Q}$ pour la partie de rationalité de ETNC , c'est-à-dire pour la conjecture 5.1, alors il vient la formulation explicite

$$(10) \quad \text{ETNC}_\mathbb{Q} \text{ est vraie} \iff u \in \zeta(\mathbb{Q}[G])^\times.$$

6.2. Conjecture d'intégralité. — L'idée naïve pour formuler la conjecture ETNC_l consisterait à remplacer le choix de $\mathbb{Q}[G]$ -base par le choix de $\mathbb{Z}_l[G]$ -base. Evidemment c'est beaucoup trop naïf parce qu'on sait bien du cas classique non-équivariant que le groupe $\text{III}(E/K)$, que les modules locaux qui donnent les facteurs de Tamagawa et aussi que la torsion de $E(K)$

doivent intervenir dans la conjecture. Mais même pour la définition d'un régulateur équivariant l -intégral l'approche décrite dans la Section 6.1 ne marche pas parce que le régulateur dépendrait du choix de l'application φ . Plus précisément, on obtient un régulateur

$$\text{Reg}_l(\varphi) \in \zeta(\mathbb{C}_l[G])^\times / \text{Nrd}_{\mathbb{C}_l[G]}(\mathbb{Z}_l[G]^\times)$$

qui dépend de

$$\varphi \in \frac{\text{Hom}_{\mathbb{Z}_l[G]}(Z, E(K)_{tf,l})}{\iota^*(\text{Hom}_{\mathbb{Z}_l[G]}(F^0, E(K)_{tf,l}))} \simeq \text{Ext}_{\mathbb{Z}_l[G]}(E(K)_l^*, E(K)_{tf,l}).$$

Pour plus de détails et un cas spécial où tous les calculs sont accomplis le lecteur peut consulter [3, Sec. 4].

Pour la suite, nous introduisons des hypothèses qui nous permettent de travailler exclusivement avec la cohomologie du complexe $R\Gamma_{c,l}$.

Soit $S_{bad}(E)$ l'ensemble des premiers où la courbe E a mauvaise réduction, et soit $S_{ram}(K/\mathbb{Q})$ l'ensemble des premiers où l'extension K/\mathbb{Q} est ramifiée. On pose $S := S_{bad}(E) \cup S_{ram}(K/\mathbb{Q})$.

Hypothèses :

(H0) $\text{III}(E/K)$ est fini.

(H1) $l \neq 2$ et $l \notin S$.

(H2) $l \nmid \bar{I}_p$ pour tout $p \in S$.

(H3) $S_{bad}(E) \cap S_{ram}(K/\mathbb{Q}) = \emptyset$.

(H4) Si $l \mid \#G$, alors

(a) $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l, (E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*$ sont $\mathbb{Z}_l[G]$ -parfaits et $l \nmid \#E(K)_{tors}$.

(b) $l \nmid \#\text{III}(E/K)$.

(H5) $l \nmid \#(E(K_v)/E_0(K_v))$ pour tout $v \in S(K)$.

Dans (H5), K_v désigne la complétion de K en v , $E(K_v)$ est le groupe des points K_v -rationnels et $E_0(K_v)$ le sous-groupe des points ayant bonne réduction en v .

Si T est un $\mathbb{Z}_l[G]$ -module parfait et fini, écrivons $\tilde{\chi}_{\mathbb{Z}_l[G], \mathbb{C}_l}(T, 0)$ pour un relèvement quelconque de $\chi_{\mathbb{Z}_l[G], \mathbb{C}_l}(T[0], 0)$.

D'après nos hypothèses, $\text{Ext}_{\mathbb{Z}_l[G]}(E(K)_l^*, E(K)_{tf,l})$ est trivial et nous disposons d'un régulateur $\text{Reg}_l \in \zeta(\mathbb{C}_l[G])^\times / \text{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times)$.

Dans la définition d'une période équivariante l -intégrale Ω_l il faut choisir un élément α_0 tel que $\mathcal{O}_{K,(l)} = \mathbb{Z}_{(l)}[G]\alpha_0$ (ici l'indice (l) indiquant la localisation). Posons

$$u_l := \frac{\mathcal{L}^*}{\Omega_l \text{Reg}_l} \in \zeta(\mathbb{C}_l[G])^\times / \text{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times).$$

Théorème 6.1. — *Supposons les hypothèses (H0) - (H5) vérifiées. Supposons aussi la conjecture de rationalité vraie. Si l'on pose*

$$\xi_l := \tilde{\chi}(E(K)_{l^\infty}, 0)^{-1} \cdot \tilde{\chi}(E(K)_{l^\infty}^\vee, 0)^{-1} \cdot \tilde{\chi}(\text{III}(E/K)_{l^\infty}, 0),$$

alors on a

$$(11) \quad ETNC_l \text{ est vraie} \iff u_l \xi_l^{-1} \equiv 1 \pmod{\text{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times)}$$

Nous remarquons que $\text{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times) = \mathcal{O}_{C,l}^\times$ si $l \nmid \#G$. Alors ETNC_l est vraie, si et seulement si $u_l \xi_l^{-1}$ est une unité l -adique de \mathcal{O}_C . Par contre, si $l \mid \#G$, ETNC_l est vraie si et seulement si $u_l \xi_l^{-1}$ est une unité l -adique qui, en plus, satisfait des congruences explicites pour lesquelles nous avons donné des exemples dans 2.7.

Pour un résultat un peu plus général que le théorème 6.1 le lecteur est renvoyé à [2, Prop. 4.4]. Dans celui-ci, nous avons utilisé le théorème 6.1 pour calculer des exemples numériques. Décrivons en un. Les calculs ont été effectués avec le logiciel MAGMA.

6.3. Un exemple numérique. — Soit $E : y^2 + xy = x^3 - x^2 + 4x - 3$. C'est une courbe elliptique de conducteur $N_E = 73$. Dans la notation de Cremona c'est la courbe 73A1. Soit $F = \mathbb{Q}(\sqrt{401})$ et K le corps de classes de Hilbert de F . On a $h_F = 5$ et K/\mathbb{Q} est une extension galoisienne de groupe $G \simeq D_{10}$, le groupe diédral d'ordre 10. Avec MAGMA on trouve facilement un polynôme irréductible pour K/\mathbb{Q} , par exemple,

$$f(x) = x^{10} - 2x^9 - 20x^8 + 2x^7 + 69x^6 - x^5 - 69x^4 + 2x^3 + 20x^2 - 2x - 1.$$

On a $d_{K/\mathbb{Q}} = 401^5$ et $S = \{73, 401\}$. Comme nous l'avons expliqué dans l'exemple 2.7(2) la table des caractères absolument irréductibles de D_{10} est donnée par (on note le changement de notation),

	id	τ	σ	σ^2
χ_1	1	1	1	1
χ_2	1	-1	1	1
χ_3	2	0	$\zeta_5 + \zeta_5^{-1}$	$\zeta_5^2 + \zeta_5^{-2}$
χ_4	2	0	$\zeta_5^2 + \zeta_5^{-2}$	$\zeta_5 + \zeta_5^{-1}$

Le calcul des valeurs des fonctions L , effectué avec l'implémentation de T. Dokchitser dans MAGMA (cf. aussi [16]), donne

$$\text{ord}_{s=1}(L(E/\mathbb{Q}, \chi_i, s)) = 0 \text{ pour } i = 1, 2, 3, 4.$$

D'après [15, Th. 3.7] (démontrée indépendamment par Longo et Tian-Zhang) on a

$$E(K) = E(K)_{tors} = E(\mathbb{Q})_{tors}.$$

Considérons d'abord la conjecture de rationalité. Les valeurs numériques des fonctions L ont été calculées avec une précision de 20 chiffres. On n'en donne que 6,

$$(L(E/\mathbb{Q}, \chi, 1))_{\chi \in \text{Irr}_{\mathbb{Q}}(G)} = (1.18266, 2.12613, 0.163048, 7.659819).$$

Les calculs de la période équivariante Ω donnent pour $u = \mathcal{L}^*/\Omega$

$$u = (0.499999, 18.0000, 0.583592, 27.4164).$$

Remarquons que ces valeurs dépendent du choix d'une base normale α_0 . Pour obtenir des valeurs avec des petits dénominateurs on choisit favorablement un générateur de base normale intégrale. C'est ce que nous avons fait en appliquant l'algorithme de [5].

Numériquement on vérifie la conjecture de rationalité parce que u est proche de

$$(1/2, 18, -12\beta + 8, 12\beta + 20)$$

et $\varphi(-12\beta + 8) = 12\beta + 20$, où $\langle \varphi \rangle = \text{Gal}(\mathbb{Q}(\zeta_5)^+/\mathbb{Q})$. Le polynôme minimal de $-12\beta + 8$ est $x^2 - 28x + 16$.

Lorsqu'on suppose BSD pour E/K on peut calculer l'ordre conjectural du groupe de Tate-Shafarevic :

$$\#\text{III}(E/K) = 2^8 3^2.$$

On peut s'assurer que les hypothèses (H) sont satisfaites pour tous les premiers $l \neq 2, 3$ (cf. [2, Ex. 6.2] pour plus de détails). Alors on peut vérifier ETNC_l pour tous les premiers $l \neq 2, 3$ modulo la précision du calcul (parce que nous n'obtenons pas une démonstration de la conjecture de rationalité) et l'ordre conjectural du groupe de Tate-Shafarevic.

Le nombre premier le plus intéressant est $l = 5$. On a

$$\eta := u\xi_5^{-1} = (1/2, 18, -12\beta + 8)$$

et par l'exemple 2.7(2) on doit vérifier la congruence

$$\eta_0\eta_1 \equiv \eta_2 \pmod{(1 - \zeta_5)},$$

qui est effectivement satisfaite.

6.4. Conjecture d'intégralité en $l \mid \#G$. — Le but de cette partie de l'article est de décrire l'approche de [3] pour obtenir des résultats d'intégralité dans le cas où l divise l'ordre du groupe G et où $\text{rg}(E(K))$ n'est pas trivial. Pour plus de détails le lecteur peut consulter [3].

Désormais nous travaillerons avec des hypothèses motivées par le travail de D. Burns qui dans [13] a introduit des conditions similaires.

Hypothèses :

(B0) $\text{III}(E/K)$ est fini.

(B1) $[K : \mathbb{Q}] = l^n$, $G = \langle g_0 \rangle$, $l \neq 2$,

(B2) l ne divise pas d_K , N_E , $\#E(\mathbb{Q})_{\text{tors}}$, $\#\bar{E}_{\text{ns}}(\mathbb{F}_p)$ pour $p \mid d_K$, et $\#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p))$ pour $p \mid N_E$.

(B3) $(d_K, N_E) = 1$.

(B4) l ne divise pas $\#\text{III}(E/K)$.

(B5) $\text{rk}_{\mathbb{Z}}E(K) = \text{rk}_{\mathbb{Z}}E(\mathbb{Q})$.

Sous ces hypothèses l'élément ξ_l du théorème 6.1 change un peu. On a la même conclusion avec

$$\xi_l = \prod_{p \mid d_K} (L_p(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \text{Irr}(G)}^{-1},$$

et comme $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ n'est plus projectif sur $\mathbb{Z}_l[G]$, le calcul du régulateur change aussi. Sous nos hypothèses on peut démontrer qu'il existe une suite exacte de la forme

$$0 \longrightarrow E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l \longrightarrow A \longrightarrow B \longrightarrow (E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^* \longrightarrow 0$$

telle que

– le complexe $C^\bullet := [A \longrightarrow B]$ est parfait (où les modules sont placés en les degrés 0 et 1).

– le régulateur équivariant est donné par $\chi_{\mathbb{Z}_l[G], C_1}(C^\bullet, \lambda_{NT})$.

Posons $H_l^0 := E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ et $H_l^1 := (E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*$ et rappelons que la caractéristique d'Euler dépend de la classe de la suite exacte ci-dessus dans $\text{Ext}_{\mathbb{Z}_l[G]}^2(H_l^1, H_l^0)$. Le problème qui se pose est que nous n'avons aucune information explicite sur cette classe.

Pour cette raison nous suivons la stratégie suivante. Nous calculons une suite exacte comme ci-dessus pour toutes les classes parfaites dans $\text{Ext}_{\mathbb{Z}_l[G]}^2(H_l^1, H_l^0)$ et vérifions ETNC_l pour toute suite exacte ainsi obtenue.

Nous posons $N_G := \sum_{g \in G} g$ et considérons la suite exacte standard

$$(12) \quad 0 \longrightarrow \mathbb{Z}_l \xrightarrow{\eta} \mathbb{Z}_l[G] \xrightarrow{g_0-1} \mathbb{Z}_l[G] \xrightarrow{\text{aug}} \mathbb{Z}_l \longrightarrow 0$$

où $\eta(1) := N_G$ et $\text{aug}(g) = 1$ pour tout $g \in G$.

On prend r copies de la suite (12) et on l'utilise pour calculer $\text{Ext}_{\mathbb{Z}_l[G]}^2(H_l^1, H_l^0)$. Pour toute application $\varphi \in \text{Hom}_{\mathbb{Z}_l[G]}(\mathbb{Z}_l^r, \mathbb{Z}_l^r)$ nous obtenons un diagramme commutatif de la forme

$$(13) \quad \begin{array}{ccccccc} & & & & H_l^1 & & \\ & & & & \downarrow \simeq & & \\ 0 & \longrightarrow & \mathbb{Z}_l^r & \xrightarrow{\iota} & \mathbb{Z}_l[G]^r \oplus^{(g_0-1)} & \mathbb{Z}_l[G]^r \oplus^{\text{aug}} & \mathbb{Z}_l^r \longrightarrow 0 \\ & & \downarrow \varphi & & \downarrow = & & \downarrow = \\ 0 & \longrightarrow & \mathbb{Z}_l^r & \longrightarrow & A(\varphi) & \longrightarrow & \mathbb{Z}_l[G]^r \longrightarrow \mathbb{Z}_l^r \longrightarrow 0 \\ & & \downarrow \simeq & & & & \\ & & H_l^0 & & & & \end{array}$$

Ici $\iota = \oplus \eta$ et $A(\varphi)$ désigne le "pushout" le long de ι et φ . On sait que les suites exactes en bas parcourent toutes les classes de $\text{Ext}_{\mathbb{Z}_l[G]}^2(H_l^1, H_l^0)$ si φ parcourt un système de représentants de

$$\frac{\text{Hom}_{\mathbb{Z}_l[G]}(\mathbb{Z}_l^r, \mathbb{Z}_l^r)}{\iota^*(\text{Hom}_{\mathbb{Z}_l[G]}(\mathbb{Z}_l[G]^r, \mathbb{Z}_l^r))}.$$

De plus, le complexe $[A(\varphi) \longrightarrow \mathbb{Z}_l[G]^r]$ est parfait si et seulement si $l \nmid \det_{\mathbb{Z}_l}(\varphi)$.

Alors pour toute application φ nous obtenons un régulateur équivariant que nous notons $\text{Reg}_l(\varphi) = (\text{Reg}_{l,\chi}(\varphi))_{\chi \in \text{Irr}(G)}$. Soit e_1, \dots, e_r la base standard de \mathbb{Z}_l^r et $\Phi \in \text{GL}_r(\mathbb{Z}_l)$ la matrice représentant φ par rapport à cette base. Soient P_1, \dots, P_r une \mathbb{Z} -base de $E(K)_{tf}$ et $\Psi := (\langle P_i, P_j \rangle_{NT})_{1 \leq i, j \leq r} \in \text{GL}_r(\mathbb{R})$.

Un calcul élémentaire montre (cf. [3, Sec. 4])

$$\text{Reg}_{l,\chi}(\varphi) = \begin{cases} (\chi(g_0) - 1)^r, & \text{si } \chi \text{ est non-trivial,} \\ \frac{1}{(\#G)^r} \det(\Psi) \det(\Phi), & \text{si } \chi \text{ est trivial.} \end{cases}$$

Posons

$$u_l(\varphi) := \frac{\mathcal{L}^*}{\Omega_l \text{Reg}_l(\varphi)} = \frac{\mathcal{L}^*}{\Omega_l \text{Reg}_l(\text{id})} \cdot \frac{1}{E(\varphi)}$$

avec

$$(14) \quad E(\varphi) = (E_\chi(\varphi))_{\chi \in \text{Irr}(G)}, \quad E_\chi(\varphi) = \begin{cases} 1, & \text{si } \chi \text{ est non-trivial,} \\ \det(\Phi), & \text{si } \chi \text{ est trivial,} \end{cases}$$

et rappelons qu'il faut calculer Ω_l par rapport à une $\mathbb{Z}_l[G]$ -base α_0 de $\mathcal{O}_{K,l}$.

Soit $\varepsilon_0 \in \text{Ext}_{\mathbb{Z}_l[G]}^2(H_l^1, H_l^0)$ la classe correspondant à la suite exacte correcte, c'est-à-dire, la suite exacte qui est définie par $R\Gamma_{c,l}$ (cf. [3, Sec. 4]). Soit $\varphi_0 : \mathbb{Z}_l^r \rightarrow \mathbb{Z}_l^r$ une application représentant ε_0 si on calcule $\text{Ext}_{\mathbb{Z}_l[G]}^2(H_l^1, H_l^0)$ par la suite en haut du diagramme (13). On obtient

$$(15) \quad \text{ETNC}_l \text{ est valide} \iff u_l(\varphi_0)\xi_l^{-1} \in \text{Nrd}(\mathbb{Z}_l[G]^\times).$$

Soit

$$\delta_l : \zeta(\mathbb{C}_l[G]^\times / \text{Nrd}_{\mathbb{C}_l[G]}(\mathbb{Z}_l[G]^\times)) \rightarrow K_0(\mathbb{Z}_l[G], \mathbb{C}_l)$$

l'isomorphisme canonique (cf. [6, Th. 2.3(ii)]).

Définition 6.2. — Posons

$$\mathcal{E} := \{ \delta_l(E(\varphi)) \mid \varphi \text{ comme ci-dessus} \}.$$

On peut démontrer que \mathcal{E} est un sous-groupe de $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$. En résumé, nous avons

Théorème 6.3. — *Supposons les hypothèses (B0) - (B5) vérifiées. Alors les assertions suivantes (i), (ii) et (iii) sont équivalentes, où*

(i) *ETNC_l est valide modulo \mathcal{E} .*

(ii) $\mathcal{E} = \{ \delta_l(u_l(\varphi)\xi_l^{-1}) \mid \varphi \text{ comme ci-dessus} \}$.

(iii) $\delta_l(u_l(id)\xi_l^{-1}) \in \mathcal{E}$.

Dans [3] nous avons utilisé le théorème 6.3 pour vérifier ETNC_l numériquement pour beaucoup d'exemples. Signalons aussi que le sous-groupe \mathcal{E} est beaucoup plus petit que le groupe de torsion de $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$. On a

$$\#K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} = (l-1)^n l^{\frac{l^n-1}{l-1}-n} \gg l^{n-1}(l-1) = \#\mathcal{E}.$$

6.5. Conjecture d'intégralité et symboles modulaires. — Finalement nous esquissons un cas très spécial où l'on peut démontrer ETNC_l. On suppose les hypothèses (B) et, en plus, on renforce (B5) en exigeant que $\text{rg}(E(K)) = 0$. Ces résultats se trouvent dans [4].

Sous ces hypothèses le régulateur est trivial et on rappelle que

$$u_{l,\chi} = \frac{L^*(E/\mathbb{Q}, \bar{\chi}, 1)R_\chi}{\Omega_+}$$

avec la résolvante $R_\chi = R_\chi(\alpha_0) = \sum_{\sigma \in G} \sigma(\alpha_0)\chi(\sigma^{-1})$.

Comme G est abélien on a $\text{Nrd}_{\mathbb{Q}_l[G]}(\mathbb{Z}_l[G]^\times) = \mathbb{Z}_l[G]^\times$. Ainsi on doit démontrer que $u_l\xi_l^{-1} \in \mathbb{Z}_l[G]^\times$.

On dénote par f le conducteur de K et par f_χ le conducteur d'un caractère χ de Dirichlet. Soit $G_f = \text{Gal}(\mathbb{Q}(\zeta_f)^+/\mathbb{Q})$ et soit la somme de Gauss

$$\tau(\chi) = \sum_{a \in (\mathbb{Z}/f\mathbb{Z})^\times} \chi(a)e^{2\pi ia/f}.$$

En utilisant la théorie des symboles modulaires, Mazur et Tate dans [22] ont construit un élément $\Theta^{MT} \in \mathbb{Z}_l[G_f]$ tel que

$$\chi(\Theta^{MT}) = c \frac{f}{f_\chi} \frac{\tau(\chi)L_f(E/\mathbb{Q}, \chi, 1)}{c_\infty \Omega_+},$$

où $L_f(E/\mathbb{Q}, \bar{\chi}, 1)$ dénote la fonction L de Hasse-Weil tordue sans les facteurs d'Euler pour $p \mid f$, c est la constante de Manin et c_∞ est le nombre de composantes de $E(\mathbb{R})$.

En posant $\alpha_0 := \text{Tr}_{\mathbb{Q}(\zeta_f)/K}(\zeta_f)$ on obtient la relation fondamentale

$$(16) \quad \bar{\chi}(\Theta_f^{MT}) = \frac{c}{c_\infty} \frac{f}{f_\chi} u_\chi \xi_{l,\chi}^{-1}.$$

On peut énoncer le théorème suivant :

Théorème 6.4. — *Soit K/\mathbb{Q} une extension abélienne et soit E/\mathbb{Q} une courbe elliptique satisfaisant les hypothèses (B) avec $\text{rg}(E(K)) = 0$. On suppose que $l \nmid c\#\text{III}(E/\mathbb{Q})$ et que la l -partie de BSD est vraie pour E/\mathbb{Q} . Alors la conjecture ETNC $_l$ est vraie.*

On remarque que grâce aux travaux de Gross/Zagier et de Kolyvagin on sait que pour toute courbe elliptique E/\mathbb{Q} telle que $L(E/\mathbb{Q}, 1) \neq 0$, il existe une infinité de premiers l tel que $l \nmid c\#\text{III}(E/\mathbb{Q})$ et BSD $_l$ est valide pour E/\mathbb{Q} .

En généralisant des résultats de [19] on peut démontrer le

Théorème 6.5. — *Soit E/\mathbb{Q} une courbe elliptique telle que $L(E/\mathbb{Q}, 1) \neq 0$. Alors il existe une infinité de premiers l tel que BSD $_l$ est valide pour E/\mathbb{Q} et pour de tel nombre premier l , il existe une infinité d'extensions K/\mathbb{Q} telles que les hypothèses (B) soient satisfaites avec $\text{rg}(E(K)) = 0$.*

Références

- [1] H. Bass, J. Milnor, J.-P. Serre, *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*, Publ. Math. Hautes Études Sci. **33** (1967), 59–137.
- [2] W. Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture*, Exp.Math. **20** (4), (2011) 426 - 456.
- [3] W. Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (part II)*, Preprint 2010, à paraître dans Math. Comp.
- [4] W. Bley, *The equivariant Tamagawa number conjecture and modular symbols*, Preprint 2011.
- [5] W. Bley, H. Johnston, *Computing generators of free modules over orders in group algebras*, J.Algebra (Computational Section) **320** (2008), 836–852.
- [6] W. Bley, S. M.J. Wilson, *Computations in relative algebraic K-groups*, LMS JCM **12** (2009), 166–194.
- [7] M. Breuning, D. Burns, *Leading terms of Artin L-functions at $s = 0$ and $s = 1$* , Compositio Math. **143** (2007), 1427-1464.
- [8] D. Burns, M. Flach, *Motivic L-functions and Galois module structures*, Math. Ann. **305** (1996) 65-102.
- [9] D. Burns, M. Flach, *On Galois structure invariants associated to Tate motives*, Amer. J. Math. **120** (1998) 1343-1397.
- [10] D. Burns, M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Documenta Math. **6** (2001) 501-570.
- [11] D. Burns, *Equivariant Tamagawa numbers and Galois module theory I*, Compositio Math. **129** (2001), 203–237.

- [12] D. Burns, *Equivariant Whitehead torsion and refined Euler characteristics*, CRM Proceedings and Lecture Notes, vol. 36 (American Mathematical Society, Providence, RI, 2004), 35-59. Whitehead.
- [13] D. Burns, *On leading terms and values of equivariant motivic L-functions*, Pure App. Math. Q. **6** (John Tate Special Issue, Part II) (2010) 83-172.
- [14] C. CURTIS, I. REINER : *Methods of representation theory*, volume I and II. Wiley, 1981 and 1987.
- [15] H. Darmon, *Heegner points, Stark-Heegner points and values of L-series*, International Congress of Mathematicians. Vol.II, 313–345, Eur. Math. Soc., Zürich, 2006.
- [16] T. Dokchitser, *Computing Special Values of Motivic L-Functions*, Experiment. Math. **13** (2004), 137–149.
- [17] M. Flach, *The equivariant Tamagawa number conjecture - A survey*, in : ‘Stark’s Conjecture : recent progress and new directions’ (eds. D.Burns, C.Popescu, J.Sands and D.Solomon), Contemp. Math. **358** Amer. Math. Soc.,(2004) 79-126.
- [18] M. Flach, *Iwasawa theory and motivic L-functions*, Pure and Applied Mathematics Quaterly **5**, Number 1, (2009) 255-294.
- [19] J. Fearnley, H. Kisilevsky, M. Kuwata, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, preprint 2008.
- [20] C. Greither, *Introduction à la conjecture ETNC et application*, Publ. Math. de Besançon (2012), 55–73.
- [21] G. Kings, *An introduction to the equivariant Tamagawa number conjecture : the relation to the Birch-Swinnerton-Dyer conjecture*, Preprint Nr. 26/2009, Universität Regensburg.
- [22] B. MAZUR, J. TATE : *Refined Conjectures of the Birch and Swinnerton-Dyer Type* , Duke Math.J., **54** (1987), 711–750.
- [23] J. Milnor, *Introduction to Algebraic K-theory*, Annals of Mathematics Studies Number 72, Princeton University Press, Princeton, New Jersey (1971).
- [24] T. Nakayama, *On modules of trivial cohomology over a finite group. II. Finitely generated modules*, Nagoya Math. J. **12**, (1957) 171–176.
- [25] J. ROSENBERG : *Algebraic K-Theory and Its Applications*, Springer, 1994.
- [26] J. Tate, *The cohomology groups of tori in finite Galois extensions of number fields*, Nagoya Math. J. **27** (1966) 709-719.
- [27] J. Tate, *Les Conjectures de Stark sur les Fonctions L d’Artin en $s = 0$* , Progress in Math. **47**, Birkhäuser 1984.
- [28] T. Nguyen Quang Do, *Théorie d’Iwasawa non-commutative*, Publ. Math. de Besançon (2012), 75–104.
- [29] O. Venjakob, *From the Birch and Swinnerton-Dyer Conjecture over the Equivariant Tamagawa Number Conjecture to non-commutative Iwasawa theory*, in L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge 2007, 333- 380.

01 juillet 2011

WERNER BLEY, Mathematisches Institut der Universität München, Theresienstr. 39, 80333 München, Germany • E-mail : bley@math.lmu.de