Synthèse des travaux présentés en vue de l'habilitation à diriger des recherches

présentée par

Jean Gillibert

Prolongement de torseurs : approche via la cohomologie log plate et applications arithmétiques

Soutenue le 31 mai 2013, devant un jury composé de :

Daniel BERTRAND, professeur à l'université Pierre et Marie Curie.

Philippe CASSOU-NOGUÈS, professeur émérite à l'université Bordeaux 1.

Ted CHINBURG, professeur à l'université de Pennsylvanie *(rapporteur)*.

Michel EMSALEM, professeur à l'université Lille 1 *(rapporteur)*.

Luc ILLUSIE, professeur émérite à l'université Paris-Sud.

Martin J. TAYLOR, Warden of Merton College, Oxford.

Angelo VISTOLI, professeur à l'École normale supérieure de Pise *(rapporteur)*.

Table des matières

Introduction

Ce petit mémoire est une synthèse des travaux de recherche présentés en vue de mon habilitation. Pour démarrer cet exercice, on peut dégager plusieurs axes autour desquels mon travail s'est développé :

1. Structures galoisiennes géométriques/*class-invariant homomorphism* ;
2. Prolongement de torseurs sous des schémas en groupes finis et plats ;
3. Prolongement de (bi)extensions de variétés abéliennes par $\mathbf{G}_{\mathrm{m}}$;
4. Pull-back des $\mathbf{G}_{\mathrm{m}}$-torseurs obtenus par une section entière/*class group pairing* ;
5. Utilisation des log schémas et de la cohomologie log plate pour l'étude des problèmes précédents, en particulier visualiser les obstructions qui se présentent.
6. Cohomologie log plate et actions modérées.

Bien sûr, ces différents thèmes sont étroitement liés. Le découpage ci-dessus est, d'un certain point de vue, assez artificiel.

Par souci de cohérence, on trouvera ici un résumé de mes travaux depuis le début, c'est-à-dire ma thèse. L'ordre de présentation est *grosso modo* chronologique.

Les articles [Gil05], [Gil06] et [Gil07b] sont issus de ma thèse, soutenue en décembre 2004 à l'université de Caen. En vue de mon habilitation, je présente les travaux [Gil07a], [Gil09], [Gil12a], [GW13], [GL12] et [Gil12b].

Chapitre 1

Structures galoisiennes géométriques

1.1 Origines et motivations

La motivation première de mes travaux de thèse est l'étude de la structure galoisienne des anneaux d'entiers des corps de nombres. Ce problème m'a naturellement amené à me pencher sur d'autres questions.

La structure de module galoisien des anneaux d'entiers des corps de nombres est un sujet classique en théorie des nombres, depuis son apparition dans le *Zahlbericht* de D. Hilbert. Le point culminant de cette théorie est la démonstration par M. J. Taylor [Tay81] de la conjecture de A. Fröhlich, laquelle décrit complètement la structure galoisienne absolue des extensions modérément ramifiées.

Dans le but d'étudier la structure galoisienne relative d'une famille d'extensions sauvages, M. J. Taylor a initié dans [Tay88] l'étude du *class-invariant homomorphism*, dont je donne une description ci-dessous.

1.2 Le class-invariant homomorphism

Soit R un anneau de Dedekind, de corps de fractions K, et soit $G \to S = \mathrm{Spec}(R)$ un schéma en groupes commutatif, fini et plat. Soit G^D le dual de Cartier de G. Nous disposons d'un homomorphisme

$$\pi : H^1_{\mathrm{fppf}}(S, G^D) \longrightarrow \mathrm{Pic}(G)$$

explicité en premier par Waterhouse (voir [Wat71], Theorem 5). Si l'on considère que la notion de torseur fppf (sous un schéma en groupes fini) généralise celle d'extension galoisienne, alors on peut dire que π mesure la structure galoisienne des G^D-torseurs, le groupe $\mathrm{Pic}(G)$ étant identifié à un groupe de classes (voir [CNT95]).

Le *class-invariant homomorphism* a été introduit par M. J. Taylor [Tay88] dans le but de construire des G^D-torseurs dont l'image par π est triviale, c'est-à-dire des torseurs dont la structure galoisienne est triviale.

Pour fixer les idées, supposons que G soit un sous-groupe d'un S-schéma abélien A. Soit $\phi : A \to B$ l'isogénie de noyau G, et soit $\phi^t : B^t \to A^t$ l'isogénie duale. Alors le noyau de ϕ^t n'est autre que G^D, ce qui nous donne une suite exacte de faisceaux abéliens pour la topologie fppf sur S

$$0 \longrightarrow G^D \longrightarrow B^t \xrightarrow{\phi^t} A^t \longrightarrow 0.$$

Cette suite donne lieu, par application du foncteur des sections globales, à un morphisme cobord $\partial : A^t(S) \to H^1(S, G^D)$. Nous obtenons ainsi le *class-invariant homomorphism*

$$\psi := \pi \circ \partial : A^t(S) \longrightarrow \mathrm{Pic}(G)$$

qui étudie la structure galoisienne des torseurs construits à l'aide du cobord. Dans [Tay88], M. J. Taylor énonce la conjecture suivante

Conjecture (M. J. Taylor, 1988)**.** *Si A_K est une courbe elliptique, alors $A^t(S)_{\mathrm{Tors}}$ est inclus dans* $\ker \psi$*.*

Du point de vue de l'arithmétique, cette conjecture prévoit l'existence de bases normales (relativement à certaines algèbres de Hopf) pour les anneaux d'entiers d'extensions abéliennes de K engendrées par les coordonnées des points de ϕ^t-division d'un point de torsion de $A^t_K(K)$. Elle peut être vue comme une version au niveau entier du *Jugendtraum* de Kronecker.

Srivastav et Taylor [ST90], puis Agboola [Agb96], et enfin Pappas [Pap98] ont démontré cette conjecture, dans le cas où l'ordre de G est premier à 6. Dans le cas d'un groupe G d'ordre pair, Cassou-Noguès et Jehanne [CNJ01] ont donné des contre-exemples à cette conjecture.

Dans ma thèse, j'ai généralisé la construction de ψ, et — sous l'hypothèse de semi-stabilité — le résultat d'annulation sur les points de torsion, à des modèles de Néron de variétés abéliennes.

Plus précisément, on se donne une K-variété abélienne A_K, on note A^t_K sa duale, et $\mathcal{A}$ (resp. $\mathcal{A}^t$) le modèle de Néron de A_K (resp. A^t_K). On se donne également sous-groupe fini et plat G de $\mathcal{A}$.

Soit U l'ouvert de bonne réduction de $\mathcal{A}$. Comme $\mathcal{A}_U$ est un schéma abélien sur U, nous pouvons définir comme précédemment des isogénies $\phi : \mathcal{A}_U \to \mathcal{B}_U$ et $\phi^t : \mathcal{B}^t_U \to \mathcal{A}^t_U$, et un cobord

$$\Delta_U : \mathcal{A}^t_U(U) \longrightarrow H^1_{\mathrm{fppf}}(U, G^D). \tag{1.1}$$

On se pose la question suivante : étant donné un point $y \in \mathcal{A}^t_U(U)$, quelle condition doit-on imposer sur y pour que le torseur $\Delta_U(y)$ appartienne à $H^1_{\mathrm{fppf}}(S, G^D)$, que l'on identifie naturellement à un sous-groupe de $H^1_{\mathrm{fppf}}(U, G^D)$?

Pour répondre à cette question, on se sert d'une observation élémentaire : le diagramme suivant est commutatif

$$\begin{array}{ccc} \mathcal{A}^t_U(U) & \xrightarrow{\sim} & \mathrm{Ext}^1(\mathcal{A}_U, \mathbf{G}_{\mathrm{m}}) \\ {\scriptstyle \Delta_U}\downarrow & & \downarrow{\scriptstyle i^*} \\ H^1(U, G^D) & \xrightarrow[\rho]{\sim} & \mathrm{Ext}^1(G_U, \mathbf{G}_{\mathrm{m}}) \end{array} \tag{1.2}$$

dans lequel :

1. l'isomorphisme du haut est induit par la dualité des schémas abéliens ;
2. l'isomorphisme ρ découle de la suite spectrale locale-globale pour les faisceaux Ext.
3. le morphisme i^* est induit par l'inclusion $i : G \hookrightarrow \mathcal{A}$.

La construction de ρ et de i^* est valable aussi bien sur U que sur S. Ainsi, pour étendre la construction de Δ_U au niveau entier, c'est-à-dire sur S, il suffit d'étendre la dualité $\mathcal{A}^t_U(U) \simeq \mathrm{Ext}^1(\mathcal{A}_U, \mathbf{G}_{\mathrm{m}})$ aux modèles de Néron. Cette question de dualité sur les modèles de Néron a été étudiée par Grothendieck dans [Gro72], en utilisant le langage des biextensions. Nous y reviendrons en détail dans la section 2.1.1. Pour l'instant, contentons-nous de dire que l'on obtient un morphisme [1]

$$\mathcal{A}^{t,0}(S) \xrightarrow{\gamma} \mathrm{Ext}^1(\mathcal{A}, \mathbf{G}_{\mathrm{m}})$$

où $\mathcal{A}^{t,0}$ est la composante neutre de $\mathcal{A}^t$. En considérant l'analogue du diagramme (1.2) sur la base S, on obtient ainsi une flèche

$$\rho^{-1} \circ i^* \circ \gamma : \mathcal{A}^{t,0}(S) \longrightarrow H^1(S, G^D)$$

qui est égale à la restriction de Δ_U au sous-groupe $\mathcal{A}^{t,0}(S) \subseteq \mathcal{A}^t(S)$. Cela fournit la réponse à la question que l'on se posait : si y appartient à $\mathcal{A}^{t,0}(S)$, alors $\Delta_U(y)$ appartient à $H^1(S, G^D)$. Pour un tel y, l'extension engendrée par les points de ϕ^t-division de y est partout non ramifiée, sauf éventuellement en les places où G^D n'est pas étale.

D'autre part, Waterhouse a défini son morphisme π comme étant la composée

$$H^1(S, G^D) \xrightarrow[\rho]{\sim} \mathrm{Ext}^1(G, \mathbf{G}_{\mathrm{m}}) \longrightarrow \mathrm{Pic}(G)$$

où la deuxième flèche est le morphisme naturel. Il en résulte que le diagramme suivant commute

$$\begin{array}{ccccc} \mathcal{A}^{t,0}(S) & \xrightarrow{\gamma} & \mathrm{Ext}^1(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) & \xrightarrow{\rho^{-1}\circ i^*} & H^1(S, G^D) \\ & & \downarrow & & \downarrow{\scriptstyle \pi} \\ & & \mathrm{Pic}(\mathcal{A}) & \xrightarrow{i^*} & \mathrm{Pic}(G) \end{array}$$

1. Si K est de caractéristique 0, ou si les corps résiduels des points fermés de S sont parfaits, alors ce morphisme γ est un isomorphisme.

On note

$$\psi : \mathcal{A}^{t,0}(S) \longrightarrow \mathrm{Pic}(G)$$

le morphisme obtenu en composant les flèches de ce diagramme. En regardant de plus près ledit diagramme, on constate que

$$\psi(y) = (i \times y)^*(t(W)) \tag{1.3}$$

où W est la biextension de $(\mathcal{A}, \mathcal{A}^{t,0})$ par $\mathbf{G}_{\mathrm{m}}$ qui permet de définir la flèche γ, et $t(W)$ est le $\mathbf{G}_{\mathrm{m}}$-torseur sur $\mathcal{A} \times_S \mathcal{A}^{t,0}$ sous-jacent à W. *Grosso modo*, $t(W)$ prolonge le fibré de Poincaré associé à la dualité sur $A_K \times A_K^t$ (voir la section 2.1.1 pour les détails).

La relation (1.3) est un fil conducteur très important pour la suite. Elle signifie que ψ est tout simplement une opération de restriction (ou pull-back) du fibré en droites $t(W)$ à certains sous-schémas finis et plats de $\mathcal{A} \times_S \mathcal{A}^{t,0}$.

Si A_K est une courbe elliptique, il est possible de décrire explicitement $t(W)$. Ceci nous permet de montrer dans [Gil05] le résultat suivant :

Théorème 1. *Si A_K est une courbe elliptique à réduction semi-stable sur S, et si l'ordre de G est premier à 6, alors $\mathcal{A}^{t,0}(S)_{\mathrm{Tors}}$ est contenu dans* $\ker \psi$.

D'autre part, j'ai étudié dans [Gil07b] les propriétés fonctorielles de l'homomorphisme ψ, qui permettent de déduire du résultat d'annulation pour les courbes elliptiques des résultats d'annulation pour certaines variétés semi-abéliennes.

1.3 Contre-exemples en dimension supérieure

Pour une variété abélienne de dimension 2 ou plus, qu'advient-il de la conjecture de Taylor ? Pappas a donné dans [Pap98] des contre-exemples sur certaines bases S de caractéristique positive. Plus précisément, pour tout choix de deux nombres premiers $r \neq \ell$, il construit une courbe affine lisse S sur un corps fini de caractéristique r, et un S-schéma abélien A de dimension relative 2, possédant un point de torsion d'ordre ℓ sur lequel l'homomorphisme ψ_ℓ ne s'annule pas.

Quand la base est le spectre de l'anneau des entiers d'un corps de nombres, aucun résultat n'était connu jusqu'à mon article [Gil07a] dans lequel je m'intéresse à la construction d'un homomorphismes de classes surjectif. J'obtiens le résultat suivant :

Théorème 2. *Soient*

1. *$p \geq 3$ un nombre premier,*
2. *K un corps quadratique imaginaire tel que $\mathrm{Pic}(\mathcal{O}_K)[p] \neq 0$; si $p = 3$ on exige de plus que p soit non ramifié dans K,*
3. *K' une extension de K dans laquelle les éléments de $\mathrm{Pic}(\mathcal{O}_K)[p]$ capitulent,*

4. E une K'-courbe elliptique, ayant bonne réduction au-dessus de p, telle que $E(K')$ soit fini et contienne un élément d'ordre p.

Alors il existe une K-variété abélienne de dimension $[K' : K]$, de modèle de Néron $\mathcal{A}$, et une suite exacte

$$0 \longrightarrow \mu_p \longrightarrow \mathcal{A} \longrightarrow B \longrightarrow 0$$

où $B(S)$ est un groupe de torsion, telle que l'homomorphisme de classes associé

$$\psi : B(S) \longrightarrow H^1(S, \mu_p) \longrightarrow \mathrm{RPic}((\mathbb{Z}/p\mathbb{Z})) \simeq \mathrm{Pic}(\mathcal{O}_K)[p]$$

soit surjectif, donc non nul sur les points de torsion.

Ceci fournit un critère permettant de construire une variété abélienne contenant un point de torsion qui n'est pas dans le noyau de ψ.

Malheureusement, la finitude de $E(K')$ est assez difficile à vérifier numériquement. J'ai donné dans [Gil07a] des exemples pour $p = 3$ et $p = 5$. Il est cependant raisonnable de croire que de tels exemples existent pour d'autres valeurs de p.

Plus généralement, on peut poser la question suivante :

Question 1. *Soient K un corps de nombres, p un nombre premier. Existe-t-il une extension finie L/K et une L-courbe elliptique E telle que :*

- (i) $\mathrm{rang}(E/L) = 0$ *;*
- (ii) $E(L)$ *contient un point d'ordre p.*

Si la réponse à cette question est positive, alors on peut construire pour tout premier $p \geq 3$ un exemple où ψ ne s'annule pas sur un point de p-torsion.

Notons que Mazur et Rubin ont récemment démontré le résultat suivant : étant donné un corps de nombres K, il existe une courbe elliptique E sur K telle que $\mathrm{rang}(E/K) = 0$. C'est une piste qui mériterait sans doute d'être explorée.

Chapitre 2

Cohomologie log plate

2.1 Prolongement de torseurs en cohomologie log plate

Les travaux [Gil09], [Gil12a] et [Gil12b] font ressortir un nouvel outil pour l'étude des actions modérées en géométrie arithmétique : la cohomologie log plate et ses torseurs. Je pense que c'est le point le plus marquant de la présente synthèse.

Notons que la notion de champ algébrique modéré, introduite récemment par Abramovich, Olsson et Vistoli, fait également son apparition dans [Gil12b] en tant qu'outil technique extrêmement efficace. Je suis persuadé que ces objets seront amenées jouer un rôle important dans les développements futurs.

Reprenons le fil conducteur. Comme indiqué plus haut, dans [Gil05] et [Gil06] on construit et on étudie un invariant de classes

$$\mathcal{A}^{t,0}(S) \xrightarrow{\gamma} \mathrm{Ext}^1(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) \longrightarrow H^1(S, G^D) \xrightarrow{\pi} \mathrm{Pic}(G)$$

Dans l'idéal, on aimerait prolonger ce morphisme à $\mathcal{A}^t(S)$ tout entier. L'obstruction à cela est un problème de ramification : d'une part, si y est un point de $\mathcal{A}^t_K(K)$ alors l'extension engendrée par les points de ϕ^t-division de y a tendance à être ramifiée en les places (de mauvaise réduction) au-dessus desquelles y ne se réduit pas en un point de la composante neutre de la fibre spéciale de $\mathcal{A}^t$. D'autre part, un G^D-torseur est le spectre d'une algèbre non ramifiée en dehors des places divisant l'ordre de G^D.

Une réponse à ce problème est fournie par la cohomologie log plate (définie par Kato), dans la catégorie des log schémas fins saturés. Plus précisément, soit U l'ouvert de bonne réduction de $\mathcal{A}$, nous munissons S de sa structure logarithmique définie par U, et nous notons $H^1_{\mathrm{kpl}}(S, G^D)$ le groupe de cohomologie calculé pour la topologie Kummer log plate. En particulier, les élements de $H^1_{\mathrm{kpl}}(S, G^D)$ sont des log schémas (fins saturés) dont le schéma sous-jacent est fini et plat sur S, et dont la restriction à U est un G^D_U-torseur pour la topologie fppf.

Si l'on peut considérer que les torseurs pour la topologie fppf sont des objets non ramifiés par nature, au contraire les torseurs pour la topologie log plate nous permettent d'envisager de la ramification modérée. Par exemple, si Γ est un S-schéma en groupes constant, alors $H^1_{\mathrm{kpl}}(S,\Gamma)$ s'identifie à l'ensemble des Γ-algèbres galoisiennes qui sont modérément ramifiées en les points de $S \setminus U$, et non ramifiées partout ailleurs.

2.1.1 Prolongement de biextensions de variétés abéliennes

Supposons pour l'instant que S soit un trait. Il est bien connu que la variété duale A^t_K de A_K est munie d'un isomorphisme canonique

$$A^t_K \xrightarrow{\sim} \underline{\mathrm{Ext}}^1_{\text{ét}}(A_K, \mathbf{G}_{\mathrm{m}}) \tag{2.1}$$

qui est parfois utilisé comme définition de A^t_K. On peut se demander ce qu'il advient de cet isomorphisme si l'on remplace les variétés abéliennes A_K et A^t_K par leurs modèles de Néron sur S, que nous noterons respectivement $\mathcal{A}$ et $\mathcal{A}^t$.

Grothendieck a utilisé le concept de biextension (introduit par Mumford) pour étudier ce problème. Plus précisément, prolonger l'isomorphisme (2.1) au niveau des modèles de Néron équivaut à prolonger la biextension de Weil W_K de (A_K, A^t_K) par $\mathbf{G}_{\mathrm{m}}$ en une biextension de $(\mathcal{A}, \mathcal{A}^t)$ par $\mathbf{G}_{\mathrm{m}}$. Soit Φ (resp. Φ') le groupe des composantes de (la fibre spéciale de) $\mathcal{A}$ (resp. $\mathcal{A}^t$), Grothendieck construit dans [Gro72, exposé VIII, théorème 7.1, b)] un accouplement (dit de monodromie)

$$\Phi \times \Phi' \longrightarrow \mathbb{Q}/\mathbb{Z}$$

qui représente l'obstruction à l'existence d'un tel prolongement. Plus précisément, si Γ et Γ' sont des sous-groupes respectifs de Φ et Φ', alors W_K se prolonge en une biextension de $(\mathcal{A}^\Gamma, \mathcal{A}^{t,\Gamma'})$ par $\mathbf{G}_{\mathrm{m}}$ si et seulement si Γ et Γ' sont orthogonaux sous l'accouplement, lequel prolongement induit alors un morphisme

$$\gamma : \mathcal{A}^{t,\Gamma'} \longrightarrow \underline{\mathrm{Ext}}^1_{\text{ét}}(\mathcal{A}^\Gamma, \mathbf{G}_{\mathrm{m}})$$

entre faisceaux sur le site des S-schémas lisses, muni de la topologie étale. Si en outre $\Gamma = 0$ et $\Gamma' = \Phi'$ (ou si l'accouplement de monodromie est non dégénéré et si Γ' est l'orthogonal de Γ), alors γ est un isomorphisme. Ce résultat est explicité dans [Mil06, Appendix C, Prop. C.14]. Notons que l'idée de considérer le site lisse apparaît déjà (sous forme d'une « Autocritique ») dans [Gro72, exposé VIII, 6.9].

Munissons le trait S de sa log structure canonique ; en travaillant dans la catégorie des faisceaux pour la topologie Kummer log plate sur S, nous montrons dans [Gil09] le résultat suivant :

Théorème 3. (*i*) *Soit P un schéma en groupes commutatif lisse de type fini sur S. Alors le morphisme de restriction à la fibre générique*

$$\mathrm{Ext}^1_{\mathrm{kpl}}(P, \mathbf{G}_{\mathrm{m}}) \longrightarrow \mathrm{Ext}^1_{\mathrm{fppf}}(P_\eta, \mathbf{G}_{\mathrm{m}})$$

est un isomorphisme.

(*ii*) *Soient P et Q deux schémas en groupes commutatifs lisses de type fini sur S. Alors le morphisme de restriction à la fibre générique*

$$\mathrm{Biext}^1_{\mathrm{kpl}}(P,Q;\mathbf{G}_{\mathrm{m}}) \longrightarrow \mathrm{Biext}^1_{\mathrm{fppf}}(P_\eta,Q_\eta;\mathbf{G}_{\mathrm{m}})$$

est un isomorphisme.

Une fois ce résultat établi on retrouve, par le truchement d'une suite spectrale comparant la cohomologie log plate avec la cohomologie fppf, les obstructions définies par Grothendieck dans [Gro72, exposé VIII, théorème 7.1].

Dans le cas particulier où $(P,Q) = (\mathcal{A},\mathcal{A}^t)$, nous obtenons l'existence d'une unique biextension $W^{\log} \in \mathrm{Biext}^1_{\mathrm{kpl}}(\mathcal{A},\mathcal{A}^t;\mathbf{G}_{\mathrm{m}})$ prolongeant la biextension de Weil. Il découle en outre du théorème ci-dessus que le morphisme

$$\gamma^{\log} : \mathcal{A}^t \longrightarrow \underline{\mathrm{Ext}}^1_{\mathrm{kpl}}(\mathcal{A},\mathbf{G}_{\mathrm{m}})$$

induit par $W^{\log}$ est un isomorphisme entre faisceaux sur le site lisse de S.

Dans le cas global où la base S n'est plus forcément un trait, on peut définir à l'aide de $W^{\log}$ un accouplement de classes logarithmique qui combine le *class group pairing*[1] défini par Mazur et Tate, et l'accouplement de monodromie. Au passage, on obtient une interprétation logarithmique de l'accouplement de monodromie.

2.1.2 Conséquences

Revenons au problème de ramification des torseurs. On sait que l'image du sous-groupe $\mathcal{A}^{t,0}(S)$ par le cobord Δ_U défini dans (1.1) est à valeurs dans $H^1(S,G^D)$. Grâce à la biextension $W^{\log}$, nous montrons dans [Gil12a] le résultat suivant, qui affine cette première observation.

Théorème 4. (*i*) *Le cobord Δ_U défini dans* (1.1) *se relève en un morphisme*

$$\Delta : \mathcal{A}^t(S) \longrightarrow H^1_{\mathrm{kpl}}(S,G^D)$$

(*ii*) *Pour tout point $y \in \mathcal{A}^t(S)$, $\Delta(y)$ appartient au sous-groupe $H^1_{\mathrm{fppf}}(S,G^D)$ si et seulement si l'image de y dans Φ' est orthogonale à l'image de G dans Φ sous l'accouplement de monodromie.*

Le point (*i*) constitue une propriété frappante des torseurs obtenus en divisant des points par une isogénie entre variétés abéliennes : ceux-ci sont en effet de nature modérée au-dessus des places de mauvaise réduction.

1. Voir la section 3.2

Le point (ii) montre que la ramification desdits torseurs est contrôlée par l'accouplement de monodromie. En particulier les constructions précédentes étaient optimales du point de vue de la cohomologie fppf.

Une fois construits les torseurs log plats, on peut définir

$$\psi^{\log} : \mathcal{A}^t(S) \xrightarrow{\gamma^{\log}} \mathrm{Ext}^1_{\mathrm{kpl}}(\mathcal{A}, \mathbf{G}_{\mathrm{m}}) \longrightarrow H^1_{\mathrm{kpl}}(S, G^D) \xrightarrow{\pi^{\log}} H^1_{\mathrm{kpl}}(G, \mathbf{G}_{\mathrm{m}})$$

tous les groupes étant calculés à l'aide de cohomologie Kummer log plate. Ici, $\pi^{\log}$ est un morphisme, défini dans [Gil12a], qui généralise celui de Waterhouse et qui mesure la structure galoisienne des G^D-torseurs pour la cohomologie log plate. Il est à noter que cet invariant de structure galoisienne a l'avantage d'être un morphisme de groupes, contrairement à celui étudié classiquement.

Bien sûr, $\psi^{\log}$ ne s'annule pas sur les points de torsion, car il contient les informations sur la monodromie. En fait, d'après le (ii) du théorème ci-dessus, une condition nécessaire pour que $\psi^{\log}(y) = 0$ est que y soit dans l'orthogonal de G sous l'accouplement de monodromie, c'est-à-dire que, pour toute mauvaise place v, la composante de $\mathcal{A}^t_v$ dans laquelle y se réduit soit orthogonale à toutes les composantes de $\mathcal{A}_v$ qui rencontrent G.

2.2 Torseurs log plats *versus* actions modérées

Dans [Gil12a], on montre que l'action sous-jacente à un torseur log plat est toujours une action modérée au sens de Chinburg, Erez, Pappas et Taylor. C'est un premier jalon dans l'étude des actions modérées à l'aide d'outils logarithmiques.

Dans [Gil12b], je généralise une partie de ce mécanisme au cas général où le schéma en groupes n'est plus supposé commutatif. Plus précisément, je montre que l'action sous-jacente à un torseur log plat définit un champ algébrique modéré au sens de Abramovich, Olsson et Vistoli. Puis je montre que les torseurs log plats jouent le rôle d'objets universels dans la catégorie des revêtements modérés.

Pour fixer les idées, soient X un schéma noethérien régulier, D un diviseur à croisements normaux sur X, et $U := X \setminus D$ l'ouvert complémentaire de D. On se donne un X-schéma en groupes fini localement libre G.

Grosso modo, un G-revêtement modéré de X relativement à D est un morphisme fini et plat $Y \to X$ tel que G agit modérément sur Y, et tel que $Y_U \to U$ est un G-torseur.

Les questions suivantes viennent immédiatement à l'esprit :

1. Étant donné un G-torseur sur U, à quelle condition est-il possible de le prolonger en un G-revêtement modéré de X ?
2. Parmi tous les prolongements possibles d'un G-torseur donné en un G-revêtement modéré, existe-t-il un choix canonique ?

Nous donnons une réponse à ces questions en termes de torseurs log plats. Plus précisément, nous montrons :

Théorème 5. *Un G-torseur t sur U admet un prolongement en un G-revêtement modéré de X si et seulement s'il admet un prolongement en un G-torseur log plat $t^{\log}$ sur $X(\log D)$. En outre, le schéma sous-jacent à $t^{\log}$ est l'objet initial dans la catégorie des G-revêtements modérés prolongeant t.*

Autrement dit, étant donné un G-revêtement modéré $Y \to X$, dont la restriction à U est un G-torseur fppf, il existe un unique G-torseur log plat $T^{\log} \to X$ qui prolonge $Y_U \to U$, et un unique morphisme $T^{\log} \to Y$. Cela fournit un choix canonique pour les actions modérées étudiées par Chinburg, Pappas et Taylor.

Cette approche entretient des liens de parenté évidents avec celle de Grothendieck et Murre dans [GM71], dont elle s'inspire. Rappelons que le site défini par les revêtements étales de U qui sont modérés au-dessus de D (au sens de Grothendieck-Murre) est équivalent au petit site log étale de $X(\log D)$.

Chapitre 3

Pull-back des fibrés de torsion

3.1 Fibrés de torsion et groupes de classes

Dans [GL12], nous étudions une technique permettant de spécialiser les fibrés en droites de torsion sur une variété définie sur $\mathbb{Q}$ dans le groupe de classes de certains corps de nombres. La principale difficulté est de rendre cette opération optimale, c'est-à-dire de s'assurer que le noyau de la spécialisation soit le plus petit possible.

Le résultat principal donne une nouvelle technique pour construire et compter des corps de nombres avec un « grand » groupe de classes.

Si A est un groupe abélien de type fini et si $m \geq 2$ est un entier, nous notons $\operatorname{rang}_m A$ le plus grand entier r tel que A possède un sous-groupe isomorphe à $(\mathbb{Z}/m)^r$. Nous démontrons le résultat suivant :

Théorème 6. *Soit V une variété projective lisse géométriquement connexe sur $\mathbb{Q}$, et soit $m > 1$ un entier. Soit S l'ensemble des places de mauvaise réduction de V, et soit $\mathcal{V} \to \operatorname{Spec}(\mathbb{Z}_S)$ un modèle projectif lisse de V. Alors il existe une infinité de corps de nombres K avec un point $P \in V(K)$ tels que le morphisme de spécialisation*

$$P^* : \operatorname{Pic}(V)[m] = \operatorname{Pic}(\mathcal{V})[m] \longrightarrow \operatorname{Cl}(\mathcal{O}_{K,S})[m]$$

satisfait

$$\operatorname{rang}_m \operatorname{Im}(P^*) \geq \operatorname{rang}_m \operatorname{Pic}(V)[m] + \#S - \operatorname{rang}_{\mathbb{Z}} \mathcal{O}_{K,S}^{\times}.$$

Plus précisément, étant donné une application rationnelle $V \to \mathbb{A}^l$ génériquement finie de degré d, il est possible de trouver une infinité de tels K de degré d.

Bien évidemment, on aimerait que le terme perturbateur

$$\operatorname{rang}_{\mathbb{Z}} \mathcal{O}_{K,S}^{\times} - \#S$$

soit le plus petit possible. Soulignons ici que $\mathcal{O}_{K,S}$ désigne l'anneau des S_K-entiers de K, où S_K est l'ensemble des places de K au-dessus de S.

Dans le cas particulier où la variété V est une courbe superelliptique, on peut utiliser une équation de ladite courbe pour forcer le corps K à avoir le plus de places complexes que possible, ce qui, en vertu du théorème de Dirichlet sur les unités, a pour effet de minimiser le $\mathbb{Z}$-rang de $\mathcal{O}_K^\times$. D'autre part, par le même procédé, on peut s'assurer que tous les premiers dans S sont totalement ramifiés dans K, auquel cas les ensembles S et S_K ont même cardinal. Nous obtenons ainsi le résultat suivant :

Corollaire 7. *Soit C un modèle projectif lisse de la courbe plane définie par l'équation*

$$y^n = f(x), \quad f(x) \in \mathbb{Q}[x], \quad n > 1,$$

avec $(\deg f, n) = 1$. *Soit $m > 1$ un entier. Alors il existe $\gg X^{\frac{1}{(n-1)\deg f}} / \log X$ corps de nombres k de degré $[k : \mathbb{Q}] = n$ et de discriminant d_k, $|d_k| < X$, tels que*

$$\operatorname{rang}_m \operatorname{Cl}(k) \geq \operatorname{rang}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} - \left[\frac{n-1}{2}\right].$$

Si $n = 2$, c'est-à-dire si C est une courbe hyperelliptique avec un point de Weierstrass, alors le terme perturbateur $[\frac{n-1}{2}]$ disparaît. Ainsi, la construction d'une infinité de corps quadratiques imaginaires k tel que $\operatorname{rang}_m \operatorname{Cl}(k) = r$ se ramène à la construction d'une telle courbe satisfaisant $\operatorname{rang}_m \operatorname{Jac}(C)(\mathbb{Q})_{\text{tors}} = r$.

D'un autre côté, la question de la non trivialité du pull-back d'un fibré en droites sur une variété arithmétique dans le groupe de classes d'un corps de nombres a été posée par Agboola et Pappas dans [AP00]. Le théorème ci-dessus permet de répondre positivement à leur question dans le cas d'un fibré de torsion sur une courbe hyperelliptique.

D'autre part, comme on s'en doute, le morphisme $P^* : \operatorname{Pic}(\mathcal{V})[m] \longrightarrow \operatorname{Cl}(\mathcal{O}_{K,S})[m]$ est fortement lié au *class group pairing* sur la variété de Picard de V.

Supposons pour simplifier que la variété soit une courbe projective lisse C, munie d'un point rationnel. Soit $\mathcal{C} \to \operatorname{Spec}(\mathbb{Z}_S)$ un modèle projectif lisse de C. Soit $\mathcal{J} \to \operatorname{Spec}(\mathbb{Z}_S)$ le modèle de Néron de $\operatorname{Jac}(C)$. Alors $\mathcal{J}$ est isomorphe au foncteur de Picard relatif de la courbe $\mathcal{C}$, d'où l'existence d'un fibré universel (dit de Poincaré) $\mathcal{P}$ sur $\mathcal{C} \times \mathcal{J}$. Étant donné un point $P \in C(K)$, l'application

$$P^* : \operatorname{Pic}(\mathcal{C}) \longrightarrow \operatorname{Cl}(\mathcal{O}_{K,S})$$

s'identifie naturellement à l'application

$$\begin{aligned} \operatorname{Jac}(C)(\mathbb{Q}) &\longrightarrow \operatorname{Cl}(\mathcal{O}_{K,S}) \\ Q &\longmapsto (P \times Q)^* \mathcal{P} \end{aligned}$$

On fixe à présent un plongement $C \to \operatorname{Jac}(C)$, ce qui est loisible puisque $C(\mathbb{Q}) \neq \emptyset$. Comme $\mathcal{C}$ est lisse, ce plongement se prolonge en une immersion fermée $i : \mathcal{C} \to \mathcal{J}$. Cette immersion permet de construire un isomorphisme entre $\mathcal{J}$ et son schéma abélien dual, lequel isomorphisme donne naissance à une biextension de Weil W de $(\mathcal{J}, \mathcal{J})$ par $\mathbf{G}_{\mathrm{m}}$. Par construction, nous avons $\mathcal{P} = (i \times \mathrm{id})^*(t(W))$, d'où

$$(P \times Q)^*\mathcal{P} = (i(P) \times Q)^*(t(W))$$

Enfin, d'après le théorème de Raynaud, seul un nombre fini de $i(P)$ sont des points de torsion. Par conséquent, on déduit du corollaire 7 le résultat suivant :

Corollaire 8. *Soit C une courbe hyperelliptique avec un point de Weierstrass. Soit $m > 1$ un entier. Alors il existe une infinité de corps quadratiques imaginaires K munis d'un point $P \in \mathrm{Jac}(C)(K)$ d'ordre infini, tels que l'application*

$$\begin{aligned} \mathrm{Jac}(C)(\mathbb{Q})[m] &\longrightarrow \mathrm{Cl}(\mathcal{O}_{K,S}) \\ Q &\longmapsto \langle P, Q\rangle^{\mathrm{cl}} := (P \times Q)^*(t(W)) \end{aligned}$$

soit injective.

On voit réapparaître les préoccupations du premier chapitre. En particulier nous obtenons, via la relation (1.3), des points d'ordre infini sur une variété abélienne dont l'image par le *class-invariant homomorphism* n'est pas nulle.

3.2 Class group pairing et descente

Dans cette section, K est un corps de nombres, et nous posons $X = \mathrm{Spec}(\mathcal{O}_K)$. Soit E une K-courbe elliptique, et $\mathcal{E}$ son modèle de Néron. Le *class group pairing*, introduit par Mazur et Tate, est une application bilinéaire définie par

$$\begin{aligned} \mathcal{E}(X) \times \mathcal{E}^0(X) &\longrightarrow \mathrm{Pic}(X) \\ (x, y) &\longmapsto \langle x, y\rangle^{\mathrm{cl}} := (x \times y)^*(t(W)) \end{aligned}$$

où W est la biextension qui prolonge le fibré de Poincaré.

Soit $S \subset X$ l'ensemble des places de mauvaise réduction de $\mathcal{E}$. Grâce à [Gil09], on sait que W se prolonge en une biextension $W^{\log}$ de $(\mathcal{E}, \mathcal{E})$ par $\mathbf{G}_{\mathrm{m}}$ pour la topologie log plate sur $X(\log S)$. Ainsi, le *class group pairing* se prolonge en

$$\begin{aligned} \mathcal{E}(X) \times \mathcal{E}(X) &\longrightarrow \mathrm{LogPic}(X, S) \\ (x, y) &\longmapsto \langle x, y\rangle^{\log} := (x \times y)^*(t(W^{\log})) \end{aligned}$$

où $\mathrm{LogPic}(X, S) = H^1_{\mathrm{kpl}}(X(\log S), \mathbf{G}_{\mathrm{m}})$ est le groupe de Picard du log schéma $X(\log S)$.

Dans [GW13], nous donnons des formules explicites pour le calcul de ce *class group pairing* logarithmique sur une courbe elliptique. D'autre part, nous effectuons une descente relativement à une isogénie de noyau μ_p à l'aide de la cohomologie fppf sur l'ouvert $X \backslash S$ de bonne réduction de $\mathcal{E}$. Ensuite, nous relions, via le *class group pairing*, le groupe de Selmer obtenu au groupe $\mathrm{LogPic}(X, S)$. Toutes ces constructions sont explicites et se prêtent à une expérimentation sur machine, que nous avons implémentée à l'aide du logiciel de calcul `Sage`.

D'un point de vue conceptuel, les questions qui apparaissent ici sont des analogues du problème de « visibilité » introduit par Cremona et Mazur.

Pour fixer les idées, soit $p \neq 2$ un premier, et soit $\varphi\colon E \to E'$ une isogénie de noyau μ_p entre courbes elliptiques définies sur K. Alors l'isogénie duale $\hat{\varphi} : E' \to E$ a un noyau isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Nous supposons dans toute la suite que K, E et p satisfont quelques hypothèses techniques. Si les places de K au-dessus de p ne sont pas trop ramifiées, c'est-à-dire si leur indice de ramification absolu est $< p-1$, et si E est semi-stable, alors ces hypothèses sont satisfaites.

On peut d'abord décrire $\mathrm{Sel}^{\varphi}(E/K)$ en tant que sous-groupe de $H^1_{\mathrm{fppf}}(U_1, \mu_p)$, où U_1 est un ouvert obtenu en retirant à X un certain ensemble S_1 de places où E a réduction multiplicative déployée. On définit un autre ensemble de places S_2 en lesquelles on doit imposer des conditions locales, et on obtient une suite exacte

$$0 \longrightarrow \mathrm{Sel}^{\varphi}(E/K) \longrightarrow H^1_{\mathrm{fppf}}(U_1, \mu_p) \longrightarrow \bigoplus_{v \in S_2} H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mu_p)$$

D'autre part, on peut décrire le conoyau de la flèche de droite en termes du groupe de Selmer $\mathrm{Sel}^{\hat{\varphi}}(E'/K)$ de l'isogénie duale $\hat{\varphi}$. Plus précisément, en utilisant les méthodes de dualité globale en cohomologie fppf, nous obtenons une suite exacte

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}^{\varphi}(E/K) \arrow[r] & H^1(U_1, \mu_p) \arrow[r] & \bigoplus_{v \in S_2} H^1(\mathcal{O}_v, \mu_p) \arrow[dll, rounded corners] \\
& \mathrm{Sel}^{\hat{\varphi}}(E'/K)^{\vee} \arrow[r] & \mathrm{Cl}\big(\mathcal{O}_{K,S_1}\big)/p \arrow[r] & 0
\end{tikzcd}$$

qui est un analogue de la suite exacte de Cassels, Poitou et Tate. Les méthodes sont inspirées de [MS10], avec le grain de sel que représente l'usage systématique de la cohomologie fppf et des modèles de Néron.

Citons deux conséquences immédiates de ces calculs :

1) l'égalité

$$\dim_{\mathbb{F}_p} \mathrm{Sel}^{\varphi}(E/K) - \dim_{\mathbb{F}_p} \mathrm{Sel}^{\hat{\varphi}}(E'/K) = \#S_1 + \#\{v \mid \infty\} - \sum_{v \in S_2} n_v + \dim_{\mathbb{F}_p}(\mu_p(K)) - 1$$

où $n_v = [K_v : \mathbb{Q}_p]$ si $v \mid p$ et $n_v = 1$ sinon.

2) l'encadrement

$$\dim_{\mathbb{F}_p}(\mathrm{Cl}\big(\mathcal{O}_{K,S_1}\big)/p) \leq \dim_{\mathbb{F}_p} \mathrm{Sel}^{\hat{\varphi}}(E'/K) \leq \dim_{\mathbb{F}_p}(\mathrm{Cl}\big(\mathcal{O}_{K,S_1}\big)/p) + \sum_{v \in S_2} n_v$$

Nous exploitons ensuite le lien entre le *class group pairing* logarithmique et le groupe de Selmer $\mathrm{Sel}^{\varphi}(E/K)$. En fait, on montre que

$$H^1_{\mathrm{kpl}}(X(\log S_1), \mu_p) \simeq H^1_{\mathrm{fppf}}(U_1, \mu_p)$$

donc la théorie de Kummer en cohomologie log plate donne une suite exacte

$$0 \longrightarrow \mathcal{O}_K^{\times}/p \longrightarrow H^1_{\mathrm{fppf}}(U_1, \mu_p) \longrightarrow \mathrm{LogPic}(X, S_1)[p] \longrightarrow 0.$$

Soit $\psi_{\mathrm{Sel}} \colon \mathrm{Sel}^{\varphi}(E/K) \to \mathrm{LogPic}(X, S_1)[p]$ la restriction de la flèche de droite au sous-groupe $\mathrm{Sel}^{\varphi}(E/K)$. Par construction du *class-invariant homomorphism* logarithmique, le diagramme suivant commute :

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/\varphi(E(K)) \arrow[r, "\kappa"] \arrow[dr, "\psi"'] & \mathrm{Sel}^{\varphi}(E/K) \arrow[r] \arrow[d, "\psi_{\mathrm{Sel}}"] & Ш(E/K)[\varphi] \arrow[r] & 0 \\
& & \mathrm{LogPic}(X, S_1)[p] & &
\end{tikzcd}$$

où $Ш(E/K)$ est le groupe de Tate-Shafarevich group de E/K, et la ligne horizontale est exacte comme chacun sait.

D'autre part, on montre que ψ s'exprime en fonction du *class group pairing* logarithmique de la façon suivante :

$$\psi(Q) = \langle P, Q \rangle^{\log}$$

où $P \in E'(K)[p]$ est le point de p-torsion engendrant le noyau de l'isogénie duale de φ. Ceci relie le *class group pairing* au calcul de la φ-descente.

Enfin, le lemme du noyau-conoyau nous permet d'obtenir à partir du diagramme précédent une suite exacte

$$0 \longrightarrow \ker(\psi) \longrightarrow \ker(\psi_{\mathrm{Sel}}) \longrightarrow Ш(E/K)[\varphi] \longrightarrow \mathrm{coker}(\psi) \longrightarrow \mathrm{coker}(\psi_{\mathrm{Sel}}) \longrightarrow 0$$

Comprendre cette suite peut se traduire en termes de « visibilité » au sens de Cremona et Mazur [CM00] : au lieu de comparer les flèches de descente pour deux isogénies distinctes, nous comparons la φ-descente avec la théorie de Kummer en topologie log plate. Par exemple, quand $\mathrm{coker}(\psi) = 0$, on pourrait dire, en analogie avec la terminologie de [CM00], que tous les éléments de $Ш(E/K)[\varphi]$ sont *expliqués* par les unités.

Pour finir, le lien ci-dessus entre groupe de Selmer et groupe de classes suggère un parallèle entre les questions de taille de chacun des deux objets. La question suivante appartient justement au folklore.

Question 2. *Soit E une courbe elliptique définie sur $\mathbb{Q}$, et p un nombre premier. La quantité*

$$\dim_{\mathbb{F}_p} \mathrm{Sel}^p(E/K)$$

prend-elle des valeurs arbitrairement grandes quand K parcourt l'ensemble des corps quadratiques ?

Dans un travail récent, Mazur et Rubin ont montré que la réponse à cette question est oui pour $p = 2$ et une courbe E telle que $E(\mathbb{Q})[2] = 0$.

Soit maintenant E une courbe elliptique sur $\mathbb{Q}$ contenant μ_p comme sous-groupe. Bien sûr, cela n'est possible que pour $p \leq 7$. Supposons pour simplifier que E est semi-stable. Alors, d'après ce qui précède, nous avons

$$\dim_{\mathbb{F}_p} \mathrm{Sel}^p(E/K) \leq 2 \cdot (\dim_{\mathbb{F}_p} \mathrm{Cl}(K)[p] + \#S + 1)$$

où $S = S_1 \cup S_2$ est l'ensemble des places de mauvaise réduction de E. En particulier, si la réponse à la question 2 est positive pour une seule telle courbe elliptique, alors $\dim_{\mathbb{F}_p} \mathrm{Cl}(K)[p]$ prend des valeurs arbitrairement grandes quand K parcourt l'ensemble des corps quadratiques.

Par exemple, la courbe $E = 11a2$ contient μ_5 et satisfait $E(\mathbb{Q})[5] = 0$. Si la question 2 a une réponse positive pour $E = 11a2$ et $p = 5$, alors il existe des corps quadratiques dont le 5-rang du groupe des classes est arbitrairement grand. Cela serait une avancée importante au vu de l'état actuel des connaissances.

Bibliographie

[Agb96] Adebisi Agboola, *Torsion points on elliptic curves and Galois module structure*, Invent. Math. **123** (1996), 105–122.

[AP00] Adebisi Agboola and George Pappas, *Line bundles, rational points and ideal classes*, Math. Res. Letters **7** (2000), 1–9.

[CM00] John Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experimental Math. **9** (2000), 13–28.

[CNJ01] Philippe Cassou-Noguès and Arnaud Jehanne, *Espaces homogènes principaux et points de 2-division de courbes elliptiques*, J. London Math. Soc. **63** (2001), 257–287.

[CNT95] Philippe Cassou-Noguès and Martin J. Taylor, *Structures galoisiennes et courbes elliptiques*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 307–331.

[Gil05] Jean Gillibert, *Invariants de classes : le cas semi-stable*, Compos. Math. **141** (2005), no. 4, 887–901.

[Gil06] ———, *Variétés abéliennes et invariants arithmétiques*, Ann. Inst. Fourier (Grenoble) **56** (2006), 277–297.

[Gil07a] ———, *Invariants de classes : exemples de non-annulation en dimension supérieure*, Math. Annalen **338** (2007), 475–495.

[Gil07b] ———, *Invariants de classes : propriétés fonctorielles et applications à l'étude du noyau*, J. Théor. Nombres Bordeaux **19** (2007), 415–432.

[Gil09] ———, *Prolongement de biextensions et accouplements en cohomologie log plate*, Int. Math. Res. Not. IMRN **2009** (2009), 3417–3444.

[Gil12a] ———, *Cohomologie log plate, actions modérées et structures galoisiennes*, J. Reine Angew. Math. **666** (2012), 1–33.

[Gil12b] ———, *Tame stacks and log flat torsors*, Preprint, 2012.

[GL12] Jean Gillibert and Aaron Levin, *Pulling back torsion line bundles to ideal classes*, Math. Res. Lett. **19** (2012), no. 05, 1–14.

[GM71] Alexandre Grothendieck and Jacob P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Mathematics, Vol. 208, Springer-Verlag, Berlin, 1971.

[Gro72] Alexandre Grothendieck, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim.

[GW13] Jean Gillibert and Christian Wuthrich, *The class group pairing and p-descent on elliptic curves*, Proc. London Math. Soc. **106** (2013), no. 2, 345–374.

[Mil06] James S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.

[MS10] Robert Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, `http://arxiv.org/abs/1010.3334`, 2010.

[Pap98] George Pappas, *On torsion line bundles and torsion points on abelian varieties*, Duke Math. J. **91** (1998), no. 2, 215–224.

[ST90] Anupam Srivastav and Martin J. Taylor, *Elliptic curves with complex multiplication and Galois module structure*, Invent. Math. **99** (1990), 165–184.

[Tay81] Martin J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41–79.

[Tay88] ———, *Mordell-Weil groups and the Galois module structure of rings of integers*, Illinois J. Math. **32** (1988), no. 3, 428–452.

[Wat71] William C. Waterhouse, *Principal homogeneous spaces and group scheme extensions*, Trans. Amer. Math. Soc. **153** (1971), 181–189.