Caractère d'isogénie et critères d'irréductibilité

Agnès David
Laboratoire de mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45 avenue des États-Unis
78035 Versailles Cedex
Agnes.David@ens-lyon.org

Résumé

This article deals with the Galois representation attached to the torsion points of an elliptic curve defined over a number field. We first determine explicit uniform criteria for the irreducibility of this Galois representation for elliptic curves varying in some infinite families, characterised by their reduction type at some fixed places of the base field. Then, we deduce from these criteria an explicit form for a bound that appear in a theorem of Momose. Finally, we use these results to precise a previous theorem of the author about the homotheties contained in the image of the Galois representation.

Introduction

Cet article traite de la représentation galoisienne associée aux points de torsion d'une courbe elliptique définie sur un corps de nombres. Son objectif est triple : on détermine d'abord des critères uniformes d'irréductibilité de cette représentation galoisienne pour des familles infinies de courbes elliptiques, définies par un type de réduction prescrit en certaines places du corps de base (théorème I ci-dessous) ; on donne ensuite une forme explicite pour une borne annoncée dans un théorème de Momose sur les courbes elliptiques possédant sur un corps de nombres une isogénie de degré premier (théorème A de l'introduction de [10] ; théorème II ci-dessous) ; enfin, on déduit de ces travaux une borne uniforme pour les homothéties contenues dans l'image de la représentation galoisienne considérée, lorsqu'elle est réductible, qui précise des résultats précédents de l'auteur ([4] ; théorèmes III et III' ci-dessous).

Le cadre précis est le suivant. On fixe un corps de nombres K et un plongement de K dans $\mathbb{C}$ (dans tout le texte, on considérera ainsi K comme un sous-corps de $\mathbb{C}$). Soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$; on note G_K le groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ de K. À partir de la partie 2 et pour toute la fin du texte, on suppose que l'extension $K/\mathbb{Q}$ est galoisienne. On fixe une courbe elliptique E définie sur K et on note $j(E)$ son invariant j. Pour toute place finie du corps K, on dit que le *type de réduction semi-stable* de E en cette place est *multiplicatif*, *bon* *ordinaire* ou *bon supersingulier* selon si E a potentiellement mauvaise réduction multiplicative, bonne réduction ordinaire ou bonne réduction supersingulière en cette place. On fixe un nombre premier p supérieur ou égal à 5 et non ramifié dans K. On note E_p l'ensemble des points de E dans $\overline{\mathbb{Q}}$ qui sont de p-torsion ; c'est un espace vectoriel de dimension 2 sur $\mathbb{F}_p$, sur lequel le groupe de Galois absolu G_K de K agit $\mathbb{F}_p$-linéairement. On désigne par $\varphi_{E,p}$ la représentation de G_K ainsi obtenue ; elle prend ses valeurs dans le groupe $\mathrm{GL}(E_p)$ qui, après choix d'une base pour E_p, est isomorphe à $\mathrm{GL}_2(\mathbb{F}_p)$. On note enfin χ_p le caractère cyclotomique de G_K dans $\mathbb{F}_p^\times$; il coïncide avec le déterminant de la représentation $\varphi_{E,p}$.

Les questions traitées dans cet article trouvent leur origine dans le théorème suivant de Serre selon lequel, lorsque la courbe E n'a pas de multiplication complexe, la représentation $\varphi_{E,p}$ est « asymptotiquement surjective ».

Théorème (Serre, [13]). *On suppose que la courbe E n'a pas de multiplication complexe (sur $\overline{\mathbb{Q}}$). Alors il existe une borne $C(K,E)$, ne dépendant que de K et de E et telle que pour tout nombre premier p strictement supérieur à $C(K,E)$, la représentation $\varphi_{E,p}$ est surjective.*

La question, posée également dans [13], d'éliminer la dépendance en la courbe elliptique E dans la borne $C(K,E)$, pour obtenir une version uniforme de ce théorème, s'est révélée ardue. Mazur a néanmoins démontré que lorsque le corps de base est $\mathbb{Q}$, la représentation $\varphi_{E,p}$ est « uniformément asymptotiquement irréductible » au sens suivant.

Théorème (Mazur, [8]). *On suppose que le corps K est égal à $\mathbb{Q}$ et que le nombre premier p n'appartient pas à l'ensemble* $\{2,3,5,7,13,11,17,19,37,43,67,163\}$. *Alors la représentation $\varphi_{E,p}$ est irréductible.*

Momose a ensuite obtenu un résultat semblable (avec une borne non effective) lorsque le corps de base est un corps quadratique qui n'est pas imaginaire de nombre de classes 1 (théorème B de l'introduction de [10]).

Dans la lignée du théorème de Mazur, il est naturel de considérer le problème suivant (qui figure par exemple dans l'introduction de [1]).

Question. *Trouver un ensemble infini $\mathcal{E}$ de courbes elliptiques définies sur K et une borne $C(K,\mathcal{E})$ ne dépendant que de K et de l'ensemble $\mathcal{E}$ et vérifiant : si E appartient à $\mathcal{E}$ et p est strictement supérieur à $C(K,\mathcal{E})$, alors la représentation $\varphi_{E,p}$ est irréductible.*

La généralisation du théorème de Mazur au corps de base K consisterait à résoudre cette question pour l'ensemble $\mathcal{E}$ des courbes elliptiques définies sur K qui n'ont pas de multiplication complexe (sur $\overline{\mathbb{Q}}$).

Le présent article apporte une réponse à la question ci-dessus, avec des bornes $C(K,\mathcal{E})$ explicites, pour deux classes d'ensembles infinis de courbes elliptiques, définis par un type de réduction semi-stable des courbes prescrit en des places fixées du corps de base.

Notations. On suppose que le corps K est galoisien sur $\mathbb{Q}$.

On note d_K son degré, Δ_K son discriminant, h_K son nombre de classes d'idéaux, et R_K son régulateur. On note $C_1(K)$ la borne c_3 de [2] : elle ne dépend que du degré d_K de K (voir les notations 2.8 et la définition 2.9 de ce texte pour une expression explicite de $C_1(K)$). On pose alors

$$C_2(K) = \exp\left(12 d_K C_1(K) R_K\right)$$

et pour tout entier n

$$C(K,n) = \left(n^{12h_K} C_2(K) + n^{6h_K}\right)^{2d_K}.$$

Théorème I (Deux critères d'irréductibilité). *On suppose que le corps K est galoisien sur $\mathbb{Q}$.*

1. *Soit M un entier naturel supérieur ou égal 1.*
   On note $\mathcal{E}(K;M)$ l'ensemble des courbes elliptiques E définies sur K pour lesquelles il existe
   - *q et q' des nombres premiers totalement décomposés dans K et inférieurs ou égaux à M,*
   - *une place $\mathfrak{q}$ de K au-dessus de q et une place $\mathfrak{q}'$ de K au-dessus de q' tels que les types de réduction semi-stable de E en $\mathfrak{q}$ et $\mathfrak{q}'$ sont différents*

   (les premiers q et q' et les places $\mathfrak{q}$ et $\mathfrak{q}'$ peuvent dépendre de E).
   Alors pour toute courbe elliptique E dans $\mathcal{E}(K;M)$ et tout nombre premier p strictement supérieur à $C(K,M)$, la représentation $\varphi_{E,p}$ est irréductible.
2. *Soit q un nombre premier rationnel totalement décomposé dans K.*
   On note $\mathcal{E}'(K;q)$ l'ensemble des courbes elliptiques E définies sur K vérifiant : il existe une place (pouvant dépendre de E) de K au-dessus de q en laquelle E a potentiellement mauvaise réduction multiplicative.
   On pose
   $$B(K;q) = \max\left(C(K,q), \left(1+3^{6d_K h_K}\right)^2\right).$$
   Alors pour toute courbe elliptique E dans $\mathcal{E}(K;q)$ et tout nombre premier p strictement supérieur à $B(K;q)$, la représentation $\varphi_{E,p}$ est irréductible.

En utilisant le théorème I, associé à une forme effective du théorème de Chebotarev ([6]), on donne ensuite une formule explicite pour une borne C_K satisfaisant le théorème A de [10], dont on rappelle ici l'énoncé (A désigne une constante absolue qui apparaît dans le théorème de Chebotarev effectif de [6], voir partie 4.1 de ce texte ; voir aussi [3] pour un énoncé similaire).

Théorème II (Version effective du théorème A de [10]). *On suppose que le corps K est galoisien sur $\mathbb{Q}$. On pose*

$$C_K = \max\left(C\left(K, 2(\Delta_K)^{Ah_K}\right), \left(1+3^{6d_K h_K}\right)^2\right).$$

On suppose que p est strictement supérieur à C_K et que la courbe E possède une isogénie de degré p définie sur K. On note λ le caractère de G_K dans $\mathbb{F}_p^\times$ donnant l'action de G_K sur le sous-groupe d'ordre p de E_p définissant l'isogénie. Alors on est dans l'un des deux cas suivants.

Type supersingulier

1. *Le nombre premier p est congru à 3 modulo 4 ;*
2. *En toute place de K au-dessus de p, la courbe E a mauvaise réduction additive et potentiellement bonne réduction supersingulière.*
3. *La puissance sixième du caractère λ est égale à $\chi_p^{3+\frac{p-1}{2}}$.*

Type ordinaire *Il existe un corps quadratique imaginaire L satisfaisant les conditions suivantes.*

1. *Le corps K contient L et son corps de classes de Hilbert (en particulier, la norme dans l'extension K/L de tout idéal fractionnaire de K est un idéal fractionnaire principal de L).*
2. *Le nombre premier p est décomposé dans L.*
3. *Il existe un idéal premier $\mathfrak{p}_L$ de L au-dessus de p tel que le caractère λ^{12} est non ramifié aux places finies de K premières à $\mathfrak{p}_L$.*
4. *Soient $\mathfrak{q}$ un idéal premier de K premier à $\mathfrak{p}_L$, $\alpha_\mathfrak{q}$ dans $\mathcal{O}_L$ un générateur de l'idéal $N_{K/L}(\mathfrak{q})$ et $\sigma_\mathfrak{q}$ dans G_K un relèvement du frobenius du corps résiduel de K en $\mathfrak{q}$; alors on a $\lambda^{12}(\sigma_\mathfrak{q}) = \alpha_\mathfrak{q}^{12} \bmod \mathfrak{p}_L$.*

Remarques.

1. L'énoncé initial du théorème A de [10] présente un troisième cas possible, dans lequel le caractère λ^{12} ou le caractère $\left(\chi_p\lambda^{-1}\right)^{12}$ est trivial. On l'a ici éliminé avec les bornes uniformes pour l'ordre des points de torsion d'une courbe elliptique qui figurent dans [9] et [11].
2. La terminologie *type supersingulier ou ordinaire* est propre au présent article ; elle fait référence au type de réduction semi-stable de la courbe E, non pas aux places de K au-dessus de p, mais en toute place d'une famille finie ne dépendant que de K (voir la définition 4.1 et la proposition 4.4).
3. D'après Momose (remarque 8, p. 341 de [10]), l'hypothèse de Riemann généralisée entraînerait que le cas supersingulier ne se produit pas, pour p assez grand. Larson et Vaintrob obtiennent ainsi, sous cette hypothèse, un analogue du théorème II (voir [7], §5).

Le théorème II a pour conséquence un critère d'irréductibilité pour l'ensemble des courbes elliptiques semi-stables sur K, lorsque les propriétés du corps K empêchent le cas ordinaire de survenir. Par exemple (voir aussi l'appendice B de [5]) :

Corollaire. *On suppose que le corps K est galoisien sur $\mathbb{Q}$ et ne contient le corps de classes de Hilbert d'aucun corps quadratique imaginaire. Alors pour toute courbe elliptique E semi-stable sur K et tout nombre premier p strictement supérieur à C_K, la représentation $\varphi_{E,p}$ est irréductible.*

Enfin, l'étude menée pour de la démonstration du théorème II donne le résultat uniforme suivant pour les homothéties contenues dans l'image de la représentation $\varphi_{E,p}$.

Théorème III (Homothéties dans le cas réductible). *On se place dans les hypothèses du théorème II.*

1. *Dans le cas supersingulier, l'image de $\varphi_{E,p}$ contient les carrés des homothéties.*
2. *Dans le cas ordinaire, l'image de $\varphi_{E,p}$ contient les puissances douzièmes des homothéties.*

Avec les résultats de [4] lorsque la représentation est irréductible, on obtient l'énoncé général suivant.

Théorème III' (Homothéties). *On suppose que le corps K est galoisien sur $\mathbb{Q}$. Alors pour toute courbe elliptique E définie sur K et tout nombre premier p strictement supérieur à C_K, on est dans l'un des deux cas suivants :*

1. *l'image de $\varphi_{E,p}$ contient les carrés des homothéties ;*
2. *la représentation $\varphi_{E,p}$ est réductible de type ordinaire ; dans ce cas l'image de $\varphi_{E,p}$ contient les puissances douzièmes des homothéties.*

Dans toute la suite du texte, à l'exception de la partie 3, on suppose que la représentation $\varphi_{E,p}$ est réductible. La courbe E possède alors un sous-groupe d'ordre p défini sur K. On fixe un tel sous-groupe W ; il lui est associé une isogénie de E de degré p, définie sur K. L'action de G_K sur $W(\overline{\mathbb{Q}})$ est donnée par un caractère continu de G_K dans $\mathbb{F}_p^\times$; on le note λ et, suivant la terminologie introduite dans [8], on l'appelle le caractère d'isogénie associé au couple (E, W). On fixe également une base de E_p dont le premier vecteur engendre $W(\overline{\mathbb{Q}})$; dans cette base la matrice de la représentation $\varphi_{E,p}$ est triangulaire supérieure, de caractères diagonaux $(\lambda, \chi_p\lambda^{-1})$.

Pour la détermination de la borne C_K, on suit la méthode introduite dans [10].

Dans la partie 1, on établit les propriétés locales du caractère d'isogénie : à l'aide des résultats de [14], [13] et [12], on détermine sa restriction aux sous-groupes d'inertie de G_K et l'image par λ d'un élément de Frobenius associé à une place hors de p, en fonction du type de réduction semi-stable de la courbe en cette place.

Dans la partie 2, on utilise la théorie du corps de classes (appliquée à l'extension abélienne trivialisant une puissance du caractère d'isogénie) pour relier le type de réduction de la courbe en une place hors de p à l'action sur le sous-groupe d'isogénie des sous-groupes d'inertie des places au-dessus de p. La détermination de la borne au-delà de laquelle p doit être pris pour qu'on puisse établir un tel lien fait intervenir des bornes de Bugeaud et Győry ([2]) sur la hauteur d'un représentant d'une classe d'entiers de K modulo ses unités.

Dans la partie 3, on utilise les résultats de la partie 2 pour démontrer les deux critères d'irréductibilité qui constituent le théorème I ci-dessus ; la démonstration de ce théorème nécessite également les bornes uniformes pour l'ordre des points de torsion des courbes elliptiques qui figurent dans [9] et [11].

Dans la partie 4, on emploie les résultats de la partie 3, associés à une version effective du théorème de Chebotarev ([6]), pour établir la forme de la borne C_K du théorème II ; on vérifie ensuite (partie 4.2) qu'elle permet d'aboutir aux conclusions du théorème II. Enfin, on fait le lien entre les deux types du théorème II et l'étude locale initiale du caractère d'isogénie (partie 1) pour obtenir le théorème III.

1 Étude locale du caractère d'isogénie

1.1 Défaut de semi-stabilité

Soient ℓ un nombre premier rationnel et $\mathfrak{L}$ un idéal premier de K au-dessus de ℓ.

Notations 1.1. On fixe $D_{\mathfrak{L}}$ un sous-groupe de décomposition pour $\mathfrak{L}$ dans G_K ; on note $I_{\mathfrak{L}}$ son sous-groupe d'inertie (deux choix différents de $D_{\mathfrak{L}}$ sont conjugués par un élément de G_K ; leur image par le caractère abélien λ coïncident donc). On note $K_{\mathfrak{L}}$ le complété de K en $\mathfrak{L}$, $\overline{K_{\mathfrak{L}}}$ sa clôture algébrique associée au sous-groupe $D_{\mathfrak{L}}$ et $K_{\mathfrak{L}}^{nr}$ l'extension non ramifiée maximale de $K_{\mathfrak{L}}$ dans $\overline{K_{\mathfrak{L}}}$. On note $k_{\mathfrak{L}}$ le corps résiduel de K en $\mathfrak{L}$, $N\mathfrak{L}$ son cardinal et $\overline{k_{\mathfrak{L}}}$ sa clôture algébrique associée à $\overline{K_{\mathfrak{L}}}$. On fixe dans $D_{\mathfrak{L}}$ un relèvement $\sigma_{\mathfrak{L}}$ du frobenius de $k_{\mathcal{L}}$ (le sous-groupe $D_{\mathfrak{L}}$ étant fixé, deux tels relèvements diffrent par un élément de $I_{\mathfrak{L}}$; leurs images par un caractère non ramifié en $\mathcal{L}$ coïncident donc).

Enfin, on note K^{λ} l'extension de K trivialisant le caractère λ ; l'extension K^{λ}/K est galoisienne, cyclique, de degré divisant $p-1$. La courbe E possède un point d'ordre p défini sur K^{λ}.

Lemme 1. *On suppose ℓ différent de p ; alors en toute place de K^{λ} au-dessus de $\mathfrak{L}$, E n'a pas réduction additive.*

Démonstration. On renvoie pour la démonstration au §6 de [8] ou au lemme 3.4 (§3.2.2) de [4]. □

1.1.1 Définition de $e_{\mathfrak{L}}$ lorsque $j(E)$ n'est pas entier en $\mathfrak{L}$

On suppose que l'invariant j de E n'est pas entier en la place $\mathfrak{L}$, c'est-à-dire que E a potentiellement réduction multiplicative en $\mathfrak{L}$.

Alors il existe une unique extension $K'_{\mathfrak{L}}$ de $K_{\mathfrak{L}}$ de degré inférieur ou égal à 2, sur laquelle E est isomorphe à une courbe de Tate ; cette extension est de degré 1 si et seulement si E a réduction multiplicative déployée en $\mathfrak{L}$, de degré 2 sinon ; elle est ramifiée si et seulement si E a réduction additive en $\mathfrak{L}$ (voir [15] appendice C théorème 14.1).

On note $e_{\mathfrak{L}}$ l'indice de ramification de cette extension ; on a donc $e_{\mathfrak{L}}$ égal à 1 si et seulement si E a réduction multiplicative (déployée ou non) en $\mathfrak{L}$ et $e_{\mathfrak{L}}$ égal à 2 si et seulement si E a réduction additive en $\mathfrak{L}$.

1.1.2 Définition de $e_{\mathfrak{L}}$ lorsque $j(E)$ est entier en $\mathfrak{L}$

On suppose que l'invariant j de E est entier en la place $\mathfrak{L}$, c'est-à-dire que E a potentiellement bonne réduction en $\mathfrak{L}$.

Alors il existe une plus petite extension de $K_{\mathfrak{L}}^{nr}$ sur laquelle E a bonne réduction et cette extension est galoisienne ([14], §2, corollaire 3, p. 498). On note $M_{\mathfrak{L}}$ cette extension et $\Phi_{\mathcal{L}}$ le groupe de Galois de $M_{\mathfrak{L}}$ sur $K_{\mathfrak{L}}^{nr}$.

Lorsque ℓ est différent de p, on sait de plus ([14], *loc. cit.*) que $M_{\mathfrak{L}}$ est l'extension de $K_{\mathfrak{L}}^{nr}$ engendrée par les coordonnées des points de p-torsion de E. En particulier, le corps $M_{\mathfrak{L}}$ contient l'extension de $K_{\mathfrak{L}}^{nr}$ engendrée par les coordonnées des points du sous-groupe d'isogénie W ; on note $M_{\mathfrak{L}}^{\lambda}$ cette extension. D'après le lemme 1, E a bonne réduction sur $M_{\mathfrak{L}}^{\lambda}$; par minimalité de $M_{\mathfrak{L}}$, le corps $M_{\mathfrak{L}}$ est donc inclus dans $M_{\mathfrak{L}}^{\lambda}$. Ainsi, les corps $M_{\mathfrak{L}}$ et $M_{\mathfrak{L}}^{\lambda}$ coïncident et le groupe $\Phi_{\mathcal{L}}$ s'identifie au sous-groupe d'inertie en $\mathfrak{L}$ de l'extension abélienne K^{λ}/K. En particulier, le groupe $\Phi_{\mathfrak{L}}$ est cyclique et son ordre divise $p-1$.

Par ailleurs, que ℓ soit égal ou différent de p, le groupe $\Phi_{\mathcal{L}}$ s'identifie à un sous-groupe du groupe des automorphismes de la courbe elliptique définie sur $\overline{k_{\mathfrak{L}}}$ qu'on obtient par réduction de $E \times_K M_{\mathfrak{L}}$ ([14], §2, démonstration du théorème 2, p. 497). On note $\widetilde{E}_{\mathfrak{L}}$ cette courbe elliptique réduite et $\mathrm{Aut}(\widetilde{E}_{\mathfrak{L}})$ son groupe d'automorphismes. Le groupe $\mathrm{Aut}(\widetilde{E}_{\mathfrak{L}})$ dépend de l'invariant j de $\widetilde{E}_{\mathfrak{L}}$, qui est égal à la classe de $j(E)$ modulo $\mathfrak{L}$, de la manière suivante ([15] appendice A, proposition 1.2 et exercice A.1) :

- si $j(E)$ est différent de 0 et 1728 modulo $\mathfrak{L}$, $\mathrm{Aut}(\widetilde{E}_{\mathfrak{L}})$ est cyclique d'ordre 2 ;
- si ℓ est différent de 2 et de 3 et $j(E)$ est congru à 1728 modulo $\mathfrak{L}$, $\mathrm{Aut}(\widetilde{E}_{\mathfrak{L}})$ est cyclique d'ordre 4 ;
- si ℓ est différent de 2 et de 3 et $j(E)$ est congru à 0 modulo $\mathfrak{L}$, $\mathrm{Aut}(\widetilde{E}_{\mathfrak{L}})$ est cyclique d'ordre 6 ;
- si ℓ est égal à 3 et $j(E)$ est congru à $0 = 1728$ modulo $\mathfrak{L}$, $\mathrm{Aut}(\widetilde{E}_{\mathfrak{L}})$ est un groupe d'ordre 12, produit semi-direct d'un groupe cyclique d'ordre 3 par un groupe cyclique d'ordre 4 (le deuxième agissant sur le premier de l'unique manière non triviale) ; on vérifie que les sous-groupes cycliques d'un tel groupe sont d'ordre 1, 2, 3, 4 ou 6 ;
- si ℓ est égal à 2 et $j(E)$ est congru à $0 = 1728$ modulo $\mathfrak{L}$, $\mathrm{Aut}(\widetilde{E}_{\mathfrak{L}})$ est un groupe d'ordre 24, produit semi-direct du groupe des quaternions (d'ordre 8) par un groupe cyclique d'ordre 3 (le deuxième agissant sur le premier en permutant les générateurs) ; on vérifie que les sous-groupes cycliques d'un tel groupe sont également d'ordre 1, 2, 3, 4 ou 6.

On déduit de ce qui précède que pour tout ℓ, le groupe $\Phi_{\mathfrak{L}}$ est cyclique d'ordre 1, 2, 3, 4 ou 6. On note $e_{\mathfrak{L}}$ l'ordre de $\Phi_{\mathcal{L}}$; il est donc dans l'ensemble $\{1, 2, 3, 4, 6\}$ et vérifie :

- $e_{\mathfrak{L}}$ est égal à 1 si et seulement si E a bonne réduction en $\mathfrak{L}$;
- si $e_{\mathfrak{L}}$ est égal à 4, alors $j(E)$ est congru à 1728 modulo $\mathfrak{L}$;
- si $e_{\mathfrak{L}}$ est égal à 3 ou 6, alors $j(E)$ est congru à 0 modulo $\mathfrak{L}$;
- si ℓ est différent de p, alors $e_{\mathfrak{L}}$ est l'ordre de $\lambda(I_{\mathfrak{L}})$ et divise $p-1$.

1.2 Action des sous-groupes d'inertie des places au-dessus de p

Soit $\mathfrak{p}$ un idéal premier de K situé au-dessus de p ; on reprend les notations 1.1. Cette partie précise la proposition 3.2 (§ 3.1) de [4] qui décrit la restriction de la puissance douzième du caractère d'isogénie à un sous-groupe d'inertie $I_{\mathfrak{p}}$ associé à $\mathfrak{p}$.

Proposition 1.2. *On suppose que E a potentiellement réduction multiplicative en $\mathfrak{p}$. Alors*

1. *le caractère* $\lambda^{e_\mathfrak{p}}$ *restreint à* $I_\mathfrak{p}$ *est trivial ou égal à* $\chi_p^{e_\mathfrak{p}}$;
2. *en particulier* λ^2 *restreint à* $I_\mathfrak{p}$ *est trivial ou égal à* χ_p^2.

Lorsque p *est supérieur ou égal à* 17*, il existe un unique entier* $a_\mathfrak{p}$ *valant* 0 *ou* 12 *tel que le caractère* λ^{12} *restreint à* $I_\mathfrak{p}$ *coïncide avec* $\chi_p^{a_\mathfrak{p}}$.

Démonstration. Soit $K'_\mathfrak{p}$ l'unique extension de $K_\mathfrak{p}$ de degré inférieur ou égal à 2 sur laquelle E est isomorphe à une courbe de Tate (voir partie 1.1.1) ; on note $I'_\mathfrak{p}$ le sous-groupe d'inertie de $D_\mathfrak{p}$ associé à $K'_\mathfrak{p}$.

D'après [13] (proposition 13 de §1.12 et page 273 de §1.11), le caractère λ restreint au sous-groupe $I'_\mathfrak{p}$ est soit trivial soit égal au caractère cyclotomique χ_p. Par définition de $e_\mathfrak{p}$ (partie 1.1.1), $I'_\mathfrak{p}$ est un sous-groupe d'indice $e_\mathfrak{p}$ de $I_\mathfrak{p}$; on en déduit le premier point de la proposition ; le second découle du fait que $e_\mathfrak{p}$ est égal à 1 ou 2. □

Proposition 1.3. *On suppose que* E *a potentiellement bonne réduction en* $\mathfrak{p}$*. Alors il existe un entier* $r_\mathfrak{p}$ *compris entre* 0 *et* $e_\mathfrak{p}$ *tel que le caractère* $\lambda^{e_\mathfrak{p}}$ *restreint au sous-groupe d'inertie* $I_\mathfrak{p}$ *coïncide avec* $\chi_p^{r_\mathfrak{p}}$ *(les couples* $(e_\mathfrak{p}, r_\mathfrak{p})$ *possibles, ainsi que des informations supplémentaires pour certains cas, sont rassemblés dans le tableau suivant). En particulier, lorsque* p *est supérieur ou égal à* 17*, il existe un unique entier* $a_\mathfrak{p}$ *dans l'ensemble* $\{0, 4, 6, 8, 12\}$ *tel que le caractère* λ^{12} *restreint à* $I_\mathfrak{p}$ *coïncide avec* $\chi_p^{a_\mathfrak{p}}$.

<table>
<tr><th>$e_\mathfrak{p}$</th><th>$r_\mathfrak{p}$</th><th>$a_\mathfrak{p} = \frac{12}{e_\mathfrak{p}} r_\mathfrak{p}$</th><th>$p$</th><th>$j(E)$</th><th>Type de réduction semi-stable en $\mathfrak{p}$</th></tr>
<tr><td rowspan="2">1</td><td>0</td><td>0</td><td rowspan="2">–</td><td rowspan="2">–</td><td rowspan="2">–</td></tr>
<tr><td>1</td><td>12</td></tr>
<tr><td rowspan="2">2</td><td>0</td><td>0</td><td rowspan="2">–</td><td rowspan="2">–</td><td rowspan="2">–</td></tr>
<tr><td>2</td><td>12</td></tr>
<tr><td rowspan="4">3</td><td>0</td><td>0</td><td>$p \equiv 1 \mod 3$</td><td rowspan="4">$j(E) \equiv 0 \mod \mathfrak{p}$</td><td>ordinaire</td></tr>
<tr><td>1</td><td>4</td><td rowspan="2">$p \equiv 2 \mod 3$</td><td rowspan="2">supersingulier</td></tr>
<tr><td>2</td><td>8</td></tr>
<tr><td>3</td><td>12</td><td>$p \equiv 1 \mod 3$</td><td>ordinaire</td></tr>
<tr><td rowspan="3">4</td><td>0</td><td>0</td><td>$p \equiv 1 \mod 4$</td><td rowspan="3">$j(E) \equiv 1728 \mod \mathfrak{p}$</td><td>ordinaire</td></tr>
<tr><td>2</td><td>6</td><td>$p \equiv 3 \mod 4$</td><td>supersingulier</td></tr>
<tr><td>4</td><td>12</td><td>$p \equiv 1 \mod 4$</td><td>ordinaire</td></tr>
<tr><td rowspan="4">6</td><td>0</td><td>0</td><td>$p \equiv 1 \mod 3$</td><td rowspan="4">$j(E) \equiv 0 \mod \mathfrak{p}$</td><td>ordinaire</td></tr>
<tr><td>2</td><td>4</td><td rowspan="2">$p \equiv 2 \mod 3$</td><td rowspan="2">supersingulier</td></tr>
<tr><td>4</td><td>8</td></tr>
<tr><td>6</td><td>12</td><td>$p \equiv 1 \mod 3$</td><td>ordinaire</td></tr>
</table>

Démonstration. Pour l'existence et les valeurs possibles de $r_\mathfrak{p}$ et $a_\mathfrak{p}$ et les trois premières colonnes du tableau, on renvoie à la démonstration de la proposition 3.2 (§ 3.1) de [4] (voir aussi la remarque 1 de la partie 2 de [10]).

Pour la quatrième colonne, la démonstration de la proposition 3.2 de [4] donne qu'il existe un entier $a'_{\mathfrak{p}}$ satisfaisant la congruence $e_{\mathfrak{p}} a'_{\mathfrak{p}} \equiv r_{\mathfrak{p}} \mod p-1$. Alors :

- si 3 divise $e_{\mathfrak{p}}$ et $r_{\mathfrak{p}}$ (couples $(3,0)$, $(3,3)$, $(6,0)$ et $(6,6)$), alors 3 divise $p-1$, donc p est congru à 1 modulo 3 ;
- si 3 divise $e_{\mathfrak{p}}$ et ne divise pas $r_{\mathfrak{p}}$ (couples $(3,1)$, $(3,2)$, $(6,2)$ et $(6,4)$), alors 3 ne divise pas $p-1$, donc p est congru à 2 modulo 3 ;
- si $e_{\mathfrak{p}}$ est égal à 4 et divise $r_{\mathfrak{p}}$ (couples $(4,0)$ et $(4,4)$), alors 4 divise $p-1$ donc p est congru à 1 modulo 4 ;
- si $e_{\mathfrak{p}}$ est égal à 4 et ne divise pas $r_{\mathfrak{p}}$ (couple $(4,2)$), alors 4 ne divise pas $p-1$ donc p est congru à 3 modulo 4.

Pour la cinquième colonne, la discussion de la partie 1.1.2 donne :

- si $e_{\mathfrak{p}}$ est égal à 4, alors $j(E)$ est congru à 1728 modulo $\mathfrak{p}$;
- si 3 divise $e_{\mathfrak{p}}$, alors $j(E)$ est congru à 0 modulo $\mathfrak{p}$.

Enfin, la dernière colonne résulte de la détermination de l'invariant de Hasse des courbes d'invariant j égal 0 ou 1728 sur un corps fini de caractéristique p (supérieur ou égal à 5 ; voir [15], §V.4, exemples 4.4 et 4.5). En effet, soit k un corps fini de caractéristique p ; alors :

- la courbe elliptique définie sur k par l'équation $y^2 = x^3 + 1$, d'invariant j égal à 0, est ordinaire si et seulement si p est congru à 1 modulo 3 ;
- la courbe elliptique définie sur k par l'équation $y^2 = x^3 + x$, d'invariant j égal à 1728, est ordinaire si et seulement si p est congru à 1 modulo 4.

□

1.3 Ramification et action du frobenius aux places hors de p

Soient q un nombre premier rationnel différent de p et $\mathfrak{q}$ un idéal premier de K au-dessus de q.

1.3.1 Lorsque $j(E)$ n'est pas entier en $\mathfrak{q}$

Proposition 1.4. *On suppose que E a potentiellement réduction multiplicative en $\mathfrak{q}$. Alors :*

1. *le groupe $\lambda(I_{\mathfrak{q}})$ est d'ordre $e_{\mathfrak{q}}$; en particulier, le caractère λ^{12} est non ramifié en $\mathfrak{q}$;*
2. *$\lambda^2(\sigma_{\mathfrak{q}})$ vaut 1 ou $(N\mathfrak{q})^2$ modulo p.*

Démonstration. La proposition 3.3 (§3.2.1) de [4] donne la deuxième assertion et que $\lambda(I_{\mathfrak{q}})$ est d'ordre au plus 2. Comme $e_{\mathfrak{q}}$ est égal à 1 ou 2 (voir partie 1.1.1), il ne reste qu'à prouver qu'on ne peut avoir à la fois $e_{\mathfrak{q}}$ égal à 2 et $\lambda(I_{\mathfrak{q}})$ trivial.

Supposons par l'absurde que c'est le cas. Alors, avec les notations de la partie 1.1, E a mauvaise réduction additive sur $K_{\mathfrak{q}}$ et l'extension K^{λ}/K est non ramifiée en $\mathfrak{q}$. Ceci implique qu'en toute place de K^{λ} au-dessus de $\mathfrak{q}$, E a mauvaise réduction additive ([15] §VII.5 proposition 5.4). On obtient alors une contradiction avec le lemme 1. □

1.3.2 Lorsque $j(E)$ est entier en $\mathfrak{q}$

On suppose dans cette partie que l'invariant j de E est entier en $\mathfrak{q}$, c'est-à-dire que E a potentiellement bonne réduction en $\mathfrak{q}$.

La proposition suivante résulte de la discussion de la partie 1.1.2.

Proposition 1.5. *On suppose que E a potentiellement bonne réduction en $\mathfrak{q}$. Alors le groupe $\lambda(I_\mathfrak{q})$ est d'ordre $e_\mathfrak{q}$; en particulier, le caractère λ^{12} est non ramifié en $\mathfrak{q}$.*

La proposition suivante est le théorème 3 (§2) de [14].

Proposition 1.6. *On suppose que E a potentiellement bonne réduction en $\mathfrak{q}$. Alors le polynôme caractéristique de l'action de $\sigma_\mathfrak{q}$ sur le module de Tate en p de E est à coefficients dans $\mathbb{Z}$ (et indépendant de p) ; ses racines ont pour valeur absolue complexe $\sqrt{N\mathfrak{q}}$.*

Notations 1.7.

1. On note $P_\mathfrak{q}(X)$ le polynôme caractéristique de l'action de $\sigma_\mathfrak{q}$ sur le module de Tate en p de E. Comme le déterminant de la représentation de G_K sur le module de Tate en p de E est le caractère cyclotomique (à valeurs dans $\mathbb{Z}_p^\times$), $P_\mathfrak{q}(X)$ est de la forme $X^2 - T_\mathfrak{q}X + N\mathfrak{q}$ avec $T_\mathfrak{q}$ un entier de valeur absolue inférieure ou égale à $2\sqrt{N\mathfrak{q}}$. Son discriminant $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ est donc un entier négatif et ses racines sont conjuguées complexes l'une de l'autre.
2. On note $L^\mathfrak{q}$ le sous-corps engendré dans $\mathbb{C}$ par les racines de $P_\mathfrak{q}(X)$; le corps $L^\mathfrak{q}$ est soit $\mathbb{Q}$ soit un corps quadratique imaginaire.

Proposition 1.8. *On suppose que E a potentiellement bonne réduction en $\mathfrak{q}$. Soit $\mathcal{P}^\mathfrak{q}$ un idéal premier de $L^\mathfrak{q}$ au-dessus de p. Alors les images dans $\mathcal{O}_{L^\mathfrak{q}}/\mathcal{P}^\mathfrak{q}$ des racines de $P_\mathfrak{q}(X)$ sont dans $\mathbb{F}_p^\times$; il existe une racine $\beta_\mathfrak{q}$ de $P_\mathfrak{q}(X)$ vérifiant :*

$$\left(\lambda(\sigma_\mathfrak{q}), \left(\chi_p\lambda^{-1}\right)(\sigma_\mathfrak{q})\right) = \left(\beta_\mathfrak{q} \mod \mathcal{P}^\mathfrak{q}, \overline{\beta_\mathfrak{q}} \mod \mathcal{P}^\mathfrak{q}\right).$$

Démonstration. Soit $\widetilde{P_\mathfrak{q}}(X)$ la réduction modulo p de $P_\mathfrak{q}(X)$. Alors $\widetilde{P_\mathfrak{q}}(X)$ est le polynôme caractéristique de $\varphi_{E,p}(\sigma_\mathfrak{q})$; il est donc scindé dans $\mathbb{F}_p$ et ses racines sont $\lambda(\sigma_\mathfrak{q})$ et $\chi_p\lambda^{-1}(\sigma_\mathfrak{q})$. D'autre part, $\widetilde{P_\mathfrak{q}}(X)$ est aussi la réduction modulo $\mathcal{P}^\mathfrak{q}$ de $P_\mathfrak{q}(X)$, dont les racines dans le corps $\mathcal{O}_{L^\mathfrak{q}}/\mathcal{P}^\mathfrak{q}$ sont les classes modulo $\mathcal{P}^\mathfrak{q}$ des racines de $P_\mathfrak{q}(X)$ dans $L^\mathfrak{q}$. □

Remarques 1.9.

1. Le corps $L^\mathfrak{q}$ est égal à $\mathbb{Q}$ si et seulement si le discriminant $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ est nul ; lorsque c'est le cas, $P_\mathfrak{q}(X)$ a une racine double, appartenant à $\mathbb{Z}$, égale à $T_\mathfrak{q}/2$ et $N\mathfrak{q}$ est le carré de $T_\mathfrak{q}/2$; ceci implique notamment que le degré résiduel de $\mathfrak{q}$ dans l'extension $K/\mathbb{Q}$ est pair et que E a potentiellement bonne réduction supersingulière en $\mathfrak{q}$.
2. Plus généralement, la courbe E a potentiellement bonne réduction supersingulière en $\mathfrak{q}$ si et seulement si q divise $T_\mathfrak{q}$. Lorsque $\mathfrak{q}$ est de degré 1 dans $K/\mathbb{Q}$, q divise $T_\mathfrak{q}$ si et seulement si $((T_\mathfrak{q} = 0)$ ou $(q = 2$ et $(T_\mathfrak{q} = 0,$ 2 ou $-2))$ ou $(q = 3$ et $(T_\mathfrak{q} = 0,$ 3 ou $-3))$.

3. Le polynôme caractéristique de $\varphi_{E,p}(\sigma_{\mathfrak{q}})$ est scindé dans $\mathbb{F}_p$ et égal à $P_{\mathfrak{q}}(X)$ modulo p ; l'entier $T_{\mathfrak{q}}^2 - 4N\mathfrak{q}$ est donc un carré modulo p. On en déduit que soit p divise $T_{\mathfrak{q}}^2 - 4N\mathfrak{q}$, soit $L^{\mathfrak{q}}$ est un corps quadratique imaginaire dans lequel p est décomposé (les deux cas ne s'excluant pas).

2 Compatibilité en et hors de p

Notations 2.1. Dans toute la suite du texte, on note μ la puissance douzième du caractère d'isogénie λ ; on rappelle (notations 1.1) que K^{λ} désigne l'extension abélienne de K trivialisant le caractère λ et on note K^{μ} l'extension de K trivialisant μ. Le corps K^{μ} est inclus dans le corps K^{λ} et l'extension K^{λ}/K^{μ} est cyclique, de degré divisant le pgcd de 12 et $p-1$; l'extension K^{μ}/K est cyclique et d'ordre divisant $p-1$. On note $\overline{\mu}$ le morphisme de groupes injectif du groupe de Galois $\mathrm{Gal}(K^{\mu}/K)$ dans $\mathbb{F}_p^{\times}$ induit par μ.

2.1 Théorie du corps de classes pour le caractère μ

La théorie du corps de classes globale appliquée à l'extension abélienne K^{μ}/K fournit un morphisme de groupes du groupe des idèles de K dans le groupe de Galois $\mathrm{Gal}(K^{\mu}/K)$ qui est continu, surjectif et trivial sur les idèles diagonales. On note r ce morphisme.

Notations 2.2. On note $\mathbb{A}_K^{\times}$ le groupe des idèles de K. Soit ν une place (finie ou infinie) de K. On note K_{ν} le complété de K en ν et r_{ν} la composée de l'injection de $K_{\nu}^{\times}$ dans les idèles $\mathbb{A}_K^{\times}$ et de l'application de réciprocité r introduite ci-dessus. Lorsque ν est une place finie, on note $U_{K_{\nu}}$ les unités du corps local K_{ν} ; dans ce cas, on utilise indifféremment en indice la place ν et l'idéal maximal de K qui lui correspond.

2.1.1 En une place infinie

Soit ν une place infinie de K ; alors l'application r_{ν} est triviale.

En effet, soit r'_{ν} le morphisme de groupes de $K_{\nu}^{\times}$ dans $\mathrm{Gal}(K^{\lambda}/K)$ associé de manière analogue à l'extension abélienne K^{λ}/K. Alors r_{ν} est égale à la puissance douzième de la composée de r'_{ν} et de la surjection naturelle de $\mathrm{Gal}(K^{\lambda}/K)$ dans $\mathrm{Gal}(K^{\mu}/K)$. Comme ν est une place infinie, l'application r'_{ν} a pour image un groupe d'ordre divisant 2 ; on en déduit que r_{ν} est triviale.

2.1.2 En une place hors de p

Soit $\mathfrak{q}$ un idéal maximal de K qui n'est pas au-dessus de p.

D'après l'étude locale menée dans la partie 1, l'extension K^{μ}/K est non ramifiée en $\mathfrak{q}$ (propositions 1.4 et 1.5). Ceci implique que l'application $r_{\mathfrak{q}}$ est triviale sur les unités $U_{K_{\mathfrak{q}}}$. Soit $\overline{\sigma}_{\mathfrak{q}}$ la restriction de $\sigma_{\mathfrak{q}}$ à K^{μ} ; alors $\overline{\sigma}_{\mathfrak{q}}$ est l'unique élément de Frobenius de $\mathrm{Gal}(K^{\mu}/K)$ associé à $\mathfrak{q}$; l'application $r_{\mathfrak{q}}$ envoie toute uniformisante de $K_{\mathfrak{q}}$ sur $\overline{\sigma}_{\mathfrak{q}}$.

2.1.3 En une place au-dessus de p

Soit $\mathfrak{p}$ un idéal premier de K au-dessus de p ; alors le morphisme $\overline{\mu}\circ r_{\mathfrak{p}}$ coïncide sur les unités $U_{K_{\mathfrak{p}}}$ avec la composée suivante :

$$U_{K_{\mathfrak{p}}} \xrightarrow{N_{K_{\mathfrak{p}}/\mathbb{Q}_p}} U_{\mathbb{Q}_p} \xrightarrow[\text{modulo } p]{\text{réduction}} \mathbb{F}_p^{\times} \xrightarrow[\text{à la puissance } -a_{\mathfrak{p}}]{\text{élévation}} \mathbb{F}_p^{\times}.$$

2.2 Loi de réciprocité pour le caractère μ

Notations 2.3. Pour toute place ν de K, on note ι_ν le plongement de K dans le complété K_ν. Pour tout idéal maximal $\mathfrak{L}$ de K, on note $\mathrm{val}_{\mathfrak{L}}$ la valuation de K associée à $\mathfrak{L}$ dont l'image est $\mathbb{Z}$.

Proposition 2.4. *Soient α un élément de K non nul et premier à p et $\prod_{\mathfrak{q}\nmid p}\mathfrak{q}^{\mathrm{val}_{\mathfrak{q}}(\alpha)}$ la décomposition de l'idéal fractionnaire $\alpha\mathcal{O}_K$ en produit d'idéaux premiers de K. Alors on a :*

$$\prod_{\mathfrak{q}\nmid p}\mu\left(\sigma_{\mathfrak{q}}\right)^{\mathrm{val}_{\mathfrak{q}}(\alpha)} = \prod_{\mathfrak{p}\mid p} N_{K_{\mathfrak{p}}/\mathbb{Q}_p}\left(\iota_{\mathfrak{p}}(\alpha)\right)^{a_{\mathfrak{p}}} \mod p.$$

Démonstration. L'image par r de l'idèle principale $(\iota_\nu(\alpha))_\nu$ est triviale. On détermine l'image de $\iota_\nu(\alpha)$ par $\overline{\mu}\circ r_\nu$ pour les différentes places ν de K en utilisant la partie 2.1.

- Si ν est une place infinie de K, l'application r_ν est triviale, donc $\overline{\mu}\circ r_\nu(\iota_\nu(\alpha))$ l'est également.
- Si $\mathfrak{q}$ est un idéal maximal de K premier à p, alors $\iota_{\mathfrak{q}}(\alpha)$ est un élément de $K_{\mathfrak{q}}^{\times}$ de valuation $\mathrm{val}_{\mathfrak{q}}(\alpha)$; son image par $r_{\mathfrak{q}}$ est $\overline{\sigma}_{\mathfrak{q}}^{\mathrm{val}_{\mathfrak{q}}(\alpha)}$ et son image par $\overline{\mu}\circ r_{\mathfrak{q}}$ est $\overline{\mu}\left(\overline{\sigma}_{\mathfrak{q}}\right)^{\mathrm{val}_{\mathfrak{q}}(\alpha)}$.
- Si $\mathfrak{p}$ est un idéal maximal de K au-dessus de p, alors, α étant supposé premier à p, $\iota_{\mathfrak{p}}(\alpha)$ est une unité de $K_{\mathfrak{p}}$; on a donc $\overline{\mu}\circ r_{\mathfrak{p}}(\iota_{\mathfrak{p}}(\alpha)) = N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\iota_{\mathfrak{p}}(\alpha))^{-a_{\mathfrak{p}}}$ mod p.

Finalement on a (tous les produits étant finis) :

$$\begin{aligned}
1 &= \overline{\mu}\circ r\left(\left(\iota_\nu(\alpha)\right)_\nu\right)\\
&= \overline{\mu}\left(\prod_\nu r_\nu\left(\iota_\nu(\alpha)\right)\right)\\
&= \prod_\nu \overline{\mu}\circ r_\nu\left(\iota_\nu(\alpha)\right)\\
&= \prod_{\nu\mid\infty} 1 \times \prod_{\mathfrak{q}\nmid p}\overline{\mu}\circ r_{\mathfrak{q}}\left(\iota_{\mathfrak{q}}(\alpha)\right) \times \prod_{\mathfrak{p}\mid p}\overline{\mu}\circ r_{\mathfrak{p}}\left(\iota_{\mathfrak{p}}(\alpha)\right)\\
&= \prod_{\mathfrak{q}\nmid p}\overline{\mu}\left(\overline{\sigma}_{\mathfrak{q}}\right)^{\mathrm{val}_{\mathfrak{q}}(\alpha)} \times \prod_{\mathfrak{p}\mid p}\left(N_{K_{\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}}\left(\iota_{\mathfrak{p}}(\alpha)\right)^{-a_{\mathfrak{p}}} \mod p\right)\\
&= \prod_{\mathfrak{q}\nmid p}\overline{\mu}\left(\overline{\sigma}_{\mathfrak{q}}\right)^{\mathrm{val}_{\mathfrak{q}}(\alpha)} \times \left(\left(\prod_{\mathfrak{p}\mid p} N_{K_{\mathfrak{p}}/\mathbb{Q}_{\mathfrak{p}}}\left(\iota_{\mathfrak{p}}(\alpha)\right)^{a_{\mathfrak{p}}}\right) \mod p\right)^{-1}.
\end{aligned}$$

Avec l'égalité $\mu\left(\sigma_{\mathfrak{q}}\right) = \overline{\mu}\left(\overline{\sigma}_{\mathfrak{q}}\right)$ pour tout idéal maximal de K premier à p, on obtient le résultat de la proposition. □

Notations 2.5.

1. Dans tout la suite du texte, on suppose que l'extension $K/\mathbb{Q}$ est galoisienne ; on note G son groupe de Galois.
2. On fixe également pour toute la suite du texte un idéal $\mathfrak{p}_0$ de K au-dessus de p.
3. Pour tout élément τ de G, on note a_τ l'entier $a_\mathfrak{p}$ associé à l'idéal $\mathfrak{p} = \tau^{-1}(\mathfrak{p}_0)$.
4. On note $\mathcal{N}$ l'application de K dans lui-même qui envoie un élément α sur la norme tordue par les entiers $(a_\tau)_{\tau\in G}$: $\mathcal{N}(\alpha) = \prod_{\tau\in G}\tau(\alpha)^{a_\tau}$. On note que l'application $\mathcal{N}$ préserve $K^\times$, $\mathcal{O}_K$ et les éléments de K premiers à p.

Avec ces notations, la proposition 2.4 admet la reformulation globale suivante (qui redonne le lemme 1 du §2 de [10]).

Proposition 2.6. *Soient α un élément de K non nul et premier à p et $\prod_{\mathfrak{q}\nmid p}\mathfrak{q}^{\mathrm{val}_\mathfrak{q}(\alpha)}$ la décomposition de l'idéal fractionnaire $\alpha\mathcal{O}_K$ en produit d'idéaux premiers de K. Alors on a :*

$$\prod_{\mathfrak{q}\nmid p}\mu\left(\sigma_\mathfrak{q}\right)^{\mathrm{val}_\mathfrak{q}(\alpha)} = \iota_{\mathfrak{p}_0}\left(\mathcal{N}(\alpha)\right) \mod \mathfrak{p}_0.$$

Démonstration. On vérifie que l'élément $\prod_{\mathfrak{p}|p}N_{K_\mathfrak{p}/\mathbb{Q}_p}\left(\iota_\mathfrak{p}(\alpha)\right)^{a_\mathfrak{p}}$ de $\mathbb{Z}_p$ est l'image par l'injection canonique $\iota_{\mathfrak{p}_0}$ de K dans son complété $K_{\mathfrak{p}_0}$ de l'élément $\prod_{\tau\in G}\tau(\alpha)^{a_\tau}$ de K. □

2.3 Une borne pour la hauteur des associés d'un entier

Notation 2.7. Soit α un élément non nul de K. On note H la hauteur absolue de α définie par

$$\mathrm{H}(\alpha) = \left(\prod_{\nu \text{ place de } K}\max\left(1, |\alpha|_\nu\right)\right)^{1/d_K},$$

avec les normalisations suivantes pour les valeurs absolues $|\cdot|_\nu$:

- si ν est une place réelle, correspondant à un élément τ de G, on pose $|\cdot|_\nu = |\tau(\cdot)|_\mathbb{C}$;
- si ν est une place complexe, correspondant à un élément τ de G, on pose $|\cdot|_\nu = |\tau(\cdot)|_\mathbb{C}^2$;
- si ν est une place finie, correspondant à un idéal maximal $\mathfrak{L}$ de K, on pose $|\cdot|_\nu = (N\mathfrak{L})^{-\mathrm{val}_\mathfrak{L}(\cdot)}$.

On remarque que lorsque α est entier dans K, les seules places apportant une contribution non triviale dans le produit définissant $\mathrm{H}(\alpha)$ sont les places infinies.

Lemme 2. *Soit α un élément non nul de $\mathcal{O}_K$; alors, pour tout τ dans G, on a :*

$$\left|\tau\left(\mathcal{N}(\alpha)\right)\right|_\mathbb{C} \le \mathrm{H}(\alpha)^{12d_K}.$$

Démonstration. Soit τ dans G fixé ; on a :

$$\tau\left(\mathcal{N}(\alpha)\right) = \tau\left(\prod_{\tau'\in G}\tau'(\alpha)^{a_{\tau'}}\right) = \prod_{\tau'\in G}\tau'(\alpha)^{a_{\tau^{-1}\tau'}},$$

Pour tout τ' dans G, on a ($a_{\tau^{-1}\tau'}$ étant un entier compris entre 0 et 12)) :

$$\left|\tau'\left(\alpha\right)\right|_{\mathbb{C}}^{a_{\tau^{-1}\tau'}} \leq \left(\max\left(1,\left|\tau'\left(\alpha\right)\right|_{\mathbb{C}}\right)\right)^{a_{\tau^{-1}\tau'}} \leq \left(\max\left(1,\left|\tau'\left(\alpha\right)\right|_{\mathbb{C}}\right)\right)^{12}.$$

Comme le corps K est supposé galoisien sur $\mathbb{Q}$, ses places infinies sont soit toutes réelles, soit toutes complexes.

Lorsque toutes les places de K sont réelles, il y en a exactement d_K, qui correspondent bijectivement aux éléments de G ; on a alors :

$$\begin{aligned}\left|\tau\left(\mathcal{N}(\alpha)\right)\right|_{\mathbb{C}} = \prod_{\tau'\in G}\left|\tau'(\alpha)\right|_{\mathbb{C}}^{a_{\tau^{-1}\tau'}} &\leq \left(\prod_{\tau'\in G}\max\left(1,\left|\tau'\left(\alpha\right)\right|_{\mathbb{C}}\right)\right)^{12}\\ &\leq \left(\prod_{\nu\mid\infty}\max\left(1,\left|\alpha\right|_{\nu}\right)\right)^{12} = \mathrm{H}(\alpha)^{12d_K}.\end{aligned}$$

Lorsque toutes les places de K sont complexes, le degré d_K de K sur $\mathbb{Q}$ est pair et la conjugaison complexe induit dans G un élément c d'ordre 2. Le corps K a exactement $d_K/2$ places infinies ; deux éléments de G définissent la même place infinie si et seulement s'ils sont égaux ou conjugués complexes l'un de l'autre. On fixe un système $\widetilde{G}$ de représentants de G modulo le sous-groupe d'ordre 2 engendré par c. On a alors :

$$\begin{aligned}\left|\tau\left(\mathcal{N}(\alpha)\right)\right|_{\mathbb{C}} &= \prod_{\tau'\in\widetilde{G}}\left|\tau'(\alpha)\right|_{\mathbb{C}}^{a_{\tau^{-1}\tau'}}\left|c\tau'(\alpha)\right|_{\mathbb{C}}^{a_{\tau^{-1}c\tau'}}\\ &\leq \left(\prod_{\tau'\in\widetilde{G}}\max\left(1,\left|\tau'\left(\alpha\right)\right|_{\mathbb{C}}\right)\max\left(1,\left|c\tau'\left(\alpha\right)\right|_{\mathbb{C}}\right)\right)^{12}\\ &\leq \left(\prod_{\tau'\in\widetilde{G}}\max\left(1,\left|\tau'\left(\alpha\right)\right|_{\mathbb{C}}\right)^{2}\right)^{12}\\ &\leq \left(\prod_{\tau'\in\widetilde{G}}\max\left(1,\left|\tau'\left(\alpha\right)\right|_{\mathbb{C}}^{2}\right)\right)^{12}\\ &\leq \left(\prod_{\nu\mid\infty}\max\left(1,\left|\alpha\right|_{\nu}\right)\right)^{12} = \mathrm{H}(\alpha)^{12d_K}.\end{aligned}$$

□

Notations 2.8. Suivant [2], on note :
- R_K le régulateur de K ;
- r_K le rang du groupe des unités de K (r_K vaut $d_K - 1$ si K est totalement réel et $\frac{d_K}{2} - 1$ sinon) ;

- δ_K un réel strictement positif minorant $d_K \ln(\mathrm{H}(\alpha))$ pour tout élément non nul α de K qui n'est pas une racine de l'unité ; si d_K vaut 1 ou 2, on peut prendre δ_K égal à $\frac{\ln 2}{r_K+1}$; si d_K est supérieur ou égal à 3, on peut prendre δ_K égal à $\frac{1}{53 d_K \ln(6 d_K)}$ ou $\frac{1}{1201}\left(\frac{\ln(\ln d_K)}{\ln d_K}\right)^3$.

Définition 2.9 (Borne $C_1(K)$). On pose :

$$C_1(K) = \frac{r_K^{r_K+1}\delta_K^{-(r_K-1)}}{2}.$$

On remarque que $C_1(K)$ peut s'exprimer en n'utilisant que le degré d_K de K sur $\mathbb{Q}$. Avec ces notations, le lemme 2 (partie 3) de [2] s'écrit de la manière suivante.

Lemme 3. *Pour tout élément non nul α de $\mathcal{O}_K$, il existe une unité u de K vérifiant :*

$$\mathrm{H}(u\alpha) \leq \left|N_{K/\mathbb{Q}}(\alpha)\right|^{1/d_K} \exp\left(C_1(K)R_K\right).$$

2.4 Type de réduction en une place hors de p et action de l'inertie en p

Dans cette partie, on suit le raisonnement de la partie 2 de [10] pour établir un lien entre les actions sur le groupe d'isogénie du frobenius en une place hors de p d'une part et des sous-groupes d'inertie aux places au-dessus de p d'autre part ; ce lien est valide lorsque p est pris strictement plus grand qu'une borne dont on détermine une forme explicite.

Définition 2.10 (Borne $C_2(K)$). On définit :

$$C_2(K) = \exp\left(12 d_K C_1(K) R_K\right).$$

On remarque que le nombre réel $C_2(K)$ ne dépend que du degré et du régulateur de K. On rappelle (notations de l'introduction) que h_K désigne le nombre de classes d'idéaux de K.

Proposition 2.11. *Soit $\mathfrak{L}$ un idéal maximal de K. Il existe un générateur $\gamma_{\mathfrak{L}}$ de $\mathfrak{L}^{h_K}$ satisfaisant pour tout τ dans G :*

$$\left|\tau\left(\mathcal{N}(\gamma_{\mathfrak{L}})\right)\right|_{\mathbb{C}} \leq (N\mathfrak{L})^{12h_K} C_2(K).$$

Démonstration. Étant donné un générateur quelconque de $\mathfrak{L}^{h_K}$, on peut le multiplier par une unité donnée par le lemme 3 pour obtenir un générateur $\gamma_{\mathfrak{L}}$ qui vérifie :

$$\mathrm{H}(\gamma_{\mathfrak{L}}) \leq \left|N_{K/\mathbb{Q}}(\gamma_{\mathfrak{L}})\right|^{1/d_K} \exp\left(C_1(K)R_K\right).$$

Comme $\gamma_{\mathfrak{L}}$ engendre dans $\mathcal{O}_K$ l'idéal $\mathfrak{L}^{h_K}$, la norme de $\gamma_{\mathfrak{L}}$ dans l'extension $K/\mathbb{Q}$ est un entier relatif égal ou opposé à $(N\mathfrak{L})^{h_K}$. D'après le lemme 2, on a pour tout τ dans G :

$$\left|\tau\left(\mathcal{N}(\gamma_{\mathfrak{L}})\right)\right|_{\mathbb{C}} \leq \mathrm{H}(\gamma_{\mathfrak{L}})^{12 d_K},$$

d'où

$$
\begin{aligned}
|\tau(\mathcal{N}(\gamma_{\mathfrak{L}}))|_{\mathbb{C}} &\leq \left|N_{K/\mathbb{Q}}(\gamma_{\mathfrak{L}})\right|^{12}(\exp(C_1(K)R_K))^{12d_K} \\
&\leq (N\mathfrak{L})^{12h_K}\exp(12d_K C_1(K)R_K) = (N\mathfrak{L})^{12h_K}C_2(K).
\end{aligned}
$$

□

Notations 2.12. Soit $\mathfrak{q}$ un idéal maximal de K premier à p en lequel E a potentiellement bonne réduction.

1. On fixe un idéal $\mathfrak{p}_0^{\mathfrak{q}}$ de $KL^{\mathfrak{q}}$ au-dessus de $\mathfrak{p}_0$ (voir les notations 1.7 et 2.5). Comme le corps $L^{\mathfrak{q}}$ est soit $\mathbb{Q}$, soit un corps quadratique imaginaire, il y a au plus deux choix possibles pour $\mathfrak{p}_0^{\mathfrak{q}}$; si $L^{\mathfrak{q}}$ est inclus dans K, le seul choix possible pour $\mathfrak{p}_0^{\mathfrak{q}}$ est $\mathfrak{p}_0^{\mathfrak{q}} = \mathfrak{p}_0$.
2. On note $\mathcal{P}_0^{\mathfrak{q}}$ l'unique idéal de $L^{\mathfrak{q}}$ situé au-dessous de $\mathfrak{p}_0^{\mathfrak{q}}$.
3. D'après la proposition 1.8, il existe une racine du polynôme $P_{\mathfrak{q}}(X)$ dont la classe modulo $\mathcal{P}_0^{\mathfrak{q}}$ (qui est dans $\mathbb{F}_p$) vaut $\lambda(\sigma_{\mathfrak{q}})$; on note $\beta_{\mathfrak{q}}$ une telle racine.

Définition 2.13 (Borne $C(K,n)$). Pour tout entier n, on pose :

$$
C(K,n) = \left(n^{12h_K}C_2(K) + n^{6h_K}\right)^{2d_K}.
$$

Proposition 2.14. *Soient $\mathfrak{q}$ un idéal maximal de K premier à p et $\gamma_{\mathfrak{q}}$ un générateur de $\mathfrak{q}^{h_K}$ vérifiant l'inégalité de la proposition 2.11. On suppose que p est strictement supérieur à $C(K,N\mathfrak{q})$. Alors on est dans l'un des trois cas suivants (avec les notations 2.5 et 2.12) :*

Type de réduction semi-stable de E en $\mathfrak{q}$	$\mu(\sigma_{\mathfrak{q}})$	$\mathcal{N}(\gamma_{\mathfrak{q}})$	*Cas*
multiplicatif	$1 \bmod p$	$\mathcal{N}(\gamma_{\mathfrak{q}}) = 1$	*M0*
	$(N\mathfrak{q})^{12} \bmod p$	$\mathcal{N}(\gamma_{\mathfrak{q}}) = (N\mathfrak{q})^{12h_K}$	*M1*
bon	$\beta_{\mathfrak{q}}^{12} \bmod \mathcal{P}_0^{\mathfrak{q}}$	$\mathcal{N}(\gamma_{\mathfrak{q}}) = \beta_{\mathfrak{q}}^{12h_K}$	*B*

Démonstration. Comme $\gamma_{\mathfrak{q}}$ engendre dans $\mathcal{O}_K$ l'idéal $\mathfrak{q}^{h_K}$, la proposition 2.6 appliquée à $\gamma_{\mathfrak{q}}$ donne :

$$
\mu(\sigma_{\mathfrak{q}})^{h_K} = \iota_{\mathfrak{p}_0}(\mathcal{N}(\gamma_{\mathfrak{q}})) \mod \mathfrak{p}_0
$$

On raisonne ensuite selon le type de réduction semi-stable de E en $\mathfrak{q}$ et les valeurs possibles de $\mu(\sigma_{\mathfrak{q}})$ déterminées dans la partie 1.3.

On suppose d'abord que E a potentiellement mauvaise réduction multiplicative en $\mathfrak{q}$ et que $\lambda^2(\sigma_{\mathfrak{q}})$ est égal à 1 modulo p. Alors $\mu(\sigma_{\mathfrak{q}})$ est aussi égal à 1 modulo p et l'élément $\mathcal{N}(\gamma_{\mathfrak{q}})$ de $\mathcal{O}_K$ est congru à 1 modulo $\mathfrak{p}_0$. Comme $\mathfrak{p}_0$ est au-dessus de p, ceci implique que p divise l'entier relatif $N_{K/\mathbb{Q}}(\mathcal{N}(\gamma_{\mathfrak{q}}) - 1)$. Par choix de $\gamma_{\mathfrak{q}}$, on a pour tout τ dans G :

$$
|\tau(\mathcal{N}(\gamma_{\mathfrak{q}}) - 1)|_{\mathbb{C}} \leq |\tau(\mathcal{N}(\gamma_{\mathfrak{q}}))|_{\mathbb{C}} + |\tau(1)|_{\mathbb{C}} \leq (N\mathfrak{q})^{12h_K}C_2(K) + 1,
$$

d'où

$$\left|N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-1\right)\right|_{\mathbb{Q}}=\prod_{\tau\in G}\left|\tau\left(\mathcal{N}(\gamma_{\mathfrak{q}})-1\right)\right|_{\mathbb{C}}\leq\left((N\mathfrak{q})^{12h_K}C_2(K)+1\right)^{d_K}\leq C(K,N\mathfrak{q}).$$

Comme p est supposé strictement plus grand que $C(K,N\mathfrak{q})$, on en déduit que l'entier $N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-1\right)$ est nul, ce qui implique que $\mathcal{N}(\gamma_{\mathfrak{q}})$ est égal à 1.

On suppose ensuite que E a potentiellement mauvaise réduction multiplicative en $\mathfrak{q}$ et que $\lambda^2(\sigma_{\mathfrak{q}})$ est égal à $(N\mathfrak{q})^2$ modulo p. Alors $\mu(\sigma_{\mathfrak{q}})$ est égal à $(N\mathfrak{q})^{12}$ modulo p et l'élément $\mathcal{N}(\gamma_{\mathfrak{q}})$ de $\mathcal{O}_K$ est congru à $(N\mathfrak{q})^{12h_K}$ modulo $\mathfrak{p}_0$. Ainsi, p divise l'entier relatif $N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-(N\mathfrak{q})^{12h_K}\right)$. Or on a :

$$\begin{array}{rcl}\left|N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-(N\mathfrak{q})^{12h_K}\right)\right|_{\mathbb{Q}} & = & \prod_{\tau\in G}\left|\tau\left(\mathcal{N}(\gamma_{\mathfrak{q}})-(N\mathfrak{q})^{12h_K}\right)\right|_{\mathbb{C}}\\ & \leq & \prod_{\tau\in G}\left((N\mathfrak{q})^{12h_K}C_2(K)+(N\mathfrak{q})^{12h_K}\right)\\ & \leq & \left((N\mathfrak{q})^{12h_K}C_2(K)+(N\mathfrak{q})^{12h_K}\right)^{d_K}\\ & \leq & C(K,N\mathfrak{q}).\end{array}$$

Comme p est supposé strictement plus grand que $C(K,N\mathfrak{q})$, on en déduit que l'entier $N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-(N\mathfrak{q})^{12h_K}\right)$ est nul, ce qui implique que $\mathcal{N}(\gamma_{\mathfrak{q}})$ est égal à $(N\mathfrak{q})^{12h_K}$.

On suppose enfin que E a potentiellement bonne réduction en $\mathfrak{q}$. Alors $\mu(\sigma_{\mathfrak{q}})$ est égal à la classe de $\beta_{\mathfrak{q}}^{12}$ modulo $\mathcal{P}_0^{\mathfrak{q}}$ (notations 2.12) et $\mathcal{N}(\gamma_{\mathfrak{q}})$ et $\beta_{\mathfrak{q}}^{12h_K}$ sont congrus modulo l'idéal $\mathfrak{p}_0^{\mathfrak{q}}$ de $KL^{\mathfrak{q}}$. Ceci implique que p divise l'entier relatif $N_{KL^{\mathfrak{q}}/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-\beta_{\mathfrak{q}}^{12h}\right)$.

Comme $L^{\mathfrak{q}}$ est soit $\mathbb{Q}$ soit un corps quadratique imaginaire, le corps $KL^{\mathfrak{q}}$ est galoisien sur $\mathbb{Q}$, de degré égal à d_K ou $2d_K$. Tout élément τ de $\mathrm{Gal}(KL^{\mathfrak{q}}/\mathbb{Q})$ induit sur K un élément de $\mathrm{Gal}(K/\mathbb{Q})$ et sur $L^{\mathfrak{q}}$ un élément de $\mathrm{Gal}(L^{\mathfrak{q}}/\mathbb{Q})$, qui est donc soit l'identité soit la conjugaison complexe. On a ainsi pour tout τ dans $\mathrm{Gal}(KL^{\mathfrak{q}}/\mathbb{Q})$:

$$\begin{array}{rcl}\left|\tau\left(\mathcal{N}(\gamma_{\mathfrak{q}})-\beta_{\mathfrak{q}}^{12h_K}\right)\right|_{\mathbb{C}} & \leq & \left|\tau_{|K}\left(\mathcal{N}(\gamma_{\mathfrak{q}})\right)\right|_{\mathbb{C}}+\left|\tau_{|L^{\mathfrak{q}}}\left(\beta_{\mathfrak{q}}^{12h_K}\right)\right|_{\mathbb{C}}\\ & \leq & (N\mathfrak{q})^{12h_K}C_2(K)+\left(\sqrt{N\mathfrak{q}}\right)^{12h_K}\\ & \leq & (N\mathfrak{q})^{12h_K}C_2(K)+(N\mathfrak{q})^{6h_K}.\end{array}$$

D'où finalement :

$$\begin{array}{rcl}\left|N_{KL^{\mathfrak{q}}/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-\beta_{\mathfrak{q}}^{12h_K}\right)\right|_{\mathbb{Q}} & = & \prod_{\tau\in\mathrm{Gal}(KL^{\mathfrak{q}}/\mathbb{Q})}\left|\tau\left(\mathcal{N}(\gamma_{\mathfrak{q}})-\beta_{\mathfrak{q}}^{12h_K}\right)\right|_{\mathbb{C}}\\ & \leq & \left((N\mathfrak{q})^{12h_K}C_2(K)+(N\mathfrak{q})^{6h_K}\right)^{2d_K}=C(K,N\mathfrak{q}).\end{array}$$

Comme p est supposé strictement plus grand que $C(K,N\mathfrak{q})$, on en déduit que l'entier $N_{KL^{\mathfrak{q}}/\mathbb{Q}}\left(\mathcal{N}(\gamma_{\mathfrak{q}})-\beta_{\mathfrak{q}}^{12h_K}\right)$ est nul, ce qui implique que $\mathcal{N}(\gamma_{\mathfrak{q}})$ est égal à $\beta_{\mathfrak{q}}^{12h_K}$. $\square$

La proposition suivante donne une forme effective du lemme 2 de la partie 2 de [10].

Proposition 2.15. *Soient q un nombre premier rationnel totalement décomposé dans K et $\mathfrak{q}$ un idéal premier de K au-dessus de q. On suppose que p est strictement plus grand que $C(K,q)$. Alors on est dans l'un des cinq cas suivants (avec les notations 2.12) :*

<table>
<tr><th colspan="2">Type de réduction semi-stable de E en $\mathfrak{q}$</th><th>Corps $L^{\mathfrak{q}}$</th><th>$\mu(\sigma_{\mathfrak{q}})$</th><th>Famille $(a_\tau)_{\tau\in G}$</th><th>Cas</th></tr>
<tr><td colspan="2" rowspan="2">multiplicatif</td><td rowspan="2"></td><td>$1 \mod p$</td><td>$\forall \tau \in G, a_\tau = 0$</td><td>M0</td></tr>
<tr><td>$q^{12} \mod p$</td><td>$\forall \tau \in G, a_\tau = 12$</td><td>M1</td></tr>
<tr><td rowspan="3">bon</td><td>supersingulier</td><td>$L^{\mathfrak{q}} = \mathbb{Q}(\sqrt{-q})$</td><td>$\beta_{\mathfrak{q}}^6 = -q^3$</td><td>$\forall \tau \in G, a_\tau = 6$</td><td>BS</td></tr>
<tr><td rowspan="2">ordinaire</td><td rowspan="2">quadratique, inclus dans K, p décomposé dans $L^{\mathfrak{q}}$</td><td>$N_{K/L^{\mathfrak{q}}}(\mathfrak{q}) = \beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}$</td><td>$\forall \tau \in \mathrm{Gal}(K/L^{\mathfrak{q}}), a_\tau = 12$ et $a_\tau = 0$ sinon</td><td>BO</td></tr>
<tr><td>$N_{K/L^{\mathfrak{q}}}(\mathfrak{q}) = \overline{\beta_{\mathfrak{q}}}\mathcal{O}_{L^{\mathfrak{q}}}$</td><td>$\forall \tau \in \mathrm{Gal}(K/L^{\mathfrak{q}}), a_\tau = 0$ et $a_\tau = 12$ sinon</td><td>BO'</td></tr>
</table>

Démonstration. Comme le nombre premier q est supposé totalement décomposé dans l'extension galoisienne $K/\mathbb{Q}$, les idéaux $\tau(\mathfrak{q})$ sont deux à deux distincts lorsque τ décrit G, leur produit est l'idéal $q\mathcal{O}_K$ et la norme de $\mathfrak{q}$ dans $K/\mathbb{Q}$ est égale à q. En particulier, en supposant que p est strictement supérieur à $C(K,q)$, on se place dans les hypothèses de la proposition 2.14. On raisonne donc selon les trois cas de cette proposition.

On remarque que l'élément $\mathcal{N}(\gamma_{\mathfrak{q}})$ engendre dans $\mathcal{O}_K$ l'idéal

$$\begin{aligned} \mathcal{N}(\gamma_{\mathfrak{q}})\mathcal{O}_K &= \left(\prod_{\tau\in G} \tau(\gamma_{\mathfrak{q}})^{a_\tau}\right)\mathcal{O}_K = \prod_{\tau\in G}\left(\tau\left(\gamma_{\mathfrak{q}}\mathcal{O}_K\right)\right)^{a_\tau} \\ &= \prod_{\tau\in G}\left(\tau\left(\mathfrak{q}^{h_K}\right)\right)^{a_\tau} = \left(\prod_{\tau\in G}\tau\left(\mathfrak{q}\right)^{a_\tau}\right)^{h_K}. \end{aligned}$$

Lorsque $\mathfrak{q}$ est de type M0, $\mathcal{N}(\gamma_{\mathfrak{q}})$ est égal à 1 donc engendre dans $\mathcal{O}_K$ l'idéal $\mathcal{O}_K$ lui-même. L'égalité

$$\mathcal{O}_K = \left(\prod_{\tau\in G}\tau\left(\mathfrak{q}\right)^{a_\tau}\right)^{h_K}$$

avec h_K dans $\mathbb{N}^*$ implique alors que pour tout τ dans G, a_τ est nul.

Lorsque $\mathfrak{q}$ est de type M1, $\mathcal{N}(\gamma_{\mathfrak{q}})$ est égal à q^{12h_K} et on a :

$$\left(\prod_{\tau\in G}\tau\left(\mathfrak{q}\right)^{a_\tau}\right)^{h_K} = \mathcal{N}(\gamma_{\mathfrak{q}})\mathcal{O}_K = \left(q^{12h_K}\right)\mathcal{O}_K = \left(q\mathcal{O}_K\right)^{12h_K} = \left(\prod_{\tau\in G}\tau\left(\mathfrak{q}\right)\right)^{12h_K}.$$

On en déduit que pour tout τ dans G, a_τ est égal à 12.

Lorsque $\mathfrak{q}$ est de type B, $\mathcal{N}(\gamma_{\mathfrak{q}})$ est égal à $\beta_{\mathfrak{q}}^{12h_K}$ (dans le corps $KL^{\mathfrak{q}}$). En particulier, l'élément $\mathcal{N}(\gamma_{\mathfrak{q}})$ de K est contenu dans $L^{\mathfrak{q}}$ et deux sous-cas sont possibles : soit $\mathcal{N}(\gamma_{\mathfrak{q}})$ est rationnel, soit $\mathcal{N}(\gamma_{\mathfrak{q}})$ engendre $L^{\mathfrak{q}}$ qui est alors contenu dans K.

On suppose d'abord que $\mathcal{N}(\gamma_{\mathfrak{q}})$ est rationnel. Alors $\beta_{\mathfrak{q}}^{12h_K}$ est également rationnel, donc $\beta_{\mathfrak{q}}^{12h_K}$ est égal à $\overline{\beta_{\mathfrak{q}}}^{12h_K}$. Ceci implique qu'il existe une racine $12h_K$-ième de l'unité ζ dans $L^{\mathfrak{q}}$ telle que $\overline{\beta_{\mathfrak{q}}}$ est égal à $\zeta\beta_{\mathfrak{q}}$. Comme $L^{\mathfrak{q}}$ est soit $\mathbb{Q}$ soit un corps quadratique imaginaire, ζ est en fait une racine deuxième, quatrième ou sixième de l'unité. Ceci implique que $\beta_{\mathfrak{q}}^{12}$ est déjà rationnel ; comme $\beta_{\mathfrak{q}}$ est un entier algébrique, $\beta_{\mathfrak{q}}^{12}$ est un entier relatif ; sa valeur absolue étant q^6, on a $\beta_{\mathfrak{q}}^{12} = \pm q^6$. On en déduit qu'on a dans $\mathcal{O}_K$:

$$\left(\prod_{\tau\in G} \tau\left(\mathfrak{q}\right)^{a_\tau}\right)^{h_K} = \mathcal{N}(\gamma_{\mathfrak{q}})\mathcal{O}_K = \beta_{\mathfrak{q}}^{12h_K}\mathcal{O}_K = q^{6h_K}\mathcal{O}_K = \left(\prod_{\tau\in G} \tau\left(\mathfrak{q}\right)\right)^{6h_K}.$$

Ceci implique que pour tout τ dans G, a_τ est égal à 6. D'après la proposition 1.3, le nombre premier p est donc congru à 3 modulo 4.

On va maintenant montrer que E a potentiellement réduction supersingulière en $\mathfrak{q}$, que le corps $L^{\mathfrak{q}}$ est $\mathbb{Q}(\sqrt{-q})$ et qu'on a $\beta_{\mathfrak{q}}^6 = -q^3$.

La relation
$$q = N\mathfrak{q} = \overline{\beta_{\mathfrak{q}}}\beta_{\mathfrak{q}} = \zeta\beta_{\mathfrak{q}}^2.$$
implique dans $\mathcal{O}_{L^{\mathfrak{q}}}$
$$q\mathcal{O}_{L^{\mathfrak{q}}} = \left(\beta_{\mathfrak{q}}^2\right)\mathcal{O}_{L^{\mathfrak{q}}} = \left(\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}\right)^2.$$
Ainsi, q est ramifié dans $L^{\mathfrak{q}}$ et l'unique idéal premier de $L^{\mathfrak{q}}$ au-dessus de q est $\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}$ (ceci force notamment $L^{\mathfrak{q}}$ à être différent de $\mathbb{Q}$).

On traite d'abord le cas $q = 2$. La trace $T_{\mathfrak{q}}$ (voir notations 1.7) est alors un entier relatif de valeur absolue inférieure à $2\sqrt{2}$; il vaut donc 0, 1, 2, -1 ou -2. Les valeurs correspondantes du discriminant $T_{\mathfrak{q}}^2 - 4N\mathfrak{q}$ du polynôme $P_{\mathfrak{q}}(X)$ sont -8, -7, -4, -7, -4. Les entiers relatifs sans facteurs carrés dont une racine carrée engendre $L^{\mathfrak{q}}$ sont alors respectivement -2, -7, -1, -7, -1. Or, 2 est ramifié dans $L^{\mathfrak{q}}$ si et seulement si ce dernier entier est congru à 2 ou 3 modulo 4. Les valeurs de $T_{\mathfrak{q}}$ qui réalisent cette condition sont 0, 2 et -2. Or d'après la remarque 1.9, l'entier $T_{\mathfrak{q}}^2 - 4N\mathfrak{q}$ est un carré modulo p. Si $T_{\mathfrak{q}}$ est égal à 2 ou -2, le discriminant $T_{\mathfrak{q}}^2 - 4N\mathfrak{q}$ est égal à -4. Or, p étant congru à 3 modulo 4, -4 n'est pas un carré modulo p. On en déduit que $T_{\mathfrak{q}}$ est nul.

Lorsque q est différent de 2, le fait qu'il soit ramifié dans $L^{\mathfrak{q}}$ implique qu'il divise le discriminant $T_{\mathfrak{q}}^2 - 4N\mathfrak{q}$. Comme q divise $N\mathfrak{q}$ (et lui est même ici égal), on en déduit que q divise $T_{\mathfrak{q}}$. Alors $T_{\mathfrak{q}}^2$ est un carré, multiple de q, compris entre 0 et $4q$. Ceci implique que soit $T_{\mathfrak{q}}$ est nul, soit q est égal à 3 et $T_{\mathfrak{q}}^2$ est égal à 9.

On a ainsi montré :
- si q est différent de 3, alors $T_{\mathfrak{q}}$ est nul ;
- si q est égal à 3, alors $T_{\mathfrak{q}}^2$ est soit nul, soit égal à 9.

Dans les deux cas, q divise $T_{\mathfrak{q}}$, donc la courbe elliptique obtenue sur $\overline{k_{\mathfrak{q}}}$ par réduction de E est supersingulière.

Si la trace $T_{\mathfrak{q}}$ est nulle, alors le polynôme $P_{\mathfrak{q}}(X)$ dont $\beta_{\mathfrak{q}}$ est racine est égal à X^2+q. On a alors $\beta_{\mathfrak{q}}^2$ égal à $-q$, donc $\beta_{\mathfrak{q}}^6$ est égal à $-q^3$ et le corps $L^{\mathfrak{q}}$ est $\mathbb{Q}(\sqrt{-q})$.

Si q est égal à 3 et $T_{\mathfrak{q}}^2$ est égal à 9, alors $T_{\mathfrak{q}}^2 - 4N\mathfrak{q}$ vaut -3 et il existe $\varepsilon_{\mathfrak{q}}$ valant $+1$ ou -1 vérifiant :

$$\beta_{\mathfrak{q}} = \frac{T_{\mathfrak{q}} + i\varepsilon_{\mathfrak{q}}\sqrt{3}}{2}.$$

On a alors encore $L^{\mathfrak{q}}$ égal à $\mathbb{Q}(\sqrt{-3})$ et on vérifie par le calcul que $\beta_{\mathfrak{q}}^6$ est égal à -3^3.

On suppose enfin que l'élément $\mathcal{N}(\gamma_{\mathfrak{q}})$ de K engendre $L^{\mathfrak{q}}$ qui est un corps quadratique imaginaire. Alors $L^{\mathfrak{q}}$ est inclus dans K, le degré d_K de K sur $\mathbb{Q}$ est pair et le groupe de Galois de K sur $\mathbb{Q}$ contient comme sous-groupe d'indice 2 le groupe $\mathrm{Gal}(K/L^{\mathfrak{q}})$; on note $H^{\mathfrak{q}}$ ce sous-groupe.

Comme $\mathcal{N}(\gamma_{\mathfrak{q}})$ est contenu dans $L^{\mathfrak{q}}$, on a pour tout élément ρ de $H^{\mathfrak{q}}$:

$$\mathcal{N}(\gamma_{\mathfrak{q}}) = \rho\left(\mathcal{N}(\gamma_{\mathfrak{q}})\right).$$

On en déduit :

$$\left(\prod_{\tau\in G}\tau(\mathfrak{q})^{a_\tau}\right)^{h_K} = \mathcal{N}(\gamma_{\mathfrak{q}})\mathcal{O}_K = \rho\left(\mathcal{N}(\gamma_{\mathfrak{q}})\mathcal{O}_K\right) = \rho\left(\left(\prod_{\tau\in G}\tau(\mathfrak{q})^{a_\tau}\right)^{h_K}\right) = \left(\prod_{\tau\in G}\tau(\mathfrak{q})^{a_{\rho^{-1}\tau}}\right)^{h_K}.$$

On a donc pour tout ρ dans $H^{\mathfrak{q}}$ et tout τ dans G l'égalité $a_{\rho\tau} = a_\tau$. Ainsi la valeur de a_τ est constante sur les classes à gauche (qui sont aussi les classes à droite) de G modulo $H^{\mathfrak{q}}$.

Le groupe G possède deux classes modulo $H^{\mathfrak{q}}$: celle, égale à $H^{\mathfrak{q}}$, de l'identité et celle, égale à $H^{\mathfrak{q}}\gamma$, d'un élément γ de G qui induit la conjugaison complexe sur $L^{\mathfrak{q}}$. On a alors :

$$\begin{aligned}
\mathcal{N}(\gamma_{\mathfrak{q}}) &= \prod_{\tau\in G}\tau(\gamma_{\mathfrak{q}})^{a_\tau} \\
&= \left(\prod_{\tau\in H^{\mathfrak{q}}}\tau(\gamma_{\mathfrak{q}})\right)^{a_{id}}\left(\prod_{\tau\in\gamma H^{\mathfrak{q}}}\tau(\gamma_{\mathfrak{q}})\right)^{a_\gamma} \\
&= \left(\prod_{\tau\in H^{\mathfrak{q}}}\tau(\gamma_{\mathfrak{q}})\right)^{a_{id}}\left(\gamma\left(\prod_{\tau\in H^{\mathfrak{q}}}\tau(\gamma_{\mathfrak{q}})\right)\right)^{a_\gamma} \\
&= \left(N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})\right)^{a_{id}}\left(\gamma\left(N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})\right)\right)^{a_\gamma} \\
&= \left(N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})\right)^{a_{id}}\left(\overline{N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})}\right)^{a_\gamma}.
\end{aligned}$$

Comme $N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})$ engendre dans $\mathcal{O}_{L^{\mathfrak{q}}}$ l'idéal

$$N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})\mathcal{O}_{L^{\mathfrak{q}}} = N_{K/L^{\mathfrak{q}}}\left(\gamma_{\mathfrak{q}}\mathcal{O}_K\right) = N_{K/L^{\mathfrak{q}}}\left(\mathfrak{q}^{h_K}\right) = N_{K/L^{\mathfrak{q}}}\left(\mathfrak{q}\right)^{h_K},$$

alors $\overline{N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})}$ engendre dans $\mathcal{O}_{L^{\mathfrak{q}}}$ l'idéal $\overline{N_{K/L^{\mathfrak{q}}}(\mathfrak{q})}^{h_K}$ et on obtient :

$$\begin{aligned}
\left(\beta_{\mathfrak{q}}^{12h_K}\right)\mathcal{O}_{L^{\mathfrak{q}}} &= \mathcal{N}(\gamma_{\mathfrak{q}})\mathcal{O}_{L^{\mathfrak{q}}} \\
\left(\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}\right)^{12h_K} &= \left(N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})\mathcal{O}_{L^{\mathfrak{q}}}\right)^{a_{id}}\left(\overline{N_{K/L^{\mathfrak{q}}}(\gamma_{\mathfrak{q}})}\mathcal{O}_{L^{\mathfrak{q}}}\right)^{a_\gamma} \\
&= \left(N_{K/L^{\mathfrak{q}}}(\mathfrak{q})^{h_K}\right)^{a_{id}}\left(\overline{N_{K/L^{\mathfrak{q}}}(\mathfrak{q})}^{h_K}\right)^{a_\gamma} \\
&= \left(\left(N_{K/L^{\mathfrak{q}}}(\mathfrak{q})\right)^{a_{id}}\left(\overline{N_{K/L^{\mathfrak{q}}}(\mathfrak{q})}\right)^{a_\gamma}\right)^{h_K}.
\end{aligned}$$

Comme on a supposé q totalement décomposé dans l'extension $K/\mathbb{Q}$, q est également totalement décomposé dans les extensions $L^{\mathfrak{q}}/\mathbb{Q}$ et $K/L^{\mathfrak{q}}$. La norme $N_{K/L^{\mathfrak{q}}}(\mathfrak{q})$ est donc un idéal premier de $L^{\mathfrak{q}}$ au-dessus de q. Or l'égalité $q = \beta_{\mathfrak{q}}\overline{\beta_{\mathfrak{q}}}$ indique que les deux idéaux premiers (distincts) de $L^{\mathfrak{q}}$ au-dessus de q sont $\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}$ et $\overline{\beta_{\mathfrak{q}}}\mathcal{O}_{L^{\mathfrak{q}}}$. Ainsi $N_{K/L^{\mathfrak{q}}}(\mathfrak{q})$ est égal soit à $\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}$ soit à $\overline{\beta_{\mathfrak{q}}}\mathcal{O}_{L^{\mathfrak{q}}}$.

Si $N_{K/L^{\mathfrak{q}}}(\mathfrak{q})$ est égal à $\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}$, alors la relation

$$(\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}})^{12h_K} = \left((\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}})^{a_{id}}\,(\overline{\beta_{\mathfrak{q}}}\mathcal{O}_{L^{\mathfrak{q}}})^{a_\gamma}\right)^{h_K}$$

implique $a_{id} = 12$ et $a_\gamma = 0$. On en déduit que a_τ vaut 12 si τ est dans $H^{\mathfrak{q}}$ et 0 sinon.

Si $N_{K/L^{\mathfrak{q}}}(\mathfrak{q})$ est égal à $\overline{\beta_{\mathfrak{q}}}\mathcal{O}_{L^{\mathfrak{q}}}$, alors la relation

$$(\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}})^{12h_K} = \left((\overline{\beta_{\mathfrak{q}}}\mathcal{O}_{L^{\mathfrak{q}}})^{a_{id}}\,(\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}})^{a_\gamma}\right)^{h_K}$$

implique $a_{id} = 0$ et $a_\gamma = 12$. On en déduit que a_τ vaut 0 si τ est dans $H^{\mathfrak{q}}$ et 12 sinon.

D'après la remarque 1.9, soit p est décomposé dans $L^{\mathfrak{q}}$, soit p divise $T_{\mathfrak{q}}^2 - 4q$. Supposons par l'absurde que p divise $T_{\mathfrak{q}}^2 - 4q$; on remarque que la valeur absolue de $T_{\mathfrak{q}}^2 - 4q$ est $4q - T_{\mathfrak{q}}^2$, elle donc inférieure ou égale à $4q$. Comme p est supposé strictement supérieur à $C(K,q)$, p est strictement supérieur à $4q$. On obtient alors que $T_{\mathfrak{q}}^2 - 4q$ est nul, ce qui est impossible. On en déduit que p est décomposé dans le corps quadratique $L^{\mathfrak{q}}$.

Enfin, on suppose par l'absurde que E a potentiellement réduction supersingulière en $\mathfrak{q}$; alors d'après la remarque 1.9, on est dans l'un des cas suivants : $T_{\mathfrak{q}}$ est nul ; q est égal à 2 et $T_{\mathfrak{q}}$ est égal à 0, 2 ou -2 ; q est égal à 3 et $T_{\mathfrak{q}}$ est égal à 0, 3 ou -3. Si $T_{\mathfrak{q}}$ est nul ou q est égal à 3 et $T_{\mathfrak{q}}$ vaut ± 3, alors $L^{\mathfrak{q}}$ est égal à $\mathbb{Q}(\sqrt{-q})$, dans lequel q est ramifié ; si q est égal à 2 et $T_{\mathfrak{q}}$ vaut ± 2, alors $L^{\mathfrak{q}}$ est égal à $\mathbb{Q}(i)$, dans lequel 2 est ramifié. Or, on a montré que q est décomposé dans le corps $L^{\mathfrak{q}}$. On en déduit que E a potentiellement réduction ordinaire en $\mathfrak{q}$. $\square$

3 Deux critères d'irréductibilité

3.1 Types de réduction semi-stable différents

Soit M un entier naturel supérieur ou égal 1.

Définition 3.1 (Ensemble $\mathcal{E}(K;M)$). On note $\mathcal{E}(K;M)$ l'ensemble des courbes elliptiques E définies sur K pour lesquelles il existe

- q et q' des nombres premiers totalement décomposés dans K et inférieurs ou égaux à M,
- une place $\mathfrak{q}$ de K au-dessus de q et une place $\mathfrak{q}'$ de K au-dessus de q' tels que les types de réduction semi-stable de E en $\mathfrak{q}$ et $\mathfrak{q}'$ (de la proposition 2.15) sont différents

(les premiers q et q' et les places $\mathfrak{q}$ et $\mathfrak{q}'$ peuvent dépendre de E ; les premiers q et q' peuvent être égaux).

Proposition 3.2. *Soit M un entier naturel supérieur ou égal* 1*. Alors pour toute courbe elliptique E dans $\mathcal{E}(K;M)$ et tout nombre premier p strictement supérieur à $C(K,M)$, la représentation $\varphi_{E,p}$ est irréductible.*

Démonstration. On suppose par l'absurde que la représentation $\varphi_{E,p}$ est réductible. Alors pour les places $\mathfrak{q}$ et $\mathfrak{q}'$, on est dans les hypothèses de la proposition 2.15. Le type de réduction semi-stable de E en $\mathfrak{q}$ ou $\mathfrak{q}'$ détermine donc la famille $(a_\tau)_\tau$, qui décrit l'action sur le sous-groupe d'isogénie des sous-groupes d'inertie de G_K aux places de K au-dessus de p. Comme deux types de réduction semi-stable pour $\mathfrak{q}$ ou $\mathfrak{q}'$ donnent des familles $(a_\tau)_\tau$ différentes (on distingue les cas BO et BO' par le fait que dans le cas BO, l'ensemble des éléments τ de G pour lesquels a_τ est égal à 12 est un sous-groupe de G alors que dans le cas BO', c'est le complémentaire d'un sous-groupe), ces types doivent être les mêmes : on obtient une contradiction. $\square$

3.2 Réduction semi-stable multiplicative

Soit q un nombre premier rationnel totalement décomposé dans K.

Définition 3.3 (Ensemble $\mathcal{E}'(K;q)$ et borne $B(K;q)$). Soit q un nombre premier rationnel totalement décomposé dans K.

1. On note $\mathcal{E}'(K;q)$ l'ensemble des courbes elliptiques E définies sur K vérifiant : il existe une place (qui peut dépendre de E) de K au-dessus de q en laquelle E a potentiellement mauvaise réduction multiplicative.
2. On pose
$$B(K;q) = \max\left(C(K,q), \left(1+3^{6d_K h_K}\right)^2\right).$$

Proposition 3.4. *Soit q un nombre premier rationnel totalement décomposé dans K. Alors pour toute courbe elliptique E dans $\mathcal{E}'(K;q)$ et tout nombre premier p strictement supérieur à $B(K;q)$, la représentation $\varphi_{E,p}$ est irréductible.*

Démonstration. On suppose par l'absurde que la représentation $\varphi_{E,p}$ est réductible. Alors on est dans les hypothèses de la proposition 2.15 et comme E appartient à $\mathcal{E}'(K;q)$, on est dans le cas M0 ou dans le cas M1. On remarque que d'après les propositions 1.4 et 1.5, le caractère μ est non ramifié en toute place finie de K première à p.

Dans le cas M0, pour tout idéal premier $\mathfrak{p}$ de K au-dessus de p, $a_\mathfrak{p}$ est nul. Par définition de $a_\mathfrak{p}$ (partie 1.2), cela implique que caractère μ est non ramifié en toute place de K au-dessus de p. Ainsi, l'extension K^μ de K trivialisant μ, qui est abélienne, est non ramifiée en toute place finie de K ; le corps K^μ est donc inclus dans le corps de classes de Hilbert de K et son degré (sur $\mathbb{Q}$) est inférieur ou égal à $d_K h_K$. Le corps K^λ qui trivialise le caractère λ est une extension de degré divisant 12 de K^μ ; son degré (sur $\mathbb{Q}$) est donc inférieur ou égal à $12 d_K h_K$.

Or, la courbe E possède un point d'ordre p défini sur K^λ. D'après des travaux de Merel et Oesterlé mentionnés dans les introductions de [11] et [9], on a alors

$$p \leq \left(1+3^{\frac{12 d_K h_K}{2}}\right)^2 = \left(1+3^{6d_K h_K}\right)^2,$$

ce qui contredit le choix de p strictement supérieur à $B(K;q)$.

Dans le cas M1, pour tout idéal premier $\mathfrak{p}$ de K au-dessus de p, $a_{\mathfrak{p}}$ est égal à 12. Ainsi, le caractère $\chi_p^{12}\mu^{-1}$ est non ramifié en toute place de K au-dessus de p, et par suite en toute place finie de K. On considère alors le quotient de E par le sous-groupe d'isogénie W. On obtient une courbe elliptique E' définie sur K, isogène à E sur K ; le sous-groupe $E[p]/W$ de E' est défini sur K et d'ordre p et le caractère d'isogénie associé à ce sous-groupe est $\chi_p\lambda^{-1}$. La puissance douzième de $\chi_p\lambda^{-1}$ étant non ramifiée en toute place finie de K, on applique le même raisonnement que précédemment. □

4 Forme du caractère d'isogénie et homothéties

À partir de maintenant et jusqu'à la fin du texte, on suppose à nouveau la représentation $\varphi_{E,p}$ réductible.

4.1 Une version effective du théorème de Chebotarev

Théorème (Chebotarev effectif, [6]). *Il existe une constante absolue et effectivement calculable A ayant la propriété suivante : soient M un corps de nombres, N une extension finie galoisienne de M, Δ_N le discriminant de N, C une classe de conjugaison du groupe de Galois $\mathrm{Gal}(N/M)$; alors il existe un idéal premier de M, non ramifié dans N, dont la classe de conjugaison des frobenius dans l'extension N/M est la classe de conjugaison C et dont la norme dans l'extension $M/\mathbb{Q}$ est un nombre premier rationnel inférieur ou égal à $2(\Delta_N)^A$.*

Définition 4.1 (Ensemble d'idéaux $\mathcal{J}_K$). On note $\mathcal{J}_K$ l'ensemble des idéaux maximaux de K dont la norme dans l'extension $K/\mathbb{Q}$ est un nombre premier rationnel totalement décomposé dans K et inférieur ou égal à $2(\Delta_K)^{Ah_K}$.

Proposition 4.2. *Toute classe d'idéaux de K contient un idéal de $\mathcal{J}_K$.*

Démonstration. On note H_K le corps de classes de Hilbert de K. Démontrer la proposition est équivalent à montrer que pour tout élément σ du groupe de Galois de l'extension H_K/K, il existe un idéal premier non nul $\mathfrak{q}$ de K appartenant à $\mathcal{J}_K$ tel que l'élément de Frobenius associé à $\mathfrak{q}$ dans $\mathrm{Gal}(H_K/K)$ par l'application de réciprocité d'Artin est égal à σ.

Comme on a supposé le corps K galoisien sur $\mathbb{Q}$, le corps H_K est également une extension galoisienne de $\mathbb{Q}$. On va utiliser la version effective du théorème de Chebotarev pour les corps $N = H_K$ et $M = \mathbb{Q}$. On remarque que le discriminant Δ_{H_K} de H_K est égal à $\Delta_K^{h_K}$ et que le groupe $\mathrm{Gal}(H_K/K)$ est un sous-groupe (distingué) du groupe $\mathrm{Gal}(H_K/\mathbb{Q})$.

Soit σ un élément de $\mathrm{Gal}(H_K/K)$ et C la classe de conjugaison de σ dans $\mathrm{Gal}(H_K/\mathbb{Q})$. D'après le théorème de Chebotarev effectif, il existe un nombre premier rationnel q, non ramifié dans H_K et inférieur ou égal à $2(\Delta_{H_K})^A$, tel que la classe de conjugaison formée par les frobenius de q dans l'extension $H_K/\mathbb{Q}$ est égale à C. Il existe donc un idéal $\tilde{\mathfrak{q}}$ de H_K au-dessus de q tel que le frobenius $\mathrm{Frob}(\tilde{\mathfrak{q}}/q)$ de $\tilde{\mathfrak{q}}$ dans l'extension $H_K/\mathbb{Q}$ est égal à σ.

Soit $\mathfrak{q}$ l'idéal de K situé au-dessous de $\tilde{\mathfrak{q}}$. Alors la caractéristique de $\mathfrak{q}$ est le nombre premier rationnel q. Par choix, q est inférieur ou égal à $2(\Delta_K)^{Ah_K}$ et non ramifié dans H_K, donc dans K. Le frobenius $\mathrm{Frob}(\mathfrak{q}/q)$ de $\mathfrak{q}$ dans l'extension $K/\mathbb{Q}$ est égal à la restriction à K du frobenius $\mathrm{Frob}(\tilde{\mathfrak{q}}/q)$ de $\tilde{\mathfrak{q}}$ dans $H_K/\mathbb{Q}$. Or, $\mathrm{Frob}(\tilde{\mathfrak{q}}/q)$ est égal à σ, qui est un élément de $\mathrm{Gal}(H_K/K)$. Ceci implique que $\mathrm{Frob}(\mathfrak{q}/q)$ est l'identité de K, donc que le degré résiduel de $\mathfrak{q}$ dans $K/\mathbb{Q}$ est 1 et finalement que la norme de $\mathfrak{q}$ dans $K/\mathbb{Q}$ est q. Comme K est supposé galoisien sur $\mathbb{Q}$, on obtient que q est totalement décomposé dans K et ainsi que $\mathfrak{q}$ est dans l'ensemble $\mathcal{J}_K$.

Enfin, comme $\mathfrak{q}$ est de degré 1 dans $K/\mathbb{Q}$, l'élément de Frobenius $\mathrm{Frob}(\tilde{\mathfrak{q}}/\mathfrak{q})$ associé à $\mathfrak{q}$ dans l'extension H_K/K vérifie

$$\mathrm{Frob}(\tilde{\mathfrak{q}}/\mathfrak{q}) = \mathrm{Frob}(\tilde{\mathfrak{q}}/q) = \sigma.$$

□

4.2 Les deux formes possibles du caractère d'isogénie

Dans cette partie, on s'inspire de la démonstration du théorème 1 (§2) de [10] pour obtenir le théorème II de l'introduction.

Définition 4.3 (Borne C_K). On pose

$$C_K = \max\left(C\left(K, 2(\Delta_K)^{Ah_K}\right), \left(1+3^{6d_K h_K}\right)^2\right).$$

Le nombre C_K ne dépend que du corps de nombres K.

Proposition 4.4. *On suppose que p est strictement supérieur à C_K. Alors, en tout idéal de $\mathcal{J}_K$, la courbe E a potentiellement bonne réduction et tous les idéaux de $\mathcal{J}_K$ appartiennent au même cas (BS, BO ou BO') de la proposition 2.15.*

Démonstration. Par construction, la borne C_K est supérieure ou égale à $C\left(K, 2(\Delta_K)^{Ah_K}\right)$ et à $B(K;q)$ pour tout idéal $\mathfrak{q}$ de $\mathcal{J}_K$ de caractéristique q . Comme la représentation $\varphi_{E,p}$ est supposé réductible, les propositions 3.2 et 3.4 donnent que la courbe E n'appartient pas à la famille $\mathcal{E}(K; 2(\Delta_K)^{Ah_K})$ ni à la famille $\mathcal{E}'(K;q)$ pour tout premier rationnel q totalement décomposé dans K et inférieur ou égal à $2(\Delta_K)^{Ah_K}$.

Ceci implique que E a même type de réduction semi-stable (parmi les cinq types possibles de la proposition 2.15) en tout idéal de $\mathcal{J}_K$ et que ce type n'est pas multiplicatif. □

4.2.1 Type supersingulier

Proposition 4.5. *On suppose que p est strictement supérieur à C_K et que tous les idéaux de $\mathcal{J}_K$ sont de type supersingulier (BS dans la proposition 2.15). Alors :*

1. *le nombre premier p est congru à 3 modulo 4 ;*
2. *en toute place de K au-dessus de p, la courbe E a mauvaise réduction additive et potentiellement bonne réduction supersingulière ;*
3. *on a $\lambda^6 = \left(\chi_p \lambda^{-1}\right)^6 = \left(\chi_p^{\frac{p+1}{2}}\right)^3$.*

Démonstration. Soit $\mathfrak{p}$ un idéal premier de K au-dessus de p. Comme tous les idéaux de $\mathcal{J}_K$ sont de type BS, la proposition 2.15 donne que $a_\mathfrak{p}$ est égal à 6. D'après les parties 1.1.2 et 1.2 (notamment la proposition 1.3), ceci implique que p est congru à 3 modulo 4, E a potentiellement bonne réduction supersingulière en $\mathfrak{p}$ et, comme $e_\mathfrak{p}$ est égal à 4, E a réduction additive en $\mathfrak{p}$.

D'après les propositions 1.4, 1.5 et 2.15, le caractère $\mu\chi_p^{-6}$ est ainsi non ramifié en toute place finie de K. Il définit donc une extension abélienne de K contenue dans son corps de classes de Hilbert H_K. Comme les classes des éléments de $\mathcal{J}_K$ forment tout le groupe des classes d'idéaux de K, le caractère $\mu\chi_p^{-6}$ est entièrement déterminé par sa valeur sur les éléments $\sigma_\mathfrak{q}$, lorsque $\mathfrak{q}$ décrit $\mathcal{J}_K$.

Soit $\mathfrak{q}$ un idéal dans $\mathcal{J}_K$; alors d'après la proposition 2.15 (et avec les notations 2.12), on a :

$$\mu(\sigma_\mathfrak{q}) = \beta_\mathfrak{q}^{12} \mod \mathcal{P}_0^\mathfrak{q} = q^6 \mod p = (N\mathfrak{q})^6 \mod p = \chi_p(\sigma_\mathfrak{q})^6.$$

On en déduit que μ est égal à χ_p^6 sur G_K, ce qui implique :

$$\left(\chi_p\lambda^{-1}\right)^6 = \lambda^{12}\lambda^{-6} = \lambda^6.$$

Soit ψ le caractère $\chi_p\lambda^{-2}$ de G_K dans $\mathbb{F}_p^\times$. On a $\psi^6 = \chi_p^6\lambda^{-12} = \chi_p^6\mu^{-1} \equiv 1$ donc l'ordre de ψ divise 6. On peut ainsi écrire ψ comme produit d'un caractère ψ_2 d'ordre divisant 2 et d'un caractère ψ_3 d'ordre divisant 3. Comme p est congru à 3 modulo 4 et que l'image de ψ_3 est formée de carrés de $\mathbb{F}_p^\times$, on a :

$$\psi_2 = \psi_2^{\frac{p-1}{2}} = \psi_2^{\frac{p-1}{2}}\psi_3^{\frac{p-1}{2}} = \psi^{\frac{p-1}{2}} = \chi_p^{\frac{p-1}{2}}\lambda^{-(p-1)} = \chi_p^{\frac{p-1}{2}}.$$

On en déduit finalement :

$$\left(\chi_p\lambda^{-1}\right)^6 = \lambda^6 = \left(\chi_p\psi^{-1}\right)^3 = \left(\chi_p\psi_2^{-1}\right)^3\psi_3^{-3} = \left(\chi_p\chi_p^{\frac{p-1}{2}}\right)^3.$$

□

4.2.2 Type ordinaire

Proposition 4.6. *On suppose que p est strictement supérieur à C_K et que tous les idéaux de $\mathcal{J}_K$ sont de type BO ou que tous les idéaux de $\mathcal{J}_K$ sont de type BO' (proposition 2.15). Alors il existe un unique corps quadratique imaginaire L inclus dans K vérifiant : pour tout idéal $\mathfrak{q}$ dans $\mathcal{J}_K$, $L^\mathfrak{q}$ est égal à L.*

Démonstration. Lorsque tous les idéaux dans $\mathcal{J}_K$ sont de type BO, l'ensemble des éléments τ de G tels que a_τ est égal à 12 est un sous-groupe d'indice 2 de G, égal à $\mathrm{Gal}(K/L^\mathfrak{q})$ pour tout idéal $\mathfrak{q}$ de $\mathcal{J}_K$, $L^\mathfrak{q}$ étant quadratique imaginaire et inclus dans K. (proposition 2.15). Ainsi, le groupe $\mathrm{Gal}(K/L^\mathfrak{q})$, et par suite le corps $L^\mathfrak{q}$, est indépendant de l'idéal $\mathfrak{q}$ dans $\mathcal{J}_K$. Ce corps quadratique commun fournit le corps L de la proposition.

Lorsque tous les idéaux dans $\mathcal{J}_K$ sont de type BO', on applique le même raisonnement à l'ensemble des éléments τ de G tels que a_τ est nul. □

Proposition 4.7. *La norme dans l'extension K/L de tout idéal fractionnaire de K est un idéal fractionnaire principal de L. Le corps de classes de Hilbert de L est contenu dans K.*

Démonstration. Comme toute classe d'idéaux de K contient un idéal de $\mathcal{J}_K$ (proposition 4.2), la première assertion est vraie si et seulement si elle l'est pour tous les idéaux de $\mathcal{J}_K$. Or pour tout idéal $\mathfrak{q}$ de $\mathcal{J}_K$, la norme de $\mathfrak{q}$ dans l'extension K/L est la norme de $\mathfrak{q}$ dans l'extension $K/L^{\mathfrak{q}}$, qui est un idéal principal engendré par $\beta_{\mathfrak{q}}$ (type BO) ou $\overline{\beta_{\mathfrak{q}}}$ (type BO').

On montre ensuite que la première assertion implique la deuxième. Soit H_L le corps de classes de Hilbert de L. L'extension KH_L/K est galoisienne, abélienne et la théorie du corps de classes fournit le diagramme commutatif suivant :

$$\begin{tikzcd} \mathrm{Gal}(KH_L/K) \arrow[r, "\sim"] \arrow[d, hook, "restriction"'] & \mathbb{A}_K^\times/K^\times N_{KH_L/K}\left(\mathbb{A}_{KH_L}^\times\right) \arrow[d, "N_{K/L}"] \\ \mathrm{Gal}(H_L/L) \arrow[r, "\sim"] & \mathbb{A}_L^\times/L^\times N_{H_L/L}\left(\mathbb{A}_{H_L}^\times\right). \end{tikzcd}$$

D'après la première assertion, la flèche verticale de droite est d'image triviale. Comme la flèche verticale de gauche est injective, les corps KH_L et K coïncident, ce qui implique que H_L est inclus dans K. $\square$

Proposition 4.8. *Le nombre premier p est décomposé dans L. Il existe un unique idéal premier $\mathfrak{p}_L$ de L au-dessus de p vérifiant : pour tout idéal premier $\mathfrak{p}$ de K au-dessus de $\mathfrak{p}_L$, $a_{\mathfrak{p}}$ est égal à 12 et pour tout idéal premier $\mathfrak{p}$ de K au-dessus de $\overline{\mathfrak{p}_L}$, $a_{\mathfrak{p}}$ est égal à 0.*

Démonstration. D'après la proposition 2.15, p est décomposé dans le corps $L^{\mathfrak{q}}$, égal à L, pour tout $\mathfrak{q}$ dans $\mathcal{J}_K$.

On rappelle que les entiers a_τ ont été définis par $a_\tau = a_{\tau^{-1}(\mathfrak{p}_0)}$ pour un idéal $\mathfrak{p}_0$ de K au-dessus de p fixé (notations 2.5).

Lorsque tous les idéaux de $\mathcal{J}_K$ sont de type BO, on note $\mathfrak{p}_L$ l'idéal de L situé au-dessous de $\mathfrak{p}_0$ (pour tout idéal $\mathfrak{q}$ dans $\mathcal{J}_K$, $\mathfrak{p}_L$ est donc l'idéal $\mathcal{P}_0^{\mathfrak{q}}$ des notations 2.12). Soit $\mathfrak{p}$ un idéal premier de K au-dessus de $\mathfrak{p}_L$. Il existe un élément τ dans $\mathrm{Gal}(K/L)$ vérifiant $\tau^{-1}(\mathfrak{p}_0) = \mathfrak{p}$. Alors $a_{\mathfrak{p}}$ est égal à a_τ, lui-même égal à 12 car τ est dans $\mathrm{Gal}(K/L)$ qui coïncide avec $\mathrm{Gal}(K/L^{\mathfrak{q}})$. Réciproquement, soit $\mathfrak{p}$ un idéal premier de K au-dessus de p tel que $a_{\mathfrak{p}}$ est égal à 12. Soit τ dans G vérifiant $\tau^{-1}\mathfrak{p}_0 = \mathfrak{p}$. On a alors $a_\tau = a_{\mathfrak{p}} = 12$ donc τ est dans $\mathrm{Gal}(K/L^{\mathfrak{q}})$, qui est égal à $\mathrm{Gal}(K/L)$. Cela implique :

$$\mathfrak{p} \cap \mathcal{O}_L = \left(\tau^{-1}\mathfrak{p}_0\right) \cap \mathcal{O}_L = \tau^{-1}\left(\mathfrak{p}_0 \cap \mathcal{O}_L\right) = \mathfrak{p}_0 \cap \mathcal{O}_L = \mathfrak{p}_L.$$

Ainsi on a $a_{\mathfrak{p}}$ égal à 12 si et seulement si $\mathfrak{p}$ est au-dessus de $\mathfrak{p}_L$ et $a_{\mathfrak{p}}$ égal à 0 sinon ; dans ce deuxième cas, $\mathfrak{p}$ est au-dessus de $\overline{\mathfrak{p}_L}$, qui est l'autre idéal de L au-dessus de p.

Lorsque tous les idéaux de $\mathcal{J}_K$ sont de type BO', on note $\mathfrak{p}_L$ le conjugué complexe de l'idéal de L situé au-dessous de $\mathfrak{p}_0$ (pour tout idéal $\mathfrak{q}$ dans $\mathcal{J}_K$, $\mathfrak{p}_L$

est donc le conjugué complexe de l'idéal $\mathcal{P}_0^{\mathfrak{q}}$ des notations 2.12). Soit $\mathfrak{p}$ un idéal premier de K au-dessus de $\mathfrak{p}_L$. Il existe un élément τ dans G privé de $\mathrm{Gal}(K/L)$ vérifiant $\tau^{-1}(\mathfrak{p}_0) = \mathfrak{p}$. Alors $a_{\mathfrak{p}}$ est égal à a_τ, donc à 12. Réciproquement, soit $\mathfrak{p}$ un idéal premier de K au-dessus de p tel que $a_{\mathfrak{p}}$ est égal à 12. Soit τ dans G vérifiant $\tau^{-1}(\mathfrak{p}_0) = \mathfrak{p}$. On a alors a_τ égal à $a_{\mathfrak{p}}$ qui vaut 12, donc τ est dans G privé de $\mathrm{Gal}(K/L)$. Alors τ et τ^{-1} induisent sur L la conjugaison complexe et on obtient :

$$\mathfrak{p} \cap \mathcal{O}_L = \left(\tau^{-1}(\mathfrak{p}_0)\right) \cap \mathcal{O}_L = \tau^{-1}\left(\mathfrak{p}_0 \cap \mathcal{O}_L\right) = \overline{\mathfrak{p}_0 \cap \mathcal{O}_L} = \mathfrak{p}_L.$$

On a donc encore $a_{\mathfrak{p}}$ égal à 12 si et seulement si $\mathfrak{p}$ est au-dessus de $\mathfrak{p}_L$ et $a_{\mathfrak{p}}$ égal à 0 sinon. □

Proposition 4.9. *Soient α un élément non nul de K premier à $\mathfrak{p}_L$ et $\prod_{\mathfrak{q}\nmid\mathfrak{p}_L} \mathfrak{q}^{\mathrm{val}_{\mathfrak{q}}(\alpha)}$ la décomposition de l'idéal fractionnaire principal $\alpha\mathcal{O}_K$ en produit d'idéaux maximaux de K. Alors on a :*

$$\prod_{\mathfrak{q}\nmid\mathfrak{p}_L} \mu\left(\sigma_{\mathfrak{q}}\right)^{\mathrm{val}_{\mathfrak{q}}(\alpha)} = N_{K/L}\left(\alpha\right)^{12} \mod \mathfrak{p}_L.$$

Démonstration. Le caractère μ est non ramifié aux places finies de K premières à $\mathfrak{p}_L$ et pour tout idéal premier de K au-dessus de $\mathfrak{p}_L$, $a_{\mathfrak{p}}$ est égal à 12. Par une démonstration analogue à celle de la proposition 2.4, on obtient :

$$\prod_{\mathfrak{q}\nmid\mathfrak{p}_L} \mu\left(\sigma_{\mathfrak{q}}\right)^{\mathrm{val}_{\mathfrak{q}}(\alpha)} = \prod_{\mathfrak{p}\mid\mathfrak{p}_L} N_{K_{\mathfrak{p}}/\mathbb{Q}_p}\left(\iota_{\mathfrak{p}}(\alpha)\right)^{12} \mod p.$$

Le nombre premier p étant décomposé dans L (proposition 4.8), le complété $L_{\mathfrak{p}_L}$ de L en $\mathfrak{p}_L$ coïncide avec $\mathbb{Q}_p$ et on a :

$$\begin{aligned}\prod_{\mathfrak{p}\mid\mathfrak{p}_L} N_{K_{\mathfrak{p}}/\mathbb{Q}_p}\left(\iota_{\mathfrak{p}}(\alpha)\right)^{12} \mod p &= \left(\prod_{\mathfrak{p}\mid\mathfrak{p}_L} N_{K_{\mathfrak{p}}/L_{\mathfrak{p}_L}}\left(\iota_{\mathfrak{p}}(\alpha)\right)\right)^{12} \mod p \\ &= N_{K/L}\left(\alpha\right)^{12} \mod \mathfrak{p}_L.\end{aligned}$$

□

Proposition 4.10. *Soient $\mathfrak{q}$ un idéal maximal de K premier à $\mathfrak{p}_L$ et $\alpha_{\mathfrak{q}}$ dans L un générateur de $N_{K/L}(\mathfrak{q})$. Alors on a :*

$$\mu(\sigma_{\mathfrak{q}}) = \alpha_{\mathfrak{q}}^{12} \mod \mathfrak{p}_L.$$

Démonstration. Il existe un idéal $\mathfrak{q}'$ dans $\mathcal{J}_K$ et un élément α non nul de K vérifiant :

$$\mathfrak{q} = \mathfrak{q}' \cdot \left(\alpha\mathcal{O}_K\right).$$

D'après la démonstration de la proposition 4.8 :

- si tous les idéaux de $\mathcal{J}_K$ sont de type BO, alors $\mathfrak{p}_L$ est égal à l'idéal $\mathcal{P}_0^{\mathfrak{q}'}$, la norme de $\mathfrak{q}'$ dans l'extension K/L est $\beta_{\mathfrak{q}'}\mathcal{O}_L$ et on a (notations 2.12 et proposition 2.15)

$$\mu(\sigma_{\mathfrak{q}'}) = \beta_{\mathfrak{q}'}^{12} \mod \mathcal{P}_0^{\mathfrak{q}'} = \beta_{\mathfrak{q}'}^{12} \mod \mathfrak{p}_L;$$

- si tous les idéaux de $\mathcal{J}_K$ sont de type BO' alors $\mathfrak{p}_L$ est le conjugué complexe de l'idéal $\mathcal{P}_0^{\mathfrak{q}'}$, la norme de $\mathfrak{q}'$ dans K/L est $\overline{\beta_{\mathfrak{q}'}}\mathcal{O}_L$ et on a

$$\mu(\sigma_{\mathfrak{q}'}) = \beta_{\mathfrak{q}'}^{12} \mod \mathcal{P}_0^{\mathfrak{q}'} = \beta_{\mathfrak{q}'}^{12} \mod \overline{\mathfrak{p}_L} = \overline{\beta_{\mathfrak{q}'}}^{12} \mod \mathfrak{p}_L.$$

Dans les deux cas, il existe un élément $\alpha_{\mathfrak{q}'}$ de $\mathcal{O}_L$ qui engendre l'idéal $N_{K/L}(\mathfrak{q}')$ et vérifie :

$$\mu(\sigma_{\mathfrak{q}'}) = \alpha_{\mathfrak{q}'}^{12} \mod \mathfrak{p}_L.$$

Soit $\alpha_{\mathfrak{q}}$ dans $\mathcal{O}_L$ un générateur de l'idéal $N_{K/L}(\mathfrak{q})$. On a :

$$N_{K/L}(\mathfrak{q}) = N_{K/L}(\mathfrak{q}') \times \left(N_{K/L}(\alpha)\mathcal{O}_L\right),$$

ce qui implique que les éléments $\alpha_{\mathfrak{q}}$ et $\alpha_{\mathfrak{q}'}N_{K/L}(\alpha)$ de L diffèrent d'une unité de L. Comme L est un corps quadratique imaginaire, cette unité est une racine douzième de l'unité ; on a donc

$$\alpha_{\mathfrak{q}}^{12} = \left(\alpha_{\mathfrak{q}'}N_{K/L}(\alpha)\right)^{12}.$$

Enfin, on a d'après la proposition 4.9

$$\mu(\sigma_{\mathfrak{q}}) = \mu(\sigma_{\mathfrak{q}'}) \times \left(N_{K/L}(\alpha)^{12} \mod \mathfrak{p}_L\right)$$

d'où

$$\mu(\sigma_{\mathfrak{q}}) = \left(\alpha_{\mathfrak{q}'}^{12} \mod \mathfrak{p}_L\right) \times \left(N_{K/L}(\alpha)^{12} \mod \mathfrak{p}_L\right) = \alpha_{\mathfrak{q}}^{12} \mod \mathfrak{p}_L.$$

□

4.3 Homothéties dans l'image de la représentation $\varphi_{E,p}$

On remarque qu'on a, pour tout couple (α, β) dans $\mathbb{F}_p^\times \times \mathbb{F}_p$, l'égalité suivante dans $\mathrm{M}_2(\mathbb{F}_p)$:

$$\begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix}^p = \begin{pmatrix} \alpha^p & p\alpha^{p-1}\beta \\ 0 & \alpha^p \end{pmatrix} = \begin{pmatrix} \alpha^p & 0 \\ 0 & \alpha^p \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}.$$

Pour montrer que l'image de $\varphi_{E,p}$ contient une homothétie de rapport x (x appartenant à $\mathbb{F}_p^\times$), il suffit donc de montrer que l'image de $\varphi_{E,p}$ contient un élément dont la diagonale est (x, x).

4.3.1 Homothéties pour le type supersingulier

Proposition 4.11. *On suppose que p est strictement supérieur à C_K et qu'on est dans le cas supersingulier (partie 4.2.1). Alors l'image de $\varphi_{E,p}$ contient les carrés des homothéties.*

Démonstration. Soit $\mathfrak{p}$ un idéal premier de K au-dessus de p. Comme $a_\mathfrak{p}$ est égal à 6 (proposition 2.15), la proposition 1.3 donne que le caractère λ^4 restreint au sous-groupe d'inertie $I_\mathfrak{p}$ est égal au carré du caractère cyclotomique. Le deuxième caractère diagonal de $\varphi_{E,p}$ est $\chi_p\lambda^{-1}$ et vérifie alors également en restriction à $I_\mathfrak{p}$:

$$\left(\chi_p\lambda^{-1}\right)^4 = \chi_p^4\lambda^{-4} = \chi_p^4\chi_p^{-2} = \chi_p^2.$$

Comme on a supposé p non ramifié dans K, le caractère cyclotomique restreint à $I_\mathfrak{p}$ est surjectif dans $\mathbb{F}_p^\times$. Ainsi, pour tout x dans $\mathbb{F}_p^\times$, l'image de $\varphi_{E,p}$ contient un élément de diagonale (x^2, x^2) et la puissance p-ième de cet élément qui est une homothétie de rapport x^2. □

4.3.2 Homothéties pour le type ordinaire

Proposition 4.12. *On suppose que p est strictement supérieur à C_K et qu'on est dans le cas ordinaire (partie 4.2.2). Alors l'image de $\varphi_{E,p}$ contient les puissances douzièmes des homothéties.*

Démonstration. Soit x un élément de $\mathbb{F}_p^\times$.

Soit $\mathfrak{p}$ un idéal premier de K au-dessus de $\mathfrak{p}_L$. D'après la proposition 4.8, $a_\mathfrak{p}$ est égal à 12 donc la restriction à $I_\mathfrak{p}$ de la diagonale de $\varphi_{E,p}$, élevée à la puissance 12, vaut $(\mu, \chi_p^{12}\mu^{-1}) = (\chi_p^{12}, 1)$. Comme χ_p est surjectif de $I_\mathfrak{p}$ dans $\mathbb{F}_p^\times$, il existe dans G_K un élément σ tel que la diagonale de $\varphi_{E,p}(\sigma)$ est $(x^{12}, 1)$.

Soit $\mathfrak{p}'$ un idéal premier de K au-dessus de $\overline{\mathfrak{p}_L}$. D'après la proposition 4.8, $a_{\mathfrak{p}'}$ est nul donc la restriction à $I_{\mathfrak{p}'}$ de la diagonale de $\varphi_{E,p}$, élevée à la puissance 12, vaut $(\mu, \chi_p^{12}\mu^{-1}) = (1, \chi_p^{12})$. Comme χ_p est surjectif de $I_{\mathfrak{p}'}$ dans $\mathbb{F}_p^\times$, il existe dans G_K un élément σ' tel que la diagonale de $\varphi_{E,p}(\sigma')$ est $(1, x^{12})$.

Alors l'image par $\varphi_{E,p}$ du produit $\sigma\sigma'$ de G_K a pour diagonale (x^{12}, x^{12}) ; sa puissance p-ième est donc une homothétie de rapport x^{12} contenue dans l'image de $\varphi_{E,p}$. □

Références

[1] Nicolas Billerey. Critères d'irréductibilité pour les représentations des courbes elliptiques. *Int. J. Number Theory*, 7(4):1001–1032, 2011.

[2] Yann Bugeaud and Kálmán Győry. Bounds for the solutions of unit equations. *Acta Arith.*, 74(1):67–80, 1996.

[3] Agnès David. *Caractère d'isogénie et borne uniforme pour les homothéties.* PhD thesis, IRMA, Strasbourg, 2008.

[4] Agnès David. Borne uniforme pour les homothéties dans l'image de Galois associée aux courbes elliptiques. *J. Number Theory*, 131(11):2175–2191, 2011. Disponible en ligne arXiv:1007.4725v1.

[5] Alain Kraus. Courbes elliptiques semi-stables sur les corps de nombres. *Int. J. Number Theory*, 3(4):611–633, 2007.

[6] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[7] Eric Larson and Dmitry Vaintrob. Determinants of subquotients of Galois representations associated to abelian varieties. *preprint*, 2011. Disponible en ligne arXiv:1110.0255v2.

[8] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[9] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[10] Fumiyuki Momose. Isogenies of prime degree over number fields. *Compositio Math.*, 97(3):329–348, 1995.

[11] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[12] Michel Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[13] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[14] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[15] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.