Caractère d'isogénie et borne uniforme pour les homothéties

Agnès David

Agnès David

CARACTÈRE D'ISOGÉNIE ET BORNE UNIFORME POUR LES HOMOTHÉTIES

Agnès David

CARACTÈRE D'ISOGÉNIE ET BORNE UNIFORME POUR LES HOMOTHÉTIES

Agnès David

TABLE DES MATIÈRES

INTRODUCTION

L'objet de cette thèse est l'obtention de résultats uniformes sur l'image des représentations galoisiennes associées aux points de torsion des courbes elliptiques possédant une isogénie de degré premier.

Le cadre précis se compose d'un corps de nombres K différent de $\mathbb{Q}$, d'une courbe elliptique E définie sur K et d'un nombre premier p.

Le module de Tate $\mathrm{T}_p(E)$ de E en p est un $\mathbb{Z}_p$-module libre de rang 2 sur lequel le groupe de Galois absolu G_K de K agit $\mathbb{Z}_p$-linéairement. Cette action fournit donc une représentation ρ_p de G_K dans le groupe $\mathrm{GL}_{\mathbb{Z}_p}(\mathrm{T}_p(E))$.

Le groupe $E(\overline{K})[p]$ des points de p-torsion de E dans une clôture algébrique $\overline{K}$ de K est un $\mathbb{F}_p$-espace vectoriel de dimension 2, isomorphe au quotient $\mathrm{T}_p(E)/p\mathrm{T}_p(E)$. L'action de G_K sur $\mathrm{T}_p(E)$ induit une action $\mathbb{F}_p$-linéaire de G_K sur $E(\overline{K})[p]$ qui donne une représentation φ_p de G_K dans $\mathrm{GL}_{\mathbb{F}_p}(E(\overline{K})[p])$.

Lorsque des bases compatibles de $\mathrm{T}_p(E)$ et $E(\overline{K})[p]$ sont fixées, on peut considérer que ρ_p est à valeurs dans $\mathrm{GL}_2(\mathbb{Z}_p)$ et φ_p à valeurs dans $\mathrm{GL}_2(\mathbb{F}_p)$; φ_p correspond alors à la réduction de ρ_p modulo p.

Dans tout ce texte, on se place dans le cas où la courbe elliptique E possède une isogénie de degré p définie sur K. Cela signifie que E possède un sous-groupe d'ordre p défini sur K. Pour tout la suite on fixe V un tel sous-groupe.

L'existence d'une isogénie de degré p définie sur K implique que l'image de la représentation φ_p est incluse dans un sous-groupe de Borel de $\mathrm{GL}_{\mathbb{F}_p}(E(\overline{K})[p])$: dans une base de $E(\overline{K})[p]$ dont le premier vecteur appartient à $V(\overline{K})$, la représentation φ_p est triangulaire supérieure.

Dans toute la suite du texte on fixe également une telle base de $E(\overline{K})[p]$ et on considère la représentation φ_p comme à valeur dans $\mathrm{GL}_2(\mathbb{F}_p)$. Elle est alors de la forme

$$\begin{pmatrix} \lambda & \star \\ 0 & \lambda' \end{pmatrix}$$

où λ et λ' sont deux caractères de G_K dans $\mathbb{F}_p^\times$. Le caractère λ correspond à l'action de G_K sur $V(\overline{K})$; suivant la terminologie de [**Maz78**] et [**Mom95**], on l'appelle « caractère d'isogénie ». On sait de plus que le déterminant de la représentation φ_p est le caractère cyclotomique χ_p ; ceci implique que le caractère λ' est égal au caractère $\chi_p\lambda^{-1}$.

On suppose également (à partir de la partie 2.2 et jusqu'à la fin du texte) que le corps K est galoisien sur $\mathbb{Q}$.

On obtient le résultat suivant (partie 3.2) sur la forme du caractère d'isogénie λ :

Théorème I. — *Il existe un nombre réel C_K ne dépendant que du corps K et vérifiant : si p est strictement plus grand que C_K, le caractère d'isogénie est de l'un des deux types suivants.*

Type (0) : *Le caractère λ^{12} est égal à χ_p^6 (dans ce cas, p est congru à 3 modulo 4) ;*

Type (MC) : *Il existe un corps quadratique imaginaire L vérifiant*

- *L est contenu dans K ;*
- *p est totalement décomposé dans L ;*
- *le corps de classes de Hilbert de L est contenu dans K (en particulier la norme dans l'extension K/L d'un idéal de K est un idéal principal de L) ;*
- *il existe un idéal $\mathfrak{p}_L$ de L au-dessus de p vérifiant : pour tout idéal maximal $\mathfrak{q}$ de K premier à p, et tout élément $\alpha_\mathfrak{q}$ de $\mathcal{O}_L$ générateur de $N_{K/L}(\mathfrak{q})$, l'image par λ^{12} d'un relèvement à G_K du Frobenius de $\mathfrak{q}$ est $\alpha_\mathfrak{q}^{12} \bmod \mathfrak{p}_L$.*

On s'attend à ce que le type (0) ne se produise pas lorsque p est « assez grand » et à ce que le type (MC) provienne de courbes à multiplication complexe.

Le théorème I a pour conséquence (partie 3.3) :

Théorème II. — *Un nombre réel C_K satisfaisant le théorème I vérifie également : si p est strictement supérieur à C_K, alors l'image de φ_p contient les homothéties qui sont des puissances douzièmes.*

De plus, on détermine de manière effective un nombre réel C_K satisfaisant le théorème I. Les grandeurs associées au corps K qui entrent en jeu sont les suivantes :

- d le degré de K sur $\mathbb{Q}$;
- h le nombre de classes d'idéaux de K ;
- Δ_K le discriminant de K ;
- r_K le rang du groupe des unités de K (comme on a supposé l'extension $K/\mathbb{Q}$ galoisienne, r_K est égal à $d-1$ si K est inclus dans $\mathbb{R}$ et à $\frac{d}{2}-1$ sinon) ;
- R_K le régulateur de K ;
- δ_K un réel strictement positif minorant $d\ln(\mathrm{h}(\alpha))$ pour tout élément non nul α de K qui n'est pas une racine de l'unité, où h désigne la hauteur absolue sur K ; on peut prendre (voir partie 2.3 et [**BG96**])
  - δ_K égal à $\frac{\ln 2}{r_K+1}$ si d vaut 1 ou 2 ;
  - δ_K égal à $\frac{1}{53d\ln(6d)}$ ou $\frac{1}{1201}\left(\frac{\ln\ln d}{\ln d}\right)^3$ si d est supérieur ou égal à 3.

À partir de ces données on définit :

$$C_1(K)=\frac{r_K^{r_K+1}\delta_K^{-(r_K-1)}}{2} \text{ et } C_2(K)=\exp\left(12dC_1(K)R_K\right).$$

On utilise également une constante absolue (et calculable) A, intervenant dans une forme effective du théorème de Chebotarev (voir [**LMO79**] et partie 3.1). On a alors le résultat suivant :

Théorème I'. — *Le maximum des deux quantités*

$$65(3^{12d}-1)(24d)^6 \text{ et } \left[\left(2(\Delta_K)^{Ah}\right)^{12h}C_2(K)+\left(2(\Delta_K)^{Ah}\right)^{6h}\right]^{2d}$$

satisfait le théorème I.

Une forme du théorème I figure déjà dans l'article [**Mom95**] de Momose, mais sans détermination explicite de la constante C_K ; le théorème de Momose présente également un troisième type, que l'on a ici éliminé (partie 3.2.1).

Ces résultats s'inscrivent dans le domaine des bornes uniformes sur l'image des représentations galoisiennes associées aux points de torsion des courbes elliptiques.

On s'attend à ce que l'image de φ_p soit « asymptotiquement grosse » au sens du résultat démontré par Serre dans [**Ser72**] :

Théorème (Serre). — *On suppose que la courbe elliptique E n'a pas de multiplication complexe. Alors il existe un nombre réel $C(K,E)$, ne dépendant que du corps de nombres K et de la courbe elliptique E, qui vérifie : si p est plus grand que $C(K,E)$ alors la représentation φ_p est surjective.*

Un problème difficile consiste à s'affranchir de la dépendance en la courbe elliptique E dans la constante $C(K,E)$.

Sous l'hypothèse que le nombre premier p est non ramifié dans le corps K, le déterminant χ_p de la représentation φ_p est surjectif dans $\mathbb{F}_p^\times$. Si l'image de φ_p n'est pas tout $\mathrm{GL}_2(\mathbb{F}_p)$, elle est alors incluse dans un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_p)$ d'un des types suivants : sous-groupe de Borel, normalisateur d'un sous-groupe de Cartan (déployé ou non déployé) ou sous-groupe exceptionnel.

Le cas des sous-groupes exceptionnels n'est pas difficile à écarter (voir par exemple [**Maz77**]).

Sur le corps $\mathbb{Q}$ des rationnels, Mazur a éliminé, à un nombre fini de nombres premiers près, le cas d'un sous-groupe de Borel, correspondant à une isogénie rationnelle de degré p ([**Maz78**]) :

Théorème (Mazur). — *S'il existe une courbe elliptique définie sur $\mathbb{Q}$ possédant une isogénie de degré premier p définie également sur $\mathbb{Q}$, alors p est égal à* 2, 3, 5, 7, 13, 11, 17, 19, 37, 43, 67 *ou* 163.

Une conséquence de ce théorème est la classification des groupes pouvant apparaître comme le sous-groupe de torsion du groupe de Mordell-Weil d'une courbe elliptique définie sur $\mathbb{Q}$.

À la suite de Mazur, Merel ([**Mer96**]) puis Parent ([**Par99**]) ont obtenu des bornes uniformes pour l'ordre des points de torsion d'une courbe elliptique sur un corps de nombres quelconque :

Théorème (Merel). — *Si le degré d de K sur $\mathbb{Q}$ est strictement plus grand que* 1 *et si E possède un point d'ordre p défini sur K, alors p est strictement inférieur à d^{3d^2}.*

Dans un texte non publié, Oesterlé montre qu'on peut remplacer « p est strictement inférieur à d^{3d^2} » par « p est inférieur ou égal à $(1+3^{d/2})^2$ ». On pourrait ainsi remplacer $65(3^{12d}-1)(24d)^6$ par $(1+3^{6d})^2$ dans le théorème I'.

Théorème (Parent). — *Si E possède un point d'ordre p^n défini sur K, alors on a :*
- *si p est différent de 2 et 3, $p^n \leq 65(3^d-1)(2d)^6$;*
- *si p est égal à 3, $3^n \leq 65(5^d-1)(2d)^6$;*
- *si p est égal à 2, $2^n \leq 129(3^d-1)(3d)^6$.*

Dans [**Ara08**], Arai démontre qu'il existe un ensemble fini Σ, dépendant de p, d'éléments de K, qui vérifie : si l'invariant j de la courbe E n'appartient pas à Σ, alors l'image de la représentation ρ_p contient $\mathrm{SL}_2(\mathbb{Z}_p)$. La méthode suivie, qui utilise le théorème de Mordell sur la finitude du nombre de points rationnels sur des courbes modulaires de genre supérieur ou égal à 2, ne donne pas de borne effective sur la hauteur des éléments dans Σ.

Sans condition sur l'anneau des endomorphismes de la courbe elliptique E, il est possible de prouver qu'il existe un nombre réel $C'(K,E)$ ne dépendant que du corps de nombres K et de E, qui vérifie : si p est plus grand que $C'(K,E)$, alors l'image de φ_p contient les homothéties $\mathbb{F}_p^\times$.

Dans sa thèse ([**Eck05**]), Eckstein démontre le résultat suivant :

Théorème (Eckstein). — *Si p est strictement supérieur à*

$$\max\left(\Delta_K, (48dh)^{3(48dh)^2}\right),$$

alors
- *soit l'image de la représentation ρ_p contient les puissances douzième des homothéties $\left(\mathbb{Z}_p^\times\right)^{12}$,*
- *soit la courbe E n'a pas multiplication complexe, elle possède une isogénie de degré p définie sur K et il existe une place de K au-dessus de p en laquelle E a potentiellement bonne réduction de hauteur 2, avec un polygone de Newton ayant deux pentes distinctes.*

Eckstein montre que l'on ne peut pas se passer de la puissance 12 si on souhaite une borne indépendante de la courbe elliptique (elle exhibe un contre-exemple où la courbe E a multiplication complexe).

Le cas écarté dans son théorème ne se produit que lorsque l'image de la représentation φ_p est incluse dans un sous-groupe de Borel de $\mathrm{GL}_2(\mathbb{F}_p)$. Avec le théorème II, on obtient donc un résultat uniforme (et effectif) sur les homothéties contenues dans l'image de la représentation φ_p.

Les méthodes suivies pour démontrer le théorème I sont celles développées par Mazur ([**Maz78**]) puis Momose ([**Mom95**]) ; elles consistent en l'étude du caractère d'isogénie λ.

Dans la première partie de ce texte, on s'intéresse à la situation locale aux places finies de K.

Pour les places hors de p, on détermine la restriction du caractère λ à un sous-groupe de décomposition ; à l'aide de [**ST68**] on borne notamment l'image de la ramification. On obtient que la puissance douzième λ^{12} du caractère d'isogénie est non ramifiée hors de p et les valeurs possibles de l'image d'un relèvement du Frobenius en fonction du type de réduction de la courbe elliptique.

Pour les places au-dessus de p, on utilise les résultats de [**Ser72**] et un théorème de Raynaud ([**Ray74**]) pour déterminer la restriction de λ au sous-groupe d'inertie. On obtient que le caractère λ^{12} restreint au sous-groupe d'inertie en une place $\mathfrak{p}$ de K au-dessus de p est égal à une puissance $\chi_p^{a_\mathfrak{p}}$ du caractère cyclotomique pour un entier $a_\mathfrak{p}$ valant 0, 4, 6, 8 ou 12.

Dans la deuxième partie on considère l'application de réciprocité associée par la théorie du corps de classes globale à l'extension cyclique du corps K trivialisant le caractère λ^{12}. Ceci permet d'établir des relations entre les informations locales obtenues dans la première partie. On constate que pour p « assez grand » par rapport à une place finie $\mathfrak{q}$ de K hors de p, le comportement de la courbe en la place $\mathfrak{q}$ détermine, à travers la famille des entiers $(a_\mathfrak{p})_\mathfrak{p}$, la ramification du caractère λ^{12} aux places au-dessus de p. La détermination du nombre réel au delà duquel p est « assez grand » fait intervenir les bornes de Bugeaud et Győry ([**BG96**]) sur la hauteur d'un représentant d'une classe d'entiers de K modulo les unités.

Dans la troisième partie, on se ramène à un nombre fini de places hors de p en utilisant une forme effective du théorème de Chebotarev ([**LMO79**]). Avec les résultats de la deuxième partie, on obtient pour p « assez grand » (« assez grand » ne dépendant plus que du corps K) trois formes possibles du caractère d'isogénie, dont les deux types du théorème I. Le troisième type, correspondant au cas où l'un des deux caractères λ^{12} ou λ'^{12} est partout non ramifié, est éliminé en utilisant les bornes uniformes sur l'ordre des points de torsion d'une courbe elliptique. On obtient ainsi l'expression finale du nombre C_K et le théorème I ; on en déduit enfin le théorème II.

CHAPITRE 1

ÉTUDE LOCALE AUX PLACES FINIES

Dans cette partie, on considère les restrictions aux places finies de K du caractère d'isogénie λ donnant l'action du groupe de Galois absolu de K sur le sous-groupe $V(\overline{K})$ d'ordre p des points de p-torsion de E (V étant un sous-groupe d'ordre p de E rationnel sur K fixé dans l'introduction).

On note K^λ l'extension cyclique de K trivialisant le caractère λ et μ la puissance douzième de λ ; c'est encore un caractère de G_K dans $\mathbb{F}_p^\times$. Les résultats obtenus sur les formes locales du caractère μ sont résumés à la fin de cette partie (1.3).

Pour toute la suite du texte, on fixe un plongement du corps K dans $\mathbb{C}$ (on considère ainsi K comme un sous-corps de $\mathbb{C}$) ; on suppose également p strictement plus grand que 5 et non ramifié dans l'extension $K/\mathbb{Q}$ (en particulier p est strictement plus grand que $\max(5, \Delta_K)$).

1.1. Hors de p

Dans cette partie, $\mathfrak{q}$ désigne un idéal maximal de K premier à p. On note q la caractéristique de $\mathfrak{q}$ (c'est un nombre premier rationnel différent de p), $N\mathfrak{q}$ la norme de $\mathfrak{q}$, $k_\mathfrak{q}$ son corps résiduel (il est fini, de caractéristique q et de cardinal $N\mathfrak{q}$) et $K_\mathfrak{q}$ le complété de K en $\mathfrak{q}$.

On fixe une place $\overline{\mathfrak{q}}$ de $\overline{K}$ au-dessus de $\mathfrak{q}$. Le corps résiduel de $\overline{\mathfrak{q}}$ est une clôture algébrique $\overline{k_\mathfrak{q}}$ du corps $k_\mathfrak{q}$. On note $D_\mathfrak{q}$ le sous-groupe de décomposition de $\overline{\mathfrak{q}}$ dans G_K et $I_\mathfrak{q}$ son sous-groupe d'inertie. Le groupe $D_\mathfrak{q}$ est isomorphe au groupe de Galois absolu $G_{K_\mathfrak{q}}$ de la complétion $K_\mathfrak{q}$, et le quotient $D_\mathfrak{q}/I_\mathfrak{q}$ est canoniquement isomorphe au groupe de Galois

absolu $\mathrm{Gal}(\overline{k_\mathfrak{q}}/k_\mathfrak{q})$ de $k_\mathfrak{q}$. On fixe également un élément $\sigma_\mathfrak{q}$ de $D_\mathfrak{q}$ qui induit sur $\overline{k_\mathfrak{q}}$ le morphisme de Frobenius de $k_\mathfrak{q}$ (c'est-à-dire l'élévation à la puissance $N\mathfrak{q}$ dans $\overline{k_\mathfrak{q}}$).

On cherche à déterminer les images dans $\mathbb{F}_p^\times$ de $I_\mathfrak{q}$ et $\sigma_\mathfrak{q}$ par λ. Les résultats obtenus dépendent notamment du type de réduction de la courbe E en $\mathfrak{q}$.

1.1.1. Réduction semi-stable. —

Proposition 1.1.1. — *Si E a réduction multiplicative en $\mathfrak{q}$, alors :*

(i) *l'image de $I_\mathfrak{q}$ par λ est triviale ;*
(ii) *$\lambda(\sigma_\mathfrak{q})$ est égal à la classe de 1, -1, $N\mathfrak{q}$ ou $-N\mathfrak{q}$ modulo p ;*
(iii) *les valeurs correspondantes de $(\chi_p\lambda^{-1})(\sigma_\mathfrak{q})$ sont les classes de $N\mathfrak{q}$, $-N\mathfrak{q}$, 1 et -1 modulo p.*

Démonstration. — D'après [**Sil92**] (app. C thm 14.1), il existe une extension K' de $K_\mathfrak{q}$, non ramifiée et de degré 2, sur laquelle la courbe E est isomorphe à une courbe de Tate.

Le groupe de Galois absolu de K' est un sous-groupe $G_{K'}$ de $G_{K_\mathfrak{q}}$ d'indice 2. Comme l'extension $K'/K_\mathfrak{q}$ est non ramifiée, le sous-groupe d'inertie $I_{K'}$ de $G_{K'}$ coïncide avec celui $I_\mathfrak{q}$ de $G_{K_\mathfrak{q}}$. De plus le corps résiduel k' de K' est de degré 2 sur $k_\mathfrak{q}$ (il est donc de cardinal $(N\mathfrak{q})^2$) et $\sigma_\mathfrak{q}^2$ est un élément de $G_{K'}$ qui induit sur $\overline{k_\mathfrak{q}}$ le morphisme de Frobenius de k'.

Soit x un élément de K', de valuation strictement positive, tel que E est isomorphe sur K' à la courbe de Tate associée à x. Alors l'ensemble $E(\overline{K'})$ des points de E sur $\overline{K'}$ est isomorphe comme $G_{K'}$-module au quotient $\overline{K'}^\times/x^\mathbb{Z}$. L'ensemble $E(\overline{K'})[p]$ des points de p-torsion de E sur $\overline{K'}$ s'insère donc dans la suite exacte de $G_{K'}$-modules suivante :

$$0 \longrightarrow \mu_p(\overline{K'}) \longrightarrow E(\overline{K'})[p] \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

où $\mu_p(\overline{K'})$ désigne le groupe des racines p-ièmes de l'unité de $\overline{K'}$ et $G_{K'}$ agit trivialement sur $\mathbb{Z}/p\mathbb{Z}$.

Le sous-groupe V de E, d'ordre p et rationnel sur K, donne un sous-$G_{K'}$-module $V(\overline{K'})$ d'ordre p de $E(\overline{K'})[p]$. Deux cas sont possibles.

Soit l'intersection $\mu_p(\overline{K'}) \cap V(\overline{K'})$ est réduite à l'élément neutre. Dans ce cas $V(\overline{K'})$ s'envoie isomorphiquement comme $G_{K'}$-module dans $\mathbb{Z}/p\mathbb{Z}$.

Alors $G_{K'}$ agit trivialement sur $V(\overline{K'})$ donc il en est de même pour son sous-groupe $I_{K'}$, égal à $I_\mathfrak{q}$, et pour l'élément $\sigma_\mathfrak{q}^2$. Leurs images par λ sont donc égales à 1 dans $\mathbb{F}_p^\times$.

Soit $\mu_p(\overline{K'})$ et $V(\overline{K'})$ coïncident. Comme p est différent de la caractéristique résiduelle q de K', le groupe $\mu_p(\overline{K'})$ s'identifie, par réduction modulo l'idéal maximal de K', donc de manière compatible avec les actions des groupes $G_{K'}$ et $G_{k'}$, au groupe $\mu_p(\overline{k'})$ des racines p-ièmes de l'unité dans $\overline{k'}$. On obtient alors que $I_{K'}$ agit trivialement sur $V(\overline{K'})$ et que $\lambda(\sigma_\mathfrak{q}^2)$ vaut $(N\mathfrak{q})^2$ mod p.

La dernière assertion de la proposition résulte de l'égalité $\chi_p(\sigma_\mathfrak{q}) = N\mathfrak{q}$ mod p. □

Proposition 1.1.2. — *Si E a bonne réduction en $\mathfrak{q}$, alors :*

(i) *l'image de $I_\mathfrak{q}$ par λ est triviale ;*
(ii) *le polynôme caractéristique $P_\mathfrak{q}(X)$ de l'action de $\sigma_\mathfrak{q}$ sur le module de Tate de E en p est à coefficients dans $\mathbb{Z}$;*
(iii) *les racines de $P_\mathfrak{q}(X)$ ont même valeur absolue complexe $\sqrt{N\mathfrak{q}}$; le corps $L^\mathfrak{q}$ qu'elles engendrent est soit $\mathbb{Q}$ soit un corps quadratique imaginaire ;*
(iv) *soit $\mathcal{P}^\mathfrak{q}$ un idéal maximal de $L^\mathfrak{q}$ au-dessus de p ; alors il existe une racine $\beta_\mathfrak{q}$ de $P_\mathfrak{q}(X)$ telle que la classe de $\beta_\mathfrak{q}$ modulo $\mathcal{P}^\mathfrak{q}$ soit dans $\mathbb{F}_p$ et y soit égale à $\lambda(\sigma_\mathfrak{q})$; le conjugué complexe $\overline{\beta_\mathfrak{q}}$ de $\beta_\mathfrak{q}$ est l'autre racine de $P_\mathfrak{q}(X)$; sa classe modulo $\mathcal{P}^\mathfrak{q}$ est dans $\mathbb{F}_p$ et y vaut $(\chi_p\lambda^{-1})(\sigma_\mathfrak{q})$.*

Démonstration. — Par le critère de Néron-Ogg-Shafarevich (ou [**ST68**] thm 1)), la représentation φ_p de G_K sur les points de p-torsion de E est non ramifiée en $\mathfrak{q}$. En particulier, l'inertie $I_\mathfrak{q}$ agit trivialement sur le sous-groupe $V(\overline{K_\mathfrak{q}})$ de $E(\overline{K_\mathfrak{q}})[p]$.

Les points (ii) et (iii) découlent des conjectures de Weil pour les courbes elliptiques (voir aussi [**ST68**] §2 thm 3).

Soit $P_\mathfrak{q}(X) = X^2 - T_\mathfrak{q}X + N\mathfrak{q}$ le polynôme caractéristique de l'action de $\sigma_\mathfrak{q}$ sur le module de Tate de E en p. Le polynôme caractéristique de $\varphi_p(\sigma_\mathfrak{q})$ donnant l'action de $\sigma_\mathfrak{q}$ sur les points de p-torsion de E vaut alors $X^2 - (T_\mathfrak{q} \bmod p)X + (N\mathfrak{q} \bmod p)$. Comme $\varphi_p(\sigma_\mathfrak{q})$ est une matrice triangulaire supérieure (de taille 2) dont les coefficients diagonaux

sont $\lambda(\sigma_{\mathfrak{q}})$ et $(\chi_p\lambda^{-1})(\sigma_{\mathfrak{q}})$, ce polynôme caractéristique est aussi égal à $(X-\lambda(\sigma_{\mathfrak{q}}))(X-(\chi_p\lambda^{-1})(\sigma_{\mathfrak{q}}))$.

Soient β et β' les racines de $P_{\mathfrak{q}}(X)$. On a dans le corps $L^{\mathfrak{q}}$ engendré par β (ou β') : $X^2 - T_{\mathfrak{q}}X + N\mathfrak{q} = (X-\beta)(X-\beta')$. Soit $\mathcal{P}^{\mathfrak{q}}$ un idéal maximal du corps $L^{\mathfrak{q}}$ situé au-dessus de p. On a alors l'égalité suivante entre polynômes à coefficients dans le corps résiduel de $L^{\mathfrak{q}}$ en $\mathcal{P}^{\mathfrak{q}}$:

$$\begin{aligned}(X-(\beta \bmod \mathcal{P}^{\mathfrak{q}}))(X-(\beta' \bmod \mathcal{P}^{\mathfrak{q}})) &= X^2-(T_{\mathfrak{q}} \bmod p)X+(N\mathfrak{q} \bmod p)\\ &= (X-\lambda(\sigma_{\mathfrak{q}}))(X-(\chi_p\lambda^{-1})(\sigma_{\mathfrak{q}}))\,.\end{aligned}$$

Ceci prouve le point (iv). □

1.1.2. Réduction non semi-stable. —

Lemme 1.1.3. — *Soient ℓ et ℓ' deux nombres premiers rationnels distincts, avec ℓ' supérieur ou égal à 5 ; soient $\mathcal{L}$ un idéal premier de K au-dessus de ℓ, $K_{\mathcal{L}}$ le complété de K en $\mathcal{L}$ et K' une extension finie de $K_{\mathcal{L}}$. On suppose que E possède un point d'ordre ℓ' défini sur K'. Alors E n'a pas réduction additive sur K'.*

Démonstration. — Les idées de cette démonstration proviennent de [**Maz78**] (démonstration du théorème 4.1 ou §6).

On suppose par l'absurde que E a réduction additive sur K'. Soit $\mathcal{E}_{K'}$ le modèle de Néron de E sur K', $\widetilde{\mathcal{E}}_{K'}$ sa fibre spéciale, $\widetilde{\mathcal{E}}^0_{K'}$ la composante neutre de cette fibre spéciale et k' le corps résiduel de K'. Alors :

(i) le groupe $\widetilde{\mathcal{E}}^0_{K'}(k')$ est isomorphe à $(k',+)$;
(ii) le quotient $\widetilde{\mathcal{E}}_{K'}(k')/\widetilde{\mathcal{E}}^0_{K'}(k')$ est un groupe d'ordre au plus 4 ([**Sil92**] app. C §15 tableau 15.1) ;
(iii) on dispose d'une application de réduction de $E(K')$ dans $\widetilde{\mathcal{E}}_{K'}(k')$ qui est un morphisme de groupes.

Par hypothèse, $E(K')$ possède un point P d'ordre ℓ'. On raisonne selon l'image $\widetilde{P}$ de P dans $\widetilde{\mathcal{E}}_{K'}(k')$ par l'application de réduction.

Soit $\widetilde{P}$ appartient à la composante neutre de $\widetilde{\mathcal{E}}_{K'}(k')$. Alors P est dans le sous-groupe $E^0(K')$ de $E(K')$ formé des points envoyés dans $\widetilde{\mathcal{E}}^0_{K'}(k')$ par l'application de réduction. Ce sous-groupe est décrit par la suite exacte de groupes suivante ([**Sil92**] VII §2 prop. 2.1 et 2.2) :

$$0 \longrightarrow \widehat{E}_{K'}(\mathfrak{m}_{K'}) \longrightarrow E^0(K') \longrightarrow k'^{+} \longrightarrow 0,$$

où $\widehat{E}_{K'}$ désigne le groupe formel associé à une équation de Weierstrass minimale de E sur l'anneau des entiers $\mathcal{O}_{K'}$ de K' et $\mathfrak{m}_{K'}$ désigne l'unique idéal maximal de $\mathcal{O}_{K'}$.

Comme ℓ' est différent de la caractéristique résiduelle ℓ de K', le groupe $\widehat{E}_{K'}(\mathfrak{m}_{K'})$ n'a pas de sous-groupe d'ordre ℓ' ([**Sil92**] IV §3 prop. 3.2). Ceci implique que le sous-groupe engendré par P est envoyé injectivement dans $(k', +)$. Or le corps $(k', +)$, de caractéristique ℓ, n'a pas non plus de point d'ordre ℓ'. On obtient donc une contradiction.

Soit $\widetilde{P}$ n'est pas dans $\widetilde{\mathcal{E}}^0_{K'}(k')$. Alors $\widetilde{P}$ engendre dans $\widetilde{\mathcal{E}}_{K'}(k')$ un sous-groupe d'ordre ℓ' d'intersection triviale avec $\widetilde{\mathcal{E}}^0_{K'}(k')$. Ce sous-groupe s'envoie donc injectivement dans le quotient $\widetilde{\mathcal{E}}_{K'}(k')/\widetilde{\mathcal{E}}^0_{K'}(k')$. Ce quotient étant d'ordre au plus 4, on obtient une contradiction avec le choix de ℓ' supérieur ou égal à 5. □

On rappelle que K^λ désigne l'extension du corps K trivialisant le caractère λ (c'est donc la plus petite extension de K sur laquelle les points du sous-groupe V sont définis).

Proposition 1.1.4. — *Si E a mauvaise réduction additive et potentiellement réduction multiplicative en $\mathfrak{q}$, alors :*

(i) *l'image de $I_\mathfrak{q}$ par λ est d'ordre 2 ;*
(ii) *$\lambda(\sigma_\mathfrak{q})$ est égal à la classe de 1, -1, $N\mathfrak{q}$ ou $-N\mathfrak{q}$ modulo p ;*
(iii) *les valeurs correspondantes de $(\chi_p\lambda^{-1})(\sigma_\mathfrak{q})$ sont les classes de $N\mathfrak{q}$, $-N\mathfrak{q}$, 1 et -1 modulo p.*
(iv) *E a réduction multiplicative en toute place de K^λ au-dessus de $\mathfrak{q}$.*

Démonstration. — D'après [**Sil92**] (app. C thm 14.1), il existe une extension K' de $K_\mathfrak{q}$, totalement ramifiée et de degré 2, sur laquelle E est isomorphe à une courbe de Tate (en particulier, E a réduction multiplicative sur K').

Le groupe de Galois absolu de K' est un sous-groupe $G_{K'}$ de $G_{K_\mathfrak{q}}$ d'indice 2 et son sous-groupe d'inertie $I_{K'}$ est un sous-groupe d'indice 2 de $I_\mathfrak{q}$. Le corps résiduel k' de K' coïncide avec $k_\mathfrak{q}$ et $\sigma_\mathfrak{q}^2$ est un élément de $G_{K'}$ qui induit sur $\overline{k_\mathfrak{q}}$ le carré du morphisme de Frobenius commun de k' et $k_\mathfrak{q}$.

Comme dans la démonstration de la proposition 1.1.1, l'ensemble $E(\overline{K'})[p]$ des points de p-torsion de E sur $\overline{K'}$ est décrit par la suite exacte de $G_{K'}$-modules suivante :

$$0 \longrightarrow \mu_p(\overline{K'}) \longrightarrow E(\overline{K'})[p] \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

où $\mu_p(\overline{K'})$ désigne le groupe des racines p-ièmes de l'unité de $\overline{K'}$ et $G_{K'}$ agit trivialement sur $\mathbb{Z}/p\mathbb{Z}$. Deux cas sont possibles pour le sous-$G_{K'}$-module $V(\overline{K'})$ d'ordre p de $E(\overline{K'})[p]$.

Soit l'intersection $\mu_p(\overline{K'}) \cap V(\overline{K'})$ est réduite à l'élément neutre. Alors $V(\overline{K'})$ s'envoie isomorphiquement comme $G_{K'}$-module dans $\mathbb{Z}/p\mathbb{Z}$. Ceci implique que $G_{K'}$ agit trivialement sur $V(\overline{K'})$; il en est de même pour $I_{K'}$ et $\sigma_{\mathfrak{q}}^2$, qui ont donc une image triviale par λ.

Soit $\mu_p(\overline{K'})$ et $V(\overline{K'})$ coïncident. Alors $I_{K'}$ agit trivialement sur $V(\overline{K'})$ et $\sigma_{\mathfrak{q}}^2$ agit sur $V(\overline{K'})$ comme le carré du Frobenius de k' sur $\mu_p(\overline{k'})$. Ceci implique $\lambda(\sigma_{\mathfrak{q}}^2) = (N\mathfrak{q})^2 \bmod p$.

On obtient ainsi le point (ii) de la proposition et le point (iii) (qui résulte de l'égalité $\chi_p(\sigma_{\mathfrak{q}}) = N\mathfrak{q} \bmod p$). On a également obtenu que l'image du caractère λ restreint à $I_{\mathfrak{q}}$, qui se factorise par $I_{\mathfrak{q}}/I_{K'}$, est d'ordre au plus 2.

Si cet ordre est 1, alors le caractère λ est non ramifié en $\mathfrak{q}$. L'extension $K_{\mathfrak{q}}^{\lambda}$ de $K_{\mathfrak{q}}$ qui trivialise l'action de $G_{K_{\mathfrak{q}}}$ sur $V(\overline{K_{\mathfrak{q}}})$ est donc non ramifiée. Ceci implique que E a le même type de réduction sur $K_{\mathfrak{q}}^{\lambda}$ que sur $K_{\mathfrak{q}}$, à savoir réduction additive. Or E possède un point d'ordre p (supérieur ou égal à 5) rationnel sur $K_{\mathfrak{q}}^{\lambda}$. On obtient alors une contradiction avec le lemme 1.1.3. Ceci prouve que l'image de λ restreint à $I_{\mathfrak{q}}$ est d'ordre exactement 2.

De plus, l'extension $K_{\mathfrak{q}}^{\lambda}$ s'identifie à la complétion du corps K^{λ} en sa place au-dessus $\mathfrak{q}$ induite par la place $\overline{\mathfrak{q}}$ de $\overline{K}$ choisie au début de la partie 1.1. On en déduit que E a réduction multiplicative en cette place de K^{λ}. Le raisonnement étant valable pour tout choix de $\overline{\mathfrak{q}}$ au-dessus de $\mathfrak{q}$, on obtient le même résultat pour toutes les places de K^{λ} au-dessus de $\mathfrak{q}$. Ceci prouve le point (iv). □

Proposition 1.1.5. — *Si E a mauvaise réduction additive et potentiellement bonne réduction en $\mathfrak{q}$, alors :*

(i) *l'image de $I_{\mathfrak{q}}$ par λ est cyclique d'ordre* 2, 3, 4 *ou* 6 *;*

(ii) *E a bonne réduction en toute place de K^λ au-dessus de $\mathfrak{q}$;*
(iii) *le polynôme caractéristique $P_\mathfrak{q}(X)$ de l'action de $\sigma_\mathfrak{q}$ sur le module de Tate en p de E est à coefficients dans $\mathbb{Z}$;*
(iv) *les racines de $P_\mathfrak{q}(X)$ ont même valeur absolue complexe $\sqrt{N\mathfrak{q}}$; le corps $L^\mathfrak{q}$ qu'elles engendrent est soit $\mathbb{Q}$ soit un corps quadratique imaginaire ;*
(v) *soit $\mathcal{P}^\mathfrak{q}$ un idéal maximal de $L^\mathfrak{q}$ au-dessus de p ; alors il existe une racine $\beta_\mathfrak{q}$ de $P_\mathfrak{q}(X)$ telle que la classe de $\beta_\mathfrak{q}$ modulo $\mathcal{P}^\mathfrak{q}$ soit dans $\mathbb{F}_p$ et y soit égale à $\lambda(\sigma_\mathfrak{q})$; le conjugué complexe $\overline{\beta_\mathfrak{q}}$ de $\beta_\mathfrak{q}$ est l'autre racine de $P_\mathfrak{q}(X)$; sa classe modulo $\mathcal{P}^\mathfrak{q}$ est dans $\mathbb{F}_p$ et y vaut $(\chi_p\lambda^{-1})(\sigma_\mathfrak{q})$.*

Démonstration. — En utilisant le lemme 1.1.3 et avec un raisonnement similaire à celui de la fin de la démonstration de la proposition 1.1.4, on montre que la courbe E a bonne réduction sur l'extension $K_\mathfrak{q}^\lambda$ de $K_\mathfrak{q}$ qui trivialise l'action de $G_{K_\mathfrak{q}}$ sur $V(\overline{K_\mathfrak{q}})$ (et donc en toute place de K^λ au-dessus de $\mathfrak{q}$) et que cette extension est ramifiée (donc que l'image de $I_\mathfrak{q}$ par λ n'est pas triviale dans $\mathbb{F}_p^\times$).

Le sous-groupe $\lambda(I_\mathfrak{q})$ de $\mathbb{F}_p^\times$ est un groupe cyclique ; il est isomorphe au sous-groupe d'inertie de l'extension $K_\mathfrak{q}^\lambda/K_\mathfrak{q}$ et donc également au groupe de Galois de l'extension $K_\mathfrak{q}^\lambda K_\mathfrak{q}^{nr}/K_\mathfrak{q}^{nr}$, où $K_\mathfrak{q}^{nr}$ désigne l'extension maximale non ramifiée de $K_\mathfrak{q}$. Dans le cours de cette démonstration on note $M = K_\mathfrak{q}^{nr}$ et $M^\lambda = K_\mathfrak{q}^\lambda K_\mathfrak{q}^{nr}$ l'extension de M qui trivialise l'action du groupe de Galois absolu G_M de M sur $V(\overline{M})$.

Comme E a bonne réduction sur $K_\mathfrak{q}^\lambda$, E a également bonne réduction sur M^λ. On note $\widetilde{\mathcal{E}}_{M^\lambda}$ la fibre spéciale du modèle de Néron de E sur M^λ ; $\widetilde{\mathcal{E}}_{M^\lambda}$ est une courbe elliptique sur le corps résiduel de M^λ, égal à celui de M qui est une clôture algébrique $\overline{k_\mathfrak{q}}$ de $k_\mathfrak{q}$.

D'après [**ST68**] (§2 démonstration du théorème 2), le groupe $\mathrm{Gal}(M^\lambda/M)$ agit par $\overline{k_\mathfrak{q}}$-automorphismes sur $\widetilde{\mathcal{E}}_{M^\lambda}$. On obtient ainsi un morphisme de groupes de $\mathrm{Gal}(M^\lambda/M)$ dans $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$.

Tout $\overline{k_\mathfrak{q}}$-automorphisme de $\widetilde{\mathcal{E}}_{M^\lambda}$ induit un automorphisme du groupe $\widetilde{\mathcal{E}}_{M^\lambda}(\overline{k_\mathfrak{q}})[p]$ des points de p-torsion de $\widetilde{\mathcal{E}}_{M^\lambda}$ sur $\overline{k_\mathfrak{q}}$. Comme la caractéristique q de $\overline{k_\mathfrak{q}}$ est différente de p, l'application de réduction fournit un isomorphisme de $\mathbb{F}_p$-espace vectoriel entre $\widetilde{\mathcal{E}}_{M^\lambda}(\overline{k_\mathfrak{q}})[p]$ et les points de p-torsion de E sur $\overline{K_\mathfrak{q}}$, $E(\overline{K_\mathfrak{q}})[p]$. On en déduit un morphisme de

groupes de $\mathrm{Gal}(M^\lambda/M)$ dans $\mathrm{Aut}\left(E(\overline{K_\mathfrak{q}})[p]\right)$ donné par la composition d'applications :

$$\mathrm{Gal}(M^\lambda/M) \to \mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda}) \to \mathrm{Aut}\left(\widetilde{\mathcal{E}}_{M^\lambda}(\overline{k_\mathfrak{q}})[p]\right) \to \mathrm{Aut}\left(E(\overline{K_\mathfrak{q}})[p]\right).$$

La composition de la projection canonique de $\mathrm{Gal}(\overline{M}/M)$ sur $\mathrm{Gal}(M^\lambda/M)$ avec ce morphisme coïncide avec la représentation $\varphi_{p|G_M}$ donnée par l'action de G_M sur les points de p-torsion de E. Le noyau de cette représentation correspond à l'extension de M engendrée par les coordonnées des points de p-torsion de E ; cette extension contient M^λ (engendrée par les coordonnées des points de V). Ceci prouve que la composée des trois applications ci-dessus, allant de $\mathrm{Gal}(M^\lambda/M)$ dans $\mathrm{Aut}\left(E(\overline{K_\mathfrak{q}})[p]\right)$, est injective. On obtient donc que la première application de cette composition, de $\mathrm{Gal}(M^\lambda/M)$ dans $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$, est injective. Ainsi le groupe $\lambda(I_\mathfrak{q})$ s'injecte dans $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$.

Les différentes formes possibles pour le groupe $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$ sont connues ; elles dépendent de la valeur de l'invariant j de la courbe $\widetilde{\mathcal{E}}_{M^\lambda}$ qui est égal à la classe modulo $\mathfrak{q}$ de l'invariant j de E, $j(E)$, dans $\overline{k_\mathfrak{q}}$. On rappelle qu'en tant que sous-groupe de $\mathbb{F}_p^\times$, l'image $\lambda(I_\mathfrak{q})$ est un groupe cyclique (non restreint à l'élément neutre). Les cas possibles sont alors les suivants ([**Sil92**] app. A, prop. 1.2 et exercice A.1) :

- si $j(E)$ est différent de 0 et 1728 modulo $\mathfrak{q}$, alors $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$ est cyclique d'ordre 2, donc $\lambda(I_\mathfrak{q})$ est cyclique d'ordre 2 ;
- si q est différent de 2 et 3 et $j(E)$ est congru à 1728 modulo $\mathfrak{q}$, alors $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$ est cyclique d'ordre 4, donc $\lambda(I_\mathfrak{q})$ est cyclique d'ordre 2 ou 4 ;
- si q est différent de 2 et 3 et $j(E)$ est congru à 0 modulo $\mathfrak{q}$, alors $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$ est cyclique d'ordre 6, donc $\lambda(I_\mathfrak{q})$ est cyclique d'ordre 2, 3 ou 6 ;
- si q est égal à 3 et $j(E)$ est congru à $0 = 1728$ modulo $\mathfrak{q}$, alors $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$ est d'ordre 12 ; c'est le 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 2, 3, 4 ou 6 ;

– si q est égal à 2 et $j(E)$ est congru à $0 = 1728$ modulo $\mathfrak{q}$, alors $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M^\lambda})$ est d'ordre 24 ; c'est le 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 2, 3, 4 ou 6.

Ceci prouve le point (i).

Enfin, les points (iii) à (v) découlent du théorème 3 de [**ST68**] (§2) comme dans le cas semi-stable. □

Notations 1.1.6. — Lorsque E a potentiellement bonne réduction en $\mathfrak{q}$ (y compris bonne réduction en $\mathfrak{q}$) 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. Le polynôme $P_\mathfrak{q}(X)$ est à coefficients dans $\mathbb{Z}$ et de la forme $X^2 - T_\mathfrak{q}X + N\mathfrak{q}$ où $N\mathfrak{q}$ est la norme de $\mathfrak{q}$ dans l'extension $K/\mathbb{Q}$ et $T_\mathfrak{q}$ est un entier de valeur absolue complexe inférieure à $2\sqrt{N\mathfrak{q}}$.

Le discriminant $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ est un nombre entier négatif. S'il est nul, $P_\mathfrak{q}(X)$ a une seule racine double égale à $T_\mathfrak{q}/2$, qui est un entier relatif. Si le discriminant est strictement négatif, $P_\mathfrak{q}(X)$ a deux racines distinctes, conjuguées dans $\mathbb{C}$ et de valeur absolue complexe $\sqrt{N\mathfrak{q}}$; elles engendrent un corps quadratique imaginaire. Dans les deux cas, on note $L^\mathfrak{q}$ le corps engendré par les racines de $P_\mathfrak{q}(X)$.

Remarque 1.1.7. —

(1) Lorsque la courbe E n'a pas bonne réduction en $\mathfrak{q}$, mais seulement potentiellement bonne réduction, le polynôme $P_\mathfrak{q}(X)$ (et par suite ses racines et le corps $L^\mathfrak{q}$ qu'elles engendrent) ne dépend pas que de l'idéal $\mathfrak{q}$ mais aussi du relèvement $\sigma_\mathfrak{q}$ du morphisme de Frobenius choisi au début de la partie 1.1.

(2) Le polynôme caractéristique de $\varphi_p(\sigma_\mathfrak{q})$ donnant l'action de $\sigma_\mathfrak{q}$ sur les points de p-torsion de E vaut $X^2 - (T_\mathfrak{q} \bmod p)X + (N\mathfrak{q} \bmod p)$. Comme $\varphi_p(\sigma_\mathfrak{q})$ est une matrice triangulaire supérieure, son polynôme caractéristique est scindé dans $\mathbb{F}_p$. Son discriminant est donc un carré modulo p. On en déduit que si p ne divise pas $T_\mathfrak{q}^2 - 4N\mathfrak{q}$, alors $L^\mathfrak{q}$ est un corps quadratique imaginaire dans lequel p est décomposé.

1.2. Au-dessus de p

Dans cette partie, $\mathfrak{p}$ désigne un idéal maximal de K au-dessus de p. On note $K_\mathfrak{p}$ la complétion de K en $\mathfrak{p}$ et $k_\mathfrak{p}$ son corps résiduel.

On fixe une place $\overline{\mathfrak{p}}$ de $\overline{K}$ au-dessus de $\mathfrak{p}$. Le corps résiduel de $\overline{\mathfrak{p}}$ est une clôture algébrique du corps $k_\mathfrak{p}$. On note $D_\mathfrak{p}$ le sous-groupe de décomposition de $\overline{\mathfrak{p}}$ dans $\mathrm{Gal}(\overline{K}/K)$ et $I_\mathfrak{p}$ son sous-groupe d'inertie. Le groupe $D_\mathfrak{p}$ est isomorphe au groupe de Galois absolu $G_{K_\mathfrak{p}}$ de la complétion $K_\mathfrak{p}$ et le quotient $D_\mathfrak{p}/I_\mathfrak{p}$ est canoniquement isomorphe au groupe de Galois absolu $\mathrm{Gal}(\overline{k_\mathfrak{p}}/k_\mathfrak{p})$ de $k_\mathfrak{p}$.

On cherche à déterminer la forme du caractère λ restreint au sous-groupe d'inertie $I_\mathfrak{p}$. On rappelle que le nombre premier p est choisi non ramifié dans le corps K.

1.2.1. Réduction semi-stable. —

Proposition 1.2.1. —

(i) *Si E a réduction multiplicative en $\mathfrak{p}$, alors le caractère λ restreint à $I_\mathfrak{p}$ est soit trivial soit égal au caractère cyclotomique χ_p.*

(ii) *Si E a bonne réduction en $\mathfrak{p}$, alors cette bonne réduction est ordinaire et λ restreint à $I_\mathfrak{p}$ est soit trivial soit égal à χ_p.*

Démonstration. — Si E a réduction multiplicative en $\mathfrak{p}$, alors il existe une extension K' de $K_\mathfrak{p}$, non ramifiée et de degré 2, sur laquelle la courbe E est isomorphe à une courbe de Tate. Le groupe de Galois absolu de K' est un sous-groupe $G_{K'}$ de $G_{K_\mathfrak{p}}$ d'indice 2 et son sous-groupe d'inertie $I_{K'}$ coïncide avec $I_\mathfrak{p}$.

D'après [**Ser72**] (§1.12 prop. 13), le caractère λ restreint au sous-groupe d'inertie $I_{K'}$ est trivial ou se factorise par le caractère fondamental de niveau 1 de l'inertie modérée de K'. Comme les extensions $K'/K_\mathfrak{p}$ et $K_\mathfrak{p}/\mathbb{Q}_p$ sont non ramifiées, ce caractère fondamental de niveau 1 est le caractère cyclotomique χ_p. Les sous-groupes $I_{K'}$ et $I_\mathfrak{p}$ étant égaux, on obtient le point (i) de la proposition.

Si E a bonne réduction en $\mathfrak{p}$, on utilise le paragraphe 1.11 de [**Ser72**]. On suppose d'abord par l'absurde que cette bonne réduction est supersingulière. Alors d'après *loc. cit.* (§1.11(2) prop. 12), l'image de $I_\mathfrak{p}$ par φ_p est un groupe cyclique d'ordre p^2-1. Or, par hypothèse, l'image de φ_p

est incluse dans un sous-groupe de Borel de $\mathrm{GL}_2(\mathbb{F}_p)$. Un tel sous-groupe, d'ordre $p(p-1)^2$, ne contient pas d'élément d'ordre p^2-1. On obtient donc que E a bonne réduction ordinaire en $\mathfrak{p}$.

Alors d'après *loc. cit.* (§1.11(1) corollaire à la proposition 11), le caractère λ restreint au sous-groupe d'inertie $I_\mathfrak{p}$ est trivial ou se factorise par le caractère fondamental de niveau 1 de l'inertie modérée de $K_\mathfrak{p}$. Comme l'extension $K_\mathfrak{p}/\mathbb{Q}_p$ est non ramifiée, ce caractère fondamental de niveau 1 est le caractère cyclotomique, ce qui prouve le point (ii). □

1.2.2. Réduction non semi-stable. —

Proposition 1.2.2. — *Si E a mauvaise réduction additive et potentiellement réduction multiplicative en $\mathfrak{p}$, alors λ^2 restreint à $I_\mathfrak{p}$ est soit trivial soit égal à χ_p^2. En particulier, λ^{12} restreint à $I_\mathfrak{p}$ est égal à $\chi_p^{a_\mathfrak{p}}$ avec $a_\mathfrak{p}$ égal à 0 ou 12.*

Démonstration. — D'après [**Sil92**] (app. C thm 14.1), il existe une extension K' de $K_\mathfrak{p}$, totalement ramifiée et de degré 2, sur laquelle E est isomorphe à une courbe de Tate (en particulier, E a réduction multiplicative sur K').

Le groupe de Galois absolu $G_{K'}$ de K' est un sous-groupe d'indice 2 de $G_{K_\mathfrak{p}}$; son sous-groupe d'inertie $I_{K'}$ est un sous-groupe d'indice 2 du sous-groupe $I_\mathfrak{p}$.

D'après la proposition 13 de [**Ser72**] §1.12, le caractère λ restreint au sous-groupe d'inertie $I_{K'}$ est trivial ou se factorise par $\left(\theta_{p-1}^{K'}\right)^2$, où $\theta_{p-1}^{K'}$ désigne le caractère fondamental de niveau 1 de l'inertie modérée de K' et 2 est l'indice de ramification absolu de K' (on rappelle que $K_\mathfrak{p}$ est non ramifié sur $\mathbb{Q}_p$).

Alors le caractère $\left(\theta_{p-1}^{K'}\right)^2$ est égal au caractère cyclotomique χ_p. Comme le sous-groupe $I_{K'}$ est d'indice 2 dans $I_\mathfrak{p}$, on obtient que λ^2 restreint à $I_\mathfrak{p}$ est soit trivial soit égal à χ_p^2. □

Proposition 1.2.3. — *Si E a mauvaise réduction additive et potentiellement bonne réduction en $\mathfrak{p}$, alors il existe un entier $a_\mathfrak{p}$ dans l'ensemble $\{0,4,6,8,12\}$ tel que λ^{12} restreint à $I_\mathfrak{p}$ soit égal à $\chi_p^{a_\mathfrak{p}}$.*

Démonstration. — Le caractère λ restreint au sous-groupe $I_{\mathfrak{p}}$ est continu et à valeurs dans $\mathbb{F}_p^\times$. Il se factorise donc par un caractère $\lambda_{\mathfrak{p}}^t$ du groupe d'inertie modérée $I_{\mathfrak{p}}^t$ de $K_{\mathfrak{p}}$, encore à valeurs dans $\mathbb{F}_p^\times$. D'après [**Ser72**] §1.7 prop. 5, un tel caractère $\lambda_{\mathfrak{p}}^t$ est égal à une puissance entière $\left(\theta_{p-1}^{K_{\mathfrak{p}}}\right)^{a'_{\mathfrak{p}}}$ du caractère fondamental de niveau 1, $\theta_{p-1}^{K_{\mathfrak{p}}}$, de $I_{\mathfrak{p}}^t$. Comme p est choisi non ramifié dans K, le caractère $\theta_{p-1}^{K_{\mathfrak{p}}}$ est égal au caractère cyclotomique ; ainsi λ restreint à $I_{\mathfrak{p}}$ est égal à $\chi_p^{a'_{\mathfrak{p}}}$ et λ^{12} restreint à $I_{\mathfrak{p}}$ est égal à $\chi_p^{12a'_{\mathfrak{p}}}$.

En suivant un raisonnement semblable à celui de la fin de la démonstration de la proposition 1.1.5, on montre qu'il existe une extension finie K' de $K_{\mathfrak{p}}$, d'indice de ramification e égal à 2, 3, 4 ou 6, sur laquelle E a bonne réduction.

En effet, soit K' la plus petite extension de $K_{\mathfrak{p}}$ sur laquelle les points d'ordre 5 de E sont définis. Comme p est choisi strictement plus grand que 5, le lemme 1.1.3 implique que E n'a pas réduction additive sur K'. Comme on suppose que E a potentiellement bonne réduction en $\mathfrak{p}$, alors E a bonne réduction sur K'.

On remarque que l'extension $K'/K_{\mathfrak{p}}$ est ramifiée. En effet, si elle ne l'était pas, la courbe E aurait le même type de réduction sur $K_{\mathfrak{p}}$ et sur K'. Or E a bonne réduction sur K' alors qu'on suppose qu'elle a mauvaise réduction sur $K_{\mathfrak{p}}$.

On cherche donc à déterminer le groupe d'inertie de l'extension $K'/K_{\mathfrak{p}}$. Ce groupe d'inertie est isomorphe au groupe de Galois de l'extension $K'K_{\mathfrak{p}}^{nr}/K_{\mathfrak{p}}^{nr}$, où $K_{\mathfrak{p}}^{nr}$ désigne l'extension non ramifiée maximale de $K_{\mathfrak{p}}$. Dans la suite de la démonstration, on note $M = K_{\mathfrak{p}}^{nr}$ et $M' = K'K_{\mathfrak{p}}^{nr}$.

La courbe E a encore bonne réduction sur M' ; on note $\widetilde{\mathcal{E}}_{M'}$ la courbe elliptique obtenue par réduction, définie sur le corps résiduel de M' qui est une clôture algébrique $\overline{k_{\mathfrak{p}}}$ de $k_{\mathfrak{p}}$. D'après [**ST68**] (§2 démonstration du théorème 2), le groupe $\mathrm{Gal}(M'/M)$ agit par $\overline{k_{\mathfrak{p}}}$-automorphismes sur $\widetilde{\mathcal{E}}_{M'}$. On obtient ainsi un morphisme de groupes de $\mathrm{Gal}(M'/M)$ dans $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M'})$.

Tout $\overline{k_{\mathfrak{p}}}$-automorphisme de $\widetilde{\mathcal{E}}_{M'}$ induit un automorphisme de $\mathbb{F}_5$-espace vectoriel des points de 5-torsion de $\widetilde{\mathcal{E}}_{M'}$. Comme la caractéristique de $\overline{k_{\mathfrak{p}}}$ est le nombre premier p qui est différent de 5, l'application induite par réduction est un isomorphisme de $\mathbb{F}_5$-espaces vectoriels entre les points

de 5-torsion de E sur $\overline{K_\mathfrak{p}}$, $E(\overline{K_\mathfrak{p}})[5]$, et les points de 5-torsion de $\widetilde{\mathcal{E}}_{M'}$ sur $\overline{k_\mathfrak{p}}$, $\widetilde{\mathcal{E}}_{M'}(\overline{k_\mathfrak{p}})[5]$. La composée de la suite d'applications

$$\mathrm{Gal}(M'/M) \to \mathrm{Aut}(\widetilde{\mathcal{E}}_{M'}) \to \mathrm{Aut}\left(\widetilde{\mathcal{E}}_{M'}(\overline{k_\mathfrak{p}})[5]\right) \to \mathrm{Aut}\left(E(\overline{K_\mathfrak{p}})[5]\right)$$

avec la surjection canonique du groupe de galois absolu G_M de M dans $\mathrm{Gal}(M'/M)$ coïncide avec l'action naturelle de G_M sur les points de 5-torsion de $E(\overline{K_\mathfrak{p}})$. Par définition de M', les points de 5-torsion de $E(\overline{K_\mathfrak{p}})$ sont définis sur M' ; on obtient donc que la composée de trois applications ci-dessus est injective. En particulier, la première de ces applications est injective. Ceci implique que le groupe d'inertie de $K'/K_\mathfrak{p}$, isomorphe au groupe $\mathrm{Gal}(M'/M)$, s'injecte dans le groupe des automorphismes de la courbe $\widetilde{\mathcal{E}}_{M'}$.

Les formes possibles pour ce groupe d'automorphismes ont été discutées dans la démonstration de la proposition 1.1.5 ; elles dépendent de la valeur de l'invariant j de la courbe elliptique $\widetilde{\mathcal{E}}_{M'}$, qui est l'élément de $\overline{k_\mathfrak{p}}$ défini par la classe de $j(E)$ modulo $\mathfrak{p}$. Le nombre premier p étant différent de 2 et 3, le groupe $\mathrm{Aut}(\widetilde{\mathcal{E}}_{M'})$ est cyclique, d'ordre 2 (si $j(E)$ est différent de 0 et 1728 modulo $\mathfrak{p}$), 4 (si $j(E)$ est congru à 1728 modulo $\mathfrak{p}$) ou 6 (si $j(E)$ est congru à 0 modulo $\mathfrak{p}$). Dans tous les cas, on obtient que le sous-groupe d'inertie de $K'/K_\mathfrak{p}$ est cyclique d'ordre 2, 3, 4 ou 6.

Comme E a bonne réduction sur K', le corollaire 3.4.4 de [**Ray74**] (ou [**Ser72**] §1.13) donne qu'il existe un entier $r_\mathfrak{p}$, compris entre 0 et l'indice de ramification absolu de K', tel que le caractère λ restreint au sous-groupe $I_{K'}$ se factorise par un caractère de l'inertie modérée $I^t_{K'}$ de K' égal à $\left(\theta^{K'}_{p-1}\right)^{r_\mathfrak{p}}$, $\theta^{K'}_{p-1}$ désignant le caractère fondamental de niveau 1 de $I^t_{K'}$.

On note que comme l'extension $K_\mathfrak{p}/\mathbb{Q}_p$ est non ramifiée, l'indice de ramification absolu de K' est égal à l'indice de ramification e de l'extension $K'/K_\mathfrak{p}$; il appartient donc à l'ensemble $\{2, 3, 4, 6\}$ (en particulier il divise 12).

Le sous-groupe d'inertie modérée $I^t_{K'}$ de K' peut être vu comme un sous-groupe de l'inertie modérée $I^t_\mathfrak{p}$ de $K_\mathfrak{p}$, sur lequel le caractère fondamental de niveau 1 de $K_\mathfrak{p}$, $\theta^{K_\mathfrak{p}}_{p-1}$, vaut $\left(\theta^{K'}_{p-1}\right)^e$ ([**Ser72**] §1.4). On a ainsi

sur $I^t_{K'}$:

$$\left(\theta^{K'}_{p-1}\right)^{r_\mathfrak{p}} = \left(\theta^{K_\mathfrak{p}}_{p-1}\right)^{a'_\mathfrak{p}} = \left(\theta^{K'}_{p-1}\right)^{ea'_\mathfrak{p}}.$$

Comme le caractère $\theta^{K'}_{p-1}$ est d'ordre $p-1$, on obtient la congruence

$$ea'_\mathfrak{p} \equiv r_\mathfrak{p}\ [p-1].$$

On parcourt alors toutes les valeurs possibles de e et $r_\mathfrak{p}$ (elles sont en nombre fini) ; on obtient ainsi des congruences vérifiées par $a'_\mathfrak{p}$, et la valeur de $12a'_\mathfrak{p}$ modulo $p-1$. On détaille quelques cas :

- si $r_\mathfrak{p}$ est égal à 0 alors on a $12a'_\mathfrak{p} \equiv 0\ [p-1]$;
- si $r_\mathfrak{p}$ est égal à e alors on a $12a'_\mathfrak{p} \equiv 12\ [p-1]$;
- si e est pair et $r_\mathfrak{p}$ est impair, la congruence n'a pas de solutions, $p-1$ étant pair ;
- lorsque le couple $(e, r_\mathfrak{p})$ appartient à l'ensemble $\{(3,1),(6,2)\}$ (resp. $\{(3,2),(6,4)\}$), on obtient $12a'_\mathfrak{p} \equiv 4\ [p-1]$ (resp. $12a'_\mathfrak{p} \equiv 8\ [p-1]$) ; ces deux congruences impliquent que 3 ne divise pas $p-1$; la seule congruence possible pour le nombre premier p (strictement supérieur à 5) est $p \equiv 2[3]$;
- si e est égal à 4 et $r_\mathfrak{p}$ est égal à 2, alors on a $4a'_\mathfrak{p} \equiv 2\ [p-1]$ et par suite $12a'_\mathfrak{p} \equiv 6\ [p-1]$; on obtient de plus que 4 ne divise pas $p-1$ (sinon 4 diviserait 2) ; la seule congruence possible pour le nombre premier p est donc $p \equiv 3[4]$.

Le tableau suivant résume les valeurs possibles de la classe de $12a'_\mathfrak{p}$ modulo $p-1$, ainsi que les informations supplémentaires obtenues sur p et $j(E)$, en fonction des valeurs de e et $r_\mathfrak{p}$. Les colonnes comportant des croix sont celles pour lesquelles la congruence $ea'_\mathfrak{p} \equiv r_\mathfrak{p}\ [p-1]$ n'a pas de solutions. □

e	2			3				4					6						
$r_{\mathfrak{p}}$	0	1	2	0	1	2	3	0	1	2	3	4	0	1	2	3	4	5	6
$12a'_{\mathfrak{p}} \mod (p-1)$	0	$\times$	12	0	4	8	12	0	$\times$	6	$\times$	12	0	$\times$	4	$\times$	8	$\times$	12
p	$-$	$\times$	$-$	$-$	$p \equiv 2[3]$	$p \equiv 2[3]$	$-$	$-$	$\times$	$p \equiv 3[4]$	$\times$	$-$	$-$	$\times$	$p \equiv 2[3]$	$\times$	$p \equiv 2[3]$	$\times$	$-$
$j(E)$	$-$			$j(E) \equiv 0 \mod \mathfrak{p}$				$j(E) \equiv 1728 \; mod \; \mathfrak{p}$					$j(E) \equiv 0 \mod \mathfrak{p}$						

1.3. Résumé

On note μ la puissance douzième du caractère d'isogénie λ. L'étude locale qui précède fournit les informations suivantes sur le caractère μ de G_K dans $\mathbb{F}_p^\times$ (les notations des parties précédentes restant en vigueur ; voir notamment les débuts de 1.1 et 1.2 et les notations 1.1.6) :

Théorème 1.3.1. —

(i) *Le caractère μ est non ramifié aux places finies de K hors de p.*

(ii) *Si $\mathfrak{p}$ est un idéal premier de K au-dessus de p, alors il existe un entier $a_\mathfrak{p}$ valant 0, 4, 6, 8 ou 12 tel que μ restreint à $I_\mathfrak{p}$ est égal au caractère cyclotomique à la puissance $a_\mathfrak{p}$.*

(iii) *Si $\mathfrak{q}$ est un idéal maximal de K premier à p, alors on est dans l'un des trois cas suivants :*

- **(Cas M) :** *E a potentiellement mauvaise réduction multiplicative (y compris mauvaise réduction multiplicative) en $\mathfrak{q}$ et*
  - **(M0) :** *$\mu(\sigma_\mathfrak{q}) = 1 \bmod p$ ou*
  - **(M1) :** *$\mu(\sigma_\mathfrak{q}) = (N\mathfrak{q})^{12} \bmod p$;*
- **(Cas B) :** *E a potentiellement bonne réduction (y compris bonne réduction) en $\mathfrak{q}$; si $\mathcal{P}^\mathfrak{q}$ est un idéal premier de $L^\mathfrak{q}$ au-dessus de p, alors il existe une racine $\beta_\mathfrak{q}$ de $P_\mathfrak{q}(X)$ telle que la classe de $\beta_\mathfrak{q}$ modulo $\mathcal{P}^\mathfrak{q}$ soit dans $\mathbb{F}_p$ et y soit égale à $\mu(\sigma_\mathfrak{q})$.*

CHAPITRE 2

LES TYPES DE FAMILLES $(a_\mathfrak{p})_\mathfrak{p}$ POSSIBLES

Dans cette partie, on utilise l'application de réciprocité associée dans la théorie du corps de classes globale à l'extension du corps K trivialisant le caractère μ pour obtenir des liens entre les informations obtenues lors de l'étude locale.

On détermine ensuite comment choisir p « assez grand » pour que la situation en une place finie de K hors de p impose le type de ramification du caractère μ aux places au-dessus de p. On obtient ainsi cinq formes possibles pour la famille d'entiers $(a_\mathfrak{p})_\mathfrak{p}$ (proposition 2.4.2).

2.1. Théorie du corps de classes pour le caractère μ

On note K^μ l'extension du corps K trivialisant la puissance douzième μ du caractère d'isogénie λ allant de G_K dans $\mathbb{F}_p^\times$. Il s'agit d'une extension cyclique, d'ordre divisant $p-1$, de K. 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.

La théorie du corps de classes appliquée à l'extension abélienne de corps de nombres K^μ/K fournit un morphisme de groupes r des idèles $\mathbb{A}_K^\times$ de K dans le groupe de Galois $\mathrm{Gal}(K^\mu/K)$. Ce morphisme est continu, surjectif, et de noyau $K^\times N_{K^\mu/K}\left(\mathbb{A}_{K^\mu}^\times\right)$.

Pour toute place (finie ou infinie) ν 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_ν} les unités du corps local K_ν ; dans ce cas, on

utilise indifféremment en indice la place ν et l'idéal maximal auquel elle correspond.

En utilisant la définition de l'application de réciprocité dans la théorie du corps de classes globale, on peut traduire les résultats obtenus au chapitre 1 dans l'étude locale du caractère μ en informations sur les applications $(r_\nu)_\nu$.

Si ν est une place infinie de K, l'application r_ν est triviale. En effet, le caractère λ définit également une extension cyclique de K ; on peut donc lui associer de manière analogue une application r'_ν. Alors r_ν est égale à la puissance douzième de r'_ν. Comme ν est une place infinie, l'application r'_ν a pour image un groupe d'ordre divisant 2 ; ceci implique que r_ν est triviale.

Si $\mathfrak{q}$ est un idéal maximal de K qui n'est pas au-dessus de p, alors d'après l'étude locale (théorème 1.3.1), l'extension K^μ/K est non ramifiée en $\mathfrak{q}$. Ceci implique que l'application $r_\mathfrak{q}$ est triviale sur les unités $U_{K_\mathfrak{q}}$. Le groupe de Galois $\mathrm{Gal}(K^\mu/K)$ contient un élément de Frobenius associé à $\mathfrak{q}$, uniquement déterminé. Si $\sigma_\mathfrak{q}$ est choisi dans $\mathrm{Gal}(\overline{K}/K)$ comme au début de la partie 1.1, cet élément de $\mathrm{Gal}(K^\mu/K)$ est égal à la restriction de $\sigma_\mathfrak{q}$ à K^μ ; on le note $\overline{\sigma}_\mathfrak{q}$. En particulier, on a $\overline{\mu}(\overline{\sigma}_\mathfrak{q}) = \mu(\sigma_\mathfrak{q})$. L'application $r_\mathfrak{q}$ envoie toute uniformisante de $K_\mathfrak{q}$ sur $\overline{\sigma}_\mathfrak{q}$.

Si $\mathfrak{p}$ est un idéal premier de K au-dessus de p, alors $\overline{\mu} \circ r_\mathfrak{p}$ coïncide sur les unités $U_{K_\mathfrak{p}}$ avec la composée d'applications 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

L'application de réciprocité r possède également la propriété d'être triviale sur les idèles principales (c'est-à-dire sur l'image du plongement diagonal de $K^\times$ dans $\mathbb{A}_K^\times$). Cette propriété permet de relier les applications locales r_ν entre elles.

Pour toute place ν de K, on note ι_ν l'injection canonique de K dans le complété K_ν.

Proposition 2.2.1. — *Soit α un élément de K non nul et premier à p ; on note $\alpha\mathcal{O}_K = \prod_{\mathfrak{q}\nmid p} \mathfrak{q}^{\nu_\mathfrak{q}(\alpha)}$ la décomposition de l'idéal fractionnaire*

$\alpha\mathcal{O}_K$ en produit d'idéaux maximaux de K. Alors on a :

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

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 :

- si ν est une place infinie de K, l'application r_ν est triviale, donc $\overline{\mu}\circ r_\nu(\iota_\nu(\alpha))$ également ;
- si $\mathfrak{q}$ est un idéal maximal de K premier à p, alors $\iota_{\mathfrak{q}}(\alpha)$ est un élément de $K_{\mathfrak{q}}$ de valuation $\nu_{\mathfrak{q}}(\alpha)$; son image par $r_{\mathfrak{q}}$ est $\overline{\sigma}_{\mathfrak{q}}^{\nu_{\mathfrak{q}}(\alpha)}$ et celle par $\overline{\mu}\circ r_{\mathfrak{q}}$ est $\overline{\mu}\left(\overline{\sigma}_{\mathfrak{q}}\right)^{\nu_{\mathfrak{q}}(\alpha)}$;
- si $\mathfrak{p}$ est un idéal maximal de K au-dessus de p, alors, comme α est supposé premier à p, $\iota_{\mathfrak{p}}(\alpha)$ est une unité dans $U_{K_{\mathfrak{p}}}$; 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) :

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

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. □

Dans toute la suite de cette partie, $\mathfrak{q}$ désigne un idéal maximal de K premier à p. On note h le nombre de classes d'idéaux de K. L'idéal $\mathfrak{q}^h$

est alors un idéal principal de $\mathcal{O}_K$; on considère $\gamma_\mathfrak{q}$ un élément de $\mathcal{O}_K$ qui l'engendre. On a alors comme corollaire de la proposition 2.2.1 :

Corollaire 2.2.2. — *On a :*

$$\mu\left(\sigma_\mathfrak{q}\right)^h = \overline{\mu}\left(\overline{\sigma}_\mathfrak{q}\right)^h = \prod_{\mathfrak{p}|p} N_{K_\mathfrak{p}/\mathbb{Q}_p}\left(\iota_\mathfrak{p}(\gamma_\mathfrak{q})\right)^{a_\mathfrak{p}} \mod p.$$

On a déterminé (partie 1.3) les valeurs possibles de $\mu\left(\sigma_\mathfrak{q}\right)$ en terme de classes modulo p (ou modulo un idéal d'un corps quadratique imaginaire au-dessus de p) d'entiers relatifs (ou d'un corps quadratique imaginaire). Afin de comparer ces valeurs avec le résultat du corollaire 2.2.2, on cherche à exprimer la classe modulo $p\mathbb{Z}_p$ de l'élément $\prod_{\mathfrak{p}|p} N_{K_\mathfrak{p}/\mathbb{Q}_p}\left(\iota_\mathfrak{p}(\gamma_\mathfrak{q})\right)^{a_\mathfrak{p}}$ de $\mathbb{Z}_p$ comme la classe d'un élément d'un corps global.

Notations 2.2.3. —

(1) Pour toute la suite du texte, on fixe un idéal $\mathfrak{p}_0$ de K au-dessus de p.
(2) On suppose également pour toute la suite du texte que l'extension $K/\mathbb{Q}$ est galoisienne ; on note G le groupe de Galois de K sur $\mathbb{Q}$.
(3) Pour tout élément τ de G, on définit le coefficient a_τ comme l'entier $a_\mathfrak{p}$ pour 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 coefficients $(a_\tau)_{\tau\in G}$ » $\prod_{\tau\in G} \tau(\alpha)^{a_\tau}$.

On vérifie alors que l'élément $\prod_{\mathfrak{p}|p} N_{K_\mathfrak{p}/\mathbb{Q}_p}\left(\iota_\mathfrak{p}(\gamma_\mathfrak{q})\right)^{a_\mathfrak{p}}$ 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 $\prod_{\tau\in G} \tau(\gamma_\mathfrak{q})^{a_\tau}$ de $\mathcal{O}_K$. On remarque que l'application $\mathcal{N}$ préserve $K^\times$, $\mathcal{O}_K$, et les éléments de K premiers à p.

Avec ces notations, la reformulation globale du corollaire 2.2.2 est la suivante :

Proposition 2.2.4. — *La classe modulo $\mathfrak{p}_0$ de l'élément $\mathcal{N}(\gamma_\mathfrak{q})$ de $\mathcal{O}_K$ est dans $\mathbb{F}_p^\times$ et y vaut $\mu\left(\sigma_\mathfrak{q}\right)^h$.*

Lorsque la courbe elliptique E a potentiellement bonne réduction en $\mathfrak{q}$, on introduit également les notations suivantes (voir aussi les notations 1.1.6).

Notations 2.2.5. —

(1) On fixe un idéal $\mathfrak{p}_0^{\mathfrak{q}}$ de $KL^{\mathfrak{q}}$ au-dessus de $\mathfrak{p}_0$;
(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 les propositions 1.1.2 et 1.1.5, il existe une racine du polynôme $P_{\mathfrak{q}}(X)$ dont la classe modulo $\mathcal{P}_0^{\mathfrak{q}}$ est dans $\mathbb{F}_p$ et y vaut $\lambda(\sigma_{\mathfrak{q}})$; on note $\beta_{\mathfrak{q}}$ une telle racine.

Remarque 2.2.6. — Comme le corps $L^{\mathfrak{q}}$ est soit $\mathbb{Q}$ soit un corps quadratique imaginaire, il y a au plus deux choix possibles pour $\mathfrak{p}_0^{\mathfrak{q}}$ ($\mathfrak{p}_0$ étant fixé). Si $L^{\mathfrak{q}}$ est inclus dans K, le seul choix possible pour $\mathfrak{p}_0^{\mathfrak{q}}$ est $\mathfrak{p}_0^{\mathfrak{q}} = \mathfrak{p}_0$.

Avec le théorème 1.3.1 et la proposition 2.2.4, on obtient finalement :

Proposition 2.2.7. — *On est dans l'un des trois cas suivants :*

(Cas M) : *E a potentiellement mauvaise réduction multiplicative en $\mathfrak{q}$ et on a*
  (M0) : $\mathcal{N}(\gamma_{\mathfrak{q}}) \equiv 1 \bmod \mathfrak{p}_0$ *ou*
  (M1) : $\mathcal{N}(\gamma_{\mathfrak{q}}) \equiv (N\mathfrak{q})^{12h} \bmod \mathfrak{p}_0$ *;*
(Cas B) : *E a potentiellement bonne réduction en $\mathfrak{q}$ et on a* $\mathcal{N}(\gamma_{\mathfrak{q}}) \equiv \beta_{\mathfrak{q}}^{12h} \bmod \mathfrak{p}_0^{\mathfrak{q}}$.

2.3. Borne pour la hauteur

On veut maintenant choisir le nombre premier p « assez grand » pour que les congruences de la proposition 2.2.7 deviennent des égalités. Pour cela, on cherche à contrôler toutes les valeurs absolues archimédiennes de l'élément $\mathcal{N}(\gamma_{\mathfrak{q}})$ de $\mathcal{O}_K$. Comme on a fixé un plongement de K dans $\mathbb{C}$ et supposé l'extension $K/\mathbb{Q}$ galoisienne (voir notations 2.2.3), cela revient à trouver une borne pour la valeur absolue complexe des éléments $\tau\left(\mathcal{N}(\gamma_{\mathfrak{q}})\right)$ lorsque τ décrit le groupe de Galois G de K sur $\mathbb{Q}$.

La borne obtenue dépend de la hauteur absolue du générateur $\gamma_{\mathfrak{q}}$, définie par (d désignant toujours le degré de K sur $\mathbb{Q}$) :

$$\mathrm{h}(\gamma_{\mathfrak{q}}) = \left(\prod_{\nu} \max\left(1, |\gamma_{\mathfrak{q}}|_{\nu}\right) \right)^{1/d}$$

où ν parcourt toutes les places de K et avec les normalisations suivantes pour les valuations :

– 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 I de K, on pose $|\cdot|_\nu = (NI)^{-ord_I(\cdot)}$.

On remarque que comme $\gamma_{\mathfrak{q}}$ est entier dans K, les seules places apportant une contribution non triviale dans le produit définissant sa hauteur sont les places infinies.

Le premier résultat obtenu est le suivant :

Proposition 2.3.1. — *Pour tout τ dans G, on a*

$$|\tau\left(\mathcal{N}(\gamma_{\mathfrak{q}})\right)|_{\mathbb{C}} \leq \mathrm{h}(\gamma_{\mathfrak{q}})^{12d}.$$

Démonstration. — Soit τ dans G fixé. On a :

$$\begin{aligned} \tau\left(\mathcal{N}(\gamma_{\mathfrak{q}})\right) &= \tau\left(\prod_{\tau' \in G} \tau'(\gamma_{\mathfrak{q}})^{a_{\tau'}}\right) \\ &= \prod_{\tau' \in G} \tau'(\gamma_{\mathfrak{q}})^{a_{\tau^{-1}\tau'}}, \end{aligned}$$

les coefficients $(a_{\tau^{-1}\tau'})_{\tau'}$ restant des entiers compris entre 0 et 12. Pour tout τ' dans G, on a :

$$\begin{aligned} |\tau'\left(\gamma_{\mathfrak{q}}\right)|_{\mathbb{C}}^{a_{\tau^{-1}\tau'}} &\leq \left(\max\left(1, |\tau'\left(\gamma_{\mathfrak{q}}\right)|_{\mathbb{C}}\right)\right)^{a_{\tau^{-1}\tau'}} \\ &\leq \left(\max\left(1, |\tau'\left(\gamma_{\mathfrak{q}}\right)|_{\mathbb{C}}\right)\right)^{12}. \end{aligned}$$

Comme K est galoisien sur $\mathbb{Q}$, soit toutes les places infinies de K sont réelles, soit elles sont toutes complexes.

Dans le premier cas, K a exactement d places infinies, correspondant bijectivement aux éléments de G. On a alors :

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

Dans le deuxième cas, le degré d est pair et la conjugaison complexe induit dans G un élément c d'ordre 2. Le corps K a exactement $d/2$ places infinies ; deux éléments de G définissent la même place infinie si et seulement si 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 :

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

□

On souhaite maintenant une borne qui ne dépende que de l'idéal $\mathfrak{q}$ et du corps K. On cherche donc un générateur de l'idéal $\mathfrak{q}^h$ dont la hauteur soit contrôlée par des grandeurs ne dépendant que de K et $\mathfrak{q}$.

On part pour cela d'un générateur quelconque, qu'on multiplie par une unité bien choisie de K pour obtenir le résultat voulu. On utilise ici les

résultats de [**BG96**]. Les grandeurs associées au corps K qui entrent en jeu sont les suivantes :

- R_K le régulateur de K ;
- r_K le rang du groupe des unités de K (r_K est égal à $d-1$ si K est inclus dans $\mathbb{R}$ et à $\frac{d}{2}-1$ sinon) ;
- δ_K un réel strictement positif minorant $d\ln(\mathrm{h}(\alpha))$ pour tout élément non nul α de K qui n'est pas une racine de l'unité ; si d vaut 1 ou 2, on peut prendre δ_K égal à $\frac{\ln 2}{r_K+1}$; si d est supérieur ou égal à 3, on peut prendre δ_K égal à $\frac{1}{53d\ln(6d)}$ ou $\frac{1}{1201}\left(\frac{\ln\ln d}{\ln d}\right)^3$.

Notation 2.3.2. — Avec ces données on définit :

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

On remarque que $C_1(K)$ peut s'exprimer uniquement en fonction du degré d.

Le lemme 2 (partie 3) de [**BG96**] s'écrit ici :

Lemme 2.3.3. — *Pour tout élément non nul α de $\mathcal{O}_K$, il existe une unité u de K telle qu'on ait*

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

On obtient alors le résultat suivant :

Proposition 2.3.4. — *Soit*

$$C_2(K) = \exp\left(12dC_1(K)R_K\right).$$

Le nombre réel $C_2(K)$ ne dépend que du degré et du régulateur du corps de nombres K.

Il existe un générateur $\gamma_\mathfrak{q}$ de $\mathfrak{q}^{\mathrm{h}}$ satisfaisant pour tout τ dans G :

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

Démonstration. — Étant donné un générateur quelconque de $\mathfrak{q}^h$, on peut le multiplier par une unité donnée par le lemme 2.3.3 pour obtenir un générateur $\gamma_\mathfrak{q}$ qui vérifie

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

Comme $\gamma_\mathfrak{q}$ engendre dans $\mathcal{O}_K$ l'idéal $\mathfrak{q}^h$, la norme de $\gamma_\mathfrak{q}$ dans l'extension $K/\mathbb{Q}$ est un entier relatif égal à $\pm(N\mathfrak{q})^h$. D'après la proposition 2.3.1, on a pour tout τ dans G :

$$|\tau\left(\mathcal{N}(\gamma_\mathfrak{q})\right)|_\mathbb{C} \leq \mathrm{h}(\gamma_\mathfrak{q})^{12d},$$

d'où

$$\begin{aligned} |\tau\left(\mathcal{N}(\gamma_\mathfrak{q})\right)|_\mathbb{C} &\leq \left|N_{K/\mathbb{Q}}(\gamma_\mathfrak{q})\right|^{12} \left(\exp\left(C_1(K)R_K\right)\right)^{12d} \\ &\leq (N\mathfrak{q})^{12h} \exp\left(12dC_1(K)R_K\right) = (N\mathfrak{q})^{12h} C_2(K). \end{aligned}$$

□

2.4. Les familles de coefficients $(a_\mathfrak{p})_\mathfrak{p}$ possibles

On fixe comme précédemment $\mathfrak{q}$ un idéal maximal de K premier à p. On choisit $\gamma_\mathfrak{q}$ un générateur de l'idéal principal $\mathfrak{q}^h$ qui vérifie la borne de la proposition 2.3.4.

On peut alors choisir p assez grand pour que les congruences de la proposition 2.2.7 impliquent des égalités entre éléments globaux. Avec les notations des propositions 2.2.7 et 2.3.4 on obtient :

Proposition 2.4.1. — *On pose*

$$C_3(K,\mathfrak{q}) = \left((N\mathfrak{q})^{12h} C_2(K) + (N\mathfrak{q})^{6h}\right)^{2d}.$$

Si p est strictement plus grand que $C_3(K,\mathfrak{q})$, alors on est dans l'un des trois cas suivants :

- **(Cas M) :** *E a potentiellement mauvaise réduction multiplicative en $\mathfrak{q}$ et on a*
  - **(M0) :** *$\mathcal{N}(\gamma_\mathfrak{q})$ est égal à 1 ou*
  - **(M1) :** *$\mathcal{N}(\gamma_\mathfrak{q})$ est égal à $(N\mathfrak{q})^{12h}$;*
- **(Cas B) :** *E a potentiellement bonne réduction en $\mathfrak{q}$ et $\mathcal{N}(\gamma_\mathfrak{q})$ est égal à $\beta_\mathfrak{q}^{12h}$.*

Démonstration. — On traite successivement les trois cas introduits à la partie 1.3 et traités dans la proposition 2.2.7.

Si l'idéal $\mathfrak{q}$ est de type (M0), alors l'élément $\mathcal{N}(\gamma_\mathfrak{q})$ de $\mathcal{O}_K$ est congru à 1 modulo l'idéal $\mathfrak{p}_0$ de K fixé dans les notations 2.2.3. Comme $\mathfrak{p}_0$ est au-dessus de p, ceci implique que p divise l'entier relatif $N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q})-1\right)$. Par choix de $\gamma_\mathfrak{q}$ on a pour tout τ dans G :

$$\begin{aligned} \left|\tau\left(\mathcal{N}(\gamma_\mathfrak{q})-1\right)\right|_\mathbb{C} &\leq \left|\tau\left(\mathcal{N}(\gamma_\mathfrak{q})\right)\right|_\mathbb{C} + \left|\tau\left(1\right)\right|_\mathbb{C} \\ &\leq (N\mathfrak{q})^{12h} C_2(K) + 1, \end{aligned}$$

d'où

$$\begin{aligned} \left|N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q})-1\right)\right|_\mathbb{Q} &= \left|\prod_{\tau\in G} \tau\left(\mathcal{N}(\gamma_\mathfrak{q})-1\right)\right|_\mathbb{C} \\ &= \prod_{\tau\in G} \left|\tau\left(\mathcal{N}(\gamma_\mathfrak{q})-1\right)\right|_\mathbb{C} \\ &\leq \left((N\mathfrak{q})^{12h} C_2(K)+1\right)^d \\ &\leq C_3(K,\mathfrak{q}). \end{aligned}$$

Comme p est supposé strictement plus grand que $C_3(K,\mathfrak{q})$, 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.

Si l'idéal $\mathfrak{q}$ est de type (M1), on raisonne comme dans le cas (M0) : l'élément $\mathcal{N}(\gamma_\mathfrak{q})$ de $\mathcal{O}_K$ est congru à $(N\mathfrak{q})^{12h}$ modulo l'idéal $\mathfrak{p}_0$ de K qui est au-dessus de p, donc p divise l'entier relatif $N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q})-(N\mathfrak{q})^{12h}\right)$. Or on a :

$$\begin{aligned} \left|N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q})-(N\mathfrak{q})^{12h}\right)\right|_\mathbb{Q} &= \prod_{\tau\in G} \left|\tau\left(\mathcal{N}(\gamma_\mathfrak{q})-(N\mathfrak{q})^{12h}\right)\right|_\mathbb{C} \\ &\leq \prod_{\tau\in G} \left((N\mathfrak{q})^{12h} C_2(K) + (N\mathfrak{q})^{12h}\right) \\ &\leq \left((N\mathfrak{q})^{12h} C_2(K) + (N\mathfrak{q})^{12h}\right)^d \\ &\leq C_3(K,\mathfrak{q}). \end{aligned}$$

Comme on a supposé p strictement plus grand que $C_3(K,\mathfrak{q})$, l'entier $N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q})-(N\mathfrak{q})^{12h}\right)$ est nul, ce qui implique que $\mathcal{N}(\gamma_\mathfrak{q})$ est égal à $(N\mathfrak{q})^{12h}$.

Si on est dans le cas (B) alors $\mathcal{N}(\gamma_\mathfrak{q})$ et $\beta_\mathfrak{q}^{12h}$ sont congrus modulo l'idéal $\mathfrak{p}_0^\mathfrak{q}$ de $KL^\mathfrak{q}$ (voir les notations 2.2.5 pour les définitions de $\beta_\mathfrak{q}$ et $\mathfrak{p}_0^\mathfrak{q}$). Ceci implique que p divise l'entier relatif $N_{KL^\mathfrak{q}/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q}) - \beta_\mathfrak{q}^{12h}\right)$.

On rappelle (voir aussi les notations 1.1.6) que $L^\mathfrak{q}$ est le corps engendré par la valeur propre $\beta_\mathfrak{q}$ du Frobenius $\sigma_\mathfrak{q}$; il s'agit soit de $\mathbb{Q}$ soit d'un corps quadratique imaginaire ; $\beta_\mathfrak{q}$ a pour valeur absolue complexe $\sqrt{N\mathfrak{q}}$.

Alors le corps $KL^\mathfrak{q}$ est galoisien sur $\mathbb{Q}$, de degré égal à d ou $2d$. 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 donc pour tout τ dans $\mathrm{Gal}(KL^\mathfrak{q}/\mathbb{Q})$:

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

D'où finalement :

$$\begin{aligned}
\left|N_{KL^\mathfrak{q}/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q}) - \beta_\mathfrak{q}^{12h}\right)\right|_\mathbb{Q} &= \prod_{\tau \in \mathrm{Gal}(KL^\mathfrak{q}/\mathbb{Q})} \left|\tau\left(\mathcal{N}(\gamma_\mathfrak{q}) - \beta_\mathfrak{q}^{12h}\right)\right|_\mathbb{C} \\
&\leq \left((N\mathfrak{q})^{12h} C_2(K) + (N\mathfrak{q})^{6h}\right)^{2d} \\
&\leq C_3(K, \mathfrak{q}).
\end{aligned}$$

Comme p est choisi strictement plus grand que $C_3(K, \mathfrak{q})$, l'entier $N_{K/\mathbb{Q}}\left(\mathcal{N}(\gamma_\mathfrak{q}) - \beta_\mathfrak{q}^{12h}\right)$ est nul, ce qui implique que $\mathcal{N}(\gamma_\mathfrak{q})$ est égal à $\beta_\mathfrak{q}^{12h}$. □

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

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

Les égalités obtenues dans la proposition 2.4.1 permettent de déterminer les valeurs possibles pour la famille de coefficients $(a_\mathfrak{p})_\mathfrak{p}$.

Pour le dernier résultat de cette partie, on suppose que le nombre premier q est totalement décomposé dans l'extension galoisienne $K/\mathbb{Q}$. Dans ce cas, la norme de $\mathfrak{q}$ est égale à q, les idéaux $\tau(\mathfrak{q})$ sont deux à deux distincts lorsque τ décrit G et leur produit est l'idéal $q\mathcal{O}_K$.

Proposition 2.4.2. — *On suppose q totalement décomposé dans K. Si p est strictement plus grand que $C_3(K,\mathfrak{q})$, on est dans l'un des cinq cas suivants :*

- **(Cas M) :** *E a potentiellement mauvaise réduction multiplicative en $\mathfrak{q}$ et on a*
  - **(M0) :** *tous les entiers a_τ sont nuls ou*
  - **(M1) :** *tous les entiers a_τ sont égaux à 12 ;*
- **(Cas B) :** *E a potentiellement bonne réduction en $\mathfrak{q}$ et*
  - **(B1/2) :** *tous les entiers a_τ sont égaux à 6 ; $\beta_\mathfrak{q}^{12} = q^6$; $L^\mathfrak{q} = \mathbb{Q}(\sqrt{-q})$; E a potentiellement bonne réduction supersingulière en $\mathfrak{q}$;*
  - **(B10) :** *$L^\mathfrak{q}$ est un corps quadratique imaginaire contenu dans K ; la norme de l'idéal $\mathfrak{q}$ dans l'extension $K/L^\mathfrak{q}$ est l'idéal $\beta_\mathfrak{q}\mathcal{O}_{L^\mathfrak{q}}$; l'entier a_τ vaut 12 si τ est dans $\mathrm{Gal}(K/L^\mathfrak{q})$ et 0 sinon ;*

(B01) : *$L^\mathfrak{q}$ est un corps quadratique imaginaire contenu dans K ; la norme de l'idéal $\mathfrak{q}$ dans l'extension $K/L^\mathfrak{q}$ est l'idéal $\overline{\beta_\mathfrak{q}}\mathcal{O}_{L^\mathfrak{q}}$; l'entier a_τ vaut 0 si τ est dans $\mathrm{Gal}(K/L^\mathfrak{q})$ et 12 sinon.*

Démonstration. — Comme p est supposé strictement plus grand que $C_3(K,\mathfrak{q})$, on raisonne selon les différents cas de la proposition 2.4.1.

Dans le cas (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

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

avec h non nul implique alors que tous les coefficients a_τ sont nuls.

Dans le cas (M1), $\mathcal{N}(\gamma_\mathfrak{q})$ est égal à q^{12h} et on a :

$$\begin{aligned}
\mathcal{N}(\gamma_\mathfrak{q})\mathcal{O}_K &= \left(q^{12h}\right)\mathcal{O}_K \\
\left(\prod_{\tau\in G} \tau\left(\mathfrak{q}\right)^{a_\tau}\right)^h &= \left(q\mathcal{O}_K\right)^{12h} \\
&= \left(\prod_{\tau\in G} \tau\left(\mathfrak{q}\right)\right)^{12h}
\end{aligned}$$

ce qui implique que tous les coefficients a_τ sont égaux à 12.

Dans le cas (B), $\mathcal{N}(\gamma_\mathfrak{q})$ est égal à $\beta_\mathfrak{q}^{12h}$ (dans le corps $KL^\mathfrak{q}$). En particulier, $\mathcal{N}(\gamma_\mathfrak{q})$ 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.

Si $\mathcal{N}(\gamma_\mathfrak{q})$ est rationnel, alors $\beta_\mathfrak{q}^{12h}$ l'est également, donc $\beta_\mathfrak{q}^{12h}$ est égal à $\overline{\beta_\mathfrak{q}}^{12h}$. Ceci implique qu'il existe une racine $12h$-ième de l'unité 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 même un entier relatif. La relation

$$q = \overline{\beta_\mathfrak{q}}\beta_\mathfrak{q} = \zeta\beta_\mathfrak{q}^2$$

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 1.1.6) est alors un entier relatif de valeur absolue inférieure à $2\sqrt{2}$; elle 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.

Lorsque q est impair, le fait qu'il soit ramifié dans $L^\mathfrak{q}$ implique qu'il divise $T_\mathfrak{q}^2 - 4N\mathfrak{q}$. Comme $N\mathfrak{q}$ est égal à q, on en déduit que q divise $T_\mathfrak{q}$. Alors $T_\mathfrak{q}^2$ est un carré, multiple de q (nombre premier impair), 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 2 et 3, alors $T_\mathfrak{q}$ est nul ;

– si q est égal à 2 ou 3, alors $T_\mathfrak{q}^2$ est soit nul, soit égal à q^2.

Dans les deux cas, q divise $T_\mathfrak{q}$, donc la courbe elliptique sur $\mathbb{F}_q$ obtenue par réduction de E en $\mathfrak{q}$ (si besoin après une extension pour obtenir la bonne réduction) est supersingulière.

On montre maintenant que l'entier relatif $\beta_\mathfrak{q}^{12}$ est égal à $\pm q^6$.

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 $\beta_\mathfrak{q}^{12}$ égal à q^6. Dans ce cas 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 tel qu'on ait

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

On a alors $L^\mathfrak{q}$ égal à $\mathbb{Q}(\sqrt{-3})$ et on vérifie par le calcul que $\beta_\mathfrak{q}^6$ est égal à -3^3, donc $\beta_\mathfrak{q}^{12}$ est égal à 3^6.

Si q est égal à 2 et $T_\mathfrak{q}^2$ est égal à 4, alors $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ vaut -4 et il existe $\varepsilon_\mathfrak{q}$ valant $+1$ ou -1 tel qu'on ait

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

Ceci implique que $L^\mathfrak{q}$ est $\mathbb{Q}(i)$ et on vérifie par le calcul que $\beta_\mathfrak{q}^4 = -2^2$ donc $\beta_\mathfrak{q}^{12} = -2^6$.

On en déduit qu'on a dans $\mathcal{O}_K$, et pour toutes les valeurs de q :

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

Ceci qui implique que tous les coefficients a_τ sont égaux à 6.

On peut alors montrer que le cas où $q = 2$, $T_\mathfrak{q}^2 = 4$ et $L^\mathfrak{q} = \mathbb{Q}(i)$ ne se produit pas. En effet, on sait (remarque 1.1.7 (2)) que soit p divise $T_\mathfrak{q}^2 - 4N\mathfrak{q}$, soit $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ est un carré dans $\mathbb{F}_p^\times$. Dans le cas considéré on a $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ égal à -4. Comme p est choisi strictement plus grand que 5, ceci implique que -4 et par suite -1 est un carré dans $\mathbb{F}_p^\times$. On en déduit que p est congru à 1 modulo 4. Or, d'après le tableau dans la démonstration de la proposition 1.2.3, les coefficients a_τ ne peuvent valoir 6 que si p est congru à 3 modulo 4. On obtient donc une contradiction.

On vérifie que dans tous les autres cas traités on a bien $\beta_\mathfrak{q}^{12} = q^6$ et $L^\mathfrak{q} = \mathbb{Q}(\sqrt{-q})$.

Enfin, si $\mathcal{N}(\gamma_\mathfrak{q}) = \beta_\mathfrak{q}^{12h}$ engendre $L^\mathfrak{q}$ qui est un corps quadratique imaginaire, alors $L^\mathfrak{q}$ est inclus dans K (car $\mathcal{N}(\gamma_\mathfrak{q})$ est un élément de K). Le degré d de K sur $\mathbb{Q}$ est pair et le groupe $G = \mathrm{Gal}(K/\mathbb{Q})$ contient comme sous-groupe d'indice 2 le groupe $H^\mathfrak{q} = \mathrm{Gal}(K/L^\mathfrak{q})$.

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

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

d'où

$$\begin{aligned}
\mathcal{N}(\gamma_\mathfrak{q})\mathcal{O}_K &= \rho\left(\mathcal{N}(\gamma_\mathfrak{q})\right)\mathcal{O}_K = \rho\left(\mathcal{N}(\gamma_\mathfrak{q})\mathcal{O}_K\right) \\
\left(\prod_{\tau\in G}\tau(\mathfrak{q})^{a_\tau}\right)^h &= \rho\left(\left(\prod_{\tau\in G}\tau(\mathfrak{q})^{a_\tau}\right)^h\right) \\
&= \left(\prod_{\tau\in G}\left(\rho\circ\tau\right)(\mathfrak{q})^{a_\tau}\right)^h \\
&= \left(\prod_{\tau\in G}\tau(\mathfrak{q})^{a_{\rho^{-1}\tau}}\right)^h
\end{aligned}$$

On obtient donc pour tout ρ dans $H^\mathfrak{q}$ et tout τ dans G l'égalité $a_{\rho\tau} = a_\tau$. Ainsi les coefficients $(a_\tau)_\tau$ sont constants sur les classes à gauche modulo $H^\mathfrak{q}$.

Le groupe G possède deux classes à gauche 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 qui induit la conjugaison complexe sur $L^\mathfrak{q}$. On note que comme $H^\mathfrak{q}$ est d'indice 2 dans G, on a $H^\mathfrak{q}\gamma = \gamma H^\mathfrak{q}$. On a alors

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

où $\overline{N_{K/L^\mathfrak{q}}(\gamma_\mathfrak{q})}$ désigne le conjugué complexe de l'élément $N_{K/L^\mathfrak{q}}(\gamma_\mathfrak{q})$ de $L^\mathfrak{q}$. Comme $N_{K/L^\mathfrak{q}}(\gamma_\mathfrak{q})$ engendre dans $\mathcal{O}_{L^\mathfrak{q}}$ l'idéal

$$\begin{aligned} N_{K/L^\mathfrak{q}}(\gamma_\mathfrak{q})\mathcal{O}_{L^\mathfrak{q}} &= N_{K/L^\mathfrak{q}}\left(\gamma_\mathfrak{q}\mathcal{O}_K\right) \\ &= N_{K/L^\mathfrak{q}}\left(\mathfrak{q}^h\right) \\ &= N_{K/L^\mathfrak{q}}\left(\mathfrak{q}\right)^h, \end{aligned}$$

alors $\overline{N_{K/L^\mathfrak{q}}(\gamma_\mathfrak{q})}$ engendre l'idéal $\overline{N_{K/L^\mathfrak{q}}\left(\mathfrak{q}\right)}^h$ et on obtient :

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

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 $\overline{\beta_\mathfrak{q}}\mathcal{O}_{L^\mathfrak{q}}$.

Si $N_{K/L^\mathfrak{q}}(\mathfrak{q})$ est égal à $\beta_\mathfrak{q}\mathcal{O}_{L^\mathfrak{q}}$ (cas (B10)), alors la relation

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

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 $\overline{\beta_\mathfrak{q}}\mathcal{O}_{L^\mathfrak{q}}$ (cas (B01)), alors la relation

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

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.

□

CHAPITRE 3

FORME DU CARACTÈRE D'ISOGÉNIE - HOMOTHÉTIES

3.1. Une version effective du théorème de Chebotarev

On utilise ici une forme effective du théorème de Chebotarev démontrée par Lagarias, Montgomery et Odlyzko dans [**LMO79**] (voir aussi [**Ser81**]).

Théorème 3.1.1 **(Lagarias, Montgomery, Odlyzko)**
Il existe une constante absolue et effectivement calculable A ayant la propriété suivante.

Soit 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 le symbole d'Artin 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 plus petit que $2(\Delta_N)^A$.

Ce résultat permet d'obtenir un système de représentants des classes d'idéaux de K formé d'idéaux dont la norme dans l'extension $K/\mathbb{Q}$ est un nombre premier rationnel totalement décomposé dans K et inférieur à une borne ne dépendant que du corps de base K. On rappelle que h désigne le nombre de classes d'idéaux de K et Δ_K son discriminant.

Proposition 3.1.2. — *Soit $\mathcal{J}$ 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 $2(\Delta_K)^{Ah}$. Alors toute classe d'idéaux de K contient un idéal de $\mathcal{J}$.

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 $\mathcal{J}$ 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 Δ_K^h 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 3.1.1, il existe un nombre premier rationnel q, non ramifié dans H_K et inférieur ou égal à $2(\Delta_{H_K})^A = 2(\Delta_K)^{Ah}$, tel que la classe de conjugaison formée par ses Frobenius 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 $2(\Delta_K)^{Ah}$ 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 que la norme de $\mathfrak{q}$ 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 $\mathcal{J}$.

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

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

□

On définit

$$C'_K = \left[\left(2(\Delta_K)^{Ah}\right)^{12h} C_2(K) + \left(2(\Delta_K)^{Ah}\right)^{6h}\right]^{2d}.$$

Le nombre C'_K ne dépend que du corps de nombres K ; d'après la définition (notation 2.3.2 et proposition 2.3.4) des constantes $C_1(K)$ et $C_2(K)$, C'_K dépend du degré de K, de son discriminant, de son nombre de classes, et de son régulateur.

On remarque que le nombre C'_K est toujours strictement supérieur à 5 et au discriminant Δ_K ; ainsi, l'hypothèse faite au début de la partie 1 que p est strictement plus grand que 5 et non ramifié dans K est vérifiée dès que p est supposé supérieur ou égal à C'_K.

Si p est strictement supérieur à C'_K, alors tout idéal maximal $\mathfrak{q}$ dans $\mathcal{J}$ est de caractéristique différente de p, et vérifie que le nombre $C_3(K, \mathfrak{q})$ (proposition 2.4.1) est inférieur ou égal à C'_K ; on peut donc appliquer la proposition 2.4.2. On a précisément :

Proposition 3.1.3. — *Si p est strictement supérieur à C'_K alors tous les idéaux de $\mathcal{J}$ appartiennent au même cas de la proposition 2.4.2.*

Démonstration. — On rappelle que les entiers $(a_\tau)_\tau$ sont définis (notations 2.2.3) par $a_\tau = a_{\tau^{-1}\mathfrak{p}_0}$, pour un idéal premier $\mathfrak{p}_0$ de K au-dessus de p fixé, et les entiers $(a_\mathfrak{p})_\mathfrak{p}$ par $\mu_{|I_\mathfrak{p}} = \chi_p^{a_\mathfrak{p}}$ (partie 1.3), pour tout idéal premier $\mathfrak{p}$ de K au-dessus de p. En particulier, la famille $(a_\tau)_\tau$ ne dépend que des propriétés de la courbe E aux places de K au-dessus de p.

Soient $\mathfrak{q}$ et $\mathfrak{q}'$ deux idéaux dans $\mathcal{J}$. Comme p est choisi strictement supérieur à C'_K, p est aussi strictement supérieur à $C_3(K, \mathfrak{q})$ et $C_3(K, \mathfrak{q}')$; ceci implique que les cas de la proposition 2.4.2 auxquels appartiennent $\mathfrak{q}$ et $\mathfrak{q}'$ déterminent la famille de coefficients $(a_\tau)_\tau$.

Or, deux cas différents de la proposition 2.4.2 donnent deux familles $(a_\tau)_\tau$ différentes (on distingue les cas (B10) et (B01) par le fait que dans le cas (B10), l'ensemble des τ pour lesquels a_τ est égal à 12 est un sous-groupe de G alors que dans le cas (B01), c'est le complémentaire d'un sous-groupe).

Ceci prouve que $\mathfrak{q}$ et $\mathfrak{q}'$ appartiennent au même cas dans la proposition 2.4.2. □

3.2. Deux formes pour le caractère d'isogénie

Le corps K^μ trivialisant l'action du caractère μ est une extension cyclique du corps de base K, non ramifiée hors de p. Le théorème de Chebotarev pour cette extension fournit que tout élément du groupe de Galois $\mathrm{Gal}(K^\mu/K)$ est de la forme $\overline{\sigma}_\mathfrak{q}$ (voir partie 2.1) pour un idéal maximal $\mathfrak{q}$ de K premier à p. Pour déterminer le caractère $\overline{\mu}$, et par suite le caractère μ, il suffit donc de déterminer la forme de $\overline{\mu}(\overline{\sigma}_\mathfrak{q}) = \mu(\sigma_\mathfrak{q})$ pour ces idéaux.

La proposition 2.2.1 relie la valeur de $\mu(\sigma_\mathfrak{q})$ pour un idéal maximal de $\mathfrak{q}$ de K premier à p aux entiers $(a_\mathfrak{p})_\mathfrak{p}$ et aux valeurs de $\mu(\sigma_{\mathfrak{q}'})$ pour une famille d'idéaux maximaux $\mathfrak{q}'$ premiers à p engendrant le groupe des classes de K.

À l'aide de la proposition 2.4.2 et de la partie 3.1, on montre que la puissance douzième μ du caractère d'isogénie ne peut prendre que deux formes.

Théorème 3.2.1. — *On suppose que p est strictement supérieur à $\max(65(3^{12d}-1)(24d)^6, C'_K)$. Alors on est dans l'un des deux cas suivants.*

Type (0) : *Le caractère μ est égal à χ_p^6 et p est congru à 3 modulo 4.*

Type (MC) : *Il existe un corps quadratique imaginaire L vérifiant*

- *L est contenu dans K ;*
- *p est totalement décomposé dans L ;*
- *le corps de classes de Hilbert de L est contenu dans K (en particulier, la norme dans l'extension K/L d'un idéal de K est un idéal principal de L) ;*
- *il existe un idéal $\mathfrak{p}_L$ de L au-dessus de p vérifiant : le caractère μ est non ramifié hors de $\mathfrak{p}_L$; pour tout idéal $\mathfrak{q}$ de K premier à $\mathfrak{p}_L$ et tout élément $\alpha_\mathfrak{q}$ de $\mathcal{O}_L$ générateur de $N_{K/L}(\mathfrak{q})$, $\mu(\sigma_\mathfrak{q})$ est égal à $\alpha_\mathfrak{q}^{12} \bmod \mathfrak{p}_L$.*

Une forme de ce théorème figure déjà dans l'article [**Mom95**] de Momose, avec un cas supplémentaire. Ce cas supplémentaire correspond aux cas (M0) et (M1) de la proposition 2.4.2 et à un caractère μ respectivement trivial ou égal à χ_p^{12}. On utilise les bornes uniformes sur la torsion des courbes elliptiques (Merel ([**Mer96**]) ou Parent ([**Par99**]) pour montrer que ces cas ne se produisent pas pour p « assez grand ».

Le type (0) du théorème 3.2.1 correspond au cas (B1/2) de la proposition 2.4.2. Le type (MC) réunit les cas (B10) et (B01).

Dans les sous-parties suivantes, on démontre le théorème 3.2.1 en traitant successivement les cas apparaissant dans la proposition 2.4.2.

3.2.1. Élimination des cas (M0) et (M1). —

Proposition 3.2.2. — *Si tous les idéaux de $\mathcal{J}$ sont de type (M0), alors le caractère μ est trivial ; si tous les idéaux de $\mathcal{J}$ sont de type (M1), alors le caractère μ est égal à χ_p^{12}.*

Démonstration. — Si tous les idéaux de $\mathcal{J}$ sont de type (M0), alors d'après la partie 1.3, $\mu(\sigma_{\mathfrak{q}})$ vaut 1 mod p pour tout $\mathfrak{q}$ dans $\mathcal{J}$; d'après la proposition 2.4.2, tous les coefficients $a_{\mathfrak{p}}$ sont nuls.

Soit $\mathfrak{q}'$ un idéal maximal de K premier à p. D'après la proposition 3.1.2, il existe un idéal maximal $\mathfrak{q}$ dans $\mathcal{J}$ et un élément α non nul de K vérifiant

$$\mathfrak{q}'\mathfrak{q}^{-1} = \alpha\mathcal{O}_K.$$

Alors d'après la proposition 2.2.1 on a :

$$\mu\left(\sigma_{\mathfrak{q}'}\right)\mu\left(\sigma_{\mathfrak{q}}\right)^{-1} = \prod_{\mathfrak{p}|p} N_{K_{\mathfrak{p}}/\mathbb{Q}_p}\left(\iota_{\mathfrak{p}}(\alpha)\right)^{a_{\mathfrak{p}}} \mod p.$$

Comme tous les coefficients $a_{\mathfrak{p}}$ sont nuls et que $\mu(\sigma_{\mathfrak{q}})$ vaut 1 mod p, on obtient

$$\mu\left(\sigma_{\mathfrak{q}'}\right) = 1 \mod p.$$

Ceci étant vrai pour tout idéal maximal $\mathfrak{q}'$ de K premier à p, on en déduit que le caractère μ est trivial.

Si tous les idéaux de $\mathcal{J}$ sont de type (M1), alors d'après la partie 1.3, $\mu(\sigma_{\mathfrak{q}})$ vaut $(N\mathfrak{q})^{12}$ mod p pour tout $\mathfrak{q}$ dans $\mathcal{J}$; d'après la proposition 2.4.2, tous les coefficients $a_{\mathfrak{p}}$ sont égaux à 12.

Soit $\mathfrak{q}'$ un idéal maximal de K premier à p. D'après 3.1.2, il existe un idéal maximal $\mathfrak{q}$ dans $\mathcal{J}$ et un élément α de $K^\times$ vérifiant

$$\mathfrak{q}'\mathfrak{q}^{-1} = \alpha\mathcal{O}_K.$$

Alors d'après la proposition 2.2.1 on a :

$$\mu\left(\sigma_{\mathfrak{q}'}\right)\mu\left(\sigma_{\mathfrak{q}}\right)^{-1} = \prod_{\mathfrak{p}|p} N_{K_{\mathfrak{p}}/\mathbb{Q}_p}\left(\iota_{\mathfrak{p}}(\alpha)\right)^{a_{\mathfrak{p}}} \mod p.$$

Comme tous les coefficients $a_{\mathfrak{p}}$ sont égaux à 12 le membre de droite vaut :

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

Or, $N_{K/\mathbb{Q}}(\alpha)$ est un nombre rationnel égal à $N\mathfrak{q}'/N\mathfrak{q}$ ou à $-N\mathfrak{q}'/N\mathfrak{q}$. On en déduit :

$$\mu\left(\sigma_{\mathfrak{q}'}\right) = (N\mathfrak{q}')^{12} \mod p = \chi_p(\sigma_{\mathfrak{q}'})^{12}.$$

Ceci étant vrai pour tout idéal maximal $\mathfrak{q}'$ de K premier à p, on obtient que μ est égal à χ_p^{12}. □

Si la puissance douzième μ du caractère d'isogénie λ est triviale, alors l'extension cyclique K^{λ}/K trivialisant le caractère λ est de degré inférieur ou égal à 12. Comme λ donne l'action de G_K sur le sous-groupe V d'ordre p de la courbe elliptique E, on obtient que E possède un point d'ordre p défini sur K^{λ}.

Si μ est égal à χ_p^{12}, alors le caractère $\chi_p\lambda^{-1}$ élevé à la puissance 12 est trivial. Or, ce caractère de G_K est le caractère d'isogénie associé au sous-groupe $E[p]/V$ rationnel sur K de la courbe E/V qui est isogène à E. On en déduit que cette courbe possède un point d'ordre p défini sur une extension de K de degré inférieur ou égal à 12.

On peut éliminer ces deux cas en utilisant les bornes sur l'ordre des points de torsion des courbes elliptiques en fonction du degré du corps de nombres sur lequel ils sont définis.

Théorème (Merel). — *On suppose qu'il existe une courbe elliptique définie sur un corps de nombres de degré δ strictement plus grand que 1 qui possède un point d'ordre p défini sur ce même corps. Alors p est strictement inférieur à $\delta^{3\delta^2}$.*

Théorème (Parent). — *On suppose qu'il existe une courbe elliptique définie sur un corps de nombres de degré δ qui possède un point d'ordre p défini sur ce même corps. Alors p est inférieur ou égal à $65(3^{\delta}-1)(2\delta)^6$.*

Corollaire 3.2.3. — *On suppose que p est strictement supérieur à $\max(65(3^{12d}-1)(24d)^6, C'_K)$. Alors les idéaux de $\mathcal{J}$ sont tous de type (B1/2), (B10) ou (B01).*

3.2.2. Cas (B1/2). —

Proposition 3.2.4. — *Si tous les idéaux de $\mathcal{J}$ sont de type (B1/2), alors le caractère μ est égal à χ_p^6 et p est congru à 3 modulo 4.*

Démonstration. — Si tous les idéaux de $\mathcal{J}$ sont de type (B1/2), alors d'après la proposition 2.4.2 tous les coefficients $a_\mathfrak{p}$ sont égaux à 6 et la courbe E a potentiellement bonne réduction en tout idéal de $\mathcal{J}$. De plus, le tableau de la proposition 1.2.3 indique que les entiers $a_\mathfrak{p}$ ne peuvent prendre la valeur 6 que lorsque p est congru à 3 modulo 4.

Soit $\mathfrak{q}$ un idéal dans $\mathcal{J}$. Alors il existe une valeur propre $\beta_\mathfrak{q}$ du Frobenius $\sigma_\mathfrak{q}$ et un idéal $\mathcal{P}_0^\mathfrak{q}$ de $L^\mathfrak{q}$ au-dessus de p tels qu'on ait (voir notations 2.2.5) :

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

D'après 2.4.2, $\beta_\mathfrak{q}^{12}$ est égal à q^6, d'où l'égalité :

$$\mu(\sigma_\mathfrak{q}) = q^6 \mod p = (N\mathfrak{q})^6 \mod p = \chi_p(\sigma_\mathfrak{q})^6.$$

Soit $\mathfrak{q}'$ un idéal maximal de K premier à p. D'après 3.1.2, il existe un idéal maximal $\mathfrak{q}$ dans $\mathcal{J}$ et un élément α non nul de K vérifiant

$$\mathfrak{q}'\mathfrak{q}^{-1} = \alpha\mathcal{O}_K.$$

Alors d'après la proposition 2.2.1 on a :

$$\mu(\sigma_{\mathfrak{q}'})\,\mu(\sigma_\mathfrak{q})^{-1} = \prod_{\mathfrak{p}|p} N_{K_\mathfrak{p}/\mathbb{Q}_p}(\iota_\mathfrak{p}(\alpha))^{a_\mathfrak{p}} \mod p.$$

Comme tous les coefficients $a_\mathfrak{p}$ sont égaux à 6 le membre de droite vaut :

$$\begin{aligned}\prod_{\mathfrak{p}|p} N_{K_\mathfrak{p}/\mathbb{Q}_p}(\iota_\mathfrak{p}(\alpha))^6 \mod p &= \left(\prod_{\mathfrak{p}|p} N_{K_\mathfrak{p}/\mathbb{Q}_p}(\iota_\mathfrak{p}(\alpha))\right)^6 \mod p \\ &= \left(N_{K/\mathbb{Q}}(\alpha)\right)^6 \mod p.\end{aligned}$$

Le nombre rationnel $N_{K/\mathbb{Q}}(\alpha)$ étant égal à $N\mathfrak{q}'/N\mathfrak{q}$ ou à $-N\mathfrak{q}'/N\mathfrak{q}$, on obtient :

$$\mu(\sigma_{\mathfrak{q}'}) = (N\mathfrak{q}')^6 \mod p = \chi_p(\sigma_{\mathfrak{q}'})^6.$$

Ceci étant vrai pour tout idéal maximal $\mathfrak{q}'$ de K premier à p, on en déduit que μ est égal à χ_p^6. □

3.2.3. Cas (B10) et (B01). —

Proposition 3.2.5. — *On suppose que tous les idéaux de $\mathcal{J}$ sont de type (B10) ou (B01). Alors il existe un unique corps quadratique imaginaire L inclus dans K vérifiant : pour tout idéal $\mathfrak{q}$ dans $\mathcal{J}$, $L^{\mathfrak{q}}$ est égal à L.*

Démonstration. — Si tous les idéaux de $\mathcal{J}$ sont de type (B10), alors d'après la proposition 2.4.2, l'ensemble des éléments τ de G tels que a_τ est égal à 12 est un sous-groupe d'indice 2 de G. Pour tout idéal $\mathfrak{q}$ de $\mathcal{J}$, c'est le sous-groupe $\mathrm{Gal}(K/L^{\mathfrak{q}})$, $L^{\mathfrak{q}}$ étant un corps quadratique imaginaire inclus dans K. 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 $\mathcal{J}$. Ce corps quadratique commun fournit le corps L de la proposition.

Si tous les idéaux de $\mathcal{J}$ sont de type (B01), alors d'après la proposition 2.4.2, l'ensemble des éléments τ de G tels que a_τ est égal à 0 est un sous-groupe d'indice 2 de G. Pour tout idéal $\mathfrak{q}$ de $\mathcal{J}$, c'est le sous-groupe $\mathrm{Gal}(K/L^{\mathfrak{q}})$, $L^{\mathfrak{q}}$ étant un corps quadratique imaginaire inclus dans K. 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 $\mathcal{J}$. Ce corps quadratique commun fournit le corps L de la proposition. □

Notation 3.2.6. — On note H le groupe de Galois $\mathrm{Gal}(K/L)$. Si tous les idéaux de $\mathcal{J}$ sont de type (B10), le coefficient a_τ vaut 12 si τ est dans H et 0 sinon ; si tous les idéaux de $\mathcal{J}$ sont de type (B01), le coefficient a_τ vaut 0 si τ est dans H et 12 sinon.

Remarque 3.2.7. — Soit $\mathfrak{q}$ un idéal dans $\mathcal{J}$. Comme le corps $L^{\mathfrak{q}}$, égal à L, est inclus dans K, il n'y a qu'un seul choix possible pour l'idéal $\mathfrak{p}_0^{\mathfrak{q}}$, qui est égal à $\mathfrak{p}_0$ (voir notations 2.2.3 et 2.2.5 et remarque 2.2.6). L'idéal $\mathcal{P}_0^{\mathfrak{q}}$ est donc l'idéal de L situé au-dessous de $\mathfrak{p}_0$. En particulier, les idéaux $\mathcal{P}_0^{\mathfrak{q}}$ coïncident lorsque $\mathfrak{q}$ varie dans $\mathcal{J}$.

Lemme 3.2.8. — *La norme de tout idéal fractionnaire de K dans l'extension K/L est un idéal fractionnaire principal de L ; le corps de classes de Hilbert de L est contenu dans K.*

Démonstration. — La première assertion est vraie si et seulement si elle l'est pour les idéaux maximaux de $\mathcal{O}_K$.

Soit $\mathfrak{q}$ un idéal dans $\mathcal{J}$. Si tous les idéaux de $\mathcal{J}$ sont de type (B10), alors d'après la proposition 2.4.2, la norme dans l'extension $K/L^{\mathfrak{q}}$ de $\mathfrak{q}$ est l'idéal $\beta_{\mathfrak{q}}\mathcal{O}_{L^{\mathfrak{q}}}$. Comme le corps $L^{\mathfrak{q}}$ est égal au corps L on obtient

$$N_{K/L}(\mathfrak{q}) = \beta_{\mathfrak{q}}\mathcal{O}_L.$$

Si tous les idéaux de $\mathcal{J}$ sont de type (B01) alors d'après la proposition 2.4.2, la norme dans l'extension $K/L^{\mathfrak{q}}$ de $\mathfrak{q}$ est l'idéal $\overline{\beta_{\mathfrak{q}}}\mathcal{O}_{L^{\mathfrak{q}}}$. Comme le corps $L^{\mathfrak{q}}$ est égal au corps L on obtient

$$N_{K/L}(\mathfrak{q}) = \overline{\beta_{\mathfrak{q}}}\mathcal{O}_L.$$

Soit $\mathfrak{q}'$ un idéal maximal quelconque de $\mathcal{O}_K$ ($\mathfrak{q}'$ pouvant également être au-dessus de p). Alors d'après la proposition 3.1.2, il existe un idéal $\mathfrak{q}$ dans $\mathcal{J}$ et un élément α non nul dans K tels qu'on ait :

$$\mathfrak{q}' = \mathfrak{q} \times (\alpha\mathcal{O}_K)\,.$$

On obtient alors dans le groupe des idéaux fractionnaires de L :

$$\begin{aligned} N_{K/L}(\mathfrak{q}') &= N_{K/L}(\mathfrak{q}) \times N_{K/L}\,(\alpha\mathcal{O}_K) \\ &= N_{K/L}(\mathfrak{q}) \times N_{K/L}\,(\alpha)\,\mathcal{O}_K. \end{aligned}$$

La norme $N_{K/L}(\mathfrak{q})$ étant un idéal principal de $\mathcal{O}_L$, on obtient la première assertion de la proposition.

Soit H_L le corps de classes de Hilbert de L. L'extension KH_L/K est abélienne et la théorie du corps de classes fournit le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathrm{Gal}(KH_L/K) & \xrightarrow{\sim} & \mathbb{A}_K^\times/K^\times N_{KH_L/K}\left(\mathbb{A}_{KH_L}^\times\right) \\ {\scriptstyle res}\big\downarrow & & \big\downarrow{\scriptstyle N_{K/L}} \\ \mathrm{Gal}(H_L/L) & \xrightarrow{\sim} & \mathbb{A}_L^\times/L^\times N_{H_L/L}\left(\mathbb{A}_{H_L}^\times\right). \end{array}$$

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. □

Lemme 3.2.9. — *Le nombre premier p est décomposé dans L. Il existe un idéal premier $\mathfrak{p}_L$ de L au-dessus de p tel qu'on ait : $a_\mathfrak{p}$ vaut 12 si $\mathfrak{p}$ est au-dessus de $\mathfrak{p}_L$ et 0 sinon.*

Démonstration. — Soit $\mathfrak{q}$ un idéal dans $\mathcal{J}$ fixé. Alors la courbe E a potentiellement bonne réduction en $\mathfrak{q}$ et le corps quadratique imaginaire $L^\mathfrak{q}$ engendré par les valeurs propres du Frobenius associé à $\mathfrak{q}$ est L.

D'après la remarque 1.1.7(2), soit p divise $T_\mathfrak{q}^2 - 4N\mathfrak{q}$, soit p est décomposé dans $L^\mathfrak{q}$. Comme p est choisi en particulier strictement plus grand que la valeur absolue de l'entier $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ (qui est inférieure à $4N\mathfrak{q}$), si p divise ce nombre entier, alors il est nul. Or, si $T_\mathfrak{q}^2 - 4N\mathfrak{q}$ est nul, le corps $L^\mathfrak{q}$ est $\mathbb{Q}$, ce qui induit une contradiction. On en déduit que p est décomposé dans le corps quadratique L égal à $L^\mathfrak{q}$.

On rappelle que les entiers a_τ ont été définis (notations 2.2.3) par : $a_\tau = a_{\tau^{-1}\mathfrak{p}_0}$ pour l'idéal $\mathfrak{p}_0$ de K au-dessus de p fixé.

Si tous les idéaux de $\mathcal{J}$ sont de type (B10), on note $\mathfrak{p}_L$ l'idéal de L situé au-dessous de $\mathfrak{p}_0$ (c'est donc l'idéal $\mathcal{P}_0^\mathfrak{q}$ pour tout idéal $\mathfrak{q}$ dans $\mathcal{J}$). Soit $\mathfrak{p}$ un idéal maximal de K au-dessus de $\mathfrak{p}_L$. Il existe un élément τ dans H tel qu'on ait $\tau^{-1}\mathfrak{p}_0 = \mathfrak{p}$. L'entier $a_\mathfrak{p}$ est donc égal à a_τ, lui-même égal à 12 car τ est dans H.

Réciproquement, soit $\mathfrak{p}$ un idéal maximal de K au-dessus de p tel que $a_\mathfrak{p}$ soit 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 H. Cela implique :

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

Si tous les idéaux de $\mathcal{J}$ sont de type (B01), on note $\mathfrak{p}_L$ le conjugué complexe de l'idéal de L situé au-dessous de $\mathfrak{p}_0$ (c'est donc le conjugué complexe de l'idéal $\mathcal{P}_0^\mathfrak{q}$ pour tout idéal $\mathfrak{q}$ dans $\mathcal{J}$). Soit $\mathfrak{p}$ un idéal maximal de K au-dessus de $\mathfrak{p}_L$. Alors il existe un élément τ dans G privé de H tel qu'on ait $\tau^{-1}\mathfrak{p}_0 = \mathfrak{p}$. L'entier $a_\mathfrak{p}$ est alors égal à a_τ, donc à 12.

Réciproquement, soit $\mathfrak{p}$ un idéal maximal de K au-dessus de p tel que $a_\mathfrak{p}$ soit 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 G privé de H. Alors τ et τ^{-1} induisent sur L la conjugaison complexe et on obtient :

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

□

Remarque 3.2.10. — Si tous les idéaux de $\mathcal{J}$ sont de type (B10), l'idéal $\mathfrak{p}_L$ est égal à l'idéal $\mathcal{P}_0^\mathfrak{q}$ pour tout $\mathfrak{q}$ dans $\mathcal{J}$; si tous les idéaux de $\mathcal{J}$ sont de type (B01), l'idéal $\mathfrak{p}_L$ est égal au conjugué complexe de l'idéal $\mathcal{P}_0^\mathfrak{q}$ pour tout $\mathfrak{q}$ dans $\mathcal{J}$ (voir remarque 3.2.7).

Comme les entiers $a_\mathfrak{p}$ sont définis (voir partie 1.3) par $\mu_{|I_\mathfrak{p}} = \chi_p^{a_\mathfrak{p}}$, le lemme 3.2.9 montre que le caractère μ est non ramifié hors de $\mathfrak{p}_L$.

Soit $\mathfrak{q}$ un idéal maximal de K au dessus de p mais premier à $\mathfrak{p}_L$. On fixe un élément $\sigma_\mathfrak{q}$ de G_K qui induit dans $\mathrm{Gal}(K^\mu/K)$ l'élément $\overline{\sigma}_\mathfrak{q}$ de Frobenius associé à $\mathfrak{q}$ (voir les parties 1.1 et 2.1)). La proposition 2.2.1 admet alors la version suivante :

Lemme 3.2.11. — *Soit α un élément non nul de K premier à $\mathfrak{p}_L$. Soit $\alpha\mathcal{O}_K = \prod_{\mathfrak{q}\nmid\mathfrak{p}_L} \mathfrak{q}^{\nu_\mathfrak{q}(\alpha)}$ l'unique décomposition de l'idéal fractionnaire principal $\alpha\mathcal{O}_K$ en produit d'idéaux maximaux de K. Alors on a :*

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

Démonstration. — Comme tous les coefficients $a_\mathfrak{p}$ sont égaux à 12 pour les idéaux maximaux $\mathfrak{p}$ au-dessus de $\mathfrak{p}_L$, on obtient, par une démonstration analogue à celle de la proposition 2.2.1 :

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

Le nombre premier p étant totalement décomposé dans L (lemme 3.2.9), le complété $L_{\mathfrak{p}_L}$ de L en $\mathfrak{p}_L$ est égal à $\mathbb{Q}_p$ et on a :

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

ce qui prouve le lemme. □

Proposition 3.2.12. — *Soit* $\mathfrak{q}$ *un idéal maximal de* K *premier à* $\mathfrak{p}_L$ *et* $\alpha_\mathfrak{q}$ *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 $\mathcal{J}$ et un élément α non nul de K tels qu'on ait :

$$\mathfrak{q} = \mathfrak{q}' \times (\alpha\mathcal{O}_K)\,.$$

Si tous les idéaux de $\mathcal{J}$ sont de type (B10) alors $\mathfrak{p}_L$ est égal à l'idéal $\mathcal{P}_0^{\mathfrak{q}'}$ (remarque 3.2.10), la norme de $\mathfrak{q}'$ dans l'extension K/L est $\beta_{\mathfrak{q}'}\mathcal{O}_L$ (proposition 2.4.2) et on a (notations 2.2.5) :

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

Si tous les idéaux de $\mathcal{J}$ sont de type (B01) alors $\mathfrak{p}_L$ est le conjugué complexe de l'idéal $\mathcal{P}_0^{\mathfrak{q}'}$ (remarque 3.2.10), la norme de $\mathfrak{q}'$ dans K/L est $\overline{\beta_{\mathfrak{q}'}}\mathcal{O}_L$ (proposition 2.4.2) et on a (notations 2.2.5) :

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

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

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

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, ce qui implique

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

Enfin, on a d'après le lemme 3.2.11 :

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

d'où

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

□

3.3. Homothéties

On remarque qu'on a dans $\mathrm{M}_2(\mathbb{F}_p)$ l'égalité suivante :

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

Le terme hors diagonale de φ_p n'est donc pas gênant dans la recherche des homothéties. Il suffit de déterminer les éléments $\mathbb{F}_p^\times$ qui sont égaux à l'image par λ d'une part et $\chi_p\lambda^{-1}$ d'autre part d'un même élément de G_K.

Proposition 3.3.1. — *Si tous les idéaux de $\mathcal{J}$ sont de type (B1/2), alors l'image de φ_p contient les homothéties $(\mathbb{F}_p^\times)^6$.*

Démonstration. — Soit $\mathfrak{p}$ un idéal maximal de K au-dessus de p. Comme l'entier $a_\mathfrak{p}$ est égal à 6, le caractère μ restreint au sous-groupe d'inertie $I_\mathfrak{p}$ est égal au caractère cyclotomique à la puissance 6. Alors c'est aussi le cas pour le caractère $(\chi_p\lambda^{-1})^{12}$ égal à $\chi_p^{12}\mu^{-1}$.

On en déduit que les caractères diagonaux de φ_p^{12} restreints au sous-groupe d'inertie $I_\mathfrak{p}$ sont tous les deux égaux à χ_p^6. Comme on a supposé p non ramifié dans K, le caractère cyclotomique restreint à $I_\mathfrak{p}$ est surjectif dans $\mathbb{F}_p^\times$, ce qui prouve la proposition. □

Proposition 3.3.2. — *Si tous les idéaux de $\mathcal{J}$ sont de type (B10) ou (B01), alors l'image de φ_p contient les homothéties $(\mathbb{F}_p^\times)^{12}$.*

Démonstration. — Soit x un élément de $\mathbb{F}_p^\times$ et $\mathfrak{p}$ un idéal premier de K au-dessus de $\mathfrak{p}_L$.

D'après le lemme 3.2.9, l'entier $a_\mathfrak{p}$ est égal à 12 donc le caractère μ restreint au sous-groupe d'inertie $I_\mathfrak{p}$ est égal au caractère cyclotomique à la puissance 12. Comme p est supposé non ramifié dans K, le caractère cyclotomique restreint au sous-groupe d'inertie $I_\mathfrak{p}$ est surjectif dans $\mathbb{F}_p^\times$; il existe donc un élément σ de G_K, appartenant à $I_\mathfrak{p}$, dont l'image par μ est x^{12}.

Le deuxième caractère λ' apparaissant sur la diagonale de la représentation φ_p est égal à $\chi_p\lambda^{-1}$; sa puissance douzième est donc

triviale sur $I_{\mathfrak{p}}$. Comme σ est choisi appartenant à $I_{\mathfrak{p}}$, on obtient que les termes diagonaux de $\varphi_p^{12}(\sigma)$ sont $(x^{12}, 1)$.

Soit $\mathfrak{p}'$ un idéal premier de K au-dessus de $\overline{\mathfrak{p}_L}$. D'après le lemme 3.2.9, l'entier $a_{\mathfrak{p}'}$ est égal à 0. Le caractère μ est donc trivial sur le sous-groupe d'inertie $I_{\mathfrak{p}'}$ et le second caractère diagonal λ' de la représentation φ_p vérifie :

$$\lambda'^{12}_{|I_{\mathfrak{p}'}} = \left(\chi_p \lambda^{-1}\right)^{12}_{|I_{\mathfrak{p}'}} = \left(\chi_{p|I_{\mathfrak{p}'}}\right)^{12}.$$

Ainsi, il existe un élément σ' de G_K, appartenant à $I_{\mathfrak{p}'}$, dont l'image par λ'^{12} est x^{12}. Les deux termes diagonaux de $\varphi_p^{12}(\sigma')$ sont alors $(1, x^{12})$.

Enfin, l'image par φ_p^{12} du produit $\sigma\sigma'$ de G_K a pour diagonale (x^{12}, x^{12}). Ceci étant valable pour tout élément x dans $\mathbb{F}_p^\times$, on en déduit que l'image de la représentation φ_p contient les homothéties $(\mathbb{F}_p^\times)^{12}$. □

On a ainsi obtenu :

Théorème 3.3.3. — *Si p est strictement supérieur à*

$$\max\left(65(3^{12d}-1)(24d)^6; \left[\left(2(\Delta_K)^{Ah}\right)^{12h} C_2(K) + \left(2(\Delta_K)^{Ah}\right)^{6h}\right]^{2d}\right)$$

alors l'image de la représentation φ_p contient les homothéties qui sont des puissances douzièmes.

NOTATIONS

K	un corps de nombres, supposé plongé dans $\mathbb{C}$ et galoisien sur $\mathbb{Q}$	p. i
E	une courbe elliptique définie sur K	p. i
p	un nombre premier rationnel (non ramifié dans K)	p. i
$\mathrm{T}_p(E)$	le module de Tate de la courbe E en p	p. i
$\overline{K}$	une clôture algébrique de K	p. i
G_K	le groupe de Galois absolu de K	p. i
ρ_p	la représentation de G_K agissant sur $\mathrm{T}_p(E)$	p. i
$E(\overline{K})[p]$	les points de p-torsion de E sur $\overline{K}$	p. i
φ_p	la représentation de G_K agissant sur $E(\overline{K})[p]$	p. i
V	un sous-groupe d'ordre p de E défini sur K, fixé	p. i
$V(\overline{K})$	les points de V sur $\overline{K}$	p. i
λ	le caractère de G_K dans $\mathbb{F}_p^\times$ donnant l'action de G_K sur $V(\overline{K})$	p. ii
λ'	le caractère $\chi_p\lambda^{-1}$	p. ii
χ_p	le caractère cyclotomique de G_K dans $\mathbb{F}_p^\times$	p. ii
d	le degré de l'extension $K/\mathbb{Q}$	p. iii
h	le cardinal du groupe des classes d'idéaux de K	p. iii
h	la hauteur absolue sur K	p. iii
Δ_K	le discriminant de K	p. iii
r_K	le rang du groupe des unités de K	p. iii
R_K	le régulateur de K	p. iii
δ_K		p. iii
K^λ	l'extension (cyclique) de K trivialisant λ	p. 1
$\mathfrak{q}$	un idéal maximal de K premier à p	p. 1
q	la caractéristique de $\mathfrak{q}$ (nombre premier rationnel différent de p)	p. 1
$N\mathfrak{q}$	la norme de $\mathfrak{q}$ dans $K/\mathbb{Q}$	p. 1

$k_\mathfrak{q}$	le corps résiduel de K en $\mathfrak{q}$	p. 1
$K_\mathfrak{q}$	le complété de K en $\mathfrak{q}$	p. 1
$\overline{\mathfrak{q}}$	une place de $\overline{K}$ au-dessus de $\mathfrak{q}$	p. 1
$\overline{k_\mathfrak{q}}$	le corps résiduel de $\overline{K}$ en $\overline{\mathfrak{q}}$	p. 1
$D_\mathfrak{q}$	le sous-groupe de décomposition de $\overline{\mathfrak{q}}$ dans G_K	p. 1
$I_\mathfrak{q}$	le sous-groupe d'inertie de $D_\mathfrak{q}$	p. 1
$\sigma_\mathfrak{q}$	un élément de $D_\mathfrak{q}$ relevant le Frobenius de $k_\mathfrak{q}$	p. 2
$L^\mathfrak{q}$	le corps de décomposition de $P_\mathfrak{q}(X)$	p. 3
$\beta_\mathfrak{q}$, $\overline{\beta_\mathfrak{q}}$	les racines de $P_\mathfrak{q}(X)$	p. 3
$j(E)$	l'invariant j de la courbe E	p. 8
$P_\mathfrak{q}(X)$	le polynôme caractéristique de l'action de $\sigma_\mathfrak{q}$ sur $\mathrm{T}_p(E)$	p. 9
$\mathfrak{p}$	un idéal maximal de K au-dessus de p	p. 10
$K_\mathfrak{p}$	le complété de K en $\mathfrak{p}$	p. 10
$\overline{\mathfrak{p}}$	une place de $\overline{K}$ au-dessus de $\mathfrak{p}$ (fixée dans tout le texte)	p. 10
$k_\mathfrak{p}$	le corps résiduel de K en $\mathfrak{p}$	p. 10
$D_\mathfrak{p}$	le sous-groupe de décomposition de $\overline{\mathfrak{p}}$ dans G_K	p. 10
$I_\mathfrak{p}$	le sous-groupe d'inertie de $D_\mathfrak{p}$	p. 10
$a_\mathfrak{p}$		p. 11
μ	le caractère de G_K dans $\mathbb{F}_p^\times$ égal à λ^{12}	p. 16
K^μ	l'extension (cyclique) de K trivialisant μ	p. 17
$\overline{\mu}$	l'injection de $\mathrm{Gal}(K^\mu/K)$ dans $\mathbb{F}_p^\times$ induite par μ	p. 17
ν	une place de K	p. 17
K_ν	le complété de K en ν	p. 17
U_{K_ν}	les unités de K_ν (pour ν finie)	p. 17
$\mathbb{A}_K^\times$	les idèles de K	p. 17
r_ν		p. 17
ι_ν	l'injection canonique de K dans K_ν	p. 19
$\mathfrak{p}_0$	un idéal maximal de K au-dessus de p, fixé	p. 20
$\mathcal{N}$		p. 20
G	le groupe de Galois de K sur $\mathbb{Q}$	p. 20
τ	un élément de G	p. 20
a_τ		p. 20
$\mathfrak{p}_0^\mathfrak{q}$	un idéal maximal de $KL^\mathfrak{q}$ au-dessus de $\mathfrak{p}_0$, fixé	p. 21
$\mathcal{P}_0^\mathfrak{q}$	l'idéal maximal de $L^\mathfrak{q}$ au-dessous de $\mathfrak{p}_0^\mathfrak{q}$	p. 21
$\gamma_\mathfrak{q}$	un générateur de l'idéal $\mathfrak{q}^h$	p. 25
$\mathcal{J}$		p. 35
L		p. 42
$\mathfrak{p}_L$		p. 44

BIBLIOGRAPHIE

[Ara08] Keisuke Arai. On uniform lower bound of the Galois images associated to elliptic curves. *J. Théor. Nombres Bordeaux*, 20(1):23–43, 2008.

[BG96] Yann Bugeaud and Kálmán Győry. Bounds for the solutions of unit equations. *Acta Arith.*, 74(1):67–80, 1996.

[Eck05] Carola Eckstein. *Homothéties, à chercher dans l'action de Galois sur des points de torsion*. PhD thesis, IRMA, Strasbourg, 2005.

[Lan65] Serge Lang. Division points on curves. *Ann. Mat. Pura Appl. (4)*, 70:229–234, 1965.

[LMO79] 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.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[Mom95] Fumiyuki Momose. Isogenies of prime degree over number fields. *Compositio Math.*, 97(3):329–348, 1995.

[Par99] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[Ray74] Michel Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Sil92] 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.

[ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.