INSTITUT DE RECHERCHE MATHÉMATIQUE AVANCÉE
Universit Louis Pasteur et CNRS (UMR 7501)
7, rue Ren Descartes
67084 Strasbourg Cedex

Homothéties,

à chercher dans l'action de Galois sur des points de torsion

par

Carola Eckstein

Classification AMS : 11F80, 11G05, 11G10, 14G25, 14K15
Mots clés : représentation galoisienne, image de Galois, homothéties, conjecture de Lang, points de torsion, module de Tate, arithmétique des variétés abéliennes, variété abélienne à multiplication complexe, courbe elliptique

Remerciements

Avant toute chose je dois un grand, grand MERCI à Jean-Pierre Wintenberger. Sans lui, je n'aurais pas fait de thèse, je n'aurais pas eu un bon sujet sur lequel j'ai travaillé plus que volontiers et que, sans ses bonnes remarques au bon moment j'aurais abandonné plus d'une fois. Donc, merci de m'avoir soutenue, malgré une situation difficile au départ. Et merci de m'avoir si bien encadrée.

Je remercie également les membres de jury et rapporteurs pour le temps et le soin qu'ils ont consacrés à ma thèse. Leurs remarques ont bien aidé à rendre ce texte plus lisible.

La Studienstiftung des deutschen Volkes m'a permis de me lancer dans ce travail sans le moindre souci financier. Max Brocker en particulier m'a soutenue 'against the odds'. Je lui suis reconnaissante pour la confiance qu'il m'a accordée au moment le plus difficile.

Je remercie Marco pour le ю et tous les Mar℀i pour le support TEXnique, servi avec beaucoup de thé. Un grand merci également à ceux qui avec beaucoup de patience ont corrigé mon français, mon orthographe, mes expressions bizarres, ...

Last not least je remercie tous ceux qui m'ont aidée et soutenue ces dernières années et qui ont rendu ma vie à Strasbourg agréable, intéressante, amusante, ...

Carola Eckstein

Homothéties, à chercher dans l'action de Galois sur des points de torsion

Soit A une variété abélienne de dimension g, définie sur un corps de nombres F que l'on suppose plongé dans $\mathbb{C}$. On note d le degré de F sur $\mathbb{Q}$. Soit A_{tor} le sous-groupe de torsion du groupe $A(\overline{\mathbb{Q}})$ (tous les points de torsion dans $A(\mathbb{C})$ sont algébriques sur F car pour tout $n \in \mathbb{Z}$, $n \neq 0$, il n'y a qu'un nombre fini de points de n-torsion). Pour tout premier p et tout entier n on a le sous-groupe A_{p^n} des points de p^n-torsion dans A_{tor}. En regardant $A(\mathbb{C})$, on voit que A_{p^n} est isomorphe à $\mathbb{Z}/p^n\mathbb{Z} \times \ldots \times \mathbb{Z}/p^n\mathbb{Z}$ ($2g$ facteurs). Le module de Tate $T_p(A) = \varprojlim_n A_{p^n}$ est donc un $\mathbb{Z}_p$-module libre de rang $2g$ et son groupe de $\mathbb{Z}_p$-automorphismes est isomorphe à $\mathrm{Gl}_{2g}(\mathbb{Z}_p)$. Le centre de ce groupe d'automorphismes est formé des homothéties $\mathbb{Z}_p^*$, plongées diagonalement dans $\mathrm{Gl}_{2g}(\mathbb{Z}_p)$.

Comme les coordonnées des points de torsion sont algébriques sur F, le groupe de Galois $G_F = G(\overline{\mathbb{Q}}/F)$ agit sur A_{p^n} et sur $T_p(A)$.

Dans [11] Lang a proposé la conjecture suivante :

Conjecture 1 (Lang). *Soit A une variété abélienne définie sur F. Il existe un entier $c \geq 1$ avec la propriété suivante : pour tout point de n-torsion P de A le sous-groupe des $d \in (\mathbb{Z}/n\mathbb{Z})^*$ tels que dP soit conjugué à P sur F est d'indice au plus c dans $(\mathbb{Z}/n\mathbb{Z})^*$.*

Pour la suite on va raisonner en termes de représentations du groupe Galois. L'action de G_F sur $T_p(A)$ donne lieu à la représentation suivante :

$$\rho_p : G_F \longrightarrow \mathrm{Aut}(T_p(A)) \simeq \mathrm{Gl}_{2g}(\mathbb{Z}_p)$$

On regarde également le produit de toutes les ρ_p, avec la topologie produit sur $\prod_p \mathrm{Gl}_{2g}(\mathbb{Z}_p)$:

$$\rho : G_F \longrightarrow \mathrm{Aut}(\prod_p T_p(A)) \simeq \prod_p \mathrm{Gl}_{2g}(\mathbb{Z}_p).$$

Pour une variété abélienne A fixée, définie sur un corps F, notons $c_p(A,F)$ l'indice de $\rho_p(G_F) \cap \mathbb{Z}_p^*$ dans $\mathbb{Z}_p^*$ et $c_n(A,F)$ l'indice de $(\prod_{p|n} \rho_p)(G_F) \cap \prod_{p|n} \mathbb{Z}_p^*$ dans $\prod_{p|n} \mathbb{Z}_p^*$. La conjecture de Lang dit alors qu'il existe un entier $c(A,F)$ tel que, pour tout entier n, l'indice $c_n(A,F)$ est borné par $c(A,F)$, ce qui équivaut à ce que $\rho(G_F)$ contient un sous-groupe ouvert des homothéties $\prod_p \mathbb{Z}_p^*$.

Dans [3] Bogomolov montre que $\rho_p(G_F)$ contient toujours un sous-groupe ouvert des homothéties. Autrement dit, les indices $c_p(A,F)$ sont tous finis.

Serre a prouvé une version affaiblie de la conjecture de Lang ([19, cours 1985-86 (136), thm. 2′, p. 34] voir aussi [25]) :

Théorème 2. *Soit A une variété abélienne, définie sur un corps de nombres F. Il existe un entier $c(A,F) \geq 1$ tel que $\rho_p(G_F)$ contienne les homothéties qui sont des puissances $c(A,F)$-ièmes (en particulier tous les $c_p(A,F)$ divisent $c(A,F)$).*

Dans le même cours ([19, cours 1985-86 (136), thm. 1, p. 34]) Serre a démontré

Théorème 3. *Soit A une variété abélienne, définie sur un corps de nombres F. Alors il existe une extension finie F' de F telle que les ρ_p soient indépendantes sur F' (c'est-à-dire l'homomorphisme $\rho(G_{F'}) \to \prod_p \rho_p(G_{F'})$ est surjectif).*

Ce qui manque maintenant pour prouver la conjecture de Lang est la

Conjecture 4. *Pour toute variété abélienne A il existe un premier rationnel q_A, dépendant de A, tel que pour tout $p \geq q_A$ l'image $\rho_p(G_F)$ contienne toutes les homothéties $\mathbb{Z}_p^*$ (c'est à dire $c_p(A,F) = 1$ pour tout $p \geq q_A$).*

D'autre part, on peut se demander s'il existe des bornes uniformes pour les indices $c_p(A,F)$. On fait la conjecture suivante et on l'étudie pour les cas particuliers des variétés abéliennes à multiplication complexe et des courbes elliptiques.

Conjecture 5. (*a*) *Pour p premier, g et d entiers, il existe un entier $c_p(g,d)$ tel que pour toute variété abélienne A de dimension g, définie sur un corps F de degré d sur $\mathbb{Q}$, les homothéties $(\mathbb{Z}_p^*)^{c_p(g,d)}$ sont contenues dans l'image $\rho_p(G_F)$ (c'est-à-dire $c_p(A,F)$ divise $c_p(g,d)$).*

(*b*) *Pour p assez grand on peut être plus précis : pour tout entier g il existe un entier $c(g)$ vérifiant que pour tout corps de nombres F il existe un premier $q(g,F)$ tel que pour tout $p \geq q(g,F)$ l'indice $c_p(g,d)$ divise $c(g)$.*

Théorème 6. *Les conjectures 4 et 5 sont vraies pour les variétés abéliennes à multiplication complexe. On peut choisir la constante $c(g)$ de la partie (b) égal à $|\mathrm{Gl}_2(\mathbb{F}_3)| < 3^{4g^2}$.*

Ce théorème est démontré dans le premier chapitre (théorème 7).

Dans le cas des variétés abéliennes à multiplication complexe toutes les indices $c_p(A,F)$ divisent $[F:\mathbb{Q}]\cdot c(g)$ avec la constante $c(g) = |\mathrm{Gl}_2(\mathbb{F}_3)|$ qui ne dépend que de la dimension g de A (ce qui donne la partie (a) de la conjecture 5). Pour tous les premiers p non ramifiés dans F l'indice $c_p(A,F)$ divise $c(g) = |\mathrm{Gl}_2(\mathbb{F}_3)|$ (partie (b) de la conjecture 5). Si la variété abélienne A a bonne réduction en p et si F n'est pas ramifié au-dessus de ce premier, alors $\rho_p(G_F)$ contient toutes les homothéties (conjecture 4). On peut en déduire le résultat global $(\prod_p \mathbb{Z}_p^*)^{c'(g)} \subseteq \rho(G_F)$ avec $c'(g) = [F:\mathbb{Q}]\cdot c(g)$ et on montre que l'image $\rho(G_F)$ contient un sous-groupe ouvert des homothéties (cor. 15).

L'exemple du paragraphe 1.3 prouve que le premier q_A dans la conjecture 4 dépend réellement de A : pour tout entier q, il existe des variétés abéliennes (même des courbes elliptiques à multiplication complexe) telles que pour un $p > q$, l'image $\rho_p(G_F)$ ne contient pas tout $\mathbb{Z}_p^*$.

Dans le deuxième chapitre on considère le cas d'une courbe elliptique E définie sur un corps de nombres F et sans multiplication complexe ($\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$). On note d le degré de F sur $\mathbb{Q}$ et h_F le nombre de classes de F. Entre autre, on a les résultats suivants :

Théorème 18. *Pour tout $p > (48dh_F)^{3(48dh_F)^2}$ qui n'est pas ramifié dans F, soit $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^{12}$, soit le groupe E_p des points de p-torsion de E a un sous-groupe non trivial qui est rationnel sur F et la courbe E a, par rapport à une place v divisant p, potentiellement bonne réduction de hauteur 2 avec un groupe formel dont le polygone de Newton a deux pentes non nulles distinctes* (*voir p.* 24).

En utilisant le résultat de Mazur [13] on en déduit le

Corollaire 61. *Si la courbe elliptique E est définie sur $\mathbb{Q}$, alors $\rho_p(G_\mathbb{Q})$ contient les homothéties $(\mathbb{Z}_p^*)^{12}$ pour tout $p > 163$.*

Cela démontre la partie (b) de la conjecture 5 pour des courbes elliptiques définies sur $\mathbb{Q}$.

Des résultats similaires à celui utilisé pour $F = \mathbb{Q}$ sont vrais pour d'autre corps. En particulier il y a des résultats de Momose ([15]) qui généralisent celui de Mazur ([13]) et impliquent que dans beaucoup de cas on devrait pouvoir borner les p pour lesquels peut se produire le "mauvais cas" du théorème 18.

Théorème 39. *Si le premier p est plus grand que $(48dh_F)^{3(48dh_F)^2}$ et non ramifié dans $F(E_3)$, alors l'image $\rho_p(G_F)$ contient les homothéties $\mathbb{Z}_p^*$.*

Ce dernier théorème donne une démonstration de la conjecture 4 pour les courbes elliptiques.

Pour les démonstrations on distingue différents cas selon le type de réduction de E par rapport aux places au-dessus de p. Lorsque, pour une place divisant p, la courbe E a bonne réduction de hauteur 2, sans coude dans le polygone de Newton, on se sert d'une généralisation d'un résultat de Fontaine ([7]) pour retrouver les homothéties dans l'image (thm. 45).

Dans les autres cas on utilise le travail de Serre, surtout [18] : on généralise légèrement et remonte à $\rho_p(G_F)$ les résultats obtenus par Serre modulo p pour trouver que
- soit $\rho_p(G_F)$ contient un grand sous-groupe des homothéties
- soit une courbe E', isogène à E et également définie sur F, possède un point de p-torsion P tel que le corps $F(P)$ est de degré au plus $48h_F$ sur F
- soit le groupe E_p a un sous-groupe non trivial qui est rationnel sur F et la courbe E a, par rapport à une place v divisant p, potentiellement bonne réduction de hauteur 2 avec un polygone de Newton qui a deux pentes non nulles distinctes.

Lorsqu'on a une courbe elliptique E' avec un point de p-torsion rationnel sur une

extension de degré $48dh_F$ sur $\mathbb{Q}$ le résultat [14] de Merel implique que p doit être inférieur à $(48dh_F)^{3(48dh_F)^2}$.

Finalement on a le théorème 45 comme résultat auxiliaire. Ce théorème généralise un résultat de Fontaine ([7]). La démonstration du théorème 45 suit essentiellement des indications données par Fontaine pour la démonstration du résultat énoncé dans [7].

Théorème 45. *Soit $\mathcal{F}$ un groupe formel de hauteur 2, défini sur un corps local $K/\mathbb{Q}_p$ avec $p > 2$. On suppose que le polygone de Newton de $\mathcal{F}$ n'a qu'une seule pente non nulle et que le degré de ramification e de K sur $\mathbb{Q}_p$ est strictement plus petit que $p-1$ et divise p^2-1. Alors l'image de la représentation de Galois ρ_p contient un sous-groupe d'indice e d'un sous-groupe de Cartan non déployé. En particulier $\rho_p(G_K)$ contient les homothéties $(\mathbb{Z}_p^*)^e$.*

Table des matières

Who's who, CM

G_K	$G(\overline{K}/K)$, le groupe de Galois absolu pour un corps K quelconque	
p	un premier rationnel	
A	une variété abélienne à multiplication complexe	
g	la dimension de A	
$\mathrm{End}_{\overline{\mathbb{Q}}}(A)$	anneau des endomorphismes de A sur $\overline{\mathbb{Q}}$	
F	le corps de nombres sur lequel A est défini	
d	$[F : \mathbb{Q}]$	
L	le corps sur lequel A a bonne réduction	$[L : F] < 3^{4g^2}$
c	$[L : \mathbb{Q}]$	
A_{p^n}	les points de p^n-torsion dans $A(\overline{\mathbb{Q}})$ (ou dans $A(\overline{\mathbb{Q}}_p)$)	c'est un $(\mathbb{Z}/p^n\mathbb{Z})$-module libre de rang 2g
$T_p(A)$	le module de Tate	un $\mathbb{Z}_p$-module libre de rang 2g
(K', Φ)	le CM-type de A	$\iota : K' \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$
$\mathcal{O}$	$\iota^{-1}(\iota(K') \cap \mathrm{End}(A))$	
(K, Ψ)	le type reflex de (K', Φ)	
K^0	sous-corps totalement réel de K	$[K : K^0] = 2$
S_Φ, S_Ψ	plongements qui, restreints à K', respectivement K, sont contenus dans Φ, respectivement Ψ	p. 9
t	l'espace tangent de A à l'origine	
$\det_\Psi$	une application $L^* \to K'^*$	voir p. 10
T_K	$R_{K/\mathbb{Q}}(\mathbb{G}_m)$	
$\mathbf{\Psi}$	application $T_L \to T_{K'}$ définie par $\det_\Psi : L^* \to K'^*$	p. 10, [20, §7, p. 510]
$\mathbf{\Psi}_p$	l'application $(L \otimes \mathbb{Q}_p)^* \to (K' \otimes \mathbb{Q}_p)^*$ donné par $\mathbf{\Psi}$	
$\hat{\mathbf{\Psi}}$	voir p. 11	
w	une place de L au-dessus de p	
L_w	le complété de L par rapport à w	
L_p	$L \otimes \mathbb{Q}_p$	
U_{L_w}	les unités de L_w	
U_{L_p}	$\prod_{w\mid p} U_{L_w}$	
I_v	un sous-groupe d'inertie	
E_χ	une courbe elliptique tordue par un caractère χ	
ρ_p^χ	les représentations associés à E_χ	

1 Les variétés abéliennes CM

On se donne une variété abélienne A, définie sur un corps de nombres F. On note d le degré de F sur $\mathbb{Q}$ et on suppose F plongé dans $\overline{\mathbb{Q}}$. La dimension de A sera notée g. Pour tout corps K, on note G_K le groupe de Galois absolu $G(\overline{K}/K)$.

Soit $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$ l'anneau des endomorphismes de A sur $\overline{\mathbb{Q}}$. On dit que A a multiplication complexe s'il existe un corps K' qui est de degré $2g$ sur $\mathbb{Q}$ et un plongement $\iota : K' \hookrightarrow \mathbb{Q} \otimes \mathrm{End}_{\overline{\mathbb{Q}}}(A)$.

Pour tout premier rationnel p, l'ensemble des points de p-torsion dans $A(\overline{\mathbb{Q}})$ sera noté A_p et le module de Tate, $T_p(A)$. Alors la variété abélienne A donne lieu aux représentations de Galois suivantes :

$$\begin{array}{ll} \rho : & G_F \longrightarrow \mathrm{Aut}(\prod_p T_p(A)) \simeq \prod_p \mathrm{Gl}_{2g}(\mathbb{Z}_p) \\ \rho_p : & G_F \longrightarrow \mathrm{Aut}(T_p(A)) \simeq \mathrm{Gl}_{2g}(\mathbb{Z}_p) \end{array}$$

Théorème 7. *Soit A une variété abélienne, définie sur un corps de nombres F et à multiplication complexe (sur $\overline{\mathbb{Q}}$). Alors l'image $G = \rho(G_F)$ contient un sous-groupe ouvert des homothéties ainsi que le sous-groupe $(\prod_p \mathbb{Z}_p^*)^c$ avec c divisant $|\mathrm{Aut}(A_3)| \cdot d < 3^{4g^2} d$.*

Si F n'est pas ramifié au dessus d'un premier p et A/F a bonne réduction pour les places au dessus de p, alors $\rho_p(G_F)$ contient toutes les homothéties $\mathbb{Z}_p^*$.

On montre d'abord (thm. 10) que pour tout premier $p \in \mathbb{N}$, l'image $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^c$. On trouvera ces homothéties dans le groupe engendré par les images $\rho_p(I_v)$, où $I_v \subseteq G_F$ sont les sous-groupes d'inertie au-dessus de p. Cela permettra de passer au produit $G = \prod_p G_p$ et de conclure que G contient les homothéties $(\prod_p \mathbb{Z}_p^*)^c$ (cor. 15).

1.1 Préliminaires

Avant tout on se place sur l'extension $L = F(A_3)$ de F, car on a :

Lemme 8. *Soit A une variété abélienne, définie sur un corps de nombres F.*

- *(a) Tous les endomorphismes de A (sur $\overline{\mathbb{Q}}$) sont définis sur $L = F(A_3)$*
- *(b) Si la variété A a potentiellement bonne réduction en une place, alors elle y a bonne réduction sur L*

Du corps $L = F(A_3)$ on sait que

- *(c) le degré $[L : F]$ divise l'ordre $|\mathrm{Aut}(A_3)| < 3^{4g^2}$*
- *(d) L'extension L/F est non ramifiée en dehors de 3 et les places de mauvaise réduction de A/F.*

Remarque : Lorsque la variété A est à multiplication complexe, elle a potentiellement bonne réduction partout [20, thm. 6, p. 503].

On utilise le lemme suivant ([5, lemma IV-2.1, p. 46]) :

Lemme 9. *Soit p un premier impair. Pour tout $\mathbb{Z}_p$-module libre B, le noyau de l'application* réduction-modulo-p : $\mathrm{Aut}(B) \xrightarrow{\pi} \mathrm{Aut}(B/pB)$ *ne contient aucun élément d'ordre fini autre que l'identité.*

Démonstration (lemme 8) : (a) Tous les endomorphismes de A sont définis sur une extension finie et galoisienne L' de L [21, II-8.5. prop. 30, p. 65]. Le groupe $G(L'/L)$ agit sur $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$. D'autre part, les points de 3-torsion A_3 forment un $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$-module et la théorie analytique montre que c'est un $\mathrm{End}_{\overline{\mathbb{Q}}}(A)/3\mathrm{End}_{\overline{\mathbb{Q}}}(A)$-module fidèle.

On obtient une suite

$$G(L'/L) \xrightarrow{\nu} \mathrm{Aut}(\mathrm{End}_{\overline{\mathbb{Q}}}(A)) \xrightarrow{\pi} \mathrm{Aut}(\mathrm{End}_{\overline{\mathbb{Q}}}(A)/3\mathrm{End}_{\overline{\mathbb{Q}}}(A)) \hookrightarrow \mathrm{Aut}(\mathrm{End}(A_3)).$$

Le groupe $G(L'/L)$ agit trivialement sur les points de 3-torsion A_3, son image dans $\mathrm{Aut}(\mathrm{End}_{\overline{\mathbb{Q}}}(A))$ est donc contenue dans le noyau de π. Mais d'après le lemme 9 ce noyau contient comme seul élément d'ordre fini l'identité. On en déduit que $G(L'/L)$ agit trivialement sur $\mathrm{End}_{\overline{\mathbb{Q}}}(A)$. C'est-à-dire tous ces endomorphismes sont définis sur L.

(b) Pour les places w de caractéristique résiduelle différente de 3 c'est un théorème de Raynaud [22, thm. 3.5, p. 406] ou [1, cor. 5.18, p. 33] (il y a des résultats plus précis de Zarhin et Silverberg [22]).

Soit maintenant w une place au-dessus de 3 et K le completé de L par rapport à cette place. La variété abélienne A a bonne réduction sur la plus grande extension non ramifié K_{nr} de K si et seulement si elle a bonne réduction sur K [20, thm. 1]. On sait que A a bonne réduction sur une extension finie et galoisienne K' de K_{nr}. On regarde le modèle de Néron $\mathcal{A}$ de A sur K' et sa fibre spéciale $\tilde{\mathcal{A}}$. Par la définition de L, le groupe d'inertie I de K' sur K_{nr} agit trivialement sur le schéma en groupes de 3-torsion $\tilde{\mathcal{A}}_3$ de $\tilde{\mathcal{A}}$. Soit M le module de Dieudonné associé au 3-groupe $\tilde{\mathcal{A}}_{3^\infty}$ [8, thm. 1, chap. III, §1.4, p. 127], alors I agit aussi trivialement sur $M/3M$. En utilisant le lemme 9 on déduit que I agit trivialement sur M ce qui implique qu'il agit aussi trivialement sur $\tilde{\mathcal{A}}_{3^\infty}$. Le résultat est alors donné par [6, §2.5, p. 304].

(c) Comme le groupe de Galois $G(F(A_3)/F)$ est un sous-groupe de $\mathrm{Aut}(A_3) = \mathrm{Gl}_{2g}(\mathbb{Z}/3\mathbb{Z})$ son ordre divise $|\mathrm{Aut}(A_3)| < 3^{4g^2}$.

(d) C'est le corollaire 2(b) de [20, p. 497]. □

On aura besoin d'un certain nombre de notations concernant la multiplication complexe : on rappelle que la variété A est dite avoir multiplication complexe s'il existe un corps K' de degré $2g$ sur $\mathbb{Q}$ et un morphisme $\iota : K' \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$.

L'anneau des endomorphismes de A contient l'image d'un ordre $\mathcal{O} = \iota^{-1}(\iota(K') \cap \mathrm{End}(A))$ de K'. La variété étant définie sur L, l'espace tangent t de A à l'origine est un L-espace vectoriel de dimension g. D'autre part, les endomorphismes de A agissent sur t et donc K' agit sur t. Sur $\mathbb{C}$, cette action se diagonalise. Dans une base adaptée tout $\kappa \in K'$ correspond alors à une matrice diagonale (κ^{φ_i}) avec g plongements $\varphi_i : K' \hookrightarrow \mathbb{C}$. Ces plongements φ_i sont distincts et pas deux sont conjugués complexes [21, II §6.1, p. 41]. Le couple (K', Φ) avec $\Phi = \{\varphi_1, \ldots, \varphi_g\}$ est le CM-type de A.

A tout CM-type (K', Φ) on associe un type réflexe (K, Ψ) [21, II §8.3,prop. 28, p. 62]. Soit M un corps galoisien sur $\mathbb{Q}$ qui contient K', soient S_Φ les éléments de $G(M/\mathbb{Q})$ qui, restreints à K', sont contenus dans Φ et soit H le sous-groupe des $\gamma \in G(M/\mathbb{Q})$ tels que $E_\Phi \gamma^{-1} = S_\Phi$. Alors le corps réflexe K est le corps fixe de H dans M et Ψ est l'ensemble des $\sigma \in G(M/\mathbb{Q})$ avec $\sigma^{-1} \in S_\Phi$, restreint à K [21, p. 62]. Le corps réflexe K, comme le corps K', est totalement complexe avec un sous-corps K^0 totalement réel, telle que l'extension K/K^0 est de degré 2. Les $\psi_i \in \Psi$ donnent tous les plongements de K^0 dans $\overline{\mathbb{Q}}$. Tout corps de définition de A, sur lequel tous les endomorphismes de A sont définis, contient le corps reflex K [21, II §8.5, prop. 30, p. 65]. En particulier le corps L contient K (lemme 8(a)).

1.2 Le théorème

Théorème 10. *Soit A encore notre variété abélienne, définie sur un corps de nombres F et à multiplication complexe (sur $\overline{\mathbb{Q}}$). Soit L une extension finie de F sur laquelle tous les endomorphismes de A soient définis et telle que A/L ait bonne réduction partout.*

Alors, pour tout premier p, l'indice $(\mathbb{Z}_p^* : \rho_p(G_L) \cap \mathbb{Z}_p^*)$ divise le degré c de L sur $\mathbb{Q}$. Si le premier p est non ramifié dans L l'image $\rho_p(G_L)$ de la représentation ρ_p contient tout $\mathbb{Z}_p^*$ (c'est à dire toutes les homothéties).

Remarque : On peut prendre $L = F(A_3)$ (lemme 8). Les seuls premiers ramifiés dans $L = F(A_3)$ sont 3, les premiers ramifiés dans F et les premiers au-dessus desquels A a mauvaise réduction sur F.

En fait notre démonstration donne un peu plus :

Proposition 11. *Soit I_p le sous-groupe de G_L engendré par les sous-groupes d'inertie $I_w \subseteq G_L$, $w|p$. Sous les hypothèses du théorème 10 les homothéties $\mathbb{Z}_p^*$ (ou $(\mathbb{Z}_p^*)^c$ s'il y a ramification) sont contenues dans l'image $\rho_p(I_p)$ du sous-groupe $I_p \subseteq G_L$.*

Démonstration : L'espace tangent t de A_L est à la fois un L-espace vectoriel de dimension g et un K'-espace vectoriel de dimension $\frac{c}{2} = \frac{[L:\mathbb{Q}]}{2}$. Les actions de L et de K' commutent. Tout élément λ de L donne un endomorphisme K'-linéaire

de t dont on peut calculer le déterminant sur K'. On note $\det_\Psi : L^* \to K'^*$ l'application qui en résulte.

Lemme 12. *L'application* $\det_\Psi : L^* \to K'^*$ *est donnée par* $\lambda \mapsto \prod_{\psi \in S_\Psi} \lambda^\psi$ *où* S_Ψ *est l'ensemble des plongements* $\psi : L \hookrightarrow \mathbb{C}$ *qui, restreints à* K, *sont contenus dans* Ψ.

Démonstration : On va démontrer le lemme pour $t \otimes_L M$ avec un corps M qui contient L et K' et qui est galoisien sur $\mathbb{Q}$. Sur L le résultat en suit parce qu'on a $\det_{M/K'} = \det_{L/K'} \circ N_{M/L}$.

L'action de K' sur $t \otimes_L M \simeq M^g$ est donnée par les g plongements φ_i de K' dans M. L'espace tangent t est isomorphe à la somme directe de g espaces t_i de dimension un sur M, où K' agit sur t_i par $\varphi_i : K' \hookrightarrow M$. Chaque t_i est aussi un K'-espace vectoriel de dimension $[M : \mathbb{Q}]/2g$.

Sur M, l'action de M sur le K'-espace vectoriel t_i se diagonalise et est donnée, pour tout $\lambda \in M$, par la matrice diagonale (λ^{σ_j}) avec $\sigma_j : M \hookrightarrow \overline{\mathbb{Q}}$ tel que $\sigma|_{\varphi_i(K')} = \varphi_i^{-1}$.

En total, l'action de M sur le K'-espace vectoriel t est alors donnée par les matrices $(\lambda^\psi)_{\psi \in S_\Psi}$ avec $S_\Psi = \{\sigma \in G(M/\mathbb{Q}) : \sigma^{-1}|_{K'} \in \Phi\}$ et le déterminant est bien le produit donné. □

Soit $T_L = R_{L/\mathbb{Q}}(\mathbb{G}_m)$ (resp. $T_{K'} = R_{K'/\mathbb{Q}}(\mathbb{G}_m)$) le tore obtenu du groupe multiplicatif par restriction des scalaires de L à $\mathbb{Q}$ (resp. de K' à $\mathbb{Q}$). On définit le morphisme $\mathbf{\Psi} : T_L \to T_{K'}$ par la propriété que pour toute $\mathbb{Q}$-algèbre B l'application $\mathbf{\Psi}_B : (L \otimes B)^* \to (K' \otimes B)^*$ est donnée par $\lambda \otimes b \mapsto \prod_{\psi \in S_\Psi} (\lambda^\psi \otimes b)$ (l'image de cette application est bien dans $T_{K'}$, voir [20, pp. 510, 511]). En particulier on a pour tout premier $p \in \mathbb{N}$ un morphisme $\mathbf{\Psi}_p : (L \otimes \mathbb{Q}_p)^* \to (K' \otimes \mathbb{Q}_p)^*$ (comparer [20, pp. 510, 511]).

On revient aux représentations ρ_p : D'après le corollaire 2 de [20, p. 502], lorsque A a multiplication complexe, l'image de ρ_p est contenue dans le groupe $\mathcal{O}_p^*$ des éléments inversibles de $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$. Cette image est donc commutative et la représentation ρ_p passe au quotient : $\rho_p : \mathrm{Gal}(L^{ab}/L) \to \mathrm{Aut}(T_p(A))$.

Par la théorie du corps de classes, on en déduit une application des idèles $\mathbb{G}_m(\mathbb{A}_L)$ dont l'image est contenue dans $K_p'^* = (K' \otimes \mathbb{Q}_p)^*$. Le §7 de [20] décrit cette fonction $\rho_p : \mathbb{G}_m(\mathbb{A}_L) \to K_p'^*$ avec laquelle on travaille désormais. On veut montrer que l'image de ρ_p contient les homothéties, c'est à dire les unités rationnelles $\mathbb{Z}_p^* \subseteq K_p'^*$. On considère $L_p^* = (L \otimes \mathbb{Q}_p)^*$ plongé dans $\mathbb{G}_m(\mathbb{A}_L)$.

On note U_{L_w} le groupe des unités de L_w et on regarde l'image du sous-groupe $U_{L_p} = \prod_{w|p} U_{L_w}$ de L_p^*. Comme la variété A/L est supposée d'avoir bonne réduction partout, le corollaire 2 de [20, p. 513] dit qu'on a $\rho_p = 1/\mathbf{\Psi}_p$ sur tout le sous-groupe $U_{L_p} = \prod_{w|p} U_{L_w}$.

Lemme 13. *Si $L/\mathbb{Q}$ n'est pas ramifié au-dessus de p, alors l'image $\mathbf{\Psi}_p(U_{L_p})$ du sous-groupe $U_{L_p} \subseteq L_p^*$ contient toutes les unités $\mathbb{Z}_p^*$ de $\mathbb{Q}_p^* \subseteq K'^*_p$.*

Si p est ramifié dans L, on note e le plus petit multiple commun des indices de ramification de p dans L. L'indice $(\mathbb{Z}_p^* : \mathbf{\Psi}_p(U_{L_p}) \cap \mathbb{Z}_p^*)$ divise alors e et l'image $\mathbf{\Psi}_p(U_{L_p})$ contient les puissances e-ièmes $(\mathbb{Z}_p^*)^e$ des homothéties.

Démonstration : L'application $\mathbf{\Psi}$ est liée à la norme $N_{L/\mathbb{Q}} : T_L \to T_\mathbb{Q}$: si $\overline{\mathbf{\Psi}}$ est le conjugué complexe de $\mathbf{\Psi}$ on a $\mathbf{\Psi} \cdot \overline{\mathbf{\Psi}} = N_{L/\mathbb{Q}}$. Si $K \subseteq L$ est le corps réflexe du type (K', Φ) on peut décomposer notre application en $\mathbf{\Psi} = \hat{\mathbf{\Psi}} \circ N_{L/K}$ où $\hat{\mathbf{\Psi}} : T_K \to T_{K'}$ est donné par $(K \otimes B)^* \to (K' \otimes B)^* : \kappa \otimes b \mapsto \prod_{\psi \in \Psi} \kappa^\psi \otimes b$. Le corps K contient le sous-corps totalement réel K^0 et le tore T_{K^0} peut être considéré comme sous-tore de T_K. Restreints à K^0, les $\psi \in \Psi$ donnent exactement tous les plongements de K^0 dans $\overline{\mathbb{Q}}$, ce qui implique que, restreinte à T_{K^0}, l'application $\hat{\mathbf{\Psi}}$ n'est autre que la norme $N_{K^0/\mathbb{Q}} : T_{K^0} \to T_\mathbb{Q}$.

On s'intéresse donc à l'application norme : Soit L un corps de nombres et $p \in \mathbb{N}$ un premier. Si $w_1, \ldots, w_n$ sont les places de L au-dessus de p, alors $L_p^* = L_{w_1}^* \times \ldots \times L_{w_n}^*$ est la p-composante dans les idèles de L. Si M est un sous-corps de L, les idèles de M se plongent dans les idèles de L, leur p-composante s'écrit comme $M_p^* = M_{w_1}^* \times \ldots \times M_{w_n}^*$, les w_i étant les places de L restreintes à M. La norme $N_{L/M}$ envoie L_p^* dans M_p^*, l'image de $U_{L_p} = \prod_{w|p} U_{L_w}$ est contenue dans $U_{M_p} = \prod_{w|p} U_{M_w}$.

Lemme 14. *Soit L/M une extension de corps de nombres. Si cette extension n'est pas ramifiée au-dessus de p, alors $N_{L/M}(U_{L_p}) = U_{M_p}$.*

Si L/M est ramifié au-dessus de p soient $v_1, \ldots, v_s$ les places de M au-dessus de p et soient $w_{i,1}, \ldots, w_{i,r}$ les places de L au-dessus de v_i. Soient $e_{i,1}, \ldots, e_{i,r}$ leurs degrés de ramification respectives et $e_i = \operatorname{pgcd}(e_{i,j})$. Alors l'indice $(U_{M_{v_i}} : N_{L/M}(U_{L_{v_i}}))$ divise e_i.

Démonstration : On considère d'abord les normes locales $N_{L_w/M_v} : U_{L_w} \to U_{M_v}$. Entre L_w et M_v il y a un corps M_{nr} tel que M_{nr}/M_v et non ramifié et L_w/M_{nr} et totalement ramifié (le degré étant le degré de ramification $e_{w/v}$ de L_w sur M_v). Le corollaire [17, V-2, p. 90] dit que la norme N_{M_{nr}/M_v} est surjectif sur les unités, d'après le corollaire 3 dans [17, XV-2, p. 234] l'indice $(U_{M_{nr}} : N_{L_w/M_{nr}}(U_{L_w}))$ divise $e_{w/v}$. Comme on a $N_{L_w/M_v} = N_{M_{nr}/M_v} \circ N_{L_w/M_v}$ on en déduit que $(U_{M_v} : N_{L_w/M_v}(U_{L_w}))$ divise $e_{w/v}$.

Pour toute place v de M, la norme $N_{L/M}$ est le produit des normes N_{L_w/M_v} (pour tout $w|v$, [12, cor. 3, p. 39]) et donc $(U_{M_{v_i}} : N_{L/M}(U_{L_{v_i}}))$ divise le plus grand diviseur commun des $(U_{M_{v_i}} : N_{L_{w_{i,j}}/M_{v_i}}(U_{L_{w_{i,j}}}))$. Ce dernier divise e_i. □

Maintenant on sait que pour toute place v_i divisant p dans K et sa restriction v_i^0 à K^0, l'indice de $N_{L/K}(U_{L_{v_i}})$ dans $U_{K_{v_i}}$, et à fortiori l'indice de $N_{L/K}(U_{L_{v_i}}) \cap U_{K^0_{v_i^0}}$ dans $U_{K^0_{v_i^0}}$, divise l'indice de ramification e_i.

Les indices e_i divisent tous le degré $[L : K]$ parce que pour tout v_i ce degré est égal à la somme $\sum_{w_{i,j}|v_i} e_{i,j} f_{i,j}$ [12, prop. 21, p. 24] et e_i divise tous les $e_{i,j}$. On note $e_{L/K} = \text{ppcm}\,(e_i)$.

Restreint à $U_{K_p^0}$, l'application $\hat{\mathbf{\Psi}}$ est égal à la norme $N_{K_p^0/\mathbb{Q}_p}$. Comme avant, l'indice $(\mathbb{Z}_p^* : N_{K_v^0/\mathbb{Q}_p}(U_{K_v^0}))$ divise le degré de ramification $e_v = e_{K_v^0/\mathbb{Q}_p}$ pour toute place v divisant p. L'indice $(\mathbb{Z}_p^* : N_{K_v^0/\mathbb{Q}_p}(N_{L/K}(U_{L_v}) \cap U_{K_v^0}))$ divise $e_{L/M} \cdot e_v$. De nouveau l'indice $(\mathbb{Z}_p^* : N_{K^0/\mathbb{Q}}(N_{L/K}(U_{L_p}) \cap U_{K_p^0}))$ divise le $\text{pgcd}\,(e_{L/M} e_v)$ (sur toutes les v qui divisent p dans K^0).

Comme on a $\mathbf{\Psi} = \hat{\mathbf{\Psi}} \circ N_{L/K}$ et, restreint à K^0,l'application $\hat{\mathbf{\Psi}}$ est égale à la norme, l'indice $(\mathbb{Z}_p^* : \mathbf{\Psi}_p(U_{L_p}) \cap \mathbb{Z}_p^*)$ divise $(\mathbb{Z}_p^* : N_{K^0/\mathbb{Q}}(N_{L/K}(U_{L_p}) \cap U_{K_p^0}))$ et l'indice $(\mathbb{Z}_p^* : \mathbf{\Psi}_p(U_{L_p}) \cap \mathbb{Z}_p^*) = (\mathbb{Z}_p^* : \rho_p(U_{L_p}) \cap \mathbb{Z}_p^*)$ divise $e_{L/K} \cdot e_{K^0/\mathbb{Q}}$ ce qui divise $\frac{1}{2}[L : \mathbb{Q}]$.

q. e. d.

Corollaire 15. *On peut passer du résultat local du théorème* 10 *au résultat global du théorème* 7 : *sous les hypothèses du théorème* 7 *l'image* $\rho(G_F)$ *contient les homothéties* $(\prod_p \mathbb{Z}_p^*)^c$ *avec* $c = [L : \mathbb{Q}]$ *divisant* $|\text{Aut}(A_3)| \cdot d$. *De plus* $\rho(G_F)$ *contient un sous-groupe ouvert des homothéties.*

Démonstration : On fixe $L = F(A_3)$. Par le lemme 8 le degré $[L : \mathbb{Q}]$ divise $|\text{Aut}(A_3)| \cdot d$, tous les endomorphismes de A sont définis sur ce corps et A a bonne réduction partout sur L. On sait alors que, sur L, les ρ_p ne sont pas ramifiées en dehors de p [20, thm. 1, p. 493]. La proposition 11 implique donc que pour tout premier p et tout élément $\lambda \in (\mathbb{Z}_p^*)^c$ il existe un élément $\sigma \in G_F$ tel que $\rho_p(\sigma) = \lambda$ et $\rho_q(\sigma) = 1$ pour tout $q \neq p$. On peut conclure que, pour toute collection finie $p_1, \ldots, p_s$ de premiers, l'image $\prod_{i=1}^s \rho_{p_i}(G_L)$ contient les homothéties $\prod_{i=1}^s (\mathbb{Z}_{p_i}^*)^c$. Les applications ρ_p, et donc ρ, sont continues. les groupes G_L et $\rho(G_L)$ sont compacts. Comme tout élément x de $\prod_p (\mathbb{Z}_p^*)^c$ est la limite d'une suite d'éléments $x_j \in \prod_{i=1}^j (\mathbb{Z}_{p_i}^*)^c$, on sait que l'image $\rho(G_L)$ contient les homothéties $\prod_p (\mathbb{Z}_p^*)^c$. L'image $\rho(G_L)$ contient un sous-groupe ouvert des homothéties comme pour tout premier p non ramifié dans L, donc pour presque tout p, l'image $\rho_p(I_p)$ contient tout $\mathbb{Z}_p^*$. □

1.3 Un exemple

Pour notre variété abélienne A, définie toujours sur le corps F, on pose q_A égal au plus grand premier rationnel qui est ramifié dans $L = F(A_3)$. Dans le théorème 10 on a vu que pour tout $p > q_A$ l'image $\rho_p(G_F)$ contient toutes les homothéties $\mathbb{Z}_p^*$. On donne maintenant un exemple qui montre que, même pour $g = 1$ fixé, il n'existe pas d'entier q avec cette propriété et qui serait indépendant de A.

Soit E une courbe elliptique à multiplication complexe avec un ordre d'un corps

imaginaire quadratique K'. Lorsque le nombre de classes $h_{K'}$ de K' est égal à 1 on peut supposer que E est définie sur le corps K' (voir l'exemple plus bas). On peut alors considérer les représentations ρ_p comme applications de $G_{K'}^{ab}$ dans les unités $U_{K'_p}$ de $K' \otimes \mathbb{Q}_p$ [20, Cor. 2, p. 502].

D'autre part on se donne un caractère $\chi : G_{K'}^{ab} \to \mathrm{Aut}(E)$ $(\subseteq U_{K'_p})$. On note E_χ la courbe tordue par ce caractère et ρ_p^χ les représentations associées à la courbe tordue E_χ.

Lemme 16. *Les représentations associées à la courbe $E\chi$ sont donnés par $\rho_p^\chi = \rho_p \cdot \chi^{-1}$ (la multiplication étant la multiplication dans $U_{K'_p}$).*

Démonstration : La courbe E et son twist E_χ sont liées par un isomorphisme $\Upsilon : E_\chi \to E$ qui est défini sur une extension finie de K'. On peut choisir Υ tel que pour tout $\sigma \in G_{K'}$ on a $\chi(\sigma) = \Upsilon^\sigma \circ \Upsilon^{-1}$ (avec $\Upsilon^\sigma : E' \to E : P_\chi \mapsto (\Upsilon(P_\chi^{\sigma^{-1}}))^\sigma$).

Pour un $P_\chi \in E_\chi$ on a le diagramme commutatif suivant :

$$\begin{array}{ccc} P_\chi & \xrightarrow{\rho_p^\chi(\sigma)} & P_\chi^\sigma \\ \downarrow \Upsilon & & \downarrow \Upsilon = \Upsilon \circ (\Upsilon^\sigma)^{-1} \circ \Upsilon^\sigma = \chi(\sigma)^{-1} \Upsilon^\sigma \\ P & \xrightarrow{\chi(\sigma)^{-1} \cdot \rho_p} & \chi(\sigma)^{-1}(P^\sigma) \end{array}$$

Ce qui donne bien $\chi(\sigma)^{-1}\rho_p(\sigma) = \rho_p^\chi(\sigma)$ pour tout $\sigma \in G_{K'}$ □

La courbe à laquelle on s'intéresse est la courbe $E : y^2 + jy = x^3$ (avec j une racine troisième de l'unité). Elle a multiplication complexe par l'ordre maximal de $\mathbb{Q}(j)$ (donné par $j : (x, y) \mapsto (jx, y)$). Son discriminant est égal à $-27j$ ([24, p. 483]). Cette courbe a mauvaise réduction au-dessus de 3 uniquement. Les représentations ρ_p qui vont avec sont abéliennes et ramifiées en 3 et en p [20, thm. 1, p. 493]. On fixe $\pi_3 = j - 1$ comme uniformisante de $\mathbb{Q}_3(j)$

Proposition 17. *Soit p un premier qui est congruent à 1 modulo 3 et congruent à 3 modulo 4. Alors on peut tordre la courbe $E : y^2 + jy = x^3$ par un caractère χ_p tel que l'image de la représentation $\rho_p^{\chi_p}$ ne contienne pas toutes les homothéties.*

Démonstration : On note U_p les unités de $\mathbb{Q}(j) \otimes \mathbb{Q}_p$, considéré comme sous-groupe des idèles $\mathbb{G}_m(\mathbb{A}_{\mathbb{Q}_{(j)}})$ et on commence par regarder l'image de U_3 par les ρ_p. On a $U_3 = \mu_6 \times U_3^{(2)}$ où les racines sixièmes de l'unité μ_6 sont les unités globales μ_6 de $\mathbb{Q}(j)$ et $U_3^{(2)} = \{u \in U_3 : u \equiv 1 \bmod \pi_3^2\}$.

La représentation ρ_3 est ramifié en 3 uniquement et triviale sur les unités globales dans U_3. Pour tout $p \neq 3$, l'application $\rho_p|_{U_3}$ est un caractère η à valeurs dans μ_6 $(= \mu_6 \cap \mathbb{Z}(j))$ et indépendant de p [20, thm. 6, p. 503].

Le corps $\mathbb{Q}(j)$ n'a pas d'extension abélienne non ramifiée non triviale. La courbe E a mauvaise réduction en 3 uniquement et comme elle à multiplication complexe sur

$\mathbb{Q}(j)$, les représentations ρ_p sont abéliennes. On a donc $\rho_p(G_{\mathbb{Q}(j)}) = \rho_p(U_p \times U_3)$. Cette image est contenue dans U_p. Pour tout $p \neq 3$ on sait $\rho_p|_{U_3} = \eta$ et $\rho_p|_{U_p} = \frac{1}{id}$ parce que E a bonne réduction en p [20, cor. 2, p. 513]. De plus ρ_p doit être trivial sur les unités globales μ_6 dans $U_p \times U_3$ (ce qui implique en particulier que η doit être l'identité sur $\mu_6 \subseteq U_3$).

Maintenant on choisit un premier $p \equiv 1 \bmod 3$, c'est à dire un premier qui se décompose dans $\mathbb{Q}(j)$. On écrit $p = p_1 \cdot p_2$ et $U_p = U_{p_1} \times U_{p_2}$. Si de plus on prend $p \equiv 3 \bmod 4$, les composantes 2-primaires des groupes U_{p_1}, U_{p_2} et U_3 sont toutes les trois isomorphes à $\mathbb{F}_2$. On regarde l'application $\rho_p : U_{p_1} \times U_{p_2} \times U_3 \to U_{p_1} \times U_{p_2}$ sur ces composantes 2-primaires et fixe la base naturelle (e_1, e_2, e_3) de $\mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$. Sous cette base $(x_1, x_2, x_3) \mapsto (x_1 + x_3,\ x_2 + x_3)$ est la seule application linéaire qui vérifie $\rho_p|_{U_{p_1} \times U_{p_2}} = \frac{1}{id}$ et $\mu_6 \subseteq \ker \rho_p$.

Finalement on considère le caractère $\chi_p : U_{p_1} \times U_{p_2} \times U_3 \to \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$, $(u_1, u_2, u_3) \mapsto (x_1, x_2, x_3) \mapsto x_1 + x_3$. Cette application est triviale sur les unités globales μ_6. D'après le théorème 5 de [2, chap. X, §2, p. 103] il existe un caractère globale $\chi_p : G_{\mathbb{Q}(j)} \to \{\pm 1\} \subseteq \mathrm{Aut}(E)$ qui prolonge ce caractère. On tord la courbe E par ce caractère pour obtenir une courbe E_{χ_p} qui a mauvaise réduction en p_1. La représentation $\rho_p^{\chi_p}$ de cette courbe est donnée par $\rho_p^{\chi_p} = \frac{\rho_p}{\chi_p}$. Elle est non ramifiée en dehors de $3p$ et si on regarde comme avant les composantes 2-primaires dans l'application $\rho_p^{\chi_p} : U_{p_1} \times U_{p_2} \times U_3 \to U_{p_1} \times U_{p_2}$ on a maintenant $(x_1, x_2, x_3) \mapsto (0, x_1 + x_2)$. L'image de $\rho_p^{\chi_p}$ ne contient plus toutes les homothéties $\mathbb{Z}_p^*$. □

Who's who

G_K	$G(\bar{K}/K)$, le groupe de Galois absolu pour un corps K quelconque	
p	un premier rationnel	$p \geq 7$
F	un corps de nombres	
d	$[F : \mathbb{Q}]$	
c	le plus grand diviseur commun des indices de ramification de F au-dessus de p	
∂	le plus petit multiple commun des indices de ramification de F au-dessus de p	
H_F	le corps de classes de Hilbert de F	
h_F	$[H_F : F]$	
E	une courbe elliptique sans multiplication complexe	E est définie sur F, $\mathrm{End}_{\bar{\mathbb{Q}}}(E) = \mathbb{Z}$
$E(F)$	les points F-rationnels de E	
E_{p^n}	les points de p^n-torsion dans $E(\bar{\mathbb{Q}})$	c'est un $(\mathbb{Z}/p^n\mathbb{Z})$-module libre de rang 2
$T_p(E)$	le module de Tate	un $\mathbb{Z}_p$-module libre de rang 2
$\mathrm{End}_{\overline{\mathbb{Q}}}(E)$	anneau des endomorphismes de E sur $\overline{\mathbb{Q}}$	
v, v_1, …, v_r	les places de F au-dessus de p	
F_{v_j}	le complété de F par rapport à v_j	
K_j	une extension de F_{v_j}	E a réduction semi-stable sur K_j, p. 20
e_j	le degré de ramification de $K_j/\mathbb{Q}_p$	p. 20
$\mathbf{e}$	ppcm $\{e_j\}_{v_j \mid p}$	$\mathbf{e} \mid 12\partial$, si p n'est pas ramifié dans F alors $\mathbf{e} \mid 12$
I_j	le sous-groupe d'inertie de $G(\bar{\mathbb{Q}}_p/K_j)$	p. 20
K	une extension finie de $\mathbb{Q}_p$	E/K a réduction semi-stable, le degré de ramification de K sur F_v divise 12, lemme 19, p. 19
k	le corps résiduel de K	} p. 21
$\tilde{E}/k$	la courbe réduite de E/K	
π	une uniformisante de K	
e	le degré de ramification de $K/\mathbb{Q}_p$	$e < \frac{p-1}{2}$

e_1	voir p. 24	
μ_d	le groupe des racines d-ièmes de l'unité	
K_d	le corps $K(\pi^{\frac{1}{d}})$ avec d premier à p	voir p. 21
K_{nr}, K_t	la plus grande extension non ramifié, respectivement modérément ramifieé, de K	voir p. 21
$\mathcal{O}_K$, $\mathcal{O}_{\bar{K}}$	l'anneau des entiers de K, respectivement de la clôture algébrique $\bar{K}$	voir p. 21
$\mathfrak{m}$, $\bar{\mathfrak{m}}$	l'idéal maximale de $\mathcal{O}_K$ (resp. de $\mathcal{O}_{\bar{K}}$)	voir p. 21
I, I_p	le (pro-p-) groupe d'inertie dans G_K	voir p. 21
I_t	I/I_p	voir p. 21
$\mathfrak{m}_\alpha$, $\mathfrak{m}_\alpha^+$, V_α	voir p. 21	
L	$L = F(E_3)$	E/L a réduction semi-stable, p. 31
δ	$[L : F]$	$\delta \mid 48$, p. 31
$\tilde{X}_j$, $\tilde{Y}$	des droites dans E_p	$\tilde{X}_j$ est stable par l'action du groupe G_{K_j}, p. 31 $\tilde{Y}$ est stable par l'action de G_F, p. 43
X, X_j	des droites dans $T_p(E)$	X_j est stable par l'action de G_{K_j}, on a $X_j/pX_j = \tilde{X}_j$, pp. 31, 29
$\tilde{B}$	un sous-groupe de Borel dans $\mathrm{Gl}_2(\mathbb{F}_p)$	
$L_{\chi'}$, $L_{\chi''}$	voir pp. 44, 45	

Représentations et caractères :

ρ	$: G_F \longrightarrow \mathrm{Aut}(\prod_p T_p) \simeq \prod_p \mathrm{Gl}_2(\mathbb{Z}_p)$	
ρ_p	$: G_F \longrightarrow \mathrm{Aut}(T_p) \simeq \mathrm{Gl}_2(\mathbb{Z}_p)$	
φ_p	$: G_F \longrightarrow \mathrm{Aut}(E_p) \simeq \mathrm{Aut}(T_p/pT_p) \simeq \mathrm{Gl}_2(\mathbb{Z}/p\mathbb{Z})$	
χ_p	$: G_F \to \mathbb{Z}_p^*$	le caractère cyclotomique
θ_{p^n-1}	$: I \to \mu_{p^n-1} = \mathbb{F}_{p^n}^*$	caractère fondamental de niveau n (p. 21)
χ', χ''	$: G_F \to \mathbb{F}_p^*$	voir p. 43

H	$\rho_p(G_K) \subseteq \mathrm{Gl}_2(\mathbb{Z}_p)$	p. 36
$\mathcal{H}$	$\rho_p(G_F) \cap \mathbb{Z}_p^*$	les homothéties contenues dans l'image
$\mathcal{F}$	le groupe formel associé à E/K	p. 22
$[p]$	la multiplication par p selon la loi de groupe formel $\mathcal{F}$	

E_∞	les points de torsion du groupe $\mathcal{F}(\bar{\mathfrak{m}})$	p. 36
T	le module de Tate de $\mathcal{F}(\bar{\mathfrak{m}})$	p. 36
M	$\mathrm{End}_{\mathbb{Z}_p}(T)$	
$\tilde{M}$	$\mathrm{End}_{\mathbb{F}_p}(T/pT)$	
G	$\mathrm{Gl}_2(\mathbb{Z}_p)$	
$G(n)$	$\{g \in \mathrm{Gl}_2(\mathbb{Z}_p) :\ g-1 \in p^n M\}$	
$H(n)$	$H \cap G(n)$	
$\tilde{H}_n$	$H(n)/H(n+1) \simeq$ $\simeq G(K(E_{p^{n+1}})/K(E_{p^n}))$	$\tilde{H}_n \subseteq \tilde{M}$, p. 37
q	$p^{ht\mathcal{F}} = p^2$	
J	$\varphi_p(G_K) \subseteq \mathrm{Aut}_{\mathbb{F}_p}(E_p)$	p. 37
$\{id, \tau\}$	le groupe de Galois $G(\mathbb{F}_q/\mathbb{F}_p)$	
$\tilde{M}_{id}$, $\tilde{M}_\tau$	voir p. 37	
π_n	un point d'ordre exacte p^n	p. 38
K_n	$K(\pi_n)$	

2 Les courbes elliptiques

Maintenant on regarde une courbe elliptique E qui n'a pas multiplication complexe ($\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$). Comme avant on suppose que E est définie sur un corps de nombres F. On s'intéresse aux représentations

$$\begin{array}{ll} \rho: & G_F \longrightarrow \mathrm{Aut}(\prod_p T_p(E)) \simeq \prod_p \mathrm{Gl}_2(\mathbb{Z}_p) \\ \rho_p: & G_F \longrightarrow \mathrm{Aut}(T_p(E)) \simeq \mathrm{Gl}_2(\mathbb{Z}_p) \\ \varphi_p: & G_F \longrightarrow \mathrm{Aut}(E_p) \simeq \mathrm{Aut}(T_p(E)/pT_p(E)) \simeq \mathrm{Gl}_2(\mathbb{Z}/p\mathbb{Z}). \end{array}$$

On note d le degré $[F:\mathbb{Q}]$ et h_F le nombre de classes de F.

On traitera séparément différents cas et obtiendra des résultats légèrement différents sous des hypothèses légèrement différentes selon le cas (voir chap. 2.3). Comme résultat global on a

Théorème 18. *Pour tout $p \geq (48dh_F)^{3(48dh_F)^2}$ qui n'est pas ramifié dans F, soit $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^{12}$, soit le groupe de points de p-torsion E_p a un sous-groupe non trivial rationnel sur F et la courbe E a, par rapport à une place v divisant p, potentiellement bonne réduction de hauteur 2 avec un polygone de Newton qui a deux pentes non nulles distinctes* (*voir p.* 24).

voir théorème 40 et la remarque qui s'en suit.

2.1 Le point de départ : la situation modulo p

On regarde la situation modulo p avant de remonter ces résultats à $\rho_p(G_F)$. Pour l'étude de $\varphi_p(G_F)$ on s'appuie essentiellement sur les travaux de Serre ([16] et surtout [18]).

Avant de décrire les images des sous-groupes d'inertie, on veut s'assurer que E ait réduction semi-stable par rapport à une place considérée. Fixons une place v au-dessus de $p > 3$. Si E n'a pas réduction semi-stable par rapport à cette place on agrandit le corps de base :

Lemme 19. *Pour toute courbe elliptique E, définie sur un corps local F_v de caractéristique résiduelle $p > 3$, il existe une extension K de F_v telle que, sur K, la courbe E a réduction semi-stable et le degré de ramification de K sur F_v divise* 12, *ou, plus précisément, ce degré divise soit* 4 *soit* 6. *Si E a potentiellement mauvaise réduction de type multiplicatif on peut choisir K tel que E soit isomorphe, sur K, à une courbe de Tate E_T.*

Démonstration : Si E n'a pas réduction semi-stable, on fixe une équation de Weierstraß minimale de la forme $E: y^2 = x^3 - 27c_4x - 54c_6$. La courbe E a réduction additive (non semi-stable), ce qui équivaut à $v(\Delta) > 0$ et $v(c_4) > 0$ [23, chap. VII,

§5, prop. 5.1, p. 180]. Comme l'équation est minimale on a soit $v(\Delta) < 12$ soit $v(c_4) < 4$ [23, chap. VII, ex.7.1, p. 186].

La formule $\Delta = \frac{c_4^3 - c_6^2}{1728}$ donne $v(\Delta) \geq \min(3v(c_4),\, 2v(c_6))$ et montre qu'on ne peut pas avoir $v(\Delta) = 1$, donc $v(\Delta) \geq 2$. Soit π une uniformisante de F_v. Si $v(\Delta) = \min(3v(c_4),\, 2v(c_6))$ la courbe a bonne réduction sur le corps $K = F_v(\pi^{\frac{v(\Delta)}{12}})$. Ce corps est de degré divisant soit 6 soit 4 puisque soit 2, soit 3 divise $v(\Delta)$. Après le changement de variables $x = \pi^{\frac{v(\Delta)}{6}} x'$ et $y = \pi^{\frac{v(\Delta)}{4}} y'$ la nouvelle équation de E est $y^2 = x^3 - 27\pi^{\frac{-v(\Delta)}{3}} c_4 x - 54\pi^{\frac{-v(\Delta)}{2}} c_6$ avec $\Delta' = \pi^{-v(\Delta)}\Delta$.

Si $v(\Delta)$ est plus grand que $\min(3v(c_4),\, 2v(c_6))$ on a nécessairement $3v(c_4) = 2v(c_6)$. La courbe a réduction multiplicative sur le corps $K' = F_v(\pi^{\frac{v(c_4)}{4}})$ et après le changement de variables $x = \pi^{\frac{v(c_4)}{2}} x'$ et $y = \pi^{\frac{3v(c_4)}{4}} y'$ [23, chap. III, §1, p. 48, 49]. La courbe E est alors isomorphe à une courbe de Tate E_T. Cet isomorphisme est défini sur une extension K de K' qui est au plus quadratique et non ramifiée [23, app. C, thm. 14.1, p. 357]. □

Pour la suite on fixe ce corps K qu'on vient de trouver. Soient $v_1, \ldots, v_r$ les différentes places de F divisant p et soit F_{v_j} le complété de F par rapport à une de ces places v_j. Si E n'a pas réduction semi-stable sur F_{v_j}, on note K_j cette extension trouvé dans le lemme 19 sur laquelle E a réduction semi-stable. On note e_j le degré de ramification de K_j sur $\mathbb{Q}_p$ et $\mathbf{e}$ le plus petit multiple commun des e_j (correspondants aux $v_j|p$). Le sous-groupe d'inertie de $G(\overline{\mathbb{Q}}_p/K_j)$ sera noté I_j et considéré comme sous-groupe de G_F. Si ∂ est le plus petit multiple commun des indices de ramification de p dans F, le lemme 19 montre en particulier que $\mathbf{e}$ divise 12∂ et $\mathbf{e}$ divise 12 si p n'est pas ramifié dans F. Si E/K_j a mauvaise réduction on suppose que E est une courbe de Tate.

Remarque : Pour chaque place v, on associe à E un groupe formel $\mathcal{F}$ et le polygone de Newton de ce groupe formel [23, chap. IV]. Une fois que E a réduction semi-stable au-dessus de v, ce groupe formel $\mathcal{F}$, et donc son polygone de Newton, ne change plus lorsqu'on agrandit le corps de base [23, prop. 5.4, p. 181]. Ce groupe formel et avec lui le polygone de Newton et le type de réduction semi-stable que a E en une place v ne dépend pas du corps K : supposons que K' est une autre extension finie de F_v sur laquelle E a réduction semi-stable. Alors KK' est une extension finie de K et de K' et le type de réduction que a $E/_{KK'}$ est égal au type de réduction de $E/_K$ et au type de réduction de $E/_{K'}$.

On fait les

Hypothèses globales. *On se donne une courbe elliptique E définie sur un corps de nombres F. On suppose que E n'a multiplication complexe sur aucune extension de F* ($\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$).

On choisit un premier rationnel $p \geq 7$. Pour tous les indices e_j (voir ci-dessus) on suppose $e_j < \frac{p-1}{2}$ et on suppose qu'il en existe un qui est plus petit que $\frac{p-1}{6}$. On

note $\mathbf{e} = \mathrm{ppcm}\,(e_j)$.

En utilisant le §1 de [18] on décrit maintenant l'image des sous-groupes d'inertie par φ_p pour ensuite préciser quel forme a $\varphi_p(G_F)$ en fonction du type de réduction de E.

2.1.1 Bild der Trägheit

Serre considère dans [18] une courbe E définie sur un corps local K. Il fait l'étude de l'image du sous-groupe d'inertie I de G_K sous l'application $\varphi_p : G_K \to \mathrm{Aut}(E_p)$, en fonction du type de réduction de E/K.

Dans notre cas le corps K sera le corps déterminé dans le lemme 19. En particulier E a réduction semi-stable sur K, donc soit bonne réduction de hauteur 1 ou 2, soit mauvaise réduction de type multiplicatif. C'est une extension finie de $\mathbb{Q}_p$. Le groupe de Galois G_K est isomorphe à un sous-groupe ouvert d'un sous-groupe de décomposition de G_F. Le corps résiduel de K est appelé k et est une extension finie de $\mathbb{F}_p$. On dénote par $\mathcal{O}_K$ l'anneau des entiers de K, celui de $\overline{K}$ par $\mathcal{O}_{\overline{K}}$ et par $\mathfrak{m}$, respectivement $\overline{\mathfrak{m}}$, les idéaux maximaux. Lorsque la courbe E est définie et a bonne réduction sur K on note $\widetilde{E}/k$ la courbe réduite. Comme d'habitude, on appelle I le sous-groupe d'inertie de G_K, le p-groupe d'inertie est I_p et $I_t = I/I_p$ est le quotient qui est le groupe d'inertie modérée. L'indice de ramification de K sur $\mathbb{Q}_p$ est noté e et est toujours supposé plus petit que $\frac{p-1}{2}$.

On note K_{nr} la plus grande extension non ramifiée de K et K_t la plus grande extension modérément ramifiée. Pour tout d premier à p le corps K_{nr} contient les racines d-ièmes de l'unité et si π est une uniformisante de K_{nr}, alors K_t est engendré par les extensions $K_d = K_{nr}(\pi^{\frac{1}{d}})$ avec d encore premier à p (comparer [18, §1.3, p. 263]).

Le groupe de Galois de K_d sur K_{nr} s'identifie au groupe μ_d des racines d-ièmes de l'unité par un caractère $\theta_d \colon G(K_d/K_{nr}) \to \mu_d$ qui, pour $d = p^n - 1$, s'identifie à un caractère $\theta_{p^n-1} \colon I_t \to \mu_{p^n-1} \simeq \mathbb{F}_{p^n}^*$ dont le noyau est $G(K_t/K_d)$. On appelle ce caractère θ_{p^n-1} caractère fondamental de niveau n (voir [18, §1.3]).

En fait les caractères θ_d (d toujours premier à p) paramètrent le groupe de caractères $\mathrm{Hom}(I_t, \overline{\mathbb{F}}_p^*)$ [18, §1.7]. Ils vont servir pour décrire l'image de I sous la représentation φ_p.

Dans l'étude de l'image de φ_p on se sert de l'espace suivant (voir [18, §1.8]) : on étend la valuation v de K à la clôture algébrique $\overline{K}$. Son groupe de valeurs $v(\overline{K}^*)$ est égal à $\mathbb{Q}$ et on définit pour tout $\alpha \in \mathbb{Q}$ les ensembles $\mathfrak{m}_\alpha = \{x \in \overline{K} : v(x) \geq \alpha\}$ et $\mathfrak{m}_\alpha^+ = \{x \in \overline{K} : v(x) > \alpha\}$ ainsi que leur quotient $V_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+$. Le quotient V_α est un espace vectoriel de dimension 1 sur le corps résiduel $\overline{k}$ de $\overline{K}$. Le groupe de Galois G_K agit sur V_α naturellement.

Lemme 20. (*a*) *Soit $\sigma \in G_K$. On note $\overline{\sigma}$ son image dans le groupe G_k. L'action de σ sur V_α est $\overline{\sigma}-$linéaire.*

(*b*) *Le sous-groupe d'inertie agit linéairement, le p-groupe I_p agit trivialement sur V_α. Si $\alpha = \frac{a}{d}$ avec a, $d \in \mathbb{Z}$ et $p \nmid d$ alors l'action du groupe I_t sur V_α est donnée par le caractère $\theta_d^a \colon I_t \to \mu_d \subseteq \overline{k}^*$.*

Démonstration : [18, §1.8, Prop. 6 et 7, p. 268]

En outre on a les résultats suivants :

Lemme 21. (*a*) *Le déterminant de la représentation ρ_p est le caractère cyclotomique $\chi_p \colon G_F \to \mathbb{Z}_p^*$.*

(*b*) *Le groupe d'inertie I_t agit sur les racines p-ièmes de l'unité μ_p par la puissance e-ième du caractère fondamental θ_{p-1} (où e est l'indice de ramification de K sur $\mathbb{Q}_p$).*

(*c*) *Si e est premier à p (en particulier si $e < p$), alors l'image du groupe d'inertie I par le caractère cyclotomique $\chi_p \colon G_K \to \mathbb{Z}_p^*$ contient la p-partie $1 + p\mathbb{Z}_p$ de $\mathbb{Z}_p^*$.*

Démonstration : (a) [16, §1.2.2, p. I-4]
(b) [18, §1.8, Prop. 8, p. 269]
(c) L'extension $\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p$ est totalement ramifiée, $\mathbb{Q}_p(\mu_p)/\mathbb{Q}_p$ est modérément ramifiée, $\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p(\mu_p)$ totalement sauvagement ramifiée. Comme e est supposé premier à p, ça implique que $K \cap \mathbb{Q}_p(\mu_{p^\infty}) = K \cap \mathbb{Q}_p(\mu_p)$ et la partie pro-p du groupe d'inertie $I(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, est contenu dans le groupe d'inertie $I(\overline{\mathbb{Q}}_p/K)$. Ce pro-$p$-groupe est surjecté sur $1 + p\mathbb{Z}_p$ par le caractère cyclotomique. □

On considère maintenant la courbe E définie sur le corps K et la représentation $\varphi_p : G_K \to \mathrm{Gl}_2(\mathbb{F}_p)$.

Lemme 22. *Si la courbe elliptique E/K a bonne réduction de hauteur 1 ou mauvaise réduction (de type multiplicatif), alors le $\mathbb{F}_p$-espace vectoriel et Galois-module E_p possède un sous-espace propre, stable par l'action de G_K. Dans ces cas-là, restreint à I, l'application φ_p s'écrit dans la forme $\begin{pmatrix} \theta_{p-1}^e & * \\ & 1 \end{pmatrix}$ par rapport à une base convenable. Son image contient le sous-groupe $\begin{pmatrix} (\mathbb{F}_p^*)^e & \\ & 1 \end{pmatrix}$ (encore par rapport à une base bien choisie). Ce groupe est un sous-groupe d'indice au plus e d'un demi-sous-groupe de Cartan déployé. Son ordre est au moins $\frac{p-1}{e}$.*

Démonstration : [18, §§1.11, 12, pp. 273, 277]

Une courbe E/K a bonne réduction de hauteur 2 si le groupe formel associé à la courbe est de hauteur 2 (comparer [23, chapitre IV]). On notera $\mathcal{F}$ ce groupe formel. Le passage à la courbe réduite $\widetilde{E}$ donne une suite exacte

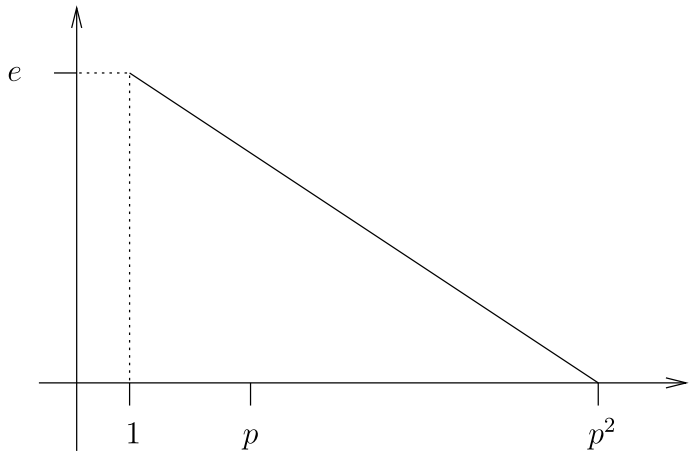
$$0 \to E_1(K) \to E(K) \to \widetilde{E}(k) \to 0.$$

Le noyau $E_1(K)$ de la réduction est isomorphe à $\mathfrak{m}$, muni de la loi de groupe définie par le groupe formel $\mathcal{F}$. D'après [23, VII-2, Prop. 2.2, p. 175] l'isomorphisme $E_1(K) \to \mathfrak{m}$ est donné par les applications suivantes :

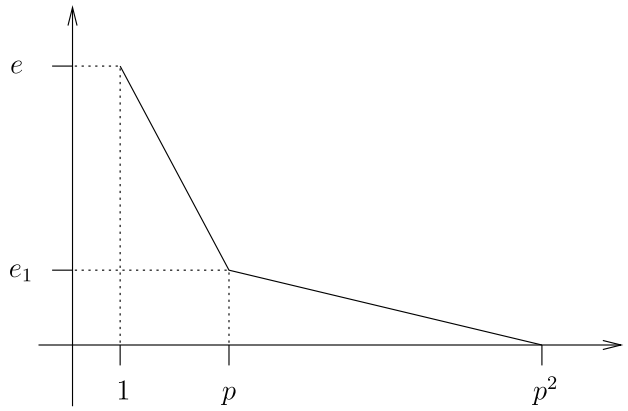
$$\begin{array}{rcl} E_1(K) & \to & \mathfrak{m} \\ (x,\, y) & \mapsto & \dfrac{x}{y} \\ \left(\dfrac{t}{\omega(t)}, \dfrac{-1}{\omega(t)}\right) & \leftarrow\!\shortmid & t \end{array}$$

où $\omega(t)$ est une série formelle à coefficients dans $\mathcal{O}_K$ [23, p. 175]. Comme E/K a réduction semi-stable, une équation de Weierstraß minimale de E/K reste minimale sur toute extension K' de K, le groupe formel $\mathcal{F}$ associé à E/K' est le même que celui associé à E/K. Par conséquence, les applications données définissent un isomorphisme $E_1(\overline{K}) \to \overline{\mathfrak{m}}$, avec sur $\overline{\mathfrak{m}}$ la loi de groupe définie par $\mathcal{F}$. Si le groupe formel $\mathcal{F}$ est de hauteur 2 il y a p^2 points de $[p]$-torsion dans $\overline{\mathfrak{m}}$ (où $[p]$ est la multiplication par p selon la loi de groupe formel $\mathcal{F}$), et tous les points de p-torsion de la courbe $E(\overline{K})$ sont contenus dans le noyau $E_1(\overline{K})$ [9, thm. 1, chap. IV§2, p. 107]. On peut identifier E_p au noyau de la multiplication par $[p]$ dans $\overline{\mathfrak{m}}$. En regardant les applications donnant l'isomorphisme entre $E_1(\overline{K})$ et $\overline{\mathfrak{m}}$ on voit que l'action de Galois commute avec cet isomorphisme. Puisque K est complet, les corps engendrés par les coordonnées des points de p-torsion dans E_p sont les mêmes que ceux engendrés par les points de $[p]$-torsion dans $\overline{\mathfrak{m}}$. On va dans la suite confondre ces deux ensembles de points de p-torsion et l'appeler toujours E_p.

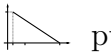
Si E/K a bonne réduction de hauteur 2, le Galois-module E_p peut être simple ou avoir un sous-espace stable selon la forme du polygone de Newton. Concrètement, on considère la loi de groupe formel $\mathcal{F}$ donné par E et le polygone de Newton associé à la multiplication par $[p]$. Ce polygone de Newton peut être de la forme



ou de la forme



Dans le deuxième cas E_p a un sous-espace stable par l'action de G_K [18, §1.10].

Remarque : Si p n'est pas ramifié dans K (i.e. $e = 1$) et E/K a bonne réduction de hauteur 2, alors le polygone de Newton est toujours de la forme  puisque la valuation e_1 du p-ième coefficient de $[p](X)$ ne peut pas être plus petit que $e = 1$.

Lemme 23. *Supposons que la courbe elliptique E/K a bonne réduction de hauteur 2 et qu'on a un polygone de Newton de la forme*  *. Alors E_p se plonge dans le $\overline{k}$-espace vectoriel V_α avec $\alpha = \frac{e}{p^2-1}$. Le p-groupe d'inertie I_p opère trivialement sur E_p, le quotient $I/I_p = I_t$ opère par le caractère $\theta^e_{p^2-1} \colon I_t \to \mathbb{F}^*_{p^2}$ qui est la puissance e-ième du caractère fondamental de niveau 2.*

L'image de I par φ_p est un sous-groupe d'indice au plus e d'un sous-groupe de Cartan non déployé de $Gl_2(\mathbb{F}_p)$. Son ordre divise $p^2 - 1$ et est au moins $\frac{p^2-1}{e}$.

Démonstration : (Comparer [18, §1.9, p. 270]) Vu le polygone de Newton, on sait que tous les éléments $t \in E_p$ avec $t \neq 0$ ont même valuation $v(t) = \frac{e}{p^2-1} = \alpha$ [18, §1.10, p. 272]. Donc $E_p \subseteq \mathfrak{m}_\alpha$ et pour $s, t \in E_p$ on a $\mathcal{F}(s, t) \equiv s + t \mod \mathfrak{m}^+_\alpha$. Cela entraîne qu'on a un homomorphisme injectif qui plonge E_p dans V_α et qui commute avec l'action de G_K. On sait que l'action d'un élément $\sigma \in G_K$ sur V_α est $\overline{\sigma}-$linéaire (lemme 20) et on connaît l'action de I sur V_α. Notamment I agit par le caractère $\theta^e_{p^2-1} \colon I \to \mathbb{F}^*_{p^2}$. L'image de I sous ce caractère est un sous-groupe de $\mathbb{F}^*_{p^2}$ dont l'indice est au plus e, son ordre est au moins $\frac{p^2-1}{e}$. L'image $\varphi_p(I)$ est donc un sous-groupe d'un sous-groupe de Cartan, non déployé puisque $\varphi_p(I)$ est cyclique d'ordre plus grand que $p - 1$. □

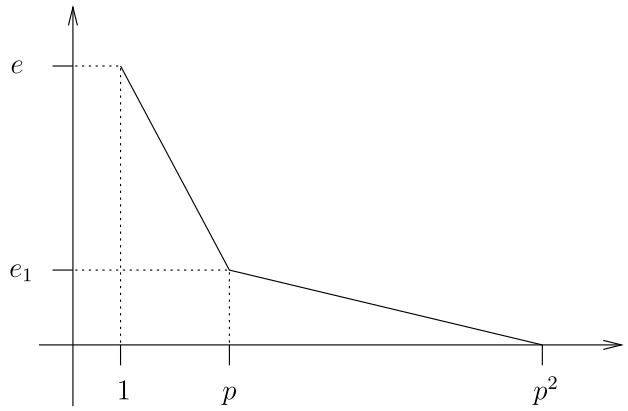
Lemme 24. *Supposons que le groupe formel $\mathcal{F}$, associé à la courbe elliptique E/K est de hauteur 2 et notons e_1 la valuation du p-ième coefficient de la série formelle correspondante à $[p]$. Si le polygone de Newton de la multiplication par $[p]$ est de la forme*  *, alors E_p a un sous-espace $\tilde{X}$ (de dimension 1) dont les éléments sont de valuation $\alpha_1 = \frac{e-e_1}{p-1}$. Les autres éléments de E_p sont de valuation $\alpha_2 = \frac{e_1}{p(p-1)} < \alpha_1$. Le groupe d'inertie (modéré) agit sur $\tilde{X}$ par la puissance $(e - e_1)$-ième du caractère fondamental θ_{p-1}, sur $E_p/\tilde{X}$ il agit par la puissance e_1-ième du même*

caractère. Par rapport à une base convenable φ_p, restreint à I, est de la forme $\begin{pmatrix} \theta_{p-1}^{e-e_1} & * \\ & \theta_{p-1}^{e_1} \end{pmatrix}$.

Démonstration : [18, §1.10, p. 272]

Lemme 25. *Dans la situation du lemme* 24 *(E/K a bonne réduction de hauteur* 2 *avec un polygone de Newton de la forme*  *), si le degré de ramification e est plus petit que p, l'ordre de $\varphi_p(I)$ (et celle de $\varphi_p(G_F)$) est divisible par p.*

Démonstration : L'image $\varphi_p(I)$, qui est un sous-groupe de $\varphi_p(G_F)$, est isomorphe au sous-groupe d'inertie de $G(K(E_p)/K)$. On verra que l'indice de ramification de $K(E_p)$ sur K, et donc l'ordre du groupe d'inertie $I_{K(E_p)/K}$, est divisible par p. Pour cela on regarde le polygone de Newton de $\mathcal{F}$, qui est de la forme suivante :



D'après [4] les points de p-torsion P de E qui ne sont pas contenus dans $\tilde{X}$ sont de valuation $v_K(P) = \frac{e_1}{p(p-1)}$ (la droite $\tilde{X}$ consiste de 0 et des $p-1$ points Q de valuation $v_K(Q) = \frac{e-e_1}{p-1}$. Ces points Q correspondent au segment s_1 qui est de pente $-\frac{e-e_1}{p-1}$. Au segment s_2, de pente $-\frac{e_1}{p(p-1)}$, correspondent $p(p-1)$ points P de valuation $\frac{e_1}{p(p-1)}$). Comme p ne divise pas e_1 (qui est plus petit que e), le degré de ramification de $K(E_p)$ sur K doit être divisible par p. La même chose est vraie pour l'ordre de $\varphi_p(G_F)$, car $\varphi_p(I) \simeq I_{K(E_p)/K}$ est un sous-groupe de ce groupe. □

2.1.2 Sous-groupes de $\mathrm{Gl}_2(\mathbb{F}_p)$ et type de réduction de E

Utilisant le §2 de [18], on va maintenant préciser quels sous-groupes de $\mathrm{Gl}_2(\mathbb{F}_p)$ peuvent apparaître en tant qu'image de φ_p.

Lemme 26. *Soit G un sous-groupe de $\mathrm{Gl}_2(\mathbb{F}_p)$. On suppose, soit que l'ordre de G est divisible par p, soit que G contient un sous-groupe C qui est soit un sous-groupe d'ordre au moins* 6 *d'un demi-sous-groupe de Cartan déployé, soit un sous-groupe d'ordre au moins $6(p-1)$ d'un sous-groupe de Cartan non déployé, alors*
– *ou bien G contient $\mathrm{Sl}_2(\mathbb{F}_p)$*

– *ou bien G est contenu dans un sous-groupe de Borel B*
– *ou bien G est contenu dans le normalisateur d'un sous-groupe de Cartan*
Si G ne contient pas $Sl_2(\mathbb{F}_p)$ et p divise l'ordre de G, alors G est contenu dans un sous-groupe de Borel.

Démonstration : Lorsque l'ordre de G est divisible par p, le résultat est donné par [18, prop. 15, p. 280].

Si l'ordre de G est premier à p, on regarde l'image H de G dans $\mathrm{PGl}_2(\mathbb{F}_p)$. Le §2.6 de [18] dit que dans ce cas il y a les trois possibilités suivantes :
– soit H est un groupe cyclique et G est contenu dans un sous-groupe de Cartan de $\mathrm{Gl}_2(\mathbb{F}_p)$
– soit H est diédral et G est contenu dans le normalisateur d'un sous-groupe de Cartan
– soit H est isomorphe à $\mathfrak{A}_4$, $\mathfrak{S}_4$ ou $\mathfrak{A}_5$. Les éléments de H sont alors d'ordre au plus 5.
Le dernier cas ne peut pas se produire puisque par hypothèse l'image de C dans $\mathrm{PGl}_2(\mathbb{F}_p)$ contient un sous-groupe cyclique d'ordre au moins 6. □

Tenant compte des résultats sur l'image de I sous φ_p, ce lemme s'applique notamment à $\varphi_p(G_F)$:

Lemme 27. *Sous les hypothèses globales (p. 20) le sous-groupe $\varphi_p(G_F)$ de $\mathrm{Gl}_2(\mathbb{F}_p)$ vérifie une des conditions suivantes :*
– *soit $\varphi_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{F}_p)$*
– *soit il est contenu dans un sous-groupe de Borel B*
– *soit il est contenu dans le normalisateur d'un sous-groupe de Cartan déployé mais pas dans un sous-groupe de Cartan*
– *soit il est contenu dans le normalisateur d'un sous-groupe de Cartan non déployé*
Si la courbe E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  *, alors soit $\varphi_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{F}_p)$, soit il est contenu dans un sous-groupe de Borel.*

Démonstration : Sauf éventuellement dans le cas décrit dans le lemme 24 (bonne réduction de hauteur 2 avec un polygone de Newton de la forme ), les lemmes 22 et 23 garantissent l'existence d'un sous-groupe convenable pour appliquer le lemme 26 (par les hypothèses globales on a $\frac{p-1}{e} > 6$ pour au moins une place au-dessus de p, voir p. 20).

Si la courbe E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  (le cas du lemme 24) l'ordre du groupe $\varphi_p(G_F)$ est divisible par p (lemme 25) et le lemme 26 implique que $\varphi_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{F}_p)$ ou est contenu dans un sous-groupe de Borel. □

Remarque : Si $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan déployé, alors il a un sous-groupe d'indice deux qui est contenu dans ce sous-groupe de Cartan et donc aussi dans un sous-groupe de Borel.

Lemme 28. *Si $\varphi_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{F}_p)$, alors $\rho_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{Z}_p)$ et les homothéties $(\mathbb{Z}_p^*)^c$ avec c le plus grand diviseur commun des indices de ramification de F au-dessus de p.*

Démonstration : Comme $\varphi_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{F}_p)$, le lemme 3 de [16, IV-3.4, p. IV-23] dit que $\rho_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{Z}_p) = \ker(\det)$.

D'après [16, 1.2.2, p. I-4], le déterminant de la représentation ρ_p est le caractère cyclotomique $\chi_p : G_F \to \mathbb{Z}_p^*$, donné par l'action du groupe de Galois G_F sur les racines p-ièmes de l'unité. L'indice de $\chi_p(G_F)$ dans $\mathbb{Z}_p^*$ est au plus c. Cela implique que $(\mathbb{Z}_p^*)^c \subseteq \rho_p(G_F)$. □

Lemme 29. *Soit C' un sous-groupe d'un sous-groupe de Cartan non déployé. On suppose que l'image de C' dans $\mathrm{PGl}_2(\mathbb{F}_p)$ est d'ordre au moins 3. Alors C' n'est pas contenu dans le normalisateur $N(C)$ d'un sous-groupe de Cartan déployé, ni dans un sous-groupe de Borel.*

Démonstration : L'image d'un sous-groupe de Cartan non déployé dans $\mathrm{PGl}_2(\mathbb{F}_p)$ est cyclique d'ordre $p+1$. L'image du normalisateur d'un sous-groupe de Cartan déployé est diédrale. Il contient un sous-groupe cyclique d'ordre $p-1$, tous les autres éléments sont d'ordre 2. L'image de C' dans $\mathrm{PGl}_2(\mathbb{F}_p)$ est donc d'ordre divisant $p+1$ et strictement plus grand que 2. Comme 2 est le seul diviseur commun entre $p+1$ et $(p-1)$, le groupe C' ne peut pas être contenu dans $N(C)$. L'intersection entre un sous-groupe de Cartan et un sous-groupe de Borel B est forcément contenu dans un sous-groupe de Cartan déployé puisque B fixe une droite. □

Lemme 30. *Soit $C' \subseteq \mathrm{Gl}_2(\mathbb{F}_p)$ un sous-groupe d'ordre strictement plus grand que 2 d'un demi-sous-groupe de Cartan déployé. Un tel groupe n'est pas contenu dans le normalisateur $N(C)$ d'un sous-groupe de Cartan non déployé.*

Démonstration : L'image de C' dans $\mathrm{PGl}_2(\mathbb{F}_p)$ est cyclique, son ordre divise $p-1$ et est strictement plus grand que 2 alors que les éléments de l'image de $N(C)$ dans $\mathrm{PGl}_2(\mathbb{F}_p)$ sont d'ordre divisant $(p+1)$. Ça implique que C' ne peut pas être contenu dans $N(C)$. □

Revenons à notre courbe elliptique E, définie sur un corps de nombres F. Il y a plusieurs places $v_1, \ldots, v_r$ de F au-dessus d'un premier p et E peut se réduire différemment selon la place choisie. Pour chaque place $v_j | p$ on considère le groupe d'inertie I_j défini au début (p. 20).

Lemme 31. *Supposons les hypothèses globales (p. 20).*

(a) *Si $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel, alors E_p possède un sous-espace stable par l'action de Galois. Dans ce cas il ne peut pas y avoir de place v, au-dessus de p, telle que, par rapport à cette place, E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme*  .

(*b*) *Si $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan déployé mais pas dans le sous-groupe de Cartan, alors potentiellement E a bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif par rapport à toutes les places divisant p.*

(*c*) *Le cas que $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan non déployé ne se produit que si E a potentiellement bonne réduction de hauteur 2 et le polygone de Newton est de la forme*  *pour toutes les places au-dessus de p.*

Démonstration : S'il existe une place une place $v|p$ telle que E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  , alors les lemmes 23 et 29 impliquent que $\varphi_p(G_F)$ n'est pas contenu dans un sous-groupe de Borel ni dans le normalisateur d'un sous-groupe de Cartan déployé (par les hypothèses globales on a $\frac{p^2-1}{e} > 2(p+1)$).

Le lemme 25 implique que l'ordre de $\varphi_p(G_F)$ est divisible par p si E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  pour une place $v|p$. L'ordre du normalisateur d'un sous-groupe de Cartan étant égal à $2(p^2-1)$ ou $2(p-1)^2$, l'image $\varphi_p(G_F)$ ne peut pas être contenue dans un tel sous-groupe dans ce cas.

Finalement les lemmes 22 et 30 impliquent que E a potentiellement bonne réduction de hauteur 2 par rapport a toute place $v|p$ si $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan non déployé (on a $\frac{p-1}{e} > 2$ par les hypothèses globales). Comme on vient de voir, le polygone de Newton doit alors être de la forme  . □

Lemme 32. *Supposons que tous les indices e_j (voir p. 20) soient strictement plus petits que $\frac{p-1}{2}$. Si $\varphi_p(G_F)$ est contenu dans le normalisateur $N(C)$ d'un sous-groupe de Cartan C, alors toutes les images $\varphi_p(I_j)$ (voir p. 20 pour les I_j) sont contenues dans ce sous-groupe de Cartan C.*

Démonstration : Par rapport aux places divisant p, la courbe E ne peut pas avoir potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  parce que l'ordre de $N(C)$ n'est pas divisible par p (lemme 25). Pour la même raison, si E a potentiellement bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif, le lemme 22 implique que $\varphi_p(I_j)$ est contenu dans un demi-sous-groupe de Cartan déployé. Maintenant soient $\tilde{C}'$, $\tilde{C}$ et $\tilde{N}$ les images de $\varphi_p(I_j)$, C, et $N(C)$ dans $\mathrm{PGl}_2(\mathbb{F}_p)$. Les lemmes 22 et 23 impliquent que $\tilde{C}'$ est cyclique d'ordre strictement plus grand que 2 (on suppose $e < \frac{p-1}{2}$). Le groupe $\tilde{N}$ est diédral, tous ses éléments sont soit contenus dans $\tilde{C}$, soit d'ordre 2. Si σ est un générateur de $\tilde{C}'$ il est contenu dans $\tilde{C}$ parce que autrement il ne pourrait pas être d'ordre strictement plus grand que 2. Ça implique $\varphi_p(I_j) \subseteq C$. □

2.2 Weitere Zutaten

2.2.1 Dies und das

On utilisera les résultats suivants, ainsi que des travaux de Fontaine ([7]) qui seront explicités dans le chapitre 2.5.

Théorème 33 (Merel, [14]). *Soit E une courbe elliptique, définie sur un corps de nombres F de degré $d > 1$ sur $\mathbb{Q}$. Si $E(F)$ possède un point d'ordre premier p, on a $p < d^{3d^2}$.*

Théorème 34 (Mazur, [13]). *Soit E une courbe elliptique définie sur $\mathbb{Q}$. Si E admet une p-isogénie rationnelle sur $\mathbb{Q}$, alors le premier p est contenu dans l'ensemble* $\{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$.

Théorème 35 (Zassenhaus, [10] §18.1.2.3, p. 126). *Soit N un sous-groupe normal d'un groupe pro-fini G, tel que l'ordre de N est premier à l'ordre de G/N (si N contient une partie pro-p non-triviale, alors la p-partie de G/N est triviale et vice versa). Alors il existe dans G un complément de N et tous les compléments sont conjugués.*

2.2.2 Sous-groupes de Borel

Lemme 36. *Soit E une courbe elliptique définie sur une extension finie K de $\mathbb{Q}_p$ qui est ramifié d'indice $e < p$. Si E/K a bonne réduction de hauteur* 1*, les points de torsion qui sont contenus dans le noyau de la réduction $E(\overline{K}) \to \tilde{E}(\overline{k})$ définissent un sous-module X de rang* 1 *qui est un facteur directe de $T_p(E)$. Ce sous-module X est stable par l'action de G_K, l'image $\rho_p(G_K)$ est contenue dans le sous-groupe de Borel de $\mathrm{Aut}(T_p(E))$ qui correspond à la droite X. Si on choisit un premier vecteur de base dans ce sous-module X, alors l'action du groupe d'inertie $I \subseteq G_K$ sur le module de Tate $T_p(E)$ est donnée par des matrices de la forme $\left(\begin{smallmatrix} \chi_p & * \\ & 1 \end{smallmatrix}\right)$ où χ_p est la restriction du caractère cyclotomique $\chi_p : G_K \to \mathbb{Z}_p^*$. L'image du caractère cyclotomique $\chi_p(I)$ est d'indice au plus e dans $\mathbb{Z}_p^*$.*

Démonstration : Comme E a bonne réduction de hauteur 1, on a pour chaque entier $r \in \mathbb{N}$ une suite exacte

$$0 \to X_{p^r} \to E_{p^r} \to \tilde{E}_{p^r} \to 0 \tag{1}$$

avec E_{p^r} l'ensemble des points de p^r-torsion dans $E(\overline{K})$ ainsi que $\tilde{E}_{p^r}$ sont les points de p^r-torsion de la courbe réduite $\tilde{E}(\overline{\mathbb{F}}_p)$ et X_{p^r} est le noyau, dans E_{p^r}, de cette réduction. L'ordre de $\tilde{E}_{p^r}$ est égal a p^r et donc le même est vrai pour X_{p^r} [23, thm. V.3.1, p. 137]. Pour tout $r \in \mathbb{N}$, l'action du groupe de Galois G_K laisse la droite X_{p^r} stable.

En passant à la limite projective on obtient une suite exacte

$$0 \to T_p(X) \to T_p(E) \to T_p(\tilde{E}) \to 0 \tag{2}$$

avec $T_p(X) = \varprojlim X_{p^r}$. Puisque $|X_p| = p$ on peut choisir une base (e_1, e_2) de $T_p(E)$ tel que $T_p(X) = \mathbb{Z}_p e_1$. Par rapport à cette base l'image de G_K dans $\mathrm{Aut}(E_p) \simeq \mathrm{Gl}_2(\mathbb{Z}_p)$ est contenue dans le sous-groupe de Borel $\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)$.

Le sous-groupe $I \subseteq G_K$ opère sur $T_p(X)$ et sur $T_p(\tilde{E}) \simeq T_p(E)/T_p(X)$ par deux caractères χ_X et $\chi_Y : I \longrightarrow \mathbb{Z}_p^*$. Comme l'inertie I opère trivialement sur $T_p(\tilde{E})$ le caractère χ_Y doit être trivial. D'autre part le déterminant de notre représentation est égal au caractère cyclotomique χ_p (lemme 21(a)). On a donc $\chi_X = \chi_p$ et l'image de I est de la forme $\left(\begin{smallmatrix} \chi_p & * \\ & 1 \end{smallmatrix}\right)$. D'après le lemme 21 la p-partie $1 + p\mathbb{Z}_p$ de $\mathbb{Z}_p^*$ est contenue dans $\chi_p(I)$. Le même lemme nous dit que, modulo p, le caractère cyclotomique $\chi_p|_I$ est égal à θ_{p-1}^e dont l'image est d'indice au plus e dans $\mathbb{F}_p^*$. On en conclut que l'indice de $\chi_p(I)$ dans $\mathbb{Z}_p^*$ est également au plus e. □

Maintenant on regarde le cas d'une courbe E qui a potentiellement mauvaise réduction de type multiplicatif par rapport à une place v.

La situation est tout à fait analogue au cas de bonne réduction de hauteur 1 décrit dans le lemme 36 :

Lemme 37. *Soit E une courbe elliptique définie sur une extension finie K de $\mathbb{Q}_p$ qui est ramifié d'indice $e < p$. Si E/K est isomorphe à une courbe de Tate (et donc a mauvaise réduction de type multiplicatif) les racines de l'unité μ_{p^n} contenues dans E_{p^n} définissent un sous-module X de rang 1 qui est un facteur directe de $T_p(E)$. Ce sous-module X est stable par l'action de G_K. Si on choisit un premier vecteur de base dans ce sous-module X, alors l'action du groupe d'inertie $I \subseteq G_K$ sur le module de Tate $T_p(E)$ est donnée par des matrices de la forme $\left(\begin{smallmatrix} \chi_p & * \\ & 1 \end{smallmatrix}\right)$ où χ_p est la restriction du caractère cyclotomique $\chi_p : G_K \to \mathbb{Z}_p^*$. L'indice de $\chi_p(I)$ dans $\mathbb{Z}_p^*$ est au plus e.*

Démonstration : Si E_{p^r} dénote encore l'ensemble des points de p^r-torsion et μ_{p^r} les p^r-ièmes racines de l'unité, alors on a les suites exactes suivantes [16, A.1.2, p. IV-31]

$$0 \to \mu_{p^r} \to E_{p^r} \to \mathbb{Z}/p^r\mathbb{Z} \to 0$$

et

$$0 \to T_p(\mu) \to T_p(E) \to \mathbb{Z}_p \to 0$$

qui prennent la place des suites (1) et (2) qu'on a lorsque E a bonne réduction de hauteur 1 (p.. 29).

Le groupe de Galois G_K, et son sous-groupe d'inertie I en particulier, agit sur les racines de l'unité par le caractère cyclotomique χ_p et trivialement sur $\mathbb{Z}/p^r\mathbb{Z}$, respectivement sur $\mathbb{Z}_p$. Les racines de l'unité forment un sous-espace stable par l'action de Galois.

L'image $\rho_p(G_K)$ est donc contenue dans le sous-groupe de Borel correspondant à la droite $T_p(\mu)$ dans $T_p(E)$. Dans une base adaptée cette image est de la forme $\left(\begin{smallmatrix}\chi_p & * \\ & 1\end{smallmatrix}\right)$ comme dans le cas de bonne réduction de hauteur 1. □

Remarque : On vient de voir que pour toute place v_j de F, par rapport à laquelle E a potentiellement bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif, l'image $\rho_p(G_{K_j})$ est contenue dans un sous-groupe de Borel de $\mathrm{Gl}_2(\mathbb{Z}_p)$ aussi bien que $\varphi_p(G_{K_j})$ est contenu dans un sous-groupe de Borel de $\mathrm{Gl}_2(\mathbb{F}_p)$ [18, §1.11(1), p. 273]. Les sous-espaces propres correspondant aux caractère cyclotomique χ_p sont stables par ces groupes de Borel seront notés X_j et $\tilde{X_j} = X_j/pX_j$.

2.2.3 Réduction semi-stable

Lemme 38. *Soit E une courbe elliptique définie sur un corps de nombres F. Sur le corps $L = F(E_3)$ la courbe E a réduction semi-stable partout. Le degré $[L : F]$ divise $48 = |\mathrm{Gl}_2(\mathbb{F}_3)|$. Si E a potentiellement mauvaise réduction de type multiplicatif, alors elle est isomorphe, sur L, à une courbe de Tate.*

Démonstration : Si E a potentiellement bonne réduction en une place w, c'est le lemme 8.

Supposons donc que E a potentiellement réduction multiplicative en une place w de L et soit K le complété de L par rapport à w. Dans ce cas le j-invariant de E est de valuation négative et la courbe E est un twist d'une courbe de Tate E_q, avec $q \in K^*$ [16, A1.1, p. IV-30]. Un twist d'une courbe elliptique E_q correspond à un caractère $\chi : G_K \to \mathrm{Aut}(E_q) = \{\pm 1\}$, si ce caractère est trivial, la courbe E est isomorphe à E_q sur K et elle a réduction semi-stable déjà sur L [23, chap. X§2, p. 284]. Le caractère χ est donné de la façon suivante : il existe un isomorphisme $\Phi : E \to E_q$, défini sur une extension finie de K. A chaque $\sigma \in G_K$ on associe l'automorphisme $\Phi^\sigma \circ \Phi^{-1}$ de E_q. On regarde l'action de cet automorphisme sur les points de 3-torsion : si $P \in E_q(\overline{K})$ est un point de 3-torsion, sa préimage $\Phi^{-1}(P)$ est un point de 3-torsion de E et, par définition de L, il est rationnel sur K, on a $(\Phi^{-1}(P))^\sigma = \Phi^{-1}(P)$ pour tout $\sigma \in G_K$. Ça donne

$$\chi(\sigma).P = \Phi^\sigma(\Phi^{-1}(P)) = \Phi^\sigma((\Phi^{-1}(P))^\sigma) = (\Phi(\Phi^{-1}(P)))^\sigma = P^\sigma,$$

c'est à dire $\chi(\sigma) = -1$ implique $P^\sigma = -P$ pour tout les points de 3-torsion de E_q. Regardons les points de 3-torsion de E_q : d'après [16, A1.2, p. IV-31] on a une suite exacte de G_K-modules

$$1 \to \mu_3 \to E_3 \to \mathbb{Z}/3\mathbb{Z} \to 0,$$

G_K agissant trivialement sur $\mathbb{Z}/3\mathbb{Z}$. Mais alors on ne peut pas avoir $P^\sigma = -P$ pour un point $P \in E_3$ dont l'image dans $\mathbb{Z}/3\mathbb{Z}$ est différent de 0. Ça veut dire que le caractère $\chi : G_K \to \{\pm 1\}$ doit être trivial et E est isomorphe à E_q sur K déjà. □

2.3 Zu zeigen

On suppose toujours les

Hypothèses globales. *On se donne une courbe elliptique E définie sur un corps de nombres F. On suppose que E n'a multiplication complexe sur aucune extension de F* ($\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$).

On choisit un premier rationnel $p \geq 7$. Pour tous les indices e_j (voir p. 20) on suppose $e_j < \frac{p-1}{2}$ et on suppose qu'il en existe un qui est plus petit que $\frac{p-1}{6}$. On note $\mathbf{e} = \mathrm{ppcm}\,(e_j)$.

On note d le degré $[F : \mathbb{Q}]$ et h_F le nombre de classes de F.

Remarque : Tous les indices e_j divisent $12d$.

Une fois fixé un premier $p \geq 7$, on regarde les places au-dessus de p et le type de réduction que a E par rapport à ces places. On traite séparément les cas suivants :

(a) il existe une place $v|p$ par rapport à laquelle E a potentiellement bonne réduction de hauteur 2 et le polygone de Newton associé est de la forme 

(b) E a potentiellement bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif par rapport à toutes les places $v|p$

(c) il existe une place pour laquelle E a potentiellement bonne réduction de hauteur 2 et dont le polygone de Newton a la forme 

On obtient des résultats légèrement différents sous des hypothèses légèrement différentes selon le cas :

Théorème 39. *Si le premier p est plus grand que $(48dh_F)^{3(48dh_F)^2}$ et non ramifié dans $L = F(E_3)$, alors l'image $\rho_p(G_F)$ contient les homothéties $\mathbb{Z}_p^*$.*

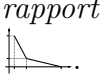
Démonstration : On remarque d'abord que les hypothèses globales sont vérifiées pour tout $p > (48dh_F)^{3(48dh_F)^2}$. Le lemme 27 implique que le groupe $\varphi_p(G_F)$ peut soit contenir $\mathrm{Sl}_2(\mathbb{F}_p)$, soit il est contenu dans un sous-groupe de Borel, dans le normalisateur d'un sous-groupe de Cartan déployé ou dans le normalisateur d'un sous-groupe de Cartan non déployé. Dans le premier cas le résultat est donné par le lemme 28. Dans le dernier cas la courbe E a potentiellement bonne réduction de hauteur 2 au dessus de p et le polygone de Newton est de la forme  (lemme 31). Le résultat sera alors établie par le théorème 45. Lorsque $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan déployé et pas dans un sous-groupe de Borel le résultat sera donné par le théorème 60. Reste le cas que $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel. Sur $F(E_3)$ la courbe E a réduction semi-stable (lemme 38). Comme p est supposé non ramifié dans $F(E_3)$ la courbe E ne peut pas avoir bonne réduction de hauteur 2 dans ce cas (lemme 31

et la remarque p. 24). Le théorème 52 et le corollaire 53 donneront alors le résultat souhaité.

Théorème 40. *Si les degrés de ramification e_j des corps K_j (voir p. 20) vérifient les hypothèses globales ci-dessus et divisent p^2-1, alors il y a les possibilités suivantes :*

(*a*) *soit le sous-groupe $\mathcal{H} = \rho_p(G_F) \cap \mathbb{Z}_p^*$ des homothéties dans l'image est un sous-groupe d'indice au plus* $\mathbf{e}$ *dans le groupe des homothéties.*

(*b*) *soit E_p a un sous-groupe (non trivial) rationnel sur F et $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel de $\mathrm{Gl}_2(\mathbb{F}_p)$.*

Pour $p > (48dh_F)^{3(48dh_F)^2}$ le deuxième cas peut se produire uniquement si E a potentiellement bonne réduction de hauteur 2 par rapport à une place v divisant p et le polygone de Newton associé est de la forme  .

Remarque : L'hypothèse que les degrés de ramification e_j divisent p^2-1 est toujours vérifié lorsque p n'est pas ramifié dans F (remarque p. 36). C'est d'ailleurs dans le lemme 49 que joue cette hypothèse.

Démonstration : Comme dans le cas du théorème 39, le groupe $\varphi_p(G_F)$ peut soit contenir $\mathrm{Sl}_2(\mathbb{F}_p)$, soit il est contenu dans un sous-groupe de Borel ou dans le normalisateur d'un sous-groupe de Cartan, le premier cas étant réglé par le lemme 28. Le dernier cas se traite également comme avant : si $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan non déployé le lemme 31 implique qu'on pourra appliquer le théorème 45 qui donnera le résultat. Autrement on appliquera le théorème 60.

Si finalement $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel, alors E a soit potentiellement bonne réduction de hauteur 1, mauvaise réduction de type multiplicatif ou bonne réduction de hauteur 2 avec un polygone de Newton de la forme  . Lorsque par rapport à toute place divisant p la courbe E a potentiellement bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif le résultat est donné par le théorème 52 et le corollaire 53. Si par rapport à une place divisant p la courbe E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  , alors soit $\varphi_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{F}_p)$ et $\rho_p(G_F)$ contient $(\mathbb{Z}_p^*)^{\mathbf{e}}$ (lemme 28), soit $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel (lemme 27). Dans ce dernier cas le groupe E_p a un sous-groupe rationnel sur F.

Corollaire 41. *Si la courbe elliptique E est définie sur $\mathbb{Q}$, alors pour tout $p > 163$ l'image $\rho_p(G_{\mathbb{Q}})$ contient les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$.*

C'est le lemme 61

Théorème 42. *On suppose $p > 2$ et qu'il existe une place v_j au-dessus de p par rapport à laquelle la courbe elliptique E a potentiellement bonne réduction de*

hauteur 2 *et telle que le polygone de Newton correspondant est de la forme*  . *Si de plus l'indice de ramification* e_j *est plus petit que* $p-1$ *et divise* p^2-1, *alors* $\rho_p(G_F)$ *contient un sous-groupe d'indice* e_j *d'un sous-groupe de Cartan non déployé. En particulier il contient les homothéties* $(\mathbb{Z}_p^*)^{e_j}$.

voir chapitre 2.5, théorème 45

Théorème 43. *Si les degrés de ramification* e_j *(voir p. 20) vérifient les hypothèses globales (p. 20) et la courbe elliptique* $E/F(E_3)$ *n'a bonne réduction de hauteur* 2 *pour aucune place divisant p alors*

(*a*) *soit le sous-groupe* $\mathcal{H} = \rho_p(G_F) \cap \mathbb{Z}_p^*$ *des homothéties dans l'image est un sous-groupe d'indice au plus* $\mathbf{e}$ *dans le groupe des homothéties.*

(*b*) *soit on trouve une courbe elliptique* E', *isogène à* E *et également définie sur* F, *et un point de p-torsion* $P \in E'_p$ *qui devient rationnel sur un corps* $F(P)$ *dont le degré vérifie* $[F(P) : F] \leq 48dh_F$. *Ceci n'est possible que si* $p < (48dh_F)^{3(48dh_F)^2}$.

Démonstration : Si la courbe E n'a potentiellement bonne réduction de hauteur 2 pour aucune place, alors $\varphi_p(G_F)$ est soit contenu dans un sous-groupe de Borel ou dans le normalisateur d'un sous-groupe de Cartan déployé, soit il contient $\mathrm{Sl}_2(\mathbb{F}_p)$ (lemmes 27 et 31). Dans les deux derniers cas $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$ (lemme 28 et théorème 60). Dans le premier cas il y a les deux possibilités énoncées dans le théorème (théorème 52).

Corollaire 44. *Sous les hypothèses du théorème* 43 *et pour tout p plus grand que* $(48dh_F)^{3(48dh_F)^2}$, *l'image* $\rho_p(G_F)$ *contient les homothéties* $(\mathbb{Z}_p^*)^{\mathbf{e}}$.

voir corollaire 53

Remarque : Le cas critique se trouve être le cas que, par rapport à une place w au-dessus de p, la courbe E ait bonne réduction de hauteur 2 avec un polygone de Newton de la forme  . Dans ce cas-là, et seulement dans ce cas, c'est possible que, d'une part, $\rho_p(G_F)$ ne contient pas un grand sous-groupe des homothéties, d'autre part, le groupe E_p des points de p-torsion a un sous-groupe non trivial, rationnel sur F, sans qu'il y ait un point de p-torsion rationnel sur une petite extension de F (voir chapitre 2.6.3).

Si w n'est pas ramifié, le polygone de Newton n'est jamais de la forme  ([18, §1.10, p. 271], → thm. 39).

Lorsque E est définie déjà sur $\mathbb{Q}$, le groupe E_p ne peut avoir un sous-groupe rationnel sur $F = \mathbb{Q}$ que pour $p \leq 163$ (théorème 34, → cor. 41).

Il y a des résultats de Momose ([15]) qui généralisent celui de Mazur (thm. 34) et impliquent que, dans beaucoup de cas, on peut borner les p, pour lesquels peut se produire ce "mauvais cas" (le cas (b) du théorème 40).

2.4 Маршрут

On avait vu que l'image $\varphi_p(G_F)$ peut soit contenir $\mathrm{Sl}_2(\mathbb{F}_p)$, soit elle est contenue dans un sous-groupe de Borel, dans le normalisateur d'un sous-groupe de Cartan déployé ou dans le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{Gl}_2(\mathbb{F}_p)$ (lemme 27).

On sait déjà que $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^c$ si $\varphi_p(G_F)$ contient $\mathrm{Sl}_2(\mathbb{F}_p)$ (lemme 28).

Lorsque $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan non déployé la courbe E a potentiellement bonne réduction de hauteur 2 avec polygone de Newton de la forme  à toutes les places au-dessus de p (lemme 31). Si w est une telle place, ramifié de degré e divisant p^2-1, on utilisera une généralisation d'un résultat de Fontaine ([7]) qui démontre que $\rho_p(I_w)$ contient un sous-groupe d'indice e d'un sous-groupe de Cartan non déployé et en particulier les homothéties $(\mathbb{Z}_p^*)^e$ (thm. 45, chap. 2.5).

Ensuite il y a le cas que $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel de $\mathrm{Gl}_2(\mathbb{F}_p)$. Dans ce cas, au-dessus de p, la courbe E peut avoir potentiellement bonne réduction de hauteur 1, mauvaise réduction de type multiplicatif ou bonne réduction de hauteur 2, avec un polygone de Newton de la forme  . Le chapitre 2.6.1 traite le cas que E a potentiellement bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif par rapport à toute place divisant p. On suit le raisonnement de Serre ([18]) : soit on trouve deux sous-groupes d'inertie dont les images par φ_p contiennent, par rapport à une même base, les deux sous-groupes $\begin{pmatrix} (\mathbb{F}_p^*)^{\mathbf{e}} & \\ & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \\ & (\mathbb{F}_p^*)^{\mathbf{e}} \end{pmatrix}$ et donc $\varphi_p(G_F)$ contient les homothéties $(\mathbb{F}_p^*)^{\mathbf{e}}$, soit E, ou une courbe isogène à E, a un point de p-torsion rationnel sur une extension M de F. On peut borner le degré de M sur F par $48h_F$ (lemme 57). En utilisant le résultat de Merel ([14]) cela permet de borner les p pour lesquels $\varphi_p(G_F)$ ne contient pas les homothéties $(\mathbb{F}_p^*)^{\mathbf{e}}$. Si $\varphi_p(G_F)$ contient ces homothéties on peut les remonter a $\rho_p(G_F)$ et conclure que $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$ (cor. 59).

Si $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan déployé et pas dans un sous-groupe de Borel on trouve deux sous-groupes d'inertie dont les images par φ_p contiennent, par rapport à une même base, les deux sous-groupes $\begin{pmatrix} (\mathbb{F}_p^*)^{\mathbf{e}} & \\ & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \\ & (\mathbb{F}_p^*)^{\mathbf{e}} \end{pmatrix}$ et on peut remonter à $\rho_p(G_F)$ comme dans le cas avant (théorème 60).

Reste le cas, considéré dans le chapitre 2.6.3, que $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel et que E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  par rapport à une place au-dessus de p. En général, on ne peut pas dire grand chose dans ce cas-là. Si la courbe E est définie déjà sur $\mathbb{Q}$, le résultat de Mazur ([13]) dit que $\varphi_p(G_{\mathbb{Q}})$ ne peut pas être contenu dans un groupe de Borel pour $p > 163$ et [15] donne des résultats similaires pour d'autre corps.

2.5 Un sous-groupe de Cartan non déployé

On commence par traiter le cas de bonne réduction de hauteur 2 : on suppose qu'on a une courbe elliptique E, définie sur un corps de nombres F et qu'il existe une place v de F par rapport à laquelle E a potentiellement bonne réduction de hauteur 2 et telle que le polygone de Newton est de la forme  (c'est le cas du lemme 23). On considère la courbe E définie sur l'extension K de F_v sur laquelle E a réduction semi-stable (voir lemme 19). Le groupe formel $\mathcal{F}/\mathcal{O}_K$ associé à E est de hauteur 2, avec un polygone de Newton de la forme  . Tous les points de p^n-torsion $E_{p^n} \subseteq E(\overline{K})$ sont contenus dans le noyau de la réduction $E(\overline{K}) \to \tilde{E}(\overline{k})$. Ils correspondent aux points de torsion du groupe $\mathcal{F}(\overline{\mathfrak{m}})$. Si $K/\mathbb{Q}_p$ n'est pas ramifié, l'article de Fontaine ([7]) décrit l'action de Galois sur les points de torsion d'un groupe formel $\mathcal{F}/\mathcal{O}_K$. Si p est plus grand que 2 ces résultats restent vrais si $K/\mathbb{Q}_p$ est ramifié d'indice e plus petit que $p-1$ et divisant p^2-1 :

On considère un groupe formel $\mathcal{F}/\mathcal{O}_K$ qui est de hauteur 2. On note maintenant E_{p^n} l'ensemble des points de p^n-torsion de $\mathcal{F}$ et T son module de Tate (qui est un $\mathbb{Z}_p$-module libre de rang 2). Pour la représentation $\rho_p : G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T) \simeq \mathrm{Gl}_2(\mathbb{Z}_p)$ on a le résultat suivant :

Théorème 45. *Soit $\mathcal{F}$ un groupe formel de hauteur 2, défini sur un corps local $K/\mathbb{Q}_p$ avec $p > 2$. On suppose que le polygone de Newton de $\mathcal{F}$ est de la forme*  *et que le degré de ramification e de K sur $\mathbb{Q}_p$ est strictement plus petit que $p-1$ et divise p^2-1. Alors l'image de la représentation de Galois ρ_p contient un sous-groupe d'indice e d'un sous-groupe de Cartan non déployé. Plus précisément, ce sous-groupe est contenu dans l'image du sous-groupe d'inertie I de G_K. En particulier $\rho_p(G_K)$ contient les homothéties $(\mathbb{Z}_p^*)^e$.*

Remarque : Si p est plus grand que 5 et e divise 12 on a aussi $e|(p^2-1)$ car $p+1$ et $p-1$ sont divisibles par 2 et l'un des deux est divisible par 3. En particulier l'hypothèse que e divise p^2-1 est vérifié si p est plus grand que 5 et n'est pas ramifié dans le corps de définition F de E (lemme 19).

Avant de commencer la démonstration on a besoin d'un certain nombre de définitions et de quelques lemmes (comparer [7]) : Si $K(E_\infty)$ est l'extension de K engendré par les points de torsion de $\mathcal{F}$, alors l'image H de la représentation $\rho_p : G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(T) \simeq \mathrm{Gl}_2(\mathbb{Z}_p)$ est isomorphe au groupe de Galois $G(K(E_\infty)/K)$ et on va identifier ces deux groupes. Comme on ne s'intéresse que à l'image du sous-groupe d'inertie $I \subseteq G_K$ on peut remplacer K par sa plus grande extension non ramifié dans $K(E_\infty)$ et on suppose $K(E_\infty)/K$ totalement ramifié pour la suite. L'algèbre des $\mathbb{Z}_p$-endomorphismes de T (respectivement des $\mathbb{F}_p$-endomorphismes de $E_p \simeq T/pT$) sera noté M (respectivement $\tilde{M}$). Sur $G = \mathrm{Gl}_2(\mathbb{Z}_p)$ on a la filtration donné par les sous-groupes $G(n) = \{g \in \mathrm{Gl}_2(\mathbb{Z}_p) : g-1 \in p^n M\}$. Les sous-groupes $H(n) = H \cap G(n)$ de l'image H sont les groupes de Galois de $K(E_\infty)/K(E_{p^n})$.

Le groupe $G/G(1)$ s'identifie à $\tilde{G} = \mathrm{Gl}_2(\mathbb{F}_p)$ et le quotient $H/H(1)$ est isomorphe à l'image de la représentation $\varphi_p : G(\overline{\mathbb{Q}}_p/K) \to \mathrm{Aut}_{\mathbb{F}_p}(E_p) \simeq \mathrm{Gl}_2(\mathbb{F}_p)$. C'est le groupe de Galois $G(K(E_p)/K)$.

On écrit $p^2 \,(= p^{ht\mathcal{F}}) = q$. L'algèbre $\tilde{M}$ des $\mathbb{F}_p$-endomorphismes de E_p contient le corps $\mathbb{F}_q$, son groupe multiplicatif $\mathbb{F}_q^*$ est un sous-groupe de $\mathrm{Aut}_{\mathbb{F}_p}(E_p)$. Le sous-groupe d'inertie I de $G(K(E_p)/K)$ agit sur E_p par la puissance e-ième du caractère fondamental : $\theta_{q-1}^e : I \to \mathbb{F}_q^*$ (lemme 23).

L'image du groupe de Galois $G(K(E_p)/K)$ dans $\mathrm{Aut}_{\mathbb{F}_p}(E_p)$ sera noté J. Comme $K(E_p)/K$ est supposé totalement ramifié, le groupe J est un sous-groupe de $\mathbb{F}_q^*$, qui lui, est un sous-groupe de Cartan non déployé de $\mathrm{Gl}_2(\mathbb{F}_p)$. L'indice de J dans $\mathbb{F}_q^*$ est e (voir lemme 23).

Pour tout $n \geq 1$, le groupe $G/G(n+1)$ opère par conjugaison sur $G(n)/G(n+1)$, le noyau de cette opération contenant le sous-groupe $G(1)/G(n+1)$. Cela fait de $G(n)/G(n+1)$ un $\mathrm{Gl}_2(\mathbb{F}_p)$-module et a fortiori un $\mathbb{F}_q^*$-module, ainsi qu'un J-module. Le groupe $H(n)/H(n+1)$ est un sous-J-module de $G(n)/G(n+1)$.

L'espace $\tilde{M}$ des $\mathbb{F}_p$-endomorphismes de E_p est également un $\mathbb{F}_q^*$-, et puis un J-module, l'action étant donné par conjugaison. Finalement on a un $\mathbb{F}_q^*$-isomorphisme entre $G(n)/G(n+1)$ et $\tilde{M}$, donné par l'application qui envoie $g \in G(n)$ sur $(g-1)/p^n \in \tilde{M}$. Cet isomorphisme fait de $G(K(E_{p^{n+1}})/K(E_{p^n})) \simeq H(n)/H(n+1)$ un sous-J-module de $\tilde{M}$ qu'on note $\tilde{H}_n$.

Si le groupe de Galois de $\mathbb{F}_q$ sur $\mathbb{F}_p$ est donné par $\{id, \tau\}$, l'algèbre des $\mathbb{F}_p$-endomorphismes $\tilde{M}$ du $\mathbb{F}_q$-espace vectoriel E_p se décompose en somme directe $\tilde{M} = \tilde{M}_{id} \oplus \tilde{M}_\tau$ où $\tilde{M}_{id}$ est l'algèbre des endomorphismes $\mathbb{F}_q$-linéaires, son supplémentaire $\tilde{M}_\tau$ est formé des endomorphismes τ-linéaires de E_p. C'est à dire $\mathbb{F}_q^*$ agit trivialement sur $\tilde{M}_{id}$, sur $\lambda \in \tilde{M}_\tau$ un élément $\epsilon \in \mathbb{F}_q^*$ agit par $\epsilon : \lambda \mapsto \epsilon\lambda\epsilon^{-1} = \epsilon^{1-p}\lambda$. L'ordre de J est plus grand que $p+1$ puisqu'on a supposé $e < p-1$. Ça implique que, aussi restreint à J, le caractère τ est différent de l'identité. C'est à dire, aussi en tant que J-module, l'espace $\tilde{M}$ se décompose en somme directe $\tilde{M} = \tilde{M}_{id} \oplus \tilde{M}_\tau$ avec deux sous-J-modules $\tilde{M}_{id}$ et $\tilde{M}_\tau$ bien définis, distincts et non triviales.

Pour la suite on doit supposer que l'indice de ramification $e = e_{K/\mathbb{Q}_p}$ divise $q-1 = (p-1)(p+1)$. Dans ce cas l'extension $K(E_p)/K$ est de degré $\frac{q-1}{e}$, son groupe de Galois J est égal à $(\mathbb{F}_q^*)^e$ et d'indice e dans $\mathbb{F}_q^*$.

Lemme 46. *Si l'indice de ramification e divise $q-1$, alors pour tout $n \geq 1$, le J-module $G(K(E_{p^{n+1}})/K(E_{p^n})) \simeq \tilde{H}_n \subseteq \tilde{M}$ contient la partie triviale $\tilde{M}_{id}$ de $\tilde{M}$.*

Démonstration : D'abord on remarque que, si on voit tous les $\tilde{H}_n$ comme sous-espaces de $\tilde{M}$, on a pour tout $n \geq 1$ que $\tilde{H}_n$ est contenu dans $\tilde{H}_{n+1}$. Ceci est vrai parce que l'élévation à la puissance p-ième définit, par passage au quotient, un isomorphisme entre $G(n)/G(n+1)$ et $G(n+1)/G(n+2)$ et donc un plongement de

$\tilde{H}_n$ dans $\tilde{H}_{n+1}$ (rappelons qu'on a supposé $p > 2$). Si on identifie tous ces groupes à (des sous-groupes de) $\tilde{M}$, cet isomorphisme devient l'identité. Le groupe $\tilde{H}_n$ est donc contenu dans $\tilde{H}_{n+1}$ et il suffit de montrer le lemme pour $\tilde{H}_1$.

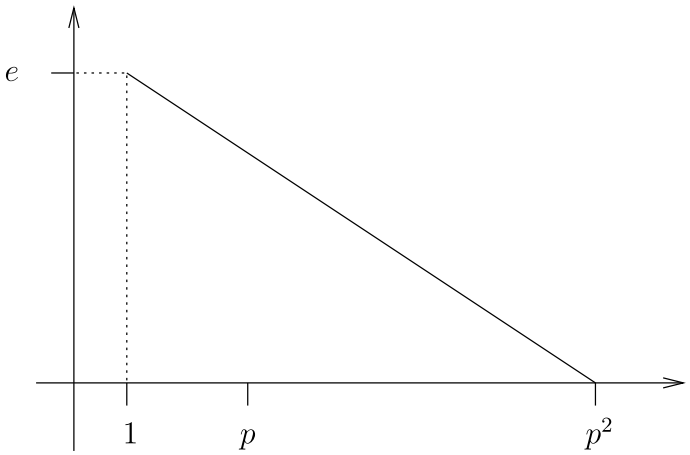
Au lieu de regarder les extensions $K(E_{p^n})$ on commence par étudier les extensions suivantes : Pour tout $n \geq 1$ on choisit un point $\pi_n \in E_{p^n}$ dont l'ordre est exactement p^n. De plus on choisit les π_n de façon compatible : $[p]\pi_{n+1} = \pi_n$ (ici $[p]$ est la multiplication par p selon la loi de groupe formel $\mathcal{F}$). On considère les extensions $K_n = K(\pi_n)$ engendré par ces points.

Lemme 47. *Tout élément $\pi \in E_\infty \subseteq \overline{\mathfrak{m}}$ d'ordre exactement p^n est de valuation $v_K(\pi) = \frac{e}{q^{n-1}(q-1)}$.*

Démonstration : On regarde la série formelle

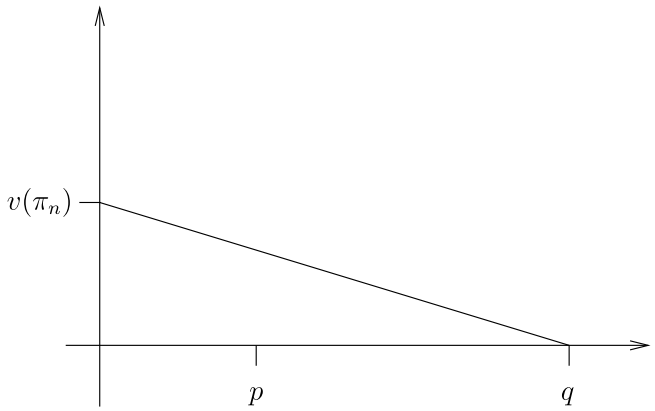
$$[p](X) = \sum_{i=1}^{\infty} a_i X^i = X(\sum_{i=0}^{\infty} a_{i+1} X^i)$$

qui donne la multiplication par p (selon la loi de groupe formelle $\mathcal{F}$). Le polygone de Newton de cette multiplication par p est supposé d'être de la forme



Il n'a qu'une seule pente négative, à savoir $-\frac{e}{q-1}$ entre $i = 1$ et $i = q$. Selon [4] on a donc exactement $q - 1$ racines π de valuation $v(\pi) = \frac{e}{q-1}$ et ce sont les seules racines de valuation positive, donc dans notre cas les seuls points $\pi \neq 0$ d'ordre p. Ce qui donne le résultat pour $n = 1$.

Un point π_{n+1} d'ordre exactement p^{n+1} est une racine d'une série formelle $f_{\pi_n}(X) = \pi_n - [p](X)$ avec un point π_n dont l'ordre est exactement p^n. Le polygone de Newton d'une telle série est de la forme



Par le même raisonnement que avant, cette série $f_{\pi_n}(X)$ a q racines, toutes de valuation $\frac{v(\pi_n)}{q}$. Par récurrence on obtient alors la formule $v(\pi_n) = \frac{e}{(q-1)q^{n-1}}$ pour tout point $\pi_n \in E_{p^n}$ d'ordre exactement p^n. □

Comme on avait supposé $K(E_\infty)/K$ totalement ramifiée, le groupe de Galois $J = G(K(E_p)/K)$ est égal à son sous-groupe d'inertie J. Il est un sous-groupe de $\mathbb{F}_q^*$ et d'ordre $\frac{q-1}{e}$. On a $K(E_p) = K_1$.

Lemme 48. *Pour tout $n \geq 1$ l'extension K_{n+1}/K_n est galoisienne, totalement ramifiée et de groupe de Galois isomorphe (en tant que groupe) à E_p. L'élément π_n est une uniformisante de K_n.*

Démonstration : Si τ est un élément de G_{K_n} on regarde le point $\tau(\pi_{n+1}) -_{\mathcal{F}} \pi_{n+1}$. C'est un point de p-torsion puisque τ fixe $[p]\pi_{n+1} = \pi_n$. C'est à dire, tous les conjugués de π_{n+1} sont donnés par $\pi_{n+1} +_{\mathcal{F}} a$ avec un point $a \in E_p$ et ils sont tous contenus dans K_n. L'extension K_{n+1}/K_n est galoisienne et on a un morphisme $G(K_{n+1}/K_n) \to E_p$ qui est injectif car l'action d'un $\tau \in G(K_{n+1}/K_n)$ sur K_{n+1} est complètement déterminée par son action sur π_{n+1}. Ça donne q comme borne supérieure de $[K_{n+1} : K_n]$. Mais ce degré ne peut pas être plus petit que q, puisque les valuations satisfont $v_K(\pi_{n+1}) = \frac{1}{q} v_K(\pi_n)$. Le degré de ramification de K_{n+1}/K_n est égal à q et aussi égal au degré $[K_{n+1} : K_n]$. Le morphisme $G(K_{n+1}/K_n) \to E_p$ est un isomorphisme et on a $v_{K_n}(\pi_n) = 1$. □

Lemme 49. *Pour tout $n \geq 0$, le groupe de Galois $G(K_{n+1}/K_n)$ n'a qu'un seul nombre de ramification, i.e. il existe un j tel que $G(K_{n+1}/K_n) = G(K_{n+1}/K_n)_{j-1}$ et $G(K_{n+1}/K_n)_j = \{id\}$. Si l'indice de ramification e divise $q-1$, on a $j = q^n$.*

Démonstration : On commence avec $G(K_1/K) = J$. On avait supposé $J = J_0$, reste a montrer que $J_1 = \{id\}$. D'après le lemme 23, tout $\tau \in J$ agit comme $\mathbb{F}_q$-automorphisme de E_p (par l'intermédiaire du caractère $\theta_{q-1}^e : I \to \mathbb{F}_q^*$). Pour tout $\tau \neq id$, ça implique que $1 \neq \frac{\tau(\pi_1)}{\pi_1} \in \mathbb{F}_q^*$, c'est à dire $\frac{\tau(\pi_1)}{\pi_1} \notin U_{K_1}^1$ et $\tau \notin J_1$ (comparer [17, IV§2, p. 74]).

Pour $n \geq 1$ on vient de voir que pour tout élément $id \neq \tau \in G(K_{n+1}/K_n)$, il y a un point $0 \neq a \in E_p$ tel que $\tau(\pi_{n+1}) = \pi_{n+1} +_{\mathcal{F}} a = \mathcal{F}(\pi_{n+1}, a)$, ce qui donne

$v_{K_{n+1}}(\tau(\pi_{n+1}) - \pi_{n+1}) = v_{K_{n+1}}(\mathcal{F}(\pi_{n+1}, a) - \pi_{n+1}) = v_{K_{n+1}}(a) = q^n(\cdot\frac{e}{\text{pgcd}\,(e,q-1)})$ (Remarquer que K_{n+1}/K est totalement ramifié, ce qui d'après [17, I§7, prop. 18, p. 30] implique que l'uniformisante π_{n+1} de K_{n+1} engendre $\mathcal{O}_{K_{n+1}}$ en tant que $\mathcal{O}_K$-algèbre). Tous les éléments τ sont donc contenus dans le groupe de ramification $G(K_{n+1}/K_n)_{q^n-1}$, le groupe de ramification $G(K_{n+1}/K_n)_{q^n}$ est réduite à l'identité. □

Lemme 50. *Si K_2 est galoisien sur K, le groupe de Galois $G(K_2/K_1)$ est un quotient de $\tilde{H}_1$ qui est isomorphe à $\tilde{M}_{id}$ en tant que J-module.*

Démonstration : Lorsque K_2 est galoisien sur K le groupe de Galois $G(K(E_{p^2})/K_2)$ est stable sous l'action de J et $G(K_2/K_1)$ est le quotient des J-modules $\tilde{H}_1$ et $G(K(E_{p^2})/K_2)$.

Comme K_2/K_1 n'a qu'un seul nombre de ramification on a

$$G(K_2/K_1) = G(K_2/K_1)_{q-1} = G(K_2/K)_{q-1} \cap G(K_2/K_1)$$

et

$$\{id\} = G(K_2/K_1)_q = G(K_2/K)_q \cap G(K_2/K_1)$$

ce qui donne $G(K_2/K)_{q-1} \supseteq G(K_2/K_1)$ et $G(K_2/K)_q = \{id\}$. De même, l'extension K_1/K a zéro comme seul nombre de ramification. La numérotation supérieure est alors égale à la numérotation inférieure et on a

$$\{id\} = G(K_1/K)_1 = G(K_2/K)_1 G(K_2/K_1)/G(K_2/K_1),$$

donc $G(K_2/K)_1 \subseteq G(K_2/K_1)$ et les groupes de ramification de K_2/K sont $\{id\} = G(K_2/K)_q \subsetneq G(K_2/K)_{q-1} = G(K_2/K_1) = \ldots = G(K_2/K)_1 \subsetneq G(K_2/K)$.

Le groupe $J = G(K_2/K)_0/G(K_2/K)_1$ agit sur

$$G(K_2/K_1) = G(K_2/K)_{q-1}/G(K_2/K)_q$$

par conjugaison. La proposition 9 de [17, chap. IV§2, p. 77] explicite cette action. En particulier $J = G(K_2/K)_0/G(K_2/K)_1$ agit par des puissances $(q-1)$-ièmes sur $G(K_2/K)_{q-1}/G(K_2/K)_q$. Comme l'ordre de J divise $q-1$, on voit que J agit trivialement et le J-module $G(K_2/K_1)$, qui est d'ordre q, est isomorphe à $\tilde{M}_{id}$. □

Lorsque K_2/K n'est pas galoisien, l'extension $K(E_{p^2})/K_1$ peut être de degré p^3 ou de degré p^4. Si elle est de degré p^4 le groupe de Galois $\tilde{H}_1$ est égal à $\tilde{M}$ et contient forcément tout $\tilde{M}_{id}$.

Supposons alors que K_2/K n'est pas galoisien et que $K(E_{p^2})/K_1$ est de degré p^3.

Si K_2 n'est pas galoisien sur K, le groupe de Galois $\mathfrak{H} = G(K(E_{p^2})/K_2)$ est un sous-groupe d'ordre p de $\tilde{H}_1 = G(K(E_{p^2})/K_1)$ qui n'est pas normal dans $G(K(E_{p^2})/K)$. Il y a donc des éléments $\sigma \in G(K(E_{p^2})/K)$ qui ne fixent pas $\mathfrak{H}$ et, pour tout tel σ,

le point π_2^σ est également d'ordre exacte p^2 et l'extension $K_2^\sigma = K(\pi_2^\sigma)$ a les mêmes propriétés que K_2.

On regarde les sous-groupes de ramification de $\tilde{H}_1$: des groupes $G(K_2/K_1) = \tilde{H}_1/\mathfrak{H}$ et $G(K_2^\sigma/K_1) = \tilde{H}_1/\mathfrak{H}^\sigma$ on sait qu'ils n'ont qu'un seul nombre de ramification, qui est $q-1$ à chaque fois (lemme 49). Puisqu'il n'y a qu'un seul nombre de ramification, les numérotations inférieure et supérieure sont égales.

Si $\tilde{H}_1^\nu$ sont les groupes de ramification de $K(E_{p^2})/K_1$, on a $G(K_2/K_1)^\nu = \tilde{H}_1^\nu\mathfrak{H}/\mathfrak{H}$ donc $\tilde{H}_1^q\mathfrak{H}/\mathfrak{H} = \{id\}$ et $\tilde{H}_1^q \subseteq \mathfrak{H}$. Pareillement on a $\tilde{H}_1^q \subseteq \mathfrak{H}^\sigma$ ce qui implique $\tilde{H}_1^q \subseteq \mathfrak{H} \cap \mathfrak{H}^\sigma = \{id\}$.

Pour $\nu = q-1$ on a $|\tilde{H}_1^{q-1}\mathfrak{H}/\mathfrak{H}| = p^2$, l'ordre de $\tilde{H}_1^{q-1}$ est au moins p^2.

Supposons que $\tilde{H}_1^{q-1}$ soit d'ordre p^3, c'est à dire, c'est le groupe $\tilde{H}_1$ tout entier et l'extension $K(E_{p^2})/K_1$ n'a également qu'un seul nombre de ramification. On a $\tilde{H}_1 = \tilde{H}_{1,q-1} = G(K(E_{p^2})/K)_{q-1} \cap \tilde{H}_1$ et $\tilde{H}_{1,q} = G(K(E_{p^2})/K)_q \cap \tilde{H}_1 = \{id\}$. Ça donne $\tilde{H}_1 \subseteq G(K(E_{p^2})/K)_{q-1}/G(K(E_{p^2})/K)_q$ et la proposition 9 de [17, chap. IV§2, p. 77] implique que J agit sur $\tilde{H}_1$ par des puissances $(q-1)$-ièmes, donc trivialement. Ceci n'est pas possible puisque par hypothèse J n'agit pas trivialement sur $\mathfrak{H} \subseteq \tilde{H}_1$.

On sait alors que $\tilde{H}_1^{q-1}$ doit être d'ordre p^2 et l'extension $K(E_{p^2})/K_1$ a un deuxième nombre de ramification : $\{id\} = \tilde{H}_1^q \subsetneq \tilde{H}_1^{q-1} = \ldots = \tilde{H}_1^{\alpha+1} \subsetneq \tilde{H}_1^\alpha = \tilde{H}_1$, ou, en numérotation inférieure $\{id\} = \tilde{H}_{1,\beta+1} \subsetneq \tilde{H}_{1,\beta} = \ldots = \tilde{H}_{1,\alpha+1} \subsetneq \tilde{H}_{1,\alpha} = \tilde{H}_1$ avec deux indices β et α. En partant de la numérotation inférieure la proposition 9 de [17, chap. IV§2, p. 77] permet de déterminer l'action de J sur $\tilde{H}_{1,\alpha}/\tilde{H}_{1,\alpha+1}$ et sur $\tilde{H}_1^{q-1} = \tilde{H}_1^{q-1}/\tilde{H}_1^q = \tilde{H}_{1,\beta}/\tilde{H}_{1,\beta+1}$. Sur $\tilde{H}_{1,\alpha}/\tilde{H}_{1,\alpha+1}$ le groupe J agit par des puissances α-ièmes, sur $\tilde{H}_{1,\beta} = \tilde{H}_{1,\beta}/\tilde{H}_{1,\beta+1}$ il agit par des puissances β-ièmes. Maintenant, soit β est un multiple de l'ordre de J et J agit trivialement sur $\tilde{H}_{1,\beta}$, soit l'action de J est non triviale sur tout $\tilde{H}_{1,\beta}$. Dans le premier cas, le sous-J-module $\tilde{H}_{1,\beta}$ de $\tilde{H}_1$ est égal à $\tilde{M}_{id}$. Dans le deuxième cas J doit agir trivialement sur $\tilde{H}_{1,\alpha}/\tilde{H}_{1,\alpha+1}$ et α est un multiple de l'ordre de J . Mais l'indice de ramification β satisfait la formule $\beta = \alpha + p(q-1-\alpha) = p(q-1) - \alpha(p-1)$ [17, p. 80], c'est à dire β est aussi un multiple de l'ordre de J ; une contradiction.

Dans tous les cas on trouve que $\tilde{H}_1 \subseteq \tilde{M}$ contient le sous-J-module $\tilde{M}_{id}$. Comme remarqué au début (p. 37), ça suffit pour conclure que $\tilde{M}_{id}$ est contenu dans $\tilde{H}_n$ pour tout n. □

On a maintenant tout ce qu'il faut pour démontrer le théorème 45 :

Démonstration : Rappelons qu'on veut montrer que le groupe $H = \rho_p(G_K) \subseteq \mathrm{Gl}_2(\mathbb{Z}_p)$ contient les puissances e-ièmes d'un sous-groupe de Cartan non déployé. On sait que le lemme est vraie modulo p, plus précisément on a $(\mathbb{F}_p^*)^e \subseteq (\mathbb{F}_q^*)^e = J = H/H(1) \subseteq \varphi_p(G_F)$ (lemme 23).

Comme le noyau $H(1)$ de la réduction est un pro-p-groupe alors que l'ordre de J est premier à p, on peut remonter J dans $H \subseteq \mathrm{Aut}_{\mathbb{Z}_p}(T)$ (thm. 35).

On a donc une action de J sur T. Comme J est un sous-groupe de $\mathbb{F}_q^*$, ses éléments se diagonalisent simultanément. Comme il y a dans J des éléments $\lambda \notin \mathbb{F}_p^*$ qui ont deux valeurs propres distinctes, cette action définit deux droites (espaces propres) D_1 et D_2 dans $\overline{\mathbb{Z}}_p \times \overline{\mathbb{Z}}_p$.

Ces deux droites définissent un sous-groupe de Cartan (non déployé) $C \subseteq \mathrm{Gl}_2(\mathbb{Z}_p)$ dont on va démontrer que sa puissance e-ième est contenue dans H.

Ce sous-groupe C^e modulo son sous-groupe $C(1)$ des éléments congruent à l'identité modulo p est notre J de départ. Comme on a vu au début, le groupe $J = C^e/C(1) = H/H(1)$ se plonge dans H. Il reste à montrer qu'on a $C(1) \subseteq H(1)$. Pour cela on va se servir des algèbres de Lie $\mathfrak{h}(1),\ \mathfrak{c}$ et $\mathfrak{c}(1)$ de $H(1),\ C$ et $C(1)$ respectivement.

Sur tous ces groupes, ainsi que sur leurs algèbres de Lie, agit J par automorphismes intérieurs. Sur C, et puis aussi sur $\mathfrak{c}$, cette action est triviale puisque C est le centralisateur d'un tore contenant J.

Lemme 51. *L'algèbre de Lie* $\mathfrak{c}(1)$ *est contenue dans* $\mathfrak{h}(1)$.

Démonstration : Les deux algèbres en question sont contenues dans l'espace des endomorphismes $\mathfrak{g}(1) = p\mathrm{M}_2(\mathbb{Z}_p)$ où $\mathrm{M}_2(\mathbb{Z}_p)$ sont les 2×2-matrices sur $\mathbb{Z}_p$. Dans cet espace d'endomorphismes $\mathbb{Z}_p$-linéaires il y a le sous-espace $\mathfrak{M}_{id}$ des endomorphismes qui commutent à l'action de $\mathbb{F}_q^*$ et son complément $\mathfrak{M}_\tau$. Car l'action de J sur $\mathfrak{c}(1)$ est triviale, cette algèbre doit être contenue dans la partie $p\mathfrak{M}_{id}$ de $p\mathrm{M}_2(\mathbb{Z}_p)$.

Maintenant on regarde $\mathfrak{h}(1) \cap p\mathfrak{M}_{id}$. Dans le lemme 46 on a vue que $\tilde{H}_1 = H(1)/H(2)$, et donc aussi $\mathfrak{h}(1)/\mathfrak{h}(2)$, contient tout $\tilde{M}_{id}$. C'est à dire on a $(\mathfrak{h}(1) \cap p\mathfrak{M}_{id})/p\mathfrak{M}_{id} = \tilde{M}_{id}$. Avec le lemme de Nakayama ça implique $\mathfrak{h}(1) \cap p\mathfrak{M}_{id} = p\mathfrak{M}_{id}$, donc $\mathfrak{c}(1) \subseteq p\mathfrak{M}_{id} \subseteq \mathfrak{h}(1)$. □

Comme log et exp convergent sur $C(1)$ et $\mathfrak{c}(1)$ ce résultat sur les algèbres de Lie oblige aussi $C(1) \subseteq H(1)$. Prise ensemble avec la section $C^e/C(1) = J \hookrightarrow H$ ça prouve $C^e \subseteq H$. Comme le sous-groupe de Cartan C contient les homothéties, on trouve $(\mathbb{Z}_p^*)^e \subseteq H \subseteq \rho_p(G_K)$. □

2.6 Un sous-groupe de Borel

On considère maintenant le cas que $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel B ou dans le normalisateur d'un sous-groupe de Cartan déployé. Dans ce deuxième cas, si $\varphi_p(G_F)$ n'est pas déjà contenu dans un sous-groupe de Borel il a un sous-groupe d'indice 2 qui l'est.

2.6.1 Un sous-groupe de Borel et tout va bien

En premier on regarde le cas que $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel et que E a, soit potentiellement bonne réduction de hauteur 1, soit potentiellement mauvaise réduction de type multiplicatif pour toute place v au-dessus de p. On exclut le cas du lemme 24.

Par rapport à une base convenable, $\varphi_p(G_F)$ s'écrit sous la forme $\begin{pmatrix} \chi' & * \\ & \chi'' \end{pmatrix}$ avec deux caractères χ', χ'': $G_F \to \mathbb{F}_p^*$ dont le produit (le déterminant de la matrice) est le caractère cyclotomique χ_p: $G_F \to \mathbb{F}_p^*$.

Pour la suite on aura besoin d'un corps sur lequel la courbe E a réduction semi-stable partout. Pour ça on va travailler sur le corps de base agrandi $L = F(E_3)$ (voir lemme 38). On note δ le degré de $L = F(E_3)$ sur F.

Théorème 52. *Soit E une courbe elliptique définie sur un corps de nombres F. On suppose toujours les hypothèses globales (p. 20). Si E n'a potentiellement bonne réduction de hauteur 2 pour aucune place v au-dessus de p et si l'image $\varphi_p(G_F)$ dans $\mathrm{Aut}(E_p) \simeq \mathrm{Gl}_2(\mathbb{F}_p)$ est contenue dans un sous-groupe de Borel $\widetilde{B}$, alors l'une des deux assertions suivantes est vraie :*

- *(a) La courbe E, ou une courbe isogène à E, a un point de p-torsion rationnel sur un corps dont le degré sur F divise δh_F.*
- *(b) L'image $\rho_p(G_F)$ contient, par rapport à une base convenable, deux sous-groupes $\left(\begin{smallmatrix} S & \\ & 1 \end{smallmatrix}\right) \subseteq \left(\begin{smallmatrix} \mathbb{Z}_p^* & \\ & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & \\ & S \end{smallmatrix}\right) \subseteq \left(\begin{smallmatrix} 1 & \\ & \mathbb{Z}_p^* \end{smallmatrix}\right)$ tels que l'indice de S dans $\mathbb{Z}_p^*$ divise $\mathbf{e}$. En particulier $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$.*

Corollaire 53. *Sous les hypothèses du théorème 52 et pour tout $p > (\delta d h_F)^{3(\delta d h_F)^2}$ l'image $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$.*

Démonstration : Le résultat de Merel (théorème 33) implique que le cas (a) du théorème 52 se produit uniquement si $p < (\delta d h_F)^{3(\delta d h_F)^2}$. □

Démonstration (théorème 52) : L'image $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel $\tilde{B}$. Soit $\tilde{Y} \subseteq E_p$ la droite stable par notre sous-groupe de Borel $\tilde{B}$ et soit (y, x) une base de E_p avec $y \in \tilde{Y}$. Selon cette base l'action de $\varphi_p(G_F)$ est donnée par des matrices de la forme $\begin{pmatrix} \chi' & * \\ & \chi'' \end{pmatrix}$ avec deux caractères χ', $\chi'' : G_F \longrightarrow \mathbb{F}_p^*$.

Lemme 54. *Restreint à G_L, les caractères χ' et χ'' sont non ramifiés en toute place w ne divisant pas p.*

Démonstration : Si $\overline{w}$ est une place en dessus d'un premier $l \neq p$ où E a bonne réduction, alors la représentation ρ_p n'est pas ramifié en $\overline{w}$ [20, thm. 1, p. 493] et il en est de même pour χ' et χ''.

Si E a mauvaise réduction (semi-stable) en $\overline{w}$, alors le modèle de Tate [16, IV A1.2, IV-31] donne une suite exacte

$$0 \longrightarrow \mu_p \longrightarrow E_p \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

Le groupe de Galois G_L agit trivialement sur $\mathbb{Z}/p\mathbb{Z}$ et pour toute place $\overline{w}$ en dehors de p, le groupe d'inertie $I_{\overline{w}}$ agit trivialement sur μ_p. Ça veut dire que, par rapport a une base adaptée, l'image de $I_{\overline{w}}$ dans $\mathrm{Aut}(E_p) \simeq \mathrm{Gl}_2(\mathbb{F}_p)$ ne contient que des matrices de la forme $\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$ et est d'ordre divisant p. On en déduit que l'image de $I_{\overline{w}}$ par les caractères χ' et χ'' est triviale (comparer [18, §5.4, p. 307]). □

Lemme 55. *Si, sous les hypothèses du théorème* 52 *les deux caractères χ' et χ'', restreints à G_L, sont ramifiés au-dessus de p, alors $\varphi_p(G_F)$ contient les homothéties $(\mathbb{F}_p^*)^{\mathrm{e}}$. Si, restreint à G_L, l'un des deux caractères n'est pas ramifié, alors soit la courbe E, soit une courbe isogène à E, a un point de p-torsion rationnel sur un corps L_χ dont le degré $[L_\chi : F]$ divise δh_F.*

Démonstration : On utilise les sous-groupes $\varphi_p(I_j)$ de $\varphi_p(G_F)$ ou les I_j sont les groupes d'inertie définis au début (p. 20). On rappelle qu'on dénote $\tilde{X}_j$ les espaces propres correspondant au caractère cyclotomique sur I_j (voir p. 31). Lorsqu'on a besoin que les caractères χ' et χ'' soient non ramifiés en dehors de p, on restreint les applications à G_L. Le lemme 55 suivra des deux lemmes suivants.

Lemme 56. *Supposons les hypothèses du théorème* 52. *Alors, soit l'un des deux caractères χ' et χ'', restreint à G_L, est non ramifié aussi au-dessus de p, soit on peut trouver deux sous-groupes d'inertie I_1 et I_2 tels que $\tilde{X}_1 = \tilde{Y} \neq \tilde{X}_2$ (voir p. 31) et une base de E_p par rapport à laquelle l'image $\varphi_p(G_F)$ contient les deux sous-groupes $\begin{pmatrix} (\mathbb{F}_p^*)^{\mathrm{e}} & \\ & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \\ & (\mathbb{F}_p^*)^{\mathrm{e}} \end{pmatrix}$.*

Démonstration : Le groupe $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel $\tilde{B}$ fixant une droite $\tilde{Y}$ dans E_p. C'est à dire, il y a, dans E_p, une droite $\tilde{Y}$, stable par l'action de $\varphi_p(G_F)$, ou encore, tout vecteur $y \in \tilde{Y}$ est vecteur propre pour tout $\sigma \in \varphi_p(G_F)$.

Fixons un sous-groupe I_j. Sur I_j on a les deux caractères 1 et $\theta_{p-1}^{e_j}$. D'après le lemme 22 on a dans E_p l'espace propre $\tilde{X}_j$ correspondant au caractère $\theta_{p-1}^{e_j}$ et un espace propre correspondant au caractère 1.

La droite $\tilde{Y}$ peut soit être égal à la droite $\tilde{X}_j$, au quel cas on a $\varphi_p(I_j)|_{\tilde{Y}} = \theta_{p-1}^{e_j}(I_j)$, soit la droite $\tilde{Y}$ est différente de $\tilde{X}_j$. Dans ce cas $\tilde{Y}$ est l'espace propre correspondant au caractère 1 et $\varphi_p(I_j)$ s'écrit comme $\begin{pmatrix} 1 & \\ & \theta_{p-1}^{e_j} \end{pmatrix}$ dans la base $\langle \tilde{Y}, \tilde{X}_j \rangle$.

Si pour toute place v_j, la droite $\tilde{X}_j$ est égal à $\tilde{Y}$, alors le caractère χ'', restreint à G_L, est non ramifié aussi au-dessus de p, pareillement le caractère χ', restreint à G_L, est non ramifié, si $\tilde{X}_j$ est différent de $\tilde{Y}$ pour toute place v_j.

Il reste à considérer le cas, qu'on a une place v_1 telle que $\tilde{X}_1 = \tilde{Y}$ et une place v_2 avec $\tilde{X}_2 \neq \tilde{Y}$. Dans ce cas on sait déjà que, selon la base $\langle \tilde{Y}, \tilde{X}_2 \rangle$, le groupe $\varphi_p(I_2)$ contient le sous-groupe $\begin{pmatrix} 1 & \\ & (\mathbb{F}_p^*)^e \end{pmatrix}$.

Soit $\mathfrak{G}$ le groupe engendré par $\varphi_p(I_1)$ et $\varphi_p(I_2)$. Comme les deux caractères χ' et χ'' sont ramifiés, $\mathfrak{G}$ modulo sa p-partie est le groupe $(\mathbb{F}_p^*)^{e_1} \times (\mathbb{F}_p^*)^{e_2}$. Ce dernier groupe est d'ordre premier à p alors que le noyau de la réduction $\mathfrak{G} \to (\mathbb{F}_p^*)^{e_1} \times (\mathbb{F}_p^*)^{e_2}$ est un p-groupe. En utilisant le théorème de Zassenhaus (thm. 35) on peut remonter $(\mathbb{F}_p^*)^{e_1} \times (\mathbb{F}_p^*)^{e_2}$ dans $\mathfrak{G}$. C'est à dire, on trouve dans $\mathfrak{G}$ deux éléments σ_1 et σ_2 qui sont d'ordre $|(\mathbb{F}_p^*)^{e_1}|$, respectivement $|(\mathbb{F}_p^*)^{e_2}|$, qui commutent et qui sont tels que $\chi'(\sigma_1) = \chi''(\sigma_2) = 1$. Ces deux éléments sont diagonalisables comme ils ont chacun deux valeurs propres distincts (l'un étant égal à 1). Puisqu'ils commutent ils sont diagonalisables simultanément et ils engendrent, selon une même base, deux sous-groupes $\begin{pmatrix} (\mathbb{F}_p^*)^{e_1} & \\ & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \\ & (\mathbb{F}_p^*)^{e_2} \end{pmatrix}$ de $\mathfrak{G} \subseteq \varphi_p(G_F)$. □

Lemme 57. *Si le caractère χ', restreint à G_L, n'est pas ramifié, alors l'extension $F_{\chi'}/F$ qui lui correspond est de degré divisant δh_F. La courbe E possède un point de p-torsion rationnel sur $F_{\chi'}$. Si le caractère χ'', restreint à G_L, est non ramifié, c'est $F_{\chi''}/F$ qui est de degré divisant δh_F. Dans ce cas la courbe $E' = E/\tilde{Y}$ a un point de p-torsion rationnel sur $F_{\chi''}$.*

Démonstration : Si le caractère χ'' n'est pas ramifié, l'extension $L_{\chi''}$ de L qui lui correspond est non ramifiée et cyclique. Plus que ça, χ'' est un caractère cyclique de F. L'extension $F_{\chi''}$ de F qui lui correspond est cyclique. Le groupe de Galois $H = G(L_{\chi''}/L)$ est un sous-groupe du groupe $G = G(F_{\chi''}/F)$, les deux étant des sous-groupes du groupe cyclique $\mathbb{F}_p^*$. Dans $F_{\chi''}$, il y a une sous-extension maximale non ramifiée (aussi a l'infini) $F_{\chi'',nr}$ de F (le corps $F_{\chi'',nr}$ est contenu dans le petit corps de classes de Hilbert H_F de F et le degré $[F_{\chi'',nr} : F]$ divise le nombre de classes h_F). Le groupe de Galois $U = G(F_{\chi''}/F_{\chi'',nr})$ est le plus petit sous-groupe de G qui contient toutes les images sous χ'' des sous-groupes d'inertie. Le caractère étant non-ramifié au-dessus de L, pour tout sous-groupe d'inertie I_j de G_F on a $\chi''(I_j) = \chi''(I_j/(I_j \cap G_L)) \subseteq G(L/F)$. C'est a dire l'ordre de $\chi''(I_j)$ divise $\delta = [L : F]$. Comme U est un sous-groupe d'un groupe cyclique, engendré par des sous-groupes d'ordre divisant δ, on a $|U||\delta$. Le degré de $F_{\chi''}$ sur F divise donc δh_F. D'autre côté, $F_{\chi''}$ est le corps sur lequel deviennent rationnels une partie des points de p-torsion de la courbe $E' = E/\tilde{X}$. Cette courbe E', qui est isogène à E, a un point de p-torsion rationnel sur $F_{\chi''}$, le degré de $F_{\chi''}$ sur F divise $h_F\delta$. Si le caractère χ' n'est pas ramifié, la courbe E a un point de p-torsion rationnel sur $F_{\chi'}$, qui, par le même raisonnement est alors de degré divisant δh_F sur F. □

Avec ce dernier lemme le lemme 55 est également démontré.

Lemme 58. *Soit $\mathfrak{G}$ un sous-groupe de $\mathrm{Gl}_2(\mathbb{Z}_p)$ qui est contenu dans un Iwahori. C'est à dire, modulo p, le groupe $\mathfrak{G}$ est contenu dans un sous-groupe de Borel qui s'écrit sous la forme $\begin{pmatrix} \chi' & * \\ & \chi'' \end{pmatrix}$ avec deux caractères χ', $\chi'' \colon \mathfrak{G} \to \mathbb{F}_p^*$. On suppose que, modulo sa pro-p-partie, $\mathfrak{G}$ contient $(\mathbb{F}_p^* \times \mathbb{F}_p^*)^{\mathfrak{io}}$ avec $0 < \mathfrak{io} < p-1$. De plus on suppose que $\mathfrak{G}$ contient deux éléments g_1 et g_2 qui ont chacun une valeur propre λ_i qui engendre topologiquement $(\mathbb{Z}_p^*)^{\mathfrak{io}}$ et une valeur propre égal à 1. Finalement on suppose que $\chi'(g_1 \bmod p)$ et $\chi''(g_2 \bmod p)$ sont des générateurs de $(\mathbb{F}_p^*)^{\mathfrak{io}}$ alors que $\chi'(g_2 \bmod p) = \chi''(g_1 \bmod p) = 1$.*

On peut alors trouver une base de $\mathbb{Z}_p \times \mathbb{Z}_p$ *par rapport à laquelle* $\mathfrak{G}$ *contient les deux sous-groupes* $\begin{pmatrix} (\mathbb{Z}_p^*)^{\text{IO}} & \\ & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & \\ & (\mathbb{Z}_p^*)^{\text{IO}} \end{pmatrix}$. *En particulier* $\mathfrak{G}$ *contient les homothéties* $(\mathbb{Z}_p^*)^{\text{IO}}$.

Démonstration : On décompose g_i en sa partie p-primaire $g_{i,p}$ avec $g_{i,p} \equiv 1 \bmod p$ dans $\mathbb{Z}_p^*$ et une partie $g_i^{(p)}$ d'ordre fini, premier à p.

Le noyau de la projection $\mathfrak{G} \to \mathbb{F}_p^* \times \mathbb{F}_p^*$ est un pro-p-groupe tandis que l'image est d'ordre premier à p. Ça permet d'appliquer le théorème de Zassenhaus (théorème 35) : on peut remonter l'image de cette projection dans $\mathfrak{G}$ et tous les compléments de son noyau sont conjugués.

D'abord on regarde la préimage $\mathfrak{H}$ de $(\mathbb{F}_p^* \times \mathbb{F}_p^*)^{\text{IO}}$ dans $\mathfrak{G}$ et la suite

$$1 \to \ker \to \mathfrak{H} \to (\mathbb{F}_p^* \times \mathbb{F}_p^*)^{\text{IO}} \to 1.$$

Le groupe $(\mathbb{F}_p^* \times \mathbb{F}_p^*)^{\text{IO}}$ a les deux générateurs $\tilde{\sigma}_1 = (\tilde{\sigma}, 1)$ et $\tilde{\sigma}_2 = (1, \tilde{\sigma})$ qui commutent. Le théorème [10, p. 126] permet maintenant de trouver, dans $\mathfrak{H}$, deux éléments σ_1 et σ_2 qui sont des antécédents de $\tilde{\sigma}_1$ et $\tilde{\sigma}_2$, de même ordre que $(\mathbb{F}_p^*)^{\text{IO}}$, et qui commutent. Comme les σ_i ont deux valeurs propres distinctes (l'une étant congruent 1 modulo p, l'autre pas), ils sont diagonalisables, comme ils commutent ils sont diagonalisables simultanément. On a donc une base $\langle X_1, X_2 \rangle$ de $\mathbb{Z}_p \times \mathbb{Z}_p$ selon laquelle σ_1 et σ_2 sont diagonales.

Ensuite on regarde la préimage $\mathfrak{H}_1$ de $(\mathbb{F}_p^*)^{\text{IO}} \times 1$ dans $\mathfrak{G}$ et la suite

$$1 \to \ker \to \mathfrak{H}_1 \to (\mathbb{F}_p^*)^{\text{IO}} \times 1 \to 1.$$

Le théorème [10, p. 126] nous dit que tous les compléments de ker dans $\mathfrak{H}_1$ sont conjugués. Donc en particulier, g_1 est conjugué à un élément $\hat{g}_1$ dont la partie $\hat{g}_1^{(p)}$ d'ordre premier à p est une puissance de σ_1.

De même on trouve un élément $\hat{g}_2$ dont la partie $\hat{g}_2^{(p)}$ d'ordre $|(\mathbb{F}_p^*)^{\text{IO}}|$ est une puissance de σ_2.

Les éléments $\hat{g}_i$ ont chacun deux valeurs propres distinctes (l'une étant égal à 1), ce qui permet de les diagonaliser. Les vecteurs propres de leurs parties premier à p sont X_1 et X_2, donc les deux éléments $\hat{g}_1$ et $\hat{g}_2 \in \mathfrak{G}$ sont diagonales par rapport à la base $\langle X_1, X_2 \rangle$ et ils engendrent les sous-groupes $\begin{pmatrix} (\mathbb{Z}_p^*)^{\text{IO}} & \\ & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \\ & (\mathbb{Z}_p^*)^{\text{IO}} \end{pmatrix}$. □

Corollaire 59. *On suppose toujours les hypothèses du théorème* 52. *Si les deux caractères* χ' *et* χ'' *(voir p.* 43*), restreints à* G_L*, sont ramifiés, alors l'image* $\rho_p(G_F)$ *dans* $\mathrm{Aut}(T_p(E)) \simeq \mathrm{Gl}_2(\mathbb{Z}_p)$ *contient, par rapport à une même base, les sous-groupes* $\begin{pmatrix} (\mathbb{Z}_p^*)^{\mathbf{e}} & \\ & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & \\ & (\mathbb{Z}_p^*)^{\mathbf{e}} \end{pmatrix}$. *En particulier* $\rho_p(G_F)$ *contient les homothéties* $(\mathbb{Z}_p^*)^{\mathbf{e}}$.

Démonstration : Par hypothèse le groupe $\rho_p(G_F)$ est contenu dans un Iwahori. Si, restreint à G_L, les deux caractères χ' et χ'' sont ramifiés, on a vu (lemme 56)

que $\rho_p(G_F)$ modulo p contient les sous-groupes $\begin{pmatrix} (\mathbb{F}_p^*)^{\mathbf{e}} & \\ & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & \\ & (\mathbb{F}_p^*)^{\mathbf{e}} \end{pmatrix}$. De plus il existent alors deux places v_1 et v_2 telles que $\tilde{X}_1 = \tilde{Y} \neq \tilde{X}_2$ (où $\tilde{X}_i \subseteq E_p$ sont encore les droites correspondantes aux valeurs propres θ_{p-1}^e, voir p. 31).

Comme on suppose que E a potentiellement bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif en p, pour chaque place v_j, on a une droite $X_j \leq T_p(E)$ qui est stable sous l'action du groupe G_{K_j} car $\rho_p(G_{K_j})$ est contenu dans un sous-groupe de Borel. Cette droite est le noyau de la réduction modulo p si E a bonne réduction de hauteur 1 (lemme 36 ou [18, §1.11(1)]). Lorsque E a mauvaise réduction, alors la droite X_j consiste des racines de l'unité $T_p(\mu)$ dans $T_p(E)$ (lemme 37). On a $\tilde{X}_j = X_j/pX_j$ (voir p. 31).

Par rapport à la base $\langle X_1, X_2 \rangle$, l'image $\rho_p(I_1)$ est de la forme $\begin{pmatrix} (\mathbb{Z}_p^*)^{e_1} & * \\ & 1 \end{pmatrix}$, l'image $\rho_p(I_2)$ est de la forme $\begin{pmatrix} 1 & \\ * & (\mathbb{Z}_p^*)^{e_2} \end{pmatrix}$ (lemmes 36 et 37). Si χ_1 et χ_2 sont à chaque fois les caractères sur la diagonale, on a $\chi_j(I_j) = (\mathbb{Z}_p^*)^{e_j}$ car, restreint à I_j, le caractère χ_j est égal au caractère cyclotomique. Ça implique qu'on a les éléments g_j nécessaires pour appliquer le lemme 58. On trouve $(\mathbb{Z}_p^*)^{\mathbf{e}} \subseteq \rho_p(G_F)$. **q.e.d.**

2.6.2 Le normalisateur d'un sous-groupe de Cartan déployé

Théorème 60. *Soit E une courbe elliptique définie sur un corps de nombres F. On suppose toujours les hypothèses globales (p. 20). Si l'image $\varphi_p(G_F)$ est contenu dans le normalisateur d'un sous-groupe de Cartan déployé mais pas dans un sous-groupe de Cartan (donc pas dans un sous-groupe de Borel non plus) de $\mathrm{Aut}(E_p) \simeq \mathrm{Gl}_2(\mathbb{F}_p)$, alors cette image contient les homothéties $(\mathbb{F}_p^*)^{\mathbf{e}}$ et $\rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$.*

Démonstration : Lorsque $\varphi_p(G_F)$ est contenu dans le normalisateur $N(C)$ d'un sous-groupe de Cartan C la courbe E a potentiellement bonne réduction de hauteur 1 ou mauvaise réduction de type multiplicatif pour toutes les places divisant p (lemme 31(b)). Fixons une place $v = v_j$ et le sous-groupe d'inertie $I = I_j$ correspondant (voir p. 20). L'image $\varphi_p(I)$ est contenue dans le sous-groupe de Cartan C (lemme 32). Par rapport à une base convenable il s'écrit de la forme $\begin{pmatrix} (\mathbb{F}_p^*)^e & \\ & 1 \end{pmatrix}$ (lemme 22, la base est celle donné par les deux droites définissant C). Comme $\varphi_p(G_F)$ n'est pas contenu dans le sous-groupe de Cartan C, il contient un élément qui échange les deux droites définissant le sous-groupe de Cartan déployé C. C'est-à-dire il existe un élément $\sigma \in G_F$ tel que $\varphi_p(\sigma)$ échange ces deux droites et $\varphi_p(I^\sigma) = \begin{pmatrix} 1 & \\ & (\mathbb{F}_p^*)^e \end{pmatrix}$ (toujours par rapport à la base correspondant à C). Ce qui prouve que $\varphi_p(G_F)$ contient les homothéties $(\mathbb{F}_p^*)^e$.

Le groupe $\varphi_p(G_F) = \rho_p(G_F) \bmod p$ est contenu dans le normalisateur $N(C)$ d'un sous-groupe de Cartan C. L'image $\rho_p(G_F)$ contient donc un sous-groupe $\mathfrak{G}$ qui est

d'indice 2 et dont l'image modulo p est contenu dans le sous-groupe de Cartan C. En particulier, $\mathfrak{G}$ est contenu dans un Iwahori et il contient les images $\rho_p(I)$ et $\rho_p(I^\sigma)$. A ce groupe $\mathfrak{G}$ s'applique le lemme 58 : comme dans le cas du corollaire 59 il existe une base par rapport à laquelle $\rho_p(I)$ est de la forme $\begin{pmatrix} (\mathbb{Z}_p^*)^e & * \\ & 1 \end{pmatrix}$ et $\rho_p(I^\sigma)$ est de la forme $\begin{pmatrix} 1 & \\ * & (\mathbb{Z}_p^*)^e \end{pmatrix}$ (lemmes 36 et 37), ce qui implique qu'on a bien les éléments g_1 et g_2 nécessaires pour appliquer le lemme 58. Ce lemme 58 implique que $\mathfrak{G} \subseteq \rho_p(G_F)$ contient les homothéties $(\mathbb{Z}_p^*)^e$. □

2.6.3 Das Letzte in Kürze

Le dernier cas à traiter est le cas que la courbe E a potentiellement bonne réduction de hauteur 2 avec un polygone de Newton de la forme  par rapport à une place v divisant p. C'est la cas du lemme 24.

La situation est la suivante : on a une place v au-dessus de p tel que le corps K correspondant (voir lemme 19) est ramifié de degré $e < p$. La courbe E/K a bonne réduction de hauteur 2, le polygone de Newton associé au groupe formel $\mathcal{F}$ de E est de la forme  . On a alors dans E_p une droite $\tilde{X}$, stable par l'action de $D = G_K$. Si on choisit un premier vecteur de base dans $\tilde{X}$, l'image du sous-groupe d'inertie $I \subseteq G_K$ est de la forme $\begin{pmatrix} \theta_{p-1}^{e-e_1} & * \\ & \theta_{p-1}^{e_1} \end{pmatrix}$ (e_1 est la valuation du p-ième coefficient de la série formelle correspondante à $[p]$, voir lemme 24).

Lemme 61. *Soit E une courbe elliptique sans multiplication complexe* ($\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}$) *qui est définie sur $\mathbb{Q}$ ($F = \mathbb{Q}$). Si $\rho_p(G_\mathbb{Q})$ ne contient pas les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$, alors p est au plus* 163.

Démonstration : Pour $F = \mathbb{Q}$ tout $p > 163$ satisfait les hypothèses globales (p.20, les e_j sont au plus 12, p. 20). Si l'image $\varphi_p(G_\mathbb{Q})$ n'est pas contenue dans un sous-groupe de Borel, elle est soit contenue dans le normalisateur d'un sous-groupe de Cartan (et pas dans un sous-groupe de Cartan), soit elle contient le groupe $\mathrm{Sl}_2(\mathbb{F}_p)$ (lemme 27). Dans les deux cas, $\rho_p(G_\mathbb{Q})$ contient les homothéties $(\mathbb{Z}_p^*)^{\mathbf{e}}$ (lemmes 28, 31 et théorèmes 45 et 60). Un groupe de Borel laisse stable un sous-espace $\tilde{Y}$ de E_p. Si $\varphi_p(G_F)$ est contenu dans un sous-groupe de Borel, cet espace $\tilde{Y}$ est un sous-groupe de E_p qui est rationnel sur F. Il définit une isogénie $E \to E/\tilde{Y}$ rationnel sur F.

Si E est définie sur $F = \mathbb{Q}$, le théorème 34 dit que l'existence d'une telle isogénie implique $p \leq 163$. □

Des résultats similaire à celui utilisé ici ([13]) sont vrais pour d'autre corps. En particulier il y a des résultats de Momose ([15]) qui généralisent celui de Mazur ([13]) et impliquent que dans beaucoup de cas on devrait pouvoir borner les p pour lesquels peut se produire ce "mauvais cas" du théorème 18.

Bibliographie

[1] *Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux*, volume 86 of *Astérisque*. Société Mathématique de France, Paris, 1981.

[2] Emil Artin and John Tate. *Class field theory*. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, second edition, 1990.

[3] Fedor Alekseivich Bogomolov. Sur l'algébricité des représentations l-adiques. *C. R. Acad. Sci. Paris Sér. A-B*, 290(15) :A701–A703, 1980.

[4] F. Bruhat. *Lectures on some aspects of p-adic analysis*. Notes by Sunder Lal. Tata Institute of Fundamental Research, Bombay, 1963.

[5] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[6] A. J. de Jong. Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic. *Invent. Math.*, 134(2) :301–333, 1998.

[7] Jean-Marc Fontaine. Points d'ordre fini d'un groupe formel sur une extension non ramifiée de $\mathbb{Z}_p$. In *Journées Arithmétiques* (*Univ. Grenoble*, *Grenoble*, 1973), pages 75–79. Bull. Soc. Math. France Mém. no. 37. Soc. Math. France, Paris, 1974.

[8] Jean-Marc Fontaine. *Groupes p-divisibles sur les corps locaux*. Société Mathématique de France, Paris, 1977. Astérisque, No. 47-48.

[9] A. Fröhlich. *Formal groups*. Lecture Notes in Mathematics, No. 74. Springer-Verlag, Berlin, 1968.

[10] B. Huppert. *Endliche Gruppen. I.* Die Grundlehren der Mathematischen Wissenschaften, Band 134. Springer-Verlag, Berlin, 1967.

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

[12] Serge Lang. *Algebraic number theory*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970.

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

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

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

[16] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[17] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

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

[19] Jean-Pierre Serre. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.

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

[21] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[22] A. Silverberg and Yu. G. Zarhin. Semistable reduction and torsion subgroups of abelian varieties. *Ann. Inst. Fourier* (*Grenoble*), 45(2) :403–420, 1995.

[23] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[24] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[25] J.-P. Wintenberger. Démonstration d'une conjecture de Lang dans des cas particuliers. *J. Reine Angew. Math.*, 553 :1–16, 2002.