MAJA VOLKOV

Les représentations l-adiques associées aux courbes elliptiques définies sur $\boldsymbol{Q}_p$, 1998

ORSAY
N° d'ordre 5550

UNIVERSITÉ DE PARIS-SUD
Centre d'Orsay

THÈSE

présentée pour obtenir

LE TITRE DE DOCTEUR EN SCIENCES

Spécialité : Mathématiques

par

Maja VOLKOV

Sujet

Les représentations l-adiques associées aux courbes elliptiques définies sur $\mathbb{Q}_p$

Soutenue le 14 décembre 1998 à 14 h devant la commission d'examen composée de :

M.	Jean-Marc	FONTAINE	Directeur de thèse
M.	Roland	GILLARD	Rapporteur
M.	Guy	HENNIART	Examinateur
Mme.	Bernadette	PERRIN-RIOU	Présidente
M.	Phillipe	SATGÉ	Rapporteur

Je voudrais exprimer ma plus profonde gratitude à Jean-Marc Fontaine pour avoir accepté de diriger cette thèse. Il m'a initiée à la géométrie arithmétique avec une grande générosité et beaucoup de patience. Sans son aide constante et précieuse, ce travail n'aurait pas pu être mené à terme.

Roland Gillard et Philippe Satgé ont bien voulu être mes rapporteurs. Je les remercie pour l'intérêt qu'ils ont porté à cette thèse, ainsi que pour le temps qu'ils ont bien voulu y consacrer. Leur lecture minutieuse de mon texte a permis bien des améliorations.

Bernadette Perrin-Riou a accepté de présider ce jury et je lui en suis reconnaissante. Je n'oublie pas qu'elle avait aussi bien voulu assister à ma soutenance de mémoire de DEA.

Guy Henniart m'a enseigné en DEA les fondements de la théorie des nombres algébrique. Aujourd'hui il a accepté de faire partie de mon jury, et je l'en remercie.

Je n'oublie pas non plus la gentillesse de Daniel Perrin qui m'a guidée dans mon initiation à la géométrie algébrique en-dehors des heures officielles d'enseignement, ni l'enthousiasme avec lequel Etienne Fouvry m'a fait découvrir l'arithmétique.

Je voudrais remercier également tous mes compagnons thésards pour leur gentillesse et pour la chaleureuse ambiance qu'ils ont su créer, ainsi que toute l'équipe de l'école doctorale d'Orsay qui permet aux doctorants de travailler dans d'excellentes conditions. J'adresse un grand merci à toutes les personnes qui répondaient toujours présent à chaque fois que j'avais un problème avec l'informatique.

Enfin, je remercie Uwe Jannsen d'avoir bien voulu m'accueillir à l'institut de Mathématique de l'université de Cologne alors que ma soutenance n'était pas encore achevée.

Abstract : This thesis is devoted to the study of the l-adic representations of the absolute Galois group G of $\mathbb{Q}_p$, $p \geq 5$, associated to an elliptic curve over $\mathbb{Q}_p$, as l runs through the set of all prime numbers (including $l = p$, in which case we use the theory of potentially semi-stable p-adic representations).
For each prime l, we give the complete list of isomorphism classes of $\mathbb{Q}_l[G]$-modules coming from an elliptic curve over $\mathbb{Q}_p$, that is, those which are isomorphic to the Tate module of an elliptic curve over $\mathbb{Q}_p$. The $l = p$ case is the more delicate. It requires studying the liftings of a given elliptic curve over $\mathbb{F}_p$ to an elliptic scheme over the ring of integers of a totally ramified finite extension of $\mathbb{Q}_p$, and combining it with a descent theorem providing a Galois criterion for an elliptic curve having good reduction over a p-adic field to be defined over a closed subfield. This enables us to state necessary and sufficient conditions for an l-adic representation of G to come from an elliptic curve over $\mathbb{Q}_p$, for each prime l.

Key-words : Elliptic curves, p-adic fields, Tate modules, l-adic representations, potentially semi-stable representations, potentially crystalline representations, Weil-Deligne representations, Serre-Tate theorem, p-divisible groups, Dieudonné modules.

TABLE DES MATIÈRES

INTRODUCTION

This thesis is devoted to the study of the l-adic representations of the absolute Galois group of $\mathbb{Q}_p$, $p \geq 5$, associated to an elliptic curve over $\mathbb{Q}_p$, as l runs through the set of all prime numbers (including $l = p$).

Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and write $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Let $E/\mathbb{Q}_p$ be an elliptic curve ; for each rational prime l, let $E[l^n]$, $n \geq 1$, be the points of order l^n in $E(\overline{\mathbb{Q}}_p)$, and put $T_l(E) = \varprojlim E[l^n]$, $V_l(E) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(E)$: the first is a free $\mathbb{Z}_l$-module of rank 2, so that the second is a 2-dimensional $\mathbb{Q}_l$-vector space, and both are equipped with a linear and continuous action of G. Hence we get representations :

$$G \xrightarrow{\rho_l} \mathrm{Aut}_{\mathbb{Z}_l}(T_l(E)) \qquad \text{and} \qquad G \xrightarrow{\rho_l} \mathrm{Aut}_{\mathbb{Q}_l}(V_l(E)).$$

These representations are known to contain a certain amount of information concerning the elliptic curve $E/\mathbb{Q}_p$, and many results about them have become classics (see [Se 1], [Se 2], [Se-Ta], [Ta], [Kr], [Roh], and many others ...).
Given a Weierstrass equation for E of the form $y^2 = x^3 + Ax + B$, we show how to "read" on it the isomorphism class of $V_l(E)$ for $l \neq p$, via some invariants (effectively computable) of the curve. When $l = p$, we know (and recover the fact) that the representation $V_p(E)$ already contains all the data one can find in the $V_l(E)$'s, $l \neq p$, plus one : the filtration, furnished by Fontaine's theory of potentially semi-stable representations ; this extra data may in some cases be read on the Weierstrass equation itself.
Thus, for each prime l, we obtain a list of non-isomorphic $\mathbb{Q}_l[G]$-modules such that for every elliptic curve $E/\mathbb{Q}_p$, the $\mathbb{Q}_l[G]$-module $V_l(E)$ is isomorphic to one of the objects of the list.

Now let T_l be a free $\mathbb{Z}_l$-module of rank 2 equipped with a linear and continuous action of G ; one may ask when does T_l come from an elliptic curve over $\mathbb{Q}_p$, i.e. when does there exist an $E/\mathbb{Q}_p$ such that T_l and $T_l(E)$ are isomorphic as $\mathbb{Z}_l[G]$-modules ? In fact, this question easily reduces to that one obtained by replacing T_l by $\mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l$ and $T_l(E)$ by $V_l(E)$.
We give an answer to this question, including the case $l = p$, which is certainly the more delicate. In fact, we show that every object of the lists previously mentioned actually comes from an elliptic curve over $\mathbb{Q}_p$.

Let us state these results more precisely.
For $l \neq p$, consider the category $\mathbf{Rep}_l(G)$ of l-adic representations of G. We know how to attach in a functorial way to each object of $\mathbf{Rep}_l(G)$ a representation of the Weil-Deligne group $'W$ of $\mathbb{Q}_p$ ([Del], [Fo 3]) ; this functor is exact and fully faithfull, and its essential image consists of representations of $'W$ for which the roots of the characteristic polynomial of the

Frobenius are l-adic units. In particular, we know what means for such a representation to be defined over $\mathbb{Q}$, and also how to compare them for different l's.
For $l = p$, consider the category $\mathbf{Rep}_{pst}(G)$ of potentially semi-stable p-adic representations of G. We use Fontaine's theory ([Fo 1], [Fo 2]) which enables us to attach in a functorial way to each object of $\mathbf{Rep}_{pst}(G)$ a filtered module, equipped with a semi-linear Frobenius, a monodromy operator, and with an action of a finite quotient of G ; for 2-dimensional objects, Fontaine proved recently that this is an equivalence of categories when one restricts to the weakly admissible filtered modules. Furthermore, if we drop out the filtration datum, we know how to obtain a representation of the Weil-Deligne group defined over an unramified extension of $\mathbb{Q}_p$, and thus compare it with objects arising from the $l \neq p$ situation ([Fo 3]). Note that for $l \neq p$ as well as for $l = p$, we always use contravariant functors, that is, we apply the functors described in [Fo 2] and [Fo 3] to the dual representation. For each prime l, the object $V_l(E)$ is dual to $H^1_{\acute{e}t}(E \times_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p, \mathbb{Q}_l)$, so that one may also consider them as covariant functors on the $H^1_{\acute{e}t}$'s. We have the following theorem :

THM I : *Let $E/\mathbb{Q}_p$ be an elliptic curve.*
1) The $\mathbb{Q}_p[G]$-module $V_p(E)$ is potentially semi-stable and its Hodge-Tate type is $(0,1)$.
2) The representation of the Weil-Deligne group attached to $V_l(E)$ is independent of the prime number l, and satisfies the following conditions :
(1°) *The determinant on $V_l(E)$ is the l-adic cyclotomic character : $\wedge^2 V_l(E) = \mathbb{Q}_l(1)$.*
(2°) *It is defined over $\mathbb{Q}$.*
(3°) *If $V_l(E)$ has potentially good reduction, the roots of the characteristic polynomial of a lifting of the arithmetic Frobenius acting on it are p-Weil numbers : $|\, Trace(Frob)| \leq 2\sqrt{p}$.*

All these necessary conditions are well known.
A case-by-case examination leads to the description of all possible representations of the Weil-Deligne group arising from an elliptic curve over $\mathbb{Q}_p$; we get a finite list $\mathbf{WD}^*$ of such isomorphism classes. Then, if one computes for each object of the $\mathbf{WD}^*$ list all the possible weakly admissible filtrations of Hodge-Tate type $(0,1)$ which might be attached to it (up to isomorphism of filtered modules), this leads to an infinite list $\mathbf{D}^*$ of such isomorphism classes. Of course, the $\mathbf{WD}^*$ list classifies the $\mathbb{Q}_l[G]$-modules $V_l(E)$, for $l \neq p$ and $E/\mathbb{Q}_p$ an elliptic curve, and the $\mathbf{D}^*$ list classifies the $\mathbb{Q}_p[G]$-modules $V_p(E)$ for $E/\mathbb{Q}_p$ an elliptic curve.

Now the main result is that the necessary conditions of THM I turn out to be sufficient :

THM II :
1) Every 2-dimensional representation of the Weil-Deligne group of $\mathbb{Q}_p$ satisfying conditions (1°), (2°), (3°) *comes from an elliptic curve over $\mathbb{Q}_p$.*
2) Every 2-dimensional potentially semi-stable $\mathbb{Q}_p[G]$-module of Hodge-Tate type $(0,1)$ *satisfying conditions* (1°), (2°), (3°) *comes from an elliptic curve over $\mathbb{Q}_p$.*

The first part of this theorem is rather easy to prove ; indeed, using the Honda-Tate theorem ([Ho-Ta]), we are able for each object of the $\mathbf{WD}^*$ list to produce an elliptic curve over $\mathbb{Q}_p$ (in a Weierstrass form) whose Weil-Deligne representation is isomorphic to this object.
As for the second part, one has to work much more. The situation in the potentially multiplicative cases (i.e. when the p-adic representation is potentially semi-stable but not potentially crystalline) can be made quite explicit, and gives rise to an infinite family of iso-

morphism classes, parametrised by $\{0,1\} \times \{\pm 1\} \times \mathbb{Q}_p$. The crystalline or twisted-crystalline cases lead to a finite set of classes, and the same for the potentially ordinary ones. Now the main difficulty lies in the non-twisted-crystalline potentially supersingular cases, which arise when 12 does not divide $p-1$; then, for each integer $e \in \{3,4,6\}$ dividing $p+1$, we obtain an infinite family of classes parametrised by $\mathbf{P}^1(\mathbb{Q}_p)$. The main ingredients of the proof are the Serre-Tate theorem ([Ka]), Fontaine's description of p-divisible groups via filtered Dieudonné modules ([Fo 4]), and a descent theorem which provides us a Galois criterion for saying when an elliptic curve having good reduction may be defined over a lower field.

Finally, for completeness' sake, we recall that for each prime l, a rank two $\mathbb{Z}_l[G]$-module T_l comes from an elliptic curve over $\mathbb{Q}_p$ if and only if the $\mathbb{Q}_l[G]$-module $\mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l$ does.

Here is a brief summary of the content of each chapter.

- Chapter 1 contains : the two theorems stated above and the "easy" part of the proof of THM II ; the precise description of the **WD*** and **D*** lists, together with the connections between the invariants of a given elliptic curve over $\mathbb{Q}_p$ and the objects corresponding to it in the lists ; some quasi-explicit examples with Weierstrass equations in the potentially good reduction cases ; and also several extra results, as the number of classes of $\mathbb{Q}_l[G]$-modules arising from elliptic curves over $\mathbb{Q}_p$ (for $l \neq p$ and $l = p$), the description of order two twists, of the image of G in $\mathrm{Aut}_{\mathbb{Q}_p}(V_p(E))$ in some cases, of the $\mathbb{F}_p[G]$-modules $E[p]$ and the $\mathbb{Z}_p[G]$-modules $T_p(E)$.

- Chapter 2 contains the statement and the proof of the following descent theorem :
Theorem : *Let K be a finite extension of $\mathbb{Q}_p$, $p \geq 5$, and L a totally ramified extension of K, with residue field k and respective absolute Galois groups G_K and G_L. Let E/L be an elliptic curve, having good reduction over L. Then E is defined over K if and only if the action of G_L extends to an action of G_K on $T_p(E)$ in such a way that this extended action "comes from" k-automorphisms of the special fiber of E (in a sense we define).*
When the k-endomorphisms ring of the special fiber is commutative, we show that the latter condition is equivalent to the following : the action of G_L extends to an action of G_K on the $T_l(E)$'s, as l runs through all rational primes, in such a way that the system of representations of the Weil-Deligne group of K induced by this action is compatible. Moreover, if we consider a "reasonably" extended action only on $T_p(E)$, or on $V_p(E)$, we obtain similar results, but up to isogeny.

- Chapter 3 deals with a deformation problem : given an elliptic curve $\widetilde{E}$ over $\mathbb{F}_p$, we describe, up to isomorphism, the elliptic schemes lifting $\widetilde{E}$ over the ring of integers of a totally ramified extension (whose ramification index is an integer in $\{1,2,3,4,6\}$ smaller than $p-1$). The answer to this problem is well known when the curve $\widetilde{E}/\mathbb{F}_p$ is ordinary ([Me], [Ka]), so that here we consider with more attention the case when $\widetilde{E}/\mathbb{F}_p$ is supersingular. We then use the results of chapter 2 in order to determine which liftings correspond to elliptic curves defined over $\mathbb{Q}_p$ (for those having good reduction of supersingular type), or are isogenous to an elliptic curve defined over $\mathbb{Q}_p$ (for those having good reduction of ordinary type). This enables us to finish the proof of THM II.

- Appendix A contains all the (case-by-case) computations needed to obtain the **WD*** and the **D*** lists ; note that for $l = p$ (i.e. the **D*** list), these computations are the same as in [Fo-Ma], but with conditions.

- Appendix B contains all the (again case-by-case) computations needed to classify $\mathbb{F}_p[G]$-vector spaces $E[p]$ and the $\mathbb{Z}_p[G]$-modules $T_p(E)$, with $E/\mathbb{Q}_p$ an elliptic curve. The results obtained are in no way original, see [Se 2] and [Kr] ; here we use a method based on calculus in $BW(R) \subset B_{cris}$ ([Fo 5]) in order to recover the potentially supersingular cases.

CHAPITRE 1

Les modules de Tate provenant d'une courbe elliptique sur $\mathbb{Q}_p$

On désigne par $\mathcal{P}$ l'ensemble des nombres premiers. Dans tout ce chapitre, on fixe un $p \in \mathcal{P}$ tel que $p \geq 5$.

On fixe une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$. On note $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ le groupe de Galois absolu, I son sous-groupe d'inertie, et $\mathbb{Q}_p^{nr}$ l'extension maximale non ramifiée de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}}_p$. Pour $l \in \mathcal{P}$, on note $\mu_{l^n}(\overline{\mathbb{Q}}_p)$ le groupe des racines l^n-ièmes de l'unité contenues dans $\overline{\mathbb{Q}}_p$, $n \geq 0$, et $\mathbb{Z}_l(1) = \varprojlim \mu_{l^n}(\overline{\mathbb{Q}}_p)$, $\mathbb{Q}_l(1) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} \mathbb{Z}_l(1)$. Le caractère cyclotomique donnant l'action de G sur $\mathbb{Q}_p(1)$ est noté $\chi : G \to \mathbb{Z}_p^\times$. La valuation p-adique v_p sur $\mathbb{Q}_p$ est normalisée par $v_p(p) = 1$; on note aussi v_p la valuation qui l'étend sur $\overline{\mathbb{Q}}_p$.

Soit E une courbe elliptique sur $\mathbb{Q}_p$. Soit $l \in \mathcal{P}$; pour $n \geq 0$, on note $E[l^n]$ les points de E à valeurs dans $\overline{\mathbb{Q}}_p$ d'ordre l^n, $T_l(E) = \varprojlim E[l^n]$ le module de Tate l-adique de E, et $V_l(E) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(E)$: c'est un $\mathbb{Q}_l$-espace vectoriel de dimension deux. Le groupe G agit linéairement et continuement sur $T_l(E)$, d'où des représentations, pour tout $l \in \mathcal{P}$:

$$\rho_l : G \longrightarrow \mathrm{Aut}_{\mathbb{Z}_l}(T_l(E)) \quad , \text{ et } \quad \rho_l : G \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(V_l(E)) \ .$$

Ce chapitre contient l'énoncé de conditions nécessaires et suffisantes pour qu'une représentation l-adique de G provienne du module de Tate d'une courbe elliptique sur $\mathbb{Q}_p$, et ce pour tout $l \in \mathcal{P}$ (théorèmes **1.1.**, **1.2.**, **2.1.**, et **2.2.**).
On décrit d'abord les invariants de courbes elliptiques dont nous aurons besoin (**1.1.**). Puis le chapitre se divise en deux parties : le cas $l \neq p$ (**1.2.**), et le cas $l = p$ (**1.3.**). Dans chacune de ces parties, on commence par donner des listes de classes d'isomorphisme de $\mathbb{Q}_l[G]$-modules, et l'on montre qu'un $\mathbb{Q}_l[G]$-module provient d'une courbe elliptique sur $\mathbb{Q}_p$ si et seulement si il est isomorphe à l'un des objets de la liste (thm. **1.1.** pour $l \neq p$ et thm. **2.1.** pour $l = p$). Le fait que toute représentation provenant d'une courbe elliptique sur $\mathbb{Q}_p$ soit isomorphe à l'un des objets des listes est l'objet de l'annexe A ; la réciproque est démontrée dans ce chapitre, *sauf* dans l'un des cas $l = p$, pour lequel le résultat est établi à la fin du chapitre 3 (**3.3.4.**).

Ensuite on décrit le lien de chaque objet des listes avec les invariants d'une courbe elliptique qui lui correspond ; pour $l \neq p$, ces invariants suffisent pour retrouver la représentation. Puis on démontre que les objets de ces listes sont exactement ceux qui vérifient certaines conditions ; on obtient ainsi les théorèmes **2.1.** et **2.2.**. Pour une courbe elliptique fixée, on compare en **1.3.2.** les représentations l-adiques, $l \neq p$, avec la représentation p-adique lui correspondant. On termine en donnant des exemples explicites dans les cas de potentielle bonne réduction (en **1.2.2.** pour $l \neq p$ et en **1.3.3.** pour $l = p$). Enfin, quand $l = p$, on donne la description de l'image de G dans certains cas (**1.3.4.**), ainsi que celle des $\mathbb{F}_p[G]$-modules $E[p]$ et des $\mathbb{Z}_p[G]$-modules $T_p(E)$ (**1.3.5.**, les calculs sont dans l'annexe B).

1.1. Notations :

1.1.1. Quelques invariants de courbes elliptiques sur $\mathbb{Q}_p$:

Pour tout ce qui concerne les courbes elliptiques, on pourra se référer aux livres de J.H. Silverman, [Silv 1] et [Silv 2] ; voir aussi [Huse].

Soit E une courbe elliptique sur $\mathbb{Q}_p$, i.e. une variété abélienne sur $\mathbb{Q}_p$ de dimension 1. Elle admet un modèle sous forme de cubique plane, dit modèle de Weierstrass, qui est donné par une équation de la forme

$$E \ : \ y^2 = x^3 + Ax + B \qquad \text{avec} \qquad A, B \in \mathbb{Q}_p \ , \text{ et } \ 4A^3 + 27B^2 \neq 0 \ .$$

Nous disposons tout d'abord d'un invariant $j_E = 1728.4A^3(4A^3+27B^2)^{-1}$ (avec $1728 = 12^3$), dit invariant modulaire de E ; il caractérise la classe d'isomorphisme de E sur $\overline{\mathbb{Q}}_p$. Le discriminant de E est $\Delta_E = -16(4A^3 + 27B^2) \neq 0$, et l'on a $j_E = -12^3(4A)^3\Delta_E^{-1}$; le quotient $\Delta_E \bmod (\mathbb{Q}_p^\times)^{12}$ est un invariant de la classe d'isomorphisme de E sur $\mathbb{Q}_p$. Le modèle de Weierstrass est dit *minimal* si $A, B \in \mathbb{Z}_p$ et $0 \leq v_p(\Delta_E) < 12$; on peut toujours se ramener à un tel modèle pour E.

Si $v_p(j_E) < 0$, alors E a potentiellement réduction "multiplicative déployée". Plus précisément, il existe un unique $q = q(j_E) \in p\mathbb{Z}_p\backslash\{0\}$, vérifiant

$$j_E = \frac{1}{q} + 744 + 196844\, q + \ldots$$

tel que E est le twist par un caractère d'ordre 1 ou 2 d'une courbe de Tate E_q (cf. [Silv 2], V, §5) ; ce twist correspond à l'extension $\mathbb{Q}_p(\sqrt{\gamma_E})/\mathbb{Q}_p$, où $\gamma_E = -2AB^{-1} \bmod (\mathbb{Q}_p^\times)^2 \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ (loc.cit., lemme 5.2.).
Rappelons que le groupe des points de E_q à valeurs dans $\overline{\mathbb{Q}}_p$ est isomorphe, en tant que groupe analytique p-adique, à $\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$; pour tout entier $n \geq 0$, on note $E_q[l^n]$ le noyau de la multiplication par l^n dans $\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$. D'une part, on a une injection naturelle de $\mu_{l^n}(\overline{\mathbb{Q}}_p)$ dans $E_q[l^n]$; d'autre part, si $x \in E_q[l^n]$, et si $\widehat{x}$ est un relèvement quelconque de x dans $\overline{\mathbb{Q}}_p^\times$, il existe un entier $N_q(\widehat{x})$ tel que $\widehat{x}^{l^n} = q^{N_q(\widehat{x})}$, et l'association $x \mapsto N_q(\widehat{x}) \bmod l^n\mathbb{Z}$ définit

un morphisme surjectif de $E_q[l^n]$ sur $\mathbb{Z}/l^n\mathbb{Z}$, dont le noyau est $\mu_{l^n}(\overline{\mathbb{Q}}_p)$. En faisant agir trivialement G sur les $\mathbb{Z}/l^n\mathbb{Z}$, on obtient par passage à la limite une suite exacte courte de $\mathbb{Z}_l[G]$-modules

$$(*_m) \qquad 0 \longrightarrow \mathbb{Z}_l(1) \longrightarrow T_l(E_q) \longrightarrow \mathbb{Z}_l \longrightarrow 0 \ ,$$

où l'indice "m" signifie "multiplicatif". On notera aussi $(*_m)$ la suite exacte de $\mathbb{Q}_l[G]$-modules obtenue en tensorisant avec $\mathbb{Q}_l$:

$$(*_m) \qquad 0 \longrightarrow \mathbb{Q}_l(1) \longrightarrow V_l(E_q) \longrightarrow \mathbb{Q}_l \longrightarrow 0 \ .$$

Si $v_p(j_E) \geq 0$, alors E a potentiellement bonne réduction : elle acquiert bonne réduction sur une extension finie de $\mathbb{Q}_p$. On appelle le *défaut de semi-stabilité* de $E/\mathbb{Q}_p$ l'indice de ramification minimal d'un corps sur lequel E acquiert bonne réduction, et on le note $\mathrm{dst}(E)$. On a

$$\mathrm{dst}(E) \ = \ \frac{12}{\mathrm{pgcd}(12, v_p(\Delta_E))} \ ,$$

où Δ_E est le discriminant de E. Si l'on choisit une équation de Weierstrass minimale pour E, alors $0 \leq v_p(\Delta_E) < 12$ et $v_p(j_E) \geq 0$ impliquent que $v_p(\Delta_E)$ n'est pas premier à 12 ; on voit donc que $e = 1, 2, 3, 4$, ou 6 suivant que $v_p(\Delta_E) = 0$, $v_p(\Delta_E) = 6$, $v_p(\Delta_E) \in \{4, 8\}$, $v_p(\Delta_E) \in \{3, 9\}$, ou $v_p(\Delta_E) \in \{2, 10\}$ respectivement. Remarquons que les entiers e qui interviennent sont exactement ceux qui vérifient $\varphi(e) \in \{1, 2\}$, où φ est la fonction arithmétique d'Euler. Rappelons également le critère d'Ogg-Néron-Shafarevich : E a bonne réduction sur $K \subset \overline{\mathbb{Q}}_p$ si et seulement si $I_K = I(\overline{\mathbb{Q}}_p/K)$ agit trivialement sur tous les $V_l(E)$, $l \neq p$ (ou bien, ce qui revient au même, sur l'un des $V_l(E)$, $l \neq p$).

Comme l'entier $e = \mathrm{dst}(E)$ est premier à p, la courbe E acquiert bonne réduction sur une extension finie totalement ramifiée de $\mathbb{Q}_p$ de degré e ; si L est une telle extension, on note $\widetilde{E}_L = (E \times_{\mathbb{Q}_p} L) \times_L \mathbb{F}_p$ sa courbe réduite sur $\mathbb{F}_p$, et $a_p(E) = a_p(\widetilde{E}_L)$ la trace du polynôme caractéristique du Frobenius arithmétique agissant sur $V_l(\widetilde{E}_L)$, $l \neq p$. Rappelons que $a_p(\widetilde{E}_L)$ est un entier rationnel indépendant de $l \neq p$, que l'on a $|\, a_p(\widetilde{E}_L)\,| \leq 2\sqrt{p}$, et aussi :

$$a_p(\widetilde{E}_L) = p + 1 - \#\widetilde{E}_L(\mathbb{F}_p) \ .$$

De plus, la courbe $\widetilde{E}_L/\mathbb{F}_p$ est ordinaire si p ne divise pas $a_p(\widetilde{E}_L)$; supersingulière si p divise $a_p(\widetilde{E}_L)$, ce qui équivaut à $a_p(\widetilde{E}_L) = 0$. Si E acquiert bonne réduction de type ordinaire sur L, la partie connexe $E_L(p)^0$ du groupe p-divisible $E_L(p)$ est de hauteur 1, et l'on a une suite exacte de groupes p-divisibles sur l'anneau des entiers de L :

$$0 \longrightarrow E_L(p)^0 \longrightarrow E_L(p) \longrightarrow \widetilde{E_L}(p) \longrightarrow 0 \ ,$$

qui induit la suite exacte courte de $\mathbb{Z}_p[G]$-modules

$$(*_{ord}) \qquad 0 \longrightarrow T_p(E_L(p)^0) \longrightarrow T_p(E) \longrightarrow T_p(\widetilde{E_L}) \longrightarrow 0 \ .$$

On notera également $(*_{ord})$ la suite exacte que l'on en déduit par extension des scalaires de $\mathbb{Z}_p$ à $\mathbb{Q}_p$.

1.1.2. Notations :

On note $\mathbb{Q}_{p^2}$ l'extension non ramifiée de degré 2 de $\mathbb{Q}_p$. On choisit $\pi_{12} \in \overline{\mathbb{Q}}_p$ vérifiant $(\pi_{12})^{12} + p = 0$. On pose : $\pi_6 = {\pi_{12}}^2$; $\pi_4 = {\pi_{12}}^3$; $\pi_3 = {\pi_{12}}^4$; $\pi_2 = {\pi_{12}}^6$; $\pi_1 = -p$. On choisit ζ_{12} une racine primitive douzième de l'unité, et l'on pose : $\zeta_6 = {\zeta_{12}}^2$; $\zeta_4 = {\zeta_{12}}^3$; $\zeta_3 = {\zeta_{12}}^4$.

On considère pour tout entier naturel $e \in \{1, 2, 3, 4, 6\}$ le corps $\mathbb{Q}_p(\pi_e)$: c'est une extension totalement ramifiée de degré e de $\mathbb{Q}_p$; comme $p \geq 5$, l'entier e est premier à p, et $\mathbb{Q}_p(\pi_e)/\mathbb{Q}_p$ est *modérément* ramifiée. On note K_e la clôture galoisienne de $\mathbb{Q}_p(\pi_e)$ dans $\overline{\mathbb{Q}}_p$, et $G_{K_e/\mathbb{Q}_p} = \mathrm{Gal}(K_e/\mathbb{Q}_p)$ son groupe de Galois ; I_e est le groupe d'inertie de l'extension $\overline{\mathbb{Q}}_p/K_e$. Comme $(\mathbb{Z}/e\mathbb{Z})^\times$ est d'ordre 1 ou 2, on a $p \equiv 1 \bmod e\mathbb{Z}$ ou bien $p \equiv -1 \bmod e\mathbb{Z}$. On se trouve alors dans l'une des situations suivantes :
$K_1 = \mathbb{Q}_p$ et $G_{K_1/\mathbb{Q}_p} = 1$; $K_2 = \mathbb{Q}_p(\pi_2)$ et $G_{K_2/\mathbb{Q}_p} = < \tau_2 >$, où τ_2 est défini par $\tau_2\pi_2 = -\pi_2$;
si $e \in \{3, 4, 6\}$ et $e \mid p-1$, $K_e = \mathbb{Q}_p(\pi_e)$ et $G_{K_e/\mathbb{Q}_p} = < \tau_e >$, où τ_e est défini par $\tau_e\pi_e = \zeta_e\pi_e$;
si $e \in \{3, 4, 6\}$ et $e \mid p+1$, $K_e = \mathbb{Q}_{p^2}(\pi_e) = \mathbb{Q}_p(\pi_e, \zeta_e)$ et $G_{K_e/\mathbb{Q}_p} = < \tau_e > \rtimes < \omega >$, où τ_e est défini par $\tau_e\pi_e = \zeta_e\pi_e$, $\tau_e\zeta_e = \zeta_e$, et ω est le relèvement du Frobenius absolu qui fixe π_e et tel que $\omega\zeta_e = {\zeta_e}^{-1}$; on a $\omega\tau_e = {\tau_e}^{-1}\omega$.
Si K'_e est une autre extension galoisienne de $\mathbb{Q}_p$ d'indice de ramification e, alors il existe une extension finie non ramifiée M de $\mathbb{Q}_p$ telle que $MK_e = MK'_e$.
Lorsqu'il n'y a aucune ambiguïté, on écrit K, $G_{K/\mathbb{Q}_p}$, au lieu de K_e et $G_{K_e/\mathbb{Q}_p}$.

Pour tout $u \in \mathbb{Z}_p^\times$, on note $\eta_u : G \to G/I \to \mathbb{Z}_p^\times$ l'unique caractère non ramifié qui envoie le Frobenius arithmétique sur u. Lorsque $e \geq 2$ et $e \mid p-1$, on note $\xi_e : G \to G_{K_e/\mathbb{Q}_p} \to \mu_e(\overline{\mathbb{Q}}_p) = <\zeta_e> \subset \mathbb{Z}_p^\times$ le caractère ramifié défini par $\xi_e(g) = g\pi_e/\pi_e$ pour tout $g \in G$.

Le groupe $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ est d'ordre 4, et il y a exactement 3 extensions quadratiques de $\mathbb{Q}_p$, une non ramifiée et deux totalement ramifiées. On les notera $M_1 = \mathbb{Q}_{p^2}$, $M_2 = \mathbb{Q}_p(\pi_2)$, et M_3 (par exemple, si $4 \mid p+1$, alors $M_3 = \mathbb{Q}_p(\zeta_4\pi_2)$).

On pose $\mathcal{N}_p = \{\, a \in \mathbb{Z} \,/\, |a| \leq 2\sqrt{p} \,\}$, et $\mathcal{N}_p^\times$ est l'ensemble des éléments non nuls de $\mathcal{N}_p$; le cardinal de $\mathcal{N}_p^\times$ est $2[2\sqrt{p}]$ (partie entière).
Soit $\Phi_e \in \mathbb{Q}[X]$ le e-ième polynôme cyclotomique ; on pose $\gamma_e = \zeta_e + \zeta_e^{-1} = \mathrm{Tr}(\Phi_e) = -1, 0, 1$ pour $e = 3, 4, 6$ respectivement. Quand $e \in \{3, 4, 6\}$ et $e \mid p-1$, on note $\mathcal{N}_{p,e}^\times$ l'ensemble des $a \in \mathbb{Z}$ tels que $(\gamma_e^2 - 4)(a^2 - 4p)$ est un carré dans $\mathbb{Q}$; c'est un sous-ensemble de $\mathcal{N}_p^\times$.
L'ensemble $\mathcal{N}_{p,3}^\times = \mathcal{N}_{p,6}^\times = \{\, a \in \mathbb{Z} \,/\, a^2 - 4p \equiv -3 \mod (\mathbb{Q}^\times)^2 \}$ est d'ordre 6, et l'ensemble $\mathcal{N}_{p,4}^\times = \{\, a \in \mathbb{Z} \,/\, a^2 - 4p \equiv -1 \mod (\mathbb{Q}^\times)^2 \}$ est d'ordre 4 ; lorsque $12 \mid p-1$, ces deux ensembles sont évidemment disjoints (pour une preuve de ces assertions, voir le lemme à la fin de **A.1.2.**). Par exemple :
$\mathcal{N}_{5,4}^\times = \{\pm 2, \pm 4\} \subset \mathcal{N}_5^\times = \{\pm 1, \pm 2, \pm 3, \pm 4\}$; $\mathcal{N}_{7,3}^\times = \{\pm 1, \pm 4, \pm 5\} \subset \mathcal{N}_7^\times = \{\pm 1, \ldots, \pm 5\}$;
$\mathcal{N}_{13,3}^\times = \{\pm 2, \pm 5, \pm 7\}$ et $\mathcal{N}_{13,4}^\times = \{\pm 4, \pm 6\} \subset \mathcal{N}_{13}^\times = \{\pm 1, \ldots, \pm 7\}$.

1.2. Les cas $l \neq p$:

1.2.1. Les $\mathbb{Q}_l[G]$-modules, $l \neq p$, provenant d'une courbe elliptique sur $\mathbb{Q}_p$:

On désigne par $\mathbf{Rep}_{\mathbb{Q}_l}(G)$ la catégorie des représentations l-adiques de G, c'est-à-dire des $\mathbb{Q}_l$-espaces vectoriels de dimension finie munis d'une action linéaire et continue de G.
Un système $(V_l)_{l\neq p}$ de représentations l-adiques de G est la donnée pour chaque $l \neq p$ d'un objet V_l de $\mathbf{Rep}_{\mathbb{Q}_l}(G)$. On aimerait pouvoir comparer les V_l, $l \neq p$, entre eux ; cela n'aura de sens que si l'on "enlève la topologie sur G", c'est-à-dire si l'on se restreint au groupe de Weil de G, et si l'on plonge les $\mathbb{Q}_l$ dans $\mathbb{C}$ (voir [Roh]). Plus précisément, nous allons nous ramener pour chaque $l \neq p$ à la catégorie des représentations $\mathbb{Q}_l$-linéaires et continues du groupe de Weil-Deligne $'W$ de $\mathbb{Q}_p$.

1.2.1.1. Le groupe de Weil $W = W_{\mathbb{Q}_p}$ de G est le sous-groupe de G constitué des éléments g tels que $g \bmod I$ est une puissance entière du Frobenius (lequel est un générateur topologique de $G/I = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$). On a donc une suite exacte courte :

$$1 \longrightarrow I \longrightarrow W \xrightarrow{v} \mathbb{Z} \longrightarrow 1 ,$$

avec $v(\text{Frob.arithm.}) = 1$. On désigne par $'W = {}'W_{\mathbb{Q}_p}$ le groupe de Weil-Deligne de G : c'est le schéma en groupe sur $\mathbb{Q}$ qui est le produit semi-direct de W par le groupe additif $\mathbb{G}_a$, sur lequel W opère par $wxw^{-1} = p^{v(w)}x$, pour $w \in W$.
Soit E un corps de caractéristique 0. On note $\mathbf{Rep}_E('W)$ la catégorie des représentations E-linéaires de $'W$, i.e. des E-espaces vectoriels de dimension finie munis d'une action linéaire et continue de $'W$. Un objet dans $\mathbf{Rep}_E('W)$ peut être considéré comme un triplet (Δ, ρ_0, N), où : Δ est un espace vectoriel sur E de dimension finie ; $\rho_0 : W \longrightarrow \mathrm{Aut}_E(\Delta)$ est un morphisme dont le noyau contient un sous-groupe ouvert de I ; $N \in \mathrm{End}_E(\Delta)$ et vérifie : $\forall\, w \in W$, $\rho_0(w)N = p^{v(w)}N\rho_0(w)$. Si l'action de $'W$ est F-semi-simple (i.e. si l'action de W par ρ_0 est semi-simple), alors un objet de $\mathbf{Rep}_E('W)$ est déterminé à isomorphisme près par les traces $\mathrm{Tr}(\rho_0) : W \to E$, ainsi que par le polynôme minimal de l'opérateur N.

Soient E et E' deux corps de caractéristique 0 munis de plongements $\iota : E \hookrightarrow \mathbb{C}$ et $\iota' : E' \hookrightarrow \mathbb{C}$. Si Δ est un objet de $\mathbf{Rep}_E('W)$ qui est défini sur $\mathbb{Q}$ (cf. [Fo 3] ou bien **2.2.1.**), alors $\Delta \otimes_{E\nearrow_\iota} \mathbb{C}$ est un objet de $\mathbf{Rep}_{\mathbb{C}}('W)$ dont la classe d'isomorphisme ne dépend pas du choix de ι (voir par exemple [Roh]). Deux objets Δ et Δ' de $\mathbf{Rep}_E('W)$ et $\mathbf{Rep}_{E'}('W)$ respectivement sont dits *compatibles* s'ils sont tous deux définis sur $\mathbb{Q}$ et si $\Delta \otimes_{E\nearrow_\iota} \mathbb{C}$ et $\Delta' \otimes_{E'\nearrow_{\iota'}} \mathbb{C}$ sont isomorphes dans $\mathbf{Rep}_{\mathbb{C}}('W)$.

On désigne par $\mathbf{Rep}^\circ_{\mathbb{Q}_l}('W)$ la sous-catégorie tannakienne de $\mathbf{Rep}_{\mathbb{Q}_l}('W)$ constituée des objets sur lesquels les racines du polynôme caractéristique d'un relèvement du Frobenius sont des unités l-adiques. Il existe un foncteur (covariant) établissant une équivalence de catégories entre $\mathbf{Rep}^\circ_{\mathbb{Q}_l}('W)$ et $\mathbf{Rep}_{\mathbb{Q}_l}(G)$, qui peut être décrit de la manière qui suit (voir par exemple [Roh]). Soit (Δ_l, ρ_0, N) un objet de $\mathbf{Rep}^\circ_{\mathbb{Q}_l}('W)$. Si $N = 0$, alors on retrouve la représentation l-adique de G qui lui correspond en "complétant" le morphisme $\rho_0 : W \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$ en un morphisme $\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$ (car les racines de $\mathrm{P}_{car}(\mathrm{Frob})$ sont dans $\mathbb{Z}_l^\times$). Si $N \neq 0$, on étend ρ_0 à G comme ci-dessus, et l'on choisit un homomorphisme continu non trivial $t_l : I \to \mathbb{Q}_l$ (il est unique à multiplication par un élément de $\mathbb{Q}_l^\times$ près). Alors la représentation $\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$ est donnée par $\rho(g) = \rho_0(g)\exp(t_l(h)N)$, où l'on a écrit $g \in G$ sous la forme $g = \omega h$ avec $\omega \in \mathrm{Gal}(\mathbb{Q}_p^{nr}/\mathbb{Q}_p)$ et $h \in I$ (l'opérateur N est nilpotent). La classe d'isomorphisme dans $\mathbf{Rep}_{\mathbb{Q}_l}(G)$ de l'objet ainsi obtenu ne dépend pas du choix de t_l, et le foncteur quasi-inverse est défini de manière évidente.
Nous étudions ici le *dual* de la représentation du groupe de Weil-Deligne provenant du module de Tate l-adique $V_l(E)$ d'une courbe elliptique $E/\mathbb{Q}_p$. On utilise le foncteur $\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}$: $\mathbf{Rep}_{\mathbb{Q}_l}(G) \to \mathbf{Rep}_{\mathbb{Q}_l}('W)$ qui est la version *contravariante* de celui décrit dans [Fo 3], i.e.

$\mathbf{W\hat{D}^*_{pst,l}}$ est le foncteur obtenu en appliquant $\mathbf{W\hat{D}_{pst,l}}$ à la représentation duale ; il établit une anti-équivalence de catégories entre $\mathbf{Rep}_{\mathbb{Q}_l}(G)$ et $\mathbf{Rep}^\circ_{\mathbb{Q}_l}('W)$, et les classes d'isomorphisme que l'on obtient sont les mêmes que celles obtenues avec le dual du foncteur mentionné ci-desssus. Comme $V_l(E)$ est le dual de $H^1_{\acute{e}t}(E\times_{\mathbb{Q}_p}\overline{\mathbb{Q}}_p,\mathbb{Q}_l)$ pour une courbe elliptique $E/\mathbb{Q}_p$, on peut voir le foncteur $\mathbf{W\hat{D}^*_{pst,l}}$ comme un foncteur covariant des $H^1_{\acute{e}t}$ dans $\mathbf{Rep}^\circ_{\mathbb{Q}_l}('W)$.

Choisissons pour chaque $l\neq p$ des plongements de corps $\iota_l:\mathbb{Q}_l\hookrightarrow\mathbb{C}$. La *compatibilité* d'un système $(\Delta_l)_{l\neq p}$ de représentations l-adiques de $'W$ signifie que les Δ_l sont deux-à-deux compatibles lorsque l parcourt $\mathcal{P}\backslash\{p\}$.
Supposons que chaque Δ_l, $l\neq p$, est F-semi-simple. Si l'opérateur de monodromie N est nul pour tous les Δ_l, la compatibilité du système $(\Delta_l)_{l\neq p}$ signifie que les traces $\mathrm{Tr}\rho_0 : W\longrightarrow\mathbb{Q}_l$ sont à valeurs dans $\mathbb{Q}$ et indépendantes de $l\in\mathcal{P}\backslash\{p\}$. Sinon, pour chaque Δ_l, l'opérateur N étant nilpotent, il existe une unique filtration finie croissante $(\mathrm{Fil}^{JM}_i\Delta_l)_{i\in\mathbb{Z}}$, dite de *Jacobson-Morosov*, telle que $N(\mathrm{Fil}^{JM}_i\Delta_l)\subset\mathrm{Fil}^{JM}_{i-2}\Delta_l$ et que N induise un isomorphisme $N^i:\mathrm{Gr}^{JM}_i\Delta_l\xrightarrow{\sim}\mathrm{Gr}^{JM}_{-i}\Delta_l$ pour tout $i\in\mathbb{Z}$ ([Fo 3], 2.4.5.) ; alors la compatibilité du système $(\Delta_l)_{l\neq p}$ signifie que, pour tout $i\in\mathbb{Z}$, les traces $\mathrm{Tr}(\mathrm{Gr}^{JM}_i\Delta_l):W\longrightarrow\mathbb{Q}_l$ sont à valeurs dans $\mathbb{Q}$ et indépendantes de $l\in\mathcal{P}\backslash\{p\}$.

1.2.1.2. On note $\phi\in W$ un relèvement du Frobenius géométrique modulo $I(\overline{\mathbb{Q}}_p/\mathbb{Q}_p(\pi_{12}))$: pour tout $e\in\{1,2,3,4,6\}$, ϕ agit trivialement sur L_e et ϕ mod I_e agit par $x\mapsto x^{-p}$. Pour $e\in\{2,3,4,6\}$, on note θ_e un relèvement dans I de $\tau_e\in I/I_e=I(K_e/\mathbb{Q}_p)$.
Si $e\in\{3,4,6\}$ divise $p-1$, alors $\zeta_e\in\mathbb{Z}_p^\times$ et le polynôme $X^2-\gamma_eX+1=(X-\zeta_e)(X-\zeta_e^{-1})$ se scinde dans $\mathbb{Q}_p[X]$; il en est de même pour le polynôme X^2-aX+p lorsque $a\in\mathbb{Z}_p^\times$ (Hensel) : il existe alors un unique $u_a\in\mathbb{Z}_p^\times$ tel que $X^2-aX+p=(X-u_a)(X-u_a^{-1}p)$. On pose

$$t_\epsilon=t_\epsilon(a,e)=u_a\zeta_e^\epsilon+u_a^{-1}p\,\zeta_e^{-\epsilon}\ \text{, pour }\ \epsilon\in\{-1,1\}\,.$$

On a : $(X-t_1)(X-t_{-1})=X^2-\gamma_eaX+p{\gamma_e}^2+a^2-4p=T(X)$, et si $a\in\mathbb{Z}\cap\mathbb{Z}_p^\times$, alors $T(X)\in\mathbb{Z}[X]$. La condition $a\in\mathcal{N}^\times_{p,e}$ signifie exactement que les racines t_1 et t_{-1} du polynôme $T(X)$ sont dans $\mathbb{Q}$; elles sont distinctes.

Soit E un corps de caractéristique 0. La liste $\mathbf{WD^*}$ suivante définit à isomorphisme près des objets de $\mathbf{Rep}_E('W)$ de dimension deux, qui sont dans $\mathbf{Rep}^\circ_{\mathbb{Q}_l}('W)$ lorsque $E=\mathbb{Q}_l$:

$\mathbf{WD^*_m(e;b)}$, $e\in\{1,2\}$, $b\in\{-1,1\}$:
$\rho_0(I_2)=1$; $\rho_0(\theta_2)=(-1)^{e-1}$; $\mathrm{P}_{min}(\rho_0(\phi))=(X-b)(X-bp)$; $\mathrm{P}_{min}(N)=X^2$; $\rho_0(\phi)N=p^{-1}N\rho_0(\phi)$.

$\mathbf{WD^*_c(e;a_p)}$, $e\in\{1,2\}$, $a_p\in\mathcal{N}_p$:
$\rho_0(I_2)=1$; $\rho_0(\theta_2)=(-1)^{e-1}$; $\mathrm{P}_{min}(\rho_0(\phi))=X^2-a_pX+p$; $N=0$.

$\mathbf{WD^*_{pc}(e;a_p;\epsilon)}$, $e\in\{3,4,6\}$ et $e\mid p-1$, $a_p\in\mathcal{N}^\times_{p,e}$, $\epsilon\in\{-1,1\}$:
$\rho_0(I_e)=1$; $\mathrm{P}_{min}(\rho_0(\theta_e))=X^2-\gamma_eX+1$; $\mathrm{P}_{min}(\rho_0(\phi))=X^2-a_pX+p$; $\mathrm{P}_{min}(\rho_0(\phi)\rho_0(\theta_e))=X^2-t_\epsilon X+p$; $\rho_0(\phi)\rho_0(\theta_e)=\rho_0(\theta_e)\rho_0(\phi)$; $N=0$.

$\mathbf{WD^*_{pc}(e;0)}$, $e\in\{3,4,6\}$ et $e\mid p+1$:
$\rho_0(I_e)=1$; $\mathrm{P}_{min}(\rho_0(\theta_e))=X^2-\gamma_eX+1$; $\mathrm{P}_{min}(\rho_0(\phi))=X^2+p$; $\rho_0(\phi)\rho_0(\theta_e)=\rho_0(\theta_e)^{-1}\rho_0(\phi)$; $N=0$.

Remarque : les classes d'isomorphisme de ces objets ne dépendent pas du choix des corps K_e : si, dans la description de l'un de ces objets Δ, on remplace K_e par une autre extension galoisienne de $\mathbb{Q}_p$ d'indice de ramification e, on obtient un objet Δ' qui est isomorphe à Δ.

Chacun de ces objets est défini sur $\mathbb{Q}$. De plus, la représentation E-linéaire de $'W$ de dimension un $\wedge^2\mathbf{WD}^*$ est donnée par : $\rho_0(I) = 1$, $\rho_0(\phi) = p$, $N = 0$; et si $E = \mathbb{Q}_l$, l'objet obtenu en appliquant le foncteur quasi-inverse est $\mathbb{Q}_l(1)$.
Les objets du type $\mathbf{WD}^*_{\mathbf{m}}$ sont des twists d'ordre 1 ou 2 d'un objet semi-stable sur $\mathbb{Q}_p$, mais ils n'ont pas potentiellement bonne réduction. Les objets du type $\mathbf{WD}^*_{\mathbf{c}}$ sont des twists par un caractère d'ordre 1 ou 2 d'objets ayant bonne réduction sur $\mathbb{Q}_p$. Les objets du type $\mathbf{WD}^*_{\mathbf{pc}}$ ont potentiellement bonne réduction, mais *ne sont pas* des twists d'objets ayant bonne réduction sur $\mathbb{Q}_p$.

Description des twists d'ordre 2 :

Soit Δ un objet de la liste $\mathbf{WD}^*$ ci-dessus. En tordant par l'un des caractères (non trivial) d'ordre 2, on obtient les objets Δ_1, Δ_2, et Δ_3, correspondant respectivement aux extensions quadratiques M_1, M_2, et M_3 de $\mathbb{Q}_p$. Les quatre objets Δ, Δ_1, Δ_2 et Δ_3 sont liés entre eux par des twists d'ordre 2 de la manière suivante : les paires (Δ, Δ_1) et (Δ_2, Δ_3) sont composées d'objets liés par un twist non ramifié ; les paires (Δ, Δ_2), (Δ, Δ_3), (Δ_1, Δ_2) et (Δ_1, Δ_3) sont composées d'objets liés par un twist ramifié. En faisant varier Δ parmi les objets de la liste, on obtient :

$\Delta = \mathbf{WD}^*_{\mathbf{m}}(\mathbf{1};\mathbf{b})$; $\Delta_1 = \mathbf{WD}^*_{\mathbf{m}}(\mathbf{1};-\mathbf{b})$; $\Delta_2 = \mathbf{WD}^*_{\mathbf{m}}(\mathbf{2};\mathbf{b})$; $\Delta_3 = \mathbf{WD}^*_{\mathbf{m}}(\mathbf{2};-\mathbf{b})$.

$\Delta = \mathbf{WD}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_p})$; $\Delta_1 = \mathbf{WD}^*_{\mathbf{c}}(\mathbf{1};-\mathbf{a_p})$; $\Delta_2 = \mathbf{WD}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_p})$; $\Delta_3 = \mathbf{WD}^*_{\mathbf{c}}(\mathbf{2};-\mathbf{a_p})$.

$\Delta = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_p};\epsilon)$; $\Delta_1 = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};-\mathbf{a_p};\epsilon)$; $\Delta_2 = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_p};-\epsilon)$; $\Delta_3 = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};-\mathbf{a_p};-\epsilon)$.

$\Delta = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{a_p};\epsilon)$; $\Delta_1 = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{3};-\mathbf{a_p};\epsilon)$; $\Delta_2 = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{a_p};-\epsilon)$; $\Delta_3 = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{6};-\mathbf{a_p};-\epsilon)$.

$\Delta = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{0}) = \Delta_1 = \Delta_2 = \Delta_3$.

$\Delta = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{0}) = \Delta_1$; $\Delta_2 = \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{0}) = \Delta_3$.

Si un objet Δ de la liste $\mathbf{WD}^*$ provient d'une courbe elliptique E sur $\mathbb{Q}_p$, c'est-à-dire s'il existe $E/\mathbb{Q}_p$ telle que $\Delta \simeq \mathbf{WD}^*_{\mathbf{pst,l}}(V_l(E))$, alors les objets Δ_i, $i \in \{1,2,3\}$, proviennent des courbes elliptiques E_i sur $\mathbb{Q}_p$ obtenues en tordant E par les caractères d'ordre 2 correspondant aux extensions quadratiques M_i.

Théorème 1.1. :
Soient $p \geq 5$ et $l \in \mathcal{P}$, $l \neq p$.
1) Les représentations de la liste $\mathbf{WD}^*$ ci-dessus sont deux-à-deux non-isomorphes.
2) Soit E une courbe elliptique sur $\mathbb{Q}_p$; alors $\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(E))$ est isomorphe à l'un des objets de la liste $\mathbf{WD}^*$.
3) Réciproquement, tous ces objets proviennent d'un $V_l(E)$, où E est une courbe elliptique sur $\mathbb{Q}_p$.

1.2.1.3. Soit $E/\mathbb{Q}_p$ une courbe elliptique. On obtient la classe de $\mathbf{WD}^*_{\mathbf{pst,l}}(V_l(E))$ au moyen de certains invariants de E (voir **A.1.**) ; posons $\mathbf{WD}^*_{\mathbf{pst,l}}(V_l(E)) = \Delta_l(E)$.

$\Delta_l(E) \simeq \mathbf{WD^*_m(e;b)}$: E est une courbe elliptique dont l'invariant modulaire j_E vérifie $v_p(j_E) < 0$. Soit $\gamma_E \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ (cf. **1.1.**) ; alors on a :
$(e;b) = (1;1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_p$, et E est isomorphe sur $\mathbb{Q}_p$ à une courbe de Tate E_q, avec $q \in \mathbb{Q}_p^\times$, $v_p(q) > 0$, et q est uniquement déterminé par j_E.
$(e;b) = (1;-1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_{p^2} = M_1$, et E est le twist sur M_1 d'une courbe E_q.
$(e;b) = (2;1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_p(\pi_2) = M_2$, et E est le twist sur M_2 d'une courbe E_q.
$(e;b) = (2;-1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = M_3$, et E est le twist sur M_3 d'une courbe E_q.

$\Delta_l(E) \simeq \mathbf{WD^*_c(e;a_p)}$: on a $v_p(j_E) \geq 0$ et $e = 12/\mathrm{pgcd}(v_p(\Delta_E), 12) = \mathrm{dst}(E)$. Si $e = 1$, la courbe E a bonne réduction sur $\mathbb{Q}_p$, et a_p est la trace du polynôme caractéristique du Frobenius arithmétique agissant sur la courbe réduite $\widetilde{E}$. Si $e = 2$, la courbe E est le twist par le caractère ramifié d'ordre 2 correspondant à l'extension $M_2 = \mathbb{Q}_p(\pi_2)$ d'une courbe elliptique du type précédent.

$\Delta_l(E) \simeq \mathbf{WD^*_{pc}(e;a_p;\epsilon)}$: on a $v_p(j_E) \geq 0$ et $e = 12/\mathrm{pgcd}(v_p(\Delta_E), 12) = \mathrm{dst}(E)$ divise $p-1$; la courbe E acquiert bonne réduction ordinaire sur $\mathbb{Q}_p(\pi_e)$, et a_p est la trace du polynôme caractéristique du Frobenius arithmétique agissant sur la courbe réduite. Lorsque l'on prend une équation de Weierstrass minimale pour E, alors $\epsilon = 1$ si $v_p(\Delta_E) < 6$ (i.e. $v_p(\Delta_E) \in \{2,3,4\}$), et $\epsilon = -1$ si $v_p(\Delta_E) > 6$ (i.e. $v_p(\Delta_E) \in \{8,9,10\}$). De plus, j_E est un entier p-adique vérifiant $j_E \equiv 1728 \bmod p\mathbb{Z}_p$ si $e = 4$ et $j_E \equiv 0 \bmod p\mathbb{Z}_p$ si $e = 3$ ou 6. Pour les twists d'ordre 2, voir la description faite précédemment.

$\Delta_l(E) \simeq \mathbf{WD^*_{pc}(e;0)}$: on a $v_p(j_E) \geq 0$ et $e = 12/\mathrm{pgcd}(v_p(\Delta_E), 12) = \mathrm{dst}(E)$ divise $p+1$; la courbe E acquiert bonne réduction supersingulière sur $\mathbb{Q}_p(\pi_e)$. De plus, j_E est un entier p-adique vérifiant $j_E \equiv 1728 \bmod p\mathbb{Z}_p$ si $e = 4$ et $j_E \equiv 0 \bmod p\mathbb{Z}_p$ si $e = 3$ ou 6. Pour les twists d'ordre 2, voir la description faite précédemment.

Remarque : Soit $E/\mathbb{Q}$ fixée. Pour chaque $l \in \mathcal{P}\backslash\{p\}$, l'objet $\mathbf{WD^*_{pst,l}}(V_l(E)) = \Delta_l(E)$ est F-semi-simple et défini sur $\mathbb{Q}$; on constate de plus que les classes d'isomorphisme des représentations de $'W$ sur $\Delta_l(E)$ sont indépendantes de l : ceci exprime la compatibilité au sens de Weil-Deligne du système de représentations $V_l(E)$, $l \neq p$.

1.2.1.4. *Preuve du théorème 1.1. :*
Les parties *1)* et *2)* sont l'objet de l'annexe A, **A.1.** ; quant à la partie *3)*, nous allons la montrer ici. Si $\widetilde{E}$ est une courbe elliptique sur $\mathbb{F}_p$, on note $a_p(\widetilde{E}) \in \mathcal{N}_p$ la trace du Frobenius arithmétique agissant sur $\widetilde{E}$ (i.e. sur $V_l(\widetilde{E})$, $l \neq p$).

C'est évident pour les cas $\mathbf{WD^*_m}$: il suffit de prendre n'importe quelle courbe de Tate E_q sur $\mathbb{Q}_p$ (avec $q \in p\mathbb{Z}_p\backslash\{0\}$), et de la tordre sur l'extension quadratique M_i, $i \in \{0,1,2,3\}$, avec $i = 0$ et $M_0 = \mathbb{Q}_p$ si $(e;b) = (1;1)$, $i = 1$ si $(e;b) = (1;-1)$, $i = 2$ si $(e;b) = (2;1)$, et $i = 3$ si $(e;b) = (2;-1)$.

Les représentations $\mathbf{WD^*_c(1;a_p)}$ proviennent toutes de schémas elliptiques E sur $\mathbb{Z}_p$ dont la trace du Frobenius (arithmétique) agissant sur la courbe réduite $\widetilde{E}$ est a_p. En effet, d'après Honda-Tate, pour tout $a_p \in \mathcal{N}_p$, il existe une courbe $\widetilde{E}/\mathbb{F}_p$ telle que $a_p(\widetilde{E}) = a_p$ ([Ho-Ta]) ; puis toute courbe elliptique sur $\mathbb{F}_p$ se relève en un schéma elliptique sur $\mathbb{Z}_p$ (voir par exemple **3.2.**). Les représentations $\mathbf{WD^*_c(2;a_p)}$ proviennent d'un twist correspondant à l'extension $\mathbb{Q}_p(\pi_2) = M_2$ d'une courbe elliptique du type précédent.

Si $e \in \{3,4,6\}$ et $e \mid p+1$, la courbe elliptique E sur $\mathbb{Q}_p$ d'équation de Weierstrass :

$$E \ : \ \begin{cases} y^2 &= x^3+x & \text{si } e=4 \\ y^2 &= x^3+1 & \text{si } e \in \{3,6\} \end{cases}$$

est d'invariant modulaire $j(e)$, avec $j(4)=1728$ et $j(3)=j(6)=0$; elle a bonne réduction sur $\mathbb{Q}_p$, et sa courbe réduite est supersingulière (voir [Silv 1],V, Thm.4.1., et les exemples 4.4. et 4.5. qui suivent). Ses tordues sur $\overline{\mathbb{Q}}_p$ (voir [Silv 1],X) ont pour équation de Weierstrass :

$$E_D \ : \ \begin{cases} y^2 &= x^3+Dx & \text{si } e=4 \\ y^2 &= x^3+D & \text{si } e \in \{3,6\}\ , \end{cases}$$

avec $D \in \mathbb{Q}_p^\times$, et leurs classes d'isomorphisme sur $\mathbb{Q}_p$ sont en bijection avec $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^{n(e)}$, avec $n(4)=4$ et $n(3)=n(6)=6$ ([Silv 1],X, Prop.5.4.). Alors les courbes E_D, où $D \in \{-p,p^2\} \subset \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^{n(e)}$, fournissent des courbes elliptiques sur $\mathbb{Q}_p$ potentiellement supersingulières (d'où $a_p(E_D)=0$), dont le défaut de semi-stabilité est :

$$\begin{cases} \mathrm{dst}(E_{(-p)})=4 & \text{si } e=4 \\ \mathrm{dst}(E_{(-p)})=6 \ ; \ \mathrm{dst}(E_{p^2})=3 & \text{si } e \in \{3,6\} \end{cases}$$

On en déduit que les $\mathbf{WD}^*_{\mathbf{pst,l}}(V_l(E_D))$ sont isomorphes aux $\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0})$ (voir aussi les exemples plus loin).

Si $e \in \{3,4,6\}$ et $e \mid p-1$, les courbes E_D définies comme ci-dessus sont toujours d'invariant modulaire $j(e)$ et leur défaut de semi-stabilité est inchangé, mais elles sont cette fois potentiellement ordinaires ([Silv 1],V, 4.4. et 4.5.). Compte tenu de la description des twists d'ordre 2 (l'invariant ϵ parcourt $\{\pm 1\}$), il suffit de montrer que tous les $a_p \in \mathcal{N}_{p,e}^\times$ se réalisent comme la trace du Frobenius arithmétique agissant sur une courbe elliptique sur $\mathbb{F}_p$ d'invariant modulaire $\tilde{\jmath}(e) \in \mathbb{F}_p$, avec $\tilde{\jmath}(4)=1728$ et $\tilde{\jmath}(3)=\tilde{\jmath}(6)=0$. C'est l'objet du lemme qui suit. On en déduit que cette fois les $\mathbf{WD}^*_{\mathbf{pst,l}}(V_l(E_D))$ sont isomorphes aux $\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\mathbf{1})$; leurs tordues par un caractère ramifié d'ordre 2 donnent des courbes dont les représentations associées sont isomorphes aux $\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\mathbf{-1})$ (voir les exemples plus loin). □

Pour $u \in \mathbb{F}_p^\times$, on note $\widetilde{E}_u$ et $\widetilde{\mathcal{E}}_u$ les courbes elliptiques sur $\mathbb{F}_p$ données par les équations de Weierstrass suivantes :

$$\widetilde{E}_u \ : \ y^2=x^3+ux \qquad \text{et} \qquad \widetilde{\mathcal{E}}_u \ : \ y^2=x^3+u\ .$$

Pour tout $u \in \mathbb{F}_p^\times$, on a $j(\widetilde{E}_u)=1728=12^3$, d'où $\widetilde{E}_u$ est ordinaire si $4 \mid p-1$, supersingulière si $4 \mid p+1$; et $j(\widetilde{\mathcal{E}}_u)=0$, d'où $\widetilde{\mathcal{E}}_u$ est ordinaire si $3 \mid p-1 \Leftrightarrow 6 \mid p-1$, supersingulière si $3 \mid p+1$ ([Silv 1],V, 4.4. et 4.5.). Toute courbe elliptique $\widetilde{E}/\mathbb{F}_p$ dont l'invariant modulaire est $j(\widetilde{E})=1728$ (resp. 0) est isomorphe sur $\mathbb{F}_p$ à l'une des $\widetilde{E}_u$ (resp. $\widetilde{\mathcal{E}}_u$).
On a deux flèches $\mathbb{F}_p^\times \to \mathcal{N}_p$, l'une qui à $u \in \mathbb{F}_p^\times$ associe $a_p(\widetilde{E}_u)$, l'autre qui à u associe $a_p(\widetilde{\mathcal{E}}_u)$; la première est nulle si et seulement si $4 \mid p+1$, et la deuxième si et seulement si $3 \mid p+1$. De plus, les courbes $\widetilde{E}_u$ et $\widetilde{E}_{u'}$ (resp. $\widetilde{\mathcal{E}}_u$ et $\widetilde{\mathcal{E}}_{u'}$) sont isomorphes sur $\mathbb{F}_p$ si et seulement si $u \equiv u' \bmod (\mathbb{F}_p^\times)^4$ (resp. $u \equiv u' \bmod (\mathbb{F}_p^\times)^6$) ([Silv 1], X, Prop.5.4.). Comme l'entier $a_p(\widetilde{E})$ caractérise la classe d'isogénie sur $\mathbb{F}_p$ de la courbe $\widetilde{E}/\mathbb{F}_p$ ([Ta]), on en déduit des applications :

$$\begin{cases} \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^4 & \longrightarrow & \mathcal{N}_p \\ u \bmod (\mathbb{F}_p^\times)^4 & \longmapsto & a_p(\widetilde{E}_u) \end{cases} \qquad \text{et} \qquad \begin{cases} \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^6 & \longrightarrow & \mathcal{N}_p \\ u \bmod (\mathbb{F}_p^\times)^6 & \longmapsto & a_p(\widetilde{\mathcal{E}}_u) \end{cases}$$

de l'ensemble des classes d'isomorphisme sur $\mathbb{F}_p$ de courbes elliptiques d'invariant modulaire 1728 (resp. 0) dans l'ensemble des classes d'isogénie sur $\mathbb{F}_p$ de courbes elliptiques sur $\mathbb{F}_p$. Rappelons que si $4 \mid p-1$, l'ensemble $\mathcal{N}_{p,4}^{\times} = \{a \in \mathbb{Z}/a^2 - 4p \equiv -1 \mod (\mathbb{Q}^{\times})^2\} \subset \mathcal{N}_p^{\times}$ est d'ordre 4, et si $3 \mid p-1$, l'ensemble $\mathcal{N}_{p,3}^{\times} = \mathcal{N}_{p,6}^{\times} = \{a \in \mathbb{Z}/a^2 - 4p \equiv -3 \mod (\mathbb{Q}^{\times})^2\} \subset \mathcal{N}_p^{\times}$ est d'ordre 6 (cf. le lemme de **A.1.2.**).

Lemme :
Si $4 \mid p-1$, *l'application* $u \mapsto a_p(\widetilde{E}_u)$ *induit une bijection* $\mathbb{F}_p^{\times}/(\mathbb{F}_p^{\times})^4 \xrightarrow{\sim} \mathcal{N}_{p,4}^{\times}$.
Si $3 \mid p-1$, *l'application* $u \mapsto a_p(\widetilde{\mathcal{E}}_u)$ *induit une bijection* $\mathbb{F}_p^{\times}/(\mathbb{F}_p^{\times})^6 \xrightarrow{\sim} \mathcal{N}_{p,3}^{\times}$.
En particulier, la classe d'isogénie sur $\mathbb{F}_p$ *d'une courbe elliptique d'invariant modulaire* 1728 *ou* 0 *est aussi sa classe d'isomorphisme sur* $\mathbb{F}_p$.

Preuve :
Supposons d'abord $4 \mid p-1$: alors les $\widetilde{E}_u$ sont ordinaires, et $a_p(\widetilde{E}_u) \in \mathcal{N}_p^{\times}$. De plus, le groupe des racines quatrièmes de l'unité $\mu_4(\mathbb{F}_p)$ est d'ordre 4, d'où $\mathbb{F}_p^{\times}/(\mathbb{F}_p^{\times})^4$ aussi, et de même pour $\mathcal{N}_{p,4}^{\times}$. Il suffit donc de montrer que la flèche

$$\begin{cases} \mathbb{F}_p^{\times} & \longrightarrow & \mathcal{N}_p^{\times} \\ u & \longmapsto & a_p(\widetilde{E}_u) \end{cases}$$

prend au moins quatre valeurs distinctes dans $\mathcal{N}_p^{\times}$, et qu'elles sont en fait dans $\mathcal{N}_{p,4}^{\times}$.
Montrons d'abord la dernière assertion. On pose E_u : $y^2 = x^3 + [u]x$, où $[u] \in \mathbb{Z}_p^{\times}$ est le représentant de Teichmüller de u. C'est une courbe elliptique sur $\mathbb{Q}_p$ qui a bonne réduction et dont l'équation est minimale ; sa fibre spéciale est $\widetilde{E}_u$ et son invariant modulaire $j(E_u)$ est 1728. On pose alors : E'_u : $y^2 = x^3 - [u]px$. On a $j(E'_u) = 1728$, et E'_u est un twist de E_u ([Silv 1],X,Prop.5.4.), dont le défaut de semi-stabilité est $\mathrm{dst}(E'_u) = 4$; les courbes E'_u et E_u deviennent isomorphes sur l'extension totalement ramifiée $\mathbb{Q}_p(\pi_4)$, et la fibre spéciale de E'_u est aussi $\widetilde{E}_u$, d'où $a_p(\widetilde{E}'_u) = a_p(\widetilde{E}_u)$. Alors le fait que la représentation $V_l(E'_u)$, $l \neq p$, soit définie sur $\mathbb{Q}$ implique $a_p(\widetilde{E}_u) \in \mathcal{N}_{p,4}^{\times}$ (voir **A.1.2.**).
Montrons maintenant que l'application $u \mapsto a_p(\widetilde{E}_u)$ de $\mathbb{F}_p^{\times}$ dans $\mathcal{N}_p^{\times} \subset \mathbb{Z}$ prend au moins quatre valeurs distinctes ; pour cela, il suffit évidemment de montrer qu'elle prend quatre valeurs distinctes modulo $p\mathbb{Z}$. Comme de plus on a $a_p(\widetilde{E}_u) = 1 + p - \#(\widetilde{E}_u(\mathbb{F}_p))$, il suffit de montrer que $1 - \#(\widetilde{E}_u(\mathbb{F}_p))$ prend quatre valeurs distinctes modulo p lorsque u parcourt $\mathbb{F}_p^{\times}$. Or, d'après [Silv 1],V, démonstration du Thm.4.1.(a), on a

$$1 - \#(\widetilde{E}_u(\mathbb{F}_p)) \bmod p\mathbb{Z} = \binom{\frac{p-1}{2}}{\frac{p-1}{4}} u^{\frac{p-1}{4}},$$

ce dernier étant le coefficient de x^{p-1} dans $(x^3 + ux)^{\frac{p-1}{2}}$; le coefficient binômial est fixe dans $\mathbb{F}_p^{\times}$ lorsque u parcourt $\mathbb{F}_p^{\times}$, alors que $u^{\frac{p-1}{4}}$ parcourt $\mu_4(\mathbb{F}_p)$ qui est d'ordre 4. On en déduit le résultat.

Maintenant supposons $3 \mid p-1$: les $\widetilde{\mathcal{E}}_u$ sont ordinaires, $a_p(\widetilde{\mathcal{E}}_u) \in \mathcal{N}_p^{\times}$, et $\mathbb{F}_p^{\times}/(\mathbb{F}_p^{\times})^6$ est d'ordre 6. Alors la preuve est tout-à-fait similaire ; d'abord en utilisant la courbe sur $\mathbb{Q}_p$:

$$\mathcal{E}'_u : y^2 = x^3 - [u]px$$

(par exemple, ou bien son twist non ramifié correspondant à l'extension $\mathbb{Q}_{p^2}/\mathbb{Q}_p$), dont le défaut de semi-stabilité est $\mathrm{dst}(\mathcal{E}'_u) = 6$, et dont la courbe réduite sur $\mathbb{Q}_p(\pi_6)$ est $\widetilde{\mathcal{E}}_u$, d'où

$a_p(\widetilde{\mathcal{E}}_u) \in \mathcal{N}_{p,6}^{\times} = \mathcal{N}_{p,3}^{\times}$ (cf. **A.1.2.**) ; puis en remarquant que le coefficient de x^{p-1} dans $(x^3+u)^{\frac{p-1}{2}}$ est

$$\left(\begin{array}{c} \frac{p-1}{2} \\ \frac{p-1}{3} \end{array} \right) u^{\frac{p-1}{6}} \in \mathbb{F}_p^{\times} ,$$

et que l'application $u \mapsto u^{\frac{p-1}{6}}$ est une surjection de $\mathbb{F}_p^{\times}$ sur $\mu_6(\mathbb{F}_p)$, lequel est d'ordre 6 lorsque 3 divise $p-1$. □

1.2.1.5. Soit $\Delta = (\Delta, \rho_0, N)$ une représentation l-adique du groupe de Weil-Deligne $'W$ de dimension 2, et soit ϕ un relèvement dans W du Frobenius géométrique. On considère les conditions suivantes :
(1°) $\wedge^2(\Delta)$ est donnée par : $\rho_0(I) = 1$, $\rho_0(\phi) = p$, $N = 0$;
(2°) Δ est définie sur $\mathbb{Q}$;
(3°) si $N = 0$, les racines du polynôme caractéristique de $\rho_0(\phi)$ sont des p-nombres de Weil, i.e. $|\mathrm{Tr}(\rho_0(\phi))| \leq 2\sqrt{p}$.

Soit V un objet de $\mathbf{Rep}_{\mathbb{Q}_l}(G)$; on dira que $\Delta = (\Delta, \rho_0, N)$ est la représentation de Weil-Deligne associée à V si $\Delta = \widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V)$.

Théorème 1.2. :
Soient $p \geq 5$, et $l \in \mathcal{P}$, $l \neq p$. Une représentation l-adique de dimension 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *provient d'une courbe elliptique sur $\mathbb{Q}_p$ si et seulement si la représentation de Weil-Deligne qui lui est associée vérifie les conditions* (1°), (2°) *et* (3°).

Preuve :
Le fait que ces conditions sont nécessaires est bien connu ; nous allons montrer qu'elles sont suffisantes. Soient ϕ un relèvement dans W du Frobenius géométrique et (Δ, ρ_0, N) un objet de $\mathbf{Rep}_{\mathbb{Q}_l}('W)$ vérifiant les conditions (1°), (2°) et (3°) ; la condition (1°) donne $\det(\rho_0(\phi)) = p \in \mathbb{Z}_l^{\times}$. Donc Δ est un objet de $\mathbf{Rep}^{\circ}_{\mathbb{Q}_l}('W)$, et il suffit de montrer qu'il est isomorphe à l'un des objets de la liste $\mathbf{WD}^*$.

Si $N \neq 0$, alors les relations $N^2 = 0$ et $N\rho_0(\phi) = p\rho_0(\phi)N$ impliquent que $\rho_0(\phi)$ est diagonalisable et a deux valeurs propres distinctes (b, pb). La condition (1°) donne $b^2 p = p$, c'est-à-dire $b \in \{\pm 1\}$. Le sous-groupe d'inertie I agissant de façon potentiellement unipotente (i.e. à travers des racines de l'unité), la relation $N\rho_0(g) = \rho_0(g)N$ pour $g \in I$ implique que $\rho_0(g) = \pm 1$. Donc $\Delta \simeq \mathbf{WD}^*_{\mathbf{m}}(\mathbf{e};\mathbf{b})$ avec $e \in \{1,2\}$ et $b \in \{-1,1\}$.

Si $N = 0$, alors Δ a potentiellement bonne réduction. Soit F le sous-corps de $\overline{\mathbb{Q}}_p$ fixe par le noyau de la restriction de ρ_0 à I : c'est une extension finie galoisienne de $\mathbb{Q}_p^{nr}$ telle que $\rho_{0|I}$ induit une injection

$$I_{F/\mathbb{Q}_p^{nr}} = I/I_F \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta) ,$$

que l'on note encore ρ_0. Soit $\tau \in I_{F/\mathbb{Q}_p^{nr}}$; la condition (1°) impose $\det(\rho_0(\tau)) = 1$ (le déterminant est non ramifié), et la condition (2°) impose $\mathrm{Tr}(\rho_0(\tau)) \in \mathbb{Q}$. Comme Δ est un $\mathbb{Q}_l$-espace vectoriel de dimension 2 et que $\rho_0(\tau)$ est d'ordre fini, les deux précédentes conditions impliquent que le polynôme minimal de $\rho_0(\tau)$ est le e-ième polynôme cyclotomique $\Phi_e(X) \in \mathbb{Q}[X]$, et que e est un entier tel que $\varphi(e) \in \{1,2\}$ (où φ est la fonction arithmétique d'Euler), c'est-à-dire $e \in \{1,2,3,4,6\}$. On en déduit que l'extension $F/\mathbb{Q}_p^{nr}$ est modérée,

donc cyclique d'ordre e ; une telle extension est unique, et l'on a $F = \mathbb{Q}_p^{nr}(\pi_e) = \mathbb{Q}_p^{nr}K_e$, $I_{F/\mathbb{Q}_p^{nr}} = I(K_e/\mathbb{Q}_p) = I_e$.
Si $e \in \{1,2\}$, la condition (3°) implique que Δ est isomorphe à l'un des objets $\mathbf{WD_c^*(e;a_p)}$ avec $a_p \in \mathcal{N}_p$. Si $e \in \{3,4,6\}$ et $e \mid p+1$, alors la trace de $\rho_0(\phi)$ doit être nulle et Δ est isomorphe à l'objet $\mathbf{WD_{pc}^*(e;0)}$, voir les calculs faits en **A.1.2.**. Si $e \in \{3,4,6\}$ et $e \mid p-1$, alors la condition (2°) implique que la trace de $\rho_0(\phi)$ est dans $\mathcal{N}_{p,e}^{\times}$ (voir **A.1.2.**) ; les calculs faits en **A.1.2.** montrent qu'alors Δ est isomorphe à l'un des $\mathbf{WD_{pc}^*(e;a_p;\epsilon)}$, avec $a_p \in \mathcal{N}_{p,e}^{\times}$ et $\epsilon \in \{\pm 1\}$. □

Corollaire 1.2. :
Soient $p \geq 5$ et $l \in \mathcal{P}$ tel que $l \neq p$. Le nombre de classes d'isomorphisme d'objets de $\mathbf{Rep}_{\mathbb{Q}_l}(G)$ provenant d'une courbe elliptique sur $\mathbb{Q}_p$ est fini et indépendant de l ; il vaut :

$$4[2\sqrt{p}] + \lambda(p) \quad , \text{ où } \quad \lambda(p) = 38, 16, 31, \text{ ou } 9 \text{ suivant que } p \equiv 1, 5, 7, \text{ ou } 11 \bmod 12 \ .$$

Plus précisément, il y a : 4 classes dans $\mathbf{Rep}_{\mathbb{Q}_l}(G)$ provenant de courbes elliptiques sur $\mathbb{Q}_p$ n'ayant pas potentiellement bonne réduction ; $\mathrm{Card}(\mathcal{N}_p^{\times}) = 2[2\sqrt{p}]$ classes provenant de courbes elliptiques sur $\mathbb{Q}_p$ ayant bonne réduction ordinaire sur $\mathbb{Q}_p$, et autant provenant d'un twist ramifié d'ordre deux de courbes du type précédent ; 1 classe provenant de courbes elliptiques sur $\mathbb{Q}_p$ ayant bonne réduction supersingulière sur $\mathbb{Q}_p$, et 1 provenant d'un twist ramifié d'ordre deux de courbes du type précédent. Si $3 \mid p-1$, il y a $2.\mathrm{Card}(\mathcal{N}_{p,3}^{\times}) = 12$ classes provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement ordinaires avec $\mathrm{dst}(E) = 3$, et $2.\mathrm{Card}(\mathcal{N}_{p,6}^{\times}) = 12$ classes provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement ordinaires avec $\mathrm{dst}(E) = 6$; si $3 \mid p+1$, il y a 1 classe provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement supersingulières avec $\mathrm{dst}(E) = 3$, et 1 classe provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement supersingulières avec $\mathrm{dst}(E) = 6$. Si $4 \mid p-1$, il y a $2.\mathrm{Card}(\mathcal{N}_{p,4}^{\times}) = 8$ classes provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement ordinaires avec $\mathrm{dst}(E) = 4$; si $4 \mid p+1$, il y a 1 classe provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement supersingulières avec $\mathrm{dst}(E) = 4$.

1.2.2. Exemples :

Courbes potentiellement ordinaires :

Si $4 \mid p-1$:
Pour chaque $a_{p,j} \in \mathcal{N}_{p,4}^{\times}$, $1 \leq j \leq 4$, on choisit un élément $u_j \in \mathbb{F}_p^{\times}$ tel que la trace du Frobenius de la courbe elliptique $\widetilde{E}_j$: $y^2 = x^3 + u_j x$ est $a_{p,j}$; les u_j, $1 \leq j \leq 4$, sont un système de représentants de $\mathbb{F}_p^{\times}/(\mathbb{F}_p^{\times})^4$. Ces courbes sont ordinaires, puisque $4 \mid p-1$, et ont un invariant modulaire égal à $12^3 = 1728$. Par exemple, pour $p = 5$, on peut prendre :
$u_1 = 1$; $u_2 = 2$; $u_3 = -2$; $u_4 = -1$; cela donne : $a_{5,1} = 2$; $a_{5,2} = 4$; $a_{5,3} = -4$; $a_{5,4} = -2$.
Alors $\{[u_j](-p)^i,\ 1 \leq j \leq 4,\ 0 \leq i \leq 3\}$ est un système de représentants de $\mathbb{Q}_p^{\times}/(\mathbb{Q}_p^{\times})^4$, où $[u_j] \in \mathbb{Z}_p^{\times}$ est le représentant de Teichmüller de u_j.

Posons $E_{i,j}$: $y^2 = x^3 + [u_j](-p)^i x$, pour $1 \leq j \leq 4$, $0 \leq i \leq 3$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui possèdent toutes le même invariant modulaire $12^3 = 1728$.

Pour un j fixé, elles deviennent isomorphes sur $\mathbb{Q}_p(\pi_4)$. Elles ont toutes potentiellement bonne réduction, et la courbe réduite sur $\mathbb{Q}_p(\pi_4)$ de $E_{i,j}$ est $\widetilde{E}_j$. De plus, $E_{i+2,j}$ est le twist ramifié d'ordre 2 correspondant à $M_2 = \mathbb{Q}_p(\pi_2)$ de $E_{i,j}$ pour $i \in \{0,1\}$. On a alors, pour chaque $j \in \{1,2,3,4\}$:

$$\begin{aligned}
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(E_{0,j})) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_{p,j}}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(E_{1,j})) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_{p,j}};\mathbf{1}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(E_{2,j})) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_{p,j}}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(E_{3,j})) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_{p,j}};\mathbf{-1}) \ .
\end{aligned}$$

Si $3 \mid p-1$:
Pour chaque $a_{p,j} \in \mathcal{N}^{\times}_{p,3}$, $1 \leq j \leq 6$, on choisit un élément $v_j \in \mathbb{F}_p^{\times}$ tel que la trace du Frobenius de la courbe elliptique $\widetilde{\mathcal{E}}_j$: $y^2 = x^3 + v_j$ est $a_{p,j}$; les v_j, $1 \leq j \leq 6$, sont un système de représentants de $\mathbb{F}_p^{\times}/(\mathbb{F}_p^{\times})^6$. Ces courbes sont ordinaires (car $3 \mid p-1$) et ont un invariant modulaire égal à 0. Par exemple, pour $p = 7$, on peut prendre :
$v_1 = 1$; $v_2 = 2$; $v_3 = 3$; $v_4 = -3$; $v_5 = -2$; $v_6 = -1$; ce qui donne : $a_{7,1} = -4$; $a_{7,2} = -1$; $a_{7,3} = -5$; $a_{7,4} = 5$; $a_{7,5} = 1$; $a_{7,6} = 4$.
Alors $\{\,[v_j](-p)^i,\ 1 \leq j \leq 6\,,\ 0 \leq i \leq 5\,\}$ est un système de représentants de $\mathbb{Q}_p^{\times}/(\mathbb{Q}_p^{\times})^6$, où $[v_j] \in \mathbb{Z}_p^{\times}$ est le représentant de Teichmüller de v_j.

Posons $\mathcal{E}_{i,j}$: $y^2 = x^3 + [v_j](-p)^i$, pour $1 \leq j \leq 6$, $0 \leq i \leq 5$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui possèdent toutes le même invariant modulaire 0. Pour un j fixé, elles deviennent isomorphes sur $\mathbb{Q}_p(\pi_6)$. Elles ont toutes potentiellement bonne réduction, et la courbe réduite sur $\mathbb{Q}_p(\pi_6)$ de $\mathcal{E}_{i,j}$ est $\widetilde{\mathcal{E}}_j$. De plus, $\mathcal{E}_{i+3,j}$ est le twist ramifié d'ordre 2 correspondant à $M_2 = \mathbb{Q}_p(\pi_2)$ de $\mathcal{E}_{i,j}$ pour $i \in \{0,1,2\}$. On a alors, pour chaque $j \in \{1,2,3,4,5,6\}$:

$$\begin{aligned}
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_{0,j})) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_{p,j}}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_{1,j})) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{a_{p,j}};\mathbf{1}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_{2,j})) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{a_{p,j}};\mathbf{1}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_{3,j})) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_{p,j}}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_{4,j})) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{a_{p,j}};\mathbf{-1}) \\
\widehat{\mathbf{WD}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_{5,j})) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{a_{p,j}};\mathbf{-1}) \ .
\end{aligned}$$

Courbes potentiellement supersingulières :

Si $4 \mid p+1$:
Posons E_i : $y^2 = x^3 + (-p)^i x$, pour $i \in \{0,1,2,3\}$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui possèdent toutes le même invariant modulaire $12^3 = 1728$; elles deviennent deux-à-deux isomorphes sur $\mathbb{Q}_p(\pi_4)$. Elles ont toutes potentiellement bonne réduction, qui est de type supersingulière puisque $4 \mid p+1$ (la courbe réduite sur $\mathbb{F}_p$ a pour équation $y^2 = x^3 + x$). De plus, pour $i \in \{0,1\}$, E_{i+2} est le twist par le caractère ramifié d'ordre 2 correspondant à

l'extension $M_2 = \mathbb{Q}_p(\pi_2)$ de E_i. On a alors :

$$\begin{aligned}
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E_0)) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{1};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E_1)) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E_2)) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{2};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E_3)) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{0}) \ .
\end{aligned}$$

Si $3 \mid p+1$:
Posons $\mathcal{E}_i$: $y^2 = x^3 + (-p)^i$, pour $i \in \{0,1,2,3,4,5\}$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui possèdent toutes le même invariant modulaire 0 ; elles deviennent deux-à-deux isomorphes sur $\mathbb{Q}_p(\pi_6)$. Elles ont toutes potentiellement bonne réduction, qui est de type supersingulière puisque $3 \mid p+1$ (la courbe réduite sur $\mathbb{F}_p$ a pour équation $y^2 = x^3 + 1$). De plus, pour $i \in \{0,1,2\}$, $\mathcal{E}_{i+3}$ est le twist par le caractère ramifié d'ordre 2 correspondant à l'extension $M_2 = \mathbb{Q}_p(\pi_2)$ de $\mathcal{E}_i$. On a alors :

$$\begin{aligned}
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_0)) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{1};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_1)) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_2)) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_3)) &\simeq \mathbf{WD}^*_{\mathbf{c}}(\mathbf{2};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_4)) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{0}) \\
\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(\mathcal{E}_5)) &\simeq \mathbf{WD}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{0}) \ .
\end{aligned}$$

1.2.3. Les $\mathbb{Z}_l[G]$-modules, $l \neq p$, provenant d'une courbe elliptique sur $\mathbb{Q}_p$:

Soit $E/\mathbb{Q}_p$ une courbe elliptique, $T = T_l(E)$, et soit T' un réseau G-stable de $V_l(E)$; à homothétie près, on peut supposer que $T' \subset T$. Alors il existe une courbe elliptique E' et une l-isogénie $\psi : E' \to E$, définies sur $\mathbb{Q}_p$, telles que $\psi_l(T_l(E')) = T'$ (cf. **2.4.3**, début). D'où le résultat suivant :

Soient $l \in \mathcal{P}$, $l \neq p$, et T' un $\mathbb{Z}_l[G]$-module. Pour qu'il existe une courbe elliptique E' sur $\mathbb{Q}_p$ telle que $T' \simeq T_l(E')$, il faut et il suffit qu'il existe une courbe elliptique E sur $\mathbb{Q}_p$ telle que $\mathbb{Q}_l \otimes_{\mathbb{Z}_l} T' \simeq V_l(E)$.

1.3. Les cas $l = p$:

1.3.1. Les $\mathbb{Q}_p[G]$-modules provenant d'une courbe elliptique sur $\mathbb{Q}_p$:

On désigne par $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ la catégorie des représentations p-adiques de G, c'est-à-dire des $\mathbb{Q}_p$-espaces vectoriels de dimension finie munis d'une action linéaire et continue de G.

1.3.1.1. Soit K une extension finie galoisienne de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}}_p$. On note $\mathbf{Rep}_{cris}(G)$, $\mathbf{Rep}_{st}(G)$, $\mathbf{Rep}_{cris,K}(G)$, $\mathbf{Rep}_{st,K}(G)$, $\mathbf{Rep}_{pcris}(G)$ et $\mathbf{Rep}_{pst}(G)$ les sous-catégories pleines de $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ constituées des objets qui sont respectivement cristallins sur $\mathbb{Q}_p$, semi-stables sur $\mathbb{Q}_p$, cristallins sur K, semi-stables sur K, potentiellement cristallins et potentiellement semi-stables (voir [Fo 2]).

Soient $G_{K/\mathbb{Q}_p} = \mathrm{Gal}(K/\mathbb{Q}_p)$, et K_0 l'extension maximale non ramifiée de $\mathbb{Q}_p$ contenue dans K ; le Frobenius absolu σ agit sur K_0. On définit la catégorie des $(\varphi, N, G_{K/\mathbb{Q}_p})$-modules filtrés de la manière suivante :
- les objets sont des K_0-espaces vectoriels D munis :
(i) d'une action σ-semi-linéaire de $G_{K/\mathbb{Q}_p}$ (le sous-groupe d'inertie agit linéairement) ;
(ii) d'une application de Frobenius $\varphi : D \to D$, injective, σ-semi-linéaire et $G_{K/\mathbb{Q}_p}$-équivariante ;
(iii) d'un endomorphisme K_0-linéaire $G_{K/\mathbb{Q}_p}$-équivariant $N : D \to D$ tel que $N\varphi = p\varphi N$;
(iv) d'une filtration indexée par $\mathbb{Z}$, décroissante, exhaustive et séparée sur $D_K = K \otimes_{K_0} D$ par des sous-K-espaces vectoriels $\{\mathrm{Fil}^i D_K\ ,\ i \in \mathbb{Z}\}$ stables par $G_{K/\mathbb{Q}_p}$, l'action de $G_{K/\mathbb{Q}_p}$ étant étendue semi-linéairement sur D_K.
- un morphisme $f : D_1 \to D_2$ est une application K_0-linéaire commutant à l'action de $G_{K/\mathbb{Q}_p}$, à φ et à N, et, telle que, si l'on note f_K l'application K-linéaire déduite de f par extension des scalaires, $f_K(\mathrm{Fil}^i D_{1,K}) \subset \mathrm{Fil}^i D_{2,K}$ pour tout $i \in \mathbb{Z}$.

On désigne par $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$ la sous-catégorie pleine des $(\varphi, N, G_{K/\mathbb{Q}_p})$-modules filtrés discrets (i.e. l'action de $G_{K/\mathbb{Q}_p}$ sur D est discrète) et de dimension finie (c'est la dimension en tant que K_0-espace vectoriel), et par $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$ la sous-catégorie pleine formée des objets de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$ sur lesquels $N = 0$. Lorsque $K = \mathbb{Q}_p$ on écrit $\mathbf{MF}_{\mathbb{Q}_p}(\varphi, N)$ et $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$. Le *type de Hodge-Tate* d'un objet D de dimension 2 de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$ est le couple d'entiers (r, s) tel que $\mathrm{Fil}^i D_K = D_K$ si et seulement si $i \leq r$ et $\mathrm{Fil}^i D_K = 0$ si et seulement si $i > s$. Pour tout objet D de dimension d dans $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$, on pose $t_H(D) = t_H(\wedge^d D) = \mathrm{Max}\{\, i \in \mathbb{Z} \,/\, \mathrm{Fil}^i(\wedge^d D_K) \neq 0 \,\}$, et $t_N(D) = v_p(\lambda)$, où $\lambda \in K_0$ est tel que $\varphi x = \lambda x$ pour un élément x non nul de $\wedge^d D$; on dit que D est *faiblement admissible* si $t_H(D) = t_N(D)$, et $t_H(D') \leq t_N(D')$ pour tout sous-objet D' de D, voir [Fo 2].

On renvoie à [Fo 1] pour les définitions de B_{dR}, B_{cris} et B_{st}. On choisit un élément $\pi = (\pi^{(n)}) \in (\overline{\mathbb{Q}}_p)^{\mathbb{N}}$ avec $\pi^{(0)} = p$ et $(\pi^{(n+1)})^p = \pi^{(n)}$ (donc $\pi \in R$, cf. **A.2.1.**), et l'on pose $\mathbf{u} = \mathrm{Log}([\pi]/p) \in B_{dR}$; on prend alors $B_{st} = B_{cris}[\mathbf{u}] \subset B_{dR}$, sur lequel le Frobenius est étendu par $\varphi\mathbf{u} = p\mathbf{u}$, et N est l'unique B_{cris}-dérivation telle que $N\mathbf{u} = 1$ (pour l'influence de ces choix voir [Fo 2], 5.2.). On utilise les foncteurs *contravariants* ([Fo 2], 5.3.7.)

$$\mathbf{D}^*_{\mathbf{cris},\mathbf{K}/\mathbb{Q}_\mathbf{p}} : \mathbf{Rep}_{cris,K}(G) \to \mathbf{MF}_{K/\mathbb{Q}_p}(\varphi) \quad \text{et} \quad \mathbf{D}^*_{\mathbf{st},\mathbf{K}/\mathbb{Q}_\mathbf{p}} : \mathbf{Rep}_{st,K}(G) \to \mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$$

donnés par $\mathbf{D}^*_{\mathbf{cris},\mathbf{K}/\mathbb{Q}_\mathbf{p}}(V) = \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B_{cris})$ et $\mathbf{D}^*_{\mathbf{st},\mathbf{K}/\mathbb{Q}_\mathbf{p}}(V) = \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B_{st})$, où $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$; ils sont exacts et pleinement fidèles, et établissent donc une anti-équivalence de catégories entre $\mathbf{Rep}_{cris,K}(G)$ et $\mathbf{Rep}_{st,K}(G)$ et leur image essentielle ([Fo 2]) ; lorsque $K = \mathbb{Q}_p$ on écrit $\mathbf{D}^*_{\mathbf{cris}}$ et $\mathbf{D}^*_{\mathbf{st}}$. On note $\mathbf{D}^*_{\mathbf{pcris}}$ et $\mathbf{D}^*_{\mathbf{pst}}$ les foncteurs obtenus comme limite inductive des $\mathbf{D}^*_{\mathbf{cris},\mathbf{K}/\mathbb{Q}_\mathbf{p}}$ et $\mathbf{D}^*_{\mathbf{st},\mathbf{K}/\mathbb{Q}_\mathbf{p}}$ lorsque K parcourt l'ensemble des extensions finies galoisiennes de $\mathbb{Q}_p$ contenues dans $\overline{\mathbb{Q}}_p$; ce sont des foncteurs contravariants, respectivement de $\mathbf{Rep}_{pcris}(G)$ et $\mathbf{Rep}_{pst}(G)$ dans la limite inductive des $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$. Si D est un objet admissible de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$ ou de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$ (i.e. dans l'image essentielle de $\mathbf{D}^*_{\mathbf{st},\mathbf{K}/\mathbb{Q}_\mathbf{p}}$ ou de $\mathbf{D}^*_{\mathbf{cris},\mathbf{K}/\mathbb{Q}_\mathbf{p}}$), les foncteurs quasi-inverses respectifs sont donnés par :

$$\mathbf{V}^*_{\mathbf{st},\mathbf{K}/\mathbb{Q}_\mathbf{p}}(D) = \mathrm{Hom}_{(\varphi,N,G)-mf}(D, B_{st}) \qquad \text{et} \qquad \mathbf{V}^*_{\mathbf{cris},\mathbf{K}/\mathbb{Q}_\mathbf{p}}(D) = \mathrm{Hom}_{(\varphi,G)-mf}(D, B_{cris})\ ,$$

où G opère sur D via son quotient $G_{K/\mathbb{Q}_p}$. Tout objet de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$ (ou bien de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$) qui est admissible est faiblement admissible ([Fo 2], Prop. 5.4.2.), et on conjecture que la réciproque est vraie ([Fo 2], 5.4.4.) ; J.-M. Fontaine l'a prouvée récemment pour les objets de dimension deux. Ce critère est utile pour la détermination de la filtration d'un objet admissible.

On dit qu'un objet V de $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ est *potentiellement de Barsotti-Tate* s'il existe une extension finie galoisienne K de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}}_p$ et un groupe p-divisible (ou de Barsotti-Tate) Γ sur O_K (l'anneau des entiers de K), tels que $V \simeq V_p(\Gamma)$ en tant que $\mathbb{Q}_p[G_K]$-modules ; tout objet qui est potentiellement de Barsotti-Tate est potentiellement cristallin. Rappelons que l'on a alors un isomorphisme canonique d'objets de $\mathbf{MF_K}(\varphi)$ (c'est la catégorie obtenue en oubliant l'action de $G_{K/\mathbb{Q}_p}$ dans $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$) :

$$\mathbf{D}_L(\Gamma) = K_0 \otimes_{W(k)} \mathbf{M}_{O_K}(\Gamma) \simeq \mathbf{D}^*_{\mathbf{cris,K}}(V_p(\Gamma)) ,$$

qui fait le lien entre le Module de Dieudonné $\mathbf{M}_{O_K}(\Gamma)$ sur O_K de Γ et la théorie cristalline (voir [Fo 5] ; k est le corps résiduel de K).

Rappelons enfin que l'on a un foncteur, obtenu en oubliant la filtration sur D et en faisant agir le groupe de Weil K_0-linéairement (voir **1.3.2.** ou bien [Fo 3]) :

$$\begin{array}{ccc} \mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N) & \longrightarrow & \mathbf{Rep}_{K_0}('W) \\ D & \longmapsto & \mathbf{W}_p(D^{(0)}) . \end{array}$$

On dira que $\mathbf{W}_p(D^{(0)})$ est la représentation de Weil-Deligne associée à D ; et si V est un objet de $\mathbf{Rep}_{st,K}(G)$, la représentation de Weil-Deligne associée à V est celle qui est associée à $\mathbf{D}^*_{\mathbf{st,K/\mathbb{Q}_p}}(V)$.

Nous appliquons tout cela au $\mathbb{Q}_p[G]$-module $V_p(E)$, où E est une courbe elliptique sur $\mathbb{Q}_p$. La situation est la suivante :
- E a mauvaise réduction de type multiplicatif sur K si et seulement si $V_p(E)$ est un objet de $\mathbf{Rep}_{st,K}(G)$ et n'est pas un objet de $\mathbf{Rep}_{cris,K}(G)$.
- E a bonne réduction sur K si et seulement si $V_p(E)$ est un objet de $\mathbf{Rep}_{cris,K}(G)$.
Bien sûr, nous choisirons pour K une extension galoisienne de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}}_p$ d'indice de ramification minimal sur laquelle E devient semi-stable, de sorte que l'on travaille après application du foncteur adéquat dans la catégorie $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$ ou $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$.

1.3.1.2. On définit la liste $\mathbf{D^*}$ d'objets de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$ et de type Hodge-Tate $(0,1)$ suivants :

$\mathbf{D^*_m(e;b;\alpha)}$, $e \in \{1,2\}$, $b \in \{-1,1\}$, $\alpha \in \mathbb{Q}_p$:
Pour $e = 1$: $K = K_1 = \mathbb{Q}_p$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = be_1$, $\varphi e_2 = pbe_2$; $Ne_1 = 0$, $Ne_2 = e_1$; $\mathrm{Fil}^1 D = (\alpha e_1 + e_2)\mathbb{Q}_p$.
Pour $e = 2$: $K = K_2 = \mathbb{Q}_p(\pi_2)$, $G_{K/\mathbb{Q}_p} =< \tau_2 >$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = be_1$, $\varphi e_2 = pbe_2$; $Ne_1 = 0$, $Ne_2 = e_1$; $\tau_2 e_1 = -e_1$, $\tau_2 e_2 = -e_2$; $\mathrm{Fil}^1 D_K = (\alpha e_1 + e_2)\mathbb{Q}_p(\pi_2)$.

$\mathbf{D^*_c(e;a_p;\alpha)}$, $e \in \{1,2\}$, $a_p \in \mathcal{N}_p^\times$, $\alpha \in \{0,1\}$:
Notons u l'unique élément de $\mathbb{Z}_p^\times$ vérifiant $u + u^{-1}p = a_p$ (il existe car $a_p \in \mathbb{Z}_p^\times$).
Pour $e = 1$: $K = K_1 = \mathbb{Q}_p$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = ue_1$, $\varphi e_2 = u^{-1}pe_2$; $Ne_1 =$

$Ne_2 = 0$; $\mathrm{Fil}^1 D = (\alpha e_1 + e_2)\mathbb{Q}_p$.
Pour $e = 2$: $K = K_2 = \mathbb{Q}_p(\pi_2)$, $G_{K/\mathbb{Q}_p} =< \tau_2 >$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = u e_1$, $\varphi e_2 = u^{-1} p e_2$; $Ne_1 = Ne_2 = 0$; $\tau_2 e_1 = -e_1$, $\tau_2 e_2 = -e_2$; $\mathrm{Fil}^1 D_K = (\alpha \cdot e_1 \otimes 1 + e_2 \otimes 1)\mathbb{Q}_p(\pi_2)$.

$\mathbf{D_c^*(e;0)}$, $e \in \{1,2\}$:
Pour $e = 1$: $K = K_1 = \mathbb{Q}_p$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = e_2$, $\varphi e_2 = -p e_1$; $Ne_1 = Ne_2 = 0$; $\mathrm{Fil}^1 D = e_1 \mathbb{Q}_p$.
Pour $e = 2$: $K = K_2 = \mathbb{Q}_p(\pi_2)$, $G_{K/\mathbb{Q}_p} =< \tau_2 >$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = e_2$, $\varphi e_2 = -p e_1$; $Ne_1 = Ne_2 = 0$; $\tau_2 e_1 = -e_1$, $\tau_2 e_2 = -e_2$; $\mathrm{Fil}^1 D_K = (e_1 \otimes 1)\mathbb{Q}_p(\pi_2)$.

$\mathbf{D_{pc}^*(e;a_p;\epsilon;\alpha)}$, $e \in \{3,4,6\}$ et $e \mid p-1$, $a_p \in \mathcal{N}_{p,e}^{\times}$, $\epsilon \in \{-1,1\}$, $\alpha \in \{0,1\}$:
Notons encore u l'unique élément de $\mathbb{Z}_p^{\times}$ vérifiant $u + u^{-1}p = a_p$.
$K = K_e = \mathbb{Q}_p(\pi_e)$, $G_{K/\mathbb{Q}_p} =< \tau_e >$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = u e_1$, $\varphi e_2 = u^{-1} p e_2$; $Ne_1 = Ne_2 = 0$; $\tau_e e_1 = \zeta_e{}^{\epsilon} e_1$, $\tau_e e_2 = \zeta_e{}^{-\epsilon} e_2$; $\mathrm{Fil}^1 D_K = (\alpha \cdot e_1 \otimes \pi_e{}^{-\epsilon} + e_2 \otimes \pi_e{}^{\epsilon})\mathbb{Q}_p(\pi_e)$.

$\mathbf{D_{pc}^*(e;0;\alpha)}$, $e \in \{3,4,6\}$ et $e \mid p+1$, $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$:
$K = K_e = \mathbb{Q}_{p^2}(\pi_e)$, $G_{K/\mathbb{Q}_p} =< \tau_e > \rtimes < \omega >$, $D = \mathbb{Q}_{p^2} e_1 \oplus \mathbb{Q}_{p^2} e_2$, avec $\varphi e_1 = e_2$, $\varphi e_2 = -p e_1$; $Ne_1 = Ne_2 = 0$; $\omega e_1 = e_1$, $\omega e_2 = e_2$; $\tau_e e_1 = \zeta_e e_1$, $\tau_e e_2 = \zeta_e{}^{-1} e_2$; $\mathrm{Fil}^1 D_K = (\alpha \cdot e_1 \otimes \pi_e{}^{-1} + e_2 \otimes \pi_e)\mathbb{Q}_{p^2}(\pi_e)$.

La classe d'isomorphisme de chacun de ces objets est indépendante du choix fait pour l'extension galoisienne K_e (elle ne dépend que de l'indice de ramification e).

Tous ces objets sont de dimension 2, et vérifient $\mathrm{Fil}^0 D_K = D_K$, $\mathrm{Fil}^1 D_K = K$ – droite, et $\mathrm{Fil}^2 D_K = 0$: ils sont de type Hodge-Tate $(0,1)$. Pour chacun d'entre eux, la représentation de Weil-Deligne associée est définie sur $\mathbb{Q}$. De plus, $\wedge^2 \mathbf{D}^*$ est un objet de $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$ de dimension un décrit par : $\varphi = p$ et $\mathrm{Fil}^1(\wedge^2 \mathbf{D}^*) = \wedge^2 \mathbf{D}^*$, $\mathrm{Fil}^2(\wedge^2 \mathbf{D}^*) = 0$; l'objet obtenu en appliquant le foncteur quasi-inverse est $\mathbb{Q}_p(1)$.
Les objets du type $\mathbf{D_m^*}$ sont des twists d'ordre 1 ou 2 d'objets semi-stables sur $\mathbb{Q}_p$ mais non potentiellement cristallins. Les objets du type $\mathbf{D_c^*}$ sont des twists par un caractère d'ordre 1 ou 2 d'objets cristallins sur $\mathbb{Q}_p$. Les objets du type $\mathbf{D_{pc}^*}$ sont potentiellement cristallins, mais *ne sont pas* des twists d'objets cristallins sur $\mathbb{Q}_p$.

Description des twists d'ordre 2 :

Soit D un objet de la liste $\mathbf{D}^*$ ci-dessus. En tordant par l'un des caractères (non trivial) d'ordre 2, on obtient les objets D_1, D_2, et D_3, correspondant respectivement aux extensions quadratiques M_1, M_2, et M_3 de $\mathbb{Q}_p$. Les quatre objets D, D_1, D_2, et D_3 sont liés entre eux par des twists d'ordre 2 de la manière suivante : les paires (D, D_1) et (D_2, D_3) sont composées d'objets liés par un twist non ramifié ; les paires (D, D_2), (D, D_3), (D_1, D_2), et (D_1, D_3) sont composées d'objets liés par un twist ramifié. En faisant varier D parmi les objets de la liste $\mathbf{D}^*$, et en gardant les notations précédentes, on obtient :
$D = \mathbf{D_m^*(1;b;\alpha)}$; $D_1 = \mathbf{D_m^*(1;-b;\alpha)}$; $D_2 = \mathbf{D_m^*(2;b;\alpha)}$; $D_3 = \mathbf{D_m^*(2;-b;\alpha)}$.
$D = \mathbf{D_c^*(1;a_p;\alpha)}$; $D_1 = \mathbf{D_c^*(1;-a_p;\alpha)}$; $D_2 = \mathbf{D_c^*(2;a_p;\alpha)}$; $D_3 = \mathbf{D_c^*(2;-a_p;\alpha)}$.
$D = \mathbf{D_c^*(1;0)}$; $D_1 = D$; $D_2 = D_3 = \mathbf{D_c^*(2;0)}$. Ici les twists non ramifiés donnent des représentations isomorphes.
$D = \mathbf{D_{pc}^*(4;a_p;\epsilon;\alpha)}$; $D_1 = \mathbf{D_{pc}^*(4;-a_p;\epsilon;\alpha)}$; $D_2 = \mathbf{D_{pc}^*(4;a_p;-\epsilon;\alpha)}$; $D_3 = \mathbf{D_{pc}^*(4;-a_p;-\epsilon;\alpha)}$.
$D = \mathbf{D_{pc}^*(3;a_p;\epsilon;\alpha)}$; $D_1 = \mathbf{D_{pc}^*(3;-a_p;\epsilon;\alpha)}$; $D_2 = \mathbf{D_{pc}^*(6;a_p;-\epsilon;\alpha)}$; $D_3 = \mathbf{D_{pc}^*(6;-a_p;-\epsilon;\alpha)}$.

$D = \mathbf{D^*_{pc}(4;0;\alpha)}$; $D_1 = \mathbf{D^*_{pc}(4;0;-\alpha)}$; $D_2 = \mathbf{D^*_{pc}(4;0;p^2\alpha^{-1})}$; $D_3 = \mathbf{D^*_{pc}(4;0;-p^2\alpha^{-1})}$.
$D = \mathbf{D^*_{pc}(3;0;\alpha)}$; $D_1 = \mathbf{D^*_{pc}(3;0;-\alpha)}$; $D_2 = \mathbf{D^*_{pc}(6;0;p^2\alpha^{-1})}$; $D_3 = \mathbf{D^*_{pc}(6;0;-p^2\alpha^{-1})}$.
Remarque : pour $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, on a : $\alpha = -\alpha \Leftrightarrow \alpha \in \{0, \infty\}$; dans ces cas les twists non ramifiés donnent des représentations isomorphes.

Si un objet D de la liste $\mathbf{D^*}$ provient d'une courbe elliptique E sur $\mathbb{Q}_p$, c'est-à-dire s'il existe $E/\mathbb{Q}_p$ telle que $D \simeq \mathbf{D^*_{pst}}(V_p(E))$, alors les objets D_i, $i \in \{1,2,3\}$, proviennent des courbes elliptiques E_i sur $\mathbb{Q}_p$ obtenues en tordant E par les caractères d'ordre 2 correspondants aux extensions quadratiques M_i.

Théorème 2.1. :
Soit $p \in \mathcal{P}$ tel que $p \geq 5$.
1) Les objets de la liste $\mathbf{D^*}$ ci-dessus sont deux-à-deux non-isomorphes.
2) Soit E une courbe elliptique sur $\mathbb{Q}_p$; alors $\mathbf{D^*_{pst}}(V_p(E))$ est isomorphe à l'un des objets de la liste $\mathbf{D^*}$.
3) Réciproquement, tous ces objets proviennent d'un $V_p(E)$, où E est une courbe elliptique sur $\mathbb{Q}_p$.

Remarque : dans [Fo-Ma], J.-M. Fontaine et B. Mazur classifient les représentations potentiellement semi-stables et faiblement admissibles de G sur un $\mathbb{Q}_p$-espace vectoriel de dimension 2. Les objets de dimension 1 sont décrits au § 8, tandis que les objets de dimension 2 qui ne sont pas somme directe d'objets de dimension 1 sont décrits dans la liste du début du § 11. On remarque que 12 divise $p^2 - 1$ pour $p \geq 5$, et donc les K_e, $e \in \{2,3,4,6\}$, sont des sous-corps du corps noté F_2 dans [Fo-Ma]. Les correspondances dans les notations sont :

$\mathbf{D^*_m(1;b;\alpha)} = D_{II}(0,1;b,\alpha;0)$, $b \in \{-1,1\}$, $\alpha \in \mathbb{Q}_p$;
$\mathbf{D^*_m(2;b;\alpha)} = D_{II}(0,1;b,\alpha;\frac{p-1}{2})$, $b \in \{-1,1\}$, $\alpha \in \mathbb{Q}_p$;

$\mathbf{D^*_c(e;a_p;0)} = U_1 \oplus U_2$, $e \in \{1,2\}$, $a_p \in \mathcal{N}_p^\times$: cf. image de Galois ;
$\mathbf{D^*_c(1;a_p;1)} = D_I(0,1;a_p,p;0)$, $a_p \in \mathcal{N}_p^\times$;
$\mathbf{D^*_c(2;a_p;1)} = D_I(0,1;a_p,p;\frac{p-1}{2})$, $a_p \in \mathcal{N}_p^\times$;
$\mathbf{D^*_c(1;0)} = D_I(0,1;0,p;0)$;
$\mathbf{D^*_c(2;0)} = D_I(0,1;0,p;\frac{p-1}{2})$;

$\mathbf{D^*_{pc}(e;a_p;\epsilon;0)} = U_1 \oplus U_2$, $e \in \{3,4,6\}$, $e \mid p-1$, $a_p \in \mathcal{N}_{p,e}^\times$, $\epsilon \in \{\pm 1\}$: cf. image de Galois ;
$\mathbf{D^*_{pc}(e;a_p;\epsilon;1)} = D_{III}(0,1;u,u^{-1}p;\epsilon^{\frac{p-1}{e}},-\epsilon^{\frac{p-1}{e}})$, $e \in \{3,4,6\}$ et $e \mid p-1$, $u \in \mathbb{Z}_p^\times$ tel que $u + u^{-1}p = a_p \in \mathcal{N}_{p,e}^\times$, $\epsilon \in \{\pm 1\}$;

$\mathbf{D^*_{pc}(e;0;\alpha)} = D_{IV}(0,1;p;\frac{p+1}{e} - 1, p - \frac{p+1}{e}; p^{-2}\alpha)$, $e \in \{3,4,6\}$ et $e \mid p+1$, $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$.

1.3.1.3. Soit $E/\mathbb{Q}_p$ une courbe elliptique. On retrouve certaines propriétés de E en regardant les invariants de la classe de $\mathbf{D^*_{pst}}(V_p(E))$ (voir **A.2.**) :

$\mathbf{D^*_{pst}}(V_p(E)) \simeq \mathbf{D^*_m(e;b;\alpha)}$: E est une courbe elliptique dont l'invariant modulaire j_E vérifie $v_p(j_E) < 0$. Soit $\gamma_E \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ défini en **1.1.** ; alors on a :
$(e;b) = (1;1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_p$, et E est isomorphe sur $\mathbb{Q}_p$ à une courbe de Tate E_q, avec

$q \in \mathbb{Q}_p^\times$, $v_p(q) > 0$ (et q est uniquement déterminé par j_E, cf. **1.1.1.**). De plus, la pente de la filtration est donnée par $\alpha = \alpha(q) = -\mathrm{Log}(u_q)/v_p(q)$, où l'on a écrit $q = u_q p^{v_p(q)}$, $u_q \in {\mathbb{Z}_p}^\times$, et Log est le logarithme p-adique usuel.
$(e;b) = (1;-1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_{p^2} = M_1$, et E est le twist sur M_1 de E_q (avec $\alpha(q) = \alpha$).
$(e;b) = (2;1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_p(\pi_2) = M_2$, et E est le twist sur M_2 de E_q.
$(e;b) = (2;-1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = M_3$, et E est le twist sur M_3 de E_q.

$\mathbf{D^*_{pst}}(V_p(E)) \simeq \mathbf{D^*_c(e;a_p;\alpha)}$: on a $v_p(j_E) \geq 0$ et $e = 12/\mathrm{pgcd}(v_p(\Delta_E), 12) = \mathrm{dst}(E)$. Si $e = 1$, la courbe E a bonne réduction de type ordinaire sur $\mathbb{Q}_p$, et a_p est la trace du polynôme caractéristique du Frobenius arithmétique agissant sur la courbe réduite $\widetilde{E}$. La suite exacte $(*_{ord})$ est scindée si $\alpha = 0$ et non scindée si $\alpha = 1$, ce qui correspond au fait que le $\mathbb{Q}_p$-espace vectoriel $\mathrm{Ext}^1(\mathbb{Q}_p(\eta_u), \mathbb{Q}_p(\eta_u^{-1}\chi))$ est de dimension un (cf. rmq. à la fin de **3.2.4.**) ; de plus, $\alpha = 0$ si et seulement si E est le relèvement canonique de $\widetilde{E}$ (**3.2.4.** Prop.3). Si $e = 2$, la courbe E est le twist par le caractère ramifié d'ordre 2 correspondant à l'extension $M_2 = \mathbb{Q}_p(\pi_2)$ d'une courbe elliptique du type précédent.

$\mathbf{D^*_{pst}}(V_p(E)) \simeq \mathbf{D^*_c(e;0)}$: on a $v_p(j_E) \geq 0$ et $e = 12/\mathrm{pgcd}(v_p(\Delta_E), 12) = \mathrm{dst}(E)$. Si $e = 1$, la courbe E a bonne réduction de type supersingulière sur $\mathbb{Q}_p$. Si $e = 2$, la courbe E est le twist par un caractère ramifié d'ordre 2 d'une courbe elliptique du type précédent.

$\mathbf{D^*_{pst}}(V_p(E)) \simeq \mathbf{D^*_{pc}(e;a_p;\epsilon;\alpha)}$: on a $v_p(j_E) \geq 0$ et $e = 12/\mathrm{pgcd}(v_p(\Delta_E), 12) = \mathrm{dst}(E)$ divise $p-1$; en outre, j_E est un entier p-adique vérifiant $j_E \equiv 1728 \bmod p\mathbb{Z}_p$ si $e = 4$ et $j_E \equiv 0 \bmod p\mathbb{Z}_p$ si $e = 3$ ou 6. La courbe E a potentiellement bonne réduction de type ordinaire, elle acquiert bonne réduction sur $\mathbb{Q}_p(\pi_e)$, et $a_p \in \mathcal{N}_{p,e}^\times$ est la trace du polynôme caractéristique du Frobenius (arithmétique) agissant sur la courbe réduite. Lorsque l'on prend une équation de Weierstrass minimale pour E, alors $\epsilon = 1$ si $v_p(\Delta_E) < 6$ (i.e. $v_p(\Delta_E) \in \{2,3,4\}$), et $\epsilon = -1$ si $v_p(\Delta_E) > 6$ (i.e. $v_p(\Delta_E) \in \{8,9,10\}$). La suite exacte $(*_{ord})$ est scindée si $\alpha = 0$ et non scindée si $\alpha = 1$, ce qui correspond au fait que le $\mathbb{Q}_p$-espace vectoriel $\mathrm{Ext}^1(\mathbb{Q}_p(\eta_u\xi_e^\epsilon), \mathbb{Q}_p(\eta_u^{-1}\xi_e^{-\epsilon}\chi))$ est de dimension un ; de plus, $\alpha = 0$ si et seulement si $j_E = j(e)$, avec $j(3) = j(6) = 0$ et $j(4) = 1728$, i.e. E_{L_e} est le relèvement canonique de $\widetilde{E}$ (**3.3.1.3.**). Pour les twists d'ordre 2, voir la description faite précédemment.

$\mathbf{D^*_{pst}}(V_p(E)) \simeq \mathbf{D^*_{pc}(e;0;\alpha)}$: on a $v_p(j_E) \geq 0$ et $e = 12/\mathrm{pgcd}(v_p(\Delta_E), 12) = \mathrm{dst}(E)$ divise $p+1$; en outre, j_E est un entier p-adique vérifiant $j_E \equiv 1728 \bmod p\mathbb{Z}_p$ si $e = 4$, et $j_E \equiv 0 \bmod p\mathbb{Z}_p$ si $e = 3$ ou 6. La courbe E a potentiellement bonne réduction de type supersingulière, et acquiert bonne réduction sur $\mathbb{Q}_p(\pi_e)$. De plus, on a $\alpha \in \{0, \infty\}$ si et seulement si $j_E = j(e)$, avec $j(3) = j(6) = 0$ et $j(4) = 1728$ (voir **3.3.3.**, Prop.6). Pour les twists d'ordre 2, voir la description faite précédemment.

Proposition 2.1. :
Soit $p \geq 5$. Soit $E/\mathbb{Q}_p$ une courbe elliptique. L'assertion :

$$(*) \qquad [\ V_p(E) \text{ et } V_p(E') \text{ sont } \mathbb{Q}_p[G]\text{-isomorphes} \Leftrightarrow E \text{ et } E' \text{ sont } \mathbb{Q}_p\text{-isogènes}\ ]$$

est vraie si et seulement si on est dans l'un des trois cas suivants :
(1) *E a potentiellement mauvaise réduction multiplicative ;*

(2) *E a potentiellement bonne réduction supersingulière et* $\mathrm{dst}(E) \geq 3$;
(3) *E est le relèvement canonique sur une extension finie de $\mathbb{Q}_p$ d'une courbe ordinaire.*

Preuve :
(1) $\Rightarrow$ $(*)$ est démontré pour des courbes de Tate dans l'annexe A, en **A.2.2.**, et le cas général s'en déduit par un twist d'ordre deux.
(2) $\Rightarrow$ $(*)$ est démontré en **3.3.3.** Prop. 7, 2).
(3) $\Rightarrow$ $(*)$ provient de la remarque 2 de **3.2.4.** pour $\mathrm{dst}(E) = 1$, et de la remarque 3 à la fin de **3.3.3.** pour $\mathrm{dst}(E) > 1$.
Enfin, les remarques 4 en **3.2.3.** et en **3.2.4.** (pour $\mathrm{dst}(E) = 1$), ainsi que la fin de **3.3.2.2.** (pour $\mathrm{dst}(E) > 1$), montrent que dans tous les autres cas l'assertion $(*)$ est fausse. □

1.3.1.4. *Preuve du théorème 2.1. :*
Les parties *1)* et *2)* sont l'objet de l'annexe A, **A.2.**. Quant à la partie *3)*, nous allons démontrer ici que tous les objets de la liste $\mathbf{D^*}$, *sauf* les $\mathbf{D^*_{pc}(e;0;\alpha)}$, proviennent d'une courbe elliptique sur $\mathbb{Q}_p$. Les cas $\mathbf{D^*_{pc}(e;0;\alpha)}$ sont les plus délicats à traiter ; le résultat est établi au chapitre 3 (en **3.3.4.**), comme conséquence de l'étude des relèvements sur $\mathbb{Z}_p[\pi_e]$ de courbes elliptiques supersingulières sur $\mathbb{F}_p$, ainsi que du théorème de prolongement du chapitre 2.

Pour les cas $\mathbf{D^*_m(e;b;\alpha)}$, le résultat provient du fait que l'application de $p\mathbb{Z}_p\backslash\{0\}$ dans $\mathbb{Q}_p$ qui à q associe $\alpha(q) = -\mathrm{Log}(u_q)/v_p(q)$ est surjective (cf. **A.2.2.**), ainsi que de la description des twists d'ordre 2.

Pour les cas $\mathbf{D^*_c(1;a_p;\alpha)}$, le résultat provient du fait que : pour tout $a_p \in \mathcal{N}_p^\times$, il existe une courbe $\widetilde{E}/\mathbb{F}_p$ telle que $a_p(\widetilde{E}) = a_p$ ([Ho-Ta]) ; toute courbe elliptique sur $\mathbb{F}_p$ se relève en un schéma elliptique sur $\mathbb{Z}_p$, et il existe un relèvement tel que $(*_{ord})$ est scindée, ainsi qu'un relèvement tel que $(*_{ord})$ n'est pas scindée (voir **3.2.4.** et les exemples donnés en **1.3.3.**). Les objets $\mathbf{D^*_c(2;a_p;\alpha)}$ proviennent d'un twist correspondant à l'extension $\mathbb{Q}_p(\pi_2) = M_2$ d'une courbe elliptique du type précédent.

Pour les cas $\mathbf{D^*_c(e;0)}$, le résultat provient du fait que toute courbe elliptique sur $\mathbb{F}_p$ (ici supersingulière) se relève en un schéma elliptique sur $\mathbb{Z}_p$ ainsi que de la description des twists d'ordre 2.

Pour les cas $\mathbf{D^*_{pc}(e;a_p;\epsilon;\alpha)}$, le résultat provient du lemme énoncé en **1.2.1.4.** ainsi que de l'étude des relèvements de courbes elliptiques ordinaires sur $\mathbb{F}_p$ couplée avec le théorème de prolongement du chapitre 2 (voir **3.3.4.**, rmq. 3). Des exemples sont donnés en **1.3.3.**. □

1.3.1.5. Nous allons maintenant donner des conditions nécessaires et suffisantes pour qu'une représentation p-adique V de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ de dimension 2 provienne d'une courbe elliptique $E/\mathbb{Q}_p$, i.e. pour qu'il existe $E/\mathbb{Q}_p$ telle que $V \simeq V_p(E)$.

Théorème 2.2. :
Soit $p \geq 5$. Une représentation p-adique de dimension 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ provient d'une courbe elliptique E sur $\mathbb{Q}_p$ si et seulement si elle est potentiellement semi-stable de type Hodge-Tate $(0,1)$ et la représentation de Weil-Deligne qui lui est associée vérifie les conditions (1°), (2°), (3°) *du théorème* **1.2.**.

Remarque : la condition (3°), qui porte sur la représentation de Weil-Deligne associée à un objet D de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi, N)$, se lit en prenant le polynôme caractéristique du Frobenius sur le $\mathbb{Q}_p$-espace vectoriel $D_0 = D^{<\omega>}$, où ω est un relèvement du Frobenius absolu dans $G_{K/\mathbb{Q}_p}$ (voir **A.2.4.**).

Preuve :
Ces conditions sont clairement nécessaires. Elles sont suffisantes car tous les $D = \mathbf{D}^*_{\mathbf{pst}}(V)$ ainsi obtenus sont dans la liste $\mathbf{D}^*$. En effet, la représentation de Weil-Deligne associée à D se lit sur le $(\varphi, N, G_{K/\mathbb{Q}_p})$-module $D^{(0)}$ obtenu en oubliant la filtration sur D, et la même preuve que celle du théorème **1.2.** montre que $D^{(0)}$ est l'un des $(\varphi, N, G_{K/\mathbb{Q}_p})$-modules déduit de la liste $\mathbf{D}^*$. Puis la filtration sur D est obtenue en écrivant que D est de type Hodge-Tate $(0,1)$ et faiblement admissible (voir les calculs faits en **A.2.**). □

1.3.2. Comparaisons :

En comparant la liste $\mathbf{WD}^*$ avec la liste $\mathbf{D}^*$, on peut dire grossièrement que l'information contenue dans le G-module $V_p(E)$ contient déjà celle que l'on trouve dans les G-modules $V_l(E)$, $l \neq p$, avec une donnée en plus : la filtration. Cela exprime la compatibilité au sens de Weil-Deligne du système de représentations $V_l(E)$, $l \in \mathcal{P}$ (voir [Fo 3]).

Plus précisément, pour toute extension finie galoisienne K de $\mathbb{Q}_p$ on a un foncteur

$$\mathbf{W\widehat{D}}^*_{\mathbf{st,K}} : \mathbf{Rep}_{st,K}(G) \longrightarrow \mathbf{Rep}_{K_0}('W) .$$

Ce foncteur est obtenu en appliquant $\mathbf{D}^*_{\mathbf{st,K/\mathbb{Q}_p}}$, puis en oubliant la filtration, et enfin en faisant agir le groupe de Weil K_0-linéairement : si V est un objet de $\mathbf{Rep}_{st,K}(G)$, l'objet $\mathbf{W\widehat{D}}^*_{\mathbf{st,K}}(V)$ s'identifie au K_0-espace vectoriel $\mathbf{D}^*_{\mathbf{st,K/\mathbb{Q}_p}}(V)$ muni de l'opérateur N, avec $\rho_0(w) = (w \bmod W_K) \cdot \varphi^{-v(w)}$ pour tout $w \in W$, où W_K est le groupe de Weil relatif à K.

Pour tout $l \in \mathcal{P}$, on note $\mathbb{Q}'_l = \mathbb{Q}_l$ si $l \neq p$ et $\mathbb{Q}'_p = K_0$; choisissons des plongements de corps $\iota_l : \mathbb{Q}'_l \hookrightarrow \mathbb{C}$ pour chaque $l \in \mathcal{P}$. Soit $(\Delta_l)_{l\in\mathcal{P}}$ un système de représentations $\mathbb{Q}'_l$-linéaires de $'W$; on dit que ce système est *compatible* si chaque Δ_l est définie sur $\mathbb{Q}$ (voir [Fo 3]), et si les objets $\Delta_l \otimes_{\mathbb{Q}'_l \nearrow \iota_l} \mathbb{C}$ et $\Delta_{l'} \otimes_{\mathbb{Q}'_{l'} \nearrow \iota_{l'}} \mathbb{C}$ de $\mathbf{Rep}_{\mathbb{C}}('W)$ sont isomorphes lorsque l et l' parcourent $\mathcal{P}$. On a alors les mêmes notions et résultats que pour les systèmes $(\Delta_l)_{l\neq p}$, en remplaçant à chaque fois "$l \neq p$" par "$l \in \mathcal{P}$".

Dans les cas $\mathbf{D}^*_{\mathbf{c}}(\mathbf{e};\mathbf{0})$, $e \in \{1,2\}$, la filtration ne joue aucun rôle, mais dans tous les autres cas elle apporte des renseignements supplémentaires :

$\mathbf{WD}^*_{\mathbf{m}}(\mathbf{e};\mathbf{b})$	$\rightsquigarrow$	$\mathbf{D}^*_{\mathbf{m}}(\mathbf{e};\mathbf{b};\alpha)$	, $\alpha \in \mathbb{Q}_p$
$\mathbf{WD}^*_{\mathbf{c}}(\mathbf{e};\mathbf{a_p})$, $a_p \neq 0$	$\rightsquigarrow$	$\mathbf{D}^*_{\mathbf{c}}(\mathbf{e};\mathbf{a_p};\alpha)$	, $\alpha \in \{0,1\}$
$\mathbf{WD}^*_{\mathbf{c}}(\mathbf{e};\mathbf{0})$	$\rightsquigarrow$	$\mathbf{D}^*_{\mathbf{c}}(\mathbf{e};\mathbf{0})$	
$\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon)$	$\rightsquigarrow$	$\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\alpha)$	, $\alpha \in \{0,1\}$
$\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0})$	$\rightsquigarrow$	$\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$	, $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$

On notera que les filtrations sont obtenues simplement en écrivant qu'un objet de la liste $\mathbf{D}^*$ est de type Hodge-Tate $(0,1)$ et faiblement admissible (voir **A.2.**). On obtient la proposition suivante :

Proposition 2.2. :
Soit $p \geq 5$. Etant donné un objet Δ de la liste $\mathbf{WD^*}$*, pour obtenir un objet de la liste* $\mathbf{D^*}$ *dont la représentation du groupe de Weil-Deligne associée est isomorphe sur $\mathbb{C}$ à Δ, on a :*
- une infinité de possibilités paramétrées par $\mathbb{Q}_p$ dans les cas multiplicatifs $\mathbf{WD^*_m}(e;b)$ *; ces cas correspondent à une courbe elliptique qui est le twist par un caractère d'ordre deux d'une courbe de Tate E_q, et la filtration est donnée par $\alpha = \alpha(q) = -Log(u_q)/v_p(q)$, où l'on a écrit $q = u_q p^{v_p(q)}$, $u_q \in \mathbb{Z}_p{}^\times$, et Log est le logarithme p-adique usuel ;*
- deux possibilités dans les cas $\mathbf{WD^*_c(e;a_p)}$*, $a_p \neq 0$ et* $\mathbf{WD^*_{pc}(e;a_p;\epsilon)}$ *; ces cas correspondent à une courbe elliptique potentiellement ordinaire, et la filtration nous renseigne sur le scindage de la suite exacte $(*_{ord})$: elle est scindée si $\alpha = 0$, non scindée si $\alpha = 1$;*
- une seule possibilité dans le cas $\mathbf{WD^*_c(e;0)}$ *;*
- une infinité de possibilités paramétrées par $\mathbb{P}^1(\mathbb{Q}_p)$ dans le cas $\mathbf{WD^*_{pc}(e;0)}$.

On en déduit le résultat suivant :

Corollaire 2.2. :
Soit $p \geq 5$. Le nombre de classes d'isomorphisme d'objets de $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ *provenant d'une courbe elliptique sur $\mathbb{Q}_p$ ayant potentiellement bonne réduction est fini si et seulement si $p \equiv 1 \bmod 12$; il vaut alors $8[2\sqrt{p}] + 66$.*

Plus précisément, si $p \equiv 1 \bmod 12$, il y a : $2.\mathrm{Card}(\mathcal{N}_p^\times) = 4[2\sqrt{p}]$ classes dans $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ provenant de courbes elliptiques sur $\mathbb{Q}_p$ ayant bonne réduction ordinaire sur $\mathbb{Q}_p$, et autant provenant d'un twist ramifié d'ordre deux de courbes du type précédent ; 1 classe provenant de courbes elliptiques sur $\mathbb{Q}_p$ ayant bonne réduction supersingulière sur $\mathbb{Q}_p$, et 1 provenant d'un twist ramifié d'ordre deux de courbes du type précédent ; $2.2.\mathrm{Card}(\mathcal{N}_{p,3}^\times) = 24$ classes provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement ordinaires avec $\mathrm{dst}(E) = 3$; $2.2.\mathrm{Card}(\mathcal{N}_{p,4}^\times) = 16$ classes provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement ordinaires avec $\mathrm{dst}(E) = 4$; et $2.2.\mathrm{Card}(\mathcal{N}_{p,6}^\times) = 24$ classes provenant de courbes elliptiques E sur $\mathbb{Q}_p$ potentiellement ordinaires avec $\mathrm{dst}(E) = 6$.

1.3.3. Exemples :

Courbes potentiellement ordinaires :

Si $4 \mid p-1$:
On reprend les courbes définies en **1.2.2.** : pour chaque $a_{p,j} \in \mathcal{N}_{p,4}^\times$, $1 \leq j \leq 4$, on choisit un élément $u_j \in \mathbb{F}_p^\times$ tel que la trace du Frobenius de la courbe elliptique $\widetilde{E}_j$: $y^2 = x^3 + u_j x$ est $a_{p,j}$; ces courbes sont ordinaires et ont un invariant modulaire égal à $12^3 = 1728$.
On pose $E_{i;j}$: $y^2 = x^3 + [u_j](-p)^i x$, pour $1 \leq j \leq 4$, $0 \leq i \leq 3$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui ont toutes le même invariant modulaire $12^3 = 1728$; pour un j fixé, elles deviennent isomorphes sur $\mathbb{Q}_p(\pi_4)$; elles ont toutes potentiellement bonne réduction, et la courbe réduite sur $\mathbb{Q}_p(\pi_4)$ de $E_{i,j}$ est $\widetilde{E}_j$; la courbe $E_{i+2,j}$ est le twist ramifié d'ordre 2 correspondant à $M_2 = \mathbb{Q}_p(\pi_2)$ de $E_{i,j}$ pour $i \in \{0,1\}$. De plus, pour chacune la suite exacte

$(*_{ord})$ est scindée, cf. chapitre 3, **3.2.4.** et **3.3.1.3.**. On a alors, pour chaque $j \in \{1,2,3,4\}$:

$$\begin{aligned}
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_{0,j})) &\simeq \mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_{p,j}};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_{1,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_{p,j}};\mathbf{1};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_{2,j})) &\simeq \mathbf{D}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_{p,j}};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_{3,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_{p,j}};\mathbf{-1};\mathbf{0}) \ .
\end{aligned}$$

Posons $E'_{i;j}$: $y^2 = x^3 + [u_j](-p)^i x + (-p)^{n(i)}$, pour $1 \leq j \leq 4, 0 \leq i \leq 3$, et $n(i) = 1,2,4,5$ si $i = 0,1,2,3$ respectivement. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui possèdent toutes un invariant modulaire entier congru à $12^3 = 1728$ modulo $p\mathbb{Z}_p$, mais différent de 1728 ; elles ont toutes potentiellement bonne réduction avec un défaut de semi-stabilité égal à 1, 2 ou 4, et la courbe réduite sur $\mathbb{Q}_p(\pi_4)$ de $E'_{i,j}$ est $\widetilde{E}_j$; la courbe $E'_{i+2,j}$ est le twist ramifié d'ordre 2 correspondant à $M_2 = \mathbb{Q}_p(\pi_2)$ de $E'_{i,j}$ pour $i \in \{0,1\}$. De plus, pour chacune la suite exacte $(*_{ord})$ n'est pas scindée, cf. chapitre 3, **3.2.4.** et **3.3.1.3.**. On a alors, pour chaque $j \in \{1,2,3,4\}$:

$$\begin{aligned}
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E'_{0,j})) &\simeq \mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_{p,j}};\mathbf{1}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E'_{1,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_{p,j}};\mathbf{1};\mathbf{1}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E'_{2,j})) &\simeq \mathbf{D}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_{p,j}};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E'_{3,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{a_{p,j}};\mathbf{-1};\mathbf{1}) \ .
\end{aligned}$$

Si $3 \mid p-1$:

On reprend les courbes définies en **1.2.2.** : pour chaque $a_{p,j} \in \mathcal{N}^{\times}_{p,3}$, $1 \leq j \leq 6$, on choisit un élément $v_j \in \mathbb{F}_p^{\times}$ tel que la trace du Frobenius de la courbe elliptique $\widetilde{\mathcal{E}}_j$: $y^2 = x^3 + v_j$ est $a_{p,j}$; ces courbes sont ordinaires et ont un invariant modulaire égal à 0.
On pose $\mathcal{E}_{i;j}$: $y^2 = x^3 + [v_j](-p)^i$, pour $1 \leq j \leq 6$, $0 \leq i \leq 5$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui ont toutes le même invariant modulaire 0 ; pour un j fixé, elles deviennent isomorphes sur $\mathbb{Q}_p(\pi_6)$; elles ont toutes potentiellement bonne réduction, et la courbe réduite sur $\mathbb{Q}_p(\pi_6)$ de $\mathcal{E}_{i,j}$ est $\widetilde{\mathcal{E}}_j$; la courbe $\mathcal{E}_{i+3,j}$ est le twist ramifié d'ordre 2 correspondant à $M_2 = \mathbb{Q}_p(\pi_2)$ de $\mathcal{E}_{i,j}$ pour $i \in \{0,1,2\}$. De plus, pour chacune la suite exacte $(*_{ord})$ est scindée, cf. chapitre 3, **3.2.4.** et **3.3.1.3.**. On a alors, pour chaque $j \in \{1,2,3,4,5,6\}$:

$$\begin{aligned}
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_{0,j})) &\simeq \mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_{p,j}};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_{1,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{a_{p,j}};\mathbf{1};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_{2,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{a_{p,j}};\mathbf{1};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_{3,j})) &\simeq \mathbf{D}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_{p,j}};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_{4,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{a_{p,j}};\mathbf{-1};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_{5,j})) &\simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{a_{p,j}};\mathbf{-1};\mathbf{0}) \ .
\end{aligned}$$

Posons $\mathcal{E}'_{i;j}$: $y^2 = x^3 + (-p)^{m(i)}x + [v_j](-p)^i$, pour $1 \leq j \leq 6$, $0 \leq i \leq 5$, et $m(i) = 1,1,2,3,3,4$ si $i = 0,1,2,3,4,5$ respectivement. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui possèdent toutes un invariant modulaire entier congru à 0 modulo $p\mathbb{Z}_p$, mais non nul ; elles ont toutes potentiellement bonne réduction avec un défaut de semi-stabilité égal à 1, 2, 3 ou 6, et la courbe réduite sur $\mathbb{Q}_p(\pi_6)$ de $\mathcal{E}'_{i,j}$ est $\widetilde{\mathcal{E}}_j$; la courbe $\mathcal{E}'_{i+3,j}$ est le twist ramifié d'ordre 2 correspondant à $M_2 = \mathbb{Q}_p(\pi_2)$ de $\mathcal{E}'_{i,j}$ pour $i \in \{0,1,2\}$. De plus, pour chacune

la suite exacte $(*_{ord})$ n'est pas scindée, cf. chapitre 3, **3.2.4.** et **3.3.1.3.**. On a alors, pour chaque $j \in \{1,2,3,4,5,6\}$:

$$\begin{array}{rcl}
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}'_{0,j})) & \simeq & \mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_{p,j}};\mathbf{1}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}'_{1,j})) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{a_{p,j}};\mathbf{1};\mathbf{1}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}'_{2,j})) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{a_{p,j}};\mathbf{1};\mathbf{1}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}'_{3,j})) & \simeq & \mathbf{D}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_{p,j}};\mathbf{1}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}'_{4,j})) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{a_{p,j}};\mathbf{-1};\mathbf{1}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}'_{5,j})) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{a_{p,j}};\mathbf{-1};\mathbf{1})\ .
\end{array}$$

Courbes potentiellement supersingulières :

Si $4 \mid p+1$:

On reprend les courbes définies en **1.2.2.** : E_i : $y^2 = x^3 + (-p)^i x$, pour $i \in \{0,1,2,3\}$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui ont toutes le même invariant modulaire $12^3 = 1728$; elles deviennent deux-à-deux isomorphes sur $\mathbb{Q}_p(\pi_4)$; elles ont toutes potentiellement bonne réduction supersingulière, et la courbe réduite sur $\mathbb{F}_p$ a pour équation $y^2 = x^3 + x$; pour $i \in \{0,1\}$, E_{i+2} est le twist par le caractère ramifié d'ordre 2 correspondant à l'extension $M_2 = \mathbb{Q}_p(\pi_2)$ de E_i. On a alors:

$$\begin{array}{rcl}
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_0)) & \simeq & \mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_1)) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{0};\infty) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_2)) & \simeq & \mathbf{D}^*_{\mathbf{c}}(\mathbf{2};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_3)) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{4};\mathbf{0};\mathbf{0})\ .
\end{array}$$

On a utilisé le critère sur $v_p(\Delta_{E_i})$ pour déterminer la filtration (cf. remarque dans **1.3.5.**) ; voir aussi la proposition 6 de **3.3.3.**.

Si $3 \mid p+1$:

On reprend les courbes définies en **1.2.2.** : $\mathcal{E}_i$: $y^2 = x^3 + (-p)^i$, pour $i \in \{0,1,2,3,4,5\}$. Ce sont des courbes elliptiques sur $\mathbb{Q}_p$ qui ont toutes le même invariant modulaire 0 ; elles deviennent deux-à-deux isomorphes sur $\mathbb{Q}_p(\pi_6)$; elles ont toutes potentiellement bonne réduction supersingulière, et la courbe réduite sur $\mathbb{F}_p$ a pour équation $y^2 = x^3 + 1$; pour $i \in \{0,1,2\}$, $\mathcal{E}_{i+3}$ est le twist par le caractère ramifié d'ordre 2 correspondant à l'extension $M_2 = \mathbb{Q}_p(\pi_2)$ de $\mathcal{E}_i$. On a alors:

$$\begin{array}{rcl}
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_0)) & \simeq & \mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_1)) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{0};\infty) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_2)) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{0};\infty) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_3)) & \simeq & \mathbf{D}^*_{\mathbf{c}}(\mathbf{2};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_4)) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{0};\mathbf{0}) \\
\mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}_5)) & \simeq & \mathbf{D}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{0};\mathbf{0}).
\end{array}$$

Là encore, on a utilisé le critère sur $v_p(\Delta_{\mathcal{E}_i})$ pour déterminer la filtration ; voir aussi la proposition 6 de **3.3.3.**.

1.3.4. L'image de Galois dans $\mathrm{Aut}_{\mathbb{Q}_p}(V_p(E))$:

Les représentations $\mathbf{D}^*_{\mathbf{c}}(\mathbf{e};\mathbf{0})$, $e \in \{1,2\}$, et $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$, $e \in \{3,4,6\}$ et $e \mid p+1$, $\alpha \in \mathbf{P}^1(\mathbb{Q}_p)$, sont irréductibles (voir néanmoins **B.3.2.2.** dans l'annexe B pour une description). Tous les autres objets D de la liste $\mathbf{D}^*$ sont réductibles, et il est possible de décrire l'action de G sur (le semi-simplifié de) $V_p(E) \simeq \mathbf{V}^*_{\mathbf{pst}}(D)$.

Rappelons que $\chi : G \to \mathbb{Z}_p^\times$ est le caractère cyclotomique donnant l'action de G sur $\mathbb{Z}_p(1)$; on note χ_p sa réduction modulo $p\mathbb{Z}_p$. Pour tout $u \in \mathbb{Z}_p^\times$, on note $\eta_u : G \to G/I \to \mathbb{Z}_p^\times$ l'unique caractère non ramifié qui envoie le Frobenius arithmétique sur u. Lorsque $e \geq 2$ et $e \mid p-1$, on note $\xi_e : G \to G_{K_e/\mathbb{Q}_p} \to \mu_e(\overline{\mathbb{Q}}_p) = <\zeta_e> \subset \mathbb{Z}_p^\times$ le caractère ramifié défini par $\xi_e(g) = g\pi_e/\pi_e$, $g \in G$; on a $\xi_e = [\chi_p]^{\frac{p-1}{e}}$.

$\mathbf{D}^*_{\mathbf{m}}(\mathbf{e};\mathbf{b};\alpha) \simeq \mathbf{D}^*_{\mathbf{st}}(V_p(E))$, $e \in \{1,2\}$, $b \in \{-1,1\}$, $\alpha \in \mathbb{Q}_p$: il existe une $\mathbb{Q}_p$-base de $V_p(E)$ telle que G agit via

$$\begin{pmatrix} \eta_{-1}^{\frac{1-b}{2}}\xi_2^{e-1}\chi & * \\ 0 & \eta_{-1}^{\frac{b-1}{2}}\xi_2^{1-e} \end{pmatrix} \quad \text{avec} \quad * \neq 0 .$$

On note $u \in \mathbb{Z}_p^\times$ l'unique élément vérifiant $u + u^{-1}p = a_p \neq 0$.

$\mathbf{D}^*_{\mathbf{c}}(\mathbf{e};\mathbf{a_p};\alpha) \simeq \mathbf{D}^*_{\mathbf{pst}}(V_p(E))$, $e \in \{1,2\}$, $a_p \in \mathcal{N}_p^\times$, $\alpha \in \{0,1\}$: il existe une $\mathbb{Q}_p$-base de $V_p(E)$ telle que G agit via

$$\begin{pmatrix} \eta_u^{-1}\xi_2^{e-1}\chi & * \\ 0 & \eta_u\xi_2^{e-1} \end{pmatrix} \quad \text{avec} \quad * = 0 \Leftrightarrow \alpha = 0 .$$

$\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\alpha) \simeq \mathbf{D}^*_{\mathbf{pst}}(V_p(E))$, $e \in \{3,4,6\}$ et $e \mid p-1$, $a_p \in \mathcal{N}_{p,e}^\times$, $\epsilon \in \{-1,1\}$, $\alpha \in \{0,1\}$: il existe une $\mathbb{Q}_p$-base de $V_p(E)$ telle que G agit via

$$\begin{pmatrix} \eta_u^{-1}\xi_e^{-\epsilon}\chi & * \\ 0 & \eta_u\xi_e^{\epsilon} \end{pmatrix} \quad \text{avec} \quad * = 0 \Leftrightarrow \alpha = 0 .$$

1.3.5. Les $\mathbb{Z}_p[G]$-modules provenant d'une courbe elliptique sur $\mathbb{Q}_p$:

Nous allons donner ici la classification des $\mathbb{Z}_p[G]$-modules $T_p(E)$ ainsi que des $\mathbb{F}_p[G]$-modules $E[p] = T_p(E)/pT_p(E)$, où $E/\mathbb{Q}_p$ est une courbe elliptique. Rappelons que classifier les $\mathbb{Z}_p[G]$-modules $T_p(E)$ revient à classifier les $\mathbb{Z}_p$-réseaux G-stables des $\mathbb{Q}_p[G]$-modules provenant d'une courbe elliptique sur $\mathbb{Q}_p$. Ces résultats sont connus : voir [Se 1], [Se 2] et [Kr] ; seules certaines méthodes sont nouvelles. Les calculs sont l'objet de l'annexe B.

On note $\chi_p = \chi \bmod p\mathbb{Z}_p : G \to \mathbb{F}_p^\times$ le caractère donnant l'action de G sur les racines p-ièmes de l'unité. Soient $\pi \in \overline{\mathbb{Q}}_p$ tel que $\pi^{p^2-1} = -p$, et $\mathbb{F}_{p^2}$ le corps résiduel de $\mathbb{Q}_{p^2}$ qui est

aussi celui de $\mathbb{Q}_{p^2}(\pi)$; alors on a un isomorphisme canonique :

$$\psi_2 \ : \ \left\{ \begin{array}{ccc} I(\mathbb{Q}_{p^2}(\pi)/\mathbb{Q}_p) & \xrightarrow{\sim} & \mathbb{F}_{p^2}^\times \\ g & \longmapsto & \dfrac{g\pi}{\pi} \ . \end{array} \right.$$

On note encore ψ_2 le composé $I \to I(\mathbb{Q}_{p^2}(\pi)/\mathbb{Q}_p) \to \mathbb{F}_{p^2}^\times$ (c'est le "caractère fondamental de niveau 2", voir [Se 2]). On a $\chi_p^{p-1} = 1$ et $\psi_2^{p+1} = (\chi_p)_{|I}$, $\psi_2^{p^2-1} = 1$. Pour tout $u \in \mathbb{F}_p^\times$, on note $\eta_u : G \longrightarrow G/I \longrightarrow \mathbb{F}_p^\times$ l'unique caractère non ramifié qui envoie le Frobenius arithmétique sur u ; si $a \in \mathbb{Z}_p^\times$, on pose : $\overline{a} = a \bmod p\mathbb{Z}_p \in \mathbb{F}_p^\times$. Enfin, on notera $\mathbb{Q}_{p^4}$ l'extension non ramifiée de $\mathbb{Q}_p$ de degré 4 contenue dans $\overline{\mathbb{Q}}_p$.

$\underline{\mathbf{D}_{\mathbf{m}}^*(\mathbf{e};\mathbf{b};\alpha) \simeq \mathbf{D}_{\mathbf{pst}}^*(V_p(E))}$, $e \in \{1,2\}$, $b \in \{-1,1\}$, $\alpha \in \mathbb{Q}_p$:
E est le twist par un caractère d'ordre 1 ou 2 d'une courbe de Tate E_q, $q \in p\mathbb{Z}_p\backslash\{0\}$. La suite exacte de G-modules $(*_m)$: $0 \to \mathbb{Z}_p(1) \to T_p(E_q) \to \mathbb{Z}_p \to 0$ n'étant pas scindée, il existe un plus grand entier $n_p(q)$ tel que $X^{p^n} - q$ admet une racine dans $\mathbb{Q}_p$, c'est-à-dire tel que $q \in (\mathbb{Q}_p^\times)^{p^{n_p(q)}}$. *Alors il existe une $\mathbb{Q}_p$-base (e_1, e_2) de $V_p(E)$ telle que, à isomorphisme près, les réseaux stables par G sont les :*

$$\mathbb{Z}_p e_1 \oplus p^m \mathbb{Z}_p e_2 \quad , \quad m \geq -n_p(q) \ .$$

Remarque : $q \in (\mathbb{Q}_p^\times)^{p^n}$ implique $v_p(q) = -v_p(j_E) \equiv 0 \mod p^n\mathbb{Z}$.
Action de G sur $E[p]$: *il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via*

$$\begin{pmatrix} \eta_{-1}^{\frac{1-b}{2}} \chi_p^{1-\frac{p-1}{e}} & * \\ 0 & \eta_{-1}^{\frac{b-1}{2}} \chi_p^{\frac{p-1}{e}} \end{pmatrix} \qquad \textit{avec} \qquad * = 0 \ \Leftrightarrow \ n_p(q) \geq 1 \ .$$

$\underline{\mathbf{D}_{\mathbf{c}}^*(\mathbf{e};\mathbf{a_p};\alpha) \simeq \mathbf{D}_{\mathbf{pst}}^*(V_p(E))}$, $e \in \{1,2\}$, $a_p \in \mathcal{N}_p^\times$, $\alpha \in \{0,1\}$:
E est le twist par un caractère ramifié d'ordre 1 ou 2 d'une courbe elliptique ayant bonne réduction ordinaire sur $\mathbb{Q}_p$.
- Si $\alpha = 0$: *Les réseaux de $V_p(E)$ stables par G sont tous isomorphes.*
- Si $\alpha = 1$: La suite exacte de $\mathbb{Z}_p[G]$-modules $(*_{ord})$: $0 \to T_p(E(p)^0) \to T_p(E) \to T_p(\widetilde{E}) \to 0$ n'étant pas scindée, il existe un plus grand entier naturel n_E tel que la suite exacte de $\mathbb{Z}/p^{n_E}\mathbb{Z}[G]$-modules $(*_{ord})$ mod p^{n_E} soit scindée. *Alors il existe une $\mathbb{Q}_p$-base (e_1, e_2) de $V_p(E)$ telle que, à isomorphisme près, les réseaux stables par G sont les :*

$$\mathbb{Z}_p e_1 \oplus p^m \mathbb{Z}_p e_2 \quad , \quad m \geq -n_E \ .$$

Action de G sur $E[p]$: *il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via*

$$\begin{pmatrix} \eta_{\overline{a}_p}^{-1} \chi_p^{1-\frac{p-1}{e}} & * \\ 0 & \eta_{\overline{a}_p} \chi_p^{\frac{p-1}{e}} \end{pmatrix} \qquad \textit{avec} \qquad * = 0 \ \Leftrightarrow \ [\, \alpha = 0 \ \textit{ou} \ n_E \geq 1 \,] \ .$$

$\mathbf{D_c^*(e;0) \simeq D_{pst}^*(V_p(E))}$, $e \in \{1,2\}$:
E est le twist par un caractère ramifié d'ordre 1 ou 2 d'une courbe elliptique ayant bonne réduction supersingulière sur $\mathbb{Q}_p$.
Les réseaux de $V_p(E)$ stables par G sont tous homothétiques. Action de G sur $E[p]$:
Soient $\pi, \zeta \in \overline{\mathbb{Q}}_p$ tels que $\pi^{p^2-1} = -p$ et $\zeta^{p+1} = -1$. Il existe une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1 sur $E[p]$ telle que G agit via

$$G \longrightarrow \mathrm{Gal}(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2}) \ ,$$

où $I(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p)$ agit via $\psi_2^{1-\frac{p^2-1}{e}}$, et le relèvement du Frobenius fixant π agit semi-linéairement par $x \mapsto \zeta x^p$, $x \in \mathbb{F}_{p^2}$. La classe d'isomorphisme ne dépend pas du choix de ζ, et la représentation est absolument irréductible. Avec les notations de [Fo-Ma], pour $e = 1$ c'est l'objet $\overline{V}_{1,1}$, et pour $e = 2$ c'est l'objet $\overline{V}_{1-\frac{p^2-1}{2},1}$. *L'action de I sur $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ est diagonalisable, et il existe une $\mathbb{F}_{p^2}$-base telle que I agit via*

$$\begin{pmatrix} \psi_2^{1-\frac{p^2-1}{e}} & 0 \\ 0 & \psi_2^{p+\frac{p^2-1}{e}} \end{pmatrix} .$$

$\mathbf{D_{pc}^*(e;a_p;\epsilon;\alpha) \simeq D_{pst}^*(V_p(E))}$, $e \in \{3,4,6\}$ et $e \mid p-1$, $a_p \in \mathcal{N}_{p,e}^{\times}$, $\epsilon \in \{\pm 1\}$, $\alpha \in \{0,1\}$:
E est une courbe elliptique ayant bonne réduction ordinaire sur $K = \mathbb{Q}_p(\pi_e)$.
- Si $\alpha = 0$: *Les réseaux de $V_p(E)$ stables par G sont tous isomorphes.*
- Si $\alpha = 1$: La suite exacte de $\mathbb{Z}_p[G]$-modules $(*_{ord})$: $0 \to T_p(E_K(p)^0) \to T_p(E) \to T_p(\widetilde{E}_K) \to 0$ n'étant pas scindée, il existe un plus grand entier naturel n_E tel que la suite exacte de $\mathbb{Z}/p^{n_E}\mathbb{Z}[G]$-modules $(*_{ord})$ mod p^{n_E} soit scindée. *Alors il existe une $\mathbb{Q}_p$-base (e_1, e_2) de $V_p(E)$ telle que, à isomorphisme près, les réseaux stables par G sont les :*

$$\mathbb{Z}_p e_1 \oplus p^m \mathbb{Z}_p e_2 \quad , \quad m \geq -n_E \ .$$

Action de G sur $E[p]$: *il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via*

$$\begin{pmatrix} \eta_{\overline{a}_p}^{-1} \chi_p^{1-\epsilon\frac{p-1}{e}} & * \\ 0 & \eta_{\overline{a}_p} \chi_p^{\epsilon\frac{p-1}{e}} \end{pmatrix} \quad \textit{avec} \quad * = 0 \Leftrightarrow [\, \alpha = 0 \ \textit{ou} \ n_E \geq 1 \,] \ .$$

D'après les résultats de A. Kraus, si l'on prend une équation minimale pour E, alors on a $\epsilon = 1 \Leftrightarrow v_p(\Delta_E) < 6 \Leftrightarrow v_p(\Delta_E) \in \{2,3,4\}$, et $\epsilon = -1 \Leftrightarrow v_p(\Delta_E) > 6 \Leftrightarrow v_p(\Delta_E) \in \{8,9,10\}$ ([Kr], 2.3.1., Prop.1).

$\mathbf{D_{pc}^*(e;0;\alpha) \simeq D_{pst}^*(V_p(E))}$, $e \in \{3,4,6\}$ et $e \mid p+1$, $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$:
E est une courbe elliptique ayant bonne réduction supersingulière sur $\mathbb{Q}_{p^2}(\pi_e)$.
- *Si $v_p(\alpha) \neq 1$, alors tous les réseaux de $V_p(E)$ stables par G sont homothétiques.*
- *Si $v_p(\alpha) = 1$, alors, à isomorphisme près, il y a deux réseaux stables par G.*

Action de G sur $E[p]$: *Soient $\pi, \zeta \in \overline{\mathbb{Q}}_p$ tels que $\pi^{p^2-1} = -p$ et $\zeta^{p+1} = -1$. Les classes d'isomorphisme des représentations ci-dessous ne dépendent pas du choix de ζ.*

- *Si $v_p(\alpha) \geq 2$, il existe une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1 sur $E[p]$ telle que G agit via*

$$G \longrightarrow \mathrm{Gal}\,(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2})\ ,$$

où $I(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p)$ agit via $\psi_2^{1+\frac{p^2-1}{e}}$, et le relèvement du Frobenius fixant π agit semi-linéairement par $x \mapsto \zeta x^p$, $x \in \mathbb{F}_{p^2}$. La représentation est absolument irréductible, et correspond dans [Fo-Ma] à l'objet $\overline{V}_{1+\frac{p^2-1}{e},1}$. *L'action de I sur $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ est diagonalisable, et il existe une $\mathbb{F}_{p^2}$-base telle que I agit via*

$$\begin{pmatrix} \psi_2^{1+\frac{p^2-1}{e}} & 0 \\ 0 & \psi_2^{p-\frac{p^2-1}{e}} \end{pmatrix}\ .$$

- *Si $v_p(\alpha) \leq 0$, il existe une structure de $\mathbb{F}_{p^2}$-espace vectoriel sur $E[p]$ telle que G agit via*

$$G \longrightarrow \mathrm{Gal}\,(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2})\ ,$$

où $I(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p)$ agit via $\psi_2^{1-\frac{p^2-1}{e}}$, et le relèvement du Frobenius fixant π agit semi-linéairement par $x \mapsto \zeta x^p$, $x \in \mathbb{F}_{p^2}$. La représentation est absolument irréductible, et correspond dans [Fo-Ma] à l'objet $\overline{V}_{1-\frac{p^2-1}{e},1}$. *L'action de I sur $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ est diagonalisable, et il existe une $\mathbb{F}_{p^2}$-base telle que I agit via*

$$\begin{pmatrix} \psi_2^{1-\frac{p^2-1}{e}} & 0 \\ 0 & \psi_2^{p+\frac{p^2-1}{e}} \end{pmatrix}\ .$$

- *Si $v_p(\alpha) = 1$, il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via*

$$\begin{pmatrix} \eta_{\overline{p/\alpha}}\chi_p^{\frac{p+1}{e}} & * \\ 0 & \eta_{p/\alpha}^{-1}\chi_p^{1-\frac{p+1}{e}} \end{pmatrix} \quad \textit{ou} \quad \begin{pmatrix} \eta_{p/\alpha}^{-1}\chi_p^{1-\frac{p+1}{e}} & * \\ 0 & \eta_{\overline{p/\alpha}}\chi_p^{\frac{p+1}{e}} \end{pmatrix}\ .$$

Remarque : d'après A. Kraus, les cas $v_p(\alpha) \geq 2$ et $v_p(\alpha) = 1$, situation de gauche, correspondent à $v_p(\Delta_E) > 6$, où l'on a choisi une équation *minimale* pour la courbe elliptique E ; les cas $v_p(\alpha) \leq 0$ et $v_p(\alpha) = 1$, situation de droite, correspondent à $v_p(\Delta_E) < 6$ ([Kr], 2.3.2., Prop.2 et Lemme 2).

Pour finir, remarquons que, pour les mêmes raisons que dans le cas $l \neq p$, on a le résultat suivant :

Un $\mathbb{Z}_p[G]$-module T provient d'une courbe elliptique sur $\mathbb{Q}_p$ si et seulement si le $\mathbb{Q}_p[G]$-module $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$ provient d'une courbe elliptique sur $\mathbb{Q}_p$.

CHAPITRE 2

Actions prolongées et schémas abéliens

On note $\mathcal{P}$ l'ensemble des nombres premiers.
Dans tout ce qui suit, K est une extension finie de $\mathbb{Q}_p$, de corps résiduel $k = \mathbb{F}_q$, avec $q = p^m$. On fixe une clôture algébrique $\overline{K}$ de K ; son corps résiduel $\overline{k}$ est aussi une clôture algébrique de k. On note L une extension finie galoisienne de K contenue dans $\overline{K}$, et $G_K = \mathrm{Gal}(\overline{K}/K)$, $G_L = \mathrm{Gal}(\overline{K}/L)$.

Soit A une variété abélienne sur L. On dit que A *est définie sur* K s'il existe une variété abélienne $\mathcal{A}$ sur K et un isomorphisme de variétés abéliennes $\psi : \mathcal{A} \times_K L \simeq A$ défini sur L. On s'intéresse au cas où A a bonne réduction sur L, et L/K est une extension finie galoisienne totalement ramifiée. Le but de ce chapitre est de donner un critère portant sur le G_L-module $T_p(A)$ pour que A puisse être définie sur K.
Rappelons d'abord un résultat dû à J.-P. Serre et J. Tate (voir [Se-Ta]). Soit $\mathcal{A}$ une variété abélienne sur K ayant potentiellement bonne réduction qui acquiert bonne réduction sur L. Alors le groupe $\mathrm{Gal}(L/K)$ opère sur $\mathcal{A}_L = \mathcal{A} \times_K L$ via son action sur L, et cette action s'étend par fonctorialité sur le modèle de Néron de $\mathcal{A}_L$. Comme $\mathrm{Gal}(L/K)$ opère trivialement sur le corps résiduel k de L, son action sur la fibre spéciale $\widetilde{\mathcal{A}}$ de $\mathcal{A}_L$ s'effectue par des k-automorphismes de $\widetilde{\mathcal{A}}$, c'est-à-dire par un morphisme $\mathrm{Gal}(L/K) \to \mathrm{Aut}_k(\widetilde{\mathcal{A}})$.
Réciproquement, soit A/L une variété abélienne ayant bonne réduction sur L, et soit $\widetilde{A}$ sa fibre spéciale. Si l'action de G_L sur $T_p(A)$ s'étend en une action de G_K de sorte qu'elle "provient", en un sens que nous définissons, d'un morphisme $\mathrm{Gal}(L/K) \to \mathrm{Aut}_k(\widetilde{A})$, nous montrons qu'alors A est définie sur K ; l'isomorphisme $\psi : \mathcal{A} \times_K L \simeq A$ induira alors un isomorphisme G_K-équivariant :

$$\psi_p : \underbrace{T_p(\mathcal{A})}_{\text{action naturelle}} \simeq \underbrace{T_p(A)}_{\text{action étendue}} .$$

On essaye ensuite de donner un critère portant sur les G_L-modules $T_l(A)$, $l \in \mathcal{P}$, pour que A puisse être définie sur K. Le critère que l'on a en vue concerne la possibilité de prolonger convenablement l'action naturelle de G_L sur tous les $T_l(A)$, $l \in \mathcal{P}$; l'isomorphisme $\psi : \mathcal{A} \times_K L \simeq A$ induira alors des isomorphismes G_K-équivariants pour tous les $l \in \mathcal{P}$:

$$\psi_l : \underbrace{T_l(\mathcal{A})}_{\text{action naturelle}} \simeq \underbrace{T_l(A)}_{\text{action étendue}} .$$

On y arrive lorsque $p \geq 5$, et A est une courbe elliptique ayant bonne réduction sur L telle que l'anneau des k-endomorphismes de sa fibre spéciale est commutatif.

Les principaux outils que nous utilisons ici sont le critère de Weil ([W]) et le théorème de Serre-Tate (voir [Ka]) ; on les combine ensemble en **2.1.**. Le théorème de prolongement est énoncé en **2.1.4.**. En **2.2.**, on explique la notion de compatibilité d'un système de représentations l-adiques du groupe de Galois d'un corps local (de corps résiduel fini) lorsque l parcourt tous les nombres premiers (**2.2.1.**), et l'on dégage un résultat en **2.2.2.** permettant de se ramener à une action étendue fidèle. Puis, à partir de **2.3.**, on se restreint au cas des courbes elliptiques. Le théorème de prolongement dans le cas commutatif est énoncé en **2.4.** ; on en donne une première version suivie d'une preuve en **2.4.1.**, puis une version plus précise en **2.4.3.**. Enfin, le dernier paragraphe contient une généralisation du théorème de prolongement dans le cas commutatif ; on obtient des résultats à isogénie près (**2.4.4.**).

Les résultats établis dans ce chapitre nous serviront de façon essentielle dans le chapitre 3, en **3.3.3.**.

2.1. Variétés abéliennes et critère de Weil :

On note k_L le corps résiduel de L, et O_K (resp. O_L) l'anneau des entiers de K (resp. L). On pose $G_{L/K} = \mathrm{Gal}(L/K)$, et l'on note I_K, I_L, $I_{L/K}$ les sous-groupes d'inertie respectifs de G_K, G_L et $G_{L/K}$.

2.1.1. Actions prolongées :

Soit A une variété abélienne sur L, et $\omega \in G_{L/K}$. On note A^ω la variété déduite de A par le changement de base $\mathrm{Spec}(\omega^{-1}) : \mathrm{Spec}(L) \to \mathrm{Spec}(L)$. Plus précisément, écrivons A comme réunion d'ouverts affines : $A = \bigcup_{1 \leq i \leq r} \mathrm{Spec}\, B_i$, où les B_i sont des L-algèbres. Alors $A^\omega = \bigcup_{1 \leq i \leq r} \mathrm{Spec}\, B_i^\omega$, avec $B_i^\omega = B_i \otimes_{L \nearrow_{\omega^{-1}}} L$: l'application $b \mapsto b \otimes 1$ définit un isomorphisme d'anneaux de B_i dans B_i^ω, mais pour $\lambda \in L$ et $b \in B_i$, $\lambda \cdot (b \otimes 1) = b \otimes \lambda = \omega^{-1}(\lambda) b \otimes 1$; on écrit : $\lambda \cdot b = \omega^{-1}(\lambda) b$. On voit que pour tous $\omega, \tau \in G_{L/K}$, on a $(A^\omega)^\tau = A^{\tau\omega}$. Si A et A' sont deux variétés abéliennes sur L et si $\psi : A \to A'$ est un morphisme, alors le morphisme $\psi^\omega : A^\omega \to (A')^\omega$ est donné par $\psi^\omega = \psi \times_{\mathrm{Spec}(L)} \mathrm{Id}_{\mathrm{Spec}(L)}$. De plus, si A a bonne réduction sur L, alors A^ω aussi.
L'association $A \mapsto A^\omega$ définit un foncteur F_ω de la catégorie des variétés abéliennes sur L dans elle-même, et l'on a $F_{\omega\tau} = F_\omega \circ F_\tau$ pour tous $\omega, \tau \in G_{L/K}$, et $F_1 = \mathrm{Id}$; on dit que $G_{L/K}$ agit sur la catégorie.

Exemple : Soit E/L une courbe elliptique qui admet l'équation $y^2 = x^3 + ax + b$ pour modèle de Weierstrass, avec $a, b \in L$. Soit $\omega \in G_{L/K}$; alors $y^2 = x^3 + \omega(a)x + \omega(b)$ est un modèle de Weierstrass de la courbe E^ω.

Au niveau des points, on a :

$$A(\overline{K}) = \bigcup_{1\leq i\leq r} \mathrm{Hom}_{L-alg}\Big(B_i, \overline{K}\Big) \qquad \text{et} \qquad A^\omega(\overline{K}) = \bigcup_{1\leq i\leq r} \mathrm{Hom}_{L-alg}\Big(B_i^\omega, \overline{K}\Big) \ ;$$

Le groupe G_L agit de façon naturelle sur $A(\overline{K})$ et sur $A^\omega(\overline{K})$. Si $f_i : B_i \longrightarrow \overline{K}$ est un morphisme de L-algèbres, et si $\widehat{\omega}$ est un relèvement de ω dans G_K, alors :

$$\forall\, \lambda \in L\ ,\ \forall\, b \in B_i^\omega\ , \qquad (\widehat{\omega}\circ f_i)(\lambda\cdot b) = \widehat{\omega}\circ\Big(\omega^{-1}(\lambda) f_i(b)\Big) = \lambda(\widehat{\omega}\circ f_i)(b)\ .$$

Donc $\widehat{\omega}\circ f_i \in \mathrm{Hom}_{L-alg}(B_i^\omega, \overline{K})$. On obtient ainsi un morphisme de groupes bijectif :

$$\left\{\begin{array}{ccc} A(\overline{K}) & \xrightarrow{\sim} & A^\omega(\overline{K}) \\ \eta & \longmapsto & \widehat{\omega}\circ\eta \end{array}\right.$$

qui vérifie : $\forall\, g \in G_L\ ,\ \widehat{\omega}\circ(g\eta) = \widehat{\omega} g \widehat{\omega}^{-1}\,(\widehat{\omega}\circ\eta)$, où $\widehat{\omega} g \widehat{\omega}^{-1} \in G_L$ puisque G_L est invariant dans G_K. Ce morphisme dépend du relèvement $\widehat{\omega}$ choisi : un autre relèvement s'écrit $\widehat{\omega}h$, avec $h \in G_L$, et l'on a $(\widehat{\omega}h)\circ\eta = \widehat{\omega}h\widehat{\omega}^{-1}\,(\widehat{\omega}\circ\eta)$, pour $\eta \in A(\overline{K})$. Si l'on note $\psi(\overline{K})$: $A(\overline{K}) \to A'(\overline{K})$ le morphisme déduit de $\psi : A \to A'$, alors $\eta \mapsto \widehat{\omega}\circ\psi(\overline{K})(\widehat{\omega}^{-1}\circ\eta)$ est un morphisme de $A^\omega(\overline{K})$ dans $(A')^\omega(\overline{K})$ qui est indépendant du relèvement $\widehat{\omega}$ choisi, et l'on a $(\psi^\omega)(\overline{K})(\eta) = \widehat{\omega}\circ\psi(\overline{K})(\widehat{\omega}^{-1}\circ\eta)$ pour tout $\eta \in A^\omega(\overline{K})$.

Pour $l \in \mathcal{P}$, notons $\alpha_{\widehat{\omega}} : T_l(A) \longrightarrow T_l(A^\omega)$ la bijection $\mathbb{Z}_l$-linéaire qui se déduit de $\eta \mapsto \widehat{\omega}\circ\eta$.

Lemme 1 :
Soit $l \in \mathcal{P}$. On se donne un morphisme $\rho : G_K \to \mathrm{Aut}(T_l(A))$ tel que la restriction de ρ à G_L est l'action naturelle. Alors, pour tout $\omega \in G_{L/K}$, l'isomorphisme $\mathbb{Z}_l$-linéaire

$$f_{\omega,l} : \left\{\begin{array}{ccc} T_l(A) & \longrightarrow & T_l(A^\omega) \\ x & \longmapsto & \alpha_{\widehat{\omega}}(\rho(\widehat{\omega}^{-1})(x)) \end{array}\right.$$

est G_L-équivariant et ne dépend pas du relèvement de ω dans G_K.

Preuve :
Soient $\omega \in G_{L/K}$ et $\widehat{\omega}$ un relèvement de ω dans G_K ; soit $\widehat{\omega}h$, $h \in G_L$, un autre relèvement. Pour $x \in T_l(A)$, on a :
$\alpha_{\widehat{\omega}h}(\rho((\widehat{\omega}h)^{-1})(x)) = \widehat{\omega}h\widehat{\omega}^{-1}\,\alpha_{\widehat{\omega}}(\rho(h^{-1}\widehat{\omega}^{-1})(x)) = \widehat{\omega}h\widehat{\omega}^{-1}\widehat{\omega}h^{-1}\widehat{\omega}^{-1}\alpha_{\widehat{\omega}}(\rho(\widehat{\omega}^{-1})(x)) = \alpha_{\widehat{\omega}}(\rho(\widehat{\omega}^{-1})(x))$.
Donc $f_{\omega,l}$ ne dépend pas du relèvement de ω choisi, et $f_{\omega,l}$ est clairement une bijection. Il reste à voir qu'elle commute à l'action de G_L. Soient $g \in G_L$ et $x \in T_l(A)$; on a :
$f_{\omega,l}(gx) = \alpha_{\widehat{\omega}}(\rho(\widehat{\omega}^{-1}g)(x)) = \alpha_{\widehat{\omega}}(\rho(\widehat{\omega}^{-1}g\widehat{\omega}\widehat{\omega}^{-1})(x)) = \widehat{\omega}\widehat{\omega}^{-1}g\widehat{\omega}\widehat{\omega}^{-1}\alpha_{\widehat{\omega}}(\rho(\widehat{\omega}^{-1})(x)) = g f_{\omega,l}(x)$,
puisque $\widehat{\omega}^{-1}g\widehat{\omega} \in G_L$. □

Ainsi, si l'action de G_L sur $T_l(A)$ s'étend en une action de G_K, elle induit un isomorphisme de $\mathbb{Z}_l[G_L]$-modules entre $T_l(A)$ et $T_l(A^\omega)$ pour tout $\omega \in G_{L/K}$.
Remarque : Soit A/L ayant bonne réduction, $\widetilde{A}$ sa fibre spéciale, et soit $\tau \in I_{L/K}$; notons qu'alors $\widetilde{A^\tau} = \widetilde{A}^\tau = \widetilde{A}$, i.e. A^τ et A ont la même fibre spéciale. Pour $l \neq p$, le morphisme de réduction induit des isomorphismes de $\mathbb{Z}_l[G_L]$-modules $T_l(A) \simeq T_l(\widetilde{A}) = T_l(\widetilde{A^\tau}) \simeq T_l(A^\tau)$, de sorte que $T_l(A)$ est isomorphe à $T_l(A^\tau)$. Néanmoins, cet isomorphisme induit l'identité sur

$T_l(\widetilde{A})$, alors que ce n'est pas forcément le cas pour un $f_{\tau,l}$ provenant d'une action étendue construit comme ci-dessus.

Dans la suite, si l'on se donne une action linéaire et continue de G_K sur $T_l(A)$ dont la restriction à G_L est l'action naturelle, le morphisme ρ sera sous-entendu, pour ne pas alourdir les notations.

Soient A et B deux variétés abéliennes sur L. Pour $l \in \mathcal{P}$ et pour $\omega \in G_{L/K}$, choisissons un relèvement $\widehat{\omega}$ dans G_K, et notons $\alpha_{\widehat{\omega}} : T_l(A) \to T_l(A^\omega)$ et $\beta_{\widehat{\omega}} : T_l(B) \to T_l(B^\omega)$ les bijections déduites de $\eta \mapsto \widehat{\omega} \circ \eta$, pour $\eta \in A(\overline{K})$ et $\eta \in B(\overline{K})$ respectivement. Soit $f_l : T_l(A) \to T_l(B)$ un morphisme de $\mathbb{Z}_l[G_L]$-modules.
Les relations $\alpha_{\widehat{\omega}}^{-1}(gx) = \widehat{\omega}^{-1} g \widehat{\omega}\, \alpha_{\widehat{\omega}}^{-1}(x)$ et $\beta_{\widehat{\omega}}(gy) = \widehat{\omega} g \widehat{\omega}^{-1}\, \beta_{\widehat{\omega}}(y)$ pour $g \in G_L$ et $x \in T_l(A)$, $y \in T_l(B)$, montrent que l'application $\beta_{\widehat{\omega}} \circ f_l \circ \alpha_{\widehat{\omega}}^{-1} : T_l(A^\omega) \to T_l(B^\omega)$ est G_L-équivariante, et les relations $\alpha_{\widehat{\omega}h}^{-1} = \alpha_{\widehat{\omega}}^{-1}\, \widehat{\omega} h^{-1} \widehat{\omega}^{-1}$, $\beta_{\widehat{\omega}h} = \widehat{\omega} h \widehat{\omega}^{-1}\, \beta_{\widehat{\omega}}$ pour $h \in G_L$ montrent qu'elle ne dépend pas du relèvement de ω choisi. Si f_l provient d'un morphisme $f : A \to B$, i.e. si $f_l = T_l(f)$, alors $T_l(f^\omega) = \beta_{\widehat{\omega}} \circ f_l \circ \alpha_{\widehat{\omega}}^{-1}$.

2.1.2. Le critère de Weil :

Soit V une variété algébrique sur L. On suppose qu'il existe des isomorphismes de variétés $f_{\tau,\omega} : V^\omega \longrightarrow V^\tau$, $\omega, \tau \in G_{L/K}$, définis sur L, vérifiant pour tout $\tau' \in G_{L/K}$ les conditions :

$$(i) \quad f_{\tau,\tau'} = f_{\tau,\omega} \circ f_{\omega,\tau'}$$
$$(ii) \quad (f_{\tau,\tau'})^\omega = f_{\omega\tau,\omega\tau'} .$$

Alors il existe une variété $\mathcal{V}$ sur K et un isomorphisme de variétés $\mathcal{V} \times_K L \xrightarrow{\psi} V$ défini sur L tel que $f_{\tau,\omega} = \psi^\tau \circ (\psi^\omega)^{-1}$ pour tous $\omega, \tau \in G_{L/K}$ (donc V est définie sur K) ; le couple $(\mathcal{V}, \psi)$, où ψ vérifie $f_{\tau,\omega} = \psi^\tau \circ (\psi^\omega)^{-1}$ pour tous $\omega, \tau \in G_{L/K}$, est alors unique à K-isomorphisme près ([W]). Si de plus V est projective, on peut choisir $\mathcal{V}$ projective (loc. cit.).
On voit facilement que les conditions (i) et (ii) précédentes sont équivalentes à la suivante : il existe des L-isomorphismes de variétés $f_\omega : V \longrightarrow V^\omega$, $\omega \in G_{L/K}$, vérifiant

$$(*) \qquad f_{\omega\tau} = (f_\tau)^\omega \circ f_\omega \qquad\qquad \forall\, \omega, \tau \in G_{L/K} .$$

En effet, il suffit de poser $f_{\tau,\omega} = (f_{\omega^{-1}\tau})^\omega$ et la condition (ii) est automatiquement vérifiée, alors que (i) équivaut à (*); remarquons que (*) implique $f_1 = \mathrm{Id}_V$, où 1 est l'élément neutre de $G_{L/K}$. Alors il existe une variété $\mathcal{V}$ sur K et un L-isomorphisme $\psi : \mathcal{V} \times_K L \longrightarrow V$ tel que, pour tout $\omega \in G_{L/K}$, $f_\omega = \psi^\omega \circ \psi^{-1}$. Dans la suite, nous appellerons la condition (*) *condition de cohérence*, et les $\{f_\omega, \omega \in G_{L/K}\}$ un *système cohérent d'isomorphismes.*
Prenons maintenant $V = A$ une variété abélienne sur L, et, dans la condition (*), supposons que les $f_\omega, \omega \in G_{L/K}$, sont des isomorphismes de variétés en groupes (ce qui revient à demander $f_\omega(0_A) = 0_A$). Notons $\mathcal{A}$ la variété projective définie sur K obtenue par le critère de Weil. D'après [La] Thm. 2G, on peut transporter la loi de groupe de A sur $\mathcal{A}$, et grâce à la condition de cohérence, cette loi est définie sur K. Ainsi, $\mathcal{A}$ est une variété en groupes projective lisse sur K, donc une variété abélienne sur K.

Remarque : C'est un cas particulier de la "théorie des L/K-formes", voir [Se 3].

Lemme 2 :
Soit A/L une variété abélienne ; soit $l \in \mathcal{P}$.
Supposons que l'action naturelle de G_L sur $T_l(A)$ s'étend en une action linéaire et continue de G_K ; soient $f_{\omega,l}$, $\omega \in G_{L/K}$, les $\mathbb{Z}_l[G_L]$-isomorphismes du lemme 1. Supposons de plus qu'il existe un système cohérent d'isomorphismes $\{f_\omega : A \to A^\omega, \omega \in G_{L/K}\}$, tel que $T_l(f_\omega) = f_{\omega,l}$ pour tout $\omega \in G_{L/K}$. Soit $(\mathcal{A}, \psi)$ le couple obtenu par le critère de Weil, où $\mathcal{A}$ est une variété abélienne sur K et $\psi : \mathcal{A} \times_K L \to A$ un L-isomorphisme vérifiant $f_\omega = \psi^\omega \circ \psi^{-1}$ pour tout $\omega \in G_{L/K}$.
Alors ψ induit un isomorphisme G_K-équivariant ψ_l : $\underbrace{T_l(\mathcal{A})}_{\text{action naturelle}} \xrightarrow{\sim} \underbrace{T_l(A)}_{\text{action étendue}}$.

Preuve :
Soit $x \in T_l(\mathcal{A})$, et soit $g \in G_K$; on veut montrer que $g^{-1} \cdot \psi_l(gx) = \psi_l(x)$. Comme ψ est défini sur L, l'isomorphisme $\mathbb{Z}_l$-linéaire ψ_l est G_L-équivariant, et donc l'expression $g^{-1} \cdot \psi_l(gx)$ ne dépend que de g mod $G_L = \omega \in G_{L/K}$; notons $g = \widehat{\omega}$.
Par ailleurs, on a $\psi = f_\omega^{-1} \circ \psi^\omega$, et comme on a supposé $T_l(f_\omega) = f_{\omega,l}$, on obtient, en passant aux modules de Tate : $\psi_l = f_{\omega,l}^{-1} \circ (\psi^\omega)_l$. Reprenons les notations du lemme 1 : $\alpha_{\widehat{\omega}}$ est la bijection de $T_l(A)$ dans $T_l(A^\omega)$ déduite de $A(\overline{K}) \to A^\omega(\overline{K})$, $\eta \mapsto \widehat{\omega} \circ \eta$, et l'on a $f_{\omega,l}(x) = \alpha_{\widehat{\omega}}(\widehat{\omega}^{-1} \cdot x)$, et $f_{\omega,l}^{-1}(y) = \widehat{\omega} \cdot (\alpha_{\widehat{\omega}}^{-1}(y))$, pour $x \in T_l(A)$, $y \in T_l(A^\omega)$; notons $\beta_{\widehat{\omega}}$ la bijection de $T_l(\mathcal{A})$ dans $T_l(\mathcal{A}^\omega) = T_l(\mathcal{A})$ déduite de $\mathcal{A}(\overline{K}) \to \mathcal{A}(\overline{K})$, $\eta \mapsto \widehat{\omega} \circ \eta$ (c'est l'action naturelle de G_K sur $\mathcal{A}(\overline{K})$: $\mathcal{A}$ est une variété abélienne sur K). Alors on a : $(\psi^\omega)_l = \alpha_{\widehat{\omega}} \circ \psi_l \circ \beta_{\widehat{\omega}^{-1}}$. Finalement, on obtient : $g^{-1} \cdot \psi_l(gx) = \widehat{\omega}^{-1} \cdot f_{\omega,l}^{-1}((\psi^\omega)_l(\widehat{\omega}x)) = \widehat{\omega}^{-1} \cdot \widehat{\omega} \cdot \alpha_{\widehat{\omega}}^{-1}((\psi^\omega)_l(\widehat{\omega}x)) = \alpha_{\widehat{\omega}}^{-1} \circ \alpha_{\widehat{\omega}} \circ \psi_l \circ \beta_{\widehat{\omega}^{-1}}(\widehat{\omega}x) = \psi_l(\widehat{\omega}^{-1}\widehat{\omega}x) = \psi_l(x)$. □

2.1.3. Actions prolongées et systèmes cohérents :

Soit $\mathcal{C}$ la catégorie des schémas finis étales sur $\mathrm{Spec}(L)$. Alors on sait définir, pour tout $\omega \in G_{L/K}$ et pour tout objet $X = \mathrm{Spec}(B)$ de $\mathcal{C}$, un objet X^ω de $\mathcal{C}$, donné par $X^\omega = \mathrm{Spec}(B \otimes_{L \nearrow \omega^{-1}} L)$. De plus, l'association $F_\omega : X \mapsto X^\omega$ est fonctorielle, et l'on a $F_{\omega\tau} = F_\omega \circ F_\tau$ pour $\omega, \tau \in G_{L/K}$, et $F_1 = \mathrm{Id}_{\mathcal{C}}$: le groupe $G_{L/K}$ agit sur la catégorie $\mathcal{C}$. Il en est évidemment de même pour la catégorie des schémas finis étales sur $\mathrm{Spec}(O_L)$.
Pour toute catégorie $\mathcal{C}$ sur laquelle $G_{L/K}$ agit (au sens précédent), on dira qu'un système d'isomorphismes $\{\gamma_\omega : X \to X^\omega, \omega \in G_{L/K}\}$, où $X \in \mathrm{Ob}(\mathcal{C})$, est *cohérent* si l'on a $\gamma_{\omega\tau} = (\gamma_\tau)^\omega \circ \gamma_\omega$ pour tous $\omega, \tau \in G_{L/K}$.

Soit $\mathcal{T}$ la catégorie des ensembles finis munis d'une action de G_L. On aimerait pouvoir définir une action de $G_{L/K}$ sur la catégorie $\mathcal{T}$, comme ci-dessus.
Remarque : Soit T un objet de $\mathcal{T}$; notons $\rho : G_L \to \mathrm{Aut}(T)$. Soit $\omega \in G_{L/K}$. Si $\widehat{\omega}$ est un relèvement de ω dans G_K, alors on peut définir un objet $T^{\widehat{\omega}}$ de $\mathcal{T}$ en disant que c'est T (en tant qu'ensemble) muni de l'action $\rho^{\widehat{\omega}} : G_L \to \mathrm{Aut}(T)$ donnée par $\rho^{\widehat{\omega}}(g) = \rho(\widehat{\omega}^{-1} g \widehat{\omega})$ pour tout $g \in G_L$ (rappelons que G_L est invariant dans G_K), mais cet objet dépend du relèvement $\widehat{\omega}$ choisi.

Le choix d'une clôture algébrique $\overline{K}$ de K définit un foncteur contravariant Φ de $\mathcal{C}$ dans $\mathcal{T}$ par $\Phi : X \mapsto X(\overline{K}) = \mathrm{Hom}_{L-alg}(B, \overline{K})$, où $X = \mathrm{Spec}(B)$; de plus, le foncteur $\Psi : T \mapsto \mathrm{Spec}(\,(\mathrm{Fcts}(T, \overline{K}))^{G_L})$ de $\mathcal{T}$ dans $\mathcal{C}$ est un quasi-inverse de Φ. Alors, pour tout $\omega \in G_{L/K}$ et

pour tout $T \in \mathrm{Ob}(\mathcal{T})$, on pose :

$$T^\omega = \Phi(\Psi(T)^\omega) = \mathrm{Hom}_{L-alg}\Big((\mathrm{Fcts}(T,\overline{K}))^{G_L} \otimes_{L^{\nearrow \omega^{-1}}} L\,,\,\overline{K}\Big)\ .$$

L'objet T^ω est bien défini, et l'on obtient ainsi une action de $G_{L/K}$ sur la catégorie $\mathcal{T}$ par "transport de structure".
Remarque : Le choix d'un relèvement $\widehat{\omega}$ de ω dans G_K détermine un unique isomorphisme dans $\mathcal{T}$ de $T^{\widehat{\omega}}$ dans T^ω.
Supposons que l'action de G_L sur T s'étend en une action de G_K. Alors une construction tout-à-fait similaire à celle de **2.1.1.** montre que cette action étendue induit des isomorphismes $f_\omega : T \to T^\omega$, $\omega \in G_{L/K}$, et l'on vérifie que le système $\{f_\omega\,,\,\omega \in G_{L/K}\}$ est cohérent (c'est purement formel, voir plus loin).

Tout ceci reste bien sûr valable si l'on remplace $\mathcal{C}$ par $\mathcal{C}_0$, la catégorie des schémas en groupes commutatifs finis et étales sur $\mathrm{Spec}(L)$, et $\mathcal{T}$ par $\mathcal{T}_0$, la catégorie des groupes abéliens finis munis d'une action de G_L. Par passage à la limite, on définit T^ω, $\omega \in G_{L/K}$, où T est un module de Tate ; si $T = T_l(A)$ pour $l \in \mathcal{P}$ et A/L une variété abélienne, alors on a

$$(T_l(A))^\omega = T_l(A^\omega) \qquad , \qquad \forall\, \omega \in G_{L/K}\ .$$

On a ainsi une notion de système cohérent de $\mathbb{Z}_l[G_L]$-modules. Supposons que l'action de G_L sur $T_l(A)$ se prolonge en une action de G_K ; alors les isomorphismes du lemme 1 $\{f_{\omega,l} : T_l(A) \to T_l(A^\omega)\,,\,\omega \in G_{L/K}\}$ forment un système cohérent de $\mathbb{Z}_l[G_L]$-modules.
Vérifions-le dans ce cas. Soient $\omega, \tau \in G_{L/K}$ et $\widehat{\omega}, \widehat{\tau}$ des relèvements dans G_K. On note $\alpha_{\widehat{\omega}} : T_l(A) \to T_l(A^\omega)$ la bijection déduite de $\eta \mapsto \widehat{\omega} \circ \eta$ de $A(\overline{K})$ dans $A^\omega(\overline{K})$, et $\beta_{\widehat{\omega}} : T_l(A^\tau) \to T_l((A^\tau)^\omega) = T_l(A^{\omega\tau})$ celle déduite de $\eta \mapsto \widehat{\omega} \circ \eta$ de $A^\tau(\overline{K})$ dans $A^{\omega\tau}(\overline{K})$; avec des notations évidentes, on a $\beta_{\widehat{\omega}} \circ \alpha_{\widehat{\tau}} = \alpha_{\widehat{\omega}\widehat{\tau}}$. Le $\mathbb{Z}_l[G_L]$-isomorphisme $(f_{\tau,l})^\omega : (T_l(A))^\omega = T_l(A^\omega) \to (T_l(A^\tau))^\omega = T_l(A^{\omega\tau})$ est donné par $(f_{\tau,l})^\omega = \beta_{\widehat{\omega}} \circ f_{\tau,l} \circ \alpha_{\widehat{\omega}}^{-1}$. Alors, pour tout $x \in T_l(A)$, on a : $((f_{\tau,l})^\omega \circ f_{\omega,l})(x) = (\beta_{\widehat{\omega}} \circ f_{\tau,l} \circ \alpha_{\widehat{\omega}}^{-1})(\alpha_{\widehat{\omega}}(\widehat{\omega}^{-1} \cdot x)) = \beta_{\widehat{\omega}} \circ \alpha_{\widehat{\tau}}(\widehat{\tau}^{-1}\widehat{\omega}^{-1} \cdot x) = \alpha_{\widehat{\omega}\widehat{\tau}}((\widehat{\omega}\widehat{\tau})^{-1} \cdot x) = f_{\omega\tau,l}(x)$.

Soient K_1, K_2 deux corps tels que $K \subset K_i \subset L$, $i = 1,2$, et $K = K_1 \cap K_2$, $L = K_1K_2$. Posons $G_{L/K_i} = \mathrm{Gal}(L/K_i)$, $G_{K_i} = \mathrm{Gal}(\overline{K}/K_i)$, pour $i = 1,2$. Alors $G_{L/K} = G_{L/K_1}G_{L/K_2}$ et $G_{L/K_1} \cap G_{L/K_2} = 1$. Supposons que G_{L/K_1} est invariant dans $G_{L/K}$, i.e. que l'extension K_1/K est galoisienne (donc $G_{L/K}$ est un produit semi-direct de G_{L/K_2} par G_{L/K_1}) ; alors tout élément g de $G_{L/K}$ s'écrit de façon unique $g = g_1g_2$ avec $g_i \in G_{L/K_i}$, $i = 1,2$.

Proposition 1 :
Soit $l \in \mathcal{P}$. Soit A une variété abélienne sur L, et soient K_1, K_2 comme ci-dessus.
Supposons A définie sur K_1 et sur K_2, ce qui permet de prolonger l'action de G_L sur $T_l(A)$ en une action de G_{K_1} et une de G_{K_2}. Si l'action de G_L se prolonge sur $T_l(A)$ en une action de G_K qui coïncide avec les actions prolongées de G_{K_1} et G_{K_2}, alors A est définie sur K.

Preuve :
Comme A est définie sur K_i, $i = 1,2$, on dispose de deux systèmes cohérents d'isomorphismes $\{f_{\omega_1}\,,\,\omega_1 \in G_{L/K_1}\}$ et $\{f_{\omega_2}\,,\,\omega_2 \in G_{L/K_2}\}$. Il s'agit de montrer qu'il existe un système cohérent

d'isomorphismes $\{f_\omega : A \longrightarrow A^\omega, \omega \in G_{L/K}\}$. Tout élément ω de $G_{L/K}$ s'écrivant de manière unique $\omega = \omega_1\omega_2$, $\omega_i \in G_{L/K_i}$, $i = 1, 2$, on pose :

$$f_\omega = f_{\omega_1\omega_2} = (f_{\omega_2})^{\omega_1} \circ f_{\omega_1} .$$

Par hypothèse, l'action s'étend sur $T_l(A)$ à G_K, de sorte qu'elle coïncide avec l'action de G_{K_1} et de G_{K_2}, et les considérations précédentes montrent que le système de $\mathbb{Z}_l[G_L]$-isomorphismes $\{T_l(f_\omega) : T_l(A) \longrightarrow T_l(A^\omega) , \omega \in G_{L/K}\}$ est cohérent. Alors l'injection canonique

$$\mathrm{Hom}_L(A, B) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_l[G_L]}(T_l(A), T_l(B))$$

pour deux variétés abéliennes A et B sur L permet d'obtenir la cohérence du système $\{f_\omega , \omega \in G_{L/K}\}$ à partir de celle de $\{T_l(f_\omega) : T_l(A) \longrightarrow T_l(A^\omega) , \omega \in G_{L/K}\}$. □

Cette proposition nous permettra de traiter des situations où l'extension L/K est totalement modérérement ramifiée, mais pas nécessairement galoisienne.

2.1.4. Le théorème de prolongement :

Soit A un schéma abéloïde sur O_L, c'est-à-dire un schéma formel p-adique en groupes sur O_L tel que, pour tout $n \in \mathbb{N}$, $A \times_{O_L} O_L/p^nO_L$ est un schéma abélien sur O_L/p^nO_L. Rappelons le théorème de Serre-Tate (voir [Ka]) : l'association $A \longmapsto (A(p), \widetilde{A}, \mathrm{Id}_{\widetilde{A}(p)})$, où $A(p)$ est le groupe p-divisible sur O_L associé, $\widetilde{A} = A \times_{O_L} k_L$, $\widetilde{A}(p) = A(p) \times_{O_L} k_L = \widetilde{A(p)}$, établit une équivalence de catégories entre la catégorie des schémas abéloïdes sur O_L et la catégorie dont les objets sont les triplets $(\Gamma, \widetilde{B}, \nu)$, où Γ est un groupe p-divisible sur O_L, $\widetilde{B}$ est une variété abélienne sur k_L et ν est un isomorphisme de $\Gamma \times_{O_L} k_L = \widetilde{\Gamma}$ sur $\widetilde{B}(p)$, le groupe p-divisible associé à $\widetilde{B}$. Un morphisme $(\Gamma, \widetilde{B}, \nu) \to (\Gamma', \widetilde{B}', \nu')$ est un couple $(\psi, \tilde{f})$, où $\psi : \Gamma \to \Gamma'$ est un morphisme de groupes p-divisibles sur O_L et $\tilde{f} : \widetilde{B} \to \widetilde{B}'$ est un morphisme de variétés abéliennes sur k_L, tels que, avec des notations évidentes, $\nu' \circ \widetilde{\psi} = \tilde{f}(p) \circ \nu$.

Remarque : un schéma abéloïde A sur O_L provient d'un schéma abélien s'il est algébrisable, i.e. si et seulement si on peut le munir d'une polarisation. Pour obtenir une équivalence entre la catégorie des schémas abéliens polarisés sur O_L et une catégorie convenable, il faut considérer la catégorie formée des quadruplets $(\Gamma, \widetilde{B}, \nu, \gamma)$, où le triplet $(\Gamma, \widetilde{B}, \nu)$ est comme ci-dessus, et γ est une polarisation sur Γ qui relève une polarisation sur $\widetilde{B}$ (i.e. $\gamma : \Gamma \to \Gamma^*$ est une isogénie de groupes p-divisibles sur O_L, où Γ^* est le dual de Cartier de Γ, qui relève l'isogénie $\widetilde{B} \to \widetilde{B}^*$ associée à la polarisation sur $\widetilde{B}^*$, où $\widetilde{B}^*$ est la variété duale de $\widetilde{B}$). Rappelons que tout schéma abéloïde de dimension relative 1 est algébrisable.

Soit maintenant A un schéma abélien sur O_L. On note $A_L = A \times_{O_L} L$ la variété abélienne sur L déduite de A, et $\widehat{A}$ le schéma abéloïde sur O_L qui est le complété formel de A (plus précisément, si $u : A \to \mathrm{Spec}(O_L)$ est le morphisme structural, $\widehat{A}$ est le complété de A le long de la partie fermée $u^{-1}(V(\pi_L O_L))$, où π_L est une uniformisante de O_L, voir [EGA III] § 5). Le critère de Weil nous dit que A_L est définie sur K si et seulement si il existe un système cohérent de L-isomorphismes de variétés abéliennes $\{f_{\omega,L} : A_L \longrightarrow A_L^\omega , \omega \in G_{L/K}\}$; par l'unicité du modèle de Néron, cela équivaut à la donnée d'un système cohérent de O_L-isomorphismes de schémas abéliens $\{f_\omega : A \longrightarrow A^\omega , \omega \in G_{L/K}\}$. Puis la pleine fidélité

du foncteur "complétion formelle" ([EGA III], Thm. 5.4.1.) montre que cela équivaut à la donnée d'un système cohérent $\{\widehat{f}_\omega : \widehat{A} \longrightarrow \widehat{A}^\omega, \omega \in G_{L/K}\}$ de O_L-isomorphismes de schémas abéloïdes. Enfin, la pleine fidélité du foncteur de Serre-Tate montre que cela équivaut aussi aux données suivantes :

(1) un ensemble d'isomorphismes $\{f_\omega(p) : A(p) \longrightarrow A^\omega(p), \omega \in G_{L/K}\}$ de groupes p-divisibles sur O_L tels que

$$f_{\omega\tau}(p) = \Big(f_\tau(p)\Big)^\omega \circ f_\omega(p) \qquad \forall \omega, \tau \in G_{L/K} \qquad \text{(cohérence)}$$

(2) un ensemble d'isomorphismes $\{\tilde{f}_\omega : \widetilde{A} \longrightarrow \widetilde{A^\omega}, \omega \in G_{L/K}\}$ de variétés abéliennes sur k_L tels que

$$\tilde{f}_\omega(p) = \widetilde{f_\omega(p)} \qquad \forall \omega \in G_{L/K} \qquad \text{(recollement)} \qquad .$$

En effet, la condition de cohérence sur les $\tilde{f}_\omega$: $\forall \omega, \tau \in G_{L/K}$, $\tilde{f}_{\omega\tau} = (\tilde{f}_\tau)^\omega \circ \tilde{f}_\omega$, est vérifiée grâce aux injections canoniques

$$\mathrm{Hom}_{k_L}(\widetilde{A}, \widetilde{A^\omega}) \hookrightarrow \mathrm{Hom}_{k_L}(\widetilde{A}(p), \widetilde{A^\omega}(p)) = \mathrm{Hom}_{k_L}(\widetilde{A(p)}, \widetilde{A^\omega(p)}) \ .$$

Supposons que l'action de G_L sur $T_p(A)$ se prolonge en une action de G_K. Cette action prolongée induit un système cohérent d'isomorphismes $\{f_{\omega,p} : T_p(A) \longrightarrow T_p(A^\omega), \omega \in G_{L/K}\}$ de $\mathbb{Z}_p[G_L]$-modules. Le théorème de pleine fidélité de Tate permet de construire un ensemble cohérent $\{f_{\omega,p}(p) = f_\omega(p) : A(p) \longrightarrow A^\omega(p), \omega \in G_{L/K}\}$ d'isomorphismes de groupes p-divisibles sur O_L (condition (1)). Pour que A puisse être définie sur K, il faut aussi pouvoir disposer d'un ensemble $\{\tilde{f}_\omega : \widetilde{A} \longrightarrow \widetilde{A^\omega}, \omega \in G_{L/K}\}$ d'isomorphismes sur les fibres spéciales qui vérifient la condition de recollement avec les $f_\omega(p)$ (condition (2)) ; soit on se le donne, comme dans le théorème suivant, soit il faut le construire.
Pour le construire sans se le donner, nous allons avoir besoin (dans la plupart des cas) d'hypothèses supplémentaires : il nous faudra disposer d'une action de G_K étendue à *tous* les $T_l(A)$, $l \in \mathcal{P}$. Cette famille d'actions devra en outre vérifier des conditions de compatibilité, ce qui est l'objet du chapitre suivant. Mais tout d'abord, définissons les morphismes r_l, $l \in \mathcal{P}$, qui nous permettront de construire les isomorphismes $\tilde{f}_\omega$.

Supposons que l'action de G_L se prolonge en une action de G_K sur $T_l(A)$, $l \in \mathcal{P}$. Comme A a bonne réduction, pour $l \neq p$ on a $T_l(A) \simeq T_l(\widetilde{A})$, et l'action prolongée sur $T_l(A)$ induit un système cohérent $\{\tilde{f}_{\omega,l} : T_l(\widetilde{A}) \longrightarrow T_l(\widetilde{A^\omega}), \omega \in G_{L/K}\}$ d'isomorphismes de $\mathbb{Z}_l[G_L]$-modules. D'autre part, pour $l = p$, l'action prolongée sur $T_p(A)$ induit un système cohérent $\{\widetilde{f_\omega(p)} = \tilde{\gamma}_\omega : \widetilde{A(p)} = \widetilde{A}(p) \longrightarrow \widetilde{A}^\omega(p), \omega \in G_{L/K}\}$ d'isomorphismes de groupes p-divisibles sur k_L. Rappelons que pour $\tau \in I_{L/K}$, on a $\widetilde{A^\tau} = \widetilde{A}$. Alors la condition de cohérence signifie, pour $l \neq p$, que l'association $\tau \mapsto \tilde{f}_{\tau,l}$ est un morphisme de $I_{L/K}$ dans $(\mathrm{End}_{\mathbb{Z}_l[G_L]}(T_l(\widetilde{A})))^\times$, et pour $l = p$, que l'association $\tau \mapsto \tilde{\gamma}_\tau$ est un morphisme de $I_{L/K}$ dans $(\mathrm{End}_{p-div}(\widetilde{A}(p)))^\times$. En utilisant les isomorphismes canoniques (dûs à J. Tate, cf. [Ta] pour le premier) :

$$\mathrm{End}_{\mathbb{Z}_l[G_L]}(T_l(\widetilde{A})) \simeq \mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_{k_L}(\widetilde{A}) \quad \text{pour } l \neq p, \text{ et} \quad \mathrm{End}_{p-div}(\widetilde{A}(p)) \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_{k_L}(\widetilde{A}),$$

on définit des morphismes $r_l : I_{L/K} \longrightarrow \Big(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_{k_L}(\widetilde{A})\Big)^\times$ pour tout $l \in \mathcal{P}$.

Supposons l'extension L/K galoisienne totalement ramifiée, i.e. $G_{L/K} = I_{L/K}$ et $k_L = k$.

Théorème 1 :
Soit L/K une extension finie galoisienne totalement ramifiée de groupe de Galois $G_{L/K}$, et soit A/L une variété abélienne ayant bonne réduction sur L ; soit $\widetilde{A}$ sa fibre spéciale.
On suppose que l'action de G_L sur $T_p(A)$ s'étend en une action de G_K ; soit $r_p : G_{L/K} \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A}))^\times$ le morphisme induit par cette action prolongée construit plus haut. Alors A est définie sur K si et seulement si r_p provient par extension des scalaires d'un morphisme $r : G_{L/K} \to \mathrm{Aut}_k(\widetilde{A})$. Il existe alors une variété abélienne $\mathcal{A}$ sur K et un L-isomorphisme $\psi : \mathcal{A} \times_K L \xrightarrow{\sim} A$ qui induit un isomorphisme de $\mathbb{Z}_p[G_K]$-modules :

$$T_p(\psi) : \quad \underbrace{T_p(\mathcal{A})}_{\text{action naturelle}} \quad \simeq \quad \underbrace{T_p(A)}_{\text{action étendue}} \quad ,$$

et un tel couple $(\mathcal{A}, \psi)$ est unique à K-isomorphisme près.

Preuve :
C'est une conséquence de tout ce qui précède : la partie (1) du critère de Weil donné ci-dessus est satisfaite grâce au fait que l'action de G_L sur $T_p(A)$ s'étend en une action de G_K, et la partie (2) du critère est vérifiée en posant $f_\tau = r(\tau) \in \mathrm{Aut}_k(\widetilde{A})$ pour tout $\tau \in G_{L/K}$: ce sont des isomorphismes qui vérifient, par construction, la condition recollement. La dernière assertion du théorème provient du lemme 2 de **2.1.2.**. □

Soient $W(k)$ l'anneau des vecteurs de Witt à coefficients dans k et $L_0 = \mathrm{Frac}W(k)$. Notons g la dimension de A. Soit $\mathbf{M}(\widetilde{A}(p))$ le module de Dieudonné sur k de la fibre spéciale du groupe p-divisible de A (voir [Fo 4]) ; alors l'objet $L_0 \otimes_{W(k)} \mathbf{M}(\widetilde{A}(p))$ est un L_0-espace vectoriel de dimension $2g$, muni d'une bijection σ-semi-linéaire φ (σ est le Frobenius absolu agissant sur k par $x \mapsto x^p$). Le foncteur $\mathbf{M}$ étant, en particulier, pleinement fidèle, on obtient des isomorphismes

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A}) \simeq \mathrm{End}_{p-div}(\widetilde{A}(p)) \simeq \mathrm{End}_{W(k)[\varphi]}(\mathbf{M}(\widetilde{A}(p))),$$

et aussi

$$\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A}) \simeq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{End}_{p-div}(\widetilde{A}(p)) \simeq \mathrm{End}_{L_0[\varphi]}(L_0 \otimes_{W(k)} \mathbf{M}(\widetilde{A}(p))).$$

D'autre part, l'objet $D = \mathbf{D}^*_{\mathbf{cris,L}}(V_p(A))$ est dans $\mathbf{MF_L}(\varphi)$: c'est un L_0-espace vectoriel de dimension $2g$, muni d'une application σ-semi-linéaire bijective $\varphi : D \longrightarrow D$, et d'une filtration décroissante, exhaustive et séparée sur $D_L = D \otimes_{L_0} L$ par des sous-L-espaces vectoriels $\mathrm{Fil}^i D_L$, $i \in \mathbb{Z}$ (voir [Fo 2]). Rappelons que l'on a un isomorphisme canonique d'objets de $\mathbf{MF_L}(\varphi)$:

$$L_0 \otimes_{W(k)} \mathbf{M}_{O_L}(A(p)) \simeq \mathbf{D}^*_{\mathbf{cris,L}}(V_p(A))$$

qui fait le lien entre le Module de Dieudonné filtré sur O_L du groupe p-divisible de A et la théorie cristalline ([Fo 5]). L'objet $\mathbf{M}_{O_L}(A(p))$ représente en fait un couple formé de l'objet $\mathbf{M}(\widetilde{A}(p))$ avec en plus une filtration ; si l'on oublie celle-ci, on obtient un isomorphisme canonique $L_0 \otimes_{W(k)} \mathbf{M}(\widetilde{A}(p)) \simeq \mathbf{D}^*_{\mathbf{cris,L}}(V_p(A))$ de φ-modules sur L.

Si l'action de G_L sur $T_p(A)$ se prolonge en une action de G_K, alors bien sûr elle se prolonge sur $V_p(A)$. Or, étendre l'action de G_L à G_K sur $V_p(A)$ revient à munir D d'une structure d'objet de $\mathbf{MF_{L/K}}(\varphi)$. Cela veut dire que l'on fait agir $L_0 = K_0$-linéairement $I_{L/K}$ sur D, de sorte que cette action commute avec φ et stabilise, après extension des scalaires, la filtration sur D_L (l'action de $I_{L/K}$ sur D_L est semi-linéaire). Si l'on oublie la filtration, on obtient ainsi un morphisme $\nu : I_{L/K} \to \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(A)))$. Alors, via les isomorphismes canoniques cités plus haut, on a un diagramme commutatif :

$$\begin{array}{ccccc} & & \overset{r_p}{\to} & & \\ G_{L/K} = I_{L/K} & & & \left(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A})\right)^\times \subset \left(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A})\right)^\times & \\ \nu \quad \downarrow & & & \downarrow \wr & can \\ \mathrm{Aut}_{L_0[\varphi]}\left(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(A))\right) & \underset{can}{\overset{\sim}{\to}} & & \mathrm{Aut}_{L_0[\varphi]}\left(L_0 \otimes_{W(k)} \mathbf{M}(\widetilde{A}(p))\right) & \end{array}$$

2.2. Actions prolongées compatibles :

Rappelons que le corps résiduel de L est noté k_L et que celui de K est noté $k = \mathbb{F}_q$ avec $q = p^m$. Le groupe de Weil relatif à K (resp. L) est W_K (resp. W_L), et l'on a $W_K/W_L = G_{L/K}$. On a une suite exacte :

$$1 \longrightarrow I_K \longrightarrow W_K \xrightarrow{v} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 1 \ ,$$

où l'image par v d'un relèvement du Frobenius arithmétique relatif à k est m.

2.2.1. Systèmes de représentations compatibles :

Le groupe de Weil-Deligne $'W_K$ est le schéma en groupe sur $\mathbb{Q}$ qui est le produit semi-direct de W_K par le groupe additif $\mathbb{G}_a$ sur lequel W_K opère par $wxw^{-1} = p^{v(w)}x$.
Soit E un corps de caractéristique 0. Notons $\mathbf{Rep}_E('W_K)$ la catégorie des représentations E-linéaires et continues de $'W_K$. Soit Δ un objet de $\mathbf{Rep}_E('W_K)$; un tel objet peut être considéré comme un triplet (Δ, ρ_0, N), où :
- Δ est un E-espace vectoriel de dimension finie,
- $\rho_0 : W_K \to \mathrm{Aut}_E(\Delta)$ est un morphisme dont le noyau contient un sous-groupe ouvert de I_K,
- $N \in \mathrm{End}_E(\Delta)$ et vérifie : $\forall\, w \in W_K,\ \rho_0(w)N = p^{v(w)}N\rho_0(w)$.

On dit que Δ est *F-semi-simple* si la représentation E-linéaire ρ_0 de W_K est semi-simple. Lorsque k est fini (ce qui est le cas dans notre situation), cela équivaut à demander à ce que l'automorphisme E-linéaire $\rho_0(w_0)$ soit semi-simple, pour un $w_0 \in W_K$, $w_0 \notin I_K$ (ce fait est indépendant du choix de w_0).

Soit L une extension galoisienne finie de K, de corps résiduel k_L, avec $I_L = I(\overline{K}/L)$ et $L_0 = \mathrm{Frac}W(k_L)$. Pour tout $l \in \mathcal{P}$, notons $\mathbf{Rep}_{\mathbb{Q}_l,pst(L)}(G_K)$ la catégorie des représentations $\mathbb{Q}_l$-linéaires de G_K qui deviennent semi-stables sur L ; pour $l \neq p$, cela veut dire que l'action de I_L est unipotente. La catégorie $\mathbf{Rep}_{\mathbb{Q}_l,pst}(G_K)$ des représentations $\mathbb{Q}_l$-linéaires de G_K potentiellement semi-stables s'identifie alors à la limite inductive des $\mathbf{Rep}_{\mathbb{Q}_l,pst(L)}(G_K)$, où L parcourt l'ensemble des extensions finies galoisiennes de K contenues dans $\overline{K}$ (rappelons que pour $l \neq p$, toutes les représentations l-adiques de G_K sont potentiellement semi-stables). Choisissons un $q_0 \in K^\times$, $q_0 \notin O_K^\times$, et pour $l \neq p$, un $t_l \in \mathbb{Q}_l(1)$ non nul ; posons $\mathbb{Q}'_l = \mathbb{Q}_l$ si $l \neq p$ et $\mathbb{Q}'_p = L_0$. Dans [Fo 3], J.-M. Fontaine construit pour chaque $l \in \mathcal{P}$ un foncteur covariant $\mathbf{W\widehat{D}_{pst,l,K}}$ de $\mathbf{Rep}_{\mathbb{Q}_l,pst(L)}(G_K)$ dans $\mathbf{Rep}_{\mathbb{Q}'_l}('W_K)$. Nous utilisons ici la version contravariante de ce foncteur, que l'on note $\mathbf{W\widehat{D}^*_{pst,l,K}}$; cela revient à appliquer $\mathbf{W\widehat{D}_{pst,l,K}}$ à la représentation duale, ou bien, de façon équivalente, à prendre le dual après avoir appliqué le foncteur $\mathbf{W\widehat{D}_{pst,l,K}}$. Pour $l \neq p$, lorsque L varie, le foncteur $\mathbf{W\widehat{D}^*_{pst,l,K}}$ établit une anti-équivalence de catégories entre $\mathbf{Rep}_{\mathbb{Q}_l}(G_K) = \mathbf{Rep}_{\mathbb{Q}_l,pst}(G_K)$ et $\mathbf{Rep}^\circ_{\mathbb{Q}_l}('W_K)$, cette dernière désignant la sous-catégorie tannakienne de $\mathbf{Rep}_{\mathbb{Q}_l}('W_K)$ constituée des objets sur lesquels les racines du polynôme caractéristique du Frobenius géométrique sont des unités l-adiques. Pour $l = p$, soit V un objet de $\mathbf{Rep}_{\mathbb{Q}_p,pst(L)}(G_K)$, i.e. la représentation $\mathbb{Q}_p$-linéaire de G_K sur V devient semi-stable sur L (une telle extension existe toujours si V provient d'une variété abélienne) ; alors il faut rajouter une filtration sur $\mathbf{W\widehat{D}^*_{pst,p,K}}(V)$ pour pouvoir retrouver V (cf. [Fo 3], 2.3.5.). Plus précisément, soit $D = \mathbf{D^*_{st,L/K}}(V) = \mathrm{Hom}_{\mathbb{Q}_p[G_L]}(V, B_{st})$, c'est un objet de $\mathbf{MF}^{ad}_{L/K}(\varphi, N)$ (voir [Fo 2]). Soit $D^{(0)}$ l'objet obtenu en oubliant la filtration, c'est alors un objet de $\mathbf{Mod}(\varphi, N, G_{L/K})$, c'est-à-dire un L_0-espace vectoriel de dimension $\dim_{\mathbb{Q}_p}(V)$, muni d'un Frobenius σ-semi-linéaire $\varphi : D^{(0)} \to D^{(0)}$, d'un opérateur L_0-linéaire $N : D^{(0)} \to D^{(0)}$, ainsi que d'une action semi-linéaire de $G_{L/K}$, le tout vérifiant les relations $N\varphi = p\varphi N$ et $g\varphi = \varphi g$, $gN = Ng$ pour tout $g \in G_{L/K}$. Alors $D^{(0)}$ devient un objet de $\mathbf{Rep}_{L_0}('W_K)$ en posant $\mathbf{W}_p(D^{(0)}) = (\Delta_p, \rho_0, N)$, où $\Delta_p = D^{(0)}$ en tant que L_0-espace vectoriel, l'opérateur N est inchangé, et $\rho_0 : W_K \longrightarrow \mathrm{Aut}_{L_0}(\Delta_p)$ est donnée par : $\rho_0(w) = (w \bmod W_L) \cdot \varphi^{-v(w)}$ pour tout $w \in W_K$.

Soit $\mathcal{A}$ une variété abélienne sur K de dimension g qui devient semi-stable sur L ; alors les $\mathbf{W\widehat{D}^*_{pst,l,K}}(V_l(\mathcal{A}))$ sont des $\mathbb{Q}'_l$-espaces vectoriels de dimension $2g$ munis d'une action $\mathbb{Q}'_l$-linéaire de $'W_K$. De plus (loc.cit. 2.4.), on sait que chacune des $\mathbf{W\widehat{D}^*_{pst,l,K}}(V_l(\mathcal{A}))$ est *F-semi-simple, définie sur* $\mathbb{Q}$, et que *les* $\left(\mathbf{W\widehat{D}^*_{pst,l,K}}(V_l(\mathcal{A}))\right)_{l\in\mathcal{P}}$ *forment un système compatible de représentations de* $'W_K$ (on dira aussi, pour simplifier, que les $V_l(\mathcal{A})$, $l \in \mathcal{P}$, forment un système compatible de représentations de $'W_K$, les foncteurs $\mathbf{W\widehat{D}^*_{pst,l,K}}$ étants sous-entendus). Expliquons brièvement ce que ces deux dernières notions signifient.

Soient F une extension d'un corps E de caractéristique 0, et Δ un objet de $\mathbf{Rep}_F('W_K)$. On dit que Δ *est définie sur* E si, étant donnée une E-structure D de Δ (i.e. un E-espace vectoriel D tel que $\Delta = F \otimes_E D$), et étant donné un corps algébriquement clos Ω contenant F, la représentation Ω-linéaire de $'W_K$ obtenue par extension des scalaires est isomorphe à ses conjuguées sous $\mathrm{Aut}(\Omega/E)$: si $g \in \mathrm{Aut}(\Omega/E)$, g agit sur $\Omega \otimes_F \Delta = \Omega \otimes_E D$ par $g(\omega \otimes d) = g\omega \otimes d$, $\omega \in \Omega$, $d \in D$. Cette condition est indépendante des choix de D et Ω.

Pour chaque $l \in \mathcal{P}$, on choisit des plongements de corps $\iota_l : \mathbb{Q}'_l \hookrightarrow \mathbb{C}$. En ce qui nous concerne, on prendra $E = \mathbb{Q}$, $F = \mathbb{Q}'_l$, et $\Omega = \mathbb{C}$ avec le plongement ι_l. Alors chaque

$\mathbf{W\hat{D}^*_{pst,l,K}}(V_l(\mathcal{A})) \otimes_{\mathbb{Q}_l'^{\nearrow \iota_l}} \mathbb{C}$, $l \in \mathcal{P}$, devient un objet de $\mathbf{Rep_C}('W_K)$, est définie sur $\mathbb{Q}$, et sa classe d'isomorphisme ne dépend pas du choix de ι_l.

Remarques :
1) Si Δ est une représentation F-linéaire de $'W_K$ de dimension 1, alors l'endomorphisme N est nul et Δ est déterminée par le caractère $\rho_0 : W_K \longrightarrow F^\times$. Alors Δ est définie sur E si et seulement si $\rho_0(W_K) \subset E^\times$.
2) On dit que Δ est *rationnelle sur* E s'il existe une représentation E-linéaire D de $'W_K$ telle que $\Delta \simeq F \otimes_E D$. Si Δ est rationnelle sur E, alors elle est définie sur E, mais la réciproque est en général fausse.

Enfin, *la compatibilité du système* $V_l(\mathcal{A})$, $l \in \mathcal{P}$, *de représentations de* $'W_K$ signifie que les $\mathbf{W\hat{D}^*_{pst,l,K}}(V_l(\mathcal{A})) \otimes_{\mathbb{Q}_l'^{\nearrow \iota_l}} \mathbb{C}$, $l \in \mathcal{P}$, sont définies sur $\mathbb{Q}$ et sont deux à deux isomorphes dans $\mathbf{Rep_C}('W_K)$. Pour toutes ces notions, on pourra consulter [Del] ou [Roh] qui traitent les cas $l \neq p$, et [Fo 3] pour un traitement unifié comprenant le cas $l = p$.
Soit $\mathcal{A}$ une variété abélienne sur K ayant potentiellement bonne réduction : on a $N = 0$ sur $\Delta_l = \mathbf{W\hat{D}^*_{pst,l,K}}(V_l(\mathcal{A}))$, $l \in \mathcal{P}$. Les Δ_l étant toutes F-semi-simples, la compatibilité du système Δ_l, $l \in \mathcal{P}$, équivaut à demander aux caractères $\mathrm{Tr}\rho_0 : W_K \longrightarrow \mathbb{Q}_l'$ d'être à valeurs dans $\mathbb{Q}$ et indépendants de $l \in \mathcal{P}$. Pour un énoncé similaire avec $N \neq 0$, il faut utiliser la filtration de Jacobson-Morosov, voir [Fo 3], 2.4.5.

Soit maintenant A/L une variété abélienne ayant bonne réduction sur L. Alors l'opérateur N est nul sur chaque $\mathbf{W\hat{D}^*_{pst,l,L}}(V_l(A)) \otimes_{\mathbb{Q}_l'^{\nearrow \iota_l}} \mathbb{C}$, $l \in \mathcal{P}$, et l'on a tout simplement une famille de représentations de W_L sur lesquelles l'action de I_L est triviale. Comme le corps résiduel k_L de L est fini, la compatibilité de ce système signifie que le polynôme caractéristique du Frobenius est dans $\mathbb{Q}[X]$ et indépendant de $l \in \mathcal{P}$ (pour $l = p$, il s'agit du Frobenius du module de Dieudonné de $\widetilde{A}(p)$, le groupe p-divisible de la fibre spéciale de A).

Dorénavant, A sera un schéma abélien sur O_L, et $\widetilde{A}$ sa fibre spéciale.
Supposons que l'action de G_L sur les $T_l(A)$ s'étend pour chaque $l \in \mathcal{P}$ en une action de G_K , de sorte que l'action de W_K ainsi obtenue soit compatible. Reprenons les morphismes r_l, $l \in \mathcal{P}$, définis au paragraphe précédent, et notons encore r_l le morphisme obtenu en composant avec l'inclusion

$$r_l \ : \ I_{L/K} \longrightarrow \left(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_{k_L}(\widetilde{A})\right)^\times \hookrightarrow \left(\mathbb{Q}_l \otimes_{\mathbb{Z}} \mathrm{End}_{k_L}(\widetilde{A})\right)^\times .$$

Alors la compatibilité entraîne que $\mathrm{Ker}\,(r_l)$ *est le même pour tous les* $l \in \mathcal{P}$, *que le polynôme caractéristique de* $r_l(\tau)$, $\tau \in I_{L/K}$, *est dans* $\mathbb{Q}[X]$ *et indépendant de* $l \in \mathcal{P}$ (pour $l \neq p$, voir [Se-Ta]), *et que* $d\acute{e}t(r_l(\tau)) = \pm 1$ (voir paragraphe **2.3.1.**).

2.2.2. Réduction à une action fidèle :

Soit L/K une extension finie galoisienne totalement ramifiée, i.e. $G_{L/K} = I_{L/K}$ et $k_L = k$.

Proposition 2 :
Soit L/K *une extension finie galoisienne totalement ramifiée, et soit* A *une variété abélienne sur* L, *ayant bonne réduction sur* L.

On suppose que l'action de G_L sur $T_p(A)$ s'étend en une action de G_K. Soit $H = \mathrm{Ker}\,(r_p)$, où $r_p : G_{L/K} \longrightarrow (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A}))^\times$ est le morphisme construit précédemment.
Alors A est définie sur L^H et a bonne réduction sur L^H.

Preuve :
Montrons d'abord que A est définie sur L^H. D'après le théorème 1, il suffit de montrer que la restriction du morphisme r_p à H provient par extension des scalaires d'un morphisme $r : H \to \mathrm{Aut}_k(\widetilde{A})$; comme $r_p(H) = 1$, il suffit de poser $r(\tau) = \mathrm{Id}_{\widetilde{A}}$ pour tout $\tau \in H$. Donc A est définie sur L^H.

Soit $(\mathcal{A}, \psi)$ le couple obtenu par le critère de Weil : $\mathcal{A}$ est une variété abélienne sur L^H et $\psi : \mathcal{A} \times_{L^H} L \xrightarrow{\sim} A$ est un L-isomorphisme qui induit un $\mathbb{Z}_p[G_{L^H}]$-isomorphisme $T_p(\mathcal{A}) \simeq T_p(A)$ (thm. 1). Alors les $\mathbf{W\widehat{D}^*_{pst,l,L^H}}(V_l(\mathcal{A}))$, $l \in \mathcal{P}$, forment un système compatible de représentations de $'W_{L^H}$ (en fait de W_{L^H} puisque l'on a encore $N = 0$: $\mathcal{A}$ a potentiellement bonne réduction). Donc l'image de tous les $r_l : H = I_{L/L^H} \longrightarrow (\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A}))^\times \simeq \mathrm{End}_{\mathbb{Z}_l[G_L]}(T_l(\widetilde{A}))$, $l \in \mathcal{P}$, est triviale, puisqu'elle est triviale en $l = p$ par hypothèse. Pour $l \neq p$, l'action de I_L est triviale sur $V_l(A) \simeq V_l(\mathcal{A} \times_{L^H} L)$, et par construction, $r_l(I_{L/L^H}) = 1$ implique que l'action de I_{L/L^H} sur $V_l(\mathcal{A})$ est triviale. Donc I_{L^H} agit trivialement sur $V_l(\mathcal{A})$. Le critère d'Ogg-Néron-Schafarevich nous assure qu'alors $\mathcal{A}$ a bonne réduction sur L^H. □

Remarque : La proposition 1 de **2.1.3.** montre que l'énoncé ci-dessus reste valable lorsque l'extension L/K est finie et totalement modérément ramifiée, mais pas nécessairement galoisienne ; en effet, il suffit de se placer sur la clôture galoisienne de L dans K.

Grâce à cette proposition nous pouvons nous ramener au cas où les

$$G_{L/K} = I_{L/K} \xrightarrow{r_l} \left(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A})\right)^\times \quad , \; l \in \mathcal{P} \, ,$$

sont tous injectifs, c'est-à-dire à une action fidèle de $G_{L/K} = I_{L/K}$, ce que nous ferons toujours dans la suite.

2.3. Le cas des courbes elliptiques :

2.3.1. Le déterminant :

Soit L une extension finie de $\mathbb{Q}_p$ de corps résiduel k_L, avec $L_0 = \mathrm{Frac}W(k_L)$. Soit ϕ un relèvement dans W_L du Frobenius géométrique relatif à k_L.
Soit $V = \mathbb{Q}_p(1)$ un $\mathbb{Q}_p$-espace vectoriel de dimension 1 sur lequel G_L agit par le caractère cyclotomique $\chi_{p,L} : G_L \longrightarrow \mathbb{Z}_p^\times$ donnant l'action de G_L sur les racines p^n-ièmes de l'unité, $n \geq 1$. Cette représentation de G_L est définie sur $\mathbb{Q}$. En effet, $\Delta_p = \mathbf{W\widehat{D}^*_{pst,p,L}}(V)$ est un L_0-espace vectoriel de dimension 1, sur lequel $N = 0$, et $\rho_0 : W_L \longrightarrow \mathrm{Aut}_{L_0}(\Delta_p) = L_0^\times$ est définie par $\rho_0(I_L) = 1$ et $\rho_0(\phi)$ est la multiplication par $|k_L|$.

Remarque : Pour $l \neq p$, $V_l = \mathbb{Q}_l(1)$ est un $\mathbb{Q}_l$-espace vectoriel de dimension 1 sur lequel G_L agit par le caractère cyclotomique $\chi_{l,L} : G_L \longrightarrow \mathbb{Z}_l^\times$ donnant l'action de G_L sur les

racines l^n-ièmes de l'unité, $n \geq 1$. Il est clair que les $(V_l)_{l \in \mathcal{P}} = (\mathbb{Q}_l(1))_{l \in \mathcal{P}}$ sont toutes définies sur $\mathbb{Q}$ et forment un système compatible de représentations de W_L : pour $l \neq p$, $\Delta_l = \mathbf{W\hat{D}^*_{pst,l,L}}(V_l) = \mathrm{Hom}_{\mathbb{Q}_l[I_L]}(\mathbb{Q}_l(1), \mathbb{Q}_l)$ est un $\mathbb{Q}_l$-espace vectoriel de dimension 1, sur lequel $N = 0$, et $\rho_0(I_L) = 1$, $\rho_0(\phi) = |k_L|$.

Soit L/K une extension finie galoisienne, de groupe de Galois $G_{L/K}$.
Si $\xi : G_K \longrightarrow \mathbb{Z}_p^\times$ est un caractère dont la restriction à G_L est $\chi_{p,L}$, alors on voit que $\xi = \xi_n^{-1}\chi_{p,K}$, où $\chi_{p,K}$ est le caractère cyclotomique relatif à K, et ξ_n est un caractère qui se factorise à travers G_L et s'envoie surjectivement sur un groupe de racines n-ièmes de l'unité $\mu_n(\mathbb{Z}_p^\times)$ contenu dans $\mathbb{Z}_p^\times$:

$$\xi_n : G_K \longrightarrow G_K/G_L = G_{L/K} \longrightarrow \mu_n(\mathbb{Z}_p^\times) ,$$

avec $n \mid [L : K]$, et $n \mid p-1$ si $p \geq 3$, $n = 1$ ou 2 si $p = 2$ (en effet, cette dernière est une condition nécessaire et suffisante pour que $\mathbb{Z}_p^\times$ contienne une racine primitive n-ième de l'unité). En fait, de tels caractères sont en bijection avec $\mathcal{C}_n \times (\mathbb{Z}/n\mathbb{Z})^\times$, où $\mathcal{C}_n$ est l'ensemble des extensions cycliques de degré n de K contenues dans L.

Revenons à une extension L/K finie galoisienne totalement ramifiée, de corps résiduel $k = k_L$ à $q = p^m$ éléments.

Lemme 1 :
Soit L/K finie galoisienne totalement ramifiée. Soit V un $\mathbb{Q}_p$-espace vectoriel de dimension 1 sur lequel G_L agit par le caractère cyclotomique $\chi_{p,L}$. Les seuls caractères qui étendent l'action de G_L sur V en une action de G_K dont la restriction à W_K est définie sur $\mathbb{Q}$ sont $\chi_{p,K}$ et $\xi_2\chi_{p,K}$, où ξ_2 est un caractère non trivial d'ordre 2 qui se factorise à travers G_L.

Preuve :
Soit ϕ un relèvement dans W_L du Frobenius géométrique relatif à $k = \mathbb{F}_q$. Rappelons que $\Delta_p = \mathbf{W\hat{D}^*_{pst,p,L}}(V) = L_0$ sur lequel $N = 0$ et $\rho_0 : W_L \longrightarrow L_0^\times$ est donnée par $\rho_0(I_L) = 1$ et $\rho_0(\phi) = q$. Si l'action s'étend sur V par $\xi_n^{-1}\chi_{p,K}$, où n est comme ci-dessus, notons L_n le corps fixé par $\mathrm{Ker}(\xi_n)$: c'est une extension cyclique d'ordre n de K contenue dans L. Notons I_n le groupe d'inertie absolu de L_n. Alors $\Delta'_p = \mathbf{W\hat{D}^*_{pst,p,K}}(V) = L_0 = K_0$ sur lequel $N = 0$, et $\rho_0 : W_K \longrightarrow K_0^\times$ est définie par :

$$\begin{cases} \rho_0(I_n) = 1 \\ \rho_0(\theta_n) = \zeta_n^{-1} \\ \rho_0(\phi) = q \end{cases}$$

où θ_n est un relèvement dans I_n d'un générateur de $\mathrm{Gal}(L_n/L)$ et ζ_n est une racine primitive n-ième de l'unité. Cette action prolongée est définie sur $\mathbb{Q}$ si et seulement si elle est à valeurs dans $\mathbb{Q}$ (dimension 1), ce qui n'est possible que si $n = 1$ ou 2. □

On voudrait pouvoir éliminer le cas $\xi_2\chi_{p,K}$ pour des déterminants provenant de modules de Tate $T_p(E)$ de courbes elliptiques. En fait, on y arrive à condition de considérer une action de G_K prolongée non seulement sur $T_p(E)$, mais aussi sur les $V_l(E)$, $l \neq p$.

Soit E une courbe elliptique sur L, ayant bonne réduction sur L. Supposons pour commencer que l'action de G_L sur $T_p(E)$ s'étend en une action de G_K définie sur $\mathbb{Q}$ et dont le déterminant est $\xi_2\chi_{p,K}$ (en particulier, $[L:K]$ est pair). On suppose aussi que le morphisme r_p est injectif ; on a :

$$G_{L/K} = I_{L/K} \overset{r_p}{\hookrightarrow} \left(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})\right)^{\times} \simeq \mathrm{Aut}_{L_0[\varphi]}\left(L_0 \otimes_{W(k)} \mathrm{M}(\widetilde{E}(p))\right) \hookrightarrow \mathrm{GL}_2(L_0) \xrightarrow{\text{dét}} L_0^{\times},$$

où $\mathrm{M}(\widetilde{E}(p))$ est le module de Dieudonné de la fibre spéciale du groupe p-divisible de E. Rappelons que l'objet $L_0 \otimes_{W(k)} \mathrm{M}(\widetilde{E}(p))$ est un L_0-espace vectoriel de dimension 2, muni d'une bijection σ-semi-linéaire φ (où σ est le Frobenius absolu agissant sur k par $x \mapsto x^p$).

Soit $\tau \in I_{L/K}$ tel que $\det(r_p(\tau)) = -1$. L'action étendue étant définie sur $\mathbb{Q}$, le polynôme minimal de $r_p(\tau)$ est dans $\mathbb{Q}[X]$; notons-le $\mathrm{P}_{min}(\tau)(X)$. Si d est l'ordre exact de τ dans $I_{L/K}$, alors, comme r_p est injective, $\mathrm{P}_{min}(\tau)(X)$ divise $X^d - 1 = \prod_{e|d} \Phi_e(X)$ dans $\mathbb{Q}[X]$, où les $\Phi_e(X)$ sont les polynômes cyclotomiques. On voit alors que la seule possibilité avec $\det(r_p(\tau)) = -1$ est $\mathrm{P}_{min}(\tau)(X) = (X-1)(X+1) = X^2 - 1$, et τ est d'ordre 2. En remplaçant K par $L^{<\tau>}$, on se ramène à la situation suivante : L/K est ramifée d'ordre 2, $G_{L/K} = I_{L/K} = <\tau>$, et $\mathrm{P}_{min}(\tau)(X) = X^2 - 1$.

Comme E a bonne réduction sur L, $D = \mathbf{D}^*_{\mathbf{cris,L}}(V_p(E))$ est un objet de $\mathbf{MF_L}(\varphi)$, c'est-à-dire un L_0-espace vectoriel de dimension 2, muni d'une application σ-semi-linéaire bijective $\varphi : D \to D$, et d'une filtration décroissante, exhaustive et séparée sur $D_L = D \otimes_{L_0} L$ par des sous-L-espaces vectoriels $\mathrm{Fil}^i D_L$, $i \in \mathbb{Z}$. On sait que D est de type Hodge-Tate $(0,1)$:

$$\begin{cases} \mathrm{Fil}^0 D_L &= D_L \\ \mathrm{Fil}^1 D_L &= L - \text{droite} \\ \mathrm{Fil}^2 D_L &= 0 \end{cases}$$

De plus, D est faiblement admissible puisqu'il est admissible (voir [Fo 2] ou bien **1.3.1.1.**). Etendre l'action de G_L à G_K sur $V_p(E)$ revient à munir D d'une structure d'objet de $\mathbf{MF_{L/K}}(\varphi)$, i.e. faire agir $L_0 = K_0$-linéairement τ sur D, avec $\varphi\tau = \tau\varphi$, et $\tau \cdot (\mathrm{Fil}^i D_L) \subset \mathrm{Fil}^i D_L$ pour tout $i \in \mathbb{Z}$ (l'action de τ sur D_L est semi-linéaire) ; notons $\nu : I_{L/K} \to \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)))$ le morphisme que cela définit. L'objet de $\mathbf{MF_{L/K}}(\varphi)$ ainsi obtenu reste faiblement admissible ([Fo 2]). Rappelons enfin que l'on a un isomorphisme canonique d'objets de $\mathbf{MF_L}(\varphi)$:

$$L_0 \otimes_{W(k)} \mathrm{M}_{O_L}(E(p)) \simeq \mathbf{D}^*_{\mathbf{cris,L}}(V_p(E))$$

où $\mathrm{M}_{O_L}(E(p))$ est le module de Dieudonné filtré sur O_L du groupe p-divisible de E, et que, via cet isomorphisme, l'élément $\nu(\tau) \in \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)))$ correspond à l'image de $r_p(\tau)$ dans $\mathrm{Aut}_{L_0[\varphi]}(L_0 \otimes_{W(k)} \mathrm{M}(\widetilde{E}(p)))$, cf. la fin de **2.1.4.**. On écrira souvent τ au lieu de $\nu(\tau)$ lorsqu'aucune ambiguïté n'est possible.

Lemme 2 :
Soit L/K une extension totalement ramifiée de degré 2, de corps résiduel $k = \mathbb{F}_{p^m}$, et de groupe de Galois $G_{L/K} = <\tau>$. Soit D un objet de $\mathbf{MF_{L/K}}(\varphi)$ de dimension 2, de type Hodge-Tate $(0,1)$, faiblement admissible. Si $P_{min}(\tau)(X) = X^2 - 1$, alors $P_{car}(\varphi^m)$ a deux racines distinctes dans $\mathbb{Q}_p$.

Preuve :
Tout d'abord, remarquons que φ^m est $L_0 = K_0$-linéaire, puisque φ est σ-semi-linéaire et que $k = \mathbb{F}_{p^m}$. Comme $\mathrm{P}_{min}(\tau)(X) = X^2 - 1 = (X-1)(X+1)$, l'endomorphisme K_0-linéaire τ est diagonalisable dans D. Soit (e_1, e_2) une base de D telle que $\tau e_1 = e_1$ et $\tau e_2 = -e_2$. La condition $\varphi\tau = \tau\varphi$ donne :

$$\begin{cases} \tau(\varphi e_1) = \varphi(\tau e_1) = \varphi e_1 & \Rightarrow \quad \varphi e_1 \in K_0 e_1 \\ \tau(\varphi e_2) = \varphi(\tau e_2) = -\varphi e_2 & \Rightarrow \quad \varphi e_2 \in K_0 e_2 \ . \end{cases}$$

Posons $\varphi e_1 = a e_1$ et $\varphi e_2 = b e_2$, $a, b \in K_0^\times$. Comme D est de type Hodge-Tate $(0,1)$, on a $t_H(D) = 1$, et l'hypothèse de faible admissibilité entraîne en particulier que $t_H(D) = t_N(D) = v_p(ab) = 1$, où v_p est la valuation sur K_0 normalisée par $v_p(p) = 1$. Donc $ab = up$, $u \in W(k)^\times$, et quitte à permuter e_1 et e_2, on peut supposer que $\varphi e_1 = u_1 e_1$ et $\varphi e_2 = u_2 p e_2$, $u_1, u_2 \in W(k)^\times = W(\mathbb{F}_{p^m})^\times$. Alors on a :

$$\begin{cases} \varphi^m e_1 &= \Big(\prod\limits_{0 \le i \le m-1} \sigma^i u_1 \Big) e_1 &= \mathrm{N}_{L_0/\mathbb{Q}_p}(u_1)\ e_1 \\ \varphi^m e_2 &= \Big(\prod\limits_{0 \le i \le m-1} \sigma^i (u_2 p) \Big) e_2 &= \mathrm{N}_{L_0/\mathbb{Q}_p}(u_2) p^m\ e_2 \ , \end{cases}$$

avec $\lambda_1 = \mathrm{N}_{L_0/\mathbb{Q}_p}(u_1)$ et $\lambda_2 = \mathrm{N}_{L_0/\mathbb{Q}_p}(u_2) \in \mathbb{Z}_p^\times$. Finalement, on voit que $\mathrm{P}_{car}(\varphi^m)(X) = \mathrm{P}_{min}(\varphi^m)(X) = (X - \lambda_1)(X - \lambda_2 p^m)$, ce qui achève la démonstration. □

Notons $\widetilde{E}/k$ la courbe réduite de E/L. Le Frobenius arithmétique relatif à k agissant sur $\widetilde{E}$ correspond à φ^m dans $\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E))$, et à $\rho_0(\phi)$ dans les $\mathbf{W\widehat{D}}^*_{\mathbf{pst,l,L}}(V_l(E))$, $l \in \mathcal{P}$, où ϕ est un relèvement du Frobenius géométrique relatif à k.

Proposition 5 :
Soit L/K une extension finie galoisienne totalement ramifiée. Soit E une courbe elliptique sur L, ayant bonne réduction sur L.
Supposons que l'action de G_L s'étend en une action de G_K sur $T_p(E)$ et sur les $V_l(E)$, $l \neq p$, de sorte que l'action de W_K soit compatible. Alors le déterminant de l'action de G_K sur $V_p(E)$ est le caractère cyclotomique $\chi_{p,K}$.

Preuve :
L'hypothèse de compatibilité entraîne que l'action de W_K sur $\Delta_p = \mathbf{W\widehat{D}}^*_{\mathbf{pst,p,K}}(V_p(E))$ est définie sur $\mathbb{Q}$. Supposons que le déterminant de l'action étendue sur $V_p(E)$ soit $\xi_2 \chi_{p,K}$, où ξ_2 est comme dans le lemme 1. Alors, toujours par la compatibilité, le déterminant de l'action étendue sur $V_l(E)$, $l \neq p$, est aussi $\xi_2 \chi_{l,K}$. On se ramène, ainsi que nous l'avons vu plus haut, à L/K ramifiée d'ordre deux, $G_{L/K} = I_{L/K} =< \tau >$, et $\mathrm{P}_{min}(\tau)(X) = X^2 - 1$.

Notons $X^2 - a_q X + q$ le polynôme caractéristique du Frobenius arithmétique agissant sur $\widetilde{E}$, où $q = p^m = |k|$ et $a_q \in \mathbb{Z}$. On pose aussi $\delta = a_q^2 - 4q$. Soient ϕ un relèvement dans W_L du Frobenius géométrique relatif à k, et θ un relèvement dans I_K de τ (tous deux sont définis modulo I_L). Rappelons que $\mathbb{Q}'_l = \mathbb{Q}_l$ pour $l \neq p$, et $\mathbb{Q}'_p = L_0 = K_0$.

D'une part, pour $l \in \mathcal{P}$, $\Delta_l = \mathbf{W\widehat{D}}^*_{\mathbf{pst,l,K}}(V_l(E))$ est un $\mathbb{Q}'_l$-espace vectoriel de dimension

2 muni d'une action $\rho_0 : W_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l'}(\Delta_l)$ telle que :

$$\begin{cases} \rho_0(I_L) = 1 \\ \mathrm{P}_{car}(\rho_0(\phi)) = X^2 - a_q X + q \\ \mathrm{P}_{min}(\rho_0(\theta)) = X^2 - 1 \\ \rho_0(\phi)\rho_0(\theta) = \rho_0(\theta)\rho_0(\phi) \end{cases},$$

la dernière égalité provenant du fait que $[L : K] = 2$. En particulier, on voit que $\rho_0(\theta)$ est diagonalisable à valeurs propres distinctes, et qu'il commute avec $\rho_0(\phi)$, et cela dans tous les Δ_l, $l \in \mathcal{P}$. Donc $\rho_0(\phi)$ est diagonalisable dans tous les Δ_l, $l \in \mathcal{P}$. Ceci implique que $X^2 - a_q X + q$ se scinde dans tous les $\mathbb{Q}_l'[X]$, $l \in \mathcal{P}$, donc dans $\mathbb{Q}[X]$, et nécessairement $\delta \geq 0$.

D'autre part, le lemme 2 s'applique à $D = \mathbf{D}^*_{\mathbf{cris,L}}(V_p(E))$. Comme $\mathrm{P}_{car}(\varphi^m)(X) = \mathrm{P}_{car}(\rho_0(\phi)) = X^2 - a_q X + q$, on obtient que $X^2 - a_q X + q$ est scindé à racines distinctes dans $\mathbb{Q}[X]$. Donc $\delta > 0$.

Mais E étant une courbe elliptique, on doit avoir $\delta \leq 0$, d'où une contradiction. D'après le lemme 1, le déterminant de l'action de G_K sur $V_p(E)$ doit être le caractère cyclotomique $\chi_{p,K}$. □

Remarques :

1) On a vraiment besoin de considérer une action prolongée (convenablement) non seulement sur $T_p(E)$, mais aussi sur les $V_l(E)$, $l \neq p$.

Exemple avec $\delta < 0$: Soit E un schéma elliptique sur O_L qui est le relèvement "canonique" d'une courbe elliptique $\widetilde{E}$ ordinaire sur k (voir [Mes] ou [Ka]). Alors la suite exacte de $\mathbb{Z}_p[G_L]$-modules

$$0 \longrightarrow T_p(E(p)^0) \longrightarrow T_p(E) \longrightarrow T_p(\widetilde{E}) \longrightarrow 0$$

est scindée ($E(p)^0$ est la partie connexe du groupe p-divisible $E(p)$ de E). Posons $T_p(E(p)^0) = \mathbb{Z}_p e_1$ et $T_p(\widetilde{E}) = \mathbb{Z}_p e_2$; on a donc $T_p(E) = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$. Prenons L/K totalement ramifiée d'ordre 2, $G_{L/K} = <\tau>$. Alors on peut très bien étendre l'action sur $T_p(E)$ en posant $\tau e_1 = e_1$ et $\tau e_2 = -e_2$: la représentation de W_K est définie sur $\mathbb{Q}$, mais le déterminant sur $V_p(E)$ n'est pas $\chi_{p,K}$.

2) On a vraiment besoin de considérer une action prolongée (convenablement) non seulement sur les $V_l(E)$, $l \neq p$, mais aussi sur $T_p(E)$.

Exemple avec $\delta = 0$: Prenons E un schéma elliptique sur O_L, dont la fibre spéciale $\widetilde{E}$ est supersingulière et telle que tous ses endomorphismes sont définis sur k. Alors $\delta = a_q^2 - 4q = 0$ et nécessairement m est pair, $q = p^m = p^{2n}$. Sur les $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l,K}}(V_l(E))$, $l \in \mathcal{P}$, W_L agit par $\rho_0 : W_L \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l'}(\Delta_l)$, avec $\rho_0(I_L) = 1$ et $\rho_0(\phi) = \epsilon p^n \mathrm{Id}$ avec $\epsilon \in \{\pm 1\}$ (indépendant de l) ; l'image de ρ_0 est dans le centre de $\mathrm{Aut}_{\mathbb{Q}_l'}(\Delta_l)$. Prenons L/K totalement ramifiée d'ordre 2, $G_{L/K} = <\tau>$, et θ un relèvement de τ dans I_K. Alors en imposant $\mathrm{P}_{min}(\rho_0(\theta)) = X^2 - 1$ sur tous les Δ_l, $l \neq p$, on obtient un système compatible $(\Delta_l)_{l \neq p}$ de représentations de W_K, ce qui équivaut à étendre l'action de façon compatible sur les $(V_l(E))_{l \neq p}$ avec un déterminant sur $V_l(E)$ qui n'est pas $\chi_{l,K}$.

2.3.2. Représentations de dimension 2 :

Soit E/L une courbe elliptique ayant bonne réduction sur L. Supposons que l'action de

G_L sur $T_p(E)$ s'étend en une action de G_K telle que :
1) la représentation de W_K qui lui est associée est définie sur $\mathbb{Q}$,
2) le déterminant de l'action de G_K sur $V_p(E)$ est le caractère cyclotomique $\chi_{p,K}$ relatif à K,
3) le morphisme r_p est injectif.
En particulier, les hypothèses 1) et 2) sont vérifiées lorsque l'action de G_L s'étend sur $T_p(E)$ et sur tous les $V_l(E)$, $l \neq p$, en une action *compatible* de G_K (i.e. lorsque l'action de W_K ainsi obtenue est compatible).

On obtient alors une injection :

$$G_{L/K} \overset{r_p}{\hookrightarrow} \left(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})\right)^{\times} \simeq_{\mathbb{Q}_p-ev} \mathrm{Aut}_{L_0[\varphi]}\left(L_0 \otimes_{W(k)} \mathrm{M}(\widetilde{E}(p))\right) ,$$

où $\mathrm{M}(\widetilde{E}(p))$ est le module de Dieudonné de la fibre spéciale du groupe p-divisible de E. Soit $\tau \in G_{L/K} = I_{L/K}$, notons encore τ son image par r_p dans $\mathrm{Aut}_{L_0[\varphi]}(L_0 \otimes_{W(k)} \mathrm{M}(\widetilde{E}(p)))$: c'est une application L_0-linéaire qui commute avec φ (elle est L_0-linéaire parce que τ est dans le groupe d'inertie).

L'hypothèse 1) impose au polynôme caractéristique de τ d'être dans $\mathbb{Q}[X]$, et l'hypothèse 2) impose $\det(\tau) = 1$. Ecrivons $\mathrm{P}_{car}(\tau)(X) = X^2 - \gamma X + 1$, avec $\gamma \in \mathbb{Q}$.
Soit d l'ordre de τ dans $G_{L/K} = I_{L/K}$; comme on a supposé l'action de $G_{L/K}$ via r_p fidèle (hypothèse 3)), d est aussi l'ordre de τ dans $\mathrm{Aut}_{L_0[\varphi]}(L_0 \otimes_{W(k)} \mathrm{M}(\widetilde{E}(p)))$.
Si $\mathrm{P}_{min}(\tau)(X) \neq \mathrm{P}_{car}(\tau)(X)$, on a nécessairement $\mathrm{P}_{min}(\tau)(X) = X - \nu$, $\nu \in L_0$, et $\mathrm{P}_{car}(\tau)(X) = (X-\nu)^2$. On voit alors que $\nu \in \mathbb{Q}$ et $\nu = \pm 1$; donc $\tau = \pm \mathrm{Id}$ et $d = 1$ ou 2.
Si $d \geq 3$, alors $X^2 - \gamma X + 1$ est le polynôme minimal de τ. Comme $\tau^d = 1$, $X^2 - \gamma X + 1$ divise $X^d - 1$ dans $L_0[X]$, et donc dans $\mathbb{Q}[X]$ puisque $\gamma \in \mathbb{Q}$ (et même $\gamma \in \mathbb{Z}$). Donc $X^2 - \gamma X + 1$ est l'un des polynômes cyclotomiques $\Phi_e(X)$, $e \mid d$, et en fait $e = d$, puisque d est l'ordre de τ. On en déduit que $\varphi(e) = 2$, où φ est la fonction arithmétique d'Euler. Donc $e \in \{3, 4, 6\}$.
Si $e = 3$ (resp. 4, 6), alors $\gamma = -1$ (resp. 0, 1), et $\mathrm{P}_{car}(\tau)(X) = \mathrm{P}_{min}(\tau)(X) = X^2 + X + 1$ (resp. $X^2 + 1$, $X^2 - X + 1$).
On voit finalement que l'ordre de τ est $e \in \{1, 2, 3, 4, 6\}$; ceci implique que l'ordre de $G_{L/K} = I_{L/K}$ n'est divisible que par 2 ou par 3. On obtient ainsi le résultat sûrement bien connu :

Lemme 3 :
Soit L/K une extension finie galoisienne totalement ramifiée. Soit E/L une courbe elliptique ayant bonne réduction sur L. On suppose que l'action de G_L sur $T_p(E)$ s'étend en une action de G_K telle que :
1) la représentation de W_K qui lui est associée est définie sur $\mathbb{Q}$,
2) le déterminant de l'action de G_K est le caractère cyclotomique $\chi_{p,K}$ relatif à K,
3) le morphisme r_p est injectif.
Alors les ordres possibles des éléments de $G_{L/K}$ sont $1, 2, 3, 4$, ou 6, et l'ordre de $G_{L/K}$ est $2^n 3^m$, $n, m \in \mathbb{N}$.

Remarque : on aurait pu remplacer p par $l \neq p$ dans ce qui précède.

A partir de maintenant, on suppose $\mathbf{p \geq 5}$.

Alors $G_{L/K}$ est le groupe de Galois d'une extension de degré d totalement *modérément*

ramifiée. Or, une telle extension est cyclique et est engendrée par une racine d'un polynôme $X^d - \pi_K$, où π_K est une uniformisante de K (et d est premier à p). *Donc, sous les hypothèses du lemme, $G_{L/K} = I_{L/K}$ est cyclique d'ordre $e = 1, 2, 3, 4$ ou 6.*

Soit ζ_e une racine primitive e-ième de l'unité. Pour $e \in \{3, 4, 6\}$, L/K galoisienne impose $\zeta_e \in K$, et même $\zeta_e \in L_0 = K_0 = \mathrm{Frac}W(k)$, puisque $(e, p) = 1$. Si $\mathbb{F}_{p^2} \subseteq k$, alors c'est automatique, car $\zeta_e \in \mathbb{Q}_{p^2}$ pour $e \in \{3, 4, 6\}$. Sinon, $k = \mathbb{F}_p$, et $\zeta_e \in K_0 = \mathbb{Q}_p$ implique $p \equiv 1 \bmod e\mathbb{Z}$. Finalement, si $k = \mathbb{F}_{p^m}$, une extension L/K de degré $e \in \{3, 4, 6\}$ totalement ramifiée est galoisienne si et seulement si $p \equiv 1 \bmod e\mathbb{Z}$ ou m pair.

Conséquence : sous les hypothèses du lemme précédent, l'action prolongée sur $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l,L}}(V_l(E))$, $l \in \mathcal{P}$, est nécessairement *abélienne*. En effet, c'est évident si $e = 1$ ou 2 ; supposons $e \in \{3, 4, 6\}$. L'objet Δ_l est un $\mathbb{Q}'_l$-espace vectoriel de dimension 2 (avec $\mathbb{Q}'_l = \mathbb{Q}_l$ si $l \neq p$, $\mathbb{Q}'_p = L_0$), muni d'une action $\rho_0 : W_L \longrightarrow \mathrm{Aut}_{\mathbb{Q}'_l}(\Delta_l)$ définie par :

$$\begin{cases} \rho_0(I_L) = 1 \\ \mathrm{P}_{car}(\rho_0(\phi)) = X^2 - a_q X + q \end{cases},$$

où ϕ est un relèvement du Frobenius géométrique relatif à $k = \mathbb{F}_q = \mathbb{F}_{p^m}$. Soit θ un relèvement de τ dans I_K. Alors on a $\phi^{-1}\theta\phi \equiv \theta^q \bmod I_L \equiv \theta \bmod I_L$; en effet, $p \in (\mathbb{Z}/e\mathbb{Z})^\times = \{-1, 1\}$, et les conditions ci-dessus impliquent $q = p^m \equiv 1 \bmod e\mathbb{Z}$. Prolonger l'action à G_K sur Δ_l, $l \in \mathcal{P}$, avec un r_l injectif, revient à se donner un prolongement de ρ_0 avec action fidèle de $G_{L/K} = I_{L/K} = W_K/W_L$:

$$\rho_{0,l} : W_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}'_l}(\Delta_l),$$

c'est-à-dire à se donner un $\rho_{0,l}(\theta) \in \mathrm{Aut}_{\mathbb{Q}'_l}(\Delta_l)$ d'ordre exact e et vérifiant :

$$\rho_0(\phi)\rho_{0,l}(\theta) = \rho_{0,l}(\theta)^q\rho_0(\phi) = \rho_{0,l}(\theta)\rho_0(\phi).$$

De plus, si cette représentation est définie sur $\mathbb{Q}$, on sait que $\mathrm{P}_{min}(\rho_{0,l}(\theta)) = X^2 - \gamma_e X + 1$, avec $\gamma_e = -1, 0, 1$ si $e = 3, 4, 6$ respectivement ; si l'on considère des actions prolongées sur tous les Δ_l, $l \in \mathcal{P}$, l'hypothèse de compatibilité entraîne que c'est indépendant de l.

2.4. Le théorème de l'action prolongée, cas commutatif :

2.4.1. Démonstration du théorème :

Nous allons donner un énoncé du résultat principal de ce chapitre dans le cas d'une courbe elliptique dont l'anneau des endomorphismes (sur k) de la fibre spéciale est commutatif, et le démontrer. Cet énoncé n'est pas optimal, mais c'est le plus général (i.e. il est valable dans tous les cas). De plus, des renseignements supplémentaires vont apparaître en cours de démonstration. Un énoncé plus détaillé est donné au paragraphe suivant.

Le polynôme caractéristique du Frobenius arithmétique agissant sur $\widetilde{E}$ (par $x \mapsto x^q$) s'écrit $X^2 - a_q X + q$, où $a_q \in \mathbb{Z}$, et le discriminant $\delta = a_q^2 - 4q$ est négatif ou nul. Alors (voir par exemple [Ta]) :

- $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})$ est un corps commutatif si et seulement si $\delta < 0$; c'est alors une extension quadratique de $\mathbb{Q}$ purement imaginaire $F = \mathbb{Q}(\sqrt{\delta})$.
- $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})$ est une algèbre de quaternions sur $\mathbb{Q}$ si et seulement si $\delta = 0$; c'est alors l'unique $\mathbb{Q}$-algèbre de quaternions $\mathcal{D}$ qui se ramifie en p et à l'infini, et qui se déploie en toutes les autres places. Remarquons que cette situation $\delta = 0$ ne peut arriver que si m est pair ($q = p^m$) : si m est impair, $4q$ ne peut être un carré dans $\mathbb{Z}$.

De plus, on sait que $\mathrm{Aut}(\widetilde{E}) = \mathrm{Aut}_{\overline{k}}(\widetilde{E})$ est isomorphe au G_k-module $\mu_n(\overline{k})$ des racines n-ièmes de l'unité, avec $n = 2, 4$ ou 6 respectivement suivant si $j_{\widetilde{E}} = j_E \bmod \pi_L O_L$ est différent de 0 et de 1728, égal à $1728 = 12^3$, ou égal à 0 (voir par exemple [Silv 1]). Rappelons que si ζ_n est une racine n-ième de l'unité, avec $n = 2, 4$ ou 6, alors le morphisme $[\zeta_n] : \widetilde{E}(\overline{k}) \to \widetilde{E}(\overline{k})$ est donné par $(x, y) \mapsto (\zeta_n^2 x, \zeta_n^3 y)$. Si $n = 2$, alors $\mathrm{Aut}(\widetilde{E}) = \mathrm{Aut}_k(\widetilde{E})$, et l'élément non trivial est la multiplication par (-1) sur la courbe $\widetilde{E}$. Supposons $n = 4$ ou 6. Si $\mathbb{F}_{p^2} \subseteq k$, alors $\mathrm{Aut}(\widetilde{E}) = \mathrm{Aut}_k(\widetilde{E}) = \mu_n(\overline{k}) = \mu_n(k)$, puisque $\zeta_n \in \mathbb{F}_{p^2}$ pour $n = 4$ ou 6 (en effet, $p \equiv \pm 1 \bmod n$). Si $k = \mathbb{F}_p$, alors $\mathrm{Aut}(\widetilde{E}) = \mathrm{Aut}_k(\widetilde{E})$ si et seulement si $p \equiv 1 \bmod n$.

En recoupant avec la remarque faite à la fin du paragraphe précédent, on voit que si l'extension totalement ramifiée L/K est galoisienne, alors $\mathrm{Aut}(\widetilde{E}) = \mathrm{Aut}_k(\widetilde{E})$.

Théorème 2 :
Soient K une extension finie de $\mathbb{Q}_p$, $p \geq 5$, et L une extension finie totalement ramifiée de K. Soit E une courbe elliptique sur L, ayant bonne réduction sur L, telle que $\mathrm{End}_k(\widetilde{E})$ est commutatif.
Supposons que l'action de G_L s'étend en une action de G_K sur tous les $T_l(E)$, $l \in \mathcal{P}$, de sorte que l'action de W_K ainsi obtenue soit compatible.
Alors E est définie sur K : il existe une courbe elliptique $\mathcal{E}$ sur K et un L-isomorphisme $\psi : \mathcal{E} \times_K L \xrightarrow{\sim} E$ qui induit pour tout $l \in \mathcal{P}$ des isomorphismes de $\mathbb{Z}_l[G_K]$-modules :

$$T_l(\psi) : \quad \underbrace{T_l(\mathcal{E})}_{\text{action naturelle}} \quad \simeq \quad \underbrace{T_l(E)}_{\text{action étendue}} \quad ;$$

un tel couple $(\mathcal{E}, \psi)$ est unique à K-isomorphisme près.

Preuve :
Tout d'abord, on se ramène par la proposition 1 de **2.1.3.** au cas où l'extension L/K est galoisienne. D'après tout ce que l'on a vu précédemment, ou bien les morphismes r_l construits en **2.1.4.** :

$$G_{L/K} \xrightarrow{r_l} \left(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})\right)^\times$$

sont triviaux pour tout $l \in \mathcal{P}$, et E est définie sur K avec bonne réduction sur K ; ou bien ils ne le sont pas, et l'on peut supposer les r_l injectifs, $[L : K] = e \in \{2, 3, 4, 6\}$, et $G_{L/K} = I_{L/K}$ cyclique. Plaçons-nous dans la deuxième situation et fixons un générateur τ de $G_{L/K}$.
Pour tout $l \in \mathcal{P}$, nous disposons de morphismes injectifs $G_{L/K} = <\tau> \overset{r_l}{\hookrightarrow} (\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times$, et nous connaissons le polynôme minimal de $r_l(\tau)$. Afin de satisfaire le critère de Weil comme dans **2.1.4.**, on voudrait récupérer un morphisme

$$G_{L/K} = <\tau> \overset{r}{\hookrightarrow} \left(\mathrm{End}_k(\widetilde{E})\right)^\times = \mathrm{Aut}_k(\widetilde{E})$$

qui induit tous les r_l, $l \in \mathcal{P}$, par extension des scalaires de $\mathbb{Z}$ à $\mathbb{Z}_l$ (théorème 1) ; la dernière assertion du théorème proviendra du lemme 2 de **2.1.2.**. Notons encore r_l le morphisme obtenu en composant r_l avec l'inclusion $(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times \subset \mathbb{Q}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})$. Si l'on arrive à obtenir un morphisme

$$G_{L/K} = <\tau> \overset{r}{\hookrightarrow} \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})$$

qui induit tous les r_l par extension des scalaires de $\mathbb{Q}$ à $\mathbb{Q}_l$, alors l'image de ce morphisme est nécessairement dans $(\mathrm{End}_k(\widetilde{E}))^\times = \mathrm{Aut}_k(\widetilde{E})$, puisque, par hypothèse, l'image des r_l est dans $(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times$ pour tout $l \in \mathcal{P}$ (cet argument est indispensable si l'on veut espérer récupérer des isomorphismes sur la fibre spéciale, et non pas seulement des isogénies ; un exemple sera donné plus loin).

Fixons, pour $e \in \{3,4,6\}$, une racine primitive e-ième de l'unité ζ_e dans $\overline{\mathbb{Q}}$, une clôture algébrique de $\mathbb{Q}$; on pose aussi $\zeta_2 = -1$.
Comme l'on a supposé $\delta < 0$, $F = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}) = \mathbb{Q}(\sqrt{\delta})$ est une extension quadratique imaginaire de $\mathbb{Q}$. Soit $l \in \mathcal{P}$.
- Si δ n'est pas un carré dans $\mathbb{Q}_l^\times$, alors $X^2 - a_q X + q$ est irréductible dans $\mathbb{Q}_l[X]$ et $F \otimes_{\mathbb{Q}} \mathbb{Q}_l$ est un corps qui est une extension quadratique de $\mathbb{Q}_l$: $F \otimes_{\mathbb{Q}} \mathbb{Q}_l = \mathbb{Q}_l(\sqrt{\delta})$. L'homomorphisme injectif

$$G_{L/K} = <\tau> \overset{r_l}{\hookrightarrow} F \otimes_{\mathbb{Q}} \mathbb{Q}_l = \mathbb{Q}_l(\sqrt{\delta})$$

doit envoyer τ sur une racine primitive e-ième de l'unité, puisque l'ordre de $G_{L/K}$ est $e \in \{2,3,4,6\}$. Donc $\zeta_e \in \mathbb{Q}_l(\sqrt{\delta})$ lorsque $\delta \notin (\mathbb{Q}_l^\times)^2$. De plus, si $e = 2$, $r_l(\tau) = -1$; si $e \in \{3,4,6\}$, $r_l(\tau) = \zeta_e$ ou ζ_e^{-1}.
- Si δ est un carré dans $\mathbb{Q}_l^\times$, alors $X^2 - a_q X + q$ se scinde dans $\mathbb{Q}_l[X]$; écrivons $X^2 - a_q X + q = (X - \alpha_l)(X - \beta_l)$, avec $\alpha_l, \beta_l \in \mathbb{Q}_l$ et $\alpha_l \neq \beta_l$. Alors on a

$$F \otimes_{\mathbb{Q}} \mathbb{Q}_l \;=\; \mathbb{Q}_l[X]/(X-\alpha_l)(X-\beta_l) \;\simeq\; \mathbb{Q}_l[X]/(X-\alpha_l) \times \mathbb{Q}_l[X]/(X-\beta_l) \;\simeq\; \mathbb{Q}_l \times \mathbb{Q}_l\,.$$

Rappelons les isomorphismes canoniques : $F \otimes_{\mathbb{Q}} \mathbb{Q}_l = \mathbb{Q}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}) \simeq \mathrm{End}_{\mathbb{Q}_l[G_k]}(V_l(\widetilde{E}))$ pour $l \neq p$, et $F \otimes_{\mathbb{Q}} \mathbb{Q}_p = \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}) \simeq \mathrm{End}_{L_0[\varphi]}(L_0 \otimes_{W(k)} \mathbf{M}(\widetilde{E}(p)))$. Un élément de $F \otimes_{\mathbb{Q}} \mathbb{Q}_l$ est une application $\mathbb{Q}_l$-linéaire qui commute avec le Frobenius de $\widetilde{E}$, lequel est ici diagonalisable à valeurs propres distinctes. Donc cet élément est co-diagonalisable, et son image dans $\mathbb{Q}_l \times \mathbb{Q}_l$ correspond à son écriture dans une base de vecteurs propres. L'image du Frobenius de $\widetilde{E}$ est donc (α_l, β_l), et le déterminant de l'image (a,b) d'un élément de $F \otimes_{\mathbb{Q}} \mathbb{Q}_l$ est le produit ab.
Si $e = 2$, r_l envoie τ sur un élément d'ordre exact 2 de $\mathbb{Q}_l \times \mathbb{Q}_l$, c'est-à-dire sur $(-1,1)$, $(1,-1)$ ou $(-1,-1)$. Les deux premières possibilités sont exclues par la condition $\det(\tau) = 1$, donc τ est envoyé sur $(-1,-1)$.
Si $e \in \{3,4,6\}$, la seule façon d'injecter $G_{L/K} = <\tau>$ dans $\mathbb{Q}_l \times \mathbb{Q}_l$ avec un déterminant égal à 1 est d'envoyer τ sur (ζ_e, ζ_e^{-1}) ou bien sur (ζ_e^{-1}, ζ_e). Donc $\zeta_e \in \mathbb{Q}_l$ lorsque $\delta \in (\mathbb{Q}_l^\times)^2$, et l'on doit avoir $l \neq 2,3$ et $l \equiv 1 \bmod e$.

On en déduit : pour tout $l \in \mathcal{P}$, $\zeta_e \in \mathbb{Q}_l(\sqrt{\delta}) = F \otimes_{\mathbb{Q}} \mathbb{Q}_l$, donc $\zeta_e \in F = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})$; et $r_l(\tau) \in (\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times$ pour tout $l \in \mathcal{P}$ implique que $\zeta_e \in \mathrm{Aut}_k(\widetilde{E})$. Pour chaque $l \in \mathcal{P}$, r_l provient par extension des scalaires *soit* du morphisme $r : G_{L/K} \hookrightarrow \mathrm{Aut}_k(\widetilde{E})$ qui à τ associe ζ_e, *soit* du morphisme $r' : G_{L/K} \hookrightarrow \mathrm{Aut}_k(\widetilde{E})$ qui à τ associe ζ_e^{-1}.
Pour $e = 2$, ces deux morphismes sont identiques, et l'on a gagné : *les différents morphismes*

$r_l : G_{L/K} = <\tau> \hookrightarrow F \otimes_{\mathbb{Q}} \mathbb{Q}_l$, $l \in \mathcal{P}$, *sont tous induits par le morphisme* $G_{L/K} \hookrightarrow \mathrm{Aut}_k(\widetilde{E}) \subset F$ *qui à* τ *associe la multiplication par* (-1) *sur* $\widetilde{E}$. Pour $e \in \{3,4,6\}$, c'est l'hypothèse de compatibilité qui va nous permettre de conclure : c'est vraiment à cet endroit que l'on s'en sert.

Rappelons que sous les hypothèses du théorème, et en se ramenant à une extension L/K finie totalement ramifiée galoisienne, l'action prolongée sur les Δ_l, $l \in \mathcal{P}$, est abélienne (cf. **2.3.2.**). Soient ϕ un relèvement du Frobenius géométrique relatif à k dans G_L, et θ un relèvement de τ dans I_K. Si le morphisme r_l provient par extension des scalaires du morphisme $r : G_{L/K} = <\tau> \hookrightarrow \mathrm{Aut}_k(\widetilde{E})$ défini par $r(\tau) = \zeta_e$, notons $\tilde{\rho}_0 : W_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l'}(\Delta_l)$ la représentation qui lui correspond ; et si r_l provient du morphisme $r' : G_{L/K} \hookrightarrow \mathrm{Aut}_k(\widetilde{E})$ défini par $r'(\tau) = \zeta_e^{-1}$, notons $\tilde{\rho}_0' : W_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l'}(\Delta_l)$ la représentation qui correspond à r'. On a : $(\tilde{\rho}_0)_{|W_L} = (\tilde{\rho}_0')_{|W_L} = \rho_0$, et $\tilde{\rho}_0'(\theta) = \tilde{\rho}_0(\theta)^{-1}$. De plus :

$$\forall\, l \in \mathcal{P} \quad , \quad \rho_{0,l} = \tilde{\rho}_0 \ \text{ ou } \ \tilde{\rho}_0' \ .$$

Les représentations $\rho_{0,l}$, $l \in \mathcal{P}$, sont toutes semi-simples (parce que ρ_0 l'est). L'hypothèse de compatibilité signifie alors qu'elles ont toutes le même caractère à valeurs dans $\mathbb{Q}$:

$$\forall\, l, l' \in \mathcal{P} \quad , \quad \mathrm{Tr}(\rho_{0,l}(w)) = \mathrm{Tr}(\rho_{0,l'}(w)) \ , \ \forall\, w \in W_K \ .$$

Mais dans notre situation, $\mathrm{Tr}(\tilde{\rho}_0(\phi\theta)) \neq \mathrm{Tr}(\tilde{\rho}_0'(\phi\theta))$. En effet, comme $\rho_0(\phi)$ et $\rho_{0,l}(\theta)$ commutent et qu'ils ont des valeurs propres distinctes dans $\mathbb{C}$, ils sont co-diagonalisables lorsque l'on étend les scalaires à $\mathbb{C}$ (via les injections $\iota_l : \mathbb{Q}_l' \hookrightarrow \mathbb{C}$, cf. **2.2.1.**) ; puis si l'on écrit $\mathrm{P}_{car}(\rho_0(\phi)) = (X - z)(X - \bar{z})$, $z \in \mathbb{C}$, un calcul facile donne :

$$\mathrm{Tr}(\tilde{\rho}_0(\phi\theta)) - \mathrm{Tr}(\tilde{\rho}_0'(\phi\theta)) = \mathrm{Tr}(\tilde{\rho}_0(\phi)\tilde{\rho}_0(\theta)) - \mathrm{Tr}(\tilde{\rho}_0(\phi)\tilde{\rho}_0(\theta)^{-1}) = \pm(z - \bar{z})(\zeta_e - \zeta_e^{-1}) \neq 0 \ ,$$

car $\delta \neq 0$ et $e \geq 3$. Donc les représentations $\tilde{\rho}_0$ et $\tilde{\rho}_0'$ ne sont pas isomorphes. Finalement :

$$\left(\forall\, l \in \mathcal{P} \ , \ \rho_{0,l} = \tilde{\rho}_0 \right) \quad \text{ou} \quad \left(\forall\, l \in \mathcal{P} \ , \ \rho_{0,l} = \tilde{\rho}_0' \right)$$

et donc :

$$\left(\forall\, l \in \mathcal{P} \ , \ r_l = r \otimes_{\mathbb{Q}} \mathrm{Id}_{\mathbb{Q}_l} \right) \quad \text{ou} \quad \left(\forall\, l \in \mathcal{P} \ , \ r_l = r' \otimes_{\mathbb{Q}} \mathrm{Id}_{\mathbb{Q}_l} \right) ,$$

ce qui achève la démonstration. □

Remarque 1 : Pour des représentations abéliennes de dimension 2, sachant que $\mathrm{Tr}(\rho_0(\phi)) = a_q$ et $\mathrm{Tr}(\tilde{\rho}_0(\theta)) = \gamma_e$, la connaissance de toutes les traces équivaut à celle de $\mathrm{Tr}(\tilde{\rho}_0(\phi\theta))$; ceci détermine $\tilde{\rho}_0$ à isomorphisme près. De plus, un calcul simple montre que :

$$\mathrm{Tr}(\tilde{\rho}_0'(\phi\theta)) = \gamma_e a_q - \mathrm{Tr}(\tilde{\rho}_0(\phi\theta)) \ .$$

Pour $e \geq 3$, le fait de demander aux traces d'être dans $\mathbb{Q}$ impose des conditions sur l'entier a_q, à savoir $a_q \in \mathcal{N}_{q,e}^{\times} = \{a \in \mathbb{Z} / (\gamma_e^2 - 4)(a^2 - 4q) \in (\mathbb{Q}^{\times})^2\}$, c'est-à-dire

$$\begin{cases} e = 3 \text{ ou } 6 & \Longrightarrow \quad \delta \equiv -3 \bmod (\mathbb{Q}^{\times})^2 \\ e = 4 & \Longrightarrow \quad \delta \equiv -1 \bmod (\mathbb{Q}^{\times})^2 \end{cases}$$

ce qui équivaut aussi à $F = \mathbb{Q}(\sqrt{\delta}) = \mathbb{Q}(\zeta_e)$, $\delta = a_q^2 - 4q$.
Ce renseignement est obtenu en supposant que l'action s'étend de G_L à G_K sur *l'un* des Δ_l, $l \in \mathcal{P}$, de sorte que l'action prolongée de G_K soit définie sur $\mathbb{Q}$ et de déterminant le caractère cyclotomique. Si l'on suppose que l'action s'étend de G_L à G_K sur *tous* les $T_l(E)$ de façon compatible, alors on obtient $[\zeta_e] \in \mathrm{Aut}_k(\widetilde{E})$, d'où $\mathrm{End}_k(\widetilde{E}) = \mathbb{Z}[\zeta_e]$; on a donc $j(\widetilde{E}) = \tilde{\jmath}(e)$, avec $\tilde{\jmath}(3) = \tilde{\jmath}(6) = 0$ et $\tilde{\jmath}(4) = 1728$.

Remarque 2 : Lorsque $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}) = F$ est un corps (i.e. $\delta < 0$), deux cas peuvent se produire pour la $\mathbb{Q}$-algèbre $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(\widetilde{E}) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{\overline{k}}(\widetilde{E})$, suivant si $\widetilde{E}$ est ordinaire ($a_q \not\equiv 0 \bmod p$) ou bien supersingulière ($a_q \equiv 0 \bmod p$).
Si p ne divise pas a_q, alors $F = \mathbb{Q}(\sqrt{\delta}) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(\widetilde{E})$, et d'après Deuring ([Deu]), p se décompose dans l'anneau des entiers de F en deux idéaux premiers distincts ; si l'on écrit $\delta = ds^2$, où $s \in \mathbb{N}$ et d est un entier strictement négatif sans facteur carré, ceci équivaut, puisque $p \geq 5$, à p ne divise pas d et $(\frac{d}{p}) = 1$ (symbole de Legendre). Pour $e = 3$ ou 6, on a vu (rmq. *1*) que $d = -3$, et $(\frac{-3}{p}) = 1$ équivaut par la loi de réciprocité quadratique à $(\frac{p}{3}) = 1$, c'est-à-dire $p \equiv 1 \bmod 3$ ($\Leftrightarrow p \equiv 1 \bmod 6$, pour $p \geq 5$). Pour $e = 4$, on a vu que $d = -1$, et $(\frac{-1}{p}) = 1$ équivaut à $p \equiv 1 \bmod 4$. Donc $a_q \not\equiv 0 \bmod p$ implique $p \equiv 1 \bmod e$.
Si p divise a_q, alors $F = \mathbb{Q}(\sqrt{\delta}) \subset \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(\widetilde{E}) = \mathcal{D}$, où $\mathcal{D}$ est l'algèbre de quaternions sur $\mathbb{Q}$ qui se ramifie en p et à l'infini, et qui se déploie en toutes les autres places. On verra en **2.4.2.** que dans ce cas, pour $e \in \{3, 4, 6\}$, $\zeta_e \in \mathcal{D}$ implique $p \equiv -1 \bmod e$.

Finalement, sous les hypothèses du théorème, et si l'indice e de $\mathrm{Ker}(r_p)$ dans $I_{L/K}$ est supérieur ou égal à 3, on a :

$$\begin{cases} \widetilde{E} \text{ ordinaire} & \Longrightarrow \quad p \equiv 1 \bmod e \\ \widetilde{E} \text{ supersingulière} & \Longrightarrow \quad p \equiv -1 \bmod e\ . \end{cases}$$

Là encore, ce renseignement est obtenu en supposant que l'action s'étend de G_L à G_K sur *l'un* des Δ_l, $l \in \mathcal{P}$, de sorte que l'action prolongée de G_K soit définie sur $\mathbb{Q}$ et de déterminant le caractère cyclotomique. Si l'on sait au départ que $j(\widetilde{E}) = \tilde{\jmath}(e)$, alors c'est immédiat, voir [Silv 1] V, exemples 4.4. et 4.5.

Remarque 3 : On constate que pour $e = 2$, il suffit de considérer le seul $T_p(E)$, à condition de supposer que l'action prolongée est de déterminant $\chi_{p,K}$.

Remarque 4 : Par contre, dès que $e \geq 3$, on est obligé de prendre en compte des actions prolongées sur *tous* les $T_l(E)$, $l \in \mathcal{P}$: on pourrait avoir $\zeta_e \in F = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})$ et $\zeta_e \in (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times$, mais $\zeta_e \notin \mathrm{End}_k(\widetilde{E})$. En effet, tout ordre maximal d'un corps quadratique imaginaire $F/\mathbb{Q}$ dans lequel p se décompose en deux idéaux premiers distincts, et dont le conducteur est premier à p, se réalise comme un anneau d'endomorphismes d'une courbe elliptique $\widetilde{E}$ sur k ([Deu]). Il suffit alors de prendre, pour $e \in \{3, 4, 6\}$, une courbe elliptique $\widetilde{E}$ avec : $\mathrm{End}_k(\widetilde{E}) = \mathbb{Z} + n\mathbb{Z}[\zeta_e]$, $n \geq 2$, et n premier à p. Alors $F = \mathbb{Q}(\zeta_e)$ et $\zeta_e = \frac{1}{n} \otimes n\zeta_e \in (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times$, mais $\zeta_e \notin \mathrm{End}_k(\widetilde{E})$.

2.4.2. A propos du cas non commutatif :

Regardons maintenant ce que l'on peut dire lorsque $\delta = a_q^2 - 4q = 0$, c'est-à-dire lorsque

$\mathrm{End}_k(\widetilde{E})$ n'est pas commutatif.
Alors $a_q^2 = 4q = 4p^m$, et comme $a_q \in \mathbb{Z}$, m doit être pair. Le polynôme caractéristique du Frobenius arithmétique relatif à k agissant sur $\widetilde{E}$ est soit $X^2 - 2p^{m/2}X + p^m = (X - p^{m/2})^2$, soit $X^2 + 2p^{m/2}X + p^m = (X + p^{m/2})^2$. La courbe $\widetilde{E}$ est supersingulière, et tous ses endomorphismes sont définis sur k, i.e. $\mathrm{End}_k(\widetilde{E}) = \mathrm{End}(\widetilde{E})$. Dans ce cas, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(\widetilde{E}) = \mathcal{D}$ est l'algèbre de quaternions sur $\mathbb{Q}$ qui se ramifie en p et à l'infini et qui se déploie en toutes les autres places, et $\mathrm{End}_k(\widetilde{E}) = \mathcal{O}$ est un ordre maximal de $\mathcal{D}$. Rappelons que la $\mathbb{Q}_p$-algèbre de quaternions $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D}$ se déploie sur toute extension de degré 2 de $\mathbb{Q}_p$, par exemple sur $\mathbb{Q}_{p^2}$.

Supposons que l'action de G_L s'étend en une action de G_K sur tous les $T_l(E)$, $l \in \mathcal{P}$, de sorte que l'action de W_K ainsi obtenue soit compatible. Comme plus haut, on se ramène au cas où tous les r_l sont injectifs. Pour $l = p$, on a une injection :

$$G_{L/K} = I_{L/K} = <\tau> \overset{r_p}{\hookrightarrow} (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O})^\times \hookrightarrow (\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D})^\times \hookrightarrow (\mathbb{Q}_{p^2} \otimes_{\mathbb{Q}} \mathcal{D})^\times \simeq \mathrm{GL}_2(\mathbb{Q}_{p^2}) \ ,$$

et l'hypothèse de compatibilité implique que le polynôme caractéristique $\mathrm{P}_{car}(r_p(\tau))(X)$ de l'image de τ dans $\mathrm{GL}_2(\mathbb{Q}_{p^2})$ est $(X+1)^2$ si $e = 2$, ou $X^2 - \gamma_e X + 1$ si $e \in \{3, 4, 6\}$, avec $\gamma_e = -1, 0, 1$ si $e = 3, 4, 6$ respectivement. Dans le vocabulaire des algèbres centrales simples, il s'agit du polynôme caractéristique *réduit* de l'élément $r_p(\tau) \in \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D}$; il ne dépend pas du corps utilisé pour déployer $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D}$ ([Rei] 9a). On voudrait pouvoir en déduire que r_p est induit par un morphisme $G_{L/K} \overset{r}{\hookrightarrow} \mathcal{O}^\times = \mathrm{Aut}_k(\widetilde{E})$.

Si $e = 2$: alors $x_p = r_p(\tau) \in (\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D})^\times$ est un élément non trivial d'ordre 2. On a donc $x_p^2 - 1 = (x_p - 1)(x_p + 1) = 0$, et comme $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D}$ est un corps, on en déduit que $x_p = r_p(\tau) = -1 \in \mathcal{O}^\times$. Donc r_p est induit par extension des scalaires (de $\mathbb{Z}$ à $\mathbb{Q}_p$) par le morphisme $r : G_{L/K} \hookrightarrow \mathcal{O}^\times = \mathrm{Aut}_k(\widetilde{E})$ qui à τ associe la multiplication par (-1) sur $\widetilde{E}$.

Si $e \in \{3, 4, 6\}$: alors le polynôme minimal de $x_p = r_p(\tau) \in (\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D})^\times$ dans $\mathrm{GL}_2(\mathbb{Q}_{p^2})$ est $X^2 - \gamma_e X + 1$. En particulier, x_p ne peut être un élément diagonal (i.e. dans le centre) de $\mathrm{GL}_2(\mathbb{Q}_{p^2})$, sinon il ne pourrait pas être d'ordre exact e avec un déterminant égal à 1. On en déduit que x_p n'est pas dans le centre $\mathbb{Q}_p$ de $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D}$; autrement dit, $\mathbb{Q}_p$ ne contient pas de racine primitive e-ième de l'unité, et comme $p \geq 5$, on a nécessairement $p \equiv -1 \bmod e$. Donc $\mathbb{Q}_p(x_p) = \mathbb{Q}_p(\zeta_e)$ est un sous-corps commutatif maximal de $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D}$, et $\mathcal{D}$ se déploie sur $\mathbb{Q}_p(\zeta_e)$. On en déduit que $(\mathbb{Q}(\zeta_e))_\nu \otimes_{\mathbb{Q}} \mathcal{D}$ est déployée pour toutes les places ν de $\mathbb{Q}(\zeta_e)$ divisant une place non-archimédienne de $\mathbb{Q}$. De plus, comme $\mathbb{Q}(\zeta_e)$ est un corps quadratique imaginaire, il n'y a qu'une seule place au-dessus de ∞, et l'exactitude au centre de la suite exacte fondamentale

$$0 \longrightarrow \mathrm{Br}(\mathbb{Q}(\zeta_e)) \longrightarrow \bigoplus_{\nu \mid l \in \mathcal{P} \cup \{\infty\}} \mathrm{Br}((\mathbb{Q}(\zeta_e))_\nu) \overset{\oplus \mathrm{inv}_\nu}{\longrightarrow} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

montre que $\mathbb{Q}(\zeta_e) \otimes_{\mathbb{Q}} \mathcal{D}$ se déploie sur tous les corps $(\mathbb{Q}(\zeta_e))_\nu$, où ν parcourt toutes les places de $\mathbb{Q}(\zeta_e)$. Par l'injectivité dans la même suite, on voit que $\mathbb{Q}(\zeta_e) \otimes_{\mathbb{Q}} \mathcal{D}$ est déployée, ce qui signifie que $\mathcal{D}$ contient $\mathbb{Q}(x_p) \simeq \mathbb{Q}(\zeta_e)$ comme sous-corps commutatif maximal, c'est-à-dire $x_p \in \mathcal{D}$ (attention, $\mathcal{D}$ contient une infinité de racines de $X^2 - \gamma_e X + 1$, à savoir les $\{z x_p z^{-1} \ , \ z \in \mathcal{D}^\times\}$).

Comme x_p est racine de $X^2 - \gamma_e X + 1 \in \mathbb{Z}[X]$, c'est un élément de l'un des ordres maximaux de $\mathcal{D}$, mais on ne sait pas si $x_p \in \mathcal{O}^\times = \mathrm{Aut}_k(\widetilde{E})$. L'hypothèse d'une action

étendue compatible sur tous les $T_l(E)$, $l \in \mathcal{P}$, donne des $x_l = r_l(\tau) \in (\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathcal{O})^\times$ pour tout $l \in \mathcal{P}$, et ils ont tous le même polynôme minimal $X^2 - \gamma_e X + 1$. Malheureusement cela ne donne aucun renseignement sur $\mathcal{O}^\times$: si $l \neq p$, on a $\mathbb{Q}_l \otimes_{\mathbb{Q}} \mathcal{D} \simeq \mathrm{M}_2(\mathbb{Q}_l)$ et les ordres maximaux de $\mathrm{M}_2(\mathbb{Q}_l)$ sont tous des conjugués de $\mathrm{M}_2(\mathbb{Z}_l)$; si $l = p$, la $\mathbb{Q}_p$-algèbre $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D}$ contient un unique ordre maximal ([Rei]). De plus, même si l'on savait que $\mathcal{O}^\times$ contient un élément racine de $X^2 - \gamma_e X + 1$, on ne saurait pas en déduire que x_p provient par extension des scalaires d'un tel élément.

Remarque 1 : Si la condition du théorème 1 est satisfaite, le morphisme $r_p : G_{L/K} = I_{L/K} = <\tau> \hookrightarrow (\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathcal{D})^\times$ est induit par extension des scalaires soit par le morphisme $r : G_{L/K} \hookrightarrow \mathcal{O}^\times$ avec $r(\tau) = [\zeta_e]$, soit par le morphisme $r' : G_{L/K} \hookrightarrow \mathcal{O}^\times$ avec $r'(\tau) = [\zeta_e]^{-1}$.

Remarque 2 : Soit $\mathcal{O}'$ un ordre maximal de $\mathcal{D}$ contenant un élément x tel que $x^2 - \gamma_e x + 1$ (donc $x \in \mathcal{O}'^\times$). D'après Deuring ([Deu]), tout ordre maximal de $\mathcal{D}$ provient d'une courbe elliptique supersingulière (définie sur $\mathbb{F}_{p^2}$, et donc sur $k = \mathbb{F}_{p^m}$, m pair). Soit $\widetilde{E}'/k$ telle que $\mathcal{O}' = \mathrm{End}(\widetilde{E}') = \mathrm{End}_k(\widetilde{E}')$. Si $j(\widetilde{E}') \in \mathbb{F}_p$, alors l'unique idéal bilatère premier de $\mathcal{O}'$ au-dessus de $(p) = \mathcal{O}'p$ est principal, et l'on a $\mathcal{O}' = \mathrm{End}(\widetilde{E}') \simeq \mathrm{End}(\widetilde{E}'') = \mathcal{O}''$ si et seulement si $j(\widetilde{E}') = j(\widetilde{E}'')$, où $\simeq$ est la conjugaison par un idéal principal (tous les ordres maximaux de $\mathcal{D}$ sont conjugués par des idéaux à gauche ([Rei]), mais ces idéaux ne sont pas forcément principaux). Si $j(\widetilde{E}') \notin \mathbb{F}_p$, $j(\widetilde{E}') \in \mathbb{F}_{p^2}$, alors l'unique idéal bilatère premier de $\mathcal{O}'$ au-dessus de (p) n'est pas principal, et l'on a $\mathcal{O}' \simeq \mathrm{End}(\widetilde{E}'') = \mathcal{O}''$ si et seulement si $j(\widetilde{E}') = j(\widetilde{E}'')$ ou $j(\widetilde{E}') = \sigma(j(\widetilde{E}''))$, où σ est le Frobenius absolu ([Deu]). Pour $e \in \{3, 4, 6\}$, soit $\tilde{\mathrm{j}}(e) \in \mathbb{F}_p$ avec $\tilde{\mathrm{j}}(3) = \tilde{\mathrm{j}}(6) = 0$, et $\tilde{\mathrm{j}}(4) = 1728 = 12^3$; comme $(\mathcal{O}')^\times = <[-\zeta_e]>$, on a $j(\widetilde{E}') = \tilde{\mathrm{j}}(e)$. De plus, on a $(\mathcal{O})^\times = \mathrm{Aut}(\widetilde{E}) = \{\pm 1\}$ ssi $j(\widetilde{E}) \neq \tilde{\mathrm{j}}(e)$, et $(\mathcal{O})^\times = <[-\zeta_e]>$ ssi $j(\widetilde{E}) = \tilde{\mathrm{j}}(e)$. On en déduit qu'il n'y a qu'un seul ordre maximal de $\mathcal{D}$, à conjugaison par un idéal principal près, contenant un élément racine de $X^2 - \gamma_e X + 1$.

2.4.3. Enoncé détaillé du théorème :

Reprenons comme auparavant une extension finie K de $\mathbb{Q}_p$, de corps résiduel $\mathbb{F}_q$, une extension L finie galoisienne totalement ramifiée de K, et E/L une courbe elliptique ayant bonne réduction sur L, dont le polynôme caractéristique du Frobenius arithmétique agissant sur sa fibre spéciale $\widetilde{E}$ est $X^2 - a_q X + q$, de discriminant $\delta = a_q^2 - 4q$.

En regardant de plus près la précédente démonstration, on s'aperçoit que l'on peut, suivant les cas, affaiblir certaines hypothèses. Rappelons que si l'action de G_L s'étend en une action linéaire et continue de G_K sur $T_p(E)$, alors on construit un morphisme $r_p : G_{L/K} = I_{L/K} \longrightarrow (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times$ qui correspond à cette action prolongée (**2.1.4.**). De plus, si l'action de G_L s'étend en une action de G_K sur tous les $T_l(E)$, $l \in \mathcal{P}$, de sorte que l'action de W_K ainsi obtenue soit compatible, alors :
1) l'action de W_K sur $V_p(E)$ est définie sur $\mathbb{Q}$;
2) le déterminant de l'action prolongée est le caractère cyclotomique relatif à K ;
3) si $\delta \neq 0$ et $\mid I_{L/K}/\mathrm{Ker}\,(r_p) \mid = e \in \{3, 4, 6\}$, on a $j(\widetilde{E}) = \tilde{\mathrm{j}}(e)$, avec $\tilde{\mathrm{j}}(3) = \tilde{\mathrm{j}}(6) = 0$ et $\tilde{\mathrm{j}}(4) = 1728$.

On obtient alors la version suivante :

Théorème 2bis (version détaillée) :
Soit $p \geq 5$. Soit K une extension finie de $\mathbb{Q}_p$.
Soient L une extension finie galoisienne totalement ramifiée de K, et E une courbe elliptique sur L, ayant bonne réduction sur L. On suppose que l'action naturelle de G_L sur $T_p(E)$ se prolonge en une action linéaire et continue de G_K.

1) On note e l'indice de $\mathrm{Ker}\,(r_p)$ *dans $I_{L/K}$. Si l'action de G_K restreinte à W_K est définie sur $\mathbb{Q}$, alors $e \in \{1,2,3,4,6\}$.*

2) Si $e = 1$, alors E est définie sur K et a bonne réduction sur K.

3) Si $e = 2$, supposons que l'action de G_L sur $T_p(E)$ se prolonge en une action de G_K de déterminant le caractère cyclotomique. Alors E est définie sur K, et E est un twist ramifié d'ordre deux d'une courbe elliptique ayant bonne réduction sur K.

4) Si $\delta = a_q^2 - 4q = 0$ et $e \in \{3,4,6\}$, supposons que l'action de G_L sur $T_p(E)$ se prolonge en une action de G_K, de sorte que l'action de W_K ainsi obtenue soit définie sur $\mathbb{Q}$, et de déterminant le caractère cyclotomique. Alors $p \equiv -1 \bmod e$, et E est définie sur K si et seulement si le morphisme r_p provient par extension des scalaires d'un morphisme $r : I_{L/K} \to \mathrm{Aut}(\widetilde{E})$ (ce qui implique $j(\widetilde{E}) = \tilde{\mathrm{j}}(e)$, avec $\tilde{\mathrm{j}}(3) = \tilde{\mathrm{j}}(6) = 0$ et $\tilde{\mathrm{j}}(4) = 1728$).

5) Si $\delta \neq 0$ et $e \in \{3,4,6\}$, supposons que l'action de G_L se prolonge en une action de G_K sur <u>tous</u> les $T_l(E)$, $l \in \mathcal{P}$, de sorte que l'action de W_K soit compatible au sens de Weil-Deligne. Alors E est définie sur K. Si $p \equiv 1 \bmod e$, $\widetilde{E}$ est ordinaire, et si $p \equiv -1 \bmod e$, $\widetilde{E}$ est supersingulière. De plus, on a $j(\widetilde{E}) = \tilde{\mathrm{j}}(e)$, avec $\tilde{\mathrm{j}}(3) = \tilde{\mathrm{j}}(6) = 0$ et $\tilde{\mathrm{j}}(4) = 1728$.

Remarque : Il est très probable que, sous les hypothèses de *5)* et pour $p > 2d+1$, le résultat se généralise à un schéma abelien A de dimension d quelconque tel que $\mathrm{End}_k(\widetilde{A})$ est commutatif. Pour y arriver avec des méthodes similaires dans les cas où $\mathrm{End}_k(\widetilde{A})$ n'est pas commutatif, il faudrait savoir répondre à la question suivante, concernant la fibre spéciale de A : quand est-ce qu'une famille de morphismes

$$\left(I_{L/K} \xrightarrow{r_l} \left(\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{A})\right)^{\times}\right)_{l \in \mathcal{P}}$$

provient par extension des scalaires de $\mathbb{Z}$ à $\mathbb{Z}_l$ d'un morphisme $I_{L/K} \xrightarrow{r} \mathrm{Aut}_k(\widetilde{A})$? Il faudrait trouver un critère qui ne repose pas sur la connaissance de la structure de $\mathrm{End}_k(\widetilde{A})$.

2.4.4. Résultats à isogénie près :

On remarque en regardant la démonstration du théorème précédent que l'hypothèse concernant tous les $T_l(E)$, $l \in \mathcal{P}$ (comme dans le *5)* de la version détaillée), sert essentiellement à s'assurer que l'on récupère bien des isomorphismes au niveau de la fibre spéciale de E. Nous allons voir maintenant comment le résultat se modifie lorsque l'on considère une action prolongée sur le seul $T_p(E)$, ou bien sur le seul $V_p(E)$.

Rappelons les faits suivants :
- Soient E/L et E'/L deux courbes elliptiques, et soit $\psi : E \to E'$ une isogénie séparable définie sur L de degré $n = l_1^{m_1} \ldots l_r^{m_r}$, avec $r \geq 0$ (si $r = 0$ on pose $n = 1$), $l_i \in \mathcal{P}$, et $m_i \geq 1$. Alors ψ induit pour tout $l \in \mathcal{P}$ une injection G_L-équivariante $\psi_l : T_l(E) \hookrightarrow T_l(E')$, et l'on a

des isomorphismes G_L-équivariants

$$\mathrm{Ker}(\psi) \simeq \bigoplus_{1\leq i\leq r} \mathrm{Ker}(\psi)[l_i^{m_i}] \simeq \bigoplus_{1\leq i\leq r} T_{l_i}(E')/\psi_{l_i}(T_{l_i}(E)) \ .$$

- Soit E/L une courbe elliptique, et soit H un sous-groupe fini de E stable par G_L. Alors il existe une courbe elliptique E'/L, unique à L-isomorphisme près, et une L-isogénie séparable $\psi : E \to E'$ telle que $\mathrm{Ker}(\psi) = H$ (cf. par exemple [Silv 1] III, Prop. 4.12. et Rmq. 4.13.2.).

On en déduit le lemme ci-dessous, qui est bien connu :

Lemme 1 :
Soit E/L une courbe elliptique.
1) Soit $l \in \mathcal{P}$; soit T_l' un $\mathbb{Z}_l$-réseau de $V_l(E)$ stable par G_L contenant $T_l(E)$ et tel que $\mid T_l'/T_l(E) \mid = l^m$. Alors il existe une courbe elliptique E'/L , unique à L-isomorphisme près, et une L-isogénie séparable $\psi : E \to E'$ de degré l^m telle que $\psi_l(T_l') = T_l(E')$.
2) On se donne une famille de $\mathbb{Z}_l$-réseaux T_l' de $V_l(E)$, $l \in \mathcal{P}$, tels que $T_l(E)$ est un sous-réseau (d'indice fini) de T_l' pour tout l. Si $T_l(E) = T_l'$ pour presque tout $l \in \mathcal{P}$ (i.e. tous sauf un nombre fini), alors il existe une courbe elliptique E'/L , unique à L-isomorphisme près, et une L-isogénie séparable $\psi : E \to E'$ telle que $\psi_l(T_l') = T_l(E')$ pour tout $l \in \mathcal{P}$. De plus, si l'on écrit $\mid T_l'/T_l(E) \mid = l^{m_l}$, $m_l \in \mathbb{N}$, alors $m_l = 0$ presque partout, et $\deg \psi = \prod_{l\in\mathcal{P}} l^{m_l}$.

Revenons à une extension finie galoisienne L/K totalement ramifiée, et à une courbe elliptique E/L ayant bonne réduction sur L.

Supposons que l'action de G_L sur $V_p(E)$ s'étend en une action de G_K. Rappelons que cela revient à munir $D = \mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)) \in \mathrm{Ob}(\mathbf{MF_L}(\varphi))$ d'une structure d'objet de $\mathbf{MF_{L/K}}(\varphi)$; en particulier, on a un morphisme $\nu : G_{L/K} = I_{L/K} \to \mathrm{Aut}_{L_0[\varphi]}(D)$. Soit e l'indice de $\mathrm{Ker}(\nu)$ dans $I_{L/K}$; si l'action de G_K sur $V_p(E)$ stabilise $T_p(E)$, alors on peut construire un morphisme $r_p : I_{L/K} \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E}))^\times$ comme en **2.1.4.**, et le diagramme

$$\begin{array}{ccccc} & & \overset{r_p}{\to} & & \\ G_{L/K} = I_{L/K} & & & \left(\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})\right)^\times \subset \left(\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E})\right)^\times & \\ \nu \quad \downarrow & & & \downarrow \wr & \quad can \\ \mathrm{Aut}_{L_0[\varphi]}\left(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E))\right) & \underset{can}{\overset{\sim}{\to}} & & \mathrm{Aut}_{L_0[\varphi]}\left(L_0 \otimes_{W(k)} \mathbf{M}(\widetilde{E}(p))\right) & \end{array}$$

commute, de sorte que e sera aussi l'indice de $\mathrm{Ker}(r_p)$ dans $I_{L/K}$.

Soit $l \in \mathcal{P}$; une *l-isogénie* est une isogénie de degré une puissance de l.

Proposition 1 :
Soit L/K une extension finie galoisienne totalement ramifiée, et soit E/L une courbe elliptique ayant bonne réduction sur L. On suppose que l'action de G_L sur $V_p(E)$ s'étend en une

action linéaire et continue de G_K. Soit $H = \mathrm{Ker}\,(\nu)$, où $G_{L/K} \overset{\nu}{\hookrightarrow} \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)))$ est le morphisme obtenu en étendant l'action.
Alors E est p-isogène sur L à une courbe elliptique définie sur L^H et ayant bonne réduction sur L^H.

Preuve :
On pose $G_{LH} = \mathrm{Gal}(\overline{K}/L^H)$, et $I_{LH} = I(\overline{K}/L^H)$. Soit $T'_p = \sum_{g \in G_{LH}} gT_p(E)$ le $\mathbb{Z}_p$-réseau de $V_p(E)$ engendré par les transformés de $T_p(E)$ dans $V_p(E)$ par l'action prolongée de G_{LH} (ils sont bien sûr en nombre fini). Alors T'_p contient $T_p(E)$, $\mid T'_p/T_p(E) \mid = p^m$, $m \geq 0$, et T'_p est stable par G_{LH}.
D'après le lemme précédent, il existe une courbe elliptique E'/L, unique à L-isomorphisme près, et une L-isogénie séparable $\psi : E \to E'$ de degré p^m telle que $\psi_p(T'_p) = T_p(E')$; en particulier, E' a bonne réduction sur L. Cette isogénie induit un isomorphisme de $\mathbb{Q}_p[G_L]$-modules $\psi_p : V_p(E) \xrightarrow{\sim} V_p(E')$; par "transport de structure" (i.e. en posant, avec des notations évidentes, $\nu' = \mathbf{D}^*_{\mathbf{cris,L}}(\psi_p)^{-1} \circ \nu$), l'action de G_L sur $V_p(E')$ s'étend en une action de G_{LH} qui stabilise $T_p(E')$ (puisqu'elle stabilise T'_p). Donc l'action de G_L s'étend en une action de G_{LH} sur $T_p(E')$, et comme par hypothèse on a $\nu(H) = 1$, le morphisme $r_p : H \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{End}_k(\widetilde{E'}))^\times$ est trivial. On en déduit par la proposition 2 de **2.2.2.** que E' est définie sur L^H et a bonne réduction sur L^H. □

Remarque : Supposons $e(L) < p-1$, où $e(L)$ est l'indice de ramification absolu de L ; *alors, sous les hypothèses de la proposition, l'action de G_{LH} sur $V_p(E)$ stabilise $T_p(E)$, et donc E est définie sur L^H.*
En effet ([Fo 4]), pour $e(L) < p-1$, les $\mathbb{Z}_p$-réseaux de $V_p(E)$ stables par G_L sont en bijection avec les $W(k)$-réseaux M de $D = \mathbf{D}^*_{\mathbf{cris,L}}(V_p(E))$ stables par φ et vérifiant la propriété suivante : si $\mathcal{M} = M \otimes_{W(k)} O_L + \varphi M \otimes_{W(k)} p^{-1}\pi_L O_L$, l'inclusion $\mathcal{M} \cap \mathrm{Fil}^1 D_L \hookrightarrow \mathcal{M}$ induit un isomorphisme de k-espaces vectoriels

$$(\mathcal{M} \cap \mathrm{Fil}^1 D_L)/\pi_L(\mathcal{M} \cap \mathrm{Fil}^1 D_L) \simeq \mathcal{M}/(\varphi M \otimes_{W(k)} p^{-1}\pi_L O_L)$$

où π_L est une uniformisante de O_L. Les $\mathbb{Z}_p$-réseaux de $V_p(E)$ stables par l'action étendue de G_{LH} correspondent alors aux objets $(M; \mathcal{M} \cap \mathrm{Fil}^1 D_L)$ stables par $H = G_{L/L^H}$.
Il est fort possible que, sous les hypothèses de la proposition, l'action de G_{LH} sur $V_p(E)$ stabilise $T_p(E)$ pour $e(L)$ quelconque, voir le travail récent de Ch. Breuil ([Br]).

Quitte à changer E/L en une courbe *L-isogène* définie et ayant bonne réduction sur L^H, avec $H = \mathrm{Ker}\,(\nu)$, on se ramène au cas où E a bonne réduction sur L et l'action se prolonge de G_L à G_K sur $V_p(E)$ de sorte que le morphisme

$$G_{L/K} = I_{L/K} \overset{\nu}{\hookrightarrow} \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)))$$

est injectif, et $e = [L : K] \geq 2$. Nous allons régler le cas $e = 2$ facilement :

Proposition 1bis :
Soit L/K une extension ramifiée de degré 2, et soit E/L une courbe elliptique ayant bonne réduction sur L. On suppose que l'action de G_L sur $V_p(E)$ s'étend en une action de G_K,

de déterminant le caractère cyclotomique, et telle que $I_{L/K} \overset{\nu}{\hookrightarrow} \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)))$ *est injectif.*
Alors E est p-isogène sur L à une courbe elliptique définie sur K et dont la courbe tordue sur L/K a bonne réduction sur K.

Preuve :
Elle est complètement similaire à celle de la proposition 1 ci-dessus, en remplaçant L^H par K, et en utilisant le théorème 2bis (version détaillée), cas $e = 2$. Comme $\nu(I_{L/K}) = \{\pm 1\}$, la remarque précédente reste valable : si $e(L) < p - 1$, E est définie sur K. □

A partir de maintenant, on suppose que l'action de G_L sur $V_p(E)$ s'étend en une action de G_K, de déterminant le caractère cyclotomique, et définie sur $\mathbb{Q}$ (i.e. l'action de W_K sur $\Delta_p = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,p,L}}(V_p(E))$ est définie sur $\mathbb{Q}$). On suppose aussi que le morphisme donnant l'action prolongée $\nu : I_{L/K} \hookrightarrow \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)))$ est injectif, et que $e = [L : K] \geq 3$.
Alors on sait que ces hypothèses impliquent : $e \in \{3, 4, 6\}$, et $I_{L/K} =< \tau >$ est cyclique ; $\mathrm{P}_{car}(\nu(\tau)) = X^2 - \gamma_e X + 1$, où $\gamma_e = -1, 0, 1$ si $e = 3, 4, 6$ respectivement.
Par la compatibilité du système $\left(\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l,L}}(V_l(E))\right)_{l \in \mathcal{P}}$ de représentations de W_L et la semi-simplicité de chacune d'entre elles, une fois que l'on a étendu l'action de G_L à G_K sur $V_p(E)$ de façon convenable, c'est-à-dire avec un déterminant égal au caractère cyclotomique relatif à K et une action de W_K définie sur $\mathbb{Q}$, il n'y a qu'une seule manière, à isomorphisme près, d'étendre l'action sur les $V_l(E)$, $l \neq p$, de sorte que le système $\left(\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l,K}}(V_l(E))\right)_{l \in \mathcal{P}}$ de représentations de W_K soit compatible.

Le polynôme caractéristique du Frobenius arithmétique agissant sur la fibre spéciale $\widetilde{E}$ de E est noté $X^2 - a_q X + q$, de discriminant $\delta = a_q^2 - 4q \leq 0$. Rappelons que l'extension totalement ramifiée L/K de degré $e \in \{3, 4, 6\}$ est galoisienne si et seulement si $p \equiv 1 \bmod e\mathbb{Z}$ ou m pair. Soient ϕ un relèvement du Frobenius géométrique relatif à $k = \mathbb{F}_q = \mathbb{F}_{p^m}$, τ un générateur de $I_{L/K}$, et θ un relèvement de τ dans I_K ; on a $\phi^{-1}\theta\phi \equiv \theta^q \bmod I_L \equiv \theta \bmod I_L$.
Soit $\Delta_p = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,p,L}}(V_p(E))$; l'action prolongée $\rho_0 : W_K \longrightarrow \mathrm{Aut}_{L_0}(\Delta_p)$ est donnée, à isomorphisme près, par :

$$\begin{cases} \rho_0(I_L) = 1 \\ \mathrm{P}_{car}(\rho_0(\phi)) = X^2 - a_q X + q \\ \mathrm{P}_{car}(\rho_0(\theta)) = X^2 - \gamma_e X + 1 \\ \rho_0(\phi)\rho_0(\theta) = \rho_0(\theta)\rho_0(\phi) \end{cases}$$

On étend l'action de W_L à W_K sur tous les $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l,L}}(V_l(E))$, $l \neq p$, de façon compatible : cela revient à se donner, pour chaque $l \neq p$, un morphisme $\rho_0 : W_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$ avec les mêmes données que ci-dessus.
Notons $\phi_a = \phi^{-1}$: c'est un relèvement du Frobenius arithmétique relatif à k. Ainsi, pour $l \neq p$, on obtient des actions étendues $\rho_l : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(V_l(E))$ vérifiant : $\rho_l(I_L) = 1$; $\mathrm{P}_{car}(\rho_l(\phi_a)) = X^2 - a_q X + q$; $\mathrm{P}_{car}(\rho_l(\theta)) = X^2 - \gamma_e X + 1$; $\rho_l(\phi_a)\rho_l(\theta) = \rho_l(\theta)\rho_l(\phi_a)$.

Le cas $\delta = 0$ étant un peu à part, dans la suite nous allons nous borner à considérer le cas $\delta \neq 0$. Nous allons montrer que, sous toutes nos hypothèses, l'action étendue de G_K sur $V_l(E)$ stabilise $T_l(E)$ pour presque tous les $l \in \mathcal{P}$ (i.e. tous sauf un nombre fini). Pour cela,

nous aurons besoin du lemme suivant :

Lemme 2 :
On suppose $\delta \neq 0$. *Soit* $S(\delta) = \{2, p\} \cup \{l \in \mathcal{P}/\ l \mid \delta\}$: *c'est un ensemble fini. Soit* $l \in \mathcal{P} \backslash S(\delta)$.
- *Si* $\delta \notin (\mathbb{Q}_l^\times)^2$, *tous les* $\mathbb{Z}_l$*-réseaux de* $V_l(E)$ *stables par* G_L *sont homothétiques.*
- *Si* $\delta \in (\mathbb{Q}_l^\times)^2$, *soit* (e_1, e_2) *une* $\mathbb{Q}_l$*-base de diagonalisation de* $\rho_l(\phi_a)$ *dans* $V_l(E)$; *les* $\mathbb{Z}_l$*-réseaux de* $V_l(E)$ *stables par* G_L *sont, à homothétie près, les* $\mathbb{Z}_l e_1 \oplus \mathbb{Z}_l l^m e_2$, $m \in \mathbb{Z}$.

Preuve :
Pour $l \neq p$, comme $\rho_l(I_L) = 1$, un $\mathbb{Z}_l$-réseau de $V_l(E)$ est stable par G_L si et seulement si il est stable par $\rho_l(\phi_a)$. Soit $l \in \mathcal{P} \backslash S(\delta)$.

- Supposons $\delta \notin (\mathbb{Q}_l^\times)^2 \Leftrightarrow X^2 - a_q X + q$ est irréductible dans $\mathbb{Q}_l[X]$. Comme l ne divise pas δ et $l \neq 2$, δ n'est pas un carré dans $\mathbb{F}_l^\times$ (Hensel), et le polynôme $X^2 - a_q X + q$ est irréductible dans $\mathbb{F}_l[X]$. Alors la représentation modulo l :

$$\overline{\rho}_l \ : \ G_L \longrightarrow \mathrm{Aut}_{\mathbb{F}_l}\Big(T_l(E)/l\,T_l(E)\Big) = \mathrm{Aut}_{\mathbb{F}_l}(E[l])$$

est irréductible, et donc tous les réseaux de $V_l(E)$ stables par G_L sont homothétiques.

- Supposons $\delta \in (\mathbb{Q}_l^\times)^2 \Leftrightarrow X^2 - a_q X + q$ se scinde dans $\mathbb{Q}_l[X]$. Ecrivons $X^2 - a_q X + q = (X - u_1)(X - u_2)$, avec $u_1, u_2 \in \mathbb{Z}_l^\times$, et $u_1 \neq u_2$. L'automorphisme $\rho_l(\phi_a)$ est diagonalisable dans $V_l(E)$; soit (e_1, e_2) une $\mathbb{Q}_l$-base de diagonalisation, avec $\rho_l(\phi_a)e_i = u_i e_i$ pour $i = 1, 2$. Soit T un $\mathbb{Z}_l$-réseau de $V_l(E)$; à homothétie près, on peut supposer que $e_1 \in T$ et $e_1 \notin lT$. On complète en une $\mathbb{Z}_l$-base (e_1, f_2) de T, et l'on écrit $f_2 = ae_1 + be_2$, $a \in \mathbb{Q}_l$, $b \in \mathbb{Q}_l^\times$. Alors T est stable par G_L si et seulement si $\rho_l(\phi_a)f_2 \in T$; or, on a $\rho_l(\phi_a)f_2 = a(u_1 - u_2)e_1 + u_2 f_2$, donc

$$\rho_l(\phi_a)f_2 \in T \ \Leftrightarrow \ a(u_1 - u_2) \in \mathbb{Z}_l \ \Leftrightarrow \ v_l(a) \geq -v_l(u_1 - u_2)\ ,$$

où v_l est la valuation sur $\mathbb{Q}_l$ normalisée par $v_l(l) = 1$. Par ailleurs, on a $(u_1 - u_2)^2 = a_q^2 - 4q = \delta \in \mathbb{Z}_l^\times$, par hypothèse sur l ; on en déduit que T est stable par $\rho_l(\phi_a)$ si et seulement si $a \in \mathbb{Z}_l$. Dans ce cas, on a $T = \mathbb{Z}_l e_1 \oplus \mathbb{Z}_l b e_2$ avec $b \in \mathbb{Q}_l^\times$, ce qui s'écrit aussi $T = \mathbb{Z}_l e_1 \oplus \mathbb{Z}_l l^m e_2$, $m \in \mathbb{Z}$. □

Corollaire :
Sous toutes les hypothèses précédentes, l'action prolongée de G_K *sur* $V_l(E)$ *stabilise* $T_l(E)$ *pour tous les premiers* $l \in \mathcal{P} \backslash S(\delta)$, *où* $S(\delta) = \{2, p\} \cup \{l \in \mathcal{P}/\ l \mid \delta\}$ *est fini.*

Preuve :
Soit $l \in \mathcal{P} \backslash S(\delta)$; en particulier, $l \neq p$. On reprend les notations adoptées plus haut.

- Si $\delta \notin (\mathbb{Q}_l^\times)^2$, le $\mathbb{Z}_l$-réseau $T_l' = \sum_{g \in G_K} g T_l(E) = T_l(E) + \rho_l(\theta) T_l(E)$ de $V_l(E)$ est stable par G_K, et évidemment aussi par G_L. D'après le lemme précédent, T_l' et $T_l(E)$ sont homothétiques, donc $T_l(E)$ est stable par G_K (et bien sûr $T_l(E) = T_l'$).

- Si $\delta \in (\mathbb{Q}_l^\times)^2$, choisissons une $\mathbb{Q}_l$-base (e_1, e_2) de diagonalisation de $\rho_l(\phi_a)$ dans $V_l(E)$. Comme $\rho_l(\theta)$ commute avec $\rho_l(\phi_a)$, l'automorphisme $\rho_l(\theta)$ est co-diagonalisable ($\delta \neq 0$) ; donc le polynôme $X^2 - \gamma_e X + 1 = (X - \zeta_e)(X - \zeta_e^{-1})$ se scinde dans $\mathbb{Q}_l[X]$, et $\zeta_e \in \mathbb{Q}_l$ (ζ_e est une racine primitive e-ième de l'unité). On a donc $\rho_l(\theta)e_1 = \zeta_e^\epsilon e_1$ et $\rho_l(\theta)e_2 = \zeta_e^{-\epsilon} e_2$, avec

$\epsilon \in \{\pm 1\}$. D'après le lemme précédent, $T_l(E)$ est homothétique à un $\mathbb{Z}_l e_1 \oplus \mathbb{Z}_l l^m e_2$, $m \in \mathbb{Z}$, donc $T_l(E)$ est stable par $\rho_l(\theta)$, et par conséquent il est stable par G_K. □

Proposition 2 :
Soit L/K une extension galoisienne totalement ramifiée de degré $e \in \{3,4,6\}$.
Soit E/L une courbe elliptique ayant bonne réduction sur L et telle que le discriminant δ du polynôme caractéristique du Frobenius agissant sur sa fibre spéciale est non nul. Supposons que l'action de G_L sur $V_p(E)$ s'étend en une action de G_K, définie sur $\mathbb{Q}$, de déterminant le caractère cyclotomique, et telle que $I_{L/K} \overset{\nu}{\hookrightarrow} \mathrm{Aut}_{L_0[\varphi]}(\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)))$ est injectif.
Alors il existe une courbe elliptique E'/L définie sur K et une L-isogénie $E \to E'$ telle que les diviseurs premiers de son degré sont dans $S(\delta) = \{2,p\} \cup \{l \in \mathcal{P}/\ l \mid \delta\}$.

Preuve :
On étend l'action par compatibilité sur tous les $V_l(E)$, $l \in \mathcal{P}$, et l'on reprend toutes les notations précédentes.
Pour tout $l \in \mathcal{P}$, on pose $T'_l = \sum_{g \in G_K} gT_l(E)$: c'est un $\mathbb{Z}_l$-réseau G_K-stable de $V_l(E)$, contenant $T_l(E)$ comme sous-réseau d'indice fini ; notons l^{m_l}, $m_l \in \mathbb{N}$, l'indice de $T_l(E)$ dans T'_l. L'entier m_l est nul si et seulement si $T_l(E) = T'_l$, c'est-à-dire si et seulement si $T_l(E)$ est stable par G_K. D'après le corollaire précédent, pour tout $l \in \mathcal{P}\backslash S(\delta)$, on a $T_l(E) = T'_l$ (et donc $m_l = 0$). L'ensemble $S(\delta)$ étant fini, on en déduit (cf. lemme 1 du début de paragraphe) qu'il existe une courbe elliptique E'/L, unique à L-isomorphisme près, et une L-isogénie séparable $\psi : E \to E'$ telle que $\psi_l(T'_l) = T_l(E')$ pour tout $l \in \mathcal{P}$, et $\deg \psi = \prod_{l \in \mathcal{P}} l^{m_l} = \prod_{l \in S(\delta)} l^{m_l}$. L'action de G_L se prolonge à G_K sur tous les $V_l(E')$, $l \in \mathcal{P}$, de façon compatible, via les $\mathbb{Q}_l[G_L]$-isomorphismes $\psi_l : V_l(E) \xrightarrow{\sim} V_l(E')$ induits par ψ. Par construction, $T_l(E')$ est stable par cette action de G_K. Ainsi, l'action de G_L se prolonge en une action de G_K sur tous les $T_l(E')$, $l \in \mathcal{P}$, de façon compatible ; donc (théorème 2) E' est définie sur K. □

Remarques :

1) On notera que, une fois que l'on s'est donné une action de G_K prolongée (convenablement) sur $V_p(E)$, le couple (E', ψ) construit par le procédé ci-dessus est unique à L-isomorphisme près et *minimal*, dans le sens où le degré de l'isogénie $\psi : E \to E'$ vérifiant $\psi_l(T'_l) = T_l(E')$ pour tout $l \in \mathcal{P}$ est minimal.

2) Si l'on suppose en plus que l'action prolongée de G_K stabilise $T_p(E)$ (i.e. $m_p = 0$), et que p ne divise pas δ (i.e. p ne divise pas a_q, i.e. $\widetilde{E}$ ordinaire), alors ψ est une L-isogénie de degré premier à p (les diviseurs premiers de $\deg \psi$ sont soit 2, soit les premiers divisant $\delta = a_q^2 - 4q$).

3) Soient $\widetilde{E}$ et $\widetilde{E'}$ les fibres spéciales de E/L et de E'/L respectivement. Si $e \mid p-1$, alors $\widetilde{E'}$ est ordinaire, et si $e \mid p+1$, alors $\widetilde{E'}$ est supersingulière (théorème 1bis, cas 5)) ; comme E et E' sont isogènes, la même conclusion est valable pour $\widetilde{E}$.

Finalement, on obtient la généralisation suivante du théorème 2 :

Théorème 3 :

Soient K une extension finie de $\mathbb{Q}_p$, $p \geq 5$, et L une extension finie galoisienne totalement ramifiée de K. Soit E une courbe elliptique sur L, ayant bonne réduction sur L, et dont le discriminant du polynôme caractéristique du Frobenius agissant sur sa fibre spéciale $\widetilde{E}$ est non nul.

1) Si l'action de G_L s'étend en une action de G_K sur $V_p(E)$, définie sur $\mathbb{Q}$, de déterminant le caractère cyclotomique, alors E est L-isogène à une courbe elliptique définie sur K.

2) Si l'action de G_L s'étend en une action de G_K sur $T_p(E)$, définie sur $\mathbb{Q}$, de déterminant le caractère cyclotomique, et si de plus $\widetilde{E}$ est ordinaire, alors E est liée par une L-isogénie de degré premier à p à une courbe elliptique définie sur K.

CHAPITRE 3

Relèvements de courbes elliptiques sur $\mathbb{F}_p$

Dans tout ce qui suit, p est un nombre premier ≥ 5. On fixe une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$. Pour $e < p-1$, on choisit un élément $\pi_e \in \overline{\mathbb{Q}}_p$ vérifiant $\pi_e^e + p = 0$. On note $L_e = \mathbb{Q}_p(\pi_e)$; c'est une extension totalement modérément ramifiée de degré e de $\mathbb{Q}_p$, dont l'anneau des entiers est $O_{L_e} = \mathbb{Z}_p[\pi_e]$. Rappelons que si $E/\mathbb{Q}_p$ est une courbe elliptique ayant potentiellement bonne réduction, il existe $e \in \{1,2,3,4,6\}$ tel que E acquiert bonne réduction sur L_e.

L'objet de ce chapitre est de donner une description des relèvements, à isomorphisme près, d'une courbe elliptique $\widetilde{E}$ sur $\mathbb{F}_p$ fixée en un schéma elliptique sur O_{L_e}. Ensuite, pour $e \in \{2,3,4,6\}$, on détermine parmi ces relèvements ceux qui sont susceptibles d'être définis sur $\mathbb{Q}_p$, ou bien isogènes à une courbe définie sur $\mathbb{Q}_p$. Evidemment, le cas crucial est celui où $\widetilde{E}$ est supersingulière ; cette situation est étudiée de façon plus détaillée.

On fixe une courbe elliptique $\widetilde{E}/\mathbb{F}_p$. Dans un premier temps, on étudie les relèvements à isomorphisme près de $\widetilde{E}$ en un schéma elliptique sur O_{L_e} : on construit une bijection entre ceux-ci et O_{L_e}, sauf si $\widetilde{E}$ est une courbe ordinaire dont le groupe des automorphismes est strictement plus grand que $\{\pm 1\}$ (dans ce cas on obtient une bijection avec le quotient de O_{L_e} par une relation d'équivalence convenable) (**3.2.** et **3.3.1.**). Le théorème de Serre-Tate (voir [Ka]) et la théorie des modules de Dieudonné filtrés sur O_{L_e} (décrite par J.-M. Fontaine dans [Fo 4]) sont les outils essentiels permettant d'arriver aux résultats. On regarde d'abord le cas $e = 1$ (en **3.2.**), puis les cas $e > 1$ (en **3.3.**). Quand $\widetilde{E}$ est ordinaire, ce paramétrage est l'analogue des résultats de Katz ([Ka]) ou de Messing ([Me]). On étudie en même temps les groupes p-divisibles que ces relèvements fournissent, puisqu'en dernier ressort on s'intéresse aux représentations obtenues avec le module de Tate de leurs points de p-torsion.

On s'intéresse ensuite aux relèvements ci-dessus susceptibles d'être définis sur $\mathbb{Q}_p$. Soit $e \in \{2,3,4,6\}$. On suppose $\widetilde{E}/\mathbb{F}_p$ supersingulière, et telle que son groupe d'automorphismes (sur $\overline{\mathbb{F}}_p$) est strictement plus grand que $\{\pm 1\}$. Parmi les descriptions des relèvements données auparavant, on en choisit une qui est "adaptée" au groupe d'automorphismes de $\widetilde{E}$; on détermine alors les relèvements qui donnent des courbes définies sur $\mathbb{Q}_p$ (**3.3.3.**). Si l'on écrit :

$$\mathcal{O}_{L_e} = \mathbb{Z}_p[\pi_e] = \bigoplus_{0 \leq i \leq e-1} \mathbb{Z}_p \pi_e^i ,$$

les paramètres qui correspondent à une courbe définie sur $\mathbb{Q}_p$ parcourent $\mathbb{Z}_p\pi_e^i$ pour certains i que l'on détermine. Pour cela, l'outil principal est le théorème de prolongement du chapitre précédent. A la fin de **3.3.3.**, on regarde rapidement ce qui se passe lorsque $\widetilde{E}/\mathbb{F}_p$ est ordinaire ; on obtient alors des résultats à isogénie près.

Finalement, l'étude des cas supersinguliers nous permet d'achever la démonstration du théorème **2.1.** du chapitre 1, à savoir de prouver que pour chaque $e \in \{3,4,6\}$ divisant $p+1$ et pour chaque $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, il existe une courbe elliptique $E_{e,\alpha}$ définie sur $\mathbb{Q}_p$ telle que

$$\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_{e,\alpha})) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)\ ,$$

où les objets $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$ sont ceux décrits au chapitre 1 et sont deux-à-deux non-isomorphes. Ceci est l'objet du dernier paragraphe (**3.3.4.**).

3.1. Courbes elliptiques sur $\mathbb{F}_p$:

3.1.1. Classification à isomorphisme sur $\mathbb{F}_p$ près :

Soit $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. On sait que deux courbes elliptiques sur $\overline{\mathbb{F}}_p$ sont isomorphes si et seulement si elles ont le même invariant modulaire. Dans ce paragraphe, nous allons surtout considérer le cas supersingulier.

A isomorphisme sur $\overline{\mathbb{F}}_p$ près, il n'y a qu'un nombre fini de courbes elliptiques supersingulières définies sur $\overline{\mathbb{F}}_p$; en effet, on sait qu'une telle courbe possède un invariant modulaire $\tilde{\jmath}$ qui appartient à $\mathbb{F}_{p^2}$. Les $\tilde{\jmath} \in \mathbb{F}_{p^2}\backslash\{0,1728\}$ qui se réalisent comme invariant modulaire d'une courbe elliptique supersingulière (sur $\overline{\mathbb{F}}_p$) sont exactement les racines d'un certain polynôme dans $\mathbb{Z}[X]$, à racines simples, et de degré $[\frac{p}{12}]$ (voir [Deu] ou [Silv 1], Thm. 4.1.). De plus, une courbe elliptique ayant un $\tilde{\jmath} = 0$ (resp. $\tilde{\jmath} = 1728 = 12^3$) est supersingulière si et seulement si $3 \mid p+1$ (resp. $4 \mid p+1$), voir par exemple [Silv 1], exemples 4.4. et 4.5..

Etant donné un $\tilde{\jmath} \in \overline{\mathbb{F}}_p$, il existe une courbe elliptique $\widetilde{E}$ définie sur $\mathbb{F}_p(\tilde{\jmath})$ telle que $j(\widetilde{E}) = \tilde{\jmath}$; donc les $\tilde{\jmath} \in \mathbb{F}_{p^2}$ supersinguliers décrits plus haut qui correspondent à une courbe définie sur $\mathbb{F}_p$ sont ceux qui sont dans $\mathbb{F}_p$.

Exemples : à la fin du chapitre 8 de [Deu], Deuring donne un tableau des invariants modulaires supersinguliers possibles pour $p < 100$. En voici le début ($p < 50$) avec seulement les $\tilde{\jmath} \in \mathbb{F}_p$:

$p=5$, $\tilde{\jmath}=0$	$p=29$, $\tilde{\jmath}=2,25,0$
$p=7$, $\tilde{\jmath}=1728$	$p=31$, $\tilde{\jmath}=2,4,1728$
$p=11$, $\tilde{\jmath}=0,1728$	$p=37$, $\tilde{\jmath}=8$
$p=13$, $\tilde{\jmath}=5$	$p=41$, $\tilde{\jmath}=3,28,32,0$
$p=17$, $\tilde{\jmath}=8,0$	$p=43$, $\tilde{\jmath}=41,1728$
$p=19$, $\tilde{\jmath}=7,1728$	$p=47$, $\tilde{\jmath}=9,10,44,0,1728.$
$p=23$, $\tilde{\jmath}=19,0,1728$	

Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique d'invariant modulaire $\tilde{\jmath}$. Alors, à isomorphisme sur $\mathbb{F}_p$

près, les autres courbes elliptiques $\widetilde{E}'/\mathbb{F}_p$ telles que $j(\widetilde{E}') = j(\widetilde{E}) = \tilde{\jmath}$ sont classifiées par

$$\mathrm{Twist}((\widetilde{E},\mathbf{0}),\mathbb{F}_p) \simeq \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^{n(\tilde{\jmath})} \simeq \mu_{n(\tilde{\jmath})}(\mathbb{F}_p) ,$$

où $n(\tilde{\jmath}) = 2$ si $\tilde{\jmath} \neq 0, 1728$, $n(0) = 6$, $n(1728) = 4$, et $\mu_n(\mathbb{F}_p)$ est le groupe des racines n-ièmes de l'unité contenues dans $\mathbb{F}_p$ (voir [Silv 1], 10.5., en particulier Prop. 5.4. et Cor. 5.4.1.). Si $\widetilde{E}$ est supersingulière, $\tilde{\jmath} = 0$ (resp. $\tilde{\jmath} = 1728$) implique $3 \mid p+1$ (resp. $4 \mid p+1$), et donc $\mu_6(\mathbb{F}_p) = \{\pm 1\}$ (resp. $\mu_4(\mathbb{F}_p) = \{\pm 1\}$) ; on voit que dans tous les cas $\mathrm{Twist}((\widetilde{E},\mathbf{0}),\mathbb{F}_p)$ est d'ordre 2. On en déduit que si l'on fixe un $\tilde{\jmath} \in \mathbb{F}_p$ supersingulier, alors, à isomorphisme sur $\mathbb{F}_p$ près, il y a deux courbes elliptiques définies sur $\mathbb{F}_p$ ayant $\tilde{\jmath}$ comme invariant modulaire (l'une est un twist d'ordre 2 de l'autre, et elles deviennent isomorphes sur $\mathbb{F}_{p^2}$).

Remarque 1 : Toutes les courbes supersingulières $\widetilde{E}$ sur $\mathbb{F}_p$, $p \geq 5$, sont $\mathbb{F}_p$-isogènes. En effet, la trace $a_p = a_p(\widetilde{E}) \in \mathbb{Z}$ du Frobenius agissant sur $\widetilde{E}$ vérifie $|a_p| \leq 2\sqrt{p}$, et aussi $p \mid a_p$ puisqu'elle est supersingulière ; lorsque $p \geq 5$, ceci implique $a_p = 0$. Puis $\widetilde{E}/\mathbb{F}_p$ et $\widetilde{E}'/\mathbb{F}_p$ sont $\mathbb{F}_p$-isogènes si et seulement si $a_p(\widetilde{E}) = a_p(\widetilde{E}')$, avec des notations évidentes ([Ta]).

Remarque 2 : Soit $\widetilde{E}/\mathbb{F}_p$ supersingulière d'invariant modulaire $\tilde{\jmath} \in \mathbb{F}_p$; alors $\mathrm{End}(\widetilde{E}) = \mathrm{End}_{\overline{\mathbb{F}}_p}(\widetilde{E}) = \mathrm{End}_{\mathbb{F}_{p^2}}(\widetilde{E})$ est un ordre maximal $\mathcal{O}$ dans l'algèbre de quaternions $\mathcal{D}$ sur $\mathbb{Q}$ qui ne se ramifie qu'en p et à l'infini, dans lequel l'unique idéal bilatère au-dessus de (p) est principal. Réciproquement, étant donné un ordre maximal $\mathcal{O}$ de $\mathcal{D}$ dans lequel l'unique idéal bilatère au-dessus de (p) est principal, il existe un et un seul invariant supersingulier $\tilde{\jmath}$ qui correspond à $\mathcal{O}$, et $\tilde{\jmath} \in \mathbb{F}_p$. Par contre, si $\tilde{\jmath} \in \mathbb{F}_{p^2}$, $\tilde{\jmath} \notin \mathbb{F}_p$, est un invariant supersingulier non rationnel, la situation est différente, voir [Deu].

Remarque 3 : Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique, avec $j(\widetilde{E}) = \tilde{\jmath}$. Alors, pour tout corps k tel que $\mathbb{F}_p \subset k \subset \overline{\mathbb{F}}_p$, on a

$$\mathrm{Aut}_k(\widetilde{E}) \simeq \mu_{n(\tilde{\jmath})}(k) ,$$

où, comme plus haut, $n(\tilde{\jmath}) = 2$ (resp. 4,6) si $\tilde{\jmath} \neq 0, 1728$ (resp. $\tilde{\jmath} = 1728$, $\tilde{\jmath} = 0$), et $\mu_n(k)$ est le groupe des racines n-ièmes de l'unité contenues dans k. En particulier, on voit que $\mathrm{Aut}_{\overline{\mathbb{F}}_p}(\widetilde{E}) = \mathrm{Aut}_{\mathbb{F}_{p^2}}(\widetilde{E})$, et que $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E})$ est toujours d'ordre 2 lorsque $\widetilde{E}/\mathbb{F}_p$ est supersingulière.

Remarque 4 : $\widetilde{E}/\mathbb{F}_p$ est ordinaire si et seulement si p ne divise pas $a_p(\widetilde{E})$, ce qui équivaut à $a_p \neq 0$. Une courbe elliptique avec un invariant modulaire $j(\widetilde{E}) = 0$ (resp. $j(\widetilde{E}) = 1728$) est ordinaire si et seulement si $3 \mid p-1$ (resp. $4 \mid p-1$), et alors $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) \simeq \mu_6(\mathbb{F}_p)$ (resp. $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) \simeq \mu_4(\mathbb{F}_p)$) est d'ordre 6 (resp. d'ordre 4) ; dans tous les autres cas, $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) = \{\pm 1\}$ est d'ordre 2.

3.1.2. Groupes p-divisibles sur $\mathbb{F}_p$ associés :

Soit $k \subset \overline{\mathbb{F}}_p$ un corps fini. On note σ le Frobenius absolu agissant (par $x \mapsto x^p$) sur k et sur $W(k)$, l'anneau des vecteurs de Witt à coefficients dans k.
Soit Γ un groupe p-divisible (ou de Barsotti-Tate) sur k. On note $M = \mathrm{M}_k(\Gamma) = \mathrm{M}(\Gamma) = \mathrm{Hom}_{\mathbf{D}_k}(\Gamma, C\widehat{W}(k))$ son module de Dieudonné sur k (voir [Fo 4]) : c'est un $W(k)$-module

libre de rang fini, muni d'un opérateur de Frobenius σ-semi-linéaire φ vérifiant $pM \subset \varphi M$. Rappelons que le foncteur $\mathbf{M}$ induit une anti-équivalence de catégories entre la catégorie des groupes p-divisibles sur k et celle des $W(k)$-modules libres de rang fini munis d'un opérateur φ comme ci-dessus ([Fo 4], III Prop.6.1. et Rmq.3 qui suit). On notera $\mathbf{MD}_k$ cette dernière catégorie.

Soient $k = \mathbb{F}_q = \mathbb{F}_{p^m}$ et $\widetilde{E}/k$ une courbe elliptique, $\widetilde{E}(p)$ son groupe p-divisible ; soit $X^2 - a_q X + q$ le polynôme caractéristique du Frobenius arithmétique relatif à k agissant sur $\widetilde{E}$. Alors $M = \mathbf{M}(\widetilde{E}(p))$ est un $W(k)$-module libre de rang 2, muni d'un opérateur φ σ-semi-linéaire vérifiant :

$$\varphi^{2m} - a_q \varphi^m + q = 0 \ .$$

En particulier, si $\widetilde{E}$ est une courbe elliptique sur $k = \mathbb{F}_p$ supersingulière (resp. ordinaire), alors $a_p(\widetilde{E}) = 0$ (resp. $a_p(\widetilde{E}) \in \mathbb{Z}_p^\times$), et $M = \mathbf{M}(\widetilde{E}(p))$ est un $\mathbb{Z}_p$-module libre de rang 2 muni d'un Frobenius $\mathbb{Z}_p$-linéaire φ vérifiant $\varphi^2 + p = 0$ (resp. $\varphi^2 - a_p(\widetilde{E})\varphi + p = 0$).

Lemme 1 :
Soit a tel que $a = 0$ ou $a \in \mathbb{Z}_p^\times$. Tous les modules de Dieudonné sur $\mathbb{F}_p$ libres de rang 2 tels que $\varphi^2 - a\varphi + p = 0$ sont isomorphes sur $\mathbb{F}_p$.

Remarque : ces objets sont tous clairement isogènes sur $\mathbb{F}_p$.

Preuve :
1) Soit M un tel module de Dieudonné avec $a = 0$. Comme $\varphi^2 + p = 0$, on a $pM \subset \varphi M \subset M$ et ces inclusions sont strictes. Posons $k = \mathbb{F}_p$.
Choisissons un $x \in M$ tel que $x \notin \varphi M$; alors $\varphi x \notin \varphi^2 M = pM$, et $(x, \varphi x)$ est une $W(k)$-base de M. En effet, si $ax + b\varphi x \in pM$, alors $ax \in \varphi M$ et l'on doit avoir $a \in pW(k)$, puisque $x \notin \varphi M$. On en déduit que $b\varphi x \in pM$, et l'on doit avoir $b \in pW(k)$, puisque $\varphi x \notin pM$. Donc ($x \bmod pM, \varphi x \bmod pM$) est une base du k-espace vectoriel M/pM, et par Nakayama on a $M = W(k)x \oplus W(k)\varphi x$. L'opérateur φ envoie x sur φx, et φx sur $-px$.
Maintenant si M' (muni de φ') est un autre module de Dieudonné avec les mêmes propriétés, on écrit $M' = W(k)x' \oplus W(k)\varphi' x'$, avec $x' \notin \varphi' M'$. L'application $W(k)$-linéaire de M dans M' définie par $x \mapsto x'$, $\varphi x \mapsto \varphi' x'$, commute clairement aux Frobenius et fournit ainsi un isomorphisme de modules de Dieudonné sur k.
2) Soit M un tel module de Dieudonné avec $a \in \mathbb{Z}_p^\times$. Le polynôme $X^2 - aX + p$ est scindé à racines simples dans $\mathbb{Q}_p[X]$ (Hensel) ; il existe donc un unique $u = u(a) \in \mathbb{Z}_p^\times$ tel que $X^2 - aX + p = (X - u)(X - u^{-1}p)$. Pour prouver le lemme, il suffit de montrer qu'il existe une $\mathbb{Z}_p$-base (e_1, e_2) de M telle que $\varphi(e_1) = ue_1$ et $\varphi(e_2) = u^{-1}pe_2$.
Soit $D = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} M$; alors φ s'étend $\mathbb{Q}_p$-linéairement à D, et φ est diagonalisable dans D. Soit (e_1, e_2) une $\mathbb{Q}_p$-base de diagonalisation, avec $\varphi(e_1) = ue_1$ et $\varphi(e_2) = u^{-1}pe_2$; quitte à multiplier chaque e_i, $i = 1, 2$, par une puissance de p convenable, on peut supposer $e_i \in M$ et $e_i \notin pM$. Notons $\overline{\varphi} : M/pM \to M/pM$ l'application $\mathbb{F}_p$-linéaire déduite de φ ; avec des notations évidentes, on a : $\overline{\varphi}^2 - \overline{a}\overline{\varphi} = \overline{\varphi}(\overline{\varphi} - \overline{u}\,\mathrm{Id}) = 0$, et $\overline{\varphi}(\overline{e}_1) = \overline{u}\,\overline{e}_1$, $\overline{\varphi}(\overline{e}_2) = 0$, avec $\overline{e}_i \neq 0$, $i = 1, 2$. Donc $(\overline{e}_1, \overline{e}_2)$ est une $\mathbb{F}_p$-base de diagonalisation de $\overline{\varphi}$ dans M/pM. En particulier, par Nakayama, (e_1, e_2) est une $\mathbb{Z}_p$-base de M. □

Corollaire :
Soit $p \geq 5$. Deux courbes elliptiques sur $\mathbb{F}_p$ qui sont $\mathbb{F}_p$-isogènes ont des groupes p-divisibles

isomorphes sur $\mathbb{F}_p$.

Remarque : Soient $\widetilde{E}$ et $\widetilde{E}'$ deux courbes sur $\mathbb{F}_p$ qui sont $\mathbb{F}_p$-isogènes. L'isomorphisme canonique $\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{E}, \widetilde{E}') \simeq \mathrm{Hom}_{p-div}(\widetilde{E}(p), \widetilde{E}'(p))$ ainsi que le corollaire précédent montrent qu'il existe une isogénie de degré premier à p liant $\widetilde{E}$ et $\widetilde{E}'$.

Soit $K_0 = \mathrm{Frac}(W(k))$. Soit Γ un groupe p-divisible sur k ; alors $K_0 \otimes_{W(k)} \mathbf{M}(\Gamma)$ est un K_0-espace vectoriel de dimension finie, muni d'un opérateur de Frobenius σ-semi-linéaire injectif défini par : $\varphi(\lambda \otimes x) = \sigma(\lambda) \otimes \varphi x$, pour $\lambda \in K_0$ et $x \in \mathbf{M}(\Gamma)$.
Le foncteur $\Gamma \mapsto K_0 \otimes_{W(k)} \mathbf{M}(\Gamma) = \mathbf{D}(\Gamma)$ établit une anti-équivalence de catégories entre la catégorie des groupes p-divisibles sur k *à isogénie près* et celle des K_0-espaces vectoriels de dimension finie munis d'un opérateur de Frobenius comme ci-dessus. Donc l'objet $\mathbf{D}(\Gamma)$ caractérise la classe d'isogénie de Γ sur k, et $\mathbf{M}(\Gamma)$ est un $W(k)$-réseau de $\mathbf{D}(\Gamma)$ stable par φ. Réciproquement, tout $W(k)$-réseau M' de $\mathbf{D}(\Gamma)$ stable par φ est un $W(k)$-module libre de rang fini muni d'un opérateur de Frobenius, et donc il existe un groupe p-divisible Γ' sur k (unique à k-isomorphisme près) tel que $\mathbf{M}(\Gamma') = M'$; alors $\mathbf{D}(\Gamma') = \mathbf{D}(\Gamma)$, et Γ' et Γ sont isogènes sur k.

Lemme 2 :
Soit M un module de Dieudonné sur $\mathbb{F}_{p^2}$ libre de rang 2 tel que $\varphi^2 + p = 0$. Les $W(\mathbb{F}_{p^2})$-réseaux de $K_0 \otimes_{W(\mathbb{F}_{p^2})} M$ stables par φ sont les $\varphi^n M$, $n \in \mathbb{Z}$.

Preuve :
Posons $k = \mathbb{F}_{p^2}$. Soit M' un $W(k)$-réseau de $K_0 \otimes_{W(k)} M$ stable par φ. Comme $\varphi^2 = -p$, il suffit de montrer que, à homothétie près, $M' = M$ ou $M' = \varphi M$.
Rappelons que si $x \in M$ est tel que $x \notin \varphi M$, alors $M = W(k)x \oplus W(k)\varphi x$ (lemme 1). Choisissons alors un $x' \in M'$ tel que $x' \notin \varphi M'$. Quitte à multiplier M' par une puissance de p convenable, on peut supposer $x' \in M$ et $x' \notin pM$. Comme on a des inclusions strictes $pM \subset \varphi M \subset M$, deux cas se présentent :
- soit $x' \in \varphi M$ (et $x' \notin pM = \varphi(\varphi M)$), d'où $\varphi M = W(k)x' \oplus W(k)\varphi x' = M'$;
- soit $x' \notin \varphi M$ (et $x' \in M$), d'où $M = W(k)x' \oplus W(k)\varphi x' = M'$. □

3.2. Relèvements sur $\mathbb{Z}_p$: le cas $e = 1$.

3.2.1. Le théorème de Serre-Tate :

On note $\mathcal{SE}_{\mathbb{Z}_p}$ la catégorie des schémas elliptiques sur $\mathbb{Z}_p$. On désigne par $\mathcal{C}_{\mathbb{Z}_p}$ la catégorie suivante :
- les objets sont les triplets $(\widetilde{B}, \Gamma, \nu)$, où $\widetilde{B}$ est une courbe elliptique sur $\mathbb{F}_p$, Γ est un groupe p-divisible sur $\mathbb{Z}_p$, et $\nu : \widetilde{B}(p) \xrightarrow{\sim} \widetilde{\Gamma} = \Gamma \times_{\mathbb{Z}_p} \mathbb{F}_p$ est un isomorphisme de groupes p-divisibles sur $\mathbb{F}_p$;
- un morphisme $(\widetilde{B}, \Gamma, \nu) \to (\widetilde{B}', \Gamma', \nu')$ est un couple (γ, ψ), où $\gamma : \widetilde{B} \to \widetilde{B}'$ est un morphisme de courbes elliptiques sur $\mathbb{F}_p$ et $\psi : \Gamma \to \Gamma'$ est un morphisme de groupes p-divisibles sur $\mathbb{Z}_p$,

tels que le diagramme

$$\begin{array}{ccccc} & & \gamma(p) & & \\ & \widetilde{B}(p) & \to & \widetilde{B}'(p) & \\ \nu & \downarrow & & \downarrow & \nu' \\ & \widetilde{\Gamma} & \underset{\widetilde{\psi}}{\to} & \widetilde{\Gamma}' & \end{array}$$

commute. Le théorème de Serre-Tate (voir [Ka] et **2.1.4.**) implique que le foncteur **ST**

$$\begin{cases} \mathcal{SE}_{\mathbb{Z}_p} & \to & \mathcal{C}_{\mathbb{Z}_p} \\ A & \mapsto & (\widetilde{A}, A(p), \nu_{can}) \end{cases}$$

où $\widetilde{A} = A \times_{\mathbb{Z}_p} \mathbb{F}_p$, et ν_{can} est l'isomorphisme canonique $\widetilde{A}(p) \simeq \widetilde{A(p)}$, établit une équivalence de catégories entre $\mathcal{SE}_{\mathbb{Z}_p}$ et $\mathcal{C}_{\mathbb{Z}_p}$.

Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique. On dit qu'un schéma elliptique $A/\mathbb{Z}_p$ *relève* $\widetilde{E}$ s'il existe un $\mathbb{F}_p$-isomorphisme $f : \widetilde{A} \xrightarrow{\sim} \widetilde{E}$. On note $\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})$ la sous-catégorie pleine de $\mathcal{SE}_{\mathbb{Z}_p}$ dont les objets sont les schémas elliptiques sur $\mathbb{Z}_p$ relevant $\widetilde{E}$, et $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ la sous-catégorie pleine de $\mathcal{C}_{\mathbb{Z}_p}$ dont les objets sont les triplets $(\widetilde{E}, \Gamma, \nu)$. Soit A un objet de $\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})$, et soit $f : \widetilde{A} \xrightarrow{\sim} \widetilde{E}$ un $\mathbb{F}_p$-isomorphisme. Alors

$$\mathbf{ST}(A) = (\widetilde{A}, A(p), \nu_{can}) \simeq (\widetilde{E}, A(p), \nu_{can} \circ f(p)^{-1}) \quad \text{dans} \quad \mathcal{C}_{\mathbb{Z}_p}$$

par $(f, \mathrm{Id}_{A(p)})$; ainsi, $\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})$ est la sous-catégorie pleine de $\mathcal{SE}_{\mathbb{Z}_p}$ formée des objets A tels qu'il existe un objet X de $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ tel que $\mathbf{ST}(A) \simeq X$ dans $\mathcal{SE}_{\mathbb{Z}_p}$. La classe d'isomorphisme dans $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ de $(\widetilde{E}, A(p), \nu_{can} \circ f(p)^{-1})$ ne dépend pas du choix de f ; en effet, si $f' : \widetilde{A} \xrightarrow{\sim} \widetilde{E}$ est un autre $\mathbb{F}_p$-isomorphisme, alors $(f' \circ f^{-1}, \mathrm{Id}_{A(p)})$ est un isomorphisme de $(\widetilde{E}, A(p), \nu_{can} \circ f(p)^{-1})$ sur $(\widetilde{E}, A(p), \nu_{can} \circ f'(p)^{-1})$. De plus, si $A, A' \in \mathrm{Ob}(\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E}))$ et si $f : \widetilde{A} \xrightarrow{\sim} \widetilde{E}$, $f' : \widetilde{A}' \xrightarrow{\sim} \widetilde{E}$ sont des $\mathbb{F}_p$-isomorphismes, alors on a un isomorphisme

$$\mathrm{Hom}_{\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})}(A, A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})}\Big((\widetilde{E}, A(p), \nu_{can} \circ f(p)^{-1}), (\widetilde{E}, A'(p), \nu'_{can} \circ f'(p)^{-1})\Big)$$

obtenu en appliquant d'abord le foncteur pleinement fidèle **ST**, puis en composant avec $(\gamma, \psi) \mapsto (f' \circ \gamma \circ f^{-1}, \psi)$. Donc le foncteur **ST** induit une bijection entre les classes d'isomorphisme de $\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})$ et celles de $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$.

3.2.2. Modules de Dieudonné filtrés sur $\mathbb{Z}_p$:

Nous allons utiliser la théorie des modules de Dieudonné filtrés sur $\mathbb{Z}_p$ telle qu'elle est décrite par J.-M. Fontaine dans [Fo 4], IV,§ 1 pour étudier les relèvements de $M = \mathbf{M}(\widetilde{E}(p))$ pour $\widetilde{E}/\mathbb{F}_p$ fixée.

On définit la catégorie $\mathbf{MD}_{\mathbb{Z}_p}$ suivante :
- les objets sont les couples $(M, \mathcal{L})$, où M est un $\mathbb{Z}_p$-module libre de rang fini, muni d'un

opérateur de Frobenius $\mathbf{Z}_p$-linéaire φ tel que $pM \subset \varphi M$ (i.e. M est un objet de $\mathbf{MD}_{\mathbf{F}_p}$), et $\mathcal{L}$ est un sous-$\mathbf{Z}_p$-module de M tel que l'inclusion $\mathcal{L} \hookrightarrow M$ induit un isomorphisme de $\mathbf{F}_p$-espaces vectoriels

$$\mathcal{L}/p\mathcal{L} \simeq M/\varphi M \qquad (*)$$

Quand le couple $(M, \mathcal{L})$ vérifie $(*)$, on dit qu'il est admissible.
- un morphisme $(M, \mathcal{L}) \to (M', \mathcal{L}')$ entre deux tels objets est une application $\mathbf{Z}_p$-linéaire qui commute aux Frobenius et envoie $\mathcal{L}$ dans $\mathcal{L}'$.

Soit Γ un groupe p-divisible sur $\mathbf{Z}_p$, et $\widetilde{\Gamma} = \Gamma \times_{\mathbf{Z}_p} \mathbf{F}_p$. Dans [Fo 4] III.6.4. et IV.1.1., J.-M. Fontaine construit un sous-$\mathbf{Z}_p$-module $\mathcal{L}(\Gamma)$ de $\mathbf{M}(\widetilde{\Gamma})$ qui vérifie $(*)$, de sorte que le couple $(\mathbf{M}(\widetilde{\Gamma}), \mathcal{L}(\Gamma))$ est un objet de $\mathbf{MD}_{\mathbf{Z}_p}$. L'association

$$\Gamma \mapsto \mathbf{M}_{\mathbf{Z}_p}(\Gamma) = (\mathbf{M}(\widetilde{\Gamma}), \mathcal{L}(\Gamma))$$

est fonctorielle, et induit une anti-équivalence entre la catégorie des groupes p-divisibles sur $\mathbf{Z}_p$ et $\mathbf{MD}_{\mathbf{Z}_p}$ ([Fo 4], Prop. IV.1.6.).

Soit M un objet de $\mathbf{MD}_{\mathbf{F}_p}$. Les relèvements de M en un objet de $\mathbf{MD}_{\mathbf{Z}_p}$ sont alors en correspondance bijective avec les sous-$\mathbf{Z}_p$-modules $\mathcal{L}$ de rang 1 de M tels que l'inclusion $\mathcal{L} \hookrightarrow M$ induit un isomorphisme de $\mathbf{F}_p$-espaces vectoriels

$$\mathcal{L}/p\mathcal{L} \simeq M/\varphi M \qquad (*)\ .$$

3.2.3. Relèvements sur $\mathbf{Z}_p$ supersinguliers :

Dans tout ce paragraphe, *on fixe $\widetilde{E}/\mathbf{F}_p$ supersingulière.*
On écrit $M = \mathbf{M}(\widetilde{E}(p))$, et, comme en **3.1.2.** lemme 1, on choisit une $\mathbf{Z}_p$-base (e_1, e_2) de M telle que $\varphi e_1 = e_2$ et $\varphi e_2 = -pe_1$; cela revient à choisir un générateur e_1 du $\mathbf{Z}_p[\varphi]$-module M, ou bien, de façon équivalente, à choisir un $e_1 \in M$ tel que $e_1 \notin \varphi M$. Posons $\mathcal{L} = (\lambda e_1 + \mu e_2)\mathbf{Z}_p$ avec $\lambda, \mu \in \mathbf{Z}_p$, $(\lambda, \mu) \neq (0,0)$. Alors la flèche naturelle

$$\mathcal{L} = (\lambda e_1 + \mu e_2)\mathbf{Z}_p \xrightarrow{proj} M/\varphi M = (\mathbf{Z}_p e_1 \oplus \mathbf{Z}_p e_2) \,/\, (\mathbf{Z}_p p e_1 \oplus \mathbf{Z}_p e_2) \simeq \mathbf{F}_p(e_1 \bmod pM)$$

est surjective ssi elle est non nulle, ce qui équivaut à $\mathcal{L} \not\subset \varphi M$, c'est-à-dire $\lambda \in \mathbf{Z}_p^\times$. Dans ce cas, on a $\mathcal{L} \cap \varphi M = p\mathcal{L}$. Donc la condition $(*)$ est satisfaite si et seulement si

$$\mathcal{L} = \mathcal{L}(\beta) = (e_1 + \beta e_2)\mathbf{Z}_p \quad , \quad \beta \in \mathbf{Z}_p\ .$$

Soit $(\widetilde{E}, \Gamma, \nu) \in \mathrm{Ob}(\mathcal{C}_{\mathbf{Z}_p}(\widetilde{E}))$: Γ est un groupe p-divisible sur $\mathbf{Z}_p$, et $\nu : \widetilde{E}(p) \xrightarrow{\sim} \widetilde{\Gamma}$ est un isomorphisme de groupes p-divisibles sur $\mathbf{F}_p$. Alors $\mathbf{M}_{\mathbf{Z}_p}(\Gamma) = (\mathbf{M}(\widetilde{\Gamma}), \mathcal{L}(\Gamma))$ est un objet de $\mathbf{MD}_{\mathbf{Z}_p}$, et $\mathbf{M}(\nu) : \mathbf{M}(\widetilde{\Gamma}) \xrightarrow{\sim} \mathbf{M}(\widetilde{E}(p)) = M$ est un isomorphisme dans $\mathbf{MD}_{\mathbf{F}_p}$, d'où $\mathbf{M}(\nu)(\varphi\mathbf{M}(\widetilde{\Gamma})) = \varphi M$. Donc $\mathbf{M}(\nu)(\mathcal{L}(\Gamma))$ est un sous-$\mathbf{Z}_p$-module de rang 1 de $\mathbf{M}(\nu)(\mathbf{M}(\widetilde{\Gamma})) = M$ tel que l'inclusion induit un isomorphisme de $\mathbf{F}_p$-espaces vectoriels

$$\mathbf{M}(\nu)(\mathcal{L}(\Gamma)) \,/\, p\mathbf{M}(\nu)(\mathcal{L}(\Gamma)) \simeq M/\varphi M\ .$$

Donc, d'après ce que l'on a vu ci-dessus, et via le choix d'une base de M convenable, il existe un unique $\beta \in \mathbb{Z}_p$ tel que $\mathbf{M}(\nu)(\mathcal{L}(\Gamma)) = \mathcal{L}(\beta)$.

Proposition 1 :
Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique supersingulière. Via le choix d'un générateur du $\mathbb{Z}_p[\varphi]$-module $\mathbf{M}(\widetilde{E}(p))$, l'association décrite ci-dessus

$$\begin{cases} \mathcal{C}_{\mathbb{Z}_p}(\widetilde{E}) & \to & \mathbb{Z}_p \\ (\widetilde{E}, \Gamma, \nu) & \mapsto & \beta \text{ tel que } \mathcal{L}(\beta) = \mathbf{M}(\nu)(\mathcal{L}(\Gamma)) \end{cases}$$

induit une bijection entre les classes d'isomorphisme dans $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ et $\mathbb{Z}_p$.

Remarque 1 : Et donc, en composant avec **ST** (cf. **3.2.1.**), on obtient une bijection entre les classes d'isomorphisme dans $\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})$ et $\mathbb{Z}_p$.

Remarque 2 : Le choix d'un autre générateur du $\mathbb{Z}_p[\varphi]$-module $M = \mathbf{M}(\widetilde{E}(p))$ change l'invariant β. Plus précisément, si $e_1' \in M$ et $e_1' \notin \varphi M$, il existe $a \in \mathbb{Z}_p^\times$ et $b \in \mathbb{Z}_p$ tels que $e_1' = ae_1 + be_2$, et $e_2' = \varphi e_1' = -pbe_1 + ae_2$; alors, si l'on écrit $\mathcal{L}(\beta') = (e_1' + \beta' e_2')\mathbb{Z}_p = (e_1 + \beta e_2)\mathbb{Z}_p$, on obtient que $\beta = (a - pb\beta')^{-1}(b + a\beta')$.

Nous allons d'abord prouver le lemme suivant :

Lemme 1 :
Soient $(\widetilde{E}, \Gamma, \nu)$ et $(\widetilde{E}, \Gamma', \nu')$ deux objets de $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$, tels que, dans la description faite ci-dessus, $\mathbf{M}(\nu)(\mathcal{L}(\Gamma)) = \mathcal{L}(\beta)$ et $\mathbf{M}(\nu')(\mathcal{L}(\Gamma')) = \mathcal{L}(\beta')$, avec $\beta, \beta' \in \mathbb{Z}_p$. Alors on a un isomorphisme

$$\mathrm{Hom}_{\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})}\Big((\widetilde{E}, \Gamma, \nu), (\widetilde{E}, \Gamma', \nu')\Big) \simeq \{ \gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E}) \ / \ \mathbf{M}(\gamma(p))(\mathcal{L}(\beta')) \subset \mathcal{L}(\beta) \} .$$

Preuve du lemme :
Par définition de la catégorie $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$, les morphismes de $(\widetilde{E}, \Gamma, \nu)$ dans $(\widetilde{E}, \Gamma', \nu')$ sont les couples (γ, ψ), avec $\gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E})$, $\psi \in \mathrm{Hom}_{\mathbb{Z}_p}(\Gamma, \Gamma')$, et vérifiant $\nu' \circ \gamma(p) = \widetilde{\psi} \circ \nu$. Par la pleine fidélité des foncteurs $\mathbf{M} = \mathbf{M}_{\mathbb{F}_p}$ et $\mathbf{M}_{\mathbb{Z}_p}$, ces couples sont en bijection avec les (γ, ξ), où $\gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E})$, $\xi \in \mathrm{Hom}_{\mathbf{MD}_{\mathbb{Z}_p}}(\mathbf{M}_{\mathbb{Z}_p}(\Gamma'), \mathbf{M}_{\mathbb{Z}_p}(\Gamma))$, et $\mathbf{M}(\gamma(p)) \circ \mathbf{M}(\nu') = \mathbf{M}(\nu) \circ \xi$. Par définition de la catégorie $\mathbf{MD}_{\mathbb{Z}_p}$, ces conditions sur ξ sont équivalentes à : $\xi \in \mathrm{Hom}_{\mathbf{MD}_{\mathbb{F}_p}}(\mathbf{M}(\widetilde{\Gamma}'), \mathbf{M}(\widetilde{\Gamma}))$, avec $\xi = \mathbf{M}(\nu^{-1}) \circ \mathbf{M}(\gamma(p)) \circ \mathbf{M}(\nu')$ et $\xi(\mathcal{L}(\Gamma')) \subset \mathcal{L}(\Gamma)$. Finalement, en écrivant $\mathbf{M}(\nu)(\mathcal{L}(\Gamma)) = \mathcal{L}(\beta)$ et $\mathbf{M}(\nu')(\mathcal{L}(\Gamma')) = \mathcal{L}(\beta')$, on voit que les morphismes de $(\widetilde{E}, \Gamma, \nu)$ dans $(\widetilde{E}, \Gamma', \nu')$ sont en bijection avec les $\gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E})$ tels que $\mathbf{M}(\gamma(p))(\mathcal{L}(\beta')) \subset \mathcal{L}(\beta)$. □

Preuve de la proposition :
Montrons d'abord la surjectivité. Soit $\beta \in \mathbb{Z}_p$; alors $(M, \mathcal{L}(\beta)) = (\mathbf{M}(\widetilde{E}(p)), \mathcal{L}(\beta))$ est un objet de $\mathbf{MD}_{\mathbb{Z}_p}$. Il existe donc un groupe p-divisible J_β sur $\mathbb{Z}_p$ et un isomorphisme $\xi_\beta : \mathbf{M}_{\mathbb{Z}_p}(J_\beta) \xrightarrow{\sim} (M, \mathcal{L}(\beta))$ dans $\mathbf{MD}_{\mathbb{Z}_p}$; en particulier, on a $\xi_\beta(\mathcal{L}(J_\beta)) = \mathcal{L}(\beta)$. On note encore $\xi_\beta : \mathbf{M}(\widetilde{J}_\beta) \xrightarrow{\sim} M = \mathbf{M}(\widetilde{E}(p))$ l'isomorphisme de modules de Dieudonné sur $\mathbb{F}_p$ qu'il induit ; il existe un unique isomorphisme $\nu_\beta : \widetilde{E}(p) \xrightarrow{\sim} \widetilde{J}_\beta$ de groupes p-divisibles sur $\mathbb{F}_p$ tel que $\mathbf{M}(\nu_\beta) = \xi_\beta$. Alors le triplet $(\widetilde{E}, J_\beta, \nu_\beta)$ est un objet de $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$, et l'on a $\mathbf{M}(\nu_\beta)(\mathcal{L}(J_\beta)) =$

$\xi_\beta(\mathcal{L}(J_\beta)) = \mathcal{L}(\beta)$.

Remarque : on voit facilement que les choix de J_β et de ξ_β ne dépendent que de la classe d'isomorphisme de $(\widetilde{E}, J_\beta, \nu_\beta)$ dans $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$. En effet, si J'_β (resp. ξ'_β) est un autre groupe p-divisible sur $\mathbb{Z}_p$ (resp. un autre isomorphisme de $\mathbf{MD}_{\mathbb{Z}_p}$) tels que $\xi'_\beta : \mathbf{M}_{\mathbb{Z}_p}(J'_\beta) \xrightarrow{\sim} (M, \mathcal{L}(\beta))$, alors, en écrivant $\mathbf{M}(\nu'_\beta) = \xi'_\beta$, on a un isomorphisme $(\widetilde{E}, J_\beta, \nu_\beta) \xrightarrow{\sim} (\widetilde{E}, J'_\beta, \nu'_\beta)$ par $(\mathrm{Id}_{\widetilde{E}}, \psi)$, où ψ est l'unique isomorphisme $J_\beta \xrightarrow{\sim} J'_\beta$ de groupes p-divisibles sur $\mathbb{Z}_p$ tel que $\mathbf{M}_{\mathbb{Z}_p}(\psi) = \xi_\beta^{-1} \circ \xi'_\beta \in \mathrm{Isom}_{\mathbf{MD}_{\mathbb{Z}_p}}(\mathbf{M}_{\mathbb{Z}_p}(J'_\beta), \mathbf{M}_{\mathbb{Z}_p}(J_\beta))$.

Montrons maintenant l'injectivité. Soient $(\widetilde{E}, \Gamma, \nu)$ et $(\widetilde{E}, \Gamma', \nu')$ deux objets de $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$, avec $\mathbf{M}(\nu)(\mathcal{L}(\Gamma)) = \mathcal{L}(\beta)$ et $\mathbf{M}(\nu')(\mathcal{L}(\Gamma')) = \mathcal{L}(\beta')$, $\beta, \beta' \in \mathbb{Z}_p$. D'après le lemme précédent, on a l'équivalence

$$(\widetilde{E}, \Gamma, \nu) \simeq_{\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})} (\widetilde{E}, \Gamma', \nu') \quad \Leftrightarrow \quad \exists\, \gamma \in \mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) \;/\; \mathbf{M}(\gamma(p))(\mathcal{L}(\beta')) \subset \mathcal{L}(\beta)\ .$$

Or, $\widetilde{E}/\mathbb{F}_p$ étant supersingulière, on a $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) = \{\pm 1\}$ (**3.1.1.**, remarque 3). La multiplication par (-1) sur $\widetilde{E}$ induit $-\mathrm{Id}_M$ sur $M = \mathbf{M}(\widetilde{E}(p))$, et l'on voit que $\mathbf{M}([-1]_{\widetilde{E}}(p))(\mathcal{L}(\beta')) = \mathcal{L}(\beta')$. Finalement, pour $\widetilde{E}/\mathbb{F}_p$ supersingulière, on a

$$(\widetilde{E}, \Gamma, \nu) \simeq_{\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})} (\widetilde{E}, \Gamma', \nu') \quad \Leftrightarrow \quad \mathcal{L}(\beta') \subset \mathcal{L}(\beta) \quad \Leftrightarrow \quad \beta = \beta'\ .$$

□

Pour tout $\beta \in \mathbb{Z}_p$, on notera E_β le schéma elliptique sur $\mathbb{Z}_p$, unique à $\mathbb{Z}_p$-isomorphisme près, qui correspond par $\mathbf{ST}$ à un objet isomorphe dans $\mathcal{C}_{\mathbb{Z}_p}$ à un triplet $(\widetilde{E}, J_\beta, \nu_\beta)$, avec $\mathbf{M}(\nu_\beta)(\mathcal{L}(J_\beta)) = \mathcal{L}(\beta) \subset M$. Soient $\beta, \beta' \in \mathbb{Z}_p$. En combinant l'isomorphisme de **3.2.1.** et celui du lemme précédent, on obtient

$$\mathrm{Hom}_{\mathcal{SE}_{\mathbb{Z}_p}}(E_\beta, E_{\beta'}) \;\simeq\; \{\gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E}) \;/\; \mathbf{M}(\gamma(p))(\mathcal{L}(\beta')) \subset \mathcal{L}(\beta)\}\ .$$

Conséquence : Le Frobenius dans $\mathrm{End}_{\mathbb{F}_p}(\widetilde{E})$ *ne se relève dans aucun des* $\mathrm{End}_{\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})}(E_\beta)$, $\beta \in \mathbb{Z}_p$.

Preuve : L'image du Frobenius (relatif à $\mathbb{F}_p$) agissant sur $\widetilde{E}$ dans $\mathrm{End}_{\mathbb{F}_p}(\widetilde{E}(p))$ correspond par le foncteur $\mathbf{M}$ à l'opérateur $\varphi \in \mathrm{End}_{\mathbf{MD}_{\mathbb{F}_p}}(M)$. Soit $\beta \in \mathbb{Z}_p$; comme on a

$$\mathrm{End}_{\mathcal{SE}_{\mathbb{Z}_p}}(E_\beta) \;\simeq\; \{\gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E}) \;/\; \mathbf{M}(\gamma(p))(\mathcal{L}(\beta)) \subset \mathcal{L}(\beta)\}\ ,$$

on voit que le Frobenius de $\widetilde{E}$ se relève si et seulement si $\varphi(\mathcal{L}(\beta)) \subset \mathcal{L}(\beta)$. Dans la base (e_1, e_2) choisie plus haut, ceci équivaut à $\varphi(e_1 + \beta e_2) = -p\beta e_1 + e_2 \in (e_1 + \beta e_2)\mathbb{Z}_p$, c'est-à-dire $p\beta^2 + 1 = 0$, ce qui est impossible pour $\beta \in \mathbb{Z}_p$. □

On notera la différence avec le cas ordinaire, cf. le paragraphe suivant.

Remarque 3 : On verra plus loin (en **3.3.3.**) que si $j(\widetilde{E}) = 0$ ou 1728, il existe un choix particulier pour le générateur du $\mathbb{Z}_p[\varphi]$-module $\mathbf{M}(\widetilde{E}(p))$, qui est "adapté" au groupe d'automorphismes de $\widetilde{E}$ (lemme 4) ; un autre tel choix change β en $\eta\beta$, où $\eta \in \mathbb{Z}_p^\times$. Avec ce choix, on a $j(E_\beta) = 0$ ou 1728 si et seulement si $\beta = 0$. Par analogie avec le cas ordinaire, on appelera E_0 le relèvement *canonique* de $\widetilde{E}$ sur $\mathbb{Z}_p$.

Nous avons obtenu une famille de classes d'isomorphisme de schémas elliptiques $E_\beta/\mathbb{Z}_p$, $\beta \in \mathbb{Z}_p$, qui relèvent $\widetilde{E}/\mathbb{F}_p$ supersingulière, et qui sont deux-à-deux non-$\mathbb{Z}_p$-isomorphes. Par contre, *il est important de noter que toutes ces courbes ont des groupes p-divisibles isomorphes.* En effet, soient β, $\beta' \in \mathbb{Z}_p$; les groupes p-divisibles $E_\beta(p) \simeq J_\beta$ et $E_{\beta'}(p) \simeq J_{\beta'}$ sont isomorphes sur $\mathbb{Z}_p$ ssi les modules de Dieudonné $(M, \mathcal{L}(\beta))$ et $(M, \mathcal{L}(\beta'))$ le sont, ce qui équivaut à l'existence d'un isomorphisme $\mathbb{Z}_p$-linéaire $M \to M$ commutant à φ et envoyant $\mathcal{L}(\beta)$ sur $\mathcal{L}(\beta')$. Avec le choix précédent d'une base pour M, l'application $\mathbb{Z}_p$-linéaire ψ dont la matrice dans la base (e_1, e_2) s'écrit

$$\begin{pmatrix} 1+p\beta\beta' & -p(\beta'-\beta) \\ \beta'-\beta & 1+p\beta\beta' \end{pmatrix}$$

est une bijection qui vérifie $\varphi\psi = \psi\varphi$ et $\psi(\mathcal{L}(\beta)) = \mathcal{L}(\beta')$. On en déduit, par le théorème de pleine fidélité de Tate, que pour tous β, $\beta' \in \mathbb{Z}_p$, $T_p(E_\beta)$ et $T_p(E_{\beta'})$ sont des $\mathbb{Z}_p[G]$-modules isomorphes, avec $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Remarque 4 : Soient β, $\beta' \in \mathbb{Z}_p$; rappelons que les schémas E_β et $E_{\beta'}$ sont $\mathbb{Z}_p$-isogènes ssi il existe $\gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E})$ tel que $\mathbf{M}(\gamma(p))(\mathcal{L}(\beta)) \subset \mathcal{L}(\beta')$. En particulier, le polynôme caractéristique de $\mathbf{M}(\gamma(p))$ est dans $\mathbb{Q}[X]$. Soit $\psi : (M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$ un morphisme non nul de modules de Dieudonné filtrés. Toujours dans la même base que ci-dessus, la matrice de ψ doit s'écrire

$$\begin{pmatrix} a & -pc \\ c & a \end{pmatrix} \quad , \quad a, c \in \mathbb{Z}_p\,,\ (a,c) \neq (0,0),$$

pour commuter avec φ, et satisfaire la condition $\beta\beta' pc + a(\beta - \beta') + c = 0$ pour respecter les filtrations. Prenons $\beta' = 0$ et $\beta \in \mathbb{Z}_p$ tel que β n'appartient à aucune extension quadratique de $\mathbb{Q}$. Alors on voit qu'il n'est pas possible de choisir $a, c \in \mathbb{Z}_p$ tels que $(a,c) \neq (0,0)$, $a \in \mathbb{Q}$, $a^2 + pc^2 \in \mathbb{Q}$ et $a\beta + c = 0$. On en déduit que les schémas E_0 et E_β ne sont pas $\mathbb{Z}_p$-isogènes.

3.2.4. Relèvements sur $\mathbb{Z}_p$ ordinaires :

Dans tout ce paragraphe, *on fixe $\widetilde{E}/\mathbb{F}_p$ ordinaire.*
On écrit $M = \mathbf{M}(\widetilde{E}(p))$, et $a_p = a_p(\widetilde{E}) = \mathrm{Tr}(\mathrm{Frob}_{\widetilde{E}}) = u + u^{-1}p$, $u \in \mathbb{Z}_p^\times$.
Comme en **3.1.2.** lemme 1, on choisit une $\mathbb{Z}_p$-base (e_1, e_2) de M telle que $\varphi e_1 = u e_1$ et $\varphi e_2 = u^{-1} p e_2$. Posons $\mathcal{L} = (\lambda e_1 + \mu e_2)\mathbb{Z}_p$, avec λ, $\mu \in \mathbb{Z}_p$, $(\lambda, \mu) \neq (0,0)$. Alors la flèche naturelle

$$\mathcal{L} = (\lambda e_1 + \mu e_2)\mathbb{Z}_p \xrightarrow{proj} M/\varphi M = (\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2) \,/\, (\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p p e_2) \simeq \mathbb{F}_p(e_2 \bmod pM)$$

induit un isomorphisme de $\mathbb{F}_p$-espaces vectoriels

$$\mathcal{L}/p\mathcal{L} \simeq M/\varphi M \qquad (*)$$

si et seulement si $\mu \in \mathbb{Z}_p^\times$. Donc les relèvements de M en un module de Dieudonné sur $\mathbb{Z}_p$ correspondent bijectivement aux

$$\mathcal{L} = \mathcal{L}(\beta) = (\beta e_1 + e_2)\mathbb{Z}_p \quad , \quad \beta \in \mathbb{Z}_p\,.$$

De la même manière qu'en **3.2.3.**, on associe à tout objet $(\widetilde{E},\Gamma,\nu)$ de $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ l'unique $\beta \in \mathbb{Z}_p$ tel que $\mathbf{M}(\nu)(\mathcal{L}(\Gamma)) = \mathcal{L}(\beta)$. Si $(\widetilde{E},\Gamma',\nu')$ est un autre objet de $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ avec $\mathbf{M}(\nu')(\mathcal{L}(\Gamma')) = \mathcal{L}(\beta') = (\beta' e_1 + e_2)\mathbb{Z}_p$, alors

$$\mathrm{Hom}_{\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})}\Big((\widetilde{E},\Gamma,\nu),(\widetilde{E},\Gamma',\nu')\Big) \simeq \{\gamma \in \mathrm{End}_{\mathbb{F}_p}(\widetilde{E}) \ / \ \mathbf{M}(\gamma(p))(\mathcal{L}(\beta')) \subset \mathcal{L}(\beta)\} \ .$$

Rappelons que $\widetilde{E}/\mathbb{F}_p$ avec $j(\widetilde{E}) = 0$ (resp. $j(\widetilde{E}) = 1728$) est ordinaire si et seulement si $6 \mid p-1$ (resp. $4 \mid p-1$), et alors $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) \simeq \mu_6(\mathbb{F}_p)$ (resp. $\mu_4(\mathbb{F}_p)$) est strictement plus grand que $\{\pm 1\}$, d'ordre 6 (resp. d'ordre 4). Dans tous les autres cas, $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) = \{\pm 1\}$.

Proposition 2 :
Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique ordinaire d'invariant modulaire $j(\widetilde{E})$; on choisit une $\mathbb{Z}_p$-base de $\mathbf{M}(\widetilde{E}(p))$ qui diagonalise φ.
1) Si $j(\widetilde{E}) \notin \{0, 1728\}$, alors l'association décrite ci-dessus

$$\begin{cases} \mathcal{C}_{\mathbb{Z}_p}(\widetilde{E}) & \to & \mathbb{Z}_p \\ (\widetilde{E},\Gamma,\nu) & \mapsto & \beta \ \textit{tel que} \ \mathcal{L}(\beta) = \mathbf{M}(\nu)(\mathcal{L}(\Gamma)) \end{cases}$$

induit une bijection entre les classes d'isomorphisme dans $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ et $\mathbb{Z}_p$.
2) Si $j(\widetilde{E}) = 0$ (resp. $j(\widetilde{E}) = 1728$), alors l'association ci-dessus induit une bijection entre les classes d'isomorphisme dans $\mathcal{C}_{\mathbb{Z}_p}(\widetilde{E})$ et l'ensemble $\mathbb{Z}_p/\!\sim$, où $x \sim y \Leftrightarrow x^3 = y^3$ (resp. $x \sim y \Leftrightarrow x^2 = y^2$).

Remarque 1 : Soit (e_1', e_2') une autre base de diagonalisation de φ dans $\mathbf{M}(\widetilde{E}(p))$; si l'on écrit $\mathcal{L}(\beta') = (\beta' e_1' + e_2')\mathbb{Z}_p$, alors $\beta' = \eta\beta$ avec $\eta \in \mathbb{Z}_p^\times$.

Preuve :
La partie "surjectivité" se fait de manière tout-à-fait analogue au cas supersingulier, de même que la partie "injectivité" lorsque $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) = \{\pm 1\}$, i.e. $j(\widetilde{E}) \notin \{0, 1728\}$.
Supposons $j(\widetilde{E}) \in \{0, 1728\}$, et posons $n = 6$ si $j(\widetilde{E}) = 0$, et $n = 4$ si $j(\widetilde{E}) = 1728$; alors $n \mid p-1$, et $\mathbb{Z}_p$ contient une racine primitive n-ième de l'unité ζ_n. On a $\mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) = <[\zeta_n]>$ et

$$(\widetilde{E},\Gamma,\nu) \simeq (\widetilde{E},\Gamma',\nu') \ \Leftrightarrow \ \exists\, \gamma \in \mathrm{Aut}_{\mathbb{F}_p}(\widetilde{E}) \ / \ \mathbf{M}(\gamma(p))(\mathcal{L}(\beta')) \subset \mathcal{L}(\beta) \ .$$

L'automorphisme $\mathbb{Z}_p$-linéaire $\xi_n = \mathbf{M}([\zeta_n](p)) : M \to M$ commute avec φ, est d'ordre exact n, et de déterminant 1. La relation $\varphi\xi_n = \xi_n\varphi$ donne, dans la base (e_1, e_2)

$$\begin{cases} \varphi(\xi_n e_1) = \xi_n\varphi e_1 = \xi_n(u e_1) = u(\xi_n e_1) \\ \varphi(\xi_n e_2) = \xi_n\varphi e_2 = \xi_n(u^{-1}p e_1) = u^{-1}p(\xi_n e_1) \end{cases}$$

d'où $\xi_n e_1 \in \mathbb{Z}_p e_1$ et $\xi_n e_2 \in \mathbb{Z}_p e_2$; puis, comme ξ_n est d'ordre exact n et de déterminant 1, on doit avoir

$$\xi_n e_1 = \zeta_n^\epsilon e_1 \quad \text{et} \quad \xi_n e_2 = \zeta_n^{-\epsilon} e_2 \quad , \text{avec} \quad \epsilon \in \{\pm 1\} = (\mathbb{Z}/n\mathbb{Z})^\times \ .$$

Soient $\beta, \beta' \in \mathbb{Z}_p$, et soit $i \in \mathbb{Z}/n\mathbb{Z}$. Alors

$$\begin{aligned} & \xi_n^i(\mathcal{L}(\beta')) \subset \mathcal{L}(\beta) \\ \Leftrightarrow \ & \xi_n^i(\beta' e_1 + e_2) = \beta'\zeta_n^{i\epsilon} e_1 + \zeta_n^{-i\epsilon} e_2 \ \in \ (\beta e_1 + e_2)\mathbb{Z}_p \\ \Leftrightarrow \ & \beta' = \zeta_n^{-2i\epsilon}\beta \quad , \quad \epsilon \in \{\pm 1\} = (\mathbb{Z}/n\mathbb{Z})^\times \ . \end{aligned}$$

On en déduit que $(\widetilde{E},\Gamma,\nu)\simeq(\widetilde{E},\Gamma',\nu')$ si et seulement si $(\beta)^{n/2}=(\beta')^{n/2}$, avec $n/2=3$ si $j(\widetilde{E})=0$, et $n/2=2$ si $j(\widetilde{E})=1728$. □

Si $j(\widetilde{E})\notin\{0,1728\}$ (resp. si $j(\widetilde{E})\in\{0,1728\}$), pour tout $\beta\in\mathbb{Z}_p$ (resp. pour tout $\beta\in\mathbb{Z}_p/\sim$), on notera E_β le schéma elliptique sur $\mathbb{Z}_p$ (unique à $\mathbb{Z}_p$-isomorphisme près) qui correspond par **ST** à un triplet isomorphe dans $\mathcal{C}_{\mathbb{Z}_p}$ à un $(\widetilde{E},J_\beta,\nu_\beta)$, avec $\mathbf{M}(\nu_\beta)(\mathcal{L}(J_\beta))=\mathcal{L}(\beta)\subset M$. Lorsque $j(\widetilde{E})\notin\{0,1728\}$ on obtient donc une correspondance bijective entre les classes d'isomorphisme dans $\mathcal{SE}_{\mathbb{Z}_p}(\widetilde{E})$ et $\mathbb{Z}_p$; les isomorphismes de groupes topologiques

$$\mathbb{Z}_p\xrightarrow{\sim}p\mathbb{Z}_p\xrightarrow{Exp}1+p\mathbb{Z}_p=\mathbb{G}_m(\mathbb{Z}_p)$$

permettent de retrouver le paramétrage usuel des relèvements sur $\mathbb{Z}_p$ de $\widetilde{E}/\mathbb{F}_p$ ordinaire (voir [Me], Appendix, Prop.3.2.).

Proposition 3 :
Soit $\widetilde{E}/\mathbb{F}_p$ ordinaire.
1) Le Frobenius de $\widetilde{E}/\mathbb{F}_p$ se relève dans End $_{\mathcal{SE}_{\mathbb{Z}_p}}(E_\beta)$ *si et seulement si $\beta=0$.*
2) Supposons $j(\widetilde{E})=0$ (resp. $j(\widetilde{E})=1728$) ; alors $j(E_\beta)=0$ (resp. $j(E_\beta)=1728$) si et seulement si $\beta=0$.

Preuve :
1) Soit $\beta\in\mathbb{Z}_p$. On a $\mathbf{M}(\mathrm{Frob}_{\widetilde{E}}(p))=\varphi$, et le Frobenius de $\widetilde{E}$ se relève dans End $_{\mathcal{SE}_{\mathbb{Z}_p}}(E_\beta)$ si et seulement si $\varphi(\mathcal{L}(\beta))\subset\mathcal{L}(\beta)$, ce qui équivaut à $\beta ue_1+u^{-1}pe_2\in(\beta e_1+e_2)\mathbb{Z}_p$, c'est-à-dire $\beta(u-u^{-1}p)=0$, i.e. $\beta=0$.
2) Soit $\beta\in\mathbb{Z}_p$. Soit $\zeta_n\in\mathbb{Z}_p$ une racine primitive n-ième de l'unité, avec $n=4$ ou 6. On a

$$j(E_\beta)=0\ (\text{resp. }1728)\ \Leftrightarrow\ [\zeta_n]\in\mathrm{Aut}(E_\beta)=\mathrm{Aut}_{\mathbb{Z}_p}(E_\beta)\ ,\ \text{avec}\ n=6\ (\text{resp. }n=4)\ .$$

En reprenant la démonstration de la proposition précédente, on voit que $\xi_n=\mathbf{M}([\zeta_n](p))$ agit sur $M=\mathbb{Z}_pe_1\oplus\mathbb{Z}_pe_2$ par : $\xi_ne_1=\zeta_n^\epsilon e_1$, $\xi_ne_2=\zeta_n^{-\epsilon}e_2$, pour un $\epsilon\in\{\pm1\}$. Donc ξ_n stabilise $\mathcal{L}(\beta)$ si et seulement si $\xi_n(\beta e_1+e_2)=\beta\zeta_n^\epsilon e_1+\zeta_n^{-\epsilon}e_2\in(\beta e_1+e_2)\mathbb{Z}_p$, c'est-à-dire $\beta(\zeta_n^\epsilon-\zeta_n^{-\epsilon})=0$, i.e. $\beta=0$. □

On en déduit que E_0 est le relèvement *canonique* de $\widetilde{E}/\mathbb{F}_p$; voir [Me], V, Thm.3.3., pour une définition valable pour les schémas abéliens ordinaires de dimension quelconque, puis Appendix, Cor.1.2. et 1.3.
Remarque 2 : Soient $\widetilde{E}/\mathbb{F}_p$ et $\widetilde{E}'/\mathbb{F}_p$ deux courbes elliptiques ordinaires. Soient $E_0/\mathbb{Z}_p$ et $E_0'/\mathbb{Z}_p$ les relèvements canoniques de $\widetilde{E}$ et $\widetilde{E}'$ respectivement. Alors toute $\mathbb{F}_p$-isogénie $\widetilde{E}\to\widetilde{E}'$ se relève en une $\mathbb{Z}_p$-isogénie $E_0\to E_0'$, i.e.

$$\mathrm{Hom}_{\mathbb{Z}_p}(E_0,E_0')\ \simeq\ \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{E},\widetilde{E}').$$

En particulier, si $a_p(\widetilde{E})=a_p(\widetilde{E}')$, alors E_0 et E_0' sont liées par une isogénie de degré premier à p (cf. **3.1.2.**).

Regardons maintenant ce que donnent les groupes p-divisibles obtenus avec les E_β, $\beta\in\mathbb{Z}_p$: on a $\mathbf{M}_{\mathbb{Z}_p}(E_\beta(p))\simeq(M,\mathcal{L}(\beta))$ dans $\mathbf{MD}_{\mathbb{Z}_p}$. On reprend une $\mathbb{Z}_p$-base (e_1,e_2) de $M=\mathbf{M}(\widetilde{E}(p))$ telle que $\varphi e_1=ue_1$ et $\varphi e_2=u^{-1}pe_2$, avec $u+u^{-1}p=a_p(\widetilde{E})\in\mathbb{Z}_p^\times$; alors

$\mathcal{L}(\beta) = (\beta e_1 + e_2)\mathbb{Z}_p$.
Soient $\beta, \beta' \in \mathbb{Z}_p$; une application $\mathbb{Z}_p$-linéaire $\psi : (M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$ est un morphisme dans $\mathbf{MD}_{\mathbb{Z}_p}$ si et seulement si ψ s'écrit dans la base (e_1, e_2)

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad , \quad a, d \in \mathbb{Z}_p \, ,$$

(ce qui équivaut à $\varphi\psi = \psi\varphi$), avec la condition : $a\beta = d\beta'$ (ce qui équivaut à $\psi(\mathcal{L}(\beta)) \subset \mathcal{L}(\beta')$). Soit v_p la valuation p-adique sur $\mathbb{Z}_p$ normalisée par $v_p(p) = 1$; on en déduit que :
- $(M, \mathcal{L}(\beta))$ est $\mathbb{Z}_p$-isomorphe à $(M, \mathcal{L}(\beta'))$ ssi $v_p(\beta) = v_p(\beta')$;
- $(M, \mathcal{L}(\beta))$ est $\mathbb{Z}_p$-isogène à $(M, \mathcal{L}(\beta'))$ ssi $\beta = \beta' = 0$ ou $\beta\beta' \neq 0$.

Remarque 3 : $\mathrm{End}_{\mathbf{MD}_{\mathbb{Z}_p}}((M, \mathcal{L}(0))) \simeq \{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, a, d \in \mathbb{Z}_p\}$, et $\mathrm{End}_{\mathbf{MD}_{\mathbb{Z}_p}}((M, \mathcal{L}(\beta))) = \mathbb{Z}_p$ si $\beta \neq 0$.

Remarque 4 : Soient $\beta, \beta' \in \mathbb{Z}_p$ tels que $\beta\beta' \neq 0$, et soit $\psi : (M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$ un morphisme non nul de modules de Dieudonné filtrés ; toujours dans la même base que ci-dessus, le polynôme caractéristique de ψ est $X^2 - (a+d)X + ad$, avec $a, d \in \mathbb{Z}_p$, $(a, d) \neq (0, 0)$, tels que $a\beta = d\beta'$. Si ψ provient d'un élément de $\mathrm{End}_{\mathbf{F}_p}(\widetilde{E})$, alors $ad \in \mathbb{Z}$ et $a + d \in \mathbb{Z}$, donc $[\mathbb{Q}(a, d) : \mathbb{Q}] \leq 2$. Choisissons $\beta' \in \mathbb{Z}\backslash\{0\}$ et $\beta \in \mathbb{Z}_p\backslash\{0\}$ tel que $[\mathbb{Q}(\beta) : \mathbb{Q}] > 2$; alors les schémas E_β et E'_β ne sont pas $\mathbb{Z}_p$-isogènes.

Soit $\beta \in \mathbb{Z}_p$. Comme $\widetilde{E}$ est ordinaire, on a une suite exacte de groupes p-divisibles sur $\mathbb{Z}_p$, où $E_\beta(p)^0$ est la partie connexe (de hauteur 1) de $E_\beta(p)$:

$$0 \longrightarrow E_\beta(p)^0 \longrightarrow E_\beta(p) \longrightarrow \widetilde{E_\beta}(p) \longrightarrow 0 \, .$$

Posons $D(\beta) = (M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \, , \mathcal{L}(\beta) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = (\mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2 \, , \, (\beta e_1 + e_2)\mathbb{Q}_p)$: c'est un objet de $\mathbf{MF}^{ad}_{\mathbb{Q}_p}(\varphi)$ qui est isomorphe à $\mathbf{D}^*_{\mathbf{cris},\mathbb{Q}_p}(V_p(E_\beta))$. Posons $L_1(\beta) = \mathbb{Q}_p e_1 \cap \mathcal{L}(\beta) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ et $L_2(\beta) = \mathrm{Proj}_{\mathbb{Q}_p e_2}(\mathcal{L}(\beta) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$; on a $L_1(\beta) = 0$ et $L_2(\beta) = \mathbb{Q}_p e_2$. Soient, pour $i = 1, 2$, $D_i(\beta) = (\mathbb{Q}_p e_i \, , L_i(\beta))$: ce sont des objets de $\mathbf{MF}^{ad}_{\mathbb{Q}_p}(\varphi)$, en posant $\mathrm{Fil}^m D_i(\beta) = \mathbb{Q}_p e_i$ pour $m \leq 0$, $\mathrm{Fil}^1 D_i(\beta) = L_i(\beta)$, et $\mathrm{Fil}^m D_i(\beta) = 0$ pour $m \geq 2$. Alors $D_1(\beta) \simeq \mathbf{D}^*_{\mathbf{cris},\mathbb{Q}_p}(V_p(\widetilde{E_\beta}))$ et $D_2(\beta) \simeq \mathbf{D}^*_{\mathbf{cris},\mathbb{Q}_p}(V_p(E_\beta(p)^0))$, et l'on a une suite exacte dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$:

$$(*) \qquad 0 \longrightarrow D_1(\beta) \longrightarrow D(\beta) \longrightarrow D_2(\beta) \longrightarrow 0 \, ,$$

qui correspond, via le quasi-inverse du foncteur $\mathbf{D}^*_{\mathbf{cris},\mathbb{Q}_p}$, à une suite exacte de $\mathbb{Q}_p[G]$-modules, $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$:

$$(*) \qquad 0 \longrightarrow V_p(E_\beta(p)^0) \longrightarrow V_p(E_\beta) \longrightarrow V_p(\widetilde{E_\beta}) \longrightarrow 0 \, .$$

Ces suites sont scindées si et seulement si $D_2(\beta)$ est un sous-objet de $D(\beta)$ dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$; cette condition équivaut à $L_2(\beta) = \mathbb{Q}_p e_2 \cap \mathcal{L}(\beta) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, c'est-à-dire $\mathbb{Q}_p e_2 \subset (\beta e_1 + e_2)\mathbb{Q}_p$. Finalement, la suite exacte $(*)$ est scindée si et seulement si $\beta = 0$. Remarquons de plus que tous les $D(\beta)$, $\beta \neq 0$, sont isomorphes dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$, et par conséquent les $\mathbb{Q}_p[G]$-modules $V_p(E_\beta)$, $\beta \neq 0$, le sont également.

Remarque 5 : Soient $\chi : G \to \mathbb{Z}_p^\times$ le caractère cyclotomique et $\eta_u : G \to G/I \to \mathbb{Z}_p^\times$ le caractère non ramifié qui envoie le Frobenius arithmétique sur $u \in \mathbb{Z}_p^\times$ (avec toujours

$u + u^{-1}p = a_p(\widetilde{E})$). Alors on a $V_1 = V_p(E_\beta(p)^0) = \mathbb{Q}_p(\eta_u^{-1}\chi)$, et $V_2 = V_p(\widetilde{E_\beta}) = \mathbb{Q}_p(\eta_u)$. Les extensions de V_2 par V_1 sont classifiées par

$$\mathrm{Ext}^1(V_2, V_1) = \mathrm{Ext}^1(\mathbb{Q}_p, V_2^* \otimes_{\mathbb{Q}_p} V_1) = \mathrm{H}^1(G, \mathbb{Q}_p(\eta_u^{-2}\chi)) \ .$$

On en déduit que $\dim_{\mathbb{Q}_p}\mathrm{Ext}^1(V_2, V_1) = 1$. On retrouve ainsi le fait observé ci-dessus : les extensions de V_2 par V_1 donnent deux classes d'isomorphisme dans $\mathbf{Rep}_{\mathbb{Q}_p}(G)$, l'une correspondant aux éléments non nuls de $\mathrm{Ext}^1(V_2, V_1)$ et pour lesquels la suite exacte

$$(*) \qquad 0 \longrightarrow V_1 \longrightarrow V \longrightarrow V_2 \longrightarrow 0$$

n'est pas scindée, et l'autre correspondant à l'élément nul de $\mathrm{Ext}^1(V_2, V_1)$, pour lequel $(*)$ est scindée.

3.3. Relèvements sur un anneau totalement ramifié : le cas $1 < e < p-1$.

Nous allons maintenant étudier les relèvements d'une courbe elliptique $\widetilde{E}/\mathbb{F}_p$ fixée en un schéma elliptique sur $O_{L_e} = \mathbb{Z}_p[\pi_e]$, avec $\pi_e^e = -p$ et $1 < e < p-1$.

3.3.1. Schémas elliptiques sur O_{L_e}, $1 < e < p-1$:

3.3.1.1. On note $\mathcal{SE}_{O_{L_e}}$ la catégorie des schémas elliptiques sur O_{L_e} ; on note $\mathcal{C}_{O_{L_e}}$ la catégorie dont les objets sont les triplets $(\widetilde{B}, \Gamma, \nu)$, où $\widetilde{B}$ est une courbe elliptique sur $\mathbb{F}_p$, Γ un groupe p-divisible sur O_{L_e}, $\nu : \widetilde{B}(p) \xrightarrow{\sim} \widetilde{\Gamma} = \Gamma \times_{O_{L_e}} \mathbb{F}_p$ un isomorphisme de groupes p-divisibles sur $\mathbb{F}_p$, et les morphismes $(\widetilde{B}, \Gamma, \nu) \to (\widetilde{B}', \Gamma', \nu')$ sont les couples (γ, ψ), où $\gamma : \widetilde{B} \to \widetilde{B}'$ est un morphisme de courbes elliptiques sur $\mathbb{F}_p$ et $\psi : \Gamma \to \Gamma'$ est un morphisme de groupes p-divisibles sur O_{L_e}, tels que $\nu' \circ \gamma(p) = \widetilde{\psi} \circ \nu$. Le théorème de Serre-Tate nous dit que le foncteur $\mathbf{ST}$ de $\mathcal{SE}_{O_{L_e}}$ dans $\mathcal{C}_{O_{L_e}}$, défini par $\mathbf{ST}(A) = (\widetilde{A}, A(p), \nu_{can})$, où $\widetilde{A} = A \times_{O_{L_e}} \mathbb{F}_p$, établit une équivalence de catégories.

Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique fixée.
On note $\mathcal{SE}_{O_{L_e}}(\widetilde{E})$ la sous-catégorie pleine de $\mathcal{SE}_{O_{L_e}}$ formée des objets A de $\mathcal{SE}_{O_{L_e}}$ tels qu'il existe un $\mathbb{F}_p$-isomorphisme $f : \widetilde{A} \xrightarrow{\sim} \widetilde{E}$, et $\mathcal{C}_{O_{L_e}}(\widetilde{E})$ la sous-catégorie pleine de $\mathcal{C}_{O_{L_e}}$ formée des objets $(\widetilde{E}, \Gamma, \nu)$ de $\mathcal{C}_{O_{L_e}}$. Soit A un objet de $\mathcal{SE}_{O_{L_e}}(\widetilde{E})$, et soit $f : \widetilde{A} \xrightarrow{\sim} \widetilde{E}$ un $\mathbb{F}_p$-isomorphisme ; alors $\mathbf{ST}(A)$ est isomorphe dans $\mathcal{C}_{O_{L_e}}$ à l'objet $(\widetilde{E}, A(p), \nu_{can} \circ f(p)^{-1})$ de $\mathcal{C}_{O_{L_e}}(\widetilde{E})$, par $(f, \mathrm{Id}_{A(p)})$. La classe d'isomorphisme dans $\mathcal{C}_{O_{L_e}}(\widetilde{E})$ de $(\widetilde{E}, A(p), \nu_{can} \circ f(p)^{-1})$ ne dépend pas du choix de f, et l'on a, avec des notations évidentes :

$$\mathrm{Hom}_{\mathcal{SE}_{O_{L_e}}(\widetilde{E})}(A, A') \simeq \mathrm{Hom}_{\mathcal{C}_{O_{L_e}}(\widetilde{E})}\Big((\widetilde{E}, A(p), \nu_{can} \circ f(p)^{-1}), (\widetilde{E}, A'(p), \nu'_{can} \circ f'(p)^{-1})\Big) \ .$$

Donc le foncteur $\mathbf{ST}$ induit une bijection entre les classes d'isomorphisme de $\mathcal{SE}_{O_{L_e}}(\widetilde{E})$ et celles de $\mathcal{C}_{O_{L_e}}(\widetilde{E})$.

On aimerait pouvoir utiliser la théorie des modules de Dieudonné filtrés sur O_{L_e}, telle qu'elle est décrite dans [Fo 4],IV,§ 2 à 5. Pour cela, il nous faut supposer $e < p-1$.

Pour $e \leq p-1$, on définit la catégorie $\mathbf{MD}_{O_{L_e}}$ suivante :
- les objets sont les couples $(M, \mathcal{L})$, où M est un $\mathbb{Z}_p$-module libre de rang fini, muni d'un opérateur de Frobenius $\mathbb{Z}_p$-linéaire φ tel que $pM \subset \varphi M$ (i.e. M est un objet de $\mathbf{MD}_{\mathbf{F}_p}$), et $\mathcal{L}$ est un sous-O_{L_e}-module de

$$\mathcal{M} = M \otimes_{\mathbb{Z}_p} O_{L_e} + \varphi M \otimes_{\mathbb{Z}_p} p^{-1}\pi_e O_{L_e} = M \otimes_{\mathbb{Z}_p} O_{L_e} + \varphi M \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e} \subset M \otimes_{\mathbb{Z}_p} L_e ,$$

tel que l'inclusion $\mathcal{L} \hookrightarrow \mathcal{M}$ induit un isomorphisme de $\mathbf{F}_p$-espaces vectoriels

$$\mathcal{L}/\pi_e\mathcal{L} \simeq \mathcal{M}/(\varphi M \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e}) \qquad (**)$$

- un morphisme $(M, \mathcal{L}) \to (M', \mathcal{L}')$ est une application $\mathbb{Z}_p$-linéaire $\psi : M \to M'$ telle que $\psi\varphi = \varphi'\psi$, et qui, après extension des scalaires, envoie $\mathcal{L}$ dans $\mathcal{L}'$.

Soit Γ un groupe p-divisible sur O_{L_e}, $e \leq p-1$, et $\widetilde{\Gamma} = \Gamma \times_{O_{L_e}} \mathbf{F}_p$ sa fibre spéciale. Dans [Fo 4], IV, § 2,3,4, J.-M. Fontaine construit un sous-O_{L_e}-module $\mathcal{L}(\Gamma)$ de $\mathcal{M}(\widetilde{\Gamma}) = \mathbf{M}(\widetilde{\Gamma}) \otimes_{\mathbb{Z}_p} O_{L_e} + \varphi\mathbf{M}(\widetilde{\Gamma}) \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e}$ qui vérifie $(**)$, de sorte que le couple $(\mathbf{M}(\widetilde{\Gamma}), \mathcal{L}(\Gamma))$ est un objet de $\mathbf{MD}_{O_{L_e}}$. L'association

$$\Gamma \mapsto \mathbf{M}_{O_{L_e}}(\Gamma) = (\mathbf{M}(\widetilde{\Gamma}), \mathcal{L}(\Gamma))$$

est fonctorielle. Lorsque $e < p-1$, elle induit une anti-équivalence entre la catégorie des groupes p-divisibles sur O_{L_e} et $\mathbf{MD}_{O_{L_e}}$ ([Fo 4], V, Prop.5.1.).

Dans toute la suite, on suppose $e < p-1$. Soit M un objet de $\mathbf{MD}_{\mathbf{F}_p}$; les relèvements de M en un objet de $\mathbf{MD}_{O_{L_e}}$ sont alors en correspondance bijective avec les sous-O_{L_e}-modules $\mathcal{L}$ libres de rang 1 de $\mathcal{M}$ tels que l'inclusion $\mathcal{L} \hookrightarrow \mathcal{M}$ induit un isomorphisme de $\mathbf{F}_p$-espaces vectoriels

$$\mathcal{L}/\pi_e\mathcal{L} \simeq \mathcal{M}/(\varphi M \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e}) \qquad (**) .$$

3.3.1.2. On *fixe* $\widetilde{E}/\mathbf{F}_p$ *supersingulière.*
On note $M = \mathbf{M}(\widetilde{E}(p))$, et $\mathcal{M} = \mathcal{M}(\widetilde{E}(p))$. On choisit $e_1 \in M$ tel que $e_1 \notin \varphi M$, d'où $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$ et $M = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$. Alors on a :

$$\varphi M \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e} = O_{L_e}(e_1 \otimes \pi_e) \oplus O_{L_e}(e_2 \otimes \pi_e^{1-e}) ,$$

$$\mathcal{M} = O_{L_e}(e_1 \otimes 1) \oplus O_{L_e}(e_2 \otimes \pi_e^{1-e}) ,$$

$$\text{et} \quad \mathcal{M}/(\varphi M \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e}) \simeq O_{L_e}(e_1 \otimes 1)/O_{L_e}(e_1 \otimes \pi_e) \simeq \mathbf{F}_p((e_1 \otimes 1) \bmod \pi_e\mathcal{M})$$

est un $\mathbf{F}_p$-espace vectoriel de dimension 1. Posons $\mathcal{L} = (e_1 \otimes \lambda + e_2 \otimes \pi_e^{1-e}\mu)O_{L_e}$, avec λ, $\mu \in O_{L_e}$, et $(\lambda, \mu) \neq (0,0)$. Alors la flèche naturelle

$$\mathcal{L} = (e_1 \otimes \lambda + e_2 \otimes \pi_e^{1-e}\mu)O_{L_e} \xrightarrow{proj} \mathcal{M}/(\varphi M \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e})$$

est bijective si et seulement si $\lambda \in O_{L_e}^{\times}$. Donc la condition $(**)$ est satisfaite ssi

$$\mathcal{L} = \mathcal{L}(\beta) = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e})O_{L_e} \quad , \quad \beta \in O_{L_e} .$$

Soit $(\widetilde{E}, \Gamma, \nu)$ un objet de $\mathcal{C}_{O_{L_e}}(\widetilde{E})$. Alors $\mathbf{M}_{O_{L_e}}(\Gamma) = (\mathbf{M}(\widetilde{\Gamma}), \mathcal{L}(\Gamma))$ est un objet de $\mathbf{MD}_{O_{L_e}}$, et $\mathbf{M}(\nu) : \mathbf{M}(\widetilde{\Gamma}) \xrightarrow{\sim} \mathbf{M}(\widetilde{E}(p)) = M$ est un isomorphisme dans $\mathbf{MD}_{\mathbf{F}_p}$ (on a

donc $\mathbf{M}(\nu)(\varphi\mathbf{M}(\widetilde{\Gamma})) = \varphi M$). On note $\mathbf{M}(\nu)_{L_e} = \mathbf{M}(\nu)\otimes \mathbf{1}_{L_e}$ l'application L_e-linéaire de $\mathcal{M}(\widetilde{\Gamma})$ dans $\mathcal{M}(\widetilde{E}(p)) = \mathcal{M}$ que l'on en déduit par extension des scalaires (en particulier, on a $\mathbf{M}(\nu)_{L_e}(\varphi\mathbf{M}(\widetilde{\Gamma})\otimes_{\mathbb{Z}_p}\pi_e^{1-e}O_{L_e}) = \varphi M\otimes_{\mathbb{Z}_p}\pi_e^{1-e}O_{L_e}$, et $\mathbf{M}(\nu)_{L_e}(\mathcal{M}(\widetilde{\Gamma})) = \mathcal{M}$). Alors $\mathbf{M}(\nu)_{L_e}(\mathcal{L}(\Gamma))$ est un sous-O_{L_e}-module de rang 1 de $\mathcal{M}$, tel que l'inclusion induit un isomorphisme de $\mathbb{F}_p$-espaces vectoriels

$$\mathbf{M}(\nu)_{L_e}(\mathcal{L}(\Gamma)) \,/\, \pi_e(\mathbf{M}(\nu)_{L_e}(\mathcal{L}(\Gamma))) \;\simeq\; \mathcal{M}/(\varphi M\otimes_{\mathbb{Z}_p}\pi_e^{1-e}O_{L_e})\ .$$

Donc, d'après ce qu'on a vu ci-dessus, et via le choix d'une base de M convenable, il existe un unique $\beta\in O_{L_e}$ tel que $\mathbf{M}(\nu)_{L_e}(\mathcal{L}(\Gamma)) = \mathcal{L}(\beta)\subset\mathcal{M}$.

Proposition 4 :
Soit e tel que $1<e<p-1$. Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique supersingulière. Via le choix d'un générateur du $\mathbb{Z}_p[\varphi]$-module $\mathbf{M}(\widetilde{E}(p))$, l'association

$$\begin{cases} \mathcal{C}_{O_{L_e}}(\widetilde{E}) & \to & O_{L_e} \\ (\widetilde{E},\Gamma,\nu) & \mapsto & \beta \text{ tel que } \mathcal{L}(\beta) = \mathbf{M}(\nu)_{L_e}(\mathcal{L}(\Gamma)) \end{cases}$$

induit une bijection entre les classes d'isomorphisme dans $\mathcal{C}_{O_{L_e}}(\widetilde{E})$ et O_{L_e}.

En composant avec le foncteur **ST**, on obtient une bijection entre les classes d'isomorphisme dans $\mathcal{SE}_{O_{L_e}}(\widetilde{E})$ et O_{L_e}. De même que pour $e=1$, le choix d'un autre générateur du $\mathbb{Z}_p[\varphi]$-module $M=\mathbf{M}(\widetilde{E}(p))$ change l'invariant β.

La preuve est tout-à-fait similaire au cas $e=1$ (**3.2.3.**). En particulier, on a l'analogue du lemme 1 de **3.2.3.**, en remplaçant $\mathbb{Z}_p$ par O_{L_e} et $\mathbf{M}(\gamma(p))$ par $\mathbf{M}(\gamma(p))_{L_e} = \mathbf{M}(\gamma(p))\otimes\mathbf{1}_{L_e}$. Pour tout $\beta\in O_{L_e}$, on notera E_β le schéma elliptique sur O_{L_e}, unique à O_{L_e}-isomorphisme près, qui correspond par **ST** à un objet isomorphe dans $\mathcal{C}_{O_{L_e}}$ à un triplet $(\widetilde{E},J_\beta,\nu_\beta)$, avec $\mathbf{M}(\nu_\beta)_{L_e}(\mathcal{L}(J_\beta)) = \mathcal{L}(\beta)\subset\mathcal{M}$. Soient $\beta,\beta'\in O_{L_e}$; on a, avec des notations évidentes, un isomorphisme

$$\mathrm{Hom}_{\mathcal{SE}_{O_{L_e}}(\widetilde{E})}(E_\beta,E_{\beta'}) \;\simeq\; \{\,\gamma\in\mathrm{End}_{\mathbb{F}_p}(\widetilde{E}) \;/\; \mathbf{M}(\gamma(p))_{L_e}(\mathcal{L}(\beta'))\subset\mathcal{L}(\beta)\,\}\ .$$

Lemme 2 :
Soit e tel que $1<e<p-1$. Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique supersingulière. Le Frobenius dans $\mathrm{End}_{\mathbb{F}_p}(\widetilde{E})$ se relève dans $\mathrm{End}_{\mathcal{SE}_{O_{L_e}}(\widetilde{E})}(E_\beta)$ si et seulement si e est pair et $\beta=\pm\pi_e^{e/2-1}$.

Preuve :
Notons $\mathrm{Frob}_{\widetilde{E}}$ le Frobenius arithmétique dans $\mathrm{End}_{\mathbb{F}_p}(\widetilde{E})$. On a $\mathbf{M}(\mathrm{Frob}_{\widetilde{E}}(p)) = \varphi$, et $\mathrm{Frob}_{\widetilde{E}}$ se relève dans $\mathrm{End}_{\mathcal{SE}_{O_{L_e}}(\widetilde{E})}(E_\beta)$ si et seulement si $(\varphi\otimes\mathbf{1}_{L_e})(\mathcal{L}(\beta))\subset\mathcal{L}(\beta)$, i.e.
$(\varphi\otimes\mathbf{1}_{L_e})(e_1\otimes 1+\beta\cdot e_2\otimes\pi_e^{1-e}) = (\beta\cdot e_1\otimes\pi_e+e_2\otimes 1)\ \in\ (e_1\otimes 1+\beta\cdot e_2\otimes\pi_e^{1-e})O_{L_e}$,
ce qui équivaut à $\beta^2\pi_e^{2-e}-1=0$, c'est-à-dire $\beta^2=\pi_e^{e-2}$. □

3.3.1.3. Maintenant on *fixe $\widetilde{E}/\mathbb{F}_p$ ordinaire.*
On reprend les notations usuelles $a_p = a_p(\widetilde{E}) = \mathrm{Tr}(\mathrm{Frob}_{\widetilde{E}}) = u+u^{-1}p$, $u\in\mathbb{Z}_p^\times$, et l'on choisit une $\mathbb{Z}_p$-base (e_1,e_2) de $M=\mathbf{M}(\widetilde{E}(p))$ telle que $\varphi e_1 = ue_1$ et $\varphi e_2 = u^{-1}pe_2$. Alors

$$\varphi M\otimes_{\mathbb{Z}_p}\pi_e^{1-e}O_{L_e} \;=\; O_{L_e}(e_1\otimes\pi_e^{1-e})\oplus O_{L_e}(e_2\otimes\pi_e)\ ,$$

$$\mathcal{M} = \mathcal{M}(\widetilde{E}(p)) = O_{L_e}(e_1 \otimes \pi_e^{1-e}) \oplus O_{L_e}(e_2 \otimes 1) ,$$

et $\quad \mathcal{M}/(\varphi M \otimes_{\mathbb{Z}_p} \pi_e^{1-e} O_{L_e}) \simeq O_{L_e}(e_2 \otimes 1)/O_{L_e}(e_2 \otimes \pi_e) \simeq \mathbb{F}_p((e_2 \otimes 1) \bmod \pi_e \mathcal{M})$.

On en déduit que les relèvements de M en un module de Dieudonné sur O_{L_e} , $e < p-1$, correspondent bijectivement aux

$$\mathcal{L} = \mathcal{L}(\beta) = (\beta \cdot e_1 \otimes \pi_e^{1-e} + e_2 \otimes 1) O_{L_e} \quad , \quad \beta \in O_{L_e} .$$

Les mêmes considérations que celles faites précédemment conduisent à :

Proposition 5 :
Soit e tel que $1 < e < p-1$. Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique ordinaire d'invariant modulaire $j(\widetilde{E}) = \tilde{\jmath}$; on pose $m(\tilde{\jmath}) = 1$ si $\tilde{\jmath} \notin \{0, 1728\}$, $m(1728) = 2$ et $m(0) = 3$. Via le choix d'une $\mathbb{Z}_p$-base de diagonalisation de φ dans $\mathrm{M}(\widetilde{E}(p))$, l'association

$$\begin{cases} \mathcal{C}_{O_{L_e}}(\widetilde{E}) & \to & O_{L_e} \\ (\widetilde{E}, \Gamma, \nu) & \mapsto & \beta \text{ tel que } \mathcal{L}(\beta) = \mathrm{M}(\nu)_{L_e}(\mathcal{L}(\Gamma)) \end{cases}$$

induit une bijection entre les classes d'isomorphisme dans $\mathcal{C}_{O_{L_e}}(\widetilde{E})$ et l'ensemble $O_{L_e}/\sim$, où $x \sim y \Leftrightarrow x^{m(\tilde{\jmath})} = y^{m(\tilde{\jmath})}$.

Avec les notations de ci-dessus, pour tout $\beta \in O_{L_e}/\sim$, on note E_β le schéma elliptique sur O_{L_e} (unique à O_{L_e}-isomorphisme près) qui correspond par **ST** à un triplet isomorphe dans $\mathcal{C}_{O_{L_e}}$ à un $(\widetilde{E}, J_\beta, \nu_\beta)$, avec $\mathrm{M}(\nu_\beta)_{L_e}(\mathcal{L}(J_\beta)) = \mathcal{L}(\beta) \subset \mathcal{M}$. Rappelons que β est défini à un élément de $\mathbb{Z}_p^\times$ près.
De même que pour le cas $e = 1$, le Frobenius de $\widetilde{E}$ se relève dans $\mathrm{End}_{\mathcal{SE}_{O_{L_e}}(\widetilde{E})}(E_\beta)$ si et seulement si $\beta = 0$; et si $j(\widetilde{E}) = 0$ ou 1728, alors $j(E_\beta) = 0$ ou 1728 si et seulement si $\beta = 0$.
Donc E_0/O_{L_e} est le relèvement canonique de $\widetilde{E}$.
Soient $\widetilde{E}/\mathbb{F}_p$ et $\widetilde{E}'/\mathbb{F}_p$ deux courbes elliptiques ordinaires. Soient E_0/O_{L_e} et E_0'/O_{L_e} les relèvements canoniques de $\widetilde{E}$ et $\widetilde{E}'$ respectivement. Alors $\mathrm{Hom}_{O_{L_e}}(E_0, E_0') \simeq \mathrm{Hom}_{\mathbb{F}_p}(\widetilde{E}, \widetilde{E}')$.

3.3.2. Groupes p-divisibles sur O_{L_e} associés, $e \in \{2,3,4,6\}$ et $e < p-1$:

Pour toute la suite, $e \in \{2,3,4,6\}$, et l'on choisit $\pi_{12} \in \overline{\mathbb{Q}}_p$ vérifiant $(\pi_{12})^{12} + p = 0$. On pose : $\pi_6 = {\pi_{12}}^2$; $\pi_4 = {\pi_{12}}^3$; $\pi_3 = {\pi_{12}}^4$; $\pi_2 = {\pi_{12}}^6$, et, comme d'habitude, $L_e = \mathbb{Q}_p(\pi_e)$. On a donc $\pi_e^e + p = 0$, et $L_2 \subset L_4$, $L_2 \subset L_6$, et $L_3 \subset L_6$. L'extension $L_e/\mathbb{Q}_p$ est galoisienne si et seulement si $p \equiv 1 \bmod e$. On choisit aussi $\zeta_{12} \in \overline{\mathbb{Q}}_p$ une racine primitive douzième de l'unité, et l'on pose : $\zeta_6 = {\zeta_{12}}^2$; $\zeta_4 = {\zeta_{12}}^3$; $\zeta_3 = {\zeta_{12}}^4$. On suppose en plus que $e < p-1$. Comme $p \geq 5$, on voit que cette condition est toujours satisfaite si $e = 2$ ou 3, mais si $e = 4$ il faut écarter $p = 5$, et si $e = 6$ il faut écarter $p = 5$ et $p = 7$.

On reprend toutes les notations précédentes, en particulier, pour $\widetilde{E}/\mathbb{F}_p$ fixée, $M = \mathrm{M}(\widetilde{E}(p))$. Par le théorème de pleine fidélité de Tate, les classes d'isomorphisme sur O_{L_e} des groupes p-divisibles $E_\beta(p)$ correspondent aux classes d'isomorphisme des $\mathbb{Z}_p[G_{L_e}]$-modules

$T_p(E_\beta) = T_p(E_\beta(p))$, de sorte que l'objet $(M, \mathcal{L}(\beta))$ est aussi une description (à isomorphisme près) du $\mathbb{Z}_p[G_{L_e}]$-module $T_p(E_\beta)$.

3.3.2.1. On fixe $\widetilde{E}/\mathbb{F}_p$ *supersingulière.*
Contrairement au cas $e = 1$, les schémas elliptiques E_β, $\beta \in O_{L_e}$, obtenus ici fournissent une bien plus grande variété de groupes p-divisibles sur O_{L_e}, pour $e \in \{2, 3, 4, 6\}$ fixé.
Soient β, $\beta' \in O_{L_e}$, et soit $\psi : (M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$ un morphisme. Rappelons que ψ est une application $\mathbb{Z}_p$-linéaire $M \to M$ telle que $\psi\varphi = \varphi\psi$ et, si l'on note $\psi_{L_e} = \psi \otimes_{\mathbb{Z}_p} \mathrm{Id}_{L_e}$, telle que $\psi_{L_e}(\mathcal{L}(\beta)) \subset \mathcal{L}(\beta')$. Dans une base (e_1, e_2) de M telle que $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$, la matrice de ψ doit s'écrire

$$\begin{pmatrix} a & -pc \\ c & a \end{pmatrix} \quad , \qquad a, c \in \mathbb{Z}_p \, ,$$

pour commuter avec φ ; c'est une bijection ssi $a \in \mathbb{Z}_p^\times$ (le déterminant est $a^2 + pc^2$). Puis la condition sur les filtrations équivaut à $\psi_{L_e}(\mathcal{L}(\beta) \otimes_{O_{L_e}} L_e) = \mathcal{L}(\beta') \otimes_{O_{L_e}} L_e$, ce qui s'écrit aussi

$$(\mathcal{F}) \qquad c\pi_e^2 \beta\beta' + a\pi_e(\beta' - \beta) + pc = 0 \, , \qquad a, c \in \mathbb{Z}_p \, , \ \beta, \beta' \in O_{L_e} \, .$$

Plus précisément, la relation $(\mathcal{F})$ donne $\psi_{L_e}(\mathcal{L}(\beta)) = \pi_e^n \mathcal{L}(\beta')$, où $n = v_{L_e}(a + c\beta\pi_e)$, et v_{L_e} est la valuation normalisée sur L_e par $v_{L_e}(\pi_e) = 1$ (avec la convention que $\pi_e^n = 0$ si $n = +\infty$).

Prenons pour commencer $e = 2$. Les schémas elliptiques E_β sur $O_{L_2} = \mathbb{Z}_p[\pi_2]$ relevant $\widetilde{E}/\mathbb{F}_p$ sont paramétrés par les filtrations du module de Dieudonné

$$M = \mathrm{M}(\widetilde{E}(p)) = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 \ ; \ \varphi e_1 = e_2 \, , \ \varphi e_2 = -pe_1 \ ; \ \mathcal{L}(\beta) = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_2^{-1}) O_{L_2} \, ,$$

où β parcourt O_{L_2}. Ecrivons $O_{L_2} = \mathbb{Z}_p[\pi_2] = \mathbb{Z}_p \oplus \mathbb{Z}_p\pi_2$, et considérons les objets du type $(M, \mathcal{L}(\beta))$ avec $\beta \in \mathbb{Z}_p\pi_2^i$, $i \in \{0, 1\}$.

- Lorsque β parcourt $\mathbb{Z}_p\pi_2$, on a $\mathcal{L}(\beta) = \mathcal{L}(\alpha) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\pi_2]$, avec $\alpha = \beta\pi_2^{-1} \in \mathbb{Z}_p$ et $\mathcal{L}(\alpha) = (e_1 + \alpha e_2)\mathbb{Z}_p$; en d'autres termes, la filtration $\mathcal{L}(\beta)$ provient d'une filtration sur $\mathbb{Z}_p$. Alors $E_\beta = E_\alpha \times_{\mathbb{Z}_p} \mathbb{Z}_p[\pi_2]$, où E_α est un schéma elliptique sur $\mathbb{Z}_p$ relevant $\widetilde{E}$, et les groupes p-divisibles obtenus avec $\beta \in \mathbb{Z}_p\pi_2$ sont tous isomorphes (cf. la fin de **3.2.3.**).

- Lorsque β parcourt $\mathbb{Z}_p$, la situation est différente. Prenons β, $\beta' \in \mathbb{Z}_p$, et regardons quels sont les morphismes possibles entre $(M, \mathcal{L}(\beta))$ et $(M, \mathcal{L}(\beta'))$. La condition $(\mathcal{F})$ s'écrit alors

$$a(\beta' - \beta)\pi_2 + pc(1 - \beta\beta') = 0 \, ,$$

et comme $\pi_2 \notin \mathbb{Q}_p$, on doit avoir $a(\beta' - \beta) = 0$ et $c(1 - \beta\beta') = 0$. Si $a \neq 0$, alors $\beta = \beta'$; ceci montre que $(M, \mathcal{L}(\beta))$ et $(M, \mathcal{L}(\beta'))$ sont isomorphes ssi $\beta = \beta'$. Si $\beta \neq \beta'$, alors il existe un morphisme non nul ssi $\beta\beta' = 1$; donc pour $\beta \in \mathbb{Z}_p^\times$, $(M, \mathcal{L}(\beta))$ est isogène à $(M, \mathcal{L}(\beta^{-1}))$, et une isogénie possible est, toujours dans la base (e_1, e_2),

$$\begin{pmatrix} 0 & -p \\ 1 & 0 \end{pmatrix} .$$

Comme elle provient d'une isogénie de $\widetilde{E}$, à savoir le Frobenius, on en déduit par Serre-Tate que les schémas elliptiques E_β/O_{L_2} et $E_{\beta^{-1}}/O_{L_2}$, $\beta \in \mathbb{Z}_p^\times$, sont isogènes sur $O_{L_2} = \mathbb{Z}_p[\pi_2]$.

Preuve :
Soient $\beta, \beta' \in O_{L_e}$ et soit ψ un morphisme $(M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$. On rappelle que dans une base (e_1, e_2) de M telle que $\varphi e_1 = e_2, \varphi e_2 = -pe_1$, la matrice de ψ doit être de la forme

$$\begin{pmatrix} a & -pc \\ c & a \end{pmatrix} \quad , \quad a, c \in \mathbb{Z}_p \, ,$$

et alors la condition sur les filtrations s'écrit

$$(\mathcal{F}) \qquad c\pi_e^2 \beta\beta' + a\pi_e(\beta' - \beta) + pc = 0 \, , \qquad a, c \in \mathbb{Z}_p \, , \ \beta, \beta' \in O_{L_e} \, .$$

1) Soient $\beta = \alpha\pi_e^i$, $\beta' = \alpha'\pi_e^i$, $\alpha, \alpha' \in \mathbb{Z}_p$, $0 \leq i \leq e-1$. La condition $(\mathcal{F})$ devient

$$c\alpha\alpha'\pi_e^{2+2i} + a(\alpha' - \alpha)\pi_e^{1+i} + pc = 0 \quad , \quad a, c \in \mathbb{Z}_p \, .$$

- Si $0 \leq i < e-1$ et $2i \neq e-2$, alors la condition $(\mathcal{F})$ force π_e à être racine d'un polynôme de degré $d(i) \leq e-1$ à coefficients dans $\mathbb{Z}_p$, ce qui n'est possible que si ce polynôme est nul. On en déduit $c = 0$, et il existe un morphisme non nul $(M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$ si et seulement si $\alpha = \alpha' \Leftrightarrow \beta = \beta'$.
- Si $2 + 2i = e \Leftrightarrow (e, i) = (4, 1)$ ou $(6, 2)$, la condition $(\mathcal{F})$ devient

$$a(\alpha' - \alpha)\pi_e^{e/2} + pc(1 - \alpha\alpha') = 0 \, ,$$

et comme $\pi_e^{e/2} \notin \mathbb{Q}_p$, on doit avoir $a(\alpha' - \alpha) = 0$ et $c(1 - \alpha\alpha') = 0$. Si $\alpha \neq \alpha'$, alors $a = 0$, et il existe un morphisme non nul $(M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$ si et seulement si $\alpha\alpha' = 1$. Remarquons qu'alors une isogénie possible est donnée par $e_1 \mapsto e_2$, $e_2 \mapsto -pe_1$; comme elle provient d'une isogénie de $\widetilde{E}$ (le Frobenius), on en déduit par Serre-Tate que pour $e \in \{4, 6\}$ et $\alpha \in \mathbb{Z}_p^\times$, les courbes $E_{\alpha^{-1}\pi_e^{(e-2)/2}}$ et $E_{\alpha\pi_e^{(e-2)/2}}$ sont isogènes sur O_{L_e} .
- Si $i = e-1$, alors on retrouve la situation du cas $e = 1$ (i.e. la filtration sur O_{L_e} est obtenue par extension des scalaires à partir d'une filtration définie sur $\mathbb{Z}_p$), et ces modules de Dieudonné sont tous isomorphes. Bien sûr, les courbes obtenues avec $\beta \in \mathbb{Z}_p\pi_e^{e-1}$ sont les restrictions à O_{L_e} des schémas elliptiques sur $\mathbb{Z}_p$ relevant $\widetilde{E}$ décrits en **3.2.3.**.

2) Soient $\beta = \alpha\pi_e^i$ et $\beta' = \alpha'\pi_e^{i'}$, α, $\alpha' \in \mathbb{Z}_p$, $0 \leq i < i' \leq e-1$. La condition $(\mathcal{F})$ s'écrit

$$c\alpha\alpha'\pi_e^{2+i+i'} + a\alpha'\pi_e^{1+i'} - a\alpha\pi_e^{1+i} + pc = 0 \quad , \quad a, c \in \mathbb{Z}_p \, .$$

Le résultat s'en suit en remarquant que $2 + i + i' \equiv 0 \bmod e \Leftrightarrow 2 + i + i' = e$, puis en raisonnant sur cette équation de la même façon que ci-dessus. □

En **3.3.3.** nous allons nous intéresser, ainsi que nous l'avons fait pour $e = 2$, à une sous-famille particulière de relèvements de $\widetilde{E}$ sur $O_{L_e} = \mathbb{Z}_p[\pi_e]$, $e \in \{3, 4, 6\}$, à savoir ceux qui correspondent à des courbes elliptiques définies sur $\mathbb{Q}_p$. Mais auparavant, regardons rapidement comment se comportent les groupes p-divisibles associés à des relèvements ordinaires sur O_{L_e}, $1 < e < p-1$.

3.3.2.2. On *fixe* $\widetilde{E}/\mathbb{F}_p$ *ordinaire.*
On reprend la notation usuelle $a_p = a_p(\widetilde{E}) = \mathrm{Tr}(\mathrm{Frob}_{\widetilde{E}}) = u + u^{-1}p$, $u \in \mathbb{Z}_p^\times$, et l'on choisit une $\mathbb{Z}_p$-base (e_1, e_2) de $M = \mathbf{M}(\widetilde{E}(p))$ telle que $\varphi e_1 = ue_1$ et $\varphi e_2 = u^{-1}pe_2$, de sorte que

$\mathcal{L}(\beta) = (\beta \cdot e_1 \otimes \pi_e^{1-e} + e_2 \otimes 1)O_{L_e}$, $\beta \in O_{L_e}$.
Soient $\beta, \beta' \in O_{L_e}$, et soit $\psi : (M, \mathcal{L}(\beta)) \to (M, \mathcal{L}(\beta'))$ un morphisme dans $\mathbf{MD}_{O_{L_e}}$. La matrice de ψ dans la base (e_1, e_2) doit s'écrire

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad , \quad a, d \in \mathbb{Z}_p \, ,$$

pour commuter avec φ ; c'est une bijection ssi $a \in \mathbb{Z}_p^\times$ et $d \in \mathbb{Z}_p^\times$. Puis $\psi_{L_e}(\mathcal{L}(\beta)) \subset \mathcal{L}(\beta')$ équivaut à $a\beta = d\beta'$. On en déduit :
- $(M, \mathcal{L}(\beta))$ est O_{L_e}-isomorphe à $(M, \mathcal{L}(\beta'))$ ssi il existe $a \in \mathbb{Z}_p^\times$ tel que $\beta' = a\beta$;
- $(M, \mathcal{L}(\beta))$ est O_{L_e}-isogène à $(M, \mathcal{L}(\beta'))$ ssi il existe $x \in \mathbb{Q}_p^\times$ tel que $\beta' = x\beta$.

En particulier, si l'on écrit $O_{L_e} = \mathbb{Z}_p[\pi_e] = \bigoplus_{0 \le i \le e-1} \mathbb{Z}_p \pi_e^i$, et si $\beta = \alpha\pi_e^i$, $\beta' = \alpha'\pi_e^{i'}$, avec $\alpha, \alpha' \in \mathbb{Z}_p$ et $0 \le i, i' \le e-1$, on obtient :
- $(M, \mathcal{L}(\beta))$ est O_{L_e}-isomorphe à $(M, \mathcal{L}(\beta'))$ ssi $i = i'$ et $v_p(\alpha) = v_p(\alpha')$;
- $(M, \mathcal{L}(\beta))$ est O_{L_e}-isogène à $(M, \mathcal{L}(\beta'))$ ssi $[\beta = \beta' = 0]$ ou $[\beta\beta' \neq 0$ et $i = i']$.

Enfin, un raisonnement tout-à-fait similaire à celui fait en **3.2.4.** rmq.4, montre que si $\beta = \alpha\pi_e^i$, $\beta' = \alpha'\pi_e^i$ sont tels que $\alpha' \in \mathbb{Z}\backslash\{0\}$ et $\alpha \in \mathbb{Z}_p\backslash\{0\}$ avec $[\mathbb{Q}(\alpha) : \mathbb{Q}] > 2$, alors les schémas E_β et $E_{\beta'}$ ne sont pas O_{L_e}-isogènes.

3.3.3. Courbes elliptiques sur $\mathbb{Q}_p$ potentiellement supersingulières :

On reprend les hypothèses et notations de **3.3.1.**, en particulier $e \in \{3, 4, 6\}$ et $e < p-1$. Pour chaque $e \in \{3, 4, 6\}$, on s'intéresse au problème suivant : parmi les schémas elliptiques relevant sur $\mathbb{Z}_p[\pi_e]$ une courbe $\widetilde{E}/\mathbb{F}_p$ supersingulière décrits en **3.3.1.**, quels sont ceux qui proviennent d'une courbe elliptique définie sur $\mathbb{Q}_p$? Nous allons chercher celles qui sont définies sur $\mathbb{Q}_p$ et dont le défaut de semi-stabilité est d'ordre e exactement (c'est-à-dire, e est l'indice de ramification minimal d'un corps sur lequel cette courbe acquiert bonne réduction).

Donnons d'abord une condition nécessaire. Soit $E/\mathbb{Q}_p$ une courbe elliptique ayant potentiellement bonne réduction, ce qui équivaut à $j(E) \in \mathbb{Z}_p$. Notons Δ_E le discriminant de E et v_p la valuation sur $\mathbb{Z}_p$ normalisée par $v_p(p) = 1$. Pour $p \ge 5$, le défaut de semi-stabilité de E est donné par

$$e = \mathrm{dst}(E) = \frac{12}{\mathrm{pgcd}(v_p(\Delta_E), 12)} \in \{1, 2, 3, 4, 6\} \, .$$

Une étude élémentaire sur les valuations des coefficients d'une équation de Weierstrass minimale montre que

$$\begin{aligned} e = 3 \text{ ou } 6 \quad &\Longrightarrow \quad j(E) \equiv 0 \bmod p\mathbb{Z}_p \\ e = 4 \quad &\Longrightarrow \quad j(E) \equiv 1728 \bmod p\mathbb{Z}_p \, . \end{aligned}$$

Cela signifie que pour $e \in \{3, 4, 6\}$, la courbe E acquiert bonne réduction sur $L_e = \mathbb{Q}_p(\pi_e)$ (au minimum), et que la fibre spéciale de $E \times_{\mathbb{Q}_p} L_e$ possède un invariant modulaire égal à 0 (resp. 1728) si $e = 3$ ou 6 (resp. $e = 4$). Enfin, ces courbes sur $\mathbb{F}_p$ sont supersingulières ssi $e \mid p+1$, ce dernier fait pouvant aussi se déduire de l'étude du $\mathbb{Q}_p[G]$-module $V_p(E)$ (cf. annexe A).

Ainsi, si l'on veut espérer obtenir des courbes E définies sur $\mathbb{Q}_p$ ayant potentiellement bonne réduction de type supersingulière avec $e = \mathrm{dst}(E) \ge 3$, il nous faut supposer $e \mid p+1$

(ce qui équivaut à dire que $L_e = \mathbb{Q}_p(\pi_e)$ n'est pas une extension galoisienne de $\mathbb{Q}_p$). En particulier, pour satisfaire la condition $e < p-1$, il ne reste plus que le cas $e = 6$ et $p = 5$ à exclure (voir **3.3.1.**).

De plus, et ce pour toute la suite, on fixe $\widetilde{E}/\mathbb{F}_p$ supersingulière telle que $j(\widetilde{E}) = 0$ (resp. $j(\widetilde{E}) = 1728$) si $e = 3$ ou 6 (resp. si $e = 4$).

Remarque : On a vu en **3.1.1.** qu'à $\mathbb{F}_p$-isomorphisme près, il y a 2 courbes sur $\mathbb{F}_p$ ayant un j supersingulier donné, l'une étant un twist d'ordre 2 de l'autre (elles deviennent isomorphes sur $\mathbb{F}_{p^2}$). On verra plus loin que les relèvements (du type de ceux que l'on a en vue) de l'une ou de l'autre fournissent la même famille de représentations. Ce choix nous est donc indifférent.

On rappelle que si l'on choisit un $e_1 \in M$ tel que $e_1 \notin \varphi M$, on pose $\varphi e_1 = e_2$, d'où $\varphi e_2 = -pe_1$ et $M = \mathrm{M}(\widetilde{E}(p)) = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$. Ce choix induit une paramétrisation des relèvements de M en un module de Dieudonné sur O_{L_e} par les filtrations

$$\mathcal{L}(\beta) = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e}) O_{L_e} \quad , \quad \beta \in O_{L_e} \ ,$$

et chacun correspond par Serre-Tate à un schéma elliptique E_β sur O_{L_e} qui relève $\widetilde{E}$. Les relèvements que nous cherchons sont les courbes E_β/L_e qui sont définies sur $\mathbb{Q}_p$ et dont le défaut de semi-stabilité est $e \in \{3,4,6\}$. Nous avons en vue d'appliquer le théorème de prolongement du chapitre 2, et pour cela nous allons nous placer sur la clôture galoisienne de L_e, à savoir $K_e = \mathbb{Q}_{p^2}(\pi_e)$, dont le corps résiduel est $\mathbb{F}_{p^2}$. Mais auparavant, nous allons choisir un générateur particulier du $\mathbb{Z}_p[\varphi]$-module M qui est "adapté" au groupe d'automorphismes de $\widetilde{E}$, ce qui revient à choisir une paramétrisation des relèvements de $\widetilde{E}$ en un schéma elliptique sur O_{L_e}.

On note O_{K_e} l'anneau des entiers de K_e, et $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, $G_{K_e} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K_e)$, $G_{L_e} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/L_e)$, $G_{\mathbb{Q}_{p^2}} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^2})$. Le groupe $G_{K_e/\mathbb{Q}_p} = \mathrm{Gal}(K_e/\mathbb{Q}_p) = < \tau_e > \rtimes < \omega >$ est un produit semi-direct, où τ_e est défini par $\tau_e \pi_e = \zeta_e \pi_e$, $\tau_e \zeta_e = \zeta_e$, et ω est le relèvement du Frobenius absolu qui fixe τ_e et envoie ζ_e sur ζ_e^{-1} ; on a : $\omega \tau_e = {\tau_e}^{-1} \omega$, et bien sûr $< \omega >= \mathrm{Gal}(K_e/L_e)$, $< \tau_e >= I(K_e/\mathbb{Q}_p)$. Enfin, σ est le relèvement du Frobenius absolu agissant sur $W(\mathbb{F}_{p^2}) = \mathbb{Z}_{p^2}$ et sur $\mathbb{Q}_{p^2}$.

Lemme 4 :
Soient L une extension finie de $\mathbb{Q}_p$ totalement ramifiée, $K = L\mathbb{Q}_{p^2}$, et $\mathrm{Gal}(K/L) = \ldots$.
Soient $r \geq 3$ un entier tel que $r \mid p+1$, et $\zeta_r \in \mathbb{Z}_{p^2}$ une racine primitive r-ième de l'unité.
Soient D un $(\varphi, \mathrm{Gal}(K/L))$-module de dimension 2 tel que $\varphi^2 + p = 0$, et R un $\mathbb{Z}_{p^2}$-réseau de D stable par φ.
Supposons qu'il existe un automorphisme $\mathbb{Q}_{p^2}$-linéaire $\xi_r : D \to D$, d'ordre r, de déterminant 1, vérifiant $\xi_r \varphi = \varphi \xi_r$ et $\xi_r \omega = \omega \xi_r^{-1}$.
Alors ξ_r stabilise R, et il existe une $\mathbb{Z}_{p^2}$-base (e_1, e_2) de R, il existe $\epsilon \in (\mathbb{Z}/r\mathbb{Z})^\times$ tels que :

$$\varphi e_1 = e_2 \ , \ \varphi e_2 = -pe_1 \quad ; \quad \omega e_1 = e_1 \ , \ \omega e_2 = e_2 \quad ; \quad \xi_r e_1 = \zeta_r^\epsilon e_1 \ , \ \xi_r e_2 = \zeta_r^{-\epsilon} e_2 \ .$$

Preuve :
On note $D_0 = D^{<\omega>} = \{x \in D \ / \ \omega x = x\}$; du fait que ω agit σ-semi-linéairement sur le $\mathbb{Q}_{p^2}$-espace vectoriel D, on déduit que D_0 est un $\mathbb{Q}_p$-espace vectoriel de dimension 2 tel que

$D_0 \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^2} = D$. De plus, la relation $\omega\varphi = \varphi\omega$ montre que $\varphi D_0 \subset D_0$, et la restriction de φ à D_0 est $\mathbb{Q}_p$-linéaire.

Puis $\xi_r : D \to D$ est un automorphisme $\mathbb{Q}_{p^2}$-linéaire d'ordre $r \mid p+1$, donc diagonalisable dans D puisque son polynôme minimal divise $X^r - 1$, lequel est scindé à racines simples dans $\mathbb{Q}_{p^2}[X]$. Soit (f_1, f_2) une base de diagonalisation ; alors le fait que ξ_r soit de déterminant 1 et d'ordre r impose

$$\xi_r f_1 = \zeta_r^{\epsilon} f_1 \quad , \quad \xi_r f_2 = \zeta_r^{-\epsilon} f_2 \quad , \quad \epsilon \in (\mathbb{Z}/r\mathbb{Z})^{\times} .$$

Comme $r \mid p+1$ et $r \geq 3$, on a $\zeta_r^{\epsilon} \neq \zeta_r^{-\epsilon} = \sigma(\zeta_r^{\epsilon})$. La relation $\xi_r \omega = \omega \xi_r^{-1}$ donne :

$$\begin{cases} \xi_r(\omega f_1) &= \sigma(\zeta_r^{-\epsilon})\omega f_1 &= \zeta_r^{\epsilon}\omega f_1 \\ \xi_r(\omega f_2) &= \sigma(\zeta_r^{\epsilon})\omega f_2 &= \zeta_r^{-\epsilon}\omega f_2 \ , \end{cases}$$

ce qui montre que $\omega f_i \in \mathbb{Q}_{p^2} f_i$ pour $i = 1, 2$. Puis la σ-semi-linéarité de ω implique qu'il existe $e_i \in D_0 \cap \mathbb{Q}_{p^2} f_i$, $i = 1, 2$, non nuls. Maintenant, la relation $\xi_r \varphi = \varphi \xi_r$ donne :

$$\begin{cases} \xi_r(\varphi e_1) &= \sigma(\zeta_r^{\epsilon})\varphi e_1 &= \zeta_r^{-\epsilon}\varphi e_1 \ , \\ \xi_r(\varphi e_2) &= \sigma(\zeta_r^{-\epsilon})\varphi e_2 &= \zeta_r^{\epsilon}\varphi e_2 \ , \end{cases}$$

ce qui montre que $\varphi e_1 \in \mathbb{Q}_{p^2} e_2$ et $\varphi e_2 \in \mathbb{Q}_{p^2} e_1$. Mais $\varphi D_0 \subset D_0$, et donc $\varphi e_1 \in \mathbb{Q}_p e_2$, $\varphi e_2 \in \mathbb{Q}_p e_1$. Comme le déterminant de φ (dans D_0) est p, on obtient $\varphi e_1 = a e_2$, $\varphi e_2 = -p a^{-1} e_1$, $a \in \mathbb{Q}_p^{\times}$. Alors, quitte à changer (e_1, e_2) en $(e_1, a e_2)$, $a \in \mathbb{Q}_p^{\times}$, on en déduit qu'il existe une $\mathbb{Q}_{p^2}$-base (e_1, e_2) de D telle que

$$\varphi e_1 = e_2 \ , \ \varphi e_2 = -p e_1 \quad ; \ \omega e_1 = e_1 \ , \ \omega e_2 = e_2 \quad ; \ \xi_r e_1 = \zeta_r^{\epsilon} e_1 \ , \ \xi_r e_2 = \zeta_r^{-\epsilon} e_2 \ , \ \epsilon \in (\mathbb{Z}/r\mathbb{Z})^{\times} .$$

Soit alors R un $\mathbb{Z}_{p^2}$-réseau de D stable par φ. Comme $\mathbb{Z}_{p^2} e_1 \oplus \mathbb{Z}_{p^2} e_2$ est aussi un $\mathbb{Z}_{p^2}$-réseau de D stable par φ, le lemme 2 de **3.1.2.** montre que, à homothétie près, $R = \mathbb{Z}_{p^2} e_1 \oplus \mathbb{Z}_{p^2} e_2$ ou bien $R = \mathbb{Z}_{p^2} p e_1 \oplus \mathbb{Z}_{p^2} e_2 = \varphi(\mathbb{Z}_{p^2} e_1 \oplus \mathbb{Z}_{p^2} e_2)$. Dans le premier cas le résultat est immédiat ; dans le deuxième cas on remplace (e_1, e_2) par $(e_2, -p e_1)$, ce qui ne fait que changer ϵ en $-\epsilon \in (\mathbb{Z}/r\mathbb{Z})^{\times}$, et l'on obtient la forme voulue. □

Si l'on écrit $R = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$, avec $M = R^{<\omega>} = D_0 \cap R$, alors la $\mathbb{Z}_{p^2}$-base (e_1, e_2) de R vérifiant les propriétés du lemme est aussi une $\mathbb{Z}_p$-base de M. De plus, une autre telle base s'écrit $(u_1 e_1, u_2 e_2)$ avec $u_i \in \mathbb{Z}_p^{\times}$, $i = 1, 2$.

Soit $\widetilde{E}/\mathbb{F}_p$ supersingulière d'invariant modulaire $\tilde{\jmath}(e)$, avec $\tilde{\jmath}(3) = \tilde{\jmath}(6) = 0$ et $\tilde{\jmath}(4) = 1728$; cela équivaut à $[\zeta_e] \in \mathrm{Aut}_{\mathbb{F}_{p^2}}(\widetilde{E})$. Notons f le Frobenius arithmétique agissant sur $\widetilde{E}$ (il vérifie $f^2 + p = 0$). Rappelons que les morphismes f et $[\zeta_e]$ de la courbe $\widetilde{E}$ sont définis sur $\mathbb{F}_p$ et $\mathbb{F}_{p^2}$ respectivement, et qu'ils sont donnés au niveau des points par ([Silv 1]) :

$$f : \begin{cases} \widetilde{E}(\overline{\mathbb{F}}_p) &\to \widetilde{E}(\overline{\mathbb{F}}_p) \\ (x, y) &\mapsto (x^p, y^p) \end{cases} \qquad \text{et} \qquad [\zeta_e] : \begin{cases} \widetilde{E}(\overline{\mathbb{F}}_p) &\to \widetilde{E}(\overline{\mathbb{F}}_p) \\ (x, y) &\mapsto (\zeta_e^2 x, \zeta_e^3 y) \end{cases}$$

Comme $p \equiv -1 \bmod e\mathbb{Z}$, on a $[\zeta_e] f = f [\zeta_e]^{-1}$. Dans $M = \mathbf{M}(\widetilde{E}(p))$, on a $\mathbf{M}(f(p)) = \varphi$, et dans $R = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$, notons $\xi_e = \mathbf{M}_{\mathbb{F}_{p^2}}([\zeta_e](p))$. Alors φ est un endomorphisme σ-semi-linéaire de R vérifiant $\varphi^2 + p = 0$, et ξ_e est un automorphisme $\mathbb{Z}_{p^2}$-linéaire de R d'ordre $e \mid p+1$ et de déterminant 1, dont le polynôme minimal est $X^2 - (\zeta_e + \zeta_e^{-1})X + 1 = X^2 - \gamma_e X + 1 \in \mathbb{Z}[X]$, avec

$\gamma_e = -1, 0, 1$ si $e = 3, 4, 6$ respectivement. L'objet $D = M \otimes_{\mathbb{Z}_p} \mathbb{Q}_{p^2}$ est un $(\varphi, \mathrm{Gal}(K_e/L_e))$-module de dimension 2, dans lequel la relation $[\zeta_e]f = f[\zeta_e]^{-1}$ dans $\widetilde{E}$ se traduit par les relations $\xi_e\varphi = \varphi\xi_e$ et $\omega\xi_e = \xi_e^{-1}\omega$.
Maintenant on applique le lemme précédent (avec $r = e$) : il existe une $\mathbb{Z}_{p^2}$-base (e_1, e_2) de $R = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$, et il existe $\eta \in (\mathbb{Z}/e\mathbb{Z})^\times = \{\pm 1\}$ tels que

$$\varphi e_1 = e_2 \ , \ \varphi e_2 = -pe_1 \quad ; \quad \omega e_1 = e_1 \ , \ \omega e_2 = e_2 \quad ; \quad \xi_e e_1 = \zeta_e^\eta e_1 \ , \ \xi_e e_2 = \zeta_e^{-\eta} e_2 \ .$$

En particulier, e_1 est un générateur du $\mathbb{Z}_p[\varphi]$-module M, et ce choix induit une paramétrisation des relèvements de $\widetilde{E}$ en un schéma elliptique sur O_{L_e}. On dira que ce choix est *"adapté"* au groupe d'automorphismes de $\widetilde{E}$; il est unique à un élément de $\mathbb{Z}_p^\times$ près.

Proposition 6 :
Soient $e \in \{3, 4, 6\}$, et $p \geq 5$ tel que $e \mid p+1$ et $e < p-1$. Soit $\widetilde{E}/\mathbb{F}_p$ supersingulière d'invariant modulaire $\tilde{\jmath}(e)$, avec $\tilde{\jmath}(3) = \tilde{\jmath}(6) = 0$ et $\tilde{\jmath}(4) = 1728$.
On choisit un générateur du $\mathbb{Z}_p[\varphi]$-module $\mathrm{M}(\widetilde{E}(p))$ "adapté" au groupe d'automorphismes de $\widetilde{E}$. Dans la description des relèvements E_β de $\widetilde{E}$ en un schéma elliptique sur $\mathbb{Z}_p[\pi_e]$ induite par ce choix, ceux qui proviennent d'une courbe elliptique définie sur $\mathbb{Q}_p$ ayant potentiellement bonne réduction avec un défaut de semi-stabilité e sont les $\{E_\beta \ , \ \beta \in \mathbb{Z}_p\pi_e \cup \mathbb{Z}_p\pi_e^{e-3}\}$. De plus, $j(E_\beta) = 0$ ou 1728 si et seulement si $\beta = 0$.

Preuve :
On fixe un générateur e_1 du $\mathbb{Z}_p[\varphi]$-module $M = \mathrm{M}(\widetilde{E}(p))$ tel que, avec les notations ci-dessus et pour $\eta \in (\mathbb{Z}/e\mathbb{Z})^\times = \{\pm 1\}$: $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$, $\omega e_1 = e_1$, $\omega e_2 = e_2$, $\xi_e e_1 = \zeta_e^\eta e_1$, $\xi_e e_2 = \zeta_e^{-\eta} e_2$. Alors, via ce choix, les relèvements de $\widetilde{E}$ en un schéma elliptique E_β sur O_{L_e} sont paramétrés par les filtrations $\mathcal{L}(\beta) = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e})O_{L_e}$, $\beta \in O_{L_e}$.

Montrons d'abord la dernière assertion. Soit $\beta \in O_{L_e} = \mathbb{Z}_p[\pi_e]$; alors $j(E_\beta) = 0$ (resp. 1728) si et seulement $[\zeta_e] \in \mathrm{Aut}(E_\beta) = \mathrm{Aut}_{O_{K_e}}(E_\beta)$ avec $e = 3$ ou 6 (resp. $e = 4$). On sait que $[\zeta_e] \in \mathrm{Aut}_{\mathbb{F}_{p^2}}(\widetilde{E})$ se relève dans $\mathrm{Aut}_{O_{K_e}}(E_\beta)$ si et seulement si ξ_e stabilise, après extension des scalaires, la filtration $\mathcal{L}(\beta) \otimes_{O_{L_e}} O_{K_e} = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e})O_{K_e}$. Cette condition équivaut à :
$e_1 \otimes \zeta_e^\eta + \beta \cdot e_2 \otimes \zeta_e^{-\eta}\pi_e^{1-e} \in (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e})O_{K_e} \Leftrightarrow (\zeta_e^\eta - \zeta_e^{-\eta})\pi_e^{1-e}\beta = 0 \Leftrightarrow \beta = 0.$

Montrons maintenant la première assertion. Soit $\beta \in O_{L_e}$. Notons encore E_β le schéma elliptique $E_\beta \times_{O_{L_e}} O_{K_e}$; le polynôme caractéristique du Frobenius arithmétique (relatif à $\mathbb{F}_{p^2}$) agissant sur $E_\beta \times_{O_{K_e}} \mathbb{F}_{p^2} = \widetilde{E} \times_{\mathbb{F}_p} \mathbb{F}_{p^2}$ est $X^2 - 2pX + p^2 = (X-p)^2$, de discriminant $\delta = 0$. Le théorème de prolongement du chapitre 2 nous dit que E_β est définie sur $\mathbb{Q}_p$ avec un défaut de semi-stabilité e si et seulement si l'action de G_{K_e} sur $T_p(E_\beta)$ s'étend en une action de G, dont la restriction à $G_{\mathbb{Q}_{p^2}}$ induit une injection $< \tau_e > \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_{p^2}[\varphi]}(\mathbf{D}^*_{\mathbf{cris},K_e}(V_p(E_\beta)))$ provenant d'une injection $< \tilde{\tau}_e > \hookrightarrow \mathrm{Aut}_{\mathbb{F}_{p^2}}(\widetilde{E})$. En effet, la dernière hypothèse permet de montrer que E_β est définie sur $\mathbb{Q}_{p^2}$, avec le bon défaut de semi-stabilité ; puis la proposition 1 de **2.1.3.** permet de "recoller" le tout : E_β est déjà définie sur L_e, et $K_e = L_e\mathbb{Q}_{p^2}$, $L_e \cap \mathbb{Q}_{p^2} = \mathbb{Q}_p$, avec $I(K_e/\mathbb{Q}_p)$ invariant dans $G_{K_e/\mathbb{Q}_p}$.

L'objet $D = M \otimes_{\mathbb{Z}_p} \mathbb{Q}_{p^2} = \mathrm{M}(\widetilde{E}(p)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_{p^2}$ devient un objet de $\mathbf{MF}_{K_e}(\varphi)$ en étendant

σ-semi-linéairement φ à D et en posant :

$$\begin{cases} \mathrm{Fil}^i D_{K_e} &= D_{K_e} & \text{pour } i \leq 0 \\ \mathrm{Fil}^1 D_{K_e} &= \mathcal{L}(\beta) \otimes_{O_{L_e}} K_e &= (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e}) K_e \\ \mathrm{Fil}^i D_{K_e} &= 0 & \text{pour } i \geq 2 \ , \end{cases}$$

et l'on a $D \simeq \mathbf{D}^*_{\mathrm{cris},K_e}(V_p(E_\beta))$ dans $\mathbf{MF}_{K_e}(\varphi)$. Le $\mathbb{Z}_p[G_{K_e}]$-module $T_p(E_\beta)$ correspond alors à l'objet $(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}, \mathcal{L}(\beta) \otimes_{O_{L_e}} O_{K_e}) \subset (D, \mathcal{L}(\beta) \otimes_{O_{L_e}} K_e)$. Dire que l'action de G_{K_e} s'étend en une action de G sur $T_p(E_\beta)$ revient à munir $(D, \mathrm{Fil}^i D_{K_e})$ d'une structure d'objet de $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$ qui stabilise $(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}, \mathcal{L}(\beta) \otimes_{O_{L_e}} O_{K_e})$.
Les hypothèses faites sur l'action prolongée impliquent que $\tau_e = \xi_e$ ou bien $\tau_e = \xi_e^{-1}$; en particulier, on a bien les relations $\tau_e \omega = \omega \tau_e^{-1}$ et $\tau_e \varphi = \varphi \tau_e$, et τ_e stabilise $(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}, \mathcal{L}(\beta) \otimes_{O_{L_e}} O_{K_e})$. On a donc :

$$\tau_e e_1 = \zeta_e^\epsilon e_1 \ , \ \tau_e e_2 = \zeta_e^{-\epsilon} e_2 \ \ , \ \epsilon \in (\mathbb{Z}/e\mathbb{Z})^\times = \{\pm 1\}.$$

Maintenant écrivons que l'action de $G_{K_e/\mathbb{Q}_p}$ étendue par semi-linéarité à $D_{K_e} = M \otimes_{\mathbb{Z}_p} K_e$ stabilise la filtration $\mathcal{L}(\beta) \otimes_{O_{L_e}} K_e = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e}) K_e$. C'est automatique en ce qui concerne ω, puisque $\beta \in O_{L_e}$. Puis τ_e stabilise la filtration si et seulement si $\tau_e \cdot (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e}) = e_1 \otimes \zeta_e^\epsilon + \tau_e(\beta) \cdot e_2 \otimes \zeta_e^{-\epsilon} \pi_e^{1-e} \in \mathcal{L}(\beta)$, c'est-à-dire

$$\tau_e \beta = \zeta_e^{2\epsilon - 1} \beta \quad \Leftrightarrow \quad \tau_e(\pi_e^{-2\epsilon+1} \beta) = \pi_e^{-2\epsilon+1} \beta \ .$$

Donc $\pi_e^{-2\epsilon+1} \beta \in \mathbb{Q}_{p^2}$, et comme $\beta \in L_e$, on a en fait $\pi_e^{-2\epsilon+1} \beta \in \mathbb{Q}_p$. Finalement, en écrivant que $\beta \in O_{L_e}$, et en utilisant $\pi_e^e = -p$, on obtient : pour $\epsilon = 1$, $\beta \in \mathbb{Z}_p \pi_e$; pour $\epsilon = -1$, $\beta \in \mathbb{Z}_p \pi_e^{e-3}$. □

Remarque 1 :

- Si $e = 3$, alors $\mathbb{Z}_p \pi_e \cup \mathbb{Z}_p \pi_e^{e-3} = \mathbb{Z}_p \pi_3 \sqcup \mathbb{Z}_p$.
Pour $\beta \in \mathbb{Z}_p \pi_3 \setminus \{0\}$ (resp. $\beta \in \mathbb{Z}_p \setminus \{0\}$) fixé, il n'y a, à $\mathbb{Q}_p$-isomorphisme près, qu'une seule courbe qui prolonge E_β sur $\mathbb{Q}_p$ avec un défaut de semi-stabilité égal à 3, et elle correspond à une action prolongée de τ_3 avec $\epsilon = 1$ (resp. $\epsilon = -1$).
Si $\beta = 0$, il y a deux courbes qui prolongent E_0 avec un défaut de semi-stabilité égal à 3, l'une correspondant à une action prolongée avec $\epsilon = 1$, l'autre avec $\epsilon = -1$. Par ailleurs, E_0 se prolonge aussi en un schéma elliptique $\mathcal{E}_0$ sur $\mathbb{Z}_p$, et comme $j(E_0) = 0$, les deux courbes mentionnées ci-dessus sont des twists convenables de $\mathcal{E}_0$, correspondant aux éléments $(-p)^4$ et $(-p)^2$ de $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^6 \simeq \mathrm{Twist}((\mathcal{E}_0, \mathbf{0}), \mathbb{Q}_p)$ (cf. les exemples du chapitre 1).

- Si $e = 4$, alors $\mathbb{Z}_p \pi_e \cup \mathbb{Z}_p \pi_e^{e-3} = \mathbb{Z}_p \pi_4$.
Pour $\beta \in \mathbb{Z}_p \pi_4$ fixé, il y a deux courbes qui prolongent E_β sur $\mathbb{Q}_p$ avec un défaut de semi-stabilité égal à 4, chacune correspondant à une action prolongée de τ_4 avec $\epsilon = 1$ ou $\epsilon = -1$, et l'une est un twist sur $\mathbb{Q}_p(\pi_2)$ de l'autre.
Si $\beta = 0$, E_0 se prolonge aussi en un schéma elliptique $\mathcal{E}_0$ sur $\mathbb{Z}_p$, et comme $j(E_0) = 1728$, les deux courbes mentionnées ci-dessus sont des twists convenables de $\mathcal{E}_0$, correspondant aux éléments $(-p)^3$ et $(-p)$ de $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^4 \simeq \mathrm{Twist}((\mathcal{E}_0, \mathbf{0}), \mathbb{Q}_p)$ (cf. les exemples du chapitre 1).

- Si $e = 6$, alors $\mathbb{Z}_p \pi_e \cup \mathbb{Z}_p \pi_e^{e-3} = \mathbb{Z}_p \pi_6 \sqcup \mathbb{Z}_p \pi_6^3$.
Pour $\beta \in \mathbb{Z}_p \pi_6 \setminus \{0\}$ (resp. $\beta \in \mathbb{Z}_p \pi_6^3 \setminus \{0\}$) fixé, il n'y a qu'une seule courbe qui prolonge E_β sur $\mathbb{Q}_p$ avec un défaut de semi-stabilité égal à 6, et elle correspond à une action prolongée de

τ_6 avec $\epsilon = 1$ (resp. $\epsilon = -1$).
Si $\beta = 0$, il y en a deux, l'une correspondant à une action prolongée avec $\epsilon = 1$, l'autre avec $\epsilon = -1$. Comme $j(E_0) = 0$, si $\mathcal{E}_0$ est le schéma elliptique sur $\mathbf{Z}_p$ qui prolonge E_0, les deux courbes mentionnées ci-dessus sont des twists convenables de $\mathcal{E}_0$, correspondant aux éléments $(-p)^5$ et $(-p)$ de $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^6 \simeq \mathrm{Twist}((\mathcal{E}_0, \mathbf{0}), \mathbb{Q}_p)$ (cf. les exemples du chapitre 1).

Remarque 2 : Soit $e \in \{3, 4, 6\}$; le lemme 3 de **3.3.2.1.** donne :
- Les modules de Dieudonné $(M, \mathcal{L}(\beta))$, $\beta \in \mathbf{Z}_p\pi_e \cup \mathbf{Z}_p\pi_e^{e-3}$, sont deux-à-deux non-isomorphes sur O_{L_e}.
- Si $\alpha \in \mathbf{Z}_p^\times$, alors $(M, \mathcal{L}(\alpha\pi_e^{e-3}))$ est O_{L_e}-isogène à $(M, \mathcal{L}(\alpha^{-1}\pi_e))$ (pour $e \neq 4$, c'est le *2)* du lemme 3, et pour $e = 4$, c'est le *1)*) ; une isogénie possible est donnée par $e_1 \mapsto e_2$, $e_2 \mapsto -pe_1$, et comme elle provient d'une isogénie de $\widetilde{E}$, à savoir le Frobenius, on en déduit que les courbes elliptiques $E_{\alpha^{-1}\pi_e}$ et $E_{\alpha\pi_e^{e-3}}$ sont isogènes sur O_{L_e}. Soient $\mathcal{E}$ et $\mathcal{E}'$ les courbes elliptiques sur $\mathbb{Q}_p$ prolongeant $E_{\alpha^{-1}\pi_e}$ et $E_{\alpha\pi_e^{e-3}}$ respectivement. Les objets $D = \mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}))$ et $D' = \mathbf{D}^*_{\mathbf{pcris}}(V_p(\mathcal{E}'))$ sont dans $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$; ils sont décrits par :
$D = \mathbb{Q}_{p^2}e_1 \oplus \mathbb{Q}_{p^2}e_2$, $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$, $\omega e_1 = e_1$, $\omega e_2 = e_2$, $\tau_e e_1 = \zeta_e e_1$, $\tau_e e_2 = \zeta_e{}^{-1} e_2$,
$\mathrm{Fil}^1(D \otimes_{\mathbb{Q}_{p^2}} K_e) = (e_1 \otimes 1 + \alpha^{-1} \cdot e_2 \otimes \pi_e^{2-e})K_e$,
$D' = \mathbb{Q}_{p^2}e'_1 \oplus \mathbb{Q}_{p^2}e'_2$, $\varphi e'_1 = e'_2$, $\varphi e'_2 = -pe'_1$, $\omega e'_1 = e'_1$, $\omega e'_2 = e'_2$, $\tau_e e'_1 = \zeta_e{}^{-1} e'_1$, $\tau_e e'_2 = \zeta_e e'_2$,
$\mathrm{Fil}^1(D \otimes_{\mathbb{Q}_{p^2}} K_e) = (e'_1 \otimes 1 + \alpha \cdot e'_2 \otimes \pi_e^{-2})K_e$.
La O_{L_e}-isogénie mentionnée ci-dessus induit un morphisme $f : D' \to D$ d'objets de $\mathbf{MF}_{K_e}(\varphi)$ donné par $f(e'_1) = e_2$ et $f(e'_2) = -pe_1$. On vérifie que f commute à l'action de $G_{K_e/\mathbb{Q}_p}$, de sorte que f est un morphisme d'objets de $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$. L'injection

$$\mathrm{Hom}_{K_e}(\mathcal{E}, \mathcal{E}') \hookrightarrow \mathrm{Hom}_{\mathbb{Q}_p[G_{K_e}]}(V_p(\mathcal{E}), V_p(\mathcal{E}')) \simeq \mathrm{Hom}_{\mathbf{MF}_{K_e}(\varphi)}(D', D)$$

montre que f est définie sur $\mathbb{Q}_p$; donc $\mathcal{E}$ et $\mathcal{E}'$ sont isogènes sur $\mathbb{Q}_p$.
Dans tous les autres cas, les modules de Dieudonné $(M, \mathcal{L}(\beta))$, $\beta \in \mathbf{Z}_p\pi_e \cup \mathbf{Z}_p\pi_e^{e-3}$, ne sont pas O_{L_e}-isogènes ; en particulier, les $V_p(E_\beta)$ correspondants ne sont pas $\mathbb{Q}_p[G_{L_e}]$-isomorphes.

Remarque 3, sur les cas ordinaires :

Soit $e \in \{3, 4, 6\}$ tel que $e < p - 1$. On fixe une courbe elliptique $\widetilde{E}/\mathbb{F}_p$ *ordinaire.*

Prenons un schéma elliptique E/O_{L_e} relevant $\widetilde{E}$. Supposons qu'il est isogène sur O_{L_e} à un schéma E'/O_{L_e} qui est défini sur $\mathbb{Q}_p$ avec un défaut de semi-stabilité e. Soit $\widetilde{E}'$ la fibre spéciale de E'. La remarque du début de **3.3.3.** étant aussi valable dans les cas ordinaires, on voit que l'on doit avoir $j(\widetilde{E}') = 0$ (resp. $j(\widetilde{E}') = 1728$) si $e = 3$ ou 6 (resp. si $e = 4$) ; en particulier, $\widetilde{E}'$ étant ordinaire (puisqu'isogène à $\widetilde{E}$), l'entier $e \in \{3, 4, 6\}$ doit diviser $p - 1$ (cf. rmq. 4 de **3.1.1.**).

On suppose donc que $e \mid p - 1$; pour satisfaire $e < p - 1$, il faut écarter les valeurs $(e, p) = (4, 5)$ ainsi que $(e, p) = (6, 7)$ (cf. **3.3.1.**). L'extension $L_e = \mathbb{Q}_p(\pi_e)$ est cyclique, de groupe de Galois engendré par un élément τ_e vérifiant $\tau_e\pi_e = \zeta_e\pi_e$.
Comme $\widetilde{E}$ est ordinaire, le discriminant du polynôme caractéristique du Frobenius n'est pas nul. Le théorème de prolongement implique (cf. théorème 3 de **2.4.4.**) qu'un schéma elliptique A/O_{L_e} relevant $\widetilde{E}$ est *isogène* sur O_{L_e} à une courbe elliptique définie sur $\mathbb{Q}_p$ avec

un défaut de semi-stabilité e, si et seulement si l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L_e)$ sur $V_p(A)$ se prolonge en une action de $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, définie sur $\mathbb{Q}$, de déterminant le caractère cyclotomique, et qui induit une injection $<\tau_e> \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_p[\varphi]}(\mathbf{D}^*_{\mathbf{cris},L_e}(V_p(A)))$.

On écrit encore $a_p = a_p(\widetilde{E}) = \mathrm{Tr}(\mathrm{Frob}_{\widetilde{E}}) = u + u^{-1}p$, $u \in \mathbb{Z}_p^\times$.
Soit $\beta \in O_{L_e}$, et soit E_β/O_{L_e} l'un des schémas elliptiques relevant $\widetilde{E}$ décrits en **3.3.1.3.** (si $j(\widetilde{E}) \notin \{0, 1728\}$, il est unique à L_e-isomorphisme près). Alors $\mathbf{D}^*_{\mathbf{cris},L_e}(V_p(E_\beta))$ est isomorphe dans $\mathbf{MF}_{L_e}(\varphi)$ à l'objet décrit par :

$$D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2 \quad ; \quad \varphi e_1 = u e_1 \ , \ \varphi e_2 = u^{-1} p e_2 \ ;$$
$$\begin{cases} \mathrm{Fil}^i D_{L_e} = D_{L_e} & \text{pour } i \leq 0 \\ \mathrm{Fil}^1 D_{L_e} = \mathcal{L}(\beta) \otimes_{O_{L_e}} L_e = (\beta \cdot e_1 \otimes \pi_e^{1-e} + e_2 \otimes 1) L_e \\ \mathrm{Fil}^i D_{L_e} = 0 & \text{pour } i \geq 2 \ , \end{cases}$$

L'action de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/L_e)$ sur $V_p(E_\beta)$ se prolonge en une action de G avec les conditions mentionnées ci-dessus, si et seulement si on peut définir une application $\mathbb{Q}_p$-linéaire $\tau_e : D \to D$ d'ordre exact e et de déterminant 1, telle que $\tau_e \varphi = \varphi \tau_e$, $\mathrm{Tr}(\tau_e \varphi) \in \mathbb{Q}$, et $\tau_e \cdot (\mathrm{Fil}^1 D_{L_e}) = \mathrm{Fil}^1 D_{L_e}$. Toutes ces conditions équivalent à :
- il existe $\epsilon \in \{-1, 1\}$ tel que $\tau_e e_1 = \zeta_e^\epsilon e_1$ et $\tau_e e_2 = \zeta_e^{-\epsilon} e_2$;
- la trace du Frobenius vérifie $a_p \in \mathcal{N}_{p,e}^\times = \{a \in \mathbb{Z}/(\gamma_e^2 - 4)(a^2 - 4p) \in (\mathbb{Q}^\times)^2\}$, avec $\gamma_e = -1, 0, 1$ pour $e = 3, 4, 6$ respectivement ;
- on a $\tau_e(\beta) = \zeta_e^{-2\epsilon-1}\beta$, i.e. $\pi_e^{2\epsilon+1}\beta \in \mathbb{Q}_p$.

Finalement, on en déduit que E_β/O_{L_e} est O_{L_e}-isogène à un schéma elliptique défini sur $\mathbb{Q}_p$ avec un défaut de semi-stabilité e, si et seulement si $a_p \in \mathcal{N}_{p,e}^\times$ et $\beta \in \mathbb{Z}_p \pi_e^{e-3}$ (correspondant à une action prolongée avec $\epsilon = 1$) ou bien $\beta \in \mathbb{Z}_p \pi_e$ (correspondant à une action prolongée avec $\epsilon = -1$).

Soient $\widetilde{E}$ et $\widetilde{E}'$ deux courbes elliptiques ordinaires sur $\mathbb{F}_p$ telles que $a_p(\widetilde{E}) = a_p(\widetilde{E}') \in \mathcal{N}_{p,e}^\times$; soient $\beta, \beta' \in O_{L_e}$ et E_β et $E_{\beta'}$ des schémas elliptiques sur O_{L_e} relevant $\widetilde{E}$ et $\widetilde{E}'$ respectivement. On suppose que $\beta, \beta' \in \mathbb{Z}_p \pi_e^{e-3}$ *ou* $\beta, \beta' \in \mathbb{Z}_p \pi_e$; soient $\mathcal{E}_{\beta,\epsilon}$ et $\mathcal{E}'_{\beta',\epsilon}$ les courbes elliptiques sur $\mathbb{Q}_p$ qui sont O_{L_e}-isogènes à E_β et $E_{\beta'}$ respectivement ($\epsilon \in \{\pm 1\}$). Du fait que tout morphisme commutant avec les Frobenius commute avec τ_e dans $\mathbf{D}^*_{\mathbf{cris},K_e/\mathbb{Q}_p}(V_p(\mathcal{E}_{\beta,\epsilon}))$ et $\mathbf{D}^*_{\mathbf{cris},K_e/\mathbb{Q}_p}(V_p(\mathcal{E}'_{\beta',\epsilon}))$, on déduit que toute O_{L_e}-isogénie $E_\beta \to E_{\beta'}$ se prolonge en une $\mathbb{Q}_p$-isogénie $\mathcal{E}_{\beta,\epsilon} \to \mathcal{E}'_{\beta',\epsilon}$, i.e.

$$\mathrm{Hom}_{\mathbb{Q}_p}(\mathcal{E}_{\beta,\epsilon}, \mathcal{E}'_{\beta',\epsilon}) \simeq \mathrm{Hom}_{O_{L_e}}(E_\beta, E_{\beta'}).$$

En particulier, on obtient que les courbes $\mathcal{E}_{0,\epsilon}$ et $\mathcal{E}'_{0,\epsilon}$ sont $\mathbb{Q}_p$-isogènes. De plus, à $\mathbb{Q}_p$-isomorphisme près, il n'y a qu'un nombre fini de courbes $E/\mathbb{Q}_p$ telles que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E)) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e}; \mathbf{a_p}; \epsilon; \mathbf{0})$ pour $(e; a_p; \epsilon)$ fixé.

3.3.4. Fin de la preuve du théorème 2.1. du chapitre 1 :

Soit $e \in \{3, 4, 6\}$, et soit $p \geq 5$ tel que $e \mid p + 1$. On reprend les notations de **3.3.3.**, en particulier $K_e = \mathbb{Q}_{p^2}(\pi_e)$ avec $\pi_e^e = -p$, et $G_{K_e/\mathbb{Q}_p} = <\tau_e> \rtimes <\omega>$.

Pour $e \in \{3, 4, 6\}$ tel que $e \mid p + 1$, on a défini au chapitre 1 (en **1.3.1.2.**) les objets $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e}; \mathbf{0}; \alpha)$, $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, de $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$ et de poids Hodge-Tate (0,1) suivants :

$\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha) = \mathbb{Q}_{p^2}e_1 \oplus \mathbb{Q}_{p^2}e_2$, avec $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$; $\omega e_1 = e_1$, $\omega e_2 = e_2$; $\tau_e e_1 = \zeta_e e_1$, $\tau_e e_2 = \zeta_e{}^{-1} e_2$; $\mathrm{Fil}^1(\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha) \otimes_{\mathbb{Q}_{p^2}} K_e) = (\alpha \cdot e_1 \otimes \pi_e{}^{-1} + e_2 \otimes \pi_e)K_e$.
Ces objets sont deux-à-deux non-isomorphes dans $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$. Nous allons maintenant montrer, comme conséquence du travail fait précédemment, que chacune de ces représentations provient d'une courbe elliptique définie sur $\mathbb{Q}_p$; cela achèvera la preuve du théorème **2.1.** du chapitre 1, lequel donne une description complète des classes d'isomorphisme d'objets de $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ provenant d'une courbe elliptique, où G est le groupe de Galois absolu de $\mathbb{Q}_p$.

On suppose $e < p-1$, donc $(e,p) \neq (6,5)$. Soit $\widetilde{E}/\mathbb{F}_p$ supersingulière d'invariant modulaire $\tilde{\jmath}(e)$, avec $\tilde{\jmath}(3) = \tilde{\jmath}(6) = 0$ et $\tilde{\jmath}(4) = 1728$.

Pour $\epsilon \in \{-1,1\}$ et $\alpha \in \mathbb{Z}_p$, on note $E(e;\epsilon,\alpha)$ la courbe elliptique qui correspond dans la description de **3.3.3.** au relèvement de $\widetilde{E}$ en un schéma elliptique E_β sur $\mathbb{Z}_p[\pi_e]$ avec $\beta = \alpha(-p)^{\frac{1-\epsilon}{2}}\pi_e^{2\epsilon-1}$; on a donc $\beta = \alpha\pi_e$ si $\epsilon = 1$, et $\beta = \alpha\pi_e^{e-3}$ si $\epsilon = -1$. D'après **3.3.3.**, on sait que ces courbes sont définies sur $\mathbb{Q}_p$ avec un défaut de semi-stabilité e. De plus, on sait que $D(e;\epsilon,\alpha) = \mathbf{D}^*_{\mathbf{pcris}}(V_p(E(e;\epsilon,\alpha)))$ est un objet de $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$ de poids Hodge-Tate (0,1) dans lequel il existe une $\mathbb{Q}_{p^2}$-base (e_1,e_2) telle que :

$$\varphi e_1 = e_2 \ , \ \varphi e_2 = -pe_1 \quad ; \quad \omega e_1 = e_1 \ , \ \omega e_2 = e_2 \quad ; \quad \tau_e e_1 = \zeta_e^{\epsilon} e_1 \ , \ \tau_e e_2 = \zeta_e^{-\epsilon} e_2 \ ;$$

$$\mathrm{Fil}^1(D(e;\epsilon,\alpha) \otimes_{\mathbb{Q}_{p^2}} K_e) = \mathcal{L}(\pi_e^{2\epsilon-1}(-p)^{\frac{1-\epsilon}{2}}\alpha) \otimes_{\mathbb{Z}_p[\pi_e]} K_e = (e_1 \otimes 1 + (-p)^{\frac{1-\epsilon}{2}}\alpha \cdot e_2 \otimes \pi_e^{2\epsilon-e})K_e \ .$$

Ecrivons ces objets sous la forme $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$, $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, comme ci-dessus.

- Si $\epsilon = 1$, on a $\tau_e e_1 = \zeta_e e_1$, $\tau_e e_2 = \zeta_e^{-1} e_2$, et la filtration s'écrit $\mathrm{Fil}^1(D(e;1,\alpha) \otimes_{\mathbb{Q}_{p^2}} K_e) = (e_1 \otimes 1 + \alpha \cdot e_2 \otimes \pi_e^{2-e})K_e = (-p\alpha^{-1} \cdot e_1 \otimes \pi_e{}^{-1} + e_2 \otimes \pi_e)K_e$, avec la convention $\alpha^{-1} = \infty \in \mathbb{P}^1(\mathbb{Q}_p)$ si $\alpha = 0$. Alors on voit que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E(e;1,\alpha))) = D(e;1,\alpha) = \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\mathbf{-p\alpha^{-1}})$, et lorsque α parcourt $\mathbb{Z}_p$, $-p\alpha^{-1}$ parcourt $\{x \in \mathbb{P}^1(\mathbb{Q}_p) \ , \ v_p(x) \leq 1\}$, où v_p est la valuation normalisée sur $\mathbb{Q}_p$ (avec la convention $v_p(\infty) = -\infty$).

- Si $\epsilon = -1$, on a $\tau_e e_1 = \zeta_e^{-1} e_1$, $\tau_e e_2 = \zeta_e e_2$, et la filtration s'écrit $\mathrm{Fil}^1(D(e;-1,\alpha) \otimes_{\mathbb{Q}_{p^2}} K_e) = (e_1 \otimes 1 + \alpha \cdot e_2 \otimes \pi_e^{-2})K_e = (e_1 \otimes \pi_e + \alpha \cdot e_2 \otimes \pi_e{}^{-1})K_e$. Lorsqu'on applique à $D(e;-1,\alpha)$ la transformation $\mathbb{Q}_{p^2}$-linéaire donnée par $e_1 \mapsto e_2'$, $e_2 \mapsto -pe_1'$, on constate qu'il est isomorphe dans $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$ à un objet $D = \mathbb{Q}_{p^2}e_1' \oplus \mathbb{Q}_{p^2}e_2'$ avec

$$\varphi e_1' = e_2' \ , \ \varphi e_2' = -pe_1' \quad ; \quad \omega e_1' = e_1' \ , \ \omega e_2' = e_2' \quad ; \quad \tau_e e_1' = \zeta_e e_1' \ , \ \tau_e e_2' = \zeta_e^{-1} e_2' \ ,$$

$$\text{et} \qquad \mathrm{Fil}^1(D \otimes_{\mathbb{Q}_{p^2}} K_e) = (-p\alpha \cdot e_1' \otimes \pi_e^{-1} + e_2' \otimes \pi_e)K_e \ .$$

Alors on voit que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E(e;-1,\alpha))) = D(e;-1,\alpha) = \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\mathbf{-p\alpha})$, et lorsque α parcourt $\mathbb{Z}_p$, $-p\alpha$ parcourt $\{x \in \mathbb{P}^1(\mathbb{Q}_p) \ , \ v_p(x) \geq 1\}$.

Les deux situations présentées ci-dessus se "recoupent" en $\alpha \in \mathbb{Z}_p^\times$, dans le sens que les $D(e;1,\alpha)$ fournissent la même famille de représentations que les $D(e;-1,\alpha)$ lorsque α parcourt $\mathbb{Z}_p^\times$; on rappelle que les schémas $E(e;1,\alpha^{-1}) = E_{\alpha^{-1}1_{\pi_e}}$ et $E(e;-1,\alpha) = E_{\alpha\pi_e^{e-3}}$ sont isogènes sur $\mathbb{Z}_p[\pi_e]$, et que la L_e-isogénie liant ces deux courbes est définie sur $\mathbb{Q}_p$, de sorte qu'elles sont isogènes sur $\mathbb{Q}_p$ (rmq. 2 de **3.3.3.**).

Théorème 1 :
Soit $p \geq 5$. Pour chaque $e \in \{3,4,6\}$ divisant $p+1$, et pour chaque $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, il existe

une courbe elliptique $E_{e,\alpha}$ définie sur $\mathbb{Q}_p$ telle que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_{e,\alpha})) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$ dans $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$.

Preuve :
Si $(e,p) \neq (6,5)$, alors $e < p-1$, et le résultat découle de tout ce qui a été fait précédemment. Si $(e,p) = (6,5)$, on considère une famille de courbes $E_{3,\alpha}$, $\alpha \in \mathbb{P}^1(\mathbb{Q}_5)$, définies sur $\mathbb{Q}_5$ et telles que $\mathbf{D}^*_{\mathbf{pcris}}(V_5(E_{3,\alpha})) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{3};\mathbf{0};\alpha)$ dans $\mathbf{MF}_{K_3/\mathbb{Q}_5}(\varphi)$. Pour chaque $\alpha \in \mathbb{P}^1(\mathbb{Q}_5)$, notons $E'_{3,\alpha}$ la courbe elliptique définie sur $\mathbb{Q}_5$ obtenue en twistant $E_{3,\alpha}$ sur $\mathbb{Q}_5(\pi_2)$. L'action de $G = \mathrm{Gal}(\overline{\mathbb{Q}}_5/\mathbb{Q}_5)$ sur $V_5(E'_{3,\alpha})$ est obtenue en twistant l'action de G sur $V_5(E_{3,\alpha})$ par le caractère ramifié d'ordre 2

$$\begin{cases} G & \to & \{\pm 1\} \\ g & \mapsto & \frac{g\pi_2}{\pi_2} \end{cases}$$

Alors $D = \mathbf{D}^*_{\mathbf{pcris}}(V_5(E'_{3,\alpha}))$ est un objet de $\mathbf{MF}_{K_6/\mathbb{Q}_5}(\varphi)$ qui admet une $\mathbb{Q}_{5^2}$-base (v_1, v_2) telle que

$$\varphi v_1 = v_2 \ , \ \varphi v_2 = -pv_1 \quad ; \quad \omega v_1 = v_1 \ , \ \omega v_2 = v_2 \quad ; \quad \tau_6 v_1 = -\zeta_3 v_1 \ , \ \tau_6 v_2 = -\zeta_3^{-1} v_2 \ ,$$
$$\text{et} \qquad \mathrm{Fil}^1(D \otimes_{\mathbb{Q}_{5^2}} K_6) = (\alpha \cdot v_1 \otimes \pi_3^{-1} + v_2 \otimes \pi_3) K_6 \ .$$

Or, on a choisi $\pi_3, \pi_6, \zeta_3, \zeta_6 \in \overline{\mathbb{Q}}_5$ de sorte que $\pi_3 = \pi_6^2$, et $-\zeta_3 = \zeta_6^{-1}$ (puisque $-\zeta_3$ est d'ordre 6 et $\zeta_6^2 = \zeta_3$). Alors la transformation $\mathbb{Q}_{5^2}$-linéaire donnée par $v_1 \mapsto e_2$, $v_2 \mapsto -5e_1$ est un isomorphisme dans $\mathbf{MF}_{K_6/\mathbb{Q}_5}(\varphi)$ qui envoie D sur $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{6};\mathbf{0};\mathbf{5^2\alpha^{-1}})$. Le résultat s'en suit puisque $\alpha \mapsto 5^2\alpha^{-1}$ est une bijection de $\mathbb{P}^1(\mathbb{Q}_5)$. □

Remarque 1 : On considère toujours la même courbe $\widetilde{E}/\mathbb{F}_p$ du début de ce paragraphe, ainsi que les relèvements E_β, $\beta \in O_{L_e}$, de $\widetilde{E}$ sur $O_{L_e} = \mathbb{Z}_p[\pi_e]$. Notons $\widetilde{E}'/\mathbb{F}_p$ le twist d'ordre 2 de $\widetilde{E}$ correspondant à l'extension $\mathbb{F}_{p^2}/\mathbb{F}_p$, et E'_β le twist non ramifié d'ordre 2 de E_β correspondant à l'extension $K_e/L_e \simeq \mathbb{Q}_{p^2}/\mathbb{Q}_p$. Alors E'_β a bonne réduction sur L_e, et les relèvements de $\widetilde{E}'$ en un schéma elliptique sur O_{L_e} sont, à isomorphisme près, les E'_β , $\beta \in O_{L_e}$. De plus, E'_β est définie sur $\mathbb{F}_p$ avec un défaut de semi-stabilité $\mathrm{dst}(E'_\beta) = e$ si et seulement si E_β l'est. Dans ce cas, si dans $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$ on a $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E_\beta)) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$ pour un $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, alors $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E'_\beta)) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};-\alpha)$.

Remarque 2 : On peut donner des exemples explicites (i.e. des équations de Weiertrass) pour $\alpha \in \{0, \infty\}$, voir les exemples du chapitre 1 en **1.3.3.** ; par contre, si $\alpha \in \mathbb{Q}_p^\times$, je ne sais pas le faire. Rappelons tout de même que l'invariant α est lié au logarithme du groupe formel d'une courbe elliptique qui lui correspond ([Laf]).

Proposition 7 :
Soient $p \geq 5$ et $e \in \{3,4,6\}$ divisant $p+1$.
1) Soit $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$. Si $v_p(\alpha) \neq 1$, à $\mathbb{Q}_p$-isomorphisme près, il y a 2 courbes elliptiques $E/\mathbb{Q}_p$ telles que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E)) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$ dans $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$, et si $v_p(\alpha) = 1$, il y en a 4.
2) Soient E et E' deux courbes elliptiques sur $\mathbb{Q}_p$ potentiellement supersingulières avec $\mathrm{dst}(E) = \mathrm{dst}(E') \geq 3$. Alors $V_p(E)$ et $V_p(E')$ sont $\mathbb{Q}_p[G]$-isomorphes si et seulement si E et E' sont $\mathbb{Q}_p$-isogènes.

Preuve :
1) Soient $e \in \{3,4,6\}$ divisant $p+1$ et $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$. Soit $E/\mathbb{Q}_p$ une courbe elliptique telle que

$\mathbf{D}^*_{\mathbf{pcris}}(V_p(E)) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$. Alors $\mathrm{dst}(E) = e$, $\widetilde{E}_{L_e}$ est supersingulière, et $j(\widetilde{E}_{L_e}) = \tilde{\jmath}(e)$. A $\mathbb{F}_p$-isomorphisme près, il y a deux courbes elliptiques sur $\mathbb{F}_p$ d'invariant modulaire $\tilde{\jmath}(e)$, disons $\widetilde{E}$ et $\widetilde{E}'$, et l'une est un twist sur $\mathbb{F}_{p^2}$ de l'autre.
Considérons d'abord les courbes $E/\mathbb{Q}_p$ telles que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E)) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$ obtenues à partir de $\widetilde{E}$. Si $v_p(\alpha) \neq 1$, il y en a une seule à $\mathbb{Q}_p$-isomorphisme près, correspondant à E_β avec $\beta = -\alpha p^{-1}\pi_e^{e-3}$ si $v_p(\alpha) > 1$, et à $\beta = -\alpha^{-1}p\pi_e$ si $v_p(\alpha) < 1$; si $v_p(\alpha) = 1$, il y en a deux à $\mathbb{Q}_p$-isomorphisme près, correspondant à E_β avec $\beta = -\alpha p^{-1}\pi_e^{e-3}$ ou $\beta = -\alpha^{-1}p\pi_e$.
D'après la remarque 1 précédente, les courbes $E'_\beta/\mathbb{Q}_p$ obtenues à partir de $\widetilde{E}'$ sont des twists non ramifiés des courbes E_β. On en déduit les courbes $E'/\mathbb{Q}_p$ dont la fibre spéciale est $\widetilde{E}'$ et telles que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E')) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$: si $v_p(\alpha) \neq 1$ il y en a une seule à $\mathbb{Q}_p$-isomorphisme près (correspondant à E'_β avec $\beta = \alpha p^{-1}\pi_e^{e-3}$ si $v_p(\alpha) > 1$, et à $\beta = \alpha^{-1}p\pi_e$ si $v_p(\alpha) < 1$), et si $v_p(\alpha) = 1$ il y en a deux (correspondant à E'_β avec $\beta = \alpha p^{-1}\pi_e^{e-3}$ ou $\beta = \alpha^{-1}p\pi_e$).

2) Rappelons que $E_{\alpha^{-1}\pi_e}$ est $\mathbb{Q}_p$-isogène à $E_{\alpha\pi_e^{e-3}}$ pour tout $\alpha \in \mathbb{Z}_p$ (**3.3.3.** rmq.2). Il suffit donc de prouver que E_β est $\mathbb{Q}_p$-isogène à $E'_{(-\beta)}$ pour tout $\beta \in \mathbb{Z}_p\pi_e \cup \mathbb{Z}_p\pi_e^{e-3}$.
Soit $d \in \mathbb{F}_p^\times$ tel que $d \notin (\mathbb{F}_p^\times)^2$, et soit $\delta \in \mathbb{F}_{p^2}$ tel que $\delta^2 = d$; alors le morphisme $\gamma : \widetilde{E} \to \widetilde{E}'$ donné au niveau des points par : $\widetilde{E}(\overline{\mathbb{F}}_p) \to \widetilde{E}'(\overline{\mathbb{F}}_p)$, $(x,y) \mapsto (\delta^2 x, \delta^3 y)$, est un isomorphisme défini sur $\mathbb{F}_{p^2}$. Soit $\sigma : x \mapsto x^p$ le Frobenius absolu, $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = <\sigma>$. Soit $\xi : \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \{\pm 1\}$ l'unique caractère d'ordre 2 ; on a $g\delta = \xi(g)\delta$ et $\gamma^g = \xi(g)\gamma$ pour tout $g \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Alors

$$\begin{cases} \mathrm{End}_{\mathbb{F}_{p^2}}(\widetilde{E}) & \to & \mathrm{Hom}_{\mathbb{F}_{p^2}}(\widetilde{E},\widetilde{E}') \\ \psi & \mapsto & \gamma \circ \psi \end{cases}$$

est un isomorphisme, par lequel les éléments de $\mathrm{Hom}_{\mathbb{F}_p}(\widetilde{E},\widetilde{E}')$ correspondent aux $\psi \in \mathrm{End}_{\mathbb{F}_{p^2}}(\widetilde{E})$ tels que $\psi^g = \xi(g)\psi$ pour tout $g \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, ce qui équivaut à $\psi^\sigma = -\psi$.
Soit $\psi_e = [\zeta_e] - [\zeta_e^{-1}] \in \mathrm{End}_{\mathbb{F}_{p^2}}(\widetilde{E})$; on a $\deg\psi_e = 4 - \gamma_e^2 = 3$ si $e \in \{3,6\}$, 4 si $e = 4$.
Comme $\psi_e^\sigma = [\zeta_e^{-1}] - [\zeta_e] = -\psi_e$, l'isogénie $\gamma \circ \psi_e$ est définie sur $\mathbb{F}_p$. Soient $M = \mathbf{M}(\widetilde{E}(p))$ et $M' = \mathbf{M}(\widetilde{E}'(p))$. L'isogénie $\mathbf{M}(\gamma \circ \psi_e) : M' \to M$ est donnée par la composée de $\mathbf{M}(\gamma) : M' \otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2} \xrightarrow{\sim} M \otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2}$, qui envoie une base adaptée sur une base adaptée, avec $\mathbf{M}(\psi_e) : M \otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2} \to M \otimes_{\mathbb{Z}_p}\mathbb{Z}_{p^2}$; cette dernière s'écrit dans une base adaptée (e_1, e_2) de M :

$$\begin{pmatrix} \zeta_e - \zeta_e^{-1} & 0 \\ 0 & \zeta_e^{-1} - \zeta_e \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \sigma(\lambda) \end{pmatrix} \quad , \quad \lambda \in \mathbb{Z}_{p^2}^\times, \sigma(\lambda) = -\lambda\,.$$

Alors on voit que $\mathbf{M}(\psi_e)$ envoie, après extension des scalaires, $\mathcal{L}(\beta) = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e})O_{L_e}$ sur $\mathcal{L}(-\beta)$, et l'on en déduit par Serre-Tate que $\gamma \circ \psi_e$ se relève en une O_{L_e}-isogénie $(\gamma \circ \psi_e)_\beta : E_\beta \to E'_{(-\beta)}$ pour tout $\beta \in O_{L_e}$.
Prenons maintenant $\beta \in \mathbb{Z}_p\pi_e \cup \mathbb{Z}_p\pi_e^{e-3}$, de sorte que E_β et $E'_{(-\beta)}$ sont définies sur $\mathbb{Q}_p$, et posons $D = \mathbf{D}^*_{\mathbf{pcris}}(V_p(E_\beta))$ et $D' = \mathbf{D}^*_{\mathbf{pcris}}(V_p(E'_{(-\beta)}))$. Les objets D et D' sont dans $\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)$ et ils sont décrits par :
$D = \mathbb{Q}_{p^2}e_1 \oplus \mathbb{Q}_{p^2}e_2$, $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$, $\omega e_1 = e_1$, $\omega e_2 = e_2$, $\tau_e e_1 = \zeta_e^{\epsilon} e_1$, $\tau_e e_2 = \zeta_e^{-\epsilon} e_2$, $\mathrm{Fil}^1(D \otimes_{\mathbb{Q}_{p^2}} K_e) = (e_1 \otimes 1 + \beta \cdot e_2 \otimes \pi_e^{1-e})K_e$,
$D' = \mathbb{Q}_{p^2}e'_1 \oplus \mathbb{Q}_{p^2}e'_2$, $\varphi e'_1 = e'_2$, $\varphi e'_2 = -pe'_1$, $\omega e'_1 = -e'_1$, $\omega e'_2 = -e'_2$, $\tau_e e'_1 = \zeta_e^{-\epsilon} e'_1$, $\tau_e e'_2 = \zeta_e^{\epsilon} e'_2$, $\mathrm{Fil}^1(D' \otimes_{\mathbb{Q}_{p^2}} K_e) = (e'_1 \otimes 1 - \beta \cdot e'_2 \otimes \pi_e^{1-e})K_e$.

L'isogénie $(\gamma \circ \psi_e)_\beta$ induit un isomorphisme $D' \to D$ d'objets de $\mathbf{MF}_{K_e}(\varphi)$ par $e'_1 \mapsto \lambda e_1$, $e'_2 \mapsto \sigma(\lambda)e_2$. On vérifie que ce morphisme commute à l'action de $G_{K_e/\mathbb{Q}_p}$, donc $(\gamma \circ \psi_e)_\beta$: $E_\beta \to E'_{(-\beta)}$ est une isogénie définie sur $\mathbb{Q}_p$. □

Remarque 3, sur les cas ordinaires : Rappelons que pour $e \in \{3,4,6\}$ tel que $e \mid p-1$, on a défini les objets $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\alpha)$, $a_p \in \mathcal{N}^\times_{p,e}$, $\epsilon \in \{-1,1\}$, $\alpha \in \{0,1\}$, de $\mathbf{MF}_{L_e/\mathbb{Q}_p}(\varphi)$ et de type Hodge-Tate (0,1) suivants : soit u l'unique élément de $\mathbb{Z}_p^\times$ vérifiant $u + u^{-1}p = a_p$; $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\alpha) = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = u e_1$, $\varphi e_2 = u^{-1} p e_2$; $\tau_e e_1 = \zeta_e{}^\epsilon e_1$, $\tau_e e_2 = \zeta_e{}^{-\epsilon} e_2$; $\mathrm{Fil}^1 D_{L_e} = (\alpha \cdot e_1 \otimes \pi_e{}^{-\epsilon} + e_2 \otimes \pi_e{}^\epsilon)\mathbb{Q}_p(\pi_e)$. Ces objets sont deux-à-deux non-isomorphes dans $\mathbf{MF}_{L_e/\mathbb{Q}_p}(\varphi)$.
Soit $e \in \{3,4,6\}$, et soit $p \geq 5$ tel que $e \mid p-1$. On suppose $e < p-1$, donc $(e,p) \neq (4,5)$ et $(e,p) \neq (6,7)$. Soit $\widetilde{E}/\mathbb{F}_p$ une courbe elliptique ordinaire telle que $a_p(\widetilde{E}) = a_p \in \mathcal{N}^\times_{p,e}$ (cf. la remarque à la fin de **3.3.3.**). Pour $\epsilon \in \{-1,1\}$ et $\alpha \in \mathbb{Z}_p$, on note $E(e;a_p;\epsilon,\alpha)$ une courbe elliptique définie sur $\mathbb{Q}_p$ qui est $\mathbb{Z}_p[\pi_e]$-isogène à un schéma elliptique E_β sur $\mathbb{Z}_p[\pi_e]$, avec $\beta = \alpha(-p)^{\frac{1+\epsilon}{2}} \pi_e^{-2\epsilon-1}$ (voir la fin de **3.3.3.**). Alors on obtient des isomorphismes dans $\mathbf{MF}_{L_e/\mathbb{Q}_p}(\varphi)$:

$$\mathbf{D}^*_{\mathbf{pcris}}(V_p(E(e;a_p;\epsilon,\alpha))) \simeq \begin{cases} \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\mathbf{0}) & \text{si} \quad \alpha = 0 \\ \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\mathbf{1}) & \text{si} \quad \alpha \neq 0\,. \end{cases}$$

En fait, pour chaque $e \in \{3,4,6\}$ divisant $p-1$ et pour chaque triplet (a_p,ϵ,α) dans $\mathcal{N}^\times_{p,e} \times \{\pm 1\} \times \{0,1\}$, on peut trouver une équation de Weiertrass explicite d'une courbe elliptique $E/\mathbb{Q}_p$ telle que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E)) \simeq \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\alpha)$ dans $\mathbf{MF}_{L_e/\mathbb{Q}_p}(\varphi)$ (voir les exemples du chapitre 1, en **1.3.3.**).

ANNEXE A

Classification des $\mathbb{Q}_l[G]$-modules $V_l(E)$, $l \in \mathcal{P}$

A.1. Démonstration des parties 1) et 2) du théorème 1.1. :

Dans toute cette section **A.1.**, *on désigne par* $l \in \mathcal{P}$ *un nombre premier distinct de* p.

Nous nous proposons ici de démontrer les parties 1) et 2) du théorème **1.1** du chapitre 1. Nous allons donner une classification des $\mathbb{Q}_l[G]$-modules $V_l(E)$ qui repose sur l'équivalence de catégories entre les représentations l-adiques de G (qui sont toutes potentiellement semi-stables puisqu'on est dans le cas où le corps résiduel est fini) et les représentations l-adiques du groupe de Weil-Deligne $'W$ associé à G. C'est une légère variante des notions développées par P. Deligne dans [Del], le but étant d'obtenir une équivalence avec une catégorie dont les objets sont comparables (en un sens précis) avec des objets provenant de représentations p-adiques de G. Rappelons que l'on savait déjà comment comparer un système de représentations l-adiques $(\Delta_l)_{l \neq p}$ de $'W$ lorsque l parcourt tous les nombres premiers différents de p, voir par exemple [Roh]. Dans cet article, D.E. Rohrlich établit maints résultats concernant les systèmes de représentations l-adiques, $l \neq p$, provenant de courbes elliptiques.

Classifier les $\mathbb{Q}_l[G]$-modules $V_l(E)$ pour $l \neq p$ revient à classifier les représentations du groupe de Weil-Deligne $'W = {}'W_{\mathbb{Q}_p}$; on utilise le foncteur *contravariant* $\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}$ qui établit une anti-équivalence de catégories entre $\mathbf{Rep}_{\mathbb{Q}_l}(G)$ et $\mathbf{Rep}^{\circ}_{\mathbb{Q}_l}('W)$, voir **1.2.1.1.**. Rappelons qu'un objet dans $\mathbf{Rep}_{\mathbb{Q}_l}('W)$ peut être considéré comme un triplet (Δ_l, ρ_0, N), où : Δ_l est un $\mathbb{Q}_l$-espace vectoriel de dimension finie ; $\rho_0 : W \to \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$ est un morphisme dont le noyau contient un sous-groupe ouvert de I ; $N \in \mathrm{End}_{\mathbb{Q}_l}(\Delta_l)$ et vérifie : $\forall w \in W$, $\rho_0(w)N = p^{v(w)}N\rho_0(w)$.

A.1.1. Les cas potentiellement multiplicatifs :

Soit E une courbe elliptique sur $\mathbb{Q}_p$ telle que $v_p(j_E) < 0$; alors, quitte à tordre E par un caractère d'ordre 2, on peut supposer que $E = E_q$, où E_q est une courbe de Tate avec $q \in \mathbb{Q}_p^{\times}$, $v_p(q) \geq 1$, et q est uniquement déterminé par l'invariant modulaire j_E.
La représentation $V_l(E_q)$ est semi-stable, comme extension de $\mathbb{Q}_l$ par $\mathbb{Q}_l(1)$; par contre, elle n'est pas cristalline (i.e. n'a pas bonne réduction), puisque $q \in p\mathbb{Z}_p \backslash \{0\}$.

Soit $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{st},\mathbf{l}}(V_l(E_q))$; c'est un $\mathbb{Q}_l$-espace vectoriel de dimension 2, muni d'une action du groupe de Weil $\mathbb{Q}_l$-linéaire $\rho_0 : W \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$, et d'un opérateur $N \in \mathrm{End}_{\mathbb{Q}_l}(\Delta_l)$, vérifiant $\rho_0(w)N = p^{v(w)}N\rho_0(w)$, pour tout $w \in W$. La représentation $V_l(E_q)$ étant semi-stable, on a $\rho_0(I) = 1$; comme elle n'est pas cristalline, on a $N \neq 0$.
En appliquant le foncteur contravariant $\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{st},\mathbf{l}}$ à la suite exacte $(*_m)$, on obtient une suite exacte dans $\mathbf{Rep}^{\circ}_{\mathbb{Q}_l}('W)$:

$$0 \longrightarrow \Delta_{l,1} \longrightarrow \Delta_l \longrightarrow \Delta_{l,2} \longrightarrow 0 \ ,$$

où l'action de ϕ est triviale sur $\Delta_{l,1}$, et se fait par la multiplication par p sur $\Delta_{l,2}$; il existe donc une $\mathbb{Q}_l$-base (e_1, e_2) de Δ_l telle que $\rho_0(\phi)e_1 = e_1$ et $\rho_0(\phi)e_2 = pe_2$. Puis la relation $\rho_0(\phi)N = p^{-1}N\rho_0(\phi)$ donne $\rho_0(\phi)(Ne_1) = p^{-1}Ne_1$; on en déduit que $Ne_1 = 0$, car sinon p^{-1} serait valeur propre de $\rho_0(\phi)$. La même relation donne aussi $\rho_0(\phi)(Ne_2) = Ne_2$; on en déduit que $Ne_2 = ae_1$, avec $a \in \mathbb{Q}_l^{\times}$ (si $a = 0$ l'opérateur N serait nul). Finalement, quitte à changer e_1 en ae_1, on voit qu'il existe une $\mathbb{Q}_l$-base (e_1, e_2) de Δ_l dans laquelle les matrices de $\rho_0(\phi)$ et de N s'écrivent respectivement

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} .$$

On constate que l'on obtient qu'une seule classe d'isomorphisme, i.e. pour tous q, q' dans $p\mathbb{Z}_p\backslash\{0\}$, les $\mathbb{Q}_l[G]$-modules $V_l(E_q)$ et $V_l(E_{q'})$ sont isomorphes. De plus, on voit que $\Delta_{l,1} = \mathbb{Q}_p e_1$ est un sous-objet, alors que $\Delta_{l,2} = \mathbb{Q}_p e_2$ ne l'est pas, n'étant pas stable par N ; on en déduit que la suite exacte $(*_m)$ *n'est pas scindée* (on retrouve ainsi ce résultat qui était déjà connu, voir [Se 1], A.1.2.). Enfin, l'action de W via ρ_0 est semi-simple ; il suffit donc de connaître toutes les traces de ρ_0 ainsi que le polynôme minimal de N pour décrire la classe d'isomorphisme de $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{st},\mathbf{l}}(V_l(E_q))$.

En tordant par les trois caractères d'ordre 2 possibles (un non ramifié et deux ramifiés, correspondants aux trois extensions quadratiques M_1, M_2, et M_3 de $\mathbb{Q}_p$), on obtient les objets $\mathbf{WD}^*_{\mathbf{m}}(\mathbf{e};\mathbf{b})$, $e \in \{1,2\}$, $b \in \{-1,1\}$, de $\mathbf{Rep}^{\circ}_{\mathbb{Q}_l}('W)$ décrits par : $\rho_0(I_2) = 1$; $\rho_0(\theta_2) = (-1)^{e-1}$; $\mathrm{P}_{min}(\rho_0(\phi)) = (X-b)(X-bp)$; $\mathrm{P}_{min}(N) = X^2$; $\rho_0(\phi)N = p^{-1}N\rho_0(\phi)$.
Ils proviennent tous d'une courbe elliptique E sur $\mathbb{Q}_p$ telle que $v_p(j_E) < 0$. Plus précisément, soient $q = q(j_E)$ et $\gamma_E = -2AB^{-1} \bmod (\mathbb{Q}_p^{\times})^2$, où l'on a choisi une équation de Weierstrass $y^2 = x^3 + Ax + B$ pour E. Alors ([Silv 2], V, lemme 5.2.) :
$(e;b) = (1;1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_p$, et E est isomorphe sur $\mathbb{Q}_p$ à E_q ;
$(e;b) = (1;-1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_{p^2} = M_1$, et E est le twist sur M_1 de E_q ;
$(e;b) = (2;1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = \mathbb{Q}_p(\pi_2) = M_2$, et E est le twist sur M_2 de E_q ;
$(e;b) = (2;-1) \Leftrightarrow \mathbb{Q}_p(\sqrt{\gamma_E}) = M_3$, et E est le twist sur M_3 de E_q.
Le fait que ces représentations, pour (e,b) fixé (donc pour E fixée), soient définies sur $\mathbb{Q}$ et ne dépendent pas du nombre premier l, exprime la compatibilité au sens de Weil-Deligne du système $(\Delta_l)_{l \neq p}$, avec $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{st},\mathbf{l}}(V_l(E))$. Tous ces résultats sont dans [Roh], § 15.

A.1.2. Les cas de potentielle bonne réduction :

Soit E une courbe elliptique sur $\mathbb{Q}_p$ telle que $v_p(j_E) \geq 0$; alors E a potentiellement bonne réduction et acquiert bonne réduction sur $L_e = \mathbb{Q}_p(\pi_e)$, où $e = \mathrm{dst}(E)$ (c'est l'indice de ramification *minimal* d'un corps sur lequel E acquiert bonne réduction).
Soit $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E))$: c'est un $\mathbb{Q}_l$-espace vectoriel de dimension 2, muni d'un morphisme $\rho_0 : W \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$; l'opérateur de monodromie N est nul puisque $V_l(E)$ a potentiellement bonne réduction.
Alors on a $\rho_0(I_e) = 1$ et $\mathrm{P}_{min}(\rho_0(\phi))(X) = X^2 - a_pX + p$, avec $a_p = a_p(\widetilde{E}_{L_e})$; de plus, $< \tau_e >= I(K_e/\mathbb{Q}_p) = I/I_e$ *s'injecte* par ρ_0 mod I_e dans $\mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$, car sinon E acquerrait bonne réduction sur un corps d'indice de ramification strictement inférieur à e (à savoir sur le sous-corps de K_e fixé par le noyau de la restriction de ρ_0 mod I_e à I/I_e). De plus, le déterminant sur $V_l(E)$ est le caractère cyclotomique non ramifié donnant l'action de G sur $\mathbb{Z}_l(1)$. On sait alors que Δ_l est F-semi-simple, i.e. la représentation $\rho_0 : W \to \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$ l'est (cf. [Roh], § 14). Pour déterminer Δ_l à isomorphisme près, il suffit donc de connaître $\mathrm{Tr}(\rho_0) : W \to \mathbb{Q}_l$, ou bien, comme le déterminant est fixé, il suffit de donner les polynômes caractéristiques de tous les $\rho_0(w)$, $w \in W$. Remarquons que si la représentation ρ_0 est abélienne, alors la connaissance de toutes les traces équivaut à celle de $\mathrm{Tr}(\rho_0(\phi))$, $\mathrm{Tr}(\rho_0(\theta_e))$, et $\mathrm{Tr}(\rho_0(\phi\theta_e))$.

Si $\mathrm{dst}(E) = e = 1$, alors E a bonne réduction sur $\mathbb{Q}_p$; la classe d'isomorphisme de $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E))$ est donnée par : $\rho_0(I) = 1$; $\mathrm{P}_{car}(\rho_0(\phi))(X) = X^2 - a_pX + p$; $N = 0$, ce qui correspond à l'objet noté $\mathbf{WD}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_p})$ dans la liste $\mathbf{WD}^*$ du chapitre 1. On constate dans ce cas que la classe d'isomorphisme du $\mathbb{Q}_l[G]$-module $V_l(E)$ est déterminée par la classe de $\mathbb{F}_p$-isogénie de sa courbe réduite $\widetilde{E}/\mathbb{F}_p$, c'est-à-dire par l'entier $a_p = a_p(\widetilde{E})$.

Si $\mathrm{dst}(E) = e = 2$, alors E est le twist par le caractère ramifié d'ordre 2 correspondant à l'extension $\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p$ d'une courbe ayant bonne réduction sur $\mathbb{Q}_p$. La classe d'isomorphisme de $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E))$ est décrite par : $\rho_0(I_2) = 1$; $\rho_0(\theta_2) = -1$; $\mathrm{P}_{car}(\rho_0(\phi))(X) = X^2 - a_pX + p$; $N = 0$, ce qui correspond à l'objet noté $\mathbf{WD}^*_{\mathbf{c}}(\mathbf{2};\mathbf{a_p})$ dans la liste $\mathbf{WD}^*$ du chapitre 1.

Supposons maintenant que $\mathrm{dst}(E) = e \in \{3,4,6\}$. Alors l'automorphisme $\rho_0(\theta_e)$ est d'ordre e exactement et de déterminant 1 (puisque I agit trivialement sur $\wedge^2 V_l(E) = \mathbb{Z}_l(1)$, $l \neq p$) ; comme $(\mathbb{Z}/e\mathbb{Z})^\times = \{\pm 1\}$, cela implique

$$\mathrm{P}_{car}(\rho_0(\theta_e))(X) = \mathrm{P}_{min}(\rho_0(\theta_e))(X) = (X - \zeta_e)(X - \zeta_e^{-1}) = X^2 - \gamma_e X + 1 \ \in \mathbb{Z}[X]\,,$$

avec $\gamma_e = \zeta_e + \zeta_e^{-1} = -1, 0, 1$ si $e = 3, 4, 6$ respectivement. L'automorphisme $\rho_0(\theta_e)$ est diagonalisable à valeurs propres distinctes dans $\mathbb{Q}_l(\zeta_e) \otimes_{\mathbb{Q}_l} \Delta_l$. De plus, on a $\theta_e\phi \equiv \phi\theta_e^p$ mod I_e, d'où $\rho_0(\phi)\rho_0(\theta_e) = \rho_0(\theta_e)\rho_0(\phi)$ lorsque $p \equiv 1$ mod $e\mathbb{Z}$, et $\rho_0(\phi)\rho_0(\theta_e) = \rho_0(\theta_e)^{-1}\rho_0(\phi)$ lorsque $p \equiv -1$ mod $e\mathbb{Z}$.

Supposons $e \mid p+1$. En se plaçant dans une $\mathbb{Q}_l(\zeta_e)$-base de diagonalisation de $\rho_0(\theta_e)$ dans $\mathbb{Q}_l(\zeta_e) \otimes_{\mathbb{Q}_l} \Delta_l$, on voit facilement que tout endomorphisme $\mathbb{Q}_l(\zeta_e)$-linéaire f vérifiant $f\rho_0(\theta_e) = \rho_0(\theta_e)^{-1} f$ est de trace nulle, ainsi que celle de $f\rho_0(\theta_e)$ (car $\zeta_e \neq \zeta_e^{-1}$ pour $e \geq 3$). Donc $a_p = 0$ et la courbe $\widetilde{E}_{L_e}$ est supersingulière.
Dans ce cas, la représentation $\rho_0 : W \longrightarrow \mathrm{Aut}_{\mathbb{Q}_l}(\Delta_l)$ n'est pas abélienne, mais le fait que $\mathrm{Tr}(\rho_0(\phi)) = \mathrm{Tr}(\rho_0(\phi\theta_e)) = 0$ montre que les relations : $\rho_0(I_e) = 1$; $\mathrm{P}_{min}(\rho_0(\theta_e))(X) =$

$X^2 - \gamma_e X + 1$; $\mathrm{P}_{min}(\rho_0(\phi))(X) = X^2 + p$; $\rho_0(\phi)\rho_0(\theta_e) = \rho_0(\theta_e)^{-1}\rho_0(\phi)$; $N = 0$, avec $e \in \{3,4,6\}$ et $e \mid p+1$, suffisent pour la détermination de $\mathrm{Tr}(\rho_0) : W \to \mathbb{Q}_l$. Elles déterminent aussi la classe d'isomorphisme de $\Delta_l = \mathbf{\widehat{WD}}^*_{\mathbf{pst,l}}(V_l(E))$, qui correspond à l'objet noté $\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0})$ dans la liste $\mathbf{WD}^*$ du chapitre 1. Remarquons que toutes les traces sont à valeurs dans $\mathbb{Q}$, ce qui exprime le fait que Δ_l est définie sur $\mathbb{Q}$.

Supposons $e \mid p-1$. Plaçons-nous encore dans une $\mathbb{Q}_l(\zeta_e)$-base de diagonalisation de $\rho_0(\theta_e)$ dans $\mathbb{Q}_l(\zeta_e) \otimes_{\mathbb{Q}_l} \Delta_l$; alors sa matrice dans cette base s'écrit :

$$\begin{pmatrix} \zeta_e^{\epsilon} & 0 \\ 0 & \zeta_e^{-\epsilon} \end{pmatrix} \qquad \text{, avec} \qquad \epsilon \in \left(\mathbb{Z}/e\mathbb{Z}\right)^{\times} = \{\pm 1\} .$$

La relation $\rho_0(\phi)\rho_0(\theta_e) = \rho_0(\theta_e)\rho_0(\phi)$ montre que la représentation ρ_0 est abélienne, et que $\rho_0(\phi)$ est diagonalisable dans la même base ; écrivons sa matrice $\mathrm{Diag}(z_1, z_2)$, avec $z_i \in \mathbb{Q}_l(\zeta_e)$, et $z_1 z_2 = p$, $z_1 + z_2 = a_p$. Alors la trace de $\rho_0(\phi\theta_e)$ est $t_\epsilon = \zeta_e^{\epsilon} z_1 + \zeta_e^{-\epsilon} z_2$, et un calcul élémentaire montre qu'elle est racine du polynôme

$$T(X) = X^2 - \gamma_e a_p X + p\gamma_e^2 + a_p^2 - 4p \ \in \mathbb{Z}[X] ,$$

de discriminant $\mathrm{disc}(\mathrm{P}_{car}(\rho_0(\phi)))\mathrm{disc}(\mathrm{P}_{car}(\rho_0(\theta_e))) = (a_p^2 - 4p)(\gamma_e^2 - 4) \neq 0$. Les deux racines distinctes de $T(X)$ sont t_1 et t_{-1} ; en particulier, la représentation définie, à isomorphisme près, par $\mathrm{Tr}(\rho_0(\phi\theta_e)) = t_1$ n'est pas isomorphe à celle définie par $\mathrm{Tr}(\rho_0(\phi\theta_e)) = t_{-1}$. Enfin, le fait que $\Delta_l = \mathbf{\widehat{WD}}^*_{\mathbf{pst,l}}(V_l(E))$ doit être définie sur $\mathbb{Q}$ équivaut à $\mathrm{Tr}(\rho_0(W)) \subset \mathbb{Q}$, c'est-à-dire $\mathrm{Tr}(\rho_0(\phi\theta_e)) = t_\epsilon \in \mathbb{Q}$. Cette condition s'écrit aussi

$$\mathrm{disc}(T(X)) \ = \ (\gamma_e^2 - 4)(a_p^2 - 4p) \ \in \ (\mathbb{Q}^{\times})^2 ,$$

c'est-à-dire $a_p \in \mathcal{N}_{p,e}^{\times}$; en particulier, a_p est non nul, et la courbe $\widetilde{E}_{L_e}$ est ordinaire.
Finalement, la classe d'isomorphisme de $\Delta_l = \mathbf{\widehat{WD}}^*_{\mathbf{pst,l}}(V_l(E))$ est donnée par : $\rho_0(I_e) = 1$; $\mathrm{P}_{min}(\rho_0(\theta_e))(X) = X^2 - \gamma_e X + 1$; $\mathrm{P}_{car}(\rho_0(\phi))(X) = X^2 - a_p X + p$; $\mathrm{P}_{car}(\rho_0(\phi\theta_e))(X) = X^2 - t_\epsilon X + p$; $\rho_0(\phi)\rho_0(\theta_e) = \rho_0(\theta_e)\rho_0(\phi)$; $N = 0$, avec $e \in \{3,4,6\}$ et $e \mid p-1$, $a_p \in \mathcal{N}_{p,e}^{\times}$, $\epsilon \in \{\pm 1\}$. Ces objets sont deux-à-deux non-isomorphes, et correspondent à ceux notés $\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon)$ dans la liste $\mathbf{WD}^*$ du chapitre 1.

De plus, pour $E/\mathbb{Q}_p$ fixée, les classes d'isomorphisme des $\Delta_l = \mathbf{\widehat{WD}}^*_{\mathbf{pst,l}}(V_l(E))$ sont définies sur $\mathbb{Q}$ et indépendantes de $l \in \mathcal{P}\backslash\{p\}$: cela exprime la compatibilité du système $(\Delta_l)_{l \neq p}$. Dans les cas $e \in \{1,2\}$, cette compatibilité provient du fait que le polynôme caractéristique du Frobenius est dans $\mathbb{Q}[X]$ et indépendant de l. Dans les cas $\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0})$ lorsque $e \in \{3,4,6\}$ divise $p+1$, elle provient du fait que $\mathrm{P}_{car}(\rho_0(\phi))$ et $\mathrm{P}_{min}(\rho_0(\theta_e))$ sont dans $\mathbb{Q}[X]$ et indépendants de l. Par contre, pour déterminer l'invariant $\epsilon \in \{\pm 1\}$ qui intervient lorsque $e \in \{3,4,6\}$ divise $p-1$, il faut étudier le $\mathbb{F}_p[I]$-module $E[p]$ (voir [Kr], 2.3.1.), et utiliser le fait que le groupe cyclique $\mathrm{Gal}(\mathbb{Q}_p(\pi_e)/\mathbb{Q}_p)$ agit sur la courbe réduite $\widetilde{E}/\mathbb{F}_p$, comme dans [Se-Ta], Thm.2.

Remarque : On a montré que si $\mathrm{dst}(E) = e \geq 3$ (et pour $p \geq 5$), alors

$$\begin{cases} e \mid p-1 \ \Rightarrow \ E \text{ est potentiellement ordinaire,} \\ e \mid p+1 \ \Rightarrow \ E \text{ est potentiellement supersingulière.} \end{cases}$$

On verra que l'on obtient le même résultat en étudiant le $\mathbb{Q}_p[G]$-module $V_p(E)$ (**A.2.4.**). On peut aussi le retrouver en choisissant une équation de Weierstrass minimale pour E ; on montre alors que $j_E \equiv 0 \bmod p\mathbb{Z}_p$ si $e \in \{3,6\}$ (d'où $\mathrm{Aut}(\widetilde{E}_{L_e}) = \mu_6 =< \zeta_6 >$) et que $j_E \equiv 1728 \bmod p\mathbb{Z}_p$ si $e = 4$ (d'où $\mathrm{Aut}(\widetilde{E}_{L_e}) = \mu_4 =< \zeta_4 >$), puis on conclut en utilisant le critère que l'on peut trouver dans [Silv 1], Thm. 4.1.(a) (voir les exemples 4.4. et 4.5. qui suivent).

Ceci achève la démonstration des parties 1) et 2) du théorème **1.1.** du chapitre 1. Pour finir, nous allons montrer que les ensembles $\mathcal{N}_{p,4}^{\times}$ et $\mathcal{N}_{p,3}^{\times} = \mathcal{N}_{p,6}^{\times}$ sont de cardinal 4 et 6 respectivement. Fixons une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$; choisissons ζ_4 et $\zeta_6 \in \overline{\mathbb{Q}}$ des racines primitives quatrième et sixième de l'unité, de sorte que $\mu_4(\overline{\mathbb{Q}}) =< \zeta_4 >$ et $\mu_6(\overline{\mathbb{Q}}) =< \zeta_6 >$.

Lemme :
Soit $p \geq 5$; si $4 \mid p-1$ l'ensemble $\mathcal{N}_{p,4}^{\times} = \{a \in \mathbb{Z} \,/\, a^2 - 4p \equiv -1 \bmod (\mathbb{Q}^{\times})^2\}$ est en bijection avec $\mu_4(\overline{\mathbb{Q}})$, et si $3 \mid p-1$ l'ensemble $\mathcal{N}_{p,3}^{\times} = \{a \in \mathbb{Z} \,/\, a^2 - 4p \equiv -3 \bmod (\mathbb{Q}^{\times})^2\}$ est en bijection avec $\mu_6(\overline{\mathbb{Q}})$. Lorsque $12 \mid p-1$, ces deux ensembles sont disjoints.

Preuve : C'est de l'arithmétique élémentaire. La dernière assertion est évidente.

Si $p \equiv 1 \bmod 4$, alors $\mathcal{N}_{p,4}^{\times} = \{a \in \mathbb{Z} \,/\, -(a^2-4p) \in (\mathbb{Q}^{\times})^2\} = \{a \in \mathbb{Z} \,/\, 4p = a^2+b^2, b \in \mathbb{Z}\}$ est en bijection avec $\{a \in \mathbb{Z} \,/\, p = a^2 + b^2\,,\, b \in \mathbb{Z}\}$. Soit σ_4 la conjugaison dans $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$ (i.e. le générateur de $\mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})$), et $N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(x) = x\sigma_4(x)$, $x \in \mathbb{Q}(\zeta_4)$, la norme. L'anneau des entiers de $\mathbb{Q}(\zeta_4)$ est $\mathbb{Z}[\zeta_4] = \{a + \zeta_4 b\,, a, b \in \mathbb{Z}\}$ (c'est l'anneau des entiers de Gauss). Soit $N_{p,4} = \{x \in \mathbb{Z}[\zeta_4] \,/\, N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(x) = p\}$: c'est un ensemble non vide car $\mathbb{Z}[\zeta_4]$ est principal et $p \equiv 1 \bmod 4$ (Fermat), sur lequel σ_4 agit. Tout élément de $N_{p,4}$ fournit de façon évidente un élément de $\{a \in \mathbb{Z} \,/\, p = a^2 + b^2\,,\, b \in \mathbb{Z}\}$, d'où une application de $N_{p,4}$ dans $\mathcal{N}_{p,4}^{\times}$ qui est clairement surjective, et deux éléments x, x' de $N_{p,4}$ ont la même image dans $\{a \in \mathbb{Z} \,/\, p = a^2 + b^2\,,\, b \in \mathbb{Z}\}$ si et seulement si $x' = \sigma_4(x)$. On en déduit une bijection $N_{p,4}/ <\sigma_4> \xrightarrow{\sim} \mathcal{N}_{p,4}^{\times}$. Puis si $x_0 \in N_{p,4}$, l'ensemble $N_{p,4}$ est constitué de x_0, $\sigma_4(x_0)$, ainsi que des produits de ceux-ci avec les éléments de norme 1, i.e. les unités $(\mathbb{Z}[\zeta_4])^{\times} =< \zeta_4 >$; on en déduit une bijection $N_{p,4}/ <\sigma_4> \xrightarrow{\sim} <\zeta_4>$, d'où le résultat.

Si $p \equiv 1 \bmod 3$, posons $\zeta_3 = \zeta_6^2$: c'est une racine primitive troisième de l'unité. On note σ_3 la conjugaison et $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}$ la norme de l'extension quadratique $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ de $\mathbb{Q}$; son anneau des entiers est $\mathbb{Z}[\zeta_3] = \{(a+\sqrt{-3}b)/2, a, b \in \mathbb{Z}\,,\, a \equiv b \bmod 2\mathbb{Z}\}$, il est principal, et ses unités sont ses éléments de norme 1. L'ensemble $N_{p,3} = \{x \in \mathbb{Z}[\zeta_3] \,/\, N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(x) = p\}$ est non vide car $\mathbb{Z}[\zeta_3]$ est principal et $p \equiv 1 \bmod 3$ (i.e. (-3) est un résidu quadratique modulo p). Alors la preuve est tout-à-fait similaire : l'ensemble $\mathcal{N}_{p,3}^{\times} = \{a \in \mathbb{Z} \,/\, 12p = 3a^2 + b^2\,, b \in \mathbb{Z}\}$ est en bijection avec $N_{p,3}/ <\sigma_3>$, lequel l'est avec $(\mathbb{Z}[\zeta_3])^{\times} =< \zeta_6 >$. □

A.2. Démonstration des parties 1) et 2) du théorème 2.1. :

Nous nous proposons ici de démontrer les parties 1) et 2) du théorème **2.1.** du chapitre 1. Signalons que les calculs qui suivent sont peu ou prou les mêmes que ceux effectués dans [Fo-Ma], § A. Le seul élément nouveau est la détermination explicite de la filtration dans les cas multiplicatifs (**A.2.2.**). Les correspondances avec les notations de [Fo-Ma] se trouvent

dans le chapitre 1.

J.-M. Fontaine construit dans [Fo 2] un foncteur établissant équivalence de catégories entre $\mathbf{Rep}_{pst}(G)$ et une catégorie de modules filtrés ; on utilise ici le foncteur contravariant $\mathbf{D}^*_{\mathbf{pst}}$, voir **1.3.1.1.**.
On notera $\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,p}}$ le foncteur de $\mathbf{Rep}_{pst}(G)$ dans $\mathbf{Rep}_{P_0}('W)$, où $P_0 = \mathrm{Frac}W(\overline{\mathbb{F}}_p)$ est le complété de $\mathbb{Q}_p^{nr}$, qui s'obtient comme limite inductive des $\mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{st,K}}$ lorsque K parcourt l'ensemble des extensions finies galoisiennes de $\mathbb{Q}_p$ contenues dans $\overline{\mathbb{Q}}_p$ (cf. **1.3.2.**).

A.2.1. Quelques rappels sur les anneaux B_{cris}, B_{st}, et B_{dR} :

Si Λ est un anneau commutatif de caractéristique p, on note $W(\Lambda)$ l'anneau des vecteurs de Witt à coefficients dans Λ, et pour $\lambda \in \Lambda$, on note $[\lambda] = (\lambda, 0, 0, \ldots) \in W(\Lambda)$ son représentant de Teichmüller. Soit $C = \mathbb{C}_p$ le complété de $\overline{\mathbb{Q}}_p$, d'anneau des entiers O_C. On note $v = v_C$ la valuation sur C étendant la valuation v_p sur $\mathbb{Q}_p$, normalisée par $v(p) = 1$; on a $v(C^\times) = v(\overline{\mathbb{Q}}_p^\times) = \mathbb{Q}$. On désigne par $\sigma : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ le Frobenius absolu : $\sigma(x) = x^p$.

Soit $R = \varprojlim O_C/pO_C$, la limite projective étant indexée par $\mathbb{N}$ et se faisant suivant l'application $x \mapsto x^p$; un élément de R est une suite $(x_n)_{n\geq 0}$ telle que $x_n \in O_C/pO_C$ et $x_{n+1}^p = x_n$ pour tout n. Si l'on choisit pour tout $r \in \mathbb{N}$ un relèvement $\widehat{x}_r$ de x_r dans O_C, alors, pour tout $n \in \mathbb{N}$, la suite des $\widehat{x}_{n+m}^{p^m}$ converge lorsque $m \to +\infty$ vers un élément $x^{(n)}$ dans O_C qui ne dépend pas des relèvements choisis. Alors l'application $x = (x_n)_{n\geq 0} \mapsto (x^{(n)})_{n\geq 0}$ est une bijection par laquelle on identifie R à l'ensemble $\{x = (x^{(n)})_{n\geq 0} \in O_C^{\mathbb{N}} \ / \ (x^{(n+1)})^p = x^{(n)}\}$. Sur ce dernier la multiplication s'effectue en multipliant composante par composante, et l'addition est donnée par :

$$(x+y)^{(n)} = \lim_{m\to\infty} \left(x^{(n+m)} + y^{(n+m)}\right)^{p^m} .$$

L'application de R dans O_C qui à x associe $x^{(0)}$ est surjective, et R est un anneau intègre, parfait de caractéristique p. On définit une valuation sur R en posant, pour $x \in R$, $v_R(x) = v(x^{(0)})$. Soit $\mathcal{M}_R = \{x \in R \ / \ v_R(x) > 0\}$; alors $R/\mathcal{M}_R = \overline{\mathbb{F}}_p$. Le corps des fractions de R est algébriquement clos et complet pour la valuation v_R, et R est l'anneau de ses entiers. Aussi, $\overline{\mathbb{F}}_p$ s'identifie à un sous-corps de R par :

$$\begin{cases} \overline{\mathbb{F}}_p & \hookrightarrow & R \\ \varepsilon & \mapsto & ([\sigma^{-n}(\varepsilon)])_{n\geq 0} = ([\varepsilon^{p^{-n}}])_{n\geq 0} \cdot \end{cases}$$

On notera encore ε l'image de $\varepsilon \in \overline{\mathbb{F}}_p$ dans R. Enfin, $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ agit sur R, continuement pour la valuation v_R.
On note $R^\times = \{x \in R \ / \ v_R(x) = v(x^{(0)}) = 0\}$, et $R^{\times,+} = \{x \in R^\times \ / \ x \equiv 1 \bmod \mathcal{M}_R\}$. On a alors $R^\times = \overline{\mathbb{F}}_p^\times \times R^{\times,+}$, i.e. la suite exacte $1 \to R^{\times,+} \to R^\times \to \overline{\mathbb{F}}_p^\times \to 1$, où la projection est la réduction modulo $\mathcal{M}_R$, est scindée. On choisit $\boldsymbol{\varepsilon} = (\zeta_{p^n})_{n\geq 0}$ un générateur de $\mathbb{Z}_p(1)$; on a donc $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ pour tout $n \geq 0$, et ζ_p est une racine primitive p-ième de l'unité. On peut voir $\boldsymbol{\varepsilon}$ comme un élément de $R^{\times,+}$.

L'anneau $W(R)$ est intègre, séparé-complet pour la topologie p-adique, et c'est aussi une $W(\overline{\mathbb{F}}_p)$-algèbre sur laquelle G agit $W(k)$-linéairement et continuement. Il est également muni d'un opérateur de Frobenius $\varphi : W(R) \to W(R)$ défini par $\varphi((x_n)_{n\geq 0}) = (x_n^p)_{n\geq 0}$, $x_n \in R$, qui est σ-semi-$W(k)$-linéaire et G-équivariant. On a $[\varepsilon] \in W(R)$.
On définit une application :

$$\Theta : \begin{cases} W(R) & \longrightarrow & O_C \\ \underline{x} = (x_n)_{n\in\mathbb{N}} & \longmapsto & \sum_{n\in\mathbb{N}} p^n x_n^{(n)} \end{cases}.$$

C'est un morphisme d'anneaux surjectif, $W(k)$-linéaire et G-équivariant. On montre que son noyau est un idéal principal : $\mathrm{Ker}(\Theta) = \xi W(R)$. C'est à partir de ce morphisme que l'on construit la $\overline{\mathbb{Q}}_p$-algèbre B_{dR}^+, ainsi que la $P_0 = \mathrm{Frac}W(\overline{\mathbb{F}}_p)$-algèbre B_{cris}^+, voir [Fo 1] ; on note encore $\Theta : B_{dR}^+ \to C$ le morphisme $\mathbb{Q}_p$-linéaire qui étend Θ à B_{dR}^+.

La somme $\sum_{n\geq 1}(-1)^{n+1}\frac{(1\otimes[\varepsilon]-1)^n}{n}$ converge dans l'ideal maximal de B_{dR}^+ vers un élément que l'on notera $t = \mathrm{Log}([\varepsilon])$; on définit ainsi une injection $\mathbb{Z}_p$-linéaire G-équivariante Log : $\mathbb{Z}_p(1) \hookrightarrow B_{dR}^+$. On montre que t est une uniformisante de B_{dR}^+, i.e. $\mathrm{Ker}(\Theta) = tB_{dR}^+$. Pour tout $g \in G$, on a : $gt = \chi(g)t$, où χ est le caractère cyclotomique.

Soit $x \in R^{\times,+}$; pour n suffisamment grand, l'élément $\frac{([x]-1)^n}{n}$ est dans A_{cris}, et tend p-adiquement vers 0. Donc $\sum_{n\geq 1}(-1)^{n+1}\frac{([x]-1)^n}{n}$ converge dans $B_{cris}^+ = A_{cris}[\frac{1}{p}]$ vers un élément que l'on notera $\lambda(x)$. On obtient ainsi un morphisme injectif $\mathbb{Z}_p$-linéaire G_K-équivariant $\lambda : R^{\times,+} \hookrightarrow B_{cris}^+$, et l'on notera encore $t = \lambda(\varepsilon) = \mathrm{Log}([\varepsilon])$. On étend λ à $R^\times$ en posant $\lambda(a) = 0$ si $a \in \overline{\mathbb{F}}_p^\times$, et l'on obtient un morphisme $\mathbb{Z}_p$-linéaire G_K-équivariant λ de $R^\times$ dans B_{cris}^+ ; on a donc :

$$\lambda : \begin{cases} R^\times & \longrightarrow & B_{cris}^+ \\ x & \longmapsto & \sum_{n\geq 1}(-1)^{n+1}\frac{([x^+]-1)^n}{n} \end{cases},$$

où l'on a posé $x^+ = x.[x \bmod \mathcal{M}_R]^{-1} \in R^{\times,+} = \{x \in R^\times \,/\, x \equiv 1 \bmod \mathcal{M}_R\}$.

Rappelons enfin que $B_{st}^+ = \mathrm{Sym}((\mathrm{Frac}R)^\times) \otimes_{\mathrm{Sym}(R^\times)} B_{cris}^+$, et que l'on a un morphisme $\lambda_{dR} : (\mathrm{Frac}R)^\times \to B_{dR}^+$ qui prolonge $\lambda : R^\times \to B_{cris}^+ \subset B_{dR}^+$. En fait, pour tout $y \in (\mathrm{Frac}R)^\times$ tel que $y \notin R^\times$, on a un isomorphisme $B_{st}^+ \simeq B_{cris}^+[\lambda_{dR}(y)]$. Choisissons un élément $\pi = (\pi^{(n)}) \in R$ avec $\pi^{(0)} = p$, et posons $\mathbf{u} = \mathrm{Log}([\pi]/p) \in B_{dR}$; on prend alors $B_{st} = B_{cris}[\mathbf{u}] \subset B_{dR}$, sur lequel le Frobenius est étendu par $\varphi\mathbf{u} = p\mathbf{u}$, et N est l'unique B_{cris}-dérivation telle que $N\mathbf{u} = 1$ (pour l'influence de ces choix voir [Fo 2], 5.2.).

Ces rappels nous serviront dans le paragraphe qui suit.

A.2.2. Les cas potentiellement multiplicatifs :

Soit E une courbe elliptique sur $\mathbb{Q}_p$ telle que $v_p(j_E) < 0$; alors, quitte à tordre E par un caractère d'ordre 2, on peut supposer que $E = E_q$, où E_q est une courbe de Tate avec $q \in \mathbb{Q}_p^\times$, $v_p(q) \geq 1$, et q est uniquement déterminé par l'invariant modulaire j_E. On a une suite exacte de $\mathbb{Z}_p[G]$-modules :

$$(*_m) \qquad 0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow T_p(E_q) = T_p(\overline{\mathbb{Q}}_p^\wedge/q^{\mathbb{Z}}) \longrightarrow \mathbb{Z}_p \longrightarrow 0 .$$

On a donc $T_p(E_q) = \mathbb{Z}_p\varepsilon \oplus \mathbb{Z}_p w_q$, où $\varepsilon = (\zeta_{p^n})_{n\geq 0}$ est un générateur de $\mathbb{Z}_p(1)$, et $w_q = (w_{q,n})_{n\geq 0}$ est un élément de $T_p(\overline{\mathbb{Q}}_p^{\times}/q^{\mathbb{Z}})$ dont l'image dans $\mathbb{Z}_p$ est 1. En tensorisant par $\mathbb{Q}_p$ on obtient la suite exacte de $\mathbb{Q}_p[G]$-modules :

$$(*_m) \qquad 0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow V_p(E_q) \longrightarrow \mathbb{Q}_p \longrightarrow 0\ .$$

On sait que toute extension V de $\mathbb{Q}_p$ par $\mathbb{Q}_p(1)$ est semi-stable, et que le type de Hodge-Tate de $D = \mathbf{D}^*_{\mathbf{st}}(V) = \mathrm{Hom}_{\mathbb{Q}_p[G]}(V, B_{st})$ est $(0,1)$, c'est-à-dire que l'on a : $\mathrm{Fil}^i D = D$ pour $i \leq 0$, $\mathrm{Fil}^1 D$ est un $\mathbb{Q}_p$-espace vectoriel de dimension 1, et $\mathrm{Fil}^i D = 0$ pour $i \geq 2$. De plus, l'objet $V_p(E_q) = V_p(\overline{\mathbb{Q}}_p^{\times}/q^{\mathbb{Z}})$ n'est pas cristallin, puisque $q \notin \mathbb{Z}_p^{\times}$.

Ecrivons $q = u_q p^m$, avec $u_q \in \mathbb{Z}_p^{\times}$ et $m = v_p(q) \geq 1$.
Choisissons un système $(y_q^{(n)})_{n\geq 0}$ de relèvements des $w_{q,n}$ dans $\overline{\mathbb{Z}}_p \subset O_C$ (l'anneau des entiers de $\overline{\mathbb{Q}}_p$), tel que $y_q^{(0)} = q$ et $(y_q^{(n+1)})^p = y_q^{(n)}$ pour tout $n \geq 0$; alors $y_q = (y_q^{(n)})_{n\geq 0} \in R$, et les autres choix pour un tel élément s'écrivent $\varepsilon^\nu y_q$, avec $\nu \in \mathbb{Z}_p$. On a $v_R(y_q) = v(y_q^{(0)}) = v_p(q) = m \geq 1$, avec

$$\lambda_{dR}(y_q) \;=\; \mathrm{Log}_{dR}\Big(\frac{[y_q]}{y_q^{(0)}}\Big) + \mathrm{Log}(y_q^{(0)}) \;=\; \sum_{n\geq 1}(-1)^{n+1}\frac{1}{n}\Big(\frac{[y_q]}{q} - 1\Big)^n + \mathrm{Log}(u_q)\ ,$$

où le premier terme est dans $tB^+_{dR} = \mathrm{Ker}(\Theta)$, et le deuxième est dans $p\mathbb{Z}_p$ (c'est le logarithme p-adique usuel) ; pour tout $\nu \in \mathbb{Z}_p$, on a $\lambda_{dR}(\varepsilon^\nu y_q) = \nu t + \lambda_{dR}(y_q)$. Donc, avec le choix que l'on a fait pour B_{st}, on a $N(\lambda_{dR}(y_q)) = v_R(y_q) = m = N(\lambda_{dR}(\varepsilon^\nu y_q))$. On définit des morphismes $\mathbb{Q}_p$-linéaires G-équivariants e_1^q et e_2^q de $V_p(E_q) = \mathbb{Q}_p\varepsilon \oplus \mathbb{Q}_p w_q$ dans B^+_{st} en posant :

$$\begin{cases} e_1^q(\varepsilon) &= 0 \\ e_1^q(w_q) &= 1 \end{cases} \qquad \text{et} \qquad \begin{cases} e_2^q(\varepsilon) &= t \\ e_2^q(w_q) &= \frac{1}{m}\lambda_{dR}(y_q)\ . \end{cases}$$

L'application e_2^q est injective, et son image ne dépend pas du choix de l'élément y_q (on remarque que cette image n'est pas dans B_{cris}). Alors, comme on sait que $D = \mathbf{D}^*_{\mathbf{st}}(V_p(E_q)) = \mathrm{Hom}_{\mathbb{Q}_p[G]}(V_p(E_q), B_{st})$ est un $\mathbb{Q}_p$-espace vectoriel de dimension 2, et que (e_1^q, e_2^q) sont clairement $\mathbb{Q}_p$-indépendants, on voit que l'on a $D = \mathbb{Q}_p e_1^q \oplus \mathbb{Q}_p e_2^q$. De plus, on a les relations : $\varphi t = pt$; $\varphi(\lambda_{dR}(y_q)) = p\lambda_{dR}(y_q)$; $Nt = 0$; $N(\lambda_{dR}(y_q)) = m$. On en déduit facilement : $\varphi e_1^q = e_1^q$; $\varphi e_2^q = pe_2^q$; $Ne_1^q = 0$; $Ne_2^q = e_1^q$ (on a bien $N\varphi = p\varphi N$). Ainsi, il existe une $\mathbb{Q}_p$-base (e_1^q, e_2^q) de $D = \mathbf{D}^*_{\mathbf{st}}(V_p(E_q))$ dans laquelle les matrices de φ et de N s'écrivent respectivement

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\ .$$

Cela donne la structure de (φ, N)-module sur $\mathbb{Q}_p$ de D. On constate que $\mathbb{Q}_p e_1^q$ est un sous-objet, alors que $\mathbb{Q}_p e_2^q$ ne l'est pas, n'étant pas stable par N ; on en déduit que la suite exacte $(*_m)$ *n'est pas scindée* (on retrouve ainsi ce résultat qui était déjà connu, voir [Se 1], A.1.2.). De plus, on constate que le système de représentations $(V_l(E_q))_{l\in\mathcal{P}}$ est compatible.

Déterminons maintenant la filtration, ce qui revient à déterminer la $\mathbb{Q}_p$-droite $\mathrm{Fil}^1 D$. La condition de faible admissibilité impose $\mathrm{Fil}^1 D \neq \mathbb{Q}_p e_1^q$ (sinon, $D' = \mathbb{Q}_p e_1^q$ serait un sous-objet dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi, N)$ de D tel que $t_H(D') = 1 > t_N(D') = 0$). On a donc

$$\mathrm{Fil}^1 D \;=\; \mathbb{Q}_p(\alpha(q)e_1^q + e_2^q) \quad \text{, avec} \quad \alpha(q) \in \mathbb{Q}_p$$

(la faible admissibilité est bien vérifiée). Par définition, on a $\mathrm{Fil}^1 D = \mathrm{Hom}_{\mathbb{Q}_p[G]}(V_p(E_q), tB_{dR}^+)$ ([Fo 1]), c'est-à-dire $\Theta(\alpha(q)e_1^q(x) + e_2^q(x)) = 0$ pour tout $x \in V_p(E_q) = \mathbb{Q}_p\varepsilon \oplus \mathbb{Q}_p w_q$. Puis, comme $e_1^q(\varepsilon) = t \in \mathrm{Ker}(\Theta)$ et $e_2^q(\varepsilon) = 0$, on voit que la condition ci-dessus s'écrit $\Theta(\alpha(q)e_1^q(w_q) + e_2^q(w_q)) = \Theta(\alpha(q) + \frac{1}{m}\lambda_{dR}(y_q)) = 0$. Ceci équivaut, puisque $\lambda_{dR}(y_q) \equiv \mathrm{Log}(u_q) \bmod \mathrm{Ker}(\Theta)$, à $\Theta(m\alpha(q) + \mathrm{Log}(u_q)) = 0$; mais $m\alpha(q) + \mathrm{Log}(u_q) \in \mathbb{Q}_p$, et donc $m\alpha(q) + \mathrm{Log}(u_q) = 0$. Finalement, on obtient :

$$\alpha(q) \;=\; -\frac{\mathrm{Log}(u_q)}{v_p(q)} \qquad \text{, où} \qquad q = u_q p^{v_p(q)}\,,\; v_p(q) \geq 1\,.$$

Remarque : L'application de $p\mathbb{Z}_p\backslash\{0\}$ dans $\mathbb{Q}_p$ qui à q associe $\alpha(q) = -\mathrm{Log}(u_q)/v_p(q)$ est surjective : $\mathrm{Log}(u_q)$ parcourt $p\mathbb{Z}_p$ et $v_p(q)$ parcourt les entiers ≥ 1. Par contre, elle n'est pas injective : si $q, q' \in p\mathbb{Z}_p$, alors, avec des notations évidentes, $\alpha(q) = \alpha(q')$ si et seulement si : $\mathrm{Log}(u_q^{v_p(q')}) = \mathrm{Log}(u_{q'}^{v_p(q)}) \Leftrightarrow (u_q)^{v_p(q')(p-1)} = (u_{q'})^{v_p(q)(p-1)} \Leftrightarrow q^{v_p(q')(p-1)} = (q')^{v_p(q)(p-1)}$.

Soit maintenant q' un autre élément de $p\mathbb{Z}_p\backslash\{0\}$, et soit $D' = \mathrm{Hom}_{\mathbb{Q}_p[G]}(V_p(E_{q'}), B_{st})$, muni des opérateurs φ' et N' ; on sait qu'il existe une $\mathbb{Q}_p$-base (e_1', e_2') de D' dans laquelle les matrices de φ' et N' s'écrivent respectivement

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

et la filtation est donnée par $\mathrm{Fil}^1 D' = \mathbb{Q}_p(\alpha(q')e_1' + e_2')$, avec $\alpha(q') = -\mathrm{Log}(u_{q'})v_p(q')^{-1}$, où $q' = u_{q'}p^{v_p(q')}$. Or, on voit facilement que toute application $\mathbb{Q}_p$-linéaire non nulle $\psi : D \to D'$ telle que $\psi\varphi = \varphi'\psi$ et $\psi N = N'\psi$ est une homothétie ; donc on aura $\psi(\mathrm{Fil}^1 D) \subset \mathrm{Fil}^1 D'$ si et seulement si $\alpha(q) = \alpha(q')$.

Ainsi, $\mathbf{D}_{\mathbf{st}}^*(V_p(E_q))$ est isomorphe dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi, N)$ à l'objet $\mathbf{D}_{\mathbf{m}}^*(\mathbf{1};\mathbf{1};\alpha)$, $\alpha = \alpha(q) \in \mathbb{Q}_p$, de type Hodge-Tate (0,1), décrit par : $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$; $\varphi e_1 = e_1$; $\varphi e_2 = pe_2$; $Ne_1 = 0$; $Ne_2 = e_1$; $\mathrm{Fil}^1 D = \mathbb{Q}_p(\alpha e_1 + e_2)$.
Lorsque α parcourt $\mathbb{Q}_p$, ces objets sont deux-à-deux non-isomorphes, et ils proviennent tous d'une courbe de Tate sur $\mathbb{Q}_p$, puisque l'application $q \mapsto \alpha(q)$ est surjective. De plus, on retrouve (cf. [Se 1], A.1.4.) le fait que, pour deux courbes de Tate E_q et $E_{q'}$, on a :

$$V_p(E_q) \simeq V_p(E_{q'}) \;\Leftrightarrow\; q^{v_p(q')(p-1)} = (q')^{v_p(q)(p-1)} \;\Leftrightarrow\; E_q \text{ est } \mathbb{Q}_p\text{-isogène à } E_{q'}\,.$$

En tordant par les trois caractères d'ordre 2 possibles (voir **A.1.2.1.**), on obtient tous les objets $\mathbf{D}_{\mathbf{m}}^*(\mathbf{e};\mathbf{b};\alpha)$, $e \in \{1,2\}$, $b \in \{-1,1\}$, $\alpha \in \mathbb{Q}_p$, de la liste $\mathbf{D}^*$ du chapitre 1.

Remarque : On voit que $\mathrm{End}_{\mathbb{Q}_p[G]}(V_p(E)) = \mathbb{Q}_p$.

A.2.3. Les cas de bonne réduction ($e \in \{1,2\}$) :

Soit E une courbe elliptique sur $\mathbb{Q}_p$ telle que $v_p(j_E) \geq 0$ et dont le défaut de semi-stabilité est $e = \mathrm{dst}(E) \in \{1,2\}$; quitte à tordre E par le caractère correspondant à l'extension ramifiée $\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p$, on peut supposer que E a bonne réduction sur $\mathbb{Q}_p$ (c'est-à-dire $e = 1$). On note encore E le schéma sur $\mathbb{Z}_p$ qui la prolonge, $E(p)$ son groupe p-divisible associé, $\widetilde{E} = E \times_{\mathbb{Z}_p} \mathbb{F}_p$ sa fibre spéciale, et $a_p = a_p(\widetilde{E})$. On a $V_p(E) = V_p(E(p))$, et le déterminant est le caractère cyclotomique χ.

On sait que tout objet V de $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ provenant d'un groupe p-divisible (ou de Barsotti-Tate) est cristallin, et que le type de Hodge-Tate de $D = \mathbf{D}^*_{\mathbf{cris}}(V) = \mathrm{Hom}_{\mathbb{Q}_p[G]}(V, B_{cris})$ est $(0,1)$, c'est-à-dire que l'on a : $\mathrm{Fil}^i D = D$ pour $i \leq 0$, $\mathrm{Fil}^1 D$ est un $\mathbb{Q}_p$-espace vectoriel de dimension 1, et $\mathrm{Fil}^i D = 0$ pour $i \geq 2$.
Ainsi, l'objet $D = \mathbf{D}^*_{\mathbf{cris}}(V_p(E))$ de $\mathbf{MF}^{ad}_{\mathbb{Q}_p}(\varphi)$ est un $\mathbb{Q}_p$-espace vectoriel de dimension 2, muni d'un Frobenius $\mathbb{Q}_p$-linéaire $\varphi : D \to D$ vérifiant $\varphi^2 - a_p\varphi + p = 0$, et d'une filtration de poids $(0,1)$ sur D, qui est donc déterminée par la $\mathbb{Q}_p$-droite $\mathrm{Fil}^1 D$; ces deux données sur D doivent en outre vérifier la condition de faible admissibilité.

Supposons d'abord que $a_p = 0$, c'est-à-dire que $\widetilde{E}$ est supersingulière (la partie connexe $E(p)^0$ de $E(p)$ est de hauteur 2 et $V_p(E) = V_p(E(p)^0)$). Alors le polynôme caractéristique $\mathrm{P}_{car}(\varphi)(X) = X^2 + p$ est irréductible dans $\mathbb{Q}_p[X]$, et aucune $\mathbb{Q}_p$-droite de D n'est stable par φ. Donc, si $e_1 \in D$ est non nul et si $e_2 = \varphi e_1$, alors (e_1, e_2) est une base de D dans laquelle la matrice de φ s'écrit

$$\begin{pmatrix} 0 & -p \\ 1 & 0 \end{pmatrix}.$$

La condition de faible admissibilité est vérifiée, puisque $t_H(D) = 1 = t_N(D)$ et qu'il n'y a pas de sous-objet propre. Ecrivons $\mathrm{Fil}^1 D = \mathbb{Q}_p(\alpha e_1 + \beta e_2)$ avec $\alpha, \beta \in \mathbb{Q}_p$ et $(\alpha, \beta) \neq (0,0)$. Soit D' un autre objet de $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$ et de type de Hodge-Tate $(0,1)$, tel que $D' = \mathbb{Q}_p e'_1 \oplus \mathbb{Q}_p e'_2$ avec $\varphi' e'_1 = e'_2$, $\varphi' e'_2 = -p e'_1$, et $\mathrm{Fil}^1 D' = \mathbb{Q}_p(\alpha' e'_1 + \beta' e'_2)$, $(\alpha', \beta') \neq (0,0)$. Soit $\psi : D \to D'$ une application $\mathbb{Q}_p$-linéaire telle que $\psi\varphi = \varphi'\psi$; alors la matrice de ψ (relative aux bases choisies ci-dessus) doit s'écrire

$$\begin{pmatrix} a & -pc \\ c & a \end{pmatrix} \quad \text{, avec} \quad a, c \in \mathbb{Q}_p \text{ , } (a,c) \neq (0,0) \text{ ,}$$

et ψ est bijective puisque $a^2 + pc^2 \neq 0$. Puis la condition $\psi(\mathrm{Fil}^1 D) = \mathrm{Fil}^1 D'$ s'écrit :

$$\begin{cases} a\alpha - pc\beta &= \alpha' \\ c\alpha + a\beta &= \beta' \end{cases}$$

et comme $\alpha^2 + p\beta^2 \neq 0$, il y a une unique solution (a,c) non nulle. Donc deux tels objets D et D' sont toujours isomorphes dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$.
Finalement, $\mathbf{D}^*_{\mathbf{cris}}(V_p(E))$ est isomorphe dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$ à l'objet $\mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{0})$ de la liste $\mathbf{D}^*$ du chapitre 1 décrit par : $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$; $\varphi e_1 = e_2$; $\varphi e_2 = -p e_1$; $\mathrm{Fil}^1 D = \mathbb{Q}_p e_1$.
En tordant par le caractère d'ordre 2 correspondant à $\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p$, on obtient l'objet $\mathbf{D}^*_{\mathbf{c}}(\mathbf{2};\mathbf{0})$ de $\mathbf{MF}_{\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p}(\varphi)$ de la liste $\mathbf{D}^*$ du chapitre 1.

Supposons maintenant que $a_p \neq 0$, i.e. $a_p \in \mathcal{N}_p^\times$ et $\widetilde{E}$ est ordinaire. Dans la suite exacte courte de $\mathbb{Q}_p[G]$-modules

$$(*_{ord}) \qquad 0 \longrightarrow V_p(E(p)^0) \longrightarrow V_p(E) \longrightarrow V_p(\widetilde{E}) \longrightarrow 0\ ,$$

l'action de I sur le $\mathbb{Q}_p$-espace vectoriel de dimension un $V_p(\widetilde{E})$ est triviale. En appliquant le foncteur contravariant $\mathbf{D}^*_{\mathbf{cris}}$, on obtient une suite exacte courte, encore notée $(*_{ord})$, dans $\mathbf{MF}^{ad}_{\mathbb{Q}_p}(\varphi)$

$$(*_{ord}) \qquad 0 \longrightarrow D_1 \longrightarrow D \longrightarrow D_2 \longrightarrow 0\ ,$$

où $D = \mathbf{D}^*_{\mathbf{cris}}(V_p(E))$, $D_1 = \mathbf{D}^*_{\mathbf{cris}}(V_p(\widetilde{E}))$, et $D_2 = \mathbf{D}^*_{\mathbf{cris}}(V_p(E(p)^0))$. Bien sûr, la première suite exacte est scindée dans $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ si et seulement si la deuxième l'est dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$. Comme $a_p \not\equiv 0 \bmod p\mathbb{Z}_p$, le polynôme $\mathrm{P}_{car}(\varphi)(X) = X^2 - a_pX + p$ est scindé à racines distinctes dans $\mathbb{Q}_p[X]$ (Hensel). Soit $u = u(a_p)$ l'unique élément de $\mathbb{Z}_p^\times$ tel que $u + u^{-1}p = a_p$; on a $\mathrm{P}_{car}(\varphi)(X) = (X-u)(X-u^{-1}p)$, et φ est diagonalisable dans D. Soit (e_1, e_2) une $\mathbb{Q}_p$-base de diagonalisation de φ dans D telle que $\varphi e_1 = ue_1$ et $\varphi e_2 = u^{-1}pe_2$; on a donc $D_1 = \mathbb{Q}_p e_1$ (puisque $u \in \mathbb{Z}_p^\times$) et $D_2 = \mathbb{Q}_p e_2$. La condition de faible admissibilité impose $\mathrm{Fil}^1 D \neq \mathbb{Q}_p e_1$; sinon, $D_1 = \mathbb{Q}_p e_1 = \mathrm{Fil}^1 D$ serait un sous-objet de D tel que :

$$t_H(D_1) = \mathrm{Max}\{\, i \in \mathbb{Z} \,/\, D_1 \cap \mathrm{Fil}^i D \neq 0 \,\} = 1 \ > \ 0 = v_p(u) = t_N(D_1)\ .$$

On a donc $\mathrm{Fil}^1 D = \mathbb{Q}_p(\alpha e_1 + e_2)$ avec $\alpha \in \mathbb{Q}_p$, et D est faiblement admissible : on a bien $t_H(D) = 1 = t_N(D)$, $t_H(D_1) = 0 = t_N(D_1)$, et $t_H(D_2) = (\,0$ si $\alpha \neq 0$; 1 si $\alpha = 0\,) \leq 1 = t_N(D_2)$. On voit que D_2 est un sous-objet de D dans $\mathbf{MF}^{ad}_{\mathbb{Q}_p}(\varphi)$ si et seulement si $\alpha = 0$ (i.e. $t_H(D_2) = t_N(D_2)$, voir [Fo 2], Prop. 5.4.2.*ii)*) ; cela équivaut au fait que la suite exacte $(*_{ord})$ est scindée dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$.
Soit D' un autre objet de $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$ et de type de Hodge-Tate $(0,1)$, tel que $D' = \mathbb{Q}_p e'_1 \oplus \mathbb{Q}_p e'_2$ avec $\varphi' e'_1 = ue'_1$, $\varphi' e'_2 = u^{-1}e'_2$, $u + u^{-1}p = a_p$, et $\mathrm{Fil}^1 D' = \mathbb{Q}_p(\alpha' e'_1 + e'_2)$, $\alpha' \in \mathbb{Q}_p$. Soit $\psi : D \to D'$ une application $\mathbb{Q}_p$-linéaire bijective telle que $\psi\varphi = \varphi'\psi$; donc $\psi e_1 = ae'_1$ et $\psi e_2 = de'_2$, avec $a, d \in \mathbb{Q}_p$, $ad \neq 0$. Alors on a $\psi(\mathrm{Fil}^1 D) = \mathrm{Fil}^1 D'$ si et seulement si $a\alpha = d\alpha'$. Ainsi, deux tels objets D et D' sont isomorphes dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$ si et seulement si $\alpha\alpha' \neq 0$ ou bien $\alpha = \alpha' = 0$.
Finalement, $\mathbf{D}^*_{\mathbf{cris}}(V_p(E))$ est isomorphe à l'objet $\mathbf{D}^*_{\mathbf{c}}(\mathbf{1}; \mathbf{a_p}; \alpha)$ de la liste $\mathbf{D}^*$ du chapitre 1 décrit par : $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$; $\varphi e_1 = ue_1$; $\varphi e_2 = u^{-1}pe_2$; $\mathrm{Fil}^1 D = \mathbb{Q}_p(\alpha e_1 + e_2)$, avec $u + u^{-1}p = a_p \in \mathcal{N}_p^\times$ et $\alpha \in \{0, 1\}$. De plus, on a $\alpha = 0$ si et seulement si $(*_{ord})$ est scindée. En tordant par le caractère d'ordre 2 correspondant à l'extension ramifiée $\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p$, on obtient l'objet $\mathbf{D}^*_{\mathbf{c}}(\mathbf{2}; \mathbf{a_p}; \alpha)$ de $\mathbf{MF}_{\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p}(\varphi)$ de la liste $\mathbf{D}^*$ du chapitre 1.
On constate que dans tous les cas $e \in \{1, 2\}$ la représentation $\Delta_p = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,p}}(V_p(E))$ est définie sur $\mathbb{Q}$. Pour E fixée, le système de représentations du groupe de Weil $(\Delta_l)_{l \in \mathcal{P}}$ est clairement compatible, avec $\Delta_l = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst,l}}(V_l(E))$ pour $l \neq p$: cela provient du fait que le polynôme caractéristique du Frobenius est dans $\mathbb{Q}[X]$ et indépendant de $l \in \mathcal{P}$.

Remarque : Pour $e \in \{1, 2\}$, on a $\mathrm{End}_{\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)}(\mathbf{D}^*_{\mathbf{c}}(\mathbf{e}; \mathbf{0})) = \mathrm{End}_{\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)}(\mathbf{D}^*_{\mathbf{c}}(\mathbf{e}; \mathbf{a_p}; \mathbf{1})) = \mathbb{Q}_p$, alors que $\mathrm{End}_{\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)}(\mathbf{D}^*_{\mathbf{c}}(\mathbf{e}; \mathbf{a_p}; \mathbf{0}))$ est constitué des dilatations.

A.2.4. Les cas de potentielle bonne réduction ($e \geq 3$) :

Soit E une courbe elliptique sur $\mathbb{Q}_p$ telle que $v_p(j_E) \geq 0$ et dont le défaut de semi-stabilité est $e = \mathrm{dst}(E) \in \{3,4,6\}$; alors E acquiert bonne réduction sur l'extension totalement ramifiée $L = L_e = \mathbb{Q}_p(\pi_e)$ de degré e, et n'a bonne réduction sur aucun corps dont l'indice de ramification est strictement inférieur à e. On note K_0 l'extension maximale non ramifiée de $\mathbb{Q}_p$ contenue dans K ; on a donc $K_0 = \mathbb{Q}_p$ si $p \equiv 1 \bmod e\mathbb{Z}$, et $K_0 = \mathbb{Q}_{p^2}$ si $p \equiv -1 \bmod e\mathbb{Z}$. On note E_L et E_K les schémas qui prolongent $E \times_{\mathbb{Q}_p} L$ et $E \times_{\mathbb{Q}_p} K$ sur $O_L = \mathbb{Z}_p[\pi_e]$ et sur $O_K = \mathbb{Z}_{p^2}[\pi_e]$; $E_L(p)$ et $E_K(p) = E_L(p) \times_{O_L} O_K$ sont leurs groupes p-divisibles associés, $\widetilde{E}_L = E_L \times_{O_L} \mathbb{F}_p$ et $\widetilde{E}_K = E_K \times_{O_K} \mathbb{F}_{p^2} = \widetilde{E}_L \times_{\mathbb{F}_p} \mathbb{F}_{p^2}$ leurs fibres spéciales, et $a_p = a_p(\widetilde{E})$. On a $V_p(E_L) = V_p(E_L(p))$ en tant que $\mathbb{Q}_p[G_L]$-module, et $\wedge^2 V_p(E) = \mathbb{Q}_p(1)$.

On sait que tout objet V de $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ qui est potentiellement de Barsotti-Tate est potentiellement cristallin, et que le type de Hodge-Tate de $D = \mathbf{D}^*_{\mathbf{pcris}}(V)$ est $(0,1)$.
L'objet $D = \mathbf{D}^*_{\mathbf{pcris}}(V_p(E)) = \mathbf{D}^*_{\mathbf{cris,K/Q_p}}(V_p(E))$ est dans $\mathbf{MF}^{ad}_{K/\mathbb{Q}_p}(\varphi)$: c'est un K_0-espace vectoriel de dimension 2, muni d'un Frobenius σ-semi-linéaire $\varphi : D \to D$, d'une action semi-linéaire de $G_{K/\mathbb{Q}_p} = \mathrm{Gal}(K/\mathbb{Q}_p)$ sur D commutant à φ, ainsi que d'une filtration décroissante sur $D_K = K \otimes_{K_0} D$, stable par l'action de $G_{K/\mathbb{Q}_p}$ (étendue semi-linéairement sur D_K), et telle que $\mathrm{Fil}^0 D_K = D_K$, $\mathrm{Fil}^1 D_K = K$-droite, $\mathrm{Fil}^2 D_K = 0$. Il doit en outre vérifier la condition de faible admissibilité ; rappelons qu'un objet de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$ est faiblement admissible si et seulement si l'objet de $\mathbf{MF}_K(\varphi)$ que l'on obtient en oubliant l'action de $G_{K/\mathbb{Q}_p}$ l'est ([Fo 2], Prop. 4.4.9.). De plus, on a $\wedge^2 D = \mathbb{Q}_p\{1\}$, i.e. $\wedge^2 D = \mathbb{Q}_p$ sur lequel φ agit par la multiplication par p, $G_{K/\mathbb{Q}_p}$ agit trivialement, et $\mathrm{Fil}^1 \wedge^2 D = \mathbb{Q}_p$, $\mathrm{Fil}^2 \wedge^2 D = 0$.

Le sous-groupe d'inertie $I(K/\mathbb{Q}_p) = < \tau_e >$ de $G_{K/\mathbb{Q}_p}$ agit K_0-linéairement sur D, d'où un morphisme $\nu : < \tau_e > \to \mathrm{Aut}_{K_0}(D)$. Ce morphisme est en fait *injectif*. En effet, si $H = \mathrm{Ker}(\nu) \subset I(K/\mathbb{Q}_p)$ n'était pas trivial, alors $D = \mathbf{D}^*_{\mathbf{pcris}}(V_p(E))$ serait un objet de $\mathbf{MF}_{K^H}(\varphi)$, i.e. $V_p(E)$ deviendrait cristalline sur K^H, et E aurait donc bonne réduction sur le corps K^H dont l'indice de ramification serait strictement inférieur à $e = \mathrm{dst}(E)$. On identifie τ_e avec son image par ν ; c'est donc un élément d'ordre exact $e \in \{3,4,6\}$ de $\mathrm{Aut}_{K_0}(D)$, dont le déterminant est 1 (car $\wedge^2 D = \mathbb{Q}_p\{1\}$). Finalement, on en déduit que

$$\mathrm{P}_{car}(\tau_e)(X) = \mathrm{P}_{min}(\tau_e)(X) = (X - \zeta_e)(X - \zeta_e^{-1}) = X^2 - \gamma_e X + 1 \ \in \mathbb{Z}[X] \,,$$

puisque $(\mathbb{Z}/e\mathbb{Z})^\times = \{\pm 1\}$. En particulier, l'automorphisme $K_0 = \mathbb{Q}_p(\zeta_e)$-linéaire τ_e est diagonalisable à valeurs propres distinctes dans D.
Le Frobenius $\varphi : D \to D$ est σ-semi-linéaire, mais comme $\mathbf{D}^*_{\mathbf{cris,K}}(V_p(E))$ (c'est D sur lequel on oublie l'action de $G_{K/\mathbb{Q}_p}$) est aussi un objet de $\mathbf{MF}_L(\varphi)$ (puisque E acquiert bonne réduction sur L dont le corps résiduel est $\mathbb{F}_p$), le polynôme $X^2 - a_p X + p$ annule φ. Plus précisément, le φ-module filtré sur L : $\mathbf{D}^*_{\mathbf{cris,L}}(V_p(E)) = \mathrm{Hom}_{\mathbb{Q}_p[G_L]}(V_p(E), B_{cris})$ engendre, en tensorisant par K_0 (et la filtration par K), le $(\varphi, G_{K/L})$-module filtré $\mathbf{D}^*_{\mathbf{cris,K/L}}(V_p(E))$.

Supposons d'abord $e \mid p-1$; alors φ est $\mathbb{Q}_p$-linéaire, et la relation $\varphi\tau_e = \tau_e\varphi$ montre que φ est diagonalisable dans une base de vecteurs propres de τ_e. En particulier, son polynôme caractéristique $X^2 - a_p X + p$ se scinde dans $\mathbb{Q}_p[X]$, ce qui équivaut à $a_p \not\equiv 0 \bmod p$, d'où $a_p \neq 0$ et $\widetilde{E}_L$ est ordinaire. Soit $u = u(a_p)$ l'unique élément de $\mathbb{Z}_p^\times$ tel que $u + u^{-1}p = a_p$; alors il existe une $\mathbb{Q}_p$-base (e_1, e_2) de D dans laquelle les matrices de φ et de τ_e s'écrivent

respectivement

$$\begin{pmatrix} u & 0 \\ 0 & u^{-1}p \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} \zeta_e^{\epsilon} & 0 \\ 0 & \zeta_e^{-\epsilon} \end{pmatrix} \quad , \text{avec} \quad \epsilon \in (\mathbb{Z}/e\mathbb{Z})^{\times} = \{\pm 1\} .$$

Cela donne la structure de $(\varphi, G_{K/\mathbb{Q}_p})$-module de $D = \mathbf{D}^*_{\mathbf{cris},\mathbf{K}/\mathbf{Q_p}}(V_p(E))$, ou bien, de façon équivalente, la structure de $\Delta_p = \mathbf{W}\widehat{\mathbf{D}}^*_{\mathbf{pst},\mathbf{p}}(V_p(E))$. Le fait que Δ_p doit être définie sur $\mathbb{Q}$ implique que $a_p \in \mathcal{N}_{p,e}^{\times}$, et Δ_p est isomorphe à l'objet $\mathbf{WD}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon)$, $\epsilon \in \{\pm 1\}$, de la liste $\mathbf{WD}^*$ du chapitre 1 (cf. **A.1.2.** ; en particulier, le $(\varphi, G_{K/\mathbb{Q}_p})$-module décrit ci-dessus avec $\epsilon = 1$ n'est pas isomorphe à celui avec $\epsilon = -1$).
La condition de faible admissibilité impose $\mathrm{Fil}^1 D_K \neq (e_1 \otimes 1)K$ (pour les mêmes raisons qu'en **A.2.3.**, cas $a_p \neq 0$), d'où $\mathrm{Fil}^1 D_K = (e_1 \otimes \beta + e_2 \otimes 1)K$ avec $\beta \in K = \mathbb{Q}_p(\pi_e)$. La faible admissibilité est alors vérifiée, et il reste à écrire que $\mathrm{Fil}^1 D_K$ est stable par $G_{K/\mathbb{Q}_p}$. Cela équivaut à $\tau_e(e_1 \otimes \beta + e_2 \otimes 1) = \zeta_e^{\epsilon} e_1 \otimes \tau_e(\beta) + \zeta_e^{-\epsilon} e_2 \otimes 1 \in (e_1 \otimes \beta + e_2 \otimes 1)\mathbb{Q}_p(\pi_e)$, c'est-à-dire $\zeta_e^{2\epsilon}\tau_e(\beta) = \beta$; cela s'écrit aussi $\zeta_e^{2\epsilon}\pi_e^{2\epsilon}\tau_e(\beta) = \tau_e(\pi_e^{2\epsilon}\beta) = \pi_e^{2\epsilon}\beta$, i.e. $\pi_e^{2\epsilon}\beta \in \mathbb{Q}_p$. En écrivant $\beta = \alpha\pi_e^{-2\epsilon}$ avec $\alpha \in \mathbb{Q}_p$, on obtient $\mathrm{Fil}^1 D_K = (\alpha \cdot e_1 \otimes {\pi_e}^{-\epsilon} + e_2 \otimes {\pi_e}^{\epsilon})\mathbb{Q}_p(\pi_e)$.
Puis, avec des notations évidentes, on voit facilement (comme pour $e = 1$ ou 2), que deux tels objets $D(e; a_p; \epsilon; \alpha)$ et $D(e; a_p; \epsilon; \alpha')$ sont isomorphes dans $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$ si et seulement si $\alpha\alpha' \neq 0$ ou $\alpha = \alpha' = 0$.
Ainsi, $\mathbf{D}^*_{\mathbf{cris},\mathbf{K}/\mathbf{Q_p}}(V_p(E))$ est isomorphe à l'objet $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{a_p};\epsilon;\alpha)$ de la liste $\mathbf{D}^*$ du chapitre 1 décrit par : $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$; $\varphi e_1 = u e_1$; $\varphi e_2 = u^{-1} p e_2$; $\tau_e e_1 = {\zeta_e}^{\epsilon} e_1$; $\tau_e e_2 = {\zeta_e}^{-\epsilon} e_2$; $\mathrm{Fil}^1 D_K = (\alpha \cdot e_1 \otimes {\pi_e}^{-\epsilon} + e_2 \otimes {\pi_e}^{\epsilon})\mathbb{Q}_p(\pi_e)$, avec $e \in \{3,4,6\}$ et $e \mid p-1$, $a_p \in \mathcal{N}_{p,e}^{\times}$ et $u + u^{-1}p = a_p$, $\epsilon \in \{-1,1\}$, $\alpha \in \{0,1\}$.
En outre, lorsque le quadruplet $(e, a_p, \epsilon, \alpha)$ parcourt l'ensemble $\{n \in \{3,4,6\}/n \mid p-1\} \times \mathcal{N}_{p,e}^{\times} \times \{\pm 1\} \times \{0,1\}$, ces objets sont deux-à-deux non-isomorphes dans $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$. Pour chacun d'eux, en notant $D_i = \mathbb{Q}_p e_i$, $i = 1, 2$, on a une suite exacte courte dans $\mathbf{MF}^{ad}_{K/\mathbb{Q}_p}(\varphi)$:

$$0 \longrightarrow D_1 \longrightarrow D \longrightarrow D_2 \longrightarrow 0 ,$$

qui est scindée si et seulement si $\alpha = 0$. Elle provient par application du foncteur $\mathbf{D}^*_{\mathbf{cris},\mathbf{K}/\mathbb{Q}_\mathbf{p}}$ de la suite exacte de $\mathbb{Q}_p[G]$-modules :

$$(*_{ord}) \qquad 0 \longrightarrow V_p(E_K(p)^0) \longrightarrow V_p(E) \longrightarrow V_p(\widetilde{E}_K) \longrightarrow 0 .$$

Supposons maintenant $e \mid p+1$; alors φ est σ-semi-linéaire, $\det(\varphi) = p$, et $\sigma(\zeta_e) = \zeta_e^{-1}$. On note $D_0 = D^{<\omega>} = \{x \in D / \omega x = x\}$; on a en fait $D_0 = \mathbf{D}^*_{\mathbf{cris},\mathbf{L}}(V_p(E))$ et $\mathbb{Q}_{p^2} \otimes_{\mathbb{Q}_p} D_0 = D$. La relation $\omega\varphi = \varphi\omega$ implique $\varphi D_0 \subset D_0$, et la restriction de φ à D_0 est $\mathbb{Q}_p$-linéaire. Soit (e_1, e_2) une $\mathbb{Q}_{p^2}$-base de diagonalisation de τ_e ; quitte à changer (e_1, e_2) en (e_2, e_1), on peut supposer que $\tau_e e_1 = \zeta_e e_1$ et $\tau_e e_2 = \zeta_e^{-1} e_2$ (i.e. $\epsilon = 1$). La relation $\tau_e\omega = \omega\tau_e^{-1}$ donne $\tau_e(\omega e_1) = \zeta_e(\omega e_1)$ et $\tau_e(\omega e_2) = \zeta_e^{-1}(\omega e_2)$, d'où $\omega e_i \in \mathbb{Q}_{p^2} e_i$, $i = 1, 2$; puis la σ-semi-linéarité de ω implique $D_0 \cap \mathbb{Q}_{p^2} e_i \neq 0$, pour $i = 1, 2$. On en déduit qu'il existe une $\mathbb{Q}_p$-base de D_0, que l'on note encore (e_1, e_2), telle que $\tau_e e_1 = \zeta_e e_1$ et $\tau_e e_2 = \zeta_e^{-1} e_2$ dans $D = \mathbb{Q}_{p^2} \otimes_{\mathbb{Q}_p} D_0$. Enfin, la relation $\tau_e\varphi = \varphi\tau_e$ donne $\tau_e(\varphi e_1) = \zeta_e^{-1}(\varphi e_1)$ et $\tau_e(\varphi e_2) = \zeta_e(\varphi e_2)$, d'où $\varphi e_1 \in \mathbb{Q}_{p^2} e_2$ et $\varphi e_2 \in \mathbb{Q}_{p^2} e_1$; mais comme $\varphi D_0 \subset D_0$, on a en fait $\varphi e_1 \in \mathbb{Q}_p e_2$, $\varphi e_2 \in \mathbb{Q}_p e_1$. Comme $\det(\varphi) = p$, on a donc $\varphi e_1 = a e_2$, $\varphi e_2 = -p a^{-1} e_1$, $a \in \mathbb{Q}_p^{\times}$; alors, quitte à changer (e_1, e_2) en $(e_1, a e_2)$, on en déduit qu'il existe une $\mathbb{Q}_{p^2}$-base (e_1, e_2) de D telle que :

$$\varphi e_1 = e_2 \ , \ \varphi e_2 = -p e_1 \ ; \ \omega e_1 = e_1 \ , \ \omega e_2 = e_2 \ ; \ \tau_e e_1 = \zeta_e e_1 \ , \ \tau_e e_2 = \zeta_e^{-1} e_2 .$$

En particulier, on voit que $\varphi^2+p=0$, et donc $a_p=0$, i.e. $\widetilde{E}_L$ est supersingulière. Cela donne la structure de $(\varphi, G_{K/\mathbb{Q}_p})$-module de $D=\mathbf{D}^*_{\mathbf{cris,K/Q_p}}(V_p(E))$, ou bien, de façon équivalente, la structure de $\Delta_p=\mathbf{W\widehat{D}^*_{pst,p}}(V_p(E))$: c'est un $\mathbb{Q}_{p^2}$-espace vectoriel de dimension 2, sur lequel le groupe de Weil W agit $\mathbb{Q}_{p^2}$-linéairement (en posant $\rho_0(w)=(w \bmod W_K)\cdot\varphi^{-v(w)}$ pour tout $w\in W$), et l'on constate que Δ_p est isomorphe à l'objet $\mathbf{WD^*_{pc}(e,0)}$ de la liste $\mathbf{WD^*}$ du chapitre 1.
Déterminons la K-droite Fil^1D_K. Comme il n'y a pas de sous-K_0-espace vectoriel propre de D stable par φ, la condition de faible admissibilité est toujours vérifiée. Puis Fil^1D_K doit être stable par l'action de $G_{K/\mathbb{Q}_p}=<\tau_e>\rtimes<\omega>$ étendue semi-linéairement sur D_K, ce qui est le cas si $\mathrm{Fil}^1D_K=(e_1\otimes 1)K$. Sinon, écrivons $\mathrm{Fil}^1D_K=(e_1\otimes\beta+e_2\otimes 1)K$ avec $\beta\in K=\mathbb{Q}_{p^2}(\pi_e)$. Alors $\omega(e_1\otimes\beta+e_2\otimes 1)=e_1\otimes\omega(\beta)+e_2\otimes 1\in\mathrm{Fil}^1D_K$ si et seulement si $\omega(\beta)=\beta$, i.e. $\beta\in\mathbb{Q}_p(\pi_e)=L$ (c'est normal, puisque D_0 est un objet de $\mathbf{MF}_L(\varphi)$ et $\mathbb{Q}_{p^2}\otimes_{\mathbb{Q}_p}D_0=D$: la filtration sur D_K provient d'une filtration sur $(D_0)_L$). Puis $\tau_e(e_1\otimes\beta+e_2\otimes 1)=\zeta_e e_1\otimes\tau_e(\beta)+\zeta_e^{-1}e_2\otimes 1\in\mathrm{Fil}^1D_K$ si et seulement si $\zeta_e^2\tau_e(\beta)=\beta$, ce qui équivaut à $\pi_e^2\beta\in\mathbb{Q}_{p^2}$; donc $\pi_e^2\beta\in\mathbb{Q}_{p^2}\cap\mathbb{Q}_p(\pi_e)=\mathbb{Q}_p$, et l'on a $\beta=\alpha\pi_e^{-2}$ avec $\alpha\in\mathbb{Q}_p$. Finalement, on en déduit que $\mathrm{Fil}^1D_K=(\alpha\cdot e_1\otimes{\pi_e}^{-1}+e_2\otimes\pi_e)K$ avec $\alpha\in\mathbb{P}^1(\mathbb{Q}_p)$ (on convient que $\mathrm{Fil}^1D_K=(e_1\otimes 1)K$ si $\alpha=\infty$).
Soit maintenant un autre objet D' de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$ tel que $D'=\mathbb{Q}_{p^2}e'_1\oplus\mathbb{Q}_{p^2}e'_2$, $\varphi e'_1=e'_2$, $\varphi e'_2=-pe'_1$, $\omega e'_1=e'_1$, $\omega e'_2=e'_2$, $\tau_e e'_1=\zeta_e e'_1$, $\tau_e e'_2={\zeta_e}^{-1}e'_2$, et $\mathrm{Fil}^1D'_K=(\alpha'\cdot e'_1\otimes{\pi_e}^{-1}+e'_2\otimes\pi_e)K$, avec $\alpha'\in\mathbb{P}^1(\mathbb{Q}_p)$. Soit $\psi: D\to D'$ un morphisme non nul de $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$. Alors $\psi\omega=\omega\psi$ implique $\psi(D_0)\subset D'_0=\mathbb{Q}_p e'_1\oplus\mathbb{Q}_p e'_2$, et $\psi\tau_e=\tau_e\psi$ implique $\psi e_i\in\mathbb{Q}_{p^2}e'_i$, $i=1,2$; donc $\psi e_1=ae_1$ et $\psi e_2=de_2$ avec $a,d\in\mathbb{Q}_p$, et $\psi\varphi=\varphi\psi$ donne alors $a=d$. Enfin, on voit que $\psi_K(\mathrm{Fil}^1D_K)\subset\mathrm{Fil}^1D'_K$ si et seulement si $\alpha=\alpha'$.
Ainsi, $\mathbf{D}^*_{\mathbf{cris,K/Q_p}}(V_p(E))$ est isomorphe dans $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$ à l'un des objets $\mathbf{D^*_{pc}(e;0;\alpha)}$ de la liste $\mathbf{D^*}$ du chapitre 1, décrits par : $D=\mathbb{Q}_{p^2}e_1\oplus\mathbb{Q}_{p^2}e_2$; $\varphi e_1=e_2$; $\varphi e_2=-pe_1$; $\omega e_1=e_1$; $\omega e_2=e_2$; $\tau_e e_1=\zeta_e e_1$; $\tau_e e_2={\zeta_e}^{-1}e_2$; $\mathrm{Fil}^1D_K=(\alpha\cdot e_1\otimes{\pi_e}^{-1}+e_2\otimes\pi_e)\mathbb{Q}_{p^2}(\pi_e)$, avec $e\in\{3,4,6\}$ et $e\mid p+1$, $\alpha\in\mathbb{P}^1(\mathbb{Q}_p)$.
Lorsque le couple (e,α) parcourt l'ensemble $\{n\in\{3,4,6\}/n\mid p+1\}\times\mathbb{P}^1(\mathbb{Q}_p)$, ces objets sont deux-à-deux non-isomorphes dans $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$.

Pour $E/\mathbb{Q}_p$ fixée, on constate la compatibilité du système $(V_l(E))_{l\in\mathcal{P}}$, *sauf* dans le cas où $E/\mathbb{Q}_p$ est potentiellement ordinaire avec $\mathrm{dst}(E)\geq 3$. Dans ce cas, l'invariant $\epsilon\in\{\pm 1\}$ se lit sur la représentation $E[p]$ (voir [Kr], 2.3.1.), et le fait qu'il soit le même pour tous les $V_l(E)$, $l\in\mathcal{P}$, se déduit de [Se-Ta] et de [Fo 3], Rmq. 2.4.6. iii).

Remarques :
1) On a $\mathrm{End}_{\mathbf{MF}_{L_e/\mathbb{Q}_p}(\varphi)}(\mathbf{D^*_{pc}(e;a_p;\epsilon;1)})=\mathrm{End}_{\mathbf{MF}_{K_e/\mathbb{Q}_p}(\varphi)}(\mathbf{D^*_{pc}(e;0;\alpha)})=\mathbb{Q}_p$, alors que $\mathrm{End}_{\mathbf{MF}_{L_e/\mathbb{Q}_p}(\varphi)}(\mathbf{D^*_{pc}(e;a_p;\epsilon;0)})=\{\begin{pmatrix}a&0\\0&d\end{pmatrix},\ a,d\in\mathbb{Q}_p\}$, et $\mathrm{End}_{\mathbf{MF}_{K_e/\mathbb{Q}_{p^2}}(\varphi)}(\mathbf{D^*_{pc}(e;0;\alpha)})$ $=\mathbb{Q}_p$ si $\alpha\in\mathbb{Q}_p^\times$; $\{\begin{pmatrix}a&0\\0&\sigma(a)\end{pmatrix},\ a\in\mathbb{Q}_{p^2}\}$ si $\alpha\in\{0,\infty\}$.
2) On voit que pour $E/\mathbb{Q}_p$ telle que $v_p(j_E)\geq 0$ et $\mathrm{dst}(E)=e\geq 3$, on a :

$$\begin{cases} e\mid p-1 & \Rightarrow\ E \text{ est potentiellement ordinaire,}\\ e\mid p+1 & \Rightarrow\ E \text{ est potentiellement supersingulière.}\end{cases}$$

Ceci achève la démonstration des parties 1) et 2) du théorème **2.1.** du chapitre 1.

ANNEXE B

Les réseaux G-stables des $V_p(E)$; détermination des $T_p(E)$ et $E[p]$.

Cette partie est consacrée à la description des $\mathbb{Z}_p[G]$-modules $T_p(E)$ ainsi que des $\mathbb{F}_p[G]$-modules $E[p] = T_p(E)/pT_p(E)$ constitués des points d'ordre p des courbes elliptiques $E/\mathbb{Q}_p$. On procède de la manière suivante :
- dans chaque classe d'isomorphisme de $V_p(E)$, on détermine les réseaux stables par G, à $\mathbb{Z}_p[G]$-isomorphisme près ; de plus, si ξ est un caractère d'ordre 2, on a $T_p(E^\xi) \simeq T_p(E)(\xi)$;
- dès que $T' \subset T_p(E)$ est un autre réseau G-stable, il existe une courbe elliptique E' et une p-isogénie $\psi : E' \to E$, définies sur $\mathbb{Q}_p$, telles que $\psi_p(T_p(E')) = T'$; et si $T_p(E) \subset T''$ est un autre réseau G-stable, il existe une courbe elliptique E'' et une p-isogénie $\gamma : E \to E''$, définies sur $\mathbb{Q}_p$, telles que $\gamma_p(T'') = T_p(E'')$ (cf. chapitre 2, **2.4.4.**, lemme 1).

Signalons que tous les résultats de cette annexe sont connus : voir [Se 1], [Se 2] et [Kr]. Seules certaines méthodes sont nouvelles, et l'on a essayé de proposer des approches variées. Les résultats correspondants aux cas de bonne réduction ou de twists d'ordre 2 de ceux-ci (ce sont les cas notés $\mathbf{D}_c^*$ dans la liste du chapitre 1) ont été obtenus en utilisant la théorie des Modules de Dieudonné sur $\mathbb{Z}_p$ comme dans [Fo 4], ainsi que, bien sûr, le théorème de pleine fidélité de Tate (**B.2.**). Les résultats correspondants aux cas multiplicatifs (**B.1.**), ainsi qu'aux cas potentiellement ordinaires (**B.3.1.**), ont été obtenus en étudiant l'image de Galois dans $\mathrm{Aut}_{\mathbb{Q}_p}(V_p(E))$. Enfin, ceux correspondants aux cas potentiellement supersinguliers (et qui ne sont pas un twist ramifié d'ordre 2 d'une courbe ayant bonne réduction) ont été obtenus en faisant des calculs explicites dans $BW(R)$ (bivecteurs de Witt). Evidemment, c'est ce dernier qui est le plus intéressant, et pour lequel on propose donc une rédaction plus détaillée (**B.3.2.**). On notera que, bien souvent, une méthode employée pour l'un des cas pourrait s'appliquer à un autre.
Enfin, signalons que pour traiter les cas de potentielle bonne réduction, on peut aussi utiliser la théorie des modules de Dieudonné sur l'anneau des entiers d'une extension totalement ramifiée de degré e de $\mathbb{Q}_p$ ([Fo 4]) ; l'inconvénient est que l'on doit alors supposer $e < p-1$. C'est le point de vue qui a été adopté au chapitre 3, en **3.3.**.

Rappelons que $\chi : G \to \mathbb{Z}_p^\times$ est le caractère cyclotomique donnant l'action de G sur les racines p^n-ièmes de l'unité, $n \geq 1$, et que $\chi_p : G \to \mathbb{F}_p^\times$ est sa réduction modulo p.

Pour tout $u \in \mathbb{Z}_p^\times$, on note $\eta_u : G \to G/I \to \mathbb{Z}_p^\times$ l'unique caractère non ramifié qui envoie le Frobenius arithmétique sur u ; de même si $u \in \mathbb{F}_p^\times$. Lorsque $e \geq 2$ et e divise $p-1$, on note $\xi_e : G \to G_{K_e/\mathbb{Q}_p} \to \mu_e(\overline{\mathbb{Q}}_p) = <\zeta_e> \subset \mathbb{Z}_p^\times$ le caractère ramifié défini par $\xi_e(g) = \frac{g\pi_e}{\pi_e}$, $g \in G$. On a : $\xi_e \bmod p\mathbb{Z}_p = \chi_p^{\frac{p-1}{e}}$.

B.1. Les cas multiplicatifs :

Soit E une courbe elliptique sur $\mathbb{Q}_p$ telle que $v_p(j_E) < 0$; quitte à tordre E par un caractère d'ordre 1 ou 2, on peut supposer que E est une courbe de Tate E_q, où $q \in p\mathbb{Z}_p \backslash \{0\}$ est uniquement déterminé par l'invariant modulaire j_E. Rappelons que l'on a une suite exacte de $\mathbb{Z}_p[G]$-modules

$$(*_m) \qquad 0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow T_p(E_q) \longrightarrow \mathbb{Z}_p \longrightarrow 0 \,,$$

qui n'est pas scindée (cf. [Se 1], A.1.2., ou bien l'annexe A). Il existe donc un plus grand entier $n \in \mathbb{N}$ tel que la suite exacte

$$(*_m) \bmod p^n\mathbb{Z}_p \qquad 0 \longrightarrow \mu_{p^n}(\overline{\mathbb{Q}}_p) \longrightarrow E_q[p^n] \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

de $\mathbb{Z}/p^n\mathbb{Z}[G]$-modules se scinde.

On sait que $\mathbf{D}^*_{\mathbf{pst}}(V_p(E))$ est isomorphe à l'un des objets $\mathbf{D}^*_{\mathbf{m}}(\mathbf{1};\mathbf{1};\alpha)$, $\alpha \in \mathbb{Q}_p$, de la liste $\mathbf{D}^*$, décrit par : $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = e_1$, $\varphi e_2 = pe_2$, $Ne_1 = 0$, $Ne_2 = e_1$, et $\mathrm{Fil}^1 D = \mathbb{Q}_p(\alpha e_1 + e_2)$. L'invariant α est donné par $\alpha = -\mathrm{Log}(u_q)/v_p(q)$, où l'on a écrit $q = u_q p^{v_p(q)}$, $u_q \in \mathbb{Z}_p{}^\times$, et Log est le logarithme p-adique usuel sur $\mathbb{Z}_p{}^\times$.
En considérant la suite exacte $(*_m)$, ou bien en appliquant le foncteur quasi-inverse $\mathbf{V}^*_{\mathbf{st}}$ de $\mathbf{D}^*_{\mathbf{st}}$, on obtient facilement : il existe une $\mathbb{Q}_p$-base de $V_p(E)$ telle que G agit via

$$\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix} \qquad \text{avec} \qquad * \neq 0 \,.$$

Alors il existe une $\mathbb{Z}_p$-base (e_1, e_2) de $T_p(E) = T_p(E_q)$ sur laquelle G agit par $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$, toujours avec $* \neq 0$. On peut choisir cette base explicitement : $e_1 = \varepsilon = (\zeta_{p^n})_{n \geq 0}$ est un générateur de $\mathbb{Z}_p(1)$, et $e_2 = w_q$ est un élément de $T_p(E_q)$ dont l'image dans $\mathbb{Z}_p$ est 1, que l'on peut écrire $w_q = (z_n \bmod q^{\mathbb{Z}})_{n \geq 0}$, avec $z_n \in \overline{\mathbb{Q}}_p^\times$ et $z_0 = q$, $z_{n+1}^p = z_n$ pour tout $n \geq 0$ (les autres tels choix possibles sont les $\nu_n z_n$, $n \geq 0$, avec $\nu_n \in \mu_{p^n}$). La suite exacte $(*_m \bmod p^n)$ est scindée si et seulement si le réseau $\mathbb{Z}_p e_1 \oplus p^{-n}\mathbb{Z}_p e_2$ est stable par G, ce qui équivaut à $z_n \bmod \mu_{p^n} \in \mathbb{Q}_p$; autrement dit, $(*_m \bmod p^n)$ se scinde si et seulement si $q \in (\mathbb{Q}_p^\times)^{p^n}$. On note $n_p(q)$ le plus grand entier n tel que $q \in (\mathbb{Q}_p^\times)^{p^n}$; c'est donc aussi le plus grand entier tel que $(*_m \bmod p^n)$ se scinde.
Soit T_0 le réseau $\mathbb{Z}_p e_1 \oplus p^{-n_p(q)}\mathbb{Z}_p e_2$; il est stable par G, et si l'on considère la suite exacte de $\mathbb{Z}_p[G]$-modules

$$(*_0) \qquad 0 \longrightarrow \mathbb{Z}_p e_1 \longrightarrow T_0 \longrightarrow p^{-n_p(q)}\mathbb{Z}_p e_2 \longrightarrow 0 \,,$$

alors $(*_0)$ est scindée modulo $p^m\mathbb{Z}_p$ si et seulement si $m = 0$. Comme G agit sur la $\mathbb{Z}_p$-base $(e_1, p^{-n_p(q)}e_2)$ de T_0 par $\rho = \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$, on en déduit qu'il existe des éléments $g_i \in G$, $i = 1, 2$, tels que $\rho(g_i) = \begin{pmatrix} a_i & c_i \\ 0 & b_i \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$, avec $c_1 \in \mathbb{Z}_p^\times$ et $a_2 \not\equiv b_2 \bmod p\mathbb{Z}_p$. On montre alors que l'existence de tels automorphismes de T_0 implique que les autres réseaux G-stables de $V_p(E_q)$ sont, à homothétie près, les $\mathbb{Z}_p e_1 \oplus p^{m-n_p(q)}\mathbb{Z}_p e_2$, avec $m \in \mathbb{N}$ (voir **B.3.1.** - à partir du lemme - pour une preuve de cette affirmation).

Soit $E/\mathbb{Q}_p$ une courbe elliptique telle que $v_p(j_E) < 0$, qui est le twist par un caractère d'ordre 1 ou 2 d'une courbe de Tate E_q , avec $q \in p\mathbb{Z}_p\backslash\{0\}$. La suite exacte de G-modules $(*_m)$ n'étant pas scindée, il existe un plus grand entier $n_p(q)$ tel que $q \in (\mathbb{Q}_p^\times)^{p^{n_p(q)}}$. Alors il existe une $\mathbb{Q}_p$-base (e_1, e_2) de $V_p(E)$ telle que, à isomorphisme près, les réseaux stables par G sont les :

$$\mathbb{Z}_p e_1 \oplus p^m \mathbb{Z}_p e_2 \quad , \quad m \geq -n_p(q) \ .$$

On en déduit *l'action de G sur $E[p]$: il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via*

$$\begin{pmatrix} \eta_{-1}^{\frac{1-b}{2}} \chi_p^{1-\frac{p-1}{e}} & * \\ 0 & \eta_{-1}^{\frac{b-1}{2}} \chi_p^{\frac{p-1}{e}} \end{pmatrix} \quad \text{avec} \quad * = 0 \Leftrightarrow n_p(q) \geq 1 \ .$$

Remarque : $q \in (\mathbb{Q}_p^\times)^{p^n}$ implique $v_p(q) = -v_p(j_E) \equiv 0 \bmod p^n\mathbb{Z}$.

B.2. Les cas de bonne réduction ($e \in \{1, 2\}$) :

Soit E une courbe elliptique sur $\mathbb{Q}_p$ qui est le twist par un caractère ramifié d'ordre 1 ou 2 d'une courbe elliptique ayant bonne réduction sur $\mathbb{Q}_p$; alors $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E))$ est isomorphe à l'un des objets notés $\mathbf{D}^*_{\mathbf{c}}$ dans la liste du chapitre 1. Quitte à tordre, on peut supposer que $E/\mathbb{Q}_p$ a bonne réduction sur $\mathbb{Q}_p$, i.e. que E se prolonge en un schéma sur $\mathbb{Z}_p$, encore noté E, et auquel est associé un groupe p-divisible $E(p)$ sur $\mathbb{Z}_p$. D'après [Fo 4] (voir **3.2.2.**), les $\mathbb{Z}_p$-réseaux de $V_p(E)$ stables par G sont en bijection avec les $\mathbb{Z}_p$-réseaux M de $D = \mathbf{D}^*_{\mathbf{cris}}(V_p(E))$ stables par φ et tels que l'inclusion $M \cap \mathrm{Fil}^1 D \hookrightarrow M$ induit un isomorphisme de $\mathbb{F}_p$-espaces vectoriels

$$(M \cap \mathrm{Fil}^1 D)/p(M \cap \mathrm{Fil}^1 D) \simeq M/\varphi M \ .$$

Comme ce sont des $\mathbb{F}_p$-espaces vectoriels de dimension 1, cette condition est équivalente à $M = \varphi M + (M \cap \mathrm{Fil}^1 D)$.

Soient T et T' deux réseaux G-stables de $V_p(E)$, et soient M et M' les $\mathbb{Z}_p$-réseaux de $D = \mathbf{D}^*_{\mathbf{cris}}(V_p(E))$ leur correspondant ; alors T et T' sont $\mathbb{Z}_p[G]$-isomorphes si et seulement si il existe un isomorphisme $\mathbb{Z}_p$-linéaire $\psi : M \to M'$ commutant aux Frobenius et vérifiant $\psi(M \cap \mathrm{Fil}^1 D) = (M' \cap \mathrm{Fil}^1 D)$.

B.2.1. Les cas ordinaires :

Soit $E/\mathbb{Q}_p$ une courbe elliptique ayant bonne réduction ordinaire sur $\mathbb{Q}_p$. On a une suite exacte de $\mathbb{Z}_p[G]$-modules

$$(*_{ord}) \qquad 0 \longrightarrow T_p(E(p)^0) \longrightarrow T_p(E) \longrightarrow T_p(\widetilde{E}) \longrightarrow 0 \ ,$$

où $E(p)^0$ désigne la partie connexe (ici de hauteur 1) du groupe p-divisible associé à E, et $\widetilde{E}$ désigne sa fibre spéciale. On sait que $\mathbf{D}^*_{\mathbf{cris}}(V_p(E))$ est isomorphe à l'un des objets $\mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_p};\alpha)$, $a_p \in \mathcal{N}_p^\times$, $\alpha \in \{0,1\}$, de la liste $\mathbf{D}^*$, décrit par : $u = u(a_p)$ est l'unique élément de $\mathbb{Z}_p^\times$ vérifiant $u + u^{-1}p = a_p$; $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = ue_1$, $\varphi e_2 = u^{-1}pe_2$, et $\mathrm{Fil}^1 D = \mathbb{Q}_p(\alpha e_1 + e_2)$. On note aussi $(*_{ord})$ la suite exacte dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$:

$$(*_{ord}) \qquad 0 \longrightarrow \mathbb{Q}_p e_1 \longrightarrow D \longrightarrow \mathbb{Q}_p e_2 \longrightarrow 0 \ .$$

Soit M un $\mathbb{Z}_p$-réseau de D stable par φ ; on a des inclusions strictes $pM \subset \varphi M \subset M$. Le lemme 3 de **3.1.2.** montre qu'il existe alors une $\mathbb{Z}_p$-base (f_1, f_2) de M telle que $\varphi f_1 = uf_1$ et $\varphi f_2 = u^{-1}pf_2$; on en déduit que $M = p^{m_1}\mathbb{Z}_p e_1 \oplus p^{m_2}\mathbb{Z}_p e_2$, avec $m_1, m_2 \in \mathbb{Z}$.

- Cas $\alpha = 0 \Leftrightarrow (*_{ord})$ scindée dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$: alors $\mathrm{Fil}^1 D = \mathbb{Q}_p e_2$, d'où, à homothétie près, $M \cap \mathrm{Fil}^1 D = \mathbb{Z}_p e_2$. On a $M = p^m\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$, $m \in \mathbb{Z}$, et $\varphi M = p^m\mathbb{Z}_p e_1 \oplus p\mathbb{Z}_p e_2$; on voit que la condition $M = \varphi M + (M \cap \mathrm{Fil}^1 D)$ est bien vérifiée. Donc les réseaux G-stables de $V_p(E)$ sont en bijection avec les réseaux $M = p^{m_1}\mathbb{Z}_p e_1 \oplus p^{m_2}\mathbb{Z}_p e_2$, $m_1, m_2 \in \mathbb{Z}$, de D.
Soient m_1', m_2' deux autres entiers et $M' = p^{m_1'}\mathbb{Z}_p e_1 \oplus p^{m_2'}\mathbb{Z}_p e_2$; alors on a $M' \cap \mathrm{Fil}^1 D = p^{m_2'}\mathbb{Z}_p e_2$, et la bijection $\mathbb{Z}_p$-linéaire de M dans M' définie par $p^{m_i} e_i \mapsto p^{m_i'} e_i$, $i = 1, 2$, commute avec φ et envoie $M \cap \mathrm{Fil}^1 D$ sur $M' \cap \mathrm{Fil}^1 D$. On en déduit que les réseaux G-stables de $V_p(E)$ sont tous $\mathbb{Z}_p[G]$-isomorphes.

- Cas $\alpha = 1 \Leftrightarrow (*_{ord})$ non scindée dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$: alors $\mathrm{Fil}^1 D = \mathbb{Q}_p(e_1 + e_2)$. A homothétie près, $M = p^m\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$, $m \in \mathbb{Z}$, d'où $M \cap \mathrm{Fil}^1 D = \mathbb{Z}_p(e_1 + e_2)$ si $m < 0$, et $M \cap \mathrm{Fil}^1 D = p^m\mathbb{Z}_p(e_1 + e_2)$ si $m \geq 0$. On voit alors que la condition $M = \varphi M + (M \cap \mathrm{Fil}^1 D)$ est vérifiée pour $m \geq 0$ si et seulement si $m = 0$, et qu'elle l'est toujours pour $m < 0$. Donc, à homothétie près, les réseaux G-stables de $V_p(E)$ sont en bijection avec les réseaux $M = p^m\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$, $m \leq 0$, de D.
Soit $m' \leq 0$ un autre entier, et $M' = p^{m'}\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$. Une bijection $\mathbb{Z}_p$-linéaire ψ de M dans M' commutant avec φ doit envoyer $p^m e_1$ sur $u_1 p^{m'} e_1$, et e_2 sur $u_2 e_2$, avec $u_i \in \mathbb{Z}_p^\times$. Mais alors $\psi(M \cap \mathrm{Fil}^1 D) = \mathbb{Z}_p(u_1 p^{m'-m} e_1 + u_2 e_2) = M' \cap \mathrm{Fil}^1 D = \mathbb{Z}_p(e_1 + e_2)$ si et seulement si $u_1 = u_2$ et $m = m'$. On en déduit que les classes d'isomorphisme des réseaux G-stables de $V_p(E)$ sont en bijection avec les réseaux $M = p^m\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$, $m \leq 0$, de D.

Remarque : Fixons une courbe elliptique $\widetilde{E}$ sur $\mathbb{F}_p$ ordinaire. Comme dans le chapitre 3 (**3.2.4.**), considérons les schémas elliptiques E_β sur $\mathbb{Z}_p$ relevant $\widetilde{E}$, avec $\beta \in (\mathbb{Z}_p/\sim)\backslash\{0\}$ (ils sont deux-à-deux non-isomorphes) ; on rappelle que pour $x, y \in \mathbb{Z}_p$, on a posé $x \sim y \Leftrightarrow x^{m(\tilde{\jmath})} = y^{m(\tilde{\jmath})}$, où $\tilde{\jmath}$ est l'invariant modulaire de $\widetilde{E}$, et $m(\tilde{\jmath}) = 1$ si $\tilde{\jmath} \notin \{0, 1728\}$, $m(1728) = 2$, et $m(0) = 3$. Les objets $D_\beta = \mathbf{D}^*_{\mathbf{cris}}(V_p(E_\beta))$ de $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$ sont décrits par : $D_\beta = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, $\varphi e_1 = ue_1$, $\varphi e_2 = u^{-1}pe_2$, et $\mathrm{Fil}^1 D_\beta = \mathbb{Q}_p(\beta e_1 + e_2)$. Tous ces objets sont isomorphes dans $\mathbf{MF}_{\mathbb{Q}_p}(\varphi)$ à $\mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{a_p};\mathbf{1})$. Avec les mêmes méthodes, on trouve que les $\mathbb{Z}_p$-réseaux φ-stables de D_β vérifiant la condition de filtration sont, à homothétie près, les $p^m\mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$, avec cette fois $m \leq v_p(\beta)$, et qu'ils sont deux-à-deux non-isomorphes (c'est d'ailleurs en relevant

le module de Dieudonné du groupe p-divisible de $\widetilde{E}$ en des modules de Dieudonné sur $\mathbb{Z}_p$ que l'on a construit les E_β, cf. **3.2.**). C'est un peu plus précis que ce que l'on vient de faire ci-dessus (où l'on a choisit $\beta \equiv 1 \bmod \sim$) ; si $n(E_\beta)$ est le plus grand entier naturel tel que la suite exacte $0 \to T_p(E_\beta(p)^0) \to T_p(E_\beta) \to T_p(\widetilde{E}) \to 0$ se scinde modulo $p^{n(E_\beta)}\mathbb{Z}_p$, alors on voit que $n(E_\beta) = v_p(\beta)$.

Soit $E/\mathbb{Q}_p$ le twist par un caractère ramifié d'ordre $e \in \{1,2\}$ d'une courbe elliptique ayant bonne réduction ordinaire sur $\mathbb{Q}_p$.
- Si $\alpha = 0 \Leftrightarrow (*_{ord})$ scindée, les réseaux de $V_p(E)$ stables par G sont tous isomorphes.
- Si $\alpha = 1 \Leftrightarrow (*_{ord})$ non scindée, il existe un plus grand entier naturel n_E tel que la suite exacte de $\mathbb{Z}/p^{n_E}\mathbb{Z}[G]$-modules $(*_{ord}) \bmod p^{n_E}\mathbb{Z}_p$ soit scindée. Alors il existe une $\mathbb{Q}_p$-base (e_1, e_2) de $V_p(E)$ telle que, à isomorphisme près, les réseaux stables par G sont les :

$$\mathbb{Z}_p e_1 \oplus p^m \mathbb{Z}_p e_2 \quad , \quad m \geq -n_E \ .$$

On en déduit *l'action de G sur $E[p]$: il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via*

$$\begin{pmatrix} \eta_{\overline{a}_p}^{-1}\chi_p^{1-\frac{p-1}{e}} & * \\ 0 & \eta_{\overline{a}_p}\chi_p^{\frac{p-1}{e}} \end{pmatrix} \quad \text{avec} \quad * = 0 \Leftrightarrow [\alpha = 0 \ \text{ ou } \ n_E \geq 1] \ .$$

B.2.2. Les cas supersinguliers :

Soit $E/\mathbb{Q}_p$ une courbe elliptique ayant bonne réduction supersingulière sur $\mathbb{Q}_p$. On sait que $\mathbf{D}^*_{\mathbf{cris}}(V_p(E))$ est isomorphe à l'objet $\mathbf{D}^*_{\mathbf{c}}(\mathbf{1};\mathbf{0})$ de la liste $\mathbf{D}^*$, décrit par : $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$, et $\mathrm{Fil}^1 D = \mathbb{Q}_p e_1$.

Soit M un réseau de D stable par φ ; on a des inclusions strictes $pM \subset \varphi M \subset M$. La condition $M = \varphi M + (M \cap \mathrm{Fil}^1 D)$ et la relation $\varphi^2 = -p$ donnent $\varphi M = \varphi(M \cap \mathrm{Fil}^1 D) + pM$, d'où $M = (M \cap \mathrm{Fil}^1 D) + \varphi(M \cap \mathrm{Fil}^1 D) + pM$, et donc $M = (M \cap \mathrm{Fil}^1 D) + \varphi(M \cap \mathrm{Fil}^1 D)$ (Nakayama). Puis, $M \cap \mathrm{Fil}^1 D$ étant un $\mathbb{Z}_p$-module libre de rang 1, et le polynôme $X^2 + p$ étant irréductible dans $\mathbb{Q}_p[X]$, on en déduit que $M = (M \cap \mathrm{Fil}^1 D) \oplus \varphi(M \cap \mathrm{Fil}^1 D)$. Alors, à homothétie près, on a $M \cap \mathrm{Fil}^1 D = \mathbb{Z}_p e_1$, d'où $M = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$. Les réseaux G-stables de $V_p(E)$ sont donc tous homothétiques, et le $\mathbb{F}_p[G]$-module $E[p]$ constitué des points d'ordre p de E est irréductible.
D'après Serre ([Se 2]), il existe une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1 sur $E[p]$ sur laquelle le groupe d'inertie absolu I agit par le caractère fondamental ψ_2 de niveau 2 ; donc $E[p]$ est absolument irréductible, et, comme le déterminant est χ_p, la proposition du §9 de [Fo-Ma] implique que $E[p]$ est $\mathbb{F}_p[G]$-isomorphe à l'objet noté $\overline{V}_{1,1}$.

Remarque : on peut retrouver cela en faisant des calculs explicites dans $BW(R)$, comme dans le paragraphe **B.3.2.** (mais en plus simple).

Lorsque $E/\mathbb{Q}_p$ est le twist par un caractère ramifié d'ordre $e \in \{1,2\}$ d'une courbe elliptique ayant bonne réduction supersingulière sur $\mathbb{Q}_p$, alors les réseaux de $V_p(E)$ stables par G sont tous homothétiques.

Action de G sur $E[p]$: soient $\pi, \zeta \in \overline{\mathbb{Q}}_p$ tels que $\pi^{p^2-1} = -p$ et $\zeta^{p+1} = -1$; il existe une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1 sur $E[p]$ telle que G agit par

$$G \longrightarrow \mathrm{Gal}(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2}) \ ,$$

où $I(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p)$ agit via $\psi_2^{1-\frac{p^2-1}{e}}$, où ψ_2 est le quotient du caractère fondamental de niveau 2, et le relèvement du Frobenius fixant π agit semi-linéairement via $x \mapsto \zeta x^p$, $x \in \mathbb{F}_{p^2}$.
La classe d'isomorphisme ne dépend pas du choix de ζ, et la représentation est absolument irréductible. Avec les notations de [Fo-Ma], pour $e = 1$ c'est l'objet $\overline{V}_{1,1}$, et pour $e = 2$ c'est l'objet $\overline{V}_{1-\frac{p^2-1}{2},1}$. *L'action de I sur $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ est diagonalisable, et il existe une $\mathbb{F}_{p^2}$-base de $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ telle que I agit via*

$$\begin{pmatrix} \psi_2^{1-\frac{p^2-1}{e}} & 0 \\ 0 & \psi_2^{p+\frac{p^2-1}{e}} \end{pmatrix} .$$

B.3. Les cas de potentielle bonne réduction ($e \in \{3,4,6\}$) :

B.3.1. Les cas potentiellement ordinaires :

Soit $E/\mathbb{Q}_p$ une courbe elliptique ayant potentiellement bonne réduction ordinaire, et dont le défaut de semi-stabilité est $\mathrm{dst}(E) = e \in \{3,4,6\}$; alors E acquiert bonne réduction sur $K = \mathbb{Q}_p(\pi_e)$, et e divise $p-1$. On a une suite exacte de $\mathbb{Q}_p[G]$-modules

$$(*_{ord}) \qquad 0 \longrightarrow V_p(E_K(p)^0) \longrightarrow V_p(E) \longrightarrow V_p(\widetilde{E_K}) \longrightarrow 0 \ ,$$

où $E_K(p)^0$ désigne la partie connexe du groupe p-divisible de $E_K = E \times_{\mathbb{Q}_p} K$, et $\widetilde{E_K}$ sa fibre spéciale. On sait que $\mathbf{D}^*_{\mathbf{pcris}}(V_p(E))$ est isomorphe à l'un des objets $\mathbf{D}^*_{\mathbf{pc}}(\mathbf{e}; \mathbf{a_p}; \epsilon; \alpha)$, avec $e \in \{3,4,6\}$ et $e \mid p-1$, $a_p \in \mathcal{N}^{\times}_{p,e}$, $\epsilon \in \{-1,1\}$, $\alpha \in \{0,1\}$, de la liste $\mathbf{D}^*$, décrit par : $u = u(a_p)$ est l'unique élément de $\mathbb{Z}_p^{\times}$ tel que $u + u^{-1}p = a_p$; $K_e = \mathbb{Q}_p(\pi_e)$, $G_{K_e/\mathbb{Q}_p} = <\tau_e>$, $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$, avec $\varphi e_1 = u e_1$, $\varphi e_2 = u^{-1} p e_2$, $\tau_e e_1 = {\zeta_e}^{\epsilon} e_1$, $\tau_e e_2 = {\zeta_e}^{-\epsilon} e_2$, et $\mathrm{Fil}^1 D_{K_e} = (\alpha \cdot e_1 \otimes {\pi_e}^{-\epsilon} + e_2 \otimes {\pi_e}^{\epsilon}) \mathbb{Q}_p(\pi_e)$.

En appliquant le foncteur quasi-inverse $\mathbf{V}^*_{\mathbf{pcris}}$ de $\mathbf{D}^*_{\mathbf{pcris}}$, on obtient facilement : il existe une $\mathbb{Q}_p$-base de $V_p(E)$ telle que G agit via

$$\begin{pmatrix} \eta_u^{-1} \xi_e^{-\epsilon} \chi & * \\ 0 & \eta_u \xi_e^{\epsilon} \end{pmatrix} \quad , \text{avec} \quad * = 0 \Leftrightarrow \alpha = 0 \ .$$

Quitte à tordre E par le caractère ramifié d'ordre 2 correspondant à l'extension $\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p$, on peut supposer que $\epsilon = 1$ (cf. la description des twists d'ordre deux du chapitre 1). Soit (f_1, f_2) une $\mathbb{Q}_p$-base de $V_p(E)$ sur laquelle G agit comme ci-dessus ; soit T un réseau G-stable de $V_p(E)$. On pose $T_1 = T \cap \mathbb{Q}_p f_1$ et $T_2 = T \cap \mathbb{Q}_p f_2$; alors on a une suite exacte de $\mathbb{Z}_p[G]$-modules

$$(*_{ord}) \qquad 0 \longrightarrow T_1 \longrightarrow T \longrightarrow T_2 \longrightarrow 0 \ ,$$

et il existe une $\mathbb{Z}_p$-base de T, que l'on notera encore (f_1, f_2), telle que G sur T agit par $\begin{pmatrix} \eta_u^{-1}\xi_e^{-1}\chi & * \\ 0 & \eta_u\xi_e \end{pmatrix}$, avec $* = 0$ si et seulement si $\alpha = 0$.

- Si $\alpha = 0$, la suite exacte $(*_{ord})$ est scindée. On montre facilement qu'alors les autres réseaux de $V_p(E)$ stables par G sont les $p^{m_1}\mathbb{Z}_p f_1 \oplus p^{m_2}\mathbb{Z}_p f_2$, avec $m_1, m_2 \in \mathbb{Z}$, et qu'ils sont tous $\mathbb{Z}_p[G]$-isomorphes.

- Si $\alpha \neq 0$, alors $(*_{ord})$ n'est pas scindée. Il existe un plus grand entier $n \in \mathbb{N}$ tel que la suite exacte de $\mathbb{Z}/p^n\mathbb{Z}[G]$-modules $(*_{ord})$ mod $p^n\mathbb{Z}_p$ soit scindée ; posons $(f_1, p^{-n}f_2) = (e_1, e_2)$. Alors $T_0 = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ est un réseau G-stable de $V_p(E)$, tel que, pour tout entier $m \geq 1$, la suite exacte de $\mathbb{Z}_p[G]$-modules

$$(*_0) \qquad 0 \longrightarrow \mathbb{Z}_p e_1 \longrightarrow T_0 \longrightarrow \mathbb{Z}_p e_2 \longrightarrow 0$$

n'est pas scindée modulo $p^m\mathbb{Z}_p$; cela équivaut au fait que les réseaux $\mathbb{Z}_p e_1 \oplus p^{-r}\mathbb{Z}_p e_2$ ne sont G-stables pour aucun entier $r \geq 1$. Déterminons les autres réseaux G-stables de $V_p(E)$ par rapport à T_0 ; l'action de G sur la base (e_1, e_2) de T_0 se fait par $\rho = \begin{pmatrix} \eta_u^{-1}\xi_e^{-1}\chi & * \\ 0 & \eta_u\xi_e \end{pmatrix}$. Nous allons utiliser le petit lemme facile suivant :

Lemme :
1) Il existe $g_1 \in G$ *tel que* $\rho(g_1) = \begin{pmatrix} a_1 & c_1 \\ 0 & b_1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$, *avec* $c_1 \in \mathbb{Z}_p^\times$.

2) Il existe $g_2 \in I$ *tel que* $\rho(g_2) = \begin{pmatrix} a_2 & c_2 \\ 0 & b_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$, *avec* $a_2 \not\equiv b_2 \bmod p\mathbb{Z}_p$.

Preuve :
1) C'est évident, puisque $(*_0)$ n'est pas scindée modulo $p\mathbb{Z}_p$.
2) Supposons que pour tout $g \in I$ on ait $\xi_e^{-1}(g)\chi(g) \equiv \xi_e(g) \bmod p\mathbb{Z}_p$, c'est-à-dire $\chi(g) \equiv \xi_e^2(g) \bmod p\mathbb{Z}_p$; comme $\xi_e \equiv \chi^{\frac{p-1}{e}} \bmod p\mathbb{Z}_p$, on aurait alors $\chi(g)^{1-2\frac{p-1}{e}} \equiv 1 \bmod p\mathbb{Z}_p$ pour tout $g \in I$, ce qui est impossible ($p-1$ ne divise pas $1 - 2\frac{p-1}{e}$). □

Soit R un autre réseau de $V_p(E)$ stable par G ; quitte à effectuer une homothétie, on peut écrire $R = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2'$, avec $e_2' = ae_1 + be_2$, $a \in \mathbb{Q}_p$, $b \in \mathbb{Q}_p^\times$. Posons $v_p(b) = m \in \mathbb{Z}$.
Si $a \in \mathbb{Z}_p$, alors $R = \mathbb{Z}_p e_1 \oplus p^m\mathbb{Z}_p e_2$, où $m = v_p(b) \in \mathbb{Z}$. Soit $g_1 \in G$ comme dans le lemme précédent. On doit avoir $\rho(g_1)(p^m e_2) = p^m c_1 e_1 + p^m b_1 e_2 \in R$, c'est-à-dire $p^m c_1 \in \mathbb{Z}_p$; comme $c_1 \in \mathbb{Z}_p^\times$, cela équivaut à $m \in \mathbb{N}$.
Supposons $a \notin \mathbb{Z}_p$, et posons $v_p(a) = -m'$, $m' \geq 1$. Alors le réseau $R' = \mathbb{Z}_p e_1 \oplus p^{m'}\mathbb{Z}_p e_2' = \mathbb{Z}_p e_1 \oplus p^{m+m'}\mathbb{Z}_p e_2$ est stable par G, et, d'après ce que l'on vient de voir, on doit avoir $m + m' \geq 0$. Soit $g_2 \in I$ comme dans le lemme précédent. Le fait que R doit être stable par $\rho(g_2)$ s'écrit $\rho(g_2)e_2' = (a(a_2 - b_2) + bc_2)e_1 + b_2 e_2' \in R$, c'est-à-dire $a(a_2 - b_2) + bc_2 \in \mathbb{Z}_p$, avec $(a_2 - b_2) \in \mathbb{Z}_p^\times$, $c_2 \in \mathbb{Z}_p$, et $v_p(a) = -m' \leq m = v_p(b)$. Si $-m' < m$, on aurait $v_p(a(a_2 - b_2) + bc_2) = -m \leq -1$; donc $-m' = m$, et $e_2' = p^m(u_1 e_1 + u_2 e_2)$ avec $u_i \in \mathbb{Z}_p^\times$ et $m \leq -1$. Mais alors $R' = \mathbb{Z}_p e_1 \oplus p^{m'}\mathbb{Z}_p e_2' = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p(u_1 e_1 + u_2 e_2) = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2 = T_0$, et le fait que $R = \mathbb{Z}_p e_1 \oplus p^{-m'}\mathbb{Z}_p(u_1 e_1 + u_2 e_2)$ soit G-stable équivaut à $(*)_0)$ mod $p^{m'}\mathbb{Z}_p$ scindée, avec $m' \geq 1$, ce qui contredit notre hypothèse sur T_0. Donc nécessairement $a \in \mathbb{Z}_p$, et, à homothétie près, les réseaux G-stables de $V_p(E)$ sont les $\mathbb{Z}_p e_1 \oplus p^m\mathbb{Z}_p e_2$, $m \in \mathbb{N}$.

En remontant la construction, on arrive au résultat qui suit :

Soit $E/\mathbb{Q}_p$ une courbe elliptique ayant potentiellement bonne réduction ordinaire, dont le défaut de semi-stablité est $\mathrm{dst}(E) = e \in \{3,4,6\}$.
- si $\alpha = 0 \Leftrightarrow (*_{ord})$ scindée, les réseaux de $V_p(E)$ stables par G sont tous isomorphes.
- si $\alpha = 1 \Leftrightarrow (*_{ord})$ non scindée, il existe un plus grand entier naturel n_E tel que la suite exacte de $\mathbb{Z}/p^{n_E}\mathbb{Z}[G]$-modules $(*_{ord})$ mod $p^{n_E}\mathbb{Z}_p$ soit scindée. Alors il existe une $\mathbb{Q}_p$-base (e_1, e_2) de $V_p(E)$ telle que, à isomorphisme près, les réseaux stables par G sont les :

$$\mathbb{Z}_p e_1 \oplus p^m \mathbb{Z}_p e_2 \quad , \quad m \geq -n_E \ .$$

On en déduit *l'action de G sur $E[p]$: il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via*

$$\begin{pmatrix} \eta_{\overline{a}_p}^{-1} \chi_p^{1-\epsilon\frac{p-1}{e}} & * \\ 0 & \eta_{\overline{a}_p} \chi_p^{\epsilon\frac{p-1}{e}} \end{pmatrix} \quad \text{avec} \quad * = 0 \Leftrightarrow [\alpha = 0 \ \text{ ou } \ n_E \geq 1] \ .$$

Prenons une équation minimale pour $E/\mathbb{Q}_p$; alors, d'après A. Kraus ([Kr], 2.3.1., Prop.1), on a $\epsilon = 1$ si et seulement si $v_p(\Delta_E) < 6$, et $\epsilon = -1$ si et seulement si $v_p(\Delta_E) > 6$.

B.3.2. Les cas potentiellement supersinguliers :

Cette partie est la plus originale de toute l'annexe B, non pas par les résultats qu'elle contient, mais par la méthode employée. Elle est consacrée à l'étude de l'action de G sur les points d'ordre p ainsi que sur le p-module de Tate d'une courbe elliptique $E/\mathbb{Q}_p$ potentiellement supersingulière, et dont le défaut de semi-stabilité est $\mathrm{dst}(E) = e \in \{3,4,6\}$. Signalons que tous les résultats concernant l'action du groupe d'inertie absolu I sur les points d'ordre p sont dans [Kr].
On utilise les bivecteurs de Witt $BW(R)$ à coefficients dans R, construits par J.-M. Fontaine dans [Fo 5]. Dans la section **B.3.2.1.**, on en donne une construction ; on exhibe aussi certains réseaux de $BW(R)$ (lemme 1), pour lesquels on montre un petit résultat technique (lemme 2). Dans la section **B.3.2.2.**, on propose une description du $\mathbb{Q}_p[G]$-module $V_p(E)$. Enfin, dans la dernière section **B.3.2.3.**, on utilise les réseaux de $BW(R)$ étudiés au début pour effectuer les calculs nécessaires à la description des $\mathbb{F}_p[G]$-modules $E[p]$, de laquelle on déduit celle des $\mathbb{Z}_p[G]$-modules $T_p(E)$.
Au lieu de faire des calculs explicites dans $BW(R)$, on pourrait utiliser la théorie des modules de Dieudonné sur l'anneau des entiers de $L = \mathbb{Q}_p(\pi_e)$ comme dans le chapitre 3. L'inconvénient est que l'on doit alors se restreindre au cas où l'indice de ramification e est strictement inférieur à $p-1$; de plus, on n'obtient pas une description aussi explicite de l'action de G sur les points d'ordre p.

B.3.2.1. Les bivecteurs de Witt :

Si Λ est un anneau commutatif de caractéristique p, on note $W(\Lambda)$ l'anneau des vecteurs de Witt à coefficients dans Λ, et pour $\lambda \in \Lambda$, on note $[\lambda] \in W(\Lambda)$ son représentant de Teichmüller. Soit $C = \mathbb{C}_p$ le complété de $\overline{\mathbb{Q}}_p$, d'anneau des entiers O_C. On note $v = v_C$ la valuation sur

C étendant la valuation v_p sur $\mathbb{Q}_p$, normalisée par $v(p) = 1$; on a $v(C^\times) = v(\overline{\mathbb{Q}}_p^\times) = \mathbb{Q}$. On désigne par $\sigma : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ le Frobenius absolu : $\sigma(x) = x^p$.

Nous allons maintenant donner une description succinte des bivecteurs de Witt construits par J.-M. Fontaine ; on suivra surtout [Fo 5], 6.3., p.565, mais voir aussi [Fo 4] p.228.

Soit K un corps complet pour une valuation discrète, de corps résiduel $k \subset \overline{\mathbb{F}}_p$, d'anneau des entiers O_K, et $K_0 = \mathrm{Frac}W(k)$. Soit R l'anneau construit dans [Fo 1] et $\mathcal{M}_R$ son idéal maximal (cf. annexe A pour une description).
Soit $\mathcal{a}$ un idéal non nul de R strictement contenu dans $\mathcal{M}_R$. On note $BW_{\mathcal{a}}^u(R)$ le sous-ensemble de $K_0 \otimes_{W(k)} W(R) = W(R)[\frac{1}{p}]$ formé des

$$(\ldots, x_{-r}, \ldots, x_{-2}, x_{-1}; x_0, x_1, \ldots, x_m, \ldots) = \sum_{n \gg -\infty} p^n [x_n^{p^{-n}}] ,$$

avec $x_n \in R$ pour $n \geq 0$, $x_n \in \mathcal{a}$ pour $n < 0$, et $x_n = 0$ pour $n \gg -\infty$, i.e. les termes négatifs sont nuls en-deçà d'un certain rang. C'est un sous-$W(R)$-module de $K_0 \otimes_{W(k)} W(R)$, que l'on munit de la topologie produit, avec sur chaque composante ("fantôme") la topologie de R donnée par v_R. On note $BW_{\mathcal{a}}(R)$ le séparé complété de $BW_{\mathcal{a}}^u(R)$ pour cette topologie ; c'est un $W(k)$-module topologique. On a :

$$\begin{aligned} BW_{\mathcal{a}}(R) &= \{ \underline{x} = (\ldots, x_{-r}, \ldots, x_{-1}; x_0, \ldots, x_m, \ldots) \,/\, x_n \in R \text{ si } n \geq 0 \,,\, x_n \in \mathcal{a} \text{ si } n < 0 \} \\ &= \{ \sum_{n \in \mathbb{Z}} p^n [x_n^{p^{-n}}] \,/\, x_n \in R \text{ si } n \geq 0 \,,\, x_n \in \mathcal{a} \text{ si } n < 0 \} . \end{aligned}$$

Cette construction est fonctorielle en R et en $\mathcal{a}$. La structure de $W(k)$-module topologique sur $BW_{\mathcal{a}}(R)$ est donnée, pour $\lambda \in k$ et $\underline{a} = (a_n)_{n \in \mathbb{Z}} \in BW_{\mathcal{a}}(R)$, par :

$$[\lambda]\,\underline{a} = (\ldots, \sigma^{-r}(\lambda) a_{-r}, \ldots; \lambda a_0, \ldots, \sigma^m(\lambda) a_m, \ldots) = (\sigma^n(\lambda) a_n)_{n \in \mathbb{Z}} .$$

On voit que $\mathcal{a}$ est stable par $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}_p / K)$, et l'action de G_K sur R s'étend par fonctorialité en une action continue sur $BW_{\mathcal{a}}(R)$. On dispose de plus de deux opérateurs φ (le Frobenius) et V (le Verschiebung) sur $BW_{\mathcal{a}}(R)$ donnés par :

$$\begin{aligned} \varphi\,\underline{a} &= (\ldots, a_{-r}^p, \ldots; a_0^p, \ldots, a_m^p, \ldots) &&= (a_n^p)_{n \in \mathbb{Z}} \\ \mathsf{V}\,\underline{a} &= (\ldots, a_{-r-1}, \ldots; a_{-1}, \ldots, a_{m-1}, \ldots) &&= (a_{n-1})_{n \in \mathbb{Z}} \end{aligned}$$

et qui vérifient les relations $\varphi \mathsf{V} = \mathsf{V} \varphi = p$, et $\varphi[\lambda] = [\sigma(\lambda)]\varphi$ pour $\lambda \in k$.

Si $\mathcal{a}' \subset \mathcal{a}$ est un idéal non nul de R, alors l'inclusion $BW_{\mathcal{a}'}^u(R) \hookrightarrow BW_{\mathcal{a}}^u(R)$ induit un isomorphisme de $K_0 \otimes_{W(k)} BW_{\mathcal{a}'}(R)$ dans $K_0 \otimes_{W(k)} BW_{\mathcal{a}}(R)$. Alors on pose :

$$BW(R) = K_0 \otimes_{W(k)} BW_{\mathcal{a}}(R) ,$$

et $BW(R)$ ne dépend pas de $\mathcal{a}$; en tant qu'ensemble,

$$BW(R) = \{ \underline{x} = (x_n)_{n \in \mathbb{Z}} \,/\, \exists\, n_0 \in \mathbb{Z} \,, \exists\, \varepsilon > 0 \text{ t.q. } v_R(x_n) \geq \varepsilon \text{ pour } n \leq n_0 \} .$$

C'est un K_0-espace vectoriel topologique (on le munit de la topologie du produit tensoriel), sur lequel on étend les opérateurs φ, V, et l'action de G_K (φ est étendu σ-semi-linéairement et commute à l'action de G_K). Ainsi, $BW(R)$ est un (φ, G_K)-module au sens de [Fo 2].

On a une inclusion de (φ, G_K)-modules $BW(R) \subset B^+_{cris}$, et même, voir [Fo 5] et [Fo 1], 4.1.4., on a $BW(R) \subset \bigcap_{n\in\mathbb{N}} \varphi^n(B^+_{cris})$; d'où aussi des inclusions :

$$BW_K(R) = K\otimes_{K_0} BW(R) \;\subset\; K\otimes_{K_0} B^+_{cris} \;\subset\; K\otimes_{K_0} B_{cris} \;\subset\; B_{dR}\ ,$$

et l'on pose $\mathrm{Fil}^i BW_K(R) = BW_K(R) \cap \mathrm{Fil}^i B_{dR}$, pour tout $i \in \mathbb{Z}$. Alors $BW(R)$ devient un sous-(φ, G_K)-module filtré de B^+_{cris} au sens de [Fo 2]. Rappelons que l'on a un morphisme d'anneaux surjectif

$$\left\{\begin{array}{rcl} W(R) & \xrightarrow{\Theta} & O_C \\ \underline{x} = (x_n)_{n\in\mathbb{N}} & \mapsto & \displaystyle\sum_{n\in\mathbb{N}} p^n x_n^{(n)} \end{array}\right.$$

à partir duquel on construit les anneaux B^+_{dR} et B^+_{cris} (cf. annexe A) ; il se prolonge en un morphisme de K_0-espaces vectoriels $\Theta : BW(R) \subset B^+_{cris} \subset B^+_{dR} \to C$, et par définition $\mathrm{Fil}^1 B_{dR} = \mathrm{Ker}\,\Theta$.
Remarque : de même que B^+_{dR} et B^+_{cris}, le K_0-espace vectoriel $BW(R)$ ne dépend pas du corps K.

Soit Γ un groupe p-divisible (ou de Barsotti-Tate) sur O_K ; on note $\mathbf{M}_{O_K}(\Gamma)$ son module de Dieudonné sur O_K ([Fo 4]), et $\mathbf{D}_K(\Gamma) = K_0\otimes_{W(k)}\mathbf{M}_{O_K}(\Gamma)$. Alors on a des isomorphismes de $\mathbb{Q}_p[G_K]$-modules ([Fo 5], Thm.6.2. et Prop.6.4.) :

$$V_p(\Gamma) \simeq \mathrm{Hom}_{(\varphi,G_K)-mf}\Big(\mathbf{D}_K(\Gamma), BW(R)\Big) \simeq \mathrm{Hom}_{(\varphi,G_K)-mf}\Big(\mathbf{D}^*_{\mathbf{cris,K}}(V_p(\Gamma)), BW(R)\Big)\ .$$

De plus, si V est un objet de $\mathbf{Rep}_{\mathbb{Q}_p}(G)$, où $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, qui est potentiellement Barsotti-Tate et le devient sur une extension galoisienne K de $\mathbb{Q}_p$, alors l'isomorphisme

$$V \;\simeq\; \mathrm{Hom}_{(\varphi,G_K)-mf}\Big(\mathbf{D}^*_{\mathbf{cris,K/\mathbb{Q}_p}}(V), BW(R)\Big)$$

est G-équivariant ; l'action de G sur $\mathrm{Hom}_{(\varphi,G_K)-mf}(\mathbf{D}^*_{\mathbf{cris,K/\mathbb{Q}_p}}(V), BW(R))$ est donnée par : si u est un morphisme de $D = \mathbf{D}^*_{\mathbf{cris,K/\mathbb{Q}_p}}(V)$ dans $BW(R)$, et si $d \in D$, $g \in G$, on a $(g\cdot u)(d) = g\,u\Big((g^{-1} \bmod G_K)\,d\Big)$.

Nous allons appliquer tout cela au cas où $V = V_p(E)$, et E est une courbe elliptique sur $\mathbb{Q}_p$ potentiellement supersingulière dont le défaut de semi-stabilité est $\mathrm{dst}(E) = e \in \{3,4,6\}$; on prendra alors pour K la plus petite extension galoisienne de $\mathbb{Q}_p$ sur laquelle E acquiert bonne réduction. Notre but étant de décrire le $\mathbb{Z}_p[G]$-module $T_p(E)$ (ainsi que le $\mathbb{F}_p[G]$-module $E[p]$), nous allons étudier certains $W(k)$-réseaux de $BW(R)$.

Soit $c \in \mathbb{Q}$ tel que $c > 0$. On pose :

$$\mathcal{T}_c = \{\, \underline{x} = (x_n)_{n\in\mathbb{Z}} \in BW(R) \;/\; v_R(x_n) \geq cp^{-n}\ ,\ \forall\, n \in \mathbb{Z}\,\}$$

$$\mathcal{T}_c^+ = \{\, \underline{x} = (x_n)_{n\in\mathbb{Z}} \in BW(R) \;/\; v_R(x_n) > cp^{-n}\ ,\ \forall\, n \in \mathbb{Z}\,\}$$

On a évidemment $\mathcal{T}_{c'} \subset \mathcal{T}_c$ (resp. $\mathcal{T}^+_{c'} \subset \mathcal{T}^+_c$) pour $c \leq c'$.

Lemme 1 :
Soit $c > 0$; $\mathcal{T}_c$ est un sous-$W(k)$-module fermé de $BW(R)$ stable par φ et G_K.

Preuve :
Soit $c > 0$. Soit $\mathcal{a}$ l'idéal de R formé des a tels que $v_R(a) \geq cp$. Alors $BW_{\mathcal{a}}(R)$ est fermé dans $BW(R)$ et $\mathcal{T}_c \subset BW_{\mathcal{a}}(R)$. On a des flèches continues pour tout $n \in \mathbb{Z}$:

$$\begin{cases} BW_{\mathcal{a}}(R) & \xrightarrow{proj_n} & R & \xrightarrow{v_R} & \mathbb{Q} \cup \{+\infty\} \\ \underline{x} = (x_n)_{n\in\mathbb{Z}} & \mapsto & x_n & \mapsto & v_R(x_n) = v(x_n^{(0)}) \end{cases}$$

et $\mathcal{T}_c = \bigcap_{n\in\mathbb{Z}} (v_R \circ proj_n)^{-1}([cp^{-n}, +\infty])$ est clairement fermé dans $BW_{\mathcal{a}}(R)$.
Supposons que l'on ait montré que $\mathcal{T}_c$ est un sous-groupe additif de $BW(R)$; alors la structure de $W(k)$-module est évidente : il suffit de voir que pour $\varepsilon \in k^\times$ et $\underline{x} = (x_n)_{n\in\mathbb{Z}} \in \mathcal{T}_c$, on a

$$[\varepsilon]\,\underline{x} = (\ldots, \varepsilon^{p^{-r}} x_{-r}, \ldots; \varepsilon x_0, \ldots, \varepsilon^{p^m} x_m, \ldots) \in \mathcal{T}_c \,.$$

Or, pour tout $n \in \mathbb{Z}$, on a $v_R(\varepsilon^{p^n} x_n) = p^n v_R(\varepsilon) + v_R(x_n) = v_R(x_n)$, puisque $v([\varepsilon]) = 0$.
Les deux dernières assertions (stabilité par φ et par G_K) sont évidentes.

Soient $\underline{a} = (a_n)_{n\in\mathbb{Z}}$ et $\underline{b} = (b_n)_{n\in\mathbb{Z}}$ dans $\mathcal{T}_c$. On veut montrer que, si $\underline{a} + \underline{b} = \underline{s} = (s_n)_{n\in\mathbb{Z}}$, alors $v_R(s_n) \geq cp^{-n}$ pour tout $n \in \mathbb{Z}$. Par la construction de $BW(R)$, il suffit de le prouver pour $\underline{a}$ et $\underline{b}$ tels qu'il existe un $m \geq 0$ tel que $a_n = b_n = 0$ pour $n < -m$. Ecrivons

$$\underline{s} = (\ldots, 0, 0, c_0^{p^{-m}}, c_1^{p^{-m}}, \ldots, c_{m-1}^{p^{-m}}; c_m^{p^{-m}}, \ldots) \,,$$

avec

$$s_{n-m}^{p^m} = c_n = S_n(a_{-m}^{p^m}, \ldots, a_{-m+n}^{p^m}; b_{-m}^{p^m}, \ldots, b_{-m+n}^{p^m}) \,,$$

où les $S_n \in \mathbb{Z}[X_0, X_1, \ldots, X_n; Y_0, Y_1, \ldots, Y_n]$ sont les polynômes donnant l'addition dans $W(R)$. On veut montrer que $v_R(c_n) \geq cp^{2m-n}$ pour tout $n \geq 0$. Les relations entre les polynômes S_n donnent

$$c_n = a_{-m+n}^{p^m} + b_{-m+n}^{p^m} + Q_n(a_{-m}^{p^m}, \ldots, a_{-m+n-1}^{p^m}; b_{-m}^{p^m}, \ldots, b_{-m+n-1}^{p^m}) \,,$$

où $Q_n \in \mathbb{Z}[X_0, X_1, \ldots, X_{n-1}; Y_0, Y_1, \ldots, Y_{n-1}]$. Alors $v_R(a_{-m+n}^{p^m} + b_{-m+n}^{p^m}) \geq cp^{2m-n}$, et $v_R(Q_n(a_{-m}^{p^m}, \ldots, a_{-m+n-1}^{p^m}; b_{-m}^{p^m}, \ldots, b_{-m+n-1}^{p^m})) \geq cp^{2m-n+1}$, d'où le résultat. □

Remarques :
1) Il est clair que $\mathcal{T}_c^+$ est aussi un sous-$W(k)$-module de $BW(R)$ stable par φ et G_K.
2) En utilisant la relation $\varphi V = V\varphi = p$, on voit facilement que $p\mathcal{T}_c = \mathcal{T}_{p^2 c}$.

Nous allons avoir besoin d'une précision supplémentaire. Pour $\nu > 0$, on note $\mathcal{m}_{R,\nu} = \{ a \in R \,/\, v_R(a) \geq \nu \}$; c'est un idéal fermé de R strictement contenu dans $\mathcal{m}_R$.

Lemme 2 :
Soit $c > 0$; soient $\underline{a}, \underline{b} \in \mathcal{T}_c$, avec $\underline{a} = (a_n)_{n\in\mathbb{Z}}$, $\underline{b} = (b_n)_{n\in\mathbb{Z}}$, et soit $\underline{d} = (d_n)_{n\in\mathbb{Z}}$ tel que $\underline{a} + \underline{b} = \underline{d}$. Alors $d_0 \equiv a_0 + b_0 \bmod \mathcal{m}_{R,p^2c}$.

Preuve :
On désigne toujours par S_m, $m \in \mathbb{N}$, les polynômes donnant l'addition dans $W(R)$. On a

$$d_0 = \lim_{m \to +\infty} S_m(a_{-m}, \ldots, a_0; b_{-m}, \ldots, b_0) \ ,$$

et il suffit de montrer que $S_m(a_{-m}, \ldots, a_0; b_{-m}, \ldots, b_0) \equiv a_0 + b_0 \bmod \mathcal{M}_{R,p^2c}$, pour tout $m \geq 1$. Rappelons que les S_m sont dans $\mathbb{Z}[X_0, X_1, \ldots, X_m; Y_0, Y_1, \ldots, Y_m] \subset S_{\mathbb{Z}}$, où $S_{\mathbb{Z}}$ désigne l'anneau $\mathbb{Z}[X_0, X_1, \ldots; Y_0, Y_1, \ldots]$, et sont définis par récurrence par la relation :

$$\Phi_m(S_0, \ldots, S_m) = \Phi_m(X_0, \ldots, X_m) \ + \ \Phi_m(Y_0, \ldots, Y_m) \ ,$$

$$\text{où} \quad \Phi_m(X_0, \ldots, X_m) = X_0^{p^m} + pX_1^{p^{m-1}} + \ \ldots \ + p^m X_m \ .$$

Soit $m \in \mathbb{N}$; comme $\Phi_{m+1}(X_0, \ldots, X_{m+1}) = p^{m+1} X_{m+1} + \Phi_m(X_0^p, \ldots, X_m^p)$, on a :

$$\begin{aligned}
&S_{m+1}(X_0, \ldots, X_{m+1}; Y_0, \ldots, Y_{m+1}) \\
&= X_{m+1} + Y_{m+1} + \frac{1}{p^{m+1}} \Big(\Phi_m(X_0^p, \ldots, X_m^p) + \Phi_m(Y_0^p, \ldots, Y_m^p) - \Phi_m(S_0^p, \ldots, S_m^p) \Big) \\
&= X_{m+1} + Y_{m+1} + \frac{1}{p^{m+1}} \Big(\Phi_m(S_0(X_0^p; Y_0^p), \ \ldots \ , S_m(X_0^p, \ldots, X_m^p; Y_0^p, \ldots, Y_m^p)) - \Phi_m(S_0^p, \ldots, S_m^p) \Big) \\
&= X_{m+1} + Y_{m+1} + \sum_{0 \leq r \leq m} Q_r(X_0, \ldots, X_r; Y_0, \ldots, Y_r) \ ,
\end{aligned}$$

où les polynômes $Q_r(X_0, \ldots, X_r; Y_0, \ldots, Y_r)$ sont les

$$\frac{1}{p^{m+1-r}} \Big(S_r(X_0^p, \ldots, X_r^p; Y_0^p, \ldots, Y_r^p)^{p^{m-r}} - (S_r(X_0, \ldots, X_r; Y_0, \ldots, Y_r)^p)^{p^{m-r}} \Big)$$

et sont dans $\mathbb{Z}[X_0, X_1, \ldots, X_r; Y_0, Y_1, \ldots, Y_r]$. On a alors :

$$S_{m+1}(a_{-m-1}, \ldots, a_0; b_{-m-1}, \ldots, b_0) = a_0 + b_0 + \sum_{0 \leq r \leq m} Q_r(a_{-m-1}, \ldots, a_{-m-1+r}; b_{-m-1}, \ldots, b_{-m-1+r}).$$

Pour $0 \leq r \leq m-1$, on a $v_R(a_{-m-1+r}) \geq p^{m+1-r} c \geq p^2 c$ et $v_R(b_{-m-1+r}) \geq p^2 c$; on en déduit que $Q_r(a_{-m-1}, \ldots, a_{-m-1+r}; b_{-m-1}, \ldots, b_{-m-1+r}) \in \mathcal{M}_{R,p^2c}$, les autres termes étant de valuation supérieure. Pour $r = m$, on a :

$$Q_m(X_0, \ldots, X_m; Y_0, \ldots, Y_m) = \frac{1}{p} \Big(S_m(X_0^p, \ldots, X_m^p; Y_0^p, \ldots, Y_m^p) - S_m(X_0, \ldots, X_m; Y_0, \ldots, Y_m)^p \Big).$$

Comme $S_m(X_0, \ldots, X_m; Y_0, \ldots, Y_m) \equiv X_m + Y_m \bmod \mathcal{I}_m$, où l'on a noté $\mathcal{I}_m$ l'idéal de $S_{\mathbb{Z}}$ engendré par les $X_0, \ldots, X_{m-1}$ et les $Y_0, \ldots, Y_{m-1}$, on obtient :

$$\begin{aligned}
Q_m(X_0, \ldots, X_m; Y_0, \ldots, Y_m) \ &\equiv \ \frac{1}{p} \Big(X_m^p + Y_m^p - (X_m + Y_m)^p \Big) \bmod \mathcal{I}_m \\
&= \ - \sum_{1 \leq i \leq p-1} \frac{1}{p} \frac{p!}{(p-i)!\, i!} X_m^i \, Y_m^{p-i} \bmod \mathcal{I}_m \ ,
\end{aligned}$$

où les coefficients dans la somme sont entiers. On en déduit, toujours parce que $v_R(a_n) \geq p^2 c$ pour $-m-1 \leq n \leq -2$, que

$$Q_m(a_{-m-1}, \ldots, a_{-1}; b_{-m-1}, \ldots, b_{-1}) \equiv \sum_{1 \leq i \leq p-1} \frac{1}{p} \frac{p!}{(p-i)!\, i!} a_{-1}^i \, b_{-1}^{p-i} \bmod \mathcal{M}_{R,p^2c} \ .$$

Or, on a $v_R(a_{-1}^i b_{-1}^{p-i}) \geq ipc + (p-i)pc = p^2c$, et donc $Q_m(a_{-m-1},\dots,a_{-1};b_{-m-1},\dots,b_{-1})$ est dans $\mathcal{M}_{R,p^2c}$. □

B.3.2.2. Une description du $\mathbb{Q}_p[G]$-module $V_p(E)$:

Soit E une courbe elliptique sur $\mathbb{Q}_p$ potentiellement supersingulière, dont le défaut de semi-stabilité est $\mathrm{dst}(E) = e \in \{3,4,6\}$; alors $e \mid p+1$. On sait que $\mathbf{D}^*_{\mathbf{cris},K/\mathbb{Q}_p}(V_p(E))$ est isomorphe dans $\mathbf{MF}_{K/\mathbb{Q}_p}(\varphi)$ à l'un des objets $D_\alpha = \mathbf{D}^*_{\mathbf{pc}}(\mathbf{e};\mathbf{0};\alpha)$, avec $\alpha \in \mathbb{P}^1(\mathbb{Q}_p)$, de la liste $\mathbf{D}^*$, décrit par : $D_\alpha = \mathbb{Q}_{p^2}e_1 \oplus \mathbb{Q}_{p^2}e_2$, avec $\varphi e_1 = e_2$, $\varphi e_2 = -pe_1$, $\omega e_1 = e_1$, $\omega e_2 = e_2$, $\tau_e e_1 = \zeta_e e_1$, $\tau_e e_2 = \zeta_e^{-1} e_2$, et $\mathrm{Fil}^1(D_\alpha)_K = (\alpha \cdot e_1 \otimes \pi_e^{-1} + e_2 \otimes \pi_e)K$. Alors on a

$$V_p(E) \simeq_{\mathbb{Q}_p[G]} \mathrm{Hom}_{(\varphi,G_K)-mf}\Big(D_\alpha, BW(R)\Big) = V_\alpha .$$

L'objet V_α est un $\mathbb{Q}_p$-espace vectoriel de dimension 2, formé des applications $\mathbb{Q}_{p^2}$-linéaires $u : D_\alpha \to BW(R)$, commutant aux Frobenius, et vérifiant $u_K(\mathrm{Fil}^1(D_\alpha)_K) \subset \mathrm{Fil}^1 BW(R)_K = BW(R)_K \cap \mathrm{Fil}^1 B_{dR} = BW(R)_K \cap \mathrm{Ker}\,\Theta$, où $u_K = u \otimes_{K_0} \mathbf{1}_K$.

Soit u une telle application. Si $u(e_1) = \underline{a} \in BW(R)$, alors on a nécessairement $u(e_2) = u(\varphi e_1) = \varphi\underline{a} \in BW(R)$; on notera $u_{\underline{a}}$ l'unique application $\mathbb{Q}_{p^2}[\varphi]$-linéaire de D_α dans $BW(R)$ telle que $u_{\underline{a}}(e_1) = \underline{a}$. Comme $\varphi^2 + p = 0$ dans D_α , on doit avoir $\varphi^2\underline{a} = -p\underline{a}$ dans $BW(R)$, ce qui équivaut à $\varphi\underline{a} = -\mathrm{V}\underline{a}$ (où V est le Verschiebung). Si l'on écrit $\underline{a} = (a_n)_{n\in\mathbb{Z}}$, cela donne $a_n^p = -a_{n-1}$, pour tout $n \in \mathbb{Z}$. Donc les $\underline{a} \in BW(R)$ tels que $\varphi^2\underline{a} = -p\underline{a}$ sont exactement les

$$\underline{a} = (\dots,(-1)^r a^{p^r},\dots,a^{p^2},-a^p;a,-a^{p^{-1}},a^{p^{-2}},\dots,(-1)^m a^{p^{-m}},\dots) = \big((-1)^n a^{p^{-n}}\big)_{n\in\mathbb{Z}} ,$$

avec $a \in \mathcal{M}_R$. Si $v_R(a) = c > 0$, alors $\underline{a} \in \mathcal{T}_c$ et $\underline{a} \notin \mathcal{T}_c^+$.

Puis la condition sur la filtration équivaut à $\Theta(\alpha \cdot u_{\underline{a}}(e_1) \otimes \pi_e^{-1} + u_{\underline{a}}(e_2) \otimes \pi_e) = 0$, c'est-à-dire $\alpha\pi_e^{-1}\Theta(\underline{a}) + \pi_e\Theta(\varphi\underline{a}) = 0$. Si l'on note (abusivement !) $a^{(0)^{p^{-n}}} = a^{(n)} \in O_C$ pour $n \in \mathbb{N}$, alors on a :

$$\Theta(\underline{a}) = \sum_{n\in\mathbb{Z}} (-1)^n p^n a^{(0)^{p^{-2n}}} \quad , \quad \Theta(\varphi\underline{a}) = \sum_{n\in\mathbb{Z}} (-1)^n p^n a^{(0)^{p^{-2n+1}}} ,$$

et la condition sur la filtration devient :

$$(*_\alpha) \qquad \sum_{n\in\mathbb{Z}} (-1)^n p^n \Big(\alpha\,\pi_e^{-1} a^{(0)^{p^{-2n}}} + \pi_e a^{(0)^{p^{-2n+1}}}\Big) = 0 .$$

Soit $\mathcal{V}_\alpha = \{\, \underline{a} = \big((-1)^n a^{p^{-n}}\big)_{n\in\mathbb{Z}} \in BW(R) \;/\; a \in \mathcal{M}_R \text{ et } a = (a^{(n)})_{n\in\mathbb{N}} \text{ vérifie } (*_\alpha) \,\}$; alors V_α est le $\mathbb{Q}_p$-espace vectoriel de dimension deux formé des applications $\mathbb{Q}_{p^2}$-linéaires $u_{\underline{a}} : D_\alpha \to BW(R)$ telles que $\underline{a} \in \mathcal{V}_\alpha$.
Soit $\underline{a} \in \mathcal{V}_\alpha$ non nul ; posons $v_R(\underline{a}) = v(a^{(0)}) = c > 0$, et regardons quelles sont les valuations c possibles. Comme $p^m\underline{a} = \varphi^m \mathrm{V}^m\underline{a} = \big((-1)^{n-m} a^{p^{2m-n}}\big)_{n\in\mathbb{Z}}$ pour tout $m \in \mathbb{Z}$, on obtient $v_R\big((-1)^{-m}a^{p^{2m}}\big) = p^{2m}v_R(a) = p^{2m}c$; donc, quitte à multiplier $\underline{a}$ par une puissance de p convenable, on peut supposer que

$$\frac{1}{p^2-1} < v_R(\underline{a}) = c \leq \frac{p^2}{p^2-1} .$$

En termes de valuation, l'équation $(*_\alpha)$ devient $v(\alpha) - \frac{1}{e} + v(\Theta(\underline{a})) = \frac{1}{e} + v(\Theta(\varphi\underline{a}))$, où $v(\alpha) = v_p(\alpha) \in \mathbb{Z}$ pour $\alpha \in \mathbb{Q}_p^\times$, et l'on pose $v(0) = +\infty$, $v(\infty) = -\infty$. On a les inégalités : $\frac{1}{p^2-1} < \frac{p}{p^2-1} < \frac{p^2}{p^2-1}$. Une étude (un peu pénible...) des valuations dans l'équation $(*_\alpha)$ montre que, pour $p \geq 5$ et $e \geq 3$ divisant $p+1$, on a :

- Si $\dfrac{1}{p^2-1} < c < \dfrac{p}{p^2-1}$, alors $v(\Theta(\underline{a})) = c$ et $v(\Theta(\varphi\underline{a})) = pc$; on en déduit $0 < \frac{1+2\frac{p+1}{e}}{p+1} < v(\alpha) < \frac{p+2\frac{p+1}{e}}{p+1} < 2$, et donc $v(\alpha) = 1$. Alors $c = \dfrac{(e-2)\frac{p+1}{e}}{p^2-1}$.

- Si $\dfrac{p}{p^2-1} < c < \dfrac{p^2}{p^2-1}$, alors $v(\Theta(\underline{a})) = c$ et $v(\Theta(\varphi\underline{a})) = 1 + \frac{c}{p}$; on en déduit $0 < \frac{1+2\frac{p+1}{e}}{p+1} < v(\alpha) < \frac{p+2\frac{p+1}{e}}{p+1} < 2$, et donc $v(\alpha) = 1$. Cette fois, $c = \dfrac{2p\frac{p+1}{e}}{p^2-1}$.

- Si $c = \dfrac{1}{p^2-1}$, alors $v(\Theta(\underline{a})) \geq c$ et $v(\Theta(\varphi\underline{a})) = pc$; on en déduit $v(\alpha) \leq 0$.

- Si $c = \dfrac{p}{p^2-1}$, alors $v(\Theta(\underline{a})) = c$ et $v(\Theta(\varphi\underline{a})) \geq 1 + \frac{c}{p}$; on en déduit $v(\alpha) \geq 2$.

Posons $A_\alpha = \{\, a \in \mathcal{M}_R \,/\, a$ vérifie $(*_\alpha)\,\}$. On définit une flèche de V_α dans A_α, qui est la composée des

$$\left\{ \begin{array}{ccccc} V_\alpha & \longrightarrow & \mathcal{V}_\alpha & \longrightarrow & A_\alpha \\ u_{\underline{a}} & \mapsto & \underline{a} & \mapsto & a \end{array} \right.$$

et qui est clairement bijective. Il existe une unique structure de $\mathbb{Q}_p[G]$-espace vectoriel sur A_α qui fait de la flèche ci-dessus un isomorphisme $\mathbb{Q}_p[G]$-linéaire. Cette structure est donc définie de la manière suivante :
- loi de groupe abélien sur A_α : si $a, b \in A_\alpha$, alors

$$a\,(+)\,b = \lim_{m \to +\infty} S_m(\,(-1)^m a^{p^m}, \ldots, a; (-1)^m b^{p^m}, \ldots, b)$$

où les S_m sont les polynômes donnant l'addition dans $W(R)$;
- si $\varepsilon \in \mathbb{F}_p$ et $a \in A_\alpha$, alors $\varepsilon \cdot a = ([\varepsilon] a^{(n)})_{n \in \mathbb{N}}$; cela suffit pour décrire la structure de $\mathbb{Q}_p$-espace vectoriel sur A_α ;
- action de G sur A_α : d'après la description de l'action de G sur V_α , on voit que pour $g \in G$ et $a \in A_\alpha$, on a :

$$\left. \begin{array}{rcll} g * a & = & \zeta_e^r \cdot ga\,, & \text{si } g \bmod G_K = \omega \tau_e^r \\ & = & \zeta_e^{-r} \cdot ga\,, & \text{si } g \bmod G_K = \tau_e^r \end{array} \right\}\ ,\ 0 \leq r \leq e-1\ ,$$

où ga désigne l'action naturelle de G sur R.

Remarque : Comme $e \geq 3$ divise $p+1$, on a $\zeta_e = [\overline{\zeta}_e]$, avec $\overline{\zeta}_e \in \mathbb{F}_{p^2}$ mais $\overline{\zeta}_e \notin \mathbb{F}_p$. Alors, pour $a \in R$, on a : $\zeta_e \cdot a = \zeta_e \cdot (a^{(n)})_{n \in \mathbb{N}} = (\zeta_e a^{(0)}, \zeta_e^{p-1} a^{(1)}, \zeta_e a^{(2)}, \zeta_e^{p-1} a^{(3)}, \ldots)$.

B.3.2.3. Etude des points d'ordre p et des $\mathbb{Z}_p[G]$-modules $T_p(E)$:

On reprend toutes les notations précédentes. Soit $c > 0$; on pose :

$$T_c = \{ u_{\underline{a}} \in V_\alpha \,/\, v_R(a) \geq c \} \quad \text{et} \quad T_c^+ = \{ u_{\underline{a}} \in V_\alpha \,/\, v_R(a) > c \} .$$

On sait que ce sont des réseaux G-stables de $V_\alpha \simeq V_p(E)$, isomorphes à $\mathcal{T}_c \cap \mathcal{V}_\alpha$ et $\mathcal{T}_c^+ \cap \mathcal{V}_\alpha$ respectivement (lemme 1). Posons aussi :

$$A_c = \{ a \in A_\alpha \,/\, v_R(a) \geq c \} \quad \text{et} \quad A_c^+ = \{ a \in A_\alpha \,/\, v_R(a) > c \} .$$

Il est clair que le $\mathbb{Q}_p[G]$-isomorphisme $V_\alpha \simeq A_\alpha$ induit par restriction à T_c et à T_c^+ des $\mathbb{Z}_p[G]$-isomorphismes $T_c \simeq A_c$ et $T_c^+ \simeq A_c^+$. En particulier, on a :

$$T_c/pT_c = T_c/T_{p^2c} \xrightarrow{\sim}_{\mathbb{F}_p[G]-mod} A_c/A_{p^2c} = A_c/pA_c .$$

Pour étudier les $\mathbb{F}_p[G]$-modules T_c/pT_c , nous aurons besoin du lemme qui suit. On note $\mathcal{M}_C = \{ x \in C \,/\, v(x) > 0 \}$ l'idéal maximal de O_C ; aussi, pour tout $\nu > 0$, on note $\mathcal{M}_{C,\nu} = \{ x \in C \,/\, v(x) \geq \nu \}$ et $\mathcal{M}_{C,\nu}^+ = \{ x \in C \,/\, v(x) > \nu \}$.

Lemme 3 :
Soit $c \in]0, \frac{1}{p^2-1}]$ *; soient* $a, b \in A_c$. *Alors :*
1) pour tout $\nu \in [c, p^2c]$, $a \equiv b \bmod A_\nu$ *si et seulement si* $a^{(0)} \equiv b^{(0)} \bmod \mathcal{M}_{C,\nu}$.
2) pour tout $\nu \in [c, p^2c[$, $a \equiv b \bmod A_\nu^+$ *si et seulement si* $a^{(0)} \equiv b^{(0)} \bmod \mathcal{M}_{C,\nu}^+$.

Preuve :
Le lemme 2 montre que $a\,(+)\,b \equiv a+b \bmod \mathcal{M}_{R,p^2c}$, pour $a, b \in A_c$. On en déduit que pour tout $\nu \in [c, p^2c]$, on a $v_R(a\,(-)\,b) \geq \nu$ si et seulement si $v_R(a-b) \geq \nu$. Puis $v_R(a-b) = v((a-b)^{(0)})$, avec, si l'on écrit $a = (a^{(n)})_{n\in\mathbb{N}}$ et $b = (b^{(n)})_{n\in\mathbb{N}}$,

$$(a-b)^{(0)} = \lim_{n\to\infty} \left(a^{(n)} - b^{(n)}\right)^{p^n} .$$

Pour tout $n \in \mathbb{N}$, et p impair, on a

$$\begin{aligned} \left(a^{(n)} - b^{(n)}\right)^{p^n} &= a^{(0)} - b^{(0)} + \sum_{1\leq i\leq p^n-1} \frac{(p^n)!}{(p^n-i)!\,i!} a^{(n)^i} (-b^{(n)})^{p^n-i} \\ &\equiv a^{(0)} - b^{(0)} \bmod \mathcal{M}_{C,c+1} , \end{aligned}$$

puisque les coefficients dans la somme sont de valuation supérieure ou égale à 1, et que, par hypothèse, on a $v(a^{(n)^i}(-b^{(n)})^{p^n-i}) \geq ip^{-n}c + (p^n-i)p^{-n}c = c$. Par passage à la limite, on obtient

$$(a-b)^{(0)} \equiv a^{(0)} - b^{(0)} \bmod \mathcal{M}_{C,c+1} ,$$

et l'hypothèse $c \leq \frac{1}{p^2-1} \Leftrightarrow p^2c \leq c+1$ permet d'affirmer que pour tout $\nu \in [c, p^2c]$, on a $v_R(a-b) \geq \nu$ si et seulement si $v(a^{(0)} - b^{(0)}) \geq \nu$, ce qui prouve le *1)*. La démonstration du *2)* est tout-à-fait similaire. □

Soit $a \in A_\alpha = \{ a \in \mathcal{M}_R \,/\, a$ vérifie $(*_\alpha) \}$ non nul ; rappelons que :

$$v(\alpha) \leq 0 \Rightarrow v_R(a) \in \{p^{2n}\frac{1}{p^2-1}\ ,\ n \in \mathbb{Z}\} \quad ; \quad v(\alpha) \geq 2 \Rightarrow v_R(a) \in \{p^{2n}\frac{1}{p(p^2-1)}\ ,\ n \in \mathbb{Z}\}$$

$$v(\alpha) = 1 \Rightarrow v_R(a) \in \{\, p^{2n}\frac{1-2/e}{p^2(p-1)}\ ,\ n \in \mathbb{Z}\,\} \cup \{\, p^{2n}\frac{2/e}{p(p-1)}\ ,\ n \in \mathbb{Z}\,\}.$$

Dans chacun des cas nous allons choisir un c convenable tel que $\frac{1}{p^2(p^2-1)} < c \leq \frac{1}{p^2-1}$ et étudier le $\mathbb{F}_p[G]$-module T_c/pT_c .

Cas $v(\alpha) \leq 0$:

On prend $c = \frac{1}{p^2-1}$, et dans ce cas on a $pT_c = T_{p^2c} = T_c^+$, puisqu'il n'y a pas d'autre valuation possible dans $[p^2c, c[$. Nous allons étudier $A_c/A_c^+ \simeq T_c/T_c^+$: c'est un $\mathbb{F}_p[G]$-espace vectoriel de dimension 2. Soit $a \in A_c$ tel que $v_R(a) = c$. L'étude des valuations dans l'équation

$$(*_\alpha) \qquad \sum_{n\in\mathbb{Z}} (-1)^n p^n \Big(a^{(0)p^{-2n}} + \alpha^{-1}\pi_e^2 a^{(0)p^{-2n+1}} \Big) = 0$$

montre que $v(p^{-1}a^{(0)p^2}) = v(a^{(0)}) = c = \frac{1}{p^2-1}$, que $v(\alpha^{-1}\pi_e^2 a^{(0)p}) = -v(\alpha) + \frac{2}{e} + \frac{p}{p^2-1} \geq \frac{2}{e} + \frac{p}{p^2-1} > c$, et que les autres termes sont de valuation $\geq 1 > c$. Donc $a^{(0)}$ vérifie :

$$\frac{a^{(0)p^2}}{p} - a^{(0)} \in \mathcal{M}_{C,c}^+ = \{\, x \in C \,/\, v(x) > c \,\}\ .$$

Posons alors $\mathcal{R} = \{\, z \in \overline{\mathbb{Q}}_p \,/\, z^{p^2} - pz = 0 \,\}$: un élément non nul de $\mathcal{R}$ vérifie $z^{p^2-1} = p$, et $v(z) = \frac{1}{p^2-1} = c = v(a^{(0)})$. De plus, le cardinal de $\mathcal{R}$ est p^2, et l'on voit facilement si $z, z' \in \mathcal{R}$ avec $z \neq z'$, alors $v(z-z') = \frac{1}{p^2-1} = c$. Soit z un élément non nul de $\mathcal{R}$; comme $v(z) = v(a^{(0)})$, il existe un unique $u \in O_C^\times$ tel que $a^{(0)} = uz$, d'où :

$$\frac{uz^{p^2}}{p} - uz = z(u^{p^2} - u) \in \mathcal{M}_{C,c}^+ \Leftrightarrow u^{p^2} - u \in \mathcal{M}_C\ .$$

Donc $u \equiv [\varepsilon] \bmod \mathcal{M}_C$, avec $\varepsilon \in \mathbb{F}_{p^2}^\times$, et l'on obtient $a^{(0)} \equiv [\varepsilon]z \bmod \mathcal{M}_{C,c}^+$, avec $[\varepsilon]z \in \mathcal{R}$. On en déduit que pour $a \in A_c$ tel que $v_R(a) = c = \frac{1}{p^2-1}$, il existe un unique élément $z(a) \in \mathcal{R}$ tel que $a^{(0)} \equiv z(a) \bmod \mathcal{M}_{C,c}^+$. Puis le lemme 3 montre que, pour $a, b \in A_c$, on a :

$$a \equiv b \bmod A_c^+ \Leftrightarrow a^{(0)} \equiv b^{(0)} \bmod \mathcal{M}_{C,c}^+\ .$$

L'implication ($\Rightarrow$) permet de définir une flèche $f : A_c/A_c^+ \longrightarrow \mathcal{R}$, par $f(a \bmod A_c^+) =$ l'unique élément $z(a) \in \mathcal{R}$ tel que $a^{(0)} \equiv z(a) \bmod \mathcal{M}_{C,c}^+$, et l'implication ($\Leftarrow$) montre qu'elle est injective. De plus, comme $\mathrm{Card}(\mathcal{R}) = \mathrm{Card}(A_c/A_c^+) = p^2$, l'application f est bijective.

On munit alors $\mathcal{R}$ de l'unique structure de $\mathbb{F}_p[G]$-espace vectoriel (de dimension 2) qui fait de f un isomorphisme $\mathbb{F}_p[G]$-linéaire. Soient $z \in \mathcal{R}$ et $g \in G$; par définition, on a :

$$\left.\begin{array}{rcll} g*z & = & \zeta_e^r \cdot gz\,, & \text{si } g \bmod G_K = \omega\tau_e^r \\ & = & \zeta_e^{-r} \cdot gz\,, & \text{si } g \bmod G_K = \tau_e^r \end{array}\right\}\ ,\ 0 \leq r \leq e-1\ .$$

Soit $\pi \in \overline{\mathbb{Q}}_p$ tel que $\pi^{\frac{p^2-1}{e}} = \pi_e$ (on a donc $\pi^{p^2-1} = -p$), et posons $F = \mathbb{Q}_{p^4}(\pi)$: c'est une extension galoisienne de $\mathbb{Q}_p$, contenant $K = \mathbb{Q}_{p^2}(\pi_e)$. On écrit $G_F = \mathrm{Gal}(\overline{\mathbb{Q}}_p/F)$, et $\mathrm{Gal}(F/\mathbb{Q}_p) = <\theta> \rtimes <\theta_0>$, où la restriction de θ à K est τ_e , et celle de θ_0 est ω (θ_0 est donc un relèvement du Frobenius) ; on a $\theta_0\theta\theta_0^{-1} = \theta^p$. Le sous-groupe d'inertie $I(F/\mathbb{Q}_p) = <\theta>$ est canoniquement isomorphe à $\mathbb{F}_{p^2}^\times$, via le quotient du caractère fondamental de niveau 2 :

$$\psi_2\ :\ \left\{\begin{array}{ccc} I(F/\mathbb{Q}_p) & \xrightarrow{\sim} & \mathbb{F}_{p^2}^\times \\ g & \longmapsto & \frac{g\pi}{\pi}\ . \end{array}\right.$$

Soient $\zeta, \gamma \in \overline{\mathbb{F}}_p^\times$ tels que $\zeta^{p+1} = -1$ et $\gamma^{p-1} = \zeta$; on a $\gamma^{p^2-1} = \zeta^{p+1} = -1$, et $(\gamma^2)^{p^2-1} = 1$. Donc $\gamma^2 \in \mathbb{F}_{p^2}^\times$ et $\gamma \notin \mathbb{F}_{p^2}^\times$, d'où $\gamma \in \mathbb{F}_{p^4}^\times$.

Tout élément non nul z de $\mathcal{R}$ s'écrit $z = [\varepsilon]([\gamma]\pi)$, avec $\varepsilon \in \mathbb{F}_{p^2}^\times$. On voit que G agit sur z (vu comme élément de $\overline{\mathbb{Q}}_p$) via son quotient $G/G_F = \mathrm{Gal}(F/\mathbb{Q}_p)$ de la manière suivante : le sous-groupe d'inertie $I(F/\mathbb{Q}_p)$ agit par le caractère ψ_2 , et $\theta_0 z = \theta_0([\varepsilon]([\gamma]\pi)) = [\varepsilon^p][\gamma^p]\pi = [\zeta][\varepsilon^p]([\gamma]\pi)$. Puis l'action de G sur $\mathcal{R}$ est donnée par :

$$\theta * z = \zeta_e^{-1}\theta z = \psi_2^{-\frac{p^2-1}{e}}(\theta)\psi_2(\theta)z = \psi_2^{1-\frac{p^2-1}{e}}(\theta)z \qquad ; \qquad \theta_0 * z = \theta_0 z\ .$$

On en déduit qu'il existe sur $\mathcal{R}$ une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1, telle que G agit via $\mathrm{Gal}(F/\mathbb{Q}_p)$, le sous-groupe d'inertie $I(F/\mathbb{Q}_p)$ agit via le caractère ψ_2 à la puissance $1 - \frac{p^2-1}{e}$, et θ_0 agit semi-linéairement par $x \mapsto \zeta x^p$. La classe d'isomorphisme de cette représentation ne dépend pas du choix de ζ, et elle est irréductible. En particulier, en remontant la construction, on en conclut que les réseaux G-stables de $V_\alpha \simeq V_p(E)$ sont tous homothétiques lorsque $v(\alpha) \leq 0$, et que l'on a ainsi obtenu une description du $\mathbb{F}_p[G]$-module $E[p] = T_p(E)/pT_p(E)$ constitué des points d'ordre p de E.

Cas $v(\alpha) \leq 0$: Soit $\pi \in \overline{\mathbb{Q}}_p$ tel que $\pi^{p^2-1} = -p$, et soit ψ_2 le quotient du caractère fondamental de niveau 2 modulo $I(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^4}(\pi))$. Il existe une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1 sur $E[p]$ sur lequel G agit par

$$G \xrightarrow{proj} \mathrm{Gal}(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p) \xrightarrow{\rho} \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2})\ ,$$

où $I(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p)$ agit via $\psi_2^{1-\frac{p^2-1}{e}}$, et le relèvement du Frobenius fixant π agit semi-linéairement par $x \mapsto \zeta x^p$, $x \in \mathbb{F}_{p^2}$, avec $\zeta \in \overline{\mathbb{F}}_p$ tel que $\zeta^{p+1} = -1$.
La représentation est même absolument irréductible, et correspond dans [Fo-Ma] à l'objet $\overline{V}_{1-\frac{p^2-1}{e},1}$. De plus, *l'action du groupe d'inertie absolu I sur $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ est diagonalisable, et il existe une $\mathbb{F}_{p^2}$-base de $E[p] \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2}$ telle que I agit via*

$$\begin{pmatrix} \psi_2^{1-\frac{p^2-1}{e}} & 0 \\ 0 & \psi_2^{p+\frac{p^2-1}{e}} \end{pmatrix}\ .$$

Cas $v(\alpha) \geq 2$:

On prend $c = \dfrac{1}{p(p^2-1)}$, et l'on a $pT_c = T_{p^2c} = T_c^+$, d'où $T_c/pT_c = T_c/T_c^+ \simeq A_c/A_c^+$: c'est un $\mathbb{F}_p[G]$-espace vectoriel de dimension 2. Soit $a \in A_c$ tel que $v_R(a) = c$. L'étude des valuations dans l'équation

$$(*_\alpha) \qquad \sum_{n\in\mathbb{Z}} (-1)^n p^n \left(\alpha\, \pi_e^{-2} a^{(0)p^{-2n}} + a^{(0)p^{-2n+1}} \right) = 0$$

montre que $v(a^{(0)p}) = v(p^{-1}a^{(0)p^3}) = pc$, et que les autres termes sont de valuation strictement supérieure à pc. On obtient donc :

$$\frac{a^{(0)p^3}}{p} - a^{(0)p} \in \mathcal{M}_{C,pc}^+ = \{\, x \in C \,/\, v(x) > pc \,\} .$$

On reprend $\mathcal{R} = \{\, z \in \overline{\mathbb{Q}}_p \,/\, z^{p^2} - pz = 0 \,\}$, et cette fois on voit que pour $a \in A_c$ tel que $v_R(a) = c = \frac{1}{p(p^2-1)}$, il existe un unique élément $z(a) \in \mathcal{R}$ tel que $a^{(0)p} \equiv z(a) \bmod \mathcal{M}_{C,pc}^+$. Puis :

$$a \equiv b \bmod A_c^+ \;\Leftrightarrow\; a^{(0)} \equiv b^{(0)} \bmod \mathcal{M}_{C,c}^+ \;\Leftrightarrow\; a^{(0)p} \equiv b^{(0)p} \bmod \mathcal{M}_{C,pc}^+ .$$

On définit ainsi une flèche bijective $A_c/A_c^+ \longrightarrow \mathcal{R}$, en associant à $a \bmod A_c^+$ l'unique élément $z(a) \in \mathcal{R}$ tel que $a^{(0)p} \equiv z(a) \bmod \mathcal{M}_{C,pc}^+$, qui donne à $\mathcal{R}$ une structure de $\mathbb{F}_p[G]$-espace vectoriel de dimension 2. Par définition, pour tous $z \in \mathcal{R}$ et $g \in G$, on a : $g * z =$ l'unique élément y de $\mathcal{R}$ tel que $(g*a)^{(0)p} \equiv y \bmod \mathcal{M}_{C,pc}^+$, où $a^{(0)p} \equiv z \bmod \mathcal{M}_{C,pc}^+$. Cette fois, comme $p \equiv -1 \bmod e\mathbb{Z}$, on obtient :

$$\left.\begin{array}{rcccl} g*z & = & \zeta_e^{pr} \cdot gz & = & \zeta_e^{-r} \cdot gz \,, \quad \text{si } g \bmod G_K = \omega\tau_e^r \\ & = & \zeta_e^{-pr} \cdot gz & = & \zeta_e^{r} \cdot gz \,, \quad \text{si } g \bmod G_K = \tau_e^r \end{array}\right\} \;,\; 0 \leq r \leq e-1 \,.$$

Alors les mêmes considérations que pour le cas $v(\alpha) \leq 0$ montrent qu' il existe sur $\mathcal{R}$ une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1, telle que G agit via $\mathrm{Gal}(F/\mathbb{Q}_p)$, le sous-groupe d'inertie $I(F/\mathbb{Q}_p)$ agit via ψ_2 à la puissance $1 + \frac{p^2-1}{e}$, et le relèvement du Frobenius fixant π par $x \mapsto \zeta x^p$. La classe d'isomorphisme de cette représentation ne dépend pas du choix de ζ, et elle est irréductible. En particulier, en remontant la construction, on en conclut que les réseaux G-stables de $V_\alpha \simeq V_p(E)$ sont tous homothétiques lorsque $v(\alpha) \geq 2$, et que l'on a ainsi obtenu une description du $\mathbb{F}_p[G]$-module $E[p] = T_p(E)/pT_p(E)$ constitué des points d'ordre p de E.

Cas $v(\alpha) \geq 2$: Soit $\pi \in \overline{\mathbb{Q}}_p$ tel que $\pi^{p^2-1} = -p$, et soit ψ_2 le quotient du caractère fondamental de niveau 2 modulo $I(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p^4}(\pi))$. Il existe une structure de $\mathbb{F}_{p^2}$-espace vectoriel de dimension 1 sur $E[p]$ sur lequel G agit par

$$G \xrightarrow{proj} \mathrm{Gal}(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p) \xrightarrow{\rho} \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^2}) \,,$$

où $I(\mathbb{Q}_{p^4}(\pi)/\mathbb{Q}_p)$ agit via $\psi_2^{1+\frac{p^2-1}{e}}$, et le relèvement du Frobenius fixant π agit semi-linéairement par $x \mapsto \zeta x^p$, $x \in \mathbb{F}_{p^2}$, avec $\zeta \in \overline{\mathbb{F}}_p$ tel que $\zeta^{p+1} = -1$.

Là encore, la représentation est absolument irréductible, et correspond dans [Fo-Ma] à l'objet $\overline{V}_{1+\frac{p^2-1}{e},1}$. De plus, *l'action du groupe d'inertie absolu I sur $E[p]\otimes_{\mathbb{F}_p}\mathbb{F}_{p^2}$ est diagonalisable, et il existe une $\mathbb{F}_{p^2}$-base de $E[p]\otimes_{\mathbb{F}_p}\mathbb{F}_{p^2}$ telle que I agit via*

$$\begin{pmatrix} \psi_2^{1+\frac{p^2-1}{e}} & 0 \\ 0 & \psi_2^{p-\frac{p^2-1}{e}} \end{pmatrix} .$$

Remarque : Les deux représentations obtenues avec $v(\alpha)\leq 0$ et $v(\alpha)\geq 2$ ne sont pas isomorphes, puisque $1-\frac{p^2-1}{e}\not\equiv 1+\frac{p^2-1}{e} \bmod (p^2-1)\mathbb{Z}$ pour $e\geq 3$. En fait, avec les notations de [Fo-Ma], les objets $\overline{V}_{1+\frac{p^2-1}{3},1}$, $\overline{V}_{1+\frac{p^2-1}{4},1}$ et $\overline{V}_{1+\frac{p^2-1}{6},1}$ sont les twists ramifiés d'ordre 2 correspondant à l'extension $\mathbb{Q}_p(\pi_2)/\mathbb{Q}_p$ des objets $\overline{V}_{1-\frac{p^2-1}{6},1}$, $\overline{V}_{1-\frac{p^2-1}{4},1}$ et $\overline{V}_{1-\frac{p^2-1}{3},1}$ respectivement.

Cas $v(\alpha)=1$:

Dans toute cette section, on pose $\alpha=p\beta^{-1}$ avec $\beta\in\mathbb{Z}_p^\times$.

On prend $c=\dfrac{1-2/e}{p^2(p-1)}$ et $c'=\dfrac{2/e}{p(p-1)}$: ils sont tous les deux dans $]\frac{1}{p^2(p^2-1)},\frac{1}{p^2-1}]$. On a les inégalités $c<c'<p^2c<p^2c'$, d'où des inclusions strictes $pT_{c'}\subset pT_c\subset T_{c'}\subset T_c$.
Etudions pour commencer T_c/pT_c ; les inclusions ci-dessus induisent une suite exacte de $\mathbb{F}_p[G]$-modules :

$$0\longrightarrow T_{c'}/T_{p^2c}\longrightarrow T_c/T_{p^2c}\longrightarrow T_c/T_{c'}\longrightarrow 0 .$$

On voit facilement que si $u_{\underline{a}}, u_{\underline{a}'}\in T_c$ sont tels que $v_R(a)=c$ et $v_R(a')=c'$, alors on a $T_c=\mathbb{Z}_p u_{\underline{a}}\oplus\mathbb{Z}_p u_{\underline{a}'}$ (ou bien : $A_c=\mathbb{Z}_p a\oplus\mathbb{Z}_p a'$), et aussi $T_{c'}=p\mathbb{Z}_p u_{\underline{a}}\oplus\mathbb{Z}_p u_{\underline{a}'}$.
Nous nous proposons de décrire l'action de G sur $T_{c'}/T_{p^2c}=T_{c'}/T_{c'}^+\simeq A_{c'}/A_{c'}^+$: c'est un $\mathbb{F}_p[G]$-espace vectoriel de dimension 1. Soit $a\in A_{c'}$ tel que $v_R(a)=c'=\frac{2/e}{p(p-1)}$. L'étude des valuations dans l'équation

$$(*_\alpha)\qquad \sum_{n\in\mathbb{Z}}(-1)^n p^n\left(\alpha\,\pi_e^{-2}a^{(0)^{p^{-2n}}}+a^{(0)^{p^{-2n+1}}}\right)=0$$

montre que $v(a^{(0)^p})=v(\beta^{-1}\pi_e^{-2}a^{(0)^{p^2}})=pc'$, et que

$$\beta^{-1}\pi_e^{-2}a^{(0)^{p^2}}-a^{(0)^p}\ \in\ \mathcal{M}_{C,pc'}^+=\{\,x\in C\ /\ v(x)>pc'\,\} .$$

Soit $\mathcal{S}=\{\,x\in\overline{\mathbb{Q}}_p\ /\ x^p-\beta\pi_e^2x=0\,\}$: un élément non nul x de $\mathcal{S}$ vérifie $x^{p-1}=\beta\pi_e^2$, d'où $v(x)=\frac{2/e}{p-1}=pc'$. De plus, $\mathrm{Card}(\mathcal{S})=p-1$, et si $x,x'\in\mathcal{S}$ avec $x\neq x'$, alors $v(x-x')=pc'$.
Comme $v(x)=v(a^{(0)^p})=pc'$, il existe un unique $u\in O_C^\times$ tel que $a^{(0)^p}=ux$, d'où :

$$\beta^{-1}\pi_e^{-2}(ux)^p-ux=x(u^p-u)\ \in\ \mathcal{M}_{C,pc'}^+\ \Leftrightarrow\ u^p-u\in\mathcal{M}_C .$$

Donc $u\equiv[\varepsilon]\bmod\mathcal{M}_C$, avec cette fois $\varepsilon\in\mathbb{F}_p^\times$, et $a^{(0)^p}\equiv[\varepsilon]x\bmod\mathcal{M}_{C,pc'}^+$, $[\varepsilon]x\in\mathcal{S}$. On en déduit que pour $a\in A_{c'}$ tel que $v_R(a)=c'$, il existe un unique élément $x(a)\in\mathcal{S}$ tel que $a^{(0)^p}\equiv x(a)\bmod\mathcal{M}_{C,pc'}^+$. Comme $pc'<1$, on sait que (lemme 3), pour $a,b\in A_{c'}$, on a

$$a\equiv b\bmod A_{c'}^+\ \Leftrightarrow\ a^{(0)}\equiv b^{(0)}\bmod\mathcal{M}_{C,c'}^+\ \Leftrightarrow\ a^{(0)^p}\equiv b^{(0)^p}\bmod\mathcal{M}_{C,pc'}^+ .$$

Cela permet de définir une flèche injective $A_{c'}/A_{c'}^+ \longrightarrow \mathcal{S}$, en associant à a mod $A_{c'}^+$ l'unique élément $x(a) \in \mathcal{S}$ tel que $a^{(0)^p} \equiv x(a) \bmod \mathcal{M}_{C,pc'}^+$; cette flèche est bijective puisque $\mathrm{Card}(\mathcal{S}) = \mathrm{Card}(A_{c'}/A_{c'}^+) = p-1$. On munit alors $\mathcal{S}$ de l'unique structure de $\mathbb{F}_p[G]$-espace vectoriel de dimension 1 qui fait de cette flèche un isomorphisme $\mathbb{F}_p[G]$-linéaire. Si $g \in G$ et $x \in \mathcal{S}$, $g * x$ est par définition l'unique élément de $\mathcal{S}$ congru à $(g*a)^{(0)^p}$ modulo $\mathcal{M}_{C,pc'}^+$; cela donne :

$$\left.\begin{array}{rcll} g*x & = & \zeta_e^{-r} \cdot gx\ , & \text{si } g \bmod G_K = \omega\tau_e^r \\ & = & \zeta_e^r \cdot gx\ , & \text{si } g \bmod G_K = \tau_e^r \end{array}\right\}\ ,\ 0 \le r \le e-1\ .$$

Soit $\xi \in \mathbb{Z}_p^{nr}$ tel que $\xi^{p-1} = \beta$. Le groupe d'inertie absolu I agit trivialement sur ξ, et si g_0 est un relèvement du Frobenius arithmétique, alors $g_0\xi \equiv \beta\xi \bmod p\mathbb{Z}_p^{nr}$; le caractère de G dans $\mathbb{F}_p^\times$ qui à g associe $\frac{g\xi}{\xi}$ est évidemment indépendant du choix de ξ. On a donc $\frac{g_0\xi}{\xi} \equiv \beta \bmod p\mathbb{Z}_p^{nr}$ et $(\frac{g_0\xi}{\xi})^{p-1} = 1$, ce qui équivaut à $\frac{g_0\xi}{\xi} = [\overline{\beta}]$, où $\overline{\beta} = \beta \bmod p\mathbb{Z}_p = p\alpha^{-1} \bmod p\mathbb{Z}_p$.
Tout élément x non nul de $\mathcal{S}$ s'écrit $x = \xi\pi^{2\frac{p+1}{e}}$ (on a $(\pi^{2\frac{p+1}{e}})^{p-1} = \pi_e^2$). Alors on en déduit que pour tout $g \in I$, $g*x = \psi_2^{\frac{p^2-1}{e}}(g)gx = \psi_2^{\frac{p^2-1}{e}}(g)\psi_2^{2\frac{p+1}{e}}(g)x = \psi_2^{\frac{(p+1)^2}{e}}(g)x$; or, on a $\psi_2^{p+1} = \chi_p$, où χ_p est le caractère donnant l'action de G sur les racines p-ièmes de l'unité, donc $g*x = \chi_p^{\frac{p+1}{e}}(g)x$ pour $g \in I$. Enfin, l'action de G sur x est donnée par :

$$\forall\, g \in G \quad ,\quad g*x = \eta_{\overline{\beta}}(g)\chi_p^{\frac{p+1}{e}}(g)x\ ,$$

où $\eta_{\overline{\beta}}$ est l'unique caractère non ramifié $G \to G/I \to \mathbb{F}_p^\times$ qui envoie le Frobenius arithmétique sur $\overline{\beta}$. Cela termine la description de l'action de G sur $T_{c'}/T_{p^2c} = T_{c'}/T_{c'}^+ \simeq A_{c'}/A_{c'}^+$.
Puis, comme on sait que le déterminant sur T_c/pT_c est χ_p (puisque le déterminant sur $V_\alpha \simeq V_p(E)$ est le caractère cyclotomique dont la réduction modulo p est χ_p), on en déduit immédiatement l'action de G sur $T_c/T_{c'}$: elle se fait par le caractère $\eta_{\overline{\beta}^{-1}}\chi_p^{1-\frac{p+1}{e}}$.

Une étude parfaitement similaire du $\mathbb{F}_p[G]$-module $T_{c'}/pT_{c'} = T_{c'}/T_{p^2c'}$ montre que l'on a une suite exacte :

$$0 \longrightarrow T_{p^2c}/T_{p^2c'} \longrightarrow T_{c'}/T_{p^2c'} \longrightarrow T_{c'}/T_{p^2c} \longrightarrow 0\ ,$$

où l'action de G sur le sous-$\mathbb{F}_p[G]$-module (de dimension 1) $T_{p^2c}/T_{p^2c'} \simeq T_c/T_{c'}$ se fait par le caractère $\eta_{\overline{\beta}^{-1}}\chi_p^{1-\frac{p+1}{e}}$, et sur le quotient $T_{c'}/T_{p^2c}$ par le caractère $\eta_{\overline{\beta}}\chi_p^{\frac{p+1}{e}}$.

On en déduit facilement qu'à homothétie près, les réseaux G-stables de $V_\alpha \simeq V_p(E)$ pour $v(\alpha) = 1$ sont T_c et $T_{c'}$, avec $c = \dfrac{1-2/e}{p^2(p-1)}$ et $c' = \dfrac{2/e}{p(p-1)}$. Finalement, on obtient :

Cas $v(\alpha) = 1$: il existe une $\mathbb{F}_p$-base de $E[p]$ telle que G agit via

$$\begin{pmatrix} \eta_{\overline{p/\alpha}}\chi_p^{\frac{p+1}{e}} & * \\ 0 & \eta_{\overline{p/\alpha}}^{-1}\chi_p^{1-\frac{p+1}{e}} \end{pmatrix} \quad \textit{ou} \quad \begin{pmatrix} \eta_{\overline{p/\alpha}}^{-1}\chi_p^{1-\frac{p+1}{e}} & * \\ 0 & \eta_{\overline{p/\alpha}}\chi_p^{\frac{p+1}{e}} \end{pmatrix}\ .$$

Remarque : Soit O_K l'anneau des entiers de K. L'invariant α est lié au logarithme du groupe formel sur O_K (de hauteur 2) de E_K. D'après les résultats de A. Kraus, les cas $v(\alpha) \neq 1$ et $v(\alpha) = 1$ correspondent respectivement à $v(\tau_p) \geq \frac{p}{p+1}$ et $v(\tau_p) < \frac{p}{p+1}$, où $\tau_p \in O_K$ est le p-ième terme de la série formelle donnant la multiplication par p dans le groupe formel de E_K. De plus, les cas $v(\alpha) \geq 2$ et $v(\alpha) = 1$, situation de gauche, correspondent à $v(\Delta_E) > 6$, où l'on a choisi une équation *minimale* pour la courbe elliptique E, et les cas $v(\alpha) \leq 0$ et $v(\alpha) = 1$, situation de droite, correspondent à $v(\Delta_E) < 6$ ([Kr], 2.3.2., Prop.2 et Lemme 2).

RÉFÉRENCES

[Br] CH. BREUIL. Schémas en groupes sur un anneau de valuation discrète très ramifié, Prépublications d'Orsay 98-09, Université de Paris-Sud (1998)

[Del] P. DELIGNE. Les constantes de l'équation fonctionnelle des fonctions L, **in** *Modular functions of one variable II*, LNM 349, p. 501-595, Springer-Verlag (1973).

[Deu] M. DEURING. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg 14, p. 197-272 (1941).

[Fo 1] J.-M. FONTAINE. Le corps des périodes p-adiques, exposé II, **in** *Périodes p-adiques*, Astérisque 223, Soc. Math. de France (1994).

[Fo 2] J.-M. FONTAINE. Représentations p-adiques semi-stables, exposé III, **in** *Périodes p-adiques*, Astérisque 223, Soc. Math. de France (1994).

[Fo 3] J.-M. FONTAINE. Représentations l-adiques potentiellement semi-stables, exposé VIII, **in** *Périodes p-adiques*, Astérisque 223, Soc. Math. de France (1994).

[Fo 4] J.-M. FONTAINE. Groupes p-divisibles sur les corps locaux, Astérisque 47-48, Soc. Math. de France (1977).

[Fo 5] J.-M. FONTAINE. Sur certains types de représentations p-adiques du groupe de Galois d'un corps local ; construction d'un anneau de Barsotti-Tate, Annals of Math. 115, p. 529-577 (1982).

[Fo-Ma] J.-M. FONTAINE and B. MAZUR. Geometric Galois Representations, **in** *Conference on Elliptic Curves and Modular Forms*, Hong Kong, December 18-21 (1995).

[EGA III] A. GROTHENDIECK (avec la collaboration de J. Dieudonné). Etude cohomologique des faisceaux cohérents, EGA III, Publ. Math. I.H.E.S. 11 (1961) et 17 (1963).

[Ho-Ta] J. TATE. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. HONDA), Séminaire Bourbaki 352 (Nov. 1968).

[Huse] D. HUSEMÖLLER. Elliptic Curves, GTM 111, Springer-Verlag (1987).

[Ka] N. KATZ. Serre-Tate local moduli, **in** *Surfaces algébriques*, LNM 868, p. 138-202, Springer-Verlag (1981).

[Kr] A. KRAUS. Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique, Diss. Math. 364, 39p. (1997)

[Laf] G. LAFFAILLE. Construction de groupes p-divisibles : le cas de dimension 1, **in** *Journées de géométrie algébrique de Rennes (III)*, Astérisque 65, Soc. Math. de France, p. 103-123 (1979).

[La] S. LANG. Abelian Varieties, Interscience Publishers, New York (1959).

[Me] W. MESSING. The Crystals associated to Barsotti-Tate Groups : with Applications to Abelian Schemes, LNM 264, Springer-Verlag (1972).

[Rei] I. REINER. Maximal Orders, L.M.S. monographs, Academic Press (1975).

[Roh] D.E. ROHRLICH. Elliptic Curves and the Weil-Deligne Group, CRM Proceedings and Lecture Notes vol. 4 (1994).

[Se 1] J.-P. SERRE. Abelian l-adic representations and elliptic curves (2nd ed.), Addison-Wesley, Redwood City (1989).

[Se 2] J.-P. SERRE. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones Math. vol. 15, p. 259-331 (1972).

[Se 3] J.-P. SERRE. Cohomologie Galoisienne, 5ème éd., LNM 5, Springer-Verlag (1994).

[Se-Ta] J.-P. SERRE and J. TATE. Good reduction of abelian varieties, Annals of Math. 88, p. 492-517 (1968).

[Silv 1] J.H. SILVERMAN. The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag (1986).

[Silv 2] J.H. SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves, GTM 151, Springer-Verlag (1994).

[Ta] J. TATE. Endomorphisms of Abelian Varieties over Finite Fields, Invent. Math. 2, p. 134-144 (1966).

[W] A. WEIL. The Field of Definition of a Variety, Am. J. of Math. 78, p. 509-524 (1956).