UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE

Laboratoire de Mathématiques Pures associé au C. N. R. S.

Jean-Marc Fontaine
INSTITUT FOURIER
MATHÉMATIQUES PURES
Boite Postale 116
38402 SAINT MARTIN D'HÈRES

[redacted]

Téléphone (76) 54.81.45

le 25 juin 1979

Cher Serre,

Je vais tenter de t'expliquer comment les renseignements contenus dans ta lettre du 27 mai dernier permettent de déterminer à isomorphisme près, le semi-simplifié (et même un peu mieux) de $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(A)$ (où, comme dans ta lettre, A est le quotient de $J_1(p)$ par $J_o(p)$), en tant que $\mathbb{Q}_p[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-module. Cela devrait s'appliquer aussi à des situations beaucoup plus générales (morceaux de $J_1(N)$), car s'il est important que la variété abélienne considérée ait beaucoup d'endomorphismes et acquiert bonne réduction sur une extension finie de $\mathbb{Q}_p$, l'indice de ramification de cette extension n'intervient pas (sauf pour exploiter le résultat, par exemple pour donner l'action de l'inertie modérée, auquel cas je suis très mal à l'aise si $e > 1$

I. - Le module de Dieudonné de A .

(Comme le module de Dieudonné est contravariant, je vais faire opérer à droite (avec des " $|$ ") tout ce qui opère à gauche sur A ; comme tout est commutatif, cela n'a pas grande importance, mais cela m'évitera de m'embrouiller dans les signes, avec les représentations contragrédientes).

La variété abélienne A acquiert bonne réduction sur le corps $\mathbb{Q}_p(z) = \mathbb{Q}_p(\sqrt[p]{1})$, ce qui permet de parler de la fibre spéciale $\Gamma_{\mathbb{F}_p}$ (sur le corps résiduel $\mathbb{F}_p$ de $\mathbb{Q}_p(z)$) de son groupe p-divisible Γ . Par fonctorialité ..., $\underline{H}_p = \mathbb{Q}_p \otimes_{\mathbb{Q}} \underline{H}$ (où, comme dans ta lettre, $\underline{H}$ est la sous-algèbre de

(*) en fait, seulement si μ_p est contenu dans le groupe des valeurs des caractères qui interviennent, cf plus bas.

25/6/79

$\mathbb{Q}\otimes \mathrm{End}(A)$ engendrée, sur $\mathbb{Q}$, par les opérateurs de Hecke) e
$\mathrm{Gal}(\mathbb{Q}_p(z)/\mathbb{Q}_p)$ opèrent sur $\Gamma_{\mathbb{F}_p}$.

Soit alors $D = \mathbb{Q}_p\otimes_{\mathbb{Z}_p} \mathrm{Hom}(\Gamma_{\mathbb{F}_p}, CW)$ le module de Dieudonné "à isogénie près" de $\Gamma_{\mathbb{F}_p}$ (peu importe ce qu'est CW !). C'es un vectoriel sur $\mathbb{Q}_p$ de dimension deux fois la dimension de muni d'une action de F "à droite" (c'est celle qui provient de l'endomorphisme de Frobenius sur $\Gamma_{\mathbb{F}_p}$) et, toujours par fonctorialité, d'une action, également à droite, de $\underline{H}_p$ et de $\mathrm{Gal}(\mathbb{Q}_p(z)/\mathbb{Q}_p)$. Comme tout commute, c'est, finalement un modul à droite sur l'anneau commutatif $\underline{H}_p[F,\mathrm{Gal}(\mathbb{Q}_p(z)/\mathbb{Q}_p)]$ et la connaissance de ce module, à isomorphisme près, détermine $\Gamma_{\mathbb{F}_p}$ muni de l'action de $\underline{H}_p$ et de celle de $\mathrm{Gal}(\mathbb{Q}_p(z)/\mathbb{Q}_p)$, à isogénie près.

<u>Théorème 1</u>. - <u>Le module de Dieudonné</u> D <u>est isomorphe à</u> $\underline{H}_p \times \underline{H}$ <u>avec action évidente de</u> $\underline{H}_p$ <u>et</u>

$$(x,x')|F = (x|U', x'|U),$$

$$(x,x')|d = (x,x'|R_d)$$

(j'ai identifié $\mathrm{Gal}(\mathbb{Q}_p(z)/\mathbb{Q}_p)$ et $\mathbb{F}_p^*$ de la manière habituel

<u>Démonstration</u> : Le fait que la fibre spéciale de A soit isogène à $J\times J'$ nous fournit une décomposition de D en somme directe $D = D_J \oplus D_{J'}$. Chauqe morceau est un sous-$\underline{H}_p$-module et ce que tu dis page 12 montre que, pour démontrer le th., il suffit de vérifier que chaque morceau est libre de rang 1. Pour des raisons de dimension, cela revient à dire que $\underline{H}_p$ opère fidèlement sur J (ou sur J' si tu préfères). Un argument dire devrait permettre de le montrer, mais je ne le vois pas. En voi un autre qui utilise un lemme que se trouve plus bas, mais tu vérifieras qu'il n'y a pas de cercle vicieux :

Soit E un facteur simple de l'algèbre $\underline{H}_p$, $a : \underline{H}_p \longrightarrow E$

25/6/79

la projection can. , $\lambda = a(U)$, $\lambda' = a(U')$ (on a donc $\lambda\lambda' = p$), $\varepsilon : \mathrm{Gal}(\mathbb{Q}_p(z)/\mathbb{Q}_p) \longrightarrow E^*$ la flèche $d \longmapsto a(R_d)$. Soit V_E le morceau de $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(A)$ correspondant à E (c'es donc un $E\,\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ -module, de dim. 2 sur E) et D_E le module de Dieudonné correspondant. Il est clair que, comme vec sur E , $D_E \simeq E \times E$ et que, pour l'action de F et Gal, il y a, a priori trois possibilités suivant que la fibre spéciale du groupe p-divisible correspondant est contenue dans J , dan J' , ou à cheval sur les deux :

a) $(x,x')|F = (\lambda' x, \lambda' x')$ et $(x,x')|F = (x,x')$,

b) $(x,x')|F = (\lambda x, \lambda x')$ et $(x,x')|d = (\varepsilon(d)x, \varepsilon(d)x')$,

c) $(x,x')|F = (\lambda' x, \lambda x')$ et $(x,x')|d = (x, \varepsilon(d)x')$,

et il faut montrer que a) et b) sont impossibles.

Soit v la valuation de E normalisée par $v(p) = 1$. Plu bas dans cette lettre, va se trouver un lemme(*) qui dira que "le module de Dieudonné" de $\bigwedge^2_E V_E$ est $\bigwedge^2_E D_E$ et que

- si on est dans le cas a), on a nécessairement $v(\lambda') =$ 0, 1/2 ou 1 et le caractère de la restriction à l'inertie de la représentation caractéristique est 1, χ ou χ^2 (où χ est caractère cyclotomique) ,

- si on est dans le cas b), on a nécessairement $v(\lambda) =$ 0, 1/2 ou 1 et le car. de la rep. cor. est ε^2, $\chi\varepsilon^2$ ou $\chi^2\varepsilon^2$;

- si on est dans le cas c) , comme on a $\lambda\lambda' = p$, le caract de la rep. de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ cor. est $\chi\varepsilon$.

Si tu sais que le car. est $\chi\varepsilon$, comme $\varepsilon \neq 1$, on voit bie que l'on est dans le cas c .

(*) proposition 3. a)

 25/6/79

<u>Remarque</u> : En particulier, le th. ci-dessus et les résultats d ma lettre du 26 mai dernier démontre le th. de la page 7 de ta lettre (il n'y a donc pas de problème de "pont" entre nos deux lettres). Il n'y a qu'à regarder quels sont les sous-quotients de D_E ; ce qui amène à distinguer les cas I, I' et II de lettre !

II. - <u>Certains groupes</u> p-<u>divisibles sur</u> $\mathbb{Q}_p$.

Je me propose de montrer que la connaissance de D à isomorphisme près, autrement dit de la fibre spéciale de Γ <u>muni de l'action de</u> $\underline{H_p}$ <u>et de celle de</u> $\mathrm{Gal}(\mathbb{Q}_p(z)/\mathbb{Q}_p)$, à isogénie près, détermine "la fibre générique" (sur $\mathbb{Q}_p$) à isomorphisme près. C'est l'existence d'un très gros anneau d'endomorphismes, plus l'action du "petit groupe de Galois" qui rigidifient la situation.

Cela marche dans un cadre plus général, susceptible d'être utile et dans lequel je vais me placer maintenant :

1. - <u>Généralités sur les modules galoisiens pot. admissibles</u>.

Je choisis une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$, je pose $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Soit E un corps, de dim. finie sur $\mathbb{Q}_p$, pas néc. comm., et soit V un espace vectoriel à gauche de dim. finie n sur E , sur lequel G opère linéairement et continûment. Je suppose V potentiellement admissible au sens de mon papier à Rennes (n°7.3) et je note K' une extension finie galoisienne de $\mathbb{Q}_p$ (pour moi $K = \mathbb{Q}_p$!) contenue dans $\overline{\mathbb{Q}}_p$ su laquelle V devient admissible. Je pose $G' = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K')$ et je note K'_0 le corps des fractions de l'anneau des vecteurs de Witt à coeff. dans le corps résiduel k' de K' (dans la situation qui nous intéresse, $K' = \mathbb{Q}_p(\sqrt[p^r]{1})$ pour un r convenable et $k' = \mathbb{F}_p$, $K'_0 = \mathbb{Q}_p$, je me fatigue pour rien et je vais con-

25/6/79

tinuer un peu !).

A cette situation est associé, par mon papier de Rennes, un "module pot. filtré". Je vais plutôt prendre le dual de celui de Rennes (afin d'avoir le "vrai" module de Dieudonné de la fibre spéciale lorsque la restriction de V à K' provient d'un groupes p-divisible sur l'anneau des entiers A' de K'). C'est donc un K'_o-espace vectoriel (à droite si on veut), muni d'une action de F et d'une action semi-linéaire de G/G' , plus d'une filtration de $D_{K'} = D\otimes_{K'_o} K'$ par des sous-K'-espaces vectoriels stables par l'action de G/G' (prolongée par semi-linéarité). La structure de E-vectoriel à gauche sur V induit une structure de E-vectoriel à droite sur D qui est compatible avec tout. Autrement dit,

- on a un module à droite D sur l'anneau $(E\otimes_{\mathbb{Q}_p} K'_o)[F,G/G']$ (règles de commutation dans le dit anneau, avec des not. évidentes et σ = Frobenius absolu sur K'_o , $d \in G/G'$:

$Fd = dF$, $F.(x\otimes y) = (x\otimes\sigma(y)).F$, $d.(x\otimes y) = (x\otimes d(y)).d$

- et une filtration $(D^i_{K'})_{i\in Z}$ de $D_{K'} = D\otimes_{K'_o} K'$ par des sous-modules à droite sur l'anneau $(E\otimes_{\mathbb{Q}_p} K')[G/G']$, décroissante, exhaustive et séparée, bien sûr.

<u>Proposition</u>. - <u>Si</u> $n = \dim_E V$, D <u>est un</u> $(E\otimes_{\mathbb{Q}_p} K'_o)$-<u>module libre de rang</u> n <u>et les</u> $D^i_{K'}$ <u>sont des sous</u>-$(E\otimes_{\mathbb{Q}_p} K')$-<u>modules libres de</u> $D_{K'}$.

Tout simplement parce que σ permute les idempotents primitifs de $E\otimes_{\mathbb{Q}_p} K'_o$ et G/G' opère transitivement sur les idempotents primitifs de $E\otimes_{\mathbb{Q}_p} K'$.

25/6/79

2. - Classification des objets de dim. 1 .

Dans toute la suite, je garde les hypothèses et les notatio du n° précédent, et, pour ne pas me fatiguer, je suppose en ou E commutatif et $K'/\mathbb{Q}_p$ totalement ramifiée (j'ai donc $K'_0 =$

Je note v la valuation de E normalisée par $v(p) = 1$. Pour toute unité u de E , je note $\eta_u : G \longrightarrow E^*$ le caractère de la représentation non ramifiée définie par $\eta_u(\mathrm{Frob}) = u$. Enfin, je note χ le caractère cyclotomique.

Proposition. - Les classes d'isomorphismes des V de dimensio 1 sur E ,qui deviennent admissibles sur K' correspondent b: jectivement aux couples (λ,ε) formés d'un élément $\lambda \in E^*$ v rifiant $v(\lambda) \in \mathbb{Z}$ et d'un homomorphisme $\varepsilon : G/G' \longrightarrow E^*$.

Si $v(\lambda) = i$, le caractère de la représentation associée à un tel couple est $\varepsilon\,\eta_{p^{-i}\lambda}\chi^i$. On a $D \simeq E$, avec $x|F = \lambda x$, $x|g = \varepsilon(g)x$ et la filtration sur $D_{K'}$ est caractérisée par $\mathrm{gr}^j D_{K'} = 0$ si $j \neq i$.

Démonstration : partant de V , on voit que le D associé est dimension 1 sur E , donc que $D_{K'}$ est un $(E\otimes K')$-module libı de rang 1 et la prop. 1 montre qu'il existe un entier i tel que $\mathrm{gr}^j D_{K'} = 0$ si $j \neq i$. La condition d'admissibilité faibl montre alors que le F-iso-cristal D doit être isocline de pente i et la prop. résulte à peu près immédiatement de ce qu'on trouve dans mon papier à Rennes.

3. - Classification des objets de dimension 2 : a) les "fibres spéciales".

La connaissance de V à isomorphisme près est équivalente à celle de D avec toutes ses structures. Je vais appeler "fibre spéciale" tout ce qui concerne la structure de E-vectoriel

25/6/79

muni d'une action de F et de G/G' et "relèvement" tout ce qui concerne la filtration de $D_{K'}$.

Je me place dans la situation suivante : V est un E-vectoriel de rang 2 , qui, en tant que G'-module, est de la for $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(\Gamma)$, avec Γ groupe p-divisible défini sur les enti de K' , je suppose aussi que le caractère de la représentatio de $\Lambda^2_E V$ est $\varepsilon_o \chi$, avec $\varepsilon_o : G/G' \longrightarrow E^*$ un caractère donn et que "la fibre spéciale est scindée" , i.e. que D, comme $E[F,G/G']$-module à droite, est somme directe de deux sous-modul propres (qui sont donc tous deux nécessairement des E-vectori de dim. 1).

<u>Proposition</u>. - <u>Sous les hypothèses qui précèdent, il existe un quadruplet</u> $(\lambda,\lambda',\varepsilon,\varepsilon')$, <u>avec</u> λ,λ' <u>entiers de</u> E <u>vérifiant</u> $\lambda\lambda' = p$, $\varepsilon, \varepsilon' : G/G' \longrightarrow E^*$ <u>des caractères vérifiant</u> $\varepsilon\varepsilon' = \varepsilon$ <u>tels que</u> $D \simeq E \oplus E$, <u>avec</u> $(x,y)|F = (\lambda x,\lambda' y)$, <u>et</u> $(x,y)|g = (\varepsilon(g)x,\varepsilon'(g)y)$, <u>pour tout</u> $g \in G/G'$.

<u>Démonstration</u> : Cela résulte, l'intégralité de λ et λ' mise à part, de la proposition 2 , si tu sais (cf. Rennes) que $D(\Lambda^2_E V) = \Lambda^2_E D$. L'intégralité résulte de ce que l'hypothèse que V provient d'un p-divisible implique que les pentes du F-iso-cristal D sont comprises entre 0 et 1 ; or, ce sont les valuations de λ et λ' .

3. - <u>Classif. des objets de dim</u>. 2 : b) <u>les relèvements</u>.

On va chercher quels sont les classes d'isomorphisme de filtrations possibles a priori sur $D_{K'}$ correspondant à un D associé, comme ci-dessus, à un quadruplet $(\lambda,\lambda',\varepsilon,\varepsilon')$: la prop. 2 nous dit que les $D^j_{K'}$ doivent être des sous-$(E\otimes K')$-modules libres, stables par l'action de G/G' , de $D_{K'}$ et on va aussi écrire les conditions d'admissibilité faible, au sens

25/6/79

de Rennes : elles disent que $D_{K'} = D^0_{K'}$, que $D^2_{K'} = 0$, que $D^1_{K'}$ est libre de rang 1 (et interdisent certaines positions pour $D^1_{K'}$). On est conduit à distinguer deux cas :

Proposition. Gardons les hyp. et les not. qui précèdent. On a donc $D_{K'} = (E\otimes K')\oplus(E\otimes K')$. Notons ν l'image, dans $H^1(G/G',(E\otimes K')^*)$ de $\varepsilon^{-1}\varepsilon'$ (1). Alors

(cas I) Premier cas : $v(\lambda) = 0$, $v(\lambda') = 1$. Il y a (si j'ose dire) deux relèvements (à isomorphisme près) :

- le premier correspond à $D^{(1)}_{K'} = (0,E\otimes K')$ et donne

$$V \simeq \begin{pmatrix} \varepsilon & 0 \\ 0 & \chi\varepsilon' \end{pmatrix} ;$$

(cas II) - le deuxième, qui n'existe que si $\nu = 0$, correspond à $D^{(1)}_{K'} = (E\otimes K').(x,1)$ où x est un élément de $(E\otimes K')^*$ tel que $gx/x = (\varepsilon^{-1}\varepsilon')(g)$, pour tout $g \in G$, et donne

$$V \simeq \begin{pmatrix} \chi\varepsilon' & * \\ 0 & \varepsilon \end{pmatrix}$$

(la représentation n'est pas semi-simple, et la classe d'isom. ne dépend pas du choix de x).

(cas II) Deuxième cas : $v(\lambda) > 0$, $v(\lambda') > 0$. Il y a un seul relèvement qui n'existe d'ailleurs que si $\nu = 0$. Si x est comme ci-dessus, il correspond encore à $D^{(1)}_{K'} = (E\otimes K').(x,1)$.

(Bien sûr, il y a un cas I' qui se ramène à I en échangeant λ et λ').

Remarques. - La condition $\nu = 0$ n'est pas sérieuse ; quitte à augmenter un peu K' , elle est toujours satisfaite.

- Dans le cas I , le D donné correspond toujours à un V (que j'ai à peu près décrit dans mon énoncé). Dans le cas II, mes conjectures générales impliquent que D correspond bien à un

(1) $\varepsilon^{-1}\varepsilon' \in Hom(G/G', E^*) = Hom(G/G', (E\otimes K')^*)^{G/G'} \hookrightarrow Z^1(G/G', (E\otimes K')^*)$.

25/6/79

V et que (il faudrait que je regarde de plus près le cas $\lambda = \lambda'$) l'enveloppe algébrique de l'image de G est $GL_2(E)$ Si $\varepsilon^{-1}\varepsilon'$ est d'ordre premier à p (ce qui équivaut dans ce à d'ordre divisible par p-1 ou d'ordre $\leqslant$ p-1), ce n'est pa une conjecture, c'est un théorème et je peux tout décrire "explicitement" y compris retrouver ce qu'on sait déjà sur l'iner modérée. Le cas général est sans doute abordable, modulo des calculs horribles.

La démonstration de cette proposition n'est pas difficile du tout. Je la remets à une prochaine lettre, avec des commentaires pour en rendre le contenu ~~la proposition ci-dessus~~ plus convaincant~~e~~. Il faut maintenant que je m'occupe des corvées à régler avant mon départ !

Bien à toi

UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE DE GRENOBLE
Laboratoire de Mathématiques Pures associé au C. N. R. S.

Jean-Marc Fontaine
INSTITUT FOURIER
MATHÉMATIQUES PURES
Boite Postale 116
38402 SAINT MARTIN D'HÈRES

Téléphone (76) 54.81.45

Saint-Gildas, le 10 juillet 1979

Cher Serre,

Voici les compléments promis à ma lettre du 25 juin dernier.

Tout d'abord, quleques "précisions" sur l'énoncé de la prop. de la page 8 :

i) Dans le premier cas, ce que j'ai décrit est seulement l'action de l'inertie sur V . L'énoncé correct est

$$V \simeq \begin{pmatrix} \chi\varepsilon'\eta_\lambda^{-1} & 0 \\ 0 & \varepsilon\eta_\lambda \end{pmatrix}$$ ("premier relèvement", i.e. le cas scindé) ,

$$V \simeq \begin{pmatrix} \chi\varepsilon'\eta_\lambda^{-1} & * \\ 0 & \varepsilon\eta_\lambda \end{pmatrix}$$ ("deuxième rel.", i.e. cas non scindé).

ii) Dans le deuxième cas (cas II), le relèvement n'existe que si on a $\nu = 0$ et $(\lambda,\varepsilon) \neq (\lambda',\varepsilon')$ (*). Réciproquement, si ces conditions sont satisfaites et si l'ordre de $\varepsilon^{-1}\varepsilon'$ est premier à p (et conjecturalement sans cette restriction), le relèvement existe effectivement.

4. - Démonstration de la proposition de la p.8 (ainsi modifiée).

A chaque fois que j'ai un espace vectoriel M sur un corps L et une extension L' de L , j'identifierai M à un sous-L-espace vectoriel de $L'\otimes_L M$ en posant $\mu = 1\otimes\mu$.

Je pose d = (1,0) , d' = (0,1) . J'ai donc $D = Ed \oplus Ed'$ et $d|F = \lambda d$, $d'|F = \lambda' d'$. J'ai aussi $D_{K'} = (E\otimes K')d \oplus (E\otimes K')d'$. Comme V provient d'un groupe p-divisible Γ sur A' , anneau des entiers de K' , j'ai $D^0_{K'} = D_{K'}$ et $D^2_{K'} = 0$; la prop. du n°II.1 me dit que $D^1_{K'}$ est un sous-$(E\otimes K')$-module libre de $D_{K'}$; les pentes du F-iso-cristal sous-jacent sont $v(\lambda)$ et $v(\lambda')$; elles ne

(*) la cond. $\nu = 0$ est tjs satisfaite si $\varepsilon^{-1}\varepsilon'$ est d'ordre premier à p.

 10/7/79

sont pas toutes nulles, donc Γ n'est pas étale et $D^1_{K'} \neq 0$; elle ne sont pas toutes égales à 1 , donc Γ n'est pas de type multiplicatif et $D^1_{K'} \neq D_{K'}$. Finalement, $D^1_{K'}$ est bien libre de rang 1 .

a) Le cas $v(\lambda) = 0$, $v(\lambda') = 1$.

Le quotient $D_{K'}/(E\otimes K')d$ est le module de Dieudonné d'un groupe p-divisible de type multiplicatif et la projection de $D^1_{K'}$ sur ce quotient doit être ce quotient tout entier. On en déduit que $D^1_{K'} = (E\otimes K')(d' + xd)$, pour un $x \in E\otimes K'$ convenable.

Il est facile de voir que, réciproquement, le choix d'un $x \in E\otimes K'$ définit effectivement un groupe p-divisible Γ sur A' à isogénie près, muni d'un plongement de E dans $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{End}(\Gamma)$.

Pour avoir un objet comme on veut, il faut en outre (et il suffit) que $D^1_{K'}$ soit stable par Galois. Si $g \in \mathrm{Gal}(K'/\mathbb{Q}_p) = G/G'$, on a $g(d'+xd) = \varepsilon'(g)d' + gx.\varepsilon(g)d = \varepsilon'(g)(d' + (gx/\varepsilon^{-1}\varepsilon'(g)).d)$ et cette condition équivaut à $gx = (\varepsilon^{-1}\varepsilon')(g).x$, pour tout $g \in G/G'$.

- Si $x = 0$, c'est bien le cas : on a alors le premier relèvement ; il est clair que l'extension étale-multiplicatif est scindée et la prop. résulte de la prop. du n°2 .

- Sinon, $x \neq 0$, et, si m est l'ordre de $\varepsilon^{-1}\varepsilon'$, $x^m \neq 0$. Mais $x^m \in (E\otimes K')^{G/G'} = E$; comme il n'est pas nul, c'est un élément de E^* et il est bien inversible dans $E\otimes K'$, donc $x \in (E\otimes K')^*$. Si maintenant, on a deux relèvements distincts correspondant à x et x' tous deux non nuls, on voit que $x/x' = \mu \in E^*$. L'application E-linéaire de D dans lui-même définie par

$$d \mapsto \mu d \quad , \quad d' \mapsto d'$$

induit un isomorphisme du relèvement correspondant à x' sur celui qui correspond à x . On a alors un relèvement non scindé, unique à isomorphisme près, et la fin de la prop., dans ce cas, est immédiate.

 10/7/79

b) Le cas $v(\lambda) > 0$ et $v(\lambda') > 0$.

Je commence par un lemme :

Lemme : Soit u un élément de $E \otimes K'$. On suppose que, pour tout $g \in G/G'$, il existe $c \in E \otimes K'$ tel que $gu = cu$. Alors, si $u \neq 0$ u est inversible.

Démonstration du lemme : Soit $E \otimes K' = E_1 \times E_2 \times \ldots \times E_r$ la décomposition de $E \otimes K'$ en produit de corps. Soit $u = (u_1, u_2, \ldots, u_r)$. Si u n'est pas inversible, l'une des composantes, par ex. u_1, est nulle. Si $u \neq 0$, l'une des composantes, par ex. u_2, est $\neq 0$. Comme G/G' permute les idempotents primitifs, il existe $g \in G/G'$ tel que $gu = (v_1, v_2, \ldots)$, avec $v_1 \neq 0$. Et on a alors $gu \neq cu$, quel que soit $c = (c_1, c_2, \ldots) \in E \otimes K'$.

Démontrons maintenant la prop.: Soit $yd+y'd'$ un générateur du $(E \otimes K')$-module libre $D^1_{K'}$. Je prétend que y et y' sont tous les deux $\neq 0$. En effet si, par exemple, $y' = 0$, j'ai $D^1_{K'} = (E \otimes K')d$ et la condition d'admissibilité faible n'est pas satisfaite (sur le quotient de D par la première composante, j'ai $\mathrm{Fil}^1 = 0$ et je devrais donc avoir un module de pente 0 alors qu'il est de pente $v_p(\lambda')$).

Ecrivons maintenant que $D^1_{K'}$ est stable par Galois : pour tout $g \in G/G'$, j'ai $g(yd+y'd') = gy.\varepsilon(g).d + gy'.\varepsilon'(g).d'$ et il doit donc exister $\mu \in E \otimes K'$ tel que $gy.\varepsilon(g) = \mu y$ et $gy'.\varepsilon'(g) = \mu y'$ Pour m entier assez grand, j'ai donc $gy^m = \mu^m y^m$ et $gy'^m = \mu^m y'^m$ D'après le lemme, y^m et y'^m, donc aussi y et y', sont inversibles et j'ai $D^1_{K'} = (E \otimes K').(d'+xd)$, en posant $x = y/y'$. On termine alors comme pour le relèvement non scindé du cas I.

Mais il reste à se préoccuper de savoir si le relèvement correspondant à l'objet ainsi fabriqué existe bien.

Tout d'abord, a-t'on admissibilité faible ? Si $x \notin E$ (ce qui équivaut à $\varepsilon \neq \varepsilon'$), c'est immédiat (comme $D^1_{K'}$ n'est pas défini sur

10/7/79

E , il est "suffisamment de travers" par rapport à l'action de F)

Si $\varepsilon = \varepsilon'$ en revanche, j'ai $D^1_{K'} = K' \otimes_{\mathbb{Q}_p} D^1$ avec $D^1 = E(d'+xd)$

J'ai $(d'+xd)|F = \lambda' d' + \lambda xd$. Si $\lambda = \lambda'$, D^1 est stable par F c

qui est interdit. Si $\lambda \neq \lambda'$, c'est o.k. .

Si $[K':\mathbb{Q}_p] \leq p-1$, j'ai donc un objet qui a toutes les propriété voulues, y compris l'admissibilité faible, et mes fourbis généraux me disent qu'il correspond bien à une représentation V qui a les propriétés que je veux. Si maintenant l'ordre de $\varepsilon^{-1}\varepsilon'$ est premier à p , il divise $p-1$ et je m'en tire encore car je suis dan une situation qui se déduit, par extension des scalaires et torsion par un caractère, d'une situation avec $e \leq p-1$.

Si maintenant l'ordre de $\varepsilon^{-1}\varepsilon'$ est divisible par p , mes conjectures générales disent que le relèvement existe effectivement. D ce cas particulier, on devrait pouvoir le démontrer en se fatigant un peu, mais ça n'en vaut pas la peine puisque, dans la situation qu nous intéresse, on sait d'avance que la représentation existe.

III. - L'enveloppe algébrique de l'image de Galois.

Soit G'_0 le sous-groupe d'inertie de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K')$. Je note I l'enveloppe algébrique de l'image de G'_0 . C'est donc un sous-group algébrique connexe de $\mathrm{Aut}(V) \simeq \underline{GL}_{2/E}$.

Proposition. - i) Dans le premier cas, I est un "demi-Cartan" (resp un "demi-Borel") , i.e. $I \simeq \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ (resp. $\simeq \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$) suivant que le relèvement est scindé ou non.

- ii) dans le deuxième cas

a) si $\lambda' \neq \pm\lambda$, ou si $\varepsilon^{-1}\varepsilon'$ est d'ordre > 2 , $I = \underline{GL}_2$;

b) si $\lambda' = \pm\lambda$ et si $\varepsilon^{-1}\varepsilon'$ est d'ordre 1 ou 2 , I est un sous groupe de Cartan de $\underline{GL}_2$; on a alors

$$\mathrm{Lie}(I) \simeq \begin{cases} E(x) & \text{si } \lambda = \lambda' \text{ (qui } \cancel{\text{entraîne}}\text{ implique } x \notin E,\ x^2 \notin E \text{),} \\ E(ux) & \text{si } \lambda = -\lambda' \text{ (qui implique } x^2 \in E \text{)} \end{cases}$$

(où x est comme dans la prop. de la p.8 et où u est une racine

10/7/79

<u>primitive</u> $2(p-1)$-<u>ième de l'unité, si</u> $p \neq 2$ (<u>resp.</u> $u = \sqrt{-3}$, <u>si</u> $p = 2$)).

<u>Démonstration</u> : Le premier cas est essentiellement trivial. Je me place dans le second. Supposes que je sache que I est réductif. Alors comme je connais $\Lambda^2_E V$, je sais que $I \not\subset \underline{SL_2}$ et j'ai donc trois possibilités

- ou bien I est le centre de $\underline{GL_2}$ et $End(V) \simeq M_2(E)$,
- ou bien I est un Cartan et $End(V) \simeq Lie(I)$,
- ou bien $I = GL_2$ et $End(V) \simeq E$

(ici $End(V) = End_{E[G'_o]}(V)$). Pour démontrer la proposition, je suis donc ramené

-d'une part à montrer que I est réductif,

- d'autre part à calculer $End(V)$.

a) <u>Montrons que</u> I <u>est réductif</u>.

Le groupe G/G'_o opère sur l'ensemble des droites de V stables par G'_o . Si I n'est pas réductif, cet ensemble a un élément et un seul et il existe donc une droite de V stable par G . Mais c'est impossible (au niveau Dieudonné, il lui correspondrait un quotient de D ayant toutes les bonnes propriétés ; comme $D^1_{K'}$ est libre de rang 1 , son image dans le quotient en question serait libre de rang 0 ou 1 ; le dit quotient correspondrait donc à un morceau non trivial de Γ qui serait soit étale, soit de type multiplicatif ce qui est impossible puisque les pentes sont comprises <u>strict</u>. entre 0 et 1).

b) <u>Calcul de</u> $End(V)$.

Je m'intéresse à V seulement en tant que $E[G'_o]$-module. Son pendant du côté Dieudonné est ce que l'on obtient à partir de D en étendant les scalaires de $\mathbb{Q}_p$ à P , complété de $\mathbb{Q}_p^{nr}$, et en oubliant l'action de Galois. C'est donc le $(P \otimes_{\mathbb{Q}_p} E)$-module libre

10/7/79

$D_P = P \otimes_{\mathbb{Q}_p} D$, de base d et d', muni

- d'une part de l'action de F déduite par extension des scalaire (en prolongeant par semi-linéarité par rapport au Frobenius absolu sur P),

d'autre part, si je pose $P' = K' \otimes_{\mathbb{Q}_p} P$, de la filtration de $D_{P'} = P' \otimes_P D_P$ ($\simeq P \otimes_{\mathbb{Q}_p} D_{K'}$) déduite de $D_{K'}$ par extension des scalaires (on a donc $D^1_{P'} = P \otimes_{\mathbb{Q}_p} D^1_{K'}$).

Alors $\mathrm{End}_{E[G'_0]}(V)$ s'identifie à l'anneau (opposé) à $\mathrm{End}(D_P)$, lui-même formé des applications $(P \otimes E)$-linéaires de D_P dans lui-même qui commutent à l'action de F et qui, après extension des scalaires, respecte la filtration.

Lemme. - i) Si $v(\lambda) \neq v(\lambda')$, on a $\mathrm{End}(D_P) = E$.

ii) Si $v(\lambda) = v(\lambda')$, pour $\sum x_i \otimes y_i \in P \otimes E$, je pose $(\sum x_i \otimes y_i)^{\tau}$ $\sum \sigma^{-1}(x_i) \otimes y_i$ (où σ = Frobenius absolu). Soit u un élément inversible de $P \otimes E$ tel que $u^{\tau}/u = \lambda'/\lambda$ (un tel élément existe grâce au fait que λ'/λ est une unité). Alors $\mathrm{End}(D_P)$ s'identifie au sous-anneau des matrices $(2,2)$, à coefficients dans $P \otimes E$, de la forme

$$\begin{pmatrix} a & bu^{-1} \\ a'u & b' \end{pmatrix}, \text{ avec } a, a', b, b' \in E,$$

vérifiant

$$a'ux^2 + (b'-a)x - bu^{-1} = 0 .$$

Dém. du lemme. - i) Le F-iso-cristal $(P \otimes E)d$ (resp. $(P \otimes E)d'$) est isocline de pente $v(\lambda)$ (resp. $v(\lambda')$). Si $\alpha : D_P \to D_P$ est $(P \otimes E)$-linéaire et commute à F, $v(\lambda) \neq v(\lambda')$ implique que $\alpha(d) \in (P \otimes E)d$, $\alpha(d') \in (P \otimes E)d'$. Il existe donc a, $b' \in P \otimes E$ tels que $\alpha(d) = ad$, $\alpha(d') = b'd$. Si l'on écrit que α commute à

10/7/79

F , on trouve que $a^{\tau} = a$, $b'^{\tau} = b'$, ce qui équivaut à $a, b' \in E$
Si l'on écrit que l'application déduite par ext. des scalaires respecte la filtration, on trouve $a = b'$ et on a bien $\mathrm{End}(D_p) = E$.
le cas ii). - Soit $\alpha \in \mathrm{End}(D_p)$. C'est d'abord une application $(P \otimes E)$-linéaire de D_p dans lui-même. Elle est donc définie par la donnée de $\alpha(d) = ad + a'ud'$, et $\alpha(d') = bu^{-1}d + b'd'$,
avec $a, a'u, bu^{-1}, b' \in P \otimes E$.

On écrit que α commute à F . Si l'on ne se trompe pas (il fau faire attention, par exemple, que $(ad)|F = d|(aF) = a^{\tau}(d|F)$), on trouve que cela équivaut à $a^{\tau} = a$, $a'^{\tau} = a'$, ... , ce qui revient à $a, a', b, b' \in E$.

On écrit ensuite que α respecte la filtration, i.e. que $\alpha(d'+xd)$ appartient au sous-$(P' \otimes E)$-module engendré par $d'+xd$ et on trouve la dernière relation.

<u>Suite de la dém. de la prop.</u>. - Le cas $v(\lambda) \neq v(\lambda')$ est maintenan clair. Aussi, je suppose que $v(\lambda) = v(\lambda') = 1/2$ (remarques que, si $\lambda = -\lambda'$, je peux choisir u comme dans l'énoncé de la prop.).

En appliquant τ aux coefficients du polynôme du second degré dont x est racine, on voit que l'on doit aussi avoir

$$a'u^{\tau}x^2 + (b'-a)x - b\,u^{-\tau} = 0 .$$

En retranchant cette équation à la première, on trouve que

$$a'(u-u^{\tau})x^2 - b\,(u^{-1}-u^{-\tau}) = 0 ,$$ ou encore, en remplaçant u^{τ} par $u\lambda'/\lambda$ et en faisant le calcul

$$a'x^2 = -b\,(\lambda/\lambda')u^{-2} .$$

Si, pour tout $\alpha \in \mathrm{End}(D_p)$, on a $a' = 0$, on doit avoir $b = 0$ et l'équation initiale se réduit à $(b'-a)x = 0$, donc $b' = a$ et $\mathrm{End}(D_p) = E$.

Sinon, il existe $\alpha \in \mathrm{End}(D_p)$ avec $a' \neq 0$, et on doit avoir

10/7/79

$$x^2 = -ba'^{-1}.(\lambda/\lambda')u^{-2} \quad .$$

Le membre de gauche est un élément non nul de $K'\otimes_{\mathbb{Q}_p} E$, celui d droite doit être non nul, donc $b \neq 0$ et c'est alors un élément de $P\otimes_{\mathbb{Q}_p} E$. Donc x^2 et u^2 sont tous deux dans l'intersection de $K'\otimes E$ et $P\otimes E$ qui est E.

En particulier, j'ai $u^2 = u^{2\tau}$, donc $(\lambda'/\lambda)^2 = u^{2\tau}/u^2 = 1$ et on a bien $\lambda' = \pm\lambda$. De plus $x^2 \in E$; comme $gx = (\varepsilon^{-1}\varepsilon')(g)x$, pour tout $g \in G/G'$, et comme $E = (\mathcal{E}\otimes K')^{G/G'}$, on a bien $(\varepsilon^{-1}\varepsilon')^2 = 1$.

Réciproquement,

- si $\lambda = \lambda'$, on peut choisir $u = 1$ et on voit que $\zeta = \begin{pmatrix} 0 & x^2 \\ 1 & 0 \end{pmatrix} \in \mathrm{End}(D_p)$. Comme $\zeta^2 = x^2$, $\mathrm{End}(D_p) \supset E(\zeta) \simeq E(x)$ (puisque $x \notin E$, cf. énoncé p.1), d'où $\mathrm{End}(D_p) \simeq E(x)$, pour des raisons de dimensions.
- Si $\lambda = -\lambda'$, on voit que $\zeta' = \begin{pmatrix} 0 & u^2x^2 \\ 1 & 0 \end{pmatrix} \in \mathrm{End}(D_p)$, et on conclue de la même manière.

<u>Remarque</u>. - Si l'on revient au cas où V est le morceau de $\mathbb{Q}_p\otimes_{\mathbb{Z}_p} T_p(J_1(p))$ correspondant au facteur simple E de l'algèbre de Hecke, on est dans la situation où $\varepsilon = 1$ et

$\varepsilon' = (\text{car. fond. de niveau } 1)^{k-1}$ (avec $2 \leq k \lneq p-1$).

Tu vois donc que, si l'on est dans le cas II, on a $I \simeq \underline{GL_2}$, sauf si et seulement si $\lambda = \pm\lambda'$ <u>et</u> $k = (p+1)/2$. J'espère que cela ne contredit pas ce que tu sais !

+

Merci pour le papier de Wiles que j'ai trouvé en arrivant à St Gildas et que je n'ai pas encore regardé.

Merci aussi pour le preprint de Lubin qui m'a rappelé de vieux souvenirs. Sa conjecture p. 8 est un cas particulier de la conj. suivante qui résulte de mes conj. générales :

10/7/79

<u>Conjecture</u>. - Soit A l'anneau des ent. d'un corps local K de car. 0, à corps résiduel parfait de car. $p \neq 0$. Soit V un vectoriel de dimension finie sur $\mathbb{Q}_p$ sur lequel Galois opère (lin. et cont.) et qui est dans la $\otimes$-catégorie engendrée par les modules de Tate des groupes p-divisibles. Pour tout $i \in \mathbb{Z}$, soit $n_i = \dim_K \mathrm{Hom}_{\mathbb{Q}_p[\mathrm{Gal}]}(V, C(\chi^i))$. Pour que V provienne lui-même d'un groupe p-divisible, il faut et il suffit que $n_i = 0$ si $i \neq 0,1$.

Le fait que la cond. soit nécessaire est dû à Tate. J'ai dit, au moins implicitement, dans mon papier à Rennes que la conjecture est vrai si $e = 1$ (cor.5.2.4) ou si $n_1 = 0$ ou 1 (cor.1 du n°5.2.5). Je sais maintenant que je peux remplacer $e = 1$ par $e \leq p-1$, mais si j'ai à la fois $e > p-1$ et $n_1 > 2$, je ne sais la démontrer que dans des cas particuliers.

Bien à toi

Jean-Marc Fontaine

<u>P.S.</u> : (mercredi) 1) Le temps n'est pas désagréable et la mer est bonne, mais la rédaction de cette lettre ne m'a guère laissé de temps depuis notre arrivée ici lundi au début de l'après-midi. Je vais me rattraper !

2) (En cas) : les Cabanague, chez qui nous sommes jusqu'à la fin du mois, ont maintenant le <u>téléphone</u> : leur n° est <u>(97).53.42.47</u>. (leur adresse exacte est Cabanague, 15 route du Grand-Mont, 56730 - Saint-Gildas de Rhuys).

3) Petite question technique : Quand tu emmènes ta Smith-Corona aux States, comment résouds tu les problèmes de courant électrique (voltage et fréquence) ?

4) Bon Durham et bonne Irlande. Nous connaissons maintenant notre adresse à Princeton (169 Von Neumann Drive, Princeton N.J. 08540) où nous devons arriver le 3 ou le 4 septembre. Nous aurons le téléphone mais je ne connais pas encore le n°.