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 26 mai 1979

Cher Serre,

Voici les résultats promis sur les schémas en groupes de type (p,p) .

I. - <u>Généralités sur les</u> (A'/A)-<u>groupes</u>.

La notion de "bonne réduction potentielle" pour les schémas en groupes finis et plats semble devoir être utile dans des circonstances variées et peut être définie dans un cadre très général. Mais, pour éviter de m'enliser dans les sorites, je vais me restreindre à la situation suivante :

K est un corps local de car. 0 , à corps résiduel parfait k de car. $p \neq 0$, $\overline{K}$ est une clôture algébrique de K , $G = \mathrm{Gal}(\overline{K}/K)$, G' = sous-groupe ouvert de G , $K' = \overline{K}^{G'}$, $J = G/G' = \mathrm{Gal}(K'/K)$, G_o , G'_o et J_o sont les sous-groupes d'iner tie de G , G' et J , A = entiers de K , A' = entier de K' k' = corps résiduel de K' .

J'appelle (A'/A)-<u>groupe</u> (abrévation pour (A'/A)-schéma en groupes fini et plat de rang une puissance de p) la donnée d'un A'-schéma en groupes $\underline{U}_{A'}$, fini et plat, de rang une puissance d p , muni d'une action semi-linéaire de J (si tu préfères, on a une action de J sur l'algèbre affine de $\underline{U}_{A'}$, compatible avec la structure de A-algèbre, avec le coproduit et la counité, et vérifiant

$$g(ax) = ga.gx \quad , \text{ si } \quad g \in J \ , \quad a \in A' \ , \quad x \in \underline{O}(\underline{U}_{A'}) \quad).$$

De même, j'emploierai l'expression " K-<u>groupe</u>" comme abrévatio pour " p-groupe abélien fini sur lequel G opère linéairement."

Si U est un K-groupe, je note $\underline{U}_K$ le K-schéma en groupes fini et plat défini par $\underline{U}_K(\overline{K}) = U$ et je pose $\underline{U}_{K'} = \underline{U}_K \times K'$. Je dirai que U <u>acquiert bonne réduction sur</u> K' si $\underline{U}_{K'}$ admet un prolongement fini et plat sur A' .

A tout (A'/A)-groupe $\underline{U}_{A'}$, on peut associer un K-groupe U qui acquiert bonne réduction sur K' : on a $U = \underline{U}_{A'}(\overline{K}) = \mathrm{Hom}_{A'\text{-alg}}(\underline{O}(\underline{U}_{A'}),\overline{K})$, l'action de G étant définie par

$$(gu)(x) = g(u(\overline{g}^{-1}x))$$

(en notant $\overline{g}$ l'image de $g \in G$ dans J).

On a également un foncteur dans l'autre sens : si U est un K-groupe qui acquiert bonne réduction sur K' , on peut associer à U le "modèle de Raynaud" $\underline{U}_{A'}$ de $\underline{U}_{K'}$, i.e. ce que Raynaud appelle son prolongement minimal. Par unicité dudit modèle, J opère semi-linéairement sur $\underline{U}_{A'}$.

Quelques remarques triviales(*) pour en terminer avec ces généralités :

1. - Si l'indice de ramification absolu $e_{K'}$ de K' est $< p-1$ (avec le grain de sel habituel, cela reste vrai s'il est égal à $p-1$), il résulte de Raynaud que le prolongement fini et plat de U , lorsqu'il existe, est unique, ce qui nous donne alors une équivalence entre la catégorie des K-groupes ayant bonne réduction sur K' et celle des (A'/A)-groupes.

2. - Si K'' est une extension finie de K' contenue dans $\overline{K}$, et si U est un K-groupe qui acquiert bonne réduction sur K' , alors il acquiert évidemment aussi bonne réduction sur K'' . La réciproque est fausse en général, mais vraie si K''/K' est non ramifiée : si $\underline{U}_{A''} = \mathrm{Spec}\, B$ et si $J' = \mathrm{Gal}(K''/K')$, alors $\underline{U}_{A'} = \mathrm{Spec}\, B^{J'}$ (cela résulte immédiatement de ce que $A'' \otimes_{A'} B^{J'} = B$).

(*) ou conséquences triviales des résultats de Raynaud

3. - Si $e_{K'} = p-1$, ce qui précède et Raynaud montrent que tout K-groupe U ,qui est semi-simple en tant que G_o-module, acquiert bonne réduction sur K' .

De même, si $e_{K'} < p-1$, il est facile de caractériser les K-groupes U semi-simples en tant que G_o-modules, qui acquièrent bonne réduction sur K' : si $\chi_h : G_o \to \mathbb{F}^*_{p^h}$ est un caractère fondamental de niveau h , sa restriction à G'_o est la puissance $e_{K'}$-ième d'un caractère fondamental de niveau h . On voit donc que , pour que U ~~acquiert~~ ait bonne réduction sur K' , il faut et il suffit que, pour tout h et tout $i \neq 0$ tels que le caractère χ_h^i intervient dans U avec une multiplicité non nulle , si l'on pose $e_{K'}i \equiv i_o + i_1 p + \ldots + i_{h-1}p^{h-1} \pmod{p^h - 1}$, avec $0 \leq i_j \leq p-1$, on ait $i_j \leq e_{K'}$ pour $j = 0,1,\ldots,h-1$.
(Par exemple, pour $p = 5$, si $e_{K'} = 2$ ou 3 , χ_1^i a bonne réduction pour tout i ; en revanche χ_2^i , avec $0 \leq i < 24$, $i \neq 0,6,12,18$, a bonne réduction, si et seulement si,
- lorsque $e_{K'} = 2$, $i = 1,3,5,13,15$ ou 17 ,
- lorsque $e_{K'} = 3$, $i = 1,2,4,5,8,9,10,13,14,16,17,20,21,22$).

4. - Contrairement à ce qui se passe pour les variétés abéliennes ou les groupes p-divisibles, dans la notion de K-groupe ayant bonne réduction sur K' , il est essentiel que K' soit fixé : pour un U donné, il y a toujours un K' sur lequel il acquiert bonne réduction, mais les exemples précédents montrent que, même lorsque le corps résiduel est algébriquement clos, il n'y en a pas un qui est plus beau que les autres (du moins de façon à la fois évidente et non triviale, si j'ose dire)

5. - Si $\underline{U}_{A'}$ est un (A'/A)-groupe, par réduction, J opère k'-semi-linéairement sur la fibre spéciale $\underline{U}_{k'}$ (ainsi que sur tous les objets qui lui sont fonctoriellement associés, tels que module de Dieudonné, espace tangent, différentielles invariantes,

etc...). C'est particulièrement intéressant lorsque K'/K est to-talement ramifiée (i.e. lorsque $k = k'$) puisque l'on dispose alors d'un homomorphisme de J dans le groupe des automorphismes de la fibre spéciale.

II. - Venons-en maintenant à la situation qui nous intéresse : le <u>cas</u> $p \neq 2$, $K = \mathbb{Q}_p$, K' = <u>l'unique extension de degré</u> $(p-1)/2$ <u>contenue dans</u> $\mathbb{Q}_p(\sqrt[p]{1})$.

Il est facile de décrire les (A'/A)-groupes $\underline{U}_{A'}$ qui sont t[els] que l'action de G_o sur U est semi-simple : (I.3) nous donne la liste des U possibles ; pour chacun d'eux, on regarde le K'-groupe défini par restriction ; par hypothèse, il admet un prolongement fini et plat, et, comme celui-ci est unique, c'est $\underline{U}_{A'}$; le papier de Raynaud au bull. de la S.M.F. nous fournit des équations explicites pour $\underline{U}_{A'}$ et l'action de J s'écrit toute seule.

On peut alors regarder comment est fichue la fibre spéciale $\underline{U}_{F_p}$, munie de l'action de J ; on peut aussi décrire le module de Dieudonné $M = \mathrm{Hom}(\underline{U}_{F_p}, CW)$ de $\underline{U}_{F_p}$, qui est un vectoriel sur F_p de même dim. que (U) muni d'une action de F et V (linéaires avec $FV = VF = 0$) et d'une action de J , également linéaire et qui commute avec F et V .

Le point est que, si $\dim U = 1$ ou 2 , la connaissance de $\underline{U}_{F_p}$ muni de l'action de J (ou, ce qui revient au même, de M muni de l'action de F , V et J) <u>détermine</u> l'action de G_o sur U ; il détermine même l'action de G sur U , sauf si $\dim U = 2$ et U est un G_o-module simple.

~~Il reste le cas $\dim U = 2$ et action de G_o non semi-simple; mais tu vas voir que ce que tu sais sur ta représentation associée à ta forme modulaire interdit ce cas là (que a_p soit ou non divisible par p).~~

nm cf. p. 6

1. Le cas où $\dim U = 1$.

Soit $\chi : G \longrightarrow \mathbb{F}_p^*$ le caractère cyclotomique (on a donc, pour tout $g \in G$, $g\varepsilon = \varepsilon^{\chi(g)}$, pour tout $\varepsilon \in \mu_p$ et aussi, si π est une uniformisante de K' telle que $\pi^{(p-1)/2} \in \mathbb{Q}_p$, $g\pi = [\chi(g)]\pi$, en notant $[a]$ le représentant de Teichmüller de $a \in \mathbb{F}_p$ dans $\mathbb{Z}_p$). Pour tout $a \in \mathbb{F}_p^*$, notons $\eta_a : G \longrightarrow \mathbb{F}_p^*$ le caractère non ramifié tel que $\eta_a(\mathrm{Frob}) = a$ (si $\alpha^{p-1} = [a]$, on a donc $g\alpha = [\eta_a(g)]\alpha$, pour tout $g \in G$).

On trouve alors (il n'y a rien à faire, il n'y a qu'à écrire)

Proposition. - Soit U un K-groupe de dimension 1 sur $\mathbb{F}_p$ et soit $\eta_a\chi^i$, avec $a \in \mathbb{F}_p^*$, $0 \leq i < p-1$, le caractère de la rep sentation qu'il définit. Alors U a bonne réduction sur K' et

i) si i est pair, $U_{A'}$ est étale, $\mathcal{O}(U_{\mathbb{F}_p}) = \mathbb{F}_p[x]/(x^p-ax)$, avec $gx = \chi^{-i}(\hat{g})x$, pour tout $g \in J$; M s'identifie au sous-$\mathbb{F}_p$-espace vectoriel de $\mathcal{O}(U_{\mathbb{F}_p})$ engendré par x avec même action de J et $Fx = ax$, $Vx = 0$.

ii) si i est impair, $U_{A'}$ est de type mult. (i.e. son dual est ~~connexe~~ étale), $\mathcal{O}(U_{\mathbb{F}_p}) = \mathbb{F}_p[x]/x^p$, avec $gx = \chi^{1-i}(\hat{g})x$, pour tout $g \in J$; M s'identifie au sous-$\mathbb{F}_p$-espace vectoriel de $\mathcal{O}(U_{\mathbb{F}_p})$ engendré par x avec même action de J et $Fx = 0$, $Vx = a^{-1}x$).

(j'ai noté $\hat{g}$ un relèvement quelconque, dans G de $g \in J$).

Tu remarqueras que le cas $\dim U = 1$ est en fait stupide : $U_{A'}$ se déduit par extension des scalaires d'un groupe défini sur $A = \mathbb{Z}_p$ et on tord par le caractère χ^i ou χ^{i-1} , l'exposant étant choisi pair pour que ce soit un caractère de J .

2. Le cas où $\dim U = 2$ et U a une droite stable par G_o .

Le cas (1) nous montre qu'il y a trois possibilités pour

$U_{\overline{\mathbb{F}}_p} = U_{\mathbb{F}_p} \times \overline{\mathbb{F}}_p$:

- ou bien c'est $\underline{Z/pZ} \times \underline{Z/pZ}$,
- ou bien c'est $\mu_p \times \mu_p$,
- ou bien c'est $\mu_p \times \underline{Z/pZ}$.

Dans les deux premiers cas, l'action de G_o sur $\det U$ se fait via une puissance paire de χ (somme de deux nombres pairs dans le premier cas, impairs dans le second).

Dans le troisième cas, on voit que le groupe des points de la composante neutre de $\underline{U}_{A'}$, à valeurs dans $\overline{K}$, est stable par G donc U lui-même n'est pas irréductible et l'étude de son semi-simplifié se ramène au cas (1) .

Remarque. -Contrairement à ce que j'avais annoncé un peu vite en bas de la page 4 , la donnée de $\underline{U}_{F_p}$ (tel que $\underline{U}_{F_p} = \mu_p \times \underline{Z/pZ}$) muni d'une action de J ne me permet pas de dire si l'action de G_o sur U est ou non semi-simple. Quelque soit l'action de J , je peux donner un exemple de chacun des deux types.

3. Le cas où $\dim U = 2$ et U est un G_o-module simple.

Je ne m'intéresse qu'à l'action de l'inertie et je vais m'autoriser à tordre implicitement par des caractères non ramifiés. Là encore, il suffit de tout écrire (je note $\chi_2 : G_o \longrightarrow \mathbb{F}^*_{p^2}$ un caractère fondamental de niveau 2):

Proposition. - Soit U un K-groupe, qui est un $\mathbb{F}_p$-vectoriel de dimension 2 . On suppose que l'action de G_o sur U se fait à travers les caractères χ_2^i et $\chi_2^{i'}$, avec i et i' des entiers non divisibles par p+1 (donc $i \equiv pi' \bmod (p^2-1)$). Soient j,j',r,r' les entiers définis par

$$i.(p-1)/2 = j + pj' + r(p^2-1) ,$$
$$i'.(p-1)/2 = j' + pj + r'(p^2-1) ,$$

avec $0 \leqslant j,j' \leqslant p-1$.

Pour que U ait bonne réduction sur K', il faut et il suffit que $j \leqslant (p-1)/2$ et $j' \leqslant (p-1)/2$. S'il en est ainsi, on a $\underline{O}(\underline{U}_{A'}) = A'[X,X']/(X^p - \pi^{j'}X', X'^p - \pi^j X)$, avec, pour tout $g \in J$,

$gX = \chi^{-2r}(\hat{g})X$, $gX' = \chi^{-2r'}(\hat{g})X'$. M <u>est un $\mathbb{F}_p$-vectoriel de dimension 2 sur lequel l'action de F et celle de V sont toutes deux nilpotentes et l'action de J se fait à travers les caractères χ^{-2r} et $\chi^{-2r'}$</u> .

<u>Remarque</u> : Plus précisément, j'ai $M = \mathbb{F}_p.x \oplus \mathbb{F}_p.x'$, avec $g(x) = \chi^{-2r}(\hat{g})x$, $g(x') = \chi^{-2r'}(\hat{g})x'$,

$$Fx = \begin{cases} x' & \text{si } j' = 0 , \\ 0 & \text{sinon} ; \end{cases} \quad \text{et} \quad Fx' = \begin{cases} x & \text{si } j = 0 , \\ 0 & \text{sinon} ; \end{cases}$$

$$Vx = \begin{cases} x' & \text{si } j = (p-1)/2 , \\ 0 & \text{sinon} ; \end{cases} \quad \text{et} \quad Vx' = \begin{cases} x & \text{si } j' = (p-1)/2 , \\ 0 & \text{sinon} . \end{cases}$$

<u>Proposition</u>. - <u>Soit $U_{A'}$ un (A'/A)-groupe, tel que M est un $\mathbb{F}_p$-vectoriel de dimension 2 , avec action de F et V nilpotente, et action de J à travers les caractères χ^{-2s} et $\chi^{-2s'}$ avec s et s' des entiers vérifiants</u> $0 \leq s \leq s' < (p-1)/2$. <u>Alors l'action de G_o sur U se fait à travers les caractères χ_2^{i} et $\chi_2^{i'}$, avec</u> $i = 1 + 2s' + 2sp$ <u>et</u> $i' = p + 2s + 2s'p$.

<u>Démonstration</u>. - Comme F et V sont nilpotents, II.1 et II.2 impliquent qu'il n'y a pas de droite de U stable par G_o . On est donc dans la situation de la proposition précédente, avec des entiers i,i',j,j',r,r' convenables. Si r et r' sont définis modulo $(p-1)/2$, $r(p^2-1)$ et $r'(p^2-1)$ sont définis modulo $(p^2-1)(p-1)/2$, tout comme $i(p-1)/2$ et $i'(p-1)/2$ (puisque i et i' ne sont définis que modulo p^2-1). On peut donc choisir i et i' pour que $r = s$, $r' = s'$.

De $i.(p-1)/2 = j + pj' + s(p^2-1)$, on tire $i.(p-1)/2 = j + j' + (2j' + 2s(p+1)).(p-1)/2$, et $(p-1)/2$ divise donc $j+j'$. Comme $0 \leq j,j' \leq (p-1)/2$ et comme ($j = j' = 0$ ou $(p-1)/2$) entraîne que $p+1$ divise i , on a $j+j' = (p-1)/2$. D'où $i = 1 + 2j' + 2s(p+1)$.

De même $i' = 1 + 2j + 2s'(p+1) = 1 + (p-1) - 2j' + 2s'(p+1) =$ $p - 2j' + 2s'(p+1)$.

Comme $i' \equiv pi \pmod{(p^2-1)}$, on a

$$p - 2j' + 2s'(p+1) \equiv p + 2pj' + 2s(p+1) \pmod{(p^2-1)}$$ (car $p(p+1) \equiv p+1$ (mod ...)),

ou encore, en divisant par $2(p+1)$,

$$s' \equiv j' + s \pmod{(p-1)/2} ,$$

ou $j' \equiv s'-s \pmod{(p-1)/2}$.

Or $0 \leq j' \leq (p-1)/2$ et $0 \leq s'-s < (p-1)/2$. Donc $j' = s'-s$, sauf peut être si $s' = s$, où l'on peut avoir $j' = (p-1)/2$ et donc $j = 0$; Dans ce dernier cas, il suffit d'échanger i et i' ,donc j et j' , pour se ramener à $j' = s'-s$.

Finalement, $i = 1 + 2(s'-s) + 2s(p+1) = 1 + 2s' + 2sp$ et $i' = p - 2(s'-s) + 2s'(p+1) = p + 2s + 2s'p$.

III. Applications.

Dans la situation qui t'intéresse, comme on connaît $\det U$, il suffit d'informations très partielles sur le module galoisien M pour connaître U . Si tu n'aimes pas le module de Dieudonné, tu peux t'en passer parce que

- le noyau de V dans M s'identifie canoniquement à $\mathrm{Hom}(\underline{U}_{F_p}, G_a)$ et aussi à l'espace tangent du dual de $\underline{U}_{F_p}$;
- le quotient M/FM s'identifie canoniquement à l'espace cotangent de $\underline{U}_{F_p}$, et aussi à l'espace vectoriel des formes différentielles invariantes sur $\underline{U}_{F_p}$ (l'action de V étant alors l'opération de Cartier).

De l'examen des différentes possiblités, tu peux déduire alors des tas d'énoncés variés. Par exemple :

Soit k un entier pair $< p$ et soit $\underline{U}_{A'}$ un (A'/A)-groupe de type (p,p) . On suppose que G opère sur $\det U$ par χ^{k-1}

a) G_o opère sur U par χ_2^{k-1} et $\chi_2^{p(k-1)}$ dès que l'une des

<u>conditions suivantes est réalisée</u>

i) $\underline{U}_{\mathbb{F}_p}$ est connexe et il existe un élément non nul de l'espace tangent qui est invariant par J ;

ii) $\underline{U}_{\mathbb{F}_p}$ est connexe et il existe un élément non nul de l'espace tangent sur lequel J opère comme χ^{k-2} ;

iii) $\underline{U}_{\mathbb{F}_p}$ est connexe et J opère sur l'espace tangent à travers les caractères χ^{2s} et $\chi^{2s'}$, avec $0 \leq s \leq s' < (p-1)/2$ où s et s' appartiennent à une certaine liste qui est telle que la seule façon d'avoir $1+2s+2s' = k-1$ est $s = 0$, $2s' = k-2$ (e.g. $2s, 2s' \in \{0, k-2, p+1-k\}$, en excluant une ou deux valeurs de k pour chaque p).

b) <u>S'il existe</u> $a \in \mathbb{F}_p$ <u>tel que l'une des deux conditions suivantes est réalisée</u>

i) il existe une forme différentielle invariante non nulle ω de $\underline{U}_{\mathbb{F}_p}$ telle que $V\omega = a\omega$ et $g\omega = \chi^{p+1-k}(\hat{g})\omega$, pour tout $g \in$

ii) il existe un élément non nul φ de l'espace tangent du dual de $\underline{U}_{\mathbb{F}_p}$ qui est tel que $F\varphi = a\varphi$ et qui est invariant par J,

<u>Alors</u>

– <u>si</u> $a \neq 0$, $\quad U \sim \begin{pmatrix} \eta_{a^{-1}}\chi^{k-1} & ? \\ 0 & \eta_a \end{pmatrix}$,

– <u>si</u> $a = 0$, <u>l'action de</u> G_0 <u>sur</u> U <u>se fait par</u> χ_2^{k-1} <u>et</u> $\chi_2^{p(k-1)}$.

<u>Question</u> : Lorsque a_p est premier à p est-ce que Deligne sait que l'action de l'inertie est semi-simple ? Si oui, comment le sait-il ?

IV. – L'ingrédient essentiel de toute cette histoire est donc le papier de Raynaud et je ne me suis finalement pas servi de ma classification des schémas en groupes finis et plats sur A'. Celle-ci en revanche devrait être utile si on veut aller plus loin et regarder les groupes p-divisibles associés aux courbes modulaires.

Par exemple, dans la situation qui nous intéresse, et lorsque $a_p \equiv 0$ (mod p), le groupe $\underline{U}_{A'}$ se plonge dans un groupe p-divisible connexe de dim. 2 et hauteur 4 (en fait, bien sûr, "un $\mathbb{Q}_p$-groupe p-divisible qui acquiert bonne réduction sur K' "); c lui-ci n'est pas unique, mais il y en a un qui est plus beau que les autres.

Bien à toi,