Démonstration d'une conjecture de Lang dans des cas particuliers..

Jean-Pierre Wintenberger

Démonstration d'une conjecture de Lang dans des cas particuliers.

J.-P. Wintenberger

October 3, 2000

Soit $K \subset \overline{\mathbb{Q}}$ un corps de nombres. Soit G_K le groupe de Galois de $\overline{\mathbb{Q}}/K$. Soit A une variété abélienne définie sur K. Soit, pour tout nombre premier p, $T_p(A)$ le module de Tate de A et :

$$\underline{\rho}_p : G_K \to \mathrm{GL}_{\mathbb{Z}_p}(T_p(A))$$

la représentation p-adique associée. S. Lang a conjecturé que l'image du groupe de Galois dans la représentation adélique :

$$\underline{\rho} = \prod_p \underline{\rho}_p : G_K \to \prod_p \mathrm{GL}_{\mathbb{Z}_p}(T_p(A))$$

contient un sous-groupe ouvert des homothéties ([17]). J.-P. Serre a prouvé qu'il existe un entier $c > 0$ tel que toute homothétie qui est une puissance c-ième est dans l'image de Galois (cours au collège de France 85-86). Nous montrons cette conjecture de Lang lorsque A vérifie la conjecture de Mumford-Tate ou lorsque A est de dimension ≤ 4. Nous référons à [23] pour un point sur ce qui est connu sur la conjecture de Mumford-Tate. En fait, le théorème principal (th. 1) est une légère extension, d'ailleurs donnée comme vraisemblablement possible à prouver , des résultats du cours de J.-P. Serre au collège de France 85-86 (Remarque du 2.5. du résumé du cours). Nous reprenons les idées de la démonstration de J.-P. Serre. Le théorème 1 est très proche du résultat principal de M. Larsen ([18]). Il est plus précis en le sens qu'il concerne les nombres premiers sauf en nombre fini d'entre eux alors que le résultat de M. Larsen porte sur un ensemble de nombres premiers de densité 1. Le résultat de M. Larsen est plus général puisqu'il concerne les systèmes compatibles de représentations ℓ-adiques semi-simples qui ne proviennent

pas nécessairement de variétés abéliennes. M. Larsen n'utilise pas l'inertie modérée qui joue un grand rôle ici.

Je tiens à remercier M. Raynaud, M. Rapoport et J.-P. Serre en particulier pour les conversations que nous avons eues sur les groupes réductifs sur $\mathbb{Z}_p$.

1 Groupes réductifs sur $\mathbb{Z}_p$ ([8],[9]).

1.1

Soit $\underline{H}$ un schéma en groupes affine et lisse sur $\mathbb{Z}_p$. Notons H la fibre générique de $\underline{H}$ et $H(p)$ sa fibre spéciale. Rappelons que $\underline{H}$ est réductif si H et $H(p)$ sont des groupes réductifs, *i.e.* sont connexes et que leurs radicaux unipotents sont triviaux ([2] 11.21.).

Supposons qu'il en soit ainsi. Alors, comme $H(p)$ est quasi-déployé ([15] 35.2.) et comme la variété des sous-groupes de Borel de $\underline{H}$ est lisse ([9] exp. 22 cor. 5.8.3.), $\underline{H}$ possède un sous-groupe de Borel défini sur $\mathbb{Z}_p$. Il en résulte que H est quasi-déployé et que $\underline{H}$ est une forme tordue d'un schéma en groupes réductif déployé par un morphisme de $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ dans le groupe des automorphismes de son diagramme de Dynkin. Ce schéma en groupes déployé est obtenu par extension des scalaires de $\mathbb{Z}$ à $\mathbb{Z}_p$ d'un schéma en groupes déployé défini sur $\mathbb{Z}$ (schéma de Chevalley).

On note $(X, Y, R, \alpha \to \alpha^\vee, B)$ le système de racines muni d'une base associé à $\underline{H}$ (ou H)(voir par exemple [27]) : X est le groupe des caractères d'un tore maximal T de H défini sur $\overline{\mathbb{Q}_p}$, Y le groupe des cocaractères de T, $R \subset X$ les racines, $\alpha^\vee$ la racine duale de la racine α, et B une base de R associée à un sous-groupe de Borel contenant T. Le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ agit sur $(X, Y, R, \alpha \to \alpha^\vee, B)$. La donnée de cette action est équivalente à celle de l'action de $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ sur le le diagramme de Dynkin.

1.2

On note $\underline{S}$ le groupe dérivé de $\underline{H}$ et $\underline{S}_{sc}$ le revêtement universel de $\underline{S}$([9] exp. 22 6.2.). On note les fibres génériques en ne soulignant pas et les fibres spéciales par (p). On note $\underline{S}(\mathbb{Z}_p)_{\mathbf{u}}$, $S(\mathbb{Q}_p)_{\mathbf{u}}$ et $S(p)(\mathbb{F}_p)_{\mathbf{u}}$ les images de $\underline{S}_{sc}(\mathbb{Z}_p)$, $S_{sc}(\mathbb{Q}_p)$ et $S(p)_{sc}(\mathbb{F}_p)$ dans $\underline{S}(\mathbb{Z}_p)$, $S(\mathbb{Q}_p)$ et $S(p)(\mathbb{F}_p)$ respectivement. Le groupe $S(\mathbb{Q}_p)_{\mathbf{u}}$ est donc le noyau du

morphisme $H(\mathbb{Q}_p) \to H^0_{\mathbf{ab}}(\mathbb{Q}_p, H)$ défini dans [5]. Si $p > 3$, le groupe $S(p)(\mathbb{F}_p)_{\mathbf{u}}$ est le sous-groupe de $S(p)(\mathbb{F}_p)$ engendré par ses éléments unipotents et aussi le groupe dérivé de $S(p)(\mathbb{F}_p)$; il est égal à son groupe dérivé et, si $S(p)$ est simplement connexe, égal à $S(p)(\mathbb{F}_p)$ ([3] 6.5. et 6.6.).

Proposition 1 *On a :*

$$\underline{S}(\mathbb{Z}_p)_{\mathbf{u}} = S(\mathbb{Q}_p)_{\mathbf{u}} \cap \underline{S}(\mathbb{Z}_p).$$

Si l'ordre du centre de $S_{\mathbf{sc}}$ est premier à p, $\underline{S}(\mathbb{Z}_p)_{\mathbf{u}}$ est l'image réciproque de $S(p)(\mathbb{F}_p)_{\mathbf{u}}$ par le morphisme de réduction : $\underline{S}(\mathbb{Z}_p) \to S(p)(\mathbb{F}_p)$.

Démonstration. Comme $\underline{S}_{\mathbf{sc}} \to \underline{S}$ est fini, on a : $\underline{S}(\mathbb{Z}_p)_{\mathbf{u}} = S(\mathbb{Q}_p)_{\mathbf{u}} \cap \underline{S}(\mathbb{Z}_p)$.

Notons avec des indices $_1$ les noyaux des réductions modulo l'idéal maximal. Clairement, $S(p)(\mathbb{F}_p)_{\mathbf{u}}$ est l'image de $\underline{S}(\mathbb{Z}_p)_{\mathbf{u}}$ dans $S(p)(\mathbb{F}_p)$. Pour prouver la proposition, il suffit donc de prouver que, si le rang du noyau $\underline{C}$ de $\underline{S}_{\mathbf{sc}} \to \underline{S}$ est premier à p, le morphisme $\underline{S}_{\mathbf{sc}}(\mathbb{Z}_p)_1 \to \underline{S}(\mathbb{Z}_p)_1$ est surjectif. Soient $\overline{\mathbb{Q}_p}$ une clôture algébrique de $\mathbb{Q}_p$ et $\overline{\mathbb{Z}_p}$ la fermeture intégrale de $\mathbb{Z}_p$ dans $\overline{\mathbb{Q}_p}$. Montrons que le morphisme naturel : $\underline{S}_{\mathbf{sc}}(\overline{\mathbb{Z}_p})_1 \to \underline{S}(\overline{\mathbb{Z}_p})_1$ est un isomorphisme. Il est en effet surjectif car $\underline{S}_{\mathbf{sc}} \to \underline{S}$ est fini et fidèlement plat et que $\underline{C}(\overline{\mathbb{Z}_p}) \to \underline{C}(\overline{\mathbb{F}_p})$ est surjectif, puisque le schéma en groupes $\underline{C}$, de rang premier à p, est étale sur $\mathbb{Z}_p$. Il est injectif car $\underline{S}_{\mathbf{sc}}(\overline{\mathbb{Z}_p})_1$ est un pro-p-groupe et que $\underline{C}(\overline{\mathbb{Z}_p})$ est d'ordre premier à p. Prenant les invariants par $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, il en résulte que

$$\underline{S}_{\mathbf{sc}}(\mathbb{Z}_p)_1 \to \underline{S}(\mathbb{Z}_p)_1$$

est un isomorphisme, ce qui prouve la proposition.

1.3

Le théorème suivant et l'application que nous en donnons aux représentations galoisiennes associées aux variétés abéliennes est une variante de résultats de M. Larsen et R. Pink ([19] prop. 1.3. et th. 3.2.).

Théorème 1 *Soient H un groupe réductif sur $\mathbb{Q}_p$, $H \hookrightarrow \mathrm{GL}_V$ une représentation linéaire fidèle de H, T un tore maximal de H et L*

un réseau de V. On suppose que l'adhérence schématique $\underline{T}$ de T dans GL_L est un tore et que $\dim_{\mathbb{Q}_p}(V) \leq p$. Alors, l'adhérence schématique $\underline{H}$ de H dans GL_L est un groupe lisse sur $\mathbb{Z}_p$. Si de plus la fibre spéciale $H(p)$ de $\underline{H}$ agit de façon semi-simple sur L/pL, $\underline{H}$ est réductif sur $\mathbb{Z}_p$.

Démonstration.

Montrons que $\underline{H}$ est lisse sur $\mathbb{Z}_p$. Le tore T se déploie sur une extension non ramifiée F de $\mathbb{Q}_p$. Notons O_F l'anneau des entiers de F. Comme O_F est plat sur $\mathbb{Z}_p$, on voit facilement que $\underline{H}_{O_F}$ est l'adhérence schématique de $\underline{H}_F$ dans $\mathrm{GL}_{O_F \otimes L}$ et qu'il suffit de prouver que $\underline{H}_{O_F}$ est lisse sur O_F. Notons, pour chaque racine α de H relativement à T, U_α le sous-groupe unipotent associé à α. Le théorème 2.2.5. de [6] nous dit que $\underline{H}_{O_F}$ est lisse si nous prouvons que les adhérences schématiques de T_F et des $(U_\alpha)_F$ dans $\mathrm{GL}_{O_F \otimes L}$ sont lisses. Pour T_F, il en est ainsi par hypothèse. Prouvons le pour $(U_\alpha)_F$. Soit n un générateur de l'algèbre de Lie de $(U_\alpha)_F$ qui engendre le O_F module libre de rang un $O_F \otimes \mathrm{Lie}(U_\alpha) \cap \mathrm{End}(O_F \otimes L)$. Comme $\dim_{\mathbb{Q}_p}(V) \leq p$, on a $n^p = 0$, et $t \mapsto \exp(tn)$ définit un morphisme du groupe additif dans $\mathrm{GL}_{O_F \otimes L}$. Comme, dans une base de L, la matrice de $tn = \log(\exp(tn))$ a une coordonnée de la forme ut, avec u unité de O_F, on voit que $t \mapsto \exp(tn)$ est une immersion fermée. Cela prouve que l'adhérence schématique de $(U_\alpha)_F$ est bien lisse, et par suite aussi $\underline{H}$.

Si de plus, $H(p)$ agit de façon semi-simple sur L/pL, le radical unipotent de la composante neutre de $H(p)$ est trivial. Il résulte de la prop. 4.6.31. de [6] que $H(p)$ est connexe, et $\underline{H}$ est bien réductif sur $\mathbb{Z}_p$.

2 Enoncés.

2.1

On reprend les notations de l'introduction. Donc K est un corps de nombres et A une variété abélienne définie sur K. Pour p nombre premier, on note $V_p(A) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(A)$ le module de Tate tensorisé par $\mathbb{Q}_p$ de A et $\rho_p : G_K \to \mathrm{GL}_{\mathbb{Q}_p}(V_p(A))$ la représentation galoisienne associée. On note $H_{K,p}$ l'adhérence de Zariski de $\rho_p(G_K)$ dans le groupe linéaire $\mathrm{GL}_{V_p(A)}$. Notons $H^0_{K,p}$ la composante neutre de $H_{K,p}$. J.-P. Serre a prouvé que le noyau de $G_K \to H_{K,p}(\mathbb{Q}_p)/H^0{}_{K,p}(\mathbb{Q}_p)$

est indépendant de p ([31] 133 ; voir aussi [32], [33] et [20]). Soit K' le corps de nombres fixé par ce noyau. Remplaçant K par K', on peut supposer que $H_{K,p}$ est connexe, ce que nous supposerons désormais. Alors, pour tout corps de nombres K' contenant K, on a : $H_{K,p} = H_{K',p}$. Nous poserons $H_p = H_{K,p}$.

Un théorème de Bogomolov dit que H_p contient les homothéties et que $\underline{\rho}_p(G_K)$ contient un sous-groupe ouvert des homothéties ([1]). Un théorème de Faltings prouve que H_p est réductif et son commutant est $\mathbb{Q}_p \otimes \mathrm{End}(A)$ ([10]). Comme on a supposé que l'adhérence de Zariski de $\rho_p(G_K)$ est connexe, $\mathrm{End}(A) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$. Un théorème de Borovoi et Piatetski-Shapiro dit que H_p est contenu dans le groupe obtenu par extension des scalaires de $\mathbb{Q}$ à $\mathbb{Q}_p$ à partir du groupe de Mumford-Tate MT ([4], [24]).

Notons $\underline{H}_p$ l'adhérence de Zariski de $\underline{\rho}_p(G_K)$ dans $\mathrm{GL}_{T_p(A)}$. La fibre générique de $\underline{H}_p$ est donc H_p. On sait que, pour p grand, $\underline{H}_p$ est un groupe réductif sur $\mathbb{Z}_p$ ([19]). Cela résulte du théorème 1 ([19]). En effet, Y. Zarhin a prouvé que il existe un idéal premier $\mathcal{Q}$ de K tel que le tore de Frobenius $T_{\mathcal{Q}}$ soit un tore maximal des groupes H_p ([37]).De plus, pour p grand, $T_{\mathcal{Q}}$ se prolonge en un sous-tore de $\mathrm{GL}_{T_p(A)}$. Enfin, comme l'action de G_K sur le groupe $V(p)(A)$ des points d'ordre p de $A_{\overline{\mathbb{Q}}}$ est semi-simple avec comme commutant $\mathbb{F}_p \otimes \mathrm{End}(A)$, on voit facilement que l'action sur $V(p)(A)$ de la fibre spéciale $H(p)$ de $\underline{H}_p$ est semi-simple.

Notons $\underline{S}_p$ le groupe des commutateurs de $\underline{H}_p$ et soit $\underline{S}_p(\mathbb{Z}_p)_{\mathrm{u}}$ comme au 1.

Théorème 2 *Il existe un entier $p_?$ tel que, pour $p \geq p_?$, $\underline{\rho}_p(G_K)$ contient $\underline{S}_p(\mathbb{Z}_p)_{\mathrm{u}}$.*

(Nous employons la notation $p_?$ à plusieurs reprises dans l'article pour désigner des entiers qui peuvent être différents).

On sait que les ρ_p sont "presque linéairement indépendantes" ([31] 138, le lemme du 1.1. de *loc. cit.* est une conséquence du théorème ci-dessus): il existe un corps de nombres K' contenant K tel que :

$$\underline{\rho}(G_{K'}) = \prod_p \underline{\rho}_p(G_{K'}).$$

Il en résulte avec le théorème de Bogomolov, qu'il suffit, pour

prouver la conjecture de Lang, de prouver que pour p grand, $\underline{\rho}_p(G_K)$ contient le groupe des homothéties.

Le théorème de Bogomolov entraîne que $\underline{H}_p$ contient l'image du groupe à un paramètre des homothéties. Notons le $h_p : (\mathbb{G}_{\mathbf{m}})_{\mathbb{Z}_p} \to \underline{H}_p$. D'après la proposition 1, $\underline{S}(\mathbb{Z}_p)_{\mathbf{u}}$ est le noyau de la restriction à $\underline{H}_p(\mathbb{Z}_p)$ de $\rho_p^{\mathbf{ab}} : H_p(\mathbb{Q}_p) \to H^0_{\mathbf{a}b}(E, H_p)$. Notons $h_p^{\mathbf{ab}} : \mathbb{Z}_p^* \to H^0_{\mathbf{a}b}(E, H_p)$ le composé de h_p et de $\rho_p^{\mathbf{ab}}$. Le théorème ci-dessus entraîne que pour p grand, on a l'injection :

$$h_p(\mathbb{Z}_p^*) \ / \ (h_p(\mathbb{Z}_p^*) \cap \rho_p(G_K)) \ \hookrightarrow \ h_p^{\mathbf{ab}}(\mathbb{Z}_p^*) \ / \ (h_p^{\mathbf{ab}}(\mathbb{Z}_p^*) \cap \rho_p^{\mathbf{ab}}(G_K)).$$

Le corollaire 2.7.5. de [35] entraîne alors :

Corollaire 1 *Supposons que A vérifie la conjecture de Mumford-Tate ou que la dimension de A soit ≤ 4. Alors, il existe un entier $p_?$ tel que, pour $p \geq p_?$, $\underline{\rho}_p(G_K)$ contient les homothéties et A vérifie la conjecture de Lang.*

2.2 Remarque.

On voit facilement que la validité pour $p_?$ du théorème et du corollaire ne dépend que de la classe d'isogénie de A. Soit S un ensemble fini d'idéaux premiers de K. Comme d'après Faltings, il n'y a qu'un nombre fini de classes d'isogénie de variétés abéliennes définies sur K et ayant bonne réduction en dehors de S, on voit que les entiers $p_?$ ne dépendent que de K et de l'ensemble S des idéaux de mauvaise réduction de A. Pour pouvoir calculer des $p_?$ en fonction de K et de S, il faudrait pouvoir calculer des entiers $p_?$ vérifiant :

- 1) si $p \geq p_?$, il existe un idéal premier $\mathcal{Q}$ de K, qui n'est pas au dessus de p, et tel que le tore de Frobenius $T_{\mathcal{Q}}$ soit un tore maximal de H_p et que l' adhérence de Zariski de $T_{\mathcal{Q}}$ dans $\mathrm{GL}_{T_p(A)}$ soit un tore (l'existence d'un tel $p_?$ est assurée par [37]) ;

- 2) si $p \geq p_?$, le groupe de Galois G_K agit de façon semi-simple sur le noyau $V(p)(A)$ de la multiplication par p de A avec comme commutant $\mathbb{F}_p \otimes \mathrm{End}(A)$.

Il est possible que $p_?$ vérifiant 1) puisse être rendue effectif grâce à [28]. Pour 2), voir [21] où des bornes sont données en fonction de la hauteur de Faltings de A ; il est possible qu'en reprenant les exposés 7 et 8 de [34] on puisse obtenir des bornes en fonction de K et de S.

2.3

Esquissons une démonstration du théorème de J.-P. Serre.

Supposons que A a réduction semi-stable en tous les premiers de K. Notons h_p^{ab} le composé de $h_p : \mathbb{Z}_p^* \to H_p(\mathbb{Q}_p)$ avec $H_p(\mathbb{Q}_p) \to (H_p/S_p)(\mathbb{Q}_p)$ et ρ_p^{ab} le composé de ρ_p avec $H_p(\mathbb{Q}_p) \to (H_p/S_p)(\mathbb{Q}_p)$. Soit S_K le groupe de type multiplicatif défini dans [30] correspondant au modulus définissant les unités de K qui sont positives pour toutes les places réelles de K . Comme A a réduction semi-stable en tous les idéaux premiers de K, ρ_p^{ab} est non ramifiée hors de p. En les idéaux premiers de K au dessus de p, elle est semi-stable, donc cristalline puisqu'abélienne (3.1.4). Il en résulte que ρ_p^{ab} est le composé de la représentation universelle ([30]) $G_K \to S_K(\mathbb{Q}_p)$ et d'un morphisme $S_K(\mathbb{Q}_p) \to (H_p/S_p)(\mathbb{Q}_p)$ provenant d'un morphisme de groupes algébriques $S_K \to H_p/S_p$. Le groupe à un paramètre $w_K : \mathbb{G}_{\mathrm{m}} \to S_K$ donnant le poids ([30]) s'envoie par ce morphisme sur l'inverse de h_p^{ab}. Pour le vérifier, on se ramène au cas où A est absolument simple et, dans ce cas, on le fait en considérant la représentation abélienne $\wedge^{\max} V_p(A)$, la puissance extérieure étant prise relativement au centre de $\mathbb{Q} \otimes \mathrm{End}(A)$. Le corollaire 2.4. de [35] entraîne alors que si K est non ramifié au dessus de p, $h_p^{\mathrm{ab}}(\mathbb{Z}_p^*)$ est contenu dans l'image de G_K. On déduit du théorème 2 que, si c_p est un annulateur du quotient $\underline{S}(\mathbb{Z}_p)/\underline{S}(\mathbb{Z}_p)_{\mathrm{u}}$, l'image de Galois G_p contient les puissances c_p des homothéties : $h_p(\mathbb{Z}_p^*)^{c_p}$. Soit C_p le noyau de $S_{p,\mathrm{sc}} \to S_p$, On a un homomorphisme injectif du quotient $\underline{S}(\mathbb{Z}_p)/\underline{S}(\mathbb{Z}_p)_{\mathrm{u}}$ dans $H^1(\mathbb{Q}_p, C_p(\overline{\mathbb{Q}_p}))$. On voit donc que l'on peut prendre pour c_p un annulateur de C_p. Pour un entier a, notons $c(a)$ le plus petit commun multiple des annulateurs des groupes fondamentaux des sous-groupes semi-simples de $\mathrm{GL}_a(\mathbb{C})$. Si S est un sous-groupe algébrique simple de $\mathrm{GL}_a(\mathbb{C})$, le rang $\mathrm{rg}(S)$ de S est $\leq a-1$ et le cardinal du centre du revêtement universel de S est plus petit que $\mathrm{rg}(S)+1$ puisque les poids minuscules sont en bijection avec les éléments de ce centre qui ne sont pas égaux à l'identité. On voit alors facilement que $c(a)$ est plus petit que le plus petit commun multiple des $a' \leq a$. En paticulier, $H^1(\mathbb{Q}_p, C_p(\overline{\mathbb{Q}_p}))$ est annulé par un entier ne dépendant que de $\dim(A)$. On en déduit le théorème suivant dû à Serre:

Théorème 3 *(J.-P. Serre) Il existe un entier $c \geq 1$ tel que le groupe $\underline{\rho}(G_K)$ contienne toutes les homothéties dans $\widehat{\mathbb{Z}}^*$ qui sont des puis-*

sances c-ièmes.

On voit plus précisément que, pour p grand, G_p contient les puissances $c(2\dim(A))$-ièmes des homothéties, $c()$ comme ci-dessus.

3 Démonstrations.

3.1 Inertie modérée ([26]) ; le cas local.

3.1.1 Groupe de l'inertie modérée.

Soit F un corps valué discret complet de caractéristique 0 à corps résiduel parfait de caractéristique p. Soit $\overline{F}$ une clôture algébrique de F et notons G_F le groupe de Galois de $\overline{F}/F$. Notons k et $\overline{k}$ les corps résiduels de F et $\overline{F}$ respectivement. Notons I le sous-groupe d'inertie de G_F, $I_{\rm s}$ son sous-groupe sauvage, *i.e.* son p-Sylow, et $I_{\rm m} = I/I_{\rm s}$ son quotient modéré.

On sait que $I_{\rm m}$ s'identifie à $\varprojlim \mu_d$, μ_d désignant les racines de l'unité d'ordre d de $\overline{F}$, d parcourant les entiers premiers à p, $\mu_{d'} \to \mu_d$, pour d divisant d' étant l' élévation à la puissance d'/d. Le morphisme $I_{\rm m} \to \mu_d$ est le caractère de Kummer pour l'extension $F_{\rm nr}(\pi^{1/d})/F_{\rm nr}$, $F_{\rm nr}$ étant l'extension maximale non ramifiée de F et π étant une uniformisante de F. On peut aussi écrire $I_{\rm m}$ comme la limite projective des groupes μ_{p^r-1}, pour $r' \geq r$, le morphisme $\mu_{p^{r'}-1} \to \mu_{p^r-1}$ étant l'élévation à la puissance $(p^{r'}-1)/(p^r-1)$. La réduction modulo l'idéal maximal identifie μ_{p^r-1} au groupe multiplicatif du sous-corps k_r à p^r éléments du corps résiduel de $\overline{k}$ de $\overline{F}$. Le groupe $I_{\rm m}$ s'identifie au groupe limite projective des groupes k_r^*, les morphismes de transition étant induits par la norme.

Notons $T_r(p)$ le tore sur $\mathbb{F}_p$, obtenu par restriction des scalaires à la Weil de k_r à $\mathbb{F}_p$ à partir du groupe multiplicatif $\mathbb{G}_{\rm m}$ sur k_r. Donc, pour toute $\mathbb{F}_p$-algèbre A, $T_r(p)(A) = (k_r \otimes_{\mathbb{F}_p} A)^*$. En particulier, $T_r(p)(\mathbb{F}_p) = k_r^*$, d' où un isomorphisme $I_{\rm m} \simeq \varprojlim_r T_r(p)(\mathbb{F}_p)$, les morphismes de transition étant induits, pour $r' \geq r$, par la norme. On note $T_\infty(p) = \varprojlim_r T_r(p)$.

Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$. Les corps $\cup_r k_r$ et $\overline{\mathbb{F}_p}$ sont donc isomorphes. Choisissons un tel isomorphisme ι. Soit χ_r le caractère de $T_r(p)$ défini sur $\overline{\mathbb{F}_p}$ par le morphisme $T_r(p)(\overline{\mathbb{F}_p}) \simeq (k_r \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p})^* \to \overline{\mathbb{F}_p}^*$ défini par ι. Soit σ le Frobenius $x \mapsto x^p$ de $\overline{\mathbb{F}_p}$. Pour s

entier dans $[0, r-1]$, les $\sigma^s(\chi_r)$ forment une base du groupe abélien libre des caractères de $T_r(p)$ sur $\overline{\mathbb{F}_p}$.

3.1.2 Algébrisation des représentations de l'inertie modérée.

Soit δ une représentation de I dans un espace vectoriel U sur $\mathbb{F}_p$ de dimension finie.

Supposons tout d'abord δ simple. Alors, puisque le p-Sylow I_{s} de I est distingué, δ se factorise à travers I_{m}. Le commutant de I_{m} agissant sur U est un corps L, extension finie de $\mathbb{F}_p$. Notons r son degré sur $\mathbb{F}_p$. La représentation de I_{m} sur $\overline{\mathbb{F}_p} \otimes_{\mathbb{F}_p} U$ se décompose en une somme directe de r représentations $(\overline{\mathbb{F}_p} \otimes_{\mathbb{F}_p} U)_\tau$, de dimension 1, indexées par les différents plongements τ de L dans $\overline{\mathbb{F}_p}$, L agissant sur $(\overline{\mathbb{F}_p} \otimes_{\mathbb{F}_p} U)_\tau$ à travers le plongement τ. Le groupe I_{m} agit sur $(\overline{\mathbb{F}_p} \otimes_{\mathbb{F}_p} U)_\tau$ par un caractère $\theta_\tau : I_{\mathrm{m}} \to \overline{\mathbb{F}_p}^*$, dont l'image est contenue dans le sous-corps de $\overline{\mathbb{F}_p}$ à p^r éléments. Par l'isomorphisme ι de $\overline{\mathbb{F}_p}$ dans $\cup k_r$, on peut voir θ_τ comme un caractère de I_{m} dans k_r^*. Comme I_{m} est limite projective des groupes cycliques k_r^*, il existe un entier $a_\tau \in [0, p^r - 2]$, bien déterminé, tel que θ_τ soit le composé de la projection $\theta_r : I_{\mathrm{m}} \to k_r^*$ avec l'élévation à la puissance a_τ. Ecrivons a_τ en base p : $a_\tau = \sum_{s=0}^{r-1} a_{\tau,s} p^s$, les $a_{\tau,s}$ étant dans l'intervalle $[0, p-1]$ et n' étant pas tous égaux à $p-1$. Pour les différents τ (et un autre choix de ι (3.1.1)) , les suites $a_{\tau,s}$ se déduisent par permutations circulaires. On note $(a_s)_{0 \le s < r}$ la suite ainsi obtenue. Elle n'est définie qu' à permutation circulaire près, mais ainsi elle est indépendante du choix de l'isomorphisme ι entre $\cup_r k_r$ et $\overline{\mathbb{F}_p}$. Noter que la longueur r de la suite $(a_s)_{0 \le s < r}$ est égale à la dimension de U. L'irréductiblité de δ entraîne que l'image de θ_τ n'est pas contenue dans $k_{r'}$, pour $r' < r$ divisant r. On en déduit que $(a_s)_{0 \le s < r}$ n'est pas périodique de période $r' < r$ divisant r. L'entier r est appelé le *niveau* de δ (ou des caractères θ_τ). Les représentations irréductibles de I dans un $\mathbb{F}_p$-espace vectoriel de dimension r sont classées à isomorphisme près par les suites $(a_s)_{0 \le s < r}$ d'entiers dans l'intervalle $[0, p-1]$, non tous égaux à $p-1$, définies à permutation circulaire près, et n'admettant pas de période $r' < r$ divisant r.

Notons χ_τ le caractère de $T_r(p)$ défini par la formule :

$$\chi_\tau = \sum_{s=0}^{r-1} a_{\tau,s} \sigma^s(\chi_r).$$

On vérifie aisément que la représentation de $T_r(p)$ dans U qui a $(k_r \otimes_{\mathbb{F}_p} U)_\tau$ comme sous-espace propre de caractère χ_τ est définie sur $\mathbb{F}_p$. Composant avec la projection $T_\infty(p) \to T_r(p)$, on obtient une représentation $\delta^{\mathrm{alg}} : T_\infty(p) \to \mathrm{GL}_U$. La représentation δ^{alg} algébrise δ : si on la compose avec l'isomorphisme $I_{\mathrm{m}} \simeq T_\infty(p)(\mathbb{F}_p)$, on obtient δ. Elle est simple et de même commutant L que δ.

La représentation δ^{alg} est caractérisée parmi celles qui algébrise δ par la propriété suivante :

- si r' est un entier tel que δ^{alg} se factorise à travers $T_\infty(p) \to T_{r'}(p)$, les caractères de $T_{r'}(p)$ dans U ont, écrits dans la base $\sigma^s(\chi_{r'})$, $0 \leq s \leq r'-1$, des coordonnées dans l'intervalle $[0, p-1]$ et ne sont pas tous égaux à $p-1$.

Nous dirons que δ^{alg} est *restreinte*.

Si l'on suppose δ semi-simple, on définit, en décomposant δ en ses composantes simples, une représentation $\delta^{\mathrm{alg}} : T_\infty(p) \to \mathrm{GL}_U$ qui est caractérisée par le fait qu'elle algébrise δ et est restreinte.

Si l'on ne suppose pas δ semi-simple, on peut choisir une section du morphisme de groupes : $I \to I_{\mathrm{m}}$. On obtient une représentation de I qui se factorise à travers I_{m} à laquelle on peut associer une représentation de $T_\infty(p)$. Cette représentation est bien définie à conjugaison près par automorphisme du type $\mathrm{int}(\delta(\tau))$, pour $\tau \in I_{\mathrm{s}}$, puisqu'il en est ainsi de la section. En particulier les entiers a_i provenant des différentes composantes irréductibles et leurs multiplicités sont bien définis : ils sont appelés *les poids de l'inertie modérée* (le nombre des a_i comptés avec leurs multiplicités est la dimension de U).

Lemme 1 *Supposons δ semi-simple, donc que δ se factorise à travers I_{m}.*

a) Les points fixes, commutants, sous-espaces stables de δ et de δ^{alg} agissant sur U sont les mêmes.

b) Soit b un entier > 0. On suppose de plus que les poids de l'inertie modérée de δ sont $\leq b$ et que l'un d'entre eux est $< b$. Soit J un sous-groupe de I_{m} d'indice $< (p-1)/b$. Alors les points fixes, commutants, sous-espaces stables de δ, I_{m}, et de la restriction de δ à Jsont les mêmes.

c) On fait les mêmes hypothèses que dans b). Soit i un entier $< (p-1)/b$. Alors les deux représentations $\otimes^i(\delta^{\mathrm{alg}})$ et $(\otimes^i\delta)^{\mathrm{alg}}$ de T_∞ sur $\otimes^i U$ coïncident.

3.1.3

Démonstration. Les a) et c) résultent de la construction de δ^{alg} et du fait que si δ est simple, δ^{alg} l'est et δ et δ^{alg} ont même commutant. Pour le b), soit θ un caractère de I_{m} dans $\overline{\mathbb{F}_p}^*$ qui est de niveau r et dont les poids vérifie l'hypothèse de b). Soit $(a_s)_{0\leq s\leq r-1}$ la suite associée à θ. Soit e l'indice de J dans I_{m}. Soit F' une extension modérément ramifiée de F d'indice de ramification e. La restriction $\theta_{|J}$ de θ à J s'identifie à un caractère de l'inertie modérée de F'. On voit sans peine (*cf* 1.4. de [26]), que, comme les entiers $e\ a_s$ sont $\leq p-1$ et que l'un d'entre eux est $< p-1$, la suite d'entiers associée à $\theta_{|J}$ est la suite $(e\ a_s)_{0\leq s\leq r-1}$, le niveau de $\theta_{|J}$ étant encore r. Le b) du lemme en résulte si δ est simple, et le cas général s'en déduit aisément.

3.1.4 Représentations abéliennes et inertie modérée.

On suppose dans ce numéro que l'indice de ramification absolu de F est 1. Soit $\rho : I \to \mathrm{GL}_{\mathbb{Q}_p}(V)$ une représentation de G_F dans un $\mathbb{Q}_p$-espace vectoriel de dimension finie. On suppose que ρ est abélienne et cristalline. Il revient au même de supposer que ρ est abélienne et semi-stable puisqu'une représentation abélienne de Hodge-Tate est potentiellement cristalline ([27]), et qu'une représentation semi-stable et potentiellement cristalline est cristalline ([12]).

Soit, pour tout entier r, F_r l'extension non ramifiée de degré r de $\mathbb{Q}_p$, O_r l'anneau de ses entiers et $\underline{T}_r$ le tore sur $\mathbb{Z}_p$ obtenu par restriction des scalaires à la Weil de O_r à $\mathbb{Z}_p$ à partir du groupe multiplicatif sur O_r. Notons $\underline{T}_\infty$ le groupe proalgébrique $\varprojlim_r \underline{T}_r$, les morphismes de transition étant induits par la norme. Les réductions modulo p des tores $\underline{T}_r$ et $\underline{T}_\infty$ s'identifient aux tores $T_r(p)$ et $T_\infty(p)$ du 3.1.1. Si $\overline{\mathbb{Q}_p}$ est une clôture algébrique de $\mathbb{Q}_p$ dont le corps résiduel est $\overline{\mathbb{F}_p}$, les groupes des caractères de $\underline{T}_r$ définis sur $\overline{\mathbb{Q}_p}$ et de T_r définis sur $\overline{\mathbb{F}_p}$ s'identifient : c'est le groupe abélien libre engendré par les caractères $\sigma^s(\chi_r)$, pour $0 \leq s \leq r-1$.

Les groupes formels de Lubin et Tate pour les corps F_r fournissent une représentation de I dans $\underline{T}_\infty(\mathbb{Z}_p) \subset \underline{T}_\infty(\mathbb{Q}_p)$; on a une représentation linéaire ρ^{alg} de $(\underline{T}_\infty)_{\mathbb{Q}_p}$ dans V telle que ρ soit le composé de $I \to \underline{T}_\infty(\mathbb{Q}_p)$ et de $\rho^{\mathrm{alg}}(\mathbb{Q}_p) : \underline{T}_\infty(\mathbb{Q}_p) \to \mathrm{GL}_{\mathbb{Q}_p}(V)$ ([27]).

Lemme 2 *On suppose de plus que les poids de la décomposition de Hodge-Tate de ρ sont dans l'intervalle $[0, p-2]$. Soit L un réseau de V qui est stable sous l'action de G_K. Désignons par $\rho(p)$ la réduction modulo pL de ρ. Alors, $\rho(p)$ est modérément ramifiée, ρ^{alg} se prolonge en une représentation de $\varprojlim_r \underline{T}_r$ dans GL_L dont la réduction modulo p coïncident avec la représentation $\rho(p)^{\mathrm{alg}}$ définie dans 3.1.2.*

Démonstration. Soit r un entier tel que ρ^{alg} se factorise à travers $(\underline{T}_r)_{\mathbb{Q}_p}$. Soient χ_i les différents caractères de $(\underline{T}_r)_{\mathbb{Q}_p}$ qui interviennent dans ρ^{alg}. Les caractères χ_i définissent, par composition avec $F_r^* \simeq \underline{T}_r(\mathbb{Q}_p)$, des morphismes de F_r^* dans $\overline{\mathbb{Q}_p}^*$, et donc, par restriction, des morphismes de k_r^* dans le groupe multiplicatif du corps résiduel $\overline{\mathbb{F}_p}$ de $\overline{\mathbb{Q}_p}$. On les note $\chi_{i\ |k_r^*}$. Les poids pour la décomposition de Hodge-Tate sont les coordonnées des caractères apparaissant dans les χ_i dans la base formée des $\sigma^s(\chi_r)$, $0 \leq s \leq r-1$, du groupe des caractères de $(\underline{T}_r)_{\overline{\mathbb{Q}_p}}$ ([30]). Il résulte des hypothèses que ces coordonnées sont dans l'intervalle $[0, p-2]$. Il en résulte que les $\chi_{i\ |k_r^*}$ sont distincts. Soit $W(\overline{\mathbb{F}_p})$ l'anneau des vecteurs de Witt à coefficients dans $\overline{\mathbb{F}_p}$. On voit alors que les projecteurs de l'algèbre de groupe $W(\overline{\mathbb{F}_p})[k_r^*]$ donnent les projecteurs p_i sur sur les sous-espaces propres correspondant aux χ_i. Il en résulte que ρ^{alg} se prolonge en une représentation de $\underline{T}_r$ dans GL_L. On la note $\underline{\rho}^{\mathrm{alg}}$. La représentation $I \to \mathrm{GL}_{\mathbb{Z}_p}(L)$ coïncide avec le composé de $I \to \underline{T}_\infty(\mathbb{Z}_p)$ et de $\underline{\rho}^{\mathrm{alg}}(\mathbb{Z}_p)$. L'hypothèse sur les poids entraîne que la réduction modulo p de $\underline{\rho}^{\mathrm{alg}}$ est restreinte au sens de 3.1.2. Le lemme en résulte facilement.

3.2 Le cas global : représentation modulo p à poids de l'inertie modérée bornés. Le cas abélien.

3.2.1

Soit K un corps de nombres. Soit $p_?$ un nombre premier suffisamment grand pour que, pour p premier $\geq p_?$, le corps K soit non ramifié au dessus de p (pour $p_?$, voir la parenthèse suivant le théorème 2).

On note T_K le tore sur $\mathbb{Q}$ obtenu par restriction à la Weil de K à $\mathbb{Q}$ à partir du groupe multiplicatif sur K. Donc $T_K(\mathbb{Q}) = K^*$. On note S_K^0 le quotient de T_K par l'adhérence de Zariski du

groupe E_K^+ des unités de K qui sont positives en les places réelles de K : c'est la composante neutre du groupe algébrique abélien de type multiplicatif défini dans [30] pour le modulus 1. Soit $K_{\mathrm{nr}}^{\mathrm{ab}}$ l'extension maximale abélienne de K qui est non ramifiée en toute les places finies et K_p^{ab} l'extension maximale abélienne de K qui est non ramifiée en dehors de toutes les places finies qui ne sont pas au dessus de p. Soit $U_{K\otimes\mathbb{Q}_p}$ le produit des groupes des unités des complétés de K en les premiers de K au dessus de p. L'application de réciprocité définit un isomorphisme du quotient de $U_{K\otimes\mathbb{Q}_p}$ par le l'adhérence de E_K^+ dans le groupe de Lie p-adique $U_{K\otimes\mathbb{Q}_p}$ avec le groupe de Galois $\mathrm{Gal}(K_p^{\mathrm{ab}}/K_{\mathrm{nr}}^{\mathrm{ab}})$. Il en résulte une représentation $\mathrm{Gal}(K_p^{\mathrm{ab}}/K_{\mathrm{nr}}^{\mathrm{ab}}) \to S_K^0(\mathbb{Q}_p)$. On la note $\rho_{K,p}$.

Comme on a supposé K absolument non ramifié en p, les tores $(T_K)_{\mathbb{Q}_p}$ et $(S_K^0)_{\mathbb{Q}_p}$ se prolongent naturellement en des tores $\underline{T}_K$ et $\underline{S}_K^0$ sur $\mathbb{Z}_p$. La représentation $\rho_{K,p}$ est à valeurs dans $\underline{S}_K^0(\mathbb{Z}_p)$ et par réduction on obtient une représentation $\mathrm{Gal}(K_p^{ab}/K_{\mathrm{nr}}^{\mathrm{ab}}) \to S_K^0(\mathbb{F}_p)$. On la note $\rho_K(p)$.

Soit $\eta(p) : G_K \to \mathrm{GL}_U$ une représentation de G_K dans un $\mathbb{F}_p$-espace vectoriel de dimension finie qui est abélienne, non ramifiée hors de p, à image d'ordre premier à p. Notons $T_K(p)$ et $S_K^0(p)$ les réductions modulo p des tores $T_K(p)$ et $S_K^0(p)$. La représentation $\eta(p)$ est semi-simple, et de même sa restriction à $G_{K^{\mathrm{ab}}}$ et la représentation de $U_{K\otimes\mathbb{Q}_p}$ que l'on en déduit. Si O_K est l'anneau des entiers de K, cette dernière représentation se factorise à travers $(O_K \otimes \mathbb{F}_p)^*$. Les composantes simples de cette représentation de $(O_K \otimes \mathbb{F}_p)^*$ sont des produits tensoriels de représentations des groupes multiplicatifs des différents corps résiduels de K pour les premiers de K au dessus de p. On voit alors facilement que les algébrisations des restrictions de $\eta(p)$ aux groupes de décomposition en les idéaux premiers $\wp$ au dessus de p définissent une une représentation $\eta^{\mathrm{alg}}(p)$ de la réduction modulo $T_K(p)$ dans U.

La proposition suivante est une variante de la proposition 20 ' de [26] :

Proposition 2 *Soit b un entier > 0. Il existe $p_?$ (pour $p_?$, voir la parenthèse suivant le théorème 2) tel que , si p est un nombre premier $\geq p_?$, on ait la propriété suivante :*

Soit $\eta(p) : G_K \to \mathrm{GL}_U$ une représentation de G_K dans un $\mathbb{F}_p$-espace vectoriel de dimension finie qui, comme ci-dessus, est abélienne, non ramifiée hors de p, à image d'ordre premier à p. On

suppose de plus que les poids de l'inertie modérée pour les premiers au dessus de p sont dans l'intervalle $[0,b]$. Alors, $\eta^{\mathrm{alg}}(p)$ se factorise à travers $S_K^0(p)$.

Démonstration. Soient ϵ_r des générateurs, en nombre fini, du groupe abélien de type fini E_K^+. La théorie du corps de classes entraîne que les images des ϵ_r par $\eta^{\mathrm{alg}}(p)$ sont égales à 1. Soit χ un caractère de $T_K(p)$ dans $\overline{\mathbb{F}_p}$ qui intervient dans $\eta^{\mathrm{alg}}(p)$. Ecrivons χ comme $\sum n_\tau \tau$, τ décrivant les différents plongements de K dans $\overline{\mathbb{Q}_p}$, et les n_τ étant des entiers dans l'intervalle $[0,b]$. Les valuations p-adiques $v_p(\prod_\tau \tau(\epsilon_r)^{n_\tau} - 1)$ sont donc > 0. Soit K' la clôture galoisienne de K sur $\mathbb{Q}$. Prenons $p_?$ suffisamment grand pour que pour $p \geq p_?$, p ne divise pas les $N_{K'/\mathbb{Q}}(\prod_\tau \tau(\epsilon_r)^{n_\tau} - 1)$ qui ne sont pas nuls. Pour $p \geq p_?$, $v_p(\prod_\tau \tau(\epsilon_r)^{n_\tau} - 1) > 0$ entraîne que $\prod_\tau \tau(\epsilon_r)^{n_\tau} = 1$, donc que χ est un caractère de S_K^0. Cela prouve la proposition.

3.3 Le cas global : représentation modulo p à poids de l'inertie modérée bornés.

Soient d_0 et b deux entiers. Soit $\rho(p)$ une représentation de G_K dans un $\mathbb{F}_p$-espace vectoriel $V(p)$ vérifiant :

- a) la dimension d de $V(p)$ est $\leq d_0$;
- b) $\rho(p)$ est semi-simple ;
- c) pour tout premier $\mathfrak{Q}$ de K qui n'est pas au dessus de p, le sous-groupe d'inertie en $\mathfrak{Q}$ agit sur $V(p)$ à travers un quotient qui est un p-groupe ;
- d) pour tout premier $\wp$ de K au dessus de p, les poids de l'inertie modérée en $\wp$ sont dans l'intervalle $[0,b]$.

Si $\rho(p)$ est la semi-simplifiée du dual de la réduction modulo p de la cohomologie étale à coefficients dans $\mathbb{Z}_p$ d'une variété propre et lisse sur K, la propriété c) est satisfaite pour p grand et après restriction à une extension finie de K indépendante de p grâce à un théorème de A. J. de Jong [7] et la propriété d) pour p grand grâce à un théorème de J.-M. Fontaine et B. Messing ([13], voir aussi [11]).

Notons $G(p)$ l'image du groupe de Galois G_K dans $\mathrm{GL}_{\mathbb{F}_p}(V(p))$. Supposons $p \geq d$. Les exponentielles et logarithmes tronqués $e(z) = \sum_{i=0}^{p-1} z^i/i!$ et $l(z) = -\sum_{i=1}^{p-1} (1-z)^i/i$ définissent des bijections réciproques entre les ensembles des éléments unipotents et nilpotents de $\mathrm{GL}_{\mathbb{F}_p}(V(p))$. Pour u unipotent de $\mathrm{GL}_{\mathbb{F}_p}(V(p))$, on note e_u le morphisme de groupes algébriques $\mathbb{G}_{\mathrm{a}} \to \mathrm{GL}_{V(p)}$ défini par $t \mapsto e(tl(u))$.

Soit $N(p)$ le sous-groupe de $\mathrm{GL}_{V(p)}$ engendré par les images des e_u pour u unipotent de $G(p)$. Alors, M.V. Nori a prouvé qu'il existe une constante $c'(d)$ telle que, pour $p \geq c(d)$, $N(p)(\mathbb{F}_p)^+$ et $G(p)^+$ coïncident, $^+$ désignant le sous-groupe engendré par les éléments d'ordre p (voir aussi th.D de [14]). Si $N(p)$ est semi-simple et $p \geq 5$, $N(p)(\mathbb{F}_p)^+$ coïncide avec le groupe $N(p)(\mathbb{F}_p)_{\mathrm{u}}$ défini en 1. On suppose $p \geq c'(d_0)$.

Pour tout premier $\wp$ de K au dessus de p et tout prolongement $\overline{\wp}$ de $\wp$ à $\overline{\mathbb{Q}}$, on choisit une section du quotient modéré de l'inertie et l'on note $T_{\overline{\wp}}(p)$ l'image de la représentation du tore de l'inertie modérée pour $\overline{\wp}$, comme dans 3.1.2. Notons $G(p)^{\mathrm{alg}}$ le sous-groupe algébrique de $\mathrm{GL}_{V(p)}$ engendré par $N(p)$ et les $T_{\overline{\wp}}$. Ce groupe ne dépend pas du choix des sections, car deux telles sections diffèrent par automorphisme intérieur par l'image d'un élément de l'inertie sauvage, donc d'un élément de $N(p)(\mathbb{F}_p)$.

Théorème 4 *(Serre) Il existe un entier $p_?$ et un corps de nombres K', extension finie de K, ne dépendant que de K, d_0 et b tels que pour tout $\rho(p)$ comme ci-dessus avec $p \geq p_?$:*

- $G(p)^{\mathrm{alg}}$ est un groupe réductif et $N(p)$ est son sous-groupe des commutateurs ;

- $\rho(p)(G_{K'})$ est contenu dans $G(p)^{\mathrm{alg}}(\mathbb{F}_p)$, et contient $N(p)(\mathbb{F}_p)^+ = N(p)(\mathbb{F}_p)_{\mathrm{u}}$;

- la représentation $\eta(p) : G_{K'} \to (G(p)^{\mathrm{alg}}/N(p))(\mathbb{F}_p)$ est non ramifiée en dehors de p. On a un morphisme surjectif $\eta(p)^{\mathrm{alg}}$ de $S^0_{K'}(p)$ sur le tore $G(p)^{\mathrm{alg}}/N(p)$ qui algébrise $\eta(p)$ en ce sens que la restriction de $\eta(p)$ au groupe de Galois de $K'^{\mathrm{ab}}_{\mathrm{nr}}$ coïncide avec le composé de $\rho_K(p)$ (3.2) et de $\eta(p)^{alg}(\mathbb{F}_p)$.

Remarque. Le morphisme $\eta(p)^{\mathrm{alg}}$ est caractérisé par le fait qu'il algébrise $\eta(p)$ et la propriété suivante.

Soit $C(p)^0$ la composante neutre du centre de $G(p)^{\mathrm{alg}}$. Il n'est pas difficile de voir que le noyau du morphisme surjectif de tores $C(p)^0 \to G(p)^{\mathrm{alg}}/N(p)$ est annulé par un entier qui ne dépend que de d_0. En effet, si $\rho(p)$ est simple, son commutant L est une extension finie de $\mathbb{F}_p$, $C(p)^0$ agit sur $V(p)$ à travers le groupe multiplicatif de L. Le groupe $G(p)^{\mathrm{alg}}$ agit à travers $G(p)^{\mathrm{alg}}/N(p)$ sur la représentation déterminant $\wedge_L^{\max} V(p)$. Il en résulte que le noyau de $C(p)^0 \to G(p)^{\mathrm{alg}}/N(p)$ est annulé par d si $\rho(p)$ est simple.

Il en résulte qu'il existe un entier f ne dépendant que de d_0 tel que le morphisme $S_K^0 \to G(p)^{\mathrm{alg}}/N(p)$, suivi de l'élévation à la puissance f, se relève en un morphisme η' de S_K^0 dans $C(p)^0$.

La propriété supplémentaire qui caractérise $\eta(p)^{\mathrm{alg}}$ est que les représentations des tores de l'inertie modérée pour les premiers de K' au dessus de p induites par η' sont restreintes au sens de 3.1.2. Ceci résulte de la démonstration ci-dessous et du c) du lemme 1.

Démonstration du théorème.

3.3.1

Comme $G(p)_{\mathrm{u}}$ est distingué dans $G(p)$, l'action de $G(p)_{\mathrm{u}} = N(p)(\mathbb{F}_p)_{\mathrm{u}}$ est aussi semi-simple, donc aussi celle de $U(\mathbb{F}_p)$, où U est le radical unipotent de $N(p)$. Comme $U(\mathbb{F}_p)$ est un p-groupe, il en résulte que $U(\mathbb{F}_p)$ est trivial. Le groupe unipotent U est par suite trivial, car, s'il ne l'était pas, il contiendrait un sous-groupe isomorphe à $\mathbb{G}_{\mathrm{a}}$, et donc $U(\mathbb{F}_p)$ ne serait pas trivial. Puisque $N(p)$ est engendré par des sous-groupes isomorphes à $\mathbb{G}_{\mathrm{a}}$ et que son radical unipotent est trivial, $N(p)$ est un groupe semi-simple.

Lemme 3 *Soit $N(p)$ un groupe semi-simple sur $\mathbb{F}_p$ et une représentation linéaire fidèle de $N(p)$ dans $(\mathrm{GL}_d)_{\mathbb{F}_p}$. On suppose que $p \geq d$ et que $N(p)$ est engendré par les images des e_u, pour u unipotent de $N(p)(\mathbb{F}_p)$. Alors, il existe un groupe semi-simple $\underline{N}$ sur $\mathbb{Z}_p$ et une représentation linéaire fidèle de $\underline{N}$ dans $(\mathrm{GL}_d)_{\mathbb{Z}_p}$ dont la réduction modulo p est $N(p) \hookrightarrow (\mathrm{GL}_d)_{\mathbb{F}_p}$.*

Démonstration. On se ramène immédiatement au cas où la représentation linéaire de $N(p)$ est simple. Elle est alors isomorphe à la représentation obtenue par restriction des scalaires à partir d'une représentation absolument irréductible sur une extension finie k de $\mathbb{F}_p$. Cette représentation a un plus haut poids λ et est isomorphe à la représentation $L(\lambda)$ définie dans le 2.2. de [16]. Soit $\lambda = \sum_{i=1}^{r} p^i \lambda_i$, avec les λ_i p-restreints ([16]) et $\lambda_r \neq 0$. D'après un théorème de Steinberg, on a : $L(\lambda) = \otimes_i L(\lambda_i)^{[i]}$, $L(\lambda_i)^{[i]}$ étant $L(\lambda_i)$ composée avec la puissance i-ième du Frobenius. Il existe un morphisme e_u dont l'image dans $L(\lambda_r)^{[r]}$ est non triviale. Le morphisme $e_u : \mathbb{G}_{\mathrm{a}} \to L(\lambda_r)^{[r]}$ est de degré non nul et une puissance p^r-ième. Comme e_u est de degré $< p$, c'est que $r = 1$ et λ est p-restreint. Soit $N(p)_j$ une composante simple de $N(p)$ et λ_j le plus haut poids de la restriction de $N(p)$ à $N(p)_j$. Comme λ est p-restreint, λ_j l'est. Comme

$L(\lambda)$ est de dimension $\leq p$, il en est de même de $L(\lambda_j)$. Il résulte alors des propositions 3 et 5 de [29] que λ_j est dans la petite alcôve. La proposition 5.6. de la partie 2 de [16] dit que λ_j se relève aux vecteurs de Witt à coefficients dans le corps fini k. Le lemme s'en déduit aisément.

3.3.2

On sait qu'il n'existe qu'un nombre fini de classes d'isomorphisme de système de racines R , muni d'un groupe cyclique C d'automorphismes de son diagramme de Dynkin, d'ensemble de poids dominants Ω (avec multiplicités) stable par C, tels que la représentation V du groupe semi-simple simplement connexe S de système de racines R (sur un corps algébriquement clos de caractéristique 0) associée à Ω soit de dimension d. Il en résulte qu'il existe une constante $c(d)$ telle que l'image S' du groupe S dans GL_V soit caractérisée par ses invariants tensoriels de degré $\leq c(d)$. Il résulte alors du lemme 3 qu'il existe des constantes $c_1(d)$ et $c_2(d)$ telles que pour $p \geq c_1(d)$, le groupe $N(p)$ soit caractérisé par ses invariants tensoriels de poids $\leq c_2(d)$, *i.e.* il existe $c \leq c_2(d)$ et un sous $\mathbb{F}_p$-espace vectoriel $W(p)$ de $\otimes^c V(p)$ tels que $N(p)$ soit le sous-groupe de $\mathrm{GL}_{V(p)}$ qui fixe les éléments de $W(p)$. On peut de plus supposer que $W(p)$ soit le sous-espace vectoriel de $\otimes^c V(p)$ formé des éléments de $\otimes^c V(p)$ qui sont fixés par $N(p)$. L'image $G(p)$ de G_K dans $\mathrm{GL}_{\mathbb{F}_p}(V(p))$ agit sur $\otimes^c V(p)$ en laissant stable $W(p)$, puisque $G(p)$ normalise $N(p)$. Soit $T_{\overline{\varphi}}$ un tore de l'inertie modérée comme dans l'énoncé du théorème. Comme les poids de l'inertie modérée agissant sur $\otimes^c V(p)$ sont bornés indépendamment de p, il résulte du lemme 1 que, si p est suffisamment grand, grand, le tore $T_{\overline{\varphi}}$ laisse stable $W(p)$. Il en résulte que $T_{\overline{\varphi}}$ normalise $N(p)$ et $N(p)$ est bien distingué dans $G(p)^{\mathrm{alg}}$.

L'action de $G(p)^{\mathrm{alg}}/N(p)$ sur $W(p)$ est fidèle. On note $\eta(p)$ la représentation de G_K dans $W(p)$. Il est clair que $\eta(p)(G_K)$ est d'ordre premier à p. Les sous-groupes d'inertie pour les premiers de K qui ne sont pas au dessus de p agissant sur $V(p)$ à travers un p-groupe, la représentation $\eta(p)$ est non ramifiée hors de p.

Lemme 4 *Soit K un corps de nombres. Soient d_1 et b deux entiers. Alors, il existe un entier p_0 et un corps de nombres K' extension finie de K vérifiant la propriété suivante. Soient $p \geq p_0$ est un nombre premier, et $\eta(p) : G_K \to \mathrm{GL}_{\mathbb{F}_p}(U)$ est une représentation de G_K*

dans un $\mathbb{F}_p$-espace vectoriel U de dimension $\leq d_1$ vérifiant :

a) $\eta(p)$ n'est ramifiée qu'au dessus de p ;

b) $\eta(p)(G_K)$ est d'ordre premier à p ;

c) d' après b), pour tout idéal premier $\wp$ de K au dessus de p, la restriction de $\eta(p)$ au sous-groupe d'inertie en $\wp$ est modérée. On suppose que les poids de l'inertie modérée sont bornés par b.

Alors, la restriction de $\eta(p)$ au groupe de Galois $G_{K'}$ est abélienne. On a une représentation $\eta(p)^{\mathrm{alg}}$ de $S^0_{K'}$ dans U qui est caractérisée par les deux propriétés suivantes :

- elle algébrise $\eta(p)$ en le sens que restriction de $\eta(p)$ à $\mathrm{Gal}(K'^{\mathrm{ab}}_p/K'^{\mathrm{ab}}_{\mathrm{nr}})$ coïncide avec le composé de $\rho_K(p)$ et de $\eta(p)^{\mathrm{alg}}(\mathbb{F}_p)$,

- les représentations des tores de l'inertie modérée pour les idéaux premiers de K' au dessus de p qu'elle définit par composition avec le morphisme $T_{K'}(p) \to S^0_{K'}$ sont restreintes au sens de 3.1.2.

Démonstration. Comme $\dim_{\mathbb{F}_p}(U) \leq d_1$ et $\eta(p)(G_K) \subset \mathrm{GL}_{\mathbb{F}_p}(U(p))$ est d'ordre premier à p, il résulte d'un théorème de Jordan qu'il existe une constante c (ne dépendant que de d_1) telle que pour tout p, $\eta_p(G_K)$ contienne un sous-groupe distingué abélien J d'indice $\leq c$. Soient $\wp$ et $\wp'$ deux idéaux premiers de K au dessus de p, $\overline{\wp}$ et $\overline{\wp'}$ des prolongement de $\wp$ et $\wp'$ respectivement à $\overline{\mathbb{Q}}$. Soit $I_{\overline{\wp}}$ le sous-groupe d'inertie en $\overline{\wp}$, et de même $I_{\overline{\wp'}}$. Comme J est abélien, les éléments de $\eta(p)(I_{\overline{\wp}}) \cap J$ commutent aux éléments de J. Il résulte de l'hypothèse c) et du lemme 1, que, pour $p > bc+1$, les éléments de $\eta(p)(I_{\overline{\wp}})$ commutent aux éléments de J. Ils commutent donc aux éléments de $\eta(p)(I_{\overline{\wp'}}) \cap J$. Appliquant de nouveau le lemme 1, on voit que $\eta(p)(I_{\overline{\wp}})$ et $\eta(p)(I_{\overline{\wp'}})$ commutent. Il en résulte que, pour $p > bc+1$, les images par $\eta(p)$ des différents sous-groupes d'inertie au-dessus de p et J engendrent un groupe commutatif. Soit, pour $p > bc+1$, $K_{\eta(p)}$ l'extension de K fixée par l'image réciproque par $\eta(p)$ de ce sous-groupe. Le degré de $K_{\eta(p)}/K$ est $\leq c$; $K_{\eta(p)}/K$ est non ramifiée. Il en résulte que les $K_{\eta(p)}$ sont contenues dans une même extension finie K_1 de K. On peut prendre pour K' l'extension maximale abélienne non ramifiée de K_1, et $p_0 = bc+1$. Le lemme résulte alors de la proposition 2.

Achevons de prouver le théorème. On prend pour K' le corps $K'^{\mathrm{ab}}_{\mathrm{nr}}$ donné par le lemme précédent et p suffisamment grand. Soit H le normalisateur de $N(p)$ dans $\mathrm{GL}_{V(p)}$. Donc H s'identifie au stabilisateur de $W(p)$ dans $\otimes^c V(p)$ et la représentation de $H/N(p)$ dans $W(p)$ est fidèle. On a vu que $G(p)^{\mathrm{alg}}$ est inclus dans H. Le c)

du lemme 1 entraîne que l'image de $G(p)^{\mathrm{alg}}/N(p)$ dans $\mathrm{GL}_{W(p)}$ est engendrée par les différents tores de l'inertie modérée au dessus de p agissant sur $W(p)$, donc avec l'image de $\eta(p)^{\mathrm{alg}}$. C'est en particulier un tore. Le groupe algébrique $G(p)^{\mathrm{alg}}$, extension d'un tore par le groupe semi-simple $N(p)$, est réductif. Comme l'image de $G_{K'}$ dans $\mathrm{GL}_{\mathbb{F}_p}(W(p))$ est contenue dans celle de $\eta(p)^{\mathrm{alg}}$, on voit que l'image de $G_{K'}$ dans $\mathrm{GL}_{\mathbb{F}_p}(V(p))$ est contenue dans $G(p)^{\mathrm{alg}}(\mathbb{F}_p)$. Pour p grand, p ne divise pas $[K' : K]$, ce qui entraîne que les éléments d'ordre p de $\rho(p)(G_{K'})$ engendrent $N(p)(\mathbb{F}_p)^+$ et $\rho(p)(G_{K'})$ contient $N(p)(\mathbb{F}_p)^+$. Le lemme ci-dessus entraîne la dernière assertion du théorème.

3.4 Fin de la démonstration du théorème 2

On peut changer K par une extension finie et supposer p grand et que A est absolument simple.

D'après G. Faltings et Y. Zarhin, on peut supposer que la réduction $\rho(p)$ de ρ_p de modulo p est semi-simple ([10], [36]). D'après M. Larsen et R. Pink, on peut donc supposer que l'adhérence de Zariski $\underline{H}_p$ de $\rho_p(G_K)$ dans $\mathrm{GL}_{T_p(A)}$ est réductive ([19]). On peut supposer que p est assez grand pour que le théorème 4 s'applique, puisque les poids de l'inertie modérée au dessus de p sont 0 et 1 d'après M. Raynaud ([25]). On change K en le corps K' donné par le théorème.

Lemme 5 *Notons $\underline{H}_p(p)$ la réduction modulo p de $\underline{H}_p$. Alors, $\underline{H}_p(p)$ coïncide avec $G(p)^{alg}$.*

Démonstration. Montrons tout d'abord que les composantes connexes des centres C et C' de $\underline{H}_p(p)$ et $G(p)^{alg}$ respectivement coïncident. En effet soit L le centre de l'algèbre $\mathrm{End}(A)$ des endomorphismes de A. D'après G. Faltings et Y. Zarhin, le commutant de $\rho(p)$ est $\mathrm{End}(A) \otimes \mathbb{F}_p$. On voit alors que le commutant de $G(p)^{\mathrm{alg}}$ est $\mathrm{End}(A) \otimes \mathbb{F}_p$. Pour p grand, le centre de $\mathrm{End}(A) \otimes \mathbb{F}_p$ est $L \otimes \mathbb{F}_p$. Les tores C et C' sont des sous-tore du tore des éléments inversibles de L/pL. Comme on a supposé A simple et que p est grand, $T_p(A)$ est un module libre sur $\mathbb{Z}_p \otimes L$. Soient $\wedge^{\max} T_p(A)$ et $\wedge^{\max} V(p)(A)$ les puissances extérieures maximales des $\mathbb{Z}_p \otimes L$ et L/pL-modules libres $T_p(A)$ et $V(p)(A)$ respectivement ($V(p)(A)$ désignant le noyau de la multiplication par p dans A). Puisque l'action du groupe multiplicatif de L/pL sur $\wedge^{\max} V_p(A)$ se fait à travers une isogénie, il suffit de prouver que les images des tores C et C' agissant sur

$\wedge^{\max}V(p)(A)$ coïncident. Ce sont les images de $\underline{H}_p(p)$ et $G(p)^{alg}$ agissant sur $\wedge^{\max}V(p)(A)$. La restriction à $K_{\mathrm{nr}}^{\mathrm{ab}}$ de la représentation abélienne de G_K sur $\wedge^{\max}T_p(A)$ s'algébrise en une représentation de $\underline{S}_K^0$ dans $\wedge^{\max}T_p(A)$, dont l'image coïncide avec celle de $\underline{H}_p$. La proposition 2 entraîne que la réduction modulo p de la représentation de $\underline{S}_K^0$ sur $\wedge^{\max}T_p(A)$ coïncide avec la représentation de $\underline{S}_K^0(p)$ sur $\wedge^{\max}V(p)(A)$ donnée par le morphisme $\underline{S}_K(p) \to G(p)^{\mathrm{alg}}/N(p)$. On a donc bien que $C = C'$.

Prouvons que le groupe $G(p)^{alg}$ est contenu dans $\underline{H}_p(p)$. Comme les composantes connexes des centres coïncident, il suffit de prouver que $N(p)$ est contenu dans $\underline{H}_p(p)$. Le groupe $\underline{H}_p(p)(\mathbb{F}_p)$ contient l'image de $\rho(p)$. Le groupe $N(p)$ est engendré par les images des groupes à un paramètre $t \mapsto e(t\ l(u))$, pour u unipotent de l'image de $\rho(p)$. Comme $N(p)$ est la réduction modulo p d'un groupe semi-simple sur $\mathbb{Z}_p$, l'inclusion $N(p) \subset \underline{H}_p(p)$ résulte du lemme :

Lemme 6 *Soit d un entier. Alors, il existe un premier $p_?$ vérifiant la propriété suivante. Soit p un premier $\geq p_?$. Soit $\underline{S}$ un groupe semi-simple sur $\mathbb{Z}_p$ et une représentation linéaire fidèle $\underline{S} \hookrightarrow (\mathrm{GL}_d)_{\mathbb{Z}_p}$ (morphisme de schémas en groupes qui est une immersion fermée). Soit $u \in \underline{S}(\mathbb{F}_p)$. Alors l'image du groupe à un paramètre $t \mapsto e(t\ l(u))$ est contenue dans $\underline{S}$.*

Démonstration. Comme il n'existe qu'un nombre fini de classes d'isomorphie de couples formé d'un groupe semi-simple et d'une représentation linéaire fidèle de dimension d sur un corps de caractéristique 0, il existe un premier $p_?$ et une constante D telle que, pour $p \geq p_?$, la réduction $\underline{S}(p)$ de $\underline{S}$ modulo p soit définie dans $(\mathrm{GL}_d)_{\mathbb{F}_p}$ par des équations de degré $\leq D$. Pour $p \geq 2d+1$ et a entier, $0 \leq a \leq p-1$, on a $e(a\ l(u)) = u^a \in \underline{S}(p)(\mathbb{F}_p)$, donc l'équation de degré $\leq (d-1)\ D$ qui exprime que $e(t\ l(u)) \in \underline{S}$ a au moins p solutions. Pour $p > (d-1)\ D$, cela entraîne qu'elle est nulle, et cela prouve le lemme.

3.4.1

Les groupes $G(p)^{alg}$ et $\underline{H}_p(p)$ ont mêmes rangs ([31] 137 Théorème 2). Ils ont mêmes commutants : $\mathrm{End}(A) \otimes \mathbb{F}_p$. En effet, comme $G(p)^{alg}(\mathbb{F}_p)$ contient l'image de Galois, le commutant de $G(p)^{alg}$ est contenu dans $\mathrm{End}(A) \otimes \mathbb{F}_p$, et il est clair que $\underline{H}_p(p)$ commute à

$\mathrm{End}(A) \otimes \mathbb{F}_p$. L'égalité $G(p)^{\mathrm{alg}} = \underline{H}_p(p)$ résulte alors du lemme suivant, qui est une variante d'un lemme bien connu :

Lemme 7 *Soient $G_1 \subset G_2$ deux groupes réductifs sur un corps parfait k. On suppose que G_1 et G_2 ont mêmes rangs. On suppose de plus que l'on a une représentation linéaire fidèle $G_2 \hookrightarrow \mathrm{GL}_U$ de G_2 telle que les centres des commutants de G_1 et de G_2 dans U soient la même k-algèbre ; on suppose que cette k-algèbre commutative C est semi-simple. On suppose que la caractéristique de k est 0 ou ≥ 5. Alors $G_1 = G_2$.*

Démonstration. Soit T un tore maximal de G_1. C'est aussi un tore maximal de G_2. Comme k est parfait et que C est semi-simple, le groupe multiplicatif de C définit un tore que nous noterons C^*. Les centres de G_1 et G_2 coïncident : ils sont l'intersection de T avec C^*. Soient $S_1 \subset S_2$ les groupes des commutateurs de G_1 et G_2 et $R_1 \subset R_2$ les racines de S_1 et S_2 relativement à T. Comme les centres de G_1 et G_2 coïncident, les groupes engendrés par R_1 et R_2 dans le groupe des caractères de T coïncident. Les racines R_1 forment un sous-ensemble symétrique et, puisque $p > 3$ et d'après SGA 3 exp. 23 cor. 6.6., clos dans R_2. D'après Bourbaki Groupes et Algèbres de Lie chap. 6 1 prop. 23, on a $R_1 = R_2$, donc $S_1 = S_2$ et $G_1 = T \times S_1 = T \times S_2 = G_2$. Cela prouve le lemme.

3.4.2

Achevons la démonstration du théorème 4.

Le groupe des commutateurs $[\rho_p(G_K), \rho_p(G_K)]$ de l'image de Galois est un sous-groupe de $\underline{S}_p(\mathbb{Z}_p)_{\mathrm{u}}$ dont la réduction modulo p contient $N(p)(\mathbb{F}_p)_{\mathrm{u}} = \underline{S}_p(\mathbb{F}_p)_{\mathrm{u}}$. Soit Γ son image réciproque dans $\underline{S}_{p,\mathrm{sc}}(\mathbb{Z}_p)$. L'image de Γ dans $\underline{S}_{p,\mathrm{sc}}(\mathbb{F}_p)$ est $\underline{S}_{p,\mathrm{sc}}(\mathbb{F}_p)$ tout entier. La proposition 2.6. de [18] entraîne que, pour p grand, Γ coïncide avec $\underline{S}_{p,\mathrm{sc}}(\mathbb{Z}_p)$ et donc $[\rho_p(G_K), \rho_p(G_K)]$ avec $\underline{S}_p(\mathbb{Z}_p)_{\mathrm{u}}$. Cela achève de prouver le théorème.

References

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

[2] Armand Borel. *Linear algebraic groups*. Springer-Verlag, New York, second edition, 1991.

[3] Armand Borel and Jacques Tits. Homomorphismes "abstraits" de groupes algébriques simples. *Ann. of Math. (2)*, 97:499–571, 1973.

[4] M. V. Borovoĭ. The action of the Galois group on the rational cohomology classes of type (p, p) of abelian varieties. *Mat. Sb. (N.S.)*, 94(136):649–652, 656, 1974.

[5] Mikhail Borovoi. Abelian Galois cohomology of reductive groups. *Mem. Amer. Math. Soc.*, 132(626), 1998.

[6] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. II. Schémas en groupes. Existence d'une donnée radicielle valuée. *Inst. Hautes Études Sci. Publ. Math.*, (60):197–376, 1984.

[7] A. J. de Jong. Smoothness, semi-stability and alterations. *Inst. Hautes Études Sci. Publ. Math.*, (83):51–93, 1996.

[8] Michel Demazure. Schémas en groupes réductifs. *Bull. Soc. Math. France*, 93:369–413, 1965.

[9] Michel Demazure and Alexander Grothendieck. *Schémas en groupes. III: Structure des schémas en groupes réductifs*. Springer-Verlag, Berlin, 1962/1964. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 153.

[10] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[11] Gerd Faltings. Crystalline cohomology and p-adic Galois-representations. In *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 25–80. Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[12] Jean-Marc Fontaine. Représentations p-adiques semi-stables. *Astérisque*, (223):113–184, 1994. With an appendix by Pierre Colmez, Périodes p-adiques (Bures-sur-Yvette, 1988).

[13] Jean-Marc Fontaine and William Messing. p-adic periods and p-adic étale cohomology. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, pages 179–207. Amer. Math. Soc., Providence, RI, 1987.

[14] Robert M. Guralnick. Small representations are completely reducible. *J. Algebra*, 220(2):531–541, 1999.

[15] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[16] Jens Carsten Jantzen. *Representations of algebraic groups*. Academic Press Inc., Boston, MA, 1987.

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

[18] M. Larsen. Maximality of Galois actions for compatible systems. *Duke Math. J.*, 80(3):601–630, 1995.

[19] M. Larsen and R. Pink. Abelian varieties, l-adic representations, and l-independence. *Math. Ann.*, 302(3):561–579, 1995.

[20] Michael Larsen and Richard Pink. A connectedness criterion for l-adic Galois representations. *Israel J. Math.*, 97:1–10, 1997.

[21] D. W. Masser and G. Wüstholz. Refinements of the Tate conjecture for abelian varieties. In *Abelian varieties (Egloffstein, 1993)*, pages 211–223. de Gruyter, Berlin, 1995.

[22] Madhav V. Nori. On subgroups of $\mathrm{gl}_n(\mathbf{f}_p)$. *Invent. Math.*, 88(2):257–275, 1987.

[23] Richard Pink. l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture. *J. Reine Angew. Math.*, 495:187–237, 1998.

[24] I. I. Pjateckiĭ-Šapiro. Interrelations between the Tate and Hodge hypotheses for abelian varieties. *Mat. Sb. (N.S.)*, 85(127):610–620, 1971.

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

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

[27] Jean-Pierre Serre. Groupes algébriques associés aux modules de Hodge-Tate. In *Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Vol. III*, pages 155–188. Soc. Math. France, Paris, 1979.

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

[29] Jean-Pierre Serre. Sur la semi-simplicité des produits tensoriels de représentations de groupes. *Invent. Math.*, 116(1-3):513–530, 1994.

[30] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

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

[32] A. Silverberg and Yu. G. Zarhin. Connectedness results for l-adic representations associated to abelian varieties. *Compositio Math.*, 97(1-2):273–284, 1995. Special issue in honour of Frans Oort.

[33] A. Silverberg and Yu. G. Zarhin. Connectedness extensions for abelian varieties. *Math. Z.*, 228(2):387–403, 1998.

[34] Lucien Szpiro, editor. *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell*. Société Mathématique de France, Paris, 1985. Papers from the seminar held at the École Normale Supérieure, Paris, 1983–84, Astérisque No. 127 (1985).

[35] Jean-Pierre Wintenberger. Une extension de la théorie de la multiplication complexe. *Preprint IHES*, 2000.

[36] Yu. G. Zarhin. Endomorphisms of abelian varieties and points of finite order in characteristic P. *Mat. Zametki*, 21(6):737–744, 1977.

[37] Yu. G. Zarhin. Abelian varieties, l-adic representations and Lie algebras. Rank independence on l. *Invent. Math.*, 55(2):165–176, 1979.

Jean-Pierre Wintenberger
Université Louis Pasteur
Dept Mathématiques
7, rue René Descartes
67084 Strasbourg
France
wintenb@math.u-strasbg .fr