Homothéties et images de Galois dans les représentations associées aux motifs.

Jean-Pierre Wintenberger

► To cite this version:

Jean-Pierre Wintenberger. Homothéties et images de Galois dans les représentations associées aux motifs.. Comptes Rendus de l'Academie des Sciences. Série IV, Physique, Astronomie, 2001, 333, pp.77-80. 10.1016/S0764-4442(01)02015-8 . hal-00129669

HAL Id: hal-00129669

<https://hal.science/hal-00129669>

Submitted on 8 Feb 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Homothéties et images de Galois dans les représentations associées aux motifs.

Jean -Pierre WINTENBERGER

May 28, 2001

Résumé. Nous prouvons que l'image de Galois dans la représentation galoisienne p -adique associée à un motif pur de poids non nul sur un corps de nombres contient pour p grand des homothéties non triviales d'ordre premier à p . Nous en déduisons l'annulation de groupes de cohomologie de l'image de Galois à valeurs dans ces représentations.

Title : Homotheties and image of Galois in representations associated to motives.

Abstract. We prove that the image of Galois in the p -adic Galois-representation associated to a pure motive of non zero weight on a number field contains for p big non trivial homotheties of order prime to p . The vanishing of cohomology groups of the image of Galois with values in these representations follows.

Rappelons deux définitions.

Soient $q = \ell^f$ un entier puissance d'un nombre premier ℓ et m un entier ≥ 0 . Si Ω est un corps de caractéristique 0, un élément λ de Ω est un q -nombre de Weil de poids m si c'est un entier algébrique et si pour tout plongement de τ_∞ de $\mathbb{Q}(\alpha)$ dans le corps des nombres complexes, $|\tau_\infty(\alpha)| = q^{m/2}$ ([2]).

Soient p un nombre premier, F une extension finie de $\mathbb{Q}_p$, $\overline{\mathbb{F}_p}$ le corps résiduel de $\overline{\mathbb{Q}_p}$, I_F le sous-groupe d'inertie de $\text{Gal}(\overline{\mathbb{Q}_p}/F)$. Soit $\rho : I_F \rightarrow \text{GL}(U)$ une représentation de I_F dans un $\mathbb{F}_p$ -espace vectoriel de dimension finie. Pour s entier ≥ 1 , soit $\theta_s : I_F \rightarrow \mu_{p^s-1}(\overline{\mathbb{Q}_p}) = \mu_{p^s-1}(\overline{\mathbb{F}_p})$ le caractère de Kummer associé à l'extension $F(\pi_F^{1/(p^s-1)})/F$, pour π_F uniformisante de F . Si ρ est irréductible de

dimension s , il existe des entiers $a_1, \dots, a_s$, dans l'intervalle $[0, p^s - 2]$ déterminés par la condition que I_F agisse sur $\overline{\mathbb{F}_p} \otimes U$ via les caractères $\theta_s^{a_1}, \dots, \theta_s^{a_s}$. Les poids de l'inertie modérée de ρ sont les s entiers qui apparaissent dans le développement en base p de a_i (ils ne dépendent pas du choix de i) ([4]). Si ρ n'est pas nécessairement irréductible, les poids de l'inertie modérée de ρ sont les poids de l'inertie modérée des différentes représentations irréductibles qui apparaissent dans une suite de Jordan-Hölder de ρ .

Nous utilisons à plusieurs reprises dans cette Note la notation $p_?$ pour désigner des entiers qui peuvent être différents.

On note $c(d)$ le ppcm des annulateurs des π_1 des sous-groupes semi-simples de $\mathrm{GL}_d(\mathbb{C})$: on sait que $c(d)$ divise le ppcm des entiers a qui sont $\leq d$ (2.3 de [7]).

Théorème 1 *Soit K une extension finie de $\mathbb{Q}$. Notons G_K le groupe de Galois de $\overline{\mathbb{Q}}/K$. Soient $\mathcal{L}$ un idéal premier de K de corps résiduel de cardinal $q_{\mathcal{L}}$. Soient M , d et D des entiers > 0 . Il existe un entier $p_?$ tel que pour p premier $\geq p_?$, et pour toute famille finie de représentations $\rho_i : G_K \rightarrow \mathrm{GL}_{\mathbb{F}_p}(U_i)$ dans des $\mathbb{F}_p$ -espaces vectoriels U_i de dimensions finies d_i avec $\sum d_i \leq d$, les ρ_i vérifiant 1) à 3) :*

- 1) *l'image dans $\mathrm{GL}_{\mathbb{F}_p}(U_i)$ des sous-groupes d'inertie pour les premiers de K qui ne sont pas au-dessus de p sont des pro- p -groupes,*
- 2) *les sous-groupes d'inertie au-dessus de p agissent avec poids de l'inertie modérée dans l'intervalle $[0, M]$,*

- 3) *la représentation ρ_i est non ramifiée en $\mathcal{L}$ et, pour tout i , on a un entier m_i , $0 \leq m_i \leq M$, tel que si $\overline{\alpha}$ est une valeur propre dans $\overline{\mathbb{F}_p}$ de l'image par ρ_i du Frobenius en $\mathcal{L}$, il existe un entier algébrique $\alpha \in \overline{\mathbb{Q}_p}$ dont $\overline{\alpha}$ est la réduction, le degré sur $\mathbb{Q}$ de α étant $\leq D$ et α étant un $q_{\mathcal{L}}$ -nombre de Weil de poids m_i ,*

on ait : pour tout $\lambda \in \mathbb{F}_p^$, il existe $\sigma \in G_K$ tel que pour tout i , $\rho_i(\sigma) = \lambda^{m_i c(d)} \mathrm{id}_{U_i}$.*

Corollaire 1 *Soient de plus trois entiers a, b et r , a et $b \geq 0$ et $m(a - b) + 2r \neq 0$. Il existe un premier $p_?$ vérifiant la propriété suivante. Soient p un nombre premier $\geq p_?$ et $\rho : G_K \rightarrow \mathrm{GL}_{\mathbb{F}_p}(U)$ une représentation dans un $\mathbb{F}_p$ -espace vectoriel de dimension $\leq d$ vérifiant les propriétés 1) à 3). Soient U' un sous-quotient de U stable par G_K , U'^* la représentation duale. Posons $W = U'^{\otimes a} \otimes (U'^*)^{\otimes b}(r)$, (r) désignant le twist par la puissance r -ième du caractère cyclotomique, et notons ρ_W la représentation de G_K*

dans W . Alors, pour tout entier $j \geq 0$, on a : $H^j(\rho(G_K), W) = H^j(\rho_W(G_K), W) = 0$. Si $\rho_L : G_K \rightarrow \mathrm{GL}_{\mathbb{Z}_p}(L)$ est une représentation dans un $\mathbb{Z}_p$ -module libre de rang d dont la réduction modulo p est W , on a $H^j(\rho_L(G_K), L) = 0$ pour tout $j \geq 0$.

Démonstration du corollaire. Il suffit de prouver que les images de ρ , ρ_W (resp. ρ_L) contiennent une homothétie qui agit non trivialement sur W (resp. L). Le corollaire en résulte facilement car l'action de cette homothétie par fonctorialité sur le groupe de cohomologie correspondant est triviale. Pour ρ et ρ_W , l'existence d'une telle homothétie résulte immédiatement du théorème que l'on applique à ρ et la représentation de G_K sur $\mathbb{F}_p(1)$. Montrons l'existence d'une telle homothétie pour ρ_L . Soient $\mu \in \mathbb{F}_p^*$, $\mu \neq 1$, et $\sigma \in G_K$ tel que $\rho(\sigma) = \mu \mathrm{id}_U$. Posons $g = \rho_L(\sigma)$. Décomposons g en le produit $g_p g^{(p)}$, $\lim_{n \rightarrow \infty} g_p^{p^n} = \mathrm{id}$, $g^{(p)}$ d'ordre fini premier à p , g_p et $g^{(p)}$ commutant ; g_p et $g^{(p)}$ sont dans l'image de ρ_L . Comme $g^{(p)}$ est semi-simple et que toutes ces valeurs propres sont μ , $g^{(p)}$ est l'homothétie $\mu \mathrm{id}_L$.

Remarque. Soient I un ensemble fini et $(X_i)_{i \in I}$ une famille finie de variétés algébriques propres et lisses sur K et m_i des entiers ≥ 0 . Soit, pour p nombre premier, $V_i^* = H^{m_i}((X_i)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)$ la cohomologie étale à coefficients dans $\mathbb{Q}_p$. Soient L_i^* un réseau de V_i^* stable par G_K , $U_i^* = L_i^*/pL_i^*$, $L_i = \mathrm{Hom}_{\mathbb{Z}_p}(L_i^*, \mathbb{Z}_p)$, $U_i = \mathrm{Hom}_{\mathbb{F}_p}(U_i^*, \mathbb{F}_p)$, et ρ_i (resp. ρ_i^*) la représentation de G_K dans GL_{U_i} (resp. $\mathrm{GL}_{U_i^*}$). Il résulte d'un théorème de de Jong qu'il existe une extension finie K' de K , telle que, pour tout p , tout premier $\mathcal{L}'$ de K' de norme première à p , l'image du sous-groupe d'inertie $I_{\mathcal{L}'}$ dans $\mathrm{GL}_{V_i^*}$ est un pro- p -groupe ([1]). On voit que la condition 1) du théorème est vérifiée pour la restriction $\rho_i|_{K'}$ de ρ_i à $G_{K'}$. Il résulte d'un théorème de Fontaine et Messing que, pour $\mathcal{P}$ premier de K' au-dessus de p , non ramifié sur $\mathbb{Q}$, $p > \dim(X_i)$, X_i ayant bonne réduction en $\mathcal{P}$, la restriction de ρ_i au sous-groupe d'inertie en $\mathcal{P}$ de $G_{K'}$ a ses poids de l'inertie modérée dans l'intervalle $[0, m_i]$ ([3]). Il résulte des conjectures de Weil que, pour tout p et tout idéal premier $\mathcal{L}$ de K qui n'est pas au-dessus de p et qui est tel que X_i ait bonne réduction en $\mathcal{L}$, l'image dans $\mathrm{GL}_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} L_i)$ du Frobenius en $\mathcal{L}$ a un polynôme caractéristique à coefficients rationnels et des valeurs propres dans $\overline{\mathbb{Q}_p}$ qui sont des $q_{\mathcal{L}}$ -nombres de Weil de poids m_i ([2]). On déduit du théorème qu'il existe $p_?$ tel que si $p \geq p_?$, pour tout $\lambda \in \mathbb{F}_p^*$, il existe $\sigma \in G_K$ tel que $\rho_i(\sigma) = \lambda^{m_i} \mathrm{id}_{U_i}$. Le corollaire

entraîne en particulier qu'il existe $p_?$ tel que, si $p \geq p_?$ et $m_i \neq 0$, les groupes de cohomologies $H^j(\rho_i(G_K), U_i)$ sont nuls.

Indications sur la preuve du théorème. On commence par se ramener au cas où les représentations ρ_i sont semi-simples. Pour ceci, soit ρ_i^{ss} semi-simplifiée de ρ_i . Soit $\lambda \in \mathbb{F}_p^*$. Supposons prouvé qu'il existe $\sigma \in G_K$ tel que, pour tout i , $\rho_i^{\text{ss}}(\sigma) = \lambda^{m_i c} \text{id}$. Notons G l'image de G_K dans $\Pi\text{GL}_{\mathbb{F}_p}(U_i)$, et g l'image de σ dans G . Soit $g = g_p g^{(p)}$ la décomposition de g en le produit d'éléments g_p et $g^{(p)}$ de G commutant, g_p d'ordre une puissance de p , $g^{(p)}$ d'ordre premier à p . On voit facilement que l'image de $g^{(p)}$ dans $\text{GL}_{\mathbb{F}_p}(U_i)$ est $\lambda^{m_i c} \text{id}_{U_i}$, ce qui donne alors le théorème.

Clairement on peut supposer les ρ_i simples. On reprend les notations du 3.2.1. de [7]. Pour K' extension finie de K , notons $S_{K'}^0$ le tore, quotient du tore algébrisant le groupe multiplicatif K'^* par l'adhérence de Zariski du groupe des unités de K' qui sont positives en toutes les places réelles (le tore $S_{K'}^0$ est le tore défini dans le 2.2 de [5] et noté $T_{\mathcal{M}}$, pour le modulus $\mathcal{M} = (1)$). Pour p non ramifié dans K' , le tore $S_{K'}^0$ se prolonge de manière naturelle à $\mathbb{Z}_p$ en un tore que l'on note $(S_{K'}^0)_{\mathbb{Z}_p}$. Notons alors $\rho_{K'}(p) : G_{\widetilde{K'}} \rightarrow S_{K'}^0(\mathbb{F}_p)$ la réduction modulo p de la représentation définie dans le 2.10 de [5], $\widetilde{K'}$ désignant l'extension maximale abélienne non ramifiée en toutes les places finies de K' .

Les hypothèses 1) et 2) permettent d'appliquer à la somme ρ des ρ_i le théorème 4 de [7] (134, 136 et 137 de [6]). Il existe un premier $p_?$ et une extension finie K' de K , ne dépendant que de K , d et M , tels que pour $p \geq p_?$, il existe un sous-groupe réductif $G(p)^{\text{alg}}$ de $\text{GL}_{\oplus U_i}$ vérifiant :

- $\rho(G_{K'})$ est contenue dans $G(p)^{\text{alg}}(\mathbb{F}_p)$;
- si $N(p)$ est le groupe des commutateurs de $G(p)^{\text{alg}}$, $\rho(G_{K'})$ contient un sous-groupe distingué $N(p)(\mathbb{F}_p)_u$ de $N(p)(\mathbb{F}_p)$ tel que le quotient $N(p)(\mathbb{F}_p)/N(p)(\mathbb{F}_p)_u$ soit annulé par $c(d)$;
- si T est le quotient de $G(p)^{\text{alg}}$ par $N(p)$, et si η est la représentation de $G_{K'}$ dans $T(\mathbb{F}_p)$ composée de ρ et de la projection sur T , on a un morphisme surjectif η^{alg} de $(S_{K'}^0)_{\mathbb{F}_p}$ sur T qui algébrise η en le sens que la restriction de η à $G_{\widetilde{K'}}$ coïncide avec $\eta^{\text{alg}} \circ \rho_K(p)$.

Soit $w_{K'} : \mathbb{G}_m \rightarrow S_{K'}^0$ le groupe à un paramètre défini dans le 2.3.2 de [5] (et noté j^*). Soit C la composante neutre du centre de $G(p)^{\text{alg}}$, de sorte que l'on a une isogénie $C \rightarrow T$. Le groupe à un paramètre w image de $w_{K'}$ dans T se relève en un quasi-cocaractère

w_C de C . Comme w_C est défini sur $\mathbb{F}_p$ et que les ρ_i sont simples, w_C agit avec un seul poids $m'_i \in \mathbb{Q}$ sur U_i . On voit facilement avec les propriétés de $G(p)^{\text{alg}}$ rappelées ci-dessus et les propriétés de la représentation $\rho_{K'}(p)$, que, pour prouver le théorème, il suffit de prouver que $m'_i = m_i$ pour tout i .

Pour ceci, considérons la représentation déterminant : $\det(\rho_i) : G_K \rightarrow \wedge^{\max} U_i$. Sa restriction à $G_{K'}$ se factorise par $G(p)^{\text{alg}} \rightarrow T$, donc est décrite par un caractère χ_i de $(S_{K'}^0)_{\mathbb{F}_p}$. On suppose p suffisamment grand pour que p soit non ramifié dans K' . Le caractère χ_i est alors la réduction modulo p d'un caractère, défini sur $\mathbb{Z}_p$, du tore $(S_{K'}^0)_{\mathbb{Z}_p}$. On le note $\chi_{i,\mathbb{Z}_p}$. Soit $\mathcal{L}'$ un idéal premier de K' au-dessus de $\mathcal{L}$, dont on note $q_{\mathcal{L}'}$ le cardinal du corps résiduel. La construction de η^{alg} entraîne que $\chi_{i,\mathbb{Z}_p}(\rho_{K'}(p)(\text{Frob}_{\mathcal{L}'}))$ est un entier algébrique qui est un $q_{\mathcal{L}'}$ -nombre de Weil de poids $< \chi_i, w_{K'} >$, et dont la puissance $[\widetilde{K'} : K']$ est produit d'images d'éléments de K' dans la clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$. On a : $< \chi_i, w_{K'} > = m'_i \dim(U_i)$. En utilisant la propriété 2) du théorème 1, on prouve que m'_i vérifie : $0 \leq m'_i \leq 2M \dim(U_i)$. Le théorème résulte alors de l'hypothèse 3) et du lemme :

Lemme 1 *Soit ℓ un nombre premier et $q = \ell^f$ une puissance de ℓ . Soient M et D deux entiers. Il existe p vérifiant la propriété suivante. Soient α_1 et α_2 deux éléments de la clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$, qui sont des entiers algébriques de degrés $\leq D$, qui sont des q -nombres de Weil de poids $\leq M$, et dont les réductions dans $\overline{\mathbb{F}_p}$ coïncident, alors $\alpha_1 = \alpha_2$.*

Démonstration. Soit $F = \mathbb{Q}(\alpha_1 - \alpha_2)$. Le degré $[F : \mathbb{Q}]$ est $\leq D^2$. On a $|N_{F/\mathbb{Q}}(\alpha_1 - \alpha_2)| \leq (4q)^{D^2 M/2}$ et p divise $|N_{F/\mathbb{Q}}(\alpha_1 - \alpha_2)|$. Il suffit de prendre $p > (4q)^{D^2 M/2}$.

References

- [1] A. J. de Jong. Smoothness, semi-stability and alterations. *Inst. Hautes Études Sci. Publ. Math.*, (83):51–93, 1996.
- [2] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

- [3] 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.
- [4] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
- [5] 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.
- [6] Jean-Pierre Serre. *Oeuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.
- [7] Jean-Pierre Wintenberger. Démonstration d'une conjecture de Lang dans des cas particuliers. *soumis, consultable sur le serveur de preprint de l'IRMA : <http://www-irma.u-strasbg.fr/irma/publications/index.shtml>*, 37, 2000.

Jean-Pierre Wintenberger
 Université Louis Pasteur
 Département de Mathématiques, IRMA
 7, rue René Descartes
 67084 Strasbourg Cedex
 France
 e-mail wintenb@math.u-strasbg.fr