**Independence of families of $\ell$-adic representations and uniform constructibility**

**(after J-P. Serre)**

University of Tokyo, April 28, May 7, 12, 2010

Luc Illusie



## 1. Statements

$[k : \mathrm{Q}] < \infty$ ; $\Gamma_k = \mathrm{Gal}(\overline{k}/k)$
$X/k$ finite type, separated ; $i \in \mathbf{Z}$
$\ell$ prime ; $V_\ell$ : $H^i(X_{\overline{k}}, \mathbf{Q}_\ell)$ or $H^i_c(X_{\overline{k}}, \mathbf{Q}_\ell)$

$$\rho_\ell : \Gamma_k \to \mathrm{GL}(V_\ell),$$

$$\rho = (\rho_\ell) : \Gamma_k \to \prod \mathrm{GL}(V_\ell).$$

**Theorem 1** (Serre). *$\exists k' \subset \overline{k}$, $[k' : k] < \infty$, such that*

$$\rho(\Gamma_{k'}) = \prod \rho_\ell(\Gamma_{k'}).$$

*Remark.* $\Leftrightarrow$ $(K_\ell)$ linearly disjoint $/k'$, $K_\ell = \overline{k}^{N_\ell}$, $N_\ell = \mathrm{Ker}\,\rho_\ell | \Gamma_{k'}$ ; family $(\rho_\ell)$ called "potentially independent", "independent" if $k' = k$.

*Remark.* Th. 1 conjectured by Serre [Seattle] for $X/k$ proper smooth (more generally, pure motive $E/k$, with $\ell$-adic realization $V_\ell$), $k/\mathbf{Q}$ of finite type. Fits with general conjectures for *openness of images of* $\Gamma_k$ in $\mathbf{Q}_\ell$ and adelic points of motivic Galois group $G_{M(E)} = \mathrm{Aut}^{\otimes}_{M(E)}(H_\sigma)$ ($\sigma : k \hookrightarrow \mathbf{C}$, $H_\sigma$ = Betti realization, $M(E)$ = Tannakian envelope of $E$).

*Examples.* (a) $X = \mathbf{P}^1_k$, $i = 2$ ; $V_\ell = \mathbf{Q}_\ell(-1)$ ; $\rho_\ell = \chi_\ell^{-1}$, $\chi_\ell : \Gamma_k \to \mathbf{Z}_\ell^*$ cyclotomic character ; already, for $k = \mathbf{Q}$, $\rho_\ell : \Gamma_{\mathbf{Q}} \to \mathbf{Z}_\ell^*$ independent : $/\mathbf{Q}$ : $\mathrm{Im}(\rho_\ell) = \mathbf{Z}_\ell^*$, $\mathrm{Im}(\rho) = \prod \mathbf{Z}_\ell^*$ (Gauss). (NB. Here $k_\ell = \mathbf{Q}(\zeta_{\ell^\infty})$)

(b) $X = \mathrm{Spec}\, K$, $K/k$ Galois, group $G$, $V_\ell = H^0(X_{\overline{k}}, \mathbf{Q}_\ell) = \mathbf{Q}_\ell[G]$ ; $\rho_\ell : \Gamma_k \twoheadrightarrow G \hookrightarrow \mathrm{GL}(V_\ell)$, $\rho : \Gamma_k \twoheadrightarrow G \hookrightarrow \prod \mathrm{GL}(V_\ell)$,

$$(\rho(\Gamma_k) \subset \prod \rho_\ell(\Gamma_k)) = (G \hookrightarrow \prod G)$$

(diagonal).

(c) $X =$ abelian variety, dimension $n$ ; $V_\ell = H^1(X_{\overline{k}}, \mathbf{Q}_\ell) = \mathbf{Q} \otimes \check{T}_\ell(X)$, $T_\ell(X) = \mathrm{lim.proj}_m \mathrm{Ker}\,(\ell^m : X(\overline{k}) \to X(\overline{k}))$ ; $T_\ell(X) \simeq \mathbf{Z}_\ell^{2n}$ ; $\rho_\ell : \Gamma_k \to \mathrm{GL}_{2n}(\mathbf{Z}_\ell) \subset \mathrm{GL}_{2n}(\mathbf{Q}_\ell)$. Serre (1986) : $(\rho_\ell)$ potentially independent. Extended to semi-abelian schemes (Hrushovski) (2000).

(d) (Ramanujan motive)

$$\rho_\ell : \Gamma_{\mathbf{Q}} \to \mathrm{GL}(V_\ell)(\simeq \mathrm{GL}_2(\mathbf{Q}_\ell)),$$

associated to modular form $\Delta$ ($V_\ell = H_\ell(M(\Delta))$) ; $\rho_\ell$ unramified outside $\ell$ ; $(\rho_\ell)$ independent.

*Serre's criterion*

$L =$ set of prime nbs ; $\ell \in L$, $G_\ell =$ locally compact $\ell$-adic Lie group (e. g. $G_\ell = \mathrm{GL}_{n_\ell}(\mathbf{Q}_\ell)$) ; $\rho_\ell : \Gamma_k \to G_\ell$ continuous homomorphism

*Definitions*

(a) *Independence.*

(I) $(\rho_\ell)$ independent : $\mathrm{Im}(\rho) = \prod \mathrm{Im}(\rho_\ell)$ ($\rho : \Gamma_k \to \prod G_\ell$)

(PI) (*potential independence*) $=\exists k'/k$, $[k' : k] < \infty$, $(\rho_\ell | \Gamma_{k'})$ independent

(b) *Boundedness*

(B) $\exists n \geq 0$, s. t. $\forall \ell \in L$, $\rho_\ell(\Gamma_k) =$ quotient of closed subgroup of $\mathrm{GL}_n(\mathbf{Z}_\ell)$

(c) *$\ell$-semistability*

Notations : $R = \mathcal{O}_k$, $S = \mathrm{Spec} R$, $s \in S$ (closed), $K_s = \mathrm{Frac}(\widehat{\mathcal{O}_{S,s}})$,

$$\begin{array}{ccc} \overline{k} & \longrightarrow & \overline{K_s}\,, \\ {\scriptstyle \Gamma_k}\uparrow & \supset D_s \supset I_s & \uparrow \\ k & \longrightarrow & K_s \end{array}$$

$k_s =$ residue field$(K_s)$, $p_s = \mathrm{char}(k_s)$.

(ST) $\exists\, T \subset S$ finite s. t. :

(ST1) $s \in S - T$, $\ell \neq p_s \Rightarrow \rho_\ell(I_s) = 1$ (unramified at $s$) ;

(ST2) $s \in T$, $\ell \neq p_s \Rightarrow \rho_\ell(I_s) =$ pro-$\ell$-group.

(PST) $\exists k'/k$, $[k' : k] < \infty$ s. t. $(\rho_\ell | \Gamma_{k'})$ satisfy (ST).

(NB. e. g. $\rho_\ell | I_s$ unipotent $\Rightarrow \rho_\ell(I_s)$ = pro-$\ell$-group.)

**Theorem 2** (Serre). (B) + (PST) $\Rightarrow$ (PI)

*Remark.* No assumption on $\det(1 - F_s t, V_\ell)$, $s$ unramified.

**Theorem 3**. Family $(\rho_\ell)$ of th. 1 satisfies (B), (PST).

Hence : th. 2 + th. 3 $\Rightarrow$ th. 1.

*Remark* (Serre). $k = \mathbf{Q}$, $p > 2$, $\ell_1 < \ell_2 < \cdots$, $\ell_i \equiv 1 \bmod p^i$ ; $L = \{\ell_1, \ell_2, \cdots\}$, $\rho_{\ell_i} : \Gamma_{\mathbf{Q}} \twoheadrightarrow \mathbf{Z}/p^i\mathbf{Z} \subset \mathbf{Z}_{\ell_i}^*$ ; (B) $(n = 1)$, (ST1) $(T = \{p\})$ ; not (ST2) ; not (PI).

*Remark.* (B), (PST) stable under $\otimes$, dual. $\Rightarrow H^*(X_{\overline{k}}, K_\ell)$, $H_c^*(X_{\overline{k}}, K_\ell)$ independent, $K_\ell = a_X^! \mathbf{Q}_\ell$ = dualizing complex. Independence of $IH^*(X_{\overline{k}}, \mathbf{Q}_\ell)$ (resp. $IH_c^*$) unknown.

## 2. Outline of proofs

*Proof of th. 2.*

*Step 1.* Shrinking $L$ (removing a finite set).
Use general nonsense on independence, Goursat's lemma, local structure of $p$-adic compact Lie groups.

*Step 2.* Putting $\rho_\ell(\Gamma_k)$ into standard form.
Up to shrinking $L$ and enlarging $k$ (replacing by $k'$ finite over $k$), can obtain

$$\rho_\ell(\Gamma_k) = G_\ell = G_\ell^+ . A_\ell,$$

$$\Gamma_{k,\ell} =< (I_s)_{p_s = \ell} >\subset \Gamma_k$$

($<>$ = smallest closed normal subgp)

$$A_\ell = \rho(\Gamma_{k,\ell}) \subset G_\ell \times \prod_{\ell' \neq \ell} \{1\}$$

$$G_\ell^+ =< (H)_{H = \ell-\text{Sylow}} >\subset G_\ell$$

($G_\ell^+$ open in $G_\ell$).
Use : - inputs from number theory : Hermite-Minkowski, class field,
- inputs from finite groups theory : variants of Jordan's th. on finite subgps of $\mathrm{GL}_n(\mathbf{C})$.

*Step 3.* Separating the simple subquotients of the $G_\ell^+$, end of proof.

Use Nori's th. on simple subgps $H$ of $\mathrm{GL}_n(\mathbf{F}_\ell)$ with $\ell | |H|$, E. Artin's th. on simple groups of Lie type

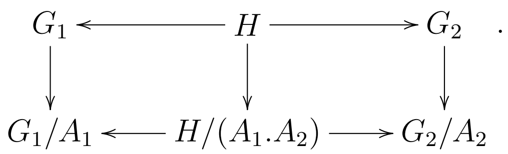
*Proof of th. 3.*

(ST1) : uniform constructibility (Katz-Laumon, I.).
Use Hironaka (or de Jong)

(ST2) : uniform quasi-unipotence.
Use Berthelot-de Jong.

### 3. Proof of th. 2 : step 1

**Proposition 3.1** (Goursat's lemma). $r = (r_1, r_2) : \Gamma \to G = G_1 \times G_2$ *s. t.* $r_i(\Gamma) = G_i$, $H = r(\Gamma)$, $A_1 = H \cap (G_1 \times \{1\}) = \mathrm{Ker}(\mathrm{pr}_2 : H \to G_2)$, $A_2 = H \cap (\{1\} \times G_2) = \mathrm{Ker}(\mathrm{pr}_1 : H \to G_1)$. *Then :*
*(i)* $A_i$ *normal in* $G_i$ *;*
*(ii)* $H/(A_1.A_2) \xrightarrow{\sim} G_i/A_i$ *;*
*(iii) diagram*



*makes*

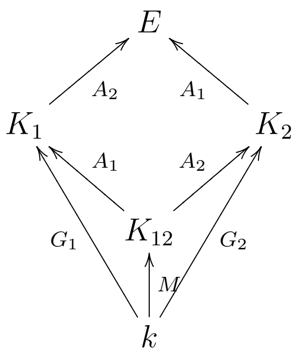
$$H \xrightarrow{\sim} G_1 \times_M G_2,$$

*where* $M = H/(A_1.A_2)$.

**Corollary 3.2.** *(r surjective)* $\Leftrightarrow$ *(*$\Gamma = N'_1 N'_2$*), where* $N'_1 = \mathrm{Ker}(r_2)$, $N'_2 = \mathrm{Ker}(r_1)$.

**Corollary 3.3.** $([G : H] < \infty) \Leftrightarrow ([\Gamma : N'_1 N'_2] < \infty)$.
*Proof.* $G/H \xrightarrow{\sim} G_2/A_2, (x_1, x_2) \mapsto \overline{x_2} f(\overline{x_1})^{-1}$, where $f : G_1/A_1 \xrightarrow{\sim} G_2/A_2$ given by diagram.

*Example 3.3.1.*




$$H = \mathrm{Gal}(E/k) = G_1 \times_M G_2,\ M = \mathrm{Gal}(K_{12}/k) = H/(A_1.A_2).$$

**Definition 3.4.** $(r_i : \Gamma \to G_i)_{i \in I}$ *independent :* $\mathrm{Im}(r) = \prod \mathrm{Im}(r_i)$*,* $r = (r_i) : \Gamma \to \prod G_i$.

**Proposition 3.5.** *$I$ finite. $N_i := \mathrm{Ker}(r_i)$, $N'_i = \cap_{j\neq i} N_j$. Equivalent conditions :*

*(i) $(r_i)$ independent ;*

*(ii) $\forall i \in I, \Gamma = N_i.N'_i$ ;*

*(iii) $\Gamma = \cdot_{i\in I} N'_i$.*

*Proof.* Induction on $|I|$, use 3.2.

**Corollary 3.6.** *$\Gamma$ profinite, $G_i$ locally compact, $r_i$ continuous, $N_i :=$ $\mathrm{Ker}(r_i)$, $N'_i = \cap_{j\neq i} N_j$. Equivalent conditions :*

*(i) $(r_i)$ independent ;*

*(i') $\forall J \subset I$ finite, $(r_i)_{i\in J}$ independent ;*

*(ii) $\forall i \in I$, $\Gamma = N_i.N'_i$ ;*

*(iii) $\Gamma$ topologically generated by the $N'_i$.*

**Corollary 3.7.** *$\Gamma'$ = smallest closed subgp of $\Gamma$ containing $N'_i$ $\forall i$. Then $\Gamma'$ = largest closed subgp $C$ of $\Gamma$ s. t. $(r_i)|C$ independent.*

**Corollary 3.8.** $[\prod r_i(\Gamma) : r(\Gamma)] < \infty \Rightarrow \exists \Gamma' \subset \Gamma$, *open, s. t. $(r_i)|\Gamma'$ independent.*

*Proof.* Take $\Gamma'$ defined in 3.7.

**Corollary 3.9.** $\Gamma = \mathrm{Gal}(K/k)$, *$(k_i/k) \subset (K/k)$ Galois, $i \in I$, $E =$ $k((k_i)_{i\in I})$, $G_i = \mathrm{Gal}(k_i/k) = \Gamma/N_i$, $k'_i = k((k_j)_{j\neq i})$, $\mathrm{Gal}(k'_i/k) = \Gamma/N'_i$, $N'_i = \cap_{j\neq i} N_j$, $r_i : \Gamma \to G_i$. Equivalent conditions :*

*(i) $\forall i$, $k_i$, $k'_i$ linearly disjoint $/k$ ;*

*(ii) $(r_i)_{i\in I}$ independent.*

*Proof.* By 3.3.1, (i) $\Leftrightarrow H = N_i.N'_i$ $\forall i$, where $H = \mathrm{Im}(r) = \mathrm{Gal}(E/k) =$ $G_i \times_{\mathrm{Gal}((k_i\cap k'_i)/k)} \mathrm{Gal}(k'_i/k)$.

*Remark.* Extension $k'$ of independence of the $k_i = \cap_{i\in I} k'_i$ ; $\mathrm{Gal}(k'/k) =$ $\Gamma/\cdot_{i\in I} N'_i$.

**Proposition 3.10.** *Notations of theorem 2 ($G_\ell$ locally compact $\ell$-adic, $\rho_\ell$ continuous). Assume $\exists I \subset L$, finite, s. t. $(\rho_\ell)_{\ell\in L-I}$ satisfies (PI). Then $(\rho_\ell)_{\ell\in L}$ satisfies (PI).*

*Proof.* WMA : - all $\rho_\ell$ surjective ($\Rightarrow G_\ell$ = $\ell$-adic compact Lie group) ;

- $I = \{p\}$ ;

- (up to shrinking $\Gamma(=\Gamma_k)$), $(\rho_\ell)_{\ell\neq p}$ independent.

Will show : $\mathrm{Im}(\rho)$ open in $\prod G_\ell = G_p \times \prod_{\ell\neq p} G_\ell$. Suffices by 3.8. Let $K = \prod_{\ell\neq p} G_\ell$. Then

$$\rho : \Gamma \to G_p \times K$$

has both projections $\Gamma \to G_p$, $\Gamma \to K$ surjective, hence (Goursat)

$$\rho(\Gamma) = G_p \times_C K,$$

where $C = G_p/(\rho(\Gamma) \cap (G_p \times \{1\}))$. By 3.3, has to show $C$ finite. $C =$ compact $p$-adic Lie group $\Rightarrow \exists U \subset C$, open, normal, torsionfree pro-$p$-group. For $J \subset L - \{p\}$, $C_J := \mathrm{Im}(\prod_{j \in J} K_j \to C)$. $K_\ell = \ell$-adic $\Rightarrow$ $p$-Sylows of $K_\ell$ finite, $\Rightarrow$ $p$-Sylows of $C_J$ finite $\Rightarrow U \cap C_J = 1 \Rightarrow |C_J| \leq [C : U] \Rightarrow \cup C_J$ finite $\Rightarrow C$ finite ($\cup C_J$ dense in $C$).

*Remark.* $L$ finite $\Rightarrow (\rho_\ell)$ (PI).

**4. Proof of th. 2 : step 2**

**Definition 4.1.** *$d > 0$ ; $G$ finite group ; $G$ satisfies $(Jor_d)$ : $\exists A \subset G$, normal, abelian, $[G : A] \leq d$.*

**Theorem 4.2** (Jordan, 1878). *$\forall n \geq 0$, $\exists d(n) > 0$ s. t. $\forall G \subset \mathrm{GL}_n(\mathbf{C})$ finite, $G$ satisfies $Jor_{d(n)}$.*

*Proof.* (Frobenius, 1911, Bieberbach, Schur) See Eva Bayer's notes of Serre's 1986 course, p. 13. $G \subset U(n)$ finite $\Rightarrow A =< \{u \in G, \mathrm{Tr}(1-u)(1-u^*) < 1/2\} >$ abelian, normal, $[G : A] \leq (\sqrt{8n}+1)^{2n^2} - (\sqrt{8n}-1)^{2n^2}$. Better bound (Weisfeiler) : $d(n) \leq n! n^{a \log n + b}$, best one (Collins) $n!$ for $n \geq 71$ (using classification of finite simple groups, listing primitive irreducible subgroups of $\mathrm{PGL}_n(\mathbf{C})$).

**Corollary 4.3.** *$n \geq 0$, $F =$ field, $G =$ quotient of finite subgroup $H$ of $\mathrm{GL}_n(F)$, $|G|$ prime to $p = \mathrm{charexp(F)}$. Then : $G$ satisfies $(Jor_{d(n)})$.*

*Proof.* (a) $p = 1$ : WMA $F/\mathbf{Q}$ f. t. ; $\Rightarrow H \subset \mathrm{GL}_n(\mathbf{C})$.

(b) $p > 1$ : WMA $F$ perfect ; $W = W(F)$

(i) $|H|$ prime to $p$. $H \subset \mathrm{GL}_n(F)$ lifts to $\mathrm{GL}(W)$ (obstructions in $H^2(H, M_n(F))$ ; OK by (a)

(ii) general case. Use :

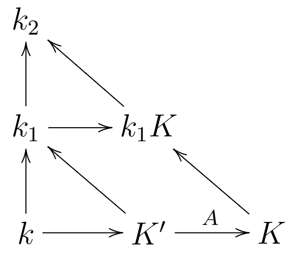
**Lemma 4.3.1** (Frattini). *$1 \to I \to H \to G \to 1$, $H$ finite, $|G|$ prime to $p$, $P = p$-Sylow of $I$. Then $N_H(P) \to G$ surjective.*

(Pf. $[H : I]$ prime to $p \Rightarrow P = p$-Sylow of $H$ ; $g \in H$ ; $gPg^{-1} = p$-Sylow of $I = xPx^{-1}$, $x \in I$, $\Rightarrow x^{-1}g \in N_H(P)$, $\Rightarrow H = I.N_H(P)$.)

$(|P|, |N_H(P)/P|) = 1 \Rightarrow \exists H' \subset N_H(P)$, of order prime to $p$, $N_H(P) = P.H'$ ; then 4.3.1 $\Rightarrow H' \twoheadrightarrow G$, reduced to case (i).

**Theorem 4.4.** (Serre) *$d > 0$, $[k : \mathbf{Q}] < \infty$, $\exists k' \subset \overline{k}$, $[k' : k]$ finite, s. t. : if $K/k =$ Galois subextension of $\overline{k}/k$, unramified $/k$, with $G = \mathrm{Gal}(K/k)$ satisfying $(Jor_d)$, then $K \subset k'$.*

*Proof.* $E/k \subset \overline{k}/k$, $[E : k] \leq d$, $E/k$ unramified $\Rightarrow |\mathrm{disc}_E| = |\mathrm{disc}_k|^{[E:k]} \leq |\mathrm{disc}_k|^d \Rightarrow$ (Hermite-Minkowski) nb. of such $E$ bounded $\Rightarrow \exists k_1/k \subset \overline{k}/k$, $[k_1 : k] < \infty$ s. t. all such $E \subset k_1$. $k_2 :=$ maximal unramified abelian extension of $k_1 \subset \overline{k}$. $[k_2 : k_1] < \infty$ (class field).




4.5. *Proof of Step 2.* 2 steps :

4.5.1. Enlarge $k$ s. t. (ST) satisfied. Shrink $L$ s. t.

$$L \cap \{p_s, s \in T\} = \emptyset. \tag{1}$$

Let $H_\ell := G_\ell/(G_\ell^+.A_\ell)$ ; $G_\ell^+ \subset G_\ell$ open $\Rightarrow H_\ell$ finite. Then :

(i) $H_\ell$ satisfies $(Jor_{d(n)})$ ;

(ii) $\Gamma_k \to G_\ell \to H_\ell$ everywhere unramified.

(Pf. (i) : $|H_\ell|$ prime to $\ell$, quotient of subgp of $\mathrm{GL}_n(\mathbf{Z}_\ell)$ hence of subgp of $\mathrm{GL}_n(\mathbf{F}_\ell)$. Apply 4.3.

(ii) : $\rho_\ell(I_s) :\subset A_\ell$ if $\ell = p_s$, $= 1$ if $\ell \neq p_s$ by (ST1) and (1).)

By 4.4, up to enlarging $k$ to $k'$ unramified $/k$, WMA $\Gamma_{k'} \to H_\ell$ trivial, i. e. $\rho_\ell(\Gamma_{k'}) \subset G_\ell^+.A_\ell$. Note : $k'$ unramified $/k \Rightarrow A_\ell$ doesn't change.

4.5.2. For $\ell > [k' : k]$, $[G_\ell : \rho_\ell(\Gamma_{k'})]$ prime to $\ell \Rightarrow \ell$-Sylows of $G_\ell$ contained in $\rho_\ell(\Gamma_{k'}) \Rightarrow \rho_\ell(\Gamma_{k'}) = G_\ell^+.A_\ell$.

## 5. Proof of theorem 1 : Step 3.

5.1. *Finite simple groups of Lie type of char. $\ell$.*

$\ell \geq 5$ ; $F = \mathbf{F}_{\ell^r}$, $H/F$ = smooth, connected linear alg. gp s. t. $H_{\overline{F}}$ simple, simply connected. Define :

$$H_F = \mathrm{Im}(H(F) \to H^{adj}(F)),$$

where $H^{adj} = H/Z$, $Z = \mathrm{center}(H)$. $H_F$ is simple. Define :

$$\Sigma_\ell = \{H_F, \mathbf{Z}/\ell\mathbf{Z}\}.$$

**Theorem 5.2.** (Nori-Serre) *$\forall n \geq 0$, $\exists c(n)$ s. t. if $\ell > c(n)$, any finite simple subquotient $S$ of $\mathrm{GL}_n(\mathbf{Z}_\ell)$ with $|S|$ divisible by $\ell$ belongs to $\Sigma_\ell$.*

(NB. Nori : $c(n) \leq n^{6n^2}$)

**Lemma 5.3.** *$G/\mathbf{F}_\ell$ linear, smooth, connected, $S$ = simple quotient of Jordan-Hölder sequence of $G(\mathbf{F}_\ell)$. Then : either $S \in \Sigma_\ell$ or $S = \mathbf{Z}/p\mathbf{Z}$, $p \neq \ell$.*

(Pf. WMA $G$ semisimple (torus, unipotent : trivial). $\tilde{G}$ = universal cover of $G$ ; $\tilde{G}$ = finite product of $R_{F/\mathbf{F}_\ell}(H)$, $H$, $F$ as in 5.1, hence $\tilde{G}(\mathbf{F}_\ell) = \prod H(F)$ ; $\tilde{G}(\mathbf{F}_\ell) \to G(\mathbf{F}_\ell) \to G^{adj}(\mathbf{F}_\ell)$ have normal images and abelian Ker and Coker of orders prime to $\ell$.)

*Proof of 5.2 (using Nori).* $c_2(n)$ = Nori's constant (e. g. $n^{6n^2}$) : $\ell > c_2(n)$ $\Rightarrow \forall G \subset \mathrm{GL}_n(\mathbf{F}_\ell)$, $G^+ = (G_N(\mathbf{F}_\ell))^+$, where $(X)^+$ = (normal) subgp of $X$ generated by $\ell$-Sylows of $X$, $G_N \subset \mathrm{GL}_n/\mathbf{F}_\ell =< (t \mapsto x^t = \sum_{i<\ell} \binom{t}{i}(x-1)^i >_{x \in G, x^\ell = 1}$.

Either $S = \mathbf{Z}/\ell\mathbf{Z}$ or $S$ = subquotient of $GL_n(\mathbf{F}_\ell)$. WMA : $S = G/I$, $G \subset \mathrm{GL}_n(\mathbf{F}_\ell)$. $S$ simple, order divisible by $\ell \Rightarrow S = S^+$. WMA : $G = G^+$. Take $c(n) = \sup(3, c_2(n))$. Nori $\Rightarrow S$ = simple quotient of Jordan-Hölder sequence of $G_N(\mathbf{F}_\ell) \Rightarrow$ (5.3) $S \in \Sigma_\ell$.

**Theorem 5.4.** (E. Artin) *$\ell$, $\ell'$ prime $\geq 5$, $\ell \neq \ell' \Rightarrow \Sigma_\ell \cap \Sigma_{\ell'} = \emptyset$.*

(NB. in fact : $|G| \neq |G'|$ if $G \in \Sigma_\ell$, $G' \in \Sigma_{\ell'}$. See : W. Kimmerle et al., *Composition factors from the group ring and Artin's theorem on orders of simple groups*, Proc. LMS **60** (1990), 89-122. $\geq 5$ avoids $\mathrm{SL}_3(\mathbf{F}_2) = \mathrm{PSL}_2(\mathbf{F}_7), \mathrm{SL}_2(\mathbf{F}_4) = \mathrm{PSL}_2(\mathbf{F}_5)$.)

**Proposition 5.5.** *$r_i : \Gamma \to G_i$, $i \in I$, continuous homomorphisms, $\Gamma$, $G_i$ profinite. Assume :*

*(*) if $i \neq j$, no finite simple subquotient of $r_i(\Gamma)$ is isomorphic to a subquotient of $r_j(\Gamma)$.*

*Then $(r_i)_{i \in I}$ independent.*

*Proof.* WMA $G_i = r_i(\Gamma)$ $\forall i$.

(i) Case $I = \{1, 2\}$. $H := r(\Gamma)$. Goursat : $H = G_1 \times_M G_2$, $M = H/(A_1.A_2)$. (*) $\Rightarrow M = 1$, hence (3.2) $(r_1, r_2)$ independent.

(ii) Case $I$ finite : induction on $|I|$. General case : 3.6.

5.6. *Completion of proof of Step 3.*

WMA $\ell > c(n)$, $\rho_\ell(\Gamma_k) = G_\ell^+.A_\ell$. 5.2 $\Rightarrow$ any finite simple subquotient of $G_\ell^+$, hence of $G_\ell/A_\ell$ is in $\Sigma_\ell$. 5.5 $\Rightarrow$ $(\rho : \Gamma_k \twoheadrightarrow \prod G_\ell/A_\ell) \Rightarrow \rho(\Gamma_k).\prod A_\ell = \prod G_\ell$. But $\rho(\Gamma_k) \supset \prod A_\ell$ (indeed : $\rho(\Gamma_k) \supset A_\ell \times 1$ $\forall \ell$). Hence $\rho(\Gamma_k) = \prod G_\ell$.

**6. Uniform constructibility**

**Theorem 6.1.** *$S$ noetherian, $\dim(S) < \infty$, $f : X \to S$ separated, finite type. Then : $\exists U \subset S$, open, dense, and $N \geq 0$ s. t. $\forall \ell$, $Rf_!\mathbf{F}_\ell|U[1/\ell]$ (resp. $Rf_*\mathbf{F}_\ell|U[1/\ell]$) belongs to $D_c^b(U[1/\ell], \mathbf{F}_\ell)$, with $R^if_!\mathbf{F}_\ell|U[1/\ell]$ (resp. $R^if_!\mathbf{F}_\ell|U[1/\ell]$) lisse $\forall i$ and zero for $i > N$, and commutes with all base change $S' \to U[1/\ell]$.*

**Corollary 6.2.** *$S$ finite type, separated over regular scheme $T$ of dim $\leq 1$; $f : X \to S$ finite type, separated. Then : $\exists U \subset S$, open, dense, and*

$N \geq 0$ *s. t.* $\forall \ell$, $Rf_!\mathbf{Z}_\ell | U[1/\ell]$ *(resp.* $Rf_*\mathbf{Z}_\ell | U[1/\ell]$*) belongs to* $D_c^b(U[1/\ell], \mathbf{F}_\ell)$*, with* $R^i f_! \mathbf{Z}_\ell | U[1/\ell]$ *(resp.* $R^i f_! \mathbf{Z}_\ell | U[1/\ell]$*) lisse* $\forall i$ *and zero for* $i > N$*, and compatible with base change* $S' \to U[1/\ell]$ *over* $T[1/\ell]$*.*

6.1 $\Rightarrow$ 6.2 : Use $Rf_!\mathbf{Z}_\ell \otimes^L_{\mathbf{Z}_\ell} \mathbf{F}_\ell = Rf_!\mathbf{F}_\ell$ (resp. * variants), $K$ perfect $\Leftrightarrow$ $K \otimes^L_{\mathbf{Z}_\ell} \mathbf{F}_\ell$ perfect (perfect : in $D_c^b$, $H^i$ lisse $\forall i$).

**Lemma 6.3.**

$$\begin{array}{ccccc} X & \xrightarrow{j} & Z & \xleftarrow{i} & D \,, \\ & {\scriptstyle f}\searrow & \downarrow{\scriptstyle h} & \swarrow{\scriptstyle g} & \\ & & S & & \end{array}$$

*$h$ proper, smooth,* $D = D_1 + \cdots + D_m \subset Z$ *relative snc divisor,* $j : X = Z - D \hookrightarrow Z$*. Then :*

$$Rf_*\mathbf{F}_\ell | S[1/\ell],\ Rf_!\mathbf{F}_\ell | S[1/\ell]$$

*perfect,* $R^q = 0$ *for* $q > 2d$, $d = \dim(f)$*, commutes with all base change* $S' \to S[1/\ell]$*.*

*Proof.* Relative purity :

$$R^q j_* \mathbf{F}_\ell = \oplus_{1 \leqslant i_1 < \cdots < i_q \leqslant m} (\mathbf{F}_\ell)_{D_{i_1} \cap \cdots \cap D_{i_q}}(-q).$$

$\Rightarrow$ assertion for $Rf_*$.

$Rf_!$ : use cover of $D$ by $D_i$'s.

**Lemma 6.4.** *$f$ as in 6.1,* $m \geq 0$*. Then :* $\exists$ *diagram*

$$\begin{array}{ccc} X_\bullet & \xrightarrow{j_\bullet} & Z_\bullet \quad , \\ \downarrow & & \downarrow{\scriptstyle \varepsilon_\bullet} \\ X_{U'} & \xrightarrow{j} & Z \\ \downarrow{\scriptstyle f_{U'}} & \swarrow{\scriptstyle h} & \\ U' & & \end{array}$$

*$U$ dense open* $\subset S$, $U' \to U$ *universal homeomorphism, $h$ proper, $j$ open, dense image,* $\varepsilon_\bullet$ *proper hypercovering, cartesian square, s. t.* $\forall n \leq m$, $h\varepsilon_n : Z_n \to U'$ *proper, smooth,* $Z_n - X_n = D_n$ *= relative snc divisor* $/U'$*.*

*Proof.* WMA $S$ integral, generic pt $\eta$. Nagata (+ Deligne-Conrad-Lütke-bohmert) $\Rightarrow$ compactification $j$. de Jong $/\eta \Rightarrow$ good $m$-truncated hypercover $/\eta'$ finite radicial $/\eta$. Spread out $/U'$, take $\mathrm{cosk}_m$.

**Lemma 6.5.** *$f$ as in 6.1 ;* $\dim(S) < \infty$*.* $\exists N \geq 0$ *s. t.* $\forall \ell$, $\forall F \,/X$*, $\ell$-torsion,* $R^q f_* F | S[1/\ell] = 0$ *for* $q > N$*.*

*Proof.* $S$ separated, finite type / regular base, dim. $\leq 1$ : standard. General case : use Gabber's th. : $T$ strictly local noetherian, $\dim(T) = d > 0$, $U \subset T$ open $\Rightarrow \mathrm{cd}_\ell(U) \leq 2d - 1$.

6.6. *Proof of 6.1.* Take $N = 2d$, $d \geq \dim(f)$ for $Rf_!$, $N$ as in 6.5 for $Rf_*$. Take diagram as in 6.4, with $m = N + 1$.

Cohomological descent $\Rightarrow Rf_*\mathbf{F}_\ell|U[1/\ell] = R(h\varepsilon_\bullet j_\bullet)_*\mathbf{F}_\ell$.

$Rf_*\mathbf{F}_\ell = \tau_{\leq N} Rf_*\mathbf{F}_\ell = \tau_{\leq N} R(h\varepsilon_\bullet j_\bullet)_*\mathbf{F}_\ell$,

$m = N + 1 \Rightarrow \tau_{\leq N} R(h\varepsilon_\bullet j_\bullet)_*\mathbf{F}_\ell \xrightarrow{\sim} \tau_{\leq N} R(h\varepsilon_{\leq m} j_{\leq m})_*\mathbf{F}_\ell$.

Use spectral sequence

$$E_1^{pq} = R^q(h\varepsilon_p)_*(Rj_{p*}\mathbf{F}_\ell) = R^q(f_{U'}\varepsilon_p)_*\mathbf{F}_\ell \Rightarrow R^{p+q}(h\varepsilon_{\leq m} j_{\leq m})_*\mathbf{F}_\ell,$$

Apply 6.3.

Similar proof for $Rf_!$.

6.7. **Generalizations.**

(a) In 6.1, replace $f : X \to S$ by $f : X \to Y$, $Y$ separated, finite type $/S$. Get a dense open $U$ and a stratification $Y_U = (Y_i)_{i \in I}$ (finite union of loc. closed subschemes) s. t. $Rf_{U!}\mathbf{F}_\ell|Y_i[1/\ell]$ (resp.$Rf_{U*}\mathbf{F}_\ell|Y_i[1/\ell]$) perfect, base change $S' \to U[1/\ell]$ compatible. Similar proof. Same corollary for $\mathbf{Z}_\ell$ as 6.2.

(b) [Katz-Laumon, *Transformation de Fourier et majoration de sommes exponentielles*, Pub. Math. IHES 62 (1986), 361-418.]

Fix $S$ separated, finite type /regular scheme of dim. $\leq 1$.

$X/S$ separated, f. t. ; $\mathcal{X} = (X_\alpha)_{\alpha \in A}$ stratification of $X$ ; $K \in D_c^b(X[1/\ell], \mathbf{Q}_\ell)$ *adapted* to $\mathcal{X}$ if $\mathcal{H}^i(K)|X_\alpha$ lisse $\forall i$, $\forall \alpha$.

**Theorem 6.7.1.** (*loc. cit.*). *$f : X \to Y = S$-morphism, $X, Y$ separated, f. t. ; $\mathcal{X} = (X_\alpha)$ stratification of $X$. Then : $\exists N \geq 1$, $\exists$ dense open $U \subset S[1/N]$, $\exists$ stratification $\mathcal{Y} = (Y_\beta)_{\beta \in B}$ of $Y_U$ s. t. $K \in D_c^b(X_U[1/\ell], \mathbf{Q}_\ell)$ adapted to $\mathcal{X}_U \Rightarrow Rf_{U!}K$ (resp. $Rf_{U*}K$) adapted to $\mathcal{Y}$, $S' \to U$ base change compatible.*

Analogues for dualizing functor $D_X$. Stronger results for $Rf_!$. Results for $Rf_! + D_X \Rightarrow$ result for $Rf_*$. Proof for $D_X$ uses Hironaka + tameness in char. zero.

NB. 6.7.1 empty for $S/\mathbf{F}_p$.

(c) Common generalization of (a) and 6.7.1 : Orgogozo (following Gabber's ideas), work in progress.

## 7. Proof of theorem 3

7.1. *Condition (B).* Choose $\sigma : \overline{k} \to \mathbf{C}$ ; $H^i(X_{\overline{k}}, \mathbf{Z}_\ell) \simeq H^i(X_\sigma, \mathbf{Z}) \otimes \mathbf{Z}_\ell$, torsion$(H^i(X_\sigma, \mathbf{Z}))$ finite $\Rightarrow \exists n_i, N$ s. t. $\forall \ell > N$, $H^i(X_{\overline{k}}, \mathbf{Z}_\ell) \simeq \mathbf{Z}_\ell^{n_i}$. Same for $H_c^i$.

*Remark.* Using de Jong, cohomological descent, can show :

**Theorem 7.1.1.** *$K$ alg. closed of char. $p > 0$, $X/K$ separated, f. t., $i \in \mathbf{Z}$. Then $\exists n_i \geq 0$ s. t. $\forall \ell \neq p$,* $\sup(\dim H^i(X, \mathbf{F}_\ell), \dim H^i_c(X, \mathbf{F}_\ell)) \leq n_i$.

7.2. *Condition (ST1).* $S = \operatorname{Spec} \mathcal{O}_k$. Choose $f : \mathcal{X} \to U$, separated, f. t., $U$ dense open $\subset S$, s. t. $\mathcal{X}_k = X$. $V_\ell = (R^i f_* \mathbf{Q}_\ell)_{\overline{k}}$ or $(R^i f_! \mathbf{Q}_\ell)_{\overline{k}}$. 6.2 or 6.7.1 $\Rightarrow$ can srink $U$ s. t. $\forall \ell$, $R^i f_* \mathbf{Q}_\ell | U[1/\ell]$ (resp. $R^i f_! \mathbf{Q}_\ell | U[1/\ell]$ lisse, hence $\rho_\ell$ unramified on $U$. (NB. If $X/k$ proper, smooth, can take $f$ proper, smooth $\Rightarrow R^i f_*$ lisse ; 6,2, 6.7.1 not needed.)

7.3. *Condition (ST2).* $T = S - U$. $s \in T$. Berthelot-de Jong $\Rightarrow$ $\exists I'_s \subset I_s$ open s. t. $\forall \ell \neq p_s$, $\rho_\ell(I'_s)$ unipotent. $K'_s := \overline{K_s}^{I'_s}$. $\rho_\ell(I_{K'_s}) \subset \mathrm{GL}_n(\mathbf{Z}_\ell)$ unipotent $\Rightarrow \rho_\ell(I_{K'_s}) = \ell$-group. Take $k(s)/k \subset \overline{k}/k$, finite, s. t. completion($k(s)$) at $s \simeq K'_s$. Take $k' = k(\cup_{s \in T} k(s))$. Then $\rho | \Gamma_{k'}$ satisfies (ST1), (ST2).

## 8. Complements

**Theorem 8.1.** *$\rho_\ell$ as in th. 3. $\exists k'/k \subset \overline{k}/k$, $[k' : k] < \infty$, $T' \subset S' = \operatorname{Spec} \mathcal{O}_{k'}$ finite, s. t. $\forall s \in S' - T'$ (resp. $s \in T'$), $\ell = p_s$, $\rho_\ell$ crystalline (resp. semistable) at $s$,*

*Proof.* - existence of $T$ s. t. $\rho_\ell$ crystalline at $\ell = p_s$, $s \notin T$ : apply 6.4, then Tsuji-Yamashita's results for truncated simplical schemes / complete mixed char. dvr, which are de Jong's semi-stable pairs $(Z_n, D_n)$ in each degree : $Z_n$ proper, smooth $\Rightarrow$ crystalline.

- semistable at $s \in T$ : Yamashita.

8.2. *Question.* Conclusion of th. 1 still valid for $k/\mathbf{Q}$ finite type ? Unknown, even for $X/k$ = abelian variety, tr.deg($k/\mathbf{Q}$) = 1.