A uniform open image theorem for ℓ-adic representations of étale fundamental groups, II

January 26, 2010

Anna Cadoret
(IMB, Univ. Bordeaux 1)
Akio Tamagawa
(RIMS, Kyoto Univ.)

II.0. Notations and Definitions.

Given $G <_{cl} GL_d(\mathbb{Z}_\ell)$ and $n \geq 0$

$$G_n \stackrel{\text{def}}{=} \text{Im}(G \to GL_d(\mathbb{Z}/\ell^n\mathbb{Z}))$$

$$G(n) \stackrel{\text{def}}{=} \text{Ker}(G \to GL_d(\mathbb{Z}/\ell^n\mathbb{Z}))$$

Def. G is Strictly Rationally Perfect

$\stackrel{\text{def}}{\iff} \forall U <_{op} G,\ |U^{ab}| < \infty$

$\iff Lie(G)^{ab} = 0$

$k = \overline{k}$, char. $= 0$

X^{cpt}: proper (smooth, connected) curve $/k$

$X \subset X^{cpt}$: open $\neq \emptyset$

$g \stackrel{\text{def}}{=} g_X \stackrel{\text{def}}{=}$ genus of X^{cpt}

$r \stackrel{\text{def}}{=} r_X \stackrel{\text{def}}{=} |X^{cpt} \setminus X|$

$$\pi_1(X) = \text{étale fundamental group of } X$$

$$\overset{\text{def}}{=} \mathrm{Aut}(F_{\overline{x}} : \mathcal{C}_X^{(1)} = (\text{fet}/X) \to FSETS)$$

$$= \mathrm{Gal}(M_X/k(X))$$

$$= \pi_1^{top}(X_{\mathbb{C}})^\wedge$$

$$= \pi_1^{top}(\Sigma_{g,r})^\wedge$$

$$= \langle \alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g, \gamma_1, \ldots, \gamma_r \\ \quad \mid [\alpha_1, \beta_1] \ldots [\alpha_g, \beta_g]\gamma_1 \ldots \gamma_r = 1\rangle^\wedge$$

$$(= F_{2g+r-1}^\wedge \text{ if } r > 0)$$

$$U <_{op} \pi_1(X) \iff X_U \overset{\text{fet}}{\to} X \text{ (connected)}$$

$$\rho : \pi_1(X) \overset{\text{cont}}{\to} GL_d(\mathbb{Z}_\ell)$$

$$G \overset{\text{def}}{=} \rho(\pi_1(X)) \ (= \text{“}G^{geo}\text{”})$$

$$U <_{op} G \implies X_U \overset{\text{def}}{=} X_{\rho^{-1}(U)} \overset{\text{fet}}{\to} X$$

$$g_U \overset{\text{def}}{=} g_{X_U}$$

ρ: (G)SRP $\overset{\text{def}}{\iff}$ G: SRP

II.1. Main Theorem.

Th.II.1 (=Th.I.G-1). $H <_{cl} G$ not open Assume that ρ is SRP. Then:

$$\lim_{n\to\infty} g_{HG(n)} = \infty$$

II.2. Proof of Main Theorem.

<u>Step 1. degree $\to \infty$</u>

Claim. $\lim_{n\to\infty} [G : HG(n)] = \infty$

Proof. Otherwise,

$$G = HG(0) \supset \cdots \supset HG(n) \supset \cdots$$

stablizes and $H = \bigcap_{n\geq 0} HG(n)$ is open. $\square$

Step 2. Riemann-Hurwitz

Write $X^{cpt} \smallsetminus X = \{P_1, \ldots, P_r\}$

$I_{P_i} < G$: inertia at P_i

For $U <_{op} G$, set $\lambda_U \stackrel{\text{def}}{=} \dfrac{2g_U - 2}{[G:U]}$.

By Riemann-Hurwitz formula

$$\lambda_{HG(n)} = 2g - 2 + \sum_{i=1}^{r} (1 - \epsilon_i(n))$$

where

$$\epsilon_i(n) \stackrel{\text{def}}{=} \frac{|I_{P_i,n} \backslash G_n / H_n|}{|G_n / H_n|}$$

In particular, Th.II.1 is clear for $g \geq 2$.

Step 3. Galois closure case

Def. G: group, $H, U < G$

$$K_H(U) \stackrel{\text{def}}{=} \bigcap_{u \in U} uHu^{-1}$$

In other words, $K_H(U)$ is:

– the maximal subgroup of H normalized by U

– the maximal subgroup of G fixing $UH/H \subset G/H$ (elementwise)

In particular, $K_H(G)$ is:
– the maximal normal subgroup of G
contained in H
– the kernel of the action $G \curvearrowright G/H$

For $I < G$, write $I_H \stackrel{\text{def}}{=} I/(I \cap K_H(G))$.
Then I_H is:
– the image of the action $I \curvearrowright G/H$

Set $\widetilde{G}(n) \stackrel{\text{def}}{=} K_{HG(n)}(G)$. In particular,

$$G(n) < \widetilde{G}(n) < HG(n).$$

Then $X_{\widetilde{G}(n)} \to X$ is:

– Galois closure of $X_{HG(n)} \to X$

By Riemann-Hurwitz formula

$$\lambda_{\widetilde{G}(n)} = 2g - 2 + \sum_{i=1}^{r} (1 - \widetilde{\epsilon}_i(n))$$

where

$$\widetilde{\epsilon}_i(n) \stackrel{\text{def}}{=} \frac{1}{|(I_{P_i,n})_{H_n}|}$$

Claim. $\lim_{n\to\infty}[G : \widetilde{G}(n)] = \infty$

(*Proof.*) $[G : \widetilde{G}(n)] \geq [G : HG(n)] \to \infty$ $\square$

Claim. $\lim_{n\to\infty} g_{\widetilde{G}(n)} = \infty$

(*Proof.*) Otherwise, $\sup_{n\geq 0}\{g_{\widetilde{G}(n)}\} \leq 1$. By classification of finite automorphism groups of curves of genus ≤ 1:

$$\exists n_0 \geq 0,\ \widetilde{G}(n_0)/\widetilde{G}(\infty) \twoheadleftarrow \mathbb{Z}_\ell^2$$

where $\widetilde{G}(\infty) = \bigcap_{n\geq 0} \widetilde{G}(n)$.

This contradticts the SRP assumption. $\square$

Claim. $\lim_{n\to\infty} \lambda_{\widetilde{G}(n)} = \lambda > 0$

where

$$\lambda = 2g-2+\sum_{i=1}^{r}(1-\widetilde{\epsilon}_i),\ \widetilde{\epsilon}_i \stackrel{\text{def}}{=} \frac{1}{|(I_{P_i})_H|}$$

(*Proof.*) The limit formula is clear. As $\lambda_{\widetilde{G}(n)}$ is monotonously non-decreasing in n and positive for $n \gg 0$, one has $\lambda > 0$. □

Step 4. Estimate of local terms

Thus, it suffices to prove $\lim_{n\to\infty} \epsilon_i(n) = \widetilde{\epsilon}_i$ for each $i = 1, \ldots, r$, where

$$\epsilon_i(n) = \frac{|I_{P_i,n} \backslash G_n/H_n|}{|G_n/H_n|}$$

$$\widetilde{\epsilon}_i = \frac{1}{|(I_{P_i})_H|}$$

Indeed, then $\lim_{n\to\infty} \lambda_{HG(n)} = \lambda > 0$, hence $\lim_{n\to\infty} g_{HG(n)} = \infty$, as desired.

This is reduced to the following general:

Th.II.2. $H, I <_{cl} G <_{cl} GL_d(\mathbb{Z}_\ell)$
Assume:

$$(\sharp)\ \forall n \geq 0,\ K_H(G(n)) = K_H(G)$$

Then:

$$\lim_{n\to\infty} \frac{|I_n \backslash G_n / H_n|}{|G_n/H_n|} = \frac{1}{|I_H|}$$

Step 5. Proof of Th.II.2

Claim. $(G/H)^I \subset_{cl} G/H$ is thin (i.e. has no interior point) unless $I_H = 1$.

(*Proof.*) Otherwise, $\exists n \geq 0$, $\exists g \in G$

$$gG(n)H/H \subset (G/H)^I$$

But this is equivalent to:

$$I \subset gK_H(G(n))g^{-1} \overset{(\sharp)}{=} gK_H(G)g^{-1}$$

Thus, $I_H = 1$. $\square$

Claim. $\lim_{n\to\infty} \frac{|(G_n/H_n)^{I_n}|}{|G_n/H_n|} = 0$
unless $I_H = 1$.

(*Proof.*) Write $\mathcal{X}_I$ for the inverse image of $(G/H)^I$ in G. Then:

$$\mathcal{X}_I \subset_{cl} G \subset_{cl} GL_d(\mathbb{Z}_\ell) \subset_{cl} \mathbb{Z}_\ell^{d^2+1}$$

are ℓ-adic analytic subsets of $\mathbb{Z}_\ell^{d^2+1}$.

Th.(Serre-Oesterlé)

$Z \subset_{cl} \mathbb{Z}_\ell^N$ ℓ-adic analytic

$\implies 0 < \exists C_Z < \infty$, s.t.

$$|Z_n| \sim C_Z \cdot \ell^{n \dim(Z)}$$

Thus:

$$\begin{aligned}
&\lim_{n\to\infty} \frac{|(G_n/H_n)^{I_n}|}{|G_n/H_n|} \\
&= \lim_{n\to\infty} \frac{|(\mathcal{X}_I)_n|}{|G_n|} \\
&= \lim_{n\to\infty} \frac{C_{\mathcal{X}_I} \cdot \ell^{n\dim(\mathcal{X}_I)}}{C_G \cdot \ell^{n\dim(G)}} = 0. \ \square
\end{aligned}$$

For simplicity, treat the case $|I_H| < \infty$. Set

$$X_n \stackrel{\text{def}}{=} G_n/H_n,$$
$$X'_n \stackrel{\text{def}}{=} \bigcup_{I_H > J \neq 1} X_n^J,$$
$$Y_n \stackrel{\text{def}}{=} X_n \setminus X'_n.$$

Thus, Y_n is the maximal subset of X_n on which I_H acts freely.

$$
\begin{aligned}
\frac{|X_n|}{|I_H|} &\leq \underline{\underline{|I_n \backslash X_n|}} = |I_n \backslash Y_n| + |I_n \backslash X_n'| \\
&\leq \frac{|Y_n|}{|I_H|} + |X_n'| \\
&= \frac{|X_n|}{|I_H|} + \left(1 - \frac{1}{|I_H|}\right) |X_n'|
\end{aligned}
$$

Now, Th.II.2 follows since

$$
\frac{|X_n'|}{|X_n|} \leq \sum_{I_H > J \neq 1} \frac{|X_n^J|}{|X_n|} \to 0 \ (n \to \infty).
$$

Step 6. Assumption (♯)

$$K_H(G) = K_H(G(0)) <_{cl} K_H(G(1)) <_{cl} \cdots K_H(G(n)) <_{cl} K_H(G(n+1)) \cdots$$

Lem. G: compact ℓ-adic Lie group
Any sequence

$$H_0 <_{cl} H_1 <_{cl} \cdots <_{cl} H_n <_{cl} \cdots <_{cl} G$$

stabilizes. □

So, (♯) is available after replacing X with $X_{HG(n)}$ for $n \gg 0$. □

A uniform open image theorem for ℓ-adic representations of étale fundamental groups, III

January 27, 2010

Anna Cadoret
(IMB, Univ. Bordeaux 1)
Akio Tamagawa
(RIMS, Kyoto Univ.)

III.0. Notations and Definitions.

Given $G <_{cl} GL_d(\mathbb{Z}_\ell)$ and $n \geq 0$

$$G_n \stackrel{\text{def}}{=} \text{Im}(G \to GL_d(\mathbb{Z}/\ell^n\mathbb{Z}))$$

$$G(n) \stackrel{\text{def}}{=} \text{Ker}(G \to GL_d(\mathbb{Z}/\ell^n\mathbb{Z}))$$

Def. G is SRP

$\stackrel{\text{def}}{\Longleftrightarrow}$ $\forall U <_{op} G,\ |U^{ab}| < \infty$

$k = \overline{k}$, char. $= 0$

X^{cpt}: proper (smooth, connected) curve $/k$

$X \subset X^{cpt}$: open $\neq \emptyset$

$g \stackrel{\text{def}}{=} g_X \stackrel{\text{def}}{=}$ genus of X^{cpt}

$\gamma \stackrel{\text{def}}{=} \gamma_X \stackrel{\text{def}}{=}$ gonality of X^{cpt}

$(\stackrel{\text{def}}{=} \min\{\deg(f) \mid f : X^{cpt} \to \mathbb{P}^1_k\})$

$\gamma_X = 1 \iff g_X = 0$

$\gamma_X = 2 \iff$ either $g_X = 1$

or $g_X \geq 2$, X is hyperelliptic

$\gamma_X \leq (g_X + 3)/2$

$$\rho : \pi_1(X) \stackrel{\text{cont}}{\to} GL_d(\mathbb{Z}_\ell)$$

$$G \stackrel{\text{def}}{=} \rho(\pi_1(X)) \ (= \text{“}G^{geo}\text{”})$$

$$U <_{op} G \implies X_U \stackrel{\text{fet}}{\to} X$$

$$g_U \stackrel{\text{def}}{=} g_{X_U}, \ \gamma_U \stackrel{\text{def}}{=} \gamma_{X_U},$$

$$\rho\text{: (G)SRP} \stackrel{\text{def}}{\iff} G\text{: SRP}$$

III.1. Main Theorem.

Th.III.1. $H <_{cl} G$ not open
Put one of the following assumptions:

(a) ρ is SRP. (Th.I.G-2)

(b) $\mathrm{codim}_G(H) \geq 3$.

Then:

$$\lim_{n \to \infty} \gamma_{HG(n)} = \infty$$

Rem.1. Th.III.1(a) is stronger than Th.II.1.

2. Th.III.1(a) is proved via Th.II.1.

3. Th.III.1(b) implies:

$$\operatorname{codim}_G(H) \geq 3 \implies \lim_{n\to\infty} g_{HG(n)} = \infty$$

But we do not know any direct proof (i.e. not via Th.III.1(b)) of this statement.

III.2. Proof of Main Theorem.

Step 1. Reduction

For a cover $f : Y \to X$, Riemann-Hurwitz gives a complete descripton of g_Y in g_X, $\deg(f)$ and ramifications. Also, $g_X \leq g_Y$.

In the case of gonality:

– No such complete description is available.

– Rough inequalities are available:

$$\gamma_X \leq \gamma_Y \leq \deg(f)\gamma_X$$

Here, the 1st inequality is too rough to get a good estimate of γ_Y. But the 2nd inequality allows us to make the following important reduction: One may replace X with any $X' \to X$ freely.

In particular, one may assume that $G = G(n_0)$ for $n_0 \gg 0$ by replacing X with $X_{G(n_0)} \to X$, unlike the genus case. We fix such an n_0.

Step 2. Successive Galois covers

Lem. $H <_{cl} G <_{cl} GL_d(\mathbb{Z}_\ell)$
Assume $G = G(n_0)$ for some $n_0 > 0$ and let $0 \leq k \leq n_0$. Then:

(i) $HG(n+k) \triangleleft HG(n)$ for $\forall n \geq 0$.

(ii) $HG(n)/HG(n+k) \simeq (\mathbb{Z}/\ell^k)^\Delta$ for $\forall n \gg 0$, where $\Delta \stackrel{\text{def}}{=} \mathrm{codim}_G(H)$.

(*Proof.*) (i) Direct computation.
(ii) Direct computation, together with Serre:
For $n \gg 0$,

$$[G : G(n)] = C_G \cdot \ell^{n\,\dim(G)},$$
$$[H : H(n)] = C_H \cdot \ell^{n\,\dim(H)}. \quad \square$$

Thus, our tower

$$\cdots \to X_n \to \cdots \to X_1 \to X_0 = X$$

with $X_n \stackrel{\text{def}}{=} X_{HG(n)}$ satisfies:

– $X_n \to X_{n-1}$ is Galois with group Γ_n

– $\Gamma_n \simeq (\mathbb{Z}/\ell)^\Delta$ for $n \gg 0$

More generally, if we set $X_n \stackrel{\text{def}}{=} X_{HG(nk)}$ for some $0 \le k \le n_0$:

– $X_n \to X_{n-1}$ is Galois with group Γ_n

– $\Gamma_n \simeq (\mathbb{Z}/\ell^k)^\Delta$ for $n \gg 0$

Step 3. Galois cover and gonality

Given a diagram of proper curves over k:

$$(*) \qquad \begin{array}{ccc} Y & \xrightarrow{\pi} & Y' \\ {\scriptstyle f}\downarrow & & \\ B & & \end{array}$$

where

– $f : Y \to B$ is a non-constant morphism,

– $\pi : Y \to Y'$ is a (possibly ramified) Galois cover with group Γ.

Then:

$(*)$ is equivariant $\overset{\text{def}}{\Longleftrightarrow}$ $\forall \sigma \in \Gamma$, $\exists \sigma_B \in \mathrm{Aut}_k(B)$, s.t. $f \circ \sigma = \sigma_B \circ f$

$(*)$ is primitive $\overset{\text{def}}{\Longleftrightarrow}$ for any factorization $Y \overset{f'}{\to} B' \to B$ of f with $\deg(f') > 1$, the diagram

$$(*) \qquad \begin{array}{ccc} Y & \overset{\pi}{\to} & Y' \\ {\scriptstyle f'} \downarrow & & \\ B' & & \end{array}$$

is not equivariant.

Lem. (T, J.Alg.Geom.13(2004))
If $(*)$ is primitive, then

$$\deg(f) \geq \sqrt{\frac{g_Y + 1}{g_B + 1}}$$

Rem. When $\deg(f)$ is a prime, $(*)$ is either equivariant or primitive. In general, we can construct an "equivariant-primitive decomposition" of $(*)$.

Step 4. Key technical result

Th.III.2. Let

$(\star)\ \cdots \to Y_n \to \cdots \to Y_1 \to Y_0$

be a tower of proper curves over k such that $Y_n \to Y_{n-1}$ is (possibly ramified) Galois with group Γ_n. Then one of the following holds:

(i) $\lim_{n\to\infty} \gamma_{Y_n} = \infty$

(ii) $\exists N \geq 0$, s.t. $\gamma_{Y_n} = \gamma$ for $\forall n \geq N$ and $(\star)$ fits into:

$$\begin{array}{ccccccccc} \cdots \to & Y_n & \to & Y_{n-1} & \to \cdots \to & Y_N & \to \cdots \\ & {\scriptstyle f_n}\downarrow & & \downarrow & & \downarrow & \\ \cdots \to & B_n & \to & B_{n-1} & \to \cdots \to & B_N & \end{array}$$

where

– $B_n \to B_{n-1}$ is Galois with group Γ_n

– each square $\begin{array}{ccc} Y_n & \to & Y_{n-1} \\ \downarrow & & \downarrow \\ B_n & \to & B_{n-1} \end{array}$ is cartesian

(up to normalization) and Γ_n-equivariant

– either $g_{B_n} = 0$, $\deg(f_n) = \gamma$ for $\forall n \geq N$
or $g_{B_n} = 1$, $\deg(f_n) = \gamma/2$ for $\forall n \geq N$

(*Proof.*) One may assume:

– $|\Gamma_n| > 1$ for infinitely many n

– $\lim_{n\to\infty} g_{Y_n} = \infty$ (Otherwise, $\sup_{n\geq 0}\{g_{Y_n}\} \leq 1$. Set $B_n \stackrel{\text{def}}{=} Y_n$ for $n \gg 0$.)

– in particular, $g_{Y_n} \geq \gamma^2$ for $\forall n \geq 0$

– $\gamma_{Y_n} = \gamma$ for $\forall n \geq 0$

Moreover, for simplicity, put the following extra assumptions:

– γ is a prime

– $(\gamma, |\Gamma_n|) = 1$ for $\forall n > 0$

– Γ_n contains an element of order ≥ 3

Now, consider any $n > 0$ and any $f : Y_n \to B$ with $\deg(f) = \gamma$ and $g_B = 0$, and the resulting diagram

$$(*) \qquad \begin{array}{ccc} Y_n & \to & Y_{n-1} \\ {\scriptstyle f}\downarrow & & \\ B & & \end{array}$$

As γ is a prime, $(*)$ is either equivariant or primitive. In the latter case, one has

$$\gamma = \deg(f) \geq \sqrt{\frac{g_{Y_n} + 1}{g_B + 1}} \geq \sqrt{\gamma^2 + 1}$$

which is absurd.

So, (∗) must be equivariant, and fits into a cartesian square:

$$\begin{array}{ccc} Y_n & \to & Y_{n-1} \\ {\scriptstyle f}\downarrow & & {\scriptstyle f'}\downarrow \\ B & \to & B' \end{array}$$

where $B' \stackrel{\text{def}}{=} B/\Gamma_n$. The correspondence $f \mapsto f'$ defines a projective system $(\mathcal{F}_n)_{n>0}$, where $\mathcal{F}_n$ is the set of $f : Y_n \to B$ with $\deg(f) = \gamma$ and $g_B = 0$ modulo isomorphisms.

Claim. $|\mathcal{F}_n| < \infty$

(*Proof.*) Reduced to the case that Γ_n is cyclic of order ≥ 3, where one can prove the desired finiteness via Kummer theory for function fields. $\square$

Now, $\varprojlim_n \mathcal{F}_n \neq \emptyset$, which completes the proof of Th.III.2. $\square$

Step 5(a). End of proof of Th.III.1(a).

Apply Th.III.2 to our tower $(X_n = X_{HG(n)})$ and obtain:

$$\begin{array}{ccccccccc} \cdots \to & X_n^{cpt} & \to \cdots \to & X_N^{cpt} & \to \cdots \to & X^{cpt} \\ & {\scriptstyle f_n}\downarrow & & \downarrow & & \\ \cdots \to & B_n & \to \cdots \to & B_N & & \end{array}$$

One can choose $B_N^{op} \subset B_N$ and $X_N^{op} \subset X_N$ such that $f_N : X_N^{cpt} \to B_N$ restricts to $X_N^{op} \xrightarrow{\text{fet}} B_N^{op}$. Then, replacing

– X with B_N^{op}

– ρ with "$\mathrm{Ind}_{\pi_1(X_N^{op})}^{\pi_1(B_N^{op})} \mathrm{Res}_{\pi_1(X_N^{op})}^{\pi_1(X)} \rho$"

Th III.1(a) is reduced to Th.II.1.

Step 5(b). End of proof of Th.III.1(b).

Apply Th.III.2 to our tower $(X_n = X_{HG(n)})$ and obtain:

$$\begin{array}{ccccccccc} \cdots \to & X_n^{cpt} & \to \cdots \to & X_N^{cpt} & \to \cdots \to & X^{cpt} \\ & {\scriptstyle f_n} \downarrow & & \downarrow & & \\ \cdots \to & B_n & \to \cdots \to & B_N & & \end{array}$$

Here, $\mathrm{Aut}(B_n/B_{n-1}) = \Gamma_n \simeq (\mathbb{Z}/\ell)^\Delta$ for $n \gg 0$.

As $\Delta \geq 3$, this is impossible by classification of finite automorphism groups of curves of genus ≤ 1. $\square$

III.3. Concluding Remarks.

We have applied Th.III.1 to obtain the following arithmetic results in I, where

– k: field finitely generated over $\mathbb{Q}$

– X: curve over k

Th.III.3 (=Th.I.1). Given:
$\rho : \pi_1(X) \to GL_d(\mathbb{Z}_\ell)$, $\delta \geq 1$

(a) If ρ is GSRP

$$X_{\rho,\delta} \stackrel{\text{def}}{=} \{x \in X^{\leq \delta} \mid G_x < G \text{ not open}\}$$

is finite, and $\exists N = N_{\rho,\delta} \geq 1$ such that $G_x > G(N)$ for $\forall x \in X^{\leq \delta} \smallsetminus X_{\rho,\delta}$.

(b) In general

$$X_{\rho,\delta,\geq 3} \stackrel{\text{def}}{=} \{x \in X^{\leq \delta} \mid \text{codim}_G(G_x) \geq 3\}$$

is finite.

CorIII.1 (=Cor.I.1). Given:
$A \to X$: abelian scheme, ℓ: prime, $\delta \geq 1$
Then $\exists N = N_{A,\ell,\delta}$ such that

$$A_x[\ell^\infty](k(x)) \subset A_x[\ell^N]$$

for $\forall x \in X^{\leq \delta}$.

Toward generalizations of arithmetic results like Th.III.4 and Cor.III.1, we first try to generalize geometric results like Th.II.1 and Th.III.1 in the following situations:

– $\dim(X) > 1$

– ℓ varies

For this, don't miss Anna's talk IV!