Oct. 16, 2008

Forschungsseminar über Fontaine-Ouyang: ℓ-adic Galois representations (*Hélène Esnault*)

1. Profinite topology

1.1. K field, $K^s \supset K$ separable closure, then $G_K = \mathrm{Gal}(K^s/K) = \mathrm{Aut}(K^s/K) = \varprojlim_L \mathrm{Aut}(L/K)$, where L/K finite Galois. By definition, profinite. It induces a topology on G_K: coarsest topology for which surjective morphisms $G \twoheadrightarrow H$, with H finite with discrete topology, are continuous. Thus fundamental system of open neighbourhoods of 1 consists of the $\mathrm{Ker}(G \twoheadrightarrow H,\ H)$ finite. Thus $G = \sqcup_H \pi^{-1}(h)$, with $\pi^{-1}h \xrightarrow{\text{homeo}} \pi^{-1}(1)$, this Ker normal subgroup which is *both* closed and open. Further, G compact.

1.2. Assume E topological field, e.g. E is a finite extension of $\mathbb{Q}_\ell$. $\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n$ is a profinite (abelian) group, thus has the profinite topology. It induces topology on $\mathbb{Q}_\ell$ where a fundamental system of open neighbourhoods of 0 consists of the $\ell^n\mathbb{Z}_\ell$. This topology is compatible with the multiplication on $\mathbb{Q}_\ell$, thus $\mathbb{Q}_\ell$ topological field, and $E/\mathbb{Q}_\ell$ finite inherits a topology: a fundamental system of neighbourhoods of 0 is $\ell^n R$ where $R \subset E$ is the ring of integers.

1.3. V finite dimensional vector space over E finite over $\mathbb{Q}_\ell$: topological vector space, where for any basis v_i, the topology is the product topology via $V \cong_E \oplus E \cdot v_i$. A fundamental system of open neighbourhoods of 0 consists of *lattices*, i.e. $L \subset V$ R-submodule of finite type with $L \otimes_R E = V$. In fact, choosing v_i, the lattices $\oplus \ell^n R \cdot v_i$ for all n is also a system of fundamental neighbourhoods of 0.

1.4. $\mathrm{End}_R(V) \cong V^\vee \otimes_E V$ as a E-vector space inherits the topology of this vector space. $\mathrm{Aut}_E(V) \subset \mathrm{End}_E(V)$ is defined by $\det \neq 0$, thus is an open. A fundamental system of open neighbourhoods of 0 in $\mathrm{End}(V)$ consists then of the $L_1^\vee \otimes_R L_2$, i.e. of the $f : V \to V$ with $f(L_1) \subset L_2$ for two given lattices. Thus a fundamental system of neighbourhoods of 1 in $\mathrm{Aut}(V)$ consists of the $\mathcal{U}(L_1 \subset L_2) := \{f : V \to V \text{ with } f \in \mathrm{Aut}(V),\ f(L_1) \subset L_2\}$ for two given lattices L_i and with $L_1 \subset L_2$ (as 1 has to be in this neighbourhood).

Definition 1. *A representation $G_K \to \mathrm{Aut}_E(V)$ is continuous if it is continuous for the profinite topology on both sides. It is called an ℓ-adic representation.*

Proposition 2. *Let $\rho : G_K \to \mathrm{Aut}_E(V)$ be a representation. Then ρ is an ℓ-adic representation (i.e. is continuous) if and only there is a lattice $L \subset V$ with a factorization*

$$\begin{tikzcd} G_K \arrow[r, "\rho"] \arrow[dr, "\exists"'] & \mathrm{Aut}_E(V) \\ & \mathrm{Aut}_R(L) = \varprojlim_n \mathrm{Aut}_R(L/\ell^n) \arrow[u] \end{tikzcd}$$

Proof. Assume ρ is continuous. Choose a lattice $L_0 \subset V$, then

$$\rho^{-1}\mathcal{U}(L_0 \subset L_0) = \{g \in G_K, \rho(g)(L_0) \subset L_0\}$$

is then an open subgroup, i.e. it contains a normal open subgroup, thus the set of residue classes $G/\rho^{-1}\mathcal{U}(L_0 \subset L_0)$ is finite, thus

$$\rho(G)(L_0) = (\rho(G)/\rho^{-1}\mathcal{U}(L_0 \subset L_0))(L_0)$$

is a lattice as well, and is invariant under G. The converse is obvious. $\square$

2. Finite fields

$K = \mathbb{F}_q$ finite field.

2.1. Abstract ℓ-adic representation.

Definition 3. *Geometric Frobenius $\tau_K \in G_K, \lambda \mapsto \lambda^{\frac{1}{q}}$. So $G_K = \hat{\mathbb{Z}} \cdot \tau_K$.*

Lemma 4. *$\rho : G_K \to \mathrm{Aut}_E(V)$ ℓ-adic representation, then by ρ uniquely determined by $\rho(\tau_K) = u \in \mathrm{Aut}_E(V)$. Then for a $u \in \mathrm{Aut}_E(V)$, there is an ℓ-adic representation ρ with $\rho(\tau_K) = u$ if and only if the eigenvalues of u in $\bar{\mathbb{Q}}_\ell \supset E$ are ℓ-adic units, i.e. in $S^\times$ for $S \supset R$ a finite extension.*

Proof. The statement is equivalent to saying that u has to stabilize a lattice. $\square$

Definition 5. *$P_\rho(t) = \det(1 - \tau_K \cdot t) \in \bar{\mathbb{Z}}_\ell[t]$ is the characteristic polynomial of ρ.*

2.2. Weil conjectures.

X/K variety. As

$$H^i(\bar{X}, \mathbb{Q}_\ell) := \varprojlim_n H^i(\bar{X}, \mathbb{Z}_\ell/n) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

and G acts on $H^i(\bar{X}, \mathbb{Z}_\ell/\ell^n)$, Proposition 2 implies that the action of G coming from the geometric Frobenius on $\bar{X}$ is an ℓ-adic representation.

Definition 6. 1) *Geometric Frobenius: $F : X \to X$ which is the identity on the topological space and is the morphism $f \mapsto f^q$ on $\mathcal{O}_X$. Induces the geometric Frobenius F : " $=$" $F \otimes 1$ on $X \otimes \bar{K}$.*

2) *Arithmetic Frobenius: F_K : $\operatorname{Spec} \bar{K} \to \operatorname{Spec} \bar{K}$ induced from $\bar{K} \to \bar{K}, \lambda \mapsto \lambda^q$.*

3) *Absolute Frobenius:*

$$\begin{tikzcd}
\bar{X} \arrow[r, "F"] \arrow[rr, bend left, "F_{\mathrm{abs}}"] \arrow[dr] & \bar{X} \otimes_{F_K} \bar{K} \arrow[r, "F_K"] \arrow[d] & \bar{X} \arrow[d] \\
& \operatorname{Spec} \bar{K} \arrow[r, "F_K"] & \operatorname{Spec} \bar{K}
\end{tikzcd}$$

with $F_{\mathrm{abs}} : \mathcal{O}_{\bar{X}} \to \mathcal{O}_{\bar{X}}, f \mapsto f^q$. Thus $F_{\mathrm{abs}} = \mathrm{Id}$ on any cohomology which depends only on the underlying topological space.

Lemma 7. *$F = F_K^{-1}$ on $H^i(\bar{X}, \mathbb{Q}_\ell)$.*

Definition 8. *Zeta function: $Z_X(t) = \exp\big(\sum_1^\infty \frac{|X(\mathbb{F}_{q^n})|}{n} t^n \big) \in \mathbb{Z}[[t]]$.*

Theorem 9. 1) *Grothendieck-Lefschetz trace formula: $Z_X(t) = \prod P_i(t)^{(-1)^{i+1}}$, with $P_i(t) = \det(1 - Ft|H^i_c(\bar{X}, \mathbb{Q}_\ell))$. In particular, $Z_X(t) \in \mathbb{Q}_\ell(t)$.*

2) *Deligne's algebraicity and integrality: $P_i \in \bar{\mathbb{Z}}[t]$ (usually not expressed, e.g. in [FO]).*

3) *1) with X smooth: functional equation coming from Poincaré duality.*

4 *Deligne's purity: if X is smooth, then $P_i(t)$ is pure of weight i, i.e. $\forall \lambda$ eigenvalue of F on $H^i(\bar{X}, \mathbb{Q}_\ell)$, for all $\mathbb{Q}(\lambda) \subset \mathbb{C}$, $|\lambda| = q^{\frac{i}{2}}$.*

Definition 10. *Algebraic numbers λ such that for all $\mathbb{Q}(\lambda) \subset \mathbb{C}$, $|\lambda| = q^{\frac{\exists i}{2}}$ are called Weil numbers.*

2.3. Some Tannaka categories. Has $\mathrm{Rep}_{\mathbb{Q}_\ell}(G_K)$ the ℓ-adic representations with $E = \mathbb{Q}_\ell$. One defines $\mathrm{Rep}_{\mathbb{Q}_\ell, GEO}(G_K)$ to be the full subcategory spanned subquotients of tensor products of $H^i(\bar{X}, \mathbb{Q}_\ell)$ and its dual for some X projective smooth. By Deligne's purity, $H^i(\bar{X}, \mathbb{Q}_\ell)$ is pure. But we do not know that τ_K-acts semisimply on $H^i(\bar{X}, \mathbb{Q}_\ell)$. It is called the *semi-simplicity conjecture*. If τ_K acted semi-simply on $H^i(\bar{X}, \mathbb{Q}_\ell)$, then any object in $\mathrm{Rep}_{\mathbb{Q}_\ell, GEO}(G_K)$ would be a finite direct sum of irreducible objects, each of which of a specific weight. The analog of the semi-simplicity conjecture in geometry is known, due to Deligne (Hodge II), and called *Théorème de semi-simplicité*: we fix S a smooth variety over $\mathbb{C}$, and consider the category $\mathcal{C}$ of polarizable $\mathbb{Q}$-variations of Hodge structures on some non-trivial open $U \subset S$, definable over $\mathbb{Z}$. As a category, it is Tannaka and semi-simple, due to the polarization. Inside, one can consider the full subcategory $\mathcal{C}_{GEO}$ spanned by subquotients of Gauß-Manin systems of smooth projective morphisms $f : X \to S$. Then Deligne's theorem asserts that $\pi_1^{\text{top}}(U, u)$ acts semi-simply on $H^i(X_u, \mathbb{Z})$.

3. Two further key examples

3.1. Tate module of $\mathbb{G}_m$. Any K.

$$T_\ell(\mathbb{G}_m) = \varprojlim_n \mu_{\ell^n}(K^s)$$

with transition functions $\xi_{n+1} \in \mu_{\ell^{n+1}}(K^s) \mapsto \xi_n = \xi_{n+1}^\ell \in \mu_{\ell^n}(K^s)$. If char. $K = \ell$, then constant prosystem $= 1$. If char. $K \neq \ell$, then by choosing $\xi_n \neq 1$ defines $t := \varprojlim_n \xi_n \in T_\ell(\mathbb{G}_m)$ and $T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell \cdot t$, i.e. for $\lambda = (\lambda_n) \in \varprojlim_n \mathbb{Z}/\ell^n$, $\lambda \cdot t = (\xi_n^{\lambda_n})$. Define $V_\ell(\mathbb{G}_m) := T_\ell(\mathbb{G}_m) \otimes \mathbb{Q} = \mathbb{Q}_\ell \cdot t$. Then G acts on $V_\ell(\mathbb{G}_m)$ via $g(t) = \chi(g) \cdot t, \chi(g) \in \mathbb{Z}_\ell^\times$ thus via a character $\chi : G \to \mathbb{Z}_\ell^\times$ called the *cyclotomic character*. As G compact, $\mathrm{Im}(\chi) \subset \mathbb{Z}_\ell^\times$ closed subgroup. $K = \mathbb{Q}_\ell$, a fortiori $K = \mathbb{Q}$, then χ surjective.

3.2. Tate module of an elliptic curve E. Any K of char. $\neq 2, 3$.

$$T_\ell(E) = \varprojlim_n E(K^s)[\ell^n]$$

with transition functions $p_{n+1} \in E(K^s)[\ell^{n+1}] \mapsto p_n = \ell \cdot p_{n+1} \in E(K^s)[\ell^n]$. If $\ell \neq \mathrm{char} K$, then $E(K^s)[\ell^n] \cong_{\mathbb{Z}/\ell^n} \oplus_1^2 \mathbb{Z}/\ell^n$. if $\ell = \mathrm{char}.K$, then either $E(K^s)[\ell^n] \cong \mathbb{Z}/\ell^n$ if E is ordinary, or $E(K^s)[\ell^n] = \{0\}$ if E is supersingular. One sets $V_\ell(E) = T_\ell(E) \otimes \mathbb{Q}$.

4. Local fields of residue characteristic $p \neq \ell$

K local field of perfect residue field k of char. $p > 0$. Then $K \subset K^{\mathrm{ur}} \subset K^s$ with $K \subset K^{\mathrm{ur}}$ maximal unramified extension. Yields the presentation

$$0 \to I_K \to G_K \to G_k \to 0$$

with I_K :=*inertia*. Has

$$\begin{tikzcd}
 & & \mathbb{Z}_\ell(1) \arrow[rr, "="] & & \mathbb{Z}_\ell(1) & \\
1 \arrow[r] & P_K \arrow[r] & I_K \arrow[u] \arrow[r] & \hat{\mathbb{Z}}'(1) := \prod_{\ell\neq p}\mathbb{Z}_\ell(1) \arrow[rr] & & 1 \\
1 \arrow[r] & P_K \arrow[u, "="] \arrow[r] & P_{K,\ell} \arrow[u, "\mathrm{inj}"] \arrow[r] \arrow[ur, phantom, "\square"] & \hat{\prod}_{\ell'\neq\ell,\ell'\neq p}\mathbb{Z}_{\ell'}(1) \arrow[rr] & & 1
\end{tikzcd}$$

where P_K :=*wild inertia* is the pro-p subgroup of I_K. It defines

$$0 \to P_{K,\ell} \to G_K \to G_{K,\ell} \to 0$$

and

$$1 \to \mathbb{Z}_\ell(1) \to G_{K,\ell} \to G_k \to 1$$

For $\rho : G_K \to \mathrm{Aut}_E(L) \subset \mathrm{Aut}_E(V)$ an ℓ-adic representation, $N_1 = \mathrm{Ker}(\mathrm{Aut}_E(L) \to \mathrm{Aut}_E(L/\ell))$ is a pro-ℓ-group. As $\rho(P_{K,\ell})$ is a profinite group, with all finite quotients of order prime to ℓ, has

$$\rho(P_{K,\ell}) \xrightarrow{\mathrm{inj}} \mathrm{Aut}_R(L/\ell).$$

So

Lemma 11. *There is a finite extension $K' \supset K$ such that ρ restricted to $G_{K'} \subset G_K$ factors through $G_{K',\ell}$.*

Definition 12.
1) *ρ unramified or has good reduction if ρ factors through G_k.*
2) *ρ has potentially good reduction if $\rho(I_K)$ is finite, i.e. if $\exists K' \supset K$ finite such that ρ restricted to $G_{K'}$ has good reduction.*
3) *ρ is semi-stable if I_K acts unipotently, i.e. if semi-simplification has good reduction.*
4) *ρ is potentially semi-stable if true after a finite extension $K' \supset K$.*

Remark 13. Note notation comes from geometry: if X/K has a semi-stable model $\mathcal{X} \to \mathrm{Spec}\, R$, R ring of integers in K, then ℓ-adic representation on étale cohomology is semi-stable. So if one had a semi-stable reduction, every such representation would be potentially semi-stable.

Theorem 14 (Grothendieck)**.** *Assume $\mu_{\ell^\infty}(K)$ is finite. Then any ℓ-adic representation is potentially semi-stable. It applies if k is finite, as $\mu_{\ell^\infty}(K) = \mu_{\ell^\infty}(k)$ by Hensel's lemma.*

Proof. May assume, after replacing K by $K' \supset K$ finite and $\mathbb{Q}_\ell$ by $E \supset \mathbb{Q}_\ell$ finite, $\rho : G_{K,\ell} \to \mathrm{Aut}_R(L)$ and eigenvalues of $\rho(t)$ with $\mathbb{Z}_\ell(1) = \mathbb{Z}_\ell \cdot t$ lies in $R^\times$. Write

$$\rho(t)(v) = a \cdot v$$

for some $a \in R^\times$, $v \neq 0$. Furthermore, as $\mathbb{Z}_\ell(1)$ is a $G_{K,\ell}$ representation via conjugation, has

$$gtg^{-1} = t^{\chi_\ell(g)} \text{ for some character } \chi_\ell : G_{K,\ell} \to \mathbb{Z}_\ell^\times$$

so

$$\rho(gtg^{-1})(v) = \rho(t^{\chi_\ell(g)})(v)$$

i.e.

$$\rho(t)(\rho(g^{-1})(v)) = a^{\chi_\ell(g)} \cdot \rho(g^{-1})(v).$$

So if a is an eigenvalue of $\rho(t)$, so is $a^{\chi_\ell(g)}$ for all $g \in G_{K,\ell}$. On the other hand

$$\mu_{\ell^\infty}(K) \text{ finite } \implies \mathrm{Im}(\chi_\ell) \subset \mathbb{Z}_\ell^\times \text{ infinite.}$$

Since V is finite dimensional, a has to be a root of 1. Thus $\rho(t)$ is quasi-unipotent. □

Corollary 15 (Grothendieck's monodromy theorem)**.** *Let K be a local field. Then any ℓ-adic representation coming from algebraic geometry is potentially semi-stable.*

Proof. An algebraic variety X is defined over a field of finite type $K_0 \subset K$ over the prime field $\mathbb{Q}$ or $\mathbb{F}_p$. Then its closure $K_0 \subset K_1 \subset K$ in K is a complete discrete valuation field with residue field k_1 of finite type over $\mathbb{F}_p$. Take perfect closure k_2 of k_1, and K_2 with residue field k_2 containing K_0. Then $\mu_{\ell^\infty}(K_2) = \mu_{\ell^\infty}(k_2)$ is finite. □

Theorem 16. *Assume $k = \bar{k}$. Then any potentially semi-stable ℓ-adic representation of G_K comes from geometry.*

Proof. Has $G_K = I_K$.
I: Assume ρ semi-stable. Then, since the action of $P_{K,\ell}$ is finite, G_K acts through $\mathbb{Z}_\ell(1)$. So V is a direct sum of Jordan blocks. Since a rank n Jordan block is $\mathrm{Sym}^{\mathrm{n}}(V_2)$ where V_2 is a rank 2 Jordan block, enough to do a rank 2 Jordan block.
Let E be an elliptic curve over K such that

$$E(K^s) \cong (K^s)^\times / \pi^{\mathbb{Z}},$$

where $\mathfrak{m}_K \subset K$ is the maximal ideal, and π is a uniformizer, i.e. a generator of $\mathfrak{m}_K$. Write

$$E(K^s)[\ell^n] = \{a \in (K^s)^\times,\ \exists m,\ a^{\ell^n} = \pi^m\}/\pi^{\ell^n},$$

which yields

$$\begin{gathered} 0 \to \mu_{\ell^n}(K) \to E(K^s)[\ell^n] \to \mathbb{Z}/\ell^n \to 0 \\ a \mapsto m \bmod \ell^n. \end{gathered}$$

Then

$$\alpha = (\alpha_n) \in T_\ell(E),\ \alpha_n \in E(K^s)[\ell^n],\ \alpha_{n+1}^\ell = \alpha_n$$

yields

$$0 \to \mathbb{Z}_\ell(1) \to T_\ell(E) \to \mathbb{Z}_\ell \to 0$$

and thus

$$0 \to \mathbb{Q}_\ell(1) \to V_\ell(E) \to \mathbb{Q}_\ell \to 0.$$

II: Assume ρ potentially semi-stable. Then ρ restricted to $G_{K'}, K' \supset K$ finite is semi-stable. let A be the Weil restriction of E/K'. Then $V_\ell(A) = \mathrm{Ind}_K^{K'} V_\ell(E)$ and it does it. $\square$