SELMER VARIETIES IN THE BIELEFELD-HANNOVER-PADERBORN SEMINAR 21 JUL. 2010

ISHAI DAN-COHEN

Let F be a number field, S a finite set of primes, R the ring of S-integers, v a nonarchimedean valuation corresponding to a prime of R, $\bar{F}$ an algebraic closure of F, F_v the local field at v, R_v its dvr,

$$\bar{F} \hookrightarrow \bar{F}_v$$

a fixed embedding in an algebraic closure of F_v,

$$G_v := \mathrm{Gal}(\bar{F}_v/F_v)\,,$$

$$T := S \cup \{v\}\,,$$

G_T the Galois group of the maximal unramified outside T extension of F, X the complement of a smooth divisor in a smooth proper scheme of relative dimension one over R, $b \in X(R)$ a fixed integral point, $U_n^{\text{ét}}$ the depth n quotient of the unipotent étale fundamental group of $X_{\bar{F}_v}$ at the $\bar{F}_v$-valued point defined by b, $U_n^{\text{ét}}(X_{\bar{F}}, b)$ the depth n quotient of the unipotent étale fundamental group of $X_{\bar{F}}$ at the $\bar{F}$-point defined by b.

Then there's a commuting diagram

$$\begin{array}{ccccc}
X(R) & \longrightarrow & X(R_v) & & \\
\downarrow & & \downarrow & \searrow & \\
H^1_f(G_T, U_n^{\text{ét}}(X_{\bar{F}}, b)(\mathbb{Q}_p)) & \longrightarrow & H^1_f(G_v, U_n^{\text{ét}}(\mathbb{Q}_p)) & \longrightarrow & U_n^{\mathrm{dR}}/F^0(F_v)
\end{array}$$

$$H^1_f(G_T, U_n^{\text{ét}}(X_{\bar{F}}, b)) \longrightarrow H^1_f(G_v, U_n^{\text{ét}}) \longrightarrow \prod_{F_v/\mathbb{Q}_p} U_n^{\mathrm{dR}}/F^0$$

The maps at the bottom are maps of $\mathbb{Q}_p$ schemes, and the middle row comes from the bottom row by taking $\mathbb{Q}_p$ points. This talk will focus mostly on the following features of this picture:

1. the cohomology set $H^1(G_v, U_n^{\text{ét}}(\mathbb{Q}_p))$ and the local unipotent Kummer map

$$X(R_v) \to H^1(G_v, U_n^{\text{ét}}(\mathbb{Q}_p))$$

2. the "Selmer variety" $H^1(G_v, U_n^{\text{ét}})$
3. the f condition.

1. $H^1(G_v, U_n^{\text{ÉT}}(\mathbb{Q}_p))$ and the local unipotent Kummer map

1.1. **Continuous nonabelian group cohomology.** Let G, H be topological groups,

$$G \times H \to H$$

a continuous action. Then we define pointed sets C^i, Z^i, B^i, H^i for small i and maps $d^0 : C^0 \to C^1$, $d^1 : C^1 \to C^2$ as follows. C^i is the set of continuous functions $G^i \to U$ together with the distinguished point $e \in C$ given by $\sigma \mapsto e$; d^0 is given by

$$(du)(\sigma) = u\sigma(u^{-1})\,;$$

d^1 is given by

$$dc(\sigma_1, \sigma_2) = c(\sigma_1\sigma_2)(\sigma_1 c(\sigma_2))^{-1}c(\sigma_1)^{-1}\,.$$

We set $H^0 := (d^0)^{-1}(e) = U^G$, and $Z^1 := (d^1)^{-1}(e)$. We define an action of U on Z^1 by

$$(uc)(\sigma) = uc(\sigma)\sigma(u^{-1})\,.$$

Then H^1 is the set of orbits.

Now let

$$1 \to V \xrightarrow{i} U \xrightarrow{p} W \to 1$$

be a short exact sequence of groups with continuous G action, suppose V is central in U, and, supposing p admits a continuous section, we fix one arbitrarily and call it q. Maps

$$\delta : H^0(W) \to H^1(V) \text{ and } \Delta : H^1(W) \to H^2(V)$$

may be defined as follows. Given $w \in H^0(W)$ lift it to a $u \in U$ and then apply d:

$$\delta(w) := d(u)$$

Similarly, given $c \in Z^1(W)$ use q to lift it to a continuous cochain $b \in C^1(U)$ and then apply d:

$$\Delta(c) := d(b)$$

Proposition 1.1. δ and Δ are well defined, independently of q and give rise to an exact sequence of pointed sets

$$e \to V^G \to U^G \to W^G \to H^1(V) \to H^1(U) \to H^1(W) \to H^2(V)$$

1.2. **Structure of path torsors.** We have the Tannakian category of lisse $\mathbb{Q}_p$ sheaves on $X_{\bar{F}_v}$, and the Tannakian subcategory generated by objects which are unipotent of depth $\leq n$, which is the category of interest. Pullback along

$$\bar{b} : \operatorname{Spec} \bar{F}_v \to X_{\bar{F}_v}$$

defines a fiber functor

$$< e_b^n >: \mathcal{V} \mapsto \bar{b}^{-1}\mathcal{V}$$

and

$U_n^{\text{ét}}$ is the corresponding fundamental group. Let

$\mathcal{A}_n$ denote the coordinate ring. If x is another rational point, we let

$P(x)$ denote the path torsor and

$\mathcal{P}(x)$ its coordinate ring. $P(x)$ has a continuous left action by G_v and a right action by $U_n^{\text{ét}}$. There's also a filtration by finite dimensional vector subspaces

$$0 = \mathcal{P}(x)[0] < \mathcal{P}(x)[1] < \mathcal{P}(x)[2] < \cdots$$

defined roughly as follows. Let

E denote the completed universal enveloping algebra of $\operatorname{Lie} U_n^{\text{ét}}$. It has a G_v action. Let

$\mathcal{E}$ be the corresponding pro-object of our Tannakian category.

Proposition 1.2. There's a canonical isomorphism

$$\bar{x}^{-1}\mathcal{E}^{\wedge} = \mathcal{P}(x)$$

Here the $^{\wedge}$ refers to the dual ind-object. It inherits a $\mathbb{Q}_p$ algebra structure from the coproduct on E. The equality is proved roughly as follows. If R is any $\mathbb{Q}_p$-algebra, then

$$\begin{array}{ccccc}
\operatorname{Hom}_{\mathbb{Q}_p-\mathrm{Alg}}(\bar{x}^{-1}\mathcal{E}^{\wedge}, R) = \overset{\text{grouplike elts in}}{R \otimes \bar{x}^{-1}\mathcal{E}} & = & \otimes\text{- homs} & = & P(x)(R) \\
\downarrow & & \downarrow & & \\
R \otimes \bar{x}^{-1}\mathcal{E} & = & \operatorname{Hom}(< e_b^n >^{(R)}, < e_x^n >^{(R)}) & &
\end{array}$$

Now set:

$E[i] := E/I^i$

$\mathcal{E}[i]$ corresp. lisse sheaf, and define

$\mathcal{P}(x)[i] := \bar{x}^{-1}\mathcal{E}[i]^{\wedge}$

All structural morphisms of $\mathcal{A}_n$ and $\mathcal{P}(x)$ are compatible with the G_v action and with the filtrations. This, in particular, gives rise to the notion of *filtered G_v-equivariant U_n torsor.*

1.3. **The unipotent Kummer map.** We construct a map

$$\{G_v\text{-equivar., filt. } U_n^{\text{ét}}\text{-torsors}\} \to H^1(G_v, U_n^{\text{ét}}(\mathbb{Q}_p))$$

Given P, there's a point $\gamma \in P(\mathbb{Q}_p)$ (Zar. triviality of torsors under unip. groups). For $\sigma \in G_v$ define $u_\sigma \in U(\mathbb{Q}_p)$ by

$$\sigma\gamma = \gamma u_\sigma\,.$$

Then $c : \sigma \mapsto u_\sigma$ will be the corresponding cocycle.

We check the cocycle condition...

$$\begin{aligned} \gamma u_{(\sigma\tau)} &= (\sigma\tau)\gamma = \sigma(\tau\gamma) = \sigma(\gamma u_\tau) \\ &= \sigma(\gamma)\sigma(u_\tau) = \gamma u_\sigma \sigma(u_\tau) \end{aligned}$$

implies

$$u_{(\sigma\tau)} = u_\sigma \sigma(u_\tau)$$

...and give an outline of the proof of continuity:

If i is so large that $\mathcal{A}_n[i]$ generates $\mathcal{A}_n$ then the left regular gives rise to a monomorphism

$$U \to \mathbb{E}\mathrm{nd}_{\mathbb{Q}_p} \mathcal{A}_n[i]$$

hence (by a lemma that shows that any map of finite type schemes gives rise to a continuous map on points) to a continuous injection

$$U(\mathbb{Q}_p) \hookrightarrow \mathrm{End}_{\mathbb{Q}_p}(\mathcal{A}_n[i])$$

So it's enough to check that the composite

$$G_v \to U(\mathbb{Q}_p) \to \mathrm{End}_{\mathbb{Q}_p}(\mathcal{A}_n[i])$$

is continuous. A calculation shows that the composite is given explicitly as follows. The isomorphism

$$U \to P$$

induced by γ gives rise to a continuous isom.

$$\mathcal{A}_n[i] \leftarrow \mathcal{P}[i]$$

which we compose with $\sigma \in G_v$ on one side and σ^{-1} on the other.

Proposition 1.3. This construction gives rise to a biection

$$\{G_v\text{-equivar., filt. } U_n^{\text{ét}}\text{-torsors}\}/\cong \to H^1(G_v, U_n^{\text{ét}}(\mathbb{Q}_p))$$

We thus get a map $X(F_v) \to H^1(G_v, U_n^{\text{ét}}(\mathbb{Q}_p))$.

1.3.1. *abelian example.* Let $X = \mathbb{G}_m$. Then

$$U(\mathbb{Q}_p) = \mathbb{Q}_p(1)\,,$$
$$H^1 = \mathbb{Q}_p \otimes \varprojlim F_v^*/F_v^{*p^n}\,,$$

and the unipotent Kummer map is the natural map

$$F_v^* \to \mathbb{Q}_p \otimes \varprojlim F_v^*/F_v^{*p^n}\,.$$

2. The Selmer variety

U will denote $U_n^{\text{ét}}$
U^i the i^{th} step in the descending central series.
$V_i := U^i/U^{i+1}$

Proposition 2.1. $H^j(G_v, V_i(\mathbb{Q}_p))$ is zero for $j = 0$ and finite dimensional for $j = 1, 2$.

Definition 2.2. $H^1(G_v, U_n)$ is the functor $\mathbb{Q}_p$-Alg $\to$ **Set** given by

$$R \mapsto H^1(G_v, U_n(R))\,.$$

Here, R is given the inductive limit topology and $U_n(R)$ gets its topology from any affine embedding.

Proposition 2.3. $H^1(G_v, U_n)$ is represented by an affine finite type scheme.

Lemma 2.4. $H^1(G_v, V_i) = \mathbb{V}H^1(G_v, V_i(\mathbb{Q}_p))^\wedge$

2.0.2. *sketch of proof of proposition.* For concreteness, let's set n equal to 2. We then have a central extension

$$1 \to V_2 \to U_2 \to V_1 \to 1\,.$$

From this, the vanishing, and the lemma, we get a long exact sequence of pointed sets

$$0 \to H^1(V_2(R)) \to H^1(U_2(R)) \to H^1(V_1(R)) \xrightarrow{\Delta(R)} H^2(V_2(R))$$

functorially in R. Let I denote the pullback

$$\begin{array}{ccc} I & \longrightarrow & H^1(V_2) \\ \downarrow & & \downarrow \Delta \\ \operatorname{Spec} \mathbb{Q}_p & \xrightarrow[e]{} & H^2(V_1)\,. \end{array}$$

I is a (potentially) nonlinear subscheme. Because of the centrality of V_2, left translation inside the group $C^1(U_2(R))$ gives rise to a well defined action of $H^1(V_2(R))$ on $H^1(U_2(R))$, and the proof proceeds by showing that for every R, $H^1(U_2(R))$ is an $H^1(V_2(R))$-torsor over $I(R)$.

3. The f condition

We need to lift the results of the previous section to B_{cris}

Proposition 3.1. $H^j(G_v, V_i(B_{\text{cris}}))$ is finite dimensional for $j = 1, 2$.

Definition 3.2. We let $H^1(G_v, U_n^{B_{\text{cris}}})$ denote the functor from $\mathbb{Q}_p$ algebras to sets

$$R \mapsto H^1(G_v, U_n(R \otimes_{\mathbb{Q}_p} B_{\text{cris}}))$$

Proposition 3.3. $H^1(G_v, U_n^{B_{\text{cris}}})$ is represented by an affine finite type scheme.

Definition 3.4. $H^1_f(G_v, U_n)$ is the pullback of the map induced by

$$U_n(R) \to U_n(R \otimes B_{\text{cris}})$$

along the identity:

$$\begin{array}{ccc} H^1_f(G_v, U_n) & \longrightarrow & H^1(G_v, U_n) \\ \downarrow & & \downarrow \\ \operatorname{Spec} \mathbb{Q}_p & \xrightarrow[e]{} & H^1(G_v, U_n^{B_{\text{cris}}}) \end{array}$$

The following proposition shows that H^1_f, thus defined, parametrizes torsors that are, in a suitable sense, *crystalline*.

Proposition 3.5. Let $P = \operatorname{Spec} \mathcal{P}$ be a G_v-equivariant filtered U_n-torsor. Then $P_{B_{\text{cris}}}$ is trivial iff the map

$$\alpha : D(\mathcal{P}) \otimes_K B_{\text{cris}} \hookrightarrow \mathcal{P} \times_{\mathbb{Q}_p} B_{\text{cris}}$$

is an isomorphism. Here $K \subset F_v$ is the maximal absolutely unramified subfield and

$$D(\mathcal{P}) := (\mathcal{P} \otimes_{\mathbb{Q}_p} B_{\text{cris}})^{G_v}$$

This depends on the theorem of Olsson:

Theorem 3.6. $\mathcal{A}_n$ is ind-crystalline.

3.0.3. *proof of proposition.* Suppose first that $P_{B_{\text{cris}}}$ is trivial, so that there's a G_v-equivariant isomorphism

$$\mathcal{P} \otimes_{\mathbb{Q}_p} B_{\text{cris}} \xrightarrow{\cong} \mathcal{A}_n \otimes_{\mathbb{Q}_p} B_{\text{cris}}$$

Then α, α^{G_v} form a commuting square

$$\begin{array}{ccc} \mathcal{P} \otimes_{\mathbb{Q}_p} B_{\text{cris}} & \xrightarrow{\cong} & \mathcal{A}_n \otimes_{\mathbb{Q}_p} B_{\text{cris}} \\ \uparrow & & \uparrow \\ D(\mathcal{P}) & \xrightarrow[\cong]{} & D(\mathcal{A}_n) \end{array}$$

from which

$$\begin{array}{ccc} \mathcal{P} \otimes_{\mathbb{Q}_p} B_{\text{cris}} & \xrightarrow{\cong} & \mathcal{A}_n \otimes_{\mathbb{Q}_p} B_{\text{cris}} \\ \alpha \uparrow & & \uparrow \cong \\ D(\mathcal{P}) \otimes_K B_{\text{cris}} & \xrightarrow[\cong]{} & D(\mathcal{A}_n) \otimes_K B_{\text{cris}} \end{array}$$

so α is an isomorphism. Now for the converse.

Lemma 3.7. If $\mathcal{P}, \mathcal{P}'$ are crystalline, then so is $\mathcal{P} \otimes_{\mathbb{Q}_p} \mathcal{P}'$ and

$$D(\mathcal{P} \otimes_{\mathbb{Q}_p} \mathcal{P}') = D(\mathcal{P}) \otimes_K D(\mathcal{P}')$$

Assuming the lemma, suppose that α is an isomorphism. Since both $\mathcal{A}_n$ and $\mathcal{P}$ are (ind-)crystalline, the lemma applies to endow $D(\mathcal{P})$ with the structure of a torsor under a unipotent group. So there's an isomorphism

$$D(\mathcal{P}) \cong D(\mathcal{A}_n)$$

equivariant with the (trivial!) G_v action. Hence there are isomorphisms of G_v representations

$$\mathcal{P} \otimes_{\mathbb{Q}_p} B_{\text{cris}} \cong D(\mathcal{P}) \otimes_{\mathbb{Q}_p} B_{\text{cris}} \cong D(\mathcal{A}_n) \otimes_{\mathbb{Q}_p} B_{\text{cris}} \cong \mathcal{A}_n \otimes_{\mathbb{Q}_p} B_{\text{cris}}$$