(φ,Γ)-Modules 6/19/20

Reference for talk: Berger, "Galois representations and (φ,Γ)-modules": Course at IHP from 2010.

§0. Motivating intuition

Let $\mathbb{Q}_{p,\infty} = \mathbb{Q}_p[\zeta_{p^\infty}] = \bigcup_{n\geq 0} \mathbb{Q}_p(\zeta_{p^n})$.

Let $H = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\infty})$, $G = G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, $\Gamma = G/H = \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_p)$.

Then we have an ex. seq.

$$1 \to H \to G_{\mathbb{Q}_p} \to \Gamma \to 1.$$

Also, Let $\chi = \chi_{cyc} : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$, defined by

$$g\zeta_{p^n} = \zeta_{p^n}^{\chi(g)}.$$

Then $H = \mathrm{Ker}(\chi)$ and $\chi : \Gamma \xrightarrow{\sim} \mathbb{Z}_p^\times$ is an iso.

<u>Fact</u> Let $L_\infty/\mathbb{Q}_{p,\infty}$ be a fin. xtn. Then

$$\mathrm{Tr}(m_{L_\infty}) = m_{\mathbb{Q}_{p,\infty}}.$$

<u>Rmk</u> From the point of view of discriminants, this is saying "Finite xtn's of $\mathbb{Q}_{p,\infty}$ are <u>almost</u> unramified." So to study $G_{\mathbb{Q}_p}$, it should be enough to study Γ with some unramified data, like a Frobenius φ.
The point of this talk is to make this intuition precise.

§1. The Rings in char p

Let $\mathbb{C}_p$ be the completion of $\overline{\mathbb{Q}}_p$, which is alg. closed, $\mathcal{O}_{\mathbb{C}_p}$ its closed unit ball.

Let $I \subseteq \mathcal{O}_{\mathbb{C}_p}$ be any ideal containing all elts of valuation at least $\frac{1}{p-1} = \mathrm{val}(\zeta_p - 1)$, which is not maximal.

Here are some rings. A tilde means the ring is perfect.

(1) Let $\widetilde{\mathbb{E}}^+ = \{(x_0, x_1, x_2, \ldots) \mid x_i \in \mathcal{O}_{\mathbb{C}_p}/I,\ x_i = x_{i+1}^p\ \forall i \geq 0\} \underset{\text{as mult. monoids}}{\cong} \varprojlim_{x\mapsto x^p} \mathcal{O}_{\mathbb{C}_p}$. This is a ring in char p. ($+, \cdot$ are component-wise in the first description)

If $x = (x_0, x_1, \ldots) \in \widetilde{\mathbb{E}}^+$, the number $\frac{1}{p^i}\mathrm{val}_p(x_i)$ eventually stabilizes, and we write $\mathrm{val}(x)$ for its limit.
Then $\widetilde{\mathbb{E}}^+$ is a valued ring w/ residue field $\overline{\mathbb{F}}_p$. It is complete

(2) Let $\varepsilon = (1, \zeta_p, \zeta_{p^2}, \ldots) \in \widetilde{\mathbb{E}}^+$, and let $T = \varepsilon - 1$. Then $\mathrm{val}(T) = \frac{p}{p-1}$, and

$$\widetilde{\mathbb{E}} := \widetilde{\mathbb{E}}^+\left[\tfrac{1}{T}\right] \text{ is a field.}$$

<u>Fact</u> $\widetilde{\mathbb{E}}$ is alg closed.

(3) Next, let $\mathbb{E}_{\mathbb{Q}_p} := \mathbb{F}_p((T)) \subseteq \widetilde{\mathbb{E}}$

(4) Finally, take $\mathbb{E} := \mathbb{E}_{\mathbb{Q}_p}^{sep} \subseteq \widetilde{\mathbb{E}}$.

Galois actions:

$G = G_{\mathbb{Q}_p}$ acts continuously on $\mathcal{O}_{\mathbb{C}_p}$, hence on $\tilde{E}^+$ and $\tilde{E}$

G acts on T by

$$gT = g(\varepsilon - 1) = \varepsilon^{\chi(g)} - 1 = (1+T)^{\chi(g)} - 1.$$

We have $G_{\mathbb{Q}_p} \circlearrowright E = E_{\mathbb{Q}_p}^{sep} = \mathbb{F}_p((T))^{sep}$, and hence we get by $\circlearrowright$,

$$H \longrightarrow \mathrm{Gal}(E/E_{\mathbb{Q}_p}).$$

Fact This is an iso: $H \cong \mathrm{Gal}(E/E_{\mathbb{Q}_p})$.

This is nontrivial. Requires knowing $\mathcal{O}_{\mathbb{C}_p}/I \xrightarrow{x \mapsto x^p} \mathcal{O}_{\mathbb{C}_p}/I$ is surj, which, in turn, requires studying ramification of $\mathbb{Q}_{p,\infty}$ carefully.

Rmk The rings $E_{\mathbb{Q}_p}, E, \ldots$ have a Frob. $\varphi : x \mapsto x^p$. Γ acts on $E_{\mathbb{Q}_p}$ (by the above formula)

§2 (φ,Γ)-modules over $E_{\mathbb{Q}_p}$.

Def A (φ,Γ)-module over $E_{\mathbb{Q}_p}$ of dim d is an $E_{\mathbb{Q}_p}$-vector space D of rank d, with semilinear commuting actions of φ and Γ.

Semilinear means:

$$\varphi(v+w) = \varphi(v) + \varphi(w), \quad v, w \in D$$
$$\varphi(cv) = \varphi(c)\varphi(v), \quad c \in E_{\mathbb{Q}_p}, v \in D$$
$$(= c^p \varphi(v))$$

and similarly for $\gamma \in \Gamma$.

Write $\Phi\Gamma^d(E_{\mathbb{Q}_p})$ for the cat. of these.

Thm There is an equivalence of cat's:

$$\mathrm{Rep}^d_{\mathbb{F}_p}(G_{\mathbb{Q}_p}) \xleftrightarrow{\sim} \Phi\Gamma^d(E_{\mathbb{Q}_p})$$
$$V \longmapsto D(V) := (E \otimes_{\mathbb{F}_p} V)^H \quad (H \text{ acts on both factors})$$
$$(E \otimes_{E_{\mathbb{Q}_p}} D)^{\varphi=1} =: V(D) \longleftarrow D$$

pf Berger, Ch. 18. Not too hard. The point is to make use of Hilbert 90.

§3 Lifting from $\mathbb{F}_p$ to $\mathbb{Z}_p$ and $\mathbb{Q}_p$

We would like to define a ring $A_{\mathbb{Q}_p}$ as the Witt vectors of $E_{\mathbb{Q}_p}$. But this is difficult since $E_{\mathbb{Q}_p}$ is not a perfect field. So we instead define $A_{\mathbb{Q}_p}$ as a certain subring of $W(\tilde{E})$. But first:

Recall (Witt vectors) If R is a perfect ring of char p, $\exists!$ (up to iso) ring $W(R)$ s.t.:

meaning $x \mapsto x^p$ is an automorphism.

- p is a nonzero divisor in $W(R)$
- $W(R)/pW(R) \cong R$
- $W(R)$ is separated and complete for the p-adic topology.

Also, if R' is another perfect ring in char p, and $\varphi: R \to R'$ ring hom, then $\exists!$ hom $W(\varphi): W(R) \to W(R')$ lifting φ.

Finally, $\exists!$ multiplicative map $[\cdot]: R \to W(R)$ s.t. $[r] \equiv r \pmod{pW(R)}$.

Eg $W(\mathbb{F}_p) = \mathbb{Z}_p$, and if $\alpha \in \mathbb{F}_p^\times$, then $[\alpha]$ is the $(p-1)$th root of 1 congruent to α mod p.

So now let

$$\tilde{\mathbb{A}} = W(\tilde{\mathbb{E}}), \quad T = [\varepsilon] - 1, \quad \overset{\text{field}}{\tilde{\mathbb{B}}} = \tilde{\mathbb{A}}[\tfrac{1}{p}]$$

and

$$\mathbb{A}_{\mathbb{Q}_p} = \left(\mathbb{Z}_p[[T]][\tfrac{1}{T}]\right)^{\wedge p} \subseteq \tilde{\mathbb{A}}, \quad \overset{\text{field}}{\mathbb{B}_{\mathbb{Q}_p}} = \mathbb{A}_{\mathbb{Q}_p}[\tfrac{1}{p}]$$

If $\mathbb{E}'_{\mathbb{Q}_p}/\mathbb{E}_{\mathbb{Q}_p}$ is fin separable, and $f(X) \in \mathbb{A}_{\mathbb{Q}_p}[X]$ has a primitive elt of $\mathbb{E}'_{\mathbb{Q}_p}$ as a root mod p, then by Hensel and Krasner, $\exists!$ ext'n $\mathbb{B}'_{\mathbb{Q}_p}/\mathbb{B}_{\mathbb{Q}_p}$ with $\mathbb{B}'_{\mathbb{Q}_p}/p\mathbb{B}'_{\mathbb{Q}_p} = \mathbb{E}'_{\mathbb{Q}_p}$ and $[\mathbb{B}'_{\mathbb{Q}_p} : \mathbb{B}_{\mathbb{Q}_p}] = [\mathbb{E}'_{\mathbb{Q}_p} : \mathbb{E}_{\mathbb{Q}_p}]$. (We say $\mathbb{B}'_{\mathbb{Q}_p}/\mathbb{B}_{\mathbb{Q}_p}$ is unramified)

Let $\mathbb{B} = (\text{union of all unram. fin xtns } \mathbb{B}'_{\mathbb{Q}_p} \text{ as above})^{\wedge p}$

Let $\mathbb{A} = \mathbb{B} \cap \tilde{\mathbb{A}}$. (Rings denoted $\mathbb{B}$ are $\mathbb{Q}_p$-alg's, those denoted $\mathbb{A}$ are $\mathbb{Z}_p$-alg's, and those denoted $\mathbb{E}$ are $\mathbb{F}_p$-alg's)

Then:
- $\mathbb{A}/p\mathbb{A} = \mathbb{E}$ $(= \mathbb{E}_{\mathbb{Q}_p}^{sep})$
- $\mathbb{B}$ and $\mathbb{A}$ are stable under $\varphi := W(x \mapsto x^p)$
- $\mathbb{B}$ and $\mathbb{A}$ are stable under the action of $G_{\mathbb{Q}_p}$, defined (on $\tilde{\mathbb{A}}$) as W of this action on $\tilde{\mathbb{E}}$
- $\mathrm{Aut}(\mathbb{B}/\mathbb{B}_{\mathbb{Q}_p}) = \mathrm{Gal}(\mathbb{E}/\mathbb{E}_{\mathbb{Q}_p}) = H$.
- $G_{\mathbb{Q}_p}$ acts through Γ on $T+1 \in \mathbb{A}_{\mathbb{Q}_p}$ as χ_{cyc}.

§4 (φ,Γ)-modules over $\mathbb{A}_{\mathbb{Q}_p}, \mathbb{B}_{\mathbb{Q}_p}$.

<u>Def</u> A (φ,Γ)-module of dim d over $\mathbb{A}_{\mathbb{Q}_p}$ (resp $\mathbb{B}_{\mathbb{Q}_p}$) is a free $\mathbb{A}_{\mathbb{Q}_p}$-mod. of rank d (resp. a d-dim'l $\mathbb{B}_{\mathbb{Q}_p}$-v.s.) with commuting semilinear actions of φ and Γ, s.t.:
- $\varphi \in GL_d(\mathbb{A}_{\mathbb{Q}_p})$ (resp. $\varphi \in GL_d(\mathbb{B}_{\mathbb{Q}_p})$)
- The action of Γ is cts for the <u>weak topology</u> on $\mathbb{A}_{\mathbb{Q}_p}$ (resp. $\mathbb{B}_{\mathbb{Q}_p}$).

The weak topology is obtained from giving $W(\tilde{\mathbb{E}}) = \tilde{\mathbb{A}}$ not only a p-adic topology, but also a topology coming from that on $\tilde{\mathbb{E}}$. See Berger, chapter 16 and the end of chapter 17, for more details.

Write $\Phi\Gamma^d(\mathbb{A}_{\mathbb{Q}_p})$ (resp $\Phi\Gamma^d(\mathbb{B}_{\mathbb{Q}_p})$) for the cat's of such modules.

<u>Def</u> $D \in \Phi\Gamma^d(\mathbb{B}_{\mathbb{Q}_p})$ is étale if $\exists$ a basis of D w.r.t. which $\varphi \in GL_d(\mathbb{A}_{\mathbb{Q}_p})$ (i.e., if it has a φ-stable $\mathbb{A}_{\mathbb{Q}_p}$-lattice). Write $\Phi\Gamma^d_{et}(\mathbb{B}_{\mathbb{Q}_p})$ for these.

Thm There are equiv's of cat's:

$$\mathrm{Rep}^d_{\mathbb{Z}_p}(G_{\mathbb{Q}_p}) \xleftrightarrow{\sim} \Phi\Gamma^d(\mathbb{A}_{\mathbb{Q}_p})$$

$$\mathrm{Rep}^d_{\mathbb{Q}_p}(G_{\mathbb{Q}_p}) \xleftrightarrow{\sim} \Phi\Gamma^d_{et}(\mathbb{B}_{\mathbb{Q}_p})$$

$$V \longmapsto D(V) = (\mathbb{A} \otimes_{\mathbb{Z}_p} V)^H$$

$$(\mathbb{A} \otimes_{\mathbb{A}_{\mathbb{Q}_p}} D)^{\varphi=1} =: V(D) \longleftarrow D$$

§5 More motivating remarks

Rmks (On the use of Γ)

- If $X/\mathbb{F}_p$ is a sm. proj curve, then it is useful to study $\pi_1(X)$ (Étale π_1.) by splitting off $\mathrm{Frob}^{\hat{\mathbb{Z}}}$ from it via:

$$1 \to \pi_1(X_{\overline{\mathbb{F}}_p}) \to \pi_1(X) \to \pi_1(\mathbb{F}_p) \to 1$$

$$\pi_1(\mathbb{F}_p) = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \langle \mathrm{Frob} \rangle$$

- If instead we want to study $\pi_1(F) = \mathrm{Gal}(\overline{F}/F)$ w/ F a nonarch. local field of char 0, we have instead the sequence

$$1 \to \underset{\text{Inertia}}{I_F} \to \mathrm{Gal}(\overline{F}/F) \to \mathrm{Gal}(F^{ur}/F) \to 1$$

$$\mathrm{Gal}(F^{ur}/F) = \mathrm{Gal}(\overline{k}/k) = \langle \mathrm{Frob} \rangle \quad (k = \text{residue field})$$

The piece I_F is much easier to study if we are only asking for ℓ-adic properties of it, and $\ell \neq \mathrm{char}\, k$.

- On the other hand, Iwasawa gives us a hint from the theory of number fields of what to do in order to study $\mathrm{Gal}(\overline{F}/F)$ p-adically.

In fact, he viewed $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$ as analogous to the constant field xtn $\overline{\mathbb{F}}_p(X)/\mathbb{F}_p(X)$ in char p.
(Indeed, the Iwasawa Main Conjecture was motivated in analogy with a theorem of Weil that says that $(\mathrm{CharPoly}(\mathrm{Frob} \mid T_\ell(\mathrm{Jac}(K)))$ can be written in terms of zeta functions)
The p-power torsion of Galois modules are easier to study up the cyclotomic tower, rather than ℓ-torsion.

- So this motivates using $\Gamma = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p)$ as the quotient when studying p-adic properties of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$:

$$1 \to H \to G_{\mathbb{Q}_p} \to \Gamma \to 1$$

Rmk (On the tilt $\tilde{E}^+$)

The char χ_{cyc} is defined as the action of $G_{\mathbb{Q}_p}$ on

$$T_p(\mu_{p^\infty}) := \varprojlim \left(\cdots \to \mu_{p^{n+1}} \xrightarrow{(\cdot)^p} \mu_{p^n} \to \cdots \right)$$

$$= \left\{ (\zeta^{(1)}, \zeta^{(2)}, \zeta^{(3)}, \ldots) \;\middle|\; \zeta^{(n)} \in \mu_{p^n}, (\zeta^{(n+1)})^p = \zeta^{(n)} \ \forall n \right\} \ni \varepsilon.$$

So tilting is perhaps the most natural construction if you want the "cyclotomic period" ε to appear.

Rmk (On Colmez's functor)

The ring $A_{\mathbb{Q}_p}$ is what Colmez calls $\mathcal{O}_{\mathcal{E}}$. It was

$$\left(\mathbb{Z}_p[[T]][\tfrac{1}{T}]\right)^{\wedge_p} = \left\{ \sum_{n\in\mathbb{Z}} a_n T^n \;\middle|\; a_n \in \mathbb{Z}_p \ \forall n,\ a_n \equiv 0 \pmod{p^i}\ \forall\, n > n(i) > -\infty,\ \forall i \right\}$$

$$= \left\{ \sum_{n\in\mathbb{Z}} a_n T^n \;\middle|\; a_n \in \mathbb{Z}_p \ \forall n,\ a_n \xrightarrow{n\to-\infty} 0 \right\}$$

and $B_{\mathbb{Q}_p}$ is $\mathcal{E} = \mathrm{Frac}(\mathcal{O}_{\mathcal{E}})$.

These are rings of functions on p-adic domains, and thus the shift to modules over them is already a step in the right direction towards the p-adic automorphic side.

Colmez's p-adic local Langlands corr. is

$$\mathrm{Montréal} \circ \mathbf{D}.$$