p-adic Hodge Theory

Abstract

This course is lectured by Keerthi Madapusi Pera at Boston College in Fall 2018.

The notes are typewritten by Dalton Fung.

The following parts of the notes are yet to be edited:

(a) The proofs of 2.4, 2.16, 4.2, 4.4, 5.4, 5.7, 5.9.

(b) The material between 3.7 and the rest of the lecture dated Sept 28.

(c) Second example given in the lecture dated Oct 15.

(d) Complements in lecture dated Nov 1, including decompletion and Tate-Sen operator.

(e) A missing diagram in lecture dated Nov 14.

(f) Starting remark in Nov 19.

(g) Index page.

Please send corrections or comments to `fungdc(at)bc.edu`.

Contents

August 27, 2018. Monday.

1. Motivation.

Let X be a smooth projective (algebraic) variety over $\mathbb{C}$. Forgetting any algebraic structures, we can associate with it a smooth compact manifold $X(\mathbb{C})$, and we can look at its singular cohomology $H^i(X(\mathbb{C}), \mathbb{Q})$ with rational coefficients. But the initial algebraic/projective structure on X equips these cohomologies with a Hodge structure, ie.

$$H^i(X(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \cong \bigoplus_{\substack{p+q=i\\ p,q\geq 0}} H^{p,q}, \text{ where } H^{p,q} = H^q(X, \Omega^p) \text{ with } \bar{H}^{p,q} = H^{q,p}.$$

This structure arises from a comparison

$$H^i_B(X, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} H^i_{\mathrm{dR}}(X/\mathbb{C}) = \mathbb{H}^i(X, \underline{\Omega}^\bullet_{X/\mathbb{C}}),$$

where we write H^i_B for singular cohomologies for clarity. We can think of this as taking forms on the right and integrating them along the cycles given from the left hand side – illustrated by an example very soon. This isomorphism is also nice since we are comparing topological and algebraic data.

This becomes interesting when X is defined over number fields or even simply over $\mathbb{Q}$. For the sake of simplicity, let's just suppose for a moment that X is defined over $\mathbb{Q}$. Then we have the de Rham complex $\Omega^\bullet_{X/\mathbb{Q}}$ already over $\mathbb{Q}$, and the de Rham cohomology $H^i_{\mathrm{dR}}(X/\mathbb{Q}) = \mathbb{H}^i(X, \Omega^\bullet_{X/\mathbb{Q}})$ (we can think of this as taking cohomology of the coherent sheaf $\Omega_{X/\mathbb{Q}}$) with

$$H^i_{\mathrm{dR}}(X/\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} = H^i_{\mathrm{dR}}(X/\mathbb{C}).$$

And so we have arrived at the comparison isomorphism

$$H^i_B(X, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \xrightarrow{\sim} H^i_{\mathrm{dR}}(X/\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}.$$

In words, we have two vector spaces over $\mathbb{Q}$, for which after tensoring with $\mathbb{C}$ is naturally isomorphic. Let's consider the example when $X = \mathbb{G}_m$. When $i = 1$, we can think of this isomorphism as a pairing

$$\begin{aligned} H_1(\mathbb{G}_m, \mathbb{C}) \times H^1_{\mathrm{dR}}(X/\mathbb{C}) &\to \mathbb{C} \\ \langle \quad \circlearrowleft \quad , \quad [dz/z] \ \rangle &= \int_{\circlearrowleft} dz/z = 2\pi i \end{aligned}$$

This is called a **period** for $\mathbb{G}_m$. This concludes the story for $\mathbb{C}$, and we move on to $\mathbb{Q}_p$.

We should think of $\mathbb{C}$ as completing $\mathbb{Q}$ at infinite place (yielding $\mathbb{R}$) and taking its algebraic closure. The infinite prime is as good as any other prime, p-adic Hodge theory is trying to mimic the above for finite places. Let's think about what happens when we naively replace $\mathbb{C}$ with $\overline{\mathbb{Q}_p}$ for a moment. Topology isn't good on left, since it's totally disconnected. So here the appropriate analogue of $H^i_B(X, \mathbb{Q})$ will be the p-adic étale cohomology.

Let's start with the example where E is an elliptic curve over $\mathbb{Q}_p$, then we can look at $E[p^n] =$

$\{x \in E(\overline{\mathbb{Q}_p}) : [p^n]x = 0\}$. We can then define the **Tate module** $T_pE = \varprojlim_n E[p^n]$, whch is a 2-dimensional finite free $\mathbb{Z}_p$-module. Our analogue of H^i_B is

$$H^1_{\text{ét}}(E, \mathbb{Q}_p) = \text{Hom}_{\mathbb{Z}_p}(T_pE, \mathbb{Q}_p).$$

As an upshot, $\Gamma := \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ acts on $E[p^n]$, so T_pE is also a continuous representation of Γ. We will talk about how Γ acts on the various terms in the comparison isomorphism later.

Let's go back to $\mathbb{G}_m$ (over $\mathbb{Q}_p$) even if it's not projective because it's simple. We would like to compare $H^1_{\text{ét}}(\mathbb{G}_m, \mathbb{Q}_p)$ and $H^1_{\text{dR}}(\mathbb{G}_m/\mathbb{Q}_p)$.

We can describe $H^1_{\text{ét}}(\mathbb{G}_m, \mathbb{Q}_p)$ as $\text{Hom}_{\mathbb{Z}_p}(T_p\mathbb{G}_m, \mathbb{Q}_p)$, where $T_p\mathbb{G}_m = \varprojlim_n \mu_{p^n}$ and $\mu_{p^n} = \{x \in \overline{\mathbb{Q}_p}^\times : x^{p^n} = 1\}$. Γ acts on $T_p\mathbb{G}_m$ and after dualizing, we get $\text{Hom}_{\mathbb{Z}_p}(T_p\mathbb{G}_m, \mathbb{Q}_p)$ which is a 1-dimensional continuous representation of Γ, given by a character $\chi_p : \Gamma \to \mathbb{Z}_p^\times$ satisfying $\gamma \cdot x = x^{\chi_p(\gamma)^{-1}}$ for $\gamma \in \Gamma$ (on $T_p\mathbb{G}_m$). We can next identify the Γ-action on $T_p\mathbb{G}_m$ with $\mathbb{Z}_p$ and see that the action on $\mathbb{Z}_p$ is given by multiplication by χ_p. Dualizing it, the action on $\text{Hom}_{\mathbb{Z}_p}(T_p\mathbb{G}_m, \mathbb{Q}_p)$ is simply given as multiplication by χ_p^{-1}.

On the other hand, $H^1_{\text{dR}}(\mathbb{G}_m/\mathbb{Q}_p)$ is a 1-dimensional $\mathbb{Q}_p$-vector space generated by $[dz/z]$. What's a natural isomorphism between $H^1_{\text{ét}}$ and H^1_{dR} then? First of all, $\overline{\mathbb{Q}_p}$ is not big enough – it's not complete, so let's define $\mathbb{C}_p$ to be the completion of $\overline{\mathbb{Q}_p}$, which turns out conveniently to be algebraically closed. Is there then a *natural* isomorphism after tensoring with $\mathbb{C}_p$? Or what does *natural* here even mean?

To answer this, one way is to think about the Γ-action – there is a Γ-action on both $H^1_{\text{ét}}$ and $\mathbb{C}_p$ (but on H^1_{dR} the action is trivial since H^1_{dR} is already defined over $\mathbb{Q}_p$). We can then ask for *natural* to mean Γ-*equivariant*. $H^1_{\text{ét}}(\mathbb{G}_m, \mathbb{Q}_p) \otimes \mathbb{C}_p$ as a Γ-representation is isomorphic to $\mathbb{C}_p(\chi_p^{-1})$, a 1-dimensional $\mathbb{C}_p$-vector space with a Γ-action given by $\gamma \cdot \alpha = \chi_p(\gamma)^{-1}(\gamma\alpha)$ ($\alpha \in \mathbb{C}_p$) (we can think of this as the usual Galois action with a twist by χ_p). $H^1_{\text{dR}}(\mathbb{G}_m/\mathbb{Q}_p) \otimes \mathbb{C}_p$ is just $\mathbb{C}_p$ with its canonical Γ-action.

Thus we are asking for a Γ-equivariant isomorphism $\phi : \mathbb{C}_p(\chi_p^{-1}) \xrightarrow{\sim} \mathbb{C}_p$. This is equivalent to specifying $0 \neq \alpha = \phi(1) \in \mathbb{C}_p$ with $\gamma\alpha = \chi_p(\gamma)^{-1}\alpha$ for all $\gamma \in \Gamma$, or equivalently $\alpha \in \mathbb{C}_p(\chi_p^{-1})^\Gamma - \{0\}$. This will be our analogue for $2\pi i$.

However, Tate proved the following

Theorem. (a) $\mathbb{C}_p^\Gamma = \mathbb{Q}_p$ *(ie. completion from $\overline{\mathbb{Q}_p}$ to $\mathbb{C}_p$ does not introduce anything extra in terms of Γ-invariants), and*

(b) $\mathbb{C}_p(\chi_p^i)^\Gamma = \{0\}$ *for $i \in \mathbb{Z} - \{0\}$. (cf. Tate twists)*

And so there is no such α! One solution to this is to consider the graded polynomial ring B_{HT} (HT stands for Hodge and Tate), defined as

$$B_{\text{HT}} := \bigoplus_{i \in \mathbb{Z}} \mathbb{C}_p(\chi_p^i)$$

along with a Γ-action. Then there is a canonical comparison isomorphism

$$H^1_{\text{ét}}(\mathbb{G}_m \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{HT}} \xrightarrow{\sim} H^1_{\mathrm{dR}}(\mathbb{G}_m/\mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{HT}}.$$

Tate next showed

Theorem. *For an abelian variety A over $\mathbb{Q}_p$, there is a canonical Γ-equivariant isomorphism*

$$H^1_{\text{ét}}(A \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{HT}} \xrightarrow{\sim} H^1_{\mathrm{dR}}(A/\mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{HT}}.$$

Moreover, this arises from a Γ-equivariant isomorphism over $\mathbb{C}_p$-vector spaces:

$$H^1_{\text{ét}}(A \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes \mathbb{C}_p \xrightarrow{\sim} (\omega_{A/\mathbb{Q}_p} \otimes \mathbb{C}_p(\chi_p)) \oplus (\mathrm{Lie}\, \widehat{A} \otimes \mathbb{C}_p)$$

where $\omega_{A/\mathbb{Q}_p} = H^0(A, \Omega^1_{A/\mathbb{Q}_p})$, $\widehat{A}$ the dual abelian variety and $\mathrm{Lie}(\widehat{A})$ its Lie algebra.

Note that there is a short exact sequence $0 \to \omega_{A/\mathbb{Q}_p} \to H^1_{\mathrm{dR}}(A/\mathbb{Q}_p) \to \mathrm{Lie}(\widehat{A}) \to 0$, and we can find a splitting (cf. Hodge Tate decomposition) thought it is not canonical.

Faltings then showed a geometric version for this theorem:

Theorem. *For a smooth projective variety $X/\mathbb{Q}_p$, we have a Γ-equivariant isomorphism*

$$H^i_{\text{ét}}(X \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes \mathbb{C}_p \xrightarrow{\sim} \bigoplus_{m+n=i} (H^n(X, \Omega^m_{X/\mathbb{Q}_p}) \otimes \mathbb{C}_p(\chi_p^m)).$$

Note that if we twist both sides by χ_p^{-m}, we get $H^n(X, \Omega^m_{X/\mathbb{Q}_p}) = (H^i_{\text{ét}}(X \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes \mathbb{C}_p(\chi_p^{-m}))^G$, so Hodge cohomology can be recovered from the p-adic étale cohomology.

Fontaine then defined a complete DVR B^+_{dR} with

(a) residue field $\mathbb{C}_p$,
(b) maximal ideal $\mathrm{Fil}^1 B^+_{\mathrm{dR}} \subset B^+_{\mathrm{dR}}$,
(c) a Γ-action on it,
(d) and a canonical uniformizer $t \in \mathrm{Fil}^1 B^+_{\mathrm{dR}}$ (depending on the choice of compatible p-power roots of unity),

and if we set $B_{\mathrm{dR}} := B^+_{\mathrm{dR}}[t^{-1}]$ its fraction field, and $\mathrm{Fil}^i B_{\mathrm{dR}} = t^i B^+_{\mathrm{dR}}$, then there is a canonical isomorphism $\mathrm{gr}\, B_{\mathrm{dR}} \xrightarrow{\sim} B_{\mathrm{HT}}$ with $\mathrm{gr}^1 B_{\mathrm{dR}} \xrightarrow{\sim} \mathbb{C}_p(\chi_p^{-1})$.

With this new construction, Faltings proved that the isomorphism from previous theorem arises from a canonical isomorphism $H^i_{\text{ét}}(X \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes B_{\mathrm{dR}} \xrightarrow{\sim} H^i_{\mathrm{dR}}(X/\mathbb{Q}_p) \otimes B_{\mathrm{dR}}$ of B_{dR}-vector spaces.

Using first theorem of Tate, we find that $H^i_{\mathrm{dR}}(X/\mathbb{Q}_p) = (H^i_{\text{ét}}(X \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes B_{\mathrm{dR}})^\Gamma$ (recovering de Rham cohomology), and the filtration $\mathrm{Fil}^j H^i_{\mathrm{dR}}(X/\mathbb{Q}_p)$ on it can be recovered from $(H^i_{\text{ét}}(X, \mathbb{Q}_p) \otimes \mathrm{Fil}^j B_{\mathrm{dR}})^\Gamma$ (cf. Hodge spectral sequence).

There is actually an additional hidden structure on de Rham cohomology, namely the Frobenius. Grothendieck proved the following

Theorem. *Assume that smooth projective varieties X, X' have good reduction, both with smooth projective special fibre $X_0/\mathbb{F}_p$ (after identifications if necessary). Then there is a canonical isomorphism between $H^i_{\mathrm{dR}}(X/\mathbb{Q}_p) \xrightarrow{\sim} H^i_{\mathrm{dR}}(X'/\mathbb{Q}_p)$.*

(In this theorem, $\mathbb{Q}_p$ here is essential, as opposed to finite extensions of $\mathbb{Q}_p$.) Frobenius on X_0 then endows $H^i_{\mathrm{dR}}(X/\mathbb{Q}_p)$ with a canonical endomorphism ϕ.

August 29, 2018. Wednesday.

Let's take a finite extension $K/\mathbb{Q}_p$, then there is a largest unramified subextension K_0 which is generated by prime-to-p roots of unity. Take a smooth projective variety X over K. Let's write $\overline{X}$ for $X_{\overline{\mathbb{Q}_p}}$ for convenience.

Let's recall what we have talked about. We have discussed two cohomologies $H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_p)$ and $H^i_{\mathrm{dR}}(X/K)$, and $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}_p}/K)$ acts on $H^i_{\text{ét}}$ (this Galois action is rarely continuous). H^i_{dR} is a filtered K-vector space. Last time we have seen a result due to Faltings: there is a canonical isomorphism

$$H^i_{\text{ét}}(X \times_{\mathbb{Q}_p} \overline{\mathbb{Q}_p}, \mathbb{Q}_p) \otimes B_{\mathrm{dR}} \xrightarrow{\sim} H^i_{\mathrm{dR}}(X/\mathbb{Q}_p) \otimes B_{\mathrm{dR}}.$$

There is a natural filtration on the right hand side: there is one on H^i_{dR} and one of B_{dR}, and hence on tensor products. $H^i_{\text{ét}}$ has a trivial filtration, and this isomorphism also preserves the filtration. We can recover the de Rham cohomology from $H^i_{\mathrm{dR}}(X/K) = \mathrm{Fil}^0(H^i_{\text{ét}}(\overline{X}/\mathbb{Q}_p) \otimes B_{\mathrm{dR}})^{\Gamma_K}$.

Last time we have ended with a result by Grothendieck; let's try to generalize it to $K/\mathbb{Q}_p$. Suppose that X has good reduction with special fibre X_0/k (where k the residue field of K), so now X_0 is a smooth projective variety over k. We have the crystalline cohomology (a cohomology that works in characteristic p) $H^i_{\mathrm{cris}}(X_0/K_0)$ which is a K_0-vector space.

This has an additional structure which arises from the Frobenius. We have a diagram

$$\begin{tikzcd} X_0 \arrow[r, dashed, "F_{X_0/k}"] & X_0^{(p)} \arrow[r] \arrow[d] \arrow[dr, phantom, "\ulcorner", very near start] & X \arrow[d] \\ & \operatorname{Spec} k \arrow[r, "F_p"] & \operatorname{Spec} k \end{tikzcd}$$

Here F_p is the Frobenius, and $F_{X_0/k}$ is the relative Frobenius: if $X_0 = \operatorname{Spec} k[T_1, \dots, T_n]/(f_1, \dots, f_r)$, then $X_0^{(p)} = \operatorname{Spec}[T_1, \dots, T_n]/(f_1^{(p)}, \dots, f_r^{(p)})$, where $f_i^{(p)}(T) = \sum a_I^p T^I$ if $f_i(T) = \sum a_I T^I$.

On the other hand, let $\sigma : K_0 \xrightarrow{\sim} K_0$ be the Frobenius automorphism – it's the unique automorphism satisfying $\sigma(\zeta_n) = \zeta_n^p$ for all prime-to-p roots of unity $\zeta_n \in K_0$ (recall that K_0 is predetermined by prime-to-p roots of unity).

With this, the additional structure on $H^i_{\mathrm{cris}}(X_0/K_0)$ is encapsulated in the following commutative diagram:

$$\begin{tikzcd} H^i_{\mathrm{cris}}(X_0^{(p)}/K_0) \arrow[r, "F^*_{X_0/k}"] \arrow[d, phantom, "\cong" rotate=90] & H^i_{\mathrm{cris}}(X_0/K_0) \\ \sigma^* H^i_{\mathrm{cris}}(X_0/K_0) \arrow[ur, "\phi"'] & \end{tikzcd}$$

Note that ϕ is σ-semilinear.

Berthelot and Ogus proved

Theorem. *There is a canonical isomorphism $H^i_{\mathrm{cris}}(X_0/K_0) \otimes_{K_0} K \xrightarrow{\sim} H^i_{\mathrm{dR}}(X/K)$.*

Remark: Grothendieck showed that if $l \neq p$, then there is a canonical isomorphism $H^i(\overline{X}, \mathbb{Q}_l) \xrightarrow{\sim} H^i(\overline{X_0}, \mathbb{Q}_l)$.

This isomorphism allows us to move properties on H^i_{dR} to H^i_{cris} (though we have to apply $\otimes_{K_0} K$. For example, $\Gamma_{\bar{K}}$ acts on H^i_{dR} via the qth-power Frobenius, and thus gives an action on the left hand side as well.

There is a subring $B_{\mathrm{cris}} \subseteq B_{\mathrm{dR}}$ with the following properties:

(a) $B_{\mathrm{cris}}^{\Gamma_K} = K_0$ (instead of K as suggested by Tate previously for B_{dR}), and

(b) there is a Frobenius lift $\phi : B_{\mathrm{cris}} \to B_{\mathrm{cris}}$ (ie. $\phi \pmod p$ is the pth-power map) with $B_{\mathrm{cris}}^{\phi=1} \cap \mathrm{Fil}^0 B_{\mathrm{dR}} = \mathbb{Q}_p$ (cf. the fundamental short exact sequence).

These properties suggest the idea that B_{cris} can only detect the unramified part, and taking ϕ invariants tend to make things nicer.

Faltings then proved the following

Theorem. *There exists a canonical isomorphism*

$$H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}} \to H^i_{\mathrm{cris}}(X_0/K_0) \otimes_{K_0} B_{\mathrm{cris}}.$$

This isomorphism also respects

(a) the Γ_K-action ($g \otimes g$ on the left and $1 \otimes g$ on the right),

(b) the filtration (a priori the filtration on B_{cris} is inherited from B_{dR}) after a base change to K (for the filtration on H_{cris} to make sense via Berthelot-Ogus; also note that B_{cris} does not contain K but only K_0), and

(c) the σ-semilinear map ϕ.

We can recover crystalline cohomology from étale cohomology:

$$H^i_{\mathrm{cris}}(X_0/K_0) = (H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})^{\Gamma_K}$$

as K_0-vector spaces: this is because the latter equals $(H^i_{\mathrm{cris}}(X_0/K_0) \otimes_{K_0} B_{\mathrm{cris}})^{\Gamma_K} = H^i_{\mathrm{cris}}(X_0/K_0) \otimes_{K_0} B_{\mathrm{cris}}^{\Gamma_K}$. Conversely, if we hit both sides by $(-)^{\phi=1} \cap \mathrm{Fil}^0(- \otimes_{B_{\mathrm{cris}}} B_{\mathrm{dR}})$, we can also recover étale cohomology from crystalline and de Rham cohomologies:

$$H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_p) = (H^i_{\mathrm{cris}}(X_0/K_0) \otimes_{K_0} B_{\mathrm{cris}})^{\phi=1} \cap \mathrm{Fil}^0(H^i_{\mathrm{dR}}(X/K) \otimes_K B_{\mathrm{dR}}).$$

(We have secretly used the isomorphism by Berthelot-Ogus in the latter term.) (cf. Grothendieck's mysterious functor)

There exists a version of Berthelot-Ogus for the case semistable reduction, dealing with monodromy over singularities.

Let's define the category $\mathsf{Rep}(\Gamma_K)$ of continuous representations of Γ_K on finite dimensional $\mathbb{Q}_p$-vector spaces. Next we define the functor D_{cris} which sends

$$V \in \mathsf{Rep}(\Gamma_K) \mapsto D_{\mathrm{cris}}(V) = (V \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})^{\Gamma_K}.$$

For example, if $V = H^i_{\text{ét}}(\overline{X}, \mathbb{Q}_p)$ where $\overline{X}$ has a good reduction, we then recover $D_{\text{cris}}(V) = H^i_{\text{cris}}(X_0/K_0)$.

In general, $D_{\text{cris}}(V)$ is a finite dim K_0-vs, with dimension $\dim_{K_0} D_{\text{cris}}(V) \le \dim_{\mathbb{Q}_p} V$. Let's write $D := D_{\text{cris}}(V)$ for simplicity. D has some additional structure:

(a) From $\phi : B_{\text{cris}} \to B_{\text{cris}}$ we obtain a canonical isom $\sigma^* D \xrightarrow{\sim} D$. In general, anything that does not interact with Γ_K will be preserved.

(b) $D \subseteq (V \otimes_{\mathbb{Q}_p} B_{\text{dR}})^{\Gamma_K} =: D_{\text{dR}}(V)$, which is a finite dimensional filtered K-vector space. So $D \otimes_{K_0} K$ inherits a filtration.

Define the category MF_K^{ϕ} of **filtered ϕ-modules over** K, by

$$\mathsf{MF}_K^{\phi} = \{(D, \phi, \mathrm{Fil}^{\bullet}(D \otimes_{K_0} K))\},$$

where

(a) D is a finite dimensional K-vector space,

(b) $\phi : \sigma^* D \xrightarrow{\sim} D$, and

(c) $\mathrm{Fil}^{\bullet}(D \otimes_{K_0} K)$ is a descending filtration by K-vector subspaces.

These objects are called isocrystals, and there is a complete classification of isocrystals by Manin.

Next we say that V is **crystalline** if $\dim_{K_0} D_{\text{cris}}(V) = \dim_{\mathbb{Q}_p}(V)$, or in other words, the equality holds in the previous inequality.

Here are some examples:

(a) The trivial representation $\mathbb{Q}_p$ is crystalline, since $B_{\text{cris}}^{\Gamma_K} = K_0$ and thus $\dim_{K_0} D_{\text{cris}}(V) = \dim_{\mathbb{Q}_p} V = 1$.

(b) $\mathbb{Q}_p(\chi_p^i)$ is crystalline for any cyclotomic character.

(c) If $\eta : \Gamma_K \to \mathbb{Z}_p^{\times}$, then $\mathbb{Q}_p(\eta)$ is crystalline iff $\eta \mid_{\Gamma_{K_\infty}}$ is unramified.

(d) By Faltings, the étale cohomology of any smooth projective variety X with good reduction is crystalline.

(e) (Non-example.) The Galois representation of the Tate curve, an elliptic curve without good reduction, is not crystalline.

Let's write $\mathsf{Rep}_{\text{cris}}(\Gamma_K)$ be the category of crystalline Galois representations. This category is closed under reasonable operations such as tensors. Then the functor D_{cris} to MF_K^{ϕ} which is fully faithful. Now here is the important question: Can we describe its image? The answer is positive! (cf. Hodge polygon and Newton polygon by Mazur) We define, for $D \in \mathsf{MF}_K^{\phi}$, the quantities $t_N(D), t_H(D)$ as follows:

(a) For $\dim_{K_0} D = 1$:
  (i) $t_H(D)$ is the unique $i \in \mathbb{Z}$ such that $\mathrm{gr}^i \mathrm{Fil}(D \otimes_{K_0} K) \neq 0$.
  (ii) $t_N(D) = v_p(a)$ where $\phi(d) = ad$, after choosing $d \in D - \{0\}$.

(b) In general, we set $t_?(D) = t_?(\wedge^{\dim D} D)$ (where $? = H$ or N).

For example, in the second example previously, $D_{\text{cris}}(\mathbb{Q}_p(\chi_p^i)) = K_0$ with $t_N(D) = t_H(D) = i$.

We say that D is **weakly admissible** if $t_H(D) = t_N(D)$, and for all $D' \subseteq D$ (inclusion in MF_K^ϕ, so this inclusion respects filtration and ϕ) with $D' \in \mathsf{MF}_K^\phi$ (ie. D' is stable under Frobenius), we have $t_H(D') \leq t_N(D')$.

Finally, Colmez and Fontaine proved

Theorem. *D is in the image of $D_{\text{cris}}|_{\mathsf{Rep}_{\text{cris}}(\Gamma_K)}$ iff D is weakly admissible.*

September 6, 2018. Thursday.

2. Valuation Fields.

2.1. Complete Discrete Valuation Fields.

Recall that $\mathbb{Q}$ has a p-adic norm $|\cdot|_p : \mathbb{Q}^\times \to \mathbb{R}_{>0}$ where one sends $x \mapsto p^{-v_p(x)}$. If $x = r/s$, then $v_p(x) = v_p(r) - v_p(s)$. By convention we also set $|0|_p = 0$. This norm has a few properties:

(a) $|x|_p \neq 0$ for $x \in \mathbb{Q}^\times$,
(b) $|xy|_p = |x||y|$, and
(c) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$. Furthermore, if $|x|_p < |y|_p$, then $|x + y|_p = |y|_p$.

In general, an extension $K/\mathbb{Q}$ is a **p-adic valuation field** if there is a multiplicative norm $|\cdot|_p : K^\times \to \mathbb{R}_{>0}$ satisfying the three above properties, and in addition this norm has to restrict to the ordinary $|\cdot|_p$ on $\mathbb{Q}^\times$.

We can look at the ring $\mathcal{O}_{K,|\cdot|_p} := \{x \in K : |x|_p \leq 1\} \subseteq K$. If the norm is clear, we simply write $\mathcal{O}_K$. This is a local ring with maxiaml ideal $\mathfrak{m}_K = \{x \in L : |x|_p < 1\}$. Caution: This ring is not necessarily Noetherian.

If $|\cdot|_p' : K^\times \to \mathbb{R}_{\geq 0}$ is another such norm on K, then TFAE:

(a) $|\cdot|_p = |\cdot|_p'$.
(b) $\mathcal{O}_{K,|\cdot|_p} = \mathcal{O}_{K,|\cdot|_p'}$.
(c) $\mathcal{O}_{K,|\cdot|_p} \subseteq \mathcal{O}_{K,|\cdot|_p'}$. [1]

Any such norm equips K with a topology, where a basis of neighbourhoods of zero is given by

$$\{U(r) : r \in \mathbb{R}_{>0}\} \text{ where } U(r) = \{x \in K : |x|_p < r\}.$$

We say that K is **complete** if it is complete with respect to this topology. As a non-example, $\mathbb{Q}$ is not complete for the p-adic norm.

However, any metric space admits a completion, using Cauchy sequences up to equivalence. Hence we can complete a p-adic valuation field $(K, |\cdot|_p)$ to get $(\widehat{K}, |\cdot|_p)$, where

$$\widehat{K} = \text{set of equivalent classes of Cauchy sequences } (x_1, x_2, \ldots) \text{ in } K \text{ for } |\cdot|_p$$

$$|(x_1, x_2, \ldots)|_p := \lim_n |x_n|_p.$$

[1] One might need the fact that if $x \in K^\times$, then either x or x^{-1} is in $\mathcal{O}_{K,|\cdot|_p}$.

In particular, we can complete $(\mathbb{Q}, |\cdot|_p)$ to obtain $(\mathbb{Q}_p, |\cdot|_p)$. For example, $1+p+p^2+\cdots$ converges in $\mathbb{Q}_p$ to $1/(1-p)$.

Every other complete p-adic valuation field contains a $\mathbb{Q}_p$: if $(K, |\cdot|_p) \to (L, |\cdot|_p)$ is a map of p-adic valuation fields with L complete, then we have $K \subseteq \widehat{K} \subseteq L$, where we embed K into $\widehat{K}$ by constant Cauchy sequences.

Proposition 2.1. *Let $(K, |\cdot|_p)$ be a complete p-adic valuation field, and let L/K be a finite extension. Then there is a unique extension of $|\cdot|_p$ to $|\cdot|_p : L^\times \to \mathbb{R}_{>0}$, given by*

$$|x|_p = |N_{L/K}(x)|_p^{[L:K]^{-1}}.$$

We will delay the proof till later.

In addition, 2.1 is not true if K is not complete: consider the case where $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, and let $p = 5$. Then there are two ways to extend $|\cdot|_5$ to L, namely

$$x \in \mathbb{Z}[i] \mapsto \begin{cases} 5^{-v_{\mathfrak{p}_1}(x)} \\ 5^{-v_{\mathfrak{p}_2}(x)}, \end{cases}$$

where $(5) = (2+i)(2-i) =: \mathfrak{p}_1\mathfrak{p}_2$.

Corollary 2.2. *If L/K is Galois and K is a complete p-adic valuation field as before, and $\sigma \in \mathrm{Gal}(L/K)$, then for any L, we have $|x|_p = |\sigma(x)|_p$.*

Proof. $|\cdot|_p$ and $|\sigma(\cdot)|_p$ are two ways to extend the norm on K. □

Corollary 2.3 (Krasner's Lemma)**.** *Let $\alpha, \beta \in L$ be such that $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$ for all $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\alpha) \neq \alpha$. Then $\alpha \in K(\beta)$.*

Proof. Replace K by $K(\beta)$ and assume $\beta \in K$. Then we just need to show that $\alpha \in K$. We know that for any $\sigma \in \mathrm{Gal}(L/K)$, either $\sigma(\alpha) = \alpha$ or $|\sigma(\alpha) - \alpha| > |\beta - \alpha|$ by assumption. Note that by 2.2, we know that $|\beta - \alpha| = |\beta - \sigma(\alpha)|$, and hence $|\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \beta + \beta - \alpha| \leq \max\{|\sigma(\alpha) - \beta|, |\alpha - \beta|\} = |\alpha - \beta|$. This means that the latter case cannot occur, thus $\sigma(\alpha) = \alpha$ for all σ, and $\alpha \in K$. □

Rephrasing 2.3, all conjugates of $\alpha \in L$ are equally far away from elements of K.

Next we introduce the Hensel's Lemma. We shall introduce a more technical version of it. First we extend the norm on K to $K[T]$, by defining

$$|q(T)|_p = \max_i |a_i|_p \text{ where } q(T) = \sum a_i T^i.$$

Let K be a complete p-adic valuation field as before[2]. Suppose that $f(T), g_0(T), h_0(T) \in \mathcal{O}_K[T]$ are such that

(a) $f(T), g_0(T)$ are monic,

[2] There are non-complete DVR's for which Hensel's Lemma stays true, and those are called Henselian. These DVR's still have the norm extension property!

(b) $|f(T) - g_0(T)h_0(T)|_p =: \alpha < 1$, and

(c) $g_0(T), h_0(T)$ are relatively prime modulo the maximal ideal, or equivalently, there are $r(T), s(T) \in \mathcal{O}_K[t]$ such that $|r(T)g_0(T) + s(T)h_0(T) - 1|_p =: \beta < 1$.

Theorem 2.4 (Hensel's Lemma)**.** *Under these conditions, we can find $g(T), h(T) \in \mathcal{O}_K[T]$ with*

(a) *$g(T)$ is monic,*
(b) *$|g(T) - g_0(T)|_p < 1$ and $|h(T) - h_0(T)|_p < 1$, and*
(c) *$f(T) = g(T)h(T)$.*

Verbally, Hensel's Lemma is stating that once we have an approximate factorization, we can tweak it to become an actual factorization.

Proof. The proof does not differ from the usual one – we will still use successive approximations. Choose $\varpi \in \mathcal{O}_K$, with $|\varpi|_p = \max\{\alpha, \beta\} < 1$. By induction, we can define $g_n(T), h_n(T) \in \mathcal{O}_K[T]$ such that

(a) $g_n(T) - g_{n-1}(T), h_n(T) - h_{n-1}(T) \in \varpi^n \mathcal{O}_K[T]$,

(b) $f(T) - g_n(T)h_n(T) \in \varpi^{n+1}\mathcal{O}_K[T]$, and

(c) $g_n(T)$ is monic.

We then define $g(T) = \lim g_n(T)$ and $h = \lim h_n(T)$, which makes sense by completeness.

By hypothesis, $n = 0$ holds, so we proceed straight into the induction step. Suppose that we have $g_i(T), h_i(T)$ where $0 \leq i \leq n-1$ such that the three criteria hold.

Write $f(T) - g_n(T)h_n(T) =: \varpi^{n+1}q(T)$. From assumption (c) we have $f(T) := q(T) - [g_n(T)r(T)q(T) + h_n(T)s(T)q(T)] \in \varpi\mathcal{O}_K[T]$. Define

(a) $s_{n+1}(T) = s(T)q(T) - g_n(T)p(T)$ where $p(T)$ is a choice made so that $\deg s_{n+1}(T) < \deg g_n(T)$,

(b) $r_{n+1}(T) = r(T)q(T) + p(T)h_n(T)$,

(c) $g_{n+1}(T) = g_n(T) + \varpi^{n+1}s_{n+1}(T)$, and

(d) $h_{n+1}(T) = h_n(T) + \varpi^{n+1}r_{n+1}(T)$.

Then $q(T) - [g_n(T)r_{n+1}(T) + h_n(T)s_{n+1}(T)] = f(T) \in \varpi\mathcal{O}_K[T]$. (yet to be fixed)

Corollary 2.5. *Let L/K be a finite extension and $\alpha \in L$. Let the minimal polynomial of α be $m_\alpha(T) \in K[T]$, and write $m_\alpha(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$. Then*

$$|m_\alpha(T)|_p = \max\{|a_0|_p, 1\}.$$

Proof. If $i \in \{1, \ldots, n-1\}$ such that $|\alpha_i|_p = |m_\alpha(T)|_p > \max\{1, |a_0|_p\}$, then $a_i^{-1}m_\alpha(T) \in \mathcal{O}_K[T]$ and is irreducible. But

$$a_i^{-1}m_\alpha(T) \equiv T^i q(T) \pmod{\mathfrak{m}_K}$$

so we can use Hensel's Lemma to factorize $m_\alpha(T)$ in $K[T]$, but this is absurd. □

In particular, TFAE:

(a) $m_\alpha(T) \in \mathcal{O}_K[T]$.

(b) α is integral over $\mathcal{O}_K$.

(c) $a_0 \in \mathcal{O}_K$.

(d) $|N_{L/K}(\alpha)|_p \leq 1$ (because $N_{L/K}(\alpha) = a_0$ up to a sign).

September 10, 2018. Monday.

Now we are in a ready position to prove 2.1.

Proof. First we show that $|\cdot| := |N(x)|_p^{[L:K]}$ is a norm on L. The only real content here is to show the non-archimedean property, ie. $|N_{L/K}(x+y)| \leq \max\{|N_{L/K}(x)|, |N_{L/K}(y)|\}$. Assume that $|y| \leq |x|$, then by replacing x by 1, y by $x^{-1}y$, it suffices to show that $|N_{L/K}(1+y)| \leq 1$. This is true iff $1+y$ is integral over $\mathcal{O}_K$, or equivalently y is integral over $\mathcal{O}_K$, or in turn the same as $|N_{L/K}(y)| \leq 1$. So we are good here.

Next we show the uniqueness of such an extension of norms. Recall the fact that if $|\cdot|_p, |\cdot|_p'$ are two norms, then $\mathcal{O}_{L,|\cdot|_p} \subseteq \mathcal{O}_{L,|\cdot|_p'}$ iff $|\cdot|_p = |\cdot|_p'$. Now it suffices to show that if x is integral over $\mathcal{O}_K$, then $|x| \leq 1$. Let's look at $m_x(T) = T^n + \cdots + a_0$. Then $|x|^n \leq \max |x|^i |a_i|_p$, thus for some i we have $|x|^{n-i} \leq |a_i|_p \leq 1$. ☐

Lemma 2.6. *For a complete valuation field K, TFAE:*

(a) $\mathfrak{m}_K$ *is finitely generated.*
(b) $\mathfrak{m}_K$ *is principal.*
(c) $\mathcal{O}_K$ *is Noetherian.*
(d) $\mathcal{O}_K$ *is a DVR.*

If K satisfies any of the above equivalent conditions, we say K is in addition discrete.

Proof. This is a basic fact and thus left as an exercise. The only real ingredient is to prove that (a) implies (b), to which we can start by assuming a is the one with the maximal norm among a chosen set of generators of $\mathfrak{m}_K$. ☐

Before we proceed, we will from now on restrict our focus to complete discrete valuation fields (CDVFs). For simplicity, we also require $k := \mathcal{O}_K/\mathfrak{m}_K$ to be perfect. Note that the property of being a CDVF (along with k being perfect) is stable under finite extensions. [3]

Definition 2.7. (a) A **uniformizer** ϖ_K of K is a generator for $\mathfrak{m}_K$.[4]
(b) The **ramification index** $e_{L/K}$ for L/K is the unique integer e such that $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L^e$, or equivalently, that $\varpi_k\mathcal{O}_L = \varpi_L^e\mathcal{O}_L$.
(c) The **inertial degree** $f_{L/K}$ for L/K is $[k_L : k_K]$.

In fact, we have $[L:K] = e_{L/K}f_{L/K}$. Furthermore, $e_{L/K} = [L:K]$ iff $k_L = k_L$, in which case we say that L/K is **totally ramified**.

Totally ramified extensions are closely related to *Eisenstein polynomials*:

Theorem 2.8. [5]

[3] This uses the topological fact that if K is complete, then any finite dimensional K-vector space with a norm is complete.

[4] Typer's note: I shall try my best to restrict to the notation ϖ for uniformizers, but π might also unintentionally come up.

[5] To prove this, one might find the following exercise useful: Let $\mathcal{O} \subseteq L$ be a DVR which contains a generator for L/K (as a field extension). Then $\mathcal{O} = \mathcal{O}_L$. This in turn uses the fact that DVRs are normal, and so they are integrally closed in their field of fractions.

(a) *If $f(T) \in K[T]$ is Eisenstein, then $f(T)$ is irreducible in $K[T]$, and $K[T]/(f(T))$ is a totally ramified field extension of K, with $\mathcal{O}_L = \mathcal{O}_K[T]/(f(T))$.*
(b) *If L/K is totally ramified, then $m_{\varpi_L}(T)$ is Eisenstein, and $\mathcal{O}_L = \mathcal{O}_K[\varpi_L]$.*

Using this, we can exhibit a famous example of a totally ramified extension, namely $L = \mathbb{Q}(\zeta_{p^n})$ and $K = \mathbb{Q}_p$. One can check explicitly that $\Phi_{p^n}(T+1)$ is a Eisenstein polynomial, and thus $\zeta_{p^n} - 1$ is a uniformizer in $\mathcal{O}_L$ and $\mathcal{O}_L = \mathbb{Z}_p[\zeta_{p^n}]$.

September 12, 2018. Wednesday.

As per last time, we will assume that K is a CDVF (which by definition includes the assumption that $k = \mathcal{O}_K/\mathfrak{m}_K$ is perfect). If L/K is a finite extension, then L is a CDVF as well. We defined the ramification index $e_{L/K}$ and the inertial degree $f_{L/K}$. Recall that L/K is totally ramified if $e_{L/K} = [L : K]$, or equivalently, $k_L = k_K$. We saw last time if L/K is totally ramified, and $\varpi_L \in L$ is a uniformizer, then

(a) $m_{\varpi_L}(T) \in \mathcal{O}_K[T]$ is Eisenstein,
(b) $\mathcal{O}_L = \mathcal{O}_K[\varpi_L]$.

The example to keep in mind should be where $L = \mathbb{Q}_p(\zeta_{p^n})$ and $K = \mathbb{Q}_p$, where we can take $\varpi_L = \zeta_{p^n} - 1$.

Today we will look at the opposite case, where we say L/K is **unramified** if $e_{L/K} = 1$, or equivalently, $[k_L : k_K] = [L : K]$, or $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L$. Our goal will be to characterize such extensions in terms of the residue fields. In addition, in fact all extensions of CDVFs are obtained by first adjoining an unramified extension and then a totally ramified extension.

Suppose that $L = K(\alpha)$ and $m_\alpha(T) \in \mathcal{O}_K[T]$. [6] Then

$$\mathcal{O}' := \mathcal{O}_K[\alpha] = \mathcal{O}_K[T]/(m_\alpha(T)) \subseteq \mathcal{O}_L.$$

We have a trace map $\mathrm{Tr}_{L/K} : L \to K$, which is defined by $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(x : L \to L)$. From this we get a trace pairing

$$\langle \cdot, \cdot \rangle : L \times L \to K, \quad (x, y) \mapsto \mathrm{Tr}_{L/K}(xy).$$

For a finite separable extension L/K, this is then non-degenerate, because $\mathrm{Tr}(xx^{-1}) = [L : K]$.

Lemma 2.9. *We have*

$$\mathrm{Tr}_{L/K}\left(\frac{\alpha^i}{m'_\alpha(\alpha)}\right) = \begin{cases} 0 & \text{if } 0 \le i \le n - w \\ 1 & \text{if } i = n-1. \end{cases}$$

Sketch of Proof of Lemma.[7] Write $f = m_\alpha$ and $\alpha_1, \dots, \alpha_n$ be the Galois conjugates of α. For any $j = 0, \dots, n-1$, we have the identity

$$\sum_{i=1}^{n} \frac{f(T)}{T - \alpha_i} \frac{\alpha_i^j}{f'(\alpha_i)} = T^i.$$

---

[6] All finite separable extensions can be obtained by adjoining one element.
[7] Writer's note: I have edited this proof to incoporate a proof I learnt from Dr. Jack Thorne.

This is because both sides are polynomials of degree at most $n-1$, and they agree at n points $T=\alpha_1,\ldots,\alpha_n$. Consider the coefficient of T^{n-1} on both sides to get the lemma. ☐

Corollary 2.10. *The dual* $(\mathcal{O}')^\vee = \{x \in L : \langle \mathcal{O}', x\rangle \subseteq \mathcal{O}_K\}$ *is equal to* $m'_\alpha(\alpha)^{-1}\mathcal{O}'$.

Proof. 2.9 shows that $m'_\alpha(\alpha)^{-1}\mathcal{O}' \subseteq (\mathcal{O}')^\vee$. Let $\{\beta_i\}_i$ be a dual basis of $\{1,\alpha,\ldots,\alpha^{n-1}\}$. Then 2.9 says that we have

$$\left(\mathrm{Tr}_{L/K}\frac{\alpha^i\alpha^j}{f'(\alpha)}\right)_{i,j} = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & \iddots & 1 & * \\ 0 & \iddots & \iddots & \vdots \\ 1 & * & \cdots & * \end{pmatrix}.$$

Hence $\beta_n = m'_\alpha(\alpha)^{-1}$, and one can see from the matrix that $\beta_{n-i} \in \langle \beta_n,\ldots,\beta_{n-(i-1)}\rangle + m'_\alpha(\alpha)^{-1}\mathcal{O}'$. Induction then gives $\{\beta_i\}_i \in m'_\alpha(\alpha)^{-1}\mathcal{O}'$. ☐

In fact, $\langle\cdot,\cdot\rangle : \mathcal{O}_L \times \mathcal{O}_L \to \mathcal{O}_K$, and $\mathcal{O}' \subseteq \mathcal{O}_L \subseteq (\mathcal{O}')^\vee$.

Corollary 2.11. *If* $m'_\alpha(\alpha) \in (\mathcal{O}')^\times$, *then* $\mathcal{O}' = \mathcal{O}_L = (\mathcal{O}')^\vee$.

Suppose that $m'_\alpha(\alpha) \in \mathcal{O}_K[\alpha]^\times$. Then we have

(a) $\mathcal{O}_K[\alpha] = \mathcal{O}_L$,

(b) L/K is unramified,

(c) If M/K is another finite extension with a commutative diagram

$$\begin{tikzcd} \mathcal{O}_L/\mathfrak{m}_L \arrow[rr, hook, "\iota_0"] \arrow[dr] & & \mathcal{O}_M/\mathfrak{m}_M \arrow[dl] \\ & \mathcal{O}_K/\mathfrak{m}_K & \end{tikzcd}$$

then ι_0 lifts to a unique embedding.

$$\begin{tikzcd} L \arrow[rr, hook, "\iota"] \arrow[dr] & & M \arrow[dl] \\ & K & \end{tikzcd}$$

Proof. (a) is immediate. (b) Consider

$$\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L = \mathcal{O}_K[\alpha]/\mathfrak{m}_K\mathcal{O}_K[\alpha] = \mathcal{O}_K[T]/(\mathfrak{m}_K + (m_\alpha(T))) = k[T]/(\overline{m_\alpha}(T)).$$

One can show that $\overline{m_\alpha}(T)$ is separable (or even stronger that $\overline{m'_\alpha}(\bar\alpha)$ is invertible), and is irreducible by Hensel's Lemma. Thus $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ is a field, and $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L$. (c) Exercise. ☐

Note that l/k is a finite separable extension, then $l = k[T]/(\bar f(T))$ where $\bar f(T)$ is irreducible and separable. We can lift $\bar f(T)$ to a monic $f(T) \in \mathcal{O}_K[T]$, then $f(T)$ stays irreducible, and $K[T]/(f(T))$ is an unramified extension of K.

Proposition 2.12. (a) *The functor*

$$\{L/K \textit{ unramified extensions}\} \mapsto \{\textit{finite separable } L/K\}, \quad L \mapsto \mathcal{O}_L/\mathfrak{m}_L$$

is an equivalence of categories.

(b) *In addition, if M/K is finite and L/K is unramified with $l = \mathcal{O}_L/\mathfrak{m}_L = \mathcal{O}_M/\mathfrak{m}_M$, then there is a canonical embedding*

$$\begin{tikzcd} L \arrow[r, hook] \arrow[dr] & M \arrow[d] \\ & K \end{tikzcd} \quad \textit{lifting} \quad \begin{tikzcd} l \arrow[r, "="] \arrow[dr] & l \arrow[d] \\ & k \end{tikzcd}$$

with M/L totally ramified.

In particular, if k is finite, then any extension of k is obtained by adjoining prime-to-2 roots of unity, thus by the above this is also the case for any unramified extensions of K. Furthermore, we can see in this case (where k is finite) that all unramified extensions are Galois (and in fact abelian).

In general, for any k perfect, there is a gadget named *étale ϕ-modules* that studies p-power extensions of k.

September 13, 2018. Thursday.

2.2. Dropping Discreteness, and the algebraically closed field $\mathbb{C}_p$.

Let K be a complete p-adic valuation field. This will be our assumption throughout today. Today our goal will be to prove that

(a) $\widehat{\overline{K}}$ is algebraically closed, and
(b) $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$ acts on $\widehat{\overline{K}}$, and we will show that its Γ_K-invariants are K.

Recall the following

Lemma 2.13 (Krasner)**.** *If L/K is finite Galois, and $\alpha, \beta \in L$ such that for any $\sigma \in \mathrm{Gal}(L/K)$ with $\sigma(\alpha) \neq \alpha$ and $|\beta - \alpha| < |\sigma(\alpha) - \sigma|$, then $\alpha \in K(\beta)$.*

Proof. Replace K with $K(\beta)$. For any $\sigma \in \mathrm{Gal}(L/K)$, we have $|\sigma(\alpha) - \alpha| = |\sigma(\alpha) - \beta + \beta - \alpha| \leq |\alpha - \beta|$. □

As a consequence, if α is algebraic over K, $m_\alpha(T) \in K[T]$, then for any monic $q(T) \in K[T]$ "close enough" to $m_\alpha(T)$, we have

(a) $q(T)$ is irreducible, and
(b) α is contained in the extension of K generated by a root of $q(T)$.

Or if one prefers, it can be rephrased as: if α, β are algebraic over K and $m_\alpha(T), m_\beta(T)$ are "close enough", then $K(\alpha) = K(\beta)$. In addition, if a polynomial $f(T)$ is irreducible and another $g(T)$ is close enough to $f(T)$, then $g(T)$ is irreducible too. So in some sense irreducibility is an open condition.

Now we are ready to prove

Proposition 2.14. *$\widehat{\overline{K}}$ is algebraically closed.*

Proof. If α is algebraic over $\widehat{\overline{K}}$, then $m_\alpha(T) \in \widehat{\overline{K}}[T]$ can be approximated by $q(T) \in \overline{K}[T]$. But $q(T)$ has all its roots in $\bar{K}$, so does $m_\alpha(T)$. □

Let's consider the following more interesting

Theorem 2.15. *We have* $\widehat{\overline{K}}^{\Gamma_K} = K$.

More concretely, this is saying that if $E \subseteq \bar{K}$, $\Gamma_E := \mathrm{Gal}(\overline{K}/E) \subseteq \mathrm{Gal}(\overline{K}/K)$, then $\widehat{\overline{K}}^{\Gamma_E} = \widehat{E}$. For this we will need a clever lemma.

Lemma 2.16 (Ax-Sen-Tate)**.** *Let E/K be a finite extension and let $\alpha \in \overline{K}$, and*

$$\Delta_E(\alpha) = \max_{\sigma \in \Gamma_E, \sigma(\alpha) \neq \alpha} |\sigma(\alpha) - \alpha|.$$

Then there is $C > 1$ which is independent of α, and exists $a \in E$ such that $|\alpha - a| \leq C\Delta_E(\alpha)$.

2.16 is assuring that for any $\alpha \in \overline{K}$, there is always $a \in E$ such that a and α are "nicely" close.

Assuming 2.16, it is then easy to prove 2.15.

Proof of 2.15. Pick $\beta \in \widehat{\overline{K}}^{\Gamma_E}$. For any $n > 1$, there is $\alpha_n \in \overline{K}$ such that $|\beta - \alpha_n| < 1/n$ (simply due to completion). Thus for any $\sigma \in \Gamma_E$, we have

$$|\sigma(\alpha_n) - \alpha_n| \leq \max\{|\sigma(\alpha_n) - \beta|, |\beta - \alpha_n|\} = |\alpha_n - \beta| < 1/n$$

since $|\sigma(\alpha_n) - \beta| = |\sigma(\alpha_n) - \sigma(\beta)| = |\alpha_n - \beta|$. Thus $\Delta_E(\alpha_n) < 1/n$. By lemma, there is $\alpha_n \in E$ such that $|\alpha_n - a_n| < C \cdot 1/n$. So $\beta = \lim a_n \in \widehat{E}$. $\square$

Proof of 2.16. Let $i \in \mathbb{Z}_{>0}$ and define $C_i = p^{1/(p^{i-1}(p-1))}$. Then define $C := \prod_{i=1}^{\infty} C_i = p^{p/(p-1)^2}$. We will show that there is $a \in E$ such that $|\alpha - a| \leq (\prod_{i=1}^{l(n)} C_i)\Delta_E(\alpha)$ where $l(n) = \max\{i : \lfloor \deg m_{\alpha,E}/p^i \rfloor \neq 0\}$ (where $n = \deg m_{\alpha,E}$).

We proceed by induction on $n := \deg m_{\alpha,E}$. If $n = 1$, this is trivial. In general, write $f(T) := m_{\alpha,E}(T) \in E[T]$. Consider

$$g(T) = f(T + \alpha) \in E(\alpha)[T] = T^n + \cdots + a_i T^i + \cdots + a_1 T.$$

This has zero constant term since $f(\alpha) = 0$. Consider $g'(T)/n = T^{n-1} + \cdots + a_1/n$. This has $n - 1$ roots, say $\gamma_1, \ldots, \gamma_{n-1}$. We have $|\gamma_1 \cdots \gamma_{n-1}| = |a_1/n|$. But $|a_1| \leq \Delta_E(\alpha)^{n-1}$ (this is the sum of product of $n-1$ nonzero roots of g). So $|a_1/n| \leq |n|^{-1}\Delta_E(\alpha)^{n-1}$. So there is i_0 such that

$$|\gamma_{i_0}| \leq |n|^{-1/(n-1)}\Delta_E(\alpha).$$

Write $\beta = \gamma_{i_0} + \alpha$. Then $f'(\beta) = g'(\gamma_{i_0}) = 0$ and $|\beta - \alpha| \leq |n|^{-1/(n-1)}\Delta_E(\alpha)$.

Applying hypothesis to f', there is $b \in E$ such that $|\alpha - (b - \gamma_{i_0})| = |\beta - b| \leq (\prod_{i=1}^{l(n-1)} C_i)\Delta_E(\beta)$. But also $|\beta - \sigma(\beta)| = |\beta - \alpha + \sigma(\alpha) - \sigma(\beta)| \leq \max\{|\beta - \alpha|, |\sigma(\alpha) - \sigma(\beta)|\} = |\beta - \alpha| \leq |n|^{-1/(n-1)}\Delta_E(\alpha)$. But this is not good enough (eg when $n = p^k$).

To fix this, we have to look at higher derivatives and apply the same idea. Write $n = p^r d$ where either $(d, p) = 1, d > 1$ or $d = p$. Write $q = p^r$. Repeat the same argument, but now look at $h(T) = f^q(T + \alpha) \cdot (n - q)!/n! \in E(\alpha)[T]$ to make it monic. The constant term is $\binom{n}{q}^{-1} a_q$. The point: $\binom{n}{q}$ cannot be very large! Show that under these hypothesis, $|\binom{n}{q}|$ is either p^{-1} if $d = p$, or 1 otherwise.

But $|a_q| \leq \Delta_E(\alpha)^{n-q}$ and so $h(0) \leq \Delta_E(\alpha)^{n-q}$ if $(d, p) = 1$, and $p\Delta_E(\alpha)^{n-q}$ if $d = p$. So there is γ such that $h(\gamma) = 0$, equivalently $f^{(q)}(\gamma + \alpha) = 0$, such that $|\gamma| \leq \Delta_E(\alpha)$ if $(d, p) = 1$, or $p^{1/(n-q)}\Delta_E(\alpha)$ if $p = d$, but $p^{1/(n-q)} = C_{r+1}$. And $\beta = \gamma + \alpha$, so $\Delta_E(\beta) \leq C_{r+1}\Delta_E(\alpha)$. Use hypothesis. $\square$

September 17, 2018. Monday.

Let K be a complete p-adic valuation field. Last time we showed that if $K \subseteq E \subseteq \overline{K}$ and $\Gamma_E = \mathrm{Gal}(\overline{K}/E) \subseteq \Gamma_K$, then $\widehat{\overline{K}}^{\Gamma_E} = \widehat{E}$. In the case where E/K is finite, then $\widehat{E} = E$ in addition.

Consider the case where $K/\mathbb{Q}_p$ is finite. Write K_0 for the maximal unramified subextension. Suppose we have a cyclotomic character $\chi_p : \Gamma_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ determined by $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi_p(\sigma)^{-1}}$ for all $n \geq 1$. This governs the Γ_K-action on the p-th power roots of unity. In particular, we can restrict χ_p to K, by which we mean to look at $\chi_p \mid_{\Gamma_K}$. Write $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$. We will be primarily interested in

$$\mathbb{C}_p(\chi_p^i)^{\Gamma_K} := \{x \in \mathbb{C}_p : \text{ for all } \sigma \in \Gamma_K, \sigma(x) = \chi_p(\sigma)^{-i}x\}.$$

Note that

(a) we write i instead of $-i$ for the index, and

(b) the superscript does not exactly mean "fixed by Γ_K", but rather fixed with a twist. (This is what χ_p^i means.)

Theorem 2.17 (Tate)**.** *For a finite extension $K/\mathbb{Q}_p$, we have*

$$\mathbb{C}_p(\chi_p^i)^{\Gamma_K} = \begin{cases} K & \text{if } i = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Remark: This is a special case of a theorem of Tate, which says that for any $\eta : \Gamma_K \to \mathbb{Z}_p^\times$, we then have $\mathbb{C}_p(\eta)^{\Gamma_K} = 0$ unless $\eta \mid_{I_K}$ has finite image, where $I_K = \mathrm{Gal}(\overline{K}/K^{nr})$ with $K^{nr} \subseteq \overline{K}$ being the maximal unramified subextension. More explicitly, K^{nr} is the extension of K adjoining all prime to p-th power roots of unity. This general statement is too elaborated to prove, so we'll focus on our simpler case.

We have also proved the case $i = 0$ in the previous lecture, so for what remains, we will focus on the latter case.

Here is our upshot: unramified and totally ramified extensions are always linearly disjoint. So a cyclotomic character when restricted to K_0 is still non trivial.

Proof of 2.17. First assume that $K_0 = K$, ie. K is unramified. In this case, for all $n \geq 1$, we have

$$\mathbb{Q}_p(\zeta_{p^n}) \cap K = \mathbb{Q}_p,$$

or for what is the same, $[K(\zeta_{p^n}) : K] = [\mathbb{Q}_p(\zeta_{p^n}) : \mathbb{Q}_p]$. The polynomial $\Phi_{p^n}(T+1)$ is still the minimal one over K and Eisenstein, and so we still have $\mathcal{O}_{K(\zeta_{p^n})} = \mathcal{O}_K[\zeta_{p^n}]$ by the correspondence between Eisenstein polynomials and totally ramified extensions.

Equivalently, let's make the following observation. Suppose we have fixed a compatible sequence of choices for ζ_{p^n}. If we set $K_n = K(\zeta_{p^n})$ and $K_\infty = \cup_{i=1}^\infty K_n$, then every element $x \in \mathcal{O}_{\widehat{K_\infty}}$ has a unique expression of the form

$$x = \sum_{r \in \frac{1}{p^\infty}\mathbb{Z} \cap [0,1)} a_r(x)\varepsilon_r$$

where $a_r(x) \in \mathbb{Z}_p$ (or equivalently a compatible sequence of elements in $\mathbb{F}_{p^n}$) and $\varepsilon_r = \zeta_{p^n}^s$ where $r = s/p^n$ in lowest terms. However we do note that not all such things are in $\mathcal{O}_{\widehat{K_\infty}}$: $a_r(x)$ needs to "go smaller" to get a convergent sequence and for x to make sense.

Pick $x \in \mathbb{C}_p(\chi_p^i)^{\Gamma_K} \subseteq \mathbb{C}_p(\chi_p^i)^{\Gamma_{K_\infty}}$. First we observe that $x \in \widehat{K_\infty}$. Indeed, for any $\sigma \in \Gamma_{K_\infty}$, we have $\sigma(x) = \chi_p(\sigma)^{-i}x$ but $\chi_p(\sigma) = 1$ since $\Gamma_{K_\infty} = \ker(\chi_p \mid_{\Gamma_K})$. So $x \in \mathbb{C}_p^{\Gamma_{K_\infty}} = \widehat{K_\infty}$ by 2.15.

We can WLOG assume $x \in \mathcal{O}_{\widehat{K_\infty}}$, so we can write $x = \sum a_r(x)\varepsilon_r$. Then for all $\sigma \in \mathrm{Gal}(K_\infty/K)$, we have $\sigma(x) = \sum_r a_r(x)\sigma(\varepsilon_r)$; and for $\varepsilon_r = \zeta_{p^n}^s$, we have $\sigma(\varepsilon_r) = \zeta_{p^n}^{\chi_p(\sigma)^{-1}s} = \varepsilon_{\chi_p(\sigma)^{-1}r}$. This notation is fine, because $\chi_p(\sigma)^{-1} \in \mathbb{Z}_p^\times$ will not interfere with the denominator in $r = s/p^n$.

So $\sigma(x) = \sum a_r(x)\sigma(\varepsilon_r) = \sum a_r(x)\varepsilon_{\chi_p(\sigma)^{-1}r} = \sum a_{\chi_p(\sigma)r}(x)\varepsilon_r$ and $\sigma(x) = \chi_p(\sigma)^{-i}(x) = \sum \chi_p(\sigma)^{-i}a_r(x)\varepsilon_r$. Equating, this is saying that for any r, we have

$$\chi_p(\sigma)^{-i}a_r(x) = a_{\chi_p(\sigma)r}(x).$$

But $\chi_p(\sigma)$, as σ varies, can be any element of $\mathbb{Z}_p^\times$. So we are saying that for any $b \in \mathbb{Z}_p^\times$, we have $b^{-i}a_r(x) = a_{br}(x)$. On the right hand side there are finitely many possibilities: when r is fixed, the denominator is then fixed, and br does not change the denominator of r, so there are only finitely many choices. But there are infinitely many possibilities on the left: again, K is unramified so χ_p surjects onto $\mathbb{Z}_p^\times$. Thus this condition fails horribly! This proves the case when K is unramified.

In general, we have shown that $\mathbb{C}_p(\chi_p^i)^{\Gamma_{K_0}} = 0$ if $i \neq 0$. If $x \in \mathbb{C}_p(\chi_p^i)^{\Gamma_K}$, first it suffices to show for the case assuming K is Galois over $\mathbb{Q}_p$, since if L/K is the Galois closure, then $\mathbb{C}_p(\chi_p^i)^{\Gamma_K} \subseteq \mathbb{C}_p(\chi_p^i)^{\Gamma_L}$. Let's look at the extension K/K_0. Take $\{\sigma_1, \dots, \sigma_r\} \subseteq \Gamma_{K_0}$ which is a set of coset representatives for $\mathrm{Gal}(K/K_0) = \Gamma_{K_0}/\Gamma_K$, and define $y = \prod \sigma_i(x)$. In general y depends on $\{\sigma_i\}_i$, but the $\mathbb{Q}_p$-line of y is easily seen to be well defined (and independent of $\{\sigma_i\}_i$): if σ_i is replaced by $\sigma_i' + \sigma$ where $\sigma \in \Gamma_K$, then σ acts on x by multiplication by $\chi_p(\sigma)^{-i}$.

Then one can check readily that

(a) the $\mathbb{Q}_p$-line generated by y in $\mathbb{C}_p$ is Γ_{K_0}-invariant (a general feature of the averaging process), and
(b) fixing $\sigma \in \Gamma_{K_0}$ and a coset representative σ_a, we have $\sigma\sigma_a = \sigma_b\sigma_{a,b}$ for some $\sigma_{a,b} \in \Gamma_{K_0}$. This gives

$$\chi_p(\sigma_{a,b})^{-i} = \chi_p(\sigma_b)^i\chi_p(\sigma)^{-i}\chi_p(\sigma_a)^{-i}.$$

Hence $\sigma(y) = \chi_p(\sigma)^{-ir}y$.

In other words, given $x \in \mathbb{C}_p(\chi_p^i)^{\Gamma_K}$, we have cooked up $y \in \mathbb{C}_p(\chi_p^{ir})^{\Gamma_{K_0}}$. This reduces the problem to unramified case. But we showed that $\mathbb{C}_p(\chi_p^{ir})^{\Gamma_{K_0}}$ is zero if $i \neq 0$, forcing $x = 0$, so we are done. □

September 19, 2018. Wednesday.

3. Formalisms and Setups.

Today we will set up the formalism of the Galois representations we will be interested in.

3.1. Admissible Representations.

Let Γ be a group and F be a field of characteristic zero. Let B be a ring[8] which has a Γ-action on it. We require

(a) B to be a F-algebra and the Γ-action to be F-linear,
(b) this Γ-action to preserve the ring structure, and
(c) B to be a domain with no non-trivial Γ-stable ideals. This will be our main assumption.

At this stage, we can think about it as if B with this Γ-action structure behaves like a field.

Let M be a B-module with a compatible Γ-action, ie. for any $\gamma \in \Gamma, m \in M, b \in B$, we have

$$\gamma(bm) = \gamma(b)\gamma(m).$$

Then we can look at $M_\eta := M \otimes_B \mathrm{Frac}(B)$. Consider

$$\mathsf{Rep}_\Gamma(B) = \{ \text{ projective } B\text{-modules with a } \Gamma\text{-action of finite rank } \}.$$

and the functor from this to $\mathsf{Rep}_\Gamma(\mathrm{Frac}(B))$, sending $M \mapsto M_\eta$.

Lemma 3.1. *This functor is fully faithful.*

In particular this means that any map from $M_\eta \to N_\eta$ comes from $M \to N$, or $\mathrm{Hom}_{B[\Gamma]}(M_1, M_2) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Frac}(B)[\Gamma]}(M_{1,\eta}, M_{2,\eta})$. Note that $\mathrm{Hom}_{B[\Gamma]}(M_1, M_2) = \mathrm{Hom}_B(M_1, M_2)^\Gamma$ and $\mathrm{Hom}_{\mathrm{Frac}(B)[\Gamma]}(M_{1,\eta}, M_{2,\eta}) = \mathrm{Hom}_B(M_1, M_2)_\eta^\Gamma$.

Proof. Let $M^\Gamma = \{m \in M : \gamma m = m \text{ for all } \gamma \in \Gamma\}$. This maps to $M_\eta^\Gamma := (M_\eta)^\Gamma$. We claim that this is a bijection.

Indeed, suppose $m \in M_\eta^\Gamma - \{0\}$. Consider $\{b \in B : bm \in M\} \subseteq B$. It is easy to check that this is a nonzero Γ-stable ideal.[9] So this ideal is all of B, and in particular $m = 1 \cdot m \in M$.

If $M_1, M_2 \in \mathsf{Rep}_\Gamma(B)$, then $\mathrm{Hom}_B(M_1, M_2) \cong M_1^\vee \otimes_B M_2$ is also a projective B-module of finite rank, which also has a natural Γ-action, given by $(\gamma f)(m) = \gamma(f(\gamma^{-1}m))$. Moreover, as we noted previously, $\mathrm{Hom}_B(M_1, M_2)^\Gamma = \{\Gamma - \text{equivariant } f : M_1 \to M_2\}$, so we deduced that

$$\mathrm{Hom}_B(M_1, M_2)^\Gamma \cong \mathrm{Hom}_B(M_1, M_2)_\eta^\Gamma$$

and we are done. $\square$

In light of this, if we let $K = B^\Gamma$, then $K = (\mathrm{Frac}\, B)^\Gamma$, and K is a field, since for example if x is Γ-invariant, then so is x^{-1} evidently. Next we will look at

$$\mathsf{Rep}_\Gamma(F) := \{ \text{ finite dimensional } F\text{-vector spaces with a } \Gamma\text{-action } \}.$$

[8] All rings in this course will be commutative.
[9] Keerthi claims this argument only requires M to be torsion free as opposed to M being projective, but it seems to me that we can even drop this assumption.

This notation for good reason should be compatible with the previous one and indeed it is. Let us define a functor

$$D_B : \mathsf{Rep}_\Gamma(F) \to \mathsf{Vect}_K, \text{ sending } V \mapsto (B \otimes_F V)^\Gamma$$

where Γ acts on the right by $\gamma(b \otimes v) = \gamma(b) \otimes \gamma(v)$.

Proposition 3.2. (a) *$D_B = D_{\operatorname{Frac} B}$ as functors.*

(b) *We have the inequality*

$$\dim_K D_B(V) \leq \dim_F V,$$

with equality iff

$$\alpha_{B,V} : B \otimes_K D_B(V) \to B \otimes_F V, \text{ sending } b \otimes (\Sigma b_j \otimes v_j) \mapsto \Sigma b b_j \otimes v_j$$

is an isomorphism of Γ-equivariant B-modules. Here Γ acts on B in the usual sense and on $D_B(V)$ trivially on the left.

Let us make two remarks before we proceed.

(a) $\alpha_{B,V}$ being an isomorphism is equivalent to saying that $B \otimes_F V \cong B^d$ as objects in $\mathsf{Rep}_\Gamma(B)$, with $d = \dim_K D_B(V)$.[10] This is in turn the same as saying that $B \otimes_F V$ is generated as a B-module by Γ-invariant elements in it.

(b) It's good to keep track of how we will use this formalism practically. In our future use, F will usually be $\mathbb{Q}_p$, and Γ will be a Galois group, which comes with a profinite topology, and we might require the representations here to be continuous.

In light of remark (a), it's good to make the following definition: let $M \in \mathsf{Rep}_\Gamma(B)$. We say that M is **trivial** if M is generated as a B-module by M^Γ. Then the equality holds in 3.2(b) iff $B \otimes_F V$ is trivial in the above sense.

Proof of 3.2. We have already shown (a). For (b) we must show $\dim_K D_{\operatorname{Frac}(B)}(V) \leq \dim_F(V)$, and it does no harm to assume that B is a field sine we can replace B by $\operatorname{Frac} B$ in both assertions. Indeed, specifically for the equality assertion, by full faithfulness from 3.1, we see that $\alpha_{B,V}$ is an isomorphism iff $\alpha_{\operatorname{Frac} B,V}$ is an isomorphism.

Given now B is a field, I claim that $\alpha_{B,V}$ is always injective. Indeed, suppose $x_1, \dots, x_n \in D_B(V)$ are linearly independent over K with $\sum b_i x_i = 0$ being a minimal linear dependence over B. We can WLOG assume that $b_1 = 1$, and we can also assume $b_2 \in B - K$, so there is $\gamma \in \Gamma$ such that $\gamma(b_2) \neq b_2$. We hit this linear dependence with γ to get $0 = \gamma(\sum b_i x_i) - \sum b_i x_i$ which is a nontrivlal linear dependence with fewer terms, giving a contradiction. This proves $\dim_K D_B(V) \leq \dim_B(B \otimes_F V) = \dim_F(V)$.

Equality holds here iff $B \otimes_K D_B(V)$ and $B \otimes_F (V)$ have the same dimension over B, but injectivity shows it's an isomorphism as finite dimensional B-vector spaces. $\square$

Rephrasing, for $V \in \mathsf{Rep}_\Gamma(F)$, the following are equivalent:

(a) $\alpha_{B,V}$ is an isomorphism.

[10] It's easy to see that taking Γ-invariants in B^d gives K^d, and this gives B^d once again after tensoring with B.

(b) $\dim_K D_B(V) = \dim_F V$.
(c) $B \otimes_F V \in \mathsf{Rep}_\Gamma(B)$ is trivial.

If any of the above conditions holds, we say that V is **B-admissible**.

Here's an example. Let $F = \mathbb{Q}_p$, and let $K/\mathbb{Q}_p$ be a finite extension, $\Gamma = \Gamma_K$ and $B = \mathbb{C}_p$. Last lecture we showed that $\mathbb{Q}_p(\chi_p^i) \in \mathsf{Rep}_{\Gamma_K}(\mathbb{Q}_p)$ is $\mathbb{C}_p$-admissible iff $i = 0$, since $B^\Gamma = K$ by the Ax-Sen-Tate lemma. In general, a continuous representation of Γ_K is $\mathbb{C}_p$-admissible iff inertia subgroup of Γ_K acts through a finite quotient (a result due to Sen), generalizing Tate's theorem on characters.

Next time we will see that B-admissible representations have some nice properties, and are stable under dualizing.

September 20, 2018. Thursday.

Last time we started with F a field of characteristic 0, B a domain which is a F-algebra, and Γ a group acting on B linearly. We had the assumption that B has no nontrivial Γ-stable ideals. This always holds when B is a field.

We defined the category

$$\mathsf{Rep}_\Gamma(B) = \{\text{ projective } B\text{-modules } M \text{ of finite rank with a compatible } \Gamma\text{-action }\}.$$

Then we had a fully faithful functor $M \mapsto M_\eta$ from $\mathsf{Rep}_\Gamma(B) \to \mathsf{Rep}_\Gamma(\operatorname{Frac} B)$. We defined $K = B^\Gamma = (\operatorname{Frac} B)^\Gamma$ and we looked at the functor

$$D_B : \mathsf{Rep}_\Gamma(F) \to \mathsf{Vect}_K, V \mapsto (B \otimes_F V)^\Gamma.$$

We had the proposition which asserts that

(a) $D_B = D_{\operatorname{Frac} B}$, and
(b) $\alpha_{B,V} : B \otimes_K D_B(V) \to B \otimes_F V$ is always injective, and is an isomorphism iff $\dim_K D_B(V) = \dim_F V$.

Towards the end, we defined that V is B-admissible if $\alpha_{B,V}$ is an isomorphism, or equivalently if $\dim_K D_B(V) = \dim_F V$. We write

$$\mathsf{Rep}_\Gamma^B(F) \text{ for the full subcategory of such } B\text{-admissible } V\text{'s.}$$[11]

B can be thought of measuring how complex the representations of V can be.

Proposition 3.3. *We have*
(a) $\mathsf{Rep}_\Gamma^B(F) = \mathsf{Rep}_\Gamma^{\operatorname{Frac} B}(F)$.
(b) $\mathsf{Rep}_\Gamma^B(F)$ *is closed under the following:*
  (i) *subrepresentations and and quotients.*
  (ii) *tensor products.*

[11]"Full" means we do not change the set of morphisms.

(iii) *duals.*[12]

(c) *The functor* $D_B : \mathsf{Rep}^B_\Gamma(F) \to \mathsf{Vect}_K$ *is faithful, and respects tensor products and duals.*[13]

Proof. (a) is clear. For (b)(i), assume that we have an exact sequence $0 \to V_1 \to V_2 \to V_3 \to 0$ in $\mathsf{Rep}_\Gamma(F)$ with V_2 B-admissible. Hit it with $B \otimes_F -$ to get another exact sequence $0 \to B \otimes_F V_1 \to B \otimes_F V_2 \to B \otimes_F V_3 \to 0$ in $\mathsf{Rep}_\Gamma(B)$. Now take Γ-invariants, which is a left exact functor, to get

$$0 \to D_B(V_1) \to D_B(V_2) \to D_B(V_3)$$

which is exact in Vect_K. Hence

$$\dim_F V_2 = \dim_K D_B(V_2) \le \dim_K D_B(V_1) + \dim_K D_B(V_3) \le \dim_F V_1 + \dim_F V_3 = \dim_F V_2.$$

This forces equality everywhere. For (b)(ii), pick $V_1, V_2 \in \mathsf{Rep}^B_\Gamma(F)$. Consider $D_B(V_1 \otimes V_2) = (B \otimes_F (V_1 \otimes_F V_2))^\Gamma$. We know that

$$D_B(V_1) \otimes_K D_B(V_2) \subseteq (B \otimes_F V_1) \otimes_B (B \otimes_F V_2) \cong B \otimes_F (V_1 \otimes_F V_2).$$

The inclusion is injective, and so we have a canonical injective map from $D_B(V_1) \otimes_K D_B(V_2) \to D_B(V_1 \otimes V_2)$. But this implies

$$\dim_F(V_1 \otimes_F V_2) = \dim_F V_1 \dim_F V_2 = \dim_K D_B(V_1) \dim_K D_B(V_2) \le \dim_K D_B(V_1 \otimes_F V_2).$$

We always have the reverse inequality, so we are good. For (b)(iii), pick $V \in \mathsf{Rep}^B_\Gamma(F)$. First assume that the $\dim_F(V) = 1$. This means that there is $\chi : \Gamma \to F^\times$ such that for any $v \in V, \gamma \in \Gamma$, we have $\gamma \cdot v = \chi(\gamma)v$. $D_B(V)$ is spanned by an element $b \otimes v$, where for it to be Γ-invariant, we have $\gamma(b) = \chi(\gamma)^{-1} b$ for all $\gamma \in \Gamma$. Consider $b^{-1} \in \operatorname{Frac} B$, then $\gamma(b^{-1}) = \chi(\gamma) b^{-1}$. If $\phi \in V^\vee - \{0\}$, then

$$\gamma(b^{-1} \otimes \phi)(1 \otimes v) = \chi(\gamma) b^{-1} \phi(\chi^{-1} v) = b^{-1} \otimes \phi(1 \otimes v).$$

So we exhibited a nonzero element in $D_{\operatorname{Frac} B}(V^\vee)$, proving that $\dim_K D_{\operatorname{Frac} B}(V^\vee) \ge 1 = \dim_F(V)$. So $V^\vee$ is $\operatorname{Frac} B$-admissible, and it's B-admissible (and so $b^{-1} \in B$).

In general, for $d = \dim_F V > 1$, first we observe that $\wedge^i_F V$ is B-admissible, for this is a quotient of $\otimes^i_F V$. We also observe that $\det(V^\vee) = \wedge^d V^\vee \cong \det(V)^\vee = (\wedge^d V)^\vee$ is also B-admissible, using our previous one-dimensional result.

There is a perfect pairing

$$\bigwedge^{d-1} V \otimes_F V \to \bigwedge^{d} V = \det(V), \text{ given by } (v_1 \wedge \cdots \wedge v_{d-1}) \otimes v \mapsto v_1 \wedge \cdots \wedge v_{d-1} \wedge v.$$

Hence we can identify $V^\vee \xrightarrow{\sim} \wedge^{d-1}_F V \otimes_F \det(V)^\vee$, which is B-admissible too.[14]

We leave (c) as an exercise. This is quite similar to the proof of 3.1. $\square$

[12]In the literature, usually this is the main assumption that is made, instead of our assumption we had on B. In other words, the assumption is that if b is acted on via a character, then b^{-1} is also in B.

[13]This functor cannot possibly be full: morphisms on the left form a F-vector spaces, and morphisms on the right form K-vector spaces.

[14]Writer's note: Keerthi jokes that he can never get around why this proof works, and while editing this I can only say the same, though I have the same feeling for plenty of other proofs.

3.2. Galois Descent and Faithfully Flat Descent.

Now let's assume that K/F is a extension of fields and $B = \overline{K}$. Let $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$. We'll always reserve the notation Γ_K for this Galois group.

Theorem 3.4 (Hilbert 90)**.** *We have*

$$\mathsf{Rep}_{\Gamma_K}^{\overline{K}}(F) = \left\{ \begin{array}{c} \textit{finite dimensional representations } V/F \textit{ of } \Gamma_K \\ \textit{on which the action is through a finite quotient} \end{array} \right\}.$$

Proof. Suppose that $V \in \mathsf{Rep}_{\Gamma_K}^{\overline{K}}(F)$. Then

$$\alpha_{\overline{K},V} : \overline{K} \otimes_K D_{\overline{K}}(V) \xrightarrow{\sim} \overline{K} \otimes_F V.$$

Fix bases $\{v_1, \dots, v_d\}$ for V and $\{w_1, \dots, w_d\}$ for $D_{\overline{K}}(V)$. Then we can write $v_i = \sum a_{ij} w_j$, and if $A := (a_{ij})$, then since there are only finitely many entries in A, A lives in $M_d(L)$ (d-by-d matrices with entries in L) for some finite extension L/K.

By construction, if $\gamma \in \Gamma_L$, then γ fixes V. Indeed,

$$\gamma(v_i) = \gamma\left(\sum_j a_{ij} w_j\right) = \sum_j \gamma(a_{ij})\gamma(w_j) \sum_j \gamma(a_{ij}) w_j = \sum_j a_{ij} w_j = v_i.$$

So the kernel of the Γ_K-action on V contains a finite index subgroup Γ_L. This proves the inclusion of the left into the right.

The other inclusion amounts to Hilbert 90 and Grothendieck's proof of it (hence the name of this theorem). Consider the finite Galois extension L/K, where $\Gamma = \mathrm{Gal}(L/K)$ is the supposed finite quotient and $B = L$. Then by definition

$$\mathsf{Rep}_\Gamma(L) = \{ \ L\text{-vector spaces } M \text{ acted on by } \Gamma = \mathrm{Gal}(L/K) \ \},$$

and there is a functor

$$\mathsf{Vect}_K \to \mathsf{Rep}_\Gamma(L) \text{ given by } V \mapsto L \otimes_K V.$$

Note that Γ acts on $L \otimes_K V$ by $\gamma(l \otimes v) = \gamma(l) \otimes v$, since V is defined over K. One formulation of Hilbert 90 then says that this is an equivalence of categories, with inverse $M \mapsto M^\Gamma = M^{\mathrm{Gal}(L/K)}$. (cf. Galois descent)

For this we must show for $M \in \mathsf{Rep}_\Gamma(L)$ where $\Gamma = \mathrm{Gal}(L/K)$, we have $L \otimes_K M^\Gamma \xrightarrow{\sim} M$. This map is always injective, with the same essential proof from last time exploiting a minimal linear dependence and hitting by $\gamma \in \Gamma$. So it is enough to show that the natural map $L \otimes_K M^\Gamma \to M$ is an isomorphism, which we can do so after tensoring with L over K. This means we can check whether

$$L \otimes_K L \otimes_K M^\Gamma \to L \otimes_K M$$

is an isomorphism. Notice that $L \otimes_K L$ is isomorphism to $\widetilde{L} = \prod_{\gamma \in \Gamma} L$ as L-algebra, where one sends $l_1 \otimes l_2 \mapsto (l_1 \gamma(l_2))_\gamma$. Γ acts on $L \otimes_K L$ only in the second copy of L. To make this equivariant though, we have to endow the right with a not-so-typical Γ-action: think of $\widetilde{L}$ as functions $f : \Gamma \to L$, and endow the action $\gamma f(\cdot) = f(\cdot\, \gamma)$. In other words, $\gamma \cdot (a_{\gamma'})_{\gamma'} = (a_{\gamma'})_{\gamma' \gamma^{-1}}$. Note that L embeds into $\widetilde{L}$ diagonally; and that $\widetilde{L}$ is not a field – one should not expect any less with $L \otimes_K L$.

Since the Γ-action on $\widetilde{L}$ has kernel L, it descends onto an Γ-action on $\widetilde{L}/L$. Let's consider

$$\mathsf{Rep}_\Gamma(\widetilde{L}) = \{ \text{ finite free } \widetilde{L}\text{-modules } \widetilde{M} \text{ with a compatible } \Gamma\text{-action } \}.$$

We have a functor $\mathsf{Vect}_L \to \mathsf{Rep}_\Gamma(\widetilde{L})$, sending $W \mapsto \widetilde{L} \otimes_L W$. Next time we will see that this is an equivalence with an inverse $\widetilde{M} \mapsto \widetilde{M}^\Gamma$, where a priori we can write $\widetilde{M} = \prod_{\gamma \in \Gamma} M_\gamma$. Here M_γ is a L-vector space with a Γ-action by $\gamma_0 : M_\gamma \to M_{\gamma_0\gamma}, lm \mapsto \gamma_0(l)\gamma_0(m)$.

September 26, 2018. Wednesday.

Today we will assume that K is a field of characteristic 0, and let $\overline{K}$ be its algebraic closure. Let $\Gamma = \mathrm{Gal}(\overline{K}/K)$, and K/F an extension of fields. Last time we claimed there is an equality of categories

$$\mathsf{Rep}_\Gamma^{\overline{K}}(F) = \{V \in \mathsf{Rep}_\Gamma(F) : \Gamma \text{ acts on } V \text{ via a finite quotient } \}.$$

We proved the $\subseteq$ inclusion. For the other inclusion, let's look at the following abstract situation. Let Γ be a finite group, A a commutative ring, and the A-algebra $\widetilde{A} := \prod_{\gamma\in\Gamma} A$, acted on by Γ using the description from last time. A embeds into $\widetilde{A}$ diagonally.[15] Let $\widetilde{M}$ be a $\widetilde{A}$-module with a compatible Γ-action. Since we have idempotents in A, namely 1 at one entry and 0's at the remaining entries, we can always hit these to $\widetilde{M}$ to break up $\widetilde{M} = \prod_{\gamma\in\Gamma} M_\gamma$. Explicitly, we have an isomorphism $M_{\gamma_1} \xrightarrow{\sim} M_{\gamma_1\gamma^{-1}}$, with the following compatible diagram for group action.

$$\begin{tikzcd}
M_\gamma \arrow[r, "\simeq"] \arrow[dr, "\simeq"'] & M_{\gamma\gamma_1^{-1}} \arrow[d, "\simeq"] \\
& M_{\gamma\gamma_1^{-1}\gamma_2^{-2}}
\end{tikzcd}$$

Consider $\widetilde{M}^\Gamma$ which consists of elements $\{(\gamma(m_1))_\gamma : m_1 \in M_1\}$. In otherwords, once $m_1 \in M_1 = M_{id}$ is fixed, we can uniquely determine a element in $\widetilde{M}^\Gamma$. I claim that the natural map

$$\widetilde{A} \otimes_A \widetilde{M}^\Gamma \xrightarrow{\sim} \widetilde{M}, \qquad (a_\gamma)_\gamma \otimes (\gamma(m_1))_\gamma \mapsto (a_\gamma\gamma(m_1))_\gamma$$

is an isomorphism. We leave this as an exercise for the readers.[16] This is completely general! We have imposed none of the finiteness, freeness or projectiveness (etc.) conditions.

There's another way to think about the above isomorphism. Consider the composition of maps

$$A \xhookrightarrow{a \mapsto (a)_\gamma} \widetilde{A} \xrightarrow{(a_\gamma)_\gamma \mapsto a_1} A.$$

This composes to identity. If $I = \ker(\pi : \widetilde{A} \to A)$, then $M_1 = \widetilde{M}/I\widetilde{M}$, and the above is saying that we can break up $\widetilde{A} = A \oplus I$, and similarly $\widetilde{M} = M_1 \oplus I\widetilde{M}$, and since $M_1 = \widetilde{M}^\Gamma$, we have $\widetilde{A} \otimes_A \widetilde{M}/I\widetilde{M} \xrightarrow{\sim} \widetilde{M}$.

---

[15] It's useful to remark at this point that A embeds into $\widetilde{A}$ diagonally, and we can also retrieve A from as a quotient by projecting onto A_{id}. We'll see this soon.

[16] Writer's note: I have worked it out, and the proof that I have goes something like this. So we can assume a minimal linear independence, and all the $a_{i,id} = 1$ by altering m_1's. This will force $a_{i,id} = a_{i,\gamma} = 1$ for all $\gamma \in \Gamma$. Then we can "factor out" $1 \otimes -$ to see that the original element (which a priori is a sum of m's) in $\widetilde{M}^\Gamma$ has to be $(0, 0, \ldots, 0)$ already. This proves injectivity. Thinking about surjectivity...

In any case, let's restrict our focus on where we were previously: L/K is a finite Galois extension, and $\Gamma = \mathrm{Gal}(L/K)$; M is a L-vector space[17] with a compatible Γ-action. Then Hilbert 90 says $L \otimes_K M^\Gamma \xrightarrow{\sim} M$. Let's see why this is true.

We have a natural map $\alpha_{L,M} : L \otimes_K M^\Gamma \to M$. We can regard α as a map of K-vector spaces, then we can tensor up to L and check whether $1 \otimes \alpha_{L,M}$ is an isomorphism. We can write $L \otimes_K M = (L \otimes_K L) \otimes_L M$, in which $L \otimes_K L = \widetilde{L}$.

As suggested, consider $1 \otimes \alpha_{L,M} : \widetilde{L} \otimes_L (L \otimes_K M^\Gamma) \to \widetilde{L} \otimes_L M$. By what we have established in the general theory, it suffices to show that $L \otimes_K M^\Gamma = (\widetilde{L} \otimes_L M)^\Gamma$ [18], for which we claim it is true. This is not difficult to check, so we again leave it to the readers. This concludes the proof of 3.4. $\square$

Let's package all of these up one last time: consider the exact sequence

$$0 \to M^\Gamma \to M \xrightarrow{m \mapsto (\gamma(m)-m)_\gamma} \bigoplus_{\gamma \in \Gamma} M.$$

Tensoring with L over K, we will get another exact sequence

$$\begin{array}{ccccccc}
0 \longrightarrow & L \otimes_K M^\Gamma & \longrightarrow & L \otimes_K M & \longrightarrow & L \otimes_K \bigoplus_{\gamma\in\Gamma} M \\
& \parallel & & \parallel & & \parallel \\
0 \longrightarrow & (\widetilde{L} \otimes_L M)^\Gamma & \longrightarrow & \widetilde{L} \otimes_L M & \longrightarrow & \bigoplus_{\gamma\in\Gamma} (\widetilde{L} \otimes_L M)
\end{array}$$

We note in the rightmost equality we have exploited the fact that $\otimes$ distributes over a finite direct sum. In full generality we would have needed some extra condition on Γ.

This is all from a gadget named **faithfully flat descent**. The property that we used is that we can check isomorphisms after tensoring up to a larger field, in which things simplify and so the verifications are nice and easy. In general, suppose we have a map of rings $R \to S$, the correct analogy is faithful flatness. We say that S is **faithfully flat** over R if the following holds for all R-modules M_1, M_2: a morphism $f : M_1 \to M_2$ of R-modules is an isomorphism iff $1 \otimes f : S \otimes_R M_1 \to S \otimes_R M_2$ is an isomorphism of S-modules. For example, field extensions are faithfully flat.

Here are some observations that we can make:

(a) The following are equivalent:[19]
   (i) S is faithfully flat over R.
   (ii) S is flat as an R-module, and $\mathrm{Spec}\, S \to \mathrm{Spec}\, R$ is a surjective map of schemes.

(b) If $R \to S$ is a map of local rings, then S is faithfully flat over R iff it is flat over R.

(c) Thus in particular, if L/K is an extension of p-adic valuation fields, then $\mathcal{O}_L$ is faithfully flat over $\mathcal{O}_K$.

We will talk more about faithfully flat descent next time.

[17] Previously we restricted ourselves to finite dimensional L-vector spaces, but in fact we can drop this assumption. The idea is that once we have picked, say, a linear dependence, which is a finite sum, we can immediately restrict ourselves back to a finite dimensional case.

[18] Remark: If we trace the L's correctly, we will see that Γ does not act on the L on the left here; and acts on $\widetilde{L} \otimes_L M$ diagonally

[19] A reference for this is Atiyah & Macdonald, Exercise 3.16.

Let's continue our discussion faithfully flat descent. Let's recall our setup, where we have a map of rings $f : R \to S$, and a base change functor $\mathsf{Mod}_R \to \mathsf{Mod}_S$ given by $M \mapsto f^*M = S \otimes_R M$[20]. We would like to describe the image of this functor. More explicitly, given a S-module N, how can we detect whether N is coming from a base change of a R-module M?

The simple example we should keep in mind throughout this discussion is the case where $f : K \to L$ and L/K is finite and Galois. The base change functor is given by $\mathsf{Vect}_K \to \mathsf{Vect}_L$ with $V \mapsto L \otimes_K V$. $\Gamma = \mathrm{Gal}(L/K)$ acts on $L \otimes_K V$ on the first coordinate, endowing $L \otimes_K V$ an extra structure for us to exploit. Thus the functor factors through $\mathsf{Vect}_K \to \mathsf{Rep}_\Gamma(L)$; and as mentioned last time, taking Γ-invariants provide an inverse to this functor.

Let's start with an observation. Suppose $M = f^*N$, where N is a R-module and M a S-module, then it has the following property: there is a canonical isomorphism α_M of $S \otimes_R S$-modules.

$$\alpha_M : \quad \begin{tikzcd} M \otimes_R S \arrow[rr, "\sim"] \arrow[d, equal] & & S \otimes_R M \arrow[d, equal] \\ (S \otimes_R N) \otimes_R S \arrow[dr, "\sim"'] & & S \otimes_R (S \otimes_R N) \arrow[dl, "\sim"] \\ & (S \otimes_R S) \otimes_R N & \end{tikzcd}$$

Both sides have an $S \otimes_R S$-action. More explicitly, $(S \otimes_R S)$ acts on $M \otimes_R S$ via $(s_1 \otimes s_2) \cdot (m \otimes s) = s_1 m \otimes s_2 s$, and on $S \otimes_R M$ by $s_1 s \otimes s_2 m$. The isomorphism α_M, is thus saying that these two actions are compatible.

Here's an alternative method to think about the isomorphism α_M. We are given $\alpha_M : M \otimes_R S \xrightarrow{\sim} S \otimes_R M$, and two maps $\phi_1, \phi_2 : S \to A$ of R-algebras. Then we have a map $\phi := \phi_1 \otimes \phi_2 : S \otimes_R S \to A$. There are two ways to pull this back to maps from S, namely via $j_1 := 1 \otimes s$ and $j_2 := s \otimes 1$.

$$S \underset{j_2 = (s \mapsto s \otimes 1)}{\overset{j_1 = (s \mapsto 1 \otimes s)}{\rightrightarrows}} S \otimes_R S \xrightarrow{\quad \phi \quad} A$$

Then the isomorphism $\alpha_M : M \otimes_R S \xrightarrow{\sim} S \otimes_R M$ is saying that $j_1^* M \xrightarrow{\sim} j_2^* M$. Taking ϕ^* now will give another commutative diagram

$$\begin{tikzcd} \phi^* j_1^* M \arrow[r, "\sim"] \arrow[d, equal] & \phi^* j_2^* M \arrow[d, equal] \\ \phi_1^* M \arrow[r, "\alpha_M(\phi_1, \phi_2)"'] & \phi_2^* M \end{tikzcd}$$

Here j_1, j_2 should be thought of as a universal pair of such maps, ie. if we are given an isomorphism for this pair of maps, then we have virtually given an isomorphism for all pairs as shown above.

Again, an example to keep track of things in mind is the Galois case. If $\gamma_1, \gamma_2 \in \Gamma$, then we have two maps $\gamma_1, \gamma_2 : L \rightrightarrows L$. If $M \in \mathsf{Vect}_L$, then there is an isomorphism $\alpha(\gamma_1, \gamma_2) : \gamma_1^* M \xrightarrow{\sim} \gamma_2^* M$. In

[20]One should think of f^* as pulling back of coherent sheaves, so in short on the level of modules f^* "does not really behave like a pullback as it might seem" on a naïve level.

particular when $\gamma_2 = 1$, then we have fixed an isomorphism $\gamma_1^* M \xrightarrow{\sim} M$, ie. $L \otimes_{L,\gamma_1} M \to M$. This data is same as saying γ_1 induces an isomorphism $M \xrightarrow{\sim} M$ and is γ_1-linear, ie. $\gamma_1(lm) = \gamma_1(l)\gamma_1(m)$.

Furthermore, consider the following situation: if $\phi_1, \phi_2, \phi_3 : S \to A$, then we require it to satisfy the commutative diagram (let's call it $(*)$ for convenience)

$$\begin{tikzcd} \phi_1^* M \arrow[r, "\alpha_M(\phi_1,\phi_2)", "\sim"'] \arrow[dr, "\sim", "\alpha_M(\phi_2,\phi_3)"'] & \phi_2^* M \arrow[d, "\alpha_M(\phi_2,\phi_3)", "\wr"'] \\ & \phi_3^* M \end{tikzcd}$$

In the Galois example, this simply translates to the fact that the automorphism $\gamma : M \xrightarrow{\sim} M$ with $\gamma \in \Gamma$ varies form a group action.

In any case let us move on. Here is the upshot. If the starting map $f : S \to R$ is already faithfully flat, then the observaton that we make, namely the existence of the isomorphism $\alpha_M : M \otimes_R S \xrightarrow{\sim} S \otimes_R M$, already gives a sufficient (and necessary a priori) condition for M to come from extension from R.

Let's be more precise. Let's take $M \in \mathsf{Mod}_S$. A **descent datum** on M for the map $f : R \to S$ is an isomorphism of $S \otimes_R S$-modules $\alpha_M : M \otimes_R S \xrightarrow{\sim} S \otimes_R M$ with the property that diagram $(*)$ commutes for all R-algebras A and all triples $\phi_1, \phi_2, \phi_3 : S \to A$. (Once again, in the Galois setting, this means that the action by group elements actually fits into a group action.)

Then we can look at the category

$$\mathsf{Mod}_S^f = \{(M, \alpha_M) : M \in \mathsf{Mod}_R, \alpha_M \text{ a descent datum on } M\}.$$

(In this Galois setting, this is equivalent to the $\mathsf{Vect}_K = \mathsf{Rep}_\Gamma(L)$ data.) There is a natural functor

$$\mathsf{Mod}_R \to \mathsf{Mod}_S^f, N \mapsto (f^* N, \alpha_{f^* N}).$$

(In the Galois setting this corresponds to the functor $\mathsf{Vect}_K \to \mathsf{Rep}_\Gamma(L)$.) The theorem of faithfully flat descent states that

Theorem 3.5 (Faithfully flat descent). *The above functor*

$$\mathsf{Mod}_R \to \mathsf{Mod}_S^f, \text{ given by } N \mapsto (f^* N, a_{f^* N})$$

is an equivalence of categories, with the inverse given by

$$(M, \alpha_M) \mapsto \{m \in M : \alpha_M(m \otimes 1) = 1 \otimes m\}.$$

In terms of Galois situation, α_M should be thought of as a galois action, and the condition is same as saying m is Galois fixed (ie. $m \in M^\Gamma$).

It's good to get away from the formalism for a while, so let's see where we are headed. Let's consider the case

(a) $\widehat{K_\infty}/\mathbb{Q}_p$, where $\widehat{K_\infty} = \widehat{\mathbb{Q}_p(\zeta_{p^\infty})}$, and over which we have $\mathbb{C}_p/\widehat{K_\infty}$.

(b) Take $\Gamma = \mathrm{Gal}(\overline{\widehat{K_\infty}}, \widehat{K_\infty})$.

Then Krasner's lemma says this is same as $\mathrm{Gal}(\overline{K_\infty}/K_\infty)$. We would have loved to study $\mathsf{Rep}_\Gamma(\mathbb{Q}_p)$, but a better object to look at is the $\mathbb{C}_p$-admissible representations $\mathsf{Rep}_\Gamma^{\mathbb{C}_p}(\mathbb{Q}_p)$. Even with this, things get pretty horrible since $\mathbb{C}_p$ is too big. So more precisely we would look at the representations which are continuous.

You might ask though, what does it mean for a representation of Γ to be continuous? Γ has a (profinite) topology where open subgroups are the ones of finite index. Giving $V \in \mathsf{Rep}_\Gamma(\mathbb{Q}_p)$ is the same as giving $\rho_V : \Gamma \to GL_n(\mathbb{Q}_p)$, where we endow $GL_n(\mathbb{Q}_p)$ with the p-adic topology: two matrices A, B are close iff $A^{-1}B$ is close to 1 p-adically), and we say that V is continuous if ρ_V is continuous.

Then we have a functor $\mathsf{Rep}_\Gamma^{\widehat{K_\infty}}(\mathbb{Q}_p) \to \mathsf{Rep}_\Gamma^{\mathbb{C}_p}(\mathbb{Q}_p)$, which is actually an equivalence; or for what is the same, every object in $\mathsf{Rep}_\Gamma^{cts}(\mathbb{C}_p)$ is trivial – this is because every object in $\mathsf{Rep}_\Gamma^{\widehat{K_\infty}}(\mathbb{Q}_p)$ is trivial. Concretely, $\mathbb{C}_p \otimes_{\widehat{K_\infty}} M^\Gamma \xrightarrow{\sim} M$. So by requiring representations to be continuous, we have a similar statement to $\mathsf{Vect}_K = \mathsf{Rep}_\Gamma(L)$. This is what we call almost étale descent, which due to fontaine. We will give a more modern perspective. The map $f : R \to S$ will be our $\widehat{K_\infty} \to \mathbb{C}_p$.

All these will definitely not be true if K_∞ replaced by $\mathbb{Q}_p$; because that would say every $\mathbb{C}_p$-admissible representation of $\Gamma_\mathbb{Q}$ is generated by invariants. This amounts to a property of $\widehat{K_\infty}$ – it is what we call a perfectoid field. We will see how to do this later.

We will end today's class with an example. Let L/K be a finite Galois extension of valuation fields with $\Gamma = \mathrm{Gal}(L/K)$, then $f : \mathcal{O}_K \to \mathcal{O}_L$ is faithfully flat. Faithfully flat descent says that

$$\mathsf{Mod}_{\mathcal{O}_K} \xrightarrow{\sim} \mathsf{Mod}_{\mathcal{O}_L}^f,$$

but we claim that

$$\mathsf{Mod}_{\mathcal{O}_L}^f \neq \mathsf{Rep}_\Gamma(\mathcal{O}_L).$$

As opposed to $L \otimes_K L \xrightarrow{\sim} \prod_\Gamma L$, the map

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \prod_{\gamma \in \Gamma} \mathcal{O}_L$$

is usually <u>not</u> an isomorphism because of ramification.

Let's take $L = \mathbb{Q}_p(\zeta_p), K = \mathbb{Q}_p$ and $\mathcal{O}_L = \mathbb{Z}_p[\zeta_p]$. Then $\Gamma = (\mathbb{Z}/p\mathbb{Z})^\times$. Consider the map

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \prod_{\gamma \in \Gamma} \mathcal{O}_L.$$

The left side has $\mathcal{O}_L$-basis $x_i := 1 \otimes \zeta_p^i$, while the right has the standard $\mathcal{O}_L$-basis $\{e_\gamma\}_{\gamma \in \Gamma}$. With respect to these basis, this map $x \otimes y \mapsto (x\gamma(y))_\gamma$ has matrix

$$\begin{pmatrix} 1 & \zeta_p & \cdots & \zeta_p^{p-1} \\ 1 & \zeta_p^2 & \cdots & \zeta_p^{2(p-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_p^{p-1} & \cdots & \zeta_p^{(p-1)^2} \end{pmatrix}$$

which is a Vandermonde matrix, and thus its determinant is $\prod_{j>i}(\zeta_p^j - \zeta_p^i)$, which has valuation at least 1 evidently and so it is not invertible in $\mathbb{Z}_p[\zeta_p]$.

In fact, in this case, the map is an isomorphism iff L/K is unramified.

September 28, 2018. Friday.

3.3. Introduction to Perfectoid Fields.

Today we will talk about $\widehat{K_\infty}$, which we will see soon is a perfectoid field. There are two observations that we can make:

(a) $\widehat{K_\infty}$ is not discrete, and
(b) the p-power map on $\mathcal{O}_{\widehat{K_\infty}}/(p)$ is surjective.

These two observations are equivalent to saying

(a') there exists an element $\varpi \in \mathcal{O}_{\widehat{K_\infty}}$ [21] such that $\varpi^p \mid p$, and that
(b') $\mathcal{O}_K/\varpi \to \mathcal{O}_K/\varpi^p$ is an isomorphism.

The proof to this can be found in 3.11.

The existence of ϖ can be checked readily. For example, one can take $\varpi = (\zeta_{p^2} - 1)^{p-1}$, where $(\zeta_{p^2} - 1)$ is a uniformizer of $\mathbb{Z}_p[\zeta_{p^2}]$. In addition, (b) implies $x \mapsto x^p$ induces an isomorphism $\mathcal{O}_{\widehat{K}_\infty}/\varpi \xrightarrow{\sim} \mathcal{O}_{\widehat{K}_\infty}/\varpi^p$. This will then show $\widehat{K_\infty}$ is not discrete, since $|\widehat{K_\infty}^\times| \subseteq \mathbb{R}_{>0}$ is p-divisible. So the heart of the equivalence lies in proving (b) assuming (a') and (b').

One can also check (b) directly. Write $K_n = \mathbb{Q}_p(\zeta_n)$, then $\mathcal{O}_{K_n} = \mathbb{Z}_p[T]/(\Phi_{p^n}(T))$, so $\mathcal{O}_{K_n}/p = \mathbb{F}_p[T]/((T-1)^{\phi(p^n)}) = \mathbb{F}_p[U]/(U^{\phi(p^n)})$ by a change of variable $U = T - 1$. Hence

$$\mathcal{O}_{\widehat{K_\infty}}/p = \mathcal{O}_{K_\infty}/p = \varinjlim_n \mathcal{O}_{K_n}/p = \varinjlim_{u \mapsto u^p} \frac{\mathbb{F}_p[U]}{(U^{\phi(p^n)})} = \frac{\mathbb{F}_p[U_1, U_2, \ldots,]}{(U_i^{\phi(p^i)}, U_i^p = U_{i-1})}.$$

Now it can readily be verified that the p-power map is indeed surjective.

These observations motivate the following definition. A **perfectoid field** K is a complete non-discrete[22] valuation field such that there is $\varpi \in \mathcal{O}_K$ with

(a) $\varpi^p \mid p$, and
(b) $x \mapsto x^p$ induces an isomorphism $\mathcal{O}_K/\varpi \xrightarrow{\sim} \mathcal{O}_K/\varpi^p$.

We can still make sense of this when $\operatorname{char} K = p$, in which case K is a nondiscrete complete perfect valuation field. We also require nondiscreteness because we would like to rule out finite fields being perfectoid. In fact, a perfect valuation field is either a finite field or nondiscrete. Indeed, being perfect means group of valuation is p-divisible, so it is either trivial (in which case it is a finite field) or non-trivial. So we can replace nondiscreteness by nontrivialness in the definition.

---

[21] ϖ is not necessarily a uniformizer despite the notation.
[22] Non-discreteness is automatic for characteristic 0 fields given (a) and (b), as explained above.

Theorem 3.6 (Almost purity). [23] *If K is perfectoid, and L/K a finite separable extension*[24]*, then L is perfectoid.*

The proof can be found at 4.4.

One can try to prove this for the characteristic p case which is easier; though it is also true for the characteristic 0 case. One difficulty is that it's not easy to describe $\mathcal{O}_L$ if L is non discrete: $\mathcal{O}_L$ is not even finitely generated over $\mathcal{O}_K$ in general. In fact, $\mathcal{O}_L$ being a finitely generated $\mathcal{O}_K$ algebra is equivalently to $\mathcal{O}_L$ being the unique "unramified" lift of a finite separable extension of k_K (Henselian still works for nondiscrete setting). Here "unramified" is in quotations because it's not entirely clear anymore what it means. Even worse $\mathcal{O}_K$ is not Noetherian, though it is still a Bezout domain: finitely generated ideals are principal.

Let K be a perfectoid field. We define

$$\mathcal{O}_{K^\flat} := \varprojlim_{x\mapsto x^p} \mathcal{O}_K/(p), \text{ and } K^\flat := \operatorname{Frac}\mathcal{O}_{K^\flat}.$$

(Verbally we call this K-tilt.) More explicitly, $\mathcal{O}_{K^\flat}$ consists of infinite sequences $(x_0, x_1, \ldots)$ where $x_i \in \mathcal{O}_K/(p)$ and $x_i^p = x_{i-1}$. We give two examples:

(a) If K has characteristic p, then $x \mapsto x^p$ is already an isomorphism, so $\mathcal{O}_{K^\flat} = \mathcal{O}_K$.
(b) (!) If $K = \widehat{K_\infty} = \widehat{\mathbb{Q}_p(\zeta_{p^\infty})}$, then $K^\flat = \mathbb{F}_p((t))(t^{1/p^\infty})$.

Theorem 3.7. *Suppose K is perfectoid, then*

(a) *$\mathcal{O}_{K^\flat}$ has a noncanonical valuation $|\cdot|^\flat : \mathcal{O}_{K^\flat} - \{0\} \to \mathbb{R}_{>0}$ and is complete with respect to this.*
(b) *$\mathcal{O}_{K^\flat}$ is an integral domain, so $K^\flat$ is well-defined, and is a perfectoid field with $\operatorname{char} K^\flat = p$.*
(c) *For every finite extension $\widetilde{L}/K^\flat$, there is a canonical perfectoid finite extension L/K such that $L^\flat = \widetilde{L}$ with $[L : K] = [\widetilde{L} : K^\flat]$.*
(d) *If $K^\flat$ is algebraically closed, then K is also algebraically closed.*

Here is one trick to use the theorem: Take union of all perfectoid guys from (iii), take tilt/flat of union, then you get union of all finite extensions of $K^\flat$, which is algebraically closed, and use (iv).

Witt Vectors.

Classical motivation: Question: $\mathbb{Z}_p$, for every n, there exists a unique unramified extension $\mathbb{Z}_{p^n} \mid \mathbb{Z}_p$ with residue field $\mathbb{F}_{p^n}$. (For $\mathbb{Z}_p$ choose coset reps for $\mathbb{F}_p$, then power series in such coefficients – same story for $\mathbb{Z}_{p^n}$.) Is there a canonical choice of coset reps, ie. a canonical injection $\mathbb{F}_{p^n} \hookrightarrow \mathbb{Z}_{p^n}$ of sets?

Question 2: If $\alpha : \mathbb{F}_{p^n} \hookrightarrow \mathbb{Z}_{p^n}$ is such an injection, how does multiplication and addition work when we write $x \in \mathbb{Z}_{p^n}$ in the form $\sum_{n=0}^\infty \alpha(t_n)p^n$?

Answer: Witt vectors.

(1) Every $t \in \mathbb{F}_{p^n}$ satisfies $t^{p^n} - t = 0$. So $X^{p^n} - X \in \mathbb{Z}_{p^n}[X]$ is a separable polynomial $\mod p$. Hensel says that for every $t \in \mathbb{F}_{p^n}$, there is a unique $[t] \in \mathbb{Z}_{p^n}$ such that (a) $[t]^{p^n} - [t] = 0$, and $[t] \equiv t$

[23] This is a special case of the traditional version of the theorem.
[24] One can deduce from the discussion above that separateness is automatic, because K is perfect in both char 0 and char p cases. In addition, one can think of finite separateness here as a special case of a finite étale map.

(mod p). Exercise: if $t_1, t_2 \in \mathbb{F}_{p^n}$, then $[t_1t_2] = [t_1][t_2]$. (NOTE: for $\mathbb{Z}_{p^n}$, $\{0, \dots, p^n - 1\}$ is not the answer!!!) So $[\cdot] : \mathbb{F}_{p^n} \to \mathbb{Z}_{p^n}$ is the unique multiplicative section of $\mathbb{Z}_{p^n} \twoheadrightarrow \mathbb{F}_{p^n}$.

(2) is the thing answered by Witt vectors: gives canonical polynomials P_n, Q_n over $\mathbb{Z}$ such that $\sum_{n=0}^{\infty}[t_n]p^n + \sum[s_n]p^n = \sum P_n([t_1], \dots, [t_n], [s_1], \dots, [s_n])p^n$, and similarly for product (coeff is $Q_n([t_1], \dots, [t_n], [s_1], \dots, [s_n])$.

October 1, 2018. Monday.

3.4. Completions.

Usually commutative algebra books deal with completion under a Noetherian setting, but that's not good enough for us. That's why we have to set up our own formalism here.

Let R be a (commutative) ring, and as motivated we will not require R to be Noetherian. A **countable linear topology** on R is a topology for which a basis of open neighbourhoods of 0 is given by a countable descending sequence of ideals

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots .$$[25]

With this, we endow R with a topological ring structure. In other words, for any other element $r \in R$, a basis of open neighbourhoods around r is given by translates from 0. More precisely, usually we say that $(R, \{I_k\}_k)$ is a **linearly topological ring**. Two such sequences $\{I_k\}_k$ and $\{J_k\}_k$ endow R with the same topology iff for any k, there is n_k, m_k such that $I_k \subseteq J_{n_k}$ and $J_k \subseteq I_{m_k}$.

If $I \subseteq R$ is an ideal, then the ***I*-adic topology** is the one associated with the sequence $\{I^k : k \geq 1\}$. For example, the norm topology on $\mathcal{O}_{\mathbb{C}_p}$ is the (p)-adic topology, and in contrast the $\mathfrak{m}_{\mathbb{C}_p}$-adic topology is uninteresting, because $\mathfrak{m}_{\mathbb{C}_p}^2 = \mathfrak{m}_{\mathbb{C}_p}$.

We then say $(R, \{I_k\}_k)$ is **complete** if for all sequences $\{i_k : i_k \in I_k\}$, there exists a unique $r \in R$ such that $r - \sum_{k=1}^{n} i_k \in I_{n+1}$. In this case we should think of r as the limit of the sequence $\{i_k\}_k$, or more precisely

$$r = \varinjlim_n \sum_{k=1}^{n} i_k := \sum_{k=1}^{\infty} i_k.$$

We remark that if $(R, \{I_k\})$ is complete, then it's separated or Hausdorff, ie. $\cap_{k\geq 1} I_k = \{0\}$. For example, since $\mathbb{C}_p = \widehat{\overline{\mathbb{Q}_p}}$ by construction, $\mathcal{O}_{\mathbb{C}_p}$ is complete for the p-adic (or (p)-adic) topology.

Here's one question that we can ask: If $I \subseteq J \subseteq R$ where I, J are ideals in R, when does R being J-adically complete imply that it's I-adically complete? The following gives a sufficient condition.

Proposition 3.8. *Suppose $J \subseteq R$ is an ideal such that R is J-adically complete. Suppose $I = (f_1, \dots, f_r) \subseteq J$ is a finitely generated ideal (while J is not necessarily finitely generated). Then R is I-adically complete.*

We shall prove this in conjunction with the following

[25] We want to define it this way as opposed to simply specifying a set of ideals as open sets, for then we would have more than a countable sequence.

Lemma 3.9. *Suppose $I = (f_1, \dots, f_r) \subseteq R$. Then TFAE:*

(a) *R is I-adically complete.*
(b) *$(R, \{I_k\}_k)$ is complete where $I_k = (f_1^k, \dots, f_r^k)$.*
(c) *For each j, R is (f_j)-adically complete.*

Proof of 3.9. (a) and (b) are equivalent because the topologies are the same: $I^{kr+1} \subseteq I_k$ for example, while $I_k \subseteq I^k$ is obvious. Furthermore (c) implies (b): if $i_k = a_{k,1} f_1^k + \dots + a_{k,r} f_r^k$, then

$$\sum_{k=1}^{\infty} i_k = \sum_{k=1}^{\infty} a_{k,1} f_1^k + \dots + \sum_{k=1}^{\infty} a_{k,r} f_r^k.$$

Each term on the right is well-defined. Finally, we will show that (a) implies (c) as a intermediate by-product while proving 3.8. $\square$

Proof of 3.8. The idea is we must show the J-adic limit is also the I-adic limit (assuming it exists); were they different then there would be two J-adic limits.

First we show the base case $r = 1$ without using 3.9. Write $I = (f)$, and suppose we have a sequence $i_k = a_k f^k$ where $a_k \in R$. It's evident that $i_k \in J^k$, so it converges J-adically to r, ie. there is $r \in R$ such that for any n, $r - \sum_{k=1}^{n} i_k \in J^{n+1}$. But alternatively we write the tail

$$i_{n+1} + i_{n+2} + \cdots = f^{n+1}(a_{n+1} + a_{n+2} f + a_{n+3} f^2 + \cdots) =: f^{n+1} L.$$

Then L also converges J-adically to some $s_n \in R$. This suggests $r - \sum_{k=1}^{n} i_k = f^{n+1} s_n \in I^{n+1}$, which completes the base case. This proves the (a) implies (c) in the lemma 3.9, so now we can use the lemma![26]

Now for the general case, let's assume that $I = (f_1, \dots, f_r)$. By the lemma it's sufficient to show that R is (f_j)-adically complete for each $j = 1, \dots, r$. But this is just a repeated use of the base case. This completes the proof of the proposition. $\square$

Suppose $I \subseteq R$ and R is I-adically complete. If $i \in I$, then $1 + i \in R^\times$, since we have

$$(1+i)^{-1} = \sum_{k=0}^{\infty} (-1)^k i^k.$$

In particular, $I \subseteq \mathrm{Jac}(R)$, where the Jacobson radical is the intersection of all maximal ideals.[27]

We then have a lemma which is akin to the Nakayama's lemma but without the finitely generatedness condition, but we'll save it for next time.

October 3, 2018. Wednesday.

We first tailor make a version of Nakayama's lemma without any finiteness condition.

Lemma 3.10. *Suppose we have $f : R \to S$ is a ring homomorphism, $I \subseteq R$ is an ideal, and define $J := f(I)S$. Suppose that*

(a) *R is I-adically complete, and*

[26] It looks like we only use that implication from (c) to (a) in the lemma, but it's nice to note their equivalence.
[27] This is due to a characterizaiton of $\mathrm{Jac}(R)$: $x \in \mathrm{Jac}(R)$ iff for any $y \in R$, we have $1 + xy \in R^\times$.

(b) *S is J-adically separated,*

(c) *the composition $R \xrightarrow{f} S \to S/J$ is surjective.*

Then f is surjective.

Proof.[28] Fix $s \in S$, and we will inductively construct $i_j \in I^j$ such that $s - f(\sum_{j=0}^{n} i_j) \in J^{n+1}$, so $s - f(\sum_{j=0}^{\infty} i_j) \in \cap J^{n+1} = 0$ by assumption (b). When $j = 0$, hypothesis (c) says there is $i_0 \in R$ such that $s - f(i_0) \in J$, which is our base case.

Next we do the inductive step. Suppose that we have constructed $i_0, \ldots, i_{n-1}$ such that $s - f(\sum_{j=0}^{n-1} i_j) \in J^n$. So we can write

$$s - f\left(\sum_{j=0}^{n-1} i_j\right) = \sum_{k=0}^{m} f(r_k) s_k$$

where $r_k \in I^n$ and $s_k \in S$. Again by (c) or the base case, we can find $u_k \in R, w_k \in J$ with $s_k = f(u_k) + w_k$. Then

$$s - f\left(\sum_{j=0}^{n-1} i_j\right) = \sum_{k=0}^{m} f(r_k)(f(u_k) + w_k)$$

and so

$$s - f\left(\sum_{j=0}^{n-1} i_j - \sum_{k=0}^{m} r_k u_k\right) = \sum_{k=0}^{m} f(r_k) w_k \in J^{n+1}$$

which completes the proof. ☐

Let's take K to be a complete valuation field over $\mathbb{Q}_p$. There were two definitions that we gave for perfectoid fields: see subsection 3.3. Let's recall it here for convenience.

Proposition 3.11. *Let K to be a complete valuation field over $\mathbb{Q}_p$. TFAE:*

(a) *K is not discrete, and the p-power map on $\mathcal{O}_K/(p)$ is surjective.*

(b) *There is an element $\varpi \in \mathcal{O}_K$ such that $\varpi^p \mid p$, and $x \mapsto x^p$ induces an isomorphism $\mathcal{O}_K/(\varpi) \to \mathcal{O}_K/(\varpi^p)$.*

If any of these equivalent conditions is satisfied, we say that K is a perfectoid field.

Proof. Let's show (a) implies (b). K is nondiscrete, so there is $\varpi \in \mathcal{O}_K$ with $p^{-1/p} \le |\varpi| < 1$, and so $|\varpi^p| \ge p^{-1} = |p|$, so $\varpi^p \mid p$.

For the other direction, consider the diagram

$$\begin{tikzcd} & \mathcal{O}_K/(\varpi) \arrow[r, "g : x \mapsto x^p"] & \mathcal{O}_K/(\varpi^p) \\ \mathcal{O}_K \arrow[r, "pr"] & \mathcal{O}_K/(p) \arrow[u, two heads, "\pi"] \arrow[r, "f : x \mapsto x^p"] & \mathcal{O}_K/(p) \arrow[u, two heads, "\pi'"'] \end{tikzcd}$$

[28] Writer's note: I have asked Keerthi why the following usual proof won't work: For a R-module M, first one can show that $M = IM$ implies $M = 0$, and apply this proof to the cokernel. Keerthi told me that this proof will not work since $\cap I^n M \neq (\cap I^n) M$ in general, for example when M is the cokernel of $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$. In fact, the proof of my claim requires either M is separated, that is $\cap I^n M = 0$, or I is nilpotent.

The vertical maps are surjective since $\varpi^p \mid p$. The top map g is also always injective. The bottom arrow f is surjective iff top arrow g is: indeed, if f is, then g is evidently. If g is, then apply 3.10 to the bottom right composition $\mathcal{O}_K \xrightarrow{f\circ pr} \mathcal{O}_K/(p) \xrightarrow{\pi'} \mathcal{O}_K/(\varpi^p)$ (with $I = (\varpi^p)$). As noted previously K is nondiscrete because if $x \in \mathcal{O}_K$ with $|x| > |p| = p^{-1}$, then $|x|^{1/p} \in |K^\times|$. $\square$

3.5. Strict p-rings and Witt Vectors.

We define a **strict p-ring** to be a p-adically complete and flat (ie. torsion free) $\mathbb{Z}_p$-algebra R, such that R/pR is a perfect $\mathbb{F}_p$-algebra. [29]

There are plenty of examples, including $\mathbb{Z}_p$, and in fact the ring of integers in any unramified extension of $\mathbb{Q}_p$ is also a strict p-ring. The upshot is, given a R/pR which is perfect $\mathbb{F}_p$-algebra, there is a unique strict p-ring that lifts it.

Lemma 3.12. *Let R be a $\mathbb{Z}_p$-algebra, and $x, y \in R$ be such that $x \equiv y \pmod{p^n}$. Then $x^p \equiv y^p \pmod{p^{n+1}}$.*

Proof. $x^p - y^p = (x-y)(x^{p-1} + x^{p-2}y + \cdots + y^{p-1})$. The first term is $0 \pmod{p^n}$ and the latter is $px^{p-1} \pmod{p^n}$, so their product is $0 \pmod{p^{n+1}}$. $\square$

Lemma 3.13. *Suppose $\overline{R}$ is a perfect $\mathbb{F}_p$-algebra, S is a p-adically complete $\mathbb{Z}_p$-algebra, and $f : \overline{R} \to S/pS$ is a ring homomorphism. Then there exists a unique multiplicative lift $\widetilde{f} : \overline{R} \to S$ of f. That is, $\widetilde{f}(a) \pmod{p} = f(a)$, and $\widetilde{f}(ab) = \widetilde{f}(a)\widetilde{f}(b)$, and $\widetilde{f}$ is unique such.*

$$\begin{tikzcd} & S \arrow[d] \\ \overline{R} \arrow[ur, dashed, "\widetilde{f}"] \arrow[r, "f"'] & S/pS \end{tikzcd} \qquad \begin{tikzcd} \overline{R} \arrow[r, "\widetilde{f}"] \arrow[d, "x \mapsto x^p"'] & S \arrow[d, "x \mapsto x^p"] \\ \overline{R} \arrow[r, "\widetilde{f}"'] & S \end{tikzcd}$$

The proof uses what is traditionally called the Dwork's trick, or at least a version of it.

Proof. A priori every element of $\overline{R}$ as a p-th root. If $\widetilde{f}$ exists, then it satisfies $\widetilde{f}(a^{p^{-1}})^p = \widetilde{f}(a)$. So $\widetilde{f}$ is equivariant for the p-power maps on $\overline{R}$ and S. Dwork's trick says approximately that the p-power map is usually a contraction, so we can given a, we can find the fixed point $\widetilde{f}(a)$ by doing the p-power map many times.

More precisely, first fix lifts $\widetilde{s}_i \in S$ of $f(a^{p^{-i}}) \in S/pS$ for each i. Then $\widetilde{s}_n^p, \widetilde{s}_{n-1}$ are both lifts of $f(a^{p^{-n-1}})$, so $\widetilde{s}_n^p \equiv \widetilde{s}_{n-1} \pmod{p}$. Then we can apply 3.12 to raise both sides to p-th power over and over again to get $\widetilde{s}_n^{p^n} \equiv \widetilde{s}_{n-1}^{p^{n-1}} \pmod{p^n}$. So the limit of $\widetilde{s}_n^{p^n}$ exists in S, and define

$$\widetilde{f}(a) := \lim_{n\to\infty} \widetilde{s}_n^{p^n}.$$

If we picked a different set of lifts, they will differ $\pmod{p}$, so their p-th powers differ modulo higher powers of p using 3.12, so they give the same limit, so the definition is well-defined.

We must also check that $\widetilde{f}$ is multiplicative: $\widetilde{f}(a)\widetilde{f}(b)$ certainly reduces to $f(a)f(b) = f(ab)$. Multiplicativeness comes for free from how we defined $\widetilde{f}(a)$ inductively. Finally we must show that

[29] This means that the Frobenius map on R/pR is an isomorphism.

such a multiplicative lift is unique, but the only choice we could have made was compatible lifts of $f(a^{p^{-i}})$, for which we have already proved that $\widetilde{f}$ is unique. $\square$

We know $\widetilde{f}$ behaves nicely multiplicatively; what happens to $\widetilde{f}(a+b)$ though? We know from the proof that

$$\widetilde{f}(a+b) = \lim_{n\to\infty} (\widetilde{f}(a^{p^{-n}}) + \widetilde{f}(b^{p^{-n}}))^{p^n},$$

because $\widetilde{f}(a+b) \equiv (\widetilde{f}(a^{p^{-n}}) + \widetilde{f}(b^{p^{-n}}))^{p^n} \pmod{p^{n+1}}$.

In particular, if R is a strict p-ring, with $R/pR = \overline{R}$, then the identity $\overline{R} \to \overline{R}$ lifts to a multiplicative map $[\cdot] : \overline{R} \to R$, which we will call the **Teichmüller lift**. Moreover, akin to $\mathbb{Z}_p$, every element of R can be written uniquely in the form $\sum_{n=0}^{\infty} p^n [a_n]$, with $a_n \in \overline{R}$, where a_n is determined inductively: Pick

$$\begin{aligned}
a_0 &= r \mod p \\
a_1 &= \frac{r - p[a_0]}{p} \mod p \\
&\vdots \\
a_n &= \frac{r - \sum_{j=0}^{n-1} p^j [a_j]}{p} \mod p
\end{aligned}$$

Torsionfreeness in the definition of a strict p-ring is used to define division by p (otherwise there won't have been a canonical choice). We shall call $[a_i]$'s the **Teichmüller coordiantes**.

It turns out as a consequence that strict p-rings are very *rigid*:

Theorem 3.14. *Let R be a strict p-ring with $\overline{R} = R/pR$, and let S be p-adically complete $\mathbb{Z}_p$-algebra. Then the functor*

$$\mathrm{Hom}_{\mathbb{Z}_p\text{-alg}}(R, S) \to \mathrm{Hom}_{\mathbb{F}_p\text{-alg}}(\overline{R}, S/pS), \text{ given by } \phi \mapsto \phi \pmod{p}$$

is a bijection with its inverse given by

$$\Theta(f) \leftarrow\!\shortmid f, \text{ where } \Theta(f)\left(\sum_{n=0}^{\infty} p^n [a_n]\right) = \sum_{n=0}^{\infty} p^n \widetilde{f}(a_n).$$

As a result, the functor $R \mapsto \overline{R}$ is an equivalence of categories from the category of strict p-rings to the category of p-adically complete $\mathbb{Z}_p$-algebras.

October 4, 2018. Thursday.

Our first goal of today will be to prove 3.14. Before that, we observe that $\Theta(f)$ commutes with multiplication by p (and thus powers of p), because the formula does.

Proof of 3.14. We must show that $\Theta(f)$ is a ring homomorphism, so we must show

$$\Theta(f)([a]) + \Theta(f)([b]) = \Theta(f)([a] + [b]).$$

The rest follows readily.

Since by definition of $\Theta(f)$ we have $\Theta(f)([a]) = \widetilde{f}(a)$, it is equivalent to showing

$$\widetilde{f}(a) + \widetilde{f}(b) \equiv \Theta(f)([a]+[b]) \pmod{p^n} \text{ for all } n.$$

We will do this by induction. For the base $n = 1$, this amounts to the statement

$$f(a) + f(b) \equiv f(a+b) \pmod{p}$$

but this is automatic. For the inductive step, you will see that we will unwrap every notation, apply hypothesis, then wrap everything back up again. Here goes: using the binomial theorem we have that

$$\begin{aligned}\widetilde{f}(a+b) &\equiv (\widetilde{f}(a^{p^{-n}}) + \widetilde{f}(b^{p^{-n}}))^{p^n} \pmod{p^{n+1}}\\ &\equiv \widetilde{f}(a) + \widetilde{f}(b) + \sum_{i=1}^{p^n-1} \binom{p^n}{i} \widetilde{f}(a^{p^{-n}})^{p^n-i} \widetilde{f}(b^{p^{-n}})^i \pmod{p^{n+1}}.\end{aligned}$$

All the binomial coefficients appearing are divisible by p, we can write $1/p$ and still make sense of it:

$$\widetilde{f}(a) + \widetilde{f}(b) \equiv \widetilde{f}(a+b) - p\sum_{i=1}^{p^n-1} \frac{1}{p}\binom{p^n}{i} \widetilde{f}(a^{p^{-n}})^{p^n-i} \widetilde{f}(b^{p^{-n}})^i \pmod{p^{n+1}}.$$

Let's note on the side that in particular, when f is the identity, by definition $\widetilde{f} = [\cdot]$, so

$$[a] + [b] \equiv [a+b] - p\sum_{i=1}^{p^n-1} \frac{1}{p}\binom{p^n}{i} [(a^{p^{-n}})^{p^n-i} (b^{p^{-n}})^i] \pmod{p^{n+1}}. \qquad (\dagger)$$

Finally using the multiplicativity of $\widetilde{f}$, and that $\widetilde{f}(\cdot) = \Theta(f)([\cdot])$, we can write

$$\widetilde{f}(a) + \widetilde{f}(b) \equiv \widetilde{f}(a+b) - p\sum_{i=1}^{p^n-1} \frac{1}{p}\binom{p^n}{i} \Theta(f)([(a^{p^{-n}})^{p^n-i} (b^{p^{-n}})^i]) \pmod{p^{n+1}}. \qquad (*)$$

But on the other hand we know from the inductive hypothesis that $\Theta(f)$ distributes over addition mod p^n, and along with the discussion that $\Theta(f)$ commutes with multiplication by p^{-1}, we know that

$$\sum_{i=1}^{p^n-1} \frac{1}{p}\binom{p^n}{i} \Theta(f)([(a^{p^{-n}})^{p^n-i} (b^{p^{-n}})^i]) \equiv \Theta(f)\left(\sum_{i=1}^{p^n-1} \frac{1}{p}\binom{p^n}{i} [(a^{p^{-n}})^{p^n-i} (b^{p^{-n}})^i]\right) \pmod{p^n}.$$

Thus modulo p^{n+1} from $(*)$ we have

$$\widetilde{f}(a) + \widetilde{f}(b) \equiv \widetilde{f}(a+b) - p\Theta(f)\left(\sum_{i=1}^{p^n-1} \frac{1}{p}\binom{p^n}{i} [(a^{p^{-n}})^{p^n-i} (b^{p^{-n}})^i]\right) \pmod{p^{n+1}}.$$

But since $\Theta(f)$ is defined on each p-adic coordinate, we can factor out $\Theta(f)$ on the right hand side:

$$\widetilde{f}(a) + \widetilde{f}(b) \equiv \Theta(f)\left([a+b] - p\sum_{i=1}^{p^n-1} \frac{1}{p}\binom{p^n}{i} [(a^{p^{-n}})^{p^n-i} (b^{p^{-n}})^i]\right) \pmod{p^{n+1}}.$$

Finally from (†) and using the fact that $\Theta(f)$ is defined on p-adic coordinates, we have

$$\begin{aligned}\widetilde{f}(a)+\widetilde{f}(b) &\equiv \Theta(f)\left([a+b]-p\sum_{i=1}^{p^n-1}\frac{1}{p}\binom{p^n}{i}[(a^{p^{-n}})^{p^n-i}(b^{p^{-n}})^i]\right)\\ &\equiv \Theta(f)([a]+[b]) \pmod{p^{n+1}}\end{aligned}$$

which completes the proof. □

We have said that this theorem makes strict p-rings very rigid if they exist. For example, as a consequence, we have

Proposition 3.15. *There is at most one strict p-ring R up to unique isomorphism with $R/(p)=\overline{R}$.*

Proof. If R_1, R_2 are two strict p-rings with $R_1/p = R_2/p = \overline{R}$, then theorem says identity $\overline{R}\to\overline{R}$ lifts uniquely to isomorphisms $\Theta_1(id): R_1\to R_2$ and $\Theta_2(id): R_2\to R_1$ which are inverses of each other. □

Remarks:

(a) This is interconnected with unramified extensions: one family of examples of strict p-rings are $\mathcal{O}_K$ where K is a complete p-adic valuation field with perfect residue field and in which p is a uniformizer. So the above is another way of saying there can only be one unramified field extension of $\mathbb{Q}_p$ lifting a finite residue field.

(b) If R is a strict p-ring, there is also the Frobenius map Frob on R/pR, which is an isomorphism. By the description of $\Theta(\text{Frob})$, Frob lifts to an isomorphism on R too.

Now that we have answer the question about uniqueness of strict p-rings, naturally we will want to construct strict p-rings. This is where Witt vectors come in.

Let A be a ring. First we define $W_n(A) := A^n$ for any n. Then for any n, we define the ghost map $\mathrm{gh}: W_n(A) = A^n \to A^n$ where

$$\mathrm{gh}:\quad (a_0,\dots,a_{n-1})\mapsto (a_0,\quad a_0^p+pa_1,\quad a_0^{p^2}+pa_1^p+p^2a_2,\quad \dots,\quad \sum_{i=0}^{k}p^ia_i^{p^{k-i}},\quad \dots)$$

Observe that

(a) If p is invertible in A, then gh is a bijection, for we can find the preimage sequentially.

(b) If A is p-torsion free, then gh is injective, for a similar reason as above.

The following characterizes the image of the ghost map under some conditions.

Lemma 3.16 (Dwork)**.** *Suppose that*

(a) *A is p-torsion free, and*

(b) *A admits a ring homomorphism $\phi: A\to A$ that lifts Frobenius, ie. $\phi(a)\equiv a^p \pmod p$ for all $a\in A$.*

Then $(b_0,\dots,b_{n-1})\in A^n$ is in $\mathrm{Im}(\mathrm{gh}) = \mathrm{gh}(W_n(A))$ iff for all i, $\phi(b_{i-1})\equiv b_i \pmod{p^i}$.

Proof. First note that $\phi(1)=1$, so $\phi(p^j)=p^j$ for any p-power. The proof uses 3.12 that if $x,y\in A$, and $x\equiv y \pmod{p^n}$, then $x^p\equiv y^p \pmod{p^{n+1}}$ (one can easily check the $\mathbb{Z}_p$-algebra condition in 3.12 can be dropped). Suppose first that $(b_0, \dots, b_{n-1}) = \mathrm{gh}(a_0, \dots, a_{n-1})$. Then

$$b_{i-1} = \sum_{j=0}^{i-1} p^j a_j^{p^{i-1-j}}.$$

Hit ϕ to it. Since $\phi(a_j) \equiv a_j^p \pmod p$, raising to the p power repeatedly will give $\phi(a_j)^{p^{i-1-j}} \equiv a_j^{p^{i-j}}$ $\pmod{p^{i-j}}$, or equivalently $p^j \phi(a_j)^{p^{i-1-j}} \equiv p^j a_j^{p^{i-j}} \pmod{p^i}$ (call this computation (†)). With this,

$$\phi(b_{i-1}) = \sum_{j=0}^{i-1} p^j \phi(a_j)^{p^{i-1-j}} \equiv \sum_{j=0}^{i} p^j a_j^{p^{i-j}} = b_i \pmod{p^i}.$$

For the other direction, suppose $(b_0, \dots, b_{n-1}) \in A^n$ is such that $\phi(b_{i-1}) \equiv b_i \pmod{p^i}$. We will solve this inductively. Base case is obvious – simply write $a_0 = b_0$; suppose we have already found $a_0, \dots, a_{i-1}$ such that

$$b_{i-1} = \sum_{j=0}^{i-1} p^j a_j^{p^{i-1-j}},$$

Then the hypothesis $\phi(b_{i-1}) \equiv b_i \pmod{p^i}$ gives

$$0 \equiv b_i - \phi(b_{i-1}) = b_i - \sum_{j=0}^{i-1} p^j \phi(a_j)^{p^{i-1-j}} \equiv b_i - \sum_{j=0}^{i} p^j a_j^{p^{i-j}} \pmod{p^i} \quad \text{(by †)},$$

so one can find a_i with $b_i - \sum_{j=0}^{i} p^j a_j^{p^{i-j}} = p^i a_i$. □

As a consequence, under the same hypothesis on A as in 3.16, $\mathrm{gh}(W_n(A)) \subseteq A^n$ is a subring. Since gh under this assumption is an injection, given

$$\mathrm{gh}(r_0, \dots, r_{n-1}) = \boldsymbol{b} := (b_0, \dots, b_{n-1}) \text{ and}$$
$$\mathrm{gh}(s_0, \dots, s_{n-1}) = \boldsymbol{c} := (c_0, \dots, c_{n-1}),$$

we can ask: what are $\mathrm{gh}^{-1}(\boldsymbol{bc})$ and $\mathrm{gh}^{-1}(\boldsymbol{b} + \boldsymbol{c})$ explicitly?

October 10, 2018. Wednesday.

Let A be a ring. We write $W_n(A) = A^n$. We defined the ghost map $\mathrm{gh} : W_n(A) \to A^n$. We showed that under the hypotheses that

(a) A has no p-torsion, and
(b) A admits a Frobenius lift,

then $\mathrm{gh}(W_n(A))$ is a subring in A^n. (If p is invertible, then gh is surjective, and condition is vacuous, concurs with previous observation.)

We apply this to the polynomial ring $A = \mathbb{Z}[T_0, \dots, T_n, U_0, \dots, U_{n-1}]$ with $2n$ variables, where $\phi : T_i \mapsto T_i^p, U_i \mapsto U_i^p$. Then what is

$$\mathrm{gh}(T_0, \dots, T_{n-1}) + \mathrm{gh}(U_0 + \dots, U_{n-1})?$$

One can show that it's $\mathrm{gh}(P_0, \dots, P_{n-1})$ where $P_j \in A$, and similarly for their product $\mathrm{gh}(\boldsymbol{T})\,\mathrm{gh}((U)) = \mathrm{gh}(Q_0, \dots, Q_{n-1})$ where $Q_j \in A$.

Let B be any ring, and two tuples $\boldsymbol{a} = (a_0, \ldots, a_{n-1}), \boldsymbol{a'} = (a'_0, \ldots, a'_{n-1}) \in W_n(B)$, there is a unique homomorphism

$$\phi_{\boldsymbol{a},\boldsymbol{a'}} : A \mapsto B, \boldsymbol{T} \mapsto \boldsymbol{a}, \boldsymbol{U} \mapsto \boldsymbol{a'}.$$

We also have (diagram)

By construction diagram commutes (whole cube commutes). ghost map on the bottom are likely to be zero? top face commutes, varying a, a' and check all of them. So A is the universal ring with $2n$ tuples. Same diagram holds for Q_i multiplications.

We obtain two binary operations, $(P_0, \ldots, P_{n-1})$ and $(Q_0, \ldots, Q_{n-1})$, on $W_n(B) \times W_n(B) \to W_n(B)$. Claim: these give rise to ring structure on $W_n(B)$ with additive identity $(0, \ldots, 0)$ and multiplicative identity $(1, 0, \ldots, 0)$. (can check all these simply on universal ring of 3 tuples.

Claim: $P_0(\boldsymbol{a}, \boldsymbol{a'}) = \boldsymbol{a} + \boldsymbol{a'}$. take $\boldsymbol{a}$ and $\boldsymbol{a'}$, take ghost coordinates, then $\mathrm{gh}(\boldsymbol{a}) + \mathrm{gh}(\boldsymbol{a'})$. compare

$$(a_0 + a'_0, ?, \ldots) \xrightarrow{\mathrm{gh}} (a_0 + a'_0, a_0^p + {a_0'}^p + p(a_0 + a'_0), \ldots)$$

So for P_1, need

$$P_1 = \frac{1}{p}(a_0^p + {a_0'}^p - (a_0 + a'_0)^p) + a_1 + a'_1$$

and this really lives in $\mathbb{Z}[\boldsymbol{a}, \boldsymbol{a'}]$ by binomial formula! (so can divide by p).

Note: P_j, Q_j only depend on $U_0, \ldots, U_j, T_0, \ldots, T_j$. ie. the restriction maps $R : W_n(A) \to W_{n-1}(A)$ is a ring homomorphism.

When A is a commutative ring, then we write $W(A) = \varprojlim_R W_n(A)$. This is the ring of **Witt vectors** with coefficients in A. $W_n(A)$ is an n-truncated ring of Witt vectors.

Proposition 3.17. *There are two natural (natural in A or functorial in A) group homomorphisms $V : W_{n-1}(A) \to W_n(A)$, and $F : W_n(A) \to W_{n-1}(A)$, with the following properties:*

(a) *functorial in A*
(b) *F is a ring homomorphism*
(c) $FV = [p] : W_{n-1}(A) \to W_{n-1}(A)$
(d) *$V(F(y)z) = yV(z)$ for $y \in W_n(A), z \in W_{n-1}(A)$ (V not a ring homomorphism)*
(e) *In ghost coordinates we have a diagram.*

Proof. First use (e) to prove when A is p-torsion free, and with a frob lift, (check images of F, V as in e satisfies Dwork's condition). // Apply Dwork's lemma in universal situation. Then (a) to (d) can be checked from diagram. $V(1)$ is a canonical third element, generates kernel of $W_n(A) \to A$ (think?). □

Note: if A has char p, then $F : W_n(A) \to W_{n-1}(A)$ sends $(a_0, \ldots, a_{n-1}) \mapsto (a_0^p, \ldots, a_{n-1}^p)$. This comes down to checking when A is p-torsion free

$$\mathrm{gh}(F(a_0, \ldots, a_{n-1})) \text{ compare with } \mathrm{gh}(a_0^p, \ldots, a_{n-1}^p) \pmod p.$$

LHS is $(a_0^p + pa, a_0^{p^2} + pa_1^p + p^2 a_2, \ldots)$, and RHS is $(a_0^p, a_0^{p^2} + pa_1^p, \ldots)$. apply ghost inverse to LHS and check it matches mod p (ghost inverse makes sense if A is p-torison free....

V is easier: $\mathrm{gh} \circ V$ gives $(0, pa_0, p(a_0^p + pa_1), \ldots)$ which is the ghost of $(0, a_0, \ldots, a_{n-2})$. So define V have image this.

So if A has char p, then $VF = FV = p : W_n(A) \mapsto W_n(A), (a_0, \ldots, a_{n-1}) \mapsto (0, a_0^p, \ldots, a_{n-1}^p)$.

October 11, 2018. Thursday.

Last time we defined the maps F, V between $W_n(A)$ and $W_{n-1}(A)$, where we recall V is the right shift operator in natural coordinates (in $W_n(A)$):

$$V(a_0, \ldots, a_{n-2}) = (0, a_0 \ldots, a_{n-2}).$$

We then had $FV = p$, and by definition

$$F(a_0, \ldots, a_{n-1}) \equiv (a_0^p, \ldots, a_{n-2}^p) \pmod p.$$

There's a subtlety here – (mod p) is not the natural reduction! But rather it means that the ghost coordinates[30] of the two terms above differ by an element in $p \operatorname{Im} \mathrm{gh}$; see below. To prove this, one can simply check this when A satisfies the hypothesis of Dwork's lemma 3.16 (since we have a universal object $(\mathbb{Z}[T_0, \ldots, T_n], \phi : T_i \mapsto T_j^p)$), and this aaounts to seeing that

$$\mathrm{gh}(F(a_0, \ldots, a_{n-1})) \equiv \mathrm{gh}(a_0^p, \ldots, a_{n-2}^p) \pmod{p \operatorname{Im} \mathrm{gh}}.$$

We will leave this for the reader. But when A has characteristic p, we can say something nice, that we know explicitly what F is, because the phrase $\pmod p$ becomes vacuous. Using $FV = p$ we then also know what multiplication-by-p-map is:

$$p(a_0, \ldots, a_{n-1}) = FV(a_0, \ldots, a_{n-1}) = F(0, a_0, \ldots, a_{n-1}) = (0, a_0^p, \ldots, a_{n-2}^p).$$

In particular, we make a note that

(a) Even if A has characteristic p, $pW_n(A) \neq 0$.
(b) In this case, we also see that $V(a) = VF(F^{-1}(a)) = p(F^{-1}(a)) = \sum [a_n^{p^{-1}}] p^{n+1}$.

Next we define $W(A) = \varprojlim W_n(A)$, where the maps in the inverse limit are given by truncation. The kernel of $W(A) \to W_n(A)$ is then given by

$$\ker(W(A) \to W_n(A)) = V^n(W(A)) = \{(0, 0, \ldots, 0, a_n, a_{n+1}, \ldots)\}.$$

So we can abuse the terminology and say that W is complete with respect to the V-adic topology. However this is not an honest I-adic topology: for example $V(W(A)) \cdot V(W(A)) \not\subseteq V^2(W(A))$.

However, if $A = \overline{R}$ is a perfect ring of characteristic p, then F is an isomorphism (because taking p-powers in A is), thus on $W(\overline{R})$ we have

$$V^n(a_0, a_1, \ldots) = p^n(a_0^{p^{-n}}, a_1^{p^{-n}}, \ldots).$$

So $V^n W(\overline{R}) = p^n W(\overline{R})$, and

$$W(\overline{R}) = \varprojlim W(\overline{R}) / p^n W(\overline{R})$$

[30]That is, the images under the ghost maps.

is p-adically complete. In addition, $W(\overline{R})/pW(\overline{R}) = W(\overline{R})/VW(\overline{R}) = \overline{R}$. Finally, $W(\overline{R})$ has no p-torsion – thus we constructed a strict p-ring $W(\overline{R})$ that lifts the modulo-p-quotient $\overline{R}$!

Hence to summarize things: if $\overline{R}$ is a perfect $\mathbb{F}_p$-algebra, and S is a p-adically complete $\mathbb{Z}_p$-algebra, then we have

$$\mathrm{Hom}_{\mathbb{Z}_p\text{–alg}}(W(\overline{R}), S) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{F}_p\text{–alg}}(\overline{R}, S/pS)$$

given by $\phi \mapsto \phi \pmod p$, and it has an inverse $\Theta(f) \leftarrow\!\shortmid f$ where $\widetilde{f} : \overline{R} \to S$ is the unique multiplicative lift of f, as defined previously.

That's all about Witt vectors for now. Let's get back to a perfectoid field.

4. Perfectoid Fields.

Let $K/\mathbb{Q}_p$ be a perfectoid field: recall this means

(a) K is a complete valuation field,
(b) there is $\varpi \in \mathfrak{m}_K$ such that $\varpi^p \mid p$, and
(c) the map $\mathcal{O}_K/\varpi \xrightarrow{\sim} \mathcal{O}_K/\varpi^p$ given by $x \mapsto x^p$ is an isomorphism.

We defined $\mathcal{O}_{K^\flat} = \varprojlim_{x \mapsto x^p} \mathcal{O}_K/p$. This is by construction a perfect $\mathbb{F}_p$-algebra (so far we didn't use anything about K being a perfectoid field). Now we define

$$A_{\mathrm{inf}}(K) = A_{\mathrm{inf}} := W(\mathcal{O}_{K^\flat}).$$

This is a strict p-ring with modulo-p-quotient $\mathcal{O}_{K^\flat}$. An element in A_{inf} is a sequence $(\bar{x}_0, \bar{x}_1, \ldots)$ where each of $\bar{x}_i \in \mathcal{O}_{K^\flat}$ is a sequence $(\bar{x}_i^{(1)}, \bar{x}_i^{(2)}, \ldots)$ with entries in $\mathcal{O}_K/p$. Notice that by construction, there is a canonical map $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p$ where we only remember the first coordinate, namely $(\bar{x}^{(1)}, \bar{x}^{(2)}, \ldots) \to \bar{x}^{(1)}$. By the theory of strict p-rings, this lifts to a map

$$\Theta_K : A_{\mathrm{inf}} \to \mathcal{O}_K \qquad \text{where explicitly } \Theta_K : \sum_{n=0}^{\infty} p^n [x_n] \mapsto \sum_{n=0}^{\infty} p^n x_n^\sharp$$
$$\text{and } x_n^\sharp = \lim_{m \geq n} (x_n^{(m)})^{p^{m-n}}$$

and $x_n^{(m)} \in \mathcal{O}_K$ is a lift of $\bar{x}_n^{(m)} \in \mathcal{O}_K/p$ (this is how we defined $\widetilde{f}$). Note if K is perfectoid, then $\mathcal{O}_K/p \mapsto \mathcal{O}_K/p$ given by $x \mapsto x^p$ is *surjective*. So this means $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p$ is also surjective, and so using our Nakayama's lemma 3.10, Θ_K is also surjective.[31]

Lemma 4.1. *We have a isomorphism of monoids*

$$\varprojlim_{x \mapsto x^p} \mathcal{O}_K \to \varprojlim_{x \mapsto x^p} \mathcal{O}_K/p = \mathcal{O}_{K^\flat}$$

which admits an inverse $x \mapsto (x^\sharp, (x^{p^{-1}})^\sharp, (x^{p^{-2}})^\sharp, \ldots)$.[32]

So we can write $\mathcal{O}_{K^\flat} \xrightarrow{\sim} \varprojlim_{x \mapsto x^p} \mathcal{O}_K$ as multiplicative monoids. From this, we can see $\mathcal{O}_{K^\flat}$ is a domain, so taking the fraction field of it really makes sense.

[31] In fact we can invert all these implications, so K being perfectoid is equivalently to Θ_K being surjective
[32] x here denotes a sequence; $(\cdot)^\sharp$ turns a sequence of $\mathcal{O}_K/p$ entries into an element in $\mathcal{O}_K$.

Next we define a valuation $|\cdot|_\flat : \mathcal{O}_{K^\flat} \to \mathbb{R}_{\geq 0}$, given by $|x|_\flat = |x^\sharp|$. Since $x^\sharp$ is multiplicative, so $|\cdot|_\flat$ is a multiplicative seminorm on $\mathcal{O}_{K^\flat}$. And it's a norm since $|x^\sharp| = 0$ means $x^\sharp = 0$ and $x = 0$.

Proposition 4.2. $(K^\flat, |\cdot|_\flat)$ *is a complete valuation field with valuation ring* $\mathcal{O}_{K^\flat}$.

Proof. First we need to show $|\cdot|_\flat$ is a nonarchimedean norm. But

$$\begin{aligned}|x+y|_\flat = |(x+y)^\sharp| &= \varinjlim |((x^\sharp)^{p^{-n}} + (y^\sharp)^{p^{-n}})^{p^n}| \\ &= \varinjlim |x^\sharp + y^\sharp + \sum \binom{p^n}{i} (x^\sharp)^\alpha (y^\sharp)^\beta| \text{ where } \alpha + \beta = 1.\end{aligned}$$

Note that $|\binom{p^n}{i}| < 1$ if $i \neq 0, p^n$. Now we exploit the nonarchimedean nature of $|\cdot|$.

(a) If $|x^\sharp| = |y^\sharp|$, then $|\binom{p^n}{i}(x^\sharp)^\alpha (y^\sharp)^\beta| < |(x^\sharp)^\alpha (y^\sharp)^\beta| = |x^\sharp| = |y^\sharp|$.
(b) If WLOG $|x^\sharp| < |y^\sharp|$, then $|\binom{p^n}{i}(x^\sharp)^\alpha (y^\sharp)^\beta| < |(x^\sharp)^\alpha (y^\sharp)^\beta| < |y^\sharp| = |x^\sharp + y^\sharp|$.

So in the case (b), then we have $|x+y|_\flat = |(x+y)^\sharp| = |x^\sharp + y^\sharp|$.

Next we check that $\mathcal{O}_{K\flat}$ is the valuation ring. This means $x, y \in \mathcal{O}_{K^\flat}, y \neq 0$ then $x/y \in K^\flat$ and $|x|_\flat \leq |y|_\flat$ iff $x/y \in \mathcal{O}_{K\flat}$. Can check this using monoid structure (using lemma and fact that $\mathcal{O}_K$ is an valuation ring).

Finally we need to show that $\mathcal{O}_{K^\flat}$ is complete – if $\{x_1, \ldots, x_n, \ldots\}$ is such that $|x_i|_\flat \to 0$, then we must show $\sum x_i$ converges in $\mathcal{O}_{K^\flat}$. We can check this term by term in $\mathcal{O}_K/p$. $\square$

We call $(K^\flat, |\cdot|_\flat)$ the **tilt** of $(K, |\cdot|)$.

If $\pi \in \mathcal{O}_{K^\flat}$ is such that $|\pi|_\flat = p^{-1} = |p|$, then $\mathcal{O}_{K^\flat}/\pi \cong \mathcal{O}_K/p$, and so $\mathcal{O}_{K^\flat} = \varprojlim_{x \mapsto x^p} \mathcal{O}_{K^\flat}/\pi$. This pins down the structure of a valuation field on $K^\flat$.

October 15, 2018. Monday.

Let's quickly recall what we have talked about last time. We started with K which a perfectoid field over $\mathbb{Q}_p$. We defined its tilt $\mathcal{O}_{K^\flat} = \varprojlim_{x \mapsto x^p} \mathcal{O}_K/p$. We said that TFAE:

(a) K is perfectoid.
(b) $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p$, given by projection onto first coordinate[33], is surjective.
(c) The lift of the aforementioned map, given by $\Theta_K : A_{\inf}(K) \to \mathcal{O}_K$, is surjective.

We also defined a norm $|\cdot|_\flat : \mathcal{O}_{K^\flat} \to \mathbb{R}_{\geq 0}$. $\mathcal{O}_{K^\flat}$ is a perfect complete valuation ring with respect to this norm. The fact that it is complete can also be seen via the following: we can describe

$$\ker(\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p) = \{x \in \mathcal{O}_{K^\flat} : p \mid x^\sharp\}$$

but $p \mid x^\sharp$ iff $|x^\sharp| \leq p^{-1}$ iff $|x|_\flat \leq p^{-1}$.

By construction of $|\cdot|_\flat$, we have

$$|\mathcal{O}_{K^\flat}| \cap (p^{-1}, 1] = |\mathcal{O}_K| \cap (p^{-1}, 1].$$

[33]This map is the same as taking $\sharp$ and then modulo p, because $\sharp$ is defined to be a multiplicative lift of the map modulo p.

More explicitly, if $x \in \mathcal{O}_{K^\flat}$ is in the left, then $x^\sharp$ is in the right; and if $x \in \mathcal{O}_K$ is in right, then any preimage of $\bar{x}$ via $\mathcal{O}_{K^\flat} \to \mathcal{O}_K/p$ will give the same norm.

Thus $|K^\flat| \cap (p^{-1}, 1] = |K| \cap (p^{-1}, 1]$. Since $K^\flat$ is perfect and K is perfectoid, both $|K|$ and $|K^\flat|_\flat$ are p-divisible (albeit for different reasons), and general principles will imply that the norm groups $|K|$ and $|K^\flat|_\flat$ are equal.

In particular there is an element $\varpi^\flat \in \mathcal{O}_{K^\flat}$ whose norm is p^{-1}. The description of the kernel says that $\varpi^\flat$ generates it, so $\mathcal{O}_{K^\flat}/\varpi^\flat \xrightarrow{\sim} \mathcal{O}_K/p$. This characterizes $\mathcal{O}_{K^\flat}$ because this then says

$$\mathcal{O}_{K^\flat} \xrightarrow{\sim} \varprojlim_{x \mapsto x^p} \mathcal{O}_{K^\flat}/\varpi^\flat.$$

That is, $\mathcal{O}_{K^\flat}$ is the unique complete perfect valuation ring in char p with a distinguished element $\varpi^\flat \in \mathcal{O}_{K^\flat}$, satisfying $|\varpi^\flat|_\flat = p^{-1}$ and admitting a norm compatible isomorphism $\mathcal{O}_{K^\flat}/\varpi^\flat \xrightarrow{\sim} \mathcal{O}_K/p$.

Let's look at two examples. They will be essentially the two only examples that we know (other than that an algebraically closed field is automatically perfectoid, because it contains every p-th root).

The first example is when $K = \mathbb{Q}_p(\zeta_{p^\infty})^\frown$. Then $\mathcal{O}_K = \mathbb{Z}_p[\zeta_{p^\infty}]^\frown$. Since direct limits commute with tensor products, we have

$$\mathcal{O}_K/p = \mathbb{Z}_p[\zeta_{p^\infty}]/p = \varinjlim_n (\mathbb{Z}_p[\zeta_{p^n}]/p) = \mathbb{F}_p[U_1, U_2, \ldots]/((U_1^p - 1)/(U_1 - 1), U_n^p = U_{n-1}).$$

Since U_1 is essentially ζ_p, and $(\zeta_p - 1)^{p-1} = p$, [34] thus we have $|U_1 - 1| = p^{-1/(p-1)}$. But now consider

$$\mathbb{F}_p[T^{p^{-\infty}}] \to \mathcal{O}_K/p \text{ where we send } T \mapsto U_1 - 1.$$

Then T^{p-1} generates the kernel, so in $\mathbb{F}_p[T^{p^{-\infty}}]^\frown$, once we declare $|T| = p^{-1/(p-1)}$ and $\varpi^\flat = T^{p-1}$, then according to our previous characterization we see that $\mathcal{O}_{K^\flat} = \mathbb{F}_p[T^{p^{-\infty}}]^\frown$.

As an exercise, one can work out what $(T^{p-1} + 1)^\sharp$ is. [35]

The other example is the following slight generalization. Take E to be a complete discrete valuation field over $\mathbb{Q}_p$, and pick a uniformizer π (of $\mathcal{O}_E$). Fix an algebraic closure $\overline{E}$. Fix $\{\pi_n\}_{n \geq 0}$, where $\pi_n^p = \pi_{n-1}$ and $\pi_0 = \pi$. Set $K = E(\{\pi_n\}_{n \geq 1})^\frown = E(\pi_n)$. Note that $K_n = E(\{\pi_i\}_{1 \leq i \leq n})$ is obtained by adjoining the polynomial $q_n(T) = T^{p^n} - \pi \in \mathcal{O}_E[T]$ which is Eisenstein. Hence

$$\mathcal{O}_{K_n} = \mathcal{O}_E[\pi_n] = \mathcal{O}_E[T]/(q_n(T)).$$

[34] Writer's note: In characteristic p this is of course 0, but the way I understood it is that to get the correct valuation, one should still think of this as p. Since we took modulo p to get $\mathbb{F}_p$, the polynomial $(U_1^p - 1)/(U_1 - 1)$ gets a bit funky – as functions on $\mathbb{F}_p$ it's the same as $(U_1 - 1)^{p-1}$ say.

[35] I have yet to complete this.

This then says that $\mathcal{O}_K = \varinjlim_n \mathcal{O}_E[\pi_n]^\frown = \varinjlim_n \mathcal{O}_E[T]/(q_n(T))$ so if we write $k = \mathcal{O}_E/\pi$, then

$$\mathcal{O}_K/\pi = \varinjlim_{T\mapsto T^p} k[T]/(T^{p^n}) = k[U_0, U_1, \ldots]/(U_0, U_n^p = U_{n-1}).$$

Here we took modulo π instead of p, but they're the same: (?)

(1. checking mod p and mod π is the same using equivalent conditions, and 2. $x \mapsto x^p$ is indeed surjective here). Consider the map

$$k[T^{p^{-\infty}}]^\frown \to \mathcal{O}_K/\pi \text{ where we send } T^{p^{-n}} \mapsto U_n,$$

then $\varpi^\flat := T^e$ generates the kernel, so we can declare $|T| = p^{-1/e}$ and $k[T^{p^{-\infty}}] = K^\flat$.

In general it's hard to decide whether a field is perfectoid, other than using the almost purity theorem (3.6) on already explicitly known cases. We also briefly note here that the tilt operation is not necessarily injective: for example there is a field other than $\mathbb{C}_p$ whose tilt is $\mathbb{C}_p^\flat$.[36]

October 18, 2018. Thursday.

First we prove

Theorem 4.3. *Let $K/\mathbb{Q}_p$ be a perfectoid field. Then K is algebraically closed iff $K^\flat$ is algebraically closed.*

Proof. First we will prove that if $K^\flat$ is algebraically closed, then so is K. Fix a monic $f(T) \in \mathcal{O}_K[T]$ of degree d. We will inductively produce $x_n \in \mathcal{O}_K$ such that

(a) $|f(x_n)| \le p^{-n}$, and
(b) $|x_{n+1} - x_n| \le p^{-n/d}$.

This will suffice, since then $x = \lim x_n$ exists and $f(x) = 0$.

Any $x_0 \in \mathcal{O}_K$ works for $n = 0$. Suppose that we have already produced $x_0, \ldots, x_n$. Consider the auxillary monic polynomial $g(T) = f(T + x_n) \in \mathcal{O}_K[T]$. Write $g(T) = \sum a_i T^i$ where $a_0 = f(x_n)$. We want to produce δ (think of δ as $x_{n+1} - x_n$) with

(a) $|g(\delta)| = |\sum a_i \delta^i| \le p^{-(n+1)}$, and
(b) $|\delta| \le p^{-n/d}$.

If $a_0 = f(x_n) = 0$, then x_n is already a root, so we are already home. So let's suppose $a_0 \ne 0$. It then suffices to find δ with $|\sum (a_i/a_0)\delta^i| \le p^{-1}$.[37] Hence let's consider $\sum (a_i/a_0) T^i \in K[T]$.

First pick $c \in K$ such that $|c| = \min_{i>0}\{|a_0/a_i|^{1/i}\}$. In particular, $|c| \le |a_0|^{1/d} \le p^{-n/d}$. By choice of c, we have $|a_i/a_0||c^i| \le 1$ for all i (and equality holds for a specific i). We next consider the modified polynomial

$$h(T) = \sum \frac{a_i}{a_0} c^i T^i \in \mathcal{O}_K[T].$$

[36] Writer's note: Keerthi mentioned that a prerequisite for the functor $K \mapsto K^\flat$ to be injective is when K is spherically closed, but I have no idea what this means.

[37] Morally speaking this is quite natural, since $\mathcal{O}_K/p$ is the only link between $K^\flat$ and K; and $\mathcal{O}_K/p$ only detects whether an element α has norm $|\alpha| \le p^{-1}$ or not, or equivalently whether $\alpha \in \mathcal{O}_K$ is trivial in $\mathcal{O}_K/p$ or not.

It's now sufficient to find $u \in \mathcal{O}_K^\times$ such that $|h(u)| \leq p^{-1}$, for then $|cu| = |c| \leq p^{-n/d}$ and we can take $\delta = cu$. To do this, we choose $\widetilde{h}(T) \in \mathcal{O}_{K^\flat}[T]$ of degree d such that $\widetilde{h}(T)$ reduces to $h(T)$ (mod p) in $(\mathcal{O}_K/p)[T] = (\mathcal{O}_{K^\flat}/\varpi)[T]$. It is then enough to show that $\widetilde{h}(T)$ has a root $u^\flat \in \mathcal{O}_{K^\flat}^\times$, for then we can take $u = \overline{(u^\flat)^\sharp}$.

There is a nice gadget to determine the norm of roots – Newton polygons. More explicitly, for $\widetilde{h} = \sum b_i T^i \in \mathcal{O}_{K^\flat}[T]$, define the Newton polygon $\mathrm{NP}(\widetilde{h})$ to be the convex hull of the points $\{(i, -\log_p |b_i|_\flat)\}$. The theory of Newton polygons asserts that the negative slopes of $\mathrm{NP}(\widetilde{h})$ are the set of valuations of the roots of $\widetilde{h}$ (one would have been more careful with what "roots" mean if $K^\flat$ is not algebraically closed). Using this, if there are two points on $\mathrm{NP}(\widetilde{h})$ with y-coordinates zero, then there is a segment of slope zero, so we are done. It now remains to show that this is indeed the case.

Indeed, first observe that when $i = 0$, $h(T)$ has coefficient 1, so this already provides one of such points. Furthermore, we chose c such that we can still have coefficient 1 for some $i > 0$.

The other direction of the theorem can be proved similarly. This concludes the proof. □

Next we'll prove the Almost Purity theorem (3.6). Let's restate the theorem more generally.

Theorem 4.4. *$\{\widetilde{L}/K^\flat$ finite$\} \to \{L/K$ finite$\}$, where $\widetilde{L} \mapsto W(\mathcal{O}_{\widetilde{L}}) \otimes_{W(\mathcal{O}_{K^\flat})} K$ (note finite of perfect is perfect). There is another functor $\{L/K$ finite perfectoid$\} \to \{\widetilde{L}/K^\flat$ finite$\}$ by $L \mapsto L^\flat$. These are all equivalence of categories and are well defined.*

Proof. First consider $W(\mathcal{O}_{\widetilde{L}}) \otimes_{W(\mathcal{O}_{K^\flat})} \mathcal{O}_K$. Note $\mathcal{O}_K = W(\mathcal{O}_{K^\flat})/\ker \Theta_K$. So the tensor product is just $W(\mathcal{O}_{\widetilde{L}})/\ker(\Theta_K) \cdot W(\mathcal{O}_{\widetilde{L}})$.

Let F be any perfectoid field over $\mathbb{F}_p$, then define $z \in W(\mathcal{O}_F)$ to be primitive if $z = [z_0] + pw$ where $|z_0| = p^{-1}$ and $w \in W(\mathcal{O}_F)^\times$. Latter is equivalent to saying $w = \sum p^i [w_i]$ where $w_0 \in \mathcal{O}_F^\times$.

EG if $F = K^\flat$, Θ_K is surjective, There is $\varpi \in \mathcal{O}_{K^\flat}$ such that $|\varpi|_\flat = p^{-1}$. Then $\varpi^\sharp = \phi_K([\varpi]) \in \mathcal{O}_K$, and $\varpi^\sharp = up$ where $u \in \mathcal{O}_K^\times$. There is $w \in W(\mathcal{O}_K)^\times$ such that $\Theta_K(w) = u^{-1}$. Then $\Theta_K(w[\varpi]) = p$, and $\Theta_K(w[\varpi] - p) = 0$, so $\Theta_K([\varpi] - pw^{-1}) = 0$. Then $z = [\varpi] - pw^{-1}$ is a primitive element in $\ker \Theta_K$.

Real example: $K = \mathbb{Q}_p(p^{1/p^\infty})$. Then $\mathfrak{p} = (p, p^{1/p}, \ldots) \in \varprojlim_{x \mapsto x^p} \mathcal{O}_K = \mathcal{O}_{K^\flat}$. Then $[\mathfrak{p}] - p$ is in $\ker \Theta_K$ and is primitive.

Real lemma: this primitive element generates the kernel of Θ_K. Rephrase: Suppose $z \in W(\mathcal{O}_F)$ is primitive, then $\mathcal{O}_z = W(\mathcal{O}_F)/z$, then $\mathcal{O}_z$ is a complete valuation ring with fraction field K_z perfectoid, and $K_z^\flat \xrightarrow{\sim} F$ canonically. (in some sense untilt)

October 22, 2018. Monday.

Let F be a perfectoid field of characteristic p.

Let $z \in W(\mathcal{O}_F)$. We said z is primitive if $z = [z_0] + pw$ where $|z_0|_F = p^{-1}$ [38] and w satisfies any

[38] $|\cdot|_F$ is the norm on F.

of the following equivalent conditions:

(a) $w \in W(\mathcal{O}_F)^\times$.
(b) $[w_0] \in \mathcal{O}_F^\times$.
(c) $|w_0|_F = 1$.

$[z_0]$ is the zero-th *Teichmüller coefficient.*

Now we also define $u \in W(\mathcal{O}_F)$ to be **stable** if $u = [u_0]w$ where $u_0 \in \mathcal{O}_F$ and $w \in W(\mathcal{O}_F)^\times$. In verbal terms, u is a Teichmüller lift up to a unit.

Proposition 4.5. *Let z be primitive.*

(a) *Every nonzero coset in $W(\mathcal{O}_F)/(z)$ has a stable representative.*
(b) *If $x, y \in W(\mathcal{O}_F)$ are stable with $x \equiv y \pmod z$, then $|x_0|_F = |y_0|_F$.* [39]
(c) *If $x \in W(\mathcal{O}_F)$ is stable, then $x \notin (z)$.*

We shall omit the proof for now (see next lecture), and focus on the following

Theorem 4.6. *$K_z := (W(\mathcal{O}_F)/(z))[p^{-1}]$ is a perfectoid field with ring of integers $\mathcal{O}_z := W(\mathcal{O}_F)/(z)$, and we have a canonical isomorphism $K_z^\flat \xrightarrow{\sim} F$.*

Proof. We shall assume 4.5. First observe that $\mathcal{O}_z$ is a domain: product of stable elements can easily be seen to be a stable element via the definition (which invokes the multiplicativity of the Teichmüller lift); and since $W(\mathcal{O}_F)$ is a domain, product of nonzero stable elements is a nonzero stable element.

Next we have to define a norm on $\mathcal{O}_z$: which we do so by considering $|\cdot|_z : \mathcal{O}_z \to \mathbb{R}_{\geq 0}$ where $|\overline{x}|_z := |x_0|_F$ where $x \in W(\mathcal{O}_F)$ is any stable lift of $\overline{x}$. This is well-defined by 4.5. [40]

This extends to a multiplicative non-archimedean norm on K_z such that $\mathcal{O}_z$ is the valuation ring:

(a) For multiplicativity: we have $|\overline{x}\overline{y}|_z = |x_0y_0|_F = |x_0|_F|y_0|_F = |\overline{x}|_z|\overline{y}|_z$.
(b) For non-archimedeanness: Postponed to next lecture.
(c) For $\mathcal{O}_z$ being the valuation ring: we must show that $|\overline{x}|_z \leq |\overline{y}|_z$ implies $\overline{y} \mid \overline{x}$. Indeed, if $|\overline{y}|_z \geq |\overline{x}|_z$, then $|y_0|_F \geq |x_0|_F$, and $y_0 \mid x_0$, so $[y_0]v \mid [x_0]u$ (if $x = [x_0]u, y = [y_0]v$ are stable lifts of $\bar{x}, \bar{y}$ respectively, so in particular u, v are units in $W(\mathcal{O}_F)$), and finally $\bar{y} \mid \bar{x}$.

In K_z, we inverted p and p^{-1} is a element with negative valuation, so K_z is indeed a field.

Finally we must show that $\mathcal{O}_z$ is complete and K_z is perfectoid with tilt F:

(a) $\mathcal{O}_z$ is complete: we postpone the proof till next lecture, and will assume this for what follows.
(b) K_z is perfectoid with tilt F: We have $\mathcal{O}_z/p = W(\mathcal{O}_F)/(p,z)$. But $z = [z_0] + pw$, so $\mathcal{O}_z/p \xrightarrow{\sim} \mathcal{O}_F/z_0$. Since $|z_0|_F = p^{-1}$ by definition of primitive elements, this isomorphism is norm compatible (assuming $|p|_z = p^{-1}$), so by the characterization of perfectoid fields, K_z is perfectoid with tilt F.

[39] In particular, if $x = [x_0]w = [x_0']v$, then $|x_0|_F = |x_0'|_F$.

[40] Here's how one can think about x_0 using an analogy. Treat $W(\mathcal{O}_F) \sim \mathcal{O}_F[[T]]$, and $z \sim p - T$. Then every coset of $\mathcal{O}_F[[T]]/(p-T)$ has a constant representative f_0 given by evaluation $f \in \mathcal{O}_F[[T]]$ at $T = p$. In our situation, we pick this corresponding f_0, namely x_0.

This completes the proof. $\square$

Before we prove 4.5, we have to set up a technical gadget called Gauss norms. For a more general theory, see 5.1.

Given $a := \sum_{n=0}^{\infty}[a_n]p^n \in W(\mathcal{O}_F)$, we define the **Gauss norm** of a to be $|a|_1 = \sup_{n\geq 0}|a_n|_F$. Verbally, the Gauss norm is the supremum of the norm of the Teichmüller coefficients.

Lemma 4.7. *$|\cdot|_1$ is a multiplicative non-archimedean norm on $W(\mathcal{O}_F)$.* [41]

Proof. For a nonnegative integer k, we define $N_k(a) = \max_{n\leq k}|a_n|$. Notice that $|a|_1 = \lim_k N_k(a)$. It suffices show for $x, y \in W(\mathcal{O}_F)$, we have

(a) $N_k(x+y) \leq \max\{N_k(x), N_k(y)\}$,
(b) $N_k(xy) \leq N_k(x)N_k(y)$ (so (a),(b) says N_k is a submultiplicative seminorm), and
(c) $N_k(x)N_l(y) \leq N_{k+l}(xy)$.

Note the obvious observation that $x \in W(\mathcal{O}_F)$ then $N_k(x) \leq |\varpi|_F$ for some $\varpi \in \mathcal{O}_F$, or equivalently $x \pmod{p^{k+1}W(\mathcal{O}_F)} \in [\varpi](W(\mathcal{O}_F)/p^{k+1})$.

If $N_k(x) = |\varpi_1|_F$ and $N_k(y) = |\varpi_2|_F$, then

$$\begin{cases} x \pmod{p^{k+1}} \in [\varpi_1]W(\mathcal{O}_F)/p^{k+1} \\ y \pmod{p^{k+1}} \in [\varpi_2]W(\mathcal{O}_F)/p^{k+1} \end{cases} \Rightarrow x+y \pmod{p^{k+1}} \in ([\varpi_1],[\varpi_2])W(\mathcal{O}_F)/p^{k+1}$$

which is $[\varpi_i]W(\mathcal{O}_F)/p^{k+1}$ where $|\varpi_i|_F = \max_{j=1,2}|\varpi_j|_F$. So $N_k(x+y) \leq \max\{N_k(x), N_k(y)\}$.

$N_k(xy) \leq N_k(x)N_k(y)$ is proved similarly: $xy \pmod{p^{k+1}} \in [\varpi_1][\varpi_2]W(\mathcal{O}_F)/(p^{k+1})$. For a more explicit explanation, see **??**.

Finally for (c), if $N_k(x) = |x_r|_F$ where $r \leq k$ and $N_l(s) = |y_s|_F$ for some $s \leq l$, where WLOG r, s is smallest such, then

$$\begin{cases} x = [x_0] + p[x_1] + \cdots + p^r[x_r] + p^{r+1}(\text{other terms}) \\ y = [y_0] + p[y_1] + \cdots + p^s[y_s] + p^{s+1}(\text{other terms}) \end{cases} \Rightarrow xy = \cdots + p^{r+s}[x_r y_s] + \cdots.$$

In addition, by our choice of r and s, in the $(r+s)$-th Teichmüller coordinate, $[x_r y_s]$ has the greatest term and the unique such. Hence $N_{k+l}(xy) \geq N_k(x)N_l(y)$ as desired. $\square$

October 24, 2018. Wednesday.

Let's briefly recap what we have done last lecture. We had a proposition (4.5) as follows: let $z \in W(\mathcal{O}_F)$ be a primitive element. Then

(a) Every coset in $W(\mathcal{O}_F)/(z)$ has a stable representative w (where stable means that $w = [x]u$ for some $x \in \mathcal{O}_F$ and $u \in W(\mathcal{O}_F)^{\times}$).
(b) If $x, y \in W(\mathcal{O}_F)$ is stable with $x \equiv y \pmod{z}$, then $|x_0|_F = |y_0|_F$.

[41] This is the equivalent of Gauss's Lemma, which states that over $\mathbb{Z}$, the product of two primitive polynomials is again primitive.

(c) No nonzero multiple of z is stable.

To prove this, we developed the Gauss norm: for $a = \sum[a_n]p^n \in W(\mathcal{O}_F)$, we defined the Gauss norm to be $|a|_1 := \sup|a_n|_F \leq 1$. We saw that this is a nonarchimedean multiplicative norm on $W(\mathcal{O}_F)$.

Now we will give a proof to the 4.5. We make three observations:

(a) $x \in W(\mathcal{O}_F)$ is stable iff $|x|_1 = |x_0|_F$.

Proof. x is stable iff x can be written as $x = [x_0] + [x_0x_1']p + [x_0x_2']p^2 + \cdots$. □

(b) If $u \in W(\mathcal{O}_F)^\times$ (equivalently $u_0 = \mathcal{O}_F^\times$) then $|u|_1 = |u_0|_F = 1$.

Proof. The equivalence is clear. $u_0 \in \mathcal{O}_F^\times$ hence $|u|_1 = |u_0|_F = 1$. □

(c) If z is primitive, then $|z|_1 = 1$.

Proof. Use part (b). □

Now we are ready to prove 4.5.

Proposition (Restatement of 4.5)**.** *Let z be primitive.*

(a) *Every nonzero coset in $W(\mathcal{O}_F)/(z)$ has a stable representative.*
(b) *If $x, y \in W(\mathcal{O}_F)$ are stable with $x \equiv y \pmod z$, then $|x_0|_F = |y_0|_F$.* [42]
(c) *If $x \in W(\mathcal{O}_F)$ is stable, then $x \notin (z)$.*

Proof of 4.5. By assumption z is primitive. Define the additive operators $S, T : W(\mathcal{O}_F) \to W(\mathcal{O}_F)$ where

$$T(a) = T\left(\sum_{n=0}^{\infty}[a_n]p^n\right) = \sum_{n=0}^{\infty}[a_{n+1}]p^n = p^{-1}(a - [a_0])$$
$$S(a) = a - w^{-1}T(a)z \text{ where we write } z = [z_0] + pw.$$

We obviously have $a \equiv S(a) \pmod z$.

The upshot is this: $S(a)$ is "more" stable – we shall make what this means more precise in the following. We observe that

$$S(a) = \sum[a_n]p^n - (w^{-1}[z_0] + p)\left(\sum[a_{n+1}]p^n\right) = [a_0] - w^{-1}[z_0]T(a).$$

Since z is primitive, $|w|_1 = 1$, and $|z_0|_F = p^{-1}$, hence $|S(a)|_1 \leq \max\{|a_0|_F, p^{-1}|T(a)|_1\}$. In particular, if a is not stable, then $|a|_1$ is not attained by $|a_0|_F$, so $|T(a)|_1 = |a|_1$.

In what follows, we aim to find a stable representation that is in the same coset as a. If a is stable, we are home. So let's assume otherwise. Then a priori $|S(a)|_1 \leq \max\{|a_0|_F, p^{-1}|a|_1\}$.

Case (i). If $|a_0|_F > p^{-1}|a|_1$, then the non-archimedean property says $|S(a)|_1 = |a_0|_F$. Since the zero-th Teichmüller coefficient $S(a)_0 = a_0 - w_0^{-1}z_0a_1$, we also have $|S(a)_0|_F = |a_0|_F = |S(a)|_1$. So $S(a)$ is stable.

[42] In particular, if $x = [x_0]w = [x_0']v$, then $|x_0|_F = |x_0'|_F$.

Case (ii). If $|a_0|_F \le p^{-1}|a|_1$, then $|S(a)|_1 \le p^{-1}|a|_1$. So we keep iterating, and we always stay in the same coset as $a, S(a), \ldots$. In other words, we exhibited a sequence of elements in this coset whose norms tend to zero. This forces us to be in the zero coset in the first place.

In both cases, $|S(a)|_1 \le |a|_1$. Thus we can conclude that, if a is unstable, and b is stable representative of the coset of $a \pmod z$, then $|b|_1 \le |a|_1$. This proves (a), in fact a stronger statement of (a).

Next we prove (c) before (b): Note that if $a \in \Omega(\mathcal{O}_F)$, then $|(az)_0|_F = |a_0|_F|z_0|_F = p^{-1}|a_0|_F$, and $|az|_1 = |a|_1|z|_1 = |a|_1 \ge |a_0|_F > p^{-1}|a_0|_F$. Hence $|(az)_0|_F \ne |az|_1$, and this means az is never stable.

Finally for (b), let's assume that x, y stable with $x \equiv y \pmod z$. Then $|x_0|_F = |y_0|_F$ is equivalently to asking $|x|_1 = |y|_1$. Suppose the otherwise that $|x|_1 > |y|_1$. Then $|x - y|_1 = |x|_1 = |x_0|_F = |x_0 - y_0|_F = |(x-y)_0|_F$. So $x - y$ is stable, but it's a multiple of z, now invoke (c) to yield a contradiction. ☐

Next we fill in the holes of in the proof of 4.6.

Theorem (Restatement of 4.6)**.** *Let $\mathcal{O}_z = W(\mathcal{O}_F)/(z)$ and $K_z = \mathcal{O}_z[p^{-1}]$. Let $|\cdot|_z : \mathcal{O}_z \to \mathbb{R}_{\ge 0}$ be an absolute value where we define $|\bar{x}|_z = |x|_1 = |x_0|_F$, where x is any stable representative for $\bar{x}$. Then*

(a) *$\mathcal{O}_z$ is a complete valuation ring with respect to the norm $|\cdot|_z$,*
(b) *K_z is the fraction field field of $\mathcal{O}_z$,*
(c) *K_z is perfectoid, and*
(d) *K_z has tilt $K_z^\flat$ canonically isomorphic to F.*

Idea: stable rep = rep with least gauss norm.

Proof. It remains to prove that

(a) $|\cdot|_z$ is non-archimedean. This is immediate since it's true for Gauss norms.
(b) $\mathcal{O}_z$ is complete with respect to $|\cdot|_z$.
(c) $|p|_z = p^{-1}$.

Let's first check that $|p|_z = p^{-1}$. Since $z = [z_0] + pw$, we have $p = w^{-1}(z - [z_0])$, so $p \equiv -w^{-1}[z_0] \pmod z$. In addition, $|-w^{-1}[z_0]|_1 = |w_0|_F|z_0|_F = |w_0z_0|_F$ (which is equal to $1 \cdot p^{-1} = p^{-1}$), so $-w^{-1}[z_0]$ is a stable representative for $p \pmod z$. So $|p|_z = |w_0z_0|_F = p^{-1}$.

Next we show (b). To check that $\mathcal{O}_z$ is complete with respect to $|\cdot|_z$, it's enough to check that $W(\mathcal{O}_F)$ is complete with respect to $|\cdot|_1$. Note that the norm topology for $|\cdot|_1$ on $W(\mathcal{O}_F)$ is equivalent to the $[z_0]$-adic topology. Indeed, $|z_0|_F = p^{-1} < 1$, so heuristically small $|\cdot|_1$ is equivalently to saying it's divisible by high powers of $[z_0]$, since $|x|_F < |y|_F$ is equivalent to $y \mid x$. So now we must check that $W(\mathcal{O}_F)$ is $[z_0]$-adically complete. This follows from (1) $W(\mathcal{O}_F)$ is p-adically complete, and (2) $\mathcal{O}_F = W(\mathcal{O}_F)/p$ is z_0-adically complete. This completes the proof. ☐

Let's wrap up. Suppose $K/\mathbb{Q}_p$ is perfectoid and $F := K^\flat$, then we constructed a map $\Theta_K : W(\mathcal{O}_F) \to \mathcal{O}_K$, which is surjective since K is perfectoid. We can construct a primitive element of $W(\mathcal{O}_F)$ as follows: Pick $z_0 \in \mathcal{O}_F$ with $|z_0|_\flat = p^{-1}$. Then by definition of $|\cdot|_\flat$, we have $|z_0^\sharp| =$

$|\Theta_K([z_0])| = |z_0|_\flat = p^{-1}$, and so $|p^{-1}z_0^\sharp| = 1$, $p^{-1}z_0^\sharp \in \mathcal{O}_K^\times$. Now choose by surjectivity $u \in W(\mathcal{O}_F)^\times$ with $\Theta_K(u) = p^{-1}z_0^\sharp$. So $z := [z_0] - pu$ is primitive, and furthermore it satisfies $\Theta_K(z) = \Theta_K([z_0] - pu) = z_0^\sharp - pp^{-1}z_0^\sharp = 0$.

So Θ_K must factor through $W(\mathcal{O}_{K^\flat})/(z)$, giving a composition of maps $W(\mathcal{O}_{K^\flat}) \to W(\mathcal{O}_{K^\flat})/(z) \twoheadrightarrow \mathcal{O}_K$, where the latter is a surjective map of valuation rings, so it's an isomorphism. [43] Hence $\mathcal{O}_K$ is of the form $\mathcal{O}_z$ for a primitive element $z \in W(\mathcal{O}_{K^\flat})$.

> This gives an equivalence of categories:
>
> $$\{\text{Perfectoid fields } K/\mathbb{Q}_p\} \longleftrightarrow \left\{\begin{matrix}\text{Pairs } (F,(z)) \text{ where } F/\mathbb{F}_p \text{ is perfectoid and} \\ (z) \subseteq W(\mathcal{O}_F) \text{ an ideal generated by a primitive element}\end{matrix}\right\}$$
>
> given by $\quad K \mapsto (K^\flat, \ker(\Theta_K)) \quad$ and $\quad (W(\mathcal{O}_F)/(z))[p^{-1}] \mapsfrom (F,(z))$

October 25, 2018. Thursday.

Our goal today will be to prove the Almost Purity Theorem (3.6), which states the following: if K is a perfectoid field, and L/K is finite, then L is perfectoid too. We remark that if $K/\mathbb{F}_p$, this theorem amounts to saying the finite extension of a perfect field is also perfect, which is easy to see. We will assume this in what follows.

Zariski-Nagata: regular scheme, finite flat morphism over it, then there's discriminant associated. In general if $A \to B$ is finite flat, can ask is it etale and unramified? unramifiedness is given by discriminant: there is $\mathrm{Tr}_{B/A} : B \to A$. So this gives a pairing $\langle \cdot, \cdot \rangle : B \times B \to A$ sending $(b_1, b_2) \mapsto \mathrm{Tr}_{B/A}(b_1 b_2)$. Disc is the determinant of this pairing. Disc only determined up to squares (because one can choose basis...) Is it invertible? The locus of when this is invertible is exactly the locus of A which is etale. Locus of etale is pure of codim 1, namely vanishing locus.

Last time we saw there is an equivalence

$$\{\text{Perfectoid fields } K/\mathbb{Q}_p\} \longleftrightarrow \left\{\begin{matrix}\text{Pairs } (F,I) \text{ where } F/\mathbb{F}_p \text{ is perfectoid and} \\ I \subseteq W(\mathcal{O}_F) \text{ an ideal generated by a primitive element}\end{matrix}\right\} \tag{†}$$

given by $\quad K \mapsto (K^\flat, \ker(\Theta_K)) \quad$ and $\quad (W(\mathcal{O}_F)/I)[p^{-1}] \mapsfrom (F,I)$

Let's fix a perfectoid field $K/\mathbb{Q}_p$. We will establish a diagram of categories:

$$\begin{tikzcd}
\{L/K \text{ finite perfectoid}\} \arrow[d, hook] \arrow[drr, squiggly] & & \{\widetilde{L}/K^\flat \text{ finite}\} \arrow[ll, dashed] \\
\{L/K \text{ finite}\} & & \{\widetilde{L}/K^\flat \text{ perfectoid}\}
\end{tikzcd}$$

Evidently we already have the solid injective arrow. Our aim will be to show that this arrow is

[43] The only element that can be mapped to 0, which has norm 0, is 0 itself.

actually an equivalence. We also have the squiggly arrow from (†) for completion, given by $L \mapsto L^\flat$, but of course the hard work lies in showing the other direction, that there is a canonical untilt, and this is what we will use.

First we establish the dashed arrow. Note that if $\widetilde{L}/K^\flat$ is a finite extension, and z is a primitive element in $W(\mathcal{O}_{K^\flat})$, then it's primitive in $W(\mathcal{O}_{\widetilde{L}})$ too.

Lemma 4.8. *Let $\widetilde{L}/K^\flat$ be a finite extension. Then*

$$L := W(\mathcal{O}_{\widetilde{L}})/(\ker \Theta_K)W(\mathcal{O}_{\widetilde{L}})[p^{-1}]$$

is also finite over K with $[L : K] = [\widetilde{L} : K^\flat]$. In addition, if $\widetilde{L}/K^\flat$ is Galois with $\mathrm{Gal}(\widetilde{L}/K^\flat) = G$, then $\mathrm{Gal}(L/K) = G$ too.

Proof. Assume first that $\widetilde{L}/K^\flat$ is Galois with $\mathrm{Gal}(\widetilde{L}/K^\flat) = G$, and $|G| = [\widetilde{L} : K^\flat]$. Then G acts on L coordinate-wise, and it's enough to show that $L^G = K$.

Note that $W(\mathcal{O}_{\widetilde{L}})^G = W(\mathcal{O}_{K^\flat})$, because G acts on the Teichmüller coefficientss entry-by-entry. So if $\ker \Theta_K = (z) \subseteq W(\mathcal{O}_{K^\flat})$, since z is fixed by G, we have $(zW(\mathcal{O}_{\widetilde{L}}))^G = zW(\mathcal{O}_{K^\flat})$. Consider the short exact sequence

$$0 \to zW(\mathcal{O}_{\widetilde{L}})[p^{-1}] \to W(\mathcal{O}_{\widetilde{L}})[p^{-1}] \to L \to 0$$

of $\mathbb{Q}$-vector spaces with a G action. Since G is finite, this allows an averaging process by G, so taking G-invariants is exact, and $K = L^G$. In general, we pass $\widetilde{L}$ to a Galois closure $\widetilde{L}'$, giving the results for $\widetilde{L}'/K$ and $\widetilde{L}/K$, and use the tower law bring us home. ☐

The above gives an equivalence from $B \to A$. Now remains to show $B \to D$ is an equivalence. the map is the composition $B \to A \to D$.

Consider the field

$$K_\infty := (\varinjlim L)\widehat{\ } = (\bigcup L)\widehat{\ } \subseteq \widehat{\overline{K}},$$

where the direct limit and union are over all L/K such that $\widetilde{L}/K^\flat$ that is finite Galois. First we claim that K_∞ is perfectoid. Indeed, $\mathcal{O}_{K_\infty}/p = \varinjlim \mathcal{O}_L/p$, and $x \mapsto x^p$ is surjective on each term on the right, so $x \mapsto x^p$ must still be surjective on the left.

However, $\mathcal{O}_{K_\infty}/p = \varinjlim \mathcal{O}_L/p = \varinjlim \mathcal{O}_{\widetilde{L}}/\varpi = \mathcal{O}_{\overline{K^\flat}}/\varpi$, we have that $K_\infty^\flat = \widehat{\overline{K^\flat}}$. Krasner's Lemma says $\widehat{\overline{K^\flat}}$ is algebraically closed, and this together with K being perfectoid says K is algebraically closed too. So $K_\infty = \widehat{\overline{K}}$. Hence any finite extension of K is contained in an untilt L of a finite Galois extension $\widetilde{L}/K^\flat$.

But once we have this, we are good, because Galois theory covers the rest – intermediate extensions L/K of a Galois extension F/K correspond to subgroups of $\mathrm{Gal}(F/K)$, which is the same as $\mathrm{Gal}(F^\flat/K^\flat)$, and in turn we can find every intermediate extension, one of which is $\widetilde{L}/K^\flat$.

This also firmly establishes tilting and untilting as inverse operators. This result is interesting, in the sense that we never checked $\mathcal{O}_L/p$ has a surjective Frobenius map, we never even figured out what $\mathcal{O}_L$ looks like!

4.1. Module of Differentials.

Let $A \to B$ be a map of commutative rings. This induces a map $B \otimes_A B \to B$ given by $b_1 \otimes b_2 \mapsto b_1 b_2$. Suppose this map has kernel I. We define the **module of differentials** to be $\Omega^1_{B/A} := I/I^2$.

A priori $\Omega^1_{B/A}$ is only a $B \otimes B$-module, but we claim $\Omega^1_{B/A}$ is canonically a B-module: note that $1 \otimes b - b \otimes 1 \in I$. If $\omega \in I/I^2$, then $(1 \otimes b - b \otimes 1)\omega = 0 \in I/I^2$, so $(1 \otimes b)\omega = (b \otimes 1)\omega \in I/I^2$. So we can define the B action on either coordinate.

In fact, as a B-module, $\Omega^1_{B/A}$ is generated by elements of the form $db := 1 \otimes b - b \otimes 1 \in \Omega^1_{B/A}$.

Suppose that $B = A[x_1, \dots, x_r]/(f_1, \dots, f_s)$, then $\Omega^1_{B/A} = (Bdx_1 \oplus \cdots \oplus Bdx_r)/(df_1, \dots, df_s)$. In particular, if $r = s = 1$, $\Omega^1_{B/A} = Bdx/(f'(x)dx)$, and so $\Omega^1_{B/A} = 0$ iff $f'(x) \in B^\times$.

Applying this to the case K be a complete discrete valuation field, and L/K be a finite extension, we know that

$$\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0 \text{ iff } L/K \text{ is unramified.}$$

October 29, 2018. Monday.

Let's make our observation from last time more precise:

Proposition 4.9. *Let K be a complete discrete valuation field over $\mathbb{Q}_p$ and L/K be a finite extension. Then TFAE:*

(a) *L/K is unramified.*
(b) $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$.
(c) *The trace pairing $\mathcal{O}_L \times \mathcal{O}_L \to \mathcal{O}_K$ given by $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is non-degenerate. And as such $\mathcal{O}_L$ can be identified with $\mathcal{O}_L^\vee$ as $\mathcal{O}_K$-modules.*
(d) *$\mathcal{O}_L$ is étale over $\mathcal{O}_K$. We have not formally discussed what this means, but for what matters we can just assume this is the definition in this case.*

In addition if L/K is Galois with Galois group $G = \mathrm{Gal}(L/K)$, then these are also equivalent to

(e) *The map $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \prod_{\gamma \in G} \mathcal{O}_L$ given by $x \otimes y \mapsto (x\gamma(y))_{\gamma \in G}$ is an isomorphism.*

Proof. Omitted or an exercise for readers. This uses the explicit description of $\mathcal{O}_L$ as an $\mathcal{O}_K$-module. Write down a basis of $\mathcal{O}_L$ as an $\mathcal{O}_K$-module. $\square$

(e) says that, given a descent datum with respect to $\mathcal{O}_L/\mathcal{O}_K$ for an $\mathcal{O}_L$-module M, is equivalent to given a G-action on M compatible with G action on $\mathcal{O}_L$. This along with faithfully flat descent, says that in this case, $\mathcal{O}_L \otimes_{\mathcal{O}_K} M^G \xrightarrow{\sim} M$.

Let's move onto the setup where K is perfectoid over $\mathbb{Q}_p$, and L/K is finite. Since in this case K is not discrete, we cannot use 4.9 at all, but let's dissect and see what we can say about it.

Theorem 4.10. *We have $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$.*

Proof. Since L/K is finite, we can choose a primitive $\alpha \in \mathcal{O}_L$ such that $L = K(\alpha)$. Write $x = m'_\alpha(\alpha)$. Since we $\mathcal{O}_K[\alpha]$ is finitely presented as an $\mathcal{O}_K$-module, we still have $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]^\vee = x^{-1}\mathcal{O}_K[\alpha]$ (see remark after 2.10). Hence in particular, $x\mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$. Since we are in a valuation field, there is $n > 0$ such that $p^n \mathcal{O}_L \subseteq \mathcal{O}_K[\alpha]$.

Notice that $m_\alpha(\alpha) = 0$ gives $xd\alpha = 0$. Given $u \in \mathcal{O}_L$, from what we have in the first place, $p^n u \in \mathcal{O}_K[\alpha]$ for some n (same n as before), and $p^n du \in \mathcal{O}_L d\alpha$, thus $xp^n du = 0$ for all $u \in \mathcal{O}_L$. By our choice of n, this means p^{2n} kills $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$.

On the other hand, the Almost Purity Theorem (3.6) says that L is perfectoid. This says that if $u \in \mathcal{O}_L$, then u has a p-th root modulo p, which means explicitly that there are $w, y \in \mathcal{O}_L$ with $w^p = u + py$. So $pw^{p-1}dw = du + pdy \in \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$, or we can write $du = p(w^{p-1}dw - dy) \in p\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$. Since $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ is generated by $\{du : u \in \mathcal{O}_L\}$, this means that $p\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$.

Combining these results, we have $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = p\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = p^2\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = \cdots = p^{2n}\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$. □

Let's make some remarks.

(a) If $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$, we say that L/K is **almost étale**. We have just proved that if K is a perfectoid field and L/K is a finite extension, then L/K is almost étale.

(b) As previously foreshadowed, we never write down what $\mathcal{O}_L$ looks like as an $\mathcal{O}_K$-module, and it's difficult to do so. In fact, in this case, $\mathcal{O}_L$ is étale over $\mathcal{O}_K$ iff $\mathcal{O}_L$ is a finitely presented $\mathcal{O}_K$-algebra.

(c) Verbally one can interpret this theorem this way: perfectoid fields contain so much ramifiedness, that any finite extension of it is always almost étale.

From what follows, our setup will be where K is a perfectoid field over $\mathbb{Q}_p$ and L/K is a finite Galois extension with Galois group G. We will see how condition (e) of 4.9 behaves.

Theorem 4.11. *The natural map*

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \prod_{\gamma \in G} \mathcal{O}_L \text{ given by } x \otimes y \mapsto (x\gamma(y))_{\gamma \in G}$$

is an almost isomorphism, ie. the kernel and cokernel of this map are both killed by $\mathfrak{m}_L$.

Remark:

(a) Again, we know that $\mathcal{O}_L$ is usually not finite generated as a $\mathcal{O}_K$-module, so after a base change to $\mathcal{O}_L$, the left is usually not a finitely generated $\mathcal{O}_L$-module. But the right is always finitely generated as an $\mathcal{O}_L$-module, so it's not correct to expect this to be an isomorphism in general.

(b) We would really like to see an explicit example of this map, but it's just not easy: even in the basic (and nontrivial) case where we adjoin $\sqrt{p}$ to $\mathbb{Q}_p(\zeta_{p^\infty})$, we already dont know what $\mathcal{O}_L$ looks like (it's not finitely generated!). However this map is always injective. (why?)

We have been trying to add the adjective "almost" everywhere, and this is exactly what *almost algebra* does. This will be what we will talk about next time.

October 31, 2018. Wednesday.

4.2. Almost Algebras.

A good reference here will be *Gabber and Romero*.

Let's fix a perfectoid field $K/\mathbb{Q}_p$ and let L/K be a Galois extension with Galois group G. We do not assume that L/K is finite; in fact the interesting part comes in when it's not.

First we define some terminologies. Let M, N be objects in the category $\mathsf{Mod}_{\mathcal{O}_K}$, and let f be a morphism from M to N.

(a) M is **almost zero** if $\mathfrak{m}_K M = 0$.
(b) $f : M \to N$ is **almost injective** if $\ker f$ is almost zero.
(c) f is **almost surjective** if $\operatorname{coker} f$ is almost zero.
(d) f is an **almost isomorphism** if both $\ker f$ and $\operatorname{coker} f$ are almost zero.

Lemma 4.12. *An $\mathcal{O}_K$-module M is almost zero iff $\mathfrak{m}_K \otimes_{\mathcal{O}_K} M = 0$.*

Proof. Let's assume that $\mathfrak{m}_K \otimes_{\mathcal{O}_K} M = 0$. Consider the bilinear map $\mathfrak{m}_K \times M \to \mathfrak{m}_K M$ given by $(a, m) \mapsto am$. This map factors through $\mathfrak{m}_K \otimes_{\mathcal{O}_K} M$, and so it's zero, which means $am = 0$ for all $a \in \mathfrak{m}_K$ and $m \in M$, or $\mathfrak{m}_K M = 0$. The other direction is obvious. $\square$

Lemma 4.13. *The full subcategory of almost zero $\mathcal{O}_K$-modules is a Serre subcategory, ie. it is closed under subobjects, quotients and extensions.*

Proof. The lemma is clear for subobjects and quotients. For a perfectoid field K, we have $\mathfrak{m}_K^2 = \mathfrak{m}_K$. If $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is a short exact sequence of $\mathcal{O}_K$-modules, and $\mathfrak{m}_K A = \mathfrak{m}_K C = 0$, it now suffices to show $\mathfrak{m}_K^2 B = 0$. suppose $b \in B, y \in \mathfrak{m}_K$, then $g(yb) = yg(b) = 0$, so there is $a \in A$ so that $f(a) = yb$. So if $x \in \mathfrak{m}_K$, then $xyb = xf(a) = 0$. $\square$

Lemma 4.14. *$f : M \to N$ is almost surjective iff $1 \otimes f : \mathfrak{m}_K \otimes M \to \mathfrak{m}_K \otimes N$ is surjective.*

Proof. This is simply due to the fact that $\mathfrak{m}_K \otimes \operatorname{coker}(f) = \operatorname{coker}(1 \otimes f)$. $\square$

4.14 will come up handy in the future, because morally speaking it allows us to reduce almost surjectivity statements to usual surjectivity ones. We will talk about this when it shows up later.

Last time we proposed a question: If K is perfectoid and L/K is finite and Galois with Galois group $G = \operatorname{Gal}(L/K)$, what can we say about the map $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \prod_{\gamma \in G} \mathcal{O}_L$ (given by $x \otimes y \to (x\gamma(y))_{\gamma \in G}$)?

Theorem (Restatement of 4.11)**.** *Let $S = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L$ and $R = \prod_{\gamma \in G} \mathcal{O}_L$. Then the natural map $S \to R$ is an almost isomorphism.*

Proof. We consider the tilts, where we abuse the notation and write $R^\flat = \prod_{\gamma \in G} \mathcal{O}_{L^\flat}$ and $S^\flat = \mathcal{O}_{L^\flat} \otimes_{\mathcal{O}_{K^\flat}} \mathcal{O}_{L^\flat}$. (This already uses the fact that L is perfectoid too.)

So now we have a map from $S^\flat \to R^\flat$. The nondegeneracy of the trace pairing says that there is $\beta^\flat \in \mathcal{O}_{K^\flat}$ with $\beta^\flat R^\flat \subseteq S^\flat$ (where we abuse the notation and write $S^\flat$ instead of $\operatorname{Im}(S^\flat)$). If $\beta^\flat$ is invertible, then the extension would have been étale so we were done. So let's assume $\beta^\flat \in \mathfrak{m}_{K^\flat}$.

Now that we have promoted the situation to their tilts, we know that $R^\flat$ and $S^\flat$ are perfect, so we can take p-th roots on both sides, and say that $(\beta^\flat)^{p^{-r}} R^\flat \subseteq S^\flat$ for all $r \geq 1$. Since in the sequence $\{(\beta^\flat)^{p^{-r}}\}_{r \geq 0}$, the norm of the entries goes to 1, we can say that $S^\flat \to R^\flat$ is almost surjective, and thus an almost isomorphism, and so is $S/p \to R/p$.

Next we claim $S/p^n \to R/p^n$ is an almost isomorphism for all n, which we will prove so by induction on n. Consider

$$\begin{tikzcd} 0 \arrow[r] & S/p^{n-1} \arrow[r] \arrow[d] & S/p^n \arrow[r] \arrow[d] & S/p \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & R/p^{n-1} \arrow[r] & R/p^n \arrow[r] & R/p \arrow[r] & 0 \end{tikzcd}$$

Snake's lemma and 4.13 will then prove the claim.

More explicitly, this means that for any $\alpha \in \mathfrak{m}_K, r \in R$ and $n \geq 1$, we can find $s_n \in S$ such that $\alpha r - s_n \in p^n R$. Since S is p-adically complete, we have $\alpha r = \lim s_n \in S$, and this finishes the proof. $\square$

The next thing on the discussion table is Galois descent. We have seen that if L/K is (finite and) unramified, in the sense that $\mathcal{O}_L/\mathcal{O}_K$ is etale, then $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L \to \prod_{\gamma \in G} \mathcal{O}_L$ is an isomorphism. In this case faithfully flat descent is equivalent to Galois descent, and says that if M is an $\mathcal{O}_L$-module with a *compatible* G-action, then $\mathcal{O}_L \otimes M^{\mathrm{Gal}(L/K)} \xrightarrow{\sim} M$. We already know $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = 0$ remains true if K is perfectoid. In our case if $\mathcal{O}_L/\mathcal{O}_K$ is not étale (we only know L/K is almost étale) and K is perfectoid, what can we say about Galois descent? No surprises:

Corollary 4.15. *If K is perfectoid and L/K is finite and Galois, and M is an $\mathcal{O}_L$-module with a* compatible *$G = \mathrm{Gal}(L/K)$-action, then the natural map $\mathcal{O}_L \otimes_{\mathcal{O}_K} M^G \to M$ is an almost isomorphsim.*

In particular, this implies that if M, N are two $\mathcal{O}_L$-modules with compatible $\mathrm{Gal}(L/K)$-action, and $M \to N$ is a Galois-equivariant surjection, then the natural map $M^G \to N^G$ is almost surjective, because this condition can be checked after $- \otimes_{\mathcal{O}_K} \mathcal{O}_L$ by faithful flatness. [44]

If we apply this specific case to $M = \mathcal{O}_L$ and $N = \mathcal{O}_L/p^n$, then we see that $\mathcal{O}_K = \mathcal{O}_L^G \to (\mathcal{O}_L/p^n)^G$ is almost surjective. Verbally, if we have an $x \in \mathcal{O}_L$ such that all its Galois conjugates are close to each other, then there's an actual element $x' \in \mathcal{O}_K$ and $\alpha \in \mathfrak{m}_K$ with $\alpha x' = x$. [45]

Next we move onto infinite extensions. A long time ago we have talked about $\mathsf{Rep}_\Gamma^{\mathrm{cont}}(C)$, let's recall what this notation means:

Let $K/\mathbb{Q}_p$ be a finite extension, and let $C = \widehat{\overline{K}}, \Gamma = \mathrm{Gal}(\overline{K}/K)$ acting on C, and Ax-Sen-Tate (2.16) says that $C^\Gamma = K$. We defined

$\mathsf{Rep}_\Gamma^{\mathrm{cont}}(C) = \{$finite dimensional C-vector spaces V with a continuous compatible Γ-action$\}$.

What does "continuous" mean? If we fix a basis $C^n \xrightarrow{\sim} V$, then the action of Γ on V is given by a homomorphism $\rho : \Gamma \to GL_n(C)$. Γ comes with a profinite topology, and $GL_n(C)$ comes with a p-adic topology. Hence continuity says that for every $m \geq 1$, there is a finite index subgroup $\Gamma_m \subseteq \Gamma$ such that $\rho(\Gamma_m) \subseteq \mathrm{Aut}(p^m \mathcal{O}_C^{n^2})$.

[44] Rephrasing, if we have a short exact sequence $0 \to K \to M \to N \to 0$ of $\mathcal{O}_L$-modules, then $H^1(G, K)$ is almost zero.
[45] It might be helpful to some to work out what this means when $L = \mathbb{Q}_p(\sqrt{p})$ and $K = \mathbb{Q}_p$, even though K here is not perfectoid.

Theorem 4.16. *If $V \in \mathsf{Rep}_\Gamma^{cont}(C)$, then it is* trivial in our sense*, ie.*

$$C \otimes_K V^\Gamma \xrightarrow{\sim} V, \text{ or equivalently } \dim_K V^\Gamma = \dim_C V.$$

Hence $\mathsf{Rep}_\Gamma^{cont}(C) \to \mathsf{Vect}_K^{fd}$ given by $V \mapsto V^\Gamma$ is an isomorphism.

November 1, 2018. Thursday.

Last time we ended with a theorem, with the setup as follows: let $C = \widehat{\overline{K}}$, where K is perfectoid over $\mathbb{Q}_p$. Write $\Gamma = \mathrm{Gal}(\overline{K}/K)$.

Theorem. *If $V \in \mathsf{Rep}_\Gamma^{cont}(C)$ is finite dimensional, then $C \otimes_K V^\Gamma \xrightarrow{\sim} V$ as C-vector spaces.*

Proof. First we reduce to the case where an finite index $\mathcal{O}_C$-lattice $V_0 \subseteq V$ is preserved by Γ. We will show that $\mathcal{O}_C \otimes_{\mathcal{O}_K} V_0^\Gamma \to V_0$ is an almost isomorphism. This will suffice, since coker and ker here are torsion, they will be killed after $C \otimes_{\mathcal{O}_C} -$, and we recover an isomorphism $C \otimes_K V^\Gamma \xrightarrow{\sim} V$.

Since the natural map $C \otimes_K V^\Gamma \to V$ is always injective, the map $\mathcal{O}_C \otimes_{\mathcal{O}_K} V_0^\Gamma \to V_0$ is always injective too. Thus it will suffice to show almost surjectivity.

$$\begin{tikzcd}
\mathcal{O}_C \otimes_{\mathcal{O}_K} (V_0^\Gamma/p^m) \arrow[r, "f"] \arrow[d, "g"'] & V_0/p^m \\
\mathcal{O}_C \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma \arrow[ur, "h"'] &
\end{tikzcd}$$

It suffices to show that f is almost surjective for all $m \geq 1$, and here's our strategy.

Step (1) We show that the natural map $V_0^\Gamma/p^m \to (V_0/p^m)^\Gamma$ is almost surjective.
Step (2) We show that $h : \mathcal{O}_C \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma \to V_0/p^m$ is an almost isomorphism.

Let's start with the second step. We start by fixing a basis $\mathcal{O}_C^n \to V_0$. The action of Γ on V_0 is then given by $\rho : \Gamma \to GL_n(\mathcal{O}_C)$. For $m \geq 1$, since $\ker(GL_n(\mathcal{O}_C) \to GL_n(\mathcal{O}_C/p^m))$ is open, by continuity, there is a finite index subgroup Γ_m that is normal in Γ, and such that $\rho(\Gamma_m)$ acts trivially on $\mathcal{O}_C^n/p^m$. As $\mathcal{O}_C$-modules with a Γ_m-action, we then have $(\mathcal{O}_C^n/p^m)^{\Gamma_m, \rho} \xrightarrow{\sim} (V_0/p^m)^{\Gamma_m}$, where the superscript ρ means Γ_m acts on $(\mathcal{O}_C^n/p^m)^{\Gamma_m}$ via ρ. More precisely, if the basis $\mathcal{O}_C^n \xrightarrow{\sim} V_0$ is given by $\{e_1, \ldots, e_n\}$, and $v = \sum v_i e_i$, then $\gamma(v) = \rho(\gamma)(\gamma(v_1), \ldots, \gamma(v_n))^t$.

Write $K_m = C^{\Gamma_m} = \widehat{\overline{K}}^{\Gamma_m} = \overline{K}^{\Gamma_m}$ which is finite Galois over K. Next we claim $\mathcal{O}_{K_m}^n/p^m \to (\mathcal{O}_C^n/p^m)^{\Gamma_m}$ is an almost isomorphism. Since we have restricted the source to $\mathcal{O}_{K_m}$, ρ is now trivial and thus irrelevant.

For this, it suffices to show that $\mathcal{O}_{K_m}/p^m \to (\mathcal{O}_C/p^m)^{\Gamma_m}$ is an almost isomorphism. We know that

$$(\mathcal{O}_C/p^m)^{\Gamma_m} = \varinjlim_{\substack{K_m \subseteq L \subseteq \overline{K} \\ L/K_m \text{ finite Galois}}} (\mathcal{O}_L/p^m)^{\mathrm{Gal}(L/K_m)}.$$

With this description, the claim is now clear, as we have previously discussed that this map is always injective, and $\mathcal{O}_{K_m}/p^m \to (\mathcal{O}_L/p^m)^{\Gamma_m}$ is almost surjective for all L, since L/K_m is finite Galois.

$$
\begin{tikzcd}
\mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} (\mathcal{O}_{K_m}^n/p^m) \arrow[r, "\mathrm{al}\sim"] \arrow[d, "\wr"'] & \mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} (V_0/p^m)^{\Gamma_m} \arrow[d, squiggly] \\
\mathcal{O}_C^n/p^m \arrow[r, "\sim"'] & V_0/p^m
\end{tikzcd}
$$

We knew from what we have discussed that the top map is an almost isomorphism. The bottom map arises from the choice of basis, and thus is an isomorphism. The left map is also an isomorphism. Hence the commutative diagram says the map of interest, denoted with a squiggly arrow, is an almost isomorphism. This proves step (2) for Γ_m.

Now we wish to relate back to $\mathcal{O}_C \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma \to V_0/p^m$, which is the map in the step (2) after all. We know that $\mathcal{O}_C \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma = \mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} (\mathcal{O}_{K_m} \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma)$. Since K_m/K is finite, we can apply almost Galois descent and say that

$$\mathcal{O}_{K_m} \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma \xrightarrow{\mathrm{al}\sim} (V_0/p^m)^{\Gamma_m}.$$

Combining everything, we know that

$$\mathcal{O}_C \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma = \mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} (\mathcal{O}_{K_m} \otimes_{\mathcal{O}_K} (V_0/p^m)^\Gamma) \xrightarrow{\mathrm{al}\sim} \mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} (V_0/p^m)^{\Gamma_m} \xrightarrow{\mathrm{al}\sim} V_0/p^m.$$

This concludes step (2).

Next we prove step (1), which states that $V_0^\Gamma/p^m \to (V_0/p^m)^\Gamma$ is almost surjective. First we claim that if V_0 is p-adically complete, and Γ acts continuously with respect to the p-adic topology, then $V_0^\Gamma \xrightarrow{\sim} \varprojlim_r (V_0/p^r)^\Gamma$. Indeed, we know that $V_0^\Gamma \hookrightarrow V_0$ and $\varprojlim_r (V_0/p^r)^\Gamma \hookrightarrow \varprojlim_r (V_0/p^r)$, and $V_0 \xrightarrow{\sim} \varprojlim_r (V_0/p^r)$ by p-adic completeness. Taking Γ-invariants yields the answer (Γ acts on the inverse limit entry-by-entry).

Finally now to prove step (1), it suffices to show that $V_0^\Gamma \to (V_0/p^m)^\Gamma$ is almost surjective. We now know that $V_0^\Gamma = \varprojlim_r (V_0/p^r)^\Gamma$. We invoke the following lemma:

Lemma 4.17. *If $\{M_n\}$ is an inverse system of $\mathcal{O}_K$-modules, such that $M_r \to M_s$ (for $r > s$) is almost surjective for all r, s, then $\varprojlim_r M_r \to M_s$ is almost surjective.*

Proof. This statement is obviously true if almost surjectivity is replaced by usual surjectivity, but we can do so by using 4.14. □

So now it remains to show that $(V_0/p^r)^\Gamma \to (V_0/p^s)^\Gamma$ is almost surjective for $r > s$, for which we can check after $\mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} -$ by faithful flatness. Consider the following diagram:

$$
\begin{tikzcd}
\mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} (V_0/p^r)^\Gamma \arrow[r, dashed, "\mathrm{al}\sim"] \arrow[d, squiggly] & V_0/p^r \arrow[d] \\
\mathcal{O}_C \otimes_{\mathcal{O}_{K_m}} (V_0/p^s)^\Gamma \arrow[r, dashed, "\mathrm{al}\sim"] & V_0/p^s
\end{tikzcd}
$$

We know the horizontal maps are almost isomorphisms. The right map is a surjection, so the left map, our map of interest, is an almost surjection, which completes our proof. $\square$

Let's look at some applications. Fix a finite extension $E/\mathbb{Q}_p$ and let $K = E(\zeta_{p^\infty})\widehat{}$. Since $K/\mathbb{Q}(\zeta_{p^\infty})$ is finite, we know that K is perfectoid. Write $\Delta := \mathrm{Gal}(E(\zeta_{p^\infty})/E)$. We know that $\Delta \hookrightarrow \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p^\times$ via the cyclotomic character, so Δ is a finite index subgroup.

Suppose $\Gamma = \mathrm{Gal}(\overline{E}/E)$, inside of which we have a normal subgroup $\Gamma_\infty = \mathrm{Gal}(\overline{E}/E(\zeta_{p^\infty}))$. Let $C = \widehat{\overline{E}} = \mathbb{C}_p$, and we have $\Delta = \Gamma/\Gamma_\infty$. Then $C^{\Gamma_\infty} = K$.

Corollary 4.18. *In this setup, applying $\Gamma = \Gamma_\infty$ in the theorem, we see that the functor*

$$\mathsf{Rep}_\Gamma^{cont}(C) \to \mathsf{Rep}_\Delta^{cont}(K) \text{ given by } V \mapsto V^{\Gamma_\infty}$$

is an equivalence of categories, with inverse given by $C \otimes_K M \leftarrow\!\shortmid M$, where Γ acts on $C \otimes_K M$ diagonally.

Morally speaking since we know Δ is a finite index subgroup of $\mathbb{Z}_p^\times$, this makes $\mathsf{Rep}_\Delta^{\mathrm{cont}}(\Delta)$ easier to study.

To conclude the section of perfectoid fields, we will state a few complements.

(a) Let's write $K^{\mathrm{fin}} := E(\zeta_{p^\infty})$ and $K = E(\zeta_{p^\infty})\widehat{}$.

5Suppose $\Gamma = \mathrm{Gal}(\overline{E}/E)$, inside of which we have normal subgroup $\Gamma_\infty = \mathrm{Gal}(\overline{E}/E(\zeta_{p^n})))$. $C = \widehat{\overline{E}} = \mathbb{C}_p$. $\Delta = \Gamma/\Gamma_\infty$. Corollary: taking Γ_∞ invariants give $\mathsf{Rep}_\Gamma^{cts}(C) \to \mathsf{Rep}_\Delta^{cts}(K)$. Note $C^{\Gamma_\infty} = K$.

Complements:

(1) $K^{fin} := E(\zeta_{p^\infty})$. Suppose $M \in \mathsf{Rep}_\Delta^{cts}(K)$. Inside M we find $M^{fin} = \{m \in M : \Delta m$ generated a fd $\mathbb{Q}_p - vs\}$. This property is preserved by K^{fin} since K^{fin} collects finite dim stuff. Then $K \otimes_{K^{fin}} M^{fin} \xrightarrow{\sim} M$ (decompletion). Can show there exists $r \geq 1$ if $K_r = E(\zeta_{p^r})$, then there exists $M_r \in \mathsf{Rep}_\Delta^{cts}(K_r)$ with $K \otimes_{K_r} M_r \xrightarrow{\sim} M$ which is Δ equivariant. This is because choose basis for M^{fin}, and basis element is already defined over some finite extension of K... M_r is not canonical but decompletion is.

November 5, 2018. Monday.

5. Fargues-Fontaine Curves.

Our goal before the end of the course will be to make sense and prove the catchphrase "Weakly admissible implies admissible", which is a statement first proved by Colmez and Fontaine [46], and later Fargues and Fontaine gave another proof. We have not made sense of what "weakly admissible" means; for now it suffices to know that this is a statement about *filtered ϕ-modules*, asking which ones arise from Galois representations (which is the definition of *admissible*). Weakly admissible is a linear or algebraic condition.

[46] in their paper titled "Construction des représentations p-adiques semi-stables."

5.1. Gauss Norms.

First we will develop more theory to Gauss norms. We fix a perfectoid field F over $\mathbb{F}_p$, and write $A_{\text{inf}} := W(\mathcal{O}_F)$. We have a (lift of) Frobenius ϕ acting on A_{inf} via each of the Teichmüller coordinates. Fixing $\rho \in (0,1]$, we define the **Gauss norm**

$$|\cdot|_\rho : A_{\text{inf}} \to \mathbb{R}_{\geq 0} \text{ by } |x|_\rho = \sup_k |x_k|_F \rho^k.$$

We write $N_k(x) := \max_{n\geq k} |x_n|_F$. Observe that:

(a) Since $|p|_\rho = \rho^{-1}$, we can extend $|\cdot|_\rho$ to $A_{\text{inf}}[p^{-1}]$ by defining $|x/p^n|_\rho = \rho^{-n}|x|_\rho$.
(b) If $\rho < 1$, then the supremum appearing in the definition of $|\cdot|_\rho$ is actually a maximum, because $|x_n|_F$ is bounded between 0 and 1, forcing $|x_k|_F \rho^k \to 0$ as $k \to \infty$.
(c) If $x \in A_{\text{inf}}$ and $\rho_1 < \rho_2$, then clearly $|x|_{\rho_1} \leq |x|_{\rho_2}$. However if $x \in A_{\text{inf}}[p^{-1}]$, then the same cannot be said; the best we can say is if $\rho_1 \leq \rho \leq \rho_2$, then $|x|_\rho \leq \max\{|x|_{\rho_1}, |x|_{\rho_2}\}$.
(d) A priori if $\rho = 1$, then we saw that $\sup_k N_k(x) = |x|_1$. In general we have

$$\sup_k N_k(x)\rho^k = \sup_k \sup_{n\leq k} |x_n|_F \rho^k = \sup_n \sup_{k\geq n} |x_n|_F \rho^k = \sup_n |x_n|_F \rho^n = |x|_\rho.$$

We have seen in 4.7 that $|\cdot|_1$ is a multiplicative non-archimedean norm on A_{inf}. This still holds in general:

Proposition 5.1. *Let $x, y \in A_\infty[p^{-1}]$. Then we have $|x+y|_\rho \leq \max\{|x|_\rho, |y|_\rho\}$ (with the natural condition for when the equality holds) and $|xy|_\rho = |x|_\rho |y|_\rho$.*

Proof. We will simplify the situation and prove for when $x, y \in A_{\text{inf}}$. We leave the reduction to this case an exercise for the readers.

Note that $N_k(x) \leq |c|_F$ where $c \in \mathfrak{m}_F$ iff $x \pmod{p^{k+1}} \in [c]A_{\text{inf}}/p^{k+1}$ as before. We can again see, as in 4.7, that $N_k(x+y) \leq \max\{N_k(x), N_k(y)\}$. Hence $\sup_k N_k(x+y)\rho^k \leq \sup_k \max\{N_k(x)\rho^k, N_k(y)\rho^k\}$, and this implies the first part of the proposition. We will leave the second part till next lecture.

November 7, 2018. Wednesday.

Last time we have yet to prove that the norm $|\cdot|_\rho$ is multiplicative.

Proof continued. Using the similar observation from last time, one can deduce that $|\cdot|_\rho$ is a seminorm, and we leave this for the readers. Assume that $\rho < 1$ for now. In this case, a priori there are n, m with $|x|_\rho = |x_n|_F \rho^n$ and $|y|_\rho = |y_n|_F \rho^m$ and are the minimal such. Write

$$\begin{aligned} x &= (\text{front terms}) + [x_n]p^n + p^{n+1}(\text{tail}) \\ y &= (\text{front terms}) + [y_m]p^m + p^{m+1}(\text{tail}) \end{aligned}$$

and their product is

$$xy = \overbrace{(\text{sum of products involving front terms})}^{z} + [x_n y_m]p^{n+m} + p^{n+m+1}(\text{tail}).$$

One can check that $|z|_\rho < |x|_\rho |y|_\rho$ by the minimality of n, m. Now on one hand we know by definition that $N_{n+m}(xy)\rho^{n+m} \leq |xy|_\rho$, but on the other hand it's the same as $N_{n+m}(z +$

$[x_n y_m]p^{n+m})\rho^{n+m}$ (ie. we cut off the tail). Since $N_{n+m}(z)\rho^{n+m} < |x|_\rho |y|_\rho$ and $N_{n+m}([x_n y_m]p^{n+m})\rho^{n+m} = |x|_\rho |y|_\rho$, using the non-archimedean property we now have

$$|x|_\rho |y|_\rho = N_{n+m}(z + [x_n y_m]p^{n+m})\rho^{n+m} = N_{n+m}(xy)\rho^{n+m} \le |xy|_\rho.$$

This gives the reverse inequality. For $\rho = 1$, we note that $|x|_1 = \lim_{\rho \to 1^-} |x|_\rho$. □

Next we make a definition. Fix an interval $I \subseteq (0,1)$, and define

$$B_I := \text{ the completion of } A_{\inf}[(p[\varpi])^{-1}] \text{ with respect to } \}\{|\cdot|_\rho : \rho \in I\}$$

where $[\varpi]$ is any Teichmüller lift. More precisely, B_I consists of all the sequences that are Cauchy with respect to all the norms $\{|\cdot|_\rho : \rho \in I\}$. We also define $B := B_{(0,1)}$. [47]

We make a few quick ovservations:

(a) If $J \subseteq I$, then there is a natural map $B_I \to B_J$. We will eventually see that this natural map is injective.
(b) In addition, if $I = \cup J_n$ is an increasing union, then $B_I = \varprojlim B_{J_n}$.
(c) If $J = [\rho_1, \rho_2]$ is compact, since we know for $\rho \in [\rho_1, \rho_2]$ we have $|x|_\rho \le \{|x|_{\rho_1}, |x|_{\rho_2}\}$, *the topology with respect to* $|\cdot|_\rho : \rho \in J\}$ is equivalent to the topology with respect to $\|\cdot\|_J = \max\{|\cdot|_{\rho_1}, |\cdot|_{\rho_2}\}$.
(d) If $\rho_1 = |a|_F$ and $\rho_2 = |b|_F$ where $a, b \in \mathfrak{m}_F$, then

$$x \in A_{\inf}[(p[\varpi])^{-1}] : \|x\|_J \le 1\} = A_{\inf}[[a]/p, p/[b]].$$

(At least this sounds convincing since $|[a]/p|_{\rho_1} = \rho_1 \rho_1^{-1} = 1$ and similarly for $p/[b]$.)
(e) Moreover, $\|\cdot\|_J$-topology on B_J is equivalent to the p-adic or $[\varpi]$-adic or $[a]$-adic or $[b]$-adic topology. Completing with respect to the p-adic topology, we get

$$B_J = A_{\inf}[[a]/p, p/[b]]^\frown[1/p].$$

In fact, using this description, we could have defined B_J without using norms at all for compact intervals, and extend such to non-compact intervals using the inverse limit.

How can one geometrically think about B_J? From a functor-of-points point of view, maps out of $\mathbb{Z}_p[[t]][a/T, T/b]^\frown$ are same as specifying the image of T where $|x| > |a|$ and $|x| < |b|$. Similarly, maps out of $\mathbb{Z}_p\langle T\rangle\,[a/T, T/b]^\frown$ correspond to specifying x with $|b| \ge |x| \ge |a|$. Thus very heuristically speaking, B_J can be thought as functions on a annnulus with $\|a\| \le \|p\| \le \|b\|$.

So where are we headed? Consider the map $\rho : (0,1) \to (0,1)$ sending $x \mapsto x^p$. This induces a map (abuse of notation) $\rho : B_{(0,1)} \to B_{\rho(0,1)}$. On the other hand, we also have the (SOMETHING'S NOT RIGHT) — Last time we have $\rho : A_{\inf} \xrightarrow{\sim} A_{\inf}$, and now $I \subseteq (0,1)$, so we consider $\rho : B_I \to B_{\rho(I)}$, where $\rho : (0,1) \to (0,1), x \mapsto x^p$, in particular $\rho : B \xrightarrow{\sim} B$.

If $x = \sum [x_n]p^n$, then $\phi(x) = \sum [x_n^p]p^n$, then $|\phi(x)|_\rho = \sup |x_n|_F^p \rho^n = (|x|_{\rho^{1/p}})^p$.

[47] One can ask what topology B_I is equipped with; we will briefly discuss this in what follows. One can also read about *Fréchet spaces.*

— Our goal will be to study $B^{\phi=p^n}$.

Once we have computed what $B^{\phi=p^n}$ is, we can define

$$X = X_F := \operatorname{Proj} \bigoplus_{n \geq 0} B^{\phi=p^n},$$

and it turns out X is a complete curve over $\mathbb{Q}_p$. Completeness here means that it's a Dedekind scheme satisfying $H^0(X, \mathcal{O}_X) = \mathbb{Q}_p$ (hence "complete"), with a degree function $|X|_{\max} \to \mathbb{Z}$. However it's not proper becaue it's not of finite type over $\mathbb{Q}_p$! Some closed points have residue fields as untilts of F if F is algebraically closed, otherwise they will be finite extensions of F. The construction X_F is functorial in F.

5.2. (Fargues's) Newton Polygons and Legendre Transform.

If $x \in A_{\inf}[(p[\varpi])^{-1}]$, then $x = \sum_{n \gg -\infty} [x_n] p^n$ where $x_n \in F$ and $\sup |x_n|_F < \infty$. Hence we can define the Newton polygon of x to be

$$\mathrm{NP}(x) := \text{ the convex hull of } \{(n, v_F(x_n)) : n \in \mathbb{Z}\}$$

where $v_F(\cdot) = -\log_p |\cdot|_F$. This is essentially the traditional Newton polygon but now we work with power series in p. Our goal will be to define the Newton polygon on B_I, but we immediately run into a brick wall: there's no Teichmüller cofficients for a general $x \in B_I$! Even if they exist, it's not entirely clear why they should be unique anyway. So we are going to need a roundabout way to construct Newton polygons for $x \in B_I$, namely the Legendre transform.

Let $f : \mathbb{R} \to (-\infty, \infty]$ be a function that is not identically ∞. We define its **Legendre transform**

$$\mathcal{L}(f) : \mathbb{R} \to [-\infty, \infty) \text{ given by } \mathcal{L}(f)(r) = \inf_t \{f(t) + rt\}.$$

Conversely if $g : \mathbb{R} \to [-\infty, \infty)$ is a function that is not identically $-\infty$, we define the inverse transform to be

$$\mathcal{L}^{-1}(g) : \mathbb{R} \to (-\infty, \infty] \text{ given by } \mathcal{L}^{-1}(g)(t) = \sup_r \{g(r) - tr\}.$$

November 8, 2018. Thursday.

Last time we have defined the Legendre transforms $\mathcal{L}$ and $\mathcal{L}^{-1}$.

Since this subsection is rather technical, it is beneficial to first give a brief overview. Our logic for this subsection will be to

(Step 1) first understand $\mathcal{L}$ in generality and see that $\mathcal{L}^{-1}\mathcal{L}$ describes the convex hull,

(Step 2) understand $\mathcal{L}(x)$ for $x \in A_{\inf}[(p[\varpi])^{-1}]$,

(Step 3) show that $\mathcal{L}(x)$ behaves reasonably nicely under Cauchy sequences (with respect to a family of norms) in $A_{\inf}[(p[\varpi])^{-1}]$, and thus

(Step 4) extend $\mathcal{L}(x)$ to B_I for an interval $I \subseteq (0, 1)$, and define the Newton polygon on B_I using $\mathcal{L}^{-1}\mathcal{L}$ (and study its properties thereafter).

Readers deserve to be warned that once we reach (c), there will be two parameters simultaneously: n for the n-th term in a Cauchy sequence, and r for parametrizing the family of norms. We will remind the reader when we reach there.

Let's begin with (Step 1). Let's define

(a) $\Delta_f^- = \{(x,y) : y \le f(x)\}$, the points below the graph of f, and
(b) $\Delta_f^+ = \{(x,y) : y \ge f(x)\}$ for the points above the graph.

A straightforward computation sees that

$$\begin{aligned}\Delta^-_{\mathcal{L}(f)} &= \{(r,s) : s \le \mathcal{L}(f)(r)\}\\ &= \{(r,s) : s \le f(t) + rt \text{ for all } t\}\\ &= \{(r,s) : s - rt \le f(t) \text{ for all } t\} \ldots (\dagger)\\ &= \{(r,s) : \ell_{-r,s} \text{ lies entirely below the graph of } f\},\end{aligned}$$

where $\ell_{a,b}$ is the line $\ell_{a,b}(t) = at + b$. In addition, we see that

$$\begin{aligned}\Delta^+_{\mathcal{L}^{-1}(\mathcal{L}(f))} &= \{(t,u) : u \ge \mathcal{L}^{-1}(\mathcal{L}(f))(t)\}\\ &= \{(t,u) : u \ge \mathcal{L}(f)(r) - rt \text{ for all } r\}\\ &= \{(t,u) : \ell_{t,u}(r) \ge \mathcal{L}(f)(r) \text{ for all } r\}\\ &= \{(t,u) : \Delta^-_{\mathcal{L}(f)} \subseteq \Delta^-_{\ell_{t,u}}\}\\ &= \{(t,u) : \ell_{-r,s} \text{ lying under } \Gamma_f \text{ implies } (r,s) \in \Delta^-_{\ell_{t,u}}\},\end{aligned}$$

but since $b > -ra + s$ iff $ar + b > s$, we have $(a,b) \in \Delta^+_{\ell_{-r,s}}$ iff $(r,s) \in \Delta^-_{\ell_{a,b}}$. Hence

$$\begin{aligned}\Delta^+_{\mathcal{L}^{-1}(\mathcal{L}(f))} &= \{(t,u) : \ell_{-r,s} \text{ lying under } \Gamma_f \text{ implies } (t,u) \in \Delta^+_{\ell_{-r,s}}\}\\ &= \bigcap_{\ell_{-r,s} \text{ lies under } \Gamma_f} \Delta^+_{\ell_{-r,s}}.\end{aligned}$$

Thus $\mathcal{L}^{-1}(\mathcal{L}(f))$ is precisely the convex hull of Γ_f.

Furthermore, one can observe from (†) that $\mathcal{L}(f)$ is concave for any f, and similarly $\mathcal{L}^{-1}(g)$ is convex for any g. Finally, if f is convex, then evidently $\mathcal{L}^{-1}(\mathcal{L}(f)) = f$.

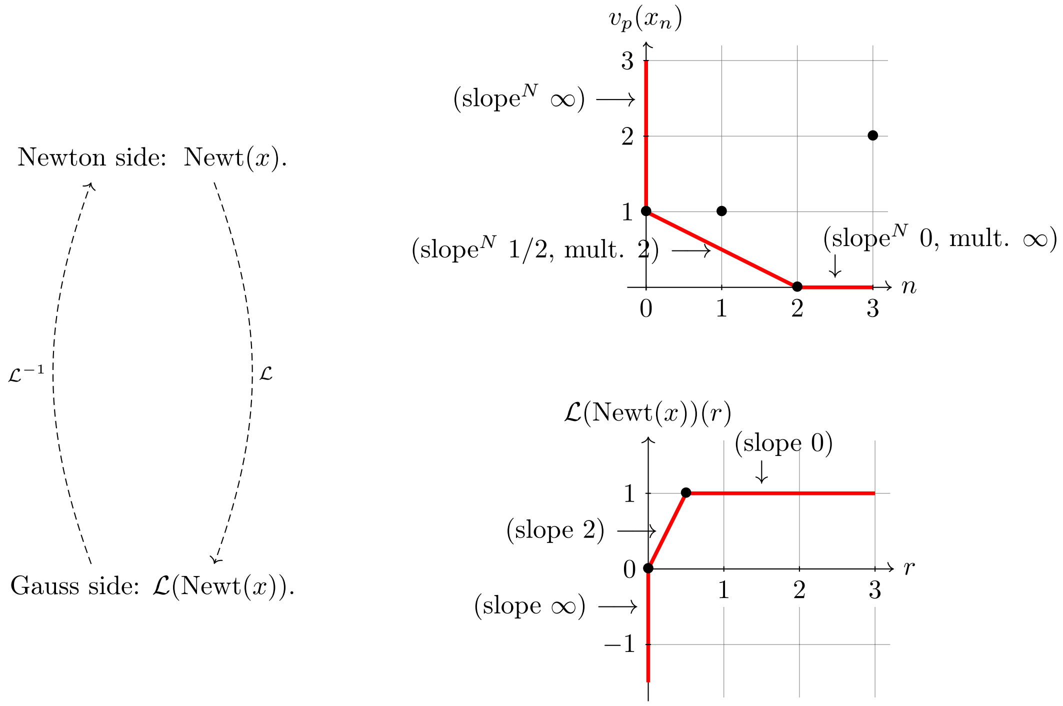
We will eventually apply $\mathcal{L}$ and $\mathcal{L}^{-1}$ in cases related to Newton polygons. Following Fargues's idea, we first fix some terminology. One can skip the bullet points and just read the picture if one desires.

(a) We say that $\mathcal{L}$ transforms from the **Newton side** to the **Gauss side**, and the converse for $\mathcal{L}^{-1}$, from the Gauss side back to the Newton side.
(b) On the Newton side, we will eventually modify the Newton polygon to only record the negative slopes (ie. the *decreasing* convex hull), so all slopes will be negative. We will denote this modified Newton polygon by $\mathrm{Newt}(x)$ as opposed to $\mathrm{NP}(x)$. Then and hence we apply the convention where *slopes* will mean the negative of the (usual) slope of a linear segment. So *slopes* will only measure the steepness of the line: the steeper the line, the greater the slope. We will provide examples later for readers to verify their intuition. I will also write slope^N from now on to emphasize that it's the modified slope in the Newton side.

(c) On the Gauss side, we keep the traditional notion of *slope*.

(d) On the Newton side, we define **multiplicity (or length) of a slope** to be length of the segment when projected onto the x-axis, as per the traditional notion of the Newton polygon.

Here's an example for when $x = [x_0]+[x_1]p+[x_2]p^2+[x_3]p^3$, where $|x_0|_F = |x_1|_F = p^{-1}$, $|x_2|_F = 1$ and $|x_3|_F = p^{-2}$.



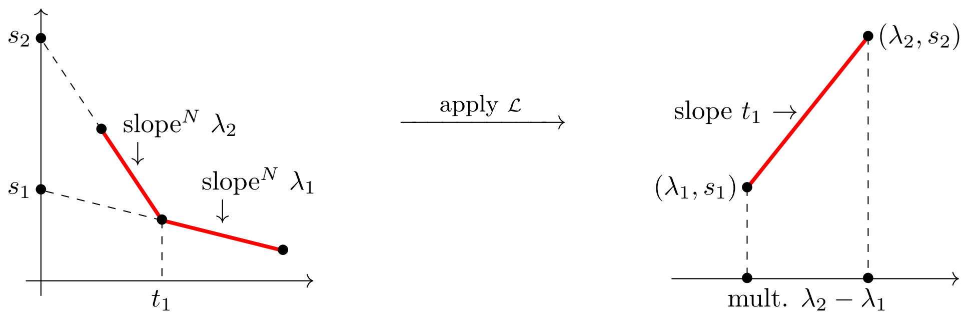
Next, we define the **break points** on both sides to mean the x-coordinates of the corners. One can suitably extend this definition to ∞ or $-\infty$ suitably, but for the current discussion this will be a red herring.

Lemma 5.2. *If f is piecewise linear, convex, and continuous, then $\mathcal{L}(f)$ is piecewise linear, and there is a duality*

$$\{\textit{slopes}^{(N)} \textit{ of } f\} = \{\textit{break points of } \mathcal{L}(f)\} \textit{ and } \{\textit{break points of } f\} = \{\textit{slopes of } \mathcal{L}(f)\}.$$

(Again, one can still make sense of this at ∞ or $-\infty$ values, but much caution is advised.)

Proof. PROOF NEEDED. □



Next we do (Step 2), where we start with the Newton polygon. Last time we have defined the Newton polygon for $x \in A_{\inf}[(p[\varpi])^{-1}]$ (where $x = \sum_{n \gg -\infty} [x_n] p^n$, $x_n \in F$ and $\sup |x_n|_F < \infty$) to be

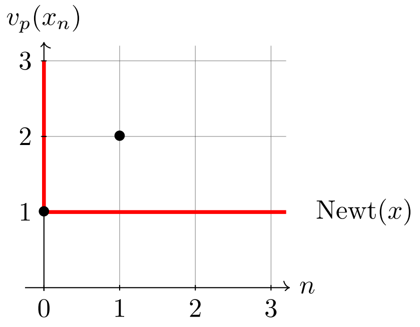
$$\mathrm{NP}(x) = \text{ the convex hull of } \{(n, v_F(x_n)) : n \in \mathbb{Z}\}.$$

We will modify $\mathrm{NP}(x)$ to

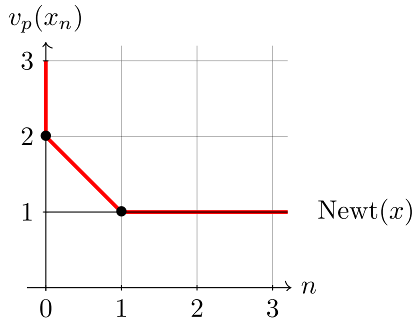
$$\mathrm{Newt}(x) = \text{ the } \textit{decreasing} \text{ convex hull of } \mathrm{NP}(x).$$

More precisely, $\mathrm{Newt}(x)$ only holds onto the negative slopes (ie. positive slopes^N) of $\mathrm{NP}(x)$. If $\sup_n |x_n|_F = |x|_1$ is not attained, then $\mathrm{Newt}(x) = \mathrm{NP}(x)$. Otherwise, $\mathrm{Newt}(x)$ is asymptotic to the horizontal line with y-intercept $v_0(x) = -\log_p |x|_1$.

For instance, if $x = [x_0] + p[x_1]$, then we have $(0, v_p(x_0))$ and $(1, v_p(x_1))$, and $\mathrm{Newt}(x)$ will look like one of the following two diagrams.



if $v_p(x_0) \le v_p(x_1)$.



if $v_p(x_0) > v_p(x_1)$.

Finally, we wish to define $v_x := \mathcal{L}(\mathrm{Newt}(x))$ (as functions of r). Next time we will see that v_x can be (re)defined alternatively without invoking $\mathrm{Newt}(x)$ at all.

November 14, 2018. Wednesday.

Previously we have started talking about Newton polygons. Again, our motivation is to define it for $x \in B_I$, and our main obstruction is that x does not admit Teichmüller coefficients.

If $x \in A_{\inf}[(p[\varpi])^{-1}]$, we can consider the function

$$v_x(r) := \begin{cases} v_r(x) := \inf_n \{v_F(x_n) + rn\} & \text{if } r \ge 0, \\ -\infty & \text{otherwise.} \end{cases}$$

This time we start (Step 3), where we show that v_r behaves nicely (ie. stabilizes) under Cauchy sequences, and so we can define $v_r(x)$ for $x \in B_I$. As promised, we remind the readers that, once we have a Cauchy sequence $\{x_n\}_n \subseteq A_{\inf}[(p[\varpi])^{-1}]$, there are two parameters: n for the n-th term in the sequence, and $r \in (0, \infty)$ to parametrize the norm $|\cdot|_{p^{-r}}$.

We warn that

(a) as one might have guessed, x_n will from here on denote the n-th term in a Cauchy sequence, as opposed to the x_n in $[x_n]$, the n-th Teichmüller coefficient, and

(b) it might be more justified to write $v(r, x)$ instead of $v_x(r)$ or $v_r(x)$, but the reader should have little trouble understand the notes knowing that they are all the same. We write $v_x(r)$ or $v_r(x)$ mainly to put emphasis on the argument, and nothing more.

Lemma 5.3. *Let $\rho \in (0,1)$, and suppose $\{x_n\}_n \subseteq A_{\text{inf}}[(p[\varpi])^{-1}]$ is Cauchy for $|\cdot|_\rho$ and is not equivalent to* 0*. Write $r = -\log_p \rho \in (0, \infty)$.*

(a) *The sequences $\{v_r(x_n)\}_n, \{\partial_L v_{x_n}(r)\}_n$ and $\{\partial_R v_{x_n}(r)\}_n$ stabilize (in n, as opposed to r), ie. they are independent of n when $n \gg 0$.*

(b) *If $\{y_n\}_n$ is another Cauchy sequence that is equivalent to* 0 *under $|\cdot|_\rho$, then when $n \gg 0$, $v_{x_n}(r) = v_{x_n+y_n}(r)$ and $\partial_? v_{x_n}(r) = \partial_? v_{x_n+y_n}(r)$ where $? \in \{R, L\}$.*

Proof. For part (a), we observe that $v_{x_n}(r)$, as a function of r, is continuous. Using Cauchyness, choose $N \gg 0$ such that for all $n \geq N$, $v_r(x_n - x_N) > v_r(x_N)$. Then for any fixed n, there is a neighbourhood $(r - \varepsilon_n, r + \varepsilon_n)$ of r, such that for any r' in it, we have $v_r(x_n - x_N) > v_r(x_N)$, and so $v_r(x_n) = v_r((x_n - x_N) + x_N) = v_r(x_N)$. Hence the sequence $\{v_r(x_n)\}_n$ stabilizes, and from here it's easy to see $\{\partial_? v_{x_n}(r)\}_n$ stabilize too, since they are determined by $\{v_r(x_n)\}_n$.

For part (b), since $\{y_n\}_n$ is equivalent to 0, this means the y_n has very large valuation when $n \gg 0$, so $v_r(x_n + y_n) = v_r(x_n)$. □

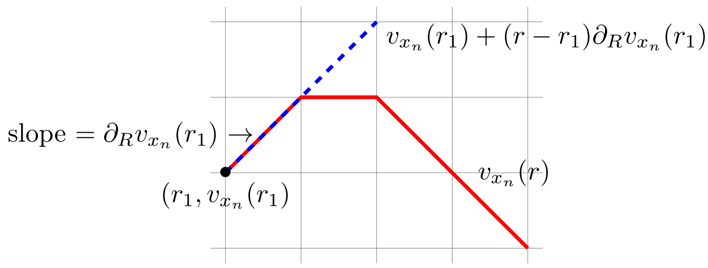
Corollary 5.4. *Suppose $\{x_n\}_n$ is Cauchy for $\{|\cdot|_\rho : \rho \in I\}$, and $\{x_n\}_n$ is not equivalent to* 0 *for some $\rho_0 \in I$. (If $r_0 := -\log_p \rho_0$, this means $\{v_{-\log_p \rho}(x_n)\}$ is bounded above). Then $\{x_n\}_n$ is not equivalent to* 0 *for all norms $\rho \in I$. In other words, if $J \subseteq I$, then the natural map $B_I \to B_J$ is injective.*

Proof. (NEEDS EDITING.) Choose $N \gg 0$ such that $\partial_? v_{x_n}(r_0)$ (where $? \in \{L, R\}$) are stable for $n \geq N$. □

Lemma 5.5. *Let $I = [p^{-r_2}, p^{-r_1}]$ and let $\{x_n\}_n$ be Cauchy for $\{|\cdot|_\rho : \rho \in I\}$. Then there is $N > 0$ such that $v_r(x_n) = v_r(x_N)$ for all $n \geq N$ and all $r \in -\log_p I = [r_1, r_2]$.*

Proof. Using 5.3, choose $M > 0$ such that $\{v_{r_i}(x_n)\}_n$ and $\{\partial_? v_{x_n}(r_i)\}_n$ stabilize for $n \geq M$ and $i \in \{1, 2\}$ and $? \in \{L, R\}$. Recall $v_{x_n}(r)$ is concave as a function on r, and as such, we have

$$\begin{aligned} v_r(x_n) = v_{x_n}(r) &\leq v_{x_n}(r_1) + (r - r_1)\partial_R v_{x_n}(r_1) \dots (\dagger) \\ &= v_{x_M}(r_1) + (r - r_1)\partial_R v_{x_M}(r_1) \text{ due to stability.} \end{aligned}$$



A pictorial depiction of the argument (†).

Since $v_{x_M}(r_1) + (r - r_1)\partial_R v_{x_M}(r_1)$ is a linear function, it must be bounded above by some $A > 0$ that is independent of $r \in [r_1, r_2]$. Now using the Cauchyness of $\{x_n\}_n$ with respect to both r_1

and r_2, choose $N \geq M$ such that for all $n, m \geq N$, we have $v_{r_i}(x_n - x_m) > A$ for $i = 1, 2$. By construction,

(a) on one hand we know that $v_r(x_n - x_m) > A$ for all $r \in [r_1, r_2]$ by concavity of $v_r(x)$ in r, and

(b) on the other hand we have $v_r(x_N) < A$ as discussed.

Hence if $n \geq N$, this forces $v_r(x_n) = v_r((x_n - x_N) + x_N) = v_r(x_N)$, as required. □

Finally we are ready to go to (Step 4).

If $x \in B_I$ where $I \subseteq (0, 1)$ is an interval, then x is represented by a Cauchy sequence $\{x_n\}_n \subseteq A_{\inf}[(p[\varpi])^{-1}]$. We now established that: for any $r \in -\log_p I$, we know $\{v_r(x_n)\}$ and $\{\partial_? v_{x_n}(r)\}_n$ (for $? \in \{L, R\}$) stabilize for $n \gg 0$, and are independent of the choice of the representing Cauchy sequence $\{x_n\}$.

Hence from $x \in B_I$ we obtain a function $v_x : -\log_p I \subseteq (0, \infty) \to \mathbb{R}$, sending $r \mapsto v_x(r)$ (where $v_x(r) = v_{x_n}(r)$ for all $n \gg 0$). Furthermore, v_x has well-defined left and right slopes $\partial_? v_x(r)$ for all $r \in -\log_p I$, even at the boundary points! – even if v_x is undefined (or ill-defined) outside of $-\log_p I$.

Finally, for any compact interval $J \subseteq I$, there is $N > 0$ such that for any $n \geq N$, $v_x = v_{x_n}$ when restricted to $-\log_p J$. In particular, on $-\log_p J$, v_x has integer slopes with finite multiplicities.

(DIAGRAM MISSING)

Now it's only a matter of gluing the compact intervals J together to get an arbitrary interval I. Given $J = [p^{-r_2}, p^{-r_1}]$ and $x \in B_J$, first we extend v_x to the entirety of $(0, \infty)$ (and to $\mathbb{R}$). We define

$$v_x^J : r \mapsto \begin{cases} v_x(r), & r \in [r_1, r_2] \\ v_x(r_1) + \partial_R v_x(r_2)(r - r_2), & r > r_2 \\ v_x(r_1) + \partial_L v_x(r_1)(r - r_1), & r \in (0, r_1) \\ -\infty, & r \leq 0. \end{cases}$$

In this case, we can define $\mathrm{Newt}_J^\circ(x) = \mathcal{L}^{-1}(v_x^J)$. In general where I is an arbitrary interval, we first define v_x^I with the property that $v_x^I |_{-\log_p J} = v_x^J$ for all compact subintervals $J \subseteq I$, and subsequently define $\mathrm{Newt}_I^\circ(x) := \mathcal{L}^{-1}(v_x^I)$.

November 15, 2018. Thursday.

Today we start by paraphrasing what we have established. If $J = [p^{-r_2}, p^{-r_1}] \subseteq (0, 1)$ is a compact interval, and $x \in B_J$, then we have defined v_x^J, which describes the picture on the Gauss side. For such a compact J, we have defined $\mathrm{Newt}_J^\circ(x)$ to be the Newton polygon via $\mathrm{Newt}_J^\circ(x) := \mathcal{L}^{-1}(v_x^J)$.

To extend from a compact interval to a general interval, we can first consider $\mathrm{Newt}_J(x)$, which is the Newton polygon with the lines of slopes^N $0, \infty$ removed. In other words, $\mathrm{Newt}_J(x)$ is essentially the Legendre transform on v_x, before we extended v_x to v_x^J – of course this would not make sense technically since Legendre transform is only defined for functions out of $\mathbb{R}$.

In any case, we have since that if $J \subseteq J'$ are both compact intervals, then $\mathrm{Newt}_J(x) \subseteq \mathrm{Newt}_{J'}(x)$, so for a general interval $I \subseteq (0,1)$, we can do the union or direct limit:

$$\mathrm{Newt}_I(x) := \bigcup_{J \subseteq I \text{ compact}} \mathrm{Newt}_J(x).$$

We also note that $\mathrm{Newt}_I(x)$ have slopes^N lying in $-\log_p I$, for this is true if I is replaced by a compact $J = [p^{-r_2}, p^{-r_1}]$: slopes^N of $\mathrm{Newt}_J(x)$ are break points of v_x, which lie in $[r_1, r_2]$ by definition.

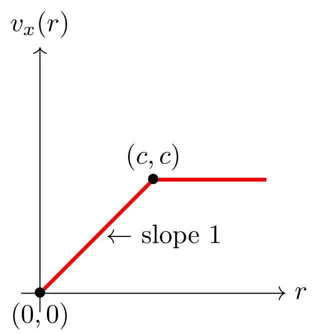
Is it really worthwhile to spend so much time to develop this Newton polygon business? Yes! As we will see, there are a lot of results that we can prove using this, and is really difficult without the Newton polygons.

As a brief diversion, here are our next two goals:

(a) Show that $B := B_{(0,1)}$ is a PID, by studying divisibility questions using the Newton polygon, and

(b) Construct and study the curve $\mathrm{Proj} \oplus B^{\phi = p^d}$.

Anyway, here's a concrete example: if $x = [\varpi] + p$ where $c = v_F(\varpi) > 0$, then v_x sends r to $\min\{r, c\}$ if $r > 0$, and $-\infty$ otherwise (see diagram).



$\mathrm{Newt}_I(x) = \mathcal{L}^{-1} v_x$ is the union of line segments in $\mathrm{Newt}(x)$ of slopes^N λ where $\lambda \in -\log_p I$ (since these are the break points one can see on the interval $-\log_p I$, ignoring break-points at $0, \infty$), and so in this case is empty (more precisely, consists of vertical and horizontal lines only) if $c \notin -\log_p I$.

What does it mean if $\mathrm{Newt}_I(x) = \varnothing$? In fact, this means that x is invertible in $B_I^\times$. Before we prove this, we have to expand our definition of a primitive element.

If $x = \sum_{n=0}^\infty [x_n] p^n \in A_{\mathrm{inf}}$, we say that x is **primitive of degree** 1[48] if

(a) $|x_0|_F < 1$ and $x_0 \neq 0$, and

(b) $x_1 \in \mathcal{O}_F^\times$, or equivalently $|x_1|_F = 1$.

We write Prim_1 for the set of primitive elements of degree 1. Earlier for a primitive element x, we required $|x_0|_F = p^{-1}$, which we used to determine that p has norm p^{-1}, and hence $(A_{\mathrm{inf}}/x)[p^{-1}]$ is a perfectoid field with tilt F. However, there is really no canonical reason why p should have norm p^{-1}, because tilting kills p.

Theorem 5.6. *Let $x \in \mathrm{Prim}_1$, then $(A_{\mathrm{inf}}/x)[p^{-1}]$ is a perfectoid field with tilt F, where $|p| = |x_0|_F$.*

Here's how one should think about Prim_1 elements. Given $x \in \mathrm{Prim}_1$, we can associate x to the *maximal* ideal $\mathfrak{m}_x := (x) \subseteq A_{\mathrm{inf}}[(p[\varpi])^{-1}]$ (maximal since quotient is a field). Then we can ask when its extension $\mathfrak{m}_x B_I$ is still a maximal ideal (in B_I). In fact, by the succeeding proposition (along

[48] In general, we can define $x \in A_{\mathrm{inf}}$ to be primitive of degree d if $|x_i|_F < 1$ for all $i < d$, and $x_0 \neq 0$, and $x_d \in \mathcal{O}_F^\times$.

with the black box that *proper ideals are maximal*), we will see that this is the case precisely when $v_F(x_0) \in -\log_p I$. We will come back to this next lecture.

Proposition 5.7. *If $x \in B_I$, then x is invertible iff* $\mathrm{Newt}_I(x) = \varnothing$.

Proof. In general

Proof of proposition. in general, if $x, y \in B_I$, then check that for any $J \subseteq I$ compact, $v_{xy}^J = v_x^J + v_y^J$ (simply because $v_p(xy) = v_p(x) + v_p(y)$. Hence $\mathrm{Newt}_J(xy) = \mathcal{L}^{-1}(v_x^J + v_y^J)$. since break points of sum = union of break points, this means that slopes of $\mathrm{Newt}_J(xy)$ is the slopes of $\mathrm{Newt}_J(x)$ union slopes of $\mathrm{Newt}_J(y)$. If $xy = 1$, then left hand side is empty (check). So both sets on the right is empty. In general exhaust I with compact Js. This shows only if. (this is not easy without legendre transform, even for A_{inf} elements!)

For if, first assume that $x = \sum_{n \leq N} [x_n] p^n \in A_{\mathrm{inf}}[(p[\varpi])^{-1}]$ with $(N, v_F(x_N))$ a break point of $\mathrm{Newt}(x)$ (equivalently $v_F(x_N) < v_F(x_n)$ for all $n < N$, just check using naive defn of newt), and that $I = [p^{-r_2}, p^{-r_1}]$ is compact. In this case, $x = p^N [x_N](1 + \sum_{n<N} [x_N^{-1} x_n] p^{n-N})$. $p^N[x_N] \in A_{\mathrm{inf}}[(p[\varpi])^{-1}]$. So we must show the bracket term is invertible too. Also add in assumption that all the slopesof $\mathrm{Newt}(x)$ are $> r_2$.

Claim: with these assumptions, for all $r \in [r_1, r_2]$ and all $n < N$, $v_r([x_N^{-1} x_n] p^{n-N}) > 0$. Then $v_r(\sum_{n<N} [x_N^{-1} x_n] p^{n-N}) > 0$ for all $r \in [r_1, r_2]$. So the bracket guy is topologically nilpotent.

November 16, 2018. Friday.

Last time we saw that when given $x \in B_I$, one can associated with it the Newton polygon $\mathrm{Newt}_I(x)$, which unlike the traditional Newton polygon, is not defined wholly on $\mathbb{R}$. We also talked about when to detect whether $x \in B_I$ is invertible:

Proposition (Restatement of 5.7)**.** *For $x \in B_I$, TFAE:*

(a) *$x \in B_I^\times$ is invertible.*
(b) $\mathrm{Newt}_I(x) = \varnothing$.
(c) *For all compact intervals $J \subseteq I$, the pre-Newton polyon* $\mathrm{Newt}_J^\circ(x) = \mathcal{L}^{-1}(v_x^J)$ *has no slopes in the interval $-\log_p J$.*

Recall that $\mathrm{Prim}_d := \{x \in A_{\mathrm{inf}} : x \text{ is primitive of degree } d\}$. We also saw

Theorem (Restatement of 5.6)**.** *If $x \in \mathrm{Prim}_1$, then $K_x := (A_{\mathrm{inf}}/x)[p^{-1}]$ is a perfectoid field with a canonical identification $\mathcal{O}_{K_x}^\flat \xrightarrow{\sim} \mathcal{O}_F$ that is norm compatible if we define $|p|_x = |x_0|_F$, where $|\cdot|_x$ is the natural norm on K_x.*

Today we will talk about how divisibility is encapsulated in Newton polygons. As suggested by the preceding theorem, for $x \in \mathrm{Prim}_1$, we define the **slope of** x to be $-\log_p |p|_x = -\log_p |x_0|_F$.

Theorem 5.8. *Assume F is algebraically closed. If $y \in B_I$ and* $\mathrm{Newt}_I(y)$ *admits a line segment of slope^N λ, then there exists $x \in \mathrm{Prim}_1$ of slope λ such that $x \mid y$ in B_I.*

In other words, any non-primitive element is divisible by a primitive element, or in a greater generality, the slopes^N of $\mathrm{Newt}_I(y)$ say precisely how y *factorizes*.

If $x \in \mathrm{Prim}_1$, then we can associate with it $(x) = \mathfrak{m}_x \in \mathrm{mSpec}\, A_{\mathrm{inf}}[p^{-1}]$. Again, invoking the black box that a proper ideal is maximal in B_I, the theorem then says TFAE:

(a) $\mathfrak{m}_x B_I$ is a maximal ideal;

(b) $x \notin B_I^\times$;

(c) $v_F(x_0) \in -\log_p I$;

(d) the slope^N λ of x satisfies $\lambda \in -\log_p I$.

To conclude, viewing $y \in B_I$ as a function on $\mathrm{mSpec}\, A_{\mathrm{inf}}[p^{-1}]$ via $y(\mathfrak{m}_x) := y \pmod{\mathfrak{m}_x}$, then y has a zero x in $\mathrm{mSpec}\, B_I$ of slope^N λ iff λ is a slope of $\mathrm{Newt}_I(y)$.

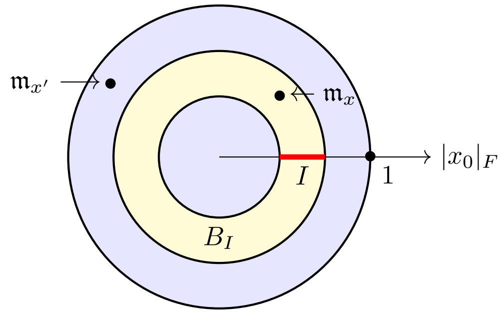


Figure. A depiction of $\mathrm{mSpec}\, A_{\mathrm{inf}}[p^{-1}]$ which contains $\mathrm{mSpec}\, B_I$. B_I only sees the annulus corresponding to the interval I in $\mathrm{mSpec}\, A_{\mathrm{inf}}[p^{-1}]$. The specified point $\mathfrak{m}_x$ represents a maximal ideal in both $A_{\mathrm{inf}}[p^{-1}]$ and $\mathfrak{m}_x B_I \in \mathrm{mSpec}\, B_I$. On the other hand, $\mathfrak{m}_x'$ is maximal in $A_{\mathrm{inf}}[p^{-1}]$ but its extension is no longer proper in B_I. Also note that we have drawn a *closed non-punctured* unit disk rather than an open punctured unit disk, suggesting B_I is still relevant when I includes 0 or 1.

Now we extend the notion of B_I for when I also includes 0 or 1. For $x \in B_I$,

(a) if $0 \in \overline{I}$, we say that $x \in B_{I \cup \{0\}}$ if there is a Cauchy sequence $\{x_n\}$ for all $\{|\cdot|_\rho : \rho \in I\}$ and *for the p-adic norm* and converges to x for all $|\cdot|_\rho, \rho \in I$.

(b) if $1 \in \overline{I}$, then we say $x \in B_{I \cup \{1\}}$ if the same aforementioned criterion is satisfied with the p-adic norm replaced by $|\cdot|_1$ (which is the same as the ϖ-adic norm).

Lemma 5.9. *Suppose $x \in B_I$.*

(a) *If $0 \in \overline{I}$ and $\mathrm{Newt}_I(x)$ is bounded to the left (ie. there is a ∞ slope^N to the left), then $x \in B_{I \cup \{0\}}$.*

(b) *If $1 \in \overline{I}$ and $\mathrm{Newt}_I(x)$ is bounded below, then $x \in B_{I \cup \{1\}}$.*

Proof. (a) If $\mathrm{Newt}_I(x)$ is bounded to the left, then $\mathrm{Newt}_I(p^n x)$ lies strictly in the positive x-axis region for some $n \gg 0$, which means all break points are positive too. Hence before the Legendre transform, $v_x(r)$ only admits positive slopes. (?)

(b) (?)

[[Lemma (i) is equivalent to saying there is $n \geq 0$ such that $\sup_{\rho \to 0^+} |p^n x|_\rho < \infty$. Lemma (ii) is saying $\sup_{\rho \to 1^-} |x|_\rho < \infty$.]]

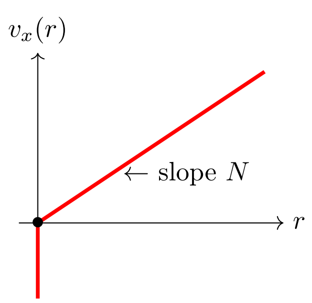
Lemma 5.10. *The ϕ-invariants of B, namely $B^{\phi=1}$, is precisely $\mathbb{Q}_p$.*

Proof. First assume that $x \in A_{\inf}[(p[\varpi])^{-1}]$. Then x is ϕ-invariant precisely when $[x_n^p] = [x_n]$ for all n. For what is the same, $x_n \in \mathbb{F}_p$ for all n, so $x \in \mathbb{Q}_p$.

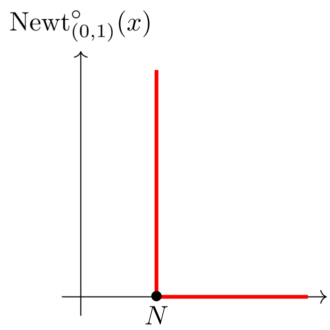
Now suppose $x \in B$ is WLOG nonzero. $\phi(x) = x$ means that for all $r > 0$, we have $v_{\phi(x)}(r) = v_x(r)$. If x is represented by the Cauchy sequence $\{x_n\}_n \subseteq A_{\inf}[(p[\varpi])^{-1}]$, we have $v_{x_n}(r) = v_{\phi(x_n)}(r)$ for $n \gg 0$. Write $y = x_n$ for a moment. Then we have

$$v_y(r) = v_{\phi(y)}(r) = \inf_n\{v_F(y_n^p) + rn\} = p\inf_n\{v_F(y_n) + rn/p\} = pv_y(r/p).$$

Replacing r/p by r, we have $v_y(pr) = pv_y(r)$. Since the y's approximate x, we have $v_x(pr) = pv_x(r)$. This implies v_x is a linear function in r passing through the origin (with extrapolation), or in other words, there is an integer N such that $v_x(r) = Nr$ for all $r > 0$. This then forces 0 to be the only break point of $v_x(r)$.



The graph of $v_x(r)$.



The graph of $\mathrm{Newt}^\circ_{(0,1)}(x)$ after applying $\mathcal{L}^{-1}$.

In particular, since the only slopes^N are 0 and ∞, we can see that x must be invertible too, but this will not be important for us for now.

After applying $\mathcal{L}^{-1}$, we see that the only break point of $\mathrm{Newt}^\circ_{(0,1)}(x)$ must be at N, so in particular the Newton polygon is bounded to the left and below. By 5.9, x can be extended to $B_{[0,1]}$. Now we claim that $B_{[0,1]} = A_{\inf}[(p[\varpi])^{-1}]$.

Indeed, if $y \in A_{\inf}[(p[\varpi])^{-1}]$ is

(a) small in p-adic topology (ie. the first power of p with a nonzero Teichmüller coefficient is large), and
(b) small in 1-norm (or equivalently $[\varpi]$-adic topology) (ie. $\sup_k |x_k|_F$ is small),

then it is also small with respect to all norms $|\cdot|_\rho$ with $\rho \in (0,1)$. Hence $B_{[0,1]}$ is the completion of $A_{\inf}[(p[\varpi])^{-1}]$ with respect to the topology given by the supremum of the 1-norm and the p-adic norm, but $A_{\inf}[(p[\varpi])^{-1}]$ is already complete with respect to the $(p,[\varpi])^{-1}$-adic norm.

Now that we have reduced to the case where $x \in A_{\inf}[(p[\varpi])^{-1}]$, we are done. $\square$

Remark. Following the same argument, we see that if $x \in B$ is invertible, then $x \in A_{\inf}[(p[\varpi])^{-1}]$ and has a Teichmüller representation.

November 19, 2018. Monday.

Our standing assumption from now on will include F being algebriacally closed, and one can usually reduce general statements to ones with this restriction using Galois descent. We won't dwell over it here.

Last time we have seen

Theorem (Restatement of 5.8)**.** *Let $y \in B_I$ and λ is a slope appearing in $\mathrm{Newt}_I(x)$ (hence necessarily $\lambda \in -\log_p I$)). Then there is $x \in \mathrm{Prim}_1$ of slope λ such that $x \mid y \in B_I$.*

Remark. If F is algebraically closed, then given $x \in \mathrm{Prim}_1$, we can assume $x = [\varpi] - p$ for some $\varpi \in \mathfrak{m}_F - \{0\}$, up to multiplying by $A_{\mathrm{inf}}^\times$. (Why not clear?) For this, it suffices to show that if (x) contains some element of the form $[\varpi] - p$. Indeed, $\Theta_x : A_{\mathrm{inf}} \to \mathcal{O}_{K_x}$ takes $[\beta]$ to $\beta^\sharp$, where if we write $\beta = (\beta^{(n)})_{n \geq 0}, \beta^{(n)} \in \mathcal{O}_{K_x}$ and $(\beta^{(n)})^p = \beta^{(n-1)}$. Then $\beta^\sharp = \beta^{(0)}$. So it's enough to show that there is $(\varpi^{(n)})$ with $\varpi^{(0)} = p$. But this is right, because F is algebraically closed, so K_x is algebraically closed, and such a sequence exists (we are simply taking p-th roots over and over again).

(Side discussion. $x \in \mathrm{Prim}_1$ is in bijection with $(K_x, |\cdot|_x)$, when we also remember the norm on the untilt.)

We have also seen

Lemma (Restatement of 5.9)**.** *$x \in B$ such that $\mathrm{Newt}_{(0,1)}(x)$ is bounded to the left and below, then $x \in A_{\mathrm{inf}}[(p[\varpi])^{-1}]$.*

This yields three consequences:

(a) $B^{\phi=1} = \mathbb{Q}_p$. We have seen this in 5.10.

(b) The units in $B = B_{(0,1)}$ lie in $A_{\mathrm{inf}}[(p[\varpi])^{-1}]$. In other words, $B^\times = A_{\mathrm{inf}}[(p[\varpi])^{-1}]^\times$.
Proof. $x \in B^\times$ iff $\mathrm{Newt}_{(0,1)}(x) = \varnothing$, and use 5.9. □

(c) If $d < 0$, then $B^{\phi=p^d} = 0$.
Proof. Let $x \in B^{\phi=p^d} - \{0\}$ (for any d) then $\phi(x) = p^d x$ by definition. As in the proof of 5.9, for $r \in (0, \infty)$, we have $v_r(\phi(x)) = pv_{r/p}(X)$. Replacing r by pr, we have $v_{pr}(p^d x) = pv_r(x)$. Hence (with approximation by elements in $A_{\mathrm{inf}}[(p[\varpi])^{-1}]$ omitted)

$$\begin{aligned} pv_x(r) = pv_r(x) = v_{pr}(p^d x) &= \inf_n \{v_F(p^d x_n) + prn\} \\ &= \inf_n \{v_F(x_{n-d}) + prn\} \\ &= \inf_n \{v_F(x_n) + prn + prd\} = prd + v_{pr}(x) = prd + v_x(pr). \end{aligned}$$

Now one can check that if $d < 0$, then $x \notin B^\times$. So suppose λ is a break point of right slope N, then $p\lambda$ is also a break point with right slope $N - d$ (one can check this using differentiation, ignoring some technnicalities).

Using duality between break points and slopes, now we know λ is a slope^N of $\mathrm{Newt}_{(0,1)}(x)$, which appears at the break point N; and $p\lambda$ is a slope^N which appears at the break point $N - d$. If $d > 0$, then $\lambda \neq 0$, because it cannot have right slopes N and $N - d$ simultaneously, and $p\lambda > \lambda$, but $N - d > N$, contradicting $\mathrm{Newt}_{(0,1)}(x)$ being a decreasing convex hull. □

Remark. One can see using this argument that if $x \in B^{\phi=p^d} - \{0\}$ where $d > 0$, then in $\mathrm{Newt}_{(0,1)}(x)$, the slopes^N of x must approach ∞ on the left. This is another glimpse of the slogan that Newton polygons give useful information about $x \in B$ where one cannot deduce otherwise.

5.3. Formalisms of "curves".

We define the graded algebra

$$P_F = \bigoplus_{d \geq 0} B^{\phi=p^d}.$$

Recall that F is the underlying perfectoid field. We wish to study P_F, which we will do so formally in a general setting.

Our setup will be as follows: suppose we have a graded algebra $P = \bigoplus P_d$ with the following properties:

(A1) $P_0 = K$ is a field. (In our case $(P_F)_0 = \mathbb{Q}_p$.)
(A2) $\bigcup_{d \geq 0}(P_d - \{0\})/K^\times$ is a monoid is freely generated by $(P_1 - \{0\})/K^\times$. (Something about Picard group being trivial.)
(A3) For all $t \in P_1 - \{0\}$, there is a field extension C_t/K such that

$$P/tP = D_t := \{f(T) \in C_t[T] : f(0) \in K\}$$

as graded algebras. (In our case C_t is the untilt of F.)

The polynomial ring in 2 variables $K[x, y]$ shall satisfy these conditions, for example.

Theorem 5.11. *Let* $X = \mathrm{Proj}(P)$. *Then*

(a) *for all* $t \in P_1 - \{0\}$, $\mathrm{Proj}(P/t) \cong \mathrm{Spec}\, C_t$. [49]
(b) *for all* $t \in P_1 - \{0\}$, $B_t = (P[t^{-1}])_0$ *is a PID.*
(c) X *is a Dedekind scheme with* $H^0(X, \mathcal{O}_X) = K$ *and* $H^1(X, \mathcal{O}_X) = 0$, *and for all* $f \in K(X)$, *we have*

$$\sum_{\infty_t} \mathrm{ord}_{\infty_t}(f) = 0$$

where $|X|$ *is the set of closed points.*
(d) $(P_1 - \{0\})/K^\times \xrightarrow{\sim} |X|$ *by* $\xi_t : t \mapsto \infty_t$.

Proof. First let us recall the Proj construction. If $Q = \bigoplus Q_d$ is any graded algebra, then as a set we have

$$\mathrm{Proj}(Q) = \{\text{homogeneous primes } \mathfrak{P} \subseteq Q \text{ not containing the irrelevant ideal}\},$$

and its structure as a scheme is described by

$$\mathrm{Proj}(Q) = \bigcup_{f \in Q_d, d > 0} \mathrm{Spec}(Q[f^{-1}])_0.$$

By (A3), one has $\mathrm{Proj}(P/t) = \mathrm{Proj}(D_t) \supseteq \mathrm{Spec}((D_t[T^{-1}])_0)$. We observe that $(D_t[T^{-1}])_0 \xrightarrow{\sim} C_t$. This gives the first inclusion. To finish (a), it now suffices to show that the only nonzero homogeneous prime ideal of D_t is $TC_t[T]$.

[49] This is saying that any divisor cuts out a degree 0 variety, which reinforces the idea that $\mathrm{Proj}(P)$ is a curve.

Suppose $\mathfrak{P}$ is such an ideal. Clearly $\mathfrak{P} \subseteq TC_t[T]$: if $p(t) \in \mathfrak{P}$ has nonzero constant term, then there must be at least one (homogeneous) generator that is a constant, but this would mean $\mathfrak{P}$ is the unit ideal. Now suppose aT^i is a generator of $\mathfrak{P}$ with minimal degree. We can multiply by $a^{-1}T \in D_t$, regardless of whether $a \in K$ or not, to get T^{i+1} in $\mathfrak{P}$, and we are home.

We will continue the proof next lecture.

November 26, 2018. Monday.

Proof of 5.11 continued. Last time we completed the proof of part (a), so we will proceed to part (b) now. We will show a stronger statement, that if $t \in P_1 - \{0\}$, then $B_t = (P[t^{-1}])_0$ is a PID with irreducible elements $\{x/t : x \in P_1 - Kt\}$.

By definition, $B_t = \{y/t^d : y \in P_d\}$. Recall that for $x \in P_1 - \{0\}$, we define $D_x := \{f(T) \in C_x[T] : f(0) \in K\}$. By assumption, the identification in (A3) $\xi_x : P/xP \to D_x$ preserves the degree 1 piece, thus maps $t \mapsto \alpha T$ where $\alpha \in C_x - \{0\}$. Inverting t, along with the fact that B_t only records degree zero elements, we see that $\xi_x : B_t/(x/t)B_t \xrightarrow{\sim} D_x[T^{-1}]_0$, and degree zero elements in $D_x[T^{-1}]$ are precisely C_x.

Since B_t quotiented by x/t gives a field, (x/t) is a maximal ideal. (Not entirely sure how to finish it.)

Up till this point, we know that X is a Dedekind scheme, and the set of closed points $|X| = \{\infty_t : t \in P_1 - \{0\}\}$, where $\{\infty_t\} = \mathrm{Proj}(P/tP)$.

Given $t \in P_1 - \{0\}$, we define $\deg_{\infty_t} : K(X) \to Z_{\geq 0} \cup \{\infty\}$, sending $f \mapsto -\mathrm{ord}_{\infty_t} f$. This is well-defined since we are working in a PID, so the term ord_{∞_t} makes sense. More explicitly, if $f = t^d y_1/y_2$ where $t \nmid y_1, y_2$, then $\deg_{\infty_t}(f) = -d$. Since f has the same degree for its numerator and denominator, we have $\sum_{\infty_t \in |X|} \deg_{\infty_t}(f) = 0$.

To finish off (c), we must show that $H^0(X, \mathcal{O}_X) = K$ and $H^1(X, \mathcal{O}_X) = 0$. So far we have been using the projective line as the intuition for such formalisms, in which case these two criteria on cohomologies are satisfied, but we can also do better and say that $H^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(-1)) = 0$. It will not be true in this generality, and is the fundamental difference.

Anyway, write the open set $U_t := \operatorname{Spec} B_t$ for a fixed $t \in P_1 - \{0\}$. Write $j : U_t \to X$ and $i : \{\infty_t\} \hookrightarrow X$. Then we have an exact sequence of sheaves

$$0 \to \mathcal{O}_X \to j_*\mathcal{O}_{U_t} \to j_*\mathcal{O}_{U_i}/\mathcal{O}_X \to 0.$$

But the last term is concentrated at ∞_t, so it's simply $i_*(K(X)/\mathcal{O}_{X,\infty_t})$. Taking the long exact sequence, with the fact that U_t is affine, we have

$$0 \to H^0(X, \mathcal{O}_X) \to B_t \to K(X)/\mathcal{O}_{X,\infty_t} \to H^1(X, \mathcal{O}_X) \to 0.$$

Hence now it remains to show that $H^0(X, \mathcal{O}_X) = B_t \cap \mathcal{O}_{X,\infty_t}$, and that $H^1(X, \mathcal{O}_X) = K(X)/(B_t + \mathcal{O}_{X,\infty_t}) = 0$, or equivalently $K(X) = B_t + \mathcal{O}_{X,\infty_t}$.

Let's write down explicitly that

$$\begin{aligned} B_t &= \{y/t^d : y \in P_d\} \\ K(X) &= \{y_1/y_2 : y_1, y_2 \in P_d \text{ and } y_2 \neq 0\} \\ \mathcal{O}_{X,\infty_t} &= \{y_1/y_2 : y_1, y_2 \in P_d \text{ and } y_2 \neq tP\}. \end{aligned}$$

Staring at these descriptions, it's not hard to see that $H^0(X.\mathcal{O}_X) = K$. $H^1(X.\mathcal{O}_X) = 0$ essentially comes from partial fractions. This finishes the proof. $\square$

Why did we switch from ord_{∞_t} to $\deg_{\infty_t}$? How should one think about $K(X) = B_t + \mathcal{O}_{X,\infty_t}$? This says that if $f \in KX()$, then there exists $b \in B_t$ such that $\deg_{\infty_t}(f - b) \leq 0$. If we write $f = a_1/a_2$ where $a_1, a_2 \in B_t$, then we have $\deg_{\infty_t}(a_1/a_2 - b) \leq 0$, or equivalently

$$\deg_{\infty_t}(a_1 - ba_2) \leq \deg(a_2).$$

As such, we call B_t *pseudo-Euclidean.* The adjective pseudo is due to the fact that one would expect a strict inequality for an Euclidean domain. Had B_t be *Euclidean*, then this would be equivalent to saying $K(X) = B_t + \mathfrak{m}_{X,\infty_t}$, or that $H^1(X, \mathcal{O}_X(-\infty_t)) = 0$ (but this is false anyway in our general setting).

Let's go on a short diversion on line bundles, that will be crucial for what is upcoming: since B_t is a PID for all t, we have $\mathrm{Pic}(U_t) = 0$, and the degree map $\deg : \mathrm{Pic}(X) \to \mathbb{Z}$ sends a line bundle $\mathcal{L} \mapsto \sum_{\infty_t} \mathrm{ord}_{\infty_t}(s)$ where s is any section of the line bundle. This has an inverse $m \mapsto \mathcal{O}_X(m\infty_t)$. One can check that $\mathcal{O}_X(m\infty_t) = \widetilde{P[m]}$, where $P[m]$ is the shifted graded P-module with $P[m]_d = P_{m+d}$.

To conclude the lecture, let us talk about where we are headed. Let's write $P_{\mathbb{Q}_p} = \bigoplus_{d \geq 0} B^{\phi = p^d}$. We will also consider the graded algebras

$$P_{\mathbb{Q}_{p^r}} = \bigoplus_{d \geq 0} B^{\phi^r = p^d} \text{ where } r \geq 1.$$

In fact, $X_r := \mathrm{Proj}\, P_{\mathbb{Q}_{p^r}}$ still satisfies properties (A1,2,3).

There is a natural map from $P_{\mathbb{Q}_p} \to P_{\mathbb{Q}_{p^r}}$ sending $a \in B^{\phi = p^d}$ to $a \in B^{\phi^r = p^{dr}}$. This map acts like the Veronese map. This natural map induces a map after taking Proj, and thus we get an inverse system $\{X_r\}_{r \geq 1}$.

Write $X = X_1$. Then in fact, $X_r \cong \mathbb{Q}_{p^r} \otimes_{\mathbb{Q}_p} X$, and $\mathrm{Pic}(X_r) \cong \mathbb{Z}$ for every r. Write the map $\pi_r : X_r \to X$, and in fact this map is finite and étale.

Define $\mathcal{O}_X(d, r) := \pi_{r,*}\mathcal{O}_{X_r}(d)$, which is a rank r vector bundle. We define for $\lambda = d/h \in \mathbb{Q}$ in lowest terms that $\mathcal{O}_X(\lambda) = \mathcal{O}_X(d, h)$, then a main result in p-adic hodge theory says that every vector bundle E on X is of the form $E = \bigoplus_\lambda \mathcal{O}_X(\lambda)$ for $\lambda \in \mathbb{Q}$. This result indeed requires the algebraically closed assumption on the perfectoid field F.

November 28, 2018. Wednesday.

As briefly mentioned last time, today we will consider, for $r \geq 1$, the graded algebra

$$P_{\mathbb{Q}_{p^r}} := \bigoplus_{d \geq 0} B^{\phi^r = p^d},$$

and write $X_r = \mathrm{Proj}(P_{\mathbb{Q}_{p^r}})$ and $X := X_1$. Note that we have $\mathbb{Q}_{p^r} = W(\mathbb{F}_{p^r})[1/p] \hookrightarrow A_{\mathrm{inf}}[1/p] \hookrightarrow B$ so we can define the map

$$B^{\phi = p^d} \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^r} \to B^{\phi^r = p^{dr}}, \text{ sending } x \otimes a \mapsto ax.$$

One can check that this is an isomorphism, hence $X_r \cong X \otimes_{\mathbb{Q}_p} \mathbb{Q}_{p^r}$.

Today we will show that these graded rings have the desired property (A2).

Theorem 5.12. $\bigcup_{d \geq 0} (B^{\phi^r = p^d})/\mathbb{Q}_{p^r}^\times$ *is freely generated by the degree* 1 *elements* $(B^{\phi^r = p} - \{0\})/\mathbb{Q}_{p^r}^\times$.

Remark. We saw that $B^{\phi = p^d} = 0$ if $d < 0$ and equals $\mathbb{Q}_p$ if $d = 0$. In fact, the same argument will imply that $B^{\phi^r = p^d} = 0$ if $d < 0$ and equals $\mathbb{Q}_{p^r}$ if $d = 0$. Moreover, every maximal ideal of B is of the form $\mathfrak{m}_x = (x)$ with $x \in A_{\mathrm{inf}}$ primitive of degree 1. We also showed that in fact one can take x to be of the form $[x_0] - p$ where $x_0 \in \mathfrak{m}_F$.

The idea of the proof will be to identify the graded algebra P with a graded monoid, that will be obviously freely generated by the degree 1 elements.

Let us first define a few terminologies. Define

$$\widetilde{\mathrm{Div}^+} = \left\{ \sum_{\mathfrak{m}_x \in \mathrm{mSpec}\, B} a_x [\mathfrak{m}_x] : \begin{array}{l} (1) \text{ (effectiveness condition) } a_x \in \mathbb{Z}_{\geq 0}, \\ (2) \text{ (local finiteness condition) for every compact} \\ \quad \text{interval } I \subseteq (0,1), \text{ there exists finitely many } \mathfrak{m}_x \\ \quad \text{with slopes in } -\log_p I \text{ with } a_x \neq 0. \end{array} \right\}.$$

We remark with caution that there's no requirement on an element in $\widetilde{\mathrm{Div}^+}$ being a finite sum: we merely require that it's a finite sum *when restricted to a compact interval.* In addition. there is a natural action of ϕ on $\widetilde{\mathrm{Div}^+}$, (induced by) sending $\mathfrak{m}_x$ to $\mathfrak{m}_{\phi(x)}$. Next we define

$$\mathrm{Div}^+(X_r) := \{D \in \widetilde{\mathrm{Div}^+} : D = \phi^r(D)\}.$$

the subset of *divisors* invariant under ϕ^r. Eventually we will see that we can identify $\mathrm{Div}^+(X_r)$ with the effective divisors on X_r, thus justifying the notation.

Lemma 5.13. (a) *If* $b \in B$ *is nonzero, then* $\mathrm{Div}(b) := \sum_{\mathfrak{m}_x} \mathrm{ord}_x(b)[\mathfrak{m}_x]$ *is in* $\widetilde{\mathrm{Div}^+}$.

(b) *If* $b \in B^{\phi^r = p^d}$ *is nonzero, then* $\mathrm{Div}(b) \in \mathrm{Div}^+(X_r)$.

Proof. (a) If I is a compact interval, then the ideal (b) is principal in B_I, and both conditions for $\widetilde{\mathrm{Div}^+}$ follow immediately. (b) The statement simply boils down to $\phi^r(b) = p^d b$ implying $\mathrm{Div}(\phi^r(b)) = \mathrm{Div}(b)$. $\square$

Let us recall again that we are working with the assumption where F is algebraically closed, or one can simply assume that $F = \widehat{\overline{\mathbb{Q}_p}}^\flat = \mathbb{C}_p^\flat$.

Proposition 5.14. *The map*

$$\bigcup_{d\geq 0}(B^{\phi^r=p^d}-\{0\})/\mathbb{Q}_{p^r}^\times \to \mathrm{Div}^+(X_r) \textit{ sending } z\mapsto \mathrm{Div}(z)$$

is an isomorphism of monoids.

Remark. This is not true if F is not algebraically closed, in which case $\mathrm{Pic}(X_r)\neq\mathbb{Z}$, and there are irreducible elements not of degree 1.

Proof. First we show injectivity. Let $z_1\in B^{\phi^r=p^{d_1}}-\{0\}$ and $z_2\in B^{\phi^r=p^{d_2}}$ with $d_2\geq d_1$ and $\mathrm{Div}(z_1)=\mathrm{Div}(z_2)$. Restricting to any compact interval I, over B_I, z_2 can only differ from z_1 by a unit, and so the same must still hold in B. Writing $z_1=uz_2$ for $u\in B^\times$, we have $u\in B^{\phi^r=p^{d_1-d_2}}$. Since $d_1-d_2\leq 0$ and u is a unit, this forces $d_1=d_2$ (recall that if $d<0$, then $B^{\phi^r=p^d}=\{0\}$). But $B^{\phi^r=1}=\mathbb{Q}_{p^r}^\times$, so we are done. Note that up until this point we still have not used the assumption that F is algebraically closed.

Next we show surjectivity, which is the hard part of the proposition. First we make an observation: fix an $\mathfrak{m}_x(=(x)$ where $x\in\mathrm{Prim}_1)$ and consider $D_x:=\sum_{n\in\mathbb{Z}}\phi^{nr}([\mathfrak{m}_x])$, to which we claim lies in $\mathrm{Div}^+(X_r)$. By construction it satisfies ϕ^r-invariance and the effectiveness condition. For the local finiteness condition, consider the interval $J=(\rho^{p^r},\rho]$. If $|p|_x\in J$, then $|p|_{\phi^{nr}(x)}\notin J$ for any $n\neq 0$. Since any compact interval $I\subseteq(0,1)$ can be covered up by finitely many such J's, this gives the local finiteness condition, and subsequently our claim.

Our next step is to observe that $\mathrm{Div}^+(X_r)$ is freely generated by $\{D_x:\mathfrak{m}_x\in\mathrm{mSpec}(B)\}$. This is obvious essentially from definition of $\mathrm{Div}^+(X_r)$.

Now the third step is to identify degree 1 elements in $B^{\phi^r=p}$ with the generators $\{D_x\}$. More precisely, we show that there is $t_x\in B^{\phi^r=p}$ such that $\mathrm{Div}(t_x)=D_x$, which we prove by showing that there are t_x^+ and t_x^- responsible for the positive and negative shiftings of $[\mathfrak{m}_x]$ by ϕ^r respectively.

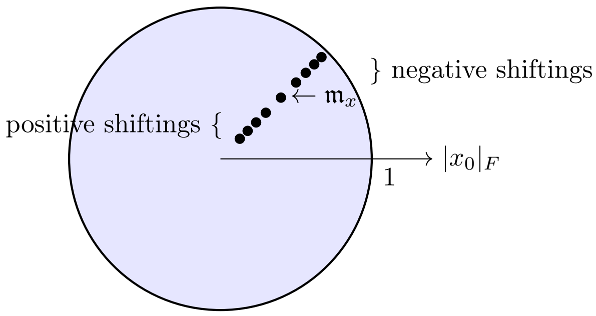


Figure. We separate the construction of t_x into t_x^+ and t_x^-.

By replace x by $-x$ if necessary, we assume $x=p-[x_0]$. The positive part is straightforward: we consider the infinite product $t_x^+=\prod_{n\geq 0}(\phi^{rn}(x)/p)$ along with some tweaking for convergence issues, to which we claim it converges in B. To see this, we first note that $\prod_{n\geq 0}(\phi^{rn}(x)/p)=\prod_{n\geq 0}(1-[x_0^{p^{rn}}]/p)$. To see the product converges, it suffices to see that $\lim|[x_0^{p^{rn}}]/p|_\rho=0$, and indeed we have $|[x_0^{p^{rn}}]/p|_\rho=\rho^{-1}|x_0|_\rho^{p^n}$. By construction we then have $\mathrm{Div}(t_x^+)=\sum_{n\geq 0}[\phi^{rn}(\mathfrak{m}_x)]$.

Finally, now we have in fact $\phi^r(t_x^+) = (p/x)t_x^+$, so it remains to show there is $t_x^- \in A_{\rm inf}$, unique up to $\mathbb{Q}_{p^r}^\times$, such that $\phi^r(t_x^-) = xt_x^-$, then $t_x := t_x^+ t_x^-$ will be pt_x and do the job. However as one might expect now, the naïve guess $t_x^- = \phi^{-r}(x)\phi^{-2r}(x)\cdots$ does not converge, so we will need something more clever.

November 29, 2018. Thursday.

Today we will continue to prove the surjevtivity of the divisor map. Let's recall the

Lemma. *For all* $x = [x_0]-p \in \mathrm{Prim}_1$*, there is* $t_x \in B^{\phi^r=p}$ *such that* $\mathrm{Div}(t_x) = D_x = \sum_{n\in\mathbb{Z}}[\phi^{nr}(\mathfrak{m}_x)]$.

We have constructed the *plus part* $t_x^+ = \prod_{n\geq 0}(\phi^{nr}(x)/p)) \in B$ which satisfies $\phi(t_x^+) = (p/x)t_x^+$ and $\mathrm{Div}(t_x^+) = D_x^+ = \sum_{n\geq 0}[\phi^{nr}(\mathfrak{m}_x)]$. Today we will start by proving there is $t_x^- \in A_{\rm inf}$, unique up to $\mathbb{Q}_{p^r}^\times$ (or equivalently $\mathbb{Z}_{p^r}^\times$), such that $\phi^r(t_x^-) = xt_x^-$. To do so, we will construct $\{b_n\}_n \subseteq A_{\rm inf}$ such that

(a) $b_n \equiv b_{n-1} \pmod{p^n}$, and
(b) $\phi^r(b_n) \equiv xb_n \pmod{p^{n+1}}$.

Then t_x^- can be defined as the p-adic limit of b_n in $A_{\rm inf}$.

For b_0, we simply need b_0 to be such that $\phi^r(b_0) \equiv xb_0 \pmod p$, or equivalently $b_0^{p^r} \equiv [x_0]b_0 \pmod p$, or again equivalently $b_0^{p^r-1} \equiv [x_0] \pmod p$. Hence we can simply take $b_0 = [x_0^{1/(p^r-1)}]$, which is well-defined up to (p^r-1)-th roots of unity, all of which convenient lie in $\mathbb{F}_{p^r}^\times$.

We then move onto the inductive step. Suppose we have found $b_0, \ldots, b_{n-1}$. We wish to take $b_n = b_{n-1} + p^n z_n$ where z_n is to be determined. Given $\phi^r(b_{n-1}) \equiv xb_{n-1} \pmod{p^n}$, we can write $\phi^r(b_{n-1}) - xb_{n-1} = p^n y$ for some $y \in A_{\rm inf}$.

Then we have

$$\begin{aligned}\phi^r(b_n) - xb_n &= \phi^r(b_{n-1}) + p^n\phi^r(z_n) - xb_{n-1} - p^n xz_n \\ &= p^n y + p^n(\phi^r(z_n) - xz_n) \\ &= p^n(y + \phi^r(z_n) - xz_n).\end{aligned}$$

Hence we need to pick z_n such that $\phi^r(z_n) - xz_n + y \equiv 0 \pmod p$, or equivalently $z_n^{p^r} - [x_0]z_n + y \equiv 0 \pmod p$. Write $\overline{y} = y \pmod p$. Using the algebraically closed condition of F, the polynomial $T^{p^r} - x_0T + \overline{y}$ has a root $\overline{z} \in \mathcal{O}_F$, so we can take $z_n = [\overline{z}]$ and we are done.

Here's the heuristic idea: though the infinite product $\phi^{-r}(x)\phi^{-2r}(x)\cdots$ does not exist literally, we exploited the fact that this element is characterized by a functional equation, to which the solution exists.

Now it remains to show that our candidate chosen this way indeed does the job, that $\mathrm{Div}(t_x^-) = D_x^- := \sum_{n<0}[\phi^{nr}(\mathfrak{m}_x)]$.

Let's write $D' = \mathrm{Div}(t_x^-)$. By construction we know that $\phi^r(t_x^-) = xt_x^-$, and hence on level of *divisors* $\mathrm{Div}(x) + D' = \phi^r(D')$. Hit this with ϕ^{-r} to get

$$\phi^{-r}(\mathrm{Div}(x)) + \phi^{-r}(D') = D'.$$

Self iterate this relation to see that for any k, we have

$$\sum_{n=1}^{k}[\phi^{-nr}(\mathfrak{m}_x)] + \phi^{-kr}(D') = D'.$$

Here's where the magic happens: since $t_x^- \in A_{\text{inf}}$, we have great understanding of its Newton polygon. By definition $\text{Newt}(t_x^-)$ is bounded to the left by the y-axis, and bounded below by the horizontal line $y = v_0(t_x^-) = -\log_p|t_x^-|_1$. Hence there is an upper bound on $\{\text{slopes}^N \text{ of Newt}(t_x^-)\}$. Since the slopes^N of $\text{Newt}(t_x^-)$ governs the factorization of t_x^-, we conclude that there is a lower bound to how close a factor of t_x^- can be located towards the origin on the punctured disk.

However, for any compact interval $I \subseteq (0,1)$, there is $k \gg 0$ such that $\phi^{-kr}(D')$ is not supported at any point with slope in $-\log_p I$, since applying ϕ^{-r} pictorially pushes D' towards the boundary and eventually outside of any fixed compact annulus.

Let's concretize this by defining a notation. For $D = \sum a_x[\mathfrak{m}_x] \in \widetilde{\text{Div}}^+$, we set

$$D|_I = \sum_{\text{slope of } x \in -\log_p I} a_x[\mathfrak{m}_x].$$

Then our discussions is saying that $\phi^{-nr}(D')|_I$ is eventually 0 for any compact interval $I \subseteq (0,1)$. So for any compact interval I, there is $k \gg 0$ such that $\sum_{n=1}^k[\phi^{-kr}(\mathfrak{m}_x)] \mid_I = D'|_I$. The same reasoning now gives $\sum_{n=1}^k[\phi^{-nr}(\mathfrak{m}_x)] \mid_I = D_x^-|_I$. So for all compact I, we have $D_x^-|_I = D_x|_I$.

Now of course, combining everything together, we see that if $t_x := t_x^+ t_x^- \in B^{\phi^r = p}$, then $\text{Div}(t_x) = D_x^+ + D_x^- = D_x$. This completes the proof that

$$\text{Div} : \bigcup_{d \ geq 1} (B^{\phi^r = p^d} - \{0\})/\mathbb{Q}_{p^r}^\times \to \text{Div}^+(X_r)$$

is an isomorphism, and in particular, the LHS is freely generated by degree 1 elements. □

Next let us fix $x = [x_0] - p \in \text{Prim}_1$, which gives an untilt $K_x = A_{\text{inf}}[p^{-1}]/(x)$ of F. This then gives a map $\Theta_x : A_{\text{inf}}[p^{-1}] \to K_x$.

Lemma 5.15. *Θ_x extends to a map $\Theta_x : B \to K_x$. Equivalently, $\Theta_x : A_{\text{inf}}[p^{-1}] \to K_x$ is continuous for all Gauss norms $|\cdot|_\rho$ for $\rho \in (0,1)$.*

Proof. First note that Θ_x is defined by $\Theta_x(\sum_{n \gg -\infty}[z_n]p^n) = \sum_{n \gg -\infty} z_n^\sharp p^n$. Then $|\sum[z_n]p^n|_\rho < \varepsilon$ and $|\sum z_n^\sharp p^n| < \varepsilon$ are easily equivalent since $|z_n^\sharp| = |z_n|_F$. □

We will see next time that the restricted map $\Theta_x : B^{\phi^r = p^d} \to K_x$ has kernel $t_x B^{\phi^r = p^{d-1}}$, and in particular $P_r/t_x P_r \xrightarrow{\sim} \{f(T) \in K_x[T] : f(0) \in \mathbb{Q}_{p^r}\}$. In addition, for the case $d = 1$, we get a short exact sequence

$$0 \to \mathbb{Q}_{p^r} \xrightarrow{t_x} B^{\phi^r = p} \to K_x \to 0,$$

which is referred to as the *fundamental short exact sequence* in p-adic hodge theory.

Dec 3, 2018. Monday.

Let's summarize our progress so far.

So far we have been assuming that $F = K^\flat$ is algebraically closed. We are interested in $X_r = \mathrm{Proj}(P_{\mathbb{Q}_{p^r}})$, where $P_{\mathbb{Q}_{p^r}}$ is the graded algebra $\bigoplus_{d\geq 0} B^{\phi^r=p^d}$. This Proj construction satisfies the axioms (A1-3) for a *curve* over $K = \mathbb{Q}_p$ (see 5.3). Restating under our setting, we have showed that

(A1) $B^{\phi^r=1} = \mathbb{Q}_{p^r}$,

(A2) $\bigcup_{d\geq 1}(B^{\phi^r=p^d} - \{0\})/\mathbb{Q}_{p^r}^\times$ is freely generated by the degree 1 part $(B^{\phi^r=p} - \{0\})/\mathbb{Q}_{p^r}^\times$, and

(A3) for $t \in B^{\phi^r=p}$, we have $P_{\mathbb{Q}_{p^r}}/tP_{\mathbb{Q}_{p^r}} \cong \{f(T) \in K_x[T] : f(0) \in \mathbb{Q}_{p^r}\}$, where $x \in \mathrm{Prim}_1$ is such that/obtained by

   (a) first considering the image of t under the Div map: $\mathrm{Div}(t) = \sum_{n\in\mathbb{Z}}[\phi^{rn}(\mathfrak{m}_x)] \in \mathrm{Div}^+(X_r)$,

   (b) and then looking at the untilt $A_{\mathrm{inf}}[p^{-1}]/\mathfrak{m}_x$ where $\mathfrak{m}_x = (x)$.

We remark that such an x requires a choice of $\mathfrak{m}_x$, and hence $\mathfrak{m}_x$ is determined only up to a ϕ^r-translate. Even if a specific $\mathfrak{m}_x$ is chosen, x, being the generator of $\mathfrak{m}_x$, is still not unique.

We make a few observations in particular:

(a) $|X_r|$, the set of closed points of X_r, is in bijection with $(B^{\phi^r=p} - \{0\})/\mathbb{Q}_{p^r}^\times$, via the map $(V^+(t) \subseteq X_r) \leftarrow\!\shortmid [t]$. (This is essentially summarizing the proof of (A3).)

(b) X_r is a Dedekind scheme, with $H^0(X_r, \mathcal{O}_{X_r}) = \mathbb{Q}_{p^r}$, and $H^1(X_r, \mathcal{O}_{X_r}) = 0$. (See November 26.)

(c) There is a (trivial) degree function on $|X|$, with $\deg(x) = 1$ for all points x, and such that for all $f \in K(X)$, $\sum_{y\in|X|}\mathrm{ord}_y(f)\deg(y) = 0$. (See November 26.)

(d) The Picard group of X_r is generated by a point and so $\mathrm{Pic}(X_r) \cong \mathbb{Z}$. (?)

Last lecture we ended with a glimpse of the fundamental short exact sequence, and this time we will prove it. Fixing a pair of choices t and x, we saw that the map $\Theta_x : A_{\mathrm{inf}} \to K_x$ can be extended to $B \to K_x$.

Proposition 5.16. *For all $d \geq 1$, we have a short exact sequence*

$$0 \to B^{\phi^r=p^{d-1}} \xrightarrow{\cdot t} B^{\phi^r=p^d} \xrightarrow{\Theta_x} K_x \to 0.$$

Proof. First we prove exactness in the middle. Suppose $z \in B^{\phi^r=p^d}$, then

$$\begin{aligned}\Theta_x(z) = 0 \text{ iff } &[\mathfrak{m}_x] \text{ appears in } \mathrm{Div}(z) \text{ with nonzero coefficient}\\ &\text{iff } \mathrm{Div}(t) = \sum[\phi^{nr}(\mathfrak{m}_x)] \text{ appears as a summand in } \mathrm{Div}(z)\\ &\text{iff } t \mid z.\end{aligned}$$

Now it remains to show surjectivity on the right, for which it's enough to consider the $d = 1$ case, since if $1 \in K_x$ has preimage $z \in B^{\phi^r=p}$, then by multiplying with suitably large power of z, one can prove the surjectivity for any d. Though we will not prove the surjectivity here, let us make two remarks:

(a) The surjectivity does not require F to be algebraically closed, and

(b) The proof is analogous to the surjectivity of $\ell : \mathfrak{m}\mathbb{C}_p - \{0\} \to \mathbb{C}_p$ (ℓ for log), given by $x \mapsto \log(x+1)$.

One can refer to the term *periods of cyclotomic groups.* $\square$

When $d = r = 1$ and $\mathbb{F} = \mathbb{C}_p^\flat$, for some certain choice of t, whose divisor $\mathrm{Div}(t)$ is the ϕ^r-translates of $\mathfrak{m}_x$, we can retrieve $K_x \cong \mathbb{C}_p$ as an untilt of $\mathbb{C}_p^\flat$. We call this choice of t the *Fontaine's cyclotomic period*. We then retrieve the short exact sequence

$$0 \to \mathbb{Q}_p \xrightarrow{\cdot t} B^{\phi=p} \to K_x \cong \mathbb{C}_p \to 0.$$

In literature, it's more common to write $(B_{\text{cris}}^+)^{\phi=p} := B^{\phi=p}$.

5.4. Vector Bundles on the Fargues-Fontaine Curves.

Consider the two curves $X_{rm} = \mathrm{Proj}(\bigoplus_{d\geq 0} B^{\phi^{rm}=p^d})$ and $X_r = \mathrm{Proj}(\bigoplus_{d\geq 0} B^{\phi^r=p^d})$. Then we have a natural map

$$\pi_r^{(m)} : X_{rm} \to X_r \text{ given by } B^{\phi^r=p^d} \to B^{\phi^{rm}=p^{dm}} \text{ sending } z \mapsto z.$$

This map of $\mathbb{Q}_{p^r}$-algebras induces $B^{\phi^r=p^d} \otimes_{\mathbb{Q}_{p^r}} \mathbb{Q}_{p^{rm}} \xrightarrow{\sim} B^{\phi^{rm}=p^{dm}}$, hence $\pi_r^{(m)}$ is

(a) finite étale (because it is a base change of a finite étale map), and is
(b) totally split over every closed point (ie. the fiber of any closed point is m distinct points)[50]

We also know that

$$\mathrm{Pic}(X_r) \xrightarrow{\sim} \mathbb{Z} \text{ with inverse given by } d \mapsto \mathcal{O}_{X_r}(d) \cong \widetilde{P_{\mathbb{Q}_{p^r}}[d]}.$$

Let's setup some notations:

(a) For all $d, h \in \mathbb{Z}$, we define $\mathcal{O}_{X_r}(d,h) := (\pi_r^{(h)})_* \mathcal{O}_{X_{rh}}(d)$, and
(b) for $\lambda = d/h \in \mathbb{Q}$ with $(d,h) = 1$, define $\mathcal{O}_{X_r}(\lambda) := \mathcal{O}_{X_r}(d,h)$.
(c) In addition, for $\lambda \in \mathbb{Q}$, define $o(\lambda)$ to be the order of $\lambda \in \mathbb{Q}/\mathbb{Z}$. [51]

We shall use the following main result without proof:

Theorem 5.17. *Let F be an algebraically closed field as all along. Then every vector bundle on X_r is of the form of direct sums of $\mathcal{O}_{X_r}(\lambda)$. (Aut group?)*

In any case, let's investigate some properties of the vector bundles $\mathcal{O}_{X_r}(\lambda)$ and $\mathcal{O}_{X_r}(d,h)$.

Proposition 5.18. *Let $\lambda \in \mathbb{Q}$.*

(a) *Without assuming $(d,h) = 1$, we have $\mathcal{O}_{X_r}(d,h) = \mathcal{O}_{X_r}(d/h)^{\gcd(d,h)}$.*
(b) *(Rank) $\mathcal{O}_{X_r}(\lambda)$ is a vector bundle of rank $o(\lambda)$.*
(c) *Considering the map $\pi_r^{(m)} : X_{rm} \to X_r$, we have*
  (i) *(Pushforward) $(\pi_r^{(m)})^* \mathcal{O}_{X_r}(d,h) = \mathcal{O}_{X_{rm}}(md,h)$, and*
  (ii) *(Pullback) $(\pi_r^{(m)})_* \mathcal{O}_{X_{rm}}(d,h) = \mathcal{O}_{X_r}(d,mh)$.*
  In particular, we have $(\pi_r^{(m)})^* \mathcal{O}_{X_r}(\lambda) = \mathcal{O}_{X_{rm}}(m\lambda)^{o(\lambda)/o(o\lambda)}$.
(d) *(Tensor) We have*
  (i) *$\mathcal{O}_{X_r}(d_1,h_1) \otimes \mathcal{O}_{X_r}(d_2,h_2) \cong \mathcal{O}_{X_r}(h_2 d_1 + h_1 d_2, h_1 h_2)$.*
  (ii) *$\mathcal{O}_{X_r}(\lambda_1) \otimes \mathcal{O}_{X_r}(\lambda_2) \cong \mathcal{O}_{X_r}(\lambda_1 + \lambda_2)^{o(\lambda_1)o(\lambda_2)/o(\lambda_1+\lambda_2)}$.*
(e) *(Derived Hom) We have*

[50] This is a usual phenomenon for a curve over $\mathbb{Q}_p$.
[51] I believe Fontaine might have used $m(\lambda)$ for this, but using $o(\lambda)$ as the notation will avoid some unfortunate terminology complications.

(i) $\operatorname{Hom}(\mathcal{O}_{X_r}(\lambda_1), \mathcal{O}_{X_r}(\lambda_2)) = 0$ *if* $\lambda_2 < \lambda_1$, *and*
(ii) $\operatorname{Ext}^1(\mathcal{O}_{X_r}(\lambda_1), \mathcal{O}_{X_r}(\lambda_2)) = 0$ *if* $\lambda_2 \geq \lambda_1$.

Dec 5, 2018. Wednesday.

Recall that $X_r = \operatorname{Proj}(P_{\mathbb{Q}_{p^r}})$ and we have a natural map $\pi_r^{(m)} : X_{rm} \to X_r$. Today we will prove most of the claims in 5.18.

Let us start by (a), the claim $\mathcal{O}_{X_r}(d,h) = \mathcal{O}_{X_r}(d/h)^{\gcd(d,h)}$.

Observe that $(\pi_4^{(h)})_* \mathcal{O}_{X_{rh}} = \mathcal{O}_{X_r} \otimes_{\mathbb{Q}_{p^r}} \mathbb{Q}_{p^{rh}} \cong \mathcal{O}_{X_r}^h$, and that $(\pi_r^{(h)})^* \mathcal{O}_{X_r}(d) = \mathcal{O}_{X_{rh}}(dh)$. Writing $\delta = \gcd(d,h)$, we then have a factoring

$$\pi = \pi_r^{(h)} : X_{rh} \xrightarrow{\pi_2 = \pi_{r(h/\delta)}^{(\delta)}} X_{r(h/\delta)} \xrightarrow{\pi_1 = \pi_r^{(h/\delta)}} X_r.$$

Hence we have

$$\begin{aligned}
\mathcal{O}_{X_r}(d,h) &= \pi_* \mathcal{O}_{X_{rh}}(d) \\
&= \pi_{2,*}\pi_{1,*}\mathcal{O}_{X_{rh}}(d) \\
&= \pi_{2,*}\pi_{1,*}\mathcal{O}_{X_{rh}}(d/\delta \cdot \delta) \\
&= \pi_{2,*}\pi_{1,*}\pi_1^*\mathcal{O}_{X_{r(h/\delta)}}(d/\delta) \\
&= \pi_{2,*}(\mathcal{O}_{X_{r(h/\delta)}}(d/\delta) \otimes \mathcal{O}_{X_{r(h/\delta)}}^\delta) \qquad (\dagger) \\
&= \mathcal{O}_{X_r}(d/h)^\delta,
\end{aligned}$$

where in ($\dagger$) we used the projection formula. $\square$

Next we will prove part (b), the claim that $\mathcal{O}_{X_r}(\lambda)$ is a vector bundle of rank $o(\lambda)$. Equivalently, if $\lambda = d/h$ in lowest terms, then $o(\lambda) = h$. Let us first restate the claim in another way. Let us define for M a vector bundle on X_r, the degree of M is $\deg(M) = \deg_{X_r}(M) := \deg(\det(M)) = \det(\bigwedge^{\operatorname{rank} m} M)$. We also define the slope of M to be $\mu(M) = \deg(M)/\operatorname{rank}(M)$. Part (b) will then say that $\mu(\mathcal{O}_{X_r}(\lambda)) = \lambda$.

Proof. The rank is $o(\lambda)$ from the definition, since it's the pushforward of $\mathcal{O}_{X_{rh}}(d)$ via $(\pi_r^{(h)})$, where $\mathcal{O}_{X_{rh}}(d)$ is a line bundle and $\pi_r^{(h)}$ is a degree h (finite) étale cover. For the claim on the slope, we see that

$$\deg_{X_r}\det(\mathcal{O}_{X_r}(\lambda)) = (1/h)\deg_{X_{rh}}((\pi_r^{(h)})^*\det(\mathcal{O}_{X_r}(\lambda))).$$

Now it's a matter of understanding what this is. We claim that if M is a vector bundle over X_r, then $\det((\pi_r^{(h)})^* M) \cong (\pi_r^{(h)})^* \det(M)$. This follows from the following three facts:

(a) Tensors behave well under pullbacks.
(b) Exterior powers are quotients of tensors.
(c) Quotients behave well under flat maps.

So now we transfer our study to $\det((\pi_r^{(h)})^*\mathcal{O}_{X_r}(\lambda))$. We claim that $(\pi_r^{(h)})^*\mathcal{O}_{X_r}(\lambda) = (\pi_r^{(h)})^*(\pi_r^{(h)})_*\mathcal{O}_{X_{rh}}(d)$ is just $\mathcal{O}_{X_{rh}}(d)^h$. To see this, we translate this back to commutative algebra language, which says that if $R \to S$ is a finite Galois(?) map, then $M \otimes_R S \cong M \otimes_S (S \otimes_R S) \cong \prod_{\operatorname{Gal}(S/R)} M$ as R-modules.

Hence $\det((\pi_r^{(h)})^*\mathcal{O}_{X_r}(\lambda)) = \det(\mathcal{O}_{X_{rh}}(d)^h) = \mathcal{O}_{X_{rh}}(dh)$. Hence $\deg(\mathcal{O}_{X_r}(\lambda)) = (1/h)\deg(\mathcal{O}_{X_{rh}}(dh)) = dh/h = d$, and $\mu(\mathcal{O}_{X_r}(\lambda)) = d/h = \lambda$ as claimed. $\square$

We also note that with this, we conclude that the slope of a vector bundle is insensitive to taking powers of the vector bundle. (?)

We shall postpone the proof of part (c) till next lecture.

So part (d), we must show that $\mathcal{O}_{X_r}(d_1,h_1)\otimes\mathcal{O}_{X_r}(d_2,h_2)\cong\mathcal{O}_{X_r}(h_2d_1+h_1d_2,h_1h_2)$. Consider the diagram [[hmm]]

—

Observe that the slope of a vector bundle is insensitive to taking powers of the vector bundle.

(iii) $\pi_r^{(m)}: X_{rm}\to X_r$. Prop says that $(\pi_r^{(m)})^*\mathcal{O}_{X_r}(d,h) = \mathcal{O}_{X_{rm}}(md,h)$, and $(\pi_r^{(m)})_*\mathcal{O}_{X_{rm}}(d,h) = \mathcal{O}_{X_r}(d,mh)$, and in particular, $(\pi_r^{(m)})^*\mathcal{O}_{X_r}(\lambda) = \mathcal{O}_{X_{rm}}(m\lambda)^{m(\lambda)/m(m\lambda)}$.

Proof. Consider the (diamond figure: $X_{rhm}\xrightarrow{p_1}X_{rh}\xrightarrow{\pi_1}X_r$ and $\xrightarrow{p_2}X_{rm}\xrightarrow{\pi_2}X_r$ and composition is q). Then $\mathcal{O}_{X_r}(d,h) = \pi_{1,*}\mathcal{O}_{X_{rh}}(d)$ and $\mathcal{O}_{X_{rm}}(md,h) = p_{2,*}\mathcal{O}_{X_{rmh}}(md)$. WTS $\pi_2^*\pi_{1,*}\mathcal{O}_{X_{rh}}(d)\cong p_{2,*}\mathcal{O}_{X_{rmh}}(md)$. Faithfully flat descent says we can pullback everything to X_{rhm} and work it out, so let's do so via p_2^*. Then

LHS $\cong q^*\pi_{1,*}\mathcal{O}_{X_{rh}}(d)$ (not very sure. let's move on.)

(iv) $\mathcal{O}_{X_r}(d_1,h_1)\otimes\mathcal{O}_{X_r}(d_2,h_2)\xrightarrow{\sim}\mathcal{O}_{X_r}(h_2d_1+h_1d_2,h_1h_2)$.

Proof. Draw a similar diamond diagram (with h becoming h_1 and m becoming h_2). p_1 has degree h_2 and p_2 has degree h_1. Consider $q_*(\mathcal{O}_{h_1h_2r}(h_2d_1)\otimes_{\mathcal{O}_{X_{h_1h_2r}}}\mathcal{O}_{X_{h_1h_2r}}(h_1d_2)$, which is definitely same as RHS. On the other hand, this is also $q_*(p_1^*\mathcal{O}_{X_{h_1r}}\otimes_{\mathcal{O}_{X_{h_1h_2r}}}p_2^*\mathcal{O}_{X_{h_2r}}(d_2))$. Claim this is $\cong p_{1,*}p_1^*\mathcal{O}_{X_{h,r}}(d_1)\otimes_{\mathcal{O}_{X_r}}p_{2,*}p_2^*\mathcal{O}_{X_{h_2,r}}(d_2)$. This is just commutative algebra: On level of modules, first thing is $(S_3\otimes_{S_1}M_1)\otimes_{S_3}(S_3\otimes_{S_2}M_2)\cong M_1\otimes_{S_1}S_3\otimes_{S_2}M_2\cong(M_1\otimes_{S_1}S_1)\otimes_R(M_2\otimes_{S_2}S_2) =$ the second guy. The main claim is $S_3 = S_1\otimes_R S_2$. This is because $X_{h_1r}\times_{X_r}X_{h_2r} = (\mathbb{Q}_{p^{h_1r}}\otimes_{\mathbb{Q}_{p^r}}X_r)\times_{X_r}(\mathbb{Q}_{p^{h_2r}}\otimes_{\mathbb{Q}_{p^r}}X_r) = ...$ seems right if relatively prime, otherwise use (a) to bootstrap it up.

In particular, $\mathcal{O}_{X_r}(\lambda_1)\otimes_{\mathcal{O}_{X_r}}\mathcal{O}_{X_r}(\lambda_2)\cong\mathcal{O}_{X_r}(\lambda_1+\lambda_2)^{something}$.

Finally for Hom and Ext statements, can be checked after pullback to any X_{rm} (along finite flat maps...) Hence can assume that $\lambda,\lambda\in\mathbb{Z}$ and write d_1,d_2 for clarity. In this case, this becomes the assertion $H^0(X_r,\mathcal{O}(d_2,d_1)) = 0$ if $d_2<d_1$. This follows from the fact that $P_{\mathbb{Q}_{p^r}}$ has no negative degree graded term, (used also that $\lambda_1>\lambda_2$ is preserved by pullback, since just multiply by degree of cover)

Finally Ext: proof: Can assume that $\lambda_1,\lambda_2 = d_1,d_2\in\mathbb{Z}$, because this becomes $H^1(X_r,\mathcal{O}_{X_r}(d_2-d_1)) = 0$ if $d_1\le d_2$. But we know that $H^1(X_r,\mathcal{O}_{X_r}) = 0$. Since we have a nonzero map $\mathcal{O}_{X_r}\to\mathcal{O}_{X_r}(d)$ for all $d\ge 0$, we have $H^1(X_r,\mathcal{O}_{X_r})\twoheadrightarrow H^1(X_r,\mathcal{O}_{X_r}(d))$. Coker is torsion, so has no H^1.... also kernel is 0? dedekind scheme so torsion free is free....

Dec 12, 2018. Wednesday.

Recall: $f : A \to A'$ such that $A_\eta \xrightarrow{\sim} A'_\eta$, then $\deg(A) \le \deg(A')$ and equality holds iff f is an isomorphism.

Lemma. $B \subseteq A$ is a subobject of minimal rank such that $\mu(B) \ge \mu(A)$ and $\mu(B)$ maximal, then B is semistable and is a strict subobject.

Proof. By schematic closure, there is $B \subseteq B' \subseteq A$ such that B' strict in$A$ and $B_\eta = B'_\eta$. But then $\deg(B) \le \deg(B')$, and equality by maximality, and $B = B'$. Check that subobject of B has smaller μ – this is semistability.

Want to build semistable guys because slope filtration gives this, and one would want to know how to build semistable guys.

Last time we talked about $\mathcal{C} = \mathrm{Fil}\,\mathsf{Vect}_K$, and $\mathcal{C} \to \mathcal{C}' = \mathsf{Vect}_K$. All our filtrations are exhaustive, descending, separated... Then $\deg((M, \mathrm{Fil}^\bullet)) = i$ where $i \in \mathbb{Z}$ is such that $gr^i_{\mathrm{Fil}^\bullet} \bigwedge^{top} M \neq 0$. Then check that $i = \sum_{i\in\mathbb{Z}} i \dim \mathrm{gr}^i_{\mathrm{Fil}^\bullet} M$.

Idea: We have $M^{\otimes k} \twoheadrightarrow \bigwedge^{top} M$, and $\mathrm{Fil}^n M^{\otimes k} = \sum_{i_1+\cdots+i_j=n} \mathrm{Fil}^{i_1} M \otimes \cdot \otimes \mathrm{Fil}^{i_k} M$, and endow the quotient filtration to $\bigwedge^{top} M$. One way to check is that to write down $M = \bigoplus_{i\in\mathbb{Z}} M^i$ such that $\mathrm{Fil}^n M = \otimes_{i\ge n} M^i$. Choose bases $\{e^{(i)}, \dots, e^{(i)}_{\dim \mathrm{gr}^i_{\mathrm{Fil}} M}\}$ for M_i, then $\bigwedge^{top} M$ is spanned by $\bigwedge_{i\in\mathbb{Z}, 1\le m \le \mathrm{gr}^i_{\mathrm{Fil}} M} e^{(i)}_m$.

Check that degree satisfies the degree axiom.

Choose K/K_0 totally ramified, then $K_0 = W(k)[1/p]$ where $k = \mathrm{char}\, p$ is perfect (no need alg closed). Look at $\mathcal{C} = MF^\phi_K \to \mathcal{C}' = \mathsf{Isoc}_{K_0}$ where MF^ϕ_K is triples $(M, \phi, \mathrm{Fil}^\bullet M_K)$ where $(M, \phi) \in \mathsf{Isoc}_{K_0}$ and $\mathrm{Fil}^\bullet M_K$ is a filtration on $M \otimes_{K_0} K$. Rank is the obvious one, filtration has usual conditions, and $\deg = -\deg(M, \phi) + \deg(M_K, \mathrm{Fil}^\bullet M_K)$. Need target to be Isoc_{K_0} (cannot be M itself, or else cant satisfy the degree).

Remark: Can also use $MF^\phi_K \to \mathrm{Fil}\,\mathsf{Vect}_K$ for generic fiber functor, in this case, can take degree to be $\deg(M, \phi) - \deg(M_K, \mathrm{Fil}^\bullet M_K)$, but target is not abelian.

Next define Category of Modifications.

Choose a point $\infty \in X$, a closed point, and consider $\mathcal{C} := \mathsf{Mod}_{X,\infty}$, containing $(\mathcal{E}_1, \mathcal{E}_2, \xi)$, where $\mathcal{E}_1, \mathcal{E}_2 \in \mathsf{Vect}_X$ (vbs) and $\xi : \mathcal{E}_1 \mid_{X-\{\infty\}} \xrightarrow{\sim} \mathcal{E}_2 \mid_{X-\{\infty\}}$.

Set $B^+_{dR,\infty} = \widehat{\mathcal{O}}_{X,\infty}$. Also, up to a $\mathbb{Q}_p$ multiple, ∞ correspond to $t_\infty \in B^{\phi=p}$. Set $B_{dR,\infty} = \widehat{\mathcal{O}}_{X,\infty}[t_\infty^{-1}]$.

Consider $\Theta_\infty : A_{\inf}[p^{-1}] \to C_\infty$, then $B^+_{dR,\infty} = \varprojlim_n A_{\inf}[p^{-1}]/(\ker \Theta_\infty)^n$.

There is a functor $(\mathcal{E}_1, \mathcal{E}_2, \xi) \mapsto \xi^{-1}(\widehat{\mathcal{E}}_{2,\infty}) \subseteq \widehat{\mathcal{E}}_{1,\infty}[t_\infty^{-1}]$, where $\widehat{\mathcal{E}}_{i,\infty} = \mathcal{E}_i \otimes \mathcal{O}_X B^+_{dR,\infty}$. This induces an equivalence between $\mathsf{Mod}_{X.\infty}$ and category of pairs $(\mathcal{E}, \widehat{E}_\infty)$, where $\mathcal{E} \in \mathsf{Vect}_X$ is a vb (that is $\mathcal{E}_1$), and $\widehat{E_\infty} \subseteq \widehat{\mathcal{E}}_\infty[t_\infty^{-1}]$ is a $B^+_{dR,\infty}$-lattice. Only works because working over dedekind domain.

In other words, there is a unique $\mathcal{E}' \subseteq \mathcal{E} \mid_{X-\{\infty\}}$ such that $\widehat{\mathcal{E}}'_\infty \subseteq \widehat{E}_\infty$ and for all $x \neq \infty \in |X|$, we have $\widehat{\mathcal{E}}'_x = \widehat{\mathcal{E}}_x$.

Fix K/K_0, and write $L = \widehat{K}^{nr}$ be the max unram extn of K_0 in $\widehat{\overline{K}}$, and write $F = \widehat{\overline{K}}^\flat$. $\mathcal{E}$ arises from an isocrystal $M \in \mathsf{Isoc}_L$. Let $B_e = B[1/t_\infty]^{\phi=1}$. Then (1) $\operatorname{Spec} B_e = X - \{\infty\}$. ($X = \operatorname{Proj} \bigoplus B^{\phi=p^d}$, and degree 0 with t_∞ inverted is ϕ invariant.)

$\mathcal{E} = \bigoplus_{d\geq 0} (\widetilde{M \otimes_L B})^{\phi=p^d}$, then (2) $\mathcal{E}\mid_{X-\{\infty\}} \leftrightarrow (M \otimes_L B[1/t_\infty])^{\phi=1}$.

Observation: $\widehat{\mathcal{E}_\infty}[1/t_\infty] = ((M \otimes L B[t_\infty^{-1}])^{\phi=1} \otimes_{B_e} B[t_\infty^{-1}]) \otimes_{B[1/t_\infty]} B_{dR,\infty}) = M \otimes_L B[1/t_\infty]) \otimes_{B[1/t_\infty]} B_{dR,\infty} = M \otimes_L B_{dR,\infty}$.

$B_e \hookrightarrow B[1/t_\infty] \hookrightarrow B_{dR,\infty}$. (Reasoning.)

So we have to find a $B^+_{dR,\infty}$-lattice.

What ∞ should we take? There's a canonical choice because we started without $^\flat$.

Γ_K acts on $\widehat{\overline{K}}$, so by functoriality of tilting, Γ_K acts on $F = \widehat{\overline{K}}^\flat$. Concretely, $\widehat{\overline{K}}^\flat = \varprojlim \widehat{\overline{K}}$ as monoids, and RHS has Γ_K action. So Γ_K acts on $A_{\inf} = W(\mathcal{O}_{\widehat{\overline{K}}^\flat})$. Then $\Theta_\infty : A_{\inf}[p^{-1}] \to \widehat{\overline{K}}$ is Γ_K-equivariant, hence kernel is Γ_K-stable. Can check that Γ_K acts on B in a ϕ-equivariant way (from action on $A_{\inf}$), so Γ_K acts on X. So we have a category $\mathsf{Vect}_X^{\Gamma_K}$ of Γ_K-equivariant vbs on X. Concretely, it's a category of pairs $(\mathcal{E}, \{a_\sigma\}_{\sigma\in\Gamma_K})$ where $\alpha_\sigma : \sigma^*\mathcal{E} \xrightarrow{\sim} \mathcal{E}$ with 1-cocycle condition.

So if $(M, \phi) \in \mathsf{Isoc}_{K_0}$, then $\mathcal{E}(M, \phi) = \bigoplus_{d\geq 0} (\widetilde{M \otimes_{K_0} B})^{\phi=p^d}$. There's a Γ_K action acts on second factor (Γ_K fixes K and hence on K_0 so we are ok). So $\mathcal{E}(M, \phi) \in \mathsf{Vect}_X^{\Gamma_K}$. [[$K$ wont embed inside $A_{\inf}$ unless K/K_0 is unram.]]

This gives a functor from $\mathsf{Isoc}_{K_0} \to \mathsf{Vect}_X^{\Gamma_K}$. Look at modifications to include the galois data. Consider $\mathsf{Mod}_{X,\infty}^{\Gamma_K} = (\mathcal{E}_1, \mathcal{E}_2, \xi)$ where $\mathcal{E}_1, \mathcal{E}_2 \in \mathsf{Vect}_X^{\Gamma_K}$ and ξ is Γ_K-equivariant isom. Then as saw before, $\mathsf{Mod}_{X,\infty}^{\Gamma_K}$ is equivalent to the category of pairs $(\mathcal{E}, \widehat{E_\infty})$, where $\mathcal{E} \in \mathsf{Vect}_X^{\Gamma_K}$ and $\widehat{E_\infty} \subseteq \widehat{\mathcal{E}}_\infty[t_\infty^{-1}]$ is a Γ_K-stable $B^+_{dR,\infty}$-lattice. If $\mathcal{E} = \mathcal{E}(M, \phi)$, where $(M, \phi) \in \mathsf{Isoc}_{K_0}$, then $\widehat{E_\infty} \subseteq M \otimes_{K_0} B_{dR,\infty}$ is a Γ_K-stable lattice (and a trivial object in $\mathsf{Rep}_{\Gamma_K}(B_{dR,\infty})$).

Proposition. there's a canonical bijection from Γ_K-stable $B^+_{dR,\infty}$-lattices $\widehat{E}_\infty \subseteq M \otimes_{K_0} B_{dR,\infty}$ to filtrations $\operatorname{Fil}^\bullet M_K$ on M_K.

In other words, $\mathsf{Mod}_{X,\infty}^{\Gamma_K, cris} = (\mathcal{E}_1, \mathcal{E}_2, \xi) \subseteq \mathsf{Mod}_{X,\infty}^{\Gamma_K}$ where $\mathcal{E}_1 = \mathcal{E}(M, \phi)$, for some $(M, \phi) \in \mathsf{Isoc}_{K_0}$, is equivalent to MF_K^ϕ.

Proof. Bijection is given by the assignment: $\widehat{E_\infty} \mapsto \operatorname{Fil}^i_{\widehat{E}_\infty} M_K = (t^i_\infty \widehat{E}_\infty)^{\Gamma_K} \subseteq (M \otimes_{K_0} B_{dR,\infty})^{\Gamma_K} = (M \otimes_{K_0} B_{dR,\infty}^{\Gamma_K}$ since Γ_K only acts on second factor. To see this is well defined, we have to check the following: $B_{dR,\infty}^{\Gamma_K} = K$. Proof: $B^+_{dR,\infty}$ is a DVR with residue field $\widehat{\overline{K}}$. Its kernel is generated by t_∞. We saw earlier on in the term that if $\chi : \Gamma_K \to \mathbb{Z}_p^\times$ is the cyclotomic character, then $\widehat{\overline{K}}(\chi^i)^{\Gamma_K}$ is K if $i = 0$ and 0 otherwise. Main point that becomes Γ_K acts on t_∞ via the cyclotomic character χ. This is because elements of $B^{\phi=p}$ can be described as follows:

Choose $\alpha \in \mathfrak{m}_F - \{0\}$, then look at $[1+\alpha] \in A_\infty$ and claim that $|[1+\alpha]-1|_\rho < 1$ for any $\rho \in (0, 1)$. With claim, we then have $\log[1 + \alpha]$ (the usual power series) is $\sum_{n=1}^\infty (-1)^{n-1}([1 + \alpha] - 1)^n)/n \in B$ (converges), and its image under ϕ is multiplication by p, so $\log[1 + \alpha] \in B^{\phi=p}$. Take $1 + \alpha = \varepsilon$ where $\varepsilon = (\zeta_{p^n})_{n\geq 0} \in \mathcal{O}_{\widehat{\overline{K}}}$. Then

$[\varepsilon]-1 \in \ker(\Theta_\infty) \subseteq A_{\inf}$. Then $\log[\varepsilon] \in \ker(\Theta_\infty) \subseteq B$ is a multiple of t_∞. So we can take $\log[\varepsilon]$ to be t_∞. This then implies Γ_K acts on t_∞ via χ (because it does so on $\log[\varepsilon]$).

With this, so $B^+_{dR,\infty} = (\bigcup_{i\in\mathbb{Z}} t^i_\infty B^+_{dR,\infty})^{\Gamma_K}$. But

$$0 \to (t^{i-1}_\infty B^+_{dR,\infty})^{\Gamma_K} \to (t^i_\infty B^+_{dR,\infty})^{\Gamma_K} \to \widehat{\overline{K}}(\chi^i)^{\Gamma_K}$$

but RHS is nonzero if $i=0$. So unless $i=0$, we have $(t^{i-1}_\infty B^+_{dR,\infty})^{\Gamma_K} = (t^i B^+_{dR,\infty})^{\Gamma_K}$. When $i=0$, middle is nonzero, but left is zero, so one can show that $B^{+,\Gamma_K}_{dR,\infty} = K$. This amounts to showing that $H^1(\Gamma_K, t_\infty B^+_{dR,\infty}) = 0$ (equivalently that $H^1(\Gamma_K, \widehat{\overline{K}}(\chi^i)) = 0$ if $i>0$.

After all this, we show that $\widehat{E}_\infty \mapsto M_K$. How to think about the inverse? It's given by follows: Take a filtration $\operatorname{Fil}^\bullet M_K \mapsto \widehat{E}_\infty = \sum_{i\in\mathbb{Z}} t^{-i}_\infty B^+_{dR,\infty} \otimes_K \operatorname{Fil}^i M_K$.

One direction of inverse is easy: filtration to lattice to filtration is easy. (you do get $\operatorname{Fil}^k M_K$). Other direction: Any lattice from inverse functor from a filtration is isomorphic to $\sum_{i=1}^n t^{k_i}_\infty B^+_{dR,\infty}$ as Γ_K-reps. Key observation: every $\widehat{E}_\infty$ is isom to such a lattice (or Γ_K-rep). This is proved by induction on $\dim M$. 1-dim is fine... For induction, if $0 \to M' \to M \to M'' \to 0$, and hit with $B_{dR,\infty}$, then inside of middle we have $\widehat{E}_\infty$, and its image on the right and intersection on the left both are Γ_K-stable, and so by hypothesis looks like desired form.

The result comes down to seeing $\ker(H^1(\Gamma_K, t^i_\infty B^+_{dR,\infty}) \to H^1(\Gamma_K, B_{dR,\infty})) = 0$. (trivial after $\otimes B_{dR,\infty}$ is trivial to begin with).

There's a degree function on modifications, which is $\deg(\mathcal{E}_2)$. On MF, the degree is $\deg(M, \operatorname{Fil} M) - \deg(M,\phi)$, and upshot is they are the same. (wrong degree on MF, should be $+$).

Semistability notions: if $\{S^\lambda \mathcal{E}_2\}$ is the slope filtration and $\{S^\lambda(M,\phi,\operatorname{Fil}^\bullet)\}$ is too, then $S^\lambda\mathcal{E}_2$ is obtained from $S^\lambda(M,\phi,\operatorname{Fil}^\bullet)$ for any λ.

Show semistable of degree zero in $MF \xrightarrow{\sim} \mathsf{Mod}^{\Gamma_K, cris, ss=0}_{X,\infty}$. But RHS has that $\mathcal{E}_2$ is ss of slope 0 iff $\mathcal{E}_2 = H^0(X,\mathcal{E}_2) \otimes_{\mathbb{Q}_p} \mathcal{O}_X$. Since Γ_K acts on the left, and Γ_K acts on H^0, so we can define a functor from $\mathsf{Mod} \to \mathsf{Rep}_{\Gamma_K}(\mathbb{Q}_p)$, and to conclude, gets galois reps from MF_K. Image in Rep is actually $\mathsf{Rep}^{cris}_{\Gamma_K}(\mathbb{Q}_p)$, the category of crystalline galois reps. $ss = 0$ is classically weakly admissible. This functor to reps is really where classification of vector bundles is needed to ensure the rep is of the correct rank.

What would happen without classification? $M \in MF$ maps to $\mathcal{E}_1 = \mathcal{E}(M,\phi)$, and $\widehat{\mathcal{E}}_{2,\infty} = \operatorname{Fil}^0(M \otimes_{K_0} B_{dR,\infty} = \sum_{i+j=0} (\operatorname{Fil}^i M \otimes t^j_\infty B^+_{dR,\infty})$. $H^0(X,\mathcal{E}_2) \hookrightarrow H^0(X - \{\infty\}, \mathcal{E}_2) = H^0(X - \{\infty\}, \mathcal{E}_1) = (M \otimes_{K_0} B[1/t])^{\phi=1}$. Patch in ∞ condition to get $H^0(X,\mathcal{E}_2) = (M \otimes_{K_0} B[1/t]))^{\phi=1} \cap \operatorname{Fil}^0(M \otimes_{K_0} B_{dR,\infty})$.

What is this really though: if we have seen this before, then we'll know: $H^0(X, \mathcal{O}_X(\lambda)) = \mathbb{Q}_p$ if $\lambda = 0$, 0 if $\lambda < 0$, and inf dim if $\lambda > 0$. For example, $H^0(X, \mathcal{O}_X(1)) = B^{\phi=p}$, and from the fund lemma $0 \to \mathbb{Q}_p t_\infty B^{\phi=p} \to \widehat{\overline{K}} \to 0$. So $H^0(X,\mathcal{E}_2)$ is inf dim unless it's ss of slope 0.

Index.

Yet to be updated.