p-DIVISIBLE GROUPS: PART II

BRANDON LEVIN

This talk discusses the main results of Tate's paper "p-Divisible Groups" [6]. From the point of view of p-adic Hodge theory, this is a foundational paper and within this setting, much of the technical work being done becomes extremely important. From our perspective, having just learned what p-divisible groups are three weeks ago, however, the significance of the results could easily be drowned in details.

I will thus proceed in an unorthodox fashion beginning with the end result and relegating a lot of technical details to appendices and references.

Before we begin, I mention a rather amazing motivation for our study of p-divisible groups. In Faltings' proof and in many other instances, one is interested in studying the structure of moduli spaces of abelian varieties (of fixed dimension, polarization of fixed degree, etc.). The primary tool for studying the local structure of moduli spaces is deformation theory. Deformation theory tells us information about the completed stalks of the structure sheaf on our moduli space.

A natural question one might ask is given an abelian variety A over $\mathbb{F}_p$, can we lift it to an abelian scheme over $\mathbb{Z}_p$? For example, in the case of elliptic curves, all we have to do is lift the Weierstrass equation and so there are many possible lifts. Given that lifts exist, we could try to lift an abelian variety together with some endomorphisms or maybe two abelian varieties with homomorphisms between them. The first step would be to pose the same problem for $\mathbb{Z}_p/p^n\mathbb{Z}_p$ as opposed to $\mathbb{Z}_p$. This is an infinitessimal deformation problem from characteristic p, and a remarkable theorem of Serre-Tate says that in residue characteristic p, the deformation theory of an abelian variety is the same as that of its p-divisible group:

Theorem 0.1 (Serre-Tate)**.** *Let R be a ring in which p is nilpotent, $I \subset R$ a nilpotent ideal (i.e., $I^n = 0$ for some $n > 0$). Define $R_0 = R/I$. Then the functor $A \mapsto (A_0, A[p^\infty], \varepsilon)$ from the category of abelian schemes over R to the category of triples $(A_0, \Gamma, \varepsilon)$ where A_0 is an abelian scheme over R_0, Γ is a p-divisible group over R, and $\varepsilon : A_0[p^\infty] \to \Gamma_{R_0}$ is an isomorphism, is an equivalence of categories.*

Proof. See Katz [3] Thm 1.2.1. □

Concretely, this says if we have an abelian scheme over R/I, to lift it to R we just have to lift its p-divisible group. Similarly, to lift a homomorphism over R/I to one over R between lifts, it suffices to lift the induced homomorphism of p-divisible groups. The deformation theory of abelian varieties in characteristic p would be totally intractable without appealing to the deformation theory of p-divisible groups, which is governed by semi-linear algebra data (for example, Dieudonne modules and its generalization provided by Grothendieck and Messing).

1. Prolonging Morphisms

One mantra to keep in mind throughout this talk is the p-divisible groups are like honorary abelian varieties. Their behavior in many ways resembles that of abelian schemes as opposed to the finite flat groups schemes of which they are composed.

For example, Mike discussed the following result (which also holds for abelian schemes, by a simpler argument with finite étale torsion levels):

Proposition 1.1. *Let (R, m) be a local noetherian ring with residue field k of characterstic p, and let G and H be p-divisible groups over R. Then, the reduction map*

$$\mathrm{Hom}_R(G, H) \to \mathrm{Hom}_k(G_k, H_k)$$

is injective.

Note this result is special to p-divisible groups and is not true for finite flat group schemes, in general. The simplest counter-example is the non-trivial homomorphism $\mathbb{Z}/p\mathbb{Z} \to \mu_p$ over $\mathbb{Z}[\mu_p]$ defined by $1 \mapsto \zeta_p$; this is trivial on the special fiber but an isomorphism on generic fibers. Over the non-noetherian valuation ring $R = \mathbb{Z}_p[\mu_{p^\infty}]$ we can make a similar counterexample with p-divisible groups: the R-homomorphism $\mathbb{Q}_p/\mathbb{Z}_p \to \mu_{p^\infty}$ defined by $p^{-n} \mapsto \zeta_{p^n}$ for a compatible system $\{\zeta_{p^n}\}$ of p-power roots of unity in $R^\times$. Raynaud's results discussed by Melanie and Rebecca imply that over a mixed-characteristic $(0, p)$ discrete valuation ring with absolute ramification degree $e < p-1$, passage to the special fiber on finite flat group schemes is faithful. Prop. 1.1 says that for p-divisible groups there is no ramification restrictions; only the Noetherian hypothesis (which one cannot remove).

There is another operation one might consider, namely, passing to the generic fiber. The main question here is: do morphisms on the generic fiber prolong to morphism of the integral models? Next quarter, Sam and Christian will show that for abelian schemes over a normal noetherian domain, morphisms between generic fibers do extend. The main result of Tate's paper [6] is that this is true for p-divisible groups:

Theorem 1.2 (Tate)**.** *Let R be an integrally closed, Noetherian, integral domain, whose field of fractions K is of characteristic 0. Let G and H be p-divisible groups over R. Then, the map*

$$\mathrm{Hom}_R(G, H) \to \mathrm{Hom}_K(G \otimes_R K, H \otimes_R K)$$

is bijective.

Before we begin the proof, note that for any v, the natural map

$$\mathrm{Hom}_R(G_v, H_v) \to \mathrm{Hom}_K(G_v \otimes_R K, H_v \otimes_R K)$$

is injective because the coordinate rings of G_v and H_v sit as lattices inside the coordinate rings of $G_v \otimes_R K$ and $H_v \otimes_R K$ respectively. Injectivity at such finite levels implies injectivity at the p-divisible group level. The difficulty is surjectivity, which fails in general at any finite level. For example, if $\dim R = 1$ (and the residue characteristic is p), the natural map $\mathcal{G}^{\max} \to \mathcal{G}^{\min}$ of the minimal and maximal prolongations from Melanie's talk is an isomorphism on generic fibers but has no inverse unless the generic fiber has a unique integral model.

We begin by reducing the case of a complete discrete valuation ring with algebraically closed residue field of characteristic p. An element

$$\varphi \in \mathrm{Hom}_K(G \otimes_R K, H \otimes_R K)$$

is the same as a compatible system of $\varphi_v \in \mathrm{Hom}_K(G_v \otimes_R K, H_v \otimes_R K)$. Since $G_v \otimes K$ and $H_v \otimes K$ are finite over K, we can think of each φ_v as a matrix with coefficients in K relative to R-bases of the coordinate rings. The content of the theorem is φ_v actually has coefficients in R. For each height one prime P of R, assume we know the result for the algebraic localization R_P (whose fraction field is also K), so φ_v has coefficients in R_P for all P. Since R is integrally closed, $R = \cap_{\mathrm{ht}(P)=1} R_P$ inside of K, so we'd get that φ_v has coefficients in R as desired. Thus, now we may and do assume that R is a discrete valuation ring. For any local dvr extension $R \to R'$ we have $R' \cap K = R$ inside of the fraction field of R', so by a similar argument with R-bases and R'-bases it suffices to check the result after scalar extension to R'. It is a general fact that for any discrete valuation ring R and any extension k'/k of its residue field, there is a local extension $R \to R'$ of discrete valuation rings such that (i) a uniformizer of R is a uniformizer of R', and (ii) the induced extension of residue fields is k'. Thus, we may use a suitable such R' renamed as R to arrange that the residue field is algebraically closed. We can also replace R by its completion, so it is complete. If the residue characteristic is not p then all G_v and H_v are etale and everything is easy.

From now one we may and do assume that the algebraically closed residue field of the complete dvr R has characteristic p. It turns out that the main obstruction to prolonging maps "is" the non-uniqueness of integral models which was exhibited in Rebecca and Melanie's talks at finite level. The following lemma (whose complete proof requires everything from §2 onwards) roughly says that p-divisible groups have unique integral models.

Lemma 1.3. *If $g : G \to H$ is a homomorphism of p-divisible groups over R such that its restriction $G \otimes_R K \to H \otimes_R K$ between generic fibers is an isomorphism, then g is an isomorphism.*

Proof. It suffices to show that it is isomorphism at each finite level, so consider $g_v : G_v \to H_v$. Since $g_v \otimes_R K$ is an isomorphism, the coordinate rings of G_v and H_v both sit as orders inside the same finite etale algebra over K, with the ring of H_v *contained in* that of G_v via g_v^*. Thus, it suffices to prove that

$$\mathrm{disc}(G_v) = \mathrm{disc}(H_v)$$

as ideals in R. In Mike's talk, he proved the remarkable formula $\mathrm{disc}(G_v) = (p^{v(n_G)p^{(h_G)v}})$ and similarly for H_v, where n_G is dimension of G and h_G is its height. Clearly, H and G have the same height but what about dimension? If the dimension could somehow be read off from $G \otimes_R K$ then we would be done. This is exactly what we will show in the next section (Cor. 2.14), relying on numerous results proved in the remainder of these notes. □

Before we state the next lemma, we need to define the Tate module of a p-divisible group over R or K.

Definition 1.4. Let G be a p-divisible group over R or K. Then the *Tate module* of G is

$$T(G) = \varprojlim G_v(\overline{K})$$

where the maps are induced by multiplication by p; this is a finite free $\mathbb{Z}_p$-module equipped with a continuous action of the Galois group $\Gamma_K = \mathrm{Gal}(\overline{K}/K)$. Following Tate, we also define

$$\Phi(G) = \varinjlim G_v(\overline{K})$$

where maps are given by natural inclusions i_v.

Remark 1.5. At the level of $\mathbb{Z}_p$-modules, $T(G) \cong \mathbb{Z}_p^h$ and $\Phi(G) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$. We have a canonical isomorphisms $\Phi(G) \cong T(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ and $T(G) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Phi(G))$ respecting the Galois actions, so knowledge of $T(G)$ is the same as knowledge of $\Phi(G)$. If we let $\overline{R}$ be the ring of integers of $\overline{K}$, then because each G_v is finite over R, we have that $G_v(\overline{K}) = G_v(\overline{R})$ so we could also define the Tate module integrally as

$$T(G) = \varprojlim G_v(\overline{R}).$$

Proposition 1.6. *Let K be any field of characteristic 0. The functor $G \rightsquigarrow T(G)$ induces an equivalence of categories between the category of p-divisible groups over K and the category of finite free $\mathbb{Z}_p$-modules equipped with a continuous $\mathbb{Z}_p$-linear action of Γ_K. In particular, the natural map $\mathrm{Hom}_K(G, H) \to \mathrm{Hom}_{\Gamma_K}(T(G), T(H))$ is an isomorphism.*

Proof. All finite flat group schemes over K are etale since we are in characteristic 0. The equivalence then follows from inductively applying the equivalence Mike stated between finite etale commutative K-group schemes and finite discrete Γ_K-modules at each finite level. □

Lemma 1.7. *Let R be a discrete valuation ring with fraction field K of characteristic 0. Let F be any p-divisible group over R and let M be any Γ_K-submodule of $T(F)$ which is a $\mathbb{Z}_p$-direct summand (equivalently, $T(F)/M$ is torsion-free). Then, there exists a p-divisible group E over R and an R-homomorphism $\varphi : E \to F$ inducing closed immersions at finite level and an isomorphism $T(E) \cong M$ via $T(\varphi)$.*

Proof. By the equivalence in the preceding proposition, the submodule $M \subset T(F)$ corresponds to a p-divisible group E^* over K which is a closed subgroup of $F \otimes_R K$ at each finite level. Let $E_v^* \subset F_v \otimes K$ be its finite levels. The scheme-theoretic closure E_v of E_v^* inside F_v is a prolongation of E_v^* over R and clearly a finite flat closed R-subgroup scheme of F_v. By functoriality of scheme-theoretic closure as discussed in Melanie's talk, there exist inclusions

$$u_v : E_v \to E_{v+1}$$

which by construction are closed immersions. Since order can be computed on the generic fiber, each E_v has order p^{vh} where h is the $\mathbb{Z}_p$-rank of M. Furthermore, triviality of maps can be checked on the generic fiber as well so each E_v is killed by p^v. For (E_v, u_v) to form a p-divisible group, it would suffice to show that $E_v \cong E_{v+1}[p^v]$ via u_v. This may not be the case (some $E_{v+1}[p^v]$ may not be R-flat), and so they may not form a p-divisible group.

However, for all i the finite flat R-group E_{i+1}/E_i is killed by p (can be checked on generic fiber), so multiplication by p induces R-homomorphisms

$$E_{i+2}/E_{i+1} \to E_{i+1}/E_i$$

which are isomorphisms between the generic fibers. The E_{i+1}/E_i thereby correspond to a rising chain of R-orders in the finite étale K-algebra $E_1 \otimes_R K$, and so by the noetherian property of R and the R-module finiteness of the integral closure of R in this finite étale K-algebra there exists some i_0 such that the sequence E_{i+1}/E_i stabilizes (i.e., transition maps are isomorphisms) for $i \geq i_0$. Set $E'_v = E_{i_0+v}/E_{i_0}$.

Note that the inclusion $E_{i_0+v} \hookrightarrow E_{i_0+v+1}$ induces an inclusion $u'_v : E'_v \hookrightarrow E'_{v+1}$. I claim that (E'_v, u'_v) forms a p-divisible group.

Consider the following diagram:

$$\begin{array}{ccc} E'_{v+1} = E_{i_0+v+1}/E_{i_0} & \xrightarrow{p^v} & E_{i_0+v+1}/E_{i_0} = E'_{v+1} \\ \downarrow \alpha & & \uparrow \gamma \\ E_{i_0+v+1}/E_{i_0+v} & \xrightarrow{\beta} & E_{i_0+1}/E_{i_0}, \end{array}$$

where α is the canonical projection, γ is the canonical inclusion, and β is induced by multiplication by p^v. By our choice of i_0, the map β is an isomorphism (it is the composite of a bunch of multiplication by p induced maps which are all isomorphisms). Since γ is a closed immersion, it follows that the $\ker(p^v) : E'_{v+1} \to E'_{v+1}$ equals $\ker(\alpha)$. But the kernel of projection, is exactly E_{i_0+v}/E_{i_0} as desired.

There is one last thing to show, which is that E' admits a morphism φ to F over R such that $T(E') \cong M$. The desired morphism comes from the composition

$$E'_v = E_{i_0+v}/E_{i_0} \xrightarrow{p^{i_0}} E_v \subset F_v.$$

□

Proof of Thm 1.2. Let G and H be p-divisible groups over R, and let $f \in \mathrm{Hom}_{\Gamma_K}(T(G), T(H))$ be a homomorphism of their generic fibers. We would like to prolong f to a morphism over R. Consider the graph M of $T(f)$ in $T(G) \times T(H)$, which is clearly a $\mathbb{Z}_p[\Gamma_K]$-submodule. Furthermore, by definition of M, the quotient $(T(G) \times T(H))/M$ injects into $T(H)$ via $(x, y) \mapsto y - T(f)(x)$, so this quotient is torsion-free. Thus, M is a $\mathbb{Z}_p$-linear direct summand of $T(G) \times T(H)$.

We therefore conclude by Lemma 1.7 that there exists a p-divisible subgroup $E \subset G \times H$ such that $T(E)$ maps isomorphically onto M; in other words, $E_K \subset G_K \times H_K$ is the graph of f at each finite level. Thus, the projection $\pi_1 : E \to G$ induces an isomorphism $T(E) \cong T(G)$ and so by Lemma 1.3, π_1 is an isomorphism. It is not hard to see then that

$$\mathrm{pr}_2 \circ \pi_1^{-1} : G \to H$$

is a R-homomorphism prolonging f. □

2. Hodge-Tate Decomposition

From the point of view of p-adic Hodge theory, there are various ways to motivate the material in this section. However, since this is not a seminar on p-adic Hodge theory, I will do my best to give more elementary motivation which may nevertheless be unsatisfying.

Let G be finite flat group scheme over R killed by p. In Rebecca's lecture, we considered $G(\overline{K})$ together with its Galois action. She showed, under particular hypotheses, that the determinant character of the Galois action is determined by the discriminant of G over R. This is an instance where the R-structure tells us something concrete about the Galois structure of the generic fiber. We will be reversing this process using the Galois action to determine things about the integral structure when working with p-divisible groups.

The main question which we answer in a rather remarkable way is: given a p-divisible group G over R, can we recover the dimension of G from the Galois module $T(G)$? The answer will be "yes", but the relationship is not an obvious one.

2.1. Galois modules and the Logarithm.

Let R be a complete discrete valution ring with residue characteristic p, maximal ideal m_R, and fraction field K of characteristic 0. Choose an algebraic (possible infinite) extension of K and equip it with the unique valuation extending the one on R. Let L be the resulting completion, and S its valuation ring. We will be especially interested in the case that L is the completion of an algebraic closure $\overline{K}$ of K. Observe that S is *not* Noetherian when L is not discretely-valued (such as the completion of $\overline{K}$), but it is always m_R-adically separated and complete (yet can fail to be m_S-adically separated, since $m_S = m_S^2$ when L is the completion of $\overline{K}$).

Let G be a p-divisible group over R. We would like to define and study the "S-points" of G, in a sense that takes into account the m_R-adic topology on S. So we make the following definitions:

$$G(B) := \lim_{\to v} G_v(B)$$

for any R-algebra B killed by m_R^i for some i, and

$$G(B) := \lim_{\leftarrow i} G(B/m_R^i B)$$

for any R-algebra B that is separated and complete with respect to the m_R-adic topology (such as $B = S$ above). We topologize $G(B)$ by making $G(B/m_R^i B)$ discrete and taking the topology of the inverse limit.

Remark 2.1. I found this definition extremely confusing at first. I think its best to think about the etale and connected cases separately with $B = S$. For an etale p-divisible group, $G_v(S/m_R^i S) = G_v(S)$ for all v and so the limit over i is constant. If G is connected and $\mathcal{A} \cong R[[X_1, \dots, X_n]]$ is the corresponding formal group, then by using arguments from the proof of the Serre-Tate equivalence (from Mike's lecture) one finds that the natural map $\mathrm{Hom}_{\mathrm{cont},R}(\mathcal{A}, S) \to G(S)$ is an isomorphism, even topological when equipping the right side with its inverse limit topology and the left side with the topology coming from the m_R-adic topology on S; in other words, $G(S)$ is the set of S-points of the formal group over R, equipped with its natural topology arising from that on S. (Here, "continuous" R-algebra homomorphisms are precisely the local R-algebra homomorphisms.) In particular, since $\mathcal{A} \cong R[[X_1, \dots, X_n]]$, $G(S)$ is in topological bijection with the set of n-tuples of elements in the maximal ideal of S. Under the formal group law obtained on this set of n-tuples, most of these points are non-torsion! Hence, in the connected case, $G(S)$ contains many points not seen at the level of the etale generic fiber (see the Example below); we will exploit this.

Example 2.2. Let $G = \mathbb{G}_m(p)$ over R so $G_v = \text{Spec } R[X]/(X^{p^v} - 1)$. Then, consider $G_v(S)$ and $G_v(S/m_R^i S)$. Each is the group of p^vth roots of unity in the respective rings S and $S/m_R^i S$, but whereas the former is finite (as S is a domain), the latter is *huge*. For example, if we consider $1 + y$ for $y \in m_S$, then for fixed i there is some power of p (depending on i) such that

$$(1 + y)^{p^v} \equiv 1 \mod m_R^i.$$

Thus, $\lim_{\to_v} G_v(S/m_R^i S)$ is in bijection with m_S/m_R^i. Hence, $G(S)$ is canonically isomorphic (including in the topological aspect!) to the group of 1-units $U_S^1 = 1 + m_S$ (with the evident m_R-adic topology). Note that $\lim_{\to} \mu_{p^v}(S)$ sits inside $G(S)$ as the torsion subgroup; this is all that is seen from the generic fiber.

Properties of $G(S)$:

- $G(S)$ is a topological $\mathbb{Z}_p$-module via compatible $\mathbb{Z}_p$-action on each $G(S/m_R^i S)$, and it is functorial in S over R.
- $G^{\text{et}}(S) = G^{\text{et}}(S/m_S)$ by the corresponding statement at each finite level.
- For G connected, $G(S)$ is an analytic group over L by identifying its points with $\prod_{i=1}^n m_S$ (equipped with a suitable topological group structure); this is functorial in G and S over R.
- The exact sequence

$$0 \to G_v(S/m_R^i S) \to G(S/m_R^i S) \to^{p^v} G(S/m_R^i S)$$

  when taken to limit over i, shows that the p^v torsion of $G(S)$ is $G_v(S)$. Thus, $G(S)_{\text{tors}} = \lim_{\to} G_v(S)$.
- If $H_S \to G_S$ is a S-homomorphism, then we get an induced homomorphism $G(S) \to H(S)$.

Proposition 2.3. *If the residue field of R is perfect, then the sequence*

$$0 \to G^0(S) \to G(S) \to G^{\text{et}}(S) \to 0$$

is exact.

Proof. The intuition here is that "G is a G^0-torsor over G^{et}" and so since G^0 is "smooth" by Serre-Tate, the morphism $G \to G^{\text{et}}$ is formally smooth. Of course, none of this means much of anything since the p-divisible group is a direct limit of schemes and the morphism $G_v \to G_v^{\text{et}}$ is certainly not formally smooth. I include a rough sketch of the proof which I hope to flesh out in an appendix eventually.

Let $\mathcal{O}(G) = \lim_{\leftarrow} \mathcal{O}(G_v)$ be the inverse limit of the coordinate rings and similarly for G^{et} and G^0. These are topological rings with the inverse limit topology, where the topology on $\mathcal{O}(G_v)$ is as a finite free R-module. In the proof of Serre-Tate equivalence, Mike showed that $\mathcal{O}(G^0) \cong R[[x_1, \ldots, x_n]]$ topologically. It is important to keep track of topologies because we identify $G(S)$ with $\text{Hom}_{\text{cont}}(\mathcal{O}(G), S)$ where S is any m_R-adically complete and separated R-algebra.

The result would then follow if we could construct a continuous R-algebra section to $\mathcal{O}(G^{\text{et}}) \to \mathcal{O}(G)$. This can be done mod m_R because over a perfect field the connected-etale sequence splits uniquely. Over R, the rings $\mathcal{O}(G^{\text{et}})$ and $\mathcal{O}(G)$ are very huge. They are not Noetherian when $G^{\text{et}} \neq 0$; they can have infinitely many idempotents. However, by putting together an appropriate theory of inverse limits of Artin rings and continuous homomorphisms between them, one can lift the section mod m_R to a continuous R-algebra section “as if” there were a theory of formally smooth morphisms at our disposal (as there is for schemes). ☐

Corollary 2.4. *If L is algebraically closed, then $G(S)$ is divisible.*

Proof. By Proposition 2.3, it suffices to consider G^{et} and G^0 separately. For G^{et} this is clear since $G^{\text{et}}(S) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{h^{\text{et}}}$. For G^0, we use that $G^0(S)$ is isomorphic to the S-points of the formal group $\mathcal{A}$. Since the endomorphism $[p]^*$ on the formal group $\mathcal{A}$ is finite and faithfully flat, the fiber over any $x \in G^0(S)$ must be non-empty since L is algebraically closed, using the identification from Remark 2.1 of $G^0(S)$ with local homomorphism $\mathcal{A}$ to S. ☐

The Logarithm

Definition 2.5. The *tangent space* t_G of G is the tangent space of the generic fiber of the formal group associated to G^0. This is naturally a K-vector space of dimension $\dim G$.

Remark 2.6. For any L/K as above, $t_G(L) := L \otimes t_G$ is identified with the tangent space over L of the generic fiber of the base change to S of the R-formal group associated to G^0. Also, if we pass from the R-formal group to its K-analytic Lie group F, we can identify $t_G(K)$ with the commutative Lie algebra $\text{Lie}(F)$.

Recall the following facts from the theory of analytic groups over K and formal groups over R:

(1) For a connected analytic group F over K and $x \in F(L)$, then $\lim_{n\to\infty} p^n x = 0$. That is given any neighborhood U of the identity in $F(L)$, $p^n x \in U$ for $n \gg 0$ depending on x.
(2) There exists an L-analytic homomorphism $\log : F(L) \to \mathrm{Lie}(F(L))$ functorial in L/K and in F_L/L, and an open subgroup $U \subset F(L)$ such that $\log : U \to \mathrm{Lie}(F(L))$ is an isomorphism onto its image.

Since $G^0(S)$ corresponds to the S-points of the associated formal group (see Remark 2.1) which are the L-points of an analytic group of K, we get a continuous logarithm map $\log : G^0(S) \to t_G(L)$ functorial in L/K. We would like to extend this to a homomorphism on all of $G(S)$. We first note that $G^{\mathrm{et}}(S)$ is torsion because $G^{\mathrm{et}}(S) = G^{\mathrm{et}}(S/m_S) = \lim_{\to} G^{\mathrm{et}}_v(S/m_S)$. Thus, for any $x \in G(S)$, there exist n such that $p^n x \in G^0(S)$. Define $\log(x) = (1/p^n)\log(p^n x)$. This is independent of n and satisfies the desired functorialities.

Remark 2.7. It is essential that $\log : G(S) \to t_G(L)$ is functorial with respect to S-homomorphism $G_S \to H_S$. This is not a triviality. The subtlety is that the Serre-Tate construction of the formal group (from which the logarithm derives) only works over a Noetherian base. The ring S is cases of interest is not Noetherian. However, using that G^0_S is a base-change from R, we *can* make the Serre-Tate construction over S by base changing the construction over R; this makes it possible to establish functoriality with respect to homomorphisms over S that need not be defined over any finite extension of R (as will be used in an essential manner later on).

One reason to emphasize functoriality in S over R is seen when $L = \mathbb{C}_K$, as follows. Applying functoriality with respect to R-homomorphisms $\gamma : S \simeq S$ arising from elements of Γ_K, we deduce that log is Γ_K-equivariant when $G(S)$ is equipped with a Γ_K-action coming from the Γ_K-action on S over R.

Proposition 2.8. (1) *The kernel of* log *is* $G(S)_{\mathrm{tors}}$. *In particular, if L is algebraically closed, then* $\ker(\log) = \Phi(G)$.
(2) *In general,* $\log(G(S))$ *is a $\mathbb{Z}_p$-submodule M of the finite dimensional L vector space* $t_G(L)$ *such that* $M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = t_G(L)$. *If L is algebraically closed, then* $\log(G(S)) = t_G(L)$.

Proof. For (1), clearly the torsion is contained in the kernel, since $t_G(L)$ is torsion free. Let $x \in \ker(\log)$. Since G^{et} is torsion, there exist some n_0 such that for $n \geq n_o$, $p^n x \in G^0(S)$. On some open subgroup $U \subset G^0(S)$, log is an isomorphism and there exists some possibly larger n such that $p^n x \in U$. But then $\log(p^n x) = 0$ implies $p^n x = 0$.

For (2), the map $\log|_U$ is an isomorphism on tangent spaces so by the L-analytic *inverse function theorem*, its image must be an *open* subgroup of $t_G(L)$. Thus, the cokernel $t_G(L)/\log(G(S))$ is torsion, since p is topologically nilpotent on $t_G(L)$. This gives the result that

$$\log(G(S)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = t_G(L).$$

In Corollary 2.4, we saw that if L is algebraically closed then $G(S)$ is divisible. In that case, $\log(G(S))$ is also divisible and so $\log(G(S)) \cong \log(G(S)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. □

The conclusion of this section is that if we take $L = \mathbb{C}_K = \widehat{\overline{K}}$, then we have the extremely useful exact sequence of Γ_K-modules

$$1 \to \Phi(G) \to G(\mathcal{O}_{\mathbb{C}_K}) \xrightarrow{\log} t_G(\mathbb{C}_K) \to 0.$$

This is the bit of extra structure on $G(\mathcal{O}_{\mathbb{C}_K})$ which has consequences that can be detected for the Galois action on the Tate module of G.

Example 2.9. In the case of $\mathbb{G}_m$, the exact sequence is

$$1 \to \mu_{p^\infty} \to U \to \mathbb{C}_K \to 0$$

where $U = 1 + m_{\mathbb{C}_K}$ and the p-adic logarithm map is the classical $x \mapsto \log(x)$. It is due to the convergence properties of the p-adic logarithm map that it is surjective in this situation, since $m_{\mathbb{C}_K}$ has elements with absolute value arbitrarily close to 1.

2.2. **Exploiting Duality.**

For this section, let G' denote the p-divisible group dual to G. Also, let $D = \mathcal{O}_{\mathbb{C}_K}$.

Proposition 2.10. *We have a natural isomorphism of $\mathbb{Z}_p[\Gamma_K]$-modules*

$$T(G') \xrightarrow{\sim} \mathrm{Hom}_D(G_D, \mathbb{G}_m(p)),$$

where G_D denotes the p-divisible group over D obtained from base change and Hom_D *denotes the group of homomorphisms as p-divisible groups over D.*

Proof. Recall that the Cartier dual is defined such that $G'_v(D) \cong \mathrm{Hom}_D(G_v \otimes_R D, \mathbb{G}_m)$. Since G_v is killed by p^v, we get naturally

$$G'_v(D) \cong \mathrm{Hom}_D(G_v \otimes_R D, \mathbb{G}_m[p^v]).$$

We now want to pass to the limit. By definition, $T(G')$ is $\lim_{\leftarrow}(G'_v(D))$, the limit taken with respect to the multiplication by p maps. Recall that because G'_v is finite over R, $G'_v(D) = G'_v(\mathbb{C}_K)$.

Let $\varphi \in \mathrm{Hom}_D(G_{v+1} \otimes_R D, \mathbb{G}_m[p^{v+1}])$. The multiplication by p map $G'_{v+1} \to G'_v$ is dual to the inclusion $i_v : G_v \to G_{v+1}$. In other words, in the diagram,

$$\begin{array}{ccc} G'_{v+1}(D) & \xrightarrow{\sim} & \mathrm{Hom}_D(G_{v+1} \otimes_R D, \mathbb{G}_m) \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle h} \\ G'_v(D) & \xrightarrow{\sim} & \mathrm{Hom}_D(G_v \otimes_R D, \mathbb{G}_m) \end{array}$$

the map h is composition with $i_v : G_v \to G_{v+1}$.

A system of elements $x_v \in G'_v(D)$ such that $px_{v+1} = x_v$ is equivalent to a sequence of the maps $\varphi_v \in \mathrm{Hom}_D(G_v \otimes_R D, \mathbb{G}_m)$ such that $\varphi_{v+1} \circ i_v = \varphi_v$.

Since G_v is killed by p^v, φ_v automatically factors through the p^v-torsion $\mathbb{G}_m[p^v]$ and so the sequence φ_v is exactly a homomorphism of p-divisible groups from G_D to $\mathbb{G}_m(p)$. □

Using that any homomorphism $\varphi : G_D \to \mathbb{G}_m(p)$ induces a homomorphism at the level of D-points and at the level of tangent spaces (by functoriality over D), we get pairings

$$T(G') \times G(D) \to (\mathbb{G}_m(p)(D)) \cong U$$

and

$$T(G') \times t_G(\mathbb{C}_K) \to t_{\mathbb{G}_m(p)}(\mathbb{C}_K) \cong \mathbb{C}_K$$

compatible with the logarithm maps.

Note also that all the pairings are $\Gamma_K := \mathrm{Gal}(\overline{K}/K)$-equivariant.

Using the structure on $G(D)$ given by the logarithm, we intend to use the pairings to find previously unknown structure on $T(G')$. Note that $T(G')$ is free of rank h over $\mathbb{Z}_p$ and we get the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Phi(G) & \longrightarrow & G(D) & \xrightarrow{\log} & t_G(\mathbb{C}_K) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle d\alpha} & & \\ 0 & \longrightarrow & \mathrm{Hom}(T(G'), \mu_{p^\infty}) & \longrightarrow & \mathrm{Hom}(T(G'), U) & \longrightarrow & \mathrm{Hom}(T(G'), \mathbb{C}_K) & \longrightarrow & 0 \end{array}$$

where the Homs in the bottom row are all $\mathbb{Z}_p$-homs and again the vertical arrows are Γ_K-equivariant. (Recall Γ_K acts on $\mathrm{Hom}(M, N)$ by $(\sigma(f))(m) = \sigma(f(\sigma^{-1}m)))$. Note that the commutativity of the right square in this diagrams rests on the functoriality of the logarithm with respect to D-homomorphisms that may not be defined over any finite extension of R.

2.3. **Main Result.** We are getting closer to our desired result, which was to read off the dimension of our p-divisible group G from its Galois representation $T(G)$. The key will be understanding the map $d\alpha$, which turns out to be injective identitifying $t_G(\mathbb{C}_K)$ with a $(\dim G)$-dimensional $\mathbb{C}_K$-subspace of $\mathrm{Hom}(T(G'), \mathbb{C}_K)$. Since $T(G')$ is determined by $T(G)$, it suffices then to identify this subspace using the Galois action on space of homomorphisms. This is what we will do.

The key input will be Thm 3.1 which you should take a look at before continuing. In particular, we will make extensive use of the following surprisingly difficult fact which will be proved later:

$$(\mathbb{C}_K)^{\Gamma_K} = K \tag{1}$$

i.e. the only Galois invariants of the completion of $\overline{K}$ are just K itself.

Lemma 2.11. *We have $t_G(\mathbb{C}_K)^{\Gamma_K} = t_G(K)$. Furthermore, if W is any finite-dimension $\mathbb{C}_K$-vector space on which Γ_K-acts semi-linearly (that is $\sigma(cw) = \sigma(c)\sigma(w)$), then $W^{\Gamma_K} \otimes_K \mathbb{C}_K \to W$ is injective.*

Proof. Choose any K-linear isomorphism $t_G(K) \cong K^n$. This induces a Γ_K-equivariant, $\mathbb{C}_K$-linear isomorphism $t_G(K) \otimes \mathbb{C}_K = t_G(\mathbb{C}_K) \cong \mathbb{C}_K^n$ and the result follows from (1). For the second part, it suffices to show that any set $w_i \in W^{\Gamma_K}$ of K-linearly independent vectors remain linearly independent over $\mathbb{C}_K$ in W. Pick the shortest hypothetical relation $\sum c_i w_i$, and scale so c_1 is 1. For any $\sigma \in \Gamma_K$, we have

$$\sum (\sigma(c_i) - c_i) w_i = 0$$

using that the w_i are Γ_K-invariant. But since $c_1 = 1$, we have $\sigma(c_1) - c_1 = 0$ so we have a shorter relation and thus $\sigma(c_i) = c_i$ for all σ. Using (1), we get $c_i \in K$ contradicting K-independence of the w_i. □

Proposition 2.12. *α_0 is bijective; α and $d\alpha$ are injective.*

Proof. **Step 1**: *α_0 is bijective.* Note this is purely a statement about points of the generic fiber of all groups involved. As a result, it follows quite directly from the perfect duality at finite level

$$G_v(\mathbb{C}_K) \times G'_v(\mathbb{C}_K) \to \mu_{p^v}$$

of Γ_K-modules. Note this is also how one would prove that the natural map

$$T(G) \to \mathrm{Hom}(T(G'), T(\mathbb{G}_m(p)))$$

as Galois modules is an isomorphism. As is customary, I denote $T(\mathbb{G}_m(p))$ by $\mathbb{Z}_p(1)$ to indicate that it is given by the p-adic cyclotomic character.

Step 2: $\ker\alpha$ *and* $\operatorname{coker}\alpha$ *are vector spaces over* $\mathbb{Q}_p$. A priori, they are only $\mathbb{Z}_p$-modules since the vertical arrows are only $\mathbb{Z}_p$-homomorphisms. However, by snake lemma the kernel and cokernel of α are isomorphic to the kernel and cokernel of $d\alpha$. Since both $t_G(\mathbb{C}_K)$ and $\operatorname{Hom}(T', \mathbb{C}_K)$ are $\mathbb{Q}_p$ vector spaces, and any $\mathbb{Z}_p$-linear map of $\mathbb{Q}_p$-vector spaces is automatically $\mathbb{Q}_p$-linear, the kernel and cokernel of $d\alpha$ are $\mathbb{Q}_p$-vector spaces.

Step 3: *We have* $G(D)^{\Gamma_K} = G(R)$. Taking the Γ_K-invariants of the exact sequence,

$$1 \to G^0(D) \to G(D) \to G^{\text{et}}(D) \to 1$$

we get

$$1 \to G^0(D)^{\Gamma_K} \to G(D)^{\Gamma_K} \to G^{\text{et}}(R)$$

which is right-exact since $G(R) \subset G(D)^{\Gamma_K}$. However, we have a Γ_K-equivariant description of $G^0(D)$ as n-tuples of elements in the maximal ideal $m_{\mathbb{C}_K}$ (which is Γ_K-equivariant), and given (1), it's not hard to see the $m_{\mathbb{C}_K}^{\Gamma_K} = m_R$. Thus, $G^0(D)^{\Gamma_K} = G^0(R)$.

Step 4: α *is injective on* $G(R)$. The main content is in the case of G connected. I leave it to the reader to perform the devissage from there. Consider $\ker(\alpha) \subset G(R)$ where $G(R)$ is now points of a formal group over R. Since $\ker(\alpha)$ is a $\mathbb{Q}_p$-vector space, it is stable under multiplication by p. However, in the formal group, we have $\cap p^v G(R) = 0$, since the valuation on R is discrete. This uses that in formal group multiplication by p looks like $pX + O(X^2)$.

Step 5: *The map* $d\alpha$ *is injective on* $t_G(K)$. From Step 1 and 4, $d\alpha$ is injective on $\log(G(R))$ which spans $t_G(K)$ as a $\mathbb{Q}_p$-vector space.

Step 6: *The map* $d\alpha$ *is injective.* We apply Lemma 2.11 and Step 5. ☐

Theorem 2.13. *The maps*

$$G(R) \xrightarrow{\alpha_R} \operatorname{Hom}_{\Gamma_K}(T(G'), U)$$

and

$$t_G(K) \xrightarrow{d\alpha_R} \operatorname{Hom}_{\Gamma_K}(T(G'), \mathbb{C}_K)$$

induced by α *and* $d\alpha$ *are bijective.*

Proof. We already know that α_R and $d\alpha_R$ are injective. Taking Γ_K-invariants of the exact sequence

$$0 \to G(D) \to \operatorname{Hom}(T(G'), U) \to \operatorname{coker}(\alpha) \to 0$$

yields a left-exact sequence

$$0 \to G(R) \to \operatorname{Hom}_{\Gamma_K}(T(G'), U) \to \operatorname{coker}(\alpha)^{\Gamma_K}.$$

Exactness in the middle tells us that $\operatorname{coker}(\alpha_R) \subset \operatorname{coker}(\alpha)^{\Gamma_K}$. The same argument works for $d\alpha_R$.

Since $\operatorname{coker}\alpha \to \operatorname{coker} d\alpha$ is bijective, $\operatorname{coker}(\alpha_R) \subset \operatorname{coker}(d\alpha_R)$, so it suffices to show the latter is 0. Since $d\alpha_R$ is K-linear and injective, we are reduced to counting dimensions.

Set $W' = \operatorname{Hom}(T(G'), \mathbb{C}_K)$ and $W = \operatorname{Hom}(T(G), \mathbb{C}_K)$. These are both finite-dimensional $\mathbb{C}_K$-vector spaces of dimension $h = ht(G)$ on which Γ_K acts semi-linearly. By Lemma 2.11, we know that if we let $d = \dim_K(W^{\Gamma_K})$ and $d' = \dim_K(W'^{\Gamma_K})$, then $d, d' \leq h$.

Letting $n = \dim G$ and $n' = \dim G'$. The injectivity of $d\alpha$ for both G and G' tells us that $d' \geq n$ and $d \geq n'$. We also know from Mike's talk that $n + n' = h$. To get equality and hence surjectivity, it suffices to show that

$$d + d' \leq h.$$

As Galois modules, we saw that

$$T(G) \cong \operatorname{Hom}(T(G'), \mathbb{Z}_p(1)) = \operatorname{Hom}(T(G'), \mathbb{Z}_p)(-1)$$

where (-1) denotes twisting by the inverse of the cyclotomic character. Twisting both sides by $\mathbb{Z}_p(1)$ and tensoring up to $\mathbb{C}_K$, we see that

$$W' = \operatorname{Hom}(T(G'), \mathbb{C}_K) = (T(G) \otimes \mathbb{C}_K)(1).$$

We clearly then get a non-degenerate Galois equivariant $\mathbb{C}_K$-linear pairing

$$W \times W' \to \mathbb{C}_K(1).$$

But then, $W^{\Gamma_K} \times W^{\Gamma_K}$ must pair into $\mathbb{C}_K(1)^{\Gamma_K}$. The second part of Thm 3.1 tells us that $\mathbb{C}_K(1)^{\Gamma_K} = 0$, applied with χ equal to p-adic cyclotomic character. Thus, W^{Γ_K} and W'^{Γ_K} are orthogonal subspaces. Clearly then, $W^{\Gamma_K} \otimes \mathbb{C}_K$ and $W'^{\Gamma_K} \otimes \mathbb{C}_K$ are also orthogonal subspaces of $\mathbb{C}_K$-dimensions d and d' respectively. By non-degeneracy, we must have

$$d + d' \leq \dim W = \dim W' = h.$$

□

Corollary 2.14. *The dimension of G is given in terms of the Tate module by*

$$\dim G = \dim_K(\operatorname{Hom}_{\Gamma_K}(T(G'), \mathbb{C}_K) = \dim_K(T(G) \otimes \mathbb{C}_K(1))^{\Gamma_K}.$$

It remains to address the Hodge-Tate decomposition, which is the title of this section.

Corollary 2.15. *There is a canonical isomorphism of $\mathbb{C}_K[\Gamma_K]$-modules*

$$\operatorname{Hom}(T(G), \mathbb{C}_K) \cong t_{G'}(\mathbb{C}_K) \oplus t_G^*(\mathbb{C}_K)(-1)$$

where t_G^* is the K-linear dual of the tangent space of G.

This is called the Hodge-Tate decomposition for a p-divisible group.

Proof. In the proof of Thm 2.13, we saw that under the pairing

$$W \times W' \to \mathbb{C}_K(1)$$

the subspaces given by $t_G(\mathbb{C}_K)$ and $t_{G'}(\mathbb{C}_K)$ were orthogonal of the largest possible dimension. This gives us an exact sequence

$$0 \to t_{G'}(\mathbb{C}_K) \to \mathrm{Hom}(T(G), \mathbb{C}_K) \to \mathrm{Hom}(t_G(\mathbb{C}_K), \mathbb{C}_K(1)) \to 0.$$

The last term in the sequence is isomorphic to $t_G^*(\mathbb{C}_K)(-1)$ as a Galois-module.

We claim this exact sequence splits and splits uniquely. The existence of a splitting follows from $H^1(\Gamma_K, \mathbb{C}_K(-1)) = 0$ by Thm 3.1 (using an appropriate notion of continuous $H^1(\Gamma_K, \cdot)$. The uniqueness follows from the vanishing of $H^0(\Gamma_K, \mathbb{C}_K(-1))$ (see Thm 3.1). □

Proposition 2.16. *Let A be an abelian variety over K with good reduction. Then, canonically*

$$H^1_{\mathrm{et}}(A_{\overline{K}}, \mathbb{Q}_p) \otimes \mathbb{C}_K \cong (H^1(A, \mathcal{O}_A) \otimes_K \mathbb{C}_K) \oplus (H^0(A, \Omega^1_{A/K}) \otimes_K \mathbb{C}_K(-1))$$

as both $\mathbb{C}_K$ and Γ_K-modules.

Remark 2.17. The similarity between this and the Hodge decomposition for complex cohomology is what gives rise to the name Hodge-Tate decomposition. A similar decomposition holds for the etale cohomology of any smooth proper K-scheme. This was conjectured by Tate [6] and proved by Faltings.

Proof. Let G be the p-divisible group of the Néron model over R (an abelian scheme). The etale cohomology is dual to the Tate-module so we can identify $H^1_{\mathrm{et}}(A_{\overline{K}}, \mathbb{Q}_p) \otimes \mathbb{C}_K$ with $\mathrm{Hom}(T(G), \mathbb{C}_K)$. I claim that

$$H^1(A, \mathcal{O}_A) \cong t_{G'}$$

and that

$$t_G^* \to H^0(A, \Omega^1_{A/K}).$$

There is a lot that goes into these statements. First, we need to identify t_G over R with the tangent space of the Néron model at the identity. This amounts to agreement of the formal groups associated to an abelian R-scheme and its p-divisible group, which Mike discussed. The harder input is the compatibility of duality for p-divisible groups over R with duality of abelian schemes over R (which we haven't discussed, and was proved by Oda in his thesis for abelian schemes over any base scheme). Granting these, we conclude via the following isomorphisms for abelian varieties X over any field F:

$$t_e(X') \cong H^1(X, \mathcal{O}_X)$$

and

$$t_e^*(X) \cong H^0(X, \Omega^1_{X/F})$$

the first by Mumford [2] §13 Cor. 3 (which is applicable over any field, not necessarily algebraically closed) and the second by using left-invariant differentials (See Cor. 3, § 4.2 of Neron Models [1]). □

3. Cohomological Input

All of the cohomology below is with respect to continuous cochains.

Theorem 3.1. *Let $\chi : \Gamma_K \to \mathbb{Z}_p^*$ be a continuous character. Let L be the splitting field of this character.*

(1) *We have $H^0(\Gamma_K, \mathbb{C}_K) = K$, and $H^1(\Gamma_K, \mathbb{C}_K)$ is a one-dimensional vector space over K.*
(2) *Suppose there exists a finite extension L_0/K contained in L such that L/L_0 is a totally ramified $\mathbb{Z}_p$-extension. Then,*

$$H^0(\Gamma_K, \mathbb{C}_K(\chi)) = 0 \text{ and } H^1(\Gamma_K, \mathbb{C}_K(\chi)) = 0.$$

The proof of these results will require the full force of the detailed ramification theory discussed in the Appendix.

3.1. Finite Extensions of K_∞.

We begin by choosing a ramified $\mathbb{Z}_p$-extension K_∞ and studying finite extension L of K_∞. If K_n/K denotes the unique subfield of K_∞ of degree p^n, then for $n \gg 0$, K_∞/K_n is totally ramified. The key result is that L/K_∞ is "almost etale" meaning that its discriminant is "almost" the unit ideal. This result will allow us to extend cohomology results from the algebraic K_∞ to the non-algebraic completion $\mathbb{C}_K$.

Denote by R_L the ring of integers of L and m_∞ the maximal ideal of R_∞.

Proposition 3.2. *We have $\mathrm{Tr}_{L/K_\infty}(R_L) \supset m_\infty$.*

Proof. The argument is an extension of the arguments made in §4.2 which are somewhat technical. This is consequence of the "almost etaleness" mentioned earlier. I refer the interested reader to §13 in Brian's CMI Notes on p-adic Hodge Theory. □

Now let L/K_∞ be a finite Galois extension with Galois group G. We now study the continuous co-chains $C^i(G, L)$ with the goal of studying cohomology with coefficients in $\mathbb{C}_K$.

Definition 3.3. If $f \in C^i(G, L)$, then define $|f|$ to be the maximum of the values $|f(g_1, \ldots, g_i)|$ where absolute value is normalized with respect to the base K. This is a non-archimedian absolute value on the space $C^i(G, L)$ since co-chains are added pointwise.

Corollary 3.4. *Let $f \in C^r(G, L)$ with $r \geq 1$, and let $c > 1$. Then there exists an $(r-1)$-cochain g such that*

$$|f - dg| \leq c|df|, \text{ and } |g| \leq c|f|.$$

By a (-1)-cochain, we mean $x \in L$ with $d(x) = \mathrm{Tr}_{L/K_\infty}(x)$.

Proof. For this proof, we denote Tr_{L/K_∞} by Tr. Since m_∞ contains elements with valuation arbitrarily close to 1, Prop. 3.2 says that there exists $x \in R_L$ (i.e. $|x| \leq 1$) such that

$$|\mathrm{Tr}(x)| > c^{-1}.$$

Case $r = 0$: A 0-cochain is just an element $y \in L$. Take $g = \frac{xy}{\mathrm{Tr}(x)}$. Clearly, we get

$$|g| \leq c|y|.$$

Now,

$$|f - dg||\mathrm{Tr}(x)| = |\mathrm{Tr}(x)y - \mathrm{Tr}(xy)| = |\sum_{\sigma \in G}(\sigma(x)y - \sigma(x)\sigma(y))| \leq |\sum_{\sigma \in G}(y - \sigma(y))|$$

since $|x| \leq 1$. Since $y - \sigma(y) = dy(\sigma)$, we get

$$|f - dg|c^{-1} \leq |f - dg||\mathrm{Tr}(x)| \leq |dy|$$

as desired.

Case $r > 0$: The construction made in the case $i = 0$ can be generalized by defining an $(r-1)$-cochain by

$$(x \cup f)(s_1, \ldots, s_{r-1}) = (-1)^r \sum_{s \in G} s_1 \cdots s_{r-1} s x \cdot f(s_1, \ldots, s_{r-1}, s)$$

where x is the (-1)-cochain as above. One then checks that the following identity

$$(dx)(f) - d(x \cup f) = x \cup (df)$$

holds. We take $g = (x \cup f)/dx$. Thus,

$$f - dg = \frac{x \cup df}{dx}.$$

Since $|x| \leq 1$, $|x \cup df| \leq |df|$ and so the first inquality follows from $|dx| \geq c^{-1}$. Similarly, $|x \cup f| \leq |f|$ implies the second inequality. □

Corollary 3.5. *Let $G = \mathrm{Gal}(\overline{K}/K_\infty)$ and consider continuous co-chains with values in $\overline{K}$ with the discrete topology on $\overline{K}$ and the pro-finite topology on G. Denote these by $C^r_{\text{disc}}(\Gamma_{K_\infty}, \overline{K})$. Then the result of Cor 3.4 still holds when $r > 0$. For $r = 0$, we have that for any $y \in \overline{K}$, there exists $x \in K_\infty$ such that $|y - x| \leq |dy|$.*

Proof. We have that

$$C^r_{\text{disc}}(\Gamma_{K_\infty}, \overline{K}) = \lim_{\rightarrow} C^r_{\text{disc}}(\mathrm{Gal}(L/K_\infty, L)$$

over Galois extensions L (Serre [5] §2.2.) This implies the result for $r > 0$ using Cor. 3.4.

Similarly, any $y \in \overline{K}$ lies in some finite Galois extension L, and then our desired x is just the trace of the x from Cor. 3.4. □

Remark 3.6 (Continuity). The issues of cochain continuity are extremely confusing. Our Galois groups always have the same topology, but for the coefficients we can either use discrete topology or p-adic topology. The p-adic topology is a weaker topology and so there are actually *more* p-adically continuous co-chains than discrete ones. In the next Proposition, we approximate p-adic cochains with discretely continuous co-chains (which are easier to work with).

Proposition 3.7. *Let Γ_{K_∞} be the absolute Galois group of K_∞. Then, we have $H^0(\Gamma_{K_\infty}, \mathbb{C}_K) = \widehat{K}_\infty$ and $H^i(\Gamma_{K_\infty}, \mathbb{C}_K) = 0$ for $i > 0$.*

Proof. The difficulty as usual lies in the continuity issues. We first show that each continuous cochain f is the limit of cochains f_v with values in $\overline{K}$ with the discrete topology.

Let $\pi \in \mathbb{C}_K$ with $\mathrm{val}(\pi) > 0$ and let D be the valuation ring of $\mathbb{C}_K$. Then, $\pi^v D$ forms a basis of open neighborhoods of 0 in $\mathbb{C}_K$. Since $\overline{K}$ is dense in $\mathbb{C}_K$, the natural map of sets

$$\overline{K} \xrightarrow{\rho_v} \mathbb{C}_K/\pi^v D$$

is surjective since the right is a discrete quotient of $\mathbb{C}_K$. We can choose a section φ_v to ρ_v for each v, and it is automatically continuous. Note the section φ_v is only set-theoretic and does not have any additive properties. Set $f_v = \varphi_v \rho_v f$. This is a continuous co-chain with values in $\overline{K}$ where the topology on $\overline{K}$ is discrete. This is because $\mathbb{C}_K/\pi^v D$ has a discrete topology. Furthermore, we have

$$f_v \equiv f \mod \pi^v D$$

by construction, so $|f - f_v| \leq |\pi|^v$.

Case $i = 0$: In this case, the cocycle f is just a Γ_{K_∞}-invariant element $y \in \mathbb{C}_K$. We will show that y is in the closure of K_∞, which we shall call X. Let $y = \lim y_v$ for some sequence $y_v \in \overline{K}$.

Then, Cor. 3.5 says that there exists $x_v \in K_\infty$ such that

$$|y_v - x_v| \leq |d(y_v)|.$$

However, $|d(y_v)| \leq |d(y - y_v)| \leq |y - y_v|$ which goes to zero. Thus, $\lim x_v = y$ as desired.

Case $i > 0$: Now let f be a continuous i-cocycle. We would like to construct g such that $dg = f$. Choose f_v as above in $C^i_{\text{disc}}(\Gamma_{K_\infty}, \overline{K})$. By Cor 3.5, there exist $(i-1)$-cochains h_v such that

$$|f_v - dg_v| \leq c|df_v|, \text{ and } |g_v| \leq c|f_v|.$$

where c is a fixed constant > 1. If we knew g_v were Cauchy, we would be done because $dg_v \to f$, but there is no reason this has to be the case. However, applying the lemma again, there exists $(i-2)$-cochains h_v such that

$$|g_{v+1} - g_v - dh_v| \leq c|d(g_{v+1}) - dg_v|$$

and the right side is going to zero since dg_v is a Cauchy sequence. In the case $i = 1$, the g_v are already 0-cochains, but we can take $dh_v = x_v \in K_\infty$ which a 0-cocycle (which is all we need). Thus,

$$g := \sum_{v=1}^{\infty} (g_{v+1} - g_v - dh_v)$$

converges, and it's clear that $d(g + g_1) = \lim dg_v = f$.

□

3.2. **Putting it all together.**

Proof of Thm 3.1. Let $X = \widehat{K}_\infty$. We start with the 0th cohomology. We have

$$H^0(\Gamma_K, \mathbb{C}_K) = H^0(\text{Gal}(K_\infty/K), H^0(\Gamma_{K_\infty}, (\mathbb{C}_K))).$$

By Prop. 3.7, $H^0(\Gamma_{K_\infty}, (\mathbb{C}_K)) = X$ and by Thm 4.12, $H^0(\text{Gal}(K_\infty/K), X) = K$.

For H^1, we use the inflation-restriction sequence

$$0 \to H^1(\text{Gal}(K_\infty/K), H^0(\Gamma_{K_\infty}, (\mathbb{C}_K))) \to H^1(\Gamma_K, \mathbb{C}_K) \to H^1(\Gamma_{K_\infty}, \mathbb{C}_K)$$

which holds just as well for cohomology with continuous cochains (see proof in VII.6 of Local Fields [5]). By Prop. 3.7 the rightmost term is 0, and $H^1(\text{Gal}(K_\infty/K), H^0(\Gamma_{K_\infty}(\mathbb{C}_K))) = H^1(\text{Gal}(K_\infty/K), X)$ which by Thm 4.12 is 0.

For the second part of the theorem, we first apply a similar argument with K replaced by L_0 to show that

$$H^0(\Gamma_{L_0}, \mathbb{C}_K(\chi)) = H^0(\text{Gal}(L_\infty/L_0), X(\chi))$$

which equals zero by Thm 4.12 since χ has infinite image. This clearly implies $H^0(\Gamma_K, \mathbb{C}_K(\chi)) = 0$.

Since $H^0(\Gamma_{L_0}, \mathbb{C}_K(\chi)) = 0$, inflation-restriction implies that

$$H^1(\Gamma_K, \mathbb{C}_K(\chi)) \cong H^1(\Gamma_{L_0}, \mathbb{C}_K(\chi)).$$

Again, applying inflation-restriction for L_∞/L_0, gives

$$H^1(\mathrm{Gal}(L_\infty/L_0), X(\chi)) \cong H^1(\Gamma_{L_0}, \mathbb{C}_K(\chi)),$$

and the left side is 0 by Thm 4.12 so we are done.

□

4. Appendix

4.1. **Ramification Theory.** In this section, we review higher ramification theory with a goal of studying how the discriminant behaves in a $\mathbb{Z}_p$-extension. This is a necessary input into Tate's result on p-divisible groups.

Let L/K be a finite Galois extension, where K is a complete discretely valued field of char 0, whose residue field is perfect of char $p > 0$. Let v_L be the valuation on L normalized so that a uniformizer has valuation 1. Note if v_K is the unique extension of normalized valuation of K. Then,

$$v_K = (1/e_{L/K})v_L.$$

Let $G = \mathrm{Gal}(L/K)$. The lower numbering subgroups are defined by $G_{-1} = G$ and

$$G_i = \{g \in G \mid v_L(g(x) - x) \geq i + 1, \forall x \in \mathcal{O}_L\}.$$

In fact, it is not necessary to check the condition for all $x \in \mathcal{O}_L$, just one that generates L; such an x exists due to perfectness of the residue field (See Lemma 1 in IV.1 of Local Fields [5]). This defines a decreasing sequence of normal subgroups of G.

The following important formula relates different of L/K, $\mathcal{D}_{L/K}$, to the higher ramification groups.

Proposition 4.1. *For any finite Galois extension L/K, then*

$$v_K(\mathcal{D}_{L/K}) = (1/e_{L/K})\sum_{i=0}^{\infty}(|G_i| - 1).$$

Proof. Prop. 4 in IV.1 of Local Fields [5] states that

$$v_L(\mathcal{D}_{L/K}) = \sum_{i=0}^{\infty}(|G_i| - 1).$$

Since $v_K(\mathcal{D}_{L/K}) = (1/e_{L/K})v_L(\mathcal{D}_{L/K})$, we get that

$$v_K(\mathcal{D}_{L/K}) = (1/e_{L/K})\sum_{i=0}^{\infty}(|G_i| - 1).$$

□

Lower numbering is well-behaved with respect to subgroups, but not quotients. Since we want to study a tower of extensions, it is necessary to work with the so-called upper numbering which behaves well with respect to quotients.

I will define them here for the purpose of proving a corresponding discriminant formula. For more information, see Local Fields [5] IV.3.

Definition 4.2. For any $u \in [-1, \infty)$, consider the function

$$\varphi(u) = \int_0^u \frac{dt}{(G_0 : G_t)}$$

where $G_t = G_{\lceil t \rceil}$. φ is continuous, piece-wise linear, increasing function and we define the upper-numbering groups by

$$G^{\varphi(u)} = G_u.$$

This defined the upper-numbering groups for all $v \in [-1, \infty)$ uniquely by the above properties of φ.

Concretely, we have that $G^{-1} = G_{-1}$ and $G^v = G_i$ for $v \in (\varphi(i-1), \varphi(i)]$. Note that $\varphi(i)$ need not be an integer.

Proposition 4.3. *Let L/K be finite Galois extension, then*

$$v_K(\mathcal{D}_{L/K}) = \int_{-1}^{\infty} (1 - \frac{1}{|G^v|})dv.$$

Proof. Essentially, we just want to rewrite the integral in terms of lower numbering and then apply the previous formula for the different. Noting as above that $|G^v|$ is constant on $(\varphi(i-1), \varphi(i)]$, we can rewrite the integral as

$$\int_{-1}^{\infty} (1 - \frac{1}{|G^v|})dv = \sum_{i=0}^{\infty}(\varphi(i) - \varphi(i-1))(1 - 1/|G_i|).$$

Looking closely at how φ is defined, we see that

$$\varphi(i) = \frac{1}{g_0}(g_1 + \ldots + g_i)$$

for $i \geq 1$, $\varphi(0) = 0$, and $\varphi(-1) = -1$ where $g_i = |G_i|$. Thus,

$$\sum_{i=0}^{\infty}(\varphi(i) - \varphi(i-1))(1 - 1/|G_i|) = (1 - 1/g_0) + \sum_{i=1}^{\infty} \frac{g_i}{g_0}(1 - 1/g_i) = \frac{1}{g_0}\sum_{i=0}^{\infty}(1 - g_i) = 1/e_{L/K}\sum_{i=0}^{\infty}(1 - g_i)$$

because g_0 is the size of the inertia group. □

The last result we need tells us how the higher ramification groups behave with respect to the local reciprocity map from local class field theory.

Proposition 4.4. *Let K be a complete discretely valued field with finite residue field, and let G denote $\mathrm{Gal}(K^{\mathrm{ab}}/K)$. Then the class field theory isomorphism, $O_K^* \to I_{K_K^{ab}} = G^0$ identifies U_K^i with G^i, where U_K^i is the units congruent to 1 modulo m_K^i.*

Proof. See Chap. XV of Local Fields [5]. □

Remark 4.5. We will also need an analogue of Prop. 4.4 when the residue field is not finite but is algebraically closed. The proper statement is too complicated to be made here. However, whenever we invoke Prop. 4.4 below, there is an analogue in this case which makes the theory work. See Serre [4] for details.

4.2. **Construction of Normalized Trace for $\mathbb{Z}_p$-Extensions.** Let K_∞ be an infinite Galois extension of K which is totally ramified with Galois group $G \cong \mathbb{Z}_p$. Let K_n be the subfield of K corresponding to subgroup $G(n) = p^n\mathbb{Z}_p$. It is a totally ramified extension of degree p^n. Let v denote valuation on K_∞ normalized with respect to uniformizer of K, and let $|\cdot|$ be corresponding absolute value.

The goal of this section is to show that the function

$$t(x) = p^{-n}\mathrm{Tr}_{K_n/K}(x)$$

is a continuous function from $K_\infty \to K$, and thus extends to a K-linear function on the completion X of K_∞.

The key input will be computation of the valuation of the different of K_{n+1}/K_n. The different controls the contraction in the trace pairing, as related in the following result from Local Fields [5].

Proposition 4.6. *Let L/K be a finite extension and let $\mathfrak{b}$ and $\mathfrak{a}$ be fractional ideals of L and K respectively. Then,*

$$\mathrm{Tr}_{L/K}(\mathfrak{b}) \subset \mathfrak{a}$$

if and only if

$$\mathfrak{b} \subset \mathfrak{a}\mathcal{D}_{L/K}^{-1}.$$

Proof. See Proposition 18 in Section I.6 of Local Fields [5]. □

The intuition here is higher the valuation of the different, the more contraction there is in the trace map. Keeping this in mind, we proceed with the computation of the discriminant.

Proposition 4.7. *There exists a constant c such that*

$$v(\mathcal{D}_{K_n/K}) = en + c + p^{-n}a_n$$

where the sequence a_n is bounded.

Proof. Since K_∞ is totally ramified, it corresponds by class field theory to a surjective continuous map

$$r : \mathcal{O}_K^* \to \mathbb{Z}_p$$

which respects upper numbering. Since $r(U_K^i)$ defines a decreasing sequence of closed finite-index subgroups of $\mathbb{Z}_p$, we can define v_{i+1} to be the greatest integer such that $r(U_K^{v_{i+1}}) \subset p^i\mathbb{Z}_p$. Then, we see that for any v with $v_i < v \leq v_{i+1}$, $G^v = p^i\mathbb{Z}_p$.

For i sufficiently large, U_K^i is isomorphic to the additive group $\mathcal{O}_K$ as topological groups, and using this fact, one can deduce that

$$(U_K^i)^p = U_K^{i+e}$$

where $e = v(p)$. Since r commutes with multiplication by p, this translate into the fact that $v_{i+1} = v_i + e$ for $i \geq n_o$ for some integer n_0.

Now, we would like to compute $v(\mathcal{D}_{K_n/K})$. Prop. 4.3 says that

$$v(\mathcal{D}_{K_n/K}) = \int_{-1}^{\infty} (1 - \frac{1}{|G^v|})dv$$

where $G = \mathrm{Gal}(K_n/K)$. Given that upper numbering behaves well with respect to quotients, we deduce immediately that $|G^v| = p^{n-i}$ if $v_i < v \leq v_{i+1}$, with $i \leq n$, and $|G^v| = 1$ otherwise. Define $c_i = v_{i+1} - vi$. Then,

$$\int_{-1}^{\infty} (1 - \frac{1}{|G^v|})dv = \sum_{i=0}^{n} c_i(1 - \frac{1}{p^{n-i}}).$$

Now, we are ready to show the sum on right has the form $en + c + p^{-n}a_n$ as desired. If all the c_i were equal to e, then we would get

$$en - e\frac{1 - 1/p^{n+1}}{1 - 1/p} = en - e\frac{1}{1 - 1/p} + p^{-n}\frac{p}{1 - 1/p}$$

which has the form we want. If we show the error term has the form $c + p^{-n}a_n$ then we are done.

The assumption holds for $i \geq n_0$, so the error term is

$$\sum_{i<=n_0} (c_i - e) + \sum_{i<=n_0} (e - c_i)1/p^{n-i}.$$

The first term is some fixed constant and the second term is

$$p^{-n}((c_0 - e) + (c_1 - e)p + ... + (c_{n_0} - e)p^{n_0}),$$

so we can take $a_n = (c_0 - e) + (c_1 - e)p + ... + (c_{n_0} - e)p^{n_0}$, where it's understood that if $n < n_0$, we only sum up to n. Clearly, a_n is bounded, since it is constant for $n \geq n_0$. □

Corollary 4.8. *$v(\mathcal{D}_{K_{n+1}/K_n}) = e + p^{-n}b_n$ where b_n is a bounded sequence.*

Proof. By transitivity of the different,

$$v(\mathcal{D}_{K_{n+1}/K_n}) = v(\mathcal{D}_{K_{n+1}/K}) - v(\mathcal{D}_{K_{n+1}/K}) = e + p^{-n}(a_{n+1}/p - a_n).$$

So we can take $b_n = a_{n+1}/p - a_n$ which is clearly bounded since the a_n's are. □

Corollary 4.9. *There is a constant a (independent of n) such that for $x \in K_{n+1}$, we have*

$$|\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leq | \, p \, |^{1-ap^{-n}} \, |x|.$$

Proof. Proposition 4.6 says in terms of absolute value that

$$|\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leq \alpha$$

if and only if

$$|x| \leq \alpha |\mathcal{D}^{-1}_{K_{n+1}/K_n}|.$$

So the desired inequality is equivalent to

$$|\mathcal{D}_{K_{n+1}/K_n}| \leq |p|^{1-ap^{-n}}.$$

In other words, $v(cD_{K_{n+1}/K_n}) \leq e(1 - ap^{-n})$, which holds by Corollary 4.8 if we choose a such that $ae \geq b_n$ for all n. □

Corollary 4.10. *There is a constant c (independent of n) such that for $x \in K_n$ we have*

$$|p^{-n}\mathrm{Tr}_{K_n/K}(x)| \leq |p|^{-c}|x|.$$

Hence the normalized trace $t(x)$ is a continuous function on K_∞. We denote its extension to $X = \widehat{K_\infty}$ by t as well.

Proof. Applying Cor 4.9, inductively we get that

$$|\mathrm{Tr}_{K_n/K}(x)| \leq |p|^{n-c_n}|x|$$

where $c_n = \sum_{i=1}^{n} ap^{-i}$. The sequence c_n is bounded, so we can c to be any bound. □

4.3. **Cohomology Results for X.** For this section, let $X = \widehat{K}_\infty$ and $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, which acts on X. Let $\chi : \Gamma \to K^*$ be any continuous character.

Definition 4.11. Let $X(\chi)$ be the space X with the twisted action given by

$$s.x = \chi(s)(sx)$$

for all $s \in \Gamma$.

Denote by $H^i(\Gamma, X(\chi))$ the Galois cohomology groups based on continuous co-chains, where Γ has the natural pro-finite topology and $X(\chi)$ has the p-adic topology.

We prove the following important preliminary result.

Theorem 4.12. (1) *$H^0(\Gamma, X) = K$, and $H^1(\Gamma, X)$ is one-dimensional over K.*

(2) *If $\chi(\Gamma)$ is infinite, then $H^0(\Gamma, X(\chi))$ and $H^1(\Gamma, X(\chi))$ are both 0.*

Lemma 4.13. *Let $X_0 \subset X$ be the K-hyperplane defined by $\ker t$. The natural map $K \oplus X_0 \to X$ is an isomorphism. Furthermore, $\cup K_{n,0}$ is dense in X_0, where $K_{n,0}$ are the trace-zero elements of K_n.*

Proof. The normalized trace t is a continuous idempotent operator so it gives a continuous projection onto subspace K which yields the splitting. The compatibility with splitting $K_n = K \oplus K_{n,0}$ at each finite level and the density of K_∞ in X imply the second result. □

Note that the splitting is also Γ-equivariant. Now, let σ be a topological generator for Γ. Then

$$H^0(\Gamma, X) = \ker(\sigma - 1).$$

To prove that $H^0(\Gamma, X) = K$, it suffices to show that $\sigma - 1$ is bijective on X_0. To do this, we need the following two lemmas.

Lemma 4.14. *There exists a constant $c > 0$ such that for all $x \in K_{n+1}$, we have*

$$|x - p^{-1}\mathrm{Tr}_{K_{n+1}/K_n}(x)| \le c|\sigma^{p^n}x - x|.$$

Proof. Let $\tau = \sigma^{p^n}$ which is a generator for $\mathrm{Gal}(K_{n+1}/K_n)$. We have

$$px - \mathrm{Tr}_{K_{n+1}/K_n}(x) = px - \sum_{i=0}^{p-1}\tau^i(x) = \sum_{i=0}^{p-1}(1-\tau^i)(x) = \sum_{i=0}^{p-1}(1+\tau+\ldots+\tau^{i-1})(1-\tau)(x).$$

Thus,

$$|px - \mathrm{Tr}_{K_{n+1}/K_n}(x)| \le \max_i |(1+\tau+\ldots+\tau^{i-1})(1-\tau)(x)| \le |x - \tau(x)|$$

using that $|\tau(y)| = |y|$ and ultrametric inequality all over the place. So we can take our constant $c = |p|^{-1}$. □

Lemma 4.15. *There exists a constant $d > 0$ such that for all $x \in K_\infty$*

$$|x - t(x)| \leq d|\sigma(x) - x|.$$

Proof. Let $x \in K_{n+1}$. We proceed by induction with $c_1 = |p|^{-1}$ and assume we have

$$|x - t(x)| \leq c_n|\sigma(x) - x|$$

for $x \in K_n$. Consider that

$$|px - pt(x)| \leq \max(|px - \mathrm{Tr}_{K_{n+1}/K_n}(x)|, |\mathrm{Tr}_{K_{n+1}/K_n}(x) - pt(x)|).$$

Since $pt(x) = t(\mathrm{Tr}_{K_{n+1}/K_n}(x))$, by inductive step we have that

$$\begin{aligned} |\mathrm{Tr}_{K_{n+1}/K_n}(x) - pt(x)| &\leq c_n|\sigma(\mathrm{Tr}_{K_{n+1}/K_n}(x)) - \mathrm{Tr}_{K_{n+1}/K_n}(x)| \\ &= c_n|\mathrm{Tr}_{K_{n+1}/K_n}(\sigma(x) - x)| \\ &\leq c_n|p|^{1-ap^{-n}}|\sigma(x) - x|. \end{aligned}$$

By the previous lemma, we have that

$$|x - p^{-1}\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leq c|\sigma^{p^n}x - x|$$

and by writing $(\sigma^{p^n} - 1) = (1 + \sigma + \ldots + \sigma^{p^n-1})(\sigma - 1)$, we get the further bound of

$$|x - p^{-1}\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leq c|\sigma(x) - x|.$$

Dividing the original thing through by p, we can take $c_{n+1} = \max(c, |p|^{-ap^{-n}}c_n)$. Since $\sum -ap^{-n}$ is bounded, there exists a contant d which works. □

Proof of Thm 4.12. (1) Since $H^0(\Gamma, K) = K$ and $H^1(\Gamma, K) = \mathrm{Hom}_{\mathrm{cont}}(\Gamma, K)$ is 1-dimensional, it suffices to show that $H^0(\Gamma, X_0)$ and $H^1(\Gamma, X_0)$ are both zero. A continuous 1-co-cycle is determined by the image of σ we get that

$$H^0(\Gamma, X_0) = \ker(\sigma - 1)$$

$$H^1(\Gamma, X_0) \subset \mathrm{coker}(\sigma - 1).$$

The idea is that at each finite level $\sigma - 1$ is bijective on the finite dimensional space $K_{n,0}$ since it is injective. Thus, $\sigma - 1$ is bijective on the dense subset $K_{\infty,0}$. To show that $\sigma - 1$ is bijection on X_0, it suffices to show that the inverse function δ on $K_{\infty,0}$ is continuous and thus extends to a continuous inverse on X_0.

Let $x = \delta(y)$ for $y \in K_{\infty,0}$ in other words $\sigma(x) - x = y$. Then, by Lemma 4.15,

$$|x - t(x)| \leq d|\sigma(x) - x|.$$

However, $x \in K_{\infty,0}$ so $t(x) = 0$ so the inequality becomes

$$|x| = |\delta(y)| \leq d|y|.$$

Hence, δ is a continuous inverse to $\sigma - 1$.

(2) For the second part, let $\frac{1}{\lambda} = \chi(\sigma)$. Note that λ is a 1-unit in K^* by continuity of χ and that χ has infinite order exactly when λ is not a p-power root of unity.

The cohomology again decomposes as

$$H^i(\Gamma, X(\chi)) = H^i(\Gamma, K(\chi)) \oplus H^i(\Gamma, X_0(\chi)).$$

Under the twisted action, we see that

$$\sigma.x = \frac{1}{\lambda}\sigma(x).$$

By the same argument as in part (1), it suffices to show that $(\frac{1}{\lambda}\sigma - 1)$ is bijective on both K and X_0. This is the same as bijectivity for $\sigma - \lambda$. Since $\lambda \neq 1$, this is clear for K. On X_0, consider

$$\delta(\sigma - \lambda) = \delta((\sigma - 1) - (\lambda - 1)) = 1 - (\lambda - 1)\delta.$$

If we can show that as as operator $|(\lambda - 1)\delta| < 1$, then it will be continuously invertible using geometric series. Since $|\delta| \leq d$, it suffices to show that

$$|\lambda - 1|d < 1$$

where d comes from Lemma 4.15.

Since d was a just chosen constant, this may not actually hold, but we can use a little trick. The d from Lemma 4.15 works for the $\mathbb{Z}_p$-extension K_∞/K_n just as well as for K_∞/K if you follow the arguments carefully. So we are free to replace K by K_n, σ by σ^{p^n} and λ by λ^{p^n}.

However, λ is a 1-unit so $|\lambda^{p^n} - 1|$ is going to zero so there is some n such that

$$|\lambda^{p^n} - 1|d < 1$$

which implies that $\sigma^{p^n} - \lambda^{p^n}$ is continuously invertible on $(X_0)_n$ where $(X_0)_n$ is the elements of trace zero with respect to trace down to K_n. Because λ is not a root of unity, $\sigma^{p^n} - \lambda^{p^n}$ is invertible on K_n as well and hence on all of X_0.

But $\sigma^{p^n} - \lambda^{p^n}$ factors as $(\sigma - \lambda)(*)$ and so $\sigma - \lambda$ is continuously invertible as well.

□

References

[1] , S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models*, Springer-Verlag, New York, 1990.

[2] D. Mumford, *Abelian varieties*, Oxford Univ. Press, 1970.

[3] N. Katz, "Serre-Tate Local Moduli" in *Surfaces Algébriques*, Lecture Notes in Math **868**, Springer-Verlag, 1981, pp. 138-202.

[4] J. P. Serre, "Sur les corps locaux a corps de restes algébriquement clos", Bull. Soc. Math. Fr. **102** (1961), pp.105-154.

[5] Jean-Pierre Serre, *Local Fields*, Springer-Verlag, 1979.

[6] J. Tate, "p-Divisible Groups" in *Proceedings of a Conference on Local Fields*, Springer-Verlag, 1967.