M702

Taught by: Dr. Matthias Strauch
Written by: Thanic Nur Samin

Tuesday, 1/14/2025

Abstract

Chapter 1: Local Class Field Theory (LCFT).
Chapter 2: p-divisible groups (eg LT formal groups) and associated Galois representations V and the Hodge-Tate Decomposition of $V \otimes_{\mathbb{Q}_p} \mathbb{C}_p$ and also the diagonal action of $\mathscr{G}_K$.
Tate: p-divisible groups.
Chapter 3: Sen theory, Fontaine's period rings (φ, Γ)-modules.

1 Local Class Field Theory (LCFT)

1.1 Lubin Tate Theory

[N] Neukirch, Alg. NT
[S] Serre, Local Class Field Theory (Cassels-Frohlich)
[LT] Lubin, Tate Formal complex multiplication
K = non-archimedean local field (locally compact) $\supset \mathcal{O} = \mathcal{O}_K$ = valuation ring $\supset P_K$ = valuation ideal.
Residue Field $k = \mathcal{O}/P_K$, $\operatorname{char}(k) = p > 0, q := |k| = p^f$.
Normalized Valuation $v = v_K : K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}, |a| = q^{-v(a)}$.
$U_K = \mathcal{O}_K^\times$.

Definition. $e(x) \in \mathcal{O}[[x]]$ (a formal power series) is called a Lubin-Tate (LT) series for the uniformizer π (fixed) if the following conditions are fulfilled:

- $e(x) \equiv \pi x \mod \deg 2$.
- $e(x) \equiv x^q \mod \pi$.

Set $\mathscr{E}_\pi$ = set of LT series for the uniformizer π.
Recall: Let R be any $\mathcal{O}$-algebra ($i : \mathcal{O} \to R$ ring homomorphism).
A formal $\mathcal{O}$-module over R is a 1-dimensional commutative formal group $F(x, y) \in R[[x, y]]$ over R (some people call it a formal group law) together with a unital (sending 1 to 1) ring homomorphism:

$$[\cdot]_F : \mathcal{O} \to \operatorname{End}_R(F) = \{f(x) \in R[[x]] \mid f(0) = 0, f(F(x, y)) = F(f(x), f(y))\}$$

such that $\forall a \in \mathcal{O} : [a]_F(x) = i(a)x \mod \deg 2$.
We have the following properties:
$F(x, y) = x + y +$ higher order terms
Associativity: $F(x, F(y, z)) = F(F(x, y), z)$
Commutativity: $F(x, y) = F(y, x)$.
$\implies \exists! \iota(x) \in R[[x]] : F(x, \iota(x)) = 0$. Also, $\iota(x) = -x +$ higher order terms.
If R is a local $\mathcal{O}$-algebra with maximal ideal M $(i^{-1}(M) = P_K, k = \mathcal{O}/P_K \to R/M)$ then a formal $\mathcal{O}$-module F over R is callled a LT $\mathcal{O}$-module over R if in addition it is a formal $\mathcal{O}$-module and for any uniformizer π of K: $[\pi]_F(x) \equiv x^q \mod M$.

Remark. If F is a LT $\mathcal{O}$-module over $\mathcal{O}$ $[i : \mathcal{O} \xrightarrow{\text{id}} \mathcal{O}]$ then $[\pi]_F(x) \in \mathscr{E}_\pi$ [meaning it is a Lubin Tate series] for any uniformizer π.

Example. 1) $K = \mathbb{Q}_p, F = \widehat{\mathbb{G}}_m, \widehat{\mathbb{G}}_m(x,y) = x + y + xy = (1+x)(1+y) - 1$.

Then, $[\cdot] : \mathbb{Z}_p \to \mathrm{End}_{\mathbb{Z}_p}(\widehat{\mathbb{G}}_m), [a](x) = (1+x)^a - 1 := \sum_{n=1}^{\infty} \binom{a}{n} x^n, \binom{a}{n} = \frac{a(a-1)\cdots(a-n+1)}{n!} \in \mathbb{Z}_p$ for any $a \in \mathbb{Z}_p, n \geq 1$.

Exercise. 1) $\forall a \in \mathbb{Z}_p \forall n \geq 0, \binom{a}{n}$ as defined above is in $\mathbb{Z}_p$.

2) If K is a proper extension of $\mathbb{Q}_p$ then $\binom{a}{n} \notin \mathcal{O}_K$ for infinitely many $a \in \mathcal{O}_K$.

2) $K = \mathbb{F}_q((t)), F = \widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a(x,y) \equiv x + y$. Set $[t](x) = tx + x^q$. Then,

$$\Bigg[\underbrace{\sum_{\nu=0}^{\infty} \alpha_\nu t^\nu}_{a}\Bigg](x) := \sum_{\nu=0}^{\infty} \alpha_\nu [t]^{\circ\nu}(x) = \sum_{n=1}^{\infty} a_n x^n \text{ where } a_1 = a$$

gives $F = \widehat{\mathbb{G}}_a$ the structure of a LT $\mathcal{O}$-module over $\mathcal{O}$.

Theorem 1.1.1. i) For all uniformizer π of K and any $e \in \mathscr{E}_\pi$ there exists unique LT $\mathcal{O}$-module F_e over $\mathcal{O}$ such that:

$$[\pi]_{F_e}(x) = e(x)$$

ii) $\forall e, e' \in \mathscr{E}_\pi$ there is an isomorphism of formal $\mathcal{O}$-modules $f : F_e \to F_{e'}$ ($f \in x\mathcal{O}[[x]], f(F_e(x,y)) = F_{e'}(f(x), f(y))$.

$\forall a \in \mathcal{O} : f([a]_{F_e}(x)) = [a]_{F_{e'}}(f(x))$.

$f'(0) \in \mathcal{O}^\times$.

iii) Let K^{nr} be the maximal unramified extension of K (inside some fixed algebraic closure $\overline{K}$) and let $K_{nr} := \widehat{K^{nr}}$ be the completion of K^{nr} and let $\mathcal{O}_{K_{nr}}$ be its valuation ring. Then for any two uniformizers π, π' of K and LT series $e \in \mathscr{E}_\pi$ and $e' \in \mathscr{E}_{\pi'}$, $\exists$ an isomorphism of formal $\mathcal{O}$-modules $F_e \to F_{e'}$ over $\mathcal{O}_{K_{nr}}$.

Formal Complex Multiplication

Let $\overline{K}$ be the fixed algebraic closure of $K \supset \mathcal{O}_{\overline{K}} \supset P_{\overline{K}}$. Let $\pi =$ the fixed uniformizer, $e \in \mathscr{E}_\pi, F_e =$ LT $\mathcal{O}$-module over $\mathcal{O}$.

Set $F[\pi^m] = \left\{ \alpha \in P_{\overline{K}} \mid \underbrace{[\pi^m]_{F_e}}_{e^{\circ m}(x)}(\alpha) = 0 \right\}$. This can be shown to be finite from Theorem 1.1.1.ii by setting $e'(x) = \pi x + x^q$. Then the isomorphism will provide a bijection to $F_{e'}[\pi^m, e' \in \mathscr{E}_\pi]$. Then the zeros of the power series are the zeros of the iteration of the polynomial. Hence the set is finite.

$L_{\pi,m} := K(F_e(\pi^m))$ called the field of π^m-torsion points of F_e. It doesn't depend on e, though it does depend on π.

Example. if $K = \mathbb{Q}_p$ and $e(x) = (1+x)^p - 1$ then, $L_{p,m} = \mathbb{Q}_p(\zeta - 1 \mid \zeta^{p^m} = 1) = \mathbb{Q}_p(\mu_{p^m})$.

If we take $e'(x) = px + x^p$, the power series and the torsion points $F_e[p^m]$ and $F_{e'}[p^m]$ are different but the fields $\mathbb{Q}_p(F_{e[p^m]})$ and $\mathbb{Q}_p(F_{e'}[p^m])$ has to be the same!

Theorem 1.1.2. i) $F_e[\pi^m]$ is a free $\mathcal{O}/(\pi^m)$ module of rank 1 [note that $[\pi^m]$ annihilates $[a](x)$ since $[\pi^m]_{F_e}(\alpha) = 0$].

ii) $\forall m \geq 1$ the maps $\mathcal{O}/(\pi^m) \to \mathrm{End}_{\mathcal{O}}(F_e[\pi^m]), a \mod \pi^m \mapsto [\alpha \mapsto [a](\alpha)]$.

Also, $\mathcal{O}^\times/(1 + (\pi^m)) \to \mathrm{Aut}_{\mathcal{O}}(F_e[\pi^m])$, same formula are isomorphism (of finite groups).

iii) $L_{\pi,m}$ does not depend on $e \in \mathscr{E}_\pi$ but depends on π. In particular, if $e'(x) = \pi x + x^q$ then $L_{\pi,m} = K(F_{e'}[\pi^m])$.

iv) $L_{\pi,m}$ is a finite purely ramified Galois extension (so it does not contain a proper unramified extension) of K of degree $(q-1)q^{m-1}$.

The map $G(L_{\pi,m}/K) \to \mathrm{Aut}_{\mathcal{O}}(F_e[\pi^m]) \overset{\text{ii, canonical}}{\cong} \mathcal{O}^\times/(1+(\pi^m))$ given by $\sigma \mapsto a \mod (1+(\pi^m))$.

If $\forall \alpha \in F_e[\pi^m]$: $\sigma(\alpha) = [a]_{F_e}(\alpha)$, is an isomorphism.

v) If $L_\pi = \bigcup_{m\geq 1} L_{\pi,m}$, then the maps in iv induce an isomorphism:

$$G(L_\pi/K) = \varprojlim_m G(L_{\pi,m}/K) \xrightarrow{\cong} \varprojlim \mathcal{O}^\times/(1+(\pi^m)) \cong \mathcal{O}^\times$$

Thursday, 1/16/2025

Recall: we fixed an algebraic closure $\overline{K}$. Residue field of $\overline{K} = \overline{k}$ = algebraic closure of $k = \mathbb{F}_q$.

Theorem 1.1.3. If L/K is abelian, $L_\pi \subset L$, and L/L_π is purely rammified, then $L_\pi = L$.

Proof. Proof uses the Hasse-Arf theorem, which says that the jumps (or breaks) of the upper ramification filtration $(G(L/K)^t, t \geq -1)$ are integers. □

Remark. $G(L_\pi/K)^m = \mathrm{Gal}(L_\pi/L_{\pi,m}), m \geq 0$.
$L_{\pi,0} := K$.

Let $K^{ab} \subset \overline{K}$ be the maximal abelian subextension.

Theorem 1.1.4. For any uniformizer π one has $K^{ab} = K^{nr}$.
K^{nr} = maximal unramified extension = $K(\mu_n \mid p \nmid n)$.

Proof. Set $L_\pi^{nr} := K^{nr}.L_\pi \subset K^{ab}$. This gives us an exact sequence:

$$1 \longrightarrow G(K^{ab}/L_\pi^{nr}) \longrightarrow G(K^{ab}/L_\pi) \twoheadrightarrow G(L_\pi^{nr}/L_\pi) \longrightarrow 1$$

$$G(L_\pi^{nr}/L_\pi) \xrightarrow{\cong} G(\overline{k} \mid k) = \langle \varphi \rangle^{\mathrm{top}}$$

Where $\varphi(\overline{\alpha}) = \overline{\alpha}^q, \overline{\alpha} \in \overline{k}$.

$$\langle \varphi \rangle^{\mathrm{top}} := \varprojlim \varphi^{\mathbb{Z}}/\varphi^{n\mathbb{Z}} \cong \varprojlim \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}}$$

Choose $\widetilde{\varphi} \in G(K^{ab}/L_\pi)$ such that $\widetilde{\varphi}\big|_{K^{nr}} = \varphi$
$\underline{L_\pi} \subset L := (K^{ab})^{\overline{\langle \widetilde{\varphi} \rangle}}$.
$\overline{\langle \widetilde{\varphi} \rangle}$ is the closed subgroup of $G(K^{ab}/L_\pi)$ generated by $\widetilde{\varphi}$.

□

Tuesday, 1/21/2025

Recall: K = local nonarch.. field, π = uniformizer, $e \in \mathscr{E}_\pi$ a LT seriess for π, F_e a LT formal $\mathcal{O}$-module, $L_\pi = \bigcup K(F_e[\pi^m]) \subset K^{ab}$ with topological isomorphism $\mathrm{Gal}(L_\pi/K) \xrightarrow[\iota_\pi]{\cong} U_K = \mathcal{O}_K^\times$.
1.1.6 $\Longrightarrow$

$$K^\times = U_K \times \pi^{\mathbb{Z}} \longrightarrow G(K^{ab}/K)$$

$$(a, \pi^n) \longmapsto \underbrace{\iota_\pi^{-1}(a)}_{\text{acts trivially on } K^{nr}} \quad \widetilde{\varphi}^n$$

$\widetilde{\varphi}$ = Frobenius element of $G(K^{ab}/K)$.
The map:

$$U_K \xrightarrow[\cong]{\text{can}} G(L_\pi/K) \xleftarrow[\cong]{\text{can}} G(L_\pi K^{nr}/K^{nr}) \hookrightarrow G(K^{ab}/K)$$

is canoncial. Here, $K^{ab} = L_\pi K^{nr}$.

Definition. The Weil group W_K is defined by:

$$W_K = \left\{\sigma \in G(\overline{K}/K) \mid \sigma\Big|_{K^{nr}} \in \varphi_{K^{nr}}^{\mathbb{Z}}\right\}$$

Here $\varphi_{K^{nr}}$ = the arithmetic Frobenius of K^{nr}.
We equip W_K with the coarsest topology which makes the inertia subgroup:

$$I_K = \left\{\sigma \in G(\overline{K}/K) \mid \sigma\Big|_{K^{nr}} = \mathrm{id}_{K^{nr}}\right\}$$

an open subgroup, and I_K is equipped witth its profinite topology. Then,

$$W_K = \sqcup_{n\in\mathbb{Z}} I_L \widetilde{\varphi}^{\mathbb{Z}}$$

(disjoint union of open cosets) with $\widetilde{\varphi}$ as in 1.1.6.

Proposition 1.1.5. The abelianization $W_K^{ab} = W_K/\overline{[W_K, W_K]}$ is isomorphic to:

$$\left\{\sigma \in G(K^{ab} \mid K) \mid \sigma\Big|_{K^{nr}} \in \varphi^{\mathbb{Z}}\right\}$$

The image of the homomorphism:

$$K^\times \to G(K^{ab}/K)$$

of 1..1.6 is W_K^{ab}.
$U_K \supset 1 + (p^m)$ is open.

Definition. Let Γ be a topological group and $\rho : \Gamma \to \mathrm{Aut}(V)$ be a representation of Γ as an E-vector space (E = any field). ρ is called smooth if $\forall v \in V$ we have:

$$\mathrm{Stab}_\rho(v) = \{\gamma \in \Gamma \mid \rho(\gamma)(v) = v\}$$

is open.

Proposition 1.1.6 (ℓ-adic local Langlands correspondence for GL_1)**.** Let $\ell \neq p$ be a prime. Then the isomorphism $K^\times \to W_K^{ab}$ from 1.1.7 induces a bijection:

$$\left\{\begin{matrix}\text{continuous homomorphisms} \\ W_K \to GL_1(\overline{\mathbb{Q}}_\ell) = \overline{\mathbb{Q}_\ell}^\times\end{matrix}\right\} \to \left\{\begin{matrix}\text{smooth irreducible} \\ \text{rep's of } GL_1(K) = K^\times \\ \text{on } \overline{\mathbb{Q}}_\ell\text{-vector space}\end{matrix}\right\} / \cong$$

$$\chi \mapsto \left[K^\times \xrightarrow{\cong} W_K^{ab} \overset{\chi}{\dashrightarrow} \overline{\mathbb{Q}_\ell}^\times\right]$$

$$\begin{tikzcd} \chi \arrow[r, mapsto] & {[K^\times} \arrow[r, "\cong"] & W_K^{ab} \arrow[r, dash, "\chi"] & \overline{\mathbb{Q}}_\ell^\times] \\ & & W_K \arrow[u] \arrow[ur, "\chi"] & \end{tikzcd}$$

Proof. Main point: a smooth irreducible representation of $K^\times$ on a $\overline{\mathbb{Q}}_\ell^\times$ vector space is 1-dimensional. $\square$

Remark. Proposition 1.1.8 is also true when $\overline{\mathbb{Q}}_\ell$ is replaced by $\mathbb{C}$ and with the appropriate modifications, when $\overline{\mathbb{Q}}_\ell$ is replaced by $\overline{Q}_p$.

1.2 1-dim formal groups: the functional equation lemma

Cf. Hazewinkel, Formal groups and Applications = [H1 Formal]
Here we let:

- K = any commutative ring
- $A \subset K$ subring
- p prime
- q power of p
- $\sigma : K \to K$ ring homomorphism
- $I \subset A$ ideal
- $s_1, s_2, s_3, \dots \in K$

We assume:

- $\sigma(A) \subset A$
- $\forall a \in A : \sigma(a) \cong a^q \mod I$
- $p \in I$ so A/I is an $\mathbb{F}_p$-algebra
- $\forall i \geq 1 : s_i I \subset A$
- $\forall b \in K \forall r \geq 0 : bI^r \subset A \implies \sigma(b)I^r \subset A$.

Lemma 1.2.1. Let $g(x) = \sum_{i=1}^{\infty} b_i x^i \in xA[[x]]$.
By HW1, $\exists! f_g(x) = \sum_{i=1}^{\infty} d_i x^i \in xK[[x]]$ so that,

$$f(x) = g(x) + \sum_{i=1}^{\infty} s_i(\sigma_*^i f)(x^{q^i}) \tag{1.2.1}$$

where $\sigma_*^i f_g$ is power series obtained from f_g obtained by applying σ^i to all coefficients.

Indeed, $d_n = \begin{cases} b_n, & \text{if } q \nmid n; \\ b_n + s_1\sigma(d_{n/q}) + \cdots + s_r\sigma(d_{n/q^r}), & \text{if } n = q^r m, q \nmid m. \end{cases}$

Lemma 1.2.2 (The functional equation lemma (FEL))**.** Let the data be as above. Let $g(x) = \sum_{i=1}^{\infty} b_i x^i$ and $\overline{g}(x) = \sum_{i=1}^{\infty} \overline{b_i} x^i$ be in $xA[[x]]$ and assume $b_1 \in A^\times$. Then, $f_g(x) = b_1 x +$ higher order terms $\implies f_g$ has inverse f_g^{-1} w.r.t. composition. Then,

i) $F_g(x, y) \coloneqq f_g^{-1}(f_g(x) + f_g(y))$ is a formal group over A.

ii) $f_g^{-1}(f_{\overline{g}}(x)) \in xA[[x]]$.

iii) Given $h(x) = \sum_{i=1}^{\infty} c_n x^n \in xA[[x]], \exists \widehat{h}(x) = \sum_{n=1}^{\infty} \widehat{c_n} x^n$ s.t. $f_g(h(x)) = f_{\widehat{h}}(x)$.

iv) If $\alpha(x) \in xA[[x]], \beta(x) \in K[[X]]$, then $\forall r \geq 0 : \alpha(x) \equiv \beta(x) \mod I^r A[[x]] \iff f_g(\alpha(x)) \equiv f_g(\beta(x)) \mod I^r A[[x]]$

Lemma 1.2.3 (HW1)**.** Write $f_g(x) = \sum_{i=1}^{\infty} d_i x^i$ and write $n = q^r m, q \nmid m$. Then $d_n I^r \subset A$.

Lemma 1.2.4. Let $G(x, y) \in A[[x, y]]$ and $n = q^r m$, and $\ell > 0$. Then,

$$G(x, y)^{q^\ell n} \cong \left((\sigma_*^\ell G)(x^{q^\ell}, y^{q^\ell}) \right)^n \mod I^{r+1}$$

$(\sigma(a) \equiv a^q \mod I)$

Proof of (i) of FEL. Note that $f_g^{-1}(x) = b_1^{-1}x + h.o.t.$ Then,

$$F_g(x, y) = b_1^{-1}(b_1 x + b_1 y + h.o.t) = x + y + h.o.t \tag{1}$$

and associativity follows from the definition.
Write $F(x, y) = F_1(x, y)+F_2(x, y)+F_3(x, y)+\cdots$ with $F_d(x, y) \in K[x, y]$ homogeneous of degree d.
We want to show, $\forall d \geq 1, F_d(x, y) \in A[x, y]$.
We prove this by induction. Case $d = 1$ already done.
Assume $d \geq 2$ and the statement is true for $F_1, \cdots, F_{d-1}$.
Note:

$$\forall r \geq 2 : (F_1(x, y) + \cdots + F_{d-1}(x, y))^r \equiv F(x, y)^r \mod \deg d + 1 \tag{2}$$

(2) and 1.2.4 together imply that $\forall i \geq 1, n = q^r m, q \nmid m$ ($n = 1, r = 0$ are ok).

$$F(x, y)^{q^i n} \cong \left((\sigma_*^i F)(x^{q^i}, y^{q^i})\right)^n \mod \deg d + 1, I^{n+1} \tag{3}$$

By definition,

$$f(F(x, y)) = f(x) + f(y) \tag{4}$$

(4) $\implies$ (5):

$$(\sigma_* f)((\sigma_*^i F)(x, y)) = (\sigma_*^i f)(x) + (\sigma_*^i f)(y) \tag{5}$$

(1.1.2) = (6)

$$f(x) = g(x) + \sum_{i=1}^{\infty} s_i(\sigma_*^i f)(x^{q^i}) \tag{6}$$

Substitute $F(x, y)$ for x in (6). We get (7):

$$f(F(x, y)) = g(F(x, y)) + \sum_{i=1}^{\infty} s_i \sum_{n=1}^{\infty} \sigma^i(d_n)F(x, y)^{q^i n} \tag{7}$$

Then we use the 12.4 congruence and our knowledge about the integrality of s_i. Eventually it turns out that $F_d(x, y) \equiv 0 \mod A[[x, y]]$. Thus F_d has coefficients in A.

Thursday, 1/23/2025

Write $n = q^r m, q \nmid m$.
$F(x, y)^{q^i n}$ in (7) satisfies (3).
1.2.3 $d_n I^r \subset A \implies \sigma(d_n)I^r \subset A$. Iterating, $\sigma^i(d_n)I^r \subset A$.
Also, $s_i I \subset A$. Multiplying both sides,

$$s_i\sigma^i(d_n)I^{r+1} \subset A$$

Multiply (3) by $s_i\sigma^i(d_n)$,

$$s_i\sigma^i(d_n)F(x, y)^{q^i n} \equiv s_i\sigma^i(d_n)((\sigma_*^i F)(x^{q^i}, y^{q^i}))^n \mod A, \deg d + 1 \tag{8}$$

(7) and (8) together imply that,

$$\cancel{f(F(x, y))} \equiv g(F(x, y)) + \sum_{i=1}^{\infty} s_i(\sigma_*^i f)((\sigma_*^i F)(x^{q^i}, y^{q^i})) \mod A, \deg d + 1$$

$$\overset{(5)}{\equiv} g(F(x, y)) + \sum_{i=1}^{\infty} s_i((\sigma_*^i f)(x^{q^i}) + (\sigma_*^i f)(y^{q^i}))$$

$$\stackrel{(6)}{=} g(F(x,y)) + \cancel{f(x)} - g(x) + \cancel{f(y)} - g(y)$$

Upshot:

$$g(F(x,y)) \equiv g(x) + g(y) \stackrel{\text{by assoc. on } g}{\equiv} 0 \mod A, \deg d+1 \tag{9}$$

$$\implies 0 \stackrel{\text{mod } A, \deg d+1}{\equiv} g(F(x,y)) = b_1 F(x,y) + b_2 F(x,y)^2 + \cdots$$

$$b_2 F^2 + \cdots \equiv b_2(\underbrace{F_1 + \cdots + F_{d-1}}_{\in A[x,y] \text{ by ind. hyp.}})^2 + b_3(F_1 + \cdots + F_{d-1})^3 + \cdots \mod \deg d+1$$

$$\implies 0 \equiv b_1(\underbrace{F_1 + \cdots + F_{d-1}}_{\in A[x,y]} + F_d) \equiv b_1 F_d(x,y)$$

Since $b_1 \in A^\times$ we have, $F_d(x,y) \in A[x,y]$.
Statement ii ($f_g^{-1}(f_{\overline{g}}(x)) \in A[[x]]$) is proved in the same way.
Satetement iii: $\forall h(x) = \sum_{n=1}^\infty c_n x^n \in xA[[x]]$, suppose $\exists \widehat{h}(x) = \sum_{n=1}^\infty \widehat{c_n} x^n \in A[[x]]$ such that $f_g(h(x)) = f_{\widehat{h}}(x)$ which is defined by the Functional Equation of same type (i.e. all the other data are the same).
Set $\widehat{f}(x) = f(h(x))$ by assoc. $h(x) \in xA[[x]]$.
Recall:

$$f(x) = g(x) + \sum_{i=1}^\infty s_i(\sigma_*^i f)(x^{q^i})$$

Then,

$$\widehat{f}(x) - \sum_{i=1}^\infty s_i(\sigma_*^i \widehat{f})(x^{q^i}) = f(h(x)) - \sum_{i=1}^\infty s_i(\sigma_*^i f)((\sigma_*^i h)(x^{q^i}))$$

When $n = q^r m, q \nmid m$,

$$= f(h(x)) - \sum_{i=1}^\infty s_i \sum_{n=1}^\infty \sigma^i(d_n) \underbrace{\left((\sigma_*^i h)(x^{q^i})\right)^n}_{\underset{1.2.4}{\equiv} h(x,y)^{q^i n} \mod I^{r+1}}$$

Use 1.2.3 and $s_i I \subset A$ to deduce that,

$$\underset{\text{mod } A}{\equiv} f(h(x)) - \sum_{i=1}^\infty s_i(\sigma_*^i f)(h(x)) \equiv g(h(x)) \equiv 0 \mod A$$

Set $\widehat{h}(x) \coloneqq \widehat{f}(x) - \sum_{i=1}^\infty s_i(\sigma_*^i \widehat{f})(x^{q^i}) \in xA[[x]]$.
Construction $\implies \widehat{f}(x) = f_{\widehat{h}}(x)$ [unique solution to the functional equation].

$\square$

For statement iv: [H, Formal, ch 1, sec. 2.4.]
So, we can write many formal group laws of the form $F(x,y) = f^{-1}(f(x) + f(y))$. where f is invertible. f is logarithm for this formal group law.
Applications:

1) If $K/\mathbb{Q}_p$ is a finite extension, $\exists$ polynomials $p_1(x), p_2(x), \cdots \in K[x]$ such that:

$$[a]_{F_e}(x) = \sum_{n=1}^\infty p_n(a) x^n$$

with $\forall n \geq 1 \forall a \in \mathcal{O}_K, p_n(a) \in \mathcal{O}_K$.

Where F_e is a LT $\mathcal{O}_K$-module.
eg when $K = \mathbb{Q}_p, e(x) = (1+x)^p - 1 \implies p_n(x) = \binom{x}{n}$.
$p_n(a) \in \mathbb{Z}_p$ if $a \in \mathbb{Z}_p$ but if $K \neq \mathbb{Q}_p$ then $\exists a \in \mathcal{O}_K$ such that $\binom{a}{n} \notin \mathcal{O}_K$.

2) Formal groups over $\mathbb{F}_p$ or $\overline{\mathbb{F}}_p$.
Fix $n \geq 1$. Set $A = \mathbb{Z}, p$ a prime, $I = p\mathbb{Z}, K = \mathbb{Q}, \sigma = \mathrm{id}, q = p$.
Define $s_i^{(n)} = \begin{cases} 0, & \text{if } i \neq n; \\ \dfrac{1}{p}, & \text{if } i = n. \end{cases}$
Let $g(x) = x, f_n(x) \in \mathbb{Z}\left[\frac{1}{p}\right][[x]]$ be the unique power series satisfying the functional equation:

$$f_n(x) = x + p^{-1} f_n(x^{p^n})$$

Then,

$$f_n(x) = x + \frac{x^{p^n}}{p} + \frac{x^{p^{2n}}}{p^2} + \cdots = \sum_{i=1}^{\infty} \frac{x^{p^{ni}}}{i} \qquad (*)$$

FEL $\implies F_n(x,y) = f_n^{-1}(f_n(x) + f_n(y)) \in \mathbb{Z}[[x]]$ by FEL.
Exercise: if ℓ is a prime $\neq p$ then $F_n(x,y) \mod \ell$ is isomorphic to $\widehat{\mathbb{G}}_{a,\mathbb{F}_\ell}$.

Set $\overline{F}_n(x,y) = F_n(x,y) \mod p\mathbb{Z} \in \mathbb{F}_p[x,y]$ a formal group over $\mathbb{F}_p$.

Proposition 1.2.5. i) $[p]_{F_n} \equiv x^{p^n} \mod p$.

ii) If $n \neq m \in \mathbb{Z}_{>0}$, then for any field k of characteristic p, we have:

$$\mathrm{Hom}_{\text{formal grp }/K}\left(\overline{F}_n \otimes k, \overline{F}_m \otimes k\right) = \{0\}$$

In particular, $\overline{F}_n$ and $\overline{F}_m$ are not isomorphic over any k.

Proof. i) Set $\alpha(x) = [p]_{F_n}(x) \in \mathbb{Z}[[x]]$ and $\beta(x) = x^{q^n}$.
Recall that $[p]_{F_n}(x) = f_n^{-1}(pf_n(x))$.

$$f_n(\alpha(x)) = p \cdot f_n(x), f_n(\beta(x)) = f_n(x^{p^n}).$$

$(*) \implies f_n([p](x)) - f_n(x^{p^n}) = px \equiv 0 \mod p$.
FEL iv $\implies \alpha(x) \equiv \beta(x) \mod p$.

ii) Let $h(x) \in xk[[x]]$ be a non-zero homomorphism $\overline{F}_n \otimes k \to \overline{F}_m \otimes k$.
Let $h(x) = ux^t + h.o.t, u \in k^\times, t \geq 1$. Then,

$$\implies h\left([p]_{\overline{F}_n}(x)\right) = [p]_{\overline{F}_m}(h(x))$$

$$\implies ux^{p^n t} + h.o.t = up^m x^{p^m t} + h.o.t.$$

$$\implies p^n t = p^m t \implies p^n = p^m$$

Which is a contradiction.

$\square$

Remark. 1) One can show [H, Formal, 18.5.1] that a 1-dimensional (commutative) formal group over a separably closed field k of char p is isomorphic to exactly one of $\overline{F}_n \otimes k$ for a unique $n \geq 1$ or $\widehat{\mathbb{G}}_{a,k}$.

We define the height of F to be:

$$ht(F) := \begin{cases} n, & \text{if } F \cong \overline{F}_n \otimes k; \\ \infty, & \text{if } F \cong \widehat{\mathbb{G}}_{a,k}. \end{cases}$$

2) Let $K = \mathbb{Q}_p(\zeta_{p^n-1})$ unramified extension of degree n over $\mathbb{Q}_p$. Let $q = p^n, e(x) = f_n^{-1}(pf_n(x))$ which we know is a Lubin-Tate series for the uniformizer $\pi = p$ of K.

Clearly, $e(x) = px + h.o.t, e(x) \equiv x^{p^n} = x^q \mod p$. These are exactly the conditions for LT series.

$\implies F_n = f_n^{-1}(f_n(x) + f_n(y)) = F_e$ is the LT $\mathcal{O}_K$-module for $e(x)$ by LT theory.

One can show the canonical map:

$$\begin{array}{ccccc} \mathcal{O}_K & \longrightarrow & \mathrm{End}(F_n \otimes_{\mathbb{Z}} \mathcal{O}_K) & \longrightarrow & \mathrm{End}(\overline{F}_n \otimes_{\mathbb{F}_p} \mathbb{F}_q) \\ & & \big\downarrow{=} & & \\ & & \mathrm{End}(F_e, \mathcal{O}_K) & & \end{array}$$

is injective but not surjective.

$$\phi(x) = x^p \text{ is an endomorphism of } \overline{F}_n$$

$\implies \mathrm{End}(\overline{F}_n \otimes \mathbb{F}_q) = \mathcal{O}_K[\phi]$ where $[a]_{\overline{F}_n} \circ \phi = \phi \circ [\phi(a)]_{\overline{F}_n}$
and $\mathcal{O}_K[\phi] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a divisional algebra over $\mathbb{Q}_p$.

$$\mathrm{End}(\overline{F}_n \otimes_{\mathbb{F}_q} \mathbb{F}_q) \otimes_{\mathbb{Q}_p} \mathbb{Q}_p =: D_n$$

We have: $\dim_{\mathbb{Q}_p}(D_n) = n^2$

Furthermore, $\mathrm{center}(D_n) = \mathbb{Q}_p$. D_n also contains K but it is not in the center.

1.3 LCFT following Hazewinkel

[H] = 'Local Class Field Theory is easy'
In this section, a local field is, by convention, a field K which is complete for a discrete non-trivial non-archimedean absolute value $|\cdot|$. i.e., $|K^\times|$ is a non-trivial discrete subgroup of $R_{>0}$.
Examples:

1) $\mathbb{Q}_p, \mathbb{F}_q((t))$

2) $(\mathbb{Q}_p)_{nr} = \widehat{\mathbb{Q}_p^{nr}}, \overline{\mathbb{F}_q}((t)) = (\underbrace{\mathbb{F}_q((t)) \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}}_{\mathbb{F}_q((t))^{nr}})^\wedge$ [the t-adic completion]

3) $\mathbb{C}((t))$ or $k((t))$ [they are complete w.r.t. a t-adic absolute value].

Outline:

1) Assume K has algebraically closed residue field k, and L/K is finite abelian extension. [Note that abelian here automatically means Galois]. Set $U(K) = \mathcal{O}_K^\times$, units of the valuation ring, and $V(L/K) = \langle \sigma(u)u^{-1} \mid \sigma \in G(L/K), u \in U(L) \rangle$ [subgroup generated by these elements].

Fix a uniformizer π_L of L and define:

$$i : G(L/K) \to U(L)/V(L/K)$$

$$i(\sigma) = \frac{\sigma(\pi_L)}{\pi_L} \mod V(L/K)$$

Note: i does not depend on the choice of π_L. Indeed, if ω is another uniformizer of L then $\omega = v\pi_L \implies \frac{\sigma(\omega)}{\omega} = \frac{\sigma(\pi_L)}{\pi_L}\frac{\sigma(v)}{v} \equiv \frac{\sigma(\pi_L)}{\pi_L} \mod V(L/K)$.

Theorem 1.3.1. The seqeunce:

$$1 \to G(L/K) \to U(L)/V(L/K) \xrightarrow{N_{L/K}} U(K) \to 1$$

is exact.

2) Now assume that K has finite residue field (equivalently, K is locally compact). Also assume that L/K is a finite abelian extension. Set $K_{nr} = \widehat{K^{nr}}, L_{nr} = \widehat{L^{nr}} = \widehat{L.K^{nr}} = L.K_{nr}$.

   Let $\varphi_K \in \mathrm{Gal}(K^{nr}/K), \varphi_L \in \mathrm{Gal}(L^{nr}/L)$ be the arithmetic Frobenius.

   Let $G(L/K)_0$ be the 0^{th} ramification group. Then, we have an exeact sequence:

$$1 \to G(L/K)_0 \to G(L/K) \to G(k_L/k) \to 0$$

   Here k_L is the residue field of L.

   Note: $G(L/K)_0 \xleftarrow[\text{res}]{\cong} G(L^{nr}(= L.K^{nr})/K^{nr}) \cong G(L/L \cap K^{nr})$. $L \cap K^{nr}$ is the maximal unramified subfield of L over K. Furthermore, $G(L^{nr}/K^{nr})$ is isomorphic to the Galois group of the completion. Then we have,

$$\begin{tikzcd}
 & & & & 1 \arrow[d] & \\
 & & & & U(K) \arrow[d] \arrow[dddlll] & \\
1 \arrow[r] & G(L/K)_0 \arrow[r, "\cong"] \arrow[d, "\sigma\mapsto 1"] & G(L_{nr}/K_{nr}) \arrow[r] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r] \arrow[d, "\psi_L"] & U(K_{nr}) \arrow[r] \arrow[d, "\psi_K"] & 1 \\
1 \arrow[r] & G(L/K)_0 \arrow[r, "\cong"] \arrow[d] & G(L_{nr}/K_{nr}) \arrow[r] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r] & U(K_{nr}) \arrow[r] & 1 \\
 & G(L/K)_0 & & & &
\end{tikzcd}$$

   by snake lemma.

   Here, $\psi_K(v) = \varphi_K(v)v^{-1}, \psi_L(v) = \varphi_L(v)v^{-1}$.

   Hence we get a canonical homomorphism:

$$U(K) \xrightarrow{i_{L/K}} G(L/K)_0$$

Theorem 1.3.2. $i_{L/K}$ is surjective and $\ker(i_{L/K}) = N_{L/K}(U(L))$.

Hence we have a canonical basis:

$$\frac{U(K)}{N_{L/K}}(V(L)) \xrightarrow[i_{L/K}]{\cong} G(L/K)_0$$

If L/K is a subextension of a finite abelian exztension L'/K one has a commutative diagram:

$$\begin{array}{ccc} \dfrac{U(K)}{N_{L'/K}(U(L'))} & \xrightarrow{i_{L'/K}} & G(L'/K)_0 \\ \downarrow & & \downarrow \\ \dfrac{U(K)}{N_{L/K}(U(L))} & \xrightarrow{i_{L/K}} & G(L/K)_0 \end{array}$$

[Use $N_{L'/K}(U_{L'}) = N_{L/K}(N_{L'/L}(U(L'))) \subset N_{L/K}(U(L))$].

Taking the limit over all finite abelian extensions of K inside a fixed maximal abelian extension K^{ab} gives:

Proposition 1.3.3. The homomorphisms $i_{L/K}$ for varying finit eabelian L/K induce canonicall isomorphism:

$$U(K) \cong \varprojlim_{L/K} \frac{U(K)}{N_{L/K}(U(L))} \cong \varprojlim_{L/K} G(L/K)_0 = G(K^{ab}/K^{nr})$$

<u>Preliminaries</u> Let K be a local field with perfect residue field k. Given a finite Galois extension L/K, we set K_L = maximal unramified subextension of L/K, $= L \cap K^{nr}$. We have an exact sequence:

$$1 \to \underbrace{G(L/K_L)}_{=G(L/K)_0} \to G(L/K) \to G(k_L/k) \to 1$$

Set $K_{nr} = \widehat{K^{nr}}, L_{nr} = \widehat{L^{nr}} = L.K_{nr}$. The maps:

$$G(L_{nr}/K_{nr}) \xrightarrow[\text{res}]{\cong} \underbrace{G(L^{nr}/K^{nr})}_{=G(L/L\cap K^{nr})} \xrightarrow[\text{res}]{\cong} G(L/K_L)$$

Proposition 1.3.4.
i) Let K be a local field with algebraically closed residue field k and L/K a finite extension. Then, $N_{L/K} : L^\times \to K^\times$ and $N_{L/K} : U(L) \to U(K)$ are both surjective.

ii) Let K be a local field with finite residue field and L/K a finite unramified extension. Then, $N_{L/K} : U(L) \to U(K)$ is surjective.

Proof. HW3 □

The Decomposition Theorem

Fix an algebraically closed field Ω containing $K_{nr} = \widehat{K^{nr}}$. All composite fields are taken in Ω.

Theorem 1.3.5. Let K be a local field with finite residue field and L/K a finite Galois extension. Then $\exists$ a totally ramified extension L'/K inside L/K such that,

$$L'K^{nr} = LK^{nr} = L^{nr}$$

$$(L')_{nr} = L'.K_{nr} = L.K_{nr} = L_{nr}$$

If $G(L/K)_0$ is contained in the center $Z(G(L/K))$ then $G(L/K)$ is abelian and L'/K is abelian

We have, K^{ab} = (totally ramified extension).K^{nr}

Thursday, 1/30/2025

Proof. Let $K_L/K \subset L/K$ be maximal unramified subextension.

$$\begin{tikzcd}
1 \arrow[r] & G(L/K)_0 \arrow[r] \arrow[d, "="] & G(L/K) \arrow[r] & G(k_L/k) \arrow[r] \arrow[d, "\cong"] & 1 \\
& G(L/K_L) & & G(K_L/K) \arrow[d, "\in"] & \\
& & \widetilde{\varphi} \arrow[r, mapsto] & \varphi_{K_L/K} &
\end{tikzcd}$$

$s = [K_L : K] = [k_L : k] = \mathrm{ord}(\varphi_{K_L/K})$. $r = \mathrm{ord}(\widetilde{\varphi})$ thus $s \mid r$.
Note: K_L is the unique unramified extension of K in Ω of degree s.
Let K_r = unique unramified extension of K in Ω of degree r.
$K_L \subseteq K_r$ since $s \mid r$.
Claim: The canonical homomorphism,

$$G(L.K_r/K) \xrightarrow{(res,res)} G(L/K) \underset{G(L\cap K_r/K)}{\times} G(K_r/K)$$

$$= \{(\sigma, \tau) \mid \sigma\Big|_{L\cap K_r} = \tau\Big|_{L\cap K_r}\}$$

is an isomorphism.
The proof of claimm is Exercise (HW3).
Claim $\implies \exists! \psi \in G(LK_r/K)$ such that $\psi\big|_L = \widetilde{\varphi}$ and $\psi\big|_{K_r} = \varphi_{K_r/K}$.
Set $L' := (L.K_r)^{\langle\psi\rangle}$
Note: the maximal unramified subextension of $L.K_r/K$:
$L' \cap K_r = K \implies L'/K$ is totally ramified.
Note: $\mathrm{ord}(\psi) = r = |\langle\psi\rangle| \implies [L' : K]r = [L' : K][LK_r : L'] = [LK_r : K]$.
Since this has the right degree, we deduce that $L'.K_r = LK_r$.
$\implies L'K^{nr} = (L'K_r)K^{nr} = (LK_r)K^{nr} = L.K^{nr} = L^{nr}$.
Same argument goes for the completion.
Note that $G(L/K)$ is generated by $\widetilde{\varphi}$ and $G(L/K)_0$. The last point follows from this. □

Corollary 1.3.6. Let K^{ab} be the maximal abelian extension of K . Then, $\exists$ a totallly ramified extension L/K such that $K^{ab} = L.K^{nr}$.

Proof. Choose a splitting of $G(K^{ab}/K) \twoheadrightarrow G(K^{nr}/K) \cong \widehat{\mathbb{Z}}$. We have $\sigma : G(K^{nr}) \to G(K^{ab}/K)$.
Set $H = \mathrm{im}\,\sigma, L \equiv (K^{ab})^H$. Then L is totally ramified.
Because of the restriction, $G(K^{ab}/K) \to G(L/K)$ has H as kernel.
Thus $G(K^{ab}/L) \cong H$. This concludes the proof. □

Corollary 1.3.7. $G(K^{ab}/K^{nr}) = \varprojlim_{M/K^{nr},\text{ finite, } M/K \text{ abelian}} G(M/K^{nr})$
$= \varprojlim_{L/K \text{ finite abelian}} G(L.K^{nr}/K^{nr})$
$= \varprojlim_{L/K \text{ finite abelian}} G(L/K_L)$
$= \varprojlim_{L/K \text{ finite}} G(L/K)_0$

Local Fields with Algebraically Closed Residue Field

For example, $K = K_{nr}, K = \mathbb{C}((t))$.

Proposition 1.3.8. Let K have algebraically closed residue field k and L/K finite abelian. Then we have,

$$1 \to G(L/K) \xrightarrow{i} \frac{U(L)}{V(L/K)} \xrightarrow{N_{L/K}} U(K) \to 1 \qquad (*)$$

Goal is to show that $(*)$ is exact.
Recall: $V(L/K) = \{\sigma(u)/u : u \in U(L), \sigma \in G(L/K)\}$.

Lemma 1.3.9. i is well-defined and a group homomorphism.

Proof. Let π be a uniformizer of L. Then, $i(\sigma) = \frac{\sigma(\pi)}{\pi} \mod V(L/K)$, clearly well defined.
$\frac{(\sigma\tau)(\pi)}{\pi} = \frac{\sigma(\tau(\pi))}{\tau(\pi)}\frac{\tau(\pi)}{\pi} \equiv \frac{\sigma(\pi)}{\pi}\frac{\tau(\pi)}{\pi} \mod V(L/K)$. □

Lemma 1.3.10. Let G be a finite abelian group and $g \in G$ an element. Then, $\exists H \leq G$ (subgroup) such that:

i) G/H is cyclic.

ii) $\mathrm{ord}(gH) = \mathrm{ord}(g)$

Proposition 1.3.11. i: $G(L/K) \to U(L)/V(L/K)$ is injective.

Proof. Set $G = G(L/K).g \in G \setminus \{1\}$. Let $H \leq G$ be as 1.3.10.
$\exists f \in G : G/H = \langle \overline{f} \rangle, \overline{f} = fH \implies g = f^r \cdot h_0, h_0 \in H$. $0 < r < s := \mathrm{ord}(\overline{f})$.
Suppose $i(g) \in V(L/K)$.
Write $\pi = \pi_L$.
$\implies \frac{g(\pi)}{\pi} = \underbrace{\frac{f^r(\pi)}{\pi}}_{=i(f^r)=i(f)^r} \frac{h_0(\pi)}{\pi} \underset{1.3.9}{\equiv} \frac{f(\pi)\cdots f(\pi)}{\pi\cdots\pi}\frac{h_0(\pi)}{\pi} = \frac{f(\pi^r)}{\pi^r}\frac{h_0(\pi)}{\pi} \mod V(L/K)$.
By assumption, this is an element of the subgroup.
So, it can be written as:

$$\prod_{0 \leq i < s} \frac{(f^i h_j)(u_{ij})}{u_{ij}} \tag{1}$$

For some $h_j inH, v_{ij} \in U(L)$.
Next: let $h \in H$ be any element.

$$\begin{aligned}
\frac{(f^i h)(v)}{u} &= \frac{(f^i h)(u)}{(f^{i-1}h)(u)}\frac{(f^{i-1}h)(u)}{(f^{i-2}h)(u)}\cdots\frac{(fh)(u)}{h(u)}\frac{h(u)}{u} \\
&= \underbrace{\frac{f((f^{i-1}h)(u))}{(f^{i-1}h)(u)}}_{=v_1}\underbrace{\frac{f((f^{i-2}h)(u))}{(f^{i-2}h)(u)}}_{=v_2}\cdots\underbrace{\frac{f(h(u))}{h(u)}}_{=v_i}\frac{h(u)}{u} \qquad (2)\\
&= \frac{f(v_1\cdots v_i)}{v_1\cdots v_i}\frac{h(u)}{u} = \frac{f(u')}{u'}\frac{h(u)}{u}
\end{aligned}$$

1 and 2 $\implies \frac{f(\pi^r)}{\pi^r}\frac{h_0(\pi)}{\pi} \underset{(3)}{=} \frac{f(w)}{w}\prod_{h\in H}\frac{h(u_h)}{u_h}$
Let $M = L^H$ and apply $N = N_{L/M}$ to both sides of 3.
$\implies \frac{f(\pi_M^r)}{\pi_M^r} = \frac{f(\widetilde{w})}{\widetilde{w}}, \pi_M = N_{L/M}(\pi), \widetilde{w} = nN_{L/M}(w) \in U(M)$.
$\implies f(\pi_m^r\widetilde{w}^{-1}) = \pi_M^r\widetilde{w}^{-1} \in M$ and fixed by f.
$\langle f, H\rangle = G$ so $\pi_M^r\widetilde{w}^{-1} \in K$.
$\implies [M : K] \mid r$. But $[M : K] = |G(M/K)| = |G/H| = s$.
We have chosen $r < s$

□

Theorem 1.3.12 (Hilbert 90)**.** Let E/F be any finite cyclic Galois extension, $\sigma \in G = G(E/F)$. Then, if $N_{E/F}(x) = 1$ for $x \in E^\times \implies \exists y \in E^\times : x = \sigma(y)y^{-1}$.

Proof. Let $n = [E : F]$. For any $a \in E$ set:

$$y = y(a) = a + \sigma(a)x^{-1} + \sigma^2(a)\sigma(x^{-1})x^{-1} + \cdots + \sigma^{n-1}(a)\sigma^{n-2}(x^{-1})\cdots\sigma(x^{-1})x^{-1}$$

$\implies \sigma(y) = \sigma(a) + \sigma^2(a)\sigma(x^{-1}) + \cdots + \underbrace{\sigma^n(a)}_{=a}\underbrace{\sigma^{n-1}(x^{-1})\cdots\sigma(x^{-1})x^{-1}}_{=1}x$
$= (\sigma(a)x^{-1} + \sigma^2(a)\sigma(x^{-1})x^{-1} + \cdots + a)x = yx.$
Let $(a_1, \cdots, a_n)$ be a K-basis of L.

$$\begin{bmatrix} y(a_1) \\ y(a_2) \\ \vdots \\ \vdots \\ y(a_n) \end{bmatrix} = \begin{bmatrix} a_1 & \sigma(a_1) & \cdots & \sigma^{n-1}(a_1) \\ a_2 & \sigma(a_2) & \cdots & \sigma^{n-1}(a_2) \\ & & & \\ a_n & \sigma(a_n) & \cdots & \sigma^{n-1}(a_n) \end{bmatrix} \begin{bmatrix} 1 \\ x^{-1} \\ \sigma(x^{-1})x^{-1} \\ \vdots \\ \sigma^{n-2}(x^{-1})\cdots\sigma(x^{-1})x^{-1} \end{bmatrix}$$

$0 \neq \operatorname{disc}(a_1, \cdots, a_n) = \det(\mathrm{mat})^2$ since E/F is separable.
$\implies \exists 1 \leq i \leq n$ such that $y(a_i) \neq 0$.
Then, $x = \sigma(y(a_i))y(a_i)^{-1}$. $\square$

Remark. Hilbert 90 is equivalent to $H^1(G(E/F), E^\times) = \{1\}$.
If E/F is any finite Galois extension and n any positive integer,
$H^1(G(E/F), \mathrm{GL}_n(E)) = \{1\}$.

Tuesday, 2/4/2025

$$\begin{tikzcd}
 & & & \ker(\psi_K) = U(K) \arrow[d] & \\
1 \arrow[r] & G(L/K)_0 \arrow[r, "i"] \arrow[d, "\sigma\mapsto 1"] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r, "N"] \arrow[d, "\psi_L"] & U(K_{nr}) \arrow[r] \arrow[d, "\psi_K"] & 1 \\
1 \arrow[r] & G(L/K)_0 \arrow[r, "i"] \arrow[d, two heads] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r, "N"] & U(K_{nr}) \arrow[r] & 1 \\
 & G(L/K) & & &
\end{tikzcd}$$

Connecting homomorphism: $\eta_{L/K} : U(K) \to G(L/K)_0$
Then theorem 1.3.2 is: $\eta_{L/K}$ is surjective and $\ker \eta_{L/K} = N(U(L))$.

Proposition 1.3.13. Suppose $k = \overline{k}$ and L/K is finite cyclic. Then,

$$1 \to G(L/K) \xrightarrow{i_{L/K}} \frac{U(L)}{V(L/K)} \xrightarrow{N_{L/K}} U(K) \to 1 \qquad (*)$$

is exact.

Proof. Exactness on left: 1.3.11.
Exactness on right: 1.3.4(i) [Haven't seen yet, HW4].
For exactness on the middle,
Set $N = N_{L/K}$.

$$(N \circ i_{L/K})(\sigma) = N\left(\frac{\sigma(\pi_L)}{\pi_L}\right) = \prod_{\tau \in G(L/K)} \tau\left(\frac{\sigma(\pi_L)}{\pi_L}\right) = 1$$

Now suppose $N(x) = 1, x \in U(L)$.
Hilbert 90 (1.3.12) implies $\exists y \in L^\times : x = \sigma(y)y^{-1}, \langle\sigma\rangle = G(L/K)$.
Write $y = v\pi_L^r, v \in U(L)$.
Then, $x = \frac{\sigma(y)}{y} = \frac{\sigma(v)}{v}\left(\frac{\sigma(\pi)}{\pi}\right)^r \equiv \left(\frac{\sigma(\pi)}{\pi}\right)^r \mod V(L/K) = i_{L/K}(\sigma)^r \overset{1.3.9}{=} i_{L/K}(\sigma^r)$
Thus, $xV(L/K) \in \operatorname{im}(i_{L/K})$.
$\square$

Lemma 1.3.14. Suppose $k = \overline{k}$ and L/K finite Galois extension (not necessarily abelian).
Let $M/K \subseteq L/K$ [Galois] be such that L/M is cyclic. Then,

$$N_{L/M} : V(L/K) \to V(M/K)$$

is cyclic.

Proof. Let $G = G(L/K)$ and $H = G(L/M)$ and consider $\overline{\gamma}(v)v^{-1} \in V(M/K)$.
$v \in U(M), \overline{\gamma} = \gamma H \in G(M/K)$.
1.3.4i $\implies N_{L/M} : U(L) \to U(M)$ is surjective.
Thus, $\exists w \in U(L)$ such that $u = N_{L/M}(w)$.

$$\implies N_{L/M}\left(\frac{\gamma(w)}{w}\right) = \frac{\overline{\gamma}(N_{L/M}(w))}{N_{L/M}(w)} = \frac{\overline{\gamma}(v)}{v}$$

□

Lemma 1.3.15. Assume $k = \overline{k}$. Let L/K be finite abelian and $M/K \subseteq L/K$ such that $H \coloneqq G(L/M)$ is cyclic. Then the sequence:

$$1 \to G(L/M) \xrightarrow{j} \frac{U(L)}{V(L/K)} \to U(K) \to 1$$

is exact.
Here j is given by the composition canonically:

$$G(L/M) \hookrightarrow G(L/K) \xrightarrow{i_{L/K}} \frac{U(L)}{V(L/K)} \xrightarrow{N_{L/M}} \frac{U(M)}{V(M/K)} \to 1$$

Proof. 1.3.11 implies:

$$G(L/K) \xrightarrow{i_{L/K}} \frac{U(L)}{V(L/K)}$$

is injective. Then trivially j is injective from definition.
Also, $N_{L/M} \circ j$ is the trivial homomorphism (trivially).
1.3.4i $\implies N_{L/M}$ is surjective.
Only nontrivial part is exactness in the middle.
Supose $N_{L/M}(v) = 1_{U(M)/V(M/K)} \implies N_{L/M}(v) = w \in V(M/K)$.
1.3.14 $\implies \exists \widetilde{w} \in (V_{L/K})$ such that $N_{L/M}(\widetilde{w}) = w$.
Thus, $N_{L/M}(v\widetilde{w}^{-1}) = 1_{U(M)} \implies \xrightarrow[L/M \text{ cyclic}]{1.3.13} \implies v\widetilde{w}^{-1} \mod V(L/M) = i_{L/M}(\sigma)$.
$\implies j(\sigma) = \underbrace{i_{L/K}(\sigma)}_{\in U(L)/V(L/K)} = \underbrace{i_{L/M}(\sigma)}_{\in U(L)/V(L/M)} V(L/K) == v\widetilde{w}^{-1}V(L/K) = uV(L/K)$.
$\implies uV(L/K) \in \operatorname{im} j$.

□

Theorem 1.3.16. Assume $k = \overline{k}$ and L/K is finite abelian. Then,

$$1 \to G(L/K) \xrightarrow{i_{L/K}} U(L)/V(L/K) \to U(K) \to 1$$

is exact.

Proof. Induction on $[L : K]$. Case $L = K$ is trivial. Assume $[L : K] > 1$.
L/K cyclic $\implies$ by 1.3.13 we're done. Assume L/K not cyclic.
Choose subextension $M/K \subsetneq L/K$ a subextension such that L/M is cyclic.
Consider the following commutative diagram:

(1)

$$\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & & \\
 & & G(L/M) \arrow[r, "id"] \arrow[d] & G(L/M) \arrow[d] & & \\
(2) & 1 \arrow[r] & G(L/K) \arrow[r, "i_{L/K}"] \arrow[d] & U(L)/V(L/K) \arrow[r, "N_{L/K}"] \arrow[d, "N_{L/M}"] & U(K) \arrow[r] \arrow[d, "id"] & 1 \\
(3) & 1 \arrow[r] & G(M/K) \arrow[r, "i_{M/K}"] \arrow[d] & U(M)/V(M/K) \arrow[r, "N_{M/K}"] \arrow[d] & U(K) \arrow[r] & 1 \\
 & & 1 & 1 & &
\end{tikzcd}$$

(1) is exact by 1.3.15, (3) is exact by induction, (2) is exact on the left [1.3.11] and on the right [1.3.4i]. Diagram chase implies exactness of 2 in the middl.

□

Remark. If L/K is any totally ramified Galois extension one still has an exact sequence:

$$\begin{tikzcd}
1 \arrow[r] & G(L/K)^{ab} \arrow[rr, "i_{L/K}"] & & \frac{U(L)}{V(L/K)} \arrow[r] & U(K) \arrow[r] & 1 \\
 & & G(L/K) \arrow[ul, dotted] \arrow[ur] & & &
\end{tikzcd}$$

Almost the Reciprocity Homomorphism

Suppose now that K has finite residue field k and $|k| = q$.
Let L/K be a totally ramified finite abelian extension.
Then the map:

$$G(\underbrace{L_{nr}}_{=L_\pi K_{nr}}/K_{nr}) \xrightarrow[\cong]{res} \underbrace{G(L^{nr}/K^{nr})}_{=G(L/(L\cap K^{nr}=K))} \xrightarrow[\cong]{res} G(L/K)$$

Define $\psi_K : U(K_{nr}) \to U(K_{nr})$ by $\psi_K(a) = \varphi_{K_{nr}/K}(a)a^{-1}$ and similarly $\psi_L : U(L_{nr}) \to U(L_{nr})$. Consider the commutative diagram:

$$\begin{tikzcd}
 & & \ker(\overline{\psi}_L) \arrow[r] \arrow[d] & \ker(\psi_K) \arrow[d] \arrow[dddll] & \\
1 \arrow[r] & G(L/K) \cong G(L_{nr}/K_{nr}) \arrow[r, "i_{L_{nr}/K_{nr}}"] \arrow[d, "\sigma\mapsto 1"] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r] \arrow[d, "\overline{\psi}_L"] & U(K_{nr}) \arrow[r] \arrow[d, "\psi_K"] & 1 \\
1 \arrow[r] & G(L/K) \arrow[r, "i_{L_{nr}/K_{nr}}"] \arrow[d, "\cong"] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r] \arrow[d] & U(K_n) \arrow[r] & 1 \\
 & G(L/K) \arrow[r] & \mathrm{coker}(\overline{\psi_L}) \arrow[d] & & \\
 & & 1 & &
\end{tikzcd}$$

$\overline{\psi}_L$ is the induced map on $U(L_{nr})/V(L_{nr}/K_{nr})$
Note: 1. $\overline{\psi}_L\left(i_{L_{nr}/K_{nr}}(\sigma)\right) = \psi_L\left(\frac{\sigma(\pi_L)}{\pi_L}\right) = 1$
2. $\varphi_{L_{nr}/L}\big|_{K_{nr}} = \varphi_{K_{nr}/K}$, hence:

$$N_{L_{nr}/K_{nr}} \circ \psi_L = \psi_K \circ N_{L_{nr}/K_{nr}}$$

These two points show the commutativity of this diagram.

Lemma 1.3.17. i) $\psi_K : U(K_{nr}) \to U(K_{nr})$ is surjective and $\psi_K^a : \mathcal{O}_{K_{nr}} \to \mathcal{O}_{K_{nr}}, \psi_K^a(a) = \varphi_{K_{nr}/K}(a) - a$.

ii) $\psi_L : V(L_{nr}/K_{nr}) \to V(L_{nr}/K_{nr})$ is surjective.

iii) $\ker \psi_K = U(K)$

Proof. Set $U^n = 1 + \pi_K^n \mathcal{O}_{K_{nr}} \leq U(K_{nr})$

i) One has $\psi_K(a) \underset{(1)}{\cong} a^{q-1} \mod U^1 \implies \psi_K \mod U^1$ is surjective since $k_{K_{nr}} = \overline{k}_{K_{nr}}$. Also,
$$\psi_K : U^n/U^{n+1} \to U^n/U^{n+1}$$

$$1 + a\pi^n \mod U^{n+1} \mapsto 1 + (a^q - a)\pi^n \mod U^{n+1}$$

$(1 + a^q\pi^n)(1 + a\pi^n)^{-1} = 1 + (a^q - a)\pi^n$

$\frac{1}{1+x} = 1 - x + \cdots$

And since $a \mapsto a^q - a$ is surjective on $k_{K_{nr}}$ this map is surjective.

By HW3/1 $\psi_K : U(K_{nr}) \to U(K_{nr})$ is surjective. Same reasoning gives that $\psi_K^a : \mathcal{O}_{K^{nr}} \to \mathcal{O}_{K_{nr}}$ is surjective.

ii) For $\sigma \in G(L/K) = G(L_{nr}/K_{nr}), x \in U(L_{nr})$ consider $\sigma(x)x^{-1} \in V(L_{nr}/K_{nr})$.

By i we can choose $y \in U(L_{nr})$ such that $x = \psi_L(y)$. $L^{nr}/K = L.K^{nr}/K$ is abelian.

Thus, $\varphi_{L_{nr}/L} \circ \sigma = \sigma \circ \varphi_{L_{nr}/L}$

$\implies \psi_L\left(\frac{\sigma(y)}{y}\right) = \sigma(x)x^{-1} \in V(L_{nr}/K_{nr})$. This shows ii.

iii) $u \in \ker \psi_K$. Write $u = \sum_{i=0}^{\infty} a_i\pi^i, a_i \in \mu(K^{nr}) \cup \{0\}, a_0 \neq 0$.

$\implies \psi_K(u) = \varphi_{K_{nr}/K}(u)u^{-1} = 1 \mod \pi . a_0^{q-1} \equiv 1 \mod \pi$. a_0 is a root of unity $\implies a_0^{q-1} = 1$. $\implies a_0 \in \mu_{q-1}(K^{nr})$. By Hensel's lemma, $a_0 \in \mu_{q-1}(K)$.

By induction, assume $a_0, \cdots, a_{n-1} \in \mu(K) \cup \{0\}, n \geq 1$. $\exists w \in U(K) : uw^{-1} = 1 + a\pi^n$ where $a \in \mathcal{O}_{K_{nr}}$.

$u = a_0 + a_1\pi + \cdots + a_{n-1}\pi^n + b\pi^n$

$= \underbrace{(a_0 + \cdots + a_{n-1}\pi^{n-1})}_{=w}\left(1 + \frac{b\pi^n}{a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1}}\right)$.

$\implies 1 = \psi_K(u) = \psi_K(uw^{-1}) = \frac{1+\varphi_{K_{nr}|K}(a)\pi^n}{1+a\pi^n} \equiv 1 + (a^q - a)\pi^n \mod \pi^{n+1}$

Therefore, $a^q \equiv a \mod \pi \implies a = c_n + b_n\pi$ with $c_n \in \mu_{q-1}(K) \cup \{0\}, b_n \in \mathcal{O}_{K_{nr}}$.

Thefefore, $a_n \in \mu_{q-1}(K) \cup \{0\}$.

$\square$

Thursday, 2/6/2025

Theorem 1.3.18. Suppose $k = k_K$ is finite. For any abelian totally ramified exttension L/K, there is a canonical homomorphism:

$$\eta_{L/L} : U(K) \to G(L/K)$$

Which is surjective and has kernel $N_{L/K}(U(L))$.
Hence $\eta_{L/K}$ induces an isomorphism:

$$\frac{U(K)}{N_{L/K}(U(L))} \xrightarrow{\eta_{L/K}} G(L/K)$$

$\eta_{L/K}$ is <u>functorial</u> in the sense that if $M/K \subseteq L/K$ is a subextension then there is a commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & N_{L/K}(U(L)) \arrow[r] \arrow[d, hook] & U(K) \arrow[r, "\eta_{L/K}"] \arrow[d, "id"] & G(L/K) \arrow[r] \arrow[d, two heads, "res"] & 1 \\
1 \arrow[r] & N_{M/K}(U(M)) \arrow[r] & U(K) \arrow[r, "\eta_{M/K}"] & G(M/K) \arrow[r] & 1
\end{tikzcd}$$

Proof. From the diagram we considered before the snake lemma gives us an exact sequence:

$$\begin{tikzcd}
U(L) \cap V(L_{nr}/K_{nr}) \arrow[r] & U(L) \arrow[r, two heads] \arrow[dr] & \ker(\overline{\psi}_L) \arrow[r, "N"] \arrow[d, "\subset"] & \ker(\psi_K) \arrow[d] \arrow[dddll] & \\
1 \arrow[r] & G(L/K) \cong G(L_{nr}/K_{nr}) \arrow[r, "i_{L_{nr}/K_{nr}}"] \arrow[d, "\sigma \mapsto 1"] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r, "N"] \arrow[d, "\overline{\psi}_L"] & U(K_{nr}) \arrow[r] \arrow[d, "\psi_K"] & 1 \\
1 \arrow[r] & G(L/K) \arrow[r, "i_{L_{nr}/K_{nr}}"] \arrow[d, "\cong"] & \frac{U(L_{nr})}{V(L_{nr}/K_{nr})} \arrow[r] \arrow[d] & U(K_n) \arrow[r] & 1 \\
 & G(L/K) \arrow[r] & \operatorname{coker}(\overline{\psi}_L) \arrow[d] & & \\
 & & 1 & &
\end{tikzcd}$$

$$\ker(\overline{\psi}_L) \to \ker(\psi_K) \overset{1.3.17ii}{=} U(K) \xrightarrow{\eta_{L/K}} G(L/K) \to \operatorname{coker}(\overline{\psi}_L) \overset{1.3.17i}{=} 1$$

Let $\overline{u} = uV(L_{nr}/K_{nr}) \in \ker(\overline{\psi}_L) \implies \psi_L(u) \in V(L_{nr}/K_{nr})$.
1.3.17ii $\implies \exists w \in V(L_{nr}/K_{nr})$ such that $\psi_L(w) = \psi_L(u)$.
Thus, $\psi_L(uw^{-1}) = 1$.
1.3.17iii $\implies uw^{-1} \in U(L)$.
Therefore we can deduce that $\ker(\overline{\psi}_L) = U(L)V(L_{nr}/K_{nr})$.
$\implies \operatorname{im}(\ker(\overline{\psi}_L) \xrightarrow{N} \ker(\psi_K) = U(K)) = N_{L/K}(U(L))$.
Hence, $\frac{U(K)}{N(U(L))} \xrightarrow[\eta_{L/K}]{\cong} G(L/K)$
The functoriality of $\eta_{L/K}$ follows from the functoriality of the connecting homomorphism of the snake lemma.

$\square$

Theorem 1.3.19. For every finite abelian extension L/K (not necessarily totally ramified), there is a canonical isomorphism

$$\eta_{L/K} : \frac{U(K)}{N_{L/K}(U(L))} \to G(L/K)_0$$

which is functorial w.r.t. subextensions M/K as in the previous theorem.

Proof. We use the decomposition theorem [1.3.5].
$\exists L' \subset L^{nr}$ such that L'/K is finite abelian [since $L^{nr} = L.K^{nr}$ the compositum of two abelian extensions] such that $(L')^{nr} = L'.K^{nr} = L.K^{nr} = L^{nr}$.
Then, $\mathrm{Gal}(L'/K) \cong G((L')^{nr}/K^{nr}) \cong G(L^{nr}/K^{nr}) \cong G(L/K)_0$.
1.3.18 $\implies \frac{U(K)}{N_{L'/K}(U(L'))} \cong G(L'/K) = G(L/K)_0$.
We can pass to the completion.
Since $L'K_r \overset{(1)}{=} L.K_r$ for some unramified K_r/K (prooof of 1.3.5).
and $N_{L'K_r/L'}(U(L'K_r)) \overset{(2)}{=} U(L')$ by 1.3.4i
$N_{LK_r/L}(U(LK_r)) \overset{(3)}{=} U(L)$ by 1.3.4i.
$\implies N_{L'/K}(U(L')) \overset{(2)}{=} N_{L'/K}(N_{L'K_r/L'}(U(L'K_r)))$
$= N_{L'K_r/K}(U)L'K_r$
$\overset{(1)}{=} N_{LK_r/K}(U(LK_r))$
$= N_{L/K}(N_{LK_r/L}(U(LK_r)))$
$\overset{(3)}{=} N_{L/K}(U(L))$
$\implies$ we get an isomorphism:

$$\frac{U(K)}{N_{L/K}(U(L))} \xrightarrow[\cong]{\eta_{L/K}} G(L/K)_0$$

□

Goal: we want to prove that there is a canonical isomorphism:

$$K^\times/N_{L/K}(L^\times) \xrightarrow{\cong} G(L/K)$$

for any finite abelian extension L/K.
We want to do something with uniformizers, and uniformizers should roughly correspond to frobenius elements.

Norm Groups of Lubin-Tate Extensions

Let π be a uniformizer of K, $|k_K| = q = p^f, \mathcal{O} = \mathcal{O}_K, e \in \mathscr{E}_\pi$ aka a LT series for π.
Let F_e be an LT $\mathcal{O}$-module for e, and $L_m = L_{\pi,m} = K(F_e[\pi^m])$ aka the series generated by π^m torsion points. This is independent of the choice of e but does depend on π.
We know that L_m/K is totally ramified abelian Galois extension of degree $(q-1)q^{m-1}$ where $m \geq 1$. Recall that $L_0 = K$.
Set $U^m(K) = 1 + \pi^m(K) \leq U(K), U^0(K) = U(K)$.
We now have two description of $G(L_m/K)$.

1) Via LT theory: the map $U(K)/U^m(K) \xrightarrow{\cong} G(L_m/K)$ defined by $aU^m(K) \leftarrow\!\shortmid \sigma$ if for all $\alpha \in F_e[\pi^m], \sigma(\alpha) = [a]_{F_e}(\alpha)$
2) Via $\eta_{L/K} : U(K)/N_{L_m/K}(U(L_m)) \xrightarrow{\cong} G(L_m/K)$ [we don't need to put ramification since it is totally ramified].

Natural questions:

i) Is $N_{L_m/K}(U(L_m)) = U^m(K)$? Answer is yes, but not obviously so.
ii) If the answer to i is yes [which it is] then are these two maps the same? [Answer is no, but kind of close! $\forall a \in U(K), \forall \alpha \in F_e[\pi^m], \eta_{L_m/K}(a)(\alpha) = [a^{-1}](\alpha)$]

Lemma 1.3.20. Given a monic polynomial $f(x) \in \mathcal{O}[x] \setminus \{0\}$ with degree n with $p \nmid n$, there exists $s \in \mathbb{Z}_{>0}$ and $r(x) \in \mathcal{O}[x]$ with $r(0) = 1, \deg r < s$ such that the mod π reduction of $h(x) := x^s f(x) + r(x)$ is separable.

Proof. HW4 □

Theorem 1.3.21. $N_{L_m/K}(U(L_m)) = U^m(K)$

Proof. We show first $N(U(L)) \subset U^m(K)$
Set $L_m = L$ and write $w \in U(L)$ as $w = \zeta u$ with $u \in U'(L)$ and $\zeta \in \mu(L)L$ $\underset{=}{\text{totally}}$ ramified $=$ $\mu(K) = \mu_{q-1}(K)$.
$\implies N(w) = N(\zeta u) = \zeta^{[L:K]}N(u) = \zeta^{(q-1)q^{m-1}}N(u) = N(u)$.
Suffices to show that $N_{L/K}(U'(L)) \subset U^m(K)$.
Case $m = 1$ is easy.
Assume $m \geq 2$, set $n = m(q-1)q^{m-1} - 1 \implies p \nmid n$. Let λ be a uniformizer of L.
Write $U'(L) \ni u = 1 + a_1\lambda + \cdots + a_n\lambda^n + x, v(x) \geq n+1 = v(\pi^m)$.
$v = v_L =$ normalized valuation on $L, v_L(\lambda) = 1(\implies v(\pi) = (q-1)q^{m-1})$.
Consider $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in \mathcal{O}[x]$. Since $p \nmid n$ we can apply 1.3.20 and get $h(x) = x^s f(x) + r(x), h \mod \pi$ separable. Then $\overline{h}$ has $s + n \coloneqq t = \deg(h) = \deg(\overline{h})$ distinct roots in $\overline{k} = \overline{\mathbb{F}_q}$. Hensel's lemma implies roots of h in $\overline{K}$ are actually in K_{nr}.
Let $z_1, \cdots, z_t$ be the roots of $h(x)$ in K_{nr}.
Since h is monic, they actually lie on $\mathcal{O}_{K_{nr}}$. $z_i \in \mathcal{O}_{K_{nr}}$.
Recall that $h(0) = r(0) = 1$ so $\prod z_i = \pm 1$.
Thus, $z_i \in \mathcal{O}_{K_{nr}}^\times = U(K_{nr})$.

Tuesday, 2/11/2025

Moreover:

$$(1 - z_1\lambda)(1 - z_2\lambda)\cdots(1 - z_t\lambda) = 1 - \left(\sum_i z_i\right)\lambda$$

$$= 1 + a_1\lambda + a_2\lambda^2 + \cdots + a_n\lambda^n + x', v_L(x') \geq n+1$$

$$= 1 + a_1\lambda + \cdots + a_n\lambda^n + x + (x' - x) = v\left(1 + \frac{x' - x}{v}\right)$$

Let $y \coloneqq \frac{x'-x}{v}$. So $v_L(y) \geq n+1$.
Therefore,

$$N(1+y) = 1 + \sum_{\sigma \in G(L/K)} \sigma(y) + \cdots = 1 + y', v_L(y') \geq n+1 = v_L(\pi^m)$$

Thus, $y' \in \mathcal{O}_K \implies y' \in \pi^m\mathcal{O}_K$.
Therefore, $N(1+y) \equiv 1 \mod \pi^m$.
Therefore, $N(u) \in U^m(K) \iff N\left(\prod_{i=1}^t (1 - z_i\lambda)\right) \in U^m(K)$ (2)
NOTE: UNUSED: Then, <u>STS</u>: $\forall 1 \leq i \leq t : N_{L_m/K}(1 - z_i\lambda) \in U^m(K)$.
Since L_m/K is totally ramified, $G(L_{nr}/K_{nr}) \xrightarrow[res]{\cong} G(L/K)$.
Therefore, $N_{L/K}(1 - z_i\lambda) = N_{L_{nr}/K_{nr}}(1 - z_i\lambda) = N_{L_{nr}/K_{nr}}(z_i(z_i^{-1} - \lambda))$
$= z_i^d N_{L_{nr}/K_{nr}}(z_i^{-1} - \lambda)$
Setting $\zeta_i = z_i^{-1}, e_m(x) = [\pi^m]_{F_e}$,
$N_{L_{nr}/K_{nr}}(\zeta_i - \lambda) = \prod_{\sigma \in G(L/K)}(\zeta_i - \sigma(\lambda)) =$ min. poly of $\lambda(\zeta_i)$.
From here WLOG assume that $e(x) = \pi x + x^q$. We can further assume that $e_m(\lambda) = 0$ but $e_{m-1}(\lambda) \neq 0$.
Then, the minimal polynomial of λ is $\frac{e_m(x)}{e_{m-1}(x)}$.
Thus, $N_{L_{nr}/K_{nr}}(\zeta_i - \lambda) = \left(\frac{e_m}{e_{m-1}}\right)(\zeta_i)$. Since ζ_i is not a root of these, $= \frac{e_m(\zeta_i)}{e_{m-1}(\zeta_i)}$.
Hence,

$$N\left(\prod_i (1 - z_i\lambda)\right) = \prod N(1 - z_i\lambda) = \left(\prod z_i^d\right)\prod_i N(\zeta_i - \lambda) = \left(\prod z_i\right)^d \prod_i N(\zeta_i - \lambda)$$

Since d is even,

$$= \prod N(\zeta_i - \lambda) = \prod_i \frac{e_m(\zeta_i)}{e_{m-1}(\zeta) i} = 1 + \frac{\prod_i e_m(\zeta_i) - \prod_i e_{m-1}(\zeta_i)}{\prod_i e_{m-1}(\zeta_i)}$$

Note that $\prod_i e_{m-1}(\zeta_i), \prod_i e_m(\zeta_i)$ have $v_L = 0$.
Then it suffices to show that $\prod_i e_m(\zeta_i) - \prod_i e_{m-1}(\zeta_i) \equiv 0 \mod \pi^m$ (3).
Note: $e(\zeta_i) \equiv \zeta_i^q \mod \pi$. It is the same as applying the frobenius. Note that the frobenius must permute the roots.
Thus, $e(\zeta_i) \equiv \zeta_{\tau(i)}$ where τ is some permutation of $\{1, \cdots, t\}$.
Lifting the Expontent? $\implies e(\zeta_i)^q = \zeta_{\tau(i)} \mod \pi^2$
$\implies e_2(\zeta_i) = e_1(\zeta_{\tau(i)}) \mod \pi^2$.
Inducting, $e_m(\zeta_i) \equiv e_{m-1}(\zeta_{\tau(i)}) \mod \pi^m$
Product $\implies \prod_i e_m(\zeta_i) \equiv \prod_i e_{m-1}(\zeta_{\tau(i)}) \mod \pi^m$
This shows (3) $\implies$ (2) $\implies$ (1).
This ends Step 1.
Step 2: $N_{L/K}(U(L)) = U^m(K)$.
Proof of Step 2 $|G(L_m/K)| \underset{1.3.18}{=} |U(K)/N(U(L))| \geq |U(K)/U^m(K)|$
inequality since $N(U(L_m)) \subset U^m(K)$ from step 1.
However, $|U(K)/U^m| = |G(L/K)|$ from LT Theory theorem 1.1.2 [as discussed in Fall].

$\square$

Local Class Field Theory

Let K be a field. Then we have a correspondence:

$$\left\{ \mathcal{N} \subset K^\times \middle| \mathcal{N} \text{ open }, [K^\times : \mathcal{N}] < \infty \right\} \leftrightarrow \left\{ L/K \subset K^{ab}/K \text{ finite exts} \right\}$$

$$\mathcal{N} \mapsto L_{\mathcal{N}} = \text{ class field assoc. to } \mathcal{N}$$

Here $N_{L_{\mathcal{N}}/K}(L_{\mathcal{N}}^\times) = \mathcal{N}$ and $K^\times/\mathcal{N} \xrightarrow{\cong} G(L_{\mathcal{N}}/K)$.

$$N_{L/K}(L^\times) \hookleftarrow L$$

$L_{\mathcal{N}}$ is called the <u>class field corresponding to $\mathcal{N}$</u>.
Let K be as above, $|k| < \infty$. Let $K^{ab} \subset \overline{K}$ be the maximal abelian extension of K.

$$G(K^{ab}/K)_0 := \ker(G(K^{ab}/K) \to G(k_{K^{ab}}/k) = G(\overline{k}/k))$$

Recall if we have $M/K \subseteq L/K$ we indeed have $G(L/K)_0 \xrightarrow{res} G(M/K)_0$. This is not true for lower numbering for larger numbers!!!

Theorem 1.3.22. i) The isomorphisms $\eta_{L/K} : U(K)/N(U(L)) \xrightarrow{\cong} G(L/K)_0$ from 1.3.19 for L/K finite abelian induce an isomorphism:

$$U(K) \xrightarrow[\eta_K]{\cong} G(K^{ab}/K)_0$$

ii) The exact sequence:

$$1 \to G(K^{ab}/K)_0 \to G(K^{ab}/K) \to G(\overline{k}/k) \to 1$$

splits continuous (but not canonically).

Proof. i) Let $\mathscr{A}$ be the set of all finite subestensions $L/K \subset K^{ab}/K$. Set $\mathcal{N}_L^0 = N_{L/K}(U(L))$. Then $(\eta_{L/K})_{L \in \mathscr{A}}$ induces an isomorphism:

$$\varprojlim_{L \in \mathscr{A}} U(K)/\mathcal{N}_L^0 \xrightarrow{\cong} \varprojlim_{L \in \mathscr{A}} G(L/K)_0 \underset{\text{exercise}}{=} G(K^{ab}/K)_0$$

Given $L \in \mathscr{A}$, $U(L)$ is compact. Since $N_{L/K}$ is continuous, $N_{L/K}(U(L))$ is compact. A compact subset in a Hausdorff space is closed. Thus, $\mathcal{N}_L^0$ is closed. $\mathcal{N}_L^0$ has finite index in $U(K)$. It is also complement of union of finitely many cosets thus it is also open..

Thus, $\exists m \geq 0 : U^m(K) \subseteq \mathcal{N}_L^0$.

1.3.21 $\implies N_{L_m/K}(U(L_m)) = U^m(K) \implies$ the system $(\mathcal{N}_L^0)_{L\in\mathscr{A}}$ is equivalent to the system $(U^m(K))_{m\geq 0}$ but the profinite completion

$$\varprojlim_m U(K)/U^m(K) \xleftarrow{\cong} U(K)$$

$$\varprojlim_{L\in\mathscr{A}} U(K)/\mathcal{N}_L^0 \xleftarrow{\cong} U(K)$$

This proves i.

ii) HW 3

□

Theorem 1.3.23. With $L_\pi = \bigcup_m L_{\pi,m}$ as in section 1.1 we have $K^{ab} = L_\pi.K^{nr}$.

Proof. Consider the commutative diagram with exact rows:

$$\begin{tikzcd}
 & U(K) \arrow[d, "1.3.22"', "\cong\eta_K"] & & & \\
1 \arrow[r] & G(K^{ab}/K)_0 \arrow[r] \arrow[d, "\alpha=res"] & G(K^{ab}/K) \arrow[r] \arrow[d, "\beta=res"] & G(\overline{k}/k) \arrow[r] \arrow[d, "\gamma=res=id"] & 1 \\
1 \arrow[r] & G(L_\pi K^{nr}/K)_0 \arrow[r] \arrow[d, "="] & G(L_\pi K^{nr}/K) \arrow[r] & G(\overline{k}/k) \arrow[r] & 1 \\
 & \varprojlim G(L_m K^{nr}/K)_0 \arrow[d, "="] & & & \\
 & \varprojlim_m G(L_m/K) \arrow[d, "="] & & & \\
 & \varprojlim_m U(K)/U^m(K) \arrow[d, "="] & & & \\
 & U(K) & & &
\end{tikzcd}$$

Note: $\alpha = id \implies \beta$ is an isomorphism, thus $G(K^{ab}/L_\pi K^{nr}) = \{1\} \implies L_\pi K^{nr} = K^{ab}$ □

Thursday, 2/13/2025

Lemma 1.3.24. Let π be a uniformizer of $K, e \in \mathscr{E}_\pi$ a LT series, $L_{\pi,m} =$ Lubin tate extension associated to F_e [which is independent of choice of e]. Then, $\pi \in N_{L_{\pi,m}/K}(L_{\pi,m}^\times =)$.

Proof. WLOG we may assume $e(x) = \pi x + x^q$. Set $e_m(x) = (\underbrace{e \circ \cdots \circ e}_{m})(x)$.

We've seen $\frac{e_m(x)}{e_{m-1}(x)} \in \mathcal{O}_K[x]$ is irreducible polynomial over K of degree $(q-1)q^{m-1}$. This is not only irreducible, but also Eisenstein. Since we're adjoining root λ_m of an Eisenstein polynomial, λ_m must be a uuniformizer.

$$\frac{e_m(x)}{e_{m-1}(x)} = \prod_{\sigma \in G_{L_{\pi,m}}} (x - \sigma(\lambda_m))$$

Now note that,

$$\pi = \left(\frac{e_m(x)}{e_{m-1}(x)}\right)(0) = \prod_{\sigma}(-\sigma(\lambda_m)) = \prod_{\sigma} \sigma(-\lambda_m) = N_{L_{\pi,m}/K}(\lambda_m)$$

□

Definition of the norm residue symbol

Let L'/K be a totally ramified finite abelian extension. Let $\lambda \in L'$ be a uniformizer and set $\pi = N_{L'/K}(\lambda)$. Since it is totally ramified, π must be a uniformizer of K. Let K_n/K be the unramified extension of degree n. Set $L := L'.K_n$. This is abelian over K. Then the exact sequence:

$$1 \longrightarrow G(L/K)_0 \longrightarrow G(L/K) \longrightarrow \underbrace{G(K_n/K)}_{\cong G(k_L/k)} \longrightarrow 1$$

The exact sequence splits since the canonical map $G(L/K) \to G(L'/K) \times G(K_n/K)$ is an isomorphism.
Hence, there exists a unique $\varphi_{L/L'} \in G(L/K)$ such that $\varphi_{L/L'}\big|_{L'} = \mathrm{id}_{L'}$ and $\varphi_{L/L'}\big|_{K_n} = \varphi_{K_n/K}$.
Then we define $r_{L/K} : K^\times \to G(L/K)$ such that,

$$r_{L/K}(a) = \eta_{L/K}\left(\underbrace{a^{-1}\pi^{v(a)}}_{\in U(K)}\right)\varphi_{L/L'}^{v(a)}$$

Where $v : K^\times \to \mathbb{Z}$ given by $\pi \mapsto 1$ is the normalized valuation and $\eta_{L/K} : U(K) \to G(L/K)$ is the surjective homomorphism in 1.3.19 with kker$(\eta_{L/K}) = N_{L/K}(U(L))$.
Note: $r_{L/K}$ is a homomorphism.
Set $\mathcal{N}_L = N_{L/K}(L^\times), \mathcal{N}_L^0 = N_{L/K}(U(L))$.
$r_{L/K}(a)$ is also written as $(a, L/K)$ and is alled the norm residue symbol.

Proposition 1.3.25. Let L'/K and $L = L'.K_n, \lambda \in L'$ a uniformizer and $\pi = N_{L'/L}(\lambda)$ be as above. Then, $r_{L/K}$ is surjective and its kernel is $\mathcal{N}_L$. Hence, $r_{L/K}$ induces an isomorphism which by abuse of notation we can also denote as $r_{L/K}$.

$$\frac{K^\times}{\mathcal{N}_L} \xrightarrow[r_{L/K}]{\cong} G(L/K)$$

Proof. We have $L^\times = U(L) \cdot \lambda^{\mathbb{Z}}$ since L/L' is unramified. Applying the norm, $\mathcal{N}_L = \mathcal{N}_L^0 \cdot N_{L/K}(\lambda)^{\mathbb{Z}} = \mathcal{N}_L^0 N_{L'/K}(N_{L/L'}(\lambda))^{\mathbb{Z}} = \mathcal{N}_L^0 \cdot N_{L'/K}(\lambda^n)^{\mathbb{Z}} = \mathcal{N}_L^0 \cdot \pi^{n\mathbb{Z}}$.
Write $a \in K^\times$ as $a = u\pi^m$ so that $u \in U(K), m \in \mathbb{Z}$.
Thus, $r_{L/K}(a) = \eta_{L/K}(u^{-1})\varphi_{L/L'}^m \stackrel{!}{=} \mathrm{id} \iff \eta_{L/K}(u) = \mathrm{id}$ and $\varphi_{L/L'}^m = \mathrm{id}$
$\stackrel{1.3.19}{\iff} u \in \mathcal{N}_L^0, n \mid m\, (\mathrm{ord}(\varphi_{L/L'}) = \mathrm{ord}(\varphi_{K_n/K}) = n) \iff a \in \mathcal{N}_L$.
1.3.19: $\eta_{L/K} : U(K) \to G(L/K)_0$ is surjective, and since $G(L/K) = G(L/K)_0 \cdot \varphi_{L/L'}^{\mathbb{Z}}$ we deduce that $r_{L/K}$ is surjective. □

Next goals:

1) Show that $r_{L/K}$ is independent of the choice $L' \subset L$.

2) To show that for any subextension $M/K \subset L/K$,

$$\ker(K^\times \to G(L/K) \to G(M/K)) = \mathcal{N}_M$$

Lemma 1.3.26. If L/K is an arbitrary finite abelian extension, then $[K^\times : \mathcal{N}_L] = [L : K]$.

Proof. Let $K_L \subset L$ be the maximal unramified subextension. Then L/K_L is totally ramified and if λ is a uniformizer of L, then $\pi := N_{L/K_L}(\lambda)$ is a unfiromizer of K_L. Hence, upto an element of $U(K_L)$ also a unfirmozer of $K \implies |K_L^\times| = |K^\times| = |\pi|^{\mathbb{Z}}$.

$$\implies \left|\frac{K^\times}{\mathcal{N}_L}\right| = \left|\frac{U(K)}{\mathcal{N}_L^0}\right| \left|\frac{|K^\times|}{|N_{L/K}(\lambda)|^{\mathbb{Z}}}\right|$$

$$\overset{1.3.19}{=} |G(L/K)_0| \left|\frac{|\pi|^{\mathbb{Z}}}{|N_{K_L/K}(\pi)|^{\mathbb{Z}}}\right| = |G(L/K)_0| \left|\frac{|\pi|^{\mathbb{Z}}}{|\pi|^{[K_L:K]\mathbb{Z}}}\right|$$

$$= |G(L/K)_0|[K_L : K] = e(L/K)f(L/K) = [L : K]$$

□

Proposition 1.3.27. Let $L', L, \lambda \in L'$ be as in the beginning of this section. Let $L'_2 \subset L$ be another totally ramified extension of K such that $L'_2.K_n = L$. Then,

$$\ker(K^\times \xrightarrow{r_{L/K}} G(L/K) \to G(L'_2/K)) = \mathcal{N}_{L'_2} \subset K^\times$$

Proof. Set $r = r_{L/K} : K^\times \to G(L/K)$. Recall $r(a) = \eta_{L/K}(a^{-1}\pi^{v(a)})\varphi_{L/L'}^{v(a)}$. Let r_2 be the composite homomorphism:

$$\begin{tikzcd} K^\times \arrow[r, "r"] \arrow[rr, bend left, "r_2"] & G(L/K) \arrow[r] & G(L'_2/K) \end{tikzcd}$$

r_2 is surjective by 1.3.25. r_2 induces an isomorphism:

$$K^\times/\ker(r_2) \to G(L'_2/K)$$

If we show that $\mathcal{N}_{L'_2} \subset \ker(r_2) \implies$ surjection $\underbrace{K^\times/\mathcal{N}_{L'_2}}_{\text{order } [L'_2:K]} \to K^\times/\ker(r_2) \xrightarrow{\cong}$ $G(L'_2/K)$

Hence $N_{L'_2} = \ker r_2$.

STS: $\mathcal{N}_{L'_2} \subset \ker(r_2)$.

$\mathcal{N}_{L'_2} = \mathcal{N}^0_{L'_2}\mathcal{N}_{L'_2/K}(\lambda_2)^{\mathbb{Z}}$ for any uniformizer λ_2 of L'_2.

Since $U(L'_2) = \left\{\lambda_2(\widetilde{\lambda}_2)^{-1} \mid \lambda_2, \widetilde{\lambda}_2 \text{ uniformizer of } L'_2\right\}$, it suffices to show $N_{L'_2/K}(\lambda_2) \in \ker(r_2)$ for any unformizer λ_2 of L'_2.

Note: L/L'_2 is unramified sicne $L = L'_2.K_n$. Therefore, $G(L/L'_2)$ is cycic and if we restrict this to $G(K_n/K)$ we get an isomorphism. Since $G(K_n/K)$ is generated by the frobenius $\langle\varphi_{K_n/K}\rangle$ and $\varphi_{L/L'}\big|_{K_n} = \varphi_{K_n/K}$:

Let φ_{L/L'_2} be the unique element with $\big|_{\varphi_{L/L'_2}} = \text{id}$. Then, $\varphi_{L/L'_2} \circ \varphi_{L/L'}^{-1}\Big|_{K_n} = \text{id}$ and $\varphi_{L/L'_2}\big|_{K_n} = \varphi_{K_n/K}$

$$\implies \varphi_{L/L'_2} \circ \varphi_{L/L'}^{-1} \in G(L/K)_0 \overset{1.3.19}{=} \eta_{L/K}(U(K))$$

Thus $\varphi_{L/L'_2} = r(u)\varphi_{L/L'}$ for some $u \in U(K)$.

Then, $G(L/L'_2) = \langle\varphi_{L/L'_2}\rangle$

Fix a uniformizer λ_2 of L'_2 which is a uniformizer of L. Then $\lambda_2 = x\lambda$ where $\lambda \in L', x \in U(L)$. Therefore,

$$\pi = N_{L'/K}(\lambda) = N_{L/K_n}(\lambda) = N_{L/K_n}(x^{-1})N_{L/K_n}(\lambda_2) = N_{L/K_n}(x^{-1})N_{L'/K}(\lambda_2) \in K$$

Therefore, $N_{L/K_n}(x) \in U(K)$.

Further, $(r(u)\varphi_{L/L'})(\lambda_2) = \varphi_{L/L'_2}(\lambda_2) = \lambda_2$.

Now we compute in $U(L_{nr}) = U((L')_{nr}) = U((L'_2)_{nr})$.

$$\frac{\eta_{L/K}(u^{-1})(\lambda)}{\lambda} = \frac{r(u)(\lambda)}{\lambda} = \frac{(r(u)\varphi_{L/L'})(\lambda)}{\lambda} = \frac{\overbrace{(r(u)\varphi_{L/L'})}^{\varphi_{L/L_2'}}(x^{-1}\lambda_2)}{x^{-1}\lambda_2}$$

$$= \frac{(r(u)\varphi_{L/L'})(x^{-1})(r(v)\varphi_{L/L'})(\lambda_2)}{x^{-1}\lambda_2} = \frac{(r(v)\varphi_{L/L'})(x^{-1})\lambda}{x^{-1}\lambda} = \frac{(r(v)\varphi_{L/L'})(x^{-1})}{x^{-1}}$$

$$= \frac{r(v)(\varphi_{L/L'}(x^{-1}))}{\varphi_{L/L'}(x^{-1})} \frac{\varphi_{L/L'}(x^{-1})}{x^{-1}} \equiv \frac{\varphi_{L/L'}(x^{-1})}{x^{-1}} \mod V(L'_{nr}/K_{nr})$$

□

Corollary 1.3.28. The definition of $r_{L/K}$ is independent of the choice of $L' \subset L$ and he uniformizer λ of L'.

Theorem 1.3.29. For any finite abelian extension Ln/K choose an unramified extension K_n/K such that $LK_n = L'K_n$ for L'/K totally ramified. Then,

$$\ker(r_{LK_n/K} : K^\times \to G(LK_n/K) \to G(L/K)) = \mathcal{N}_L$$

and induces an isomorphism:

$$\frac{K^\times}{\mathcal{N}_L} \xrightarrow[r_{L/K}]{\cong} G(L/K)$$

Tuesday, 2/18/2025

2 Tate's Article: p-divisible Groups

Let R be a complete discrete valuation ring (CDVR) with $\mathfrak{m}$ = maximal ideal, $k = R/\mathfrak{m}, K = \mathrm{Frac}(R)$.
Convention: R is not a field ($\iff \mathfrak{m} \neq 0$).
Futher Assumption: k is perfect of $\mathrm{char}(k) = p > 0$ and $\mathrm{char}(K) = 0$ (this is applicable in most settings we want to use this in).
Example: $R = \mathbb{Z}_p$ or the ring of integers in a finite extension $K/\mathbb{Q}_p =$. Then $K = \mathbb{Q}_p$ or a finite extension of $\mathbb{Q}_p$.
Example: $K = \widehat{\mathbb{Q}_p^{nr} p} \supset \mathcal{O}_{\widehat{\mathbb{Q}_p^{nr}}}, k = \overline{\mathbb{F}_p}$.
Example: k any perfect fielld of $\mathrm{char}(k) = p$ and $R = W(k)$ [Witt Vectors]. Then $\mathfrak{m} = pR$.
Goal: To study certain continuous representation of $\mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$ on finite dimensional $\mathbb{Q}_p$-vector spaces. Here we (implicitly) mean continuity by the Krull Topology
Krull Topology on $\mathrm{Gal}(K/F)$ is defined as follows:
Let $\mathcal{F} = \{L \mid L \text{ finite galois subextension of } K \text{ over } F\}$ and $\mathcal{N} = \{\mathrm{Gal}(K/L) \mid L \in \mathcal{F}\}$. Then a subset X of $\mathrm{Gal}(K/F)$ is open if $X = \varnothing$ or $X = \bigcup_i g_i N_i$ with $g_i \in G, N_i \in \mathcal{N}$. This makes $\mathrm{Gal}(K/F)$ a topological group.
The Prototypical Example is the p-adic cyclotomic character given by:

$$\chi_{cyc} : \mathscr{G}_K \to \mathbb{Z}_p^\times \curvearrowright \mathbb{Q}_q = V$$

$$\chi_{cyc}(\sigma) = a \in \mathbb{Z}_p^\times \iff \forall \zeta \in \mu_{p^\infty}(\overline{K}) : \sigma(\zeta) = \zeta^a$$

This is meant as follow: if $\zeta^{p^n} = 1$ and $a \equiv b \mod p^n$ for some $b \in \mathbb{Z}$ then $\zeta^a := \zeta^b$.
Equivalently, χ_{cyc} is obtained as the composition of:

$$\begin{tikzcd} \mathscr{G}_K \arrow[r, two heads, "\chi_{cyc}"] \arrow[rrr, bend right] & \varprojlim_n G(K(\mu_{p^n})/K) \arrow[r, hook] & \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \arrow[r, "="] & \mathbb{Z}_p^\times \end{tikzcd}$$

Note: if $K = \mathbb{Q}_p$ (or $\widehat{\mathbb{Q}_p^{nr}}$) then χ_{cyc} is surjective by the irreducibility of the cyclotomic polynomials. If $K/\mathbb{Q}_p$ is finite then $\chi_{cyc}(\mathscr{G}_K)$ is open.
Note: E/K elliptic curve, $E[p^n](\overline{K}) = \left\{x \in E(\overline{K}) \mid [p^n]_E(x) = \mathcal{O}_E\right\} \cong (\mathbb{Z}/p^n) \oplus (\mathbb{Z}/p^n) \curvearrowleft \mathscr{G}_K$. Therefore,
$\mathscr{G}_K \to \varprojlim_n \mathrm{Aut}(E[p^n](\overline{K})) = \mathrm{Aut}(\varprojlim E[p^n](\overline{K})) \cong \mathrm{Aut}(\varprojlim (\mathbb{Z}/p^n)^{\oplus 2}) = \mathrm{Aut}(\mathbb{Z}_p^{\oplus 2}) = \mathrm{GL}_2(\mathbb{Z}_p) \curvearrowright \mathbb{Q}_p^2$.
This gives us a $\mathbb{Z}_p$-linear action of $\mathscr{G}_K$ on $T_pE = \varprojlim E[p^n](\overline{K})$ called the p-adic Tate module of E, and also on $V_pE = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ which is a 2-dimensional $\mathbb{Q}_p$ vector space.
Final: Let $K/\mathbb{Q}_p$ finite and π = uniformizer. Then, $e = \mathscr{E}_\pi$ a LT series for π, F_e = LT $\mathcal{O}_K$ module.
$\mathscr{G}_K \curvearrowright T_pF_e = \varprojlim_n \underbrace{F_e[\pi^n](\overline{K})}_{\cong \mathcal{O}_K(\pi^n)} \underset{\text{non-canonically}}{\cong} \mathcal{O}_K$ as $\mathcal{O}_K$-module.
Thus, $\mathrm{im}(\mathscr{G}_K \to T_pF_e) \cong \mathcal{O}_K^\times = \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{O}_K)$.
Thus, $\mathscr{G}_K \curvearrowright V_pF_e = T_pF_e \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a vector space of dimension $[K : \mathbb{Q}_p]$.
LCFT tells us this factors through the abelianization: $\mathscr{G}_K \to \mathscr{G}_K^{ab} \curvearrowright V_pF_e$.
Question: Why p-adic representatons? Why not continuous representations $\mathscr{G}_K \to \mathrm{GL}_n(\mathbb{C})$? Why not $\mathscr{G}_K \to \mathrm{GL}(\mathbb{Q}_l), l \neq p$? Why not $\mathscr{G}_K \to \mathrm{GL}_n(\mathbb{A}_\mathbb{Q}) = \prod'_{l \leq \infty} GL_n(\mathbb{Q}_l)$ where $\mathbb{Q}_\infty = \mathbb{R}$?
Answer: We can study them, but the p-adic representations are especially interesting for the following reason: Continuous representations $\mathscr{G}_K \to \mathrm{GL}_n(\mathbb{C})$ have finite image! The topologies are incompatible.

For $\mathscr{G}_K \to \mathrm{GL}_n(\mathbb{Q}_l), l \neq p$ have finite image when restricted to the wild inertial subgroup $\mathscr{P}_K = \mathscr{G}_K^{>0} = \bigcup_{s>0} \mathscr{G}_K^s$ [upper numbering of ramification groups].
$\mathscr{G}_K \to \mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ are put together from representations into $\mathrm{GL}_n(\mathbb{Q}_l), l \leq \infty$.
About $\mathscr{G}_K$: There are two fundamental exact sequence:

$$1 \to \mathscr{I}_K \to \mathscr{G}_K \to \mathrm{Gal}(\overline{k}/k) \to 1$$

$\mathscr{I}_K$ is the inertia subgroup. It is closed, and we can write $\mathscr{I}_K = \mathscr{G}_K^0$.
Let $\pi \in K$ be a uniformizer. Then $\forall n \in \mathbb{Z}_{>0} \setminus p\mathbb{Z}, \forall \sigma \in \mathscr{I}_K$,

$$\frac{\sigma(\sqrt[n]{\pi})}{\sqrt[n]{\pi}} \in \mu_n(\overline{K})$$

is independent of the choince of $\sqrt[n]{\pi}$ and also independent of the choice of π. Hence one obtains a homomorphism $t : \mathscr{I}_K \to \varprojlim_{n>0, p\nmid n} \mu_n(\overline{K}) =: \widehat{\mathbb{Z}}^{(p)}(1)$.
superscript (p) since we're not taking the p divisible powers. 'Twist' by (1) since we're taking the roots of unity.
It is non-canonically isomorphic to $\varprojlim_{p\nmid n} \mathbb{Z}/n\mathbb{Z} = \prod_{l\neq p} \mathbb{Z}_l$.
Then, $\mathscr{P}_K = \ker(t)$. We have the following exact sequence:

$$1 \to \mathscr{P}_K \to \mathscr{I}_K \to \widehat{\mathbb{Z}}^{(p)}(1) \to 1$$

Theorem 2.0.1. $\mathscr{P}_K$ is a pro-p group, is maximal with this property, and is normal in $\mathscr{G}_K$. One has $\mathscr{P}_K = G(\overline{K}/K_{nr}(\sqrt[n]{\pi} \mid n > 0, p \nmid n))$.

$K_{nr}(\sqrt[n]{\pi} \mid n > 0, p \nmid n)$ is the maximal tamely ramified extension K^{tame}. We have the following exact sequence:

$$1 \to \widehat{\mathbb{Z}}^{(p)}(1) \to G(K^{tame}/K) \to G(K_{nr}/K) \cong G(\overline{k}/k) \to 1$$

We can be more precise: it is in fact a semidirect product.
Motto: p-adic vector spaces are the natural environment for representations of $\mathscr{G}_K$ (which is 'close to being a pro-p group', meaning it has a very large pro-p subgroup).
Plan: 2.1: Finite Group Schemes.
2.2: p-divisible groups.
2.3: $C = \widehat{\overline{K}}$. In case of $\mathbb{Q}_p$ we denote this by $\mathbb{C}_p$.
2.4: Theorems on Galois Representations attached to p-divisible groups.

2.1 Finite Group Schemes

2.1.1

Let R be a commutative ring. An affine group scheme over R is an affine scheme $G = \mathrm{Spec}(A) \xrightarrow{\uparrow s} S := \mathrm{Spec}(R)$ equipped with:

- a multiplication $m : G \underset{S}{\times} G \to G, S = \mathrm{Spec}(A \otimes_R A)$.
- A unit section $e : S \to G$
- An inversion $i : G \to G$

These are required to be morphisms over S.

Thursday, 2/20/2025

We redo:
Let R be a commutative ring. An affine group scheme over R is an affine scheme $G = \mathrm{Spec}\, A \xrightarrow{P_G} S = \mathrm{Spec}\, R$, equipped with morphisms over S:
$m = m_G : G \underset{S}{\times} G = \mathrm{Spec}(A \underset{R}{\otimes} A) \to G$
$i = i_G : G \to G$ [inverse]
$e = e_G$ unit section so that:

$$\begin{tikzcd}
S \arrow[rr] \arrow[dr, "id"'] & & G \arrow[dl, "P_G"] \\
& S &
\end{tikzcd}$$

such that the following diagrams are commutative:

1) Associativity:

$$\begin{tikzcd}
(G \underset{S}{\times} G) \underset{S}{\times} G \underset{can}{\cong} G \underset{S}{\times} (G \underset{S}{\times} G) \arrow[r, "m \times id"] \arrow[d, "id \times m"] & G \times G \arrow[d, "m"] \\
G \underset{S}{\times} G \arrow[r, "m"] & G
\end{tikzcd}$$

2) $$\begin{tikzcd}
G = S \underset{S}{\times} G = G \underset{S}{\times} \arrow[r, "e \times id"] \arrow[d, "id \times e"] \arrow[dr, "id"] & G \times G \arrow[d, "m"] \\
G \times G \arrow[r, "m"] & G
\end{tikzcd}$$

3) $$\begin{tikzcd}
G \arrow[rr, "i \times id"] \arrow[dr, "P_G"] \arrow[dd, "id \times i"'] & & G \times G \arrow[dd, "m"] \\
& S \arrow[dr, "e"] & \\
G \times G \arrow[rr, "m"] & & G
\end{tikzcd}$$

1-3 can be reformulated in terms of A.

- P_S makes A into an R-algebra.
- m corresponds to a morphism of R-algebras $\mu : A \to A \otimes_R A$, co-multiplication
- i corresponds to the morphism $\iota : A \to A$ inverson.
- e corresponds to $\varepsilon : A \to R$ called the co-unit

$(A, \mu, \iota, \varepsilon)$ has the property that the diagrams:

1') $$\begin{tikzcd}
(A \otimes_R A) \otimes_R A = A \otimes_R (A \otimes_R A) & A \otimes_R A \arrow[l, "\mu \otimes id"'] \\
A \otimes_R A \arrow[u, "id \otimes \mu"] & A \arrow[l, "\mu"] \arrow[u, "\mu"']
\end{tikzcd}$$

2') $$\begin{tikzcd}
R \otimes_R A = A \otimes_R R & A \otimes_R A \arrow[l, "\varepsilon \otimes id"'] \\
A \otimes_R A \arrow[u, "id \otimes \varepsilon"] & A \arrow[l, "\mu"] \arrow[u, "\mu"'] \arrow[ul, "id"']
\end{tikzcd}$$

3') $$\begin{tikzcd}
A & A \otimes_R A \arrow[l, "\delta"'] & A \otimes_R A \arrow[l, "\iota \otimes id"'] \\
A \otimes A \arrow[u, "\delta"] & & \\
A \otimes A \arrow[u, "id \otimes \iota"] & & A \arrow[ll, "\mu"] \arrow[uu, "\mu"']
\end{tikzcd}$$

Here $\delta : A \otimes_R A \to A$ is multiplication, $G \underset{\Delta}{\longrightarrow} G \underset{S}{\times} S$

This means that $(A, \mu, \iota, \varepsilon)$ is a Commutative Hopf Algebra.
The group scheme $G = \mathrm{Spec}(A)$ is called commutative if:

$$\begin{tikzcd} G \otimes G \arrow[r, "m"] \arrow[d, "(g,h)" above, "(h,g)" below] & G \arrow[d, "id"] \\ G \otimes G \arrow[r, "m"] & G \end{tikzcd}$$

commutes. Equivalently,

$$\begin{tikzcd} A \otimes_R A & A \arrow[l, "\mu"'] \\ A \otimes_R A \arrow[u, "a\otimes b" below, "b\otimes a" above] & A \arrow[l, "\mu"'] \arrow[u, "id"'] \end{tikzcd}$$

commutes. In this case A is called co-commutative.
Examples:

1) The additive group (scheme) $\mathbb{G}_{a,R}$ over R : $\mathbb{G}_{a,R} = \mathrm{Spec}(A), A = R[x], \mu : R[x] \to R[x] \otimes_R R[x]$ by $x \mapsto 1 \otimes x + x \otimes 1$.

   $\varepsilon : R[x] \to R$ by $\varepsilon(x) = 0, \iota : R[x] \to R[x]$ by $x \mapsto -x$.

2) The multiplicative group (scheme) $\mathbb{G}_{m,R}$ over R: $\mathbb{G}_{m,R} = \mathrm{Spec}(A)$, $A = R[x, x^{-1}] = R[x, t]/(tx - 1)$.

   $\mu : A \to A \otimes_R A, \mu(x) = x \otimes x, \mu(x^{-1}) = x^{-1} \otimes x^{-1}$.

   $\varepsilon : A \to R, \varepsilon(x) = \varepsilon(x^{-1}) = 1, \iota(x) = x^{-1}, \iota(x^{-1}) = x$.

3) The group scheme of n'th roots of unity $\underline{\mu}_{n,R} = \mathrm{Spec}(A), A = R[x]/(x^n - 1)$. Then $\mu(\overline{x}) = \overline{x} \otimes \overline{x}, \varepsilon(\overline{x}) = 1, \iota(\overline{x}) = \overline{x}^{-1} = \overline{x}^{n-1}$.

   The quotient map $R[x, x^{-1}] \to R[x]/(x^n - 1) = R[x, x^{-1}]/(x^n - 1)$ given by $x \mapsto \overline{x}$ is a morphism of Hopf algebras over R.

   This induces a closed immertion $\underline{\mu}_{n,R} \to G_{m,R}$.

4) Let Γ be any finite group of order m. Set $A = R^\Gamma$ (set of maps $f : \Gamma \to R$) equipped with pointwise addition and multiplication. Then,

   $A = R \times \cdots \times R$ product of rings,

   Comultiplication $\mu : A \to A \otimes_R A \cong R^{\Gamma \times \Gamma}, f \otimes g \mapsto [(\gamma, \delta) \mapsto f(\gamma)g(\delta)]$

   $\mu(f)(\gamma, \delta) = f(\gamma\delta)$.

   $\varepsilon : A \to R, \varepsilon(f) = f(1_\Gamma)$.

   $\iota : A \to A, \iota(f)(\gamma) = f(\gamma^{-1})$.

   Exercise: This makes $(A, \mu, \iota, \varepsilon)$ a commutative Hopf algebra, which is co-commutative if and only of Γ is commutatie.

   We set $\underline{\Gamma}_R = \mathrm{Spec}(R^\Gamma)$ and call it the constant group scheme associated to Γ.

   One can think of $\underline{\Gamma}_R$ as m copies of S labeled by the elements of Γ.

5) $\mathrm{GL}_{n,R} = \mathrm{Spec}(A), A - R[x_{ij} \mid 1 \leq i, j \leq n][t]/(t \det -1)$. $\mathrm{SL}_{n,R}$ is closed inside $\mathrm{GL}_{n,R}$. $\mathrm{SL}_{n,R} = \mathrm{Spec}(A/I)$, A as above, $\det = \det((x_{ij})), I = (\overline{t}-1) = (\det -1)$.

Caution: If G is a group scheme over S then $|G|$ = underlying set (topological space) is in general not a group.
For example, $G = \mathbb{G}_{a,\mathbb{C}} = \mathrm{Spec}(\mathbb{C}[x])$ which is bijective with $\mathbb{C} \cup \{\eta\}$ where η is a generic point associated to (0), the zero ideal.
Note: $|G \underset{\mathrm{Spec}(\mathbb{C})}{\times} G| = |\mathrm{Spec}(\mathbb{C}[x, y])| \neq |\mathrm{Spec}(\mathbb{C}[x])| \times |\mathrm{Spec}(\mathbb{C}[y])|$

Points If $T \xrightarrow{f} S$ is a scheme over $S = \mathrm{Spec}(R)$ eg $T = \mathrm{Spec}(R')$ and $G \to S$ is a group scheme, then $G(T) \coloneqq \mathrm{Mor}_{\mathrm{Scheme}\,/S}(T, G)$. In the affine scheme it is the same as $\mathrm{Hom}_{R\text{-alg}}(A, R')$ if $G = \mathrm{Spec}(A), T = \mathrm{Spec}(R')$.
$G(T)$ is naturally a group, called the group of T-valued points of G.

Given x, y :
$$\begin{tikzcd} T \arrow[rr] \arrow[dr] & & G \arrow[dl] \\ & S & \end{tikzcd}$$

There is a commutative diagram:

$$\begin{tikzcd} & G \times_S G \arrow[dr, "p_2"] \arrow[dd, "p_1"] & \\ T \arrow[ur, "\exists! xy"] \arrow[rr, "x"] \arrow[dr, "y"'] & & G \arrow[d] \\ & G \arrow[r] & S \end{tikzcd}$$

$x^{\#} - y^{\#}(b) \leftarrow\!\shortmid a \otimes b$

$$\begin{tikzcd} & A \otimes_R A \arrow[dl, "(x\,y)^{\#}"'] & \\ R' & & A \arrow[ll, "x^{\#}"] \arrow[ul] \\ & A \arrow[ul, "y^{\#}"] \arrow[uu] & R \arrow[l] \arrow[u] \end{tikzcd}$$

Then define $x \cdot y \coloneqq m \circ (x, y) : T \to G$.
$R' \xleftarrow{(x,y)^{\#}} A' \otimes_R A \xleftarrow{\mu} A$.
This gives $G(T)$ the structure of a group with unique element $e_G \circ f$ where $T \xrightarrow{f} S$ is the structure map.
For example,

1) $\mathbb{G}_{a,R}(R') = (R', +)$.

   $\mathrm{Hom}_{R\text{-alg}}(R[x], R') \xleftrightarrow{bij} R'$ with $\varphi \mapsto \varphi(x)$.

2) $G_{m,R}(R') = ((R')^{\times}, \cdot), \mathrm{Hom}_{R\text{-alg}}(R[x, x^{-1}], R')$ with $\varphi \mapsto \varphi(x) \in (R')^{\times}$.

   $\underline{\mu}_{n,R}(R') = \{a \in R' \mid a^n = 1\}$ is not necessarily finite if R' is not an integral domain. Sometimes we also have very few roots of unity.

   For example, if $n = p^m, p$ prime and $R = \mathbb{F}_p$ and R' an integral domain (and also $\mathbb{F}_p$ algebra), then,

   $\underline{\mu}_{p^m,\mathbb{F}_p}(R')$. This is because $(x^{p^m} - 1) = (x - 1)^{p^m}$.

Definition. Let $S = \mathrm{Spec}(R)$. Let $G = \mathrm{Spec}(A), H = \mathrm{Spec}(B)$ two (affine) group schemes over S. A homomorphism $f : H \to G$ over S is a morphism of schemes over S such that the following diagram commutes:

$$\begin{tikzcd} H \times H \arrow[r, "m_H"] \arrow[d, "f \times f"] & H \arrow[d, "f"] \\ G \times G \arrow[r, "m_G"] & G \end{tikzcd}$$

If G and H are affine (as indicated) then f corresponds to $f^{\#} : A \to B$ a morphism of R algebras and f is a homomorphism if and only if $f^{\#}$ is a homomorphism of Hopf Algebras.

Example Suppose p prime, $R = \mathbb{F}_p$ algebra, $\alpha_{p,R} = \mathrm{Spec}(A), A = R[x]/(x^p)$ with co-multiplication $\mu(\overline{x}) = 1 \otimes \overline{x} + \overline{x} \otimes 1$ and inversion $\iota(\overline{x}) = -\overline{x}$ and $\varepsilon(\overline{x}) = 0$.
Then $R[x] \to A$ gives a morphism:

$$\alpha_{p,R} \to \mathbb{G}_{a,R}$$

Question: Is $\alpha_{p,R}$ isomorphic to $\mu_{p,R}$?
Example 2: Suppose R is a k-algebra and k is a field containing a primitive n'th root of unity. Then $\mathrm{char}\, k \nmid n$. In this case, $\underline{\mu}_{n,R} \cong \underline{\mathbb{Z}/n\mathbb{Z}}_R$.

Tuesday, 2/25/2025

Note that, in the previous question, even though as schemes $\underline{\alpha}_{p,R} \cong \underline{\mu}_{p,R}$, they are not isomorphic as group schemes over R.

Definition. A group scheme $G \xrightarrow{p_G} S = \mathrm{Spec}(R)$ is called finite, if p_G is a finite morphism ($G = \mathrm{Spec}(A)$ is affine and $p_G^{\#} : R \to A$ makes A into a finitely generated R-module).
A finite group scheme G/R [here $G = \mathrm{Spec}(A)$] is called flat (resp. locally free) if A is flat (resp. projective) R-module.
We denote by Gps_R the category of (affine) group schemes $/R$ and $\mathrm{Gps}^{\mathrm{fin/proj}}$ category of finite locally free free group schemes $/R$ and $\mathrm{Gps}_R^{\mathrm{fin}}$ category of finite group schemes $/R$.

Example from LT Theory: Let $K/\mathbb{Q}_p$ be finite, $F_e = $ LT $\mathcal{O}_K$ module attached to the LT series $e \in \mathscr{E}_\pi, F_e[\pi^m] \coloneqq \mathrm{Spec}(\mathcal{O}_K[[x]]/([\pi^m]_{F_e}(x)))$.
Fact (HW7): $A_m \coloneqq \mathcal{O}_K[[x]]/([\pi^m]_{F_e}(x))$ is a free $\mathcal{O}_K$-module of rank q^m where $q = |k_K|$.
Hence, the co-multiplication $A_m \to A_m \otimes_{\mathcal{O}_K} A_m$ is given by the formal module structure: $x \mapsto F_e(x_1, x_2) \in \mathcal{O}_K[[x_1, x_2]]/([\pi^m](x_1), [\pi^m](x_2)) \cong \mathcal{O}_K[x_1]/([\pi^m](x_1)) \otimes_{\mathcal{O}_K} \mathcal{O}_K[[x_2]]/([\pi^m](x_2))$.
Inversion map is given by inversion on F_e.
Augmentation ($\leftrightarrow$ unit section) $A_m \to \mathcal{O}_K, x \mapsto 0$.

Remark. If M is a finitely generated projective R-module then $\forall P \in \mathrm{Spec}(R)$ the localization M_P is a finitely generated free R_P-module. This is a consequence of Nakayama's Lemma.
The function $\mathrm{Spec}(R) \to \mathbb{Z}_{\geq 0}, \mathrm{rk}(M)(P) \coloneqq \mathrm{rank}_{R_P}(M_P)$ is locally constant.
If G is in $\mathrm{Gps}_R^{\mathrm{fin,proj}}$ then we let $\mathrm{rk}(G) \coloneqq \mathrm{rk}(A)$ where $G = \mathrm{Spec}(A)$. We call it the rank or order of G.

2.1.2 Carter Duality

From now on all group schemes are assumed to be commutative. Given an affine group scheme $G = \mathrm{Spec}(A)$ over R we set $\mathcal{O}(G) = A$. So, $\mathcal{O}(G)$ is the corresponding affine algebra of G.
Let $\mu : A \to A \otimes_R A$ be the co-multiplication, and $\delta_A : A \otimes_R A \to A$ the multiplication. Then, $\delta_A(a \otimes b) = ab$.
Let $A^\vee = \mathrm{Hom}_{R\text{-mod}}(A, R)$. Now assume that A is f.g. projective ($\iff$ G is finite, locally free).
Then we have the following:
$(A \otimes_R A)^\vee = \mathrm{Hom}_{R\text{-mod}}(A \otimes_R A, R) = \mathrm{Hom}_{R\text{-mod}}(A, \mathrm{Hom}_{R\text{-mod}}(A, R))$
$= \mathrm{Hom}_{R\text{-mod}}(A, R) \otimes_R \mathrm{Hom}_{R\text{-mod}}(A, R) = A^\vee \otimes_R A^\vee$.
Consider the maps: $\delta_{A^\vee} \coloneqq \delta_A^\vee : A^\vee \to (A \otimes_R A)^\vee \underset{can}{\cong} A^\vee \otimes_R A^\vee$
$\mu_{A^\vee}$
Proposition/Definition 2.1.2.1. Let $G \in \mathrm{Gps}_R^{\mathrm{fin,\ proj}}, A = \mathcal{O}(G)$. Then $A^\vee$ equipped with the multiplication is given by $\delta_{A^\vee} = \mu_A^\vee$ is a commutative ring with unit $\varepsilon_A : A \to R (\varepsilon_A \in A^\vee)$.
If we define:

$\varepsilon_{A^\vee} : A^\vee \to R, \varepsilon_{A^\vee}(f) = f(0)$
$\iota_{A^\vee} := \iota_A^\vee : A^\vee \to A^\vee, \iota_{A^\vee}(f) = f \circ \iota_A$
Then $A^\vee, \mu_{A^\vee}, \iota_{A^\vee}, \varepsilon_{A^\vee}$ is a co-commutative Hopf algbra of the same rank as fcs on Spec(R).
Furthermore, the map $A \to (A^\vee)^\vee$ given by $a \mapsto (f \mapsto f(a))$ is an isomorphism of Hopf Algebras. We set $G^\vee$: Spec($A^\vee$) and call it the <u>Carter Dual</u> of G. Then, $(G^\vee)^\vee \underset{can}{\cong} G$.
Example: let $G = \underline{\mu}_{n,R}, A = R[x]/(x^n - 1), \mu_A(\overline{x}) = \overline{x} \otimes \overline{x}$.
$A^\vee = \bigoplus_{i=0}^{n-1} Rf_i, f_i\left(\sum_{j=0}^{n-1} a_j \overline{x}^j\right) = a_i \in R$.
Then, $(f_i \cdot f_j)(\overline{x}^k)$ can be evaluated as follows:
Recall $A^\vee \otimes_R A^\vee \to A^\vee$ is given by $f \otimes g \mapsto [a \mapsto (f \otimes g)(\mu_A(a))]$. Then,

$$(f_i \cdot f_j)(\overline{x^k}) = (f_i \otimes f_j)(\mu_A(\overline{x}^k)) = (f_i \otimes f_j)(\overline{x}^k \otimes \overline{x}^k) = f_i(\overline{x}^k) f_j(\overline{x}^k)$$

Therefore, $(f_i \cdot f_j)(\overline{x}^k) = \begin{cases} 1, & \text{if } i = j = k; \\ 0, & \text{otherwise.} \end{cases}$
Therefore, $f_i f_j = \delta_{i,j} f_i$.
Thus, $f_0, \cdots, f_{n-1}$ are <u>pairwise orthogonal idempotents</u>. Furthermore, $f_0 + \cdots + f_{n-1} = 1_{A^\vee}$.
Therefore, as an R-algebra,

$$A^\vee = \prod_{i=0}^{n-1} Rf_i \cong R \times \cdots \times R \overset{!}{=} R^{\mathbb{Z}/n\mathbb{Z}}$$

Then, the co-multiplication on $A^\vee \cong R^{\mathbb{Z}/(n)}$ is given by:

$$R^{\mathbb{Z}/(n)} \to R^{\mathbb{Z}/(n)} \times R^{\mathbb{Z}/(n)} = R^{\mathbb{Z}/(n) \times \mathbb{Z}/(n)}$$

$$f \mapsto [(i \mod n, j \mod n) \mapsto f(i + j \mod n)]$$

$f \in R^{\mathbb{Z}/n\mathbb{Z}} \leftrightarrow \left[\sum_{i=0}^{n-1} a_i \overline{x}^i \mapsto \sum_{i=0}^{n-1} a_i f(i)\right]$
Therefore, $(\underline{\mu}_{n,R})^\vee \cong \underline{\mathbb{Z}/n\mathbb{Z}}_R$
Example: Assume p is prime and R an $\mathbb{F}_p$ algebra. Then, $(\underline{\alpha}_{p,R})^\vee \cong \underline{\alpha}_{p,R}$.
Note that this proves that $\underline{\alpha}_{p,R} \ncong \underline{\mu}_{p,R}$ for any ring $R \neq 0$.

Sketch of proof of 2.1.2.1. Check Associativity of multiplication $\delta_{A^\vee}$. It comes from the associativity of the comultiplication.
Let $a \in A$. Write $\mu_A(a) = \sum_i a_i \otimes b_i$.
$\mu_A(b_i) = \sum_j b_{ij} \otimes d_{ij}, \mu_A(a_i) = \sum_k a_{ik} \otimes c_{ik} \implies \sum_{i,k} a_{ik} \otimes c_{ik} \otimes b_i = \sum_{i,j} a_i \otimes b_{ij} \otimes d_{ij}$.
For all $f, g, h \in A^\vee : ((f \cdot g) \cdot h)(a) = ((f \cdot g) \otimes h)(\mu_A(a)) = \sum_i (f \cdot g)(a_i) h(b_i) = \sum f(a_{ik}) g(c_{ik}) h(b_i) = (f \otimes g \otimes h)\left(\sum a_{ik} \otimes c_{ik} \otimes b_i\right) = (f \otimes g \otimes h)\left(\sum a_i \otimes b_{ij} \otimes d_{ij}\right) = \sum f(a_i)(gh)(b_i) = (f \cdot (g \cdot h))(a)$.
Similarly one proves the associativity of co-multiplicatin $\mu_{A^\vee}$ and verify the other axioms.

□

Functorial Description of the Carter Dual

Let $G = \text{Spec}(A) \in \text{Gps}_R^{\text{fin,proj}}$ for $R' \in R$-alg (= cattegory of comm. R-algebras) we define:

$$\underline{\text{Hom}}(G, \mathbb{G}_m)(R') := \text{Hom}_{\text{Gps}_{R'}}(G_{R'}, \mathbb{G}_{m,R'})$$

$$= \text{Hom}_{R'\text{-Hopfalg}}(\mathcal{O}(\mathbb{G}_{m,R'}), \mathcal{O}(G_{R'})) = \text{Hom}_{R'\text{-Hopfalg}}\left(R'[x, x^{-1}], A \otimes_R R'\right)$$

This is a functor: R-alg $\to$ (Groups) into the category of abstract groups.

If we have $\alpha, \beta : G_{R'} \to \mathbb{G}_{m,R'}$ we can multiply them, $\alpha \cdot \beta : G_{R'} \to \mathbb{G}_{m,R}$ is a homomorphism.
Proposition 2.1.2.2 If $G \in \mathrm{Gps}_R^{\text{fin,proj}}$, then $G^\vee \underset{can}{\cong} \underline{Hom}(G, \mathbb{G}_m)$.

Thursday, 2/27/2025

Notation: Given a ring R we denote by Ab_R the category of affine commutative group schemes over R, and $\mathrm{Ab}_R^{\text{fin}}(\mathrm{Ab}_R^{\text{fin, proj}})$ the categoory of objects which are finite (resp. finite and locally free ($\iff$ $\mathcal{O}(G)$ is projective)) over R.
For $R' \in R$-alg we defined $\underline{Hom}(G, \mathbb{G}_m)(R') = \mathrm{Hom}_{\mathrm{Ab}_{R'}}(G_{R'}, \mathbb{G}_{m,R'})$.
Proposition 2.1.2.2. For $G \in \mathrm{Ab}_R^{\text{fin,proj}}$ we have $G^\vee$ (=Carter dual) $\cong \underline{Hom}(G, \mathbb{G}_m)$.

Sketch. $R' \in R$-alg. Then,
$G(R') = \mathrm{Hom}_{R\text{-alg}}(\underset{\mathcal{O}(G)}{A}, R') \hookrightarrow \mathrm{Hom}_{R\text{-mod}}(\underset{proj}{A}, R') \cong \mathrm{Hom}_{R\text{-mod}}(A, R) \otimes_R R' = A^\vee \otimes_R R'$.
Where $\underbrace{A^\vee}_{A^\vee_{R'}} = \mathrm{Hom}_{R\text{-mod}}(A, R)$. Consider $\varphi : A \to R' \in G(R')$, an R-algebra homomorphism. We can then make φ into R'-linear in the obvious way: $A \otimes_R R' \xrightarrow{\varphi} R'$ with $a \otimes r \mapsto \varphi(a) \otimes r$.
$\mu_{A^\vee_{R'}}$
$\mu_{A^\vee_{R'}} : A^\vee_{R'} \to A^\vee_{R'} \to A^\vee_{R'} \otimes_{R'} A^\vee_{R'} \cong (A_{R'} \otimes_{R'} A_{R'})^\vee$
Therefore, $(\mu_{A^\vee_{R'}}(\varphi))(a \otimes b) = \varphi(a \otimes b)\varphi \underset{=}{\text{ring}} \text{hom}\varphi(a)\varphi(b) = (\varphi \otimes \varphi)(a \otimes b)$.
Therefore, $\mu_{A^\vee_{R'}}(\varphi) = \varphi \otimes \varphi$.

Remark. An element φ of a Hopf algebra H over R' is called group-like if the comultiplication $\mu_H(\varphi) = \varphi \otimes \varphi$.

So, φ is group-like.
On the other hand, any element Φ of $\underline{Hom}(G^\vee, \mathbb{G}_m)(R') = \mathrm{Hom}(G^\vee_{R'}, \mathbb{G}_{m,R'}) = \mathrm{Hom}_{R'\text{-alg}}(R'[x, x'], A^\vee \otimes_R R')$ is completely determined by $\Phi(x) \in A^\vee_{R'}$. Let this be Ψ.
Then we have $\Psi(ab) = \mu_{A^\vee_{R'}}(\Psi)(a \otimes b) = (\Phi \otimes \Phi)(\mu_{\mathbb{G}_{m,R'}}(x))(a \otimes b) = (\Phi \otimes \Phi)(x \otimes x)(a \otimes b) = \Psi(x) \otimes \Psi(x)(a \otimes b) = \Psi(a)\Psi(b)$.
Moreover $\Psi \cdot \Phi(x^{-1}) = \Phi(x)\Phi(x^{-1}) = \Phi(1) = 1$.
Therefore, $\Psi \in (A^\vee_{R'})^\times$.
Check: the element φ from before is a unit in $A^\vee_{R'}$.
Therefore, $\underline{Hom}(G^\vee, \mathbb{G}_m)(R') = \mathrm{Hom}_{(\text{Hopf algs}/R')}(R'[x, x^{-1}], A^\vee_{R'})$
$= \{\varphi \in (A^\vee_{R'})^\times \mid \varphi(ab) = \varphi(a)\varphi(b)\}$
$= \mathrm{Hom}_{R'\text{-alg}}(A, R') = G(R')$.
$\implies \underline{\mathrm{Hom}}(G^\vee, \mathbb{G}_m) \cong G$
Replace G by $G^\vee$ and use the fact that $G^{\vee\vee} \underset{can}{\cong} G$.
Therefore, $G^\vee \cong \underline{Hom}(G, \mathbb{G}_m)$.

□

Example: $(\underline{\alpha}_{p,R})^\vee \cong \underline{\alpha}_{p,R}$ [from HW7]
$(\mu_{n,R})^\vee \cong \underline{\mathbb{Z}/n\mathbb{Z}}_R$.

2.1.3 Short Exact Sequences

Let $G, G', G'' \in \mathrm{Ab}_R^{\text{fin,proj}}$.

Definition. A sequence $0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0$ is called exact if:

i) f is a closed immersion ($\iff$ $f^\# : \mathcal{O}(G) \to \mathcal{O}(G')$ is surjective) which identifies (G', f) with the categorical kernel of g in Ab_R.

(If $H \in \mathrm{Ab}_R$ and $h : H\searrow \xrightarrow[S=\mathrm{Spec}(R)]{} \swarrow G$ has the property that $g \circ h = e_{G''} \circ p_H$ [here p_H is the map $H \to S$] then there is a unique $h' : H \to G'$ such that $h = f \circ h'$).

ii) g is faithfully flat ($\iff$ $g^{\#} : \mathcal{O}(G'') \to \mathcal{O}(G)$ is faithfully flat).

Propositon 2.1.3.1. Let $0 \to G' \to G \to G \to G'' \to 0$ be an exact sequence in $\mathrm{Ab}_R^{\mathrm{fin,proj}}$. Then,

i) $\mathrm{rk}(G) = \mathrm{rk}(G')\,\mathrm{rk}(G'')$ as functions on $\mathrm{Spec}(R)$.

ii) The dual sequence $0 \to (G'')^\vee \to G^\vee \to (G')^\vee \to 0$ is exact.

<u>Reference</u>: Demazure, Gabriel Groupes Algebriques, SGA 3

Remark. 1) If $0 \to H \to G \to Q \to 0$ is exact sequence of affine commutative group schemes $/R$, then the sequence of R' valued points:

$$0 \to H(R') \to G(R')Q(R') \to 0$$

need <u>not</u> be exact for $R' \in R$-alg. Usually surjectivity is the problem.

Example: We take $G = \mathrm{Res}_{\mathbb{R}}^{\mathbb{C}}(\mathbb{G}_{m,\mathbb{C}}) = \mathrm{Spec}(\mathbb{R}[x,y,z]/(z(x^2+y^2)-1)) \supset H = \mathrm{Spec}(\mathbb{R}[x,y]/(x^2+y^2-1))$.

<u>Fact</u>: The morphism $G = \mathrm{Spec}(\mathbb{R}[x,y]\left[\frac{1}{x^2+y^2}\right]) \underset{\leftarrow\!\shortmid}{\to} Q : \mathbb{G}_{m,\mathbb{R}} = \underset{t}{\mathrm{Spec}}(\mathbb{R}[t,t^{-1}])$
x^2+y^2
is the quotient of G by $H :=$ we have an exact sequence of algebraic groups $1 \to H = S^1 \to \underset{(x,y)}{\mathrm{Res}_{\mathbb{R}}^{\mathbb{C}}(\mathbb{G}_{m,\mathbb{C}})} \underset{\mapsto}{\to} \underset{x^2+y^2}{\mathbb{G}_{m,\mathbb{R}}} \to 1$.

Take $\mathbb{R}$-valued points: $1 \to H(\mathbb{R}) = \underset{\subset \mathbb{C}^\times}{S^1} \to \underset{(x,y)}{\mathbb{C}^\times} \underset{\mapsto}{\to} \underset{x^2+y^2}{\mathbb{R}^\times} \to 1$

Note that $(x,y) \mapsto x^2+y^2$ is <u>not</u> surjective!

2) If $R = K$ is a field and $G \in \mathrm{Ab}_R$ has the property that $\forall$ field extensions $L/K : G(L) = \{1\}$ then this does <u>not</u> imply that G is the trivial group scheme over R.

Example: $\mathrm{char}\, K = p > 0$ and $G = \underline{\mu}_{p,K} \implies \forall L/K$ field extensions, $\underline{\mu}_{p,K}(L) = \{1\}$.

Prototypical Examples of Exact Sequences:

1)
$$\zeta \longmapsto \zeta \qquad a \longmapsto a^p$$

$$1 \longrightarrow \underline{\mu}_{p,R} \longrightarrow \underline{\mu}_{p^n,R} \longrightarrow \underline{\mu}_{p^{n-1},R} \longrightarrow 1$$

$$R[t]/(t^p-1) \longleftarrow R[x]/(x^{p^n}-1) \qquad R[y]/(y^{p^{n-1}}-1)$$

$$\bar{t} \longleftarrow\!\shortmid\; \bar{x} \qquad \bar{x}^p \longleftarrow\!\shortmid\; \bar{y}$$

2) If $F = F_e$ is a LT $\mathcal{O}_K$-module for a uniformizer π then,

$$a \longmapsto [\pi](a)$$

$$0 \longrightarrow F[\pi] \longrightarrow F[\pi^m] \longrightarrow F[\pi^{m-1}] \longrightarrow 0$$

3) If $R = k = \overline{k}$ is a field of char $p > 0$ and E an ordinary elliptic curve over k [so $E[p](k) = E(k)[p] \cong \mathbb{Z}/p$] then,

$$0 \to E[p]^0 \to E[p] \to E[p]^{\text{ét}} \cong \underline{\mathbb{Z}/p}_k \to 0$$

$E[p]^0$ is connected component of rank p.

$E[p]$ has rank p^2

$E[p]^{\text{ét}}$ is the Étale quotient.

2.1.4 Connected and étale groups

In this section $(R, \mathfrak{m})$ is a local complete noetherian ring (in particular, $R \xrightarrow{can} R/\mathfrak{m}^n$ is an isomorphism). Let $G \in \mathrm{Gps}_R^{\text{fin,loc free}} = \text{proj}, G = \mathrm{Spec}(A), A$ finite projective R-module.

Remark. In such a case A is a free R-module [since R is local] [HW7].

There is an exact sequence in $\mathrm{Gps}_R^{\text{fin, loc. free}}$

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0$$

where G^0 is connected [ie the underlying topological space is connected] and $G^{\text{ét}}$ is étale, $\mathcal{O}(G^{\text{ét}})$ is an étale R-algebra.

Definition. Let $A \xrightarrow{\varphi} B$ be a finitely generated A-algera. Then B is called étale over A, if

1) B is a flat A-module, meaning $B \otimes_A (-)$ is an exact functor.
2) $\forall \mathfrak{q} \in \mathrm{Spec}(B)$ the homomorphism $A_\mathfrak{p} \to B_\mathfrak{q}$ where $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$ is unramified. i.e:
   - $\varphi_\mathfrak{q}(\mathfrak{p}A\mathfrak{p}) \cdot B_\mathfrak{q} = \mathfrak{q} \cdot B_\mathfrak{q}$
   - $\kappa(\mathfrak{q}) := B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q} (= \mathrm{Frac}(B/\mathfrak{q}))$ is a separable (finite) extension of $\kappa(\mathfrak{p}) = \mathrm{Frac}(A/\mathfrak{p})$

Example:

1) $|\Gamma| < \infty \implies \underline{\Gamma}_R = \mathrm{Spec}(R^\Gamma)$ is étale.
2) If $A, B/R$ is étale then $A \times B$ is étale over R.
3) $\underline{\mathbb{Z}/n\mathbb{Z}}_R$ is étale over R
4) If $n \in R^\times$ then $\underline{\mu_n}_R$ is étale (HW7)

   Proposition. (Milne, Ét. Coh. I, Prop 3.2) Let A be an R-algebra of finite type. Then A is unramified over $R \iff \forall \mathfrak{p} \in \mathrm{Spec}(R)$ and any separably closed extension $\widetilde{k}/\kappa(\mathfrak{p}) = \mathrm{Frac}(R/\mathfrak{p})$, the $\widetilde{k}$-algebra

   $$A \otimes_R \widetilde{k} = (A \otimes_R \kappa(\mathfrak{p})) \otimes_{\kappa(\mathfrak{p})} \widetilde{k}$$

   Is unramified over $\widetilde{k}$, ie a finite product of copies of $\widetilde{k}$.

   For us, étale = flat + unramified. We generally already have flat since we're working in the local case.

   $$\left(\underline{\mu}_{n,R} \times_{\mathrm{Spec}(R)} \mathrm{Spec}(\kappa(\mathfrak{p}))\right) \times_{\mathrm{Spec}(\kappa(\mathfrak{p}))} \mathrm{Spec}(\widetilde{k}) = \underline{\mu}_{n,\widetilde{k}}$$

5) R is a field of char $p > 0$ then $\underline{\mu}_{p^n,R}$ and $\underline{\alpha}_{p,R}$ are not étale over R, but they are connected: $|\underline{\mu}_{p^n,R}| = n\{*\} = |\underline{\alpha}_{p,R}|$ where $|\cdot|$ denotes the underlying topological space.

6) Suppose $(R, \mathfrak{m})$ is local and $\mathrm{char}(R/\mathfrak{m}) = p > 0$ and $n = p^e m, e > 0, p \nmid m$. Then the connected-étale sequence for $\underline{\mu}_{n,R}$ is:

$$0 \to \underline{\mu}_{p^e,R} = (\underline{\mu}_{n,R})^0 \to \underline{\mu}_{n,R} \xrightarrow{\zeta \mapsto \zeta^{p^e}} \underline{\mu}_{m,R} = (\underline{\mu}_{n,R})^{\text{ét}} \to 0$$

This sequence actually splits. $\underline{\mu}_{n,R} = \underline{\mu}_{p^e,R} \times_{\mathrm{Spec}(R)} \underline{\mu}_{m,R}$.

$\underline{\mu}_{p^e,R} = \mathrm{Spec}(R[x]/(x^{p^e} - 1))$: show that $R[x]/(x^{p^e} - 1)$ is a local ring. It is known that spec of local rings are connected.

More facts:
G is connected $\iff G = G^0$. Then the order of G is a power of $p = \mathrm{char}(R/\mathfrak{m})$.
In particular, G is étale if $\mathrm{char}(R/\mathfrak{m}) = 0$.
G is étale iff $G = G^{\text{ét}}$. One has an equivalence of categories:
The category of finite affine étale commutative and co-commutative Hopf algebras over R.
The category of finite abelian groups Γ together with a continuous action of the absolute galois group $G_k \times \Gamma \to \Gamma$ by group automorphisms [here $k = R/\mathfrak{m}$].
Note that if R is local noetherian then f.g. flat $\iff$ f.g. proj. $\iff$ f.g. free.
The equivalence is given as follows: $A \mapsto \mathrm{Hom}_R(A, k^{\text{sep}})$.
If $G = \mathrm{Spec}(A)$ then $G \mapsto G(k^{\text{sep}})$.
There is a maximal étale extension $R_{\text{ét}}$, called the strict Henselization, which is local and whose residue field is k^{sep} (= separable closure of k), an done has an isomorphism of groups:

$$\mathrm{Aut}(R_{\text{ét}}/R) \xrightarrow{\cong} G_k$$

And $(R_{\text{ét}})^{G_k} = R$
Given $(\Gamma, G_k \to \mathrm{Aut}(\Gamma))$ one sets $A_\Gamma := \mathrm{Map}_{G_k}(\Gamma, R_{\text{ét}})$ [Galois Equivariant Map].
$\implies A_\Gamma$ is a finite free R-module, and étale as R-algebra and A_Γ has a Hopf-algebra structure, and then $\underline{\Gamma}_R = \mathrm{Spec}(A_\Gamma)$ is a commutative finite locally free étale group scheme over R.

Remark. If $(\Gamma, G_k \to \mathrm{Aut}(\Gamma))$ then $\forall \sigma \in G_k, \sigma(0_\Gamma) = 0_\Gamma$. Thus,

$$\mathrm{Map}_{G_k}(\Gamma, R_{\text{ét}}) = \mathrm{Map}_{G_k}(\{0_\Gamma\}, R_{\text{ét}}) \times \mathrm{Map}_{G_k}(\Gamma \setminus \{0\}, R_{\text{ét}})$$

$$= R \times \underbrace{\mathrm{Map}_{G_k}(\Gamma \setminus \{0\}, R_{\text{ét}})}_{=\ker(\varepsilon_{A_\Gamma}),\text{ kernel of co-unit}}$$

Note that $\ker(\varepsilon_{A_\Gamma})$ is itself a ring, so $A_\Gamma = R \times \ker(\varepsilon_{A_\Gamma})$ is itself a product ring.
Therefore, $\underline{\Gamma}_R = \mathrm{Spec}(A_\Gamma) = \underbrace{\mathrm{Spec}(R)}_{\text{image of unit section}} \coprod \mathrm{Spec}(\ker(\varepsilon_{A_\Gamma}))$.
Upshot: If $\Gamma \neq 0$ then $\underline{\Gamma}_R$ is not connected.
A finite locally free étale group scheme is never connected unless it is the trivial group scheme (assumption R is local).

2.2 p-divisible groups

p always denotes a prime number.

Definition. An (abstract) abelian group Γ is callled $\underline{p\text{-divisible}}$ if $[p]_\Gamma : \Gamma \to \Gamma, a \mapsto pa := a + \cdots + a$ is surjective.
In particular, every element of Γ can be 'divided' by p. Note that the result of the division need not be unique. Meaning, $[p]_\Gamma$ need not be injective.

Example. 1) $\Gamma = \mathbb{Q}$ is uniquely p-divisible: $[p]_\mathbb{Q}$ is a bijection.

2) $\Gamma = \mathbb{Q}_p/\mathbb{Z}_p = \bigcup_{\nu=0}^\infty \frac{1}{p^\nu}/\mathbb{Z}$. It is surjective but not injective: $[p]_{\mathbb{Q}_p/\mathbb{Z}_p}$ has a kernel.

In (arithmetic) algebraic geometry, 'p-divisible' has a more specific meaning. These are also called Barsotti-Tate groups.
Grothendieck, Groupes de Borsotti-Tate et eristaux de Dreudonné (1974)
Messing, The crystal associated to Borsotti-Tate groups
Berthelot-Breen-Messing
Demazure-Gabriel
Zink's Display Theory

2.2.1 Definitions

Let R be a ring, $h \in \mathbb{Z}_{\geq 0}$. A $\underline{p\text{-divisible group over } R \text{ of height } h}$ is an inductive system $G = (G_\nu, i_\nu : G_\nu \to G_{\nu+1})_{\nu \geq 0}$ where:

- G_ν is a finite loc. free comm. group scheme of order $p^{\nu h}$ over R.
- for each $\nu \geq 0$ the sequence:

$$0 \to G_\nu \xrightarrow{i_\nu} G_{\nu+1} \xrightarrow{[p^\nu]_{G_{\nu+1}}} G_{\nu+1}$$

  ie exact. $i_\nu : G_\nu \to G_{\nu+1}$ is the categorical kernel of $[p^\nu] : G_{\nu+1} \to G_{\nu+1}$.

  We have the following commutative diagram:

$$\begin{tikzcd} 0 \arrow[r] & G_\nu \arrow[r, "i_\nu"] & G_{\nu+1} \arrow[r, "{[p^\nu]_{G_{\nu+1}}}"] & G_{\nu+1} \\ & & H \arrow[u, "\varphi"] \arrow[ul, dotted, "\exists!"] \arrow[r, "p_H"] & \mathrm{Spec}(R) \arrow[u, "e_{G_{\nu+1}}"'] \end{tikzcd}$$

If G_ν would be ordinary abelian groups then G_ν would have order $p^{\nu h}$ and it would be annihilated by p^ν.
Thus, $G_1 \cong (\mathbb{Z}/p)^h$ and $G_\nu \cong \bigoplus_{i=1}^s \mathbb{Z}/p^{m_i}$ and $\sum_{i=1}^s m_i = \nu h$.
Thus, $G_\nu[p] = \bigoplus_{i=1}^s p^{m_i - 1}\mathbb{Z}/p^m\mathbb{Z} \implies s = h \implies \forall i, m_i = \nu$.
Upshot: $G_\nu = (\mathbb{Z}/p^\nu)^h$.

Thursday, 3/6/2025

If the G_ν would be just finite abelia= n groups $\implies G_\nu = (\mathbb{Z}/p^\nu)^h \implies G = (\mathbb{Q}_p/\mathbb{Z}_p)^h$.
Examples of more p-divisible groups:

1) $(\underline{(\mathbb{Z}/p^\nu)^h}_R)_\nu = \left(\underline{\left(\frac{1}{p^\nu}\mathbb{Z}/\mathbb{Z}\right)}_R\right)_\nu$ is the constant p-divisible group of ht h over R.
2) $(\underline{\mu}^{\oplus h}_{p^\nu, R})_\nu$ is a p-divisible group over R of ht h.

   Question: Are there any other p-divisible groups over $\mathbb{Z}$ other than $\underline{(\mathbb{Q}_p/\mathbb{Z}_p)^h}_{\mathbb{Z}}$ or $\underline{\mu}^{\oplus h}_{p^\infty, \mathbb{Z}}$?

   We don't know the answer.

   See Fontaine (1980's) Ji n'ya pas de courbes elliptiques sur $\mathbb{Z}$
3) F = LT Formal $\mathcal{O}_K$-module, $[K : \mathbb{Q}_p] < \infty, |k_K| = q = p^f$ then $(F[p^\nu])_{\nu \geq 0}$ is a p-divisible over $\mathcal{O}_K$ of height $h = [K : \mathbb{Q}_p]$.

   Question: $F[p^\nu] \underset{?}{\cong} (\underline{\mu}_{p^\nu, \mathcal{O}_K})^{\oplus h}, h = [K : \mathbb{Q}_p]$? Answer is no if $h > 1$.

   Lubin-Tate Theory provides us with p-divisible groups that are not obvious!

A homomorphism of p-divisible groups $f : G = (G_\nu) \to H = (H_\nu)$ is a system of morphisms of group schemes $f_\nu : G_\nu \to H_\nu$ which are compatible with the transition maps:

$$\begin{tikzcd}
G_\nu \arrow[r, "f_\nu"] \arrow[d] & H_\nu \arrow[d] \\
G_{\nu+1} \arrow[r, "f_{\nu+1}"] & H_{\nu+1}
\end{tikzcd}$$

For $\nu, \mu \geq 0$ let $i_{\nu,\mu} : G_\nu \xrightarrow{i_\nu} G_{\nu+1} \xrightarrow{i_{\nu+1}} \cdots \to G_{\nu+\mu}$ be the composition of i_j where $\nu \leq j \leq \nu + \mu$.
Then, we have $G_\nu \xrightarrow{i_{\nu,\mu}} G_{\nu+\mu} = \ker\left([p^\nu] : G_{\nu+\mu} \to G_{\nu+\mu}\right)$
$\implies [p^\nu] : G_{\nu+\mu} \to G_{\nu+\mu}$ has the property that $[p^\nu] \circ [p^\mu] = 0$. Indeed,

$$\begin{tikzcd}
{[p^\nu]} & : & G_{\nu+\mu} \arrow[r] \arrow[d, "j_{\mu,\nu}"', "\exists!"] & G_{\nu+\mu} \arrow[d, "{[p^\nu]}"] \\
& & G_\nu \arrow[ur, "i_{\nu,\mu}"] & G_{\nu+\mu}
\end{tikzcd}$$

Thus we have an exact sequence:

$$\begin{tikzcd}
& & & G_{\nu+\mu} & \\
0 \arrow[r] & G_\mu \arrow[r, "i_{\mu,\nu}"] & G_{\mu+\nu} \arrow[r, "j_{\mu,\nu}"] \arrow[ur, "{[p^\mu]}"] & G_\nu \arrow[r] \arrow[u, "i_{\nu,\mu}"'] & 0
\end{tikzcd}$$

eg $0 \to p^{-1}\mathbb{Z}/\mathbb{Z} \to p^{-2}\mathbb{Z}/\mathbb{Z} \xrightarrow{p} p^{-1}\mathbb{Z}/\mathbb{Z} \to 0$

2.2.2 Relations with Formal Lie Groups

R is assumed to be noetherian, local with maximal $\mathfrak{m}$, complete with residue field k of char $p > 0$.
An n-dimensional commutative formal Lie group F over R is given by:
$F(x,y) = (F_1(x,y), \cdots, F_n(x,y)) \in R[[x,y]]^n$
Here $R[[x,y]] = R[[x_1, \cdots, x_n, y_1, \cdots, y_n]]$
Satisfying,

i) $F(x,y) = F(y,x)$

ii) $F(0,y) = y = (y_1, \cdots, y_n)$

iii) $F(F(x,y),z) = F(x, F(y,z))$

We write $x \underset{F}{+} y = F(x,y)$ then we have $[p](x) = x \underset{F}{+} \cdots \underset{F}{+} x = ([p]_1(x), \cdots, [p]_n(x))$.
F is called p divisible if $[p](x)$ is an isogeny, i.e. the map $R[[x]] \to R[[x]]$ sending $x_i \to [p]_i(x), 1 \leq i \leq n$ turns $R[[x]]$ into a module over itself which is finitely generated and free.
Example: We look at dimension 1.

1) $F(x,y) = x + y \implies [p](x) = px$, then $R[[x]]$ is <u>not</u> a finite $R[[x]]$-module via $x \mapsto px$. Recall that k has char p so the $\mod \mathfrak{m}$ reduction of this map is $k[[x]] \to k[[x]]$ sending $x \mapsto 0$.

2) $F(x,y) = x + y + xy \implies [p](x) = (1+x)^p - 1 = px + \binom{p}{2}x^2 + \cdots + px^{p-1} + x^p$ which is regular of order p in the terminology given in the HW.

   HW7 $\implies R[[x]]$ a free $R[[x]]$-module of rank p.

3) If F is a Lubin-Tate $\mathcal{O}_K$ module, it is p-divisible when $K/\mathbb{Q}_p$ is finite.

If F is p-divisible, then not only multiplication by p is an isogeny, but iterations $[p^\nu]$ is an isogeny.
For any $\nu \geq 0, A_\nu := \frac{R[[x]]}{([p^\nu]_1(x), \cdots, [p^\nu]_n(x))R[[x]]}$ is finite free over R, and the power series $F(x,y)$ defines a co-multiplication $A_\nu \to A_\nu \otimes_R A_\nu$ given by $\overline{x_i} \mapsto F_i(x,y) \mod ([p^\nu]_j)_{j=1}^n$.

Then A_ν becomes a commutative and co-commutative Hopf-algebra $/R$ and thus $G_\nu = \mathrm{Spec}(A_\nu)$ is a finite free commutative group scheme $/R$.
Upshot: $G = (G_\nu, \underset{A_\nu}{G_\nu} \underset{\leftarrow}{\to} \underset{A_\nu+1}{G_{\nu+1}})$ is p-divisible over R and each A_ν is a local ring $\implies G_\nu$ is connected.
Proposition 2.2.2.1. Let R be a ccomplete noetherian local ring with residue field k of char $p > 0$. Then, $F \rightsquigarrow G_F$ is an equivalence of the categories of p-divisible formal Lie groups and category of connected p-divisible groups over R.

Remark. A p-divisible group $G = (G_\nu)$ is called <u>connected</u> if all (G_ν) are connected.

Example:

1) $F = \widehat{\mathbb{G}}_{m,R}$ (so $F(x,y) = x + y + xy \implies G_F = \underline{\mu}_{p^\infty,R}$)
2) F= LT $\mathcal{O}_K$-module, $[K : \mathbb{Q}_p] < \infty \implies G_F = (F[p^\nu])_\nu$.

Going from connected p-divisible groups to formal Lie Groups:
Given $G = (G_\nu, i_\nu)$ where $G_\nu = \mathrm{Spec}(A_\nu)$ connected p-divisible group over R and i_ν corresponds to morphisms of Hopf algebras $A_{\nu+1} \to A_\nu$.
Theorem. $A := \varprojlim_\nu A_\nu$ is isomorphic to $R[[x_1, \cdots, x_n]]$ and the co-multiplications $A_\nu \to A_\nu \otimes A_\nu$ give a ring homomorphism:
$A \to \varprojlim_\nu A_\nu \otimes A_\nu \cong R[[x_1, \cdots, x_n, y_1, \cdots, y_n]] (\cong A \widehat{\otimes}_R A)$.
Complete w.r.t. the ideal $\mathfrak{m} \otimes A + A \otimes \mathfrak{m}$.

Proof. Sending x_i to $F_i(x,y)$ and $F(x,y) = (F_1(x,y), \cdots, F_n(x,y))$ is a formal lie group over R as define dbefore.

□

Proposition - Definition. Given a p-divisible group $G = (G_\nu)_\nu$ over R, the systems $G^0 = (G^0_\nu)_\nu$ and $G^{\text{ét}} = n(G^{\text{ét}}_\nu)_\nu$ are p-divisible groups. One has $\mathrm{ht}(G) = \mathrm{ht}(G^0) = \mathrm{ht}(G^{\text{ét}})$. If F is the formal lie group associated to G^0 by proposition 2.2.2.1 then we set $\dim(G) := \dim(G^0) := \dim(F)$.
Example:

1) $\dim(\underline{\mu}_{p^\infty,R}) = 1$ recall that $\underline{\mu}_{p^\infty,R} \leftrightarrow \widehat{\mathbb{G}_m}$
2) $\dim(\underline{\mathbb{Q}_p/\mathbb{Z}_p}_R) = 0$
3) $\mathscr{E}/R$ elliptic curve, $\mathscr{E}[p^\infty] = (\mathscr{E}[p^\nu])_\nu \rightsquigarrow 0 \to \mathscr{E}[p^\infty]^0 \to \mathscr{E}[p^\infty] \implies \mathscr{E}[p^\infty]^{\text{ét}} \to 0$

Either $\mathscr{E}[p^\infty]^{\text{ét}} = 0 \implies \dim(\mathscr{E}[p^\infty]) = 1$ and $\mathrm{ht}(\mathscr{E}[p^\infty]^0) = \mathrm{ht}(\mathscr{E}[p^\infty]) = 2$ supersingular case.
Ordinary: $\mathscr{E}[p^\infty]^{\text{ét}} \neq 0 \implies \mathrm{ht}(\mathscr{E}[p^\infty]^{\text{ét}}) = 1$ and $\mathrm{ht}(\mathscr{E}[p^\infty]^0) = 1$
$\dim(\mathscr{E}[p^\infty]^{\text{ét}}) = 0$ and $\dim(\mathscr{E}[p^\infty]^0) = 1$
In general $\mathrm{ht}(\mathscr{A}[p^\infty]^0) \in [g, \cdots, 2g]$. Everything can be achieved inbetween. $2g$ is the supersingular case, which is extreme in the sense that the étale part is 0.

$$\dim\left(\underbrace{\mathscr{E}^a_{\text{ord}} \times \mathscr{E}^b_{\text{supersing}}}_{\text{connected part}}\right) = a + b$$

$= (\mathscr{E}^0_{\text{ord}})^a \times \mathscr{E}^b_{\text{super}}$
So, $\mathrm{ht}(\mathscr{E}[p^\infty]^0) = a + 2b$.
This shows we can achieve any number between g and $2g$.

Tuesday, 3/11/2025

The Discriminant

Let R be any ring, and A a commutative R-algebra which is f.g. and free as R-module. Then we have the trace map $\mathrm{Tr} = \mathrm{Tr}_{A/R} : A \to R$ defined as,
$\mathrm{Tr}(a) = \mathrm{trace}(\text{mult. by } a : A \to A)$ choose basis $\rightsquigarrow$ matrix $X_a \in M_n(R), n = \mathrm{rank}_R A = \mathrm{tr}(X_a)$.
The trace form of A/R is the R-bilinear map $A \times A \xrightarrow{b=b_{A/R}} R, b_{A/R}(a, a') = \mathrm{Tr}(aa')$.

Definition (Discriminant)**.** 1) The discriminant of A/R, called $\mathrm{disc}(A/R)$, is the discriminant of the trace form, which is the ideal generated by the discriminant of any basis $(e_1, \cdots, e_n)$ of A as an R-module. The latter is defined to be:

$$\det\left((b_{A/R}(e_i, e_j))_{1\le i,j\le n}\right) = \det 0\left((\mathrm{Tr}_{A/R}(e_i e_j))_{1\le i,j\le n}\right)$$

This ideal is independent of the choice of a basis.

2) If $G = \mathrm{Spec}(A)$ is a finite group scheme over R with a free R-module, we set $\mathrm{disc}(G) := \mathrm{disc}(A/R) \subset R$.

Examples:

1) Suppose $G = \underline{\mu}_{p,R} = \mathrm{Spec}\left(R[x]/(x^p - 1)\right), e_i = x^i, 0 \le i \le p-1$, then $e_i e_j = \overline{x}^{i+j} = \overline{x}^{i+j \mod p}$.

   Then, $\mathrm{Tr}_{A/R}(\overline{x}^0) = \mathrm{Tr}_{A/R}(1) = p, \mathrm{Tr}_{A/R}(\overline{x}^{\neq 0}) = 0$.

   Thus, if $i + j \equiv 0 \mod p, \mathrm{Tr}_{A/R}(e_i e_j) = p$, otherwise 0. Then, the discriminant is generated by (example: $p = 5$)

$$\begin{bmatrix} p & & & & \\ & & & & p \\ & & & p & \\ & & p & & \\ & p & & & \end{bmatrix}$$

   Therefore, $\mathrm{disc}\left(\underline{\mu}_{p,R}\right) = p^p \cdot R$.

2) If G is étale then $\mathrm{disc}(G) = 1 \cdot R$.

Proposition 2.2.2.2. If $G = (G_\nu)_\nu$ is a p-divisible group over R, R complete local noetherian of height h and dimension n, then $\mathrm{disc}(G_\nu) = p^{n\nu p^{h\nu}} \cdot R$.
Proof is involved.

2.2.3 Duality for p-divisible groups

Let $G = (G_\nu)_\nu$ be a p-divisible group over R, R not necessarily local.
Then we have an exact sequence:

$$0 \longrightarrow G_1 \longrightarrow G_{\nu+1} \xrightarrow[j_{1,\nu}]{[p]} G_\nu \longrightarrow 0$$

Applying Cartier Duality we get:

$$0 \longrightarrow G_\nu^\vee \xrightarrow[j_{1,\nu}^\vee]{} G_{\nu+1}^\vee \longrightarrow G_1^\vee \longrightarrow 0$$

Check: $(G_\nu^\vee, j_{1,\nu}^\vee)$ form a p-divisible group over R, called the Cartier dual of G.
Note: Since $\mathrm{ord}(G_\nu^\vee) = \mathrm{ord}(G_\nu) = p^{\nu h}, h = \mathrm{ht}(G)$ hence $\mathrm{ht}(G^\vee) = \mathrm{ht}(G)$.
Standard Example: $\left(\underline{\mu}_{p^\infty,R}\right)^\vee = \left(\left(\underline{\mu}_{p^\nu,R}\right)^\vee\right)_\nu = \left(\frac{1}{p^\nu}\mathbb{Z}/\mathbb{Z}\right)_\nu = \underline{\mathbb{Q}_p/\mathbb{Z}_p}_R$

Proposition 2.2.3.1. Suppose R is a complete local noetherian ring with residue vield k of char p. Then, $\dim(G) + \dim(G^\vee) = \mathrm{ht}(G)$.
Example: Let $[K : \mathbb{Q}_p] = d, F = \mathrm{LT}\ \mathcal{O}_K$ module, then we know $F[p^\infty] = (F[p^\nu])_\nu$ has height d and dimension 1.
Then, 2.2.3.1 $\implies \dim\left(F[p^\infty]^\vee\right) = d - 1$

2.3 Frobenius and Verschiebung

Let k be a field of char $p > 0$. (This should also work for any $\mathbb{F}_p$ algebra).
Let $\varphi : k \to k, \lambda \mapsto \lambda^p$ be the (absolute) Frobenius.
If $G = \mathrm{Spec}(A)$ is a group scheme $/k$ then we can form $A^{(p)} = k \otimes_{\varphi,k} A$ which we consider as a k-algebra via the left $\otimes$-factor and $G^{(p)} := \mathrm{Spec}(A^{(p)}) = \mathrm{Spec}(k) \times_{\varphi^a,\mathrm{Spec}(k)}$ $\mathrm{Spec}(A) = \mathrm{Spec}(k) \times_{\varphi 6a,\mathrm{Spec}(k)} G$
Which is again a group scheme over k via

$$pr_1 : G^{(p)} = \mathrm{Spec}(k) \times_{\varphi^a,\mathrm{Spec}(k)} G \to \mathrm{Spec}(k)$$

The morphism of k-algebras $A^{(p)} = k \otimes_{\varphi,k} A \xrightarrow{F_G^\#} A$
$\lambda \otimes a \mapsto \lambda a^p$ is well defined:
$\lambda \otimes \mu a \mapsto \lambda \mu^p a^p$
$= \lambda\mu^p. \otimes a \mapsto \lambda\mu^p a^p$
and is a morphism of Hopf algebras over k (check) and corresponds to a morphism $F_G : G \to G^{(p)}$ of group schemes over k, called the Frobenius of G.
Question: How do we think about $A^{(p)}$?
We write $A = k[x_1, \cdots, x_n]/(f_1, \cdots, f_r)$.
Then, Claim: $k \otimes_{\varphi,k} A \xrightarrow{\cong} k[x]/(f_1^\varphi, \cdots, f_r^\varphi)$ where f^φ is the polynomial obtained from f by applying φ to all coefficients.
This map sends $\lambda \otimes x_1^{m_1} \cdots x_n^{m_n} \mapsto \lambda x_1^{m_1} \cdots x_n^{m_n}$.
Well defined: Using multi index: suppose $f_j(x) = \sum_m a_m x^m, a_m \in k \implies 1 \otimes f_j(x) = \sum_m a_m^p \otimes x^m \mapsto \sum_m a_m^p x^m = f_j^\varphi(x)$
Hence $G^{(p)} = \mathrm{Spec}(A^{(p)})$ is obtained by applying the Frobenius to the coefficients of the defining equations of G.
Question: How do we think of F_G? Again write $A = k[x]/(f_1, \cdots, f_r)$.

$$\begin{tikzcd}
A^{(p)} & = & k \underset{\varphi,k}{\otimes} A \arrow[rr, "\cong"] \arrow[dr, "\ni"] \arrow[dddd, "F_G^\#"'] & & \frac{k[x]}{(f_1^\varphi,\cdots,f_r^\varphi)} \arrow[dddd] & f_j^\varphi \arrow[dddd, mapsto] \\
\lambda \otimes a \arrow[d, mapsto] & & & 1 \otimes \overline{x}_i \arrow[r, mapsto] & \overline{x}_i & \\
\lambda \otimes a^p & & & 1 \otimes \overline{x}_i^p \arrow[r, mapsto] & \overline{x}_i^p & \\
& & & & & \\
& & A \arrow[rr, "id_A"] & & \frac{k[x]}{(f_1,\cdots,f_r)} & f_j^\varphi(x^p) = (f_j(x))^p
\end{tikzcd}$$

Example:

1) $G = \underline{\mu}_{n,k}$ [any n], $(\underline{\mu}_{n,k})^{(p)} = \mathrm{Spec}\left((k[x]/(x^n-1))^{(p)}\right) \cong \mathrm{Spec}\left(k[x]/(x^n-1)\right) = \underline{\mu_{n,k}}$

   $F_G : \underline{\mu}_{n,k} \to (\underline{\mu}_{n,k})^{(p)} = \underline{\mu}_{n,k}$ hence $F_{\underline{\mu}_{n,k}} = [p]_{\underline{\mu}_{n,k}}$ is multiplication by p, with $\overline{x}^p \mapsfrom \overline{x}$. This is multiplication by p. If $p \nmid n$ then F_G is invertible.

2) If G is finite étale then $F_G : G \to G^{(p)}$ is an isomorphism.

Verschiebung G/K finite group scheme, k field of char p or $\mathbb{F}_p$-algebra.
$F_{G^\vee} : G^\vee \to (G^\vee)^{(p)} \underset{can}{\cong} (G^{(p)})^\vee$ [check], dualize again and get:
$V_G : G^{(p)} \underset{can}{\cong} ((G^{(p)})^\vee)^\vee \to (G^\vee)^\vee = G$ which is a morphism of group schemes over k.
Proposition. $V_G \circ F_G = [p]_G, F_G \circ V_G = [p]_{G^{(p)}}$.

Thursday, 3/13/2025

Recall: Forbenius and Verschiebung: $R = k =$ field of char $p > 0$.
$G^{(p)} = G \underset{\mathrm{Spec}(k),\varphi^a}{\times} \mathrm{Spec}(k), \varphi : k \to k, \lambda \mapsto \lambda^p$.
$= \mathrm{Spec}(A^{(p)}), A^{(p)} = A \underset{k,\varphi}{\otimes} k$

$$\begin{tikzcd} G \arrow[rr] \arrow[dr] & & G^{(p)} \arrow[dl] \\ & \mathrm{Spec}(k) & \end{tikzcd}, \quad V_G = (F_{G^\vee})^\vee : ((G^\vee)^{(p)})^\vee \underset{\text{check}}{\cong} G^{(p)} \to (G^\vee)^\vee \cong G$$

Lemma: $F_G \circ V_G = [p]_{G^{(p)}}$ and $V_G \circ F_G = [p]_G$.
Sketch of Proof of 2.2.3.1. $[\dim(G)+\dim(G^\vee) = \mathrm{ht}(G)]$ Note: If $I \subset R$ is an ideal and $G \mod I = G \underset{\mathrm{Spec}\, R}{\times} \mathrm{Spec}(R/I)$, then $F_{G \mod I} = F_G \mod I \in (R/I)[[x_1, \cdots, x_n]] \implies \dim(G \mod I) = \dim G$ where $F_{G \mod I}$ and F_G are the associated formal groups.
Hence we may take $I = \mathfrak{m}_R \rightsquigarrow$ reduced to the statement for $R = k$ is a field of char p.
We have universal property:

$$\begin{tikzcd} G^{(p)} & \ker\left(G_1^{(p)} \xrightarrow{V_{G_1}} G_1\right) \arrow[l, hook'] & \\ & & G_1 \arrow[ull, "F_{G_1}"] \arrow[ul, dotted, "\text{`}F_{G_1}\text{'}"'] \end{tikzcd}$$

Previous lemma $\implies \exists$ exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \ker(F_{G_1}) \arrow[r] & G_1 \arrow[rr, "\text{`}F_{G_1}\text{'}"] \arrow[dr, "F_{G_1}"'] & & \ker(V_{G_1}) \arrow[r] \arrow[dl, "V_{G_1}"] & 0 \\ & & & G_1^{(p)} & & \end{tikzcd}$$

$V_{G_1} \circ F_{G_1} = [p]_{G_1}$.
Similarly,

$$0 \longrightarrow \ker(V_{G_1}) \longrightarrow G_1^{(p)} \xrightarrow{\text{`}V_{G_1}\text{'}} \ker(F_{G_1}) \longrightarrow 0$$

2.1.4 implies,

$$0 \longrightarrow G_1^0 \longrightarrow G_1 \longrightarrow G_1^{\text{ét}} \longrightarrow 0$$

$F_{G_1}^{\text{ét}}$ is an isomorphism (HW9) $\implies \ker(F_{G_1}) \hookrightarrow G_1^0 = \mathrm{Spec}\left(\frac{k[[x_1,\cdots,x_n]]}{([p]_1(x),\cdots,[p]_n(x))}\right)$
Explcit description $\implies \ker(F_{G_1}) = \mathrm{Spec}\left(\frac{k[[x_1,\cdots,x_n]]}{(x_1^p,\cdots,x_n^p)}\right)$
$\implies \mathrm{ord}(\ker(F_{G_1})) = p^n, \mathrm{ord}(G_1) = p^h \implies \mathrm{ord}(\ker(V_{G_1})) = p^{h-n}$.
One has: $\ker(V_{G_1})^\vee \cong \ker(F_{G_1^\vee})$.
Therefore, $\dim(G^\vee) = \log_p \mathrm{ord}(\ker(F_{G_1^\vee})) = \log_p(\mathrm{ord}(\ker(V_{G_1})^\vee)) =$
$\log_p(\mathrm{ord}(\ker(V_{G_1}))) = \log_p p^{h-n} = h - n$.

2.4 S-valued points and the Galois modules $\Phi(G)$ and $T(G)$

$(R, \mathfrak{m})$ = CDVR (complete discrete valuation ring) with uniformizer ϖ and residue field k of char $p > 0, K = \mathrm{Frac}(R), L =$ completion of a Galois extension inside $\overline{K} =$ fixed alg. closure $\implies L \subset \overline{K}^{\wedge}$.
$S = \mathcal{O}_L$ is a valuation ring, not necessarily noetherian, not necessarily PID.
Example:

1) $L = \widehat{K}^{nr} \implies S$ is noetherian and its maximal ideal is generated by ϖ.

2) $L =$ completion of $K(\mu_{p^\infty})$ if $\mathrm{char}(K) = 0 \implies L$ is not discretely valued, S is not PID.

3) $L = \overline{K}^{\wedge} \implies S$ is not a PID.

Definition. Let G be a p-divisible group over R.

$$G(S) := \varprojlim_i G(S/\varpi^i S)$$

where $G(S/\varpi^i) := \varinjlim_\nu G_\nu(S/\varpi^i)$

Caution: In general, $G(S) \neq \varinjlim_\nu G_\nu(S)$.

Note:
$$\begin{tikzcd} S/\varpi^{i+1} \arrow[rr] & & S/\varpi^i \\ & \mathcal{O}(G_\nu) \arrow[ul] \arrow[ur, dotted] & \end{tikzcd} \quad \rightsquigarrow G_\nu(S/\varpi^{i+1}) \to G_\nu(S/\varpi^i).$$

$G(S/\varpi^{i+1}) = \varinjlim_\nu G_\nu(S/\varpi^{i+1}) \to \varinjlim_\nu G_\nu(S/\varpi^i) = G(S/\varpi^i)$
These are the maps in this proj. system.
Example: $K/\mathbb{Q}_p$ finite, ϖ uniformizer of $K, G = \underline{\mu}_{p^\infty,R}, L = \overline{K}^{\wedge}(= \mathbb{C}_p)$.
$G_\nu(S/\varpi^i) = \mathrm{Hom}_{R\text{-alg}}\left(R[x]/(x^{p^\nu} - 1), S/\varpi^i\right) \supset \mu_{p^\nu}(L) = \mu_{p^\nu}(\overline{K})$.

$$\xrightarrow{\text{bij}} \left\{\zeta \in S/\varpi^i \mid \zeta^{p^\nu} = 1 \text{ in } S/\varpi^i\right\}$$

$\implies \zeta \equiv 1 \mod \mathfrak{m}_S$.
Claim: $\forall a \in \mathfrak{m}_S \forall i > 0 \exists \nu \geq 0 : 1 + a \mod \varpi^i S \in G_\nu(S/\varpi^i)$.

Proof. Choose $\nu \gg 0$ such that $\forall 1 \leq j \leq p^\nu, \binom{p^\nu}{j} a^j \in \varpi^i S$.
Reason: $\binom{p^\nu}{j} = \frac{p^\nu(p^\nu-1)\cdots(p^\nu-j+1)}{j!}$, so for $\nu \gg 0$ the numerator is highly divisible by p and thus ϖ.
Exercise: such ν exists.
Therefore, $1 + a \in G_\nu(S/\varpi^i)$. The claim is proved.
The claim implies, $\forall a \in \mathfrak{m}_S, 1 + a \mod \varpi^i \in G(S/\varpi^i) = \varinjlim_\nu G_\nu(S/\varpi^i)$ [we can think about the inductive limit as union].
This gives us a coherent system $\mod \varpi^i$ therefore we have,

$$1 + a \in \varprojlim_i G(S/\varpi^i) = G(S)$$

<u>Conclusion</u>: $\exists\,\mathrm{Aut}(L/K) = \mathscr{G}_K$-equivariant isomorphism of groups $\underline{\mu}_{p^\infty,R}(S) \xrightarrow{\sim} (\mathfrak{m}_S, \underset{\widehat{\mathbb{G}}_m}{+})$ where $S = \mathcal{O}_L = \mathcal{O}_{\mathbb{C}_p}$. The map is $\zeta \mapsto \zeta - 1 \in \mathfrak{m}_S$.
Also, multiplication $\leftrightarrow a \underset{\widehat{\mathbb{G}}_m}{+} b = a + b + ab$.
This has more points than we would naively expect.
Upshot: $G(S)$ may not be a torsion group. In $\widehat{\mathbb{G}}_m$ note that $[p^m](a) = (1 + a)^{p^m} - 1$.
$1 + a$ is not necessarily a root of unity!
Similarly, $G(S)$ might not be equal to $\varinjlim G_\nu(S)$.
In fact, the p^ν torsion points $G(S)[p^\nu] = \varprojlim_i (G(S/\varpi^i)[p^\nu])$.
We have the exact sequence:

$$0 \longrightarrow G_\nu \longrightarrow G_{\nu+\mu} \xrightarrow{[p^\nu]} G_\nu \longrightarrow 0$$

This induces,

$$0 \longrightarrow G_\nu(S/\varpi \qquad i) \longrightarrow G_{\nu+\mu}(S/\varpi^i) \xrightarrow{[p^\nu]} G_\nu(S/\varpi^i) \longrightarrow 0$$

Therefore, $G_{\nu+\mu}(S/\varpi^i)[p^\nu] = G_\nu(S/\varpi^i)$
Note that $G(S)[p^\nu] = \varprojlim_i (G(S/\varpi^i)[p^\nu]) = \varprojlim_i G_\nu(S/\varpi^i)$.
Thus, $G(S/\varpi^i)[p^\nu] = \varprojlim_\mu G_\mu(S/\varpi^i)[p^\nu] = G_\nu(S/\varpi^i)$
$= \varprojlim_i \operatorname{Hom}_{R\text{-alg}}(\mathcal{O}(G_\nu), S/\varpi^i) \hookrightarrow \operatorname{Hom}_{R\text{-alg}}(\mathcal{O}(G_\nu), \varprojlim_i S/\varpi^i)$
$= \operatorname{Hom}_{R\text{-alg}}(\mathcal{O}(G_\nu), S) = G_\nu(S)$
This inclusion is bijective because $\mathcal{O}(G_\nu)$ is a f.g. S-algebra.
Caution: $\operatorname{Hom}^{\text{cont}}_{R\text{-algs}}(R[[x]], S) \neq \operatorname{Hom}_{R\text{-algs}}(R[[x]], S)$ where S is given the usual valuation topology and $R[[x]]$ the topology defined by (ϖ, x).
Conclusion: $G(S)[p^\nu] = G_\nu(S)$ hence the torsion subgroup $G(S)_{\text{torsion}} = \varinjlim G_\nu(S)$.
Also, if G is étale then $G(S) = G(S)_{\text{torsion}}$ since the connected part of the group is trivial.
If G is connected and F is the corresponding formal group then,
$G(\mathcal{O}_{\overline{K}^\wedge}) \xrightarrow[\mathscr{G}_K]{\cong} \left(\mathfrak{m}^{\oplus n}_{\mathcal{O}_{\overline{K}^\wedge}}, \underset{F}{+}\right)$
$n = \dim G$. $\square$

$G(S)$ has all the information needed to define $\Phi(G) = \bigcup_\nu G_\nu(S), T(G) \varprojlim_\nu G_\nu(S)$. But these are nicer.
$T(G)$ is something like $\mathbb{Z}_p^h$.
$G(S)_{\text{torsion}} = \Phi(G)$ if $S = \mathcal{O}_{\mathbb{C}_p}$.

Tuesday, 3/25/2025

Recall" R is a CDVR, $k = R/\mathfrak{m}_R, K = \operatorname{Frac}(R), \operatorname{char}(k) = p$, we most often assume k is perfect. $\varpi =$ uniformizer of R.
$L =$ completion of a Galois extension of K inside $\overline{K}$.
$S =$ valuation ring of $L \supset \mathfrak{m}_S =$ maximal ideal of S.
Set $G(S) = \varprojlim_i G(S/\varpi^i), G(S/\varpi^i) = \varinjlim_\nu G_\nu(S/\varpi^i)$
For example, $G = \underline{\mu}_{p^\infty,R} \implies G(S) \cong 1 + \mathfrak{m}_S \supset \mu_{p^\infty}(\overline{K}) = G(S)_{\text{tors}}$. So $G(S)$ in this case contains more than the torsion points.
Proposition.

1) $G(S)[p^\nu] = G_\nu(S)$, hence $G(S)_{\text{tors}} = \varinjlim_\nu G_\nu(S)$.
2) G étale $\implies G(S) = G(S)_{\text{tors}}$.
3) If G is commutative with associated formal group $F = F(x_1, \cdots, x_n, y_1, \cdots, y_n)$ of $\dim n$, then $\exists \mathscr{G}_K (= \operatorname{Gal}(K^{\text{sep}}/K))$ equiv. isom. $G(S) \cong (\mathfrak{m}_S^{\oplus n}, \underset{F}{+})$. On $G(S)$ the identity element is 1, but in $\mathfrak{m}_S^{\oplus n}$ the identity element is $(0, \cdots, 0)$.
4) If $\dim(G^0) = n$ then $\exists \mathscr{G}_K$-equivariant exct sequence
$$0 \to (\mathfrak{m}_S^{\oplus n}, \underset{F}{+}) \to G(S) \to G^{\text{ét}}(S) \to 0$$
and $G^{\text{ét}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{h'}$ if $L = \widehat{\overline{K}}$ and $h' = \text{height}(G^{\text{ét}})$.

Proposition 2.2.4.1. If k is perfect then $G \to G^{\text{ét}}$ has a formal section in the sense that $\mathcal{O}(G_\nu) \cong \mathcal{O}(G_\nu^{\text{ét}}) \otimes_R \mathcal{O}(G_\nu^0)$ and these isom. can be chosen such that

$$\varprojlim \mathcal{O}(G_\nu) \cong (\varprojlim \mathcal{O}(G_\nu^{\text{ét}})) \widehat{\underset{R}{\otimes}} (\varprojlim \mathcal{O}(G_\nu^0))$$

$$\cong A^{\text{ét}} \underset{R}{\widehat{\otimes}} R[[x_1, \cdots, x_n]]$$

$$:= \varprojlim_i \left(A^{\text{ét}} \underset{R}{\otimes} R[[x_1, \cdots, x_n]]/(x_1, \cdots, x_n)^i \right)$$

The sequence

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

is exact.

Corollary 2.2.4.2. Assume k is perfect. $\forall x \in G(S) \exists$ finite extension L'/L and $y \in G(S)$ such that $x = [p](y)$.

Proof. (Sketch) Reduce to the case of a connected and an étale grup using 2.2.4.1. We check them individually.
Étale case: we only need to enlarge the residue field k. In other words, we replace L by an unramified extension (at most), simply because in this case $G_\nu^{\text{ét}} \underset{k}{\times} k$ over a finite Galois extension $k'/k \implies G_\nu^{\text{ét}} \underset{R}{\times} R'$ is constant for an unramified extension R'/R with residue field k'.
Connected case:

$$\begin{array}{ccccc} & & x_i & \longmapsto & [p]_i(x_1, \cdots, x_n) \\ \varprojlim_\nu \mathcal{O}(G_\nu) & \cong & R[[x_1, \cdots, x_n]] & \xrightarrow{[p]^\#} & R[[x_1, \cdots, x_n]] \\ & & \Big\downarrow{\scriptstyle x_i \mapsto a_i \in \mathfrak{m}_S} & & \Big\downarrow \\ & & S & \hookrightarrow & S' = \mathcal{O}_{L'} \end{array}$$

Here $R[[x_1, \cdots, x_n]] =$ finitely generated module over $R[[x_1, \cdots, x_n]]$, use the theory of integral extensions. $\square$

Corollary 2.2.4.3. If L is algebraically closed (eg $\text{char}(K) = 0, L = \widehat{\overline{K}}$) then $G(S)$ is divisible, ie $\forall n \in \mathbb{Z}_{>0}$, the multiplication-by-$n$ map on $G(S)$ is surjective.

Proof. If $p \nmid n$ then $[n]_{G_\nu} : G_\nu \to G_\nu$ is an isomorphism: choose m such that $m \cdot n \equiv 1(p^\nu)$ then $[n] : G(S) \implies G(S)$ is an isomorphism.
2.2.4.2 $\implies$ multiplication by p is surjective $\implies$ multiplication by p^m is surjective. $\square$

The logarithm From now on we assume $\text{char}(K) = 0$ and k is separable.

Definition. The tangent space t_G of G is defined to be the tangent space of the formal group F associated to G [which is the same as the formal group associated to G^0, the connected component].
If $A_\nu^0 = \mathcal{O}(G_\nu^0)$ and $A^0 := \varprojlim A_\nu^0 \cong R[[x_1, \cdots, x_n]] \supset U^0 := (x_1, \cdots, x_n) = \ker(\varepsilon : A^0 \to R)$. We have $\text{Spec}(R) \xrightarrow{e_{G_\nu^0}} G_\nu^0$. Corrrespondingly, we have $R \xleftarrow{\varepsilon_{G_\nu^0}} A_\nu^0$ and also the zero section $R \xleftarrow{\varepsilon} A^0$.
Choosing the coordinates is non-canonical!
Then, $t_G = \text{Hom}_R(I^0/(I^0)^2, R)$. This is sometimes called the Zariski tangent space.

Remark. 1) If A is any ring and $P \in \text{Spec}(A) =: X$ then the Zariski tangent space of X at P is defined to be $\text{Hom}_{k_P}(PA_P/(PA_P)^2, k_P)$ where $k_P = A_P/PA_P = \text{Frac}(A/P)$.

2) $\exists$ canonical isomorphism $t_G(L) \xrightarrow{\sim} \mathrm{Der}_R(A^0, L)$
$= \{\tau : A^0 \to L \mid \tau \text{ is } R\text{-linear}, \forall f, g \in A^0 : \tau(fg) = \varepsilon(f)\tau(g) + \varepsilon(g)\tau(f)\ \}$
$\implies \tau \in \mathrm{Der}_R(A^0, L)$ and $f, g \in I^0 \implies \tau(fg) = \underbrace{\varepsilon(f)}_{=0}\tau(g) + \underbrace{\varepsilon(g)}_{=0}\tau(f) = 0$
$\implies \tau\big|_{(I^0)^2} = 0.$
Also: $\tau(1) = \tau(1 \cdot 1) = 1 \cdot \tau(1) + \tau(1) \cdot 1 \implies 2\tau(1) = \tau(1) \implies \tau(1) = 0.$
$\implies \forall a \in R : \tau(a) = 0 \implies \tau$ is uniquely determined by its restriction to $I^0/(I^0)^2$.
Note that $I^0/(I^0)^2 = Rx_1 \oplus . \cdot \oplus Rx_n \cong R^{\oplus n}$.
$\implies \dim_L(t_G(L)) = \dim(F) = \dim(G)$.

Conclusion: Since $I^0/(I^0)^2 \cong R^{\oplus n} \implies \dim_L(t_G(L)) = \dim(F) = \dim(G)$
The Logarithm Map $\log = \log_G : G(S) \to t_G(L)$ is defined by:

$$\log\Big(\underset{\in S}{a}\Big)\big(\underset{\in A^0}{f}\big) := \lim_{i\to\infty} \frac{f([p^i]_G(a)) - f(0)}{p^i}$$

If $f = x_j$ then $f([p]^i(a)) \equiv [p^i]_j(\underset{=(a_1,\cdots,a_n)\in G^0(S)\cong \mathfrak{m}_S^{\oplus n}}{a}) = p^i(\text{linear term in } a_k) + p^{2i}$higher order terms
So the limit exists in this case.
Note:

1) For $a \in G^{\text{ét}}(S)$ one has $p^i a = 0$ for $i \gg 0$. Hence $p^i a \in G^0(S)$.
2) If G is étale then $t_G(L) = 0$ and log is the zeron map.
3) $G(S)$ is a $\mathbb{Z}_p$-module: if $n_j \in \mathbb{Z}$ converges p-adically to $n \in \mathbb{Z}_p$ then $\forall a \in G(S)$: $n_j \cdot a$ converges in $G(S) = \varprojlim G(\underbrace{S/\varpi^i}_{\text{equipped with discrete top}})$

Thursday, 3/27/2025

The Galois modules Φ and T

G is a p-div gp over R, R = CDVR of mixed char with perfect residue field k of char $p > 0, K = \mathrm{Frac}(R), \mathscr{G}_K = \mathrm{Gal}(\overline{K}/K)$.
CDVR of mixed characteristic means K and k have different characteristic.
$\Phi(G) = \varinjlim_\nu G_\nu(\overline{K})$ with transition map $G_\nu \xrightarrow{i_\nu} G_{\nu+1}$
$T(G) = \varprojlim_\nu G_\nu(\overline{K})$ with transition map j_ν such that:

$$\begin{tikzcd} G_{\nu+1} \arrow[r, "{[p]}"] \arrow[dr, "j_\nu"] & G_{\nu+1} \\ & G_\nu \arrow[u, hook, "i_\nu"'] \end{tikzcd}$$

Fact(HW 10): A finite group scheme over a field of char 0 is étale.
Consequence: $G_\nu(\overline{K}) = \underbrace{(G_\nu \otimes_K \overline{K})}_{\text{étale}}(\overline{K}) = \underbrace{(G \otimes_K \overline{K})}_{\text{const fin alg grp}/\overline{K}}(\overline{K}) \underset{\text{as abstract grp}}{\cong} (\mathbb{Z}/p^\nu)^h \cong (p^{-\nu}\mathbb{Z}/\mathbb{Z})^h \xrightarrow{p} (p^{-(\nu-1)}\mathbb{Z}/\mathbb{Z})^h$
$\implies$ as groups $\Phi(G) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^h$ and $T(G) \underset{\text{top.}}{\cong} \varprojlim_\nu \underbrace{(p^{-\nu}\mathbb{Z}/\mathbb{Z})^h}_{\text{trans map are given by mult by } p} = \mathbb{Z}_p^h$.
In $\varprojlim(\mathbb{Z}/p^n)$ trans. maps are $\mod p^{n-1}$.
Important: In this description, the Galois action has been neglected. But it is there by transport of structure.
Checkk: $\Phi(G) \underset{can}{\cong} T(G) \otimes_{\mathbb{Z}_p} (\mathbb{Q}_p/\mathbb{Z}_p)$, $T(G) \underset{can}{\cong} \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Phi(G))$

$x_n \leftarrow\!\shortmid (\underset{\in G_\nu(\overline{K})}{x_\nu})_\nu \otimes \frac{1}{p^n}, (x_\nu)_\nu \mapsto \left[\frac{1}{p^n} + \mathbb{Z}_p \mapsto x_n\right]$
$T(G) \otimes_{\mathbb{Z}} \mathbb{Z}/p^n = T(G)/p^nT(G) \cong G_n(\overline{K})$
These isomorphisms are obviously $\mathscr{G}_K$-equivariant!
Moreover: $G(\mathcal{O}_{\overline{K}})_{\text{tors}} = \Phi(G)$
$\left(\cong \varprojlim_i G(\mathcal{O}_{\overline{K}}/p^i)\right)$

Tate

Section 1: Introduction
Section 2: Group scheme preliminaries
Section 3: Number theoretic preliminaries

2.5 2.3 The completion of the algebraic closure of K

$R =$ CDVR of mixed char with perfect residue field k of char $p > 0, K = \text{Frac}(R), \pi =$ uniformizer of $K, p \cdot R = p^e R, e =$ absolute ram. index of K over $\mathbb{Q}_p$.
$v = v_K : K^\times \to \mathbb{Z}, v(\pi) = 1, v(p) = e$. Extend to $\overline{K}$ and $C := \widehat{\overline{K}}, v : C^\times \to \mathbb{Q}$
Absolute value on $K : |x| = |\pi|^{v(x)}$. Similarly, $\forall x \in C, |x| = |\pi|^{v(x)}$
Recall: if M/L is a finite extension of cdvfs (complete discretely valued field) we have the codifferent:

$$D_{M/L}^{-1} = \left\{a \in M \mid \forall b \in \mathcal{O}_M : \text{Tr}_{M/L}(ab) \in \mathcal{O}_L\right\} \supset \mathcal{O}_M$$

$D_{M/L}^{-1}$ is a fractional ideal: it is nonzero and finitely generated.
We have the different: $D_{M/L} = (D_{M/K}^{-1})^{-1}$ generated by a^{-1} if $D_{M/L}^{-1} = a\mathcal{O}_M$ as $\mathcal{O}_M$-module.
Suppose L/K finite.
Given a fractional ideal $I \subset \mathcal{O}_L$ we set $v(I) = v_K(a), a \in L^\times, I = a \cdot \mathcal{O}_L$.
Recall HW4 1vi: if v_L is the normalized valuation attached to L we have:

$$v_L(D_{L/K}) = \sum_{i=0}^{\infty}(|G(L/K)_i| - 1)$$

If L/K is totally ramified, hence $[L : K] = e(L/K) = |G(L/K)_0|$ and $G(L/K)_0 = G(L/K) = G(L/K)_{-1}$
$\implies v_K(D_{L/K}) = \frac{1}{|G(L/K)_0|}\sum_{i=0}^{\infty}(|G(L/K)_i| - 1)$

$$= \sum_i^{\infty}\left(\frac{1}{[G(L/K)_0 : G(L/K)_i]} - \frac{1}{[L : K]}\right)$$

2.3.1. Study of certain totally ramified extensions:
Let K_∞/K be an infinite Galois extension of K which is totally ramified with $\mathscr{C} :=$ $\text{Gal}(K_\infty/K)$ isomorphic to $\mathbb{Z}_p$ as a profinite group.
Hence $\mathscr{C}$ has a unique closed subgroup of index p^n for any $n \geq 0$ and any finite indexed closed subgroup $\mathscr{C}(n)$ of index p^n of $\mathscr{C}$ and any finite index closed subgroup of $\mathscr{C}$ is one of $\mathscr{C}(n)$. Set $K_n = K_\infty^{\mathscr{C}(n)}$. Set $K_n = K_\infty^{\mathscr{C}(n)}$. Then K_n/K is Galois and $G(K_n/K) \cong \mathscr{C}/\mathscr{C}(n) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/(p^n)$.
Proposition 2.3.1.1. $\exists c \in \mathbb{Q}\exists$ bounded sequence $(a_n)_n$ in $\mathbb{Q}$ such that:

$$v_k(D_{K_n/K}) = e \cdot n + c + p^{-n}a_n$$

e being the absolute ramification index of K over $\mathbb{Q}_p, p \cdot R = \pi^e \cdot R$.
$\underset{e(K_n/K)=p^n}{\iff} V_{K_n}(D_{K_n/K}) = e \cdot p^n \cdot n + cp^n + a_n$

Tuesday, 4/1/2025

For simplicity let $K = \mathbb{Q}_p(\mu_p) \implies K_n = \mathbb{Q}_p(\mu_{p^{n+1}})$. Then $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n$.
In fact, $\mathrm{Gal}(K_n/K) = (1+p\mathbb{Z}_p)/(1+p^{n+1}\mathbb{Z}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$. [$p$ odd].
$G(K_n/K)_i \cong p^{m-1}\mathbb{Z}/p^n\mathbb{Z}, p^{m-1} \leq i < p^m$ [follows from $G(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}_p)_i$].
$\implies v_{K_n}(D_{K_n/K}) \overset{HW1}{=} \sum_{i=0}^{\infty}(|G(K_n/K)_i|-1) = p^n - 1 + \sum_{m=1}^{n}(p^m - p^{m-1})(p^{n-m+1} - 1) = (p-1)np^n$
Normalized means we have to divide by the ramification index. The ramification index in this case is equal to the degree p^n so:

$$v_K(D_{K_n/K}) = \frac{1}{p^n} v_{K_n}(D_{K_n/K}) = (p-1)n = e(K/\mathbb{Q}_p)n$$

Reminder: Herbrand function and upper ramification filtration
Let L/K be any finite Galois etension of local fields with $G = G(L/K)$, $G_x \coloneqq G_{\lceil x \rceil}, x \geq -1$
Herbrand function $\varphi_{L/K} : [-1,\infty) \to [-1,\infty)$

$$\varphi_{L/K}(s) = \int_0^s \frac{\mathrm{d}x}{[G_0 : G_x]}$$

This is a bijection.
We define $\psi_{L/K} \coloneqq \varphi_{L/K}^{-1}$.
The <u>upper ramification numbering</u> is a restatement: $G^t \coloneqq G_{\psi_{L/K}(t)}$.

Theorem 2.5.1 (Herbrand)**.** If $L \supset M \supset K$ and M/K is Galois, then,

$$G(M/K)^t = \mathrm{im}(G(L/K)^t \hookrightarrow G(L/K) \twoheadrightarrow G(M/K))$$

$$\equiv G(L/K)^t G(L/M)/G(L/M)$$

Theorem 2.5.2 (Hasse-Arf)**.** If L/K is abelian and $n \in [-1,\infty)$ is a break of the upper ramification filtration $[G(L/K)^t < G(L/K)^n \forall t > n]$ then n$\in \mathbb{Z}_{\geq 1}$.

Upper filtration of: $\begin{matrix} \mathscr{G}_K^t \\ \mathscr{A}_K^t \end{matrix}$

Proposition 2.5.3. L/K finite Galois and $\overline{L}/\overline{K}$ separable (hence is Galois). Then,

$$v_K(D_{L/K}) = \int_0^\infty \left(1 - \frac{1}{|G(L/K)^t|}\right) \mathrm{d}t$$

Proof. Set $G = G(L/K), \varphi = \varphi_{L/K}, \psi = \psi_{L/K}$. HW4 $\implies v_L(D_{L/K}) = \sum_{i=0}^{\infty}(|G_i| - 1)$.
$G_0 = \ker(G \to \mathrm{Aut}(\overline{L}/\overline{K})), ef = n \implies |G_0| = e(L/K)$
$\implies v_k(D_{L/K}) = \frac{1}{e(L/K)} v_L(D_{L/K}) = \sum_{i=0}^{\infty}\left(\frac{|G_i|}{|G_0|} - \frac{1}{|G_0|}\right) = \int_0^\infty \left(\frac{1}{[G_0, G_x]} - \frac{1}{|G_0|}\right) \mathrm{d}x$
Set $x = \psi(t) \implies \mathrm{d}x = \psi'(t)\mathrm{d}t, (\varphi \circ \psi)(t) \implies \varphi'(\psi(t))\psi'(t) = 1 \implies \psi'(t) = \frac{1}{\varphi'(\psi(t))}$
$= [G_0 : G_\psi(t)] = v_K(D_{L/K}) = \int_0^\infty \left(\frac{1}{\cancel{[G_0 : G_{\psi(t)}]}} - \frac{1}{|G_0|}\right) \cancel{[G_0 : G_{\psi(t)}]}\,\mathrm{d}t$

$$= \int_0^\infty \left(1 - \frac{1}{|G_{\psi(t)}|}\right) \mathrm{d}t = \int_0^\infty \left(1 - \frac{1}{|G^t|}\right) \mathrm{d}t$$

□

Let $K_\infty = \bigcup_{n \geq 0} K_n$ be as in the beginning of 2.3.1. $\mathscr{C}_n = G(K_n/K)$
$\mathscr{C}(i) \coloneqq G(K/K_i) = p^i e (\cong p^i e)$ which is unique closed subgroup of index p^i of $\mathscr{C}$.

Lemma 2.5.4. Let $v_{-1} \coloneqq -1 < v_0 < v_1 < \therefore$ be the sequence of breaks (ncessarily integers by Hasse-Arf) of $(\mathscr{C}^t)_{t \geq -1}$ so that $\forall i \geq 0 : \mathscr{C}^t = \mathscr{C}(i)$ for $v_{i-1} < t < v_i$.
Then there is $i_0 \in \mathbb{Z}_{\geq 0}$ such that $\forall i > i_0 : v_i = e + v_{i-1}$. Hence $v_i = (i - i_0)e + v_{i_0}$ for all $i > i_0$

Sketch. Assume K is locally compact, hence $K/\mathbb{Q}_p$ is finite. Write $\mathscr{A} = G(K^{ab}/K)$ which is $\cong \widehat{K^\times}$ the profinite completion and $\mathscr{A}^0 = \varprojlim G(L/K)^0, L/K$ finite abelian. $= \varprojlim_{L/K \text{ finite abelian}} G(L/K)_0 \overset{LCFT}{=} U(K) = \mathcal{O}_K^\times$. Also, LCFT tells us $\mathscr{A}^t \cong U^t(K) = 1 + \pi^t\mathcal{O}_K$ when $t \in \mathbb{Z}_{\geq 0}, U^0(K) = U(K)$.
Easy: $\exists t_0 \in \mathbb{Z}_{>0} \forall t \in [t_0, \infty) \cap \mathbb{Z} : \mathscr{A}^t \xrightarrow[\log]{\cong} \pi^t\mathcal{O}_K$ [is even on an isometry of $\mathbb{Z}_p$-modules.]
Choose i_0 minimal such that $v_{i_0} \geq t_0$
$\implies \mathscr{C}(i_0+1) = p^{0^{i+1}}\mathscr{C} = p\mathscr{C}(i_0) = p\mathscr{C}^{v_{i_0}} = p\,\mathrm{res}(\mathscr{A}^{v_{i_0}})$.
$= \mathrm{res}((\mathscr{A}^{v_{i_0}})^p)$ the subgroup of p'th powers / p-multiples.
$\cong \mathrm{res}(\mathscr{A}^{v_{i_0}+e})$
So we need:
$p\pi^t\mathcal{O}_K = \pi^e\pi^T\mathcal{O}_K = \pi^{e+t}\mathcal{O}_K$
It follows by definition: $v_{i_0+1} \leq v_{I_0} = e$.
Need to show: $v_{i_0+1} = v_{i_0} + e$. Repeat the argument with any $i > i_0$.

□

Sketch of 2.3.1.1. Let $\mathscr{C}_n = G(K_n/K)$.

$$v_K(D_{K_n/K}) \xrightarrow[\text{prop}]{\text{prev}}= \int_0^\infty \left(1 - \frac{1}{|\mathscr{C}_n^t|}\right) \mathrm{d}t$$

and $\mathscr{C}_n^t = \mathscr{C}^t\mathscr{C}(n)/\mathscr{C}(n) = \mathscr{C}(i)/\mathscr{C}(n)$ for $0 \leq i \leq n, v_{i-1} < t \leq v_i$.
Note: $\mathscr{C}(i)/\mathscr{C}(n)$ has order p^{n-i}.

$$= \int_0^{v_{i_0}} (\cdots)\ \mathrm{d}t + \sum_{i=i_0+1}^{n-1} \int_{v_{i-1}}^{v_i} \left(1 - \frac{1}{|\mathscr{C}_n^t|}\right) \mathrm{d}t$$

$$= \underbrace{\int_0^{v_{i_0}} (\cdots)\ \mathrm{d}t}_{=c' + \frac{b_n}{p^n}} + \underbrace{e \cdot \sum_{i=i_0+1}^{n-1} \left(1 - \frac{p^i}{p^n}\right)}_{n + c'' + \frac{a_n}{p^n}} = en + c + \frac{a_n}{p^n}$$

□

Thursday, 4/3/2025

<u>Lemma</u>: Let $v_{-1} \coloneqq -1 < 0 \leq v_0 < v_1 < \cdots$ be the breaks of the upper ramification filtration $(\mathscr{C}^t)_{t\geq 1}$ so that $\mathscr{C}^t = \mathscr{C}(i) = p^i\mathscr{C}$ for $v_{i-1} < t \leq v_i$ for all $i \geq 0$. Recall that $\mathscr{C} \cong \mathbb{Z}_p$.
Then $\exists i_0 \in \mathbb{Z}_{\geq 0}$ such that $\forall i \geq i_0 : v_i = e(i - i_0) + v_{i_0}$.
Complement to the proof of the Lemma: we had seen: $\forall i \geq i_0$,

$$\mathscr{C}^{v_i+e} = p\mathscr{C}^{v_i}$$

This implies $v_{i+1} \geq v_i + e$.
$\mathscr{C}^{v_i+1} = p\mathscr{C}^{v_i}$ since v_i is a break.
$v_i + e$ is a break so $v_{i+1} = v_i + e$ if $\mathscr{C}^{v_i+e+1} = p\mathscr{C}^{v_i+e}$. But this is true. Namely, since v_i is a break, $\mathscr{C}^{v_i+1} = p\mathscr{C}^{v_i}$
Therefore, $\mathscr{C}^{v_i+e+1} = \mathrm{res}(\mathscr{A}^{v_i+e+1}) = \mathrm{res}(U^{v_i+e+1}(K))$ where $\mathscr{A}$ denotes the maximal abelian extension.
$= \mathrm{res}(1 + \pi^{v_i+e_i+1}\mathcal{O}_K) = \mathrm{res}(1 + p\pi^{v_i+1}\mathcal{O}_K) = \mathrm{res}((1 + \pi^{v_i+1}\mathcal{O}_K)^p)$
$= \mathrm{res}((\mathscr{A}^{v_i+1})^p) = p\,\mathrm{res}(\mathscr{A}^{v_i+1}) = p\mathscr{C}^{v_i+1} = pp\mathscr{C}^{v_i} = p\mathscr{C}^{v_i+e}$.
Thus, v_i is a break $\implies v_{i+1} = v_i + e$. This finishes the proof of the lemma.
Proposition 2.3.1.1. $v_K(D_{K_n/K}) = en + c + \frac{a_n}{p^n}$ for some constant c and some bounded sequence a_n.

Proof. $v_K(D_{K_n/K}) = \int_0^\infty \left(1 - \frac{1}{|\mathscr{C}_n^t|}\right) \mathrm{d}t$ and use the lemma. □

Corollary 2.3.1.2. $\exists$ bounded sequence $(b_n)_n$ of real numbers b_n such that $\forall n \geq 0$:

$$v(D_{K_{n+1}/K_n}) = e + p^{-n} b_n$$

Proof. $v_{K_n}(D_{K_{n+1}/K_n}) = \int_0^\infty \left(1 - \frac{1}{|G(K_{n+1}/K_n)^t|}\right) \mathrm{d}t$. Now use the lemma and determine the unique break of $(G(K_{n+1}/K_n)^t)_{t\geq -1}$
Caution: the upper numbering of ramification groups is not compatible with passing to subgroups.
Alternatively, use that $D_{K_{n+1}/K} = D_{K_{n+1}/K_n} \cdot (D_{K_n/K}\mathcal{O}_{K_{n+1}})$.
cf Serre, Local Fields III, S4, Prop 8. $\square$

Corollary 2.3.1.3 $\exists$ constant $a \geq 0$ independent of n such that: $\forall n \geq 0 \forall x \in K_{n+1}$:

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

Proof. Write $D_{K_{n+1}/K_n} = \mathfrak{m}_{n+1}^d$ where $\mathfrak{m}_{n+1}$ is the maximal ideal of $\mathcal{O}_{K_{n+1}}$, where

$$\begin{aligned} d = v_{K_{n+1}}(D_{K_{n+1}/K_n}) &= [K_{n+1}:K] v_K(D_{K_{n+1}/K_n}) \\ &\overset{2.3.1.2.}{=} p^{n+1}(e + p^{-n}b_n) = p^{n+1}e + pb_n \end{aligned}$$

HW5/1/iii $\implies$ $\mathrm{Tr}_{K_{n+1}/K_n}(\mathfrak{m}_{n+1}^i) = \mathfrak{m}_n^j$ where $j = \left\lfloor \frac{d+i}{p} \right\rfloor$ where $p = [K_{n+1} : K_n]$
Suppose $xf \in \mathfrak{m}_{n+1}^i \setminus \mathfrak{m}_{n+1}^{i-1}$.
Then $|x| = |\pi_{n+1}^i| = |\pi|^{i/p^{n+1}}$.
$|\mathrm{Tr}_{K_{n+1}/K_n}(x)| \leq |\pi_n^j| = |\pi|^{j/p^n} \leq |\pi|^{\left(\frac{d+i}{p} - 1\right)/p^n} = |\pi|^{\frac{d}{p^{n+1}} - \frac{1}{p^n} + \frac{i}{p^{n+1}}} = |\pi|^{e + \frac{b_n}{p^n} - \frac{1}{p^n}}$.
$|\pi|^{i/p^{n+1}} = |\pi|^{e\left(1 + \frac{(b_n-1)/e}{p^n}\right)}|x| = |p|^{1+\frac{(b_n-1)/e}{p^n}}|x|$.
$(b_n)_n$ bounded, so $\exists a \geq 0 : \forall n \geq 0 : \frac{b_n - 1}{e} \geq -a$.
Thus, $|p|^{1+\frac{(b_n-1)/e}{p^n}} \leq |p|^{1-a/p^n}$.
Thus we ultimately have:

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

$\square$

Corollary 2.3.1.4. $\exists$ constant $c \geq 0$ independent of n such that $\forall n \geq 0 \forall x \in K_n$:

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

Proof. Iterate the formula in 2.3.1.3:
$|\mathrm{Tr}_{K_n/K}(x)| = |\mathrm{Tr}_{K_1/K}(\mathrm{Tr}_{K_n/K_1}(x))| \overset{2.3.1.3}{\leq} |p|^{1-a}|\mathrm{Tr}_{K_n/K_1}(x)|$
$\leq |p|^{1-a}|\mathrm{Tr}_{K_2/K_1}(\mathrm{Tr}_{K_n/K_2}(x))| \overset{2.3.1.3.}{\leq} |p|^{1-a}|p|^{1-a/p}|\mathrm{Tr}_{K_n/K_2}(x)|$
$= |p|^{2-a(1+1/p)}|\mathrm{Tr}_{K_n/K_2}(x)| \leq \cdots \leq |p|^{n-a(1+1/p+\cdots+1/p^{n-1})}|x|$
We can take $c = \frac{a}{1-1/p}$ $\square$

Let $\sigma \in \mathscr{C}$ be a topological generator, aka $\sigma \mod \mathscr{C}(n)$ is a generator of $\mathscr{C}/\mathscr{C}(n) \cong G(K_n/K)$ for all $n \geq 0$.
Lemma 2.3.1.5: $\exists c > 0$ independent of n such that $\forall n \geq 0 \forall x \in K_{n+1}$:

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

Proof. Write $\tau = \sigma^{p^n}$. Then $\tau\big|_{K_{n+1}}$ is a generator of $G(K_{n+1}/K_n)$. Then $px - \mathrm{Tr}_{K_{n+1}/K_n}(x) = \sum_{i=0}^{p-1}(\mathrm{id} - \tau^i)(x)$.

$$= \sum_{i=0}^{p-1} (\underbrace{1 + \tau + \cdots + \tau^{i-1}}_{=0 \text{ if } i=0})(1-\tau)(x)$$

$$= \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} \tau^j((1-\tau)(x)) \right)$$

Note that $|\tau^j(1-\tau)(x)| = |(1-\tau)(x)|$ so,

$$\leq |(1-\tau)(x)|$$

Divde by $|p|$ and get,

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

Can take $c = |p|^{-1}$ □

A most crucial definition:

Definition. Define $t : K_\infty \to K$ by $t(x) = p^{-n}\operatorname{Tr}_{K_n/K}(x)$ if $x \in K_n$.

Remark. This is well defined. If $x \in K_n$ and $m \geq n$ then $p^{-m}\operatorname{Tr}_{K_m/K}(x) = p^{-n}\operatorname{Tr}_{K_n/K}(p^{-(m-n)}\operatorname{Tr}_{K_m/K_n}(x)) = p^{-n}\operatorname{Tr}_{K_n/K}(p^{-(m-n)}p^{m-n}x)$

Proposition 2.3.1.6. Let σ be as above. $\exists$ constant $d > 0$ such that $\forall x \in K_\infty$,

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

Proof. Let $c_0 = 1, c_1 =$ constant in 2.3.1.5. Hence $|x - p^{-1}\operatorname{Tr}_{K_1/K_0}(x)| \leq c_1|\sigma(x) - x|$ for all $x \in K_1$ [here $K = K_0$].
For $n \geq 1, c_{n+1} := |p|^{-a/p^n} c_n$ with a as in 2.3.1.3.
Clearly, $c_n \to c > 0$.
Consider for any $n \geq 0$,

$$\forall x \in K_n : |x - t(x)| \leq c_n|\sigma(x) - x| \qquad (*)$$

For $n = 0$ both sides are 0.
For $n = 1$ this is the statement $|x - p^{-1}\operatorname{Tr}_{K_1/K_0}(x)| \leq c_1|\sigma(x) - x|$ which we have above.
To be continued.

Tuesday, 4/8/2025

Assume $(*)$ is true for $n \geq 1$. Let $x \in K_{n+1}$ and set $y = \operatorname{Tr}_{K_{n+1}/K_n}(x)$.
$\implies |y - pt(x)| = |y - p^{-n}\operatorname{Tr}_{K_{n+1}/K}(x)| = |y - p^{-n}\operatorname{Tr}_{K_n/K}(y)|$
By induction, $\leq c_n|\sigma(y) - y| = c_n \left| \left(\sum_{i=0}^{p-1}(\sigma^{p^n})^i(x)\right) - \sum_{i=0}^{p-1}(\sigma^{p^n})^i(x) \right|$
$= c_n \left| \sum_{i=0}^{p-1}(\sigma^{p^n})^i(\sigma(x)) - \sum_{i=0}^{p-1}(\sigma^{p^n})^i(x) \right| = c_n \left|\operatorname{Tr}_{K_{n+1}/K_n}(\sigma(x) - x)\right|$
by 2.3.1.3 $\leq c_n|p|^{1-ap^{-n}}|\sigma(x) - x|$
Furthermore: $|x - t(x)| \leq \max\{|x - p^{-1}y|, |p^{-1}y - t(x)|\}$ $(+)$.
2.3.1.5 and + implies $\leq \max\{c_1|\sigma^{p^n}(x) - x|, c_n|p|^{-ap^{-n}}|\sigma(x) - x|\}$. $c_{n+1} := c_n|p|^{-ap^{-n}}$.
Note: $|\sigma^{i+1}(x) - x| \leq \max\{|\sigma^{i+1}(x) - \sigma^i(x)|, |\sigma^i(x) - x|\}$
$= \max\{|\sigma^i(\sigma(x) - x)|, |\sigma^i(x) - x|\}$
$= \max\{|\sigma(x) - x|, |\sigma^i(x) - x|\}$.
Iterating, $\leq |\sigma(x) - x|$.
Thus, the thing before note $\leq \max\{c_1, c_{n+1}\}|\sigma(x) - x| = c_{n+1}|\sigma(x) - x|$
Hence we have proved $*$ for $n + 1$.
We end the proof by letting $d = \lim_{n\to\infty} c_n$.

□

Remark. An inspection of the proof of 2.3.1.6 shows that the statement of 2.3.1.6 is also true, <u>with the same constant</u> d if we replace K by K_n as base field.
Note: $G(K_\infty/K_n) \cong \mathbb{Z}_p$.

Notation: set $X = \widehat{K_\infty}$. This is a K-Banach space, since the absolute value on K_∞ extends to X.
The action of $\mathscr{C}$ also extends continuously to X.
Proposition. $t : K_\infty \to K$ extends continuously to a K-linear map $t : X \to K$ which is the identtiy on K.

Proof. t extends continuously by 2.3.1.4 or 2.3.1.6. □

Set $X_0 = \ker(t) \subset X$. It is a closed (by continuity) K-subspace of X.
Naturally $X = X_0 \oplus K$.
Proposition 2.3.1.7.

a) $X = X_0 \oplus K$ as a topological K-vector space.

b) $\sigma - \mathrm{id} : X \to X$ has kernel K and is bijective on X_0 with a continuos inverse on X_0.

c) Let $\lambda \in R$ such that $\lambda \equiv 1 \pmod{\pi}$ and assume that λ is <u>not</u> a root of unity. Then $\sigma - \lambda\,\mathrm{id} : X \to X$ is bijective with a continuous inverse.

Proof. a) Define $p_0 : X \to X_0$ by $p_0(x) = x - t(x) \implies t(p_0(x)) = t(x) - t(t(x)) = 0$.

Thus $p_0(x) \in X_0$ and the map $X \to X_0 \oplus K$ given by $x \mapsto (p_0(x), t(x))$ is a conitinuous K-linear bijection with inverse $X_0 \oplus K \to X$ given by $(x_0, a) \mapsto x_0 + a$.

b) Clear: $\ker(\sigma - \mathrm{id}) \supset K$. Write $K_n = K_{n,0} \oplus K$ with $K_{n,0} = \ker(\mathrm{Tr}_{K_n/K}) = \ker(t\big|_{K_n})$.

2.3.1.6 $\implies \forall x \in K_{n,0} : |\sigma(x) - x| \geq \frac{1}{d}|x - t(x)| = \frac{1}{d}|x| \implies (\sigma - \mathrm{id})\big|_{K_{n,0}}$ is bijective. Also, $\forall y \in K_{n,0} : |(\sigma - \mathrm{id})^{-1}(y)| \leq d|y|$ [by the previous inequality].

Therefore, $(\sigma - \mathrm{id})^{-1}$ extends continuously to $\bigcup_{n\geq 1} K_{n,0} = \ker(t\big|_{K_\infty})$.

By this inequality, $(\sigma - \mathrm{id})^{-1}$ extends continuously to the closure of $\ker(t\big|_{K_\infty})$ inside X, which is X_0.

c) $\lambda \neq 1$ thus $\sigma - \lambda\,\mathrm{id}$ is bijective on K since $\sigma - \lambda\,\mathrm{id}\big|_K = (1 - \lambda)\,\mathrm{id}_K$.

For $x \in X_0, (\sigma - \mathrm{id})^{-1}(\sigma - \lambda) = (\sigma - \mathrm{id})^{-1}(\sigma - \mathrm{id} + (1 - \lambda)\,\mathrm{id}) = \mathrm{id} - (1 - \lambda)(\sigma - \mathrm{id})^{-1}$.

If $|1 - \lambda| < d$ with d as in 2.3.1.6,

$|(\lambda - 1)(\sigma - \mathrm{id})^{-1}(y)| \leq |\lambda - 1|d|y| \leq d'|y|$ with $d' := |\lambda - 1|d < 1$.

Thus, $(\mathrm{id} - (1 - \lambda)(\sigma - \mathrm{id})^{-1})^{-1} = \sum_{n=0}^{\infty}((1 - \lambda)(\sigma - \mathrm{id})^{-1})^n$

Converges as a continuous K-linear operator on X_0.

Thus, $(\sigma - \lambda)^{-1} = (\sigma - \mathrm{id})^{-1}(\mathrm{id} - (1 - \lambda)(\sigma - \mathrm{id})^{-1})^{-1}$ exists as a continuous K-linear operator on X.

If $|1 - \lambda|d \geq 1$ instead we replace σ by σ^{p^n} and λ by λ^{p^n} with n large enough so that $|\lambda^{p^n} - 1|d < 1$. Replacing K by K_n and using the remark after 2.3.1.6, $|\sigma^{p^n} - \lambda^{p^n}|$ has a continuous inverse on X. Recall that $\lambda^{p^n} \neq 1$ by assumption. Note that:

$(\sigma - \lambda)(\sigma^{p^n - 1} + \cdots + \lambda^{p^n - 1}) = \sigma^{p^n} - \lambda^{p^n}$.

Thus, $\sigma - \lambda$ has a continuous inverse on X.

□

Continuous Cohomology (in degrees ≤ 1)

Let V be a K-Banach space. So,
$\|\cdot\| : V \to \mathbb{R}_{>0}$.
$\|\lambda v\| = |\lambda| \|v\|, \lambda \in K$
$\|v + w\| \leq \max\{\|v\|, \|w\|\}$
$\|v\| = 0 \iff v = 0$.
V is complete w.r.t. $\|\cdot\|$ topology.
We assume V is equipped with a continuous action of $\mathscr{C} (\cong \mathbb{Z}_p)$.
i.e. $\mathscr{C} \times V \to V$ is continuous.
i.e. For each $\tau \in \mathscr{C}$ the map $v \mapsto \tau v$ is continuous.
Define $Z^1(\mathscr{C}, V) := Z^1_{\text{cont}}(C, V) = \{c : \mathscr{C} \to V, \sigma \mapsto c_\sigma \mid c \text{ continuous and } \forall \sigma, \tau \in \mathscr{C} : c_{\sigma\tau} = c_\sigma + \sigma(c_\tau)\}$ K-vector space of continuous 1-cocycles.
Map $V \xrightarrow{d} Z^1(\mathscr{C}, V), (dv)_\sigma = v - \sigma(v). B^1(\mathscr{C}, V) = B^1_{\text{cont}}(\mathscr{C}, V) = \text{im}(d : V \to Z^1(\mathscr{C}, V))$ is called the K-vector space of continuous 1-coboundaries.
$H^0(\mathscr{C}, V) = V^{\mathscr{C}} = \{v \in V \mid \forall \sigma \in \mathscr{C} : \sigma(v) = v\}$.
$H^1(\mathscr{C}, V) := Z^1_{\text{cont}}(\mathscr{C}, V) / B^1_{\text{cont}}(\mathscr{C}, V)$
Let $\chi : \mathscr{C} \to R^\times$ be a continuous character. Set $X(\chi) = X(= \widehat{K_\infty})$ with the action of $\mathscr{C}$ given by $\sigma \underset{\chi}{.} x := \chi(\sigma) \cdot \sigma(x)$.
Proposition 2.3.1.8.

a) $H^0(\mathscr{C}, X) = K$ and $\dim_K H^1(\mathscr{C}, X) = 1$.

b) $|\text{im}(\chi)| = \infty \implies H^0(\mathscr{C}_{1X(\chi)}) = 0 = H^1(\mathscr{C}_1 X(\chi)) = 0$

Proof. Let $Y \subset X$ be a closed K-subspace stable under $\mathscr{C}$.
Let σ be a top. gen of $\mathscr{C}$.
Then $H^0(\mathscr{C}, Y(\chi)) = \ker(\sigma - \chi(\sigma)^{-1}\big|_Y)$ and any $c \in Z^1(\mathscr{C}, Y(\chi))$ is determined by $c_\sigma \in Y$.
$(dy)_\sigma = y - \sigma \underset{\chi}{.} y = y - \chi(\sigma)\sigma(y) = -\chi(\sigma)(\sigma - \chi(\sigma)^{-1})(y)$
Thus, $H^1(\mathscr{C}, Y(\chi)) \hookrightarrow Y / \text{im}(\sigma - \chi(\sigma)^{-1}\big|_Y)$.
$\chi(\sigma)$ not a root of 1.
To be continued. □

Thursday, 4/10/2025

Skipped

Tuesday, 4/15/2025

3.2 Finite extensions of K_∞

$L/K_\infty, R_L \subset L, R_\infty = R_{K_\infty} \supset \mathfrak{m}_\infty, \mathscr{H} = \text{Gal}(\overline{K}/K_\infty)$
Proposition 2.3.2.1. (Almost étaleness of $\overline{K}$ over K_∞)

$$\text{Tr}_{L/K_\infty}(R_L) \supset \mathfrak{m}_\infty$$

Note that Étale would mean $\text{Tr}_{L/K_\infty}(R_L) = R_\infty$ unramified.
$H^0_c(\mathscr{C}, X(\chi)), H^1_c(\mathscr{C}, X(\chi))$
The c stands for continuous.
Cohomology: M = abelian group, $\circlearrowleft G$ = pro-finite group.

Definition. M is called discrete G module if $M = \cup_{H \leq G, H \text{ open}} M^H$ ie for every $m \in M \exists$ open subgroup $H \leq G$ such that $H < \text{stab}_G(m)$.

Remark. If G is a p-adic group [eg $G = GL_n(\mathbb{Q}_p)$] then a representation of G on a vector space V is called smooth if V is a discrete G-module in the previously defined sense.

Consider $G \times M \to M$. Then $\{1\} \times \{m\} \to m$, continuity means open pre-image. Giving M discrete topology, an open neighborhood must contain a set of the form $U \times \{m\}$ where $U \subset G$ open with $1 \in U$.
Continuous cochains $C^r(G, M) = \{f : C^r \to M^\delta \mid f \text{ continuous}\}$. Notation: M^δ is M with discrete topology.
$d^r : C^r(G, M) \to C^{r+1}(G, M), (d^r f)(g_1, \cdots, g_{r+1}) = g_1 \cdot f(g_2, \cdots, g_{r+1})$
$+ \sum_{i=1}^r (-1)^i f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{r+1}) + (-1)^{r+1} f(g_1, \cdots, g_r)$
these are called 'r-cochains'. We have $d^{r+1} \circ d^r = 0$
Then $Z^r(G, M) = \ker(d^r), B^r(G, M) = \operatorname{im}(d^{r-1}), H^r(G, M) = \frac{\ker(d^r)}{\operatorname{im}(d^{r-1})}$
Example: $r = 0$ gives us $C^0(G, M) = M, d^0 : M \to C^1(G, M)$.
$(dm)(g) = g \cdot m - m$. $B^0 = 0$ thus $H^0(G, M) = M^G =$ set of elements fixed by G.
We also consider $\operatorname{Tr}_{L/K_\infty} : L \to K_\infty = Z^0(G(L/K_\infty), L) \subset C^0(G(L/K_\infty), L)$.
Referecnce: Article on group cohomology in Cossels-Fröhlich.
Serre, Galois Cohomology.
Set $L^\delta = L$ with discrete topology.
Corollary 2.3.2.2. Let L/K_∞ be a finite Galois extension with group G. Fix a real number $c > 1$. Let $r \geq 0$ and $f \in C^r(G, L)$. Then $\exists g \in C^{r-1}(G, L)$ s.t. $\|f - dg\| \leq c\|df\|$ and $\|g\| \leq c\|f\|$.
$\|f\| = \max\{|f(g)| \mid g \in G^r\} = \sup(\cdots)$ by compacntess of G. If $r = 0$ then $\exists y \in L$ such that,
$dy \coloneqq \operatorname{Tr}_{L/K_\infty}(y)$ is such that $\|f - dy\| = |f - dy| \leq c\|df\|$ and $|dy| \leq c|f|$.

Proof. Proposition 2.3.2.1 (almost étaleness) implies $\exists y \in R_L : \underbrace{|\operatorname{Tr}_{L/K_\infty}(y)|}_{=dy} \geq c^{-1}$.

Consider y as a (-1)-cochain.
Define an $(r-1)$ cochain by $y \cup f = yf$ if $r = 0$.
Formally, $C^{-1}(G, L) \coloneqq L$.
If $r \geq 1$ then
$(y \cup f)(s_1, \cdots, s_{r-1}) = (-1)^r \sum_{s_r \in G} \underbrace{(s_1, \cdots, s_r)(y)}_{\in L} \underbrace{f(s_1, \cdots, s_r)}_{\in L}$
Check: $\underbrace{dy}_{K_\infty} \cdot f - d^{r-1}(y \cup f) = y \cup (d^r f) \quad (*)$
Example: If $r = 0$ then LHS $= \operatorname{Tr}(y) \cdot f - \operatorname{Tr}(yf)$.
RHS $= (y \cup d^0 f)(1) = (-1)^1 \sum_{s \in G} s(y)(df)(s) = \sum_{s \in G} s(y)(s(f) - f) = \sum_{s \in G} s(y) f - \sum_{s \in G} s(yf) = \operatorname{Tr}(y) f - \operatorname{Tr}(yf)$. ☐

Set $x = dy \in K_\infty^\times, g = x^{-1}(y \cup f)$ [as maps $G^{r-1} \to L$].
Note: $dg = x^{-1} d(y \cup f)$.
$* \implies f - dg = x^{-1}(y \cup df)$.
Note: 1. $|x^{-1}| \leq c$.
2. $\|g\| \leq |x^{-1}| \|y \cup f\| \leq c\|f\|$.
2. $\|f - dg\| = \|x^{-1}(y \cup df)\| \leq |x^{-1}| \|y \cup df\| \leq c\|df\|$.
Now we pass to $\overline{K}$ which is a discretee module for $\mathscr{H} = \operatorname{Gal}(\overline{K}/K_\infty)$.
Corollary 2.3.2.3. Fix $c > 1$. Let $r \geq 0$ and f$\in C^r(\mathscr{H}, \overline{K})$. Let $f \in C^r(\mathscr{H}, \overline{K}^\delta)$. Then $\exists g \in C^{r-1}(\mathscr{H}, \overline{K}^\delta)$ such that $\|f - dg\| \leq c\|df\|$ and $\|g\| \leq c\|f\|$.
For $r = 0$ the conclusion is to be replaced by: $\exists x \in K^\infty$ such that $|f - x| \leq c\|df\|$.

Proof. This is because $C^r(\mathscr{H}, \overline{K}^\delta) = \cup_{L/K_\infty \subseteq \overline{K}/K_\infty, \text{finite galois}} C^r(G(L/K_\infty), L)$.
Use compactness of $\mathscr{H}^r$. ☐

Continuous Cohomology Set $C = \widehat{\overline{K}}$ endowed with the topology induced by absolute value. $\mathscr{H} = G(\overline{K}/K_\infty)$ and $\mathscr{G} = G(\overline{K}/K)$ act continuously on C.
Let $C^r(\mathscr{H}, C)$ be the continuous map $\mathscr{H}^r \to C$.
Define $d^r, Z^r(\mathscr{H}, C), B^r(\mathscr{H}, C)$ as before. We call:
$H_c^r(\mathscr{H}, C) = Z^r(\mathscr{H}, C)/B^r(\mathscr{H}, C)$.
The continuous cohomology group of $\mathscr{H}$ with coefficients in C. Similarly for $\mathscr{G}$.
Proposition 2.3.2.4. $H_c^0(\mathscr{H}, C) = \widehat{K_\infty} = X$. $H_c^r(\mathscr{H}, C) = 0$ for all $r > 0$.

Proof. Let $\mathcal{O}_C = \{x \in C \mid |x| \le 1\}$. Then $C = \overline{K} + \pi^\nu \mathcal{O}_C$ for any $\nu \ge 0$. Let $\psi_\nu : C \to C/\pi^\nu \mathcal{O}_C$, endow the target with the quotient topology, hence discrete topology.
As $\psi_\nu|_{\overline{K}}$ is surjective $\exists \phi_\nu : C/\pi^\nu \mathcal{O}_C \to \overline{K}^\delta$ such that $\psi_\nu \circ \phi_\nu = \mathrm{id}$. Note that ϕ_ν is continuous.
Set $f_\nu = \phi_\nu \circ \psi_\nu \circ f : \mathscr{H}^r \to \overline{K}$ which is continuous.
$\psi_\nu \circ f_\nu = \psi_\nu \circ \phi_\nu \circ \psi_\nu \circ f = \psi_\nu \circ f \implies \|f - f_\nu\| \le |\pi|^\nu$.
To be continued.

Thursday, 4/17/2025

Fix $c > 1$ once and for all. Consider $f \in Z^r(\mathscr{H}, C)$ to be an r-cocycle. We want to show it is a coboundary: $\exists g \in C^{r-1}(\mathscr{H}, C)$ such that $f = dg$. If $r = 0$ we instead mean $\exists g_\nu \in L_\nu \underset{\text{finite}}{/} K_\infty$ such that $f = \lim_{\nu\to\infty} \mathrm{Tr}_{L_\nu/K_\infty}(g_\nu) \in K_\infty$.
Case $r = 0$: $f \in Z^0(\mathscr{H}, C) = C^{\mathscr{H}}$. Then $f_\nu \in \overline{K}$ so we have $f_\nu \to f$.
$t : K_\infty \to K, t(a) = \frac{1}{p^n} \mathrm{Tr}_{K_n/K}(a)$.
$d : \overline{K} \to K_\infty$. $L \subset \overline{K}$ and $L \xrightarrow{\mathrm{Tr}_{L/K_\infty}} K_\infty$.
Then, for $a \in L, d(a) = \frac{1}{[L:K_\infty]} \mathrm{Tr}_{L/K_\infty}(a)$.
2.3.2.3 $\implies$ $\exists L_\nu/K_\infty$ finite, $g_\nu \in L_\nu : |f_\nu - \underbrace{dg_\nu}_{\in K_\infty}| \le c\|df_\nu\| = c \max\{\sigma \in \mathscr{H} \mid |\sigma(f_\nu) - f_\nu|\} = c\|d(f_\nu - f)\| \le c\|f_\nu - f\| \to 0$
Thus, $\|f - dg_\nu\| \le \max\{\underset{\to 0}{|f - f_\nu|}, \underset{\to 0}{f_\nu - dg_\nu}\} \to 0$. Therefore, $f \in \widehat{K_\infty}$.
Now we finish the case $r > 0$.
2.3.2.3. $\implies \exists g_\nu \in C^{r-1}(\mathscr{H}, \overline{K}^\delta) : \|f - dg_\nu\| \le c\|df_\nu\|$ and $\|g_\nu\| \le c\|f_\nu\|$.
We want: $\|g_\nu - g_\nu\| \overset{?}{\to} 0$.
Again, 2.3.2.3. $\implies$ $\exists h_\nu n\mathbb{I}C^{r-2}(\mathscr{H}, \overline{K}^\delta) : \|g_{r+1} - g_r - dh_\nu\| \le c\|d(g_{r+1} - g_r)\| \le c \max\{\underset{\to 0}{\|dg_{\nu+1} - f_{\nu+1}\|}, \|f_{\nu+1} - f_\nu\|, \underset{\to 0}{\|f_\nu - dg_\nu\|}\} \le \max\{\underset{\to 0}{\|f_{\nu+1} - f\|}, \underset{\to 0}{\|f - f_\nu\|}\}$.
Thus, $g \coloneqq g_1 + \sum_{\nu=1}^\infty \underset{\in C^{r-1}(\mathscr{H}, \overline{K}^\delta)}{(g_{\nu+1} - g_\nu - dh_\nu)}$
Converges in $C^{r-1}(\mathscr{H}, C)$.
Note: $dg = dg_1 + \sum_{\nu \ge 1} d(g_{\nu+1} - g_\nu - dh_\nu) = dg_1 + \sum_{\nu \mathbb{G}eq1}(dg_{\nu+1} - dg_\nu)$
Claim: dg converges to f.
Proof: $dg = \lim_{\mu\to\infty}(dg_1 + \sum_{\nu=1}^\mu (dg_{\nu+1} - dg_\nu)) = \lim_{\mu\to\infty} dg_{\mu+1} = \lim_{\mu\to\infty}((dg_{\mu+1} - f_{\mu+1}) + f_{\mu+1}) = \underbrace{\lim_{\mu\to\infty}(dg_{\mu+1} - f_{\mu+1})}_{=0} + \lim_{\mu\to\infty} f_{\mu+1} = f$.

□

3.3 The action of $\mathscr{G}_K$ on C

Define continuous cohomology groups $H_c^r(\mathscr{G}_K, C(\chi))$ as before. We usually droop the subscript c and K and just write $H^r(\mathscr{G}, C(\chi))$.
Recall: $\mathscr{G}$ is the absolute Galois group of K .
We have the following theorem.
Theorem 2.3.3.1. $H^0(\mathscr{G}, C) = K$ and $H^1(\mathscr{G}, C)$ is a 1-dimensional K-vector space.

Proof. $H^0(\mathscr{G}, C) = H^0(\mathscr{C}, H^0(\mathscr{H}, C)) \overset{2.3.2.4}{=} H^0(\mathscr{C}, X) \overset{2.3.1.8}{=} K$.

$$1 \to \mathscr{H} = G(\overline{K}/K_\infty) \to \mathscr{G} = \mathscr{G}_K \to G(K_\infty/K) \to G(K_\infty/K) = \mathscr{C} \to 1$$

$\underline{H^1}$: $\exists$ inflation-restriction exact sequence (Weibel, Serre, Local Fields, Galois Cohomology)

$$0 \to H^1(\mathscr{C}, H^0(\mathscr{H}, C)) \to H^1(\mathscr{G}, C) \xrightarrow{res} H^1(\mathscr{H}, C) \underset{2.3.2.4}{=} 0$$

Hence the assertion follows from 2.3.1.8

□

Theorem 2.3.3.2. Given a continuous homomorphism $\chi : \mathscr{G}_K \to R^\times$ we define $C(\chi) = C$ with $\mathscr{G}_K$ action given by the twist $\sigma \underset{\chi}{\cdot} a = \chi(\sigma)\sigma(a)$.

Let $K_\infty = \overline{K}^{\ker(\chi)}$. Then $G(\overline{K}/K_\infty) = \ker(\chi)$. Suppose $\exists$ finite extension K_0/K such that K_∞/K_0 is a purely ramified extension and $G(K_\infty/K_0) \cong \mathbb{Z}_p$ as topological groups.
Then $H^0(\mathscr{G}_K, C(\chi)) = H^1(\mathscr{G}_K, C(\chi)) = 0$.

Remark. $\underset{\cong \mathbb{Z}_p}{G(K_\infty/K_0)} \underset{\text{fin. index}}{\hookrightarrow} G(K_\infty/K) = \mathscr{G}_K/G(\overline{K}/K_\infty) \xrightarrow{\cong} \operatorname{im}(\chi)$
Furthermore, $\operatorname{im}(\chi)$ is abelian. Thus, K_0/K is Galois.
This excludes the case that K_∞ is the Lubin-Tate extension associated to a LT group over $\mathcal{O}_K$ (unless $K = \mathbb{Q}_p$). (in this case $G(K_\infty/K_0) \underset{\text{open}}{\subset} G(K_\infty/K) \xrightarrow{\sim} \mathcal{O}_K^\times$). But this includes the case of the cyclotomic class: $\chi_{cyc} : \mathscr{G}_K \xrightarrow{\text{open image}} \mathbb{Z}_p^\times \subset R^\times$.

Proof. Case H^0: $H^0(\mathscr{G}_K, C(\chi)) \subset H^0(\mathscr{G}_{K_0}, C(\chi))$
Note that:

$$1 \to G(\overline{K}/K_\infty) =: \mathscr{H} \hookrightarrow G(\overline{K}/K_0) = \mathscr{G}_{K_0} \twoheadrightarrow G(K_\infty/K_0) =: \mathscr{C} \cong \mathbb{Z}_p$$

Thus, $H^0(\mathscr{G}_{K_0}, C(\chi)) = H^0(\mathscr{C}, H^0(\mathscr{H}, C(\chi)))$
$= H^0(\mathscr{C}, H^0(\mathscr{H}, C)(\chi)) \overset{2.3.2.4}{=} H^0(\mathscr{C}, X(\chi)) \overset{2.3.1.8b, |\operatorname{im}\chi| = \infty}{=} 0.$
Case H^1: Apply infl-res. sequence to:

$$1 \to G(\overline{K}/K_0) \to G(\overline{K}/K) \to \underset{finite}{G(K_0/K)} \to 1$$

$$1 \to \mathscr{G}_{K_0} \to \mathscr{G}_K \to G(K_0/K) \to 1$$

Thus,

$$0 \to \underbrace{H^1(G(K_0/K), \underbrace{H^0(\mathscr{G}_{K_0}, C(\chi))}_{K_0\text{-v.s., char } 0})}_{=0} \to H^1(\mathscr{G}_K, C(\chi)) \to H^1(\mathscr{G}_{K_0}, C(\chi))$$

Apply infl-res. sequence to:

$$1 \to \mathscr{H} = G(\overline{K}/K_\infty) \to \mathscr{G}_{K_0} \to \mathscr{C} \to 1$$

Thus,

$$0 \to \underbrace{H^1(\mathscr{C}, \underbrace{H^0(\mathscr{H}, C(\chi))}_{\underset{2.3.2.4}{=} X(\chi)})}_{\underset{2.3.1.8}{=} 0} \to \underbrace{H^1(\mathscr{G}_{K_0}, C(\chi))}_{=0} \to H^1(\mathscr{H}, C(\chi)) = H^1(\mathscr{H}, C) \underset{2.3.2.4}{=} 0$$

□

4 Theorems on p-divisible groups

$R = $ cdvr, $k = R/\mathfrak{m}_R$ perfect field of char $p > 0, K = \operatorname{Frac}(R)$ is of char 0, $C = \widehat{\overline{K}}$.
Recall proposition 2.1.2.2: which says that the cartier dual $G_\nu^\vee = \underline{\operatorname{Hom}}_{\text{gpsch}/R}(G_\nu, \mathbb{G}_{m,R})$
($\implies \forall S \in \operatorname{Alg}_R : G_\nu^\vee(S) = \operatorname{Hom}_{\text{gpschm}/R}(G_\nu \otimes_R S, \mathbb{G}_{m,S}) = G_\nu \times_{\operatorname{Spec}(R)} \operatorname{Spec}(S)$)
Thus $G_\nu^\vee(\mathcal{O}_C) = \operatorname{Hom}_{\text{gpschm}/\mathcal{O}_C}(G_\nu \otimes_R \mathcal{O}_C, \mathbb{G}_{m,\mathcal{O}_C})$
Easily $= \operatorname{Hom}_{\text{gpsch}/\mathcal{O}_C}(G_\nu \otimes_R \mathcal{O}_C, \mu_{p^\infty,\mathcal{O}_C})$ (1).
Tate module $TG^\vee = \varprojlim_\nu G_\nu^\vee(\overline{K}) = \operatorname{Hom}_{R\text{-alg}}(\mathcal{O}(G_\nu), \overline{K}) = \varprojlim G_\nu^\vee(C) = \varprojlim G_\nu^\vee(\mathcal{O}_C)$ (2)
Here $G^\vee = (G_\nu^\vee)_\nu$
(1) and (2) togehter imply:
$TG^\vee \operatorname{Hom}_{p\text{-div gps}/\mathcal{O}_C}\left(\varinjlim_\nu G_\nu \otimes_R \mathcal{O}_C, \mu_{p^\infty,\mathcal{O}_C}\right)$

$= \mathrm{Hom}_{p\text{-div. gps}/\mathcal{O}_C}(G \otimes_R \mathcal{O}_C, \mu_{p^\infty, \mathcal{O}_C})$ (3)
Note $\mathrm{Hom}(\mu_{p^\infty}, \mu_{p^\infty}) = \mathbb{Z}_p$
$T(\mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p$ has trivial Galois action.

Tuesday, 4/22/2025

Recall: $G = (G_\nu)_\nu$ is a p-divisible group $/R$. $C = \widehat{barr\overline{K}} \supset \mathcal{O}_C \supset \mathfrak{m}_C \coloneqq \mathfrak{m}_{\mathcal{O}_C}$.
Proposition 2.1.2.2. $G_\nu^\vee = \underline{\mathrm{Hom}}_{\mathrm{gpsch}/R}(G_\nu, \mathbb{G}_{m,R})$.
$(G_\nu^\vee(S) = \mathrm{Hom}_{\mathrm{gpsch}/S})(G_\nu \otimes_R S, \mathbb{G}_{m,S})$
$TG^\vee = \varprojlim_\nu G_\nu^\vee(\overline{K}) = \varprojlim_\nu G_\nu^\vee(C) = \varprojlim_\nu G_\nu^\vee(\mathcal{O}_C) = \varprojlim_\nu \mathrm{Hom}_{\mathrm{gpsch}/\mathcal{O}_C}(G_\nu \otimes_R \mathcal{O}_C, \mu_{p^\infty, \mathcal{O}_C})$
$= \mathrm{Hom}_{p\text{-div}/\mathcal{O}_C}(\varinjlim_\nu G_\nu \otimes_R \mathcal{O}_C, \mu_{p^\infty, \mathcal{O}_C}) = \mathrm{Hom}_{p\text{-div gps}/\mathcal{O}_C}(G \otimes \mathcal{O}_C, \mu_{p^\infty, \mathcal{O}_C})$
Recall: $G(\mathcal{O}_C) \coloneqq \varprojlim_i G(\mathcal{O}_C/\pi^i) = \varprojlim_i \left(\varinjlim G_\nu(\mathcal{O}_C/\pi^i) \right)$
$(\neq \varinjlim_\nu G_\nu(\mathcal{O}_C))$
Example: $G = \mu_{p^\infty}$. Claim: $G(\mathcal{O}_C/\pi^i) = 1 + \mathfrak{m}_C/\pi^i\mathcal{O}_C$
$a \in \mathcal{O}_C, a \mod \pi^i \in \mu_{p^\nu}(\mathcal{O}_C/\pi^i)$
$\implies a^{p^\nu} \equiv 1 \mod \pi^i \implies a^{p^\nu} \equiv 1 \mod (\mathfrak{m}_C)$
Thus $\overline{a} = 1$ where $\overline{a} = a \mod \mathfrak{m}_C$ and $\mathcal{O}_C/\mathfrak{m}_C = \overline{k}$.
Then, $a \mod \pi^i \in 1 + \mathfrak{m}_C/\pi^i\mathcal{O}_C$.
Conversely, if $a \in 1 + \mathfrak{m}_C$ then $\forall \nu \gg 0 : a^{p^\nu} \equiv 1 \mod \pi^i \implies (a \mod \pi^i)^{p^\nu} = 1$ in $\mathcal{O}_C/\pi^i$.
Then $a \mod \pi^i \in \mu_{p^\nu}(\mathcal{O}_C/\pi^i)$.
Then $\mu_{p^\infty}(\mathcal{O}_C) = \varprojlim \mu_{p^\infty}(\mathcal{O}_C/\pi^i) = \varprojlim(1 + \mathfrak{m}_C/\pi^i\mathcal{O}_C) = 1 + \mathfrak{m}_C$
From now on: $U \coloneqq 1 + \mathfrak{m}_C$ considered as $\mu_{p^\infty}(\mathcal{O}_C)$.. This is $\mathbb{Z}_p$-module.
Then $[c](a) = a^c = \sum_{j=0}^\infty \binom{c}{j}(a-1)^j \in U$.
$U_{\mathrm{tors}} = \bigcup_\nu \mu_{p^\nu}(\mathcal{O}_C) = \Phi(\mu_{p^\infty})$
We have a logarithm: $\log_{\mu_{p^\infty}} : \mu_{p^\infty}(\mathcal{O}_C) = U \to C$
$a \mapsto \log(a) = \sum_{n=1}^\infty \frac{(-1)^{n-1}}{n}(a-1)^n$
Then we have exact sequence:

$$0 \to \Phi(\mu_{p^\infty}) = U_{\mathrm{tors}} \to U \xrightarrow{\log} C \to 0$$

Recall:
$TG^\vee \underset{\mathrm{can}}{\cong} \mathrm{Hom}_{\mathrm{pdivgps}/\mathcal{O}_C}(G \otimes \mathcal{O}_C, \mu_{p^\infty, \mathcal{O}_C})$

Definition. We define a pairing $TG^\nu \times G(\mathcal{O}_C) \to \mu_{p^\infty}(\mathcal{O}_C) = U$
$(\tau, \xi) \mapsto \langle \tau, \xi \rangle = \varepsilon_\xi(\tau)$ as follows: given $\xi \in G(\mathcal{O}_C)$, write $\xi = (\xi_i)_i$ with $\xi_i \in G(\mathcal{O}_C/\pi^i)$, and $\tau \in TG^\vee$, we have:

$$\tau \circ \xi_i : \qquad \begin{tikzcd} \mathrm{Spec}(\mathcal{O}_C/\pi^i) \arrow[r] \arrow[rr, bend right] & G \otimes \mathcal{O}_C \arrow[r, "\tau"] & \mu_{p^\infty, \mathcal{O}_C} \end{tikzcd}$$

$\in \mu_{p^\infty}(\mathcal{O}_C/\pi^i)$

$\implies \varepsilon_\xi(\tau) \coloneqq (\tau \circ \xi_i)_i \in \varprojlim \mu_{p^\infty}(\mathcal{O}_C/\pi^i) = \mu_{p^\infty}(\mathcal{O}_C) = U$
Check: this pairing is $\mathbb{Z}_p$-bilinear.

Recall: $\log_G : G(\mathcal{O}_C) \to t_G(C) = \mathrm{Hom}_R(I^0/(I^0)^2, C)$
Where $I^0 = \ker(A^0 \to R)$ is the augmentation ideal. $A^0 \to R$ is induced by the unit section.
$A^0 = \varprojlim_\nu \mathcal{O}(G_\nu^0)$ $[\cong R[[x_1, \cdots, x_n]], n = \dim G]$
Then for $a \in G(\mathcal{O}_C), f \in I^0$,

$$\log_G(a)(f) = \lim_{i \to \infty} \frac{f([p^i]_G(a)) - f(a)}{p^i}$$

We get an induced pairing $TG^\vee \times t_G(C) \to t_{\mu_{p^\infty}}(C)$

$(\tau, \log_G(\xi)) \mapsto \langle \tau, \log_G(\xi) \rangle = \log_{\mu_{p^\infty}}(\langle \tau, \xi \rangle)$
Recall the exact sequence:

$$\begin{tikzcd}
O \arrow[r] & G(\mathcal{O}_C)_{\text{tors}} = & \Phi(G) \arrow[d] & = \varinjlim G_\nu(\mathcal{O}_C) \\
& & G(\mathcal{O}_C) \arrow[d, "\log_G"] & \\
& & t(C) \arrow[d] & \\
& & 0 &
\end{tikzcd}$$

So independent of lift ξ of $\log_G(\xi)$.
We have the diagram $(*)$: '

$$\begin{tikzcd}
0 \arrow[r] & \Phi(G) = G(\mathcal{O}_C)_{\text{tors}} \arrow[r, hook] \arrow[d, "\alpha_0"] & G(\mathcal{O}_C) \arrow[r, "\log_G"] \arrow[d, "\alpha"] & t_G(C) \arrow[r] \arrow[d, "d\alpha"] & 0 \\
0 \arrow[r] & \operatorname{Hom}_{\mathbb{Z}_p}(TG^\vee, \Phi(\mu_{p^\infty})) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}_p}(TG^\vee, \mu_{p^\infty}(\mathcal{O}_C)) \arrow[r] & \operatorname{Hom}_{\mathbb{Z}_p}(TG^\vee, \underbrace{t_{\mu_{p^\infty}}(C)}_{=C}) \arrow[r] & 0
\end{tikzcd}$$

$\lambda \mapsto \log_{\mu_{p^\infty}} \circ \lambda$
Here $\alpha : \xi \mapsto \langle -, \xi \rangle$

<u>Exactness of Bottom Row</u>: $0 \to U_{\text{tors}} \to U \xrightarrow{\log_{\mu_{p^\infty}}} C \to 0$ exact by earlier results.
$TG^\vee$ is a free $\mathbb{Z}_p$ module of rank $h = ht(G^\vee) = ht(G)$. Hence it is projetive. Hence $\operatorname{Hom}_{\mathbb{Z}^p}(TG^\vee, -)$ produces an exact sequene.
<u>Rem</u> All groups in the diagram $(*)$ are naturally $\mathscr{G}$-modules. For the top row, this action comes from the action of $\mathscr{G} = \operatorname{Gal}(\overline{K}/K)$ on C. The $\mathscr{G}$ action on the modules in the bottom row is given by $(\sigma \cdot \lambda)(\tau) = \sigma(\lambda(\sigma^{-1}(\tau)))$. $\tau \in TG^\vee$. α_0, α and $d\alpha$ are $\mathscr{G}$-equivariant.
Check for α: $\alpha(\sigma(\xi))(\tau) = \langle \tau, \sigma(\xi) \rangle = (\tau \circ \sigma(\xi_i))_i$
$(\sigma \cdot \alpha(\xi))(\tau) = \sigma(\alpha(\xi)(\sigma^{-1}(\tau))) = \sigma(\langle \sigma^{-1}(\tau), \xi \rangle) = \sigma((\sigma^{-1}(\tau) \circ \xi_i))_i = (\tau \circ \sigma(\xi_i))_i$
Lemma 2.4.1.1. If W is a C-vector space with a semi-linear $\mathscr{G}$-action ($\sigma(c \cdot w) = \sigma(c) \cdot \sigma(w)$ for all $c \in C$ and $w \in W$), then the map $C \otimes_K W^{\mathscr{G}} \to W, c \otimes w \mapsto c \cdot w$ is injective.

Proof. Let $\{w_1, \cdots, w_n\}$ be a set of K-linearly independent vectors in $W^{\mathscr{G}}$. We want to show that for all scalars $c_1, \cdots, c_n \in C : \sum_i c_i w_i = 0$ then $c_1 = \cdots = c_n = 0$.
Suppose there is a linear combination with not all $c_i = 0$. WLOG assume $c_1 = 1$. We may also assume n is minimal with this property.
$\forall \sigma \in \mathscr{G} : 0 = \sigma\left(\sum c_i w_i\right) = \sum \sigma(c_i)\sigma(w_i) = \sum \sigma(c_i) w_i = \sum c_i w_i$
Therefore, $\sum_{i=2}^n (\sigma(c_i) - c_i) w_i = 0$.
$n = 1$ is impossible. For $n \geq 2$ we get a linear combination with fewer terms, unless $\sigma(c_i) = c_i$ for all c_i. This implies $\forall i : c_i \in K$. But this contradicts the linear independence of w_i over K. $\square$

Proposition 2.4.1.2. In the diagram $(*)$, α_0 is bijective whereas α and $d\alpha$ are injective.
Theorem 2.4.1.3. The maps $\alpha_R : G(R) = G(\mathcal{O}_C)^{\mathscr{G}} \to \operatorname{Hom}_{\mathbb{Z}_p}(TG^\vee, U)^{\mathscr{G}} = \operatorname{Hom}_{\mathbb{Z}_p(\mathscr{G})}(TG^\vee, U)$
$d\alpha_R : t_G(K) = t_G(C)^{\mathscr{G}} \to \operatorname{Hom}_{\mathbb{Z}_p}(TG^\vee, t_{\mu_{p^\infty}}(C))^{\mathscr{G}} = \operatorname{Hom}_{\mathbb{Z}_p[\mathscr{G}]}(TG^\vee, C)$
are bijective.

Thursday, 4/24/2025

Lemma 2.4.1.4.

i) $\forall \nu \geq 0$ the map $G_\nu^\vee(C) \times G_\nu(C) \to \mu_{p^\nu}(C), (\tau_\nu, \xi_\nu) \mapsto \langle \tau_\nu, \xi_\nu \rangle := \tau_\nu \circ \xi_\nu$ (recall $G_\nu^\vee(C) = \mathrm{Hom}_{\mathrm{gpsch}/C}(G_\nu \otimes_R C, \mathbb{G}_{\mathfrak{m},\mathfrak{C}}) = \mathrm{Hom}_{\mathrm{gpsch}/C}(G_\nu \otimes C, \mu_{p^\nu,C}))$ is a perfect $\mathscr{G}$-equivariant pairing, i.e. $G_\nu^\vee(C) \to \mathrm{Hom}_{\mathbb{Z}}(G_\nu(C), \mu_{p^\nu}(C))$ is bijective.

ii) The pairings in (i) induce a perfect $\mathscr{G}$-equivariant $\mathbb{Z}_p$-bilinear pairing $TG^\vee \times TG \to T\mu_{p^\infty}$.

iii) The pairings in (i) induce a $\mathscr{G}$-equivariant isomorphism $\Phi(G) \to \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, \Phi(\mu_{p_\infty}))$ and this map is equal to the map α_0 in the diagram.

Proof. i) $\underline{\Gamma}_S$ = constant gp scheme over Spec(S) associated to $\Gamma = \mathrm{Spec}(S^\Gamma)$.
$G_\nu^\vee(C) = \mathrm{Hom}_{\mathrm{gpsch}/C}(G_\nu \otimes_R C, \mu_{p^\nu,C})$, from étaleness $= \mathrm{Hom}_{\mathrm{gpsch}/R}(\underline{G_\nu(C)}_C, \underline{\mu_{p^\nu}(C)}_C) = \mathrm{Hom}_{\mathbb{Z}}(G_\nu(C), \mu_{p^\nu}(C)) = \mathrm{Hom}_{\mathbb{Z}_p}(G_\nu(C), \mu_{p^\nu}(C))$.

ii) Follows from (i).

iii) The map $\Phi(G) \to \mathrm{Hom}(TG^\vee, \Phi(\mu_{p^\infty}))$ is given by $\xi_\nu \in G_\nu(C) \subset \Phi(G)$. Then $\xi_\nu : TG^\vee \to G_\nu^\vee(C) \dashrightarrow \Phi(\mu_{p^\infty})$ is given by $(\tau_\mu)_\mu \mapsto \tau_\nu \circ \xi_\nu$.
$\mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, \Phi(\mu_{p^\infty})) = \varinjlim_\nu \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, \mu_{p^\nu}(C)) = \varinjlim_\nu \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee/p^\nu TG^\vee, \mu_{p^\nu}(C))$
Use $\Phi(G^\vee) = TG^\vee \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = \varinjlim_\nu TG^\vee \otimes (\frac{1}{p^\nu}\mathbb{Z}/\mathbb{Z}) = \varinjlim (TG^\vee/p^\nu TG^\vee)$
Then, $\varinjlim_\nu \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee/p^\nu TG^\vee, \mu_{p^\nu}(C)) = \varinjlim_\nu \mathrm{Hom}_{\mathbb{Z}_p}(\Phi(G^\vee)[p^\nu], \mu_{p^\nu}(C))$
$= \varinjlim_\nu \mathrm{Hom}_{\mathbb{Z}_p}(G_\nu^\vee(C), \mu_{p^\nu}(C)) = \varinjlim_\nu G_\nu(C) = \Phi(G)$.
To see that this map is the same map as α_0 just trace through the definition. □

Proof of Theorem 2.4.1.3. 2.4.1.2. $\implies$ the maps α_R and $d\alpha_R$ in 2.4.1.3. are injective.
Consider from $*$:

$$0 \to G(\mathcal{O}_C) \xrightarrow{\alpha} \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, U) \to \mathrm{coker}(\alpha) \to 0$$

Take $\mathscr{G}$-invariants:

$$\begin{tikzcd}
0 \arrow[r] & G(\mathcal{O}_C)^{\mathscr{G}} \arrow[r, "\alpha_R"] \arrow[d, "=2.3.3.1"] & \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, U)^{\mathscr{G}} \arrow[r] \arrow[d, "="] & \mathrm{coker}(\alpha)^{\mathscr{G}} \arrow[r] & H^1_c(\mathscr{G}, G(\mathcal{O}_C)) \\
& G(R) & \mathrm{Hom}_{\mathbb{Z}_p(\mathscr{G})}(TG^\vee, U) & &
\end{tikzcd}$$

$$\implies \mathrm{coker}(\alpha_R) \hookrightarrow \mathrm{coker}(\alpha)^{\mathscr{G}}$$

Note that 2.4.1.2. implies α is injective.
Similarly, we have $d\alpha$ is injective.

$$0 \to t_G(C) \xrightarrow{d\alpha} \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, C) \to \mathrm{coker}(d\alpha) \to 0$$

Take $\mathscr{G}$ invariants:

$$0 \to t_G(K) \xrightarrow{d\alpha_R} \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, C)^{\mathscr{G}} \to \mathrm{coker}(d\alpha)^{\mathscr{G}}$$

Thus, $\mathrm{coker}(d\alpha_R) \hookrightarrow \mathrm{coker}(d\alpha)^{\mathscr{G}}$.
We have a commutative diagram.

$$\begin{tikzcd}
\mathrm{coker}(\alpha) \arrow[r, "\cong"] & \mathrm{coker}(d\alpha) \\
\mathrm{coker}(\alpha)^{\mathscr{G}} \arrow[r, "\cong"] \arrow[u, hook] & \mathrm{coker}(d\alpha)^{\mathscr{G}} \arrow[u, hook] \\
\mathrm{coker}(\alpha_R) \arrow[r] \arrow[u, hook] & \mathrm{coker}(d\alpha_R) \arrow[u, hook]
\end{tikzcd}$$

Adding coker to $*$ and using snake lemma, the upper horizontal map is an isomorphism.
It follows that $\mathrm{coker}(\alpha_R) \to \mathrm{coker}(d\alpha_R)$ is injective.
In order to prove bijectivity, we should prove now that the cokernel vanishes.
It suffices to show $\mathrm{coker}(d\alpha_R) = 0$.
Hence we need to show: $n := \dim(G) = \dim_K t_G(K) \underset{\text{need to show}}{=} \dim \mathrm{Hom}_{\mathbb{Z}_p[\mathscr{G}]}(TG^\vee, C)^{\mathscr{G}}$ (1)
Set $W := \mathrm{Hom}_{\mathbb{Z}_p}(TG, C)$
$W' = \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, C)$
Then $\dim_C W = \mathrm{ht}(G) =: h = \dim_C(W')$
Set $d := \dim_K((W')^{\mathscr{G}}), d' = \dim_K((W')^{\mathscr{G}})$
2.4.1.2 $\implies$
$t_G(C) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(TG^\vee, C) = W' \implies n \leq d'$
$t_{G^\vee}() \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(TG, C) = W \implies n^\vee := \dim(G^\vee) \leq d$
Together they're (2).
2.2.3.1 $\implies n + n^\vee \underset{(3)}{=} h \overset{(2)}{\implies} h \underset{(4)}{\leq} d + d'$
Upshot: STS: $d + d' \underset{(5)}{\leq} h$.
Set $VG = TG \otimes \mathbb{Q}_p, VG^\vee = TG^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$
$Q_p(1) := V\mu_{p^\infty} = T\mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathbb{Q}_p \cdot \chi_{\mathrm{cyc}}$
$\chi_{\mathrm{cyc}} : \mathscr{G} \to \mathbb{Z}_p^\times, \sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi_{\mathrm{cyc}}(\sigma) \mod p^n}$
Lemma 2.4.1.4. $\implies VG \underset{\mathscr{G}}{\cong} \mathrm{Hom}_{\mathbb{Q}_p}(TG^\vee, \mathbb{Q}_p(1)) = \mathrm{Hom}_{\mathbb{Q}_p}(TG^\vee, \mathbb{Q}_p)(1)$.
$\mathbb{Q}_p$ gets the trivial $\mathscr{G}$ action.
Then $VG \otimes_{\mathbb{Q}_p} C \underset{\mathscr{G}}{\cong} \mathrm{Hom}_{\mathbb{Q}_p}(TG^\vee, C)(1) = W'(1)$
$W = \mathrm{Hom}_{\mathbb{Q}_p}(VG, C) = \mathrm{Hom}_C(VG \otimes_{\mathbb{Q}_p} C, C) = \mathrm{Hom}_C(W'(1), C)$
$\implies W \times W'(1) \to C$ perfect $\mathscr{G}$-equivariant pairing $\implies W \times W' \to C(-1)$ perfect $\mathscr{G}$-equivariant pairing.
Thus $W^{\mathscr{G}} \times (W')^{\mathscr{G}} \to C(-1)^{\mathscr{G}} \underset{2.3.3.2}{=} 0$
Thus, $W^{\mathscr{G}}, (W')^{\mathscr{G}}$ are perpendicular w.r.t. $\langle , \rangle$
Thus $W^{\mathscr{G}} \otimes C \underset{2.4.1.1}{\hookrightarrow} W$ and $(W')^{\mathscr{G}} \otimes C \underset{2.4.1.1}{\hookrightarrow} W'$ are perpendicular w.r.t. $\langle , \rangle$
it is elementary to see now that $d + d' \leq h$ hence we're done.

$\square$