WEEK 10.

(STUDENT SEMINARS.)

LUBIN-TATE THEORY LECTURE 1

RANDY MARTINEZ

We first give an overview on some key elements of power series.

1. Power Series

A will denote a commutative ring with unity. A power series with coefficients in A is an infinite series of the form

$$\sum_{n=0}^{\infty} a_n T^n, \quad a_n \in A.$$

We can make a ring structure out of the set of power series with coefficients in A by defining addition of two power series as:

$$\sum a_n T^n + \sum b_n T^n = \sum (a_n + b_n) T^n,$$

and multiplication as

$$\Big(\sum a_n T^n\Big)\Big(\sum b_n T^n\Big) = \sum \Big(\sum_{i+j=n} a_i b_j\Big) T^n.$$

This set is usually denoted as $A[[T]]$.

Note: We must be cautious when composing a power series f with g. If g has a constant term, then we would have to evaluate an infinite sum, which we cannot evaluate in general. So we must restrict the case to where g has no constant term. This composition is denoted by $f \circ g$.

Lemma 1.1. (a) (Associativity) For any $f \in A[[T]]$ and $g, h \in TA[[T]]$,

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

(b) Let $f = \sum_{n=1}^{\infty} a_n T^n$. Then there is a $g \in TA[[T]]$ such that $f \circ g = T$ if and only if $a_1 \in A^\times$. If such a g exists, then it is unique and $g \circ f = T$.

Proof: (a) By defining a product to be pointwise multiplication, we immediately deduce that $(f_1 f_2) \circ g = (f_1 \circ g)(f_2 \circ g)$, and hence $f^n \circ g = (f \circ g)^n$. If $f = T^n$, then we deduce that $f \circ (g \circ h) = (g \circ h)^n$, and similarly $(f \circ g) \circ h = g^n \circ h = (g \circ h)^n$. This implies that if $f = \sum a_n T^n$, then $f \circ (g \circ h) = \sum a_n (g \circ h)^n = (f \circ g) \circ h$.

(b) Let $f = \sum_{n=1}^{\infty} a_n T^n$. For such a $g = \sum_{n=1}^{\infty} b_n T^n$ with $f \circ g = T$ to exist, we would need that

$$a_1 b_1 = 1, \quad a_1 b_2 + a_2 b_1^2 = 0, \quad \ldots, \quad a_1 b_n + \text{ terms in } a_2, \ldots, a_{n-1}, b_1, \ldots, b_{n-1}.$$

In particular, such a g exists precisely when a_1 and b_1 are units. We then inductively define b_n for every n. For example, $b_2 = a_1^{-1}(-a_2 b_1^2) = b_1(-a_2 b_1^2)$. In general,

$$b_n = a_1^{-1}(\text{terms in } a_2, \ldots, a_{n-1}, b_1, \ldots, b_{n-1}),$$

so that b_n are completely determined by $b_1, \ldots, b_{n-1}$ and a_i's; giving uniqueness. Note that since b_1 is invertible, there is an $h \in TA[[T]]$ such that $g \circ h = T$. Hence

$$f = f \circ T = f \circ (g \circ h) = (f \circ g) \circ h = T \circ h = h,$$

which implies that $f = h$, so $g \circ f = T$. $\square$

2. Formal Group Laws

Definition 2.1. A *(one-parameter commutative) formal group law* is a power series $F \in A[[X,Y]]$ such that
(a) $F(X,Y) = X + Y +$ terms of higher degree;
(b) $F(X, F(Y,Z)) = F(F(X,Y), Z)$ (associativity);
(c) There is a unique $i_F(X) \in XA[[X]]$ such that $F(X, i_F(X)) = 0$ (inverse);
(d) $F(X,Y) = F(Y,X)$ (commutativity).

This gives a group structure without an underlying set, which is why it is a "formal" group law.

Note that by the axioms, we have that

$$F(X,0) = X + \text{higher order terms}, \quad F(F(X,0),0) = F(X,0).$$

Let $f = F(X,0)$. Then by Lemma 1.1 there exists an inverse g such that $f \circ g = T$ and $f \circ f = f$, which both imply that $f = X$. Hence $F(X,0) = X$ and similarly, $F(0,Y) = Y$.

Let $K, |\cdot|$ be local field with a non-archimedean absolute value. Let $R = \{x \in K : |x| \leq 1\}$ be the ring of integers and $\mathfrak{m} = \{x \in K : |x| < 1\}$ its maximal ideal. Define $F = \sum_{i,j} a_{ij} X^i Y^j$ to be a formal group law over R. For any $x, y \in \mathfrak{m}$, $a_{ij}x^i y^j \to 0$ as $i, j \to \infty$, so $F(x,y)$ converges to an element in $\mathfrak{m}$, which we denote by $x +_F y$, which gives us a group structure on $\mathfrak{m}$.

Example: (a) $F(X,Y) = X + Y$, normal additive group structure on $\mathfrak{m}$.
(b) $F(X,Y) = X + Y + XY$. Then $(\mathfrak{m}, +_F) \simeq (1 + \mathfrak{m}, \times)$ given by the map $a \mapsto 1 + a$. The map $a \mapsto 1 + a$ is clearly bijective, and being a group homomorphism follows from the following being a commutative diagram:

$$\begin{tikzcd}
(a,b) \arrow[r, "a \mapsto 1+a"'] \arrow[d, "+_F"'] & (1+a, 1+b) \arrow[d, "\times"] \\
a+b+ab \arrow[r] & 1+a+b+ab
\end{tikzcd}$$

3. Homomorphisms of Formal Group Laws

Definition 3.1. Let $F(X,Y), G(X,Y)$ be formal group laws. A *homomorphism* $h : F \to G$ is a power series $h \in TA[[T]]$ such that

$$h(F(X,Y)) = G(h(X), h(Y)).$$

If there exists a homomorphism $h : G \to F$ such that $h \circ h' = h' \circ h = T$, then we say h is an *isomorphism*. A homomorphism $h : F \to F$ is called an *endomorphism* of F.

Example: Let $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$. Then $f(T) = (1+T)^p - 1$ is an endomorphism of F:

$$f(F(X,Y)) = (1 + ((1+X)(1+Y) - 1))^p - 1 = (1+X)^p(1+Y)^p - 1$$

$$F(f(X), f(Y)) = (1 + (1+X)^p - 1)(1 + (1+Y)^p - 1) - 1 = (1+X)^p(1+Y)^p - 1.$$

Consider the following diagram:

$$\begin{tikzcd}
\mathfrak{m} \arrow[r, "f"'] \arrow[d, "a \mapsto 1+a"'] & \mathfrak{m} \arrow[d, "a \mapsto 1+a"] \\
1+\mathfrak{m} \arrow[r, "a \mapsto a^p"] & 1+\mathfrak{m}
\end{tikzcd}$$

This diagram commutes since

$$a \xrightarrow{1+a} 1+a \xrightarrow{a\mapsto a^p} (1+a)^p;$$
$$a \xrightarrow{f} (1+a)^p - 1 \xrightarrow{a\mapsto a^p} (1+a)^p.$$

Then we have that f corresponds to the map $a \mapsto a^p$.

For a formal group law G, define for $f, g \in TA[[T]]$:

$$f +_G g = G(f(T), g(T)),$$

which makes $TA[[T]]$ an abelian group. Notice that

$$f +_G i_g \circ f = 0.$$

Lemma 3.1. (a) For any formal group laws F and G, $\mathrm{Hom}(F, G)$ is an abelian group under $+_G$.
(b) End(F) becomes a ring with multiplication $f \circ g$.

Proof: (a) By using commutativity and associativity of $+_G$ we deduce that for $f, g \in \mathrm{Hom}(F, G)$,

$$\begin{aligned}(f +_G g)(F(X,Y)) &= G(f(F(X,Y), g(F(X,Y)) = G(G(f(X), f(Y)), G(g(X), g(Y)) \\ &= (f(X) +_G f(Y)) +_G (g(X) +_G g(Y)) \\ &= (f(X) +_G g(X)) +_G (f(Y) +_G g(Y)) \\ &= G((f +_G g)(X), (f +_G g)(Y)).\end{aligned}$$

Hence $f +_G g \in \mathrm{Hom}(F, G)$. We need to show that $i_G \circ f \in \mathrm{Hom}(F, G)$ (inverse), i.e. we want to show that $(i_G \circ f)(F(X,Y)) = G((i_G \circ f)(X), (i_G \circ f)(Y))$. Since f is a homomorphism and we have associativity,

$$(i_G \circ f)(F(X,Y)) = i_G(G(f(X), f(Y));$$
$$G((i_G \circ f)(X), (i_G \circ f)(Y)) = G(i_G(f(X)), i_G(f(Y))).$$

So it suffices to show that $i_G(G(f(X), f(Y))) = G(i_G(f(X)), i_G(f(Y)))$. By the axioms, the left hand side gives us that

$$G(G(f(X), f(Y)), i_G(G(f(X), f(Y)))) = 0.$$

Notice that

$$\begin{aligned}G(G(f(X), f(Y)), G(i_G(f(X)), i_G(f(Y)))) &= (f(X) +_G f(Y)) +_G (i_G(f(X)) +_G i_G(f(Y)) \\ &= (f(X) +_G i_G(f(X))) +_G (f(Y) + i_G(f(Y))) = 0,\end{aligned}$$

and hence we get the equality by uniqueness of the inverse i_G. Since $0 \in \mathrm{Hom}(F, G)$, we get the claim.
(b) We already have that composition is associative and the identity being X, so we only need to show distributivity. For $f, g, h \in \mathrm{End}(F)$,

$$f \circ (g +_F h) = f(F(g(T), h(T))) = F((f \circ g)(T), (f \circ h)(T)) = (f \circ g) +_F (f \circ h);$$
$$(f +_F g) \circ h = (F(f(T), g(T))(h(T)) = F((f \circ h)(T), (g \circ h)(T)) = (f \circ h) +_F (g \circ h).$$

$\square$

§0. Notations. K nonarchimedean local field with integer A. Let $\mathfrak{m} \trianglelefteq A$ denote the maximal ideal and suppose $k = A/\mathfrak{m}$ is of characteristic $p > 0$. Let $q = |k|$.

§1. Formal Modules. Let R be a commutative ring.

- A formal R-module is a pair $(F, [-])$ consisting of a commutative formal group $F \in R[[X,Y]]$ together with a ring homomorphism
$$[-] : R \longrightarrow \mathrm{End}(F).$$

- Given formal R-modules $M_1 = (F_1, [-]_1)$ and $M_2 = (F_2, [-]_2)$ a homomorphism $M_1 \longrightarrow M_2$ is a homomorphism of formal groups $\phi : F_1 \longrightarrow F_2$ such that if $r \in R$ then
$$\phi([r]_1(T)) = [r]_2(\phi(T))$$
The definition of isomorphism is the usual one.

§2. Lubin-Tate Formal Groups.

Definition: Let $\pi \in A$ be a uniformiser. A Lubin-Tate Formal Group for π is a formal A-module $(F, [-])$ such that

- LTG 1: $[\pi] \equiv T^q \pmod{\pi}$ ("π acts by a lift of Frobenius.")
- LTG 2: $[a] \equiv aT \pmod{T^2}$ ("F admits a ring of integers worth of endomorphisms")

12/03 . 2

Remarks: Let $(F, [-])$ be a Lubin-Tate Formal group for π.

- Reducing the coefficients of F mod. π, we obtain a formal group $\bar{F} \in \mathbb{F}_q[\![X,Y]\!]$. For $a \in A$ arbitrary, $\overline{[a](T)} := [a](T) \pmod{\pi}$ may not define an endomorphism of $\bar{F}$, but $\underbrace{\overline{[\pi](T)}}_{= T^q}$ certainly does.
- LTG2 $\Rightarrow$ the map $A \xrightarrow{[-]} \mathrm{End}(F)$ is injective.

§3. Technical stuff.

Question: Let $\pi \in A$ be a uniformiser. Under what hypothesis on the pair (K, π) does there exists a Lubin-Tate formal group for π? If such a Lubin-Tate formal group exists, then is it unique or can there be multiple Lubin-Tates associated to the same π? If there are many Lubin-Tate formal groups for the same π, then what are the homomorphisms between them? Can we say which of these are isomorphisms?

All the questions above admit precise and complete answers, however we need to do some technical work to prove them.

- For each uniformiser $\pi \in A$, let $\mathcal{F}_\pi = \left\{ h \in A[\![T]\!] \;\middle|\; \begin{array}{l} h \equiv \pi T \pmod{T^2} \\ h \equiv T^q \pmod{\pi} \end{array} \right\}$

Observation: A formal A-module $(F, [-])$ is Lubin-Tate for π only if $[\pi] \in \mathcal{F}_\pi$. So we can refine our first question by asking. "For $h \in \mathcal{F}_\pi$ fixed, how many Lubin Tates $(F, [-])$

are there such that $[\pi] = h$". The answer is <u>exactly one</u>! ③
This is proved in the first corollary below. The point is that the set $\mathcal{F}_\pi$ naturally parametrises the space of Lubin-Tate formal groups for π.

<u>Lemma:</u> Let $\pi \in A$ be a uniformizer and fix $f, g \in \mathcal{F}_\pi$.
If $\ell \in A[X_1, \dots, X_n]$ is homogeneous of degree 1, then there exists a <u>unique</u> power series $\Phi_\ell(f,g)(X_1, \dots, X_n) \in A[\![X_1, \dots, X_n]\!]$ such that the following conditions hold:

- $(\mathrm{I})_\ell$ $\Phi_\ell(f,g)(X_1, \dots, X_n) = \ell(X_1, \dots, X_n) + \left(\begin{smallmatrix}\text{terms of degree}\\ \geq 2\end{smallmatrix}\right)$.
- $(\mathrm{II})_{f,g}$ $f(\Phi_\ell(f,g)(X_1, \dots, X_n)) = \Phi_\ell(f,g)(g(X_1), \dots, g(X_n))$.

PROOF:
Assume ℓ is homogeneous of degree 1. By passing to sequences of partial sums we can reduce to proving ...
<u>To show</u>: $\exists!$ sequence $(\phi_1, \phi_2, \dots)$ in $A[X_1, \dots, X_n]$ such that for all $r \in \mathbb{Z}^+$, the following conditions hold.

$(0)_r$ ϕ_r is a poly. of degree $\leq r$.
$(\mathrm{I})_r$ $\phi_r - \phi_{r-1}$ is homogeneous degree r. (Note $\phi_0 := 0$).
$(\mathrm{II})_r$ $\phi_r = \ell + \left(\begin{smallmatrix}\text{terms of degree}\\ \geq 2\end{smallmatrix}\right)$

$(\mathrm{III})_r$ $f(\phi_r(X_1, \dots, X_n)) = \phi_r(g(X_1), \dots, g(X_n)) + \left(\begin{smallmatrix}\text{terms of}\\ \text{deg.} \geq r+1\end{smallmatrix}\right)$.

To simplify notation write $\mathcal{O}(d) = \left(\begin{matrix}\text{terms of}\\ \text{degree } \geq d\end{matrix}\right)$. 12/03. ④

$\boxed{\text{Base case } (r=1).}$ $\left.\begin{matrix}\text{(0)}_1 \Rightarrow \phi_1 \text{ is a poly. of degree } \leq 1 \\ \text{(II)}_1 \Rightarrow \phi_1 = \ell + \mathcal{O}(2)\end{matrix}\right\} \Rightarrow \phi_1 = \ell.$

To show: $\phi_1 = \ell$ satisfies (I)$_1$ and (III)$_1$.

(I)$_1$ is automatic since $\phi_0 = 0$.

For the proof of (III)$_1$, write $\ell = \sum a_i X_i$ for $a_i \in A$.

Then $f(\ell(x_1, \ldots, x_n)) = f(\sum a_i X_i) = \pi \sum a_i X_i + \mathcal{O}(2)$

$= \sum a_i (\pi X_i + \mathcal{O}(2)) + \mathcal{O}(2)$

$= \sum a_i\, g(x_i) + \mathcal{O}(2)$

$= \ell(g(x_1), \ldots, g(x_n)) + \mathcal{O}(2)$.

$\boxed{\text{Induction Step.}}$ Fix $r \geq 1$. Suppose ϕ_r is constructed.

Show: $\exists!\ \phi_{r+1} \in A[X_1, \ldots, X_n]$ satisfying (0)$_{r+1}, \ldots,$ (III)$_{r+1}$.

$\left.\begin{matrix}\text{(0)}_{r+1} \\ \text{(I)}_{r+1}\end{matrix}\right\} \Rightarrow \phi_{r+1} = \phi_r + Q$ where Q homog. deg. $r+1$

$\Rightarrow$ (II)$_{r+1}$ is satisfied.

Show: $\exists!\ Q \in A[X_1, \ldots, X_n]$ homog. degree $r+1$ such that $\phi_{r+1} := \phi_r + Q$

satisfies (III)$_{r+1}$.

For $Q \in K[X_1, \ldots, X_n]$, the expression $\phi_r + Q$ saties.

(III)$_{r+1}$ $\Leftrightarrow \ldots$

$$\cdots f(\phi_r(X_1,\dots,X_n)+Q(X_1,\dots,X_n)) = \phi_r(g(X_1),\dots,g(X_n)) + Q(g(X_1),\dots,g(X_n)) + O(r+2)$$

$$\Longleftrightarrow f(\phi_r(X_1,\dots,X_n)) + \pi Q(X_1,\dots,X_n) + O(r+2) = \phi_r(g(X_1),\dots,g(X_n)) + Q(\pi X_1,\dots,\pi X_n) + O(r+2)$$

$$\Longleftrightarrow \underbrace{f(\phi_r(X_1,\dots,X_n)) - \phi_r(g(X_1),\dots,g(X_n))}_{\left((\mathrm{III})_r \Rightarrow \text{ concentrated in degrees } \geq r+1\right)} \underset{(*)}{=} Q(\pi X_1,\dots,\pi X_n) - Q(X_1,\dots,X_n) + O(r+2).$$

So $(*) \Rightarrow Q$ concentrated in degree's $\geq r+1$. Hence if we impose the condition that Q be homogeneous of degree $r+1$, then $(*)$ becomes

$$\frac{f(\phi_r(X_1,\dots,X_n)) - \phi_r(g(X_1),\dots,g(X_n))}{\pi(\pi^r-1)} = Q + O(r+2)$$

and Q is uniquely determined as a poly. in $K[X_1,\dots,X_n]_{(r+1)}$.

By the fact that A is complete, $\frac{1}{\pi^r-1} \in A$.

Moreover, $f(\phi_r(X_1,\dots,X_n)) - \phi_r(g(X_1),\dots,g(X_n))$

$$\equiv \phi_r(X_1,\dots,X_n)^q - \phi_r(X_1^q,\dots,X_n^q) \pmod{\pi}$$

$$\equiv \phi_r(X_1,\dots,X_n)^q - \phi_r(X_1,\dots,X_n)^q \pmod{\pi}$$

$$\equiv 0 \pmod{\pi}$$

Hence $\dfrac{f(\phi_r(X_1,\dots,X_n)) - \phi_r(g(X_1),\dots,g(X_n))}{\pi(\pi^r-1)} \in A[X_1,\dots,X_n]$.

$\Longrightarrow Q \in A[X_1,\dots,X_n]_{(r+1)}$ ~~and is unique with~~ ∎

Corollary 1. Let $\pi \in A$ be a uniformizer and fix $\varphi \in \mathcal{F}_\pi$. Then

(i) The power series $F_\varphi := \Phi_{X+Y}(\varphi,\varphi)$ is the unique formal group law over A such that $\varphi \in \mathrm{End}_{\mathbb{Z}}(F_\varphi)$

(ii) The map $A \xrightarrow{[-]_\varphi} \mathrm{End}_{\mathbb{Z}}(F_\varphi)$, $[a]_\varphi := \Phi_{aT}(\varphi,\varphi)$ is the unique ring homomorphism such that $[\pi]_\varphi = \varphi$ and $[a]_\varphi = aT + O(2)$ $\forall\, a \in A$.

In particular, the formal A-module $(F_\varphi, [-]_\varphi)$ is Lubin-Tate for π, and $(F_\varphi, [-]_\varphi)$ is the unique Lubin-Tate formal group such that $[\pi]_\varphi = \varphi$.

Proof: If $G \in A[\![X,Y]\!]$ is a formal group over A such that $\varphi \in \mathrm{End}_{\mathbb{Z}}(G)$, then G satisfies I_{X+Y} and $\mathrm{II}_{\varphi,\varphi}$.

Hence the uniqueness statement of the lemma gives that $G = F_\varphi$.

Thus to prove (i), it suffices to prove F_φ satisfies.

(a) $F_\varphi(X,Y) = F_\varphi(Y,X)$.

(b) $F_\varphi(X, F_\varphi(Y,Z)) = F_\varphi(F_\varphi(X,Y),Z)$

(a). Let $G = F_\varphi(Y, X)$. Then $G(X,Y) = Y + X + O(2)$ and so G satisfies $(\mathrm{I})_{X+Y}$. Similarly.

$$\varphi(G(X,Y)) = \varphi(F_\varphi(Y,X)) = F_\varphi(\varphi(Y), \varphi(X))$$
$$= G(\varphi(X), \varphi(Y)).$$ So G satisfies $(\mathrm{II})_{\varphi,\varphi}$.

Hence $F_\varphi(Y,X) = G(X,Y) \overset{\text{Uniqueness.}}{=} F_\varphi(X,Y)$

(b) Let $H_1(X,Y,Z) = F_\varphi(X, F_\varphi(Y,Z))$, $H_2(X,Y,Z) = F_\varphi(F_\varphi(X,Y), Z)$

We claim H_1 and H_2 both satisfy $(\mathrm{I})_{X+Y+Z}$ and $(\mathrm{II})_{\varphi,\varphi}$

- $H_1(X,Y,Z) = X + F_\varphi(Y,Z) + O(2) = X + Y + Z + O(2)$,

  So H_1 satisfies $(\mathrm{I})_{X+Y+Z}$.

- $\varphi(H_1(X,Y,Z)) = \varphi(F_\varphi(X, F_\varphi(Y,Z))) = F_\varphi(\varphi(X), \varphi(F_\varphi(Y,Z)))$

$$= F_\varphi(\varphi(X), F_\varphi(\varphi(Y), \varphi(Z)))$$
$$= H_1(\varphi(X), \varphi(Y), \varphi(Z))$$

So H_1 satisfies $(\mathrm{II})_{\varphi,\varphi}$. The proofs for H_2 are exactly parallel. Hence $H_1 = H_2$ by uniqueness. ■ (i)

We will deduce (ii) from the following more general result, this will be of use in a later corollary.

Proposition: For $\pi \in A$ a uniformizer and $\varphi, \psi \in \mathcal{F}_\pi$ and $a \in A$, define $[a]_{\psi,\varphi} := \Phi_{aT}(\psi, \varphi)$. The following hold: ①. If $\varphi, \psi \in \mathcal{F}_\pi$ and $a \in A$, $[a]_{\psi,\varphi}$ is a homomorphism of formal groups $[a]_{\psi,\varphi} : F_\varphi \longrightarrow F_\psi$.

②. If $\varphi, \psi, \rho \in \mathcal{F}_\pi$ and $a, b \in A$, then

$$(*)\quad [a+b]_{\psi,\varphi} = [a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi}$$

(F_ψ endows $\mathrm{Hom}(F_\varphi, F_\psi)$ w/ an addition $+_{F_\psi}$ (Last Time).)

$$(**)\quad [ab]_{\rho,\varphi} = [a]_{\rho,\psi} \circ [b]_{\psi,\varphi}$$

Deduction of (ii). As we've defined things $[a]_\varphi = [a]_{\varphi,\varphi}$ for all $a \in A$. So part ① of the proposition implies that $[-]_\varphi : A \longrightarrow \mathrm{End}_{\mathbb{Z}}(F_\varphi)$ is well defined as a map of sets. By the uniqueness statement in the lemma $\Phi_{\pi T}(\varphi, \varphi) = \varphi$. So $[\pi]_\varphi := \Phi_{\pi T}(\varphi, \varphi) = \varphi$ and $[-]_\varphi$ satisfies the conditions of (ii). Again the uniqueness statement in the lemma implies that it is the unique set map satisfying these conditions.

$$\left(\begin{array}{l} \cdot\ [\pi]_\varphi = \varphi \\ \cdot\ [a]_\varphi = aT + O(2)\ \forall a. \end{array}\right)$$

So all that remains is to prove $[-]_\varphi$ defines a ring homomorphism.

The uniqueness statement in the lemma gives that $[1]_\varphi = T$ and $[0]_\varphi = 0$. The additivity and multiplicativity of $[-]_\varphi$ are got by specialising statement (2) of the proposition to the case of $\varphi = \psi = \rho$. ▨ (ii)

Proof of Proposition:

(1) It suffices to show that

$$[a]_{\psi,\varphi}(F_\varphi(X,Y)) = F_\psi([a]_{\psi,\varphi}(X), [a]_{\psi,\varphi}(Y))$$

Since F_φ and F_ψ are formal groups, and $[a]_{\psi,\varphi}$ satisfies $(\mathrm{I})_{aT}$, the LHS and RHS of the equality satisfy $(\mathrm{I})_{aX+aY}$.

The LHS satisfies $(\mathrm{II})_{\psi,\varphi}$ since

$$\psi([a]_{\psi,\varphi}(F_\varphi(X,Y))) = [a]_{\psi,\varphi}(\varphi(F_\varphi(X,Y)))$$
$$= [a]_{\psi,\varphi}(F_\varphi(\varphi(X), \varphi(Y))).$$

By a parallel calculation, the RHS also satisfies $(\mathrm{II})_{\psi,\varphi}$. Hence the uniqueness statement of the lemma $\Rightarrow$ (1).

(2). We check (*) $[a+b]_{\psi,\varphi} = [a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi}$. The proof of (**) is similar.

Since $([a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi})(T) = F_\psi([a]_{\psi,\varphi}(T), [b]_{\psi,\varphi}(T))$
$= F_\psi(aT + O(2), bT + O(2)) = (a+b)T + O(2)$, we

have that $[a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi}$ satisfies $\textcircled{\text{I}}_{(a+b)T}$.

Moreover $\psi(([a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi})(T))$

$$= \psi(F_\psi([a]_{\psi,\varphi}(T), [b]_{\psi,\varphi}(T)))$$

$$= F_\psi(\psi([a]_{\psi,\varphi}(T)), \psi([b]_{\psi,\varphi}(T)))$$

$$= F_\psi([a]_{\psi,\varphi}(\varphi(T)), [b]_{\psi,\varphi}(\varphi(T)))$$

$$= ([a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi})(\varphi(T)). \Rightarrow [a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi} \text{ satisfies } \textcircled{\text{II}}_{\psi,\varphi}.$$

Hence $[a]_{\psi,\varphi} +_{F_\psi} [b]_{\psi,\varphi} = [a+b]_{\psi,\varphi}$ by the uniqueness statement of the lemma. ▨ (Proposition)

▨ (Corollary 1.)

Example: (The multiplicative group over $\mathbb{Q}_p$).

Let $\mathbb{G}_m(\mathbb{Q}_p) = (X+Y+XY, [a] := (1+T)^a - 1)$

where $(1+T)^a = \sum_{m \geq 0} \binom{a}{m} \cdot T^m$ with $\binom{a}{m} = \frac{a(a-1)\cdot\ldots\cdot(a-m+1)}{m(m-1)\cdot\ldots\cdot 1}$

[Note: for $a \in \mathbb{Z}$, $a \mapsto \binom{a}{m}$ is p-adically continuous and $m \geq 0$.

so $\binom{a}{m} \in \mathbb{Z}_p$ $\forall a \in \mathbb{Z}_p$

$\Rightarrow [a] \in \mathbb{Z}_p[[T]]$ $\forall a \in \mathbb{Z}_p$].

In the notation of Corollary 1., we claim that

$\mathbb{G}_m(\mathbb{Q}_p) = (F_\varphi, [\cdot]_\varphi)$ for $\varphi = (1+T)^p - 1$.

Checked last time.

By Corollary 1 (i)

$$\left(F_\varphi = X+Y+XY\right) \Leftrightarrow \left(\begin{array}{c} X+Y+XY \text{ is a formal group law} \\ \text{and} \\ \varphi(X+Y+XY) = \varphi(X)+\varphi(Y)+\varphi(X)\varphi(Y) \end{array}\right)$$

Thus by Corollary 1. (ii), showing $[a]_\varphi \overset{(\star)}{=} \underbrace{(1+T)^a - 1}$ will complete the proof of the claim. The coefficients of the above power series ~~vary~~ varies p-adically continuously with a. So it suffices to check $(\star)$ when a is an integer. This amounts to showing that $(1+T)^a - 1$ satisfies I_{aT} and $\text{II}_{\varphi,\varphi}$ for $a \in \mathbb{Z}$.

I_{aT} is immediate from the fact that $\binom{a}{1} = a$.

For $\text{II}_{\varphi,\varphi}$;
$$\begin{aligned} \varphi((1+T)^a - 1) &= (1+(1+T)^a - 1)^p - 1 \\ &= (1+(1+T)^p - 1)^a - 1 \\ &= (1+\varphi(T))^a - 1. \end{aligned}$$
$\blacksquare$ (Example).

<u>Corollary 2</u>: $\pi \in A$ a uniformiser. $\varphi, \psi \in \mathcal{F}_\pi$.

(a) If $a \in A$, then $[a]_{\psi,\varphi} := \Phi_{aT}(\psi,\varphi)$ defines a homomorphism of formal A-modules $(F_\varphi, [-]_\varphi) \to (F_\psi, [-]_\psi)$.

(b) If $u \in A^\times$, then $[u]_{\psi,\varphi}$ is an isomorphism with inverse $[u^{-1}]_{\varphi,\psi}$. In particular, there is a canonical formal A-module isomorphism $[1]_{\psi,\varphi} : F_\varphi \longrightarrow F_\psi$.

(Corollary 2) $\Rightarrow$ "It makes sense to talk about <u>the</u> Lubin-Tate formal group associated to π".

Proof of Corollary 2. Part (b) follows from $1/12/03$. (12)
corollary 2 (a) combined with Proposition (2) (**)
and the fact that $[1]_{\varphi,\varphi} = \mathrm{id}_{F_\varphi}$. So it suffices to
prove (a). The fact that $[a]_{\psi,\varphi}$ defines a homomorphism
of formal groups was proven in Proposition (1). So it
remains to check that $\forall\ b \in A$,

$$[a]_{\psi,\varphi}([b]_\varphi(T)) = [b]_\psi([a]_{\psi,\varphi}(T)). \quad (**)$$

Again this follows from Proposition (2) together with the
observation that A is commutative and $[b]_\psi = [b]_{\psi,\psi}$
and $[b]_\varphi = [b]_{\varphi,\varphi}$. ▨ (Corollary 2.)

Construction of K_π

Bharatha M. Rankothge

Let K be a non-arch local field with $q = |k_K|$ (a power of p).

We have $K^{ab} = K_\pi . K^{un}$, where $K^{un} = \bigcup_{p \nmid m} K[\mu_m]$

for μ_m = set of m^{th} roots of 1 in $\bar{K}$.

Our goal is to understand K_π.

Plan: Define the following objects:

$$\Lambda_f \dashrightarrow \Lambda_n \dashrightarrow K[\Lambda_n] = K_{\pi,n} \dashrightarrow K_\pi$$

Λ_f: $\mathcal{O}_K$ module. (using Lubin-Tate formal gps.)

Λ_n: sub module.

$K_\pi = \bigcup K_{\pi,n}$.

$$\begin{array}{c} K_\pi \\ \Big| \text{ tot. ram.} \\ K \end{array}$$

$\boxed{\Lambda_f}$ Consider $\bar{K}$ over K. $|\cdot|$ on K extends uniquely to $\bar{K}$.

$\pi \in \mathcal{O}_K$ uniformizer.

$f \in \mathcal{F}_\pi$ i.e. $f(x) \in \mathcal{O}_K[[X]]$ s.t.

$f(x) = \pi X$ + terms of deg ≥ 2

$f(x) \equiv x^q \pmod{\pi}$

Given $f \in F_\pi$, $\exists$ a unique Lubin-Tate formal group law F_f

with coeffs in $\mathcal{O}_K$

and admitting f as an endomorphism.

$\Lambda_f := \{\alpha \in \bar{K} : |\alpha| < 1\}$ (as a set.)

Ab. gp. structure: $\alpha +_{\Lambda_f} \beta := \alpha +_{F_f} \beta = F_f(\alpha, \beta)$.

(converges) ✓

$\mathcal{O}_K$-mod structure: $a * \alpha = [a]_f(\alpha)$

(converges.) ✓

$\boxed{\Lambda_n}$

Λ_n = submodule of Λ_f of elts killed by $[\pi]_f^n$.

Rk: $f, g \in F_\pi$ then

$[1]_{g,f} : F_f \xrightarrow{\sim} F_g$

induces $\Lambda_f \xrightarrow{\sim} \Lambda_g$.

$[\pi]_f(T) = f(T) \Rightarrow$

$$\Lambda_n = \{\alpha \in \overline{K} : f^{(n)}(\alpha) = 0 \ , \ |\alpha| < 1\}.$$

$(f^{(n)} = \underbrace{f \circ \dots \circ f}_{n})$ using ⊛ take $f = \pi T + T^q$

Show: $\left.\begin{array}{l} f^n(\alpha) = 0 \\ \alpha \in \overline{K} \end{array}\right\} \Rightarrow |\alpha| < 1.$

$f^n(\alpha) = \alpha^{q^n} + \pi(\dots)$

α root of monic poly over $\mathcal{O}_K \Rightarrow |\alpha| \le 1$

Thm 4′, Ch. 2, Lorenz.

Then strong Δ ineq $\Rightarrow |\alpha| < 1$.

Then:

$$\Lambda_n = \{\alpha \in \overline{K} : f^n(\alpha) = 0\}.$$

Prop: (3.4) $\Lambda_n \cong \mathcal{O}_K/(\pi^n)$ as $\mathcal{O}_K$-modules.

Hence, $\mathrm{End}_{\mathcal{O}_K}(\Lambda_n) \cong \mathcal{O}_K/(\pi^n)$

$$\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) \cong \left(\mathcal{O}_K/(\pi^n)\right)^{\times}$$

$A := \mathcal{O}_K$.

Lemma: (3.3) M an A-module. $M_n := \ker(\pi^n : M \to M)$.

Assume: (a) M_1 has $q := |A/(\pi)|$ elts.

(b) $\pi : M \to M$ surj

Then, $M_n \cong A/(\pi^n)$; ($\Rightarrow$) M_n has q^n elts.

Note: ~~(f.g.)~~

~~Pf. of lemma:~~ (i) M_n torsion module over A by def.

A: PID with unique prime (upto conjugate)

if M_n f.g.

$$\Rightarrow M_n \cong A/(\pi^{n_1}) \oplus \cdots \oplus A/(\pi^{n_r})$$

$n_1 \le n_2 \le \cdots \le n_r$ (unique.)

~~Induction on n:~~ (2) $A/(\pi^n)$ has q^n elts:

Pf. of lemma:

Induction on n.

~~(a)~~ $n=1$ (a) $\#|M_1| = q = \#[A/(\pi)]$ and (1) (structure thm) above $\Rightarrow M_1 \cong A/(\pi)$.

Assume for $n-1$. Consider n.

Have:

$$0 \longrightarrow M_1 \xrightarrow{i} M_n \xrightarrow{\pi} M_{n-1} \longrightarrow 0$$

(inclusion)

$M_{n-1} \subset M_n$ clearly.

surj: $x \in M_{n-1} \subset M$

$\Rightarrow \exists y \in M$ s.t.

$x = \pi y$ by (b)

~~Then,~~ ~~=~~. And $y \in M_n$ b/c:

$$\pi^n(y) = \pi^{n-1}(\underbrace{\pi y}_{x}) = 0 \quad x \in M_{n-1}.$$

~~SES ie. ker π =~~

$x \in \ker \pi|_{M_n} \Leftrightarrow \pi x = 0 \Leftrightarrow x \in M_1$

$\ker \pi = \operatorname{im}(i)$

$\Rightarrow$ SES

Consequences:

$$M_{n-1} \cong M_n / i(M_1) \Rightarrow |M_n| = |M_{n-1}||M_1|$$
$$= q^{n-1} \cdot q = q^n.$$

and

$$\left.\begin{array}{l} M_1, M_{n-1} \text{ cyclic} \\ \pi \text{ surj } (M \xrightarrow{\pi} M) \end{array}\right\} \Rightarrow M_n \text{ cyclic}.$$

And

using Notes 1 & 2 above:

$$M_n \cong A/(\pi^n).$$

Pf. of prop:

Set $M = \Lambda_f$.

Want:

a) $M_1 = \ker(\pi) : \Lambda_f \longrightarrow \Lambda_f$ has q elts.

i.e.

f has q distinct roots.

b) $\pi : \Lambda_f \longrightarrow \Lambda_f$ is surj.

i.e.

$\forall\ \alpha \in \overline{K}$, $|\alpha| < 1$,

$\exists \beta$ s.t. $f(\beta) - \alpha = 0$ and $|\beta| < 1$.

(a). ~~$\alpha\in\bar{K}$~~ $f(x) = x^q + \pi x = x\,(x^{q-1}+\pi).$

$$\underbrace{x^{q-1}+\pi}_{\text{differentiate}} \longrightarrow (q-1)\,x^{q-2}$$

$\Big\}$ $x^{q-1}+\pi$ separable with non zero roots.

$\Downarrow$

$x^q+\pi X$ separable.

(b) $\alpha\in\bar{K},\quad |\alpha|<1.$

$f(T)-\alpha = T^q+\pi T-\alpha$ has a root $\beta\in\bar{K}.$

then,

$$\left.\begin{array}{l}\beta^q+\pi\beta-\alpha=0\\ |\pi|<,\ |\alpha|<1\end{array}\right\}\ \beta \text{ integral over } \mathcal{O}_K.$$

$\Rightarrow |\beta|\le 1.$

$\uparrow$

Thm 4', ch 23 (Lorenz).

Then, $|\beta^q| \le \max\{|\pi\beta|, |\alpha|\} < 1$

$\Rightarrow |\beta|<1.$

So, $\Lambda_n \cong \mathcal{O}_K/(\pi^n)$ by lemma 3.3.

And $\mathrm{End}_{\mathcal{O}_K}(\Lambda_n) \cong \mathrm{End}_{\mathcal{O}_K}(\mathcal{O}_K/(\pi^n)) \cong \mathcal{O}_K/(\pi^n)$.

b/c. $\gamma \in \mathrm{End}_{\mathcal{O}_K}(\mathcal{O}_K/(\pi^n))$ is det. by

$$\gamma : \underset{\in \mathcal{O}_K}{1} \longmapsto r \in \mathcal{O}_K.$$
$$\pi^n \longmapsto 0.$$

Taking units,

$$\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_n) \cong \left(\mathcal{O}_K/(\pi^n)\right)^{\times}.$$

$\boxtimes$

<u>Lemma: (3.5)</u>

L | Fin, Galois (G) K local.

$F \in \mathcal{O}_K[[X_1, \dots, X_n]]$

$\alpha_1, \dots, \alpha_n \in \mathfrak{m}_L$

$\Rightarrow F(\tau\alpha_1, \dots, \tau\alpha_n) = \tau(F(\alpha_1 \dots \alpha_n))$ $\forall \tau \in G$.

<u>Pf:-</u> <u>F poly</u>: follows from τ fixes $\mathcal{O}_K \subset K$.

$|\tau\alpha| = |\alpha|$ $\forall \alpha \in L$ b/c $|\cdot|$ extends uniquely to L. (Thm 4').

$\Rightarrow \tau$ cont's. $\Rightarrow \tau$ preserves limits.

~~F_m := by~~ Def F_m by

$$F = F_m + \text{terms of deg} \geq m+1$$

$$\tau(F(\alpha_1, \ldots)) = \tau\left(\lim_{m \to \infty} F_m(\alpha_1, \ldots)\right)$$

$$= \lim_{m \to \infty} \tau F_m(\alpha_1, \ldots)$$

$$= \lim_{m \to \infty} F_m(\tau\alpha_1, \ldots)$$

$$= F(\tau\alpha_1, \ldots) \qquad \boxtimes$$

$\boxed{\text{Thm}}$ (3.6) $K_{\pi,n} := K[\Lambda_n] \subset \bar{K}$, $A = \mathcal{O}_K$.

$\boxed{K_{\pi,n}}$

(a) $K_{\pi,n} \,|\, K$ tot. ram., deg $(q-1)q^{n-1}$.

(b) $A \cap \Lambda_n$ defines.

$$(A/\mathfrak{m}^n)^\times \longrightarrow \underbrace{\mathrm{Gal}(K_{\pi,n}/K)}_{\Rightarrow \text{ ab.}}.$$

(c) $\forall n$, π is a norm from $K_{\pi,n}$.

Pf: $f(T) = \pi T + T^q$, π_1 a root of $f(T)$

$\cdots \to \pi_n$ a root of $f(T) - \pi_{n-1}$.

$$K[\Lambda_n] \supset K[\pi_n] \supset \dots \supset K[\pi_1] \supset K.$$

Consider $(r \geq 2)$

$$\begin{array}{c} K[\pi_r] \\ \big| \\ K[\pi_{r-1}] \end{array} \qquad \phi_r(X) = X^q + \pi X - \pi_{r-1}$$

Eisenstein over $\mathcal{O}_{K[\pi_{r-1}]}$ of degree q.

$\to$ tot. ram of deg q.

$$\begin{array}{c} K[\pi_1] \\ \big| \\ K \end{array} \qquad \phi_1(X) = \frac{\pi X + X^q}{X} = \pi + X^{q-1}$$

Eisenstein of deg $q-1$.

$\to$ tot ram of deg $q-1$.

$$\begin{array}{c} K[\pi_n] \\ \big| \\ K \end{array} \quad \text{tot ram, deg } q^{n-1}(q-1).$$

Λ_n = roots of $f^{(n)}$ in $\bar{K}$

$\therefore$ $K[\Lambda_n]$ = splitting field of $f^{(n)}$.

$\Rightarrow$ $\mathrm{Gal}(K[\Lambda_n]/K) <$ Group of permutations of Λ_n.

Lemma (3.5) $\Rightarrow$

$\tau \in \mathrm{Gal}(K[\Lambda_n]/K)$ acts on Λ_n as an A-mod isom.

$$\therefore \mathrm{Gal}(K[\Lambda_n]/K) \hookrightarrow \mathrm{Aut}_A(\Lambda_n) = (A/(\pi^n))^\times.$$

$$|(A/(\pi^n))^\times| = \cancel{q(q-1)}\ q^{n-1}(q-1).$$

b/c $U^{(n)} \subseteq \dots \subseteq U^{(1)} \subseteq U^{(0)} = A$.

$$\left|U^{(0)}/U^{(n)}\right| = \underbrace{\left|U^{(0)}/U^{(1)}\right|}_{\underbrace{|(\mathcal{O}/(\pi))^\times|}_{q-1}} \underbrace{\underbrace{\left|U^{(1)}/U^{(2)}\right|}_{\underbrace{|(\mathcal{O}/(\pi))^*|}_{q}} \cdots \left|U^{(n-1)}/U^{(n)}\right|}_{q \ \cdots \ q,\ n-1}$$

$$\therefore (q-1)q^{n-1} \geq |\mathrm{Gal}(K[\Lambda_n]/K)|$$

$$= [K[\Lambda_n]:K] \geq [K[\pi_n]:K] = (q-1)q^{n-1}.$$

$\Rightarrow$ equality. $\Rightarrow \mathrm{Gal}(K[\Lambda_n]/K) \cong (A/(\pi^n))^\times$ & $K[\Lambda_n] = K[\pi_n]$

(c) $f^{[n]}(T) = \left(f/T\right) \circ \underbrace{f \circ \cdots \circ f}_{n-1}$

$f^{[n]}(T) = \pi + \cdots + T^{(q-1)q^{n-1}}$ $\longleftarrow$ monic, $\deg = [K[\pi_n] : K]$

$f^{[n]}(\pi_n) = f^{[n-1]}(\pi_{n-1}) = \cdots = f(\pi_1) = 0.$

$\Downarrow$

$f^{[n]}$ mini poly of π_n / K.

$\Rightarrow \mathrm{Nm}_{K[\Lambda_n]/K}(\pi_n) = (-1)^{q^{n-1}(q-1)} \pi$

$q^{n-1}(q-1)$ even ~~when $n \geq 2$~~.

unless $2 \mid q$, $n = 1$.

when, $n = 1$,

Λ_1 = roots of $T(\pi + T)$

$\Rightarrow K[\Lambda_1] = K \rightarrow \pi$ is a norm.