Lecture 23-Formal Groups

November 27, 2018

Throughout this lecture, we fix an algebraically closed perfectoid field $C^\flat$ of characteristic p. Let X denote the Fargues-Fontaine curve, given by

$$X = \mathrm{Proj}(\bigoplus_{m \geq 0} B^{\varphi = p^m}).$$

Let E be a finite extension of $\mathbf{Q}_p$, so that $\mathbf{Q}_p \subseteq E_0 \subseteq E$ where $\mathbf{Q}_p \hookrightarrow E_0$ is an unramified extension of degree d and $E_0 \hookrightarrow E$ is a totally ramified extension of degree e. Let $\mathcal{O}_E$ denote the ring of integers of E and let $\pi \in \mathcal{O}_E$ be a uniformizer. Our goal in this lecture is to explain the following result, which was stated without proof in the last lecture:

Theorem 1. *Let x be a closed point of X_E, corresponding to a subset $S \subseteq Y_E^\circ$ which is an orbit for the action of $\varphi^{d\mathbf{Z}}$. Then there exists an element $f \in (B \otimes_{E_0} E)^{\varphi^d = \pi}$ satisfying*

$$\mathrm{ord}_{\overline{y}}(f) = \begin{cases} 1 & \text{if } \overline{y} \in S \\ 0 & \text{otherwise.} \end{cases}$$

In the case $E = \mathbf{Q}_p$, we can take $\pi = p$ and choose f be an element of the form $\log([\epsilon])$, for some $\epsilon \in 1 + \mathfrak{m}_C^\flat$. We would like to do something analogous for a general extension E of $\mathbf{Q}_p$. Note that the power series

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$$

has a special feature: for any completely valued field K of characteristic zero, $x \mapsto \log(x)$ induces a group homomorphism from the open unit disk $1 + \mathfrak{m}_K$ (regarded as an abelian group with respect to multiplication) to K (regarded as a group under addition). To generalize this, it is useful to examine other group structures on the open unit disk.

Definition 2. Let R be a commutative ring. A *formal group law* over R is a power series $F(u,v) \in R[[u,v]]$ satisfying the identities

$$F(0,u) = u \qquad F(u,v) = F(v,u) \qquad F(u, F(v,w)) = F(F(u,v),w).$$

Let F be a formal group law over R, and let A be a commutative R-algebra. Then, for any pair of nilpotent elements $u, v \in A$, we can evaluate the power series F on the elements u and v to obtain a new nilpotent element $F(u,v) \in A$. It follows from the above identities that the induced map

$$F : \{\text{Nilpotent elements of } A\} \times \{\text{Nilpotent elements of } A\} \to \{\text{Nilpotent elements of } A\}$$

is commutative and associative, and has a unit given by the zero element $0 \in A$. It therefore equips the set $\{\text{Nilpotent elements of } A\}$ with the structure of a commutative monoid, which we will denote by $\widehat{\mathbf{G}}(A)$. The construction $A \mapsto \widehat{\mathbf{G}}(A)$ determines a functor from commutative R-algebras to commutative monoids. We will refer to $\widehat{\mathbf{G}}$ as the *formal group associated to F*.

Exercise 3. Let F be a formal group law over a commutative ring R. Show that, for every commutative R-algebra A, the commutative monoid $\mathbf{G}(A)$ is a group.

Example 4 (The Formal Additive Group)**.** The power series $F(u,v) = u+v$ satisfies the requirements of Remark **??**, and therefore gives rise to a formal group law. It corresponds to the functor

$$\widehat{\mathbf{G}}_a : \{\text{Commutative } R\text{-algebras}\} \to \{\text{Abelian groups}\},$$

where $\widehat{\mathbf{G}}_a(A)$ is the collection of nilpotent elements of A, regarded as a group under addition. We refer to $\widehat{\mathbf{G}}_a$ as the *formal additive group*.

Example 5 (The Formal Multiplicative Group)**.** The power series $F(u,v) = u+v+uv$ satisfies the requirements of Remark **??**, and therefore gives rise to a formal group law. It corresponds to the functor

$$\widehat{\mathbf{G}}_m : \{\text{Commutative } R\text{-algebras}\} \to \{\text{Abelian groups}\},$$

where $\widehat{\mathbf{G}}_m(A)$ can be identified with the set $\{x \in A : \; x-1 \text{ is nilpotent}\}$, regarded as a group under multiplication. We refer to $\widehat{\mathbf{G}}_m$ as the *formal multiplicative group*.

Note that the formal additive group and the formal multiplicative group are different in general, but are isomorphic whenever the ground ring R has characteristic zero: in that case, we have natural isomorphisms

$$\widehat{\mathbf{G}}_m(A) \simeq \widehat{\mathbf{G}}_a(A)$$

$$1+x \mapsto \log(1+x) = x - \frac{x^2}{2} + \cdots .$$

This is a general phenomenon: over a ring of characteristic zero, all formal groups look like the formal additive group $\widehat{\mathbf{G}}_a$.

Remark 6. Let F be a formal group law over a commutative ring R and let $\widehat{\mathbf{G}}$ be the associated formal group. If we ignore the group structure on $\widehat{\mathbf{G}}$ (that is, if we think of $\widehat{\mathbf{G}}$ as a set-valued functor on the category of commutative R-algebras), then it is isomorphic to the formal affine line $\widehat{\mathbf{A}}^1 \simeq \mathrm{Spf}(R[[t]])$.

Suppose that F and F' are formal group laws, defining formal groups $\widehat{\mathbf{G}}$ and $\widehat{\mathbf{G}}'$, respectively. A *homomorphism of formal groups* from $\widehat{\mathbf{G}}$ and $\widehat{\mathbf{G}}'$ is a natural transformation of group-valued functors $H : \widehat{\mathbf{G}} \to \widehat{\mathbf{G}}'$. Ignoring the group structures, we can view H as a map of formal schemes from $\mathrm{Spf}(R[[t]])$ to itself which preserves the "origin" given by the vanishing locus of t. It follows that H is induced by a map of power series rings

$$R[[t]] \to R[[t]] \qquad t \mapsto h(t),$$

where $h(t) \in R[[t]]$ is a power series with vanishing constant term. The condition that this power series induces a group homomorphism can be written concretely as the formula

$$h(F(u,v)) = F'(h(u), h(v)).$$

We say that H is an *isomorphism of formal groups* if it is an isomorphism of group valued-functors, or equivalently if the power series $h(t) = c_1 t + c_2 t^2 + c_3 t^3 + \cdots$ has $c_1 \in R^\times$.

Definition 7. Let F be a formal group law over a commutative ring R, with associated formal group $\widehat{\mathbf{G}}$. A *logarithm* for F is an isomorphism of formal groups $\widehat{\mathbf{G}} \to \widehat{\mathbf{G}}_a$, given by a power series $h(t) = c_1 t + c_2 t^2 + \cdots$ which satisfies the identity

$$h(F(u,v)) = h(u) + h(v).$$

We further assume that $c_1 = 1$ (this is a normalization condition: it can always be arranged by multiplying the power series h by a scalar).

Proposition 8. *Let R be a commutative ring which contains the field $\mathbf{Q}$ of rational numbers. Then every formal group law $F(u,v)$ has a unique logarithm.*

Proof. Let us first prove uniqueness. Write $F(u,v) = \sum c_{i,j} u^i v^j$, so that $c_{1,0} = 1$. Set

$$f(v) = \frac{\partial F}{\partial u}(0,v) = \sum c_{1,j} v^j = 1 + c_{1,1} v + c_{1,2} v^2 + \cdots .$$

Let h be a logarithm for F, so that h satisfies the identity

$$h(F(u,v)) = h(u) + h(v).$$

Differentiating with respect to u and setting $u = 0$

$$f(v) h'(v) = \frac{\partial F}{\partial u}(0,v) h'(F(0,v)) = \frac{\partial h(F(u,v))}{\partial u}|_{u=0} = h'(0) = 1.$$

It follows that h must satisfy $h(0) = 0$ and $h'(v) = \frac{1}{f(v)}$, and is therefore uniquely determined.

To prove existence, we define h to be the unique power series satisfying the preceding identities, given formally by the formula

$$h(t) = \int_0^t \frac{1}{f(v)} dv.$$

We claim that h has the desired property: that is, that we have

$$h(F(u,v)) = h(u) + h(v).$$

Since $h(0) = 0$, this identity holds after setting $u = 0$. It will therefore suffice to check that it holds after differentiating with respect to u: that is, that we have an identity of power series

$$\frac{\partial F}{\partial u}(u,v) h'(F(u,v)) = h'(u)$$

or equivalently

$$\frac{\partial F}{\partial u}(u,v) f(u) = f(F(u,v)).$$

This follows from the associativity identity

$$F(F(t,u),v) = F(t, F(u,v))$$

by differentiating with respect to t and then setting $t = 0$. □

Construction 9. Let R be a commutative ring and let F be a formal group law over R. The associated formal group $\widehat{\mathbf{G}}$ might not be isomorphic to the formal additive group $\widehat{\mathbf{G}}_a$. However, after extending scalars to the ring $R_{\mathbf{Q}} = R \otimes \mathbf{Q}$ and applying Proposition 8, we deduce that there exists a unique power series $\log_F(t)$ with coefficients in $R_{\mathbf{Q}}$ such that $\log_F(t) \equiv t \pmod{t^2}$ and

$$\log_F(F(u,v)) = \log_F(u) + \log_F(v).$$

We refer to $\log_F(t)$ as the *logarithm of F*.

Remark 10. Let us assume that R is torsion-free, so that R can be identified with a subring of $R_{\mathbf{Q}}$. In general, the coefficients of the power series $\log_F$ do not belong to $R \subseteq R_{\mathbf{Q}}$: that is, they involve denominators. Inspecting the proof of Proposition 8, we see that these denominators arise from the process of integration. That is, if we set $f(v) = \frac{\partial F}{\partial u}(0,v)$, then $f(v) = 1$ so we can write $\frac{1}{f(v)} = 1 + a_1 v + a_2 v^2 + a_3 v^3 + \cdots$. We then have

$$\log_F(t) = t + \frac{a_1}{2} t^2 + \frac{a_2}{3} t^3 + \cdots .$$

In particular, the denominators occuring in the power series $\log_F(t)$ are "no worse" than the denominators which occur in the power series expansion for the usual logarithm: the coefficient of t^n belongs to $\frac{1}{n} R$.

Let R be a commutative ring. The formal additive group $\widehat{\mathbf{G}}_a$ has some additional structure: for every commutative R-algebra A, the set

$$\widehat{\mathbf{G}}_a(A) = \{\text{Nilpotent elements of } A\}$$

is not just an abelian group under addition, but an R-module. Given a formal group law F over R with associated formal group $\widehat{\mathbf{G}}$, we can attempt to use the logarithm $\log_F$ to transport this structure to $\widehat{\mathbf{G}}$.

Construction 11. Let R be a commutative ring and let F be a formal group over R. For each element $\lambda \in R$, let $[\lambda](t) \in R_{\mathbf{Q}}[[t]]$ be the power series given by the formula

$$\log_F^{-1}(\lambda \log_F(t)).$$

Exercise 12. Let R be a commutative ring and let F be a formal group over R. Show that the construction $(\lambda \in R) \mapsto ([\lambda](t) \in R_{\mathbf{Q}}[[t]])$ has the following properties:

- We have $[\lambda](t) \equiv \lambda t \pmod{t^2}$.
- For $\lambda, \mu \in R$, we have $[\lambda\mu](t) = [\lambda]([\mu](t))$. Similarly, we have $[1](t) = t$.
- For $\lambda, \mu \in R$, we have $[\lambda + \mu](t) = F([\lambda](t), [\mu](t))$. Similarly, we have $[0](t) = 0$.

Hint: we might as well replace R by $R_{\mathbf{Q}}$.

Exercise 13. Let R be a torsion-free commutative ring, let F be a formal group law over R, and let $\widehat{\mathbf{G}}$ be the associated formal group. Set

$$R_0 = \{\lambda \in R : [\lambda](t) \text{ has coefficients in } R\}.$$

Show that R_0 is a subring of R (combine Exercises 12 and 3).

Moreover, show that for any commutative algebra R-algebra A (which might not be torsion-free!), the abelian group $\widehat{\mathbf{G}}(A)$ has the structure of a module over R_0, where multiplication by $\lambda \in R_0$ is implemented by the map

$$(x \in \widehat{\mathbf{G}}(A) = \{\text{Nilpotent elements of } A\}) \mapsto ([\lambda](x) \in \widehat{\mathbf{G}}(A) = \{\text{Nilpotent elements of } A\}$$

In the situation of Exercise 13, we will say that the formal group $\widehat{\mathbf{G}}$ is a *formal R_0-module.* (When R is torsion-free, this is simply a *property* of a formal group over R, not an additional structure.)

As a tool for proving Theorem 1, we cite the following classical result:

Theorem 14 (Lubin-Tate)**.** *Let E be a finite extension of $\mathbf{Q}_p$, let $q = p^d$ be the order of the residue field of E, and let $\pi \in \mathcal{O}_E$ be a uniformizer. Let $f(t) \in \mathcal{O}_E[[t]]$ be any power series satisfying*

$$f(t) \equiv \pi t \pmod{t^2}$$

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

Then there is a unique formal group law $F(u, v) \in \mathcal{O}_E[[u, v]]$ satisfying

$$\pi \log_F(t) = \log_F(f(t))$$

(that is, so that $f(t)$ coincides with the power series $[\pi](t)$ of Construction 11). We will denote the associated formal group by $\widehat{\mathbf{G}}_{\mathrm{LT}}$ and refer to it as the Lubin-Tate formal group of E. Moreover, $\widehat{\mathbf{G}}_{\mathrm{LT}}$ is a formal $\mathcal{O}_E$-module (that is, the power series $[\lambda](t)$ has coefficients in $\mathcal{O}_E$ for each $\lambda \in \mathcal{O}_E$).

Remark 15. One can show that the formal group $\widehat{\mathbf{G}}_{\mathrm{LT}}$ depends only on E, and not on the choice of power series $f(t)$. However, we will not need this for our applications: it will be enough to fix any choice of power series $f(t)$ satisfying the congruences above, such as $f(t) = \pi t + t^q$.

Example 16. In the case $E = \mathbf{Q}_p$ and $\pi = p$, the multiplicative formal group law $F(u, v) = u + v + uv$ satisfies the requirements of Theorem 14 for the power series

$$f(t) = (1 + t)^p - 1 = pt + \cdots + pt^{p-1} + t^p.$$