Bondarko's work on local Galois modules

Part III: Formal Group Laws

Kevin Keating
Department of Mathematics
University of Florida

May 23, 2018

Formal Group Laws

Let K be a local field with perfect residue field $\overline{K}$. Let $\mathcal{O}_K$ be the ring of integers of K.

Definition

A formal group law over $\mathcal{O}_K$ is a series $F(X, Y) \in \mathcal{O}_K[[X, Y]]$ such that

$$\begin{aligned} F(X,Y) &= X + Y + \text{higher degree terms} \\ F(X,Y) &= F(Y,X) \\ F(X,0) &= X \\ F(F(X,Y),Z) &= F(X,F(Y,Z)). \end{aligned}$$

It follows that there is a unique series $[-1]_F(X) \in \mathcal{O}_K[[X]]$ such that

$$F(X,[-1]_F(X)) = F([-1]_F(X),X) = 0.$$

Examples of Formal Group Laws

The additive formal group law:

$$\mathbb{G}_a(X, Y) = X + Y$$

$$[-1]_{\mathbb{G}_a}(X) = -X$$

The multiplicative formal group law:

$$\begin{aligned} \mathbb{G}_m(X, Y) &= X + Y + XY \\ &= (1 + X)(1 + Y) - 1 \end{aligned}$$

$$\begin{aligned} [-1]_{\mathbb{G}_m}(X) &= (1 + X)^{-1} - 1 \\ &= -X + X^2 - X^3 + \cdots \end{aligned}$$

Formal group laws also arise naturally from elliptic curves, and in local class field theory (Lubin-Tate formal groups).

A Family of Examples of Formal Group Laws

Let $c \in \mathcal{O}_K$, and define

$$F_c(X, Y) = X + Y + cXY.$$

The first three conditions for a formal group law are clearly satisfied by F_c. In addition, we have

$$\begin{aligned} F_c(F_c(X, Y), Z) &= (X + Y + cXY) + Z + c(X + Y + cXY)Z \\ &= X + Y + Z + c(X + Y + Z) + c^2XYZ \\ &= X + (Y + Z + cYZ) + cX(Y + Z + cYZ) \\ &= F_c(X, F_c(Y, Z)). \end{aligned}$$

A Family of Examples of Formal Group Laws

Let $c \in \mathcal{O}_K$, and define

$$F_c(X, Y) = X + Y + cXY.$$

The first three conditions for a formal group law are clearly satisfied by F_c. In addition, we have

$$\begin{aligned} F_c(F_c(X, Y), Z) &= (X + Y + cXY) + Z + c(X + Y + cXY)Z \\ &= X + Y + Z + c(X + Y + Z) + c^2XYZ \\ &= X + (Y + Z + cYZ) + cX(Y + Z + cYZ) \\ &= F_c(X, F_c(Y, Z)). \end{aligned}$$

In fact if $c \neq 0$ then $F_c(X, Y) = c^{-1}\mathbb{G}_m(cX, cY)$.

The Height of a Formal Group Law

We define $[n]_F(X)$ recursively for $n \geq 1$ by $[1]_F(X) = X$ and $[n+1]_F(X) = F(X, [n]_F(X))$.

Let $\overline{F}(X, Y)$ denote the image of $F(X, Y)$ in $\overline{K}[[X, Y]]$. Then $\overline{F}(X, Y)$ is a formal group law over $\overline{K}$.

It is known that if $[p]_{\overline{F}}(X) \in \mathcal{O}_K[[X]]$ is nonzero then it has the form $[p]_{\overline{F}}(X) = \eta(X^{p^h})$ for some $h \geq 1$ and some

$$\eta(X) = c_1 X + c_2 X^2 + \cdots \in \overline{K}[[X]]$$

such that $c_1 \neq 0$.

Definition

If $[p]_{\overline{F}}(X) = \eta(X^{p^h})$ with $\eta'(0) \neq 0$ we say that $F(X, Y)$ has height h. If $[p]_{\overline{F}}(X) = 0$ we say $F(X, Y)$ has infinite height.

Examples of Heights

Since $[p]_{\overline{\mathbb{G}}_a}(X) = pX = 0$, $\mathbb{G}_a$ has infinite height.

Since $[p]_{\overline{\mathbb{G}}_m}(X) = (1+X)^p - 1 = X^p$, $\mathbb{G}_m$ has height 1.

If $c \in \mathcal{M}_K$ then $\overline{F}_c(X,Y) = \overline{\mathbb{G}}_a(X,Y)$, so $F_c(X,Y)$ has infinite height.

If $c \in \mathcal{O}_K^\times$ then $F_c(X,Y)$ has height 1.

Formal group laws associated to elliptic curves have height 1 or 2.

A Lubin-Tate formal group law associated to K has height $v_K(p)$.

The Depth of a Formal Group Law

Definition

Let $F(X,Y)$ be a formal group law over $\mathcal{O}_K$ and write

$$F(X,Y) = X + Y + \sum_{i,j\geq 1} a_{ij} X^i Y^j.$$

The depth of $F(X,Y)$ is

$$d(F) = \inf\left\{\frac{v_K(a_{ij})}{i+j-1} : i,j \geq 1\right\}.$$

We clearly have $d(F) \geq 0$. Furthermore, if $F(X,Y)$ has finite height then $d(F) = 0$.

Let $F(X,Y)$ be a formal group law over $\mathcal{O}_K$ and let $c \in \mathcal{O}_K \smallsetminus \{0\}$. Then $\tilde{F}(X,Y) := c^{-1}F(cX,cY)$ is a formal group law over $\mathcal{O}_K$, and $d(\tilde{F}) = d(F) + v_K(c)$.

Groups from Formal Group Laws

Let r be an integer such that $r > -d(F)$. For $\alpha, \beta \in \mathcal{M}_K^r$ set

$$\alpha +_F \beta = F(\alpha, \beta).$$

Since $d(F) + r > 0$, the series $F(\alpha, \beta)$ converges in K.

$\mathcal{M}_K^r$ with the operation $+_F$ is an abelian group. The identity element is 0, and the inverse of $\alpha \in \mathcal{M}_K^r$ is $[-1]_F(\alpha)$.

We denote the group $(\mathcal{M}_K^r, +_F)$ by $F(\mathcal{M}_K^r)$.

We can define subtraction in the abelian group $F(\mathcal{M}_K^r)$ by

$$\alpha -_F \beta = F(\alpha, [-1]_F(\beta)).$$

Kummer Extensions from Formal Group Laws

Let $F(X,Y)$ be a formal group law over $\mathcal{O}_K$. Set $r=1$ if $d(F)=0$ and $r=0$ if $d(F)>0$. Let T be a finite subgroup of $F(\mathcal{M}_K^r)$, and set

$$P_T(X)=\prod_{t\in T}(X-_F t)\in\mathcal{O}_K[[X]].$$

Let $q=|T|$; then q is a power of p.

Proposition

Let $a\in K$ with $v_K(a)=m$ and $p\nmid m$. Assume that $m/q>-d(F)$ and $m/q<v_K(t)$ for all $t\in T$. Then there is $y\in K^{sep}$ such that $P_T(y)=a$. If we choose y to have maximum valuation then $K(y)/K$ is a totally ramified Galois extension with $Gal(K(y)/K)\cong T$.

We say that $K(y)$ is a Kummer extension of K with respect to the formal group law $F(X,Y)$.

Kummer Extensions from Formal Group Laws . . .

We sketch the proof of the proposition under the assumption $v_K(a) > 0$.

The Weierstrass degree of $P_T(X) - a$ is q. By the Weierstrass preparation theorem we get $P_T(X) - a = u(X)f(X)$ with $u(X) \in \mathcal{O}_K[[X]]^\times$ and $f(X) \in \mathcal{O}_K[X]$ a distinguished polynomial of degree q.

For $t \in T$ we have $P_T(X +_F t) = P_T(X)$, and hence $P_T(y +_F t) = a$.

It follows that the set of roots of $f(X)$ is $\{y +_F t : t \in T\}$. Thus $K(y)$ is the splitting field of $f(X)$ over K, so $K(y)/K$ is Galois.

Kummer Extensions from Formal Group Laws . . .

Since $m/q < v_K(t)$ we get

$$v_{K(y)}(y +_F t) = v_{K(y)}(y) = m/q.$$

Hence $f(X)$ is irreducible over K.

It follows that there is an isomorphism $\theta : \mathrm{Gal}(K(y)/K) \to T$ defined by

$$\theta(\sigma) = \sigma(y) -_F y.$$

For $\sigma \in \mathrm{Gal}(L/K)$ set $t_\sigma = \theta(\sigma)$.

Diagonals and Semistable Extensions

Let L/K be a totally ramified Galois extension. Recall that for $\beta \in L \otimes_K L$ with $\beta \neq 0$ we defined

$$d(\beta) = \min\{i + j : [i, j] \in D(\beta)\}.$$

We also defined the diagonal of β to be

$$N(\beta) = \{[i, j] \in D(\beta) : i + j = d(\beta)\}.$$

Finally, we defined L/K to be semistable if there exists $\beta \in L \otimes_K L$ such that $\phi(\beta) \in K[G]$, $p \nmid d(\beta)$, and $|N(\beta)| = 2$.

Semistable Extensions and Formal Group Laws

Theorem

Let L/K be a totally ramified Galois extension. The following are equivalent:

1. *L/K is a Kummer extension with respect to some formal group law over $\mathcal{O}_K$.*
2. *L/K is a semistable abelian p-extension.*

We'll outline the proof of $1 \Rightarrow 2$. We already saw that L/K is an abelian p-extension.

Kummer Extensions are Semistable

We have $a \in K$, $T \leq F(\mathcal{M}_K^r)$,

$$P_T(X) = \prod_{t \in T} (X -_F t),$$

and $y \in \mathcal{O}_L$ such that $P_T(y) = a$ and $L = K(y)$. Write

$$X -_F Y = F(X, [-1]_F(Y)) = X - Y + \sum_{i,j \geq 1} b_{ij} X^i Y^j$$

and set $\beta = (1 \otimes y) -_F (y \otimes 1)$. Then $\beta \in L \otimes_K L$ and

$$\begin{aligned}\beta &= 1 \otimes y - y \otimes 1 + \sum_{i,j \geq 1} b_{ij} y^j \otimes y^i \\ &= 1 \otimes y - y \otimes 1 + \text{terms with higher valuations.}\end{aligned}$$

Set $m = v_L(y)$. Then $d(\beta) = m$ and $N(\beta) = \{[0, m], [m, 0]\}$.

Kummer Extensions are Semistable ...

Let $\sigma \in G = \mathrm{Gal}(L/K)$. Recall that the map $\psi_\sigma : L \otimes_K L \to L$ defined by $\psi_\sigma(a \otimes b) = a\sigma(b)$ is a K-algebra homomorphism. Therefore

$$\begin{aligned}\psi_\sigma(\beta) &= \psi_\sigma(1 \otimes y -_F y \otimes 1) \\ &= \psi_\sigma(1 \otimes y) -_F \psi_\sigma(y \otimes 1) \\ &= \sigma(y) -_F y \\ &= t_\sigma \in K.\end{aligned}$$

It follows that $\phi(\beta) = \sum_{\sigma \in G} \psi_\sigma(\beta)\sigma \in K[G]$.

Since we also have $|N(\beta)| = 2$ and $p \nmid m = d(\beta)$ we conclude that L/K is semistable.

When is $\mathcal{O}_K$ Free over $\mathfrak{A}(\mathcal{O}_K)$?

Theorem

Let L/K be a totally ramified abelian extension of degree $q = p^r$. Assume that the different $\mathfrak{D}$ of L/K satisfies $\mathfrak{D} = \delta\mathcal{O}_L$ for some $\delta \in \mathcal{O}_K$ such that $\delta \notin q\mathcal{O}_K$. Then the following are equivalent:

1. *There is a formal group law $F(X, Y)$ over $\mathcal{O}_K$, a finite subgroup T of $F(\mathcal{M}_K)$, and a uniformizer π_K of K such that $L = K(y)$ for some y such that $P_T(y) = \pi_K$.*
2. *$\mathcal{O}_L$ is a free $\mathfrak{A}(\mathcal{O}_L)$-module of rank 1.*

Furthermore, when these conditions are satisfied, $\mathfrak{A}(\mathcal{O}_K)$ is a Hopf order in $K[G]$.

We will sketch the proof of $2 \Rightarrow 1$.

$\mathcal{O}_L$ free over $\mathfrak{A}(\mathcal{O}_L) \Rightarrow L/K$ Kummer

The assumptions on $\mathfrak{D}$ and δ imply that there is $\xi \in \mathfrak{A}(\mathcal{O}_L)$ such that for all $a \in L$ with $v_L(a) = q - 1$ we have $v_L(\xi(a)) = 1$.

Let $\alpha \in L \otimes_K L$ satisfy $\phi(\alpha) = \delta\xi$ and write

$$\phi(\alpha) = \sum_{\sigma \in G} t_\sigma \sigma.$$

Then $t_\sigma \in \mathcal{M}_K$ for all $\sigma \in G$. By adding a multiple of $1 \otimes 1$ to α we can assume that $t_1 = 0$.

We want to construct a formal group law $F(X, Y)$ such that $T = \{t_\sigma : \sigma \in G\}$ is a subgroup of $F(\mathcal{M}_K)$.

We need $F(t_\sigma, t_\tau) = t_{\sigma\tau}$ for all $\sigma, \tau \in G$. Bondarko shows that it is enough to check this for q particular pairs $(\sigma, \tau) \in G$.

By specializing parameters in a universal formal group law we can construct $F(X, Y)$ to make these q relations hold.

$\mathcal{O}_L$ free over $\mathfrak{A}(\mathcal{O}_L) \Rightarrow L/K$ Kummer ...

Since

$$\xi \in \mathfrak{A}(\mathcal{O}_L) = \phi(\mathfrak{D}^{-1} \otimes_{\mathcal{O}_K} \mathcal{O}_L)$$

we have

$$\alpha = \delta\phi^{-1}(\xi) \in \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_L.$$

In fact there are $y, z \in \mathcal{M}_L$ such that $\alpha = 1 \otimes y +_F z \otimes 1$. We get

$$0 = \psi_1(\alpha) = \psi_1(1 \otimes y) +_F \psi_1(z \otimes 1) = y +_F z.$$

Hence $z = [-1]_F(y)$ and $\alpha = 1 \otimes y -_F y \otimes 1$. For $\sigma \in G$ we get

$$t_\sigma = \psi_\sigma(\alpha) = \psi_\sigma(1 \otimes y) -_F \psi_\sigma(y \otimes 1) = \sigma(y) -_F y.$$

$\mathcal{O}_L$ free over $\mathfrak{A}(\mathcal{O}_L) \Rightarrow L/K$ Kummer . . .

Set $\omega = \mathrm{N}_{L/K}(y)$. Then

$$\omega = \prod_{\sigma \in G} (y +_F t_\sigma) \in K.$$

Using the fact that $\xi(a)$ is a uniformizer for L we find that ω is a uniformizer for L. Hence $L = K(y)$ and y is a root of

$$P_T(X) = \prod_{\sigma \in G} (X +_F t_\sigma) = \omega.$$

A Byproduct

Theorem

Let L/K be a totally ramified Galois extension such that the different $\mathfrak{D}$ of L/K satisfies $\mathfrak{D} = \delta\mathcal{O}_L$ for some $\delta \in \mathcal{O}_K$. Assume that there exists $\xi \in \mathfrak{A}(\mathcal{O}_L)$ and $a \in L$ with $v_L(a) = q - 1$ such that $v_L(\xi(a)) = 1$. Let $\alpha \in L \otimes_K L$ satisfy $\phi(\alpha) = \delta\xi$. Then the set

$$\{\delta^{-1}\phi(1), \delta^{-1}\phi(\alpha), \delta^{-1}\phi(\alpha^2), \ldots, \delta^{-1}\phi(\alpha^{q-1})\}$$

is a basis for $\mathfrak{A}(\mathcal{O}_L)$ over $\mathcal{O}_K$.

Semistable Extensions and Indices of Inseparability

The definition of the diagram $D(\beta)$ of $\beta \in L \otimes_K L$ is reminiscent of the definition of the indices of inseparability of L/K:

1. Both are based on expressing elements of L as power series in π_L with coefficients in the set $\mathcal{T}$ of Teichmüller representatives of K.
2. In both cases it is true, but not obvious, that the data obtained from the power series expansion does not depend on the choice of uniformizer π_L.
3. There is a tantalizing parallel between:
   - The indices of inseparability of L/K, which determine the usual ramification data.
   - $D(\beta)$, which determines $N(\beta)$.

Semistable Extensions and Galois Scaffolds

It is natural to ask what the relation is between semistable extensions and Galois scaffolds.

Indeed, both are extra structures on the Galois extension L/K which, when they exist, allow one to compute various properties of the Galois module structure of L.

We saw that every p-extension L/K which is not almost maximally ramified and which has a Galois scaffold is semistable.

Some Questions

Regarding the indices of inseparability:

1. Can the indices of inseparability of L/K be computed from $G(\beta)$ for an appropriate choice of β?

Regarding Galois scaffolds:

1. Does every semistable extension L/K admit a Galois scaffold? (Nigel Byott thinks the answer is No.)
2. If the answer is Yes, suppose L/K is semistable with respect to $\beta \in L \otimes_K L$. Can we use β to construct a scaffold for L/K?

Thank You!