Morava Stabilizer Groups (Lecture 19)

March 24, 2010

Fix a prime number p and an integer $0 < n < \infty$. Our goal in this lecture is to understand the structure of the moduli stack $\mathcal{M}_{\mathrm{FG}}^n$, whose R-points are formal groups of height exactly n over R.

Let $\overline{\mathbb{F}}_{\mathrm{p}}$ denote the algebraic closure of the field $\mathbf{F}_p$. We have seen that there exists a formal group law $f(x, y) \in \overline{\mathbb{F}}_{\mathrm{p}}[[x, y]]$ of height n, which is unique up to isomorphism. The map $\operatorname{Spec} \overline{\mathbb{F}}_{\mathrm{p}} \to \mathcal{M}_{\mathrm{FG}}^n$ is faithfully flat: for any commutative ring R and any formal group law $f'(x, y)$ over R of height exactly n, we have a pullback diagram

$$\begin{CD} \operatorname{Spec} R' @>>> \operatorname{Spec} R \\ @VVV @VVV \\ \operatorname{Spec} \overline{\mathbb{F}}_{\mathrm{p}} @>>> \mathcal{M}_{\mathrm{FG}}^n \end{CD}$$

where R' is a direct limit of finite etale extensions of $R \otimes \overline{\mathbb{F}}_{\mathrm{p}}$ (and therefore faithfully flat over R). Consequently, we can regard $\overline{\mathbb{F}}_{\mathrm{p}}$ as an atlas for $\mathcal{M}_{\mathrm{FG}}^n$. To understand $\mathcal{M}_{\mathrm{FG}}^n$, we form a pullback diagram

$$\begin{CD} \operatorname{Spec} B @>>> \operatorname{Spec} \overline{\mathbb{F}}_{\mathrm{p}} \\ @VVV @VVV \\ \operatorname{Spec} \overline{\mathbb{F}}_{\mathrm{p}} @>>> \mathcal{M}_{\mathrm{FG}}^n . \end{CD}$$

The ring $\operatorname{Spec} B$ is a direct limit of finite etale extensions of $\overline{\mathbb{F}}_{\mathrm{p}}$. Since $\overline{\mathbb{F}}_{\mathrm{p}}$ is an algebraically closed field, each of these etale extensions is just a product of finitely many copies of $\overline{\mathbb{F}}_{\mathrm{p}}$. Consequently, we can identify $\operatorname{Spec} B$ (as a topological space) with an inverse limit of a tower of finite sets

$$\cdots \to X_2 \to X_1 \to X_0 .$$

We will denote this inverse limit by $\mathbb{G}$. Unwinding the definitions, a point of $\mathbb{G}$ is given by an isomorphism class of maps $B \to k$, where k is an algebraic closure of $\mathbf{F}_p$ (noncanonically isomorphic to $\overline{\mathbb{F}}_{\mathrm{p}}$. To give such a map is equivalent to giving the following data:

(1) A pair of maps $\eta, \eta' : \overline{\mathbb{F}}_{\mathrm{p}} \to k$.

(2) An isomorphism between the formal groups $\eta(f)$ and $\eta'(f)$ over k.

Since we are interested in classifying such data up to isomorphism, we may as well assume that $k = \overline{\mathbb{F}}_{\mathrm{p}}$ and η' is the identity. Then η is an automorphism of $\overline{\mathbb{F}}_{\mathrm{p}}$: that is, we can think of η as an element of the Galois group $\operatorname{Gal}(\overline{\mathbb{F}}_{\mathrm{p}} / \mathbf{F}_p) \simeq \widehat{\mathbf{Z}}$. The data of (2) is then an isomorphism of f with $\eta(f)$, where $\eta(f)$ denotes the formal group law obtained by applying η to each coefficient in f. In other words, we can identify $\mathbb{G}$ with the automorphism group $\operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, f)$ of the pair $\overline{\mathbb{F}}_{\mathrm{p}}$, $f \in \mathrm{FGL}(\overline{\mathbb{F}}_{\mathrm{p}})$. This group sits in an exact sequence

$$0 \to \operatorname{Aut}(f) \to \operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, f) \to \operatorname{Gal}(\overline{\mathbb{F}}_{\mathrm{p}}, \mathbf{F}_p) \to 0,$$

where $\operatorname{Aut}(f)$ is the automorphism group of the formal group law f (keeping the field $\overline{\mathbb{F}}_{\mathrm{p}}$ fixed). The group $\mathbb{G} = \operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, f)$ is called the *Morava stabilizer group*. We arrive at the following conclusion:

Proposition 1. *The moduli stack* $\mathcal{M}^n_{\mathrm{FG}}$ *can be identified with the quotient (with respect to the flat topology)* $(\operatorname{Spec}\overline{\mathbb{F}}_{\mathrm{p}})/\operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, f)$*, where* $\operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, f)$ *acts via the map* $\operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, f) \to \operatorname{Gal}(\overline{\mathbb{F}}_{\mathrm{p}}/\mathbf{F}_p)$*.*

To understand the stack $\mathcal{M}^n_{\mathrm{FG}}$ better, we need to understand the group $\operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, f)$. We begin by analyzing the subgroup $\operatorname{Aut}(f)$. By definition, $\operatorname{Aut}(f)$ can be identified with the group of units in the ring $\operatorname{End}(f)$ of endomorphisms of f: that is, elements of $\operatorname{End}(f)$ are power series $g(t) \in \overline{\mathbb{F}}_{\mathrm{p}}[[t]]$ such that $gf(x,y) = f(g(x), g(y))$.

Let f^p denote the formal group law over $\overline{\mathbb{F}}_{\mathrm{p}}$ obtained by applying the Frobenius map $a \mapsto a^p$ to each coefficient of f. Then f^p is another formal group law of height n over $\overline{\mathbb{F}}_{\mathrm{p}}$, so there exists a *noncanonical* isomorphism ν of f with f^p: that is, a power series ν satisfying $\nu f^p(x,y) = f(\nu(x), \nu(y))$. Note that $f(x,y)^p \simeq f^p(x^p, y^p)$, so that

$$\nu f(x,y)^p = \nu f^p(x^p, y^p) = f(\nu(x^p), \nu(y^p)).$$

Consequently, we deduce that the power series $\pi(t) = \nu(t^p)$ is an endomorphism of f, and belongs to the ring $\operatorname{End}(f)$.

Let $g \in \operatorname{End}(f)$ be arbitrary, and write $g(t) = b_0 t + b_1 t^2 + \ldots$ If $b_0 \neq 0$, then g is invertible and belongs to $\operatorname{Aut}(f)$. Otherwise, we have seen that $g(t) = g_0(t^p)$ for some uniquely defined power series g_0, and that g_0 is an endomorphism of the formal group law f^p. Then $g_0 \circ \nu^{-1}$ is an endomorphism of f, and we have $g = g_0 \circ \nu^{-1} \circ \nu \circ (t \mapsto t^p) = (g_0 \circ \nu^{-1})\pi$. In other words:

Proposition 2. *Every non-invertible element g of the ring* $\operatorname{End}(f)$ *can be written uniquely in the form $g'\pi$, where $\pi(t) = \nu(t^p)$ is the endomorphism defined above. In particular,* $\operatorname{End}(f)$ *is a (noncommutative) local ring: the collection of non-invertible elements of* $\operatorname{End}(f)$ *is a two-sided ideal, which is the left ideal generated by π.*

More generally, we saw in lecture 12 that every nonzero endomorphism g of f can be written uniquely in the form $u\pi^k$ for some $k \geq 0$; here k is the smallest integer for which the coefficient of t^{p^k} in $g(t)$ is nonzero. We will refer to k as the *valuation* of g and write $k = v(g)$. By convention we set $v(0) = \infty$. Note that $v(gg') = v(g) + v(g')$. In particular, $v(p) = n$ where n is the height of f (this is the definition of height).

Remark 3. There is an evident ring homomorphism $\lambda : \operatorname{End}(f) \mapsto \overline{\mathbb{F}}_{\mathrm{p}}$ given by differentiation: more precisely, λ carries $g(t) = b_0 t + b_1 t^2 + \ldots$ to the element $b_0 \in \overline{\mathbb{F}}_{\mathrm{p}}$. The kernel of λ is the collection of noninvertible power series: that is, the ideal $\operatorname{End}(f)\pi$. Since the p-series for f is given by $[p](t) = \mu t^{p^n} + \cdots$ for some μ, any endomorphism g of f satisfies $g([p](t)) = [p](g(t))$, so that

$$b_0 \mu t^{p^n} + \cdots = b_0^{p^n} \mu t^{p^n} + \cdots .$$

It follows that the image of λ is contained in the subfield $\mathbf{F}_{p^n} \subseteq \overline{\mathbb{F}}_{\mathrm{p}}$. Conversely, in Lecture 14 we showed that any solution to the equation $b_0 = b_0^{p^n}$ can be extended to an automorphism of f: that is, the map $\lambda : \operatorname{End}(f) \to \mathbf{F}_{p^n}$ is surjective.

Remark 4. Since an endomorphism $g(t)$ of f is determined knowing all of its reductions modulo t^{p^k}, we deduce that $\operatorname{End}(f) \simeq \varprojlim(\operatorname{End}(f)/\operatorname{End}(f)\pi^k)$. Each of the quotients $\operatorname{End}(f)/\operatorname{End}(f)\pi^k$ has finite cardinality p^{nk}, so this inverse limit exhibits $\operatorname{End}(f)$ as a profinite set. The induced topology on the closed subset $\operatorname{Aut}(f)$ agrees with Zariski topology on $\operatorname{Spec} B = \operatorname{Aut}(\overline{\mathbb{F}}_{\mathrm{p}}, k)$.

We have a canonical map

$$\mathbf{Z}_p \simeq \varprojlim \mathbf{Z}/p^k\mathbf{Z} \to \varprojlim \operatorname{End}(f)/\operatorname{End}(f)\pi^k \simeq \operatorname{End}(f)$$

whose image is central in $\operatorname{End}(f)$.

In other words, we can think of $\operatorname{End}(f)$ as a noncommutative discrete valuation ring, having commutative residue field $\mathbf{F}_{p^n}$. Let $D = \operatorname{End}(f)[p^{-1}]$. Since $p = u\pi^n$ for some invertible constant u, π is invertible in D, so that D is a division algebra over $\mathbf{Z}_p[p^{-1}] \simeq \mathbf{Q}_p$. The valuation v extends to D formally by the formula $v(\frac{\lambda}{p^k}) = v(\lambda) - nk$.

Note that p is not a zero-divisor in $\operatorname{End}(f)$, so that $\operatorname{End}(f)$ can be identified with a subset of D.

Lemma 5. *We have* $\mathrm{End}(f) = \{x \in D : v(x) \geq 0\}$.

Proof. It is clear that $v(x) \geq 0$ if $x \in \mathrm{End}(f)$. Conversely, suppose that $x = \frac{\lambda}{p^k}$ for some $\lambda \in \mathrm{End}(f)$. If $v(x) \geq 0$, then $v(\lambda) \geq nk$ so that $\lambda = \lambda' \pi^{nk}$. It will therefore suffice to show that $\frac{\pi^{nk}}{p^k} \in \mathrm{End}(f)$. Since $\mathrm{End}(f)$ is closed under products, it suffices to show that $\frac{\pi^n}{p} \in \mathrm{End}(f)$. This is clear, since $v(p) = n$ implies that $p = u\pi^n$ for some invertible $u \in \mathrm{End}(f)$. □

Lemma 6. *As a vector space over* $\mathbf{Q}_p$*,* D *has dimension* n^2*.*

Proof. Let $\{\overline{x}_i\}_{0 \leq i < n}$ be a basis for $\mathbf{F}_{p^n}$ over $\mathbf{F}_p$. Choose elements $x_i \in \mathrm{End}(f)$ with $\lambda(x_i) = \overline{x_i}$. Then the elements $\{\pi^j x_i\}_{0 \leq i,j < n}$ form a basis for D over $\mathbf{Q}_p$. □

To identify D further, we note that conjugation by any $g \in D^\times$ is an automorphism of D which preserves $\mathrm{End}(f) \subseteq D$ and therefore acts on the quotient $\mathrm{End}(f)/\pi$.

Lemma 7. *Let* $g \in D$*. The conjugation action of* g *on* $\mathrm{End}(f)/\pi \simeq \mathbf{F}_{p^n}$ *is given by* $b \mapsto b^{p^{v(g)}}$*.*

Proof. Without loss of generality we may assume that $g \in \mathrm{End}(f)$, so that $g(t) = \lambda t^{p^{v(g)}}$ for some $\lambda \neq 0$. Fix $b \in \mathbf{F}_{p^n}$, and let $h \in \mathrm{End}(f)$ be a power series given by $h(t) = b_0 t + \cdots$. Let $h'(t) = (g \circ h \circ g^{-1})(t) = b't + \cdots \in \mathrm{End}(f)$. The equation $g \circ h = h' \circ g$ gives

$$\lambda b^{p^{v(g)}} t^{p^{v(g)}} + \cdots = b' \lambda t^{p^{v(g)}} + \cdots$$

so that $b' = b^{p^{v(g)}}$. □

Lemma 8. *The center of* D *is* $\mathbf{Q}_p$*.*

Proof. Let g be in the center of D; we wish to prove that $g \in \mathbf{Q}_p$. Multiplying by a power of p if necessary, we may assume that $g \in \mathrm{End}(f)$; we wish to prove that $g \in \mathbf{Z}_p$. Since $\mathbf{Z}_p$ is closed in $\mathrm{End}(f)$, it will suffice to show that there exists an integer m such that $g \equiv m \mod p^k$ for all k. We work by induction on k. Since $\pi g \pi^{-1} = g$, Lemma 7 implies that the reduction of g moduli π belongs to $\mathbf{F}_p \subseteq \mathbf{F}_{p^n}$. Subtracting an integer from g, we may suppose that $v(g) > 0$. Lemma 7 implies that $v(g)$ is divisible by n, so that $v(g) \geq n$ and therefore $g = g'p$ for some g' belonging to the center of $\mathrm{End}(f)$. Then g' is congruent to an integer modulo p^{k-1} by the inductive hypothesis, so that g is congruent to an integer modulo p^k. □

Remark 9. It follows from the above analysis that the division algebra D can be identified with an element of the Brauer group $\mathrm{Br}(\mathbf{Q}_p)$. There is a canonical isomorphism $\mu : \mathrm{Br}(\mathbf{Q}_p) \simeq \mathbf{Q}/\mathbf{Z}$, which is defined as follows. Every Brauer class over $\mathbf{Q}_p$ is represented by a central division algebra D' over $\mathbf{Q}_p$, which contains a ring of integers $\mathcal{O}$ and maximal ideal $\mathfrak{m}$. There is a valuation $v : D' - \{0\} \to \mathbf{Z}$ with $\mathcal{O} = v^{-1}\mathbf{Z}_{\geq 0}$ and $\mathfrak{m} = v^{-1}\mathbf{Z}_{\geq 1}$. Conjugation induces a surjective homomorphism $D' - \{0\} \to \mathrm{Gal}((\mathcal{O}/\mathfrak{m})/\mathbf{F}_p)$. In particular, the Frobenius map $x \mapsto x^p$ on the residue field $\mathcal{O}/\mathfrak{m}$ is given by conjugation by x, for some $x \in D'$. Then $\mu(D') = \frac{v(x)}{v(p)}$ (modulo $\mathbf{Z}$, this invariant does not depend on the choice of x).

In the case $D = D'$, we can take $x = \pi$, so that D is the unique central division algebra over $\mathbf{Q}_p$ with $\mu(D) = \frac{1}{n}$.

By construction, there is a canonical isomorphism $\mathrm{End}(f)^\times \simeq \mathrm{Aut}(f)$. In fact, we can extend this to a map $\chi : D^\times \to \mathrm{Aut}(\overline{\mathbb{F}}_p, f)$. Here χ is defined on $\mathrm{End}(f) - \{0\}$ by carrying a nonzero endomorphism $g(t)$ of f to the pair $(F^{v(g)}, g_0)$, where $F^{v(g)}$ is a power of the Frobenius automorphism $x \mapsto x^p$ of $\overline{\mathbb{F}}_p$, and g_0 is the isomorphism of f with $f^{p^{v(g)}}$ characterized by the formula $g(t) = g_0(t^{p^{v(g)}})$.

We have a commutative diagram of exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{End}(f)^\times & \longrightarrow & D^\times & \xrightarrow{v} & \mathbf{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Aut}(f) & \longrightarrow & \mathrm{Aut}(\overline{\mathbb{F}}_p, f) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}}_p, \mathbf{F}_p) & \longrightarrow & 0.
\end{array}$$

The left vertical map is an isomorphism, and the right vertical map is *almost* an isomorphism (the group $\mathrm{Gal}(\overline{\mathbb{F}}_\mathrm{p}, \mathbf{F}_p)$ is the profinite completion $\widehat{\mathbf{Z}}$ of the $\mathbf{Z}$). Consequently, the Morava stabilizer group is *almost* the group of units in the division algebra $D^\times$ (they differ by a completion procedure).

We can use the above picture to study the problem of *descending* the formal group law defined by f to a finite field $\mathbf{F}_{p^k} \subseteq \overline{\mathbb{F}}_\mathrm{p}$. By descent theory, this is equivalent to giving an action of $\mathrm{Gal}(\overline{\mathbb{F}}_\mathrm{p}/\mathbf{F}_{p^k}) \simeq k\widehat{\mathbf{Z}}$ on the formal group, compatible with the action of $k\widehat{\mathbf{Z}}$ on $\overline{\mathbb{F}}_\mathrm{p}$ itself. In other words, we need to give a *splitting* of the projection map $\mathrm{Aut}(\overline{\mathbb{F}}_\mathrm{p}, f) \to \mathrm{Gal}(\overline{\mathbb{F}}_\mathrm{p}/\mathbf{F}_p)$ over the subgroup $k\widehat{\mathbf{Z}} \subseteq \mathrm{Gal}(\overline{\mathbb{F}}_\mathrm{p}/\mathbf{F}_p)$. Since $k\widehat{\mathbf{Z}}$ is topologically cyclic, this is equivalent to giving a single element of $\mathrm{Aut}(\overline{\mathbb{F}}_\mathrm{p}, f)$ lying over the integer k: that is, giving an element of $x \in D^\times$ with $v(x) = k$.

Such an element exists for every integer $k \geq 1$. However, when $k = 1$ there is a canonical choice $x = p$, which belongs to the center of D. Unwinding the definitions, this proves the following:

Proposition 10. *The formal group of height n over $\overline{\mathbb{F}}_\mathrm{p}$ has a canonical form over the finite field $\mathbf{F}_{p^n}$. This formal group over $\mathbf{F}_{p^n}$ has the property that every endomorphism (and, in particular, every automorphism) is defined over $\mathbf{F}_{p^n}$.*

It follows that the moduli stack $\mathcal{M}_{\mathrm{FG}}^n$ can also be identified with the quotient $\mathrm{Spec}\, \mathbf{F}_{p^n}/\mathbb{G}'$, where $\mathbb{G}' \simeq D^\times/p^{\mathbf{Z}}$ fits into an exact sequence

$$0 \to \mathrm{End}(f)^\times \to \mathbb{G}' \to \mathbf{Z}/n\mathbf{Z} \to 0.$$

The group $\mathbb{G}'$ is also sometimes called the Morava stabilizer group.