Heights of Formal Groups (Lecture 12)

April 27, 2010

Our next goal in this course is to understand the structure of the moduli stack $\mathcal{M}_{\mathrm{FG}}$ of formal groups. Our starting point is the following result from Lecture 2:

Proposition 1. *Let R be a ring of characteristic zero. Then, for every formal group law $f \in R[[x,y]]$, there exist a unique power series $g(t) = t + b_1 t^2 + b_2 t^3 + \dots$ such that $f(x,y) = g(g^{-1}(x) + g^{-1}(y))$.*

Corollary 2. *The quotient stack $\mathcal{M}^s_{\mathrm{FG}} \times \operatorname{Spec} \mathbf{Q} = (\operatorname{Spec} L/G) \times \operatorname{Spec} \mathbf{Q}$ is isomorphic to $\operatorname{Spec} \mathbf{Q}$.*

Corollary 3. *The quotient stack $\mathcal{M}_{\mathrm{FG}} \times \operatorname{Spec} \mathbf{Q} = (\operatorname{Spec} L/G^+) \times \operatorname{Spec} \mathbf{Q}$ is isomorphic to the classifying stack $B\mathbb{G}_m$ (over $\operatorname{Spec} \mathbf{Q}$). In other words, if R is a ring of characteristic zero, then every formal group over R is determined (up to unique isomorphism) by its Lie algebra.*

Example 4. Let $f(x,y) = x + y + xy$ be the multiplicative formal group law. If R is a ring of characteristic zero, then f is isomorphic to the additive formal group law via the isomorphism $g(t) = e^t - 1 = t + \frac{1}{2}t^2 + \frac{1}{6}t^3 + \cdots$.

The coefficients of the power series $e^t - 1$ are not integral. This suggests that over rings which are not of characteristic zero, the additive and multiplicative formal groups are not isomorphic. To prove this, we need an invariant which can be used to tell two formal groups apart. First, we need a brief digression concerning endomorphisms of a formal group law.

Definition 5. Let $f \in R[[x,y]]$ be a formal group law over R. An *endomorphism* of f is a power series $g(t) \in tR[[t]]$ such that $f(g(x), g(y)) = gf(x,y)$.

To prove Proposition 1, we need to introduce the notion of a *translation invariant* differential on $\operatorname{Spf} R[[t]]$. First, let $R[[t]]dt$ denote a free module of rank 1 over $R[[t]]$; we will call elements of $R[[t]]$ *differentials*. Given a differential $g(t)dt$, we write $f^*(g(t)dt) = g(f(x,y))(\frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy) \in R[[x,y]]\{dx, dy\}$. We will say that $g(t)dt$ is an *translation invariant* differential if we have $f^*(g(t)dt) = g(x)dx + g(y)dy$.

Example 6. Let $f(x,y) = x + y$ be the additive formal group law. Then $dt \in R[[t]]$ is a translation invariant differential.

Example 7. Let $f(x,y) = x + y + xy$ is a multiplicative formal group law. Then $\frac{dt}{1+t} = dt - tdt + t^2 dt + \cdots$ is a translation invariant differential.

There exists a unique translation invariant differential of the form $\omega = dt + c_1 t dt + \dots$. Moreover, $R[[t]]dt$ can be identified with the free module $R[[t]]\omega$.

Now suppose that $h(t) = a_1 t + a_2 t^2 + \cdots \in tR[[t]]$. Composition with h determines a map h^* from $R[[t]]dt$ to itself, given by $h^*(g(t)dt) = (g \circ h)(t)dh$, where $dh = a_1 dt + 2a_2 tdt + \cdots$. Note that $h^* = 0$ if and only if each coefficient $ia_i = 0$: since $p = 0$ in R, this is equivalent to the requirement that a_i vanishes for i not divisible by p. Equivalently, $h^* = 0$ if and only if we can write $h(t) = h'(t^p)$ for some other power series h'.

Suppose that f and f' are formal groups over R, and that h is a morphism from f to f': that is, h satisfies $hf(x,y) = f'(h(x), h(y))$. Then h^* carries invariant differentials with respect to f' to invariant differentials with respect to f. In particular, if we let ω_f and $\omega_{f'}$ be defined as above, then we have $h^*\omega_{f'} = \lambda\omega_f$ for some constant $\lambda \in R$. Unwinding the definitions, we see that $h(t) \equiv \lambda t \mod (t^2)$. We conclude the following:

Claim 8. *Let $f(x,y), f'(x,y) \in R[[x,y]]$ be formal group laws over a ring R such that $p = 0$ in R, and let $h \in tR[[t]]$ satisfy $hf(x,y) = f'(h(x),h(y))$. Then one of the following conditions holds:*

(1) *There exists $\lambda \neq 0 \in R$ such that $h(t) = \lambda t + \cdots$.*

(2) *There exists another power series h' such that $h(t) = h'(t^p)$.*

Let $f'(x,y)$ be the power series defined by the equation $f'(x^p, y^p) = f(x,y)^p$ (that is, f' is obtained from f by raising all coefficients to the pth power). In the second case, we get

$$f'(h_0(x^p), h_0(y^p)) = f'(h(x),h(y)) = hf(x,y) = h_0(f(x,y)^p) = h_0 f^p(x^p, y^p),$$

so that $h_0 f^p(x,y) = f'(h_0(x), h_0(y))$. that is, h_0 can be regarded as a morphism from f^p into f'. Repeating the above argument, we arrive at the following:

Claim 9. *Let R be a commutative ring with $p = 0$, let $f(x,y), f'(x,y) \in R[[x,y]]$ be formal group laws, and let h be a power series satisfying $hf(x,y) = f'(h(x),h(y))$. If $h \neq 0$, then there exists $n \geq 0$ such that $h(t) = h'(t^{p^n})$ with $h'(t) = \lambda t + O(t^2)$, $\lambda \neq 0$.*

Definition 10. Let $f(x,y) \in R[[x,y]]$ be a formal group law over a commutative ring R. For every nonnegative integer n, we define the *n-series* $[n](t) \in R[[t]]$ as follows:

(1) If $n = 0$, we set $[n](t) = 0$.

(2) If $n > 0$, we set $[n](t) = f([n-1](t), t)$.

Remark 11. For every integer n, the n-series $[n]$ determines a homomorphism from the formal group f to itself. That is, we have $f([n](x),[n](y)) = [n]f(x,y)$.

Since $f(x,y) = x + y + \cdots$, we immediately deduce that $[n](t) = nt + O(t^2)$. Consequently, if p is a prime number such that $p = 0$ in R, then the linear term of $[p](t)$ vanishes: that is, we can write $[p](t) = ct^k + O(t^{k+1})$ for some $k > 1$.

Since $[p]$ is an endomorphism of f, we immediately obtain the following:

Proposition 12. *Let R be a commutative ring in which $p = 0$ and let f be a formal group law over R. Then either $[p](t) = 0$, or $[p](t) = \lambda t^{p^n} + O(t^{p^n+1})$ for some $n > 0$.*

Definition 13. Let f be a formal group law over a commutative ring R, and fix a prime number p. We let v_n denote the coefficient of t^{p^n} in the p-series $[p]$. We will say that f has *height* $\geq n$ if $v_i = 0$ for $i < n$. We will say that f has *height exactly* n if it has height $\geq n$ and $v_n \in R$ is invertible.

Remark 14. We have $v_0 = p$. Thus f has height ≥ 1 if and only if $p = 0$ in R, and height exactly zero if and only if p is invertible in R.

Remark 15. Let f and f' be formal group laws over a commutative ring R, having p-series $[p]_f$ and $[p]_{f'}$. If $g(t)$ is an isomorphism between f and f', then we have $[p]_{f'}(t) = (g \circ [p]_f \circ g^{-1})(t)$. It follows immediately that the heights of f and f' are the same.

Example 16. Let $f(x,y) = x + y + xy$ be the formal multiplicative group. Then $[n](t) = (1+t)^n - 1$. If $p = 0$ in R, then $[p](t) = (1+t)^p - 1 = t^p$; thus f has height exactly 1.

Example 17. Let $f(x,y) = x + y$ be the formal multiplicative group over a commutative ring R with $p = 0$. Then $[p](t) = 0$, so f has infinite height. In the next lecture, we will see that the converse holds: if f is a formal group law of infinite height, then f is isomorphic to the additive group.

It follows from Examples 16 and 17 that the additive and multiplicative formal group laws are not isomorphic over any commutative ring in which $p = 0$.