Classification of Formal Groups (Lecture 14)

April 27, 2010

Our goal in this lecture is to prove Lazard's theorem, which asserts that a formal group law over an algebraically closed field is determined up to isomorphism by its height. We will prove this result in the following more precise form:

Theorem 1. *Let $f(x,y), f'(x,y) \in R[[x,y]]$ be formal group laws of height exactly $n > 0$ and let R' be the ring which classifies isomorphisms between f and f': that is, $R' = R[b_0^{\pm 1}, b_1, b_2, \ldots]/I$, where I is the ideal generated by all coefficients in the power series $f(g(x), g(y)) - g(f'(x,y))$, where $g(t) = b_0 t + b_1 t^2 + \cdots$. Then R' is isomorphic to the direct limit of a system of (injective) finite etale maps*

$$R = R(1) \hookrightarrow R(2) \hookrightarrow \cdots$$

We will regard f and f' as fixed for the duration of the proof. Since $f'(x,y)$ has height exactly n, we may assume without loss of generality that

$$f'(x,y) \equiv x + y + \sum_{0<i<p^n} \lambda \frac{\binom{p^n}{i}}{p} x^i y^{p^n - i} \mod (x,y)^{p^n+1},$$

where λ is invertible in R.

Our first step is to choose a more convenient set of polynomial generators for the ring $R[b_0^{\mp 1}, b_1, b_2, \ldots]$.

Construction 2. *Let A be a commutative R-algebra and suppose we are given a sequence of elements $c_0, c_1, \ldots \in A$ with c_0 invertible. We define a sequence of formal group laws $f_m(x,y)$ by induction as follows:*

1. *Set $f_1(x,y) = f(x,y)$.*
2. *If m is not a power of p, we let $f_m(x,y) = g_m^{-1} f_{m-1}(g_m(x), g_m(y))$, where $g_m(x) = x + c_{m-1}x^m$.*
3. *If $m = p^{n'}$ for $n' < n$, we let $f_m = f_{m-1} = g_m^{-1} f_{m-1}(g_m(x), g_m(y))$ where $g_m(t) = t$.*
4. *If $m = p^n$, we let $f_m = g_m^{-1} f_{m-1}(g_m(x), g_m(y))$ where $g_m(t) = c_0 t$.*
5. *If $m = p^{n+n'}$ for $n' > 0$, we let $f_m = g_m^{-1} f_{m-1}(g_m(x), g_m(y))$ where $g_m(t) = f_{m-1}(t, c_{p^{n'}-1} t^{p^{n'}})$.*

We note that $f_m(x,y)$ tends to a limit $f_\infty(x,y) = g^{-1} f(g(x), g(y))$ where $g(t)$ denotes the infinite (convergent) infinite composition $g_2 \circ g_3 \circ g_4 \circ \cdots$. Note that $g(t) = b_0 t + b_1 t^2 + b_2 t^3 + \cdots$ where $b_i = c_i +$decomposables. This gives an identification of polynomial rings

$$R[b_0^{\pm 1}, b_1, b_2, \ldots] \simeq R[c_0^{\pm 1}, c_1, \ldots].$$

We can therefore identify the ring R' of Theorem 1w ith $R[c_0^{\pm 1}, c_1, \ldots]/I$, where I is the ideal generated by all coefficients in the power series $f_\infty(x,y) - f'(x,y)$.

Lemma 3. *Let $c_0, c_1, \ldots \in A$ be as above. Assume that $f_{m-1}(x,y)$ is congruent to $f'(x,y)$ modulo $(x,y)^m$. Then $f_m(x,y)$ is congruent to $f'(x,y)$ modulo $(x,y)^m$.*

Proof. In cases (1) through (3), we have $g_m(t) \equiv t \mod t^m$ so it is clear that

$$f_m(x,y) \equiv f_{m-1}(x,y) \equiv f'(x,y) \mod (x,y)^m.$$

In case (4), we have $f_{m-1}(x,y) \equiv x+y \mod (x,y)^m$ so that

$$f_m(x,y) = c_0^{-1} f_{m-1}(c_0 x, c_0 y) \equiv x+y \mod (x,y)^m$$

The tricky part is case (5).

The tricky part is case (5). Let $m = p^{n+n'}$ for $n' > 0$, and let $c = c_{p^{n'}-1}$, so that $g_m(t) = f_{m-1}(t, ct^{p^{n'}})$. For any sequence of variables $x_1, x_2, \ldots, x_a$, we let $f_{m-1}(x_1, x_2, \ldots, x_a) = f_{m-1}(x_1, f_{m-1}(x_2, \ldots f_{m-1}(x_{a-1}, x_a)) \ldots)$ (this is unambiguous since f_{m-1} is a formal group law).

We have

$$g_m f_m(x,y) = f_{m-1}(g_m(x), g_m(y)) = f_{m-1}(x, y, cx^{p^{n'}}, cy^{p^{n'}}.$$

Let $z = z(x,y)$ be such that $cf_m(x,y)^{p^{n'}} = f_{m-1}(z, cx^{p^{n'}}, cy^{p^{n'}})$, so that $f_{m-1}(f_m(x,y), z) = f_{m-1}(x,y)$. We prove the following by simultaneous induction on $m' \leq m$:

(a) We have $z \equiv 0 \mod ((x,y)^{m'})$.

(b) We have $f_m(x,y) \equiv f_{m-1}(x,y) \equiv f'(x,y) \mod ((x,y)^{m'})$.

These claims are obvious when $m' = 1$, and the implication $(a) \Rightarrow (b)$ is clear. Assume that (a) and (b) hold for some integer $m' < m$. The inductive hypothesis gives $f_{m-1}(z, cx^{p^{n'}}, cy^{p^{n'}}) \equiv z + f_{m-1}(cx^{p^{n'}}, cy^{p^{n'}})$ mod $(x,y)^{m'+1}$. Thus $z \equiv cf_m(x,y)^{p^{n'}} - f_{m-1}(cx^{p^{n'}}, cy^{p^{n'}}) \mod (x,y)^{m'+1}$. The inductive hypothesis gives $f_m(x,y)^{p^{n'}} \equiv f_{m-1}(x,y)^{p^{n'}} \mod (x,y)^{p^{n'} m'}$, so we get

$$z \equiv cf_{m-1}(x,y)^{p^{n'}} - f_{m-1}(cx^{p^{n'}}, cy^{p^{n'}}) \mod (x,y)^{m'+1}$$

By assumption, we have $f_{m-1}(x,y) \equiv f'(x,y) \equiv x+y \mod (x,y)^{p^n}$. It follows that

$$cf_{m-1}(x,y)^{p^{n'}} - f_{m-1}(cx^{p^{n'}}, cy^{p^{n'}}) \equiv c(x+y)^{p^{n'}} - cx^{p^{n'}} - cy^{p^{n'}} \equiv 0 \mod (x,y)^{p^{n+n'}}.$$

Since $m'+1 \leq m = p^{n+n'}$, we conclude that $z \equiv 0 \mod (x,y)^{m'+1}$ as desired. □

We now return to the proof of Theorem 1. By Lemma 3, we have $f_\infty(x,y) = f'(x,y)$ if and only if $f_m(x,y) \equiv f'(x,y) \mod (x,y)^{m+1}$ for all m. Note that $f_m(x,y)$ depends only on the parameters c_i where i belongs to the set $S_m = \{i < m : i \neq p^k - 1\} \cup \{p^k - 1 : p^{n+k} \leq m\}$. $R(m)$ denote the quotient ring $R[c_i]_{i \in S_m}/I(m)$ for $m < p^n$, and the quotient ring $R[c_i, c_0^{-1}]_{i \imath S_m}/I(m)$ for $m \geq p^n$, where $I(m)$ is the ideal generated by the coefficients of $x^i y^j$ in $f_m(x,y) - f'(x,y)$ where $i + j \leq m$. Then R' is the colimit of the sequence

$$R = R(1) \to R(2) \to R(3) \to \cdots$$

To prove Theorem 1, it will suffice to show that each of the inclusions $R(m-1) \to R(m)$ is a finite etale extension (which is injective). There are several cases to consider:

(a) Suppose that m is not a power of p. Then $R(m) = R(m-1)[c_{m-1}]/J$, where J is the ideal generated by coefficients of total degree m in the expression $f_m(x,y) - f'(x,y)$. Note that $f_{m-1}(x,y) \equiv f'(x,y)$ mod $(x,y)^m$, so (by the lemma of the previous lecture) we can write

$$f'(x,y) \equiv f_{m-1}(x,y) + \mu \sum_{0<i<m} \frac{\binom{m}{i}}{d} x^i y^{m-i} \mod (x,y)^{m+1}$$

where d is the greatest common divisor of the binomial coefficients $\binom{m}{i}$. Since m is not a power of p, the integer d is invertible in R. A simple calculation gives $f_m(x,y) \equiv f_{m-1}(x,y) + c_m(x^m + y^m - (x+y)^m)$ mod $(x,y)^{m+1}$. Thus $f_m(x,y) \equiv f'(x,y)$ if and only if $c_m = -\frac{\mu}{d}$. It follows that $R(m) \simeq R(m-1)$ (that is, the coefficient c_m is uniquely determined by the requirement that $f'(x,y) \equiv f_m(x,y)$ mod $(x,y)^{m+1}$.

(b) Suppose that $m = p^{n'}$, $n' < n$. Then $R(m) = R(m-1)/J$, where J is the ideal generated by coefficients of degree m in the difference $f_m(x,y) - f'(x,y)$. We have $f_m(x,y) = f_{m-1}(x,y) \equiv f'(x,y) \equiv x + y \mod (x,y)^{p^m}$. It follows from the lemma of the last lecture that $f_m(x,y) = x+y+\mu \sum_{0<i<m} \frac{\binom{p^{n'}}{i}}{p} x^i y^{m-i}$ for some uniquely determined constant μ. Since f_m is isomorphic to f, it has height exactly n, and therefore $\mu = 0$. It follows that $f_m(x,y) \equiv x+y \equiv f'(x,y) \mod (x,y)^{p^m+1}$, so that again $R(m) \simeq R(m-1)$.

(c) Suppose that $m = p^n$. Then $R(m) = R(m-1)[c_0^{\pm 1}]/J$ where J is the ideal generated by coefficients of degree m in $f_m(x,y) - f'(x,y)$. We have $f_{m-1}(x,y) \equiv f'(x,y) \equiv x+y \mod (x,y)^{p^m}$ so that

$$f_{m-1}(x,y) \equiv x + y + \lambda' \sum_{0<i<m} \frac{\binom{m}{i}}{p} x^i y^{m-j} \mod (x,y)^{m+1}$$

for some constant λ'. It follows that

$$f_m(x,y) \equiv x + y + c_0^{p^n-1} \lambda' \sum_{0<i<m} \frac{\binom{m}{i}}{p} x^i y^{m-j} \mod (x,y)^{m+1}.$$

Consequently, $f_m(x,y) \equiv f'(x,y) \mod (x,y)^{m+1}$ if and only if $c_0^{p^n-1}\lambda' = \lambda$. Since f and f' have height exactly n, the constants λ and λ' are invertible; thus $R(m) \simeq R(m-1)[c_0]/(c_0^{p_n-1} - \frac{\lambda}{\lambda'})$.

(d) Suppose that $m = p^{n+n'}$ for $n' > 0$. Let $c = c_{p^{n'}-1}$, so that $R(m) \simeq R(m-1)[c]/J$, where J is the ideal generated by coefficients on monomials of degree m in $f_m(x,y) - f'(x,y)$. This is the tricky part.

Since $f_{m-1}(x,y) \equiv f'(x,y) \mod (x,y)^m$, we can write

$$f_{m-1}(x,y) \equiv f'(x,y) + \mu \sum_{0<i<m} \frac{\binom{m}{i}}{p} x^i y^{m-i}$$

for some constant μ. Let $z = z(x,y)$ be as in the proof of Lemma 3, so that $z(x,y) \in (x,y)^m$. We have

$$f_{m-1}(x,y) = f_{m-1}(f_m(x,y), z) \equiv f_m(x,y) + z \mod (x,y)^{m+1}.$$

Consequently, we have $f_m(x,y) \equiv f'(x,y) \mod (x,y)^{m+1}$ if and only if $z \equiv \mu \sum_{0<i<m} \frac{\binom{m}{i}}{p} x^i y^{m-i} \mod (x,y)^{m+1}$.

The proof of Lemma 3 gives

$$z \equiv c f_{m-1}(x,y)^{p^{n'}} - f_{m-1}(cx^{p^{n'}}, cy^{p^{n'}}) \mod (x,y)^{m+1}.$$

We have

$$f_{m-1}(x,y) \equiv f'(x,y) \equiv x + y + \lambda \sum_{0<j<p^n} \frac{\binom{p^n}{j}}{p} x^j y^{p^n - j} \mod (x,y)^{p^n+1}.$$

It follows that

$$z \equiv (c\lambda^{p^{n'}} - \lambda c^{p^n}) \sum_{0<j<p^n} \frac{\binom{p^n}{j}}{p} x^{p^{n'}j} y^{m - p^{n'}j} \mod (x,y)^{m+1}.$$

Thus $f_m(x,y) \equiv f'(x,y) \mod (x,y)^{m+1}$ if and only if the following conditions are satisfied:

(i) The coefficients $\mu \frac{\binom{p^{n+n'}}{i}}{p}$ vanishes when i is not divisible by p^n.

(ii) For $0 < j < p^{n'}$, we have

$$\mu \frac{\binom{p^{n+n'}}{p^n j}}{p} = (\lambda^{p^{n'}} c - \lambda c^{p^n}) \frac{\binom{p^{n'}}{j}}{p}$$

We claim that these conditions are satisfied if and only if $c^{p^n} - \lambda^{p^{n'}-1} c + \frac{\mu}{\lambda} = 0$. It follows that $R(m) = R(m-1)[c]/(c^{p^n} - \lambda^{p^{n'}-1} c + \frac{\mu}{\lambda})$ is a finite étale extension of $R(m-1)$. To complete the proof, we verify the following combinatorial identity:

Lemma 4. *Let n be an integer. Then*

$$\binom{p^n}{i} \equiv \begin{cases} \binom{p}{j} & \text{if } i = p^{n-1} j \\ 0 & \text{otherwise} \end{cases} \mod p^2.$$

Proof. Let $G = \mathbf{Z}/p^n\mathbf{Z}$ be a cyclic group. Then G acts by translation on the set S of all i-element subsets of G. Let G' be the subgroup $p\mathbf{Z}/p^n\mathbf{Z}$. Any point of S is either fixed by G', or is fixed by a smaller subgroup and therefore has size divisible by p^2. It follows that the cardinality $|S|$ is congruent modulo p^2 to the cardinality of the fixed point set $|S^{G'}|$, which is the number of ways to choose a subset of the quotient G/G' having cardinality $j = \frac{i}{p^{n-1}}$. □