Lazard's Theorem (Lecture 2)

April 27, 2010

Let R be a commutative ring. We recall that a *formal group law* over R is a power series $f(x,y) \in R[[x,y]]$ satisfying the identities

$$f(x,0) = f(0,x) = x$$
$$f(x,y) = f(y,x)$$
$$f(x, f(y,z)) = f(f(x,y), z).$$

We let $\mathrm{FGL}(R)$ denote the subset of $R[[x,y]]$ consisting of all formal group laws over R. Note that a map of commutative rings $R \to R'$ induces, by substitution, a map $\mathrm{FGL}(R) \to \mathrm{FGL}(R')$. In other words, FGL is a functor from the category of commutative rings to the category of sets.

Any power series $f(x,y) \in R[[x,y]]$ can be written as a formal sum $f(x,y) = \sum c_{i,j} x^i y^j$, for some coefficients $c_{i,j} \in R$. However, for f to be a formal group law, the coefficients $c_{i,j}$ must satisfy some constraints. For example, the first condition gives

$$c_{i,0} = c_{i,0} = \begin{cases} 1 & \text{if } i = 1 \\ 0 & \text{otherwise,} \end{cases}$$

and the second condition gives $c_{i,j} = c_{j,i}$. The third condition imposes more complicated constraints on the coefficients $c_{i,j}$, which we will not write out in detail. However, we note that these constraints are simply given by polynomial equations that the coefficients $c_{i,j}$ are forced to satisfy. We can summarize the discussion as follows:

- Giving a formal group law over a ring R is equivalent to giving a collection of elements $c_{i,j} \in R$ satisfying certain polynomial equations.

Let L denote the commutative ring $\mathbf{Z}[c_{i,j}]/Q$, where Q is the ideal in $\mathbf{Z}[c_{i,j}]$ generated by the polynomial constraints mentioned above. By construction, the power series $f(x,y) = \sum c_{i,j} x^i y^j$ defines a formal group law over L. We can restate the previous assertion as follows:

- There is a formal group law $f \in \mathrm{FGL}(L)$ with the following universal property: for every commutative ring R, evaluation on f determines a bijection $\mathrm{Hom}(L, R) \to \mathrm{FGL}(R)$.

The commutative ring L is called the *Lazard ring*. Our goal in this lecture is to describe the structure of L.

Remark 1. The existence of L is equivalent to the assertion that the functor FGL is *corepresentable*. By general nonsense, the representability of FGL is equivalent to the following pair of properties, which are easy to verify directly:

(1) The functor FGL carries limits of commutative rings to limits of sets.

(2) The functor FGL carries κ-filtered colimits of commutative rings to κ-filtered colimits of sets, provided that κ is sufficiently large (in fact, we can take κ to be any uncountable cardinal: this reflects the fact that a formal group law is determined by a countable number of parameters).

We first note that the commutative ring $\mathbf{Z}[c_{i,j}]$ has a natural grading, where we define the degree of $c_{i,j}$ to be $2(i+j-1)$. This grading is dictated by the requirement that if we let x and y have degree -2, then the expression

$$f(x,y) = \sum_{i,j} c_{i,j} x^i y^j$$

again has degree -2. Then the power series $f(f(x,y),z)$ and $f(x, f(y,z))$ also have degree -2. It follows that the coefficients of $x^i y^j z^k$ in the $f(f(x,y),z)$ and $f(x,f(y,z))$ both have degree $2(i+j+k)-2$ in the ring $\mathbf{Z}[c_{i,j}]$. Consequently, the grading on $\mathbf{Z}[c_{i,j}]$ descends to a grading on the quotient ring $L = \mathbf{Z}[c_{i,j}]/Q$: that is, L has the structure of a graded ring. Since $c_{0,0} = 0$ and $c_{1,0} = c_{0,1} = 1$ in L, it is actually a *nonnegatively* graded ring, with $L_0 \simeq \mathbf{Z}$.

Remark 2. Our convention that the grading of L is *even* is irrelevant for this lecture. We introduce this convention in order to be compatible with the gradings which appear in topology.

Remark 3. The existence of the above grading on L can be explained more abstractly as follows. The collection of formal group laws admits an action of the multiplicative group $\mathbb{G}_m$. That is, for every commutative ring R, there is a canonical action of $R^\times$ on $\mathrm{FGL}(R)$, given by

$$f^\lambda(x,y) = \lambda^{-1} f(\lambda x, \lambda y).$$

This determines an action of $\mathbb{G}_m$ on the affine scheme $\operatorname{Spec} L$ representing the functor FGL, which is the same as the data of a grading of L. The nonnegativity of the grading reflects the observation that the action of $R^\times$ on $\mathrm{FGL}(R)$ extends to an action of the multiplicative monoid $(R, \times)$ on FGL (that is, $f(\lambda x, \lambda y)$ is formally divisible by λ). The isomorphism $L_0 \simeq \mathbf{Z}$ reflects the observation that for any formal group f, we have $f^\lambda(x,y) = x+y$ when $\lambda = 0$).

Our goal in this lecture is to begin the proof of the following result:

Theorem 4 (Lazard)**.** *The Lazard ring L is isomorphic to a polynomial ring $\mathbf{Z}[t_1, t_2, \ldots]$, where each t_i has degree $2i$.*

Theorem 4 implies that it is easy to write down formal group laws over a commutative ring R: one just needs to select a countable sequence of elements in R. In particular, formal group laws exist in abundance. Where do these formal group laws come from? We can get a good supply by combining the following pair of observations:

(a) The power series $f(x,y) = x+y$ is a formal group law (over any ring R).

(b) If $f(x,y)$ is a formal group law over the ring R and we are given some substitution $g(x) = x + b_1 x^2 + b_2 x^3 + \cdots$, then the power series $gf(g^{-1}(x), g^{-1}(y))$ is also a formal group law over R.

In particular:

(c) If g is defined as above, then $g(g^{-1}(x) + g^{-1}(y))$ is a formal group law over the polynomial ring $\mathbf{Z}[b_1, b_2, \ldots]$.

This formal group law is classified by a map $\phi : L \to \mathbf{Z}[b_1, b_2, \ldots]$. We will soon learn that this map is an isomorphism over the rational numbers (Lemma 10). That is, in characteristic zero, every formal group law is obtained from the additive formal group law $f(x,y) = x+y$ by a change of variables. This is not true in positive characteristic (otherwise, this course would be very short).

Remark 5. The map $\phi : L \to \mathbf{Z}[b_1, b_2, \ldots]$ is compatible with the gradings, if we let each b_i have degree $2i$. To see this, it suffices to note that if each b_i has degree $2i$, then $g(g^{-1}(x) + g^{-1}(y))$ has degree -2 when x and y are both given degree -2.

Let I denote the ideal in L consisting of elements of positive degree, and let J denote the ideal in $\mathbf{Z}[b_1, b_2, \ldots]$ generated by elements of positive degree (that is, the ideal generated by $b_1, b_2, \ldots$). Then J/J^2 can be identified with the free abelian group on generators $\{b_i\}_{i>0}$. Note that the quotient I/I^2 inherits a grading from the grading of L. The main step in the proof of Theorem 4 is the following calculation:

Lemma 6. *For every integer $n > 0$, the ring homomorphism map $\phi : L \to \mathbf{Z}[b_1, b_2, \ldots]$ induces an injection $(I/I^2)_{2n} \to (J/J^2)_{2n} \simeq \mathbf{Z}$. The image of this map is $p\mathbf{Z}$ if $n+1$ is a prime power p^f, and $\mathbf{Z}$ otherwise.*

We will prove Lemma 6 in the next lecture. For now, let us collect some of the consequences.

Corollary 7. *For every integer $n > 0$, the abelian group $(I/I^2)_{2n}$ is (canonically) isomorphic to $\mathbf{Z}$.*

In particular, we can choose homogeneous elements $t_n \in I_{2n} = L_{2n}$ lifting generators for $(I/I^2)_{2n} \simeq \mathbf{Z}$. This choice of generators determines a map of graded rings $\theta : \mathbf{Z}[t_1, t_2, \ldots] \to L$.

Lemma 8. *The map θ is surjective.*

Proof. We prove by induction on n that θ induces a surjection in degree $2n$. The inductive hypothesis shows that the image of θ contains $(I^2)_{2n}$. Since the image of θ contains a generator for $(I/I^2)_{2n} \simeq \mathbf{Z}$, it contains $I_{2n} = L_{2n}$. □

We now complete the proof of Theorem 4 as follows:

Lemma 9. *The composite map $\psi : \mathbf{Z}[t_1, t_2, \ldots,] \xrightarrow{\theta} L \xrightarrow{\phi} \mathbf{Z}[b_1, b_2, \ldots]$ is injective. In particular, the map θ is injective.*

Since the polynomial rings $\mathbf{Z}[t_1, t_2, \ldots]$ and $\mathbf{Z}[b_1, b_2, \ldots]$ are torsion-free, they inject into their rationalizations $\mathbf{Q}[t_1, t_2, \ldots]$ and $\mathbf{Q}[b_1, b_2, \ldots]$. Lemma 9 is therefore an immediate consequence of the following:

Lemma 10. *The map $\psi_{\mathbf{Q}} : \mathbf{Q}[t_1, t_2, \ldots] \to \mathbf{Q}[b_1, b_2, \ldots]$ is an isomorphism of commutative rings.*

Proof. Let J' denote the ideal in $\mathbf{Q}[t_1, t_2, \ldots]$ generated by the elements t_i. Then $J'/(J')^2$ is isomorphic to the free $\mathbf{Q}$-vector space generated by $t_1, t_2, \ldots$. Using Lemma 6, we see that $\phi_{\mathbf{Q}}$ induces a surjection $J'/(J')^2 \to (J/J^2)_{\mathbf{Q}}$. Repeating the proof of Lemma 8, we see that $\psi_{\mathbf{Q}}$ is surjective. Since the vector spaces $\mathbf{Q}[t_1, t_2, \ldots]$ and $\mathbf{Q}[b_1, b_2, \ldots]$ have the same dimension in every graded degree, we deduce that $\psi_{\mathbf{Q}}$ is also injective. □