Lazard's Theorem (Continued) (Lecture 3)

January 28, 2010

Our goal in this lecture is to complete the proof of Lazard's theorem. In the last lecture, we were reduced to proving the following result:

Lemma 1. *Let $\phi : L \to \mathbf{Z}[b_1, b_2, \ldots]$ be the ring homomorphism classifying the formal group law $g(g^{-1}(x) + g^{-1}(y))$, where g is the power series $g(x) = x + b_1 x^2 + b_2 x^3 + \cdots$. Let $I \subseteq L$ be the ideal consisting of elements of positive degree, and let $J \subseteq \mathbf{Z}[b_1, b_2, \ldots]$ be defined likewise. Then, for every integer $n > 0$, ϕ 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 regard n as a positive integer which is fixed throughout this lecture. Recall that for any commutative ring R, there is a canonical bijection $\epsilon : \mathrm{Hom}(L, R) \to \mathrm{FGL}(R)$, where FGL denotes the collection of formal group laws $f(x, y) \in R[[x, y]]$ over R. Suppose now that R is a graded ring, and let $\mathrm{Hom}^{gr}(L, R) \subseteq \mathrm{Hom}(L, R)$ denote the collection of all graded ring homomorphisms from L to R. Then ϵ restricts to a bijection $\mathrm{Hom}^{gr}(L, R) \simeq \mathrm{FGL}^{gr}(R)$, where $\mathrm{FGL}^{gr}(R)$ denotes the collection of formal group laws $f(x, y) = \sum a_{i,j} x^i y^j \in R[[x, y]]$ where the coefficients $a_{i,j}$ have degree $2(i + j - 1)$ (in other words, the collection of all formal group laws where $f(x, y)$ is homogeneous of degree -2, when we regard the variables x and y as having degree -2).

The main point of Lemma 1 is to show that the abelian group $(I/I^2)_{2n}$ is isomorphic to $\mathbf{Z}$: in other words, that it is free on one generator. Equivalently, we wish to show that for any abelian group M, the collection of group homomorphisms $\mathrm{Hom}((I/I^2)_{2n}, M)$ can be identified with M. Let us denote this collection of group homomorphisms by $F(M)$: that is, we let F be the functor corepresented by $(I/I^2)_{2n}$ (from the category of abelian groups to the category of sets). To proceed further, we would like to relate F to the functor corepresented by L. To this end, let us regard $\mathbf{Z} \oplus M$ as a graded commutative ring, with the "square zero" multiplication law $(a, m)(b, m') = (ab, am' + bm)$ and the grading

$$(\mathbf{Z} \oplus M)_k = \begin{cases} \mathbf{Z} & \text{if } k = 0 \\ M & \text{if } k = 2n \\ 0 & \text{otherwise.} \end{cases}$$

Unwinding the definitions, we see that evaluation in degree $2n$ induces a bijection $\mathrm{Hom}^{gr}(L, \mathbf{Z} \oplus M) \to \mathrm{Hom}((I/I^2)_{2n}, M) = F(M)$. In other words, $F(M)$ can be identified with the set $\mathrm{FGL}^{gr}(\mathbf{Z} \oplus M)$ of (homogeneous) formal group laws over $\mathbf{Z} \oplus M$. Any such formal group law can be written in the form

$$f(x, y) = x + y + \sum_{i+j=n+1} m_{i,j} x^i y^j.$$

In order for such a polynomial to define a formal group law, the coefficients $m_{i,j}$ need to satisfy some conditions. Since the multiplication on $\mathbf{Z} \oplus M$ is square-zero, it is possible to make these conditions very explicit. For example, the requirement that $f(x, 0) = f(0, x) = x$ translates into equations $m_{0,n+1} = m_{n+1,0} = 0$, while the commutativity of f is the requirement $m_{i,j} = m_{j,i}$. Associativity is only slightly more complicated: we require that for every triple of integers i, j, and k, the coefficient of $x^i y^j z^k$ appearing in the expressions $f(f(x,y),z)$ and $f(x,f(y,z))$ are the same. This follows immediately from the earlier conditions if i, j, or k is equal to zero. If $i,j,k>0$, then a simple computation (using the fact that $M^2=0$) shows that the coefficient in $f(f(x,y),z)$ is given by $\binom{i+j}{j}m_{i+j,k}$ if $i+j+k=n+1$ (and is zero otherwise). Similarly, the relevant coefficient in $f(x,f(y,z))$ is given by $\binom{j+k}{j}m_{i,j+k}$. We can summarize our discussion as follows:

Lemma 2. *The functor F carries an abelian group M to the collection of all sequences $\{m_{i,j}\in M\}_{i+j=n+1}$ satisfying the conditions*

$$m_{0,n+1}=m_{n+1,0}=0 \qquad m_{i,j}=m_{j,i}$$
$$\binom{i+j}{j}m_{i+j,k}=\binom{j+k}{j}m_{i,j+k} \text{ if } i,j,k>0.$$

We want to understand how to find all solutions to the equations appearing in Lemma 2. We can start by considering the solutions that we get using the homomorphism $\phi: L\to \mathbf{Z}[b_1,b_2,\ldots]$ appearing in Lemma 1. This homomorphism induces a map $(I/I^2)_{2n}\to(J/J^2)_{2n}\simeq\mathbf{Z}$, and therefore gives rise to a map

$$\lambda: M=\mathrm{Hom}(\mathbf{Z},M)\to\mathrm{Hom}((J/J^2)_{2n},M)\to\mathrm{Hom}((I/I^2)_{2n},M)=F(M).$$

To understand this map more explicitly, we note that $M\simeq\mathrm{Hom}((J/J^2)_{2n},M)$ can be identified with $\mathrm{Hom}^{gr}(\mathbf{Z}[b_1,b_2,\ldots],\mathbf{Z}\oplus M)$ by assigning to each $m\in M$ the ring homomorphism $\psi_m:\mathbf{Z}[b_1,\ldots]\to\mathbf{Z}\oplus M$ which carries b_n to m and all other b_i to zero. In this case, the change-of-variable transformation $g(x)=x+b_1x^2+\cdots$ can be written as $g(x)=x+mx^{n+1}$. Since $m^2=0$ in $\mathbf{Z}\oplus M$, the inverse transformation is simply given by $g^{-1}(x)=x-mx^{n+1}$. Then g defines the formal group law

$$f(x,y)=g(g^{-1}(x)+g^{-1}(y))=g(x-mx^{n+1}+y-my^{n+1})=x+y+m((x+y)^{n+1}-x^{n+1}-y^{n+1}).$$

We conclude that the map $\lambda: M\to F(M)$ carries an element $m\in M$ to the sequence $\{m_{i,j}\}_{i+j=n+1}$ given by

$$m_{i,j}=\begin{cases}0 & \text{if } i=0 \text{ or } j=0\\ \binom{n+1}{i}m & \text{otherwise.}\end{cases}$$

These are the "obvious" solutions to the equations of Lemma 2.

But sometimes there are more solutions. For example, if the binomial coefficients $\{\binom{n+1}{i}\}_{0<i<n+1}$ have greatest common divisor d, then we can write down another solution given by

$$m_{i,j}=\begin{cases}0 & \text{if } i=0 \text{ or } j=0\\ \frac{\binom{n+1}{i}}{d}m & \text{otherwise.}\end{cases}$$

It is therefore of interest to determine d. For this, we will need the following combinatorial fact:

Lemma 3. *Let p be a prime number, and suppose that a and b are nonnegative integers with base p expansions*

$$a=\sum a_ip^i \qquad b=\sum b_ip^i$$

Then $\binom{a}{b}$ is congruent to the product $\prod\binom{a_i}{b_i}$ modulo p.

Proof. Let S be a set of size a. We can partition S into subsets S_α whose sizes are powers of p, with exactly a_i subsets of size p^i. Regard each S_α as acted on by the cyclic group $G_\alpha=\mathbf{Z}/p^i\mathbf{Z}$. These actions together determine an action of $G=\prod_\alpha G_\alpha$ on S. Let T be the collection of all b-element subsets of S, so that $\binom{a}{b}=|T|$. The set T is acted on by G. Since G is a p-group, every nontrivial orbit of G has size divisible by p. Thus $|T|$ is congruent modulo p to the cardinality of T^G, the set of G-fixed points of T. Note that a G-fixed point of T is a subset $S_0\subseteq S$ of cardinality b which is a union of some of the subsets S_α. There are precisely $\prod\binom{a_i}{b_i}$ ways that these subsets can be chosen. $\square$

Corollary 4. *Let i and j be nonnegative integers, and let p be a prime number. Then the binomial coefficient $\binom{i+j}{i}$ is not divisible by p if and only if each digit in the base p expansion of $i+j$ is at least as large as the corresponding digit of i in base p: in other words, if and only if the sum $i+j$ can be computed in base p "without carrying".*

Corollary 5. *Let d be the greatest common divisor of the binomial coefficients $\{\binom{n+1}{i}\}_{0<i<n+1}$. Then* $d = \begin{cases} p & \text{if } n+1 = p^f \\ 1 & \text{otherwise.} \end{cases}$

Proof. If $n+1$ is not a power of p, then we can nontrivially decompose $n+1$ as a sum $i+j$, where the sum of i and j is computed in base p without carrying; it follows that $\binom{n+1}{i}$ is not divisible by p. If $n+1 = p^f$, then there is no such decomposition, so that p is a common divisor of $\{\binom{n+1}{i}\}_{0<i<n+1}$. To see that it is the greatest common divisor, we note that p^2 does not divide the binomial coefficient $\binom{p^f}{p^{f-1}}$. □

We let $\lambda' : M \to F(M)$ be the map which carries $m \in M$ to the sequence

$$m_{i,j} = \begin{cases} 0 & \text{if } i = 0 \text{ or } j = 0 \\ \frac{\binom{n+1}{i}}{d} m & \text{otherwise.} \end{cases}$$

We will prove the following:

Proposition 6. *The map λ' is an isomorphism.*

It follows from Proposition 6 that the functor $F(M)$ is corepesentable by the abelian group $\mathbf{Z}$: that is, we get an isomorphism $(I/I^2)_{2n} \simeq \mathbf{Z}$. Moreover, the map λ factors as a composition

$$M \xrightarrow{d} M \xrightarrow{\lambda'} F(M),$$

so that the map

$$\mathbf{Z} \simeq (I/I^2)_{2n} \to (J/J^2)_{2n} \simeq \mathbf{Z}$$

is given by multiplication by d. This completes the proof of Lemma 1.

To prove Proposition 6, it suffices to show that λ' induces an isomorphism $M_{(p)} \to F(M)_{(p)} \simeq F(M_{(p)})$ after localizing at every prime p. In other words, we may assume that M is a $\mathbf{Z}_{(p)}$-module.

Lemma 7. *Let $\{m_i = m_{i,j}\}_{i+j=n+1}$ be an element of $F(M)$. Then:*

- (a) *If $m_i = 0$, then $m_{n+1-i} = 0$.*
- (b) *If $m_i = 0$ and the sum $i+j$ is computed in base p without carrying, then $m_{i+j} = 0$ vanishes.*

Proof. Assertion (a) follows by symmetry. To prove (b), we use the associativity formula

$$\binom{n+1-i}{j} m_i = \binom{i+j}{j} m_{i+j}.$$

If m_i vanishes, then the left hand side vanishes, so (since $\binom{i+j}{j}$ is not divisible by p, by Corollary 4) we conclude that m_{i+j} vanishes. □

Proof of Proposition 6 when $n+1 = p^f$. Let $\chi : F(M) \to M$ be given by extracting the coefficient $m_{p^{f-1}}$. Then the composition $\chi \circ \lambda' : M \to M$ is given by multiplication by $\frac{\binom{p^f}{p^{f-1}}}{p}$, which is not divisible by p. Consequently, $\chi \circ \lambda'$ is an isomorphism, which proves that λ' is injective. To show that λ' is surjective, it suffices to show that χ is injective. Let $\{m_i\} \in F(M)$ belong to the kernel of χ, so that $m_{p^{f-1}}$ vanishes. Part (b) of Lemma 7 shows that m_k vanishes for $p^{f-1} \leq k < p^f$. Using symmetry, we deduce that m_k vanishes for all $0 < k < p^f$. □

Proof of Proposition 6 when $n+1 \neq p^f$. Let p^e be the largest power of p which divides $n+1$. We let $\chi : F(M) \to M$ be given by extracting the coefficient of m_{p^e}. Then $\chi \circ \lambda' : M \to M$ is given by multiplication by $\frac{\binom{n+1}{p^e}}{d}$; here d is either 1 or some prime distinct from p, and the binomial coefficient $\binom{n+1}{p^e}$ is not divisible by p by Corollary 4. As before, we deduce that $\chi \circ \lambda'$ is an isomorphism, λ' is injective, and we are reduced to proving that χ is injective. Suppose that $\{m_i\} \in F(M)$ belongs to the kernel of χ. Then $m_{p^e} = 0$.

Assume $e > 0$ (if not, ignore this step). By symmetry, we get $m_{n+1-p^e} = 0$. Since $n+1-p^{e-1}$ can be obtained as a sum of $n+1-p^e$ and $(p-1)p^{e-1}$ in base p without carrying, we deduce that $m_{n+1-p^{e-1}} = 0$. By symmetry, we get $m_{p^{e-1}} = 0$.

Now choose any nontrivial decomposition $n+1 = i+j$. We wish to prove that $m_i = m_j = 0$. Since $n+1$ has a nontrivial coefficient on p^e in its base p expansion, we conclude that either i or j must contain a nonzero coefficient on p^e or p^{e-1} in its base p expansion. Without loss of generality, we may suppose that i has a nonzero p^a coefficient in its base p-expansion, with $a \in \{e-1, e\}$. Then we can write $i = p^a + (i - p^a)$ in base p without carrying. Since m_{p^a} vanishes by the above argument, we conclude from Lemma 7 that $m_i = 0$. $\square$