Leisurely proof of Lazard's theorem

February 22, 2013

Introduction

This note is for topologists who are sick of hearing "And then there was a theorem proved by Lazard that we apply here..."

More specifically, we intend to show that formal group laws are given by maps out of a polynomial ring on infinitely many variables. The author learned the proof given here from Hopkins' famous notes, [1]. Also Akhil's blog post on this is nice, [2].

Enjoy!

Formal group laws

We may as well start by defining our object of study, though we hope you've seen this before.

Definition. A *formal group law* over a ring, R, is a power series $F \in R[[x, y]]$ satisfying the following axioms:

1. (Associativity) $F(x, F(y, z)) = F(F(x, y), z)$
2. (Commutativity) $F(x, y) = F(y, z)$
3. (Unit) $F(x, 0) = F(0, x) = x$

In interest of space, we usually write $f(x, y)$ as $x +_F y$.

We see that this definition gives us a functor

$$FGL : \mathbf{Ring} \to \mathbf{Set}$$

where we assign to each ring the set of formal group laws over that ring, and the functoriality is given in the obvious manner.

This functor is actually corepresentable. One can see this by abstarct nonsense (the functor preserves limits and $\aleph_1$-filtered colimits), or by direct construction:

Let $R_U = \mathbb{Z}[a_{ij}]/\sim$ where the relations are precisely those such that the formal power series $f = \sum a_{ij} x^i y^j$ satisfies the axioms for a formal group law, these are some polynomials in a_{ij}, so we're good. Now we have a universal formal group law over R_U given by $F_U(x, y) = \sum a_{ij} x^i y^j$, by definition.

It turns out this ring has a natural grading. There's a neat way to get this that we'll spell out, basically we have:

Proposition. *A ring R is graded (concentrated in even degrees if you want) if and only if there is an action of $\mathbb{G}_m$ on Spec R.*

Before we prove this we should say what we mean. For our purposes, Spec R means the functor

$$\mathbf{Rings} \to \mathbf{Set}$$

given by $A \mapsto \mathrm{Hom}_{\mathbf{Rings}}(R, A)$, i.e. the functor corepresented by R. The symbol $\mathbb{G}_m$ is the "multiplicative group," and it denotes the functor

$$\mathbb{G}_m : \mathbf{Rings} \to \mathbf{Group}$$

given by

$$A \mapsto A^\times$$

This is the same as saying that $\mathbb{G}_m$ is given by $\mathrm{Spec}(\mathbb{Z}[t, t^{-1}])$ where we need to remember the Hopf algebra structure on this ring to get a functor into groups.

An action of $\mathbb{G}_m$ on Spec R is then just given by a natural transformation

$$\mathbb{G}_m \times \mathrm{Spec}\ R \to \mathrm{Spec}\ R$$

satisfying the usual diagrams that we write down when we have, say, a group acting on a set. Ok, so now we're in a position to prove the proposition.

Proof. Suppose that R is an honestly commutative, graded ring. Define a map

$$R \to \mathbb{Z}[t, t^{-1}] \otimes R$$

given on homogeneous elements of degree n by

$$r \mapsto t^n \otimes r$$

This gives a map of functors

$$\mathbb{G}_m \times \mathrm{Spec}\ R \to \mathrm{Spec}\ R$$

satisfying the necessary axioms. Explicitly we have:

$$A^\times \times \mathrm{Hom}(R, A) \cong \mathrm{Hom}(\mathbb{Z}[t, t^{-1}] \otimes R, A) \to \mathrm{Hom}(R, A)$$

where we've used the fact that $\otimes$ is the coproduct in the category of rings.

On the other hand, given an action of the multiplicative group, we see that this is the same as a map

$$R \to \mathbb{Z}[t, t^{-1}] \otimes R$$

making a few diagrams commute (essentially via the Yoneda lemma), and so declare a grading by saying $x \in R$ is of degree n if its image is of the form $t^n \otimes x$. □

Now, there is a natural action of $\mathbb{G}_m$ on FGL given, for each $\lambda \in A^\times$ and formal group law F over A, via

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

So we get a grading on R_U. One can check that we have $|a_{ij}| = i + j - 1$. Indeed, the action defines a map

$$R_U \to \mathbb{Z}[t, t^{-1}] \otimes R_U$$

corresponding to the formal group law given by

$$t^{-1} F_U(tx, ty)$$

where F_U is the universal formal group law. The coefficient of $x^i y^j$ looks like

$$t^{-1}(t^i t^j a_{ij})$$

thus a_{ij} is homogeneous of degree $i + j - 1$.

To be consistent with the usual notion of graded commutativity and with topology, we will adjust all gradings so that

$$|a_{ij}| = 2(i + j - 1)$$

but don't worry about this- everything will be okay. One can check that R_U is connected, i.e. $(R_U)_0 = \mathbb{Z}$, and concentrated in non-negative degrees.

While innocent looking, this grading will give us a very convenient way of dealing with R_U. Any time we have a connected, non-negatively graded ring, R, we can consider a graded abelian group QR given by

$$QR = R_{>0}/R_{>0}^2$$

where $R > 0$ is the ideal of positively graded elements. Our goal will be to understand

$$(QR_U)_{2n}$$

and see if that gives us any hints about what R_U has to be. So we'll be interested in maps

$$(QR_U)_{2n} \to M$$

where M is an abelian group.

We'd like to actually prove that $(QR_U)_{2n}$ is $\mathbb{Z}$. It turns out that, amongst finitely generated abelian groups, $\mathbb{Z}$ has a universal property: it's the only one, A, for which

$$\mathrm{Hom}_{\mathbf{AbGrp}}(A, \mathbb{Q}) \cong \mathbb{Q}, \text{ and } \mathrm{Hom}_{\mathbf{AbGrp}}(A, \mathbb{Z}/p) \quad (\forall p)$$

So we are left with studying maps

$$(QR_U)_{2n} \to k, \quad k = \mathbb{Q}, \mathbb{Z}/p$$

The trouble is that R_U is defined via a property about rings, so we really only know how to study ring maps... But we can transform this problem into one with ring maps:

Lemma. *Let R be a connected, graded commutative ring concentrated in even, non-negative degrees, and M an abelian group. There is a natural bijection*

$$Hom_{\mathbf{AbGrp}}(QR_{2n}, M) \cong Hom_{\mathbf{GrRing}}(R, \mathbb{Z} \oplus M_{2n})$$

where $\mathbb{Z} \oplus M_{2n}$ is the graded ring with a $\mathbb{Z}$ in degree 0, and M in degree $2n$ and multiplication given by $(a, b)(c, d) = (ab, ac + bd)$.

Proof. Given a map $QR_{2n} \to M$ we get a map $R_{>0} \to M$, and combining with the isomorphism $R_0 \cong \mathbb{Z}$ gives us a ring map as on the right. Going backwards we note that the definition of multiplication for $\mathbb{Z} \oplus M$ forces decomposable elements to go to zero, and so we get a map as on the left. □

So we are interested in maps of graded rings $R_U \to \mathbb{Z} \oplus k_{2n}$. Notice that our requirement that this be a ring map tells us that we have an isomorphism on 0th-degree, so we are really looking for lifts in the following diagram

$$\begin{tikzcd}
 & \mathbb{Z} \oplus k_{2n} \arrow[d] \\
R_U \arrow[ur, dashed] \arrow[r] & \mathbb{Z}
\end{tikzcd}$$

These correspond to special formal group laws over $\mathbb{Z} \oplus k_{2n}$ that agree with the additive one, modulo k.

Remark 1. It'd be really neat if someone could tell me how to word this as a deformation problem of the form "We know something over the generic point, and now we want to deform over the rest of Spec $\mathbb{Z}$ to see what happens... so we look at André-Quillen cohomology..." But I haven't figured out how to do this. It seems close but a few pesky things are in the way, the first being the appearance of $\mathbb{Z}$ above instead of $\mathbb{Q}$.

So we are looking for power series that are of the form

$$F(x,y) = x + y + f(x,y)$$

where $f(x,y)$ is a polynomial with coefficients in k where each term has total degree $n+1$. This polynomial satisfies the following conditions:

1. $f(x,0) = f(0,x) = 0$
2. $f(x,y) = f(y,x)$
3. $f(y,z) - f(x+y,z) - f(x,y+z) - f(x,y) = 0$

The last condition follows from the associativity condition for a formal group law. Indeed, the degree $n+1$ part of $F(x, F(y,z))$ is

$$x + y + z + f(y,z) + f(x, y+z)$$

and the degree $n+1$ part of $F(F(x,y),z)$ is

$$x + y + z + f(x,y) + f(x+y,z)$$

Now the key point is to notice that the last condition reminds us of a "cocycle" type condition. Indeed, let $k[x]$ denote the abelian group of polynomials with coefficients in k, and consider the complex

$$\begin{tikzcd} k \arrow[r, "d^0"] & k[x] \arrow[r, "d^1"] & k[x,y] \arrow[r, "d^2"] & k[x,y,z] \end{tikzcd}$$

where

$$d^0(a) = a$$
$$d^1(f(x)) = f(x+y) - f(x) - f(y)$$
$$d^2(f(x,y)) = f(y,z) - f(x+y,z) - f(x,y+z) - f(x,y)$$

So what we are concerned with is the kernel of d^2. The 2-coboundaries are easy to understand, so it would be helpful to compute this cohomology.

Let me write this complex slightly differently, and extend it to a larger complex. We start by endowing $k[x]$ with a coalgebra structure, where x is primitive. Then we write down the cobar complex for k. This looks like:

$$\begin{tikzcd} 0 \arrow[r] & k \arrow[r] & k[x] \otimes_k k \arrow[r] & k[x]^{\otimes 2} \otimes_k k \arrow[r] & k[x]^{\otimes^3} \otimes_k k \arrow[r] & \cdots \end{tikzcd}$$

We represent an element of $k[x]^{\otimes n+1} \otimes_k k$ as having basis elements

$$[f_0|f_1|\cdots|f_n]a$$

where the $f_i \in k[x]$ are polynomials and $a \in k$. The differentials are given by

$$d([f_0|f_1|\cdots|f_n]a) = [f_0'|f_0''|f_1|\cdots|f_n]a - [f_0|f_1'|f_1''|\cdots|f_n]a + \cdots + (-1)^{n+1}[f_0|\cdots|f_n|f']a'$$

Now if we apply $\mathrm{Hom}_{k[x]}(k,-)$ to this complex we get another one that looks like

$$\begin{tikzcd} k \arrow[r] & k[x] \arrow[r] & k[x]^{\otimes 2} \arrow[r] & k[x]^{\otimes^3} \arrow[r] & \cdots \end{tikzcd}$$

and one can check that the differential agrees with what we had earlier! So even though we didn't realize it, we've been interested in

$$\mathrm{Ext}^2_{k[x]}(k,k)$$

(thinking about everything as coalgebras an comodules, and I should be inserting a grading somewhere).

If I'd had more time I would've tried to do this purely in the land of coalgebras, but alas... who has time? So let's dualize and then we're talking about computing

$$\mathrm{Ext}_{\Gamma[t]}(k,k)$$

And now I should explain what $\Gamma[t]$ is and what's going on.

The deal is that, for the polynomial algebra $k[x]$, where x is primitive, we can compute that

$$\Delta(x^n) = \sum \binom{n}{k} x^k y^{n-k} \in k[x,y]$$

So if I want to take the dual gadget (an *algebra*) then it will have generators $t^{(n)}$ that satisfy

$$t^{(n)}t^{(m)} = \binom{n+m}{n} t^{(n+m)}, \quad t^{(0)} = 1.$$

So now there are really only two cases to consider.

Case 1: $\mathbb{Q}$

When $k = \mathbb{Q}$ life is easy: divided power algebras are the same as polynomial algebras, and so we're interested in computing

$$\mathrm{Ext}_{\mathbb{Q}[t]}(\mathbb{Q},\mathbb{Q})$$

Well, consider the resolution

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Q}[t] \arrow[r] & \mathbb{Q}[t] \arrow[r] & \mathbb{Q} \arrow[r] & 0 \end{tikzcd}$$

so $\mathrm{Ext}^2 = 0$, which, if we trace everything back means that the symmetric 2-cocycles are 1-dimensional over $\mathbb{Q}$.

Case 2: $\mathbb{F}_p$

. If $k = \mathbb{F}_p$, then the coalgebra $k[x]$ actually decomposes as a tensor product of coalgebras of the form A_n where

$$A_n = k < x^{p^n}, x^{2p^n}, ..., x^{(p-1)p^n} >$$

that is to say that

$$\Delta(x^{kp^n}) = (x+y)^{kp^n} = (x^{p^n} + y^{p^n})^k, \quad 1 \le k < p$$

is a polynomial in x^{mp^n} and y^{mp^n} for $1 \le m < p$. The dual of this gadget is just a truncated polynomial algebra (since the various binomial coefficients we want to invert are invertible in $\mathbb{F}_p$- they are all less than p.) That means we have a decomposition

$$\Gamma[t] = \bigotimes \mathbb{F}_p[t^{(p^k)}]/(t^{(p^k)})^p$$

By the Künneth formula, this means we really just need to study

$$\mathrm{Ext}_A(\mathbb{F}_p,\mathbb{F}_p)$$

where $A = \mathbb{F}_p[t]/t^p$. But we already know how to do this, because this is like the group cohomology of $\mathbb{Z}/p$. We can write down a nice complex and get that, as an algebra, this looks like

$$\mathrm{Ext}_A(\mathbb{F}_p,\mathbb{F}_p) = \Lambda(\alpha) \otimes \mathbb{F}_p[\beta]$$

for p odd, and

$$\mathrm{Ext}_A(\mathbb{F}_2,\mathbb{F}_2) = \mathbb{F}_p[\alpha]$$

where $\alpha \in \mathrm{Ext}^1$ and $\beta \in \mathrm{Ext}^2$. In the bar complex, α is dual to x^{p^n} and β is dual to $\frac{1}{p^n}((x+y)^{p^n} - x^{p^n} - y^{p^n})$.

Putting all of this together we get that $\mathrm{Ext}^2_{\Gamma[t]}(\mathbb{F}_p, \mathbb{F}_p)$ is generated by elements of the form $\alpha_i\alpha_j$ and β_k, dual to $x^{p^i}y^{p^j}$ and

$$\frac{1}{p}\left((x+y)^{p^k} - x^{p^k} - y^{p^k}\right)$$

when p is odd, and by elements of the form $\alpha_i\alpha_j$ and α_k^2 where α_k^2 is dual to

$$\frac{1}{2}\left((x+y)^{2^k} - x^{2^k} - y^{2^k}\right)$$

In summary:

Corollary. *The 2-cocycles are generated by elements of the form $C_n(x,y)$ and $x^{p^i}y^{p^j}$. Therefore, the symmetric 2-cocycles are generated by elements of the form $C_n(x,y)$*

Translating this back into formal group laws, we are saying that maps of abelian groups

$$\mathbb{Z} \cong Q(R_U)_{2n} \to M$$

correspond to formal group laws over $\mathbb{Z} \oplus M$ that look like

$$x + y + aC_n(x,y)$$

where a is the image of our chosen generator of $Q(R_U)_{2n}$.

Wrapping up

Okay! So we've shown that $\mathbb{Q}(R_U)_{2n}$ is canonically isomorphic to $\mathbb{Z}$. This gives us a map of graded rings

$$\mathbb{Z}[x_1, x_2, ...] \to R_U$$

by lifting generators- here $|x_i| = 2i$. The map is surjective on indecomposables, and so it is surjective (exercise!)

So we need only show that this thingy is injective, and we're good.

To do this, let's compare R_U with the ring of "all the formal group laws one can get via isomorphisms and the additive one." That is, we have a map

$$R_U \to \mathbb{Z}[m_1, m_2, ...]$$

classifying the following formal group law... Let

$$g(x) = x + m_1x^2 + m_2x^3 + \cdots$$

and define a formal group law via

$$G(x,y) = g^{-1}(g(x) + g(y))$$

Now we have maps

$$L \to R_U \to \mathbb{Z}[\mathbf{m}]$$

And to show that the left hand side is injective it's enough to show the composite is injective. Since this is a map of graded, polynomial rings it is enough to show that the map on indecomposables is injective... so we need to check that

$$Q(R_U)_{2n} \to \mathbb{Z}$$

is injective. What is that map? Well, it's the one corresponding to a formal group law over $\mathbb{Z} \oplus Q\mathbb{Z}[\mathbf{b}]_{2n}$. To get it, we note that in this quotient we get

$$g \equiv x + m_n x^{n+1}, \quad g^{-1} \equiv x - m_n x^{n+1}$$

so that...

$$\begin{aligned} G(x,y) = g^{-1}(g(x)+g(y)) &\equiv g^{-1}(x+y+m_n(x^{n+1}+y^{n+1})) & (1) \\ &= x+y+m_n(x^{n+1}+y^{n+1}) - m_n(x+y+\cdots)^{n+1} & (2) \\ &= x+y+m_n(x^{n+1}+y^{n+1}-(x+y)^{n+1})+\cdots & (3) \\ &\equiv x+y-d_{n+1}m_nC_{n+1}(x,y) & (4) \end{aligned}$$

so the map $\mathbb{Z} \cong Q(R_U)_{2n} \to Q\mathbb{Z}[\mathbf{m}]_{2n}$ sends 1 to $-d_{n+1}m_n$, which is nonzero, so we have an injective map. This completes the proof!!

Remark 2. This proof has a few puzzling components. For example, a priori we only cared about $Q(R_U)_{2n}$ as an abelian group, but in order to study it we ended up talking about fields and coalgebras over them. We introduced an ad-hoc Hopf algebra structure that happened to fit. I have trouble finding good moral reasons for doing all of this; if anyone has insight, please let me know!

References

[1] Hopkins, MJ. *Complex Oriented Cohomology Theories and the Language of Stacks.* Topology underground.

[2] Mathews, Akhil. *Lazard's Theorem II.* amathew.wordpress.com