LAZARD'S RING AND HEIGHT

ISHAN LEVY

1. Lazard's ring and consequences

Here a formal group law over a ring R means a one-dimensional commutative formal group law over R. Lazard's ring, denoted L, is the ring with the universal formal group law, i.e. it represents the functor FGL sending a ring to the set of all formal group laws. We are interested in it because in the connection between formal group laws and complex oriented theories, L is MU_*, and the universal formal group law is exactly the one on MU. Lazard's theorem states that L is a polynomial ring $\mathbb{Z}[t_1, t_2, \dots]$ on infinitely many generators.

One way to produce formal group laws is to change coordinates: i.e. one can take a formal group law $f(x, y)$, and an invertible power series $g(t) = t + b_1 t^2 + b_2 t^3 + \dots$, $g(f(g^{-1}(x), g^{-1}(y)))$ is a formal group law. The universal way of doing this produces a formal group law over the ring $C = \mathbb{Z}[b_1, b_2, \dots]$, i.e. a map $L \to C$. In fact, C with its formal group law is $H_*(MU)$, and the map from L is the Hurewicz map!

An important observation is that L and C come with a natural grading, so that $L \to C$ is a graded map. Namely, L also represents formal group laws on $\mathbb{Z}$-graded rings. A formal group law on a $\mathbb{Z}$-graded ring is one where $f(x, y) = \sum_{i,j} c_{ij} x^i y^j$ has c_{ij} in degree $(2(i + j - 1))$. This is so that if x, y each have degree -2, then $f(x, y)$ also has degree -2. The factor of 2 is to agree with topological gradings.

Let I, J be the ideals of elements of positive degree on L, C respectively. Then the main idea leading to understanding Lazard's ring is to linearize the problem:

Lemma 1.1. *The map $L \to C$ induces a map $I/I^2 \to J/J^2$ that is an isomorphism in degree $2n$ when $n + 1 \neq p^k$ for any prime p, $k > 0$, and is the inclusion of a subgroup of index p otherwise.*

Let t_i be homogeneous in I and project to the generator of I/I^2 in degree $2i$.

Corollary 1.2. *L is $\mathbb{Z}[t_1, t_2, \dots]$. Moreover $L \otimes \mathbb{Q}$ maps isomorphically to $C \otimes \mathbb{Q}$.*

Proof. L is generated by the t_i since L is $\mathbb{Z}$ in degree 0, I/I^2 is generated by t_i, and the t_i are in positive degree. To see that there are no relations, note that the since the map $I/I^2 \to J/J^2$ is rationally an isomorphism, which again since the generators are in different degrees implies that the map $L \otimes \mathbb{Q} \to \mathbb{C} \otimes \mathbb{Q}$ is an isomorphism. Now the fact that there are no relations among the t_i follows from graded dimension counting of $C \otimes \mathbb{Q}$ and $\mathbb{Z}[t_1, t_2, \dots]$. □

We should expect that the map rationally $L \otimes \mathbb{Q} \cong C \otimes \mathbb{Q}$ since the Hurewicz map is a rationally an isomorphism for spectra. However, it has the following consequence:

Date: 3/11/2020.

Corollary 1.3. *Let R be a $\mathbb{Q}$-algebra. Then for any two formal group laws over R, there is a unique strict isomorphism between them.*

Later, the isomorphism will be made explicit.

2. The computation

Here Lemma 1.1 is proven. To understand the map $I/I^2 \to J/J^2$ in degree $2n$, we will understand the functors they corepresent. Let M be an abelian group.

$$\mathrm{Hom}((I/I^2)_{2n}, M) = \mathrm{Hom}((I/I^2)^+_{2n}, M^+_{2n}) = \mathrm{Hom}(L, M^+_{2n}) = FGL(M^+_{2n})$$

Here M^+_m is the functor that takes an abelian group M to the ring which has a $\mathbb{Z}$ in degree 0, M in degree m, and trivial multiplication apart from the action of $\mathbb{Z}$ on M and itself. Thus we need to understand formal group laws on M^+_{2n}. These are given by $f(x,y) = c_{i,j}x^iy^j$, $c_{i,j} \in M$, but because of the grading, $c_{i,j} = 0$ unless $i + j = n + 1$. Thus let us call $c_{i,j}$ just c_i for short. Then $c_0 = 0$ by the identity law, and commutativity tells us $c_i = c_{n+1-i}$. Associativity amounts to the identity $c_{i+j}\binom{i+j}{i} = c_{j+k}\binom{j+k}{j}$ whenever $i + j + k = n + 1$.

There are "obvious" solutions of these equations, namely those coming from the map $I/I^2 \to J/J^2$. These are given by changing coordinates from the additive formal group via the power series $g = t + mt^{n+1}$. These give the solutions $c_i = \binom{n+1}{i}m$ for $1 \le i \le n$. Are these all the solutions? Well, let d_n be the gcd of $\binom{n+1}{i}$ for $1 \le i \le n$. Then $c_i = \frac{\binom{n+1}{i}}{d_n}m$ are solutions. So what is d_n? Recall that to compute binomial coefficients mod p, we simply multiply the binomial coefficients of the coefficients in the p-adic expansions of the numerators and denominators. From this we get:

Lemma 2.1. *$p|\binom{i+j}{i}$ iff $i + j$ can be added in base p without carrying.*

If $n + 1$ is not a power of p, we can write $n + 1 = i + j$ where the nonzero digits of i, j in base p are distinct, so p doesn't divide $\binom{n+1}{i}$. If $n + 1 = p^k$, then regardless of which i we choose, we will have to carry, so p divides the gcd of the $\binom{n+1}{i}$. In fact, the p-adic valuation of $\binom{p^k}{p^{k-1}}$ is 1, so the gcd is p. Summarizing:

Lemma 2.2. *d_n is 1 if $n + 1$ isn't a prime power, and is p if $n + 1 = p^k$.*

Proposition 2.3. *$c_i = \frac{\binom{n+1}{i}}{d_n}m$ gives an isomorphism $\phi : M \cong \mathrm{Hom}((I/I^2)_{2n}, M)$.*

Proof. To show it is an isomorphism, it suffices to check locally at a prime p, so assume M be a $Z_{(p)}$-module. Each c_i gives a map $c_i : \mathrm{Hom}((I/I^2)_{2n}, M) \to M$. By choosing i so that $\binom{n+1}{i}$ has the smallest p-adic valuation, the composite $c_i \circ \phi$ is multiplication by an unit, so ϕ is injective. To show surjectivity, it suffices to show that this c_i is injective. If $n + 1 \neq p^k$, then we can take $i = 1$, and otherwise take $i = p^{k-1}$. From Lemma 2.1 and the associativity constraint, we obtain that $c_j = 0$ implies $c_{k+j} = 0$ whenever $k + j$ can be added without carrying. Moreover, $c_j = 0$ implies $c_{n+1-j} = 0$. These together show that $c_i = 0$ implies everything is 0. □

Thus $(I/I^2)_{2n}$ is $\mathbb{Z}$, and the map to $(J/J^2)_{2n} = \mathbb{Z}$ is multiplication by d_n.

3. Height

We saw that there is essentially one formal group for a $\mathbb{Q}$-algebra, but what about in characteristic p? Tensoring our map $L \to C$ with $\mathbb{Z}/p\mathbb{Z}$, we see that $(I/I^2)_{2n} \to (J/J^2)_{2n}$ is an isomorphism unless $n+1 = p^k$, when it is the zero map. The lack of injectivity and surjectivity suggests that not only are distinct formal group laws (surjectivity), but they can also have nontrivial strict automorphisms (injectivity), and that this failure is focused on the degrees of prime power.

The multiplicative formal group law $x + y + xy$ and the additive formal group law $x + y$ are isomorphic over $\mathbb{Q}$ via $e^x - 1$. This doesn't have integral coefficients, so they are not isomorphic over $\mathbb{Z}$ by triviality of automorphism groups over $\mathbb{Q}$. However this doesn't tell us about if they are isomorphic over $\mathbb{Z}/p\mathbb{Z}$.

To construct an invariant of formal group laws mod p, we can first construct an invariant of maps F between formal group laws. First we should observe that a formal group law f has a unique translation invariant 1-form ω_f of the form $(1+O(t))dt$, spanning the invariant forms as an R-module. For example, for the additive formal group law it is dt, and for the multiplicative one it is $\frac{dt}{1+t}$.

Lemma 3.1. *Given a formal group law f over R, there is a unique translation invariant 1-form ω_f of the form $(1 + O(t))dt$.*

Proof. For a form $g(t)dt = \sum g_i t^i dt$ to be invariant, we ask that $f^*(g(t)dt) := g(f(x,y))(\frac{df}{dx}dx + \frac{df}{dy}dy) = g(x)dx + g(y)dy$. Setting $x = dy = 0, dx = 1$, we get $g(y)\frac{df}{dx}(0,y) = g(1)$ This gives a formula for $g(y)$ in terms of $g(1)$, showing the unique solution g, and that the unique solution generates the invariant forms as an R-module. To see that the formula works, it suffices to show it on the universal formal group law on L. But the formal group law on $L \otimes \mathbb{Q}$ has an invariant form since it is isomorphic to the additive formal group law, and the form must be given by the formula by uniqueness. One could equally well compute that the formula gives an invariant form. □

One can construct explicitly the isomorphism between a formal group law and the additive formal group law by integrating the invariant differential form. Namely if $\sum_i g_i t^i dt$ is the invariant form, then $\sum_i \frac{g_i}{i+1} t^{i+1}$, called the logarithm, is the strict isomorphism to the additive formal group law. To see this, if ω_f is the invariant form, we can integrate the equation $\omega_f(f(x,y)) = \omega_f(x) + \omega_f(y)$ with respect to x to get $\log_f(f(x,y)) = \log_f(x) + c(y)$ for some constant of integration c, which by symmetry has to be $\log_f(y)$. Thus $\log_f$ is a homomorphism to the additive formal group law, and has an inverse as it is an invertible power series. For example, MU's logarithm is $\sum_n \frac{[\mathbb{CP}^n]}{n+1} t^n$ which lets you compute the logarithm for any other complex oriented theory since MU is universal.

Now given a morphism F between formal group laws f, f', we have $F^*(\omega_{f'})$ is an invariant form on f, so is $\lambda\omega_f$, where λ is the linear term of F. Assume we are in characteristic p and $\lambda = 0$. Then since $0 = F^*(\omega_{f'}) = (1 + O(t))dF$, we must have $dF = 0$, which means $F(t) = F_1(t^p)$ for some power series F_1. But if f^p is the formal group law obtained from f by applying Frobenius to the coefficient ring, then F_1 is a morphism from f^p to f', so we can repeat this argument to obtain:

Proposition 3.2. *Given a nonzero morphism F between two formal group laws f, f' in characteristic p, there is a unique k such that $F(t) = F_k(t^{p^k})$, where $F_k = \lambda t + O(t^2)$ with $\lambda \neq 0$.*

We call this k the **height** of the morphism F, denoted ht_F. We declare the 0 morphism to have infinite height. One easily sees from definition that if G, F are composable, then $ht_G + ht_F = ht_{G\circ F}$. If λ is invertible, then the kernel of the map F on $R[[x]]$ is $R[[x]]/(F)$ which is a group scheme of rank p^{ht_F}.

Since our formal group laws f are commutative, the n-series of f, $[n]$, defined by $[1] = t, [n+1] = f([n](t), t)$ is an endomorphism that looks like $nt + O(t^2)$. Thus in characteristic p, $[p]$ is an endomorphism of height ≥ 1; this is called the **height** of the formal group law f, and is easily seen to be an invariant.

For example, the additive group law is infinite height, and the multiplicative group law is height 1 since $[p] = (1+t)^p - 1 = t^p$.

Every elliptic curve E induces a formal group $\hat{E}$ in the formal neighborhood of the identity via its addition law. From this point of view, the height of a map of formal group is an analog of the inseparable degree of an isogeny. More precisely,

Proposition 3.3. *If $E_1 \to E_2$ is an isogeny of elliptic curves, then the p-adic valuation of the inseparable degree of the map is the height of $\hat{E}_1 \to \hat{E}_2$.*

Since the degree of $[p]$ on an elliptic curve is p^2, we see that there are two possible heights, 1 or 2. These two cases are called **ordinary** and **supersingular**. We see that in the super singular case, since the extension is purely inseparable, there are no nontrivial geometric p-torsion.