FORMAL GROUPS

N. P. STRICKLAND

Note: This document is not really finished. In particular, there are no references to the literature, although almost nothing is original. I have nonetheless put it online, because some people asked me about results in Section 18.

1. Introduction

Definition 1.1. A *formal group law (FGL)* over a ring R is a formal power series $F(x,y) = \sum_{i,j\geq 0} a_{ij}x^iy^j \in R[\![x,y]\!]$ that formally satisfies the axioms for a commutative group operation with 0 as the identity element. More precisely, we must have

(a) $F(x,0) = x \in R[\![x]\!]$
(b) $F(x,y) = F(y,x) \in R[\![x,y]\!]$
(c) $F(x,F(y,z)) = F(F(x,y),z) \in R[\![x,y,z]\!]$
(d) There is a power series $m(x) \in R[\![x]\!]$ such that $m(0) = 0$ and $F(x,m(x)) = 0$.

We also write $x +_F y$ for $F(x,y)$ and $[-1](x)$ or $[-1]_F(x)$ for $m(x)$. If $k > 0$ we define $[k](x) = [k]_F(x) = x +_F \ldots +_F x$, with k terms. We do not need any brackets because of condition (c). We also define $[-k](x) = [-1]([k](x))$ and $[0](x) = 0$. One checks that $[j+k](x) = [j](x) +_F [k](x)$ and $[jk](x) = [j]([k](x))$ for all $j, k \in \mathbb{Z}$.

Remark 1.2. Here and elsewhere, rings are assumed to be commutative and to have a unit unless otherwise stated.

Remark 1.3. In conditions (c) and (d) we need to substitute one formal power series into another. This leads to nonsense if the power series involved have nonzero constant terms. For example, if we try to substitute the constant series 1 for x and y we get $\sum_{ij} a_{ij}$ which typically makes no sense because we have no notion of convergence. However, if the constant terms are zero then there is no problem in expanding everything out formally.

Remark 1.4. We will later define *formal groups*, and it will turn out that a formal group law is what you get from a formal group with a specified coordinate. There are many advantages to the coordinate-free approach, but it is a bit abstract so we postpone it.

Definition 1.5. We write $\mathrm{FGL}(R)$ for the set of all FGL's over R.

Example 1.6.
(1) The simplest example is $F(x,y) = x + y$; this is called the additive FGL. It can be defined over any ring R.
(2) If $u \in R$ then we can take $F(x,y) = x + y + uxy$, so that
$$1 + u(x +_F y) = (1 + ux)(1 + uy).$$
In the case $u = 1$, this is called the multiplicative FGL. It can again be defined over any ring R.
(3) If c is an invertible element of R then we can define $F(x,y) = (x+y)/(1+xy/c^2)$. We call this the Lorenz FGL; it is the formula for relativistic addition of parallel velocities, where c is the speed of light. We are implicitly using the fact that $(1 + xy/c^2)$ is invertible in $R[\![x,y]\!]$, with inverse $\sum_{k\geq 0}(-xy/c^2)^k$.

Date: January 17, 2011.

(4) If ϵ and δ are elements of R and 2 is invertible in R we can define the Jacobi FGL over R by

$$F(x,y) = \frac{x\sqrt{Q(y)} + y\sqrt{Q(x)}}{1-\epsilon x^2y^2},$$

where $Q(x) = 1 - 2\delta x^2 + \epsilon x^4$. We need to assume that 2 is invertible so we can use the usual power series expansion of $\sqrt{1+t}$ to define $\sqrt{Q(x)}$; one can check that the denominators of the coefficients in this series are all powers of 2. The real reason why $F(x,y)$ is a formal group law involves the theory of elliptic curves and elliptic integrals. For a more direct proof, one can check that

$$\sqrt{Q(F(x,y))} = \frac{2\epsilon xy(x^2+y^2) + (x'y' - 2\delta xy)(1+\epsilon x^2y^2)}{(1-\epsilon x^2y^2)^2},$$

where $x' = \sqrt{Q(x)}$ and $y' = \sqrt{Q(y)}$. It follows that

$$\begin{aligned} F(F(x,y),z) =& (2s_3(\epsilon p_2 + \delta(A+B+C-4) - \epsilon^2 s_3^2) + \\ & x'y'z(A+B-C) + y'z'x(B+C-A) + z'x'y(C+A-B))/ \\ & (A^2+B^2+C^2+2\epsilon s_3^2(4\delta - \epsilon p_2) - 2), \end{aligned}$$

where

$$\begin{aligned} A &= 1 - \epsilon y^2z^2 \\ B &= 1 - \epsilon z^2x^2 \\ C &= 1 - \epsilon x^2y^2 \\ p_2 &= x^2+y^2+z^2 \\ s_3 &= xyz. \end{aligned}$$

This expression is symmetric in x, y and z, and it follows that F is associative. The other axioms are easy.

(5) Let p be a prime, and let $f(x)$ be a monic polynomial over $\mathbb{Z}$ such that $f(x) = px \pmod{x^2}$ and $f(x) = x^{p^n} \pmod{p}$, for some $n > 0$. The fundamental result of Lubin-Tate theory is that there is a unique FGL over the ring $\mathbb{Z}_p$ of p-adic integers such that $f(F(x,y)) = F(f(x), f(y))$, and that for this FGL we have $[p]_F(x) = f(x)$. Equivalently, this gives a compatible system of FGL's over $\mathbb{Z}/p^k$ for all k. These FGL's are important in algebraic number theory (specifically, in local class field theory). One can understand the splitting field of f and its Galois theory quite explicitly in terms of the formal group structure.

(6) In algebraic topology, one can consider a number of complex-orientable generalised cohomology theories. Such a theory assigns to each space X a graded ring E^*X, subject to various axioms. If L is a complex line bundle over X, one can define an Euler class $e(L) \in E^*X$, which is a useful invariant of L. There is a formal group law F over $E^*(\text{point})$ such that $e(L \otimes M) = F(e(L), e(M))$. In the case of ordinary cohomology, we get the additive FGL. In the case of complex K-theory, we get the multiplicative FGL. In the case of complex cobordism, we get Lazard's universal FGL (Quillen's theorem). This is the start of a very deep relationship between formal groups and the algebraic aspects of stable homotopy theory.

Exercise 1.7. Prove that $\sqrt{1+t}$ lies in $\mathbb{Z}[\frac{1}{2}][\![t]\!]$. In other words, if $f(t) = \sum_{k\geq 0} a_k t^k \in \mathbb{Q}[\![t]\!]$ is the unique power series such that $f(t)^2 = 1+t$ and $f(0) = 1$, show that for each k we can write a_k in the form $b/2^m$ for some integers b and m. One approach is to use the Newton-Raphson method: define $f_0(t) = 1$ and $f_{k+1}(t) = (f_k(t) + (1+t)/f_k(t))/2$ (checking that this makes sense). One can then show that $f_k(t)$ converges to $f(t)$ in a suitable sense. Another approach is to show that $a_k = b_{k-1} + b_k$, where $b_k = \binom{2k}{k}/(-4)^k$. Probably the best approach is to wait for Example 2.9, however.

2. Basic results

One way to think of FGL's is as a recipe for defining honest groups. We now make this precise.

Definition 2.1. Let R be a ring. We say that an element $a \in R$ is *nilpotent* if $a^N = 0$ for some integer $N > 0$. We write $\widehat{\mathbb{A}}^1(R)$ or $\mathrm{Nil}(R)$ for the set of nilpotent elements of R.

Lemma 2.2. $\mathrm{Nil}(R)$ *is an ideal in* R.

Proof. Suppose that $a, b \in \mathrm{Nil}(R)$, say $a^N = 0 = b^M$. Then if $a^i b^j \neq 0$ we must have $i < N$ and $j < M$ so $i + j < N + M$. It follows that $(a+b)^{N+M} = \sum_{N+M=i+j}(i,j)a^i b^j = 0$, so $a + b \in \mathrm{Nil}(R)$. Moreover, if c is an arbitrary element of R then $(ac)^N = a^N c^N = 0$, so $ac \in \mathrm{Nil}(R)$. This shows that $\mathrm{Nil}(R)$ is an ideal. □

Suppose that $F(x,y) = \sum_{i,j} a_{ij} x^i y^j$ is an FGL over a ring R, and that R' is an algebra over R, so we have a specified ring map $u\colon R \to R'$ say. Let b and c be nilpotent elements of R'. Then $b^i c^j = 0$ for all but finitely many pairs (i,j), so we can define $b +_F c = \sum_{i,j} u(a_{ij}) b^i c^j$ as a finite sum without worrying about any kind of convergence. This defines a group structure on $\mathrm{Nil}(R')$, whose identity element is 0.

Definition 2.3. We write $\Gamma(G_F, R')$ or $\Gamma(G_F, R', u)$ for the group $\mathrm{Nil}(R')$ equipped with the group law $+_F$ described above.

Remark 2.4. In the coordinate-free picture, it will be more natural to consider something a little different. Fix a ring R, and a FGL F over R. For any ring R', we let $X(R')$ denote the set of ring homomorphisms $u\colon R \to R'$. We write $G_F(R') = \mathrm{Nil}(R) \times X(R')$. There is an evident projection map $G_F(R') \to X(R')$, sending (a,u) to u, and the preimage of a point $u \in X(R')$ is the group $\Gamma(G_F, R', u)$. Thus $G_F(R')$ is a bundle of groups over $X(R')$, and everything depends naturally on R'. This is an example of a formal group over X (or over R).

Remark 2.5. We clearly have $\mathrm{Nil}(\mathbb{Z}) = 0$, so we cannot tell the difference between different FGL's over $\mathbb{Z}$ by just looking at $\Gamma(G_F, \mathbb{Z})$. However, we can tell the difference if we look at groups like $\Gamma(G_F, \mathbb{Z}[s,t]/(s^N, t^M))$ instead.

We now prove some basic lemmas, as practise in the use of formal power series.

Lemma 2.6. *If F is an FGL then $F(x,y) = x + y \pmod{xy}$.*

Proof. We have $F(x,y) = \sum_{i,j\geq 0} a_{ij} x^i y^j$ for some coefficients $a_{ij} \in R$. Condition (a) tells us that $a_{i0} = 0$ except for $a_{10} = 1$. Using (b) we see that $a_{0j} = 0$ except for $a_{01} = 1$. Thus

$$F(x,y) = x + y + xy \sum_{i,j>0} a_{ij} x^{i-1} y^{j-1},$$

as required. □

Lemma 2.7. *Condition (d) in Definition 1.1 actually follow from conditions (a) and (b).*

Proof. Suppose that F satisfies (a) and (b). As in the previous lemma, we have $F(x,y) = x + y \pmod{xy}$. Define $b_1 = -1$ and $m_1(x) = -x$, so $F(x, m_1(x)) = 0 \pmod{x^2}$. Suppose that we have defined a polynomial $m_k(x)$ of degree k such that $F(x, m_k(x)) = 0 \pmod{x^{k+1}}$. There is then a unique element $b_{k+1} \in R$ such that $F(x, m_k(x)) = -b_{k+1} x^{k+1} \pmod{x^{k+2}}$. Define $m_{k+1}(x) = m_k(x) + b_{k+1} x^{k+1}$. It is easy to check that when $i > 0$ or $i = 0$ and $j > 1$ we have

$$x^i m_{k+1}(x)^j = x^i m_k(x)^j \pmod{x^{k+2}}.$$

Using this and the fact that $F(x,y) = x + y \pmod{xy}$, and working everywhere modulo x^{k+2}, we find that

$$\begin{aligned} F(x, m_{k+1}(x)) &= x + m_{k+1}(x) + \sum_{i,j>0} a_{ij} x^i m_{k+1}(x)^j \\ &= F(x, m_k(x)) - a x^{k+1} \\ &= 0 \pmod{x^{k+2}}. \end{aligned}$$

By an evident recursion, we have now defined b_k and m_k for all k. We put $m(x) = \sum_{k>0} b_k x^k$, so that $m(x) = m_k(x) \pmod{x^{k+1}}$ for all k, and thus $F(x, m(x)) = 0 \pmod{x^{k+1}}$ for all k, so $F(x, m(x)) = 0$ exactly. □

We next want to define homomorphisms between formal group laws. It is convenient to give some remarks about composition of formal power series first.

Lemma 2.8. *Let f be a formal power series over a ring R such that $f(0) = 0$ and $f'(0)$ is a unit in R. Then there is a unique series $g(x) \in R[\![x]\!]$ such that $f(g(x)) = x = g(f(x))$. Moreover, we have $g'(0) = 1/f'(0)$. (This is just a formal version of the inverse function theorem.) We call this series the* reverse *of f.*

Proof. The proof is similar to that of Lemma 2.7. We define $a_1 = f'(0)$ and $b_1 = 1/a_1$ and $g_1(x) = b_1 x$. Then $f(g_1(x)) = x \pmod{x^2}$. Given a polynomial $g_k(x)$ of degree k such that $f(g_k(x)) = x \pmod{x^{k+1}}$, there is a unique element $c \in R$ such that $f(g_k(x)) = x + cx^{k+1} \pmod{x^{k+2}}$, and we define $b_{k+1} = -c/a_1$ and $g_{k+1}(x) = g_k(x) + b_{k+1}x^{k+1}$. One checks that $f(g_{k+1}(x)) = x \pmod{x^{k+2}}$. This gives a sequence of elements b_k for $k > 0$, and we define $g(x) = \sum_{k>0} b_k x^k$. This satisfies $f(g(x)) = x$. By applying the same logic to g, we get a series h with $g(h(x)) = x$. Thus $f(g(h(x))) = f(x)$ but also $f(g(y)) = y$ so $f(g(h(x))) = h(x)$ so $f = h$ so $g(f(x)) = x$ as required. One can also check that g is unique. □

Example 2.9. Take $R = \mathbb{Z}[\frac{1}{n}]$ and $f(x) = (1+x)^n - 1$, so $f^{-1}(y) = (1+y)^{1/n} - 1$. The conclusion is that the coefficients of the usual Taylor expansion of $(1+y)^{1/n}$ lie in R. In particular, the coefficients of $\sqrt{1+y}$ lie in $\mathbb{Z}[\frac{1}{2}]$, giving another answer to Exercise 1.7.

Definition 2.10. We write $\mathrm{RPS}(R)$ for the set of reversible power series over R, in other words the set of power series $f(x) \in R[\![x]\!]$ such that $f(0) = 0$ and $f'(0)$ is a unit in R. This is clearly a group under composition. We write $\mathrm{RPS}_1(R)$ for the subgroup of those f for which $f'(0) = 1$.

Definition 2.11. Let F_0 and F_1 be FGL's over a ring R. A *homomorphism* from F_0 to F_1 is a formal power series $f(x) \in R[\![x]\!]$ such that $f(0) = 0$ and $f(x +_{F_0} y) = f(x) +_{F_1} f(y) \in R[\![x, y]\!]$. We say that f is an *isomorphism* if there is a homomorphism g from F_1 to F_0 such that $f(g(x)) = x$. We say that f is a *strict isomorphism* if $f'(0) = 1$.

Remark 2.12. In the notation of Remark 2.4, a homomorphism f as above gives rise to a map $G_{F_0}(R') \to G_{F_1}(R')$ of bundles of groups over $X(R')$.

Remark 2.13. It follows from Lemma 2.8 that a homomorphism f is an isomorphism if and only if $f'(0)$ is a unit.

Example 2.14. In these examples we consider the following FGL's:

$$F_0(x, y) = x + y$$
$$F_1(x, y) = x + y + xy$$
$$F_2(x, y) = (x + y)/(1 + xy).$$

All these can be defined over any ring R.

(1) If $\mathbb{Q} \subseteq R$ then the series $f(x) = \log(1+x) = -\sum_{k>0}(-x)^k/k$ gives an isomorphism from F_1 to F_0.
(2) If 2 is invertible in R then there is an isomorphism from F_1 to F_2 given by
$$f(x) = \frac{(1+x) - (1+x)^{-1}}{(1+x) + (1+x)^{-1}}.$$
(3) If $2 = 0$ in R then $f(x) = x/(1+x^2)$ gives an isomorphism from F_2 to F_0.

Exercise 2.15. Show that in the last example, we have $f^{-1}(y) = \sum_{k>0} y^{2^k-1}$. Hint: $(a+b)^2 = a^2 + b^2 \pmod 2$.

3. FGL's over $\mathbb{Q}$-algebras

Proposition 3.1. *If R is a $\mathbb{Q}$-algebra, and F is an FGL over R, then there is a unique strict isomorphism $f\colon F \to F_a$, where F_a is the additive FGL, given by $F_a(x, y) = x + y$.*

Definition 3.2. This series $f(x)$ is called the *logarithm* of F, and is written $\log_F(x)$. Thus, we have $\log_F(x +_F y) = \log_F(x) + \log_F(y)$. We also write $\exp_F(x)$ for the inverse of $\log_F(x)$.

Proof. Suppose that $F(x,y) = \sum_{i,j} a_{ij} x^i y^j$. We write $F_2(x,y)$ for the partial derivative of F with respect to the second variable, in other words $F_2(x,y) = \sum_{i,j} j a_{ij} x^i y^{j-1}$. Because $F(x,y) = x + y \pmod{xy}$ we have $F_2(0,0) = 1$ so $F_2(t,0)$ is invertible in $R[\![t]\!]$. As R is a $\mathbb{Q}$-algebra we can formally integrate and thus define

$$f(x) = \int_{t=0}^{x} \frac{dt}{F_2(t,0)}.$$

More explicitly, if $1/F_2(t,0) = \sum_k c_k t^k$ then we define $f(x) = \sum_k c_k x^{k+1}/k+1$. (We need not try to interpret this in terms of Riemann sums or anything like that.) It is clear that $f(x) = x \pmod{x^2}$.

We are given that

$$F(F(x,y),z) = F(x,F(y,z)).$$

If we take partial derivatives with respect to z at $z = 0$ we obtain $F_2(F(x,y),0) = F_2(x,y)F_2(y,0)$, or equivalently $f'(F(x,y))^{-1} = F_2(x,y)f'(y)^{-1}$, or equivalently $f'(F(x,y))F_2(x,y) = f'(y)$. If we put $h(x,y) = f(F(x,y)) - f(x) - f(y)$ then we deduce that $\partial h(x,y)/\partial y = 0$. Thus, if $h(x,y) = \sum_{i,j} d_{ij} x^i y^j$ then $\sum_{i,j} j d_{ij} x^i y^{j-1} = 0$ in $R[\![x,y]\!]$, which implies that $d_{ij} = 0$ when $j > 0$. On the other hand, it is clear that $h(x,0) = 0$ so $d_{i0} = 0$ so $h = 0$. This means that $f(F(x,y)) = f(x) + f(y)$, so f is a homomorphism from F to F_a. It is a strict isomorphism, because $f(x) = x \pmod{x^2}$.

Now let g be another strict isomorphism, and let g^{-1} denote its reverse. Then the series $k(x) = f(g^{-1}(x))$ satisfies $k(x+y) = k(x) + k(y)$. We now expand this out and use the fact that all binomial coefficients are invertible in $\mathbb{Q}$ and thus in R. It follows easily that $k(x) = \lambda x$ for some $\lambda \in R$, but f and g were *strict* isomorphisms so $\lambda = 1$. This shows that $f = g$. □

Corollary 3.3. *If R is a $\mathbb{Q}$-algebra then there is a bijection $\phi\colon \mathrm{RPS}_1(R) \to \mathrm{FGL}(R)$ given by*

$$\phi(f)(x,y) = f^{-1}(f(x) + f(y))$$
$$\phi^{-1}(F)(x) = \log_F(x) = \int_0^x \frac{dt}{F_2(t,0)}.$$

Proof. Write $\psi(F) = \log_F$, so $\psi\colon \mathrm{FGL}(R) \to \mathrm{RPS}_1(R)$. The proposition shows that

$$\psi(F)(F(x,y)) = \psi(F)(x) + \psi(F)(y),$$

or in other words that $F = \phi\psi(F)$, so $\phi\psi = 1$. On the other hand, if $F = \phi(f)$ then f is certainly a homomorphism $F \to F_a$ with $f'(0) = 1$, and we have seen that $\log_F$ is the *unique* such homomorphism, so $f = \psi\phi(f)$. □

Example 3.4. (1) If $F(x,y) = x + y$ is the additive FGL then $\log_F(x) = x$.

(2) If $F(x,y) = x + y + uxy$ is a multiplicative FGL then

$$\log_F(x) = \log(1+ux)/u = \sum_{k>0} (-u)^{k-1} x^k/k.$$

(3) If $F(x,y) = (x+y)/(1+xy/c^2)$ is the Lorenz FGL then

$$\log_F(x) = \tanh^{-1}(x/c) = \frac{c}{2} \log\left(\frac{c+v}{c-v}\right).$$

(4) Write $Q(x) = 1 - 2\delta x^2 + \epsilon x^4$, so we have a Jacobi formal group law $F(x,y) = (x\sqrt{Q(y)} + y\sqrt{Q(x)})/(1 - \epsilon x^2 y^2)$. The logarithm is then $\log_F(x) = \int_{t=0}^{x} Q(t)^{-1/2} dt$. This expression is called an *elliptic integral*; such things arise in the theory of planetary motion, for example. The definition of the logarithm gives the following transformation property of elliptic integrals:

$$\int_0^x \frac{dt}{\sqrt{Q(t)}} + \int_0^y \frac{dt}{\sqrt{Q(t)}} = \int_0^{F(x,y)} \frac{dt}{\sqrt{Q(t)}}.$$

(5) Let F be an FGL over a p-adically complete ring R. In suitable circumstances **make this precise** we have

$$\log_F(x) = \lim_{n \to \infty} p^{-n} [p^n](x).$$

(6) Let E be a 2-periodic generalised cohomology theory with a complex orientation in degree zero. We then have a fundamental class $[M] \in E^0$ for each stably almost complex manifold M. We also have a canonical formal group law F over E^0, and it turns out that $\log_F(x) = \sum_{k\geq 0}[\mathbb{C}P^k]x^{k+1}/k+1$.

4. Affine schemes

Definition 4.1. A *functor* X from rings to sets is a rule which assigns to each ring R a set $X(R)$, and to each homomorphism $\alpha\colon R \to R'$ a map $X(\alpha)\colon X(R) \to X(R')$, such that:

(1) If $\alpha\colon R \to R'$ and $\alpha'\colon R' \to R''$ then $X(\alpha'\alpha) = X(\alpha')X(\alpha)\colon X(R) \to X(R'')$.
(2) If $1\colon R \to R$ is the identity map, then $X(1)\colon X(R) \to X(R)$ is the identity map.

Example 4.2. (1) Define $X(R) = \{(a,b) \in R^2 \mid b^2 = a^3 - a\}$ and $X(\alpha)(a,b) = (\alpha(a), \alpha(b))$. This clearly gives a scheme. This is our version of the elliptic curve $y^2 = x^3 - x$.
(2) We have a functor FGL, which sends a ring R to the set $\mathrm{FGL}(R)$ of formal group laws over R. For any ring map $\alpha\colon R \to R'$, we have an associated map $\mathrm{FGL}(\alpha)\colon \mathrm{FGL}(R) \to \mathrm{FGL}(R')$: If $F(x,y) = \sum_{i,j\geq 0} a_{ij}x^iy^j \in \mathrm{FGL}(R)$, then $\mathrm{FGL}(\alpha)(F)(x,y) = \sum_{i,j\geq 0}\alpha(a_{ij})x^iy^j$. We normally write αF rather than $\mathrm{FGL}(\alpha)(F)$.
(3) Similarly, we have a functor RPS_1, which sends a ring R to the set $\mathrm{RPS}_1(R)$ of power series $f \in R[\![x]\!]$ such that $f(x) = x \pmod{x^2}$. The maps $\mathrm{RPS}(\alpha)$ are again given by applying α to the coefficients.
(4) We have a functor $\mathbb{A}^n$ defined by $\mathbb{A}^n(R) = R^n = R \times \ldots \times R$. This contains the subfunctor $\widehat{\mathbb{A}}^n(R) = \mathrm{Nil}(R)^n$. We also have a subfunctor $G_m \subset \mathbb{A}^1$ defined by $G_m(R) = R^\times$, the group of units of R.
(5) We can define a functor T by $T(R) = R/2R$.
(6) If X and Y are functors, then we can define a functor $X \times Y$ by $(X \times Y)(R) = X(R) \times Y(R)$ and $(X \times Y)(\alpha) = X(\alpha) \times Y(\alpha)$.

Definition 4.3. A *natural transformation* (or just *map*) $f\colon X \to Y$ of functors is a rule which assigns to each ring R a map $f_R\colon X(R) \to Y(R)$. We require that for any map $\alpha\colon R \to R'$ of rings, the following diagram must commute:

$$\begin{array}{ccc} X(R) & \xrightarrow{X(\alpha)} & X(R') \\ {\scriptstyle f_R}\downarrow & & \downarrow{\scriptstyle f_{R'}} \\ Y(R) & \xrightarrow[Y(\alpha)]{} & Y(R') \end{array}$$

Example 4.4. (1) We can define a map $f\colon \mathbb{A}^3 \to \mathbb{A}^2$ by $f(a,b,c) = (a^2 + bc, c^3)$. It is easy to see that this gives a natural transformation. More generally, given any n-tuple of polynomials $f_1, \ldots, f_n$ in variables $x_1, \ldots, x_m$ over $\mathbb{Z}$, we get a map $f\colon \mathbb{A}^m \to \mathbb{A}^n$ by

$$f(a_1, \ldots, a_m) = (f_1(\underline{a}), \ldots, f_n(\underline{a})).$$

We will see later that these are all the maps from $\mathbb{A}^m$ to $\mathbb{A}^n$.
(2) We have a map $\mathrm{comp}\colon \mathrm{RPS}_1 \times \mathrm{RPS}_1 \to \mathrm{RPS}_1$ defined by $\mathrm{comp}(f,g)(x) = f(g(x))$. Using the naturality of this, one can check that the inversion map $\mathrm{inv}\colon \mathrm{RPS}_1 \to \mathrm{RPS}_1$ (sending f to f^{-1}) is also natural.
(3) We can define $\phi_R\colon \mathrm{RPS}_1(R) \to \mathrm{FGL}(R)$ by $\phi_R(f) = f^{-1}(f(x) + f(y))$, as in Corollary 3.3. This gives a map $\phi\colon \mathrm{RPS}_1 \to \mathrm{FGL}$.

Definition 4.5. For any ring A, we can define a functor $\mathrm{spec}(A)$ from rings to sets by

$$\mathrm{spec}(A)(R) = \mathrm{Rings}(A, R),$$

where $\mathrm{Rings}(A,R)$ denotes the set of ring homomorphisms from A to R. Given a homomorphism $\alpha\colon R \to R'$, the associated map $\alpha_* = \mathrm{spec}(A)(\alpha)\colon \mathrm{Rings}(A,R) \to \mathrm{Rings}(A,R')$ is just $\alpha_*(u) = \alpha \circ u$. We say that a functor X is an *affine scheme* if it is isomorphic to a functor of the form $\mathrm{spec}(A)$ for some A.

Example 4.6. (1) Recall the functor $G_m(R) = R^\times$. Consider the ring $A = \mathbb{Z}[x, x^{-1}]$ of Laurent series over $\mathbb{Z}$ in one variable x. We claim that $\mathrm{spec}(A) \simeq G_m$. Given an element $u \in \mathrm{spec}(A)(R)$ (in other words, a map $u\colon A \to R$) we define $\phi(u) = u(x)$. Given $v \in G_m(R) = R^\times$, we define $\psi(v)\colon A \to R$ by $\psi(v)(\sum_k a_k x^k) = \sum_k a_k v^k$. It is easy to check that these constructions give the required bijection. Thus, G_m is an affine scheme.

(2) Similar arguments show that $\mathbb{A}^n = \mathrm{spec}(\mathbb{Z}[x_1, \dots, x_n])$, so this is a scheme.

(3) Inside $\mathbb{A}^2$, we have the affine elliptic curve C defined by $C(R) = \{(a, b) \in R^2 \mid b^2 = a^3 - a\}$. It is easy to check that $C = \mathrm{spec}(\mathbb{Z}[x, y]/(y^2 - x^3 + x)$.

(4) Let 1 denote any one-point set. We then have

$$\mathrm{spec}(\mathbb{Q})(R) = \begin{cases} 1 & \text{if every } n > 0 \text{ is invertible in } R \\ \emptyset & \text{otherwise.} \end{cases}$$

Similarly, we have

$$\mathrm{spec}(\mathbb{F}_p)(R) = \begin{cases} 1 & \text{if } p = 0 \text{ in } R \\ \emptyset & \text{otherwise.} \end{cases}$$

(5) The functor $T(R) = R/2R$ is not an affine scheme. Indeed, if X is an affine scheme then one sees easily that the inclusion $\mathbb{Z} \subset \mathbb{Q}$ gives an injective map $X(\mathbb{Z}) \to X(\mathbb{Q})$, but clearly there is no injection $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/2\mathbb{Q} = \{0\}$.

Definition 4.7. For any functor X, we let $\mathcal{O}_X$ be the class of natural transformations from X to $\mathbb{A}^1$. In the cases of interest this will always be a set rather than a proper class. More explicitly, an element $f \in \mathcal{O}_X$ gives (for each ring R) a map $f\colon X(R) \to R$, such that $f(X(\alpha)(x)) = \alpha(f(x))$ for all $x \in X(R)$ and $\alpha\colon R \to R'$. We can make $\mathcal{O}_X$ into a ring by defining $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ in the usual way. It is called the *ring of functions on* X.

Proposition 4.8 (The Yoneda Lemma)**.** *For any functor X and any ring A, the set of natural transformations from* $\mathrm{spec}(A)$ *to X bijects with $X(A)$.*

Proof. The basic point is that a natural map $f\colon \mathrm{spec}(A) \to X$ is freely and uniquely determined by its "universal example", which is the element $f_A(1_A) \in X(A)$. We proceed to explain this more fully.

Write T for the set of natural transformations from $\mathrm{spec}(A)$ to X. If $f \in T$ then we have a map

$$f_R\colon \mathrm{Rings}(A, R) = \mathrm{spec}(A)(R) \to X(R)$$

for each ring R. In particular, we have a map $f_A\colon \mathrm{Rings}(A, A) \to X(A)$, so we can define $\phi(f) = f_A(1_A) \in X(A)$. This gives us a map $\phi\colon T \to X(A)$. Next, suppose we have an element $x \in X(A)$. For any ring R and any map $u\colon A \to R$, we have a map $X(u)\colon X(A) \to X(R)$, because X is a functor. We can thus define $g_R(u) = X(u)(x)$. This construction gives a function

$$g_R\colon \mathrm{spec}(A)(R) = \mathrm{Rings}(A, R) \to X(R).$$

We claim that these maps give a natural transformation $g\colon \mathrm{spec}(A) \to R$. If we have another map $\alpha\colon R \to R'$ of rings, we need to check that $X(\alpha)(g_R(u)) = g_{R'}(\alpha_*(u))$. This is clear because

$$X(\alpha)(g_R(u)) = X(\alpha)(X(u)(x)) = X(\alpha u)(x) = g_{R'}(\alpha_*(u)).$$

Because the definition of g depended on x, it makes sense to write $\psi(x) = g$. This gives a map $\psi\colon X(A) \to T$. We claim that this is inverse to ϕ. Indeed, we have

$$\phi(\psi(x)) = g_A(1_A) = X(1_A)(x) = x,$$

so $\phi\psi = 1$. In the other direction, suppose that $f \in T$, and define $x = \phi(f) = f_A(1_A)$, so that the map g defined above is $\psi(\phi(x))$. We need to show that $g = f$. In other words, given a ring R and an element $u \in \mathrm{spec}(A)(R) = \mathrm{Rings}(A, R)$, we need to show that $f_R(u) = g_R(u) = X(u)(x) = X(u)(f_A(1_A))$. For this, we notice that $u = u_*(1_A)$, where

$$u_* = \mathrm{spec}(A)(u)\colon \mathrm{spec}(A)(A) \to \mathrm{spec}(A)(R).$$

Because f is natural, we have

$$f_R(u) = f_R(u_*(1_A)) = X(u)(f_A(1_A))$$

as required. □

Corollary 4.9. *If A is any ring then $\mathcal{O}_{\mathrm{spec}(A)} \simeq A$.*

Proof. By definition, $\mathcal{O}_{\mathrm{spec}(A)}$ is the set of natural transformations from $\mathrm{spec}(A)$ to $\mathbb{A}^1$. By the Yoneda lemma, this bijects with $\mathbb{A}^1(A) = A$. □

Corollary 4.10. *If X is a scheme then X is isomorphic to* $\mathrm{spec}(\mathcal{O}_X)$.

Proof. By the definition of a scheme, X is isomorphic to $\mathrm{spec}(A)$ for some A, but the previous corollary tells us that $A \simeq \mathcal{O}_X$, so $X \simeq \mathrm{spec}(\mathcal{O}_X)$. □

Exercise 4.11. Exhibit a map $X \to \mathrm{spec}(\mathcal{O}_X)$ which is defined naturally for all functors X, and is an isomorphism when X is a scheme. (There are some set-theoretical problems here, but I suggest that you just ignore them.)

Corollary 4.12. *If A and B are rings then there is a canonical bijection between maps* $\mathrm{spec}(A) \to \mathrm{spec}(B)$ *of schemes, and ring maps $B \to A$.*

Proof. This is the case of Proposition 4.8 in which $X = \mathrm{spec}(B)$. □

Example 4.13.
(1) We have $\mathbb{A}^m = \mathrm{spec}(\mathbb{Z}[x_1, \dots, x_m])$, so the Yoneda lemma tells us that maps from $\mathbb{A}^m$ to $\mathbb{A}^n$ biject with elements of $\mathbb{A}^n(\mathbb{Z}[x_1, \dots, x_m])$, or in other words with n-tuples of polynomials in m variables. This proves that all maps $\mathbb{A}^m \to \mathbb{A}^n$ are of the form considered in Example 4.4.
(2) We have maps $\pi_k^{\pm} \colon G_m \to G_m$ defined by $\pi_k^{\pm}(a) = \pm a^k$. We claim that these are all the maps from G_m to itself. To see this, note that $\mathcal{O}_{G_m} = \mathbb{Z}[u, u^{-1}]$. By the Yoneda lemma, we need only check that the elements $\pm u^k$ are all the units in this ring, which is elementary.
(3) The functor RPS_1 is a scheme. Indeed, let A be the polynomial ring $\mathbb{Z}[b_2, b_3, \dots]$ in countably many variables over $\mathbb{Z}$. We have an element $u(x) = x + \sum_{k>1} b_k x^k \in \mathrm{RPS}_1(A)$, and by the Yoneda Lemma this corresponds to a map $\mathrm{spec}(A) \to \mathrm{RPS}_1$. It is easy to see that this is an isomorphism. Explicitly, for any reversible power series $v(x) = x + \sum_{k>1} c_k x^k$ over any ring R, there is a unique homomorphism $\alpha \colon A \to R$ sending b_k to c_k for all k, and thus sending $u(x)$ to $v(x)$.
(4) By a similar argument, we have $\mathrm{RPS} = \mathrm{spec}(\mathbb{Z}[b_1, b_2, \dots][b_1^{-1}])$.

Exercise 4.14. Show that $\mathrm{spec}(A \otimes B) = \mathrm{spec}(A) \times \mathrm{spec}(B)$, and thus that any finite product of schemes is a scheme.

Exercise 4.15. Let $E(R)$ be the set of 2×2-matrices M over R such that $M^2 = M$. Show that this defines an affine scheme, and investigate the structure of $\mathcal{O}_E$. You may want to consider the maps $e_0, e_2 \colon E \to \mathbb{A}^1$ given by $e_0(M) = \det(1 - M)$ and $e_2(M) = \det(M)$.

Proposition 4.16. *The functor* FGL *is an affine scheme.*

Proof. Let $L_0 = \mathbb{Z}[a_{ij} \mid i, j > 0]$ be a polynomial algebra over $\mathbb{Z}$ on countably many indeterminates $a_{i,j}$, one for each pair (i, j) of positive integers. Define $F_0(x, y) = x + y + \sum_{i,j} a_{ij} x^i y^j$, and define elements $b_{ijk} \in L_0$ by the equation

$$F_0(F_0(x, y), z) - F_0(x, F_0(y, z)) = \sum_{i,j,k} b_{ijk} x^i y^j z^k.$$

Let I be the ideal in L_0 generated by the elements $a_{ij} - a_{ji}$ (for $i, j > 0$) and the elements b_{ijk}, and put $L = L_0/I$. Let F be the image of F_0 in $L[\![x, y]\!]$. It is clear that this is a formal group law over L. We thus have a map $\mathrm{spec}(L)(R) = \mathrm{Rings}(L, R) \to \mathrm{FGL}(R)$, sending α to αF. We claim that this is a natural isomorphism. Indeed, let F' be an FGL over R, say $F'(x, y) = x + y + \sum_{i,j>0} a'_{ij} x^i y^j$. There is then a unique homomorphism $\alpha_0 \colon L_0 \to R$ such that $\alpha_0(a_{ij}) = a'_{ij}$, so that $\alpha_0 F_0 = F'$. It follows that $\alpha_0(b_{ijk})$ is the coefficient of $x^i y^j z^k$ in $F'(F'(x, y), z) - F'(x, F'(y, z))$, but this series is just zero because F' is a formal group law. Thus $\alpha_0(b_{ijk}) = 0$, and similarly $\alpha_0(a_{ij} - a_{ji}) = 0$, so there is a unique induced map $\alpha \colon L = L_0/I \to R$ with $\alpha F = F'$. Thus, we have $\mathrm{FGL} = \mathrm{spec}(L)$, as required. □

Definition 4.17. The ring $L = \mathcal{O}_{\mathrm{FGL}}$ is called the *Lazard ring*.

Remark 4.18. In topology, it turns out that one can naturally identify FGL with $\mathrm{spec}(MU_*)$ and RPS_1 with $\mathrm{spec}(H_*MU)$, in such a way that the Hurewicz map $MU_* \to H_*MU$ induces the map $\phi\colon \mathrm{RPS}_1 = \mathrm{spec}(H_*MU) \to \mathrm{spec}(MU_*) = \mathrm{FGL}$.

5. Base schemes and base change

We will often have a scheme X and want to consider other schemes equipped with a map to X, which we refer to as schemes over X. We have a correspondence between rings and schemes given by $A \leftrightarrows \mathrm{spec}(A)$; this gives a correspondence between $\mathcal{O}_X$-algebras and schemes over X.

Consider two functors V, W equipped with maps $p\colon V \to X$ and $q\colon W \to Z$. A *map from V to W of schemes over X* means a map $f\colon V \to W$ of schemes such that $qf = p$. We define the *pullback* of V and W by

$$(V \times_X W)(R) = V(R) \times_{X(R)} W(R) = \{(v, w) \in V(R) \times W(R) \mid p(v) = q(w)\}.$$

We also write p^*W for $V \times_X W$, considered as a scheme over V using the projection map $(v, w) \mapsto v$. Given a ring A and two A-algebras B and C, one can check that

$$\mathrm{spec}(B) \times_{\mathrm{spec}(A)} \mathrm{spec}(C) = \mathrm{spec}(B \otimes_A C).$$

It follows that when V, W and X are all affine schemes, the pullback is again an affine scheme, and we have

$$\mathcal{O}_{V \times_X W} = \mathcal{O}_V \otimes_{\mathcal{O}_X} \mathcal{O}_W.$$

Definition 5.1. Let X be an affine scheme, and Y a functor equipped with a map $p\colon Y \to X$. A *system of formal coordinates* on Y is a collection of maps $x_1, \dots, x_n\colon Y \to \widehat{\mathbb{A}}^1$ such that the resulting map $a \mapsto (x_1(a), \dots, x_n(a), p(a))$ gives an isomorphism $Y \to \widehat{\mathbb{A}}^n \times X$. An *$n$-dimensional formal scheme* over X is a functor which admits such a system of coordinates.

Let A be a ring, and $f(x, y)$ a power series in $A[\![x, y]\!]$. Write $X = \mathrm{spec}(A)$. Given a point $u \in X(R)$ (in other words, a homomorphism $u\colon A \to R$) we define a power series uf over R in the obvious way, and then define

$$Y(R) = \{(u, x, y) \in X(R) \times \widehat{\mathbb{A}}^2(R) \mid (uf)(x, y) = 0\}.$$

We would like to know when this is a formal scheme over X. For this, we need a formal version of the implicit function theorem.

Proposition 5.2. *Let $f_2(x, y)$ denote the partial derivative of f with respect to the second variable. If $f(0, 0) = 0$ and $f_2(0, 0)$ is a unit in A then the map $(u, x, y) \mapsto (u, x)$ is an isomorphism $Y \simeq X \times \widehat{\mathbb{A}}^1$, and thus Y is a one-dimensional formal scheme over X.*

Proof. We will construct a power series $g(x) \in A[\![x]\!]$ such that $g(0) = 0$ and $f(x, g(x)) = 0$, by the usual process of successive approximation. We start with $g_0(x) = 0$. Suppose we have constructed a polynomial g_k of degree k such that $g_k(0) = 0$ and $f(x, g_k(x)) = 0 \pmod{x^{k+1}}$, say $f(x, g_k(x)) = ax^{k+1} \pmod{x^{k+2}}$. We then have

$$f(x, g_k(x) + bx^{k+1}) = f(x, g_k(x)) + bx^{k+1} f_2(x, g_k(x)) \pmod{x^{2k+2}},$$

but $x^{k+1} f_2(x, g_k(x)) = x^{k+1} f_2(0, g_k(0)) = x^{k+1} f_2(0, 0) \pmod{x^{k+2}}$ so $f(x, g_k(x) + bx^{k+1}) = (a + bf_2(0, 0))x^{k+1} \pmod{x^{k+2}}$. Thus, we must take $g_{k+1}(x) = g_k(x) - ax^{k+1}/f_2(0, 0)$. If we let g be the formal power series such that $g(x) = g_k(x) \pmod{x^{k+1}}$ for all k, then we find that $f(x, g(x)) = 0$. We can thus define a map $\phi\colon X \times \widehat{\mathbb{A}}^1 \to Y$ by $\phi(u, x) = (u, x, (ug)(x))$. If we write π for the map $(u, x, y) \mapsto (u, x)$ then clearly $\pi\phi = 1$. Now consider the series $h(x, z) = f(x, g(x) + z) \in A[\![x, z]\!]$. We have $h(x, 0) = f(x, g(x)) = 0$, so $h(x, z) = z\, k(x, z)$ for some series k. Moreover, we have $k(0, 0) = f_2(0, 0)$, which is a unit in A, so $k(x, z)$ is a unit in $A[\![x, z]\!]$. Now suppose that $(u, x, y) \in Y(R)$ for some ring R. Writing $z = y - (ug)(x)$, we find that $(uh)(x, z) = (uf)(x, y) = 0$, so $z\,(uk)(x, z) = 0$ but k is invertible so $(uk)(x, z)$ is invertible in R so $z = 0$. This shows that $y = (ug)(x)$, and thus that $(u, x, y) = \phi\pi(u, x, y)$, so $\phi\pi = 1$. □

Exercise 5.3. Generalise this to cover more variables and more equations.

Example 5.4. Take $X = \mathbb{A}^1$, and let Z be the subfunctor of $X \times \mathbb{A}^2$ whose fibre over a point $\rho \in X(R)$ is the set of pairs (a, b) such that $(a^2 + b^2)\rho = b$. This should be thought of as a circle of diameter $1/\rho$ which is tangent to the x-axis at the origin. Where $\rho = 0$ this degenerates to a straight line. Let $Y(R)$ be the subset where a and b are nilpotent. This should be thought of as an infinitesimal neighbourhood of the origin in Z. It seems intuitively clear that the vertical projection should give an isomorphism of Y with an infinitesimal neighbourhood of the origin in the x-axis. The proposition gives us a rigorous formulation and proof of this (take $A = \mathbb{Z}[\rho]$ and $f(x, y) = (x^2 + y^2)\rho - y$).

Example 5.5. Let A be a ring, suppose that $a_1, a_2, a_3, a_4, a_6 \in A$, and consider the standard homogeneous Weierstrass cubic

$$g(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

This defines an elliptic curve C in the projective plane (provided that a certain expression $\Delta(a_1, a_2, a_3, a_4, a_6)$ is invertible; otherwise we have a "generalised elliptic curve"). We write $X = \operatorname{spec}(A)$. The *formal completion* of C is the functor $\widehat{C}$ defined by

$$\widehat{C}(R) = \{(u, x, z) \in X(R) \times \widehat{\mathbb{A}}^2(R) \mid (ug)(x, 1, z) = 0\}.$$

If we define $f(x, z) = g(x, 1, z)$ then one checks easily that $f(0, 0) = 0$ and $f_2(0, 0) = 1$ so Proposition 5.2 shows that $\widehat{C}$ is a one-dimensional formal scheme over X.

We now show that all maps between formal schemes over a fixed base are given by formal power series.

Proposition 5.6. *Let $f\colon X \times \widehat{\mathbb{A}}^n \to X \times \widehat{\mathbb{A}}^m$ be a map of formal schemes over $X = \operatorname{spec}(A)$. Then there are unique formal power series $f_1, \dots, f_m \in A[\![x_1, \dots, x_n]\!]$ such that for all rings R and all $(u, a_1, \dots, a_n) \in X(R) \times \widehat{\mathbb{A}}^n(R)$ we have*

$$f(u, a_1, \dots, a_n) = (u, (uf_1)(a_1, \dots, a_n), \dots, (uf_m)(a_1, \dots, a_n)).$$

Moreover, the elements $f_i(0, \dots, 0) \in A$ are nilpotent. Conversely, given any m-tuple of series f_i whose constant terms are nilpotent, the above formula defines a map $X \times \widehat{\mathbb{A}}^n \to X \times \widehat{\mathbb{A}}^m$ of formal schemes over X.

Proof. Write $B_k = A[x_1, \dots, x_n]/(x_1^k, \dots, x_n^k)$. Let u_k be the obvious map $A \to B_k$, considered as an element of $X(B_k)$. Let t_k be the tuple $(x_1, \dots, x_n)$, considered as an element of $\widehat{\mathbb{A}}^n(B_k)$. We thus have an element $f(u_k, t_k) \in X(B_k) \times \widehat{\mathbb{A}}^m(B_k)$. As f is supposed to be a map of formal schemes over X, the first component of $f(u_k, t_k)$ must be u_k. The remaining components are elements of $\widehat{\mathbb{A}}^1(B_k)$, in other words nilpotent elements of B_k. If b is an element of B_k with constant term b_0 then it is clear that $b - b_0$ lies in the ideal $(x_1, \dots, x_n)$ and each x_i is nilpotent so $b - b_0$ is nilpotent. Thus, b is nilpotent if and only if b_0 is nilpotent. It follows that there are polynomials $f_{k,1}, \dots, f_{k,m}$, of degree less than k in each of the variables $x_1, \dots, x_n$, whose constant terms are nilpotent, such that $f(u_k, t_k) = (u_k, f_{k,1}, \dots, f_{k,m})$. Now consider the evident quotient map $\pi\colon B_{k+1} \to B_k$. Clearly, the induced map $X(B_{k+1}) \times \widehat{\mathbb{A}}^n(B_{k+1}) \to X(B_k) \times \widehat{\mathbb{A}}^n(B_k)$ sends (u_{k+1}, t_{k+1}) to (u_k, t_k). As f is natural, we see that π must send $f(u_{k+1}, t_{k+1})$ to $f(u_k, t_k)$, which means that $f_{k+1,j} = f_{k,j} \bmod (x_1^k, \dots x_n^k)$ for all j. Thus, there are unique power series f_j such that $f_j = f_{k,j} \bmod (x_1^k, \dots, x_n^k)$ for all k.

Now consider an arbitrary ring R and a point $(u, \underline{a}) = (u, a_1, \dots, a_n) \in X(R) \times \widehat{\mathbb{A}}^n(R)$. The elements a_i are nilpotent, so there is an integer k such that $a_j^k = 0$ for all j. Let $\alpha\colon B_k \to R$ be the unique ring homomorphism such that $\alpha(a) = u(a)$ for $a \in A \subset B_k$ and $\alpha(x_j) = a_j$ for all j. It is clear that α sends $(u_k, t_k) \in X(B_k) \times \widehat{\mathbb{A}}^n(B_k)$ to $(u, \underline{a})$. As f is natural, we conclude that α sends $f(u_k, t_k) = (u_k, f_{k,1}, \dots, f_{k,m})$ to $f(u, \underline{a})$. However, α sends $f_{k,j}$ to $(uf_{k,j})(a_1, \dots, a_n)$, which is the same as $(uf_j)(a_1, \dots, a_n)$ because $a_i^k = 0$ for all i. Thus, we have

$$f(u, \underline{a}) = (u, (uf_1)(\underline{a}), \dots, (uf_m)(\underline{a}))$$

as claimed. □

Definition 5.7. A *formal group* over an affine scheme X is a one-dimensional formal scheme G over X (with projection map $\pi\colon G \to X$ say), with a specified Abelian group structure on $\pi^{-1}\{x\}$ for each ring R and point $x \in X(R)$. These structures are required to depend naturally on R. More precisely, we require

that addition in G comes from a natural map $\sigma\colon G \times_X G \to G$, and that the map $\zeta\colon X \to G$ (sending x to the zero element in $\pi^{-1}\{x\}$) is also natural.

Example 5.8. Define

$$\widehat{G}_m(R) = \{a \in R \mid a = 1 \pmod{\mathrm{Nil}(R)}\}.$$

One checks that any $a \in \widehat{G}_m(R)$ is invertible. Indeed, if $(1-a)^k = 0$ then $a^{-1} = \sum_{j=0}^{k-1}(1-a)^j$. It follows that $\widehat{G}_m(R)$ is a group under multiplication. Moreover, the function $x(a) = 1 - a$ gives an isomorphism $\widehat{G}_m \simeq \widehat{\mathbb{A}}^1$, which shows that $\widehat{G}_m$ is a formal group over $\mathrm{spec}(\mathbb{Z})$.

Example 5.9. We can also define $\widehat{G}_a(R) = \mathrm{Nil}(R)$, with the usual addition. This is clearly a formal group over $\mathrm{spec}(\mathbb{Z})$.

Example 5.10. If F is a formal group law over A then we have a formal group G_F over $X = \mathrm{spec}(A)$ defined by $G_F = X \times \widehat{\mathbb{A}}^1$. If $x \in X(R)$ then x gives a map $A \to R$, which we use to regard R as an A-algebra, so we can define $a +_F b$ for $a, b \in \widehat{\mathbb{A}}^1(R) = \pi^{-1}\{x\}$. This makes $\pi^{-1}\{x\}$ into an Abelian group, and thus G_F into a formal group, as required. The identity element is just 0. In the case $F(x,y) = x + y - xy$ we have an isomorphism $G_F \simeq \widehat{G}_m$ of formal groups, given by $a \mapsto 1 + a$.

Example 5.11. The formal scheme $\widehat{C}$ of Example 5.5 has a natural group structure. More precisely, we have a map $\nu\colon \widehat{C} \to \widehat{C}$ given by

$$\nu(u,x,z) = (u, -x/(1 + u(a_1)x + u(a_3)z), -z/(1 + u(a_1)x + u(a_3)z)).$$

We will often allow ourselves to abbreviate things like this as

$$\nu(x,z) = (-x/(1 + a_1x + a_3z), -z/(1 + a_1x + a_3z)).$$

The group structure is characterised by the following properties:

(a) The identity element is $(0,0)$ (or in other words, $\zeta(u) = (u,0,0)$).
(b) The negation map is $-(x,z) = \nu(x,z)$.
(c) If $(x_0,z_0) + (x_1,z_1) + (x_2,z_2) = (0,0)$ then the following determinant vanishes:

$$\begin{vmatrix} x_0 & 1 & z_0 \\ x_1 & 1 & z_1 \\ x_2 & 1 & z_2 \end{vmatrix} = 0.$$

Informally, this means that the points (x_0,z_0), (x_1,z_1) and (x_2,z_2) are collinear.

Example 5.12. Let E be a 2-periodic complex orientable generalised cohomology theory. Write $X = \mathrm{spec}(E^0)$, and let $G(R)$ be the set of ring homomorphisms $E^0\mathbb{C}P^\infty \to R$ that factor through $E^0\mathbb{C}P^k$ for some finite k. One can choose an element x such that $E^0\mathbb{C}P^\infty = E^0[\![x]\!]$ and $E^0\mathbb{C}P^k = E^0[\![x]\!]/x^{k+1}$, and using this we see that G is a formal group over X.

Definition 5.13. Let G be a formal group over a scheme X, with projection $\pi\colon G \to X$ and zero-section $\zeta\colon X \to G$. A *normalised coordinate* on G is a coordinate x such that $x(0) = 0$.

Proposition 5.14. *Let G be a formal group over a scheme X. Then G admits a normalised coordinate x. Moreover, for any such coordinate, there is a unique formal group law $F(x,y) = \sum_{i,j} a_{ij}x^iy^j \in \mathrm{FGL}(\mathcal{O}_X)$ with the following property. For any ring R, any $t \in X(R)$, and any $u, v \in G(R)$ with $\pi(u) = \pi(v) = a$, we have*

$$x(u+v) = \sum_{ij} a_{ij}(t)x(u)^ix(v)^j.$$

(We will allow ourselves to write this as $x(u+v) = F(x(u),x(v))$.)

Proof. First let x_0 be an arbitrary coordinate, and put $x = x_0 - (x_0 \circ \zeta \circ \pi)$, or less formally $x = x_0 - x_0(0)$. It is easy to check that x is a normalised coordinate. Consider the function $f(u,v) = x(u+v)$, so $f \in \mathcal{O}_{G\times_X G}$. We see from Proposition 5.6 that $\mathcal{O}_{G\times_X G} = \mathcal{O}_X[\![x', x'']\!]$, where $x'(a,b) = x(a)$ and $x''(a,b) = x(b)$. It follows that there is a unique formal power series F such that $x(u+v) = F(x(u),x(v))$. As $x(0) = 0$, we find that $F(0,x(v)) = x(v)$. As the group structure of G is commutative and associative, we see that F is formally commutative and associative, so it is a formal group law as claimed. □

6. The symmetric cocycle lemma

We now start working towards Lazard's classification of formal group laws.

Definition 6.1. Let $L = \mathcal{O}_{\mathrm{FGL}}$ be the Lazard ring, and let $a_{ij} \in L$ be the coefficient of $x^i y^j$ in the universal formal group law over L. Let $\epsilon\colon L \to \mathbb{Z}$ correspond to the additive formal group law $x + y$ under the isomorphism $\mathrm{Hom}(L, \mathbb{Z}) = \mathrm{FGL}(\mathbb{Z})$, so that $\epsilon(a_{ij}) = 0$ when $i + j > 1$. Write $I = \ker(\epsilon) \leq L$.

The main work is to determine the structure of the Abelian group I/I^2. For this, we need the notion of a symmetric 2-cocycle.

Definition 6.2. Let A be an Abelian group, and let $A[\![x, y]\!]$ denote the group of formal power series of the form $\sum_{i,j\geq 0} a_{ij} x^i y^j$ with $a_{ij} \in A$. This is not naturally a ring unless A is a ring, but this will not matter for our purposes here.

A *symmetric* 2*-cocycle* with coefficients in A is a power series $f(x, y) \in A[\![x, y]\!]$ such that $f(x, y) = f(y, x)$ and $f(x, 0) = 0$ and

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

We write $Z(A)$ for the set of such f's. We also write $Z_d(A)$ for the subset consisting of homogeneous polynomials of degree d, so that $Z(A) = \prod_{d>1} Z_d(A)$. (It is easy to check that $Z_0(A) = Z_1(A) = 0$.)

Proposition 6.3. *There is a natural isomorphism $Z(A) = \mathrm{Hom}(I/I^2, A)$, for all Abelian groups A.*

Proof. Write $R = \mathbb{Z} \oplus A$, and make this into a ring by defining $(n, a).(m, b) = (nm, nb + ma)$. Then the projection map $\pi\colon R \to \mathbb{Z}$ is a ring homomorphism, the kernel is A (which is thus an ideal in R), and $A^2 = 0$. Let $Y(A)$ be the set of formal group laws F over R such that $(\pi F)(x, y) = x + y$. This means that $F(x, y) = x + y + f(x, y)$ for some $f(x, y) \in A[\![x, y]\!]$. The conditions $F(x, 0) = x$ and $F(x, y) = F(y, x)$ are equivalent to $f(x, 0) = 0$ and $f(x, y) = f(y, x)$. Next, we have

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

Because f has coefficients in A and $A^2 = 0$, we see that the last term is the same as $f(x + y, z)$. Given this, the associativity condition $F(x, F(y, z)) = F(F(x, y), z)$ is just $f(x, y) + f(x + y, z) = f(y, z) + f(x, y + z)$, which is equivalent to the cocycle condition. Thus, the map $F \mapsto f$ gives a bijection $Y(A) = Z(A)$.

On the other hand, formal group laws F over R biject with ring maps $\alpha\colon L \to R$. We clearly have $(\pi F)(x, y) = x + y$ if and only if $\pi\alpha(I) = 0$, or equivalently $\alpha(I) \leq A$. If so, then $\alpha(I^2) \leq A^2 = 0$, so α induces a homomorphism $I/I^2 \to A$. One checks easily that this gives a bijection $Y(A) = \mathrm{Hom}(I/I^2, A)$, as required. □

Lemma 6.4. *We have $(x + y)^p = x^p + y^p \pmod p$.*

Proof. Suppose that $0 < k < p$. Then $k!$ is a product of integers that are strictly less than p, so $k!$ is not divisible by p. Similarly, $(p - k)!$ is not divisible by p. However, $k!(p - k)!\binom{p}{k} = p!$ is divisible by p, so the binomial coefficient $\binom{p}{k}$ must be divisible by p. Thus $(x + y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} = x^p + y^p \pmod p$. □

Lemma 6.5. *We have $(x + y)^d = x^d + y^d \pmod p$ if and only if d is a power of p.*

Proof. If $d = p^k$ then we see from Lemma 6.4 and induction on k that $(x + y)^d = x^d + y^d \pmod p$. If d is not a power of p then we can write $d = p^k e$ for some k and e, where $e > 1$ and p does not divide e. We thus have

$$(X + Y)^e = X^e + eX^{e-1}Y + \ldots + Y^e \neq X^e + Y^e \pmod p.$$

It follows that

$$(x + y)^d = (x^{p^k} + y^{p^k})^e \neq x^d + y^d \pmod p,$$

as claimed. □

Definition 6.6. Let d be an integer greater than 1. If d is a power of a prime number p, then we define $\nu(d) = p$; otherwise, we define $\nu(d) = 1$. We also define

$$b_d(x, y) = (x + y)^d - x^d - y^d = \sum_{i=1}^{d-1} \binom{d}{i} x^i y^{d-i},$$

and $c_d(x,y) = b_d(x,y)/\nu(d)$. It follows from Lemma 6.5 that $c_d(x,y) \in \mathbb{Z}[x,y]$. One can check directly that $c_d(x,y)$ is a symmetric cocycle, so $c_d \in Z_d(\mathbb{Z})$. For any A, we define $\phi_A \colon A \to Z_d(A)$ by $\phi_A(a) = ac_d(x,y)$.

Exercise 6.7. Show that if $\Phi_d(x)$ is the d'th cyclotomic polynomial (so that $x^n - 1 = \prod_{d|n} \Phi_d(x)$ for all $n > 0$) then $\nu(d) = \Phi_d(1)$. It would be nice to give an alternate approach to the results of this section based on this fact, but I have not managed to find one.

Proposition 6.8. *The map $\phi_A \colon A \to Z_d(A)$ is always an isomorphism.*

This will be proved at the end of the section.

Lemma 6.9. *If $a = b \pmod{p^j}$ (with $j > 0$) then $a^{p^k} = b^{p^k} \pmod{p^{j+k}}$ for all $k \geq 0$.*

Proof. We can reduce by induction to the case $k = 1$. We have $a = b + p^j c$ for some c, so

$$a^p - b^p = \sum_{i=1}^{p-1} \binom{p}{i} p^{ij} b^i c^j + p^{pj} c^p.$$

All the binomial coefficients are divisible by p (by the proof of Lemma 6.4) and $pj \geq j+1$ so the right hand side is zero mod p^{j+1}, as required. □

Lemma 6.10. *If p is prime and $k \geq 0$ then*

$$c_{p^{k+1}}(x,y) = c_p(x^{p^k}, y^{p^k}) \neq 0 \pmod{p}.$$

Proof. We have seen that $(x+y)^{p^k} = x^{p^k} + y^{p^k} \pmod{p}$, so Lemma 6.9 tells us that $(x+y)^{p^{k+1}} = (x^{p^k} + y^{p^k})^p \pmod{p^2}$. The left hand side is $x^{p^{k+1}} + y^{p^{k+1}} + pc_{p^{k+1}}(x,y)$, and the right hand side is $x^{p^{k+1}} + y^{p^{k+1}} + pc_p(x^{p^k}, y^{p^k})$, so we conclude that $pc_{p^{k+1}}(x,y) = pc_p(x^{p^k}, y^{p^k}) \pmod{p^2}$, so $c_{p^{k+1}}(x,y) = c_p(x^{p^k}, y^{p^k}) \pmod{p}$. We have $c_p(X,Y) = \sum_{k=1}^{p-1} \frac{(p-1)!}{k!(p-k)!} X^k Y^{p-k}$, and the coefficients here are built from numbers strictly less than p so they are nonzero mod p. It follows that $c_p(x^{p^k}, y^{p^k}) \neq 0 \pmod{p}$ as claimed. □

Exercise 6.11. Show that $c_p(x,y) = -\sum_{k=1}^{p-1} (-x)^k y^{p-k}/k \pmod{p}$.

Corollary 6.12. *For each $d > 1$, the greatest common divisor of the coefficients of $c_d(x,y)$ is 1.*

Proof. It is equivalent to say that there is no prime p such that $c_d = 0 \pmod{p}$. Suppose that such a prime p exists. Then clearly $b_d = 0 \pmod{p}$, so $(x+y)^d = x^d + y^d \pmod{p}$. Thus, Lemma 6.5 tells us that $d = p^{k+1}$ for some $k \geq 0$, but then Lemma 6.10 tells us that $c_d(x,y) \neq 0 \pmod{p}$, a contradiction. □

Definition 6.13. The corollary implies that we can choose integers λ_{di} for all $0 < i < d$ such that

$$\sum_{i=1}^{d-1} \lambda_{di} \binom{d}{i} / \nu(d) = 1$$

for all $d > 1$. We fix such a system of λ's once and for all. We also define a map $\pi_A \colon Z_d(A) \to A$ by

$$\pi_A\Big(\sum_{i=1}^{d-1} a_i x^i y^{d-i}\Big) = \sum_i \lambda_{di} a_i.$$

Lemma 6.14. *We have $\pi_A \phi_A = 1 \colon A \to A$ for all A and all $d > 1$. Thus, ϕ_A is always a split monomorphism.*

Proof. This is clear from the definitions and the choice of the λ's. □

Given this,

Lemma 6.15. *$Z_d(A)$ is the set of polynomials $f(x,y) = \sum_{i=1}^{d-1} a_i x^i y^{d-i}$ with $a_i \in A$ such that $a_i = a_{d-i}$ and*

$$(i,j)a_{i+j} = (j, d-i-j)a_i$$

whenever $i > 0$ and $j \geq 0$ and $i + j < d$. (Here $(i,j) = (i+j)!/i!j!$.)

Proof. Just expand everything out. □

Lemma 6.16. *If A is a vector space over $\mathbb{Q}$ then the map $\phi_A\colon A \to Z_d(A)$ is an isomorphism for all $d > 1$, with inverse π_A.*

Proof. Define $\psi\colon Z_d(A) \to A$ by $\psi(f) = \nu(d)a_1/d$ (where $f(x,y) = \sum_i a_i x^i y^{d-i}$). It is easy to check that $\psi(c_d) = 1$, so that $\psi\phi_A = 1$. We next claim that ψ is injective. Indeed, suppose that $\psi(f) = 0$, so that $a_1 = 0$. The case $j = 1$ in Lemma 6.15 gives $a_{i+1} = (d-i)a_i/(i+1)$, so we see inductively that $a_i = 0$ for all i so $f = 0$ as required. We have seen that $\psi\phi = 1$ so $\psi\phi\psi = \psi$ but ψ is injective so $\phi\psi = 1$. Thus ϕ is an isomorphism as claimed. We know that $\pi_A\phi_A = 1$, so we must have $\pi_A = \psi = \phi_A^{-1}$. □

Corollary 6.17. *If A is a torsion-free Abelian group then the map $\phi_A\colon A \to Z_d(A)$ is an isomorphism for all $d > 1$.*

Proof. Write $A' = \mathbb{Q} \otimes A$; because A is torsion-free we have $A \leq A'$. It is easy to see that $Z_d(A) = A[x,y] \cap Z_d(A')$, and we know that $\phi_{A'}$ is an isomorphism by the lemma. It thus suffices to check that if $a \in A'$ and $\phi_{A'}(a) \in A[x,y]$ then $a \in A$. This is clear because $a = \pi_{A'}\phi_{A'}(a)$ and $\pi_{A'}$ sends $Z_d(A)$ to A by construction. □

Lemma 6.18. *Let A be a vector space over $\mathbb{Z}/p$ and suppose that $f \in Z_d(A)$. Write $f_2(x,y)$ for the partial derivative of f with respect to the second variable and suppose that $f_2(x,0) = 0$. Then $f(x,y) = g(x^p, y^p)$ for some $g \in Z_{d/p}(A)$, which means that $f = 0$ if d is not divisible by p.*

Proof. We have the cocycle identity

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

If we differentiate with respect to z at $z = 0$ we obtain $f_2(y,0) - f_2(x+y,0) + f_2(x,y) = 0$. As $f_2(x,0) = 0$, we conclude that $f_2(y,0) = f_2(x+y,0) = 0$ and thus $f_2(x,y) = 0$. If $f(x,y) = \sum_{i+j=d} a_{ij}x^i y^j$ then $f_2(x,y) = \sum_{i+j=d} j a_{ij} x^i y^{j-1}$ so we conclude that $a_{ij} = 0$ unless p divides j. As $a_{ij} = a_{ji}$ we see that $a_{ij} = 0$ unless p divides both i and j. If p does not divide d, we see that $a_{ij} = 0$ for all i, j and thus that $f = 0$. If p does divide d we see that $f(x,y) = g(x^p, y^p)$ for some homogeneous symmetric polynomial g of degree d/p. As $(x+y)^p = x^p + y^p \pmod p$ we see that $g(y^p, z^p) - g(x^p + y^p, z^p) + g(x^p, y^p + z^p) - g(x^p, y^p) = 0$, and it follows that $g(Y,Z) - g(X+Y,Z) + g(X,Y+Z) - g(X,Y) = 0 \in A[X,Y,Z]$, so $g \in Z_{d/p}(A)$. □

Lemma 6.19. *Suppose that p divides d but that d is not a power of p. Then if $f \in Z_d(A)$ we have $f(x,y) = g(x^p, y^p)$ for some $g \in Z_{d/p}(A)$.*

Proof. Because f is homogeneous of degree d and $dA = 0$ we have $xf_1(x,y) + yf_2(x,y) = df(x,y) = 0$. Write $g(x) = xf_2(x,0)$. As $f(x,y) = f(y,x)$ we also have $g(x) = xf_1(0,x)$. If we differentiate the cocycle identity with respect to z at $z = 0$ we obtain

$$f_2(y,0) - f_2(x+y,0) + f_2(x,y) = 0.$$

If we exchange x and y and then use the symmetry of f we obtain

$$f_1(0,x) - f_2(x+y,0) + f_1(x,y) = 0.$$

We now multiply these two equations by y and x respectively, and add them together using the relation $xf_1 + yf_2 = 0$. This gives $g(x+y) = g(x) + g(y)$. Moreover, it is clear that g is homogeneous of degree d, say $g(x) = ax^d$ for some $a \in A$. It follows that $\binom{d}{i} a = 0$ for $0 < i < d$, and d is not a power of p so we must have $a = 0$. Thus $f_2(x,0) = 0$, and the conclusion follows from Lemma 6.18. □

Lemma 6.20. *If $d = p^k > p$ and $f \in Z_d(A)$ then we have $f(x,y) = g(x^p, y^p)$ for some $g \in Z_{d/p}(x,y)$.*

Proof. Write $f(x,y) = \sum_{i=1}^{d-1} a_i x^i y^{d-i}$. If we apply Lemma 6.15 with $i = 1$ and $j = p-1$ we find that $\binom{p^k-1}{p-1} a_1 = p a_p = 0$. On the other hand, we have

$$\binom{p^k-1}{p-1} = \prod_{t=1}^{p-1} \frac{p^k - t}{t},$$

which is easily seen to be nonzero mod p. It follows that $a_1 = 0$, so $f_2(x,0) = a_1 x^{d-1} = 0$, and the conclusion again follows from Lemma 6.18. □

Exercise 6.21. Give another proof of Lemma 6.19 along the same lines as that of Lemma 6.20.

Lemma 6.22. *The map $\phi_{\mathbb{Z}/p,d}\colon \mathbb{Z}/p \to Z_d(\mathbb{Z}/p)$ is an isomorphism for all primes p and all $d > 1$.*

Proof. We have seen that ϕ_A is a split monomorphism for all A, so it suffices to show either that $\phi_{\mathbb{Z}/p,d}$ is surjective, or that $Z_d(\mathbb{Z}/p)$ has dimension at most one over $\mathbb{Z}/p$. First suppose that d is not divisible by p. Then for any $f \in Z_d(\mathbb{Z}/p)$ we have $f_2(x,0) = a_1 x^{d-1}$ for some $a_1 \in \mathbb{Z}/p$ and it follows from Lemma 6.18 that the map $f \mapsto a_1$ gives an injection $Z_d(\mathbb{Z}/p) \to \mathbb{Z}/p$, so $\phi_{\mathbb{Z}/p,d}$ is an isomorphism. Now consider the case $d = p$. Again, if $a_1 = 0$ we see that $f(x,y) = g(x^p, y^p)$ for some $g \in Z_1(\mathbb{Z}/p)$, but $Z_1(A) = 0$ for all A by easy arguments, so $f = 0$. It follows as before that $\phi_{\mathbb{Z}/p,p}$ is an isomorphism.

Now suppose that $d > p$ is divisible by p. We can then write $d = p^k e$ for some $k > 0$ and $e > 1$ with either $e = p$ or $e \neq 0 \pmod p$. By repeatedly applying Lemma 6.19, we find that $f(x,y) = g(x^{p^k}, y^{p^k})$ for some $g \in Z_e(\mathbb{Z}/p)$. It follows that the map $g \mapsto g(x^{p^k}, y^{p^k})$ gives a surjection from Z_e to Z_d, and we know that $Z_e \simeq \mathbb{Z}/p$, so Z_d has dimension at most one, so $\phi_{\mathbb{Z}/p,d}$ is an isomorphism. □

Lemma 6.23. *The map $\phi_{\mathbb{Z}/p^k}\colon \mathbb{Z}/p^k \to Z_d(\mathbb{Z}/p^k)$ is an isomorphism for all $k > 0$ and $d > 1$.*

Proof. We argue by induction, using the previous lemma for the case $k = 1$. Suppose that $f \in Z_d(\mathbb{Z}/p^{k+1})$. By the inductive hypothesis applied to the image of f in $Z_d(\mathbb{Z}/p^k)$, we see that there exists $a \in \mathbb{Z}/p^{k+1}$ such that $f - \phi(a) = 0 \pmod{p^k}$, say $f = \phi(a) + p^k g$ for some g. The polynomial g is well-defined mod p, and it is easy to check that it gives an element of $Z_d(\mathbb{Z}/p)$. Thus, by the case $k = 1$, we see that $g = \phi(b)$ for some $c \in \mathbb{Z}/p$, and thus $f = \phi(a + p^k b)$. This shows that ϕ is surjective, and we have already seen that it is injective. □

Proof of Proposition 6.8. We know from Corollary 6.17 and Lemma 6.23 that ϕ_A is an isomorphism when $A = \mathbb{Z}$ or $A = \mathbb{Z}/p^k$. Any finitely generated Abelian group can be written as a direct sum of groups of these types, and it is easy to see that $Z_d(A \oplus B) = Z_d(A) \oplus Z_d(B)$, so we see that ϕ_A is an isomorphism whenever A is finitely generated. Now let A be a general Abelian group, and suppose that $f \in Z_d(A)$. Let B be the subgroup of A generated by the coefficients of f, so that B is finitely generated and $f \in Z_d(B)$. As ϕ_B is an isomorphism, we have some $b \in B \leq A$ such that $f = \phi_B(b) = \phi_A(b)$. Thus, ϕ_A is surjective, and we also know from Lemma 6.14 that it is injective. □

7. The structure of the Lazard ring

Recall the Lazard ring $L = \mathcal{O}_{\mathrm{FGL}}$ constructed in the proof of Proposition 4.16. In this section, we investigate the structure of L. In principle, this gives a classification of all formal group laws.

Definition 7.1. Fix integers λ_{di} as in definition 6.13, and write $a_d = \sum_{i=1}^{d} \lambda_{di} a_{i,d-i} \in L$.

Theorem 7.2. *The Lazard ring L is a polynomial algebra over $\mathbb{Z}$ on the generators a_d for $d > 1$. In other words, we have*

$$L = \mathbb{Z}[a_2, a_3, a_4, \ldots].$$

This will be proved at the end of this section.

It is technically convenient in the proof to regard L as a graded ring, so we pause to explain some basic ideas about gradings.

Definition 7.3. A *grading* on a ring R is a sequence of additive subgroups R_k for $k \in \mathbb{Z}$ such that $1 \in R_0$ and $R_i R_j \subseteq R_{i+j}$ and $R = \bigoplus_k R_k$. If $a \in R_k$ for some k then we say that a is a homogeneous element of degree k.

Definition 7.4. Recall that we have an affine scheme G_m defined by $G_m(R) = R^\times$. An *action* of G_m on a scheme X is a map of schemes $\alpha\colon G_m \times X \to X$ such that $\alpha(1,x) = x$ and $\alpha(u, \alpha(v,x)) = \alpha(uv, x)$ for all rings R and all $x \in X(R)$ and $u, v \in R^\times$. We will often write $u.x$ rather than $\alpha(u,x)$.

Example 7.5. We have an action of G_m on RPS_1 by $(u.f)(x) = u^{-1} f(ux)$. We also have an action of G_m on FGL by $(u.F)(x,y) = u^{-1} F(ux, uy)$.

Proposition 7.6. *An action of G_m on an affine scheme $X = \mathrm{spec}(A)$ gives a grading of $\mathcal{O}_X = A$.*

Proof. Recall that $A = \mathcal{O}_X$ can be seen as the set of natural maps $f\colon X \to \mathbb{A}^1$. We let A_k be the set of those maps that satisfy $f(u.x) = u^k f(x)$ (for all rings R and all $x \in X(R)$ and $u \in R^\times$). It is clear that A_k is an additive subgroup of A, that $1 \in A_0$ and that $A_i A_j \leq A_{i+j}$. Thus, it suffices to check that $A = \bigoplus_k A_k$. Suppose that $f \in A$. We then have a map $g\colon G_m \times X \to \mathbb{A}^1$ given by $g(u, x) = f(u.x)$. This is an element of the ring

$$\mathcal{O}_{G_m \times X} = \mathcal{O}_{G_m} \otimes \mathcal{O}_X = \mathbb{Z}[u, u^{-1}] \otimes A = A[u, u^{-1}].$$

There are thus unique elements $f_k \in A$ for $k \in \mathbb{Z}$ such that $g = \sum_k u^k f_k$, or in other words $f(u.x) = \sum_k u^k f_k(x)$ for all x and u. If $f = f_k$ then clearly $f \in A_k$. Conversely, if $f \in A_k$ then we can get a decomposition of the type described by taking $f_k = f$ and $f_j = 0$ for all $j \neq k$, and by assumption there is only one such decomposition. Thus, we have $f \in A_k$ iff $f = f_k$. Moreover, the associativity of the action gives

$$\sum_k u^k v^k f_k(x) = f((uv).x) = f(u.(v.x)) = \sum_{i,j} u^i v^j f_{ij}(x).$$

By the same argument that gives the uniqueness of the f_i's, we can conclude that $f_k = f_{kk}$, so $f_k \in A_k$. Moreover, we have $f(x) = f(1.x) = \sum_k f_k(x)$, so $f = \sum_k f_k$. This shows that $A = \sum_k A_k$, and the uniqueness of the f_k's shows that the sum is direct. Thus, we have a grading on A. □

Example 7.7. Our action of G_m on FGL gives a grading of the Lazard ring L. For any formal group law F we have $F(x, y) = x + y + \sum_{i,j>0} a_{ij}(F) x^i y^j$, so $(u.F)(x, y) = x + y + \sum_{i,j>0} u^{i+j-1} a_{ij}(F) x^i y^j$, so $a_{ij}(u.F) = u^{i+j-1} a_{ij}(F)$, so $a_{ij} \in L_{i+j-1}$. It follows that $a_k \in L_{k-1}$. Note that L is a quotient of the polynomial ring generated by the elements a_{ij}. These all have strictly positive degree, and for any integer d there are only finitely many generators a_{ij} whose degree is less than d. It follows easily that each homogeneous piece L_k is a finitely generated Abelian group. It is this finiteness property that makes the grading useful for us.

Lemma 7.8. *There are elements $b_k \in \mathbb{Q} \otimes L_{k-1}$ for $k > 0$ such that $b_1 = 1$ and $\mathbb{Q} \otimes L = \mathbb{Q}[b_2, b_3, \ldots]$.*

Proof. Let M be the ring $\mathbb{Z}[b_2, b_3, \ldots]$, so we claim that $\mathbb{Q} \otimes L \simeq \mathbb{Q} \otimes M$. As we saw in Example 4.13, we can identify RPS_1 with $\mathrm{spec}(M)$. We now want to describe $\mathrm{spec}(\mathbb{Q} \otimes M)$. Notice that if every integer $n \neq 0$ becomes invertible in R then there is a unique homomorphism $\mathbb{Q} \to R$, and in any other case there are no homomorphisms $\mathbb{Q} \to R$. It follows that $\mathrm{spec}(\mathbb{Q} \otimes M)(R)$ is $\mathrm{RPS}_1(R)$ if R admits a $\mathbb{Q}$-algebra structure, and $\emptyset$ otherwise. We have a similar description of $\mathrm{spec}(\mathbb{Q} \otimes L)$ in terms of $\mathrm{spec}(L) = \mathrm{FGL}$, so we conclude that the map ϕ in Corollary 3.3 induces an isomorphism $\mathrm{spec}(\mathbb{Q} \otimes M) \simeq \mathrm{spec}(\mathbb{Q} \otimes L)$. As maps between schemes biject with maps between rings in the opposite direction (Corollary 4.12) we conclude that there is an isomorphism $\phi^*\colon \mathbb{Q} \otimes L \simeq \mathbb{Q} \otimes M$. If we let G_m act on RPS_1 and FGL as in Example 7.5 then one can check that $\phi(u.f) = u.\phi(f)$ and thus that $\phi^*(L_k) \leq M_k$. One can also see that $b_k \in M_{k-1}$, so the preimage of b_k in $\mathbb{Q} \otimes L$ lies in L_{k-1}. This proves the lemma.

We can be a little more explicit if desired: under the various implicit identifications, the element $b_k \in \mathbb{Q} \otimes L$ is just the coefficient of x^k in the logarithm of the universal formal group law F over L. The map $\phi^*\colon L \to M$ is the unique map that sends F to $f^{-1}(f(x) + f(y))$, where $f(x) = x + \sum_{k>0} b_k x^k \in M[\![x]\!]$. □

Definition 7.9. Recall that I is the kernel of the map $L \to \mathbb{Z}$ that sends a_{ij} to 0 when $i + j > 1$. It is easy to check that $I = \bigoplus_{k>0} L_k$. We also write $Q = I/I^2$, and Q_d for the part of Q in degree d, which is just

$$Q_d = L_d / \sum_{k=1}^{d-1} L_k L_{d-k}.$$

Lemma 7.10. *For each $d > 1$, the group Q_{d-1} is freely generated by a_d.*

Proof. We know from Proposition 6.3 that $Z(A) = \mathrm{Hom}(Q, A)$, and one can deduce easily that $Z_{d-1}(A) = \mathrm{Hom}(Q_{d-1}, A)$. We also know that the map $\pi_{d-1}\colon Z_{d-1}(A) \to A$ is an isomorphism. If we identify $Z_{d-1}(A)$ with $\mathrm{Hom}(Q_{d-1}, A)$, then this becomes the map $\alpha \mapsto \alpha(a_d)$. As this is an isomorphism, we conclude that Q_{d-1} is freely generated by a_d. □

Proof of Theorem 7.2. Let L' be the polynomial ring $\mathbb{Z}[a'_2, a'_3, \ldots]$, and define a map $\phi\colon L' \to L$ by $\phi(a'_k) = a_k$. There is a unique grading on L' such that a'_k is homogeneous of degree $k-1$ for all k, and if we use this then $\phi(L'_k) \leq L_k$ for all k. We now let I' be the ideal generated by $\{a'_k \mid k > 1\}$, so that $I' = \bigoplus_{k>0} L'_k$, and we put $Q' = I'/(I')^2$. This is the direct sum of its homogeneous pieces Q'_d, and it is easy to see that Q'_d is isomorphic to $\mathbb{Z}$, freely generated by a'_{d+1}. It follows easily that the induced map $\phi\colon I'/(I')^2 \to I/I^2$ is an isomorphism, and thus that $I = \phi(I') + I^2$. We now claim that $\phi\colon L'_d \to L_d$ is surjective for all d. Indeed, this is clear for $d = 0$. Suppose that it holds for degrees less than d, where $d > 0$. If $a \in L_d$ then $a \in I$ so we have $a = \phi(b) + c$ for some $b \in I'$ and $c \in I^2 = \sum_{i=1}^{d-1} L_i L_{d-i}$. By induction we know that $\phi\colon L'_i \to L_i$ is surjective for $0 < i < d$ and it follows that c is in the image of ϕ, and thus that a is in the image of ϕ. This shows that ϕ is surjective. Next, consider the induced map $\mathbb{Q} \otimes L' \to \mathbb{Q} \otimes L$. It follows from the above that this is again surjective. On the other hand, we know from Lemma 7.8 that $\mathbb{Q} \otimes L \simeq \mathbb{Q}[b_2, b_3, \ldots]$, with b_k homogeneous of degree $k-1$. It follows that $\mathbb{Q} \otimes L'_d$ and $\mathbb{Q} \otimes L_d$ have the same, finite, dimension as vector spaces over $\mathbb{Q}$. As $\phi\colon \mathbb{Q} \otimes L'_d \to \mathbb{Q} \otimes L_d$ is surjective, we conclude easily that it must be an isomorphism. On the other hand, L'_d is a free Abelian group, so the evident map $L'_d \to \mathbb{Q} \otimes L'_d$ is injective. If $a \in L'_d$ satisfies $\phi(a) = 0 \in L_d$ then the image under the composite $L'_d \to \mathbb{Q} \otimes L'_d \xrightarrow{\phi} \mathbb{Q} \otimes L_d$ is also zero, but this composite is injective so $a = 0$. It follows that $\phi\colon L' \to L$ is injective. We have already seen that it is surjective, so it is an isomorphism as required. □

8. The Functional Equation Lemma

The functional equation lemma gives sufficient conditions under which a formal group law defined over a ring of the form $\mathbb{Q} \otimes R$ is actually defined over R. We shall not formally state the lemma, but we will prove two results that implicitly use it.

Proposition 8.1. *Let p be a prime, and let $n > 0$ be an integer. Define $l(x) = \sum_{k \geq 0} x^{p^{nk}}/p^k$ and $F(x, y) = l^{-1}(l(x) + l(y))$. Then F is a formal group law over $\mathbb{Z}$.*

Proof. It is clear that F is a formal group law over $\mathbb{Q}$, so it will be enough to show that it is integral, in other words that the coefficients lie in $\mathbb{Z}$. This is true mod $(x, y)^2$, because $F(x, y) = x + y \pmod{(x, y)^2}$. Suppose that F is integral mod $(x, y)^d$; it will be enough to deduce that it is integral mod $(x, y)^{d+1}$. Write $R_0 = \mathbb{Z}[\![x, y]\!]/(x, y)^{d+1}$ and $R = \mathbb{Q} \otimes R_0 = \mathbb{Q}[\![x, y]\!]/(x, y)^{d+1}$. Write $q = p^n$ and let ψ be the unique ring map from R to itself that sends x to x^q and y to y^q. From now on we work in R. Because F is integral mod $(x, y)^d$, we can write $F = A + B$ where $A \in R_0$ and B is homogeneous of degree d. Moreover, A actually lies in the ideal generated by x and y, so $AB = xB = yB = B^2 = 0$. We make the following claims:

(a) $l(x) + l(y) = l(A + B) = l(A) + B$.
(b) $l(x) = x + l(x^q)/p$.
(c) $\psi(l(A)) = l(x^q) + l(y^q)$.
(d) If $u, v \in R_0$ and $u - v \in pR_0$ then $l(u) - l(v) \in pR_0$ (although usually $l(u), l(v) \notin R_0$).
(e) $\psi(A) - A^q \in pR_0$.
(f) $\psi(l(A))/p - l(A^q)/p \in R_0$.

For claim (a), we note that $F = A + B$ and $l(x) + l(y) = l(F)$ by the definition of F. If we expand out $l(A + B)$ using the fact that $AB = B^2 = 0$, we get $l(A) + B$ as claimed. For claim (b), we recall that $l(x) = \sum_{k \geq 0} x^{p^{nk}}/p^k$; the $k = 0$ term is just x, and the sum of the remaining terms is $l(x^q)/p$. We next note that $\psi(B) = 0$ (because B is homogeneous of degree d). Thus, if we apply the homomorphism ψ to equation (a) we get claim (c). For claim (d), we use Lemma 6.9 to deduce that $u^{p^{nk}} = v^{p^{nk}} \pmod{p^{nk+1}R_0}$ and the result follows easily. For (e), we observe that ψ induces an endomorphism $\overline{\psi}$ of $\overline{R}_0 = R_0/pR_0 = \mathbb{F}_p[\![x, y]\!]/(x, y)^{d+1}$. We also have an iterated Frobenius endomorphism $\phi^n\colon \overline{R}_0 \to \overline{R}_0$, and these two endomorphisms have the same effect on the generators x and y, so they must be the same. By applying them to A we see that $\psi(A) = A^q \pmod{pR_0}$ as claimed. Claim (f) follows immediately from (d) and (e).

We now have

$$\begin{aligned} B &= l(x) + l(y) - l(A) \\ &= (x + y - A) + (l(x^q) + l(y^q) - l(A^q))/p \\ &= (x + y - A) + (\psi(l(A)) - l(A^q))/p \\ &\in R_0. \end{aligned}$$

Indeed, the four lines above come from claims (a), (b), (c) and (f) respectively. This proves that B is integral, so F is integral mod $(x, y)^{d+1}$, as required. □

We now use similar methods to construct a more complicated formal group law that is p-locally universal, in a sense that we will not make precise here.

Definition 8.2. Let B be the ring $\mathbb{Z}[v_1, v_2, \ldots]$, and let $\psi\colon B \to B$ be the ring map that sends v_k to v_k^p for all k. There is a unique way to extend this to an endomorphism of $B[\![x, y]\!]$ sending x to x^p and y to y^p; we again write ψ for the extended map.

Now consider a sequence $I = (i_1, \ldots, i_r)$ of strictly positive integers. We write $|I| = r$ and $\|I\| = i_1 + \ldots + i_r$. We also write $\pi_t = \prod_{s<t} p^{i_s}$ and $v_I = \prod_{t=1}^r v_{i_t}^{\pi_t}$. We define

$$l(x) = \sum_I v_I x^{p^{\|I\|}}/p^{|I|}.$$

Here the sum runs over all such sequences, including the empty sequence, with $\|\emptyset\| = |\emptyset| = 0$ and $v_\emptyset = 1$. Finally, we write

$$F(x, y) = l^{-1}(l(x) + l(y)) \in (\mathbb{Q} \otimes B)[\![x, y]\!].$$

Proposition 8.3. *The series F defined above is a formal group law over B.*

Proof. Every nonempty sequence I can be written in the form iJ for some $i > 0$ and some possibly empty sequence J. One checks that $|I| = 1 + |J|$ and $\|I\| = i + \|J\|$ and $v_I = v_i v_J^{p^i} = v_i \psi^i(v_J)$. It follows easily that

$$l(x) = x + \sum_{i>0} v_i (\psi^i l)(x^{p^i})/p.$$

The rest of the proof is much the same as that of Proposition 8.1, except that we use the above equation in place of the equation $l(x) = x + l(x^q)/p$. □

9. The Frobenius map

In the next section, we will study formal group laws over $\mathbb{F}_p$-algebras, or equivalently rings R in which $p = 0$. As preparation for this, we need some generalities about schemes of the form $\mathrm{spec}(R)$ for such rings R. These are of course just the schemes over $\mathrm{spec}(\mathbb{F}_p)$.

Definition 9.1. If R is an $\mathbb{F}_p$-algebra, then we have a ring map $\phi = \phi_R\colon a \mapsto a^p$ from R to itself, called the *algebraic Frobenius map*. It is clear that if $f\colon R \to R'$ is a map of rings, then $f(a^p) = f(a)^p$, so $f\phi_R = \phi_{R'} f$, so the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\phi_R} & R \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ R' & \xrightarrow[\phi_{R'}]{} & R' \end{array}$$

This means that ϕ is a natural transformation from the identity functor to itself.

Definition 9.2. Let X be a functor with a map $X \to \mathrm{spec}(\mathbb{F}_p)$, which just means that $X(R) = \emptyset$ if $p \neq 0$ in R. We then define a map $F_X\colon X \to X$ by $(F_X)_R = X(\phi_R)\colon X(R) \to X(R)$. We call this the *geometric*

Frobenius map. If $f\colon X \to Y$ is a map of functors over $\mathrm{spec}(\mathbb{F}_p)$, we check easily (using the naturality of f_R with respect to maps of R) that the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{F_X} & X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ Y & \xrightarrow[F_Y]{} & Y. \end{array}$$

Proposition 9.3. *Let X be a functor over $\mathrm{spec}(\mathbb{F}_p)$.*

(1) *If $x \in X(R)$ and $f \in \mathcal{O}_X$ then $f(F_X(x)) = f(x)^p$.*
(2) *If $X = \mathrm{spec}(A)$, then $F_X = \mathrm{spec}(\phi_A)$.*

Proof. The first claim follows by regarding f as a map $X \to \mathbb{A}^1$ and using the naturality of F. For the second claim, let $u\colon A \to R$ be a point of $X(R)$. Then $F_X(u) = X(\phi_R)(u) = \phi_R \circ u$ and $\mathrm{spec}(\phi_A)(u) = u \circ \phi_A$, but these are the same because ϕ is natural. □

Definition 9.4. Let $f\colon X' \to X$ be a map of affine schemes over $\mathrm{spec}(\mathbb{F}_p)$, and let Y be a formal scheme over X. Let $q\colon Y \to X$ be the given projection map. We define a functor $Y' = f^*Y$ from rings to sets by $Y'(R) = \{(a', b) \in X'(R) \times Y(R) \mid f(a') = q(b)\}$. If $\{y_1, \dots, y_n\}$ is a system of formal coordinates on Y and $y_i'(a', b) = y_i(b)$ then one can easily check that $\{y_1', \dots, y_n'\}$ is a system of formal coordinates on Y', so Y' is a formal scheme over X'.

Remark 9.5. Let G be a formal group over an affine scheme X over $\mathrm{spec}(\mathbb{F}_p)$, and let $f\colon X' \to X$ be a map of affine schemes. We can then make $G' = f^*G$ into a formal group over X' by defining $\sigma((a', b_0), (a', b_1)) = (a', \sigma(b_0, b_1))$ and $\zeta(a') = (a', \zeta(f(a')))$. Here we have used the fact that if (a', b_0) and (a', b_1) lie in $G'(R)$ then $q(b_0) = f(a') = q(b_1)$, so $\sigma(b_0, b_1)$ is defined. In a different notation, we could just write $(a', b_0) + (a', b_1) = (a', b_0 + b_1)$ and $\zeta(a') = (a', 0)$.

Remark 9.6. Now suppose that $X = \mathrm{spec}(A)$ and $X' = \mathrm{spec}(A')$, so that $f\colon X' \to X$ comes from a map $u\colon A \to A'$. Suppose also that $G = G_F$ for some formal group law F over A. We then have a formal group law uF over A', and one can then identify G' with G_{uF}.

Definition 9.7. Let X be an affine scheme over $\mathrm{spec}(\mathbb{F}_p)$, and Y a formal scheme over X, with projection map $q\colon Y \to X$. We then have a map $F_X\colon X \to X$ and thus a formal scheme F_X^*Y over X. We define the relative Frobenius map $F_{Y/X}\colon Y \to F_X^*Y$ by $F_{Y/X}(b) = (q(b), F_Y(b))$. (This lies in $F_X^*Y(R)$ because of the naturality equation $q \circ F_Y = F_X \circ q$). If $y_1, \dots, y_n$ are coordinates on Y, and $y_1', \dots, y_n'$ are coordinates on F_X^*Y as in Definition 9.4, then we see that $y_i'(F_{Y/X}(a)) = y_i(a)^p$.

Lemma 9.8. *If G is a formal group over X then the relative Frobenius map $F_{G/X}\colon G \to F_X^*G$ is a homomorphism.*

Proof. Consider the addition map $\sigma\colon G \times_X G \to G$, which is a map of schemes over X. As the relative Frobenius map is natural, we have $F_{G/X} \circ \sigma = \sigma \circ F_{G \times_X G/X}$, and one sees from the definitions that $F_{G \times_X G/X} = F_{G/X} \times_X F_{G/X}$. Thus, we have $F_{G/X}(a + b) = F_{G/X}(a) + F_{G/X}(b)$ whenever $a + b$ is defined (ie, whenever a and b lie over the same point of X). Thus, $F_{G/X}$ is a homomorphism. □

We next introduce a formal version of differential forms.

Definition 9.9. Let X be an arbitrary affine scheme, and let Y be a formal scheme of dimension n over X. Then $Y \times_X Y$ is a formal scheme of dimension $2n$ over X. As usual, we let $\mathcal{O}_{Y \times_X Y}$ denote the ring of maps $Y \times_X Y \to \mathbb{A}^1$, and we let J denote the ideal of functions $g \in \mathcal{O}_{Y \times_X Y}$ such that $g(a, a) = 0$ for all points a of Y. We define $\Omega_{Y/X} = J/J^2$.

Remark 9.10. The analogy to think of is as follows. Let $q\colon Y \to X$ be a smooth map of smooth manifolds. Suppose this has the property that for each point $x \in X$, the preimage $Y_x = q^{-1}\{x\}$ is a submanifold of Y, diffeomorphic to $\mathbb{R}^n$. For any point $y \in Y$, let V_y be the cotangent space of the manifold $Y_{q(y)}$ at y. These vector spaces form a vector bundle of dimension n over Y, and we can define $\Omega_{Y/X}$ to be the space of global sections of this bundle. The proof of the next proposition will give some justification of why this is analogous to our definition for formal schemes.

Proposition 9.11. *$\Omega_{Y/X}$ is a free module of rank n over $\mathcal{O}_Y$.*

Proof. First, suppose that $g \in J$ and that $h \in \mathcal{O}_Y$. We then have two functions $k_0(a,b) = h(a)g(a,b)$ and $k_1(a,b) = h(b)g(a,b)$, giving two different elements of J. However, the map $(a,b) \mapsto h(a) - h(b)$ lies in J, so $k_0 - k_1 \in J^2$, so k_0 and k_1 have the same image in $J/J^2 = \Omega^1_{Y/X}$. We can thus make $\Omega_{Y/X}$ into a module over $\mathcal{O}_Y$ by defining $hg = k_0 = k_1$. We can also define a function $d\colon \mathcal{O}_Y \to \Omega_{Y/X}$ by $d(h)(a,b) = h(a) - h(b)$. We then have

$$d(hk)(a,b) = h(a)\, d(k)(a,b) + k(b)\, d(h)(a,b),$$

so $d(hk) = h\, d(k) + k\, d(h)$.

Now choose coordinates $x_1, \dots, x_n$ on Y. Then each x_i is a map $Y \to \widehat{\mathbb{A}}^1 \subset \mathbb{A}^1$, and thus can be thought of as an element of $\mathcal{O}_Y$. We claim that the elements $d(x_1), \dots, d(x_n)$ form a basis for $\Omega_{Y/X}$ over $\mathcal{O}_Y$. To see this, define $x_i', x_i''\colon Y \times_X Y \to \mathbb{A}^1$ by $x_i'(a,b) = x_i(a)$ and $x_i''(a,b) = x_i(b)$. We then have $\mathcal{O}_{Y\times_X Y} = \mathcal{O}_X[\![x_i', x_i'']\!]$, and this is the same as $\mathcal{O}_X[\![x_i', y_i]\!]$, where $y_i = x_i' - x_i''$. The diagonal inclusion $Y \to Y \times_X Y$ gives rise to a map $\mathcal{O}_{Y\times_X Y} \to \mathcal{O}_Y$, which sends x_i' and x_i'' to x_i and thus y_i to 0. The ideal J is by definition the kernel of this map, which is easily seen to be generated by the elements y_i. It follows that J^2 is generated by the elements $y_i y_j$, and thus that J/J^2 is a free module over $\mathcal{O}_Y$ generated by the elements y_i. However, the image of y_i in $\Omega_{Y/X} = J/J^2$ is just $d(x_i)$, by examining the definitions. □

Remark 9.12. Let $s\colon Y \to Z$ be a map of formal schemes over X. We then have an induced map $\mathcal{O}_{Z\times_X Z} \to \mathcal{O}_{Y\times_X Y}$, sending g to $g \circ (s \times_X s)$. This in turn induces a map $s^*\colon \Omega_{Z/X} \to \Omega_{Y/X}$. One checks that this satisfies $s^* d(g) = d(g \circ s)$ for $g \in \mathcal{O}_Z$, and $s^*(g\alpha) = (g \circ s)\, s^*(\alpha)$ for $\alpha \in \Omega_{Z/X}$.

Remark 9.13. Now suppose we choose coordinates $y_1, \dots, y_n$ on Y and $z_1, \dots, z_m$ on Z. There are then power series $g_1, \dots, g_m$ over $\mathcal{O}_X$ such that $z_i(s(a)) = g_i(y_1(a), \dots, y_n(a))$, and we have $s^* d(z_i) = \sum_j \partial g_i/\partial y_j\, d(y_j)$. Thus, the map $s^*\colon \Omega_{Z/X} \to \Omega_{Y/X}$ gives a coordinate-free encoding of the partial derivatives of the series g_i.

Proposition 9.14. *Let $s\colon Y \to Z$ be a map of formal schemes over an affine scheme X, with projection maps $q\colon Y \to X$ and $r\colon Z \to X$. Suppose that the induced map $s^*\colon \Omega_{Z/X} \to \Omega_{Y/X}$ is zero.*

(a) *If X is a scheme over* spec$(\mathbb{Q})$*, then there is a unique map $s'\colon X \to Z$ such that $r \circ s' = 1$ and $s = s' \circ q$ (so s is constant along the fibres of Y).*

(b) *If X is a scheme over* spec$(\mathbb{F}_p)$ *for some prime p then there is a unique map $s'\colon F_X^* Y \to Z$ of schemes over X such that $s = s' \circ F_{Y/X}$*

Proof. Choose coordinates, as in Remark 9.13. As $s^* = 0$ we have $\partial g_i/\partial y_j = 0$ for all i and j. For the rest of the argument, we assume that Y and Z have dimension one; the general case is essentially the same, but with more elaborate notation. We thus have a single series $g(y)$ over $\mathcal{O}_X$ with $g'(y) = 0$. If $g(y) = \sum_{k\geq 0} c_k y^k$ then we have $\sum_{k>0} k c_k y^{k-1} = 0$ and thus $k c_k = 0$ for all $k > 0$. If X lies over spec$(\mathbb{Q})$ then $\mathcal{O}_X$ is a $\mathbb{Q}$-algebra so $c_k = 0$ for all k. The analysis of proposition 5.6 shows that c_0 is nilpotent, or in other words that it is a map $X \to \widehat{\mathbb{A}}^1$. We know that z is a coordinate on Z so there is a unique map $s'\colon X \to Z$ over X such that $z(s'(a)) = c_0(a)$. We then have $z(s'(q(b))) = c_0(q(b))$ but by the definition of g this is the same as $z(s(b))$ so $s'(q(b)) = s(b)$ as required.

Now suppose instead that X lies over spec$(\mathbb{F}_p)$. As $k c_k = 0$ for all k, we see that $c_k = 0$ unless p divides k, so $g(y) = h(y^p)$ for some series h, which gives a map $X \times \widehat{\mathbb{A}}^1 \to X \times \widehat{\mathbb{A}}^1$ as in Proposition 5.6. We identify the second copy of $X \times \widehat{\mathbb{A}}^1$ with Z using the coordinate z, and the first one with $F_X^* Y$ using the coordinate y' as in Definition 9.4. This gives a map $s'\colon F_X^* Y \to Z$ such that $z(s'(b)) = h(y'(b))$. We also know that $y'(F_{Y/X}(a)) = y(a)^p$, so $z(s'(F_{Y/X}(a))) = h(y(a)^p) = g(y(a)) = z(s(a))$. This shows that $s = s' \circ F_{Y/X}$ as claimed. □

Definition 9.15. Let G be a formal group over an affine scheme X. Let I be the ideal in $\mathcal{O}_G$ of functions $g\colon X \to \mathbb{A}^1$ such that $g \circ \zeta = 0$ (or more informally, $g(0) = 0$).

Define $\omega_G = \omega_{G/X} = I/I^2$, and let $d_0(g)$ denote the image of g in $\omega_{G/X}$. We also define

$$\mathrm{Prim}(\Omega_{G/X}) = \{\alpha \in \Omega_{G/X} \mid \sigma^*\alpha = \pi_0^*\alpha + \pi_1^*\alpha \in \Omega_{G\times_X G/X}\}.$$

Here $\pi_0, \pi_1\colon G \times_X G \to G$ are the two projections.