Formal Groups

N. P. Strickland

Contents

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 20.

1. Introduction

DEFINITION 1.1. A *formal group law (FGL)* over a ring R is a formal power series $F(x,y) = \sum_{i,j\geq 0} a_{ij}x^i y^j \in R[\![x,y]\!]$ 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 FGLs 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 Lorentz 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 $\sum_{k\geq 0}(-xy/c^2)^k$.
(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

$$A = 1-\epsilon y^2z^2 \qquad B = 1-\epsilon z^2x^2 \qquad C = 1-\epsilon x^2y^2$$
$$p_2 = x^2+y^2+z^2 \qquad s_3 = xyz.$$

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

(5) In Section 14 we will explain a construction of FGLs due to Lubin and Tate. These are defined over the ring $\mathbb{Z}_p$ of p-adic integers (for some prime p), which will be introduced in Section 13; a single FGL over $\mathbb{Z}_p$ is essentially the same as a compatible family of FGLs over $\mathbb{Z}/p^m$ for all m. 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 $\mathbb{Z}_p$ such that $f(F(x,y)) = F(f(x), f(y))$, and that for this FGL we have $[p]_F(x) = f(x)$. These FGLs 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 FGLs 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 $(a+b)^{N+M} = \sum_{N+M=i+j} \binom{N+M}{i} a^i b^j = 0$, 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 FGLs 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 $f(g_k(x)) = x + c x^{k+1} \pmod{x^{k+2}}$, 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 FGLs 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 FGLs:

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

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. Formal group laws 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

$\sum_{i,j} jd_{ij}x^i y^{j-1} = 0$ 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 Lorentz 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) Consider a polynomial $f(x) \in \mathbb{Z}[x]$ with $f(x) = px \pmod{x^2}$ and $f(x) = x^{p^n} \pmod{p}$ for some prime p and integer $n > 0$. In the Introduction we mentioned that Lubin-Tate theory gives a FGL F over $\mathbb{Z}_p$ with $[p]_F(x) = f(x)$. In Proposition 14.7 we will show that
$$\log_F(x) = \lim_{n\to\infty} p^{-n} f^n(x).$$
(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 functor. 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 $\mathbb{A}^n = \mathrm{spec}(\mathbb{Z}[x_1, \ldots, x_n])$, 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

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

(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* $\operatorname{spec}(A)$ *to X bijects with $X(A)$.*

PROOF. The basic point is that a natural map $f\colon \operatorname{spec}(A) \to X$ 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 $\operatorname{spec}(A)$ to X. If $f \in T$ then we have a map

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

for each ring R. In particular, we have a map $f_A\colon \operatorname{Rings}(A, A) \to X(A)$, 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

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

We claim that these maps give a natural transformation $g\colon \operatorname{spec}(A) \to R$. 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 $u \in \operatorname{spec}(A)(R) = \operatorname{Rings}(A, R)$, 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

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

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 $\mathcal{O}_{\operatorname{spec}(A)} \simeq A$.*

PROOF. By definition, $\mathcal{O}_{\operatorname{spec}(A)}$ is the set of natural transformations from $\operatorname{spec}(A)$ 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* $\operatorname{spec}(\mathcal{O}_X)$.

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

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 $\mathrm{RPS} = \mathrm{spec}(\mathbb{Z}[b_1, b_2, \dots][b_1^{-1}])$.

PROPOSITION 4.14. *Let f and g be maps $X \to Y$ of affine schemes. Suppose that $\mathcal{O}_X$ is torsion-free, and that $f_R = g_R \colon X(R) \to Y(R)$ whenever R is a $\mathbb{Q}$-algebra. Then $f = g$.*

PROOF. The hypothesis is that for any $\mathbb{Q}$-algebra R and any ring homomorphism $u \colon \mathcal{O}_X \to R$ (corresponding to a point in $X(R)$), the composites $u \circ f^*, u \circ g^* \colon \mathcal{O}_Y \to R$ are the same. In particular, this applies when $R = \mathbb{Q} \otimes \mathcal{O}_X$ and $u \colon \mathcal{O}_X \to \mathbb{Q} \otimes \mathcal{O}_X$ is just given by $u(a) = 1 \otimes a$. As $\mathcal{O}_X$ is torsion-free, this map u is injective. Thus, the relation $u \circ f^* = u \circ g^*$ gives $f^* = g^*$ and so $f = g$. □

EXERCISE 4.15. 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 4.16. 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 4.17. *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 4.18. The ring $L = \mathcal{O}_{\mathrm{FGL}}$ is called the *Lazard ring*.

REMARK 4.19. 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. 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 $qf = p$.

LEMMA 5.1. *Let $X = \mathrm{spec}(A)$ be a scheme. Then the following categories are equivalent:*

(a) *The category of schemes over X*
(b) *The opposite of the category of A-algebras*
(c) *The category of representable functors from A-algebras to sets.*

PROOF. We have a contravariant equivalence between rings and schemes given by $A \leftrightarrows \mathrm{spec}(A)$, and this clearly gives an equivalence between (a) and (b). Yoneda's Lemma gives an equivalence between (b) and (c). The resulting equivalence between (a) and (c) is as follows. An A-algebra is just a ring B equipped with a ring map $x^*\colon A \to B$, or equivalently a point $x \in X(B)$. Now suppose we have a scheme Y equipped with a morphism $p\colon Y \to X$, and an A-algebra (B, x). We then have $p_B\colon Y(B) \to X(B)$ and $x \in X(B)$ so $p_B^{-1}\{x\} \subseteq Y(B)$. We define $Y'\colon \mathrm{Alg}_A \to \mathrm{Sets}$ by

$$Y'(B, x) = p_B^{-1}\{x\}.$$

In the opposite direction, given a functor $Y'\colon \mathrm{Alg}_A \to \mathrm{Sets}$ we define

$$Y(B) = \{(x, y) \mid x \in X(B) \text{ and } y \in Y'(B, x)\},$$

and we let $p\colon Y(B) \to X(B)$ be the evident projection. It is not hard to see that these constructions give the required equivalence. □

EXAMPLE 5.2. Let $X = \mathrm{spec}(A)$ be a scheme, and let M be an A-module. We can define a functor $\mathbb{A}'(M)\colon \mathrm{Alg}_A \to \mathrm{Sets}$ by

$$\mathbb{A}'(M)(B, x) = B \otimes_{A,x^*} M.$$

(In more detail, the right hand side is the tensor product of B and M over A, where we use the algebra structure map $x^*\colon A \to B$ to regard B as an A-module.) The corresponding functor from rings to sets is

$$\mathbb{A}(M)(B) = \{(x, m) \mid x \in X(B), m \in \mathbb{A}'(B, x)(M) = B \otimes_{A,x^*} M\}.$$

If M is a free A-module of rank $d < \infty$ with dual module M^*, then we can form the symmetric algebra

$$A[M^*] = \bigoplus_{n \geq 0} (M^*)^{\otimes n}_{\Sigma_n}.$$

We then have

$$\mathrm{Alg}_A(A[M^*], B) = \mathrm{Hom}_A(M^*, B) = B \otimes_A M = \mathbb{A}'(M)(B).$$

Using this, we see that $\mathbb{A}(M) = \mathrm{spec}(A[M^*])$. Also, a choice of basis for M gives an isomorphism $A[M^*] \simeq A[x_1, \dots, x_d]$ of A-algebras, and thus an isomorphism $\mathbb{A}(M) = X \times \mathbb{A}^d$.

DEFINITION 5.3. Consider again two functors V, W equipped with maps $p\colon V \to X$ and $q\colon W \to Z$. 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 5.4. 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.

EXAMPLE 5.5. Let M be any free module of rank n over A, and define $\widehat{\mathbb{A}}(M)\colon$ Rings $\to$ Sets by

$$\widehat{\mathbb{A}}(M)(B) = \{(x, m) \mid x \in X(B), m \in \mathrm{Nil}(B) \otimes_{A,x^*} M\}.$$

Any choice of basis for M gives a system of formal coordinates, showing that $\widehat{\mathbb{A}}(M)$ is an n-dimensional formal scheme over X.

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 5.6. *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 $f(x, g_k(x) + bx^{k+1}) = (a + b f_2(0, 0))x^{k+1} \pmod{x^{k+2}}$. 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 5.7. Generalise this to cover more variables and more equations.

EXAMPLE 5.8. 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 5.9. 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

$$g(x, y, z) = y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3.$$

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 $X = \mathrm{spec}(A)$. 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 5.6 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 5.10. *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 5.11. 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 5.12. Define

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

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 $\operatorname{spec}(\mathbb{Z})$.

EXAMPLE 5.13. We can also define $\widehat{G}_a(R) = \operatorname{Nil}(R)$, with the usual addition. This is clearly a formal group over $\operatorname{spec}(\mathbb{Z})$.

EXAMPLE 5.14. If F is a formal group law over A then we have a formal group G_F over $X = \operatorname{spec}(A)$ 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 5.15. The formal scheme $\widehat{C}$ of Example 5.9 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 5.16. Let E be a 2-periodic complex orientable generalised cohomology theory. Write $X = \operatorname{spec}(E^0)$, 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 5.17. 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 5.18. *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 5.10 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. □

DEFINITION 5.19. An *additive coordinate* on G is a coordinate x with the property that $x(u + v) = x(u) + x(v)$ for all $(u, v) \in G \times_X G$. Equivalently, if $p\colon G \to X$ is the given projection, then the map $u \mapsto (p(u), x(u))$ must give an isomorphism $G \to X \times \widehat{G}_a$ of formal groups over X.

PROPOSITION 5.20. *If $\mathcal{O}_X$ is a $\mathbb{Q}$-algebra, then G has an additive coordinate. Moreover, if x and y are two additive coordinates, then there is an invertible element $m \in \mathcal{O}_X^\times$ such that $y = mx$.*

PROOF. Let t be any normalised coordinate, and let F be the formal group law such that $t(u + v) = F(t(u), t(v))$. Proposition 3.1 gives us a reversible power series $f(t) \in \mathcal{O}_X[\![t]\!]$ such that $f(F(s, t)) = f(s) + f(t)$. This means that the element $x = f(t)$ is an additive coordinate. Now let y be another additive coordinate. As x is a coordinate, we must have $y = \sum_{i>0} m_ix^i$ for some sequence of coefficients $m_i \in \mathcal{O}_X$. As y is also a coordinate, we see that m_1 must be invertible. As both x and y are additive, we must have

$$\sum_i m_i(x(u) + x(v))^i = \sum_i m_i(x(u + v))^i = y(u + v) = y(u) + y(v) = \sum_i m_i(x(u)^i + x(v)^i).$$

We now expand out the left hand side and note that all the resulting binomial coefficients are invertible in $\mathbb{Q}$ and thus in $\mathcal{O}_X$. We conclude that $m_i = 0$ for $i > 1$, so $y = m_1x$ as required. □

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 $(x + y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} = x^p + y^p \pmod p$. □

We take this opportunity to prove another result in a similar spirit, although we will not it need until much later.

LEMMA 6.5. *Let k be a positive integer, given in base p by $k = \sum_i k_i p^i$ with $k_i \in \{0, \dots, p - 1\}$. Let $v_p(m)$ denote the largest j such that p^j divides m. Then*

$$v_p(k!) = \frac{k - \sum_i k_i}{p - 1} \leq \frac{k - 1}{p - 1}.$$

PROOF. Put

$$V = \{(i, j) \mid 1 \leq j \leq k \text{ and } 1 \leq i \text{ and } p^i \text{ divides } j\}.$$

We then have $v_p(k!) = \sum_{j=1}^{k} v_p(j) = |V|$. On the other hand, we also have $|V| = \sum_{i>0} \lfloor k/p^i \rfloor$. In terms of the base p expansion, we have $\lfloor k/p^i \rfloor = \sum_{m \geq i} k_m p^{m-i}$, so

$$|V| = \sum_{i>0} \sum_{m \geq i} k_m p^{m-i} = \sum_m k_m \sum_{i=1}^{m} p^{m-i} = \sum_m k_m \frac{p^m - 1}{p-1} = \frac{k - \sum_i k_i}{p-1}.$$

We have assumed that $k > 0$ so $\sum_i k_i \geq 1$ so we also have $|V| \leq (k-1)/(p-1)$. □

LEMMA 6.6. *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 6.7. 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

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

and $c_d(x,y) = b_d(x,y)/\nu(d)$. It follows from Lemma 6.6 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 $\phi_A(a) = a c_d(x,y)$.

EXERCISE 6.8. 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 6.9. *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 6.10. *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

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

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 6.11. *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 6.10 tells us that $(x+y)^{p^{k+1}} = (x^{p^k} + y^{p^k})^p \pmod{p^2}$. The left hand side is $x^{p^{k+1}} + y^{p^{k+1}} + p c_{p^{k+1}}(x,y)$, and the right hand side is $x^{p^{k+1}} + y^{p^{k+1}} + p c_p(x^{p^k}, y^{p^k})$, so we conclude that $p c_{p^{k+1}}(x,y) = p c_p(x^{p^k}, y^{p^k}) \pmod{p^2}$, 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 6.12. Show that $c_p(x,y) = -\sum_{k=1}^{p-1} (-x)^k y^{p-k}/k \pmod p$.

COROLLARY 6.13. *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 6.6 tells us that $d = p^{k+1}$ for some $k \geq 0$, but then Lemma 6.11 tells us that $c_d(x,y) \neq 0 \pmod p$, a contradiction. □

LEMMA 6.14. *Let $u_1, \dots, u_r$ be positive integers, and put $d_i = \gcd(u_i, \dots, u_r)$, so $d_1 \mid d_2 \mid \cdots \mid d_r$. Then there is a unique list of integers $a_1, \dots, a_r$ such that*

(a) $\sum_i a_i u_i = d_1$
(b) *For $1 \leq i < r$ we have $0 \leq a_i < d_{i+1}/d_i$.*

PROOF. Put $a'_i = a_i/d_i$ and $d'_i = d_{i+1}/d_i$. As $\gcd(a_i, d_{i+1}) = d_i$ we see that a'_i and d'_i are coprime. Now define $f\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $f(s,t) = sa'_i + td'_i$. We find that this is a surjective homomorphism with kernel generated by $(d'_i, -a'_i)$. It follows easily that if we put $U_i = \{0, 1, \dots, d'_i - 1\}$, then f_i gives a bijection $U_i \times \mathbb{Z} \to \mathbb{Z}$. Now define $g_i\colon \mathbb{Z} \times D_{i+1} \to D_i$ by $g_i(s,t) = sa_i + t$, or equivalently $g_i(s, t\, d_{i+1}) = f_i(s,t)d_i$. We find that this gives a bijection $g_i\colon U_i \times D_{i+1} \to D_i$. By combining $g_1, \dots, g_{r-1}$, we get a bijection

$$g\colon U_1 \times U_2 \times \cdots \times U_{r-1} \times D_r \to D_1.$$

Note also that $d_r = u_r$ and so $D_r = \mathbb{Z}u_r$. Thus, the element $g^{-1}(d_1)$ will have the form $(a_1, \dots, a_{r-1}, a_r u_r)$ for some integers a_i, and these have the claimed properties (a) and (b). □

DEFINITION 6.15. We let λ_{di} be the unique system of integers (defined for $0 < i < d$) such that

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

and the auxiliary inequalities in Lemma 6.14 are satisfied. We also define a map $\pi_A\colon Z_d(A) \to A$ by

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

REMARK 6.16. We use Lemma 6.14 solely because we have an aesthetic preference for a fully specified set of coefficients. Any other system of coefficients with $\sum_i \lambda_{di} \binom{d}{i} = \nu(d)$ would work just as well.

LEMMA 6.17. *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. □

LEMMA 6.18. *$Z_d(A)$ 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 6.19. *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 6.18 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 6.20. *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 6.21. *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 6.22. *Let A be a vector space over $\mathbb{Z}/p$. 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 $x f_1(x,y) + y f_2(x,y) = d f(x,y) = 0$. Write $h(x) = x f_2(x,0)$. As $f(x,y) = f(y,x)$ we also have $h(x) = x f_1(0,x)$. 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 $x f_1 + y f_2 = 0$. This gives $h(x+y) = h(x) + h(y)$. Moreover, it is clear that g is homogeneous of degree d, say $h(x) = a x^d$ 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 6.21. □

LEMMA 6.23. *Let A be a vector space over $\mathbb{Z}/p$. 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 6.18 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 6.21. □

EXERCISE 6.24. Give another proof of Lemma 6.22 along the same lines as that of Lemma 6.23.

LEMMA 6.25. *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 6.21 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 6.22, 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 6.26. *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 6.9. We know from Corollary 6.20 and Lemma 6.26 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 6.17 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 4.17. 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 6.15, 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 6.10 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 $X = \operatorname{spec}(A)$ and $X' = \operatorname{spec}(A')$, 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 $\operatorname{spec}(\mathbb{F}_p)$, 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 $\operatorname{spec}(\mathbb{Q})$, 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 $\operatorname{spec}(\mathbb{F}_p)$ 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 $\sum_{k>0} kc_k y^{k-1} = 0$ and thus $kc_k = 0$ for all $k > 0$. If X lies over $\operatorname{spec}(\mathbb{Q})$ then $\mathcal{O}_X$ is a $\mathbb{Q}$-algebra so $c_k = 0$ for all k. The analysis of proposition 5.10 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 $\operatorname{spec}(\mathbb{F}_p)$. As $kc_k = 0$ 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 5.10. 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

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

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

We now give a formal version of the fact that left-invariant differential forms on a Lie group biject with elements of the cotangent space at the identity element.

PROPOSITION 9.16. *$\omega_{G/X}$ is a free module on one generator over $\mathcal{O}_X$. Moreover, there are natural isomorphisms $\omega_{G/X} \simeq \operatorname{Prim}(\Omega_{G/X})$ and $\Omega_{G/X} = \mathcal{O}_G \otimes_{\mathcal{O}_X} \omega_{G/X}$.*

PROOF. Let x be a normalised coordinate on G. We see from Proposition 5.10 that $\mathcal{O}_G = \mathcal{O}_X[\![x]\!]$, and it is easy to check that $I = (x)$ so $I^2 = (x^2)$ so $\omega_{G/X}$ is freely generated over $\mathcal{O}_X$ by $d_0(x)$.

Now let K be the ideal in $\mathcal{O}_{G\times_X G}$ of functions k such that $k(0,0) = 0$. In terms of the usual description $\mathcal{O}_{G\times_X G} = \mathcal{O}_X[\![x', x'']\!]$, this is just the ideal generated by x' and x''. Given $g \in I$, we define $\delta(g)(u,v) = g(u+v) - g(u) - g(v)$. We claim that $\delta(g) \in K^2$. Indeed, we clearly have $\delta(g)(0,v) = 0$, so $\delta(g)$ is divisible by x'. We also have $\delta(g)(u,0) = 0$, so $\delta(g)$ is divisible by x''. It follows easily that $\delta(g)$ is divisible by $x'x''$ and thus that it lies in K^2 as claimed.

Next, let J be as in Definition 9.9. For any function $g \in I$ we define $\lambda(g) \in J$ by $\lambda(g)(u,v) = g(u-v)$. As $g(0) = 0$ we see that $\lambda(g) \in J$, so λ induces a map $\omega_{G/X} \to \Omega_{G/X}$. We claim that $\lambda(g) \in \operatorname{Prim}(\Omega_{G/X})$. To make this more explicit, let L be the ideal of functions l on $G \times_X G \times_X G \times_X G$ such that $l(s,s,u,u) = 0$. The claim is that $\sigma^*\lambda(g) - \pi_0^*\lambda(g) - \pi_1^*\lambda(g) = 0$ in L/L^2, or equivalently that the function

$$k\colon (s,t,u,v) \mapsto \lambda(g)(s+u, t+v) - \lambda(g)(s,t) - \lambda(g)(u,v)$$

lies in L^2. To see this, note that $k = \delta(g) \circ \theta$, where $\theta(s,t,u,v) = (s-t, u-v)$. It is clear that $\theta^*K \subset L$ and thus that $\theta^*K^2 \subset L^2$, and we have seen that $\delta(g) \in K^2$ so $k \in L^2$ as claimed. Thus, we have a map $\lambda\colon \omega_{G/X} \to \operatorname{Prim}(\Omega_{G/X})$.

Next, given a function $h(u,v)$ in J, we have a function $\mu(h)(u) = h(u,0)$ in I. It is clear that μ induces a map $\Omega_{G/X} \to \omega_{G/X}$ with $\mu \circ \lambda = 1$. Now suppose that h gives an element of $\mathrm{Prim}(\Omega_{G/X})$ and that $\mu(h) \in I^2$. Define $k(s,t,u,v) = h(s+u,t+v) - h(s,t) - h(u,v)$. The primitivity of h means that $k \in L^2$. Define $\phi\colon G \times_X G \to G \times_X G \times_X G \times_X G$ by $\phi(s,t) = (t,t,s-t,0)$. One checks that $\phi^* L \subseteq J$ and that

$$h(s,t) = k(t,t,s-t,0) + h(t,t) + h(s-t,0).$$

Noting that $h(t,t) = 0$, we see that $h = \phi^* k + \psi^* \mu(h)$, where $\psi(u,v) = u - v$. As $\mu(h) \in I^2$ and $k \in L^2$ we conclude that $h \in J^2$. This means that μ is injective on $\mathrm{Prim}(\Omega_{G/X})$. As $\mu\lambda = 1$, we conclude that λ and μ are isomorphisms.

Finally, we need to show that the map $f \otimes \alpha \mapsto f\lambda(\alpha)$ gives an isomorphism $\mathcal{O}_G \otimes_{\mathcal{O}_X} \omega_{G/X} \to \Omega_{G/X}$. As $\Omega_{G/X}$ is freely generated over $\mathcal{O}_G$ by $d(x)$, we must have $\lambda(d_0(x)) = u(x)d(x)$ for some power series u. As $\omega_{G/X}$ is freely generated over $\mathcal{O}_X$ by $d_0(x)$, it will suffice to check that u is invertible, or equivalently that $u(0)$ is a unit in $\mathcal{O}_X$. To see this, observe that $\mu(f\, d(g)) = f(0)d_0(g)$, so that $d_0(x) = \mu\lambda(d_0(x)) = \mu(u(x)d(x)) = u(0)d_0(x)$, so $u(0) = 1$. □

Proposition 9.17. *Let G and H be formal groups over an affine scheme X, and let $s\colon G \to H$ be a homomorphism. Suppose that the induced map $s^*\colon \omega_H \to \omega_G$ is zero.*

(a) *If X is a scheme over $\mathrm{spec}(\mathbb{Q})$, then $s = 0$.*
(b) *If X is a scheme over $\mathrm{spec}(\mathbb{F}_p)$ for some prime p then there is a unique homomorphism $s'\colon F_X^* G \to H$ of formal groups over X such that $s = s' \circ F_{G/X}$.*

Proof. It follows from the definitions that our identification of $\omega_{G/X}$ with $\mathrm{Prim}(\Omega_{G/X})$ is natural for homomorphisms. Thus, if $\alpha \in \mathrm{Prim}(\Omega_{H/X})$ then $s^*\alpha = 0$. We also know that $\Omega_{H/X} = \mathcal{O}_H \otimes_{\mathcal{O}_X} \omega_{H/X}$, so any element of $\Omega_{H/X}$ can be written as $f\alpha$ with $f \in \mathcal{O}_H$. Thus $s^*(f\alpha) = (f \circ s).s^*\alpha = 0$. Thus, Proposition 9.14 applies to s. If X lies over $\mathrm{spec}(\mathbb{Q})$ then we conclude that s is constant on each fibre. As it is a homomorphism, it must be the zero map. Suppose instead that X lies over $\mathrm{spec}(\mathbb{F}_p)$. In that case we know that there is a unique map $s'\colon G' = F_X^* G \to H$ such that $s = s' \circ F_{G/X}$, and we need only check that this is a homomorphism. In other words, we need to check that the map $t'(u,v) = s'(u+v) - s'(u) - s'(v)$ (from $G' \times_X G'$ to H) is zero. Because s and $F_{G/X}$ are homomorphisms, we see that $t' \circ F_{G \times_X G/X} = 0\colon G \times_X G \to H$. Applying the uniqueness clause in Proposition 9.14 to the map $0\colon G \times_X G \to H$, we conclude that $t' = 0$ as required. □

Corollary 9.18. *Let G and H be formal groups over an affine scheme X, which lies over $\mathrm{spec}(\mathbb{F}_p)$. Let $s\colon G \to H$ be a homomorphism. Then either $s = 0$ or there is an integer $n \geq 0$ and a homomorphism $s'\colon (F_X^n)^* G \to H$ such that $s = s' \circ F_{G/X}^n$ and $(s')^*$ is nonzero on $\omega_{H/X}$.*

Before proving this, we reformulate it.

Corollary 9.19. *Let $s\colon G \to H$ be as above, and let x and y be normalised coordinates on G and H respectively. Let f be the unique series $f(t) \in \mathcal{O}_X[\![t]\!]$ such that $y(s(a)) = f(x(a))$ for all points a of G. Then either $f = 0$, or there is an integer n and a power series g such that $f(t) = g(t^{p^n})$ and $g'(0) \neq 0$ (So we cannot have $f(t) = t^p + t^{p+1}$, for example).*

Proof of Corollary 9.18. Suppose that there is a largest integer n (possibly 0) such that s can be factored in the form $s = s' \circ F_{G/X}^n$. Write $G' = (F_X^n)^* G$, so that $s'\colon G' \to H$. If $(s')^* = 0$ on $\omega_{H/X}$ then the proposition gives a factorisation $s' = s'' \circ F_{G'/X}$ and thus $s = s'' \circ F_{G/X}^{n+1}$ contradicting maximality. Thus $(s')^* \neq 0$ as claimed. On the other hand, suppose that there is no largest n. Let $f(t)$ be as in Corollary 9.19. Then $f(0) = 0$ and f is a function of t^{p^n} for arbitrarily large n. It follows that $f = 0$, as required. □

Corollary 9.20. *Let G and H be formal groups over an affine scheme X, and let $s\colon G \to H$ be a homomorphism. Suppose that the induced map $s^*\colon \omega_H \to \omega_G$ is zero, and that $\mathcal{O}_X$ is torsion-free. Then $s = 0$.*

Proof. After introducing a coordinate, the claim is that a certain power series $f(x) \in \mathcal{O}_X[\![x]\!]$ is zero. As $\mathcal{O}_X$ is torsion-free, the map $\mathcal{O}_X \to \mathbb{Q} \otimes \mathcal{O}_X$ is injective, so it will suffice to check that $f(x)$ becomes zero in $(\mathbb{Q} \otimes \mathcal{O}_X)[\![x]\!]$. This is clear from Proposition 9.17(a). □

DEFINITION 9.21. Let G and H be formal groups over an affine scheme X, which lies over $\operatorname{spec}(\mathbb{F}_p)$. Let $s\colon G \to H$ be a homomorphism. If $s = 0$, we say that s has *infinite height*. Otherwise, the *height* of s is defined to be the integer n occurring in Corollary 9.18. The height of the group G is defined to be the height of the endomorphism $p_G\colon G \to G$ (which is just p times the identity map).

DEFINITION 9.22. Let R be an $\mathbb{F}_p$-algebra, and F a formal group law over R. The *height* of F is the height of the formal group G_F over $\operatorname{spec}(R)$. Equivalently, if $[p]_F(x) = 0$ then F has infinite height. Otherwise, there is a unique integer $n > 0$ such that $[p]_F(x) = g(x^{p^n})$ for some series g with $g'(0) \neq 0$, and then the height of F is n.

LEMMA 9.23. *Let G be a formal group over X. For $m \in \mathbb{Z}$ we let $m_G\colon G \to G$ be the map $a \mapsto ma$. Then we have $m_G^*\alpha = m\alpha$ for all $\alpha \in \operatorname{Prim}(\Omega_{G/X})$.*

PROOF. We leave it to the reader to reduce to the case $m > 1$. Let $\delta\colon G \to G_X^m$ be the diagonal map, let $\sigma_m\colon G_X^m \to G$ be the addition map, and let $\pi_1, \dots, \pi_m\colon G_X^m \to G$ be the projection maps. By the definition of $\operatorname{Prim}(\Omega_{G/X})$ we have $\sigma_2^*\alpha = \pi_1^*\alpha + \pi_2^*\alpha$. It follows inductively that $\sigma_m^*\alpha = \sum_{k=1}^m \pi_k^*\alpha$. We have $\sigma_m\delta = m_G$ and $\pi_k\delta = 1$ so $m_G^*\alpha = \delta^*\sigma_m^*\alpha = \sum_{k=1}^m \alpha = m\alpha$, as claimed. □

COROLLARY 9.24. *If G is a formal group over a scheme X over $\operatorname{spec}(\mathbb{F}_p)$, then $p_G^* = p = 0$ on ω_G, so G has height at least one.*

EXAMPLE 9.25.
(1) Take $G = \widehat{G}_a \times \operatorname{spec}(\mathbb{F}_p)$, which is a formal group over $\operatorname{spec}(\mathbb{F}_p)$. With the usual coordinate we have $F(x, y) = x + y$ so $[p](x) = px = 0$, so G has infinite height.
(2) Take $G = \widehat{G}_m \times \operatorname{spec}(\mathbb{F}_p)$. We then have $p_G(u) = u^p = F_G(u)$, so $p_G = F_G$, so clearly G has height one.
(3) Take $F(x, y) = (x + y)/(1 + xy)$, considered as an FGL over $\mathbb{F}_p$. If $p = 2$ then this has infinite height, otherwise it has height one. This follows from the isomorphisms given in Example 2.14.
(4) Let C be an elliptic curve over a scheme X over $\operatorname{spec}(\mathbb{F}_p)$, and let $\widehat{C}$ be its formal completion. Then it turns out that $\widehat{C}$ has height one or two. In the case where $\mathcal{O}_X$ is a field, the curve is said to be *supersingular* if $\widehat{C}$ has height two, and *ordinary* if $\widehat{C}$ has height one.
(5) Let F be the formal group law over $\mathbb{Z}$ with logarithm $\sum_{k\geq 0} x^{p^{nk}}/p^k$, as considered in Proposition 8.1. We shall show in a minute that the reduction of this formal group law mod p has height n.
(6) 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 $n > 0$. We will see later 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 $[p]_F(x) = f(x)$. If we write $\overline{F}$ for the resulting FGL over $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ then we see that $[p]_{\overline{F}}(x) = x^{p^n}$, so that $\overline{F}$ has height n.

PROPOSITION 9.26. *Let F be the formal group law over $\mathbb{Z}$ such that $\log_F(x) = \sum_{k\geq 0} x^{p^{nk}}/p^k$ (as considered in Proposition 8.1), and let $\overline{F}$ be the resulting formal group law over $\mathbb{F}_p$. Then $[p]_{\overline{F}}(x) = x^{p^n}$, so that $\overline{F}$ has height n.*

PROOF. Write $q = p^n$. We observe from the definition that $p\log_F(x) = px + \log_F(x^q)$, and by applying $\exp_F$ we find that $[p](x) = \exp_F(px) +_F x^q$. Write

$$f(x) = \log_F(px)/p = \sum_{k\geq 0} p^{p^{nk}-k-1} x^{p^{nk}}.$$

One checks that $f(x) \in \mathbb{Z}[\![x]\!]$ and $f(x) = x \pmod{x^2}$ so f is reversible in $\mathbb{Z}[\![x]\!]$. The reverse is easily seen to be the series $g(x) = \exp_F(px)/p$, so we conclude that this series is integral, and thus that $\exp_F(px) \in p\mathbb{Z}[\![x]\!]$. We can thus reduce the equation $[p](x) = \exp_F(px) +_F x^q \bmod p$ to obtain $[p]_{\overline{F}}(x) = x^q$, as claimed. □

10. Formal groups of height at least n

DEFINITION 10.1. Fix a prime p. For any formal group law F and $k > 0$, we let $u_k(F)$ be the coefficient of x^k in $[p]_F(x)$, so $u_k \in \mathcal{O}_{\mathrm{FGL}} = L$ and $u_1 = p$. If we define $(w.F)(x, y) = w^{-1}F(wx, wy)$ then $[p]_{w.F}(x) =$

$w^{-1}[p]_F(wx)$, so $u_k(w.F) = w^{k-1}u_k(F)$, so u_k is a homogeneous element of degree $k-1$ with respect to the grading introduced in Examples 7.5 and 7.7. We also write $v_k = u_{p^k}$ (so that $v_0 = p$ and v_k has degree $p^k - 1$).

DEFINITION 10.2. Now fix an integer $n > 0$, and let $\mathrm{FGL}_{p,n}(R)$ be the set of formal group laws of height at least n over R. Write I_n for the ideal in L generated by the elements u_k for which k is not divisible by p^n. It is clear that a formal group law F has height at least n if and only if $u_k(F) = 0$ for all such k, and thus that $\mathrm{FGL}_{p,n} = \mathrm{spec}(L/I_n)$.

LEMMA 10.3. *The ideal I_n is generated by $\{v_0, \dots, v_{n-1}\}$.*

PROOF. Let F be a FGL of height $m > 0$. Then $[p]_F(x) = g(x^{p^m})$ for some series g with $g'(0) \neq 0$, say $g'(0) = a$. This means that $[p]_F(x) = ax^{p^m} \pmod{x^{p^m+1}}$, so $v_0(F) = \ldots = v_{m-1}(F) = 0$ and $v_m(F) = a \neq 0$. It follows easily that F has height at least n if and only if $v_0(F) = \ldots = v_{n-1}(F) = 0$, which means that $\mathrm{FGL}_{p,n} = \mathrm{spec}(L/(v_k \mid k < n))$ and thus that $I_n = (v_k \mid k < n)$. □

PROPOSITION 10.4. *We have*

$$L/p = \mathbb{F}_p[v_i \mid i > 0] \otimes \mathbb{F}_p[a_k \mid k \text{ is not a power of } p],$$

and thus

$$\mathcal{O}_{\mathrm{FGL}_{p,n}} = L/I_n = \mathbb{F}_p[v_i \mid i \geq n] \otimes \mathbb{F}_p[a_k \mid k \text{ is not a power of } p].$$

The proof will be given after two lemmas.

LEMMA 10.5. *Let A be an Abelian group, and $f(x,y) = \sum_{d>1} a_d c_d(x,y)$ a symmetric cocycle over A. Make $R = \mathbb{Z} \oplus A$ into a ring as in the proof of Proposition 6.3, and let $F(x,y) = x + y + f(x,y)$ be the resulting FGL over R. Then for $m > 0$ we have*

$$[m]_F(x) = mx + \sum_{d>1} (m^d - m)/\nu(d)\ a_d x^d,$$

and the numbers $(m^d - m)/\nu(d)$ are integers.

PROOF. Using the fact that $m^p = m \pmod{p}$ for all primes p, we see that $(m^d - m)/\nu(d)$ is an integer.

Suppose that A is torsion-free. In this case it is clearly sufficient to work in $A' = \mathbb{Q} \otimes A$. Write $a'_d = a_d/\nu(d)$ and $g(x) = \sum_d a'_d x^d$ so that $f(x,y) = g(x+y) - g(x) - g(y)$. As g has coefficients in A' and $x +_F y = x + y \pmod{A}$ and $A^2 = 0$, this is the same as $g(x +_F y) - g(x) - g(y)$. After feeding this into the definition $F(x,y) = x + y + f(x,y)$ we find that $x +_F y - g(x +_F y) = x - g(x) + y - g(y)$, so the series $h(x) = x - g(x)$ is a homomorphism from F to the additive FGL. This implies that $h([m]_F(x)) = mh(x)$. Using $A^2 = 0$ again we see that $g([m]_F(x)) = g(mx)$ so

$$[m]_F(x) = mh(x) + g(mx) = mx + g(mx) - mg(x) = mx + \sum_{d>1} (m^d - m)/\nu(d)\ a_d x^d,$$

as claimed.

Now let A be an arbitrary Abelian group. Write $A' = \bigoplus_{d>1} \mathbb{Z}$, and let a'_d be the evident basis vector in A', and define $f' = \sum_d a'_d c_d \in Z(A')$. Let $\pi\colon A' \to A$ be the map that sends a'_d to a_d. The previous paragraph gives the conclusion for f', and by applying π we can deduce the conclusion for f. □

LEMMA 10.6. *When $k > 0$ we have $v_k = -a_{p^k} \pmod{I^2 + (p)}$, where $I = \bigoplus_{k>0} L_k < L$ as usual.*

PROOF. We reuse the ideas in the proof of Proposition 6.3. It will be enough to show that if F is an FGL of the type considered there, over a ring $R = \mathbb{F}_p \oplus A$ in which $pA = 0$, then $v_k(F) = -a_{p^k}(F)$. If $F(x,y) = x + y + \sum_{d>1} a_d c_d(x,y)$ then $a_{p^k}(F)$ is just a_{p^k}. On the other hand, Lemma 10.5 tells us that $[p]_F(x) = px + \sum_{d>1} (p^d - p)/\nu(d)\ a_d x^d$. It is clear that $(p^d - p)/\nu(d) = 0 \pmod{p}$ unless d is a power of p, in which case $(p^d - p)/\nu(d) = p^{d-1} - 1 = -1 \pmod{p}$. Thus $[p]_F(x) = -\sum_{k>0} a_{p^k} x^{p^k}$ and $v_k(F) = -a_{p^k}$, as required. □

Proof of Proposition 10.4. Define

$$L' = \mathbb{F}_p[v'_i \mid i > 0] \otimes \mathbb{F}_p[a'_k \mid k \text{ is not a power of } p].$$

We can make this into a graded ring with v'_i in degree $p^i - 1$ and a'_k in dimension $k-1$. We can define a map $\phi\colon L' \to L/p$ of graded rings by $\phi(v'_i) = v_i$ and $\phi(a'_k) = a_k$. Let I' be the ideal in L' generated by the elements v'_i and a'_k, and let $\overline{I}$ be the image of I in L/p. It is easy to see from Lemma 10.6 that ϕ induces an isomorphism $I'/(I')^2 \simeq \overline{I}/\overline{I}^2$. It follows as in the proof of Theorem 7.2 that ϕ is surjective. On the other hand, L and L' are polynomial rings with generators in the same degrees, so we see that L'_k and L_k are vector spaces over $\mathbb{F}_p$ with the same finite dimension, and $\phi\colon L_k \to L'_k$ is surjective so it must be an isomorphism. □

Corollary 10.7. *For each $n > 1$, there is a formal group law over $\mathbb{F}_p$ of height n.*

Proof. Using the proposition, we can define a map $\alpha_n\colon L/p \to \mathbb{F}_p$ sending v_n to 1 and all other generators to 0. If F_n is the FGL that corresponds to α_n under the bijection $\mathrm{FGL}(\mathbb{F}_p) = \mathrm{Hom}(L, \mathbb{F}_p)$, then it is clear that F_n has height n. □

11. Formal groups in positive characteristic

Let $X = \mathrm{spec}(R)$ be an affine scheme over $\mathrm{spec}(\mathbb{F}_p)$. In this section, we attempt to classify formal groups over X up to isomorphism. We will succeed completely in the case where R is an algebraically closed field.

It is convenient to reformulate the problem slightly. We can let $\mathrm{RPS}(R)$ act on $\mathrm{FGL}(R)$ by $F^f(x,y) = f^{-1}F(f(x), f(y))$ (so that f is an isomorphism $F^f \to F$).

Exercise 11.1. The set of isomorphism classes of formal groups over $\mathrm{spec}(R)$ bijects naturally with $\mathrm{FGL}(R)/\mathrm{RPS}(R)$.

We first observe that the answer does not have as simple a form as one might hope for.

Proposition 11.2. *The functor $T(R) = \mathrm{FGL}(R)/\mathrm{RPS}(R)$ is not a scheme.*

Proof. Corollary 10.7 tells us that $T(\mathbb{F}_p)$ is infinite. As L is a polynomial ring, it is easy to see that the map $\mathrm{FGL}(\mathbb{Z}) \to \mathrm{FGL}(\mathbb{F}_p)$ is surjective, and thus the map $T(\mathbb{Z}) \to T(\mathbb{F}_p)$ is surjective, so $T(\mathbb{Z})$ is infinite. On the other hand, it follows from Proposition 3.1 that $T(\mathbb{Q})$ has only one element. Thus, the map $T(\mathbb{Z}) \to T(\mathbb{Q})$ cannot be injective. However, if X is a scheme then it is clear that the map $X(\mathbb{Z}) \to X(\mathbb{Q})$ is injective, because the map $\mathbb{Z} \to \mathbb{Q}$ is. □

Despite this, we can obtain some interesting results. We now start working towards this.

Definition 11.3. If $f, g \in R[\![x,y,z]\!]$ we write $f = g + O(k)$ if $f = g \pmod{(x,y,z)^k}$, and similarly for other sets of variables. A formal group law F is additive to order k if we have $F(x,y) = x + y + O(k+1)$.

Lemma 11.4. *Let F and F' be two FGLs over a ring R, and suppose that $F(x,y) = F'(x,y) + O(k)$ for some $k > 0$. Then there is a unique element $u \in R$ such that*

$$F'(x,y) = F(x,y) + uc_k(x,y) + O(k+1).$$

Proof. Clearly there is a unique homogeneous polynomial $f(x,y)$ of degree k such that $F'(x,y) = F(x,y) + f(x,y) + O(k+1)$, and by Proposition 6.9 it suffices to check that $f \in Z_k(R)$. As $F(x,y) = F(y,x)$ we have $f(x,y) = f(y,x)$. To check the cocycle condition, it suffices to work modulo $(x,y,z)^{k+1}$. To this accuracy, we have $xf(x,y) = yf(x,y) = 0$ and thus $F'(x,y) = x +_F y +_F f(x,y)$. It follows that

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

On the other hand, because $F'(y,z) = y + z \pmod{yz}$ and f is homogeneous of degree k we see that $f(x, F'(y,z)) = f(x, y+z)$ to our accuracy. It follows that

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

As F' is commutative and associative, the right hand side is invariant when we exchange x and z. We thus have

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

As f is symmetric, this gives the cocycle condition. □

Corollary 11.5. *If $F \in \mathrm{FGL}(R)$ is additive to order $k-1$ then there is a unique element $u \in R$ such that $F(x,y) = x + y + uc_k(x,y) + O(k+1)$.* □

Lemma 11.6. *If $F(x,y) = x+y+ac_k(x,y)+O(k+1)$ and $m \in \mathbb{Z}$ then $n = (m^k - m)/\nu(k)$ is an integer and $[m]_F(x) = mx + nax^k + O(k+1)$.*

Proof. This is essentially the same as Lemma 10.5. □

Corollary 11.7. *Let F be a formal group law over an $\mathbb{F}_p$-algebra R. If F is additive to order $p^r - 1$ and $r < \mathrm{height}(F)$ then F is additive to degree p^r.*

Proof. We know from Corollary 11.5 that there is some element $u \in R$ such that $F(x,y) = x + y + uc_{p^r}(x,y) + O(p^r+1)$. Lemma 11.6 tells us that $[p]_F(x) = -ux^{p^r} + O(p^r+1)$. On the other hand, if F has height n then $[p](x) = 0 + O(p^n)$. If $n > r$ we conclude that $u = 0$, so that F is additive to order p^r. □

Lemma 11.8. *If $f(x) = x + ax^k$ then $F^f(x,y) = F(x,y) - a\,b_k(x,y) + O(k+1)$, where $b_k(x,y) = (x+y)^k - x^k - y^k = \nu(k)c_k(x,y)$.*

Proof. Exercise. □

Lemma 11.9. *Suppose that $F(x,y) = x+y+ac_k(x,y)+O(k+1)$ and $f(x) = vx$ for some unit $v \in R^\times$. Then $F^f(x,y) = x + y + av^{k-1}c_k(x,y) + O(k+1)$.*

Proof. Exercise. □

Lemma 11.10. *Suppose that $F(x,y) = x+y+c_{p^n}(x,y)+O(p^n+1)$, and $k > n$ and $f(x) = x +_F vx^{p^{k-n}}$. Then*

$$F^f(x,y) = F(x,y) + (v^{p^n} - v)c_{p^k}(x,y) + O(p^k+1).$$

Proof. Let F be a formal group law over an $\mathbb{F}_p$-algebra R. We work everywhere modulo $(x,y)^{p^k+1}$. Note that to this accuracy, if $w \in (x,y)$ and $z \in (x,y)^{p^k}$ then $wz = 0$ so $w +_F z = w + z$; we shall repeatedly use this without explicit mention. We put $c = c_{p^k}(x,y) \in (x,y)^{p^k}$. The right hand side of the displayed equation can be rewritten as $x +_F y +_F v^{p^n} c -_F vc$. We thus need to check that

$$f(x) +_F f(y) = f(x +_F y +_F v^{p^n} c -_F vc),$$

or equivalently

$$x +_F y +_F vx^{p^{k-n}} +_F vy^{p^{k-n}} = x +_F y +_F v^{p^n} c -_F vc +_F v(x +_F y)^{p^{k-n}}.$$

Here we have used the fact that $k > n$, so applying the p^{k-n}'th power map kills the terms involving c. We now cancel the terms $x +_F y$ and use the approximation $F(X,Y) = X + Y + c_{p^n}(X,Y) \bmod (X,Y)^{p^n+1}$ and the fact that $c = c_{p^n}(x,y)^{p^{k-n}}$ (Lemma 6.11). We find that we need to check that

$$vx^{p^{k-n}} + vy^{p^{k-n}} + v^{p^n} c = v^{p^n} c -_F vc +_F v(x^{p^{k-n}} + y^{p^{k-n}} + c).$$

Finally, we observe that the formal sums can be rewritten as ordinary sums, and this makes the claim clear. □

Theorem 11.11. *Let F be a formal group law over an $\mathbb{F}_p$-algebra R. If F has finite height n, then F is isomorphic to a formal group law F' that is additive to order $p^n - 1$. If F has infinite height then F is isomorphic to the additive formal group law $F_a(x,y) = x + y$.*

Proof. We start with the finite height case. We will recursively define formal group laws F_k for $2 \leq k \leq p^n$ such that F_k is additive to order $k-1$. We start with $F_2 = F$, which clearly has the required form. Given F_k, we know from Corollary 11.5 that $F_k(x,y) = x + y + uc_k(x,y) + O(k+1)$ for some $u \in R$. If k is a power of p and $k < p^n$ then Corollary 11.7 tells us that $u = 0$. In that case, we put $F_{k+1} = F_k$ and $f_k(x) = x$. If k is not a power of p then $\nu(k)$ is a unit in $\mathbb{F}_p$. We define $f_k(x) = x + ux^k/\nu(k)$ and $F_{k+1} = F_k^{f_k}$. Lemma 11.8 tells us that F_{k+1} is additive to order k. At the end of this process we have a formal group law $F' = F_{p^n}$ of the required form, and isomorphisms $f_k \colon F_{k+1} \to F_k$ so $F' \simeq F_2 = F$.

In the case where F has infinite height, we can define F_k and f_k for all k, by the same procedure as that given above. We then define $g_k(x) = f_2(f_3(\dots f_k(x)))$, so that $g_k\colon F_{k+1} \to F_2 = F$, so that $F^{g_k} = F_{k+1}$. We have $f_k(x) = x + O(k)$ for all k, so $g_k = g_{k-1} + O(k)$, so there is a unique series $g(x) \in R[\![x]\!]$ such that $g(x) = g_{k-1}(x) + O(k)$ for all k. We thus have $F^g = F_k = x+y+O(k)$ for all k, so $F^g(x,y) = x+y = F_a(x,y)$. Thus g gives an isomorphism $F_a \simeq F$, as claimed. □

THEOREM 11.12. *Let K be an algebraically closed field of characteristic $p > 0$. Then any two formal group laws over K are isomorphic if and only if they have the same height.*

PROOF. Let F and F' be two formal group laws over K. If they both have infinite height then they are both isomorphic to the additive FGL and thus to each other (by Theorem 11.11). We may thus assume that they have the same finite height n. Using Theorem 11.11 again, we may replace F and F' by isomorphic formal group laws that are additive to order $p^n - 1$. We thus have $F(x,y) = x+y+uc_{p^n}(x,y) + O(p^n+1)$ for some $u \in K$. It follows that $[p]_F(x) = -ux^{p^n} + O(p^n+1)$ and we know that F has height n so $u \neq 0$. As K is algebraically closed, we can choose $v \in K$ such that $v^{p^n-1}u = 1$. Using Lemma 11.9, we can replace F by an isomorphic formal group law for which $u = 1$, or in other words $F(x,y) = x+y+c_{p^n}(x,y) \bmod (x,y)^{p^n+1}$. We may also replace F' by an isomorphic formal group law of the same type. We now define recursively a sequence of formal group laws F_k (for $k > p^n$) and isomorphisms $f_k\colon F_{k+1} \to F_k$ such that $F_k(x,y) = F'(x,y) + O(k)$. We start with $F_{p^n+1} = F$. Suppose we have defined F_k. We know from Lemma 11.4 that there is a unique element $u \in R$ such that $F'(x,y) = F_k(x,y) + uc_k(x,y) + O(k+1)$. If k is not a power of p then $\nu(k)$ is a unit in $\mathbb{F}_p$ so we can define $f_k(x) = x + ux^k/\nu(k)$ and $F_{k+1} = F_k^{f_k}$. It then follows from Lemma 11.8 that $F_{k+1}(x,y) = F'(x,y) + O(k+1)$ as required. On the other hand, suppose that $k = p^r$ for some $r > n$. As K is algebraically closed, there is an element $v \in K$ such that $v^{p^n} - v = u$. We can thus define $f_k(x) = x +_{F_k} vx^{p^{k-n}}$ and $F_{k+1} = F_k^{f_k}$. It follows from Lemma 11.10 that $F_{k+1}(x,y) = F'(x,y) + O(k+1)$.

Now define $g_{p^n}(x) = x$ and $g_{k+1}(x) = g_k(f_{k+1}(x))$ for all $k \geq p^n$. It is easy to see that the series $g_k(x)$ converges to a unique limit $g(x)$, in the sense that for any N we have $g(x) = g_k(x) + O(N)$ for $k \gg 0$. Moreover, we find that $F^g = F'$, so g is the required isomorphism from F' to F. □

12. Formal group laws of infinite height

Let $\mathrm{FGL}_{p,\infty}(R)$ be the set of formal group laws of infinite height over R. This is an affine scheme over $\mathrm{spec}(\mathbb{F}_p)$, and we see from Proposition 10.4 that the corresponding ring of functions is

$$L/I_\infty = L/(v_k \mid k \geq 0) = \mathbb{F}_p[a_k \mid k \text{ is not a power of } p].$$

This is a reasonably satisfactory picture, except that the generators a_k are not very explicit or easy to work with. In this section we give a different description of the scheme $\mathrm{FGL}_{p,\infty}$, due to Steve Mitchell.

DEFINITION 12.1. Write $C = \mathrm{RPS}_1 \times \mathrm{spec}(\mathbb{F}_p)$, which is a group scheme under composition over $\mathrm{spec}(\mathbb{F}_p)$. Let A be the subgroup scheme consisting of formal power series $f(x)$ such that $f(x) = x \pmod{x^2}$ and $f(x+y) = f(x) + f(y)$. Using Lemma 6.6, we see that this is just the group of series of the form $f(x) = x + \sum_{k>0} a_k x^{p^k}$. We write $A(R) \setminus C(R)$ for the set of right cosets of $A(R)$ in $C(R)$.

Let $Y \subset C$ be the scheme of series of the form $\sum_{k>0} b_k x^k$ such that $b_{p^k} = 0$ for all $k > 0$. Given a series $f \in C$ we define $\phi(f)(x,y) = f^{-1}(f(x) + f(y))$. This is a formal group law, and f gives an isomorphism from $\phi(f)$ to the formal group law $F_a(x,y) = x + y$, so $\phi(f)$ has infinite height.

THEOREM 12.2. *The map $(f,g) \mapsto f \circ g$ gives an isomorphism $A \times Y \to C$. The inclusion $Y \to C$ and the map $\phi\colon C \to \mathrm{FGL}_{p,\infty}$ induce isomorphisms $Y(R) \to A(R) \setminus C(R) \to \mathrm{FGL}_{p,\infty}(R)$. Thus, the functor $A \setminus C\colon R \mapsto A(R) \setminus C(R)$ is a scheme, and we have isomorphisms $Y \to A \setminus C \to \mathrm{FGL}_{p,\infty}$.*

PROOF. We may assume that R is an $\mathbb{F}_p$-algebra (otherwise the theorem merely claims a bijection between empty sets). We know from Theorem 11.11 that if $F \in \mathrm{FGL}_{p,\infty}(R)$ then there exists an isomorphism $f\colon F \to F_a$. If $f'(0) = u \in R^\times$ then we can compose with the automorphism x/u of F_a and thus assume that $f'(0) = 1$, so that $f \in C(R)$. By assumption we have $f(F(x,y)) = f(x) + f(y)$, so $F = \phi(f)$. This shows that $\phi\colon C(R) \to \mathrm{FGL}_{p,\infty}(R)$ is surjective. It is easy to see that if $g \in A(R)$ then $\phi(g \circ f) = \phi(f)$, so we get an induced map $A(R) \setminus C(R) \to \mathrm{FGL}_{p,\infty}(R)$, which is again surjective. If $\phi(f) = \phi(g) = F$ then f and g give maps $F \to F_a$ so $h(x) = g(f^{-1}(x))$ defines a map $F_a \to F_a$, in other words an element of $A(R)$.

As $g = h \circ f$ we see that f and g give the same element of $A(R) \setminus C(R)$, so our map $\phi\colon A \setminus C \to \mathrm{FGL}_{p,\infty}$ is an isomorphism.

We now define a map $\tau\colon C \to A$ by $\tau(\sum_{k>0} b_k x^k) = \sum_{k\geq 0} b_{p^k} x^{p^k}$. Note that $\tau(g)(x) = x$ if and only if $g \in Y$. If $f(x) = \sum_j a_j x^{p^j} \in A(R)$ and $g(x) = \sum_{k>0} b_k x^k \in C(R)$ then we have $f(g(x)) = \sum_{j,k} a_j b_k^{p^j} x^{kp^j}$ so

$$\tau(f \circ g) = \sum_{i,j} a_j b_{p^i}^{p^j} x^{p^{i+j}} = f \circ \tau(g).$$

Now define $\sigma(h) = \tau(h)^{-1} \circ h$, so that $h = \tau(h) \circ \sigma(h)$. By applying the above with $f = \tau(h)^{-1}$ and $g = h$, we see that $\tau(\sigma(h))(x) = \tau(h)^{-1}(\tau(h)(x)) = x$, so $\sigma(h) \in Y$. We thus have a map $(\tau, \sigma)\colon C \to A \times Y$, which is easily seen to be inverse to the map $(f, g) \mapsto f \circ g$. □

Remark 12.3. In topology, the group scheme A is naturally identified with $\mathrm{spec}(P_*)$, where P_* is the polynomial part of the dual Steenrod algebra. If X is a space then the Steenrod algebra acts on $H^*(X; \mathbb{F}_p)$. If X is a finite CW complex and $H^*(X; \mathbb{F}_p)$ is concentrated in even degrees then this gives rise to an action of the group scheme A on the scheme $X_H = \mathrm{spec}(H^*(X; \mathbb{F}_p))$. In the case $p = 2$, a similar construction gives an action of A on $\mathrm{spec}(H_*(MO; \mathbb{F}_2))$, where MO is the spectrum representing unoriented bordism. This scheme can be identified with our scheme C, in a manner compatible with the action of A. Our A-equivariant isomorphism $C \simeq A \times Y$ implies that the Adams spectral sequence for $\pi_*(MO)$ collapses and thus that $\mathrm{spec}(\pi_*(MO)) = Y = \mathrm{FGL}_{2,\infty}$. This tells us the structure of the ring $\pi_*(MO)$. On the other hand, a theorem of René Thom tells us that $\pi_*(MO)$ is the ring of cobordism classes of compact closed manifolds. (Two manifolds M and N are said to be cobordant if $M \amalg N$ is the boundary of some manifold W; addition is defined by disjoint union and multiplication by Cartesian product; this gives an algebra over $\mathbb{F}_2$ because $\partial(M \times I) = M \amalg M$.) Thus, the procedure outlined above contributes to a rather striking theorem in topology. If MU is the complex bordism spectrum then $\mathrm{spec}(\pi_*(MU)) = \mathrm{FGL}$ and $\mathrm{spec}(H_*(MU; \mathbb{F}_p)) = C$ and if R denotes the image of the Hurewicz map $\pi_*(MU) \to H_*(MU; \mathbb{F}_p)$ then $\mathrm{spec}(R) = \mathrm{FGL}_{p,\infty}$.

13. The p-adic integers

In this section we define and study the ring $\mathbb{Z}_p$ of p-adic integers, and various extensions of $\mathbb{Z}_p$. These rings will be useful for several different reasons. In Section 14 we will develop the method of Lubin and Tate for studying formal group laws over $\mathbb{Z}_p$. This will in turn give formal group laws over $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. In Section 16 we will study the endomophism rings of certain formal groups, and we will find that they contain $\mathbb{Z}_p$.

Definition 13.1. Let $\rho_k\colon \mathbb{Z}/p^k \to \mathbb{Z}/p^{k-1}$ be the evident projection map. Let $\mathbb{Z}_p$ be the set of sequences $a \in \prod_{k>0} \mathbb{Z}/p^k$ such that $\rho_k(a_k) = a_{k-1}$ for all $k > 1$. This is a ring under the obvious pointwise operations.

Definition 13.2. Let a be an integer. If $a = 0$ then we define $v_p(a) = \infty$, otherwise there is a largest number $k \geq 0$ such that p^k divides a and we define $v_p(a) = k$. Similarly, if $a \in \mathbb{Z}_p$ we let $v_p(a)$ be the largest k such that $a_k = 0 \in \mathbb{Z}/p^k$, or $v_p(a) = \infty$ if $a = 0$. These definitions are clearly compatible if we think of $\mathbb{Z}$ as a subring of $\mathbb{Z}_p$. We also define $|a|_p = p^{-v_p(a)}$, and $d_p(a, b) = |a - b|_p$. One can check that this gives a metric on $\mathbb{Z}_p$ and thus on $\mathbb{Z} \subset \mathbb{Z}_p$.

Theorem 13.3. *The topology on $\mathbb{Z}_p$ induced by our metric $d(a, b) = |a-b|_p$ is the same as its topology as a subspace of the product of the discrete spaces $\mathbb{Z}/p^k$. It is a compact Hausdorff space, and can be identified with the completion of $\mathbb{Z}$ with respect to d. Every element $a \in \mathbb{Z}_p$ has a unique expression as a convergent infinite sum $a = \sum_{k\geq 0} b_k p^k$ with $b_k \in \{0, 1, \dots, p-1\}$.*

Proof. Let a be an element of $\mathbb{Z}_p$, and suppose that $\epsilon > 0$, so $p^{-k} < \epsilon$ for some k. As $\mathbb{Z}/p^k$ is discrete, the set $\{a_k\}$ is open in $\mathbb{Z}/p^k$ so $U = \{b \in \mathbb{Z}_p \mid b_k = a_k\}$ is open in the product topology. If $b \in U$ then one sees from the definition of $\mathbb{Z}_p$ that $b_j = a_j$ for $j \leq k$ so $v_p(b - a) \geq k$ so $|b - a|_p < \epsilon$. Thus, U is contained in the ball of radius ϵ round a, and it follows that every open set in the metric topology is open in the product topology. On the other hand, the basic neighbourhoods of A in the product topology are of the form $V = \mathbb{Z}_p \cap \prod_k V_k$, where $a_k \in V_k \subset \mathbb{Z}/p^k$ and $V_k = \mathbb{Z}/p^k$ for all but finitely many k. If $V_k = \mathbb{Z}/p^k$

for all $k \geq m$ then one checks easily that the ball of radius p^{-m} round a is contained in V. It follows easily that the metric topology is the same as the product topology.

Now let $(a_1, a_2, \ldots)$ be a Cauchy sequence in $\mathbb{Z}_p$. Then for any k there exists m such that $|a_i - a_j|_p < p^{-k}$ for $i, j \geq m$. This means that $a_{i,k} = a_{m,k}$ for all $i \geq m$. If we define $b_k = a_{m,k}$ then one can check that $b \in \mathbb{Z}_p$ and the sequence converges to b. Thus, $\mathbb{Z}_p$ is complete under the metric. It is clear that any point $a \in \mathbb{Z}_p$ has distance at most p^{-k} from some integer $b \in \{0, \ldots, p^k - 1\}$. It follows both that $\mathbb{Z}_p$ is totally bounded, and that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. Any complete, totally bounded metric space is compact Hausdorff, and is the completion of any dense subspace. This shows that $\mathbb{Z}_p$ is a compact Hausdorff space, and is the completion of $\mathbb{Z}$.

Now let a be an element of $\mathbb{Z}_p$. One can easily prove by induction that there is a unique sequence of elements $b_k \in \{0, \ldots, p-1\}$ for $k \geq 0$ such that $a_k = \sum_{j<k} b_j p^j \in \mathbb{Z}/p^k$, and it follows that $a = \sum_j b_j p^j \in \mathbb{Z}_p$. □

COROLLARY 13.4. *For any $k \geq 0$ we have $\mathbb{Z}_p/p^k\mathbb{Z}_p = \mathbb{Z}/p^k$.*

PROOF. Define $\rho\colon \mathbb{Z}_p \to \mathbb{Z}/p^k$ by $\rho(a) = a_k$. The restriction of ρ to $\mathbb{Z} \subset \mathbb{Z}_p$ is clearly surjective, so ρ is surjective. If we write $a = \sum_j b_j p^j$ as in the theorem then $\rho(a) = \sum_{j=0}^{k-1} b_j p^j$. If $\rho(a) = 0$ it is easy to see that $b_0 = \ldots = b_{k-1} = 0$. As $\mathbb{Z}_p$ is complete, the series $\sum_{j \geq k} b_j p^{k-j}$ converges to an element $c \in \mathbb{Z}_p$ and $a = p^k c \in p^k \mathbb{Z}_p$. Thus, ρ induces the claimed isomorphism. □

PROPOSITION 13.5. *An element $a \in \mathbb{Z}_p$ is invertible if and only if $a \neq 0 \pmod p$.*

PROOF. The corollary above shows that p is not invertible, so if $a = 0 \pmod p$ then a is not invertible. Next, suppose that $a = 1 \pmod p$, say $a = 1 - pb$ for some $b \in \mathbb{Z}_p$. The series $\sum_{k \geq 0} p^k b^k$ then converges to an inverse for a. Finally, suppose merely that $a \neq 0 \pmod p$, so a has nontrivial image in $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p$. As $\mathbb{Z}/p$ is a field, there is an integer b such that $ab = 1 \pmod p$, so ab is a unit in $\mathbb{Z}_p$, so a must also be a unit. □

COROLLARY 13.6. *Every nonzero element of $\mathbb{Z}_p$ is a unit multiple of p^k for some $k \geq 0$; so $\mathbb{Z}_p$ is a principal ideal domain, with $p\mathbb{Z}_p$ as the only maximal ideal.* □

DEFINITION 13.7. Let A be an abelian group. We say that A is a *p-torsion group* if for each $a \in A$ there exists $k \geq 0$ with $p^k a = 0$.

Note that k is allowed to vary with a, so $\bigoplus_j \mathbb{Z}/p^j$ counts as a p-torsion group, for example.

PROPOSITION 13.8. *Let A be a p-torsion group. Then A has a natural structure as a module over $\mathbb{Z}_p$.*

PROOF. Let n be an element of $\mathbb{Z}_p$, corresponding to a sequence of elements $n_i \in \mathbb{Z}/p^i$. We use the same notation n_i for the unique representative lying in $\{0, 1, \ldots, p^i - 1\}$. Given $a \in A$ we choose k with $p^k a = 0$, and then define $na = n_k a$. It is clear that this does not depend on the choice of k. Given $a, b \in A$ we can choose k large enough that $p^k a = p^k b = 0$ and then $n(a+b) = n_k(a+b) = n_k a + n_k b = na + nb$. All the other module axioms can be checked by similar arguments. □

PROPOSITION 13.9. *Let F be a formal group law over a ring k, and fix $i, j \geq 0$. Then for sufficiently large m be have*

$$[p^m]_F(x) = 0 \pmod{p^i, x^j}.$$

PROOF. We can replace k by k/p^i and so assume that $p^i = 0$ in k. This means that $[p^i]_F(x) \in k[\![x]\!].x^2$. In general, if $f(x) \in k[\![x]\!].x^r$ and $g(x) \in k[\![x]\!].x^s$ then $f(g(x)) \in k[\![x]\!].x^{rs}$. It follows that $[p^{in}]_F(x)$ is divisible by x^{2^n}, and so is divisible by x^j for large n. □

PROPOSITION 13.10. *Let G be a formal group over a scheme $S = \operatorname{spec}(k)$, and suppose that $p^i = 0$ in k. Recall that G gives a functor G' from k-algebras to abelian groups, as in Section 5. Then $G'(R)$ is always a p-torsion group, and thus a $\mathbb{Z}_p$-module.*

PROOF. Choose a coordinate on G. This allows us to identify $G(R)$ with $\operatorname{Nil}(R)$, with the group structure given by a formal group law F over k. The claim now follows easily from Proposition 13.9. □

DEFINITION 13.11. Let F be a formal group law over a ring k in which $p^i = 0$. Fix $n \in \mathbb{Z}_p$. Proposition 13.10 tells us that multiplication by n gives a well-defined endomorphism of the groups $(\mathrm{Nil}(R), F)$, and Proposition 5.10 tells us that this corresponds to a formal power series over k. We write $[n]_F(x)$ for this power series.

Similarly, if F is a formal group law over $\mathbb{Z}_p$ then the previous paragraph gives compatible power series $[n]_F(x) \in [\![(\mathbb{Z}/p^i)]\!]x$ for all i, and these fit together to give $[n]_F(x) \in \mathbb{Z}_p[\![x]\!]$.

REMARK 13.12. More concretely, we can calculate $[n]_F(x)$ modulo (p^i, x^j) as follows: we find m such that $[p^m]_F(x) \in (p^i, x^j)$, then we find $n_0 \in \mathbb{N}$ such that $n = n_0 \pmod{p^m}$, then we define $[n_0]_F(x)$ to be the formal sum of n_0 copies of x in the usual way, and we find that $[n]_F(x)$ is the same as $[n_0](x)$ modulo (p^i, x^j).

REMARK 13.13. Using the correspondence between power series and natural transformations, it is easy to check that

(a) $[n]_F(x)$ is as in Definition 1.1 whenever $n \in \mathbb{Z} \subset \mathbb{Z}_p$.
(b) $[n]_F(F(x, y)) = F([n]_F(x), [n]_F(y))$, so $[n]_F$ is an endomorphism of F.
(c) $[nm]_F(x) = [n]_F([m]_F(x))$ and $[n + m]_F(x) = F([n]_F(x), [m]_F(x))$.

We next want to understand various finite extensions of $\mathbb{Z}_p$.

DEFINITION 13.14. We say that a ring R is *reduced* if the only nilpotent element is zero. We let $\overline{\mathcal{W}}$ be the category of finite, reduced $\mathbb{F}_p$-algebras. We also let $\mathcal{W}$ be the category of $\mathbb{Z}_p$-algebras R such that

(a) R is finitely generated and free as a $\mathbb{Z}_p$-module;
(b) R/pR is reduced.

THEOREM 13.15. *The functor $R \mapsto R/pR$ gives an equivalence $\mathcal{W} \to \overline{\mathcal{W}}$.*

The proof will be given after a number of preliminary results. First, however, we explain the structure of $\overline{\mathcal{W}}$:

PROPOSITION 13.16. *Let R be a finite $\mathbb{F}_p$-algebra, and let $\phi\colon R \to R$ be the Frobenius map, defined by $\phi(a) = a^p$. Then the following are equivalent:*

(a) *R is reduced*
(b) *R is a finite product of fields*
(c) *$\phi^m = 1$ for some $m > 0$.*

PROOF. First suppose that R is reduced. If $R = R_0 \times R_1$ with $R_0, R_1 \neq 0$ then we can argue by induction on $|R|$ that R is a product of fields. So suppose that R cannot be split in this way, or in other words that the only idempotent elements of R are 0 and 1. Let a be an arbitrary element of R. As R is finite, the powers of a cannot all be distinct, so we can choose i, j with $j > 0$ and $a^i = a^{i+j}$, so $a^i(1-a^j) = 0$. From this it follows that $a^i(1 - a^{ij}) = 0$ and then that $a^{ij}(1 - a^{ij}) = 0$ so the element a^{ij} is idempotent. If $a^{ij} = 0$ then (as R is reduced) we have $a = 0$. If $a^{ij} = 1$ then a is invertible. It follows that R is a field. This shows that (a) implies (b).

If R is a field of dimension m over $\mathbb{F}_p$, it is standard that $\phi^m = 1$ on R. If $\phi^{m_i} = 1$ on R_i for $i = 0, 1$, then we find that $\phi^{m_0 m_1} = 1$ on $R_0 \times R_1$. From this it follows easily that (b) implies (c).

Finally, suppose that $\phi^m = 1$ in R, so $\phi^{mn} = 1$ for all n. If $a \in R$ is nilpotent then $\phi^{mn}(a) = 0$ for n sufficiently large, so $a = 0$. This shows that (c) implies (a). □

COROLLARY 13.17. *If we put $U_m = \mathbb{Z}_p[t]/(t^{p^m} - t)$ then U_m/p is reduced, and is a finite product of fields.*

PROOF. The map $\phi^m\colon U_m/p \to U_m/p$ is a ring homomorphism that acts as the identity on the generator u, so it acts as the identity on the whole ring. □

DEFINITION 13.18. For $R \in \mathcal{W}$ we define $\phi_0\colon R \to R$ by $\phi_0(a) = a^p$ (so ϕ_0 preserves multiplication but not addition). We put

$$T(R) = \{a \in R \mid \phi_0^m(a) = a \text{ for some } m > 0\}.$$

PROPOSITION 13.19. *We have $0, 1 \in T(R)$, and $T(R)$ is closed under multiplication, and $T(R_0 \times R_1) = T(R_0) \times T(R_1)$.*

PROOF. It is clear that $0, 1 \in T(R)$. If $\phi_0^m(a) = a$ and $\phi_0^n(b) = b$ then $\phi_0^{mn}(ab) = ab$, so $T(R)$ is closed under multiplication. If $a_i \in R_i$ with $\phi_0^{m_i}(a_i) = a_i$ then $\phi_0^{m_0 m_1}(a_0, a_1) = (a_0, a_1)$, so $T(R_0 \times R_1) = T(R_0) \times T(R_1)$. □

PROPOSITION 13.20. *Let R be a ring in $\mathcal{W}$. Then*

(a) *The reduction map $\pi\colon R \to R/pR$ gives a bijection $T(R) \to R/pR$.*
(We will write τ for the inverse map $R/p \to T(R)$.)
(b) *Every element $a \in R$ can be expressed uniquely as $\sum_{i \geq 0} \tau(a_i)p^i$ with $a_i \in R/p$.*
(c) *If $B \subseteq R/p$ is a basis for R/p over $\mathbb{F}_p$, then $\tau(B)$ is a basis for R over $\mathbb{Z}_p$.*

PROOF. (a) By Proposition 13.16, there exists m such that $\phi^m = 1$ on R/pR. Thus, for $a \in R$ we have $\phi_0^m(a) = a \pmod p$. Define $a_i = \phi_0^{mi}(a)$. Using Lemma 6.10 we can show by induction that $a_{i+1} = a_i \pmod{p^{1+mi}}$. Also, as R is a finitely generated free module over $\mathbb{Z}_p$, we see that R is the inverse limit of the quotients R/p^tR. It follows that there is a unique element $a_\infty \in R$ with $a_\infty = a_i \pmod{p^{1+mi}}$ for all i. By uniqueness, we see that $\phi_0^m(a_\infty) = a_\infty$, so $a_\infty \in T(R)$. By construction we have $a_\infty = a \pmod p$, and it follows from this that the map $\pi\colon T(R) \to R/p$ is surjective.

Now suppose we have $a, b \in T(R)$ with $\pi(a) = \pi(b)$. We can choose $n > 0$ such that $\phi_0^n(a) = a$ and $\phi_0^n(b) = b$. As $\pi(a) = \pi(b)$ we see that $a = b \pmod p$. It follows by Lemma 6.10 that $\phi_0^{nj}(a) = \phi_0^{nj}(b) \pmod{p^{1+nj}}$, so $a = b \pmod{p^{1+nj}}$. As j was arbitrary, this gives $a = b$. Thus, we see that π is also injective.

(b) Given $a \in R$ we put $b_0 = a$ and $a_0 = \pi(b_0) \in R/p$. Then $\pi(b_0 - \tau(a_0)) = 0$, so $b_0 - \tau(a_0) = pb_1$ for some b_1. Similarly, we put $a_i = \pi(b_i)$ and $b_{i+1} = (b_i - \tau(a_i))/p$ for all i, so $a = p^i b_i + \sum_{j<i} \tau(a_j)p^j$. In the limit we get $a = \sum_{i \geq 0} \tau(a_i)p^i$.

(c) First, we have assumed that R is a free module over $\mathbb{Z}_p$ of finite rank, so we can choose a basis $u_1, \dots, u_n$. For any other list of elements $v_1, \dots, v_n$, we can write $v_i = \sum_j m_{ij}u_j$ for some matrix $m \in M_n(\mathbb{Z}_p)$, and v is a basis iff $\det(m) \in \mathbb{Z}_p^\times$. However, an element of $\mathbb{Z}_p$ is invertible iff its image in $\mathbb{F}_p$ is invertible, so we see that v is a basis for R over $\mathbb{Z}_p$ iff $\pi(v)$ is a basis for R/p over $\mathbb{F}_p$. The claim is clear from this.

□

COROLLARY 13.21. *If we put*

$$E(R) = \{e \in R \mid e^2 = e\} = \{ \textit{ idempotents in } R\}$$

then π gives a bijection $E(R) \to E(R/p)$.

PROOF. It is clear that $\pi(E(R)) \subseteq E(R/p)$. It is also clear that $E(R) \subseteq T(R)$ and $\pi\colon T(R) \to R/p$ is injective so $\pi\colon E(R) \to E(R/p)$ is injective. Finally, if $\overline{e} \in E(R/p)$, then there is a unique $e \in T(R)$ with $\pi(e) = \overline{e}$. We then have $e^2 \in T(R)$ with $\pi(e^2) = \overline{e}^2 = \overline{e}$, so $e^2 = e$, so $e \in E(R)$. This proves that we have a bijection. □

COROLLARY 13.22. *Suppose that $R \in \mathcal{W}$. Then the following are equivalent:*

(a) *$E(R) = \{0, 1\}$ (with $0 \neq 1$)*
(b) *$E(R/p) = \{0, 1\}$ (with $0 \neq 1$)*
(c) *R/p is a field.*
(d) *R is an integral domain.*

PROOF. It is clear from Corollary 13.21 that (a) and (b) are equivalent. We know that S/p is a finite product of fields, so (b) and (c) are equivalent. As every idempotent $e \in E(R)$ satisfies $e(1 - e) = 0$, we see that (d) implies (a).

We next show that that (c) implies (d). Suppose that R/p is a field, and consider nonzero elements $a, b \in R$. We then have $a = p^i a_0$ and $b = p^j b_0$ for some $i, j \geq 0$ and $a_0, b_0 \in R$ with $\pi(a_0), \pi(b_0) \neq 0$ in R/p. As R/p is a field it follows that $\pi(a_0 b_0) \neq 0$ and so $a_0 b_0 \neq 0$. As R is a free module over $\mathbb{Z}_p$ it follows that the element $ab = p^{ij} a_0 b_0$ is also nonzero, as required. □

PROPOSITION 13.23. *If F is any field of order p^d, then there is an idempotent $e \in E(U_d)$ such that the ring $R = U_d/e \in \mathcal{W}$ has $R/p \simeq F$. Moreover, if S is any other ring in $\mathcal{W}$ with $S/p \simeq F$, then $S \simeq R$.*

PROOF. It is well known that $F^\times$ is cyclic of order $p^d - 1$; let u be a generator, and let $\alpha\colon U_d \to F$ be the map that sends t to u. Let $\phi(t)$ be the minimal polynomial of u, so $t^{p^d} - t = \phi(t)\psi(t)$ for some $\psi(t)$. By differentiating this relation, we get $\phi'(t)\psi(t) + \phi(t)\psi'(t) = -1$. From this it follows that the element $\overline{e} = -\phi(t)\psi(t)$ gives an idempotent in the ring $U_d/p = \mathbb{F}_p[t]/(t^{p^d} - t)$. By Corollary 13.21, there is a unique idempotent lifting $e \in E(U_d)$. If we put $R = U_d/e$, we find that $R \in \mathcal{W}$ and that α induces an isomorphism $R/p \to F$.

Now suppose we have another ring $S \in \mathcal{W}$, and an isomorphism $\beta\colon S/p \to F$. Let $v \in T(S)$ be the element with $\pi(v) = \beta^{-1}(u)$. Then $v^{p^d} \in T(S)$ with $\pi(v^{p^d}) = \pi(v)$, so $v^{p^d} = v$, so there is a unique homomorphism $\gamma\colon U_d \to S$ with $\gamma(t) = v$. The diagram

$$\begin{array}{ccc} U_d & \xrightarrow{\gamma} & S \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\pi} \\ F & \xleftarrow[\beta]{\simeq} & S/p \end{array}$$

commutes when evaluated on $t \in U_d$, but t is a generator, so it commutes on all elements. It follows that $\pi\gamma(e) = 0$, but $\pi\colon E(S) \to E(S/p)$ is bijective, so $\gamma(e) = 0$, so we have an induced map $\overline{\gamma}\colon R = U_d/e \to S$. Using the above diagram we see that the induced map $R/p \to S/p$ is an isomorphism, and both R and S are finitely generated free modules over $\mathbb{Z}_p$, so it follows that γ is an isomorphism. □

PROOF OF THEOREM 13.15. First, Proposition 13.23 shows that the essential image of ρ contains all fields in $\overline{\mathcal{W}}$. It is also clear that the essential image is closed under products, so ρ is essentially surjective.

Next, suppose we have two morphisms $f, g \in \mathcal{W}(R, S)$ with $\rho(f) = \rho(g)\colon R/pR \to S/pS$. We have a natural bijection $T(R) \to R/p$, so we see that $f = g$ on $T(R)$. However, $T(R)$ generates R as a $\mathbb{Z}_p$-module, so $f = g$. This proves that ρ is faithful.

We now want to prove that ρ is full, or in other words that the map

$$\rho_{RS}\colon \mathcal{W}(R, S) \to \overline{\mathcal{W}}(R/p, S/p)$$

is surjective. If we know that this holds for S_0 and S_1, then it also holds for $S_0 \times S_1$. We can thus reduce to the case where S does not split as a nontrivial product, or equivalently $E(S) = \{0, 1\}$. Corollary 13.21 then tells us that S/p must be a field, and S is an integral domain. Now fix S with this property, and let $\mathcal{V}$ be the class of rings $R \in \mathcal{W}$ such that ρ_{RS} is a bijection. As S is an integral domain, it is not hard to identify $\mathcal{W}(R_0 \times R_1, S)$ with $\mathcal{W}(R_0, S) \amalg \mathcal{W}(R_1, S)$, and $\overline{\mathcal{W}}(R/p, S/p)$ with $\overline{\mathcal{W}}(R_0/p, S/p) \amalg \overline{\mathcal{W}}(R_1/p, S/p)$. It follows that $R_0 \times R_1 \in \mathcal{V}$ iff R_0 and R_1 both lie in $\mathcal{V}$. Using this in one direction, we reduce to the case where R/p is also a field. Using the opposite direction in combination with Proposition 13.23, we reduce to the case where $R = U_d$ for some d. In this case we can identify $\mathcal{W}(R, S)$ with $\{b \in S \mid b^{p^d} = b\}$, and it follows from Proposition 13.20 that ρ_{RS} is a bijection, as required. □

COROLLARY 13.24. *For $R \in \mathcal{W}$, there is a ring homomorphism $\phi\colon R \to R$ given by*

$$\phi(\sum_i \tau(a_i)p^i) = \sum_i \tau(a_i^p)p^i.$$

(We call this the lifted Frobenius map*.)*

PROOF. We temporarily write ϕ_1 for the Frobenius map $a \mapsto a^p$ on R/p. By the proposition, there is a unique ring homomorphism $\phi\colon R \to R$ with $\rho(\phi) = \phi_1$. As τ gives a natural bijection $R/p \to T(R)$, we see that $\phi(\tau(a)) = \tau(\phi_1(a)) = \tau(a^p)$. As ϕ is a ring homomorphism it must also satisfy $\phi(p) = p$, and so must be continuous with respect to the p-adic topology. It therefore preserves the relevant infinite sums, and we find that

$$\phi(\sum_i \tau(a_i)p^i) = \sum_i \tau(a_i^p)p^i.$$

□

REMARK 13.25. In Section 22 we will develop the theory of Witt vectors, which is useful for a number of reasons. One application is that it gives a more explicit functor $\overline{\mathcal{W}} \to \mathcal{W}$ that is inverse to ρ. However, this turns out to be less useful than one might imagine. Instead, we can proceed as follows. Given a finite field F, we can choose a generator $u \in F$, and let $f(t) \in \mathbb{F}_p[t]$ be the minimal polynomial, so $F \simeq \mathbb{F}_p[u]/f(u)$. We can then choose a monic polynomial $\widetilde{f}(t) \in \mathbb{Z}_p[t]$ lifting $f(t)$, and put $R = \mathbb{Z}_p[u]/f(u)$; then $R \in \mathcal{W}$ with $\rho(R) \simeq F$.

14. Lubin-Tate theory

Fix a prime p and an integer $n > 0$. Let R be a $\mathbb{Z}_p$-algebra such that

(a) R is finitely generated and free as a $\mathbb{Z}_p$-module;
(b) R/p is a field of order p^m for some m dividing n, so that $a^{p^n} = a$ for all $a \in R/p$.

(This means that R lies in the category $\mathcal{W}$ from Definition 13.14.)

Our results will already be interesting for $R = \mathbb{Z}_p$, and the reader may wish to focus on that case. However, the more general case is important in number theory (specifically, the local class field theory of finite field extensions with abelian Galois group).

Let $\mathcal{F}$ be the set of formal power series $f(x) \in R[\![x]\!]$ such that

(a) $f(x) = px \pmod{x^2}$
(b) $f(x) = x^{p^n} \pmod{p}$.

For each such f, we will define a formal group law F_f over R. It will turn out that given another series $g \in \mathcal{F}$, there is a canonical isomorphism $u_{f,g} \colon F_f \to F_g$, and we can use these to define a formal group that is independent of any choices.

All our arguments will rest on the following lemma:

LEMMA 14.1. *Suppose that $f, g \in \mathcal{F}$ and that λ_1 is a linear form in k variables over R, say*

$$\lambda_1(x_1, \dots, x_k) = \sum_i \alpha_i x_i$$

with $\alpha_i \in R$ for all i. Then there is a unique power series $\lambda \in R[\![x_1, \dots, x_k]\!]$ such that

$$\lambda = \lambda_1 \bmod (x_1, \dots, x_k)^2$$

and

$$\lambda(f(x_1), \dots, f(x_k)) = g(\lambda(x_1, \dots, x_k)).$$

PROOF. Write $I = (x_1, \dots, x_k) < R[\![x_1, \dots, x_k]\!]$, and write $\lambda \circ f^k$ for the series $\lambda(f(x_1), \dots, f(x_k))$ and so on. We will construct recursively polynomials λ_m of degree at most m such that

$$\lambda_m \circ f^k = g \circ \lambda_m + O(m+1).$$

We are given λ_1, which has the required property because $f(x) = px = g(x) + O(2)$. Suppose we have constructed λ_{m-1}. We next claim that

$$\lambda_{m-1} \circ f^k = g \circ \lambda_{m-1} \pmod{p}.$$

To see this, we work mod p until further notice. We thus have $g(x) = x^{p^n}$ and thus $g(x+y) = g(x) + g(y)$ and $g(xy) = g(x)g(y)$ and $g(a) = a$ for all $a \in R/p$. Because of this, applying g to the power series $\lambda_{m-1}(x_1, \dots, x_k)$ is just the same as raising the variables x_i to the p^n'th power, or equivalently applying f to them. This gives the congruence as claimed. Working integrally again and discarding terms of total degree greater than m, we see that there is a unique homogeneous polynomial ψ_m of degree m such that

$$\lambda_{m-1} \circ f^k = g \circ \lambda_{m-1} + p\psi_m + O(m+1).$$

Define $\psi'_m = \psi_m/(1 - p^{m-1})$ (noting that $1 - p^{m-1}$ is a unit in $\mathbb{Z}_p$) and $\lambda_m = \lambda_{m-1} + \psi'_m$. Because $g(x) = px + O(2)$ we have

$$g \circ \lambda_m = g \circ \lambda_{m-1} + p\psi'_m + O(m+1).$$

On the other hand, we have $f(x) = px + O(2)$ and ψ'_m is homogeneous of degree m so

$$\psi'_m \circ f^k = \psi'_m(px_1, \dots, px_k) = p^m \psi'_m + O(m+1).$$

Thus, working modulo I^{m+1}, we have

$$\begin{aligned}\lambda_m \circ f^k &= \lambda_{m-1} \circ f^k + p^m \psi'_m \\ &= g \circ \lambda_{m-1} + (p - p^m)\psi'_m + p^m \psi'_m \\ &= g \circ \lambda_m\end{aligned}$$

as required. It follows that there is a unique power series λ such that $\lambda = \lambda_m + O(m+1)$ for all m. This series satisfies $\lambda \circ f^k = g \circ \lambda + O(m)$ for all m, so $\lambda \circ f^k = g \circ \lambda$. One can check by induction that λ is unique modulo I^m for all m, and thus is unique. □

PROPOSITION 14.2. *If $f \in \mathcal{F}$ then there is a unique formal group law $F_f(x, y)$ over R such that $f \circ F_f = F_f \circ f^2$, and moreover we have $[p]_{F_f}(x) = f(x)$.*

PROOF. We start by applying Lemma 14.1 with $g = f$ and $\lambda_1(x, y) = x + y$. This gives a unique series $F_f = \lambda$ with $F_f \circ f^2 = f \circ F_f$ and $F_f(x, y) = x + y \bmod (x, y)^2$. We claim that this is a formal group law. Indeed, the series $F_f(y, x)$ has the defining property of $F_f(x, y)$ so $F_f(x, y) = F_f(y, x)$. Similarly, the series $F_f(F_f(x, y), z)$ and $F_f(x, F_f(y, z))$ are both equal to $x + y + z \bmod (x, y, z)^2$ and they both commute with f so the uniqueness clause in Lemma 14.1 implies that F_f is associative. Thus F_f is an FGL, so we can define $[p]_{F_f}(x)$. Both this and $f(x)$ are power series in one variable that commute with f and agree with px modulo x^2. By the same kind of uniqueness argument, we have $[p]_{F_f} = f$. □

PROPOSITION 14.3. *Given two series $f, g \in \mathcal{F}$ there is a unique strict isomorphism $u_{f,g} \colon F_f \to F_g$. Given a third such series $h \in \mathcal{F}$, we have $u_{f,h} = u_{g,h} \circ u_{f,g}$, and $u_{f,f}(x) = x$.*

PROOF. We start by applying Lemma 14.1 with $k = 1$ and $\lambda_1(x) = x$. This gives a unique power series $u = u_{f,g}$ with $u \circ f = g \circ u$ and $u(x) = x \pmod{x^2}$. We claim that this is a homomorphism of formal group laws, or in other words that $u \circ F_f = F_g \circ u^2$. Indeed, Lemma 14.1 implies that there is a unique series $G(x, y)$ such that $G(x, y) = x + y \bmod (x, y)^2$ and $G \circ f^2 = g \circ G$, so it suffices to check that $u \circ F_f$ and $F_g \circ u^2$ both have these properties. As $u(x) = x \pmod{x^2}$ and $F_f(x, y) = F_g(x, y) = x + y \bmod (x, y)^2$, we see that $u(F_f(x, y)) = F_g(u(x), u(y)) = x + y \bmod (x, y)^2$. As $F_f \circ f^2 = f \circ F_f$ and $F_g \circ g^2 = g \circ F_g$ and $u \circ f = g \circ u$, we see that

$$u \circ F_f \circ f^2 = u \circ f \circ F_f = g \circ u \circ F_f$$

and

$$F_g \circ u^2 \circ f^2 = F_g \circ g^2 \circ u^2 = g \circ F_g \circ u^2,$$

as required. Thus, u is a homomorphism of FGLs. As $u(x) = x \pmod{x^2}$, it is even a strict isomorphism. If v is any other strict isomorphism $F_f \to F_g$ then we must have $v \circ [p]_{F_f} = [p]_{F_g} \circ v$, or in other words $v \circ f = g \circ v$. We must also have $v(x) = x \pmod{x^2}$, so $v = u$.

Now suppose we have a third series $h \in \mathcal{F}$. It is clear that $u_{g,h} \circ u_{f,g}$ is a strict isomorphism $F_f \to F_h$, so by uniqueness we must have $u_{g,h} \circ u_{f,g} = u_{f,h}$. A similar argument shows that $u_{f,f}(x) = x$. □

An important feature of the formal group laws F_f is that they allow us to define series $[r]_f(x) \in R[\![x]\!]$ for $r \in R$, extending the definition for $r \in \mathbb{Z}_p$ that was given in Definition 13.11.

DEFINITION 14.4. For $r \in R$ we define $[r]_f(x) \in R[\![x]\!]$ to be the unique series such that $[r]_f(x) = rx \pmod{x^2}$ and $f([r]_f(x)) = [r]_f(f(x))$. (This is obtained by applying Lemma 14.1 to $\lambda_1(x) = rx$ with $f = g$.)

PROPOSITION 14.5. *The series $[r]_f(x)$ have the following properties.*

(a) $[0]_f(x) = 0$ *and* $[1]_f(x) = x$ *and* $[p]_f(x) = f(x)$.
(b) $[r]_f(F_f(x, y)) = F_f([r]_f(x), [r]_f(y))$, *so* $[r]_f$ *is an endomorphism of* F_f.
(c) $[rs]_f(x) = [r]_f([s]_f(x))$ *and* $[r + s]_f(x) = F_f([r]_f(x), [s]_f(x))$.
(d) *For any $i, j \geq 0$ there exists $m \geq 0$ such that $[r]_f(x) = [s]_f(x) \pmod{p^i, x^j}$ whenever $r = s \bmod p^m$. (In other words, the construction $r \mapsto [r]_f(x)$ is continuous with respect to the p-adic topology on R and the (p, x)-adic topology on $R[\![x]\!]$.)*

(It follows from (a) and (c) that $[r]_f(x)$ is as in Definition 1.1 when $r \in \mathbb{Z}$.)

PROOF. Claims (a) to (c) involve various equations. In each case, both sides have the same linear term and commute with f in an appropriate sense, so they are the same by the uniqueness clause in Lemma 14.1.

If we fix i and j, we know from Proposition 13.9 that $[p^m]_f(x) = 0 \pmod{p^i, x^j}$ for large m. Using (c) it follows that $[r]_f(x) = 0 \pmod{p^i, x^j}$ whenever $r \in p^m R$, and thus that $[r]_f(x) = [s]_f(x) \pmod{p^i, x^j}$ whenever $r = s \pmod{p^m R}$. □

We next want to understand the logarithm $\log_{F_f}(x) \in (\mathbb{Q} \otimes R)[\![x]\!]$. It will turn out that $p^{-n} f^n(x) \to \log_{F_f}(x)$ for an appropriate sense of convergence, which we now explain.

DEFINITION 14.6. For $r, s \geq 0$ we define

$$U(r,s) = p^r R[\![x]\!] + x^s (\mathbb{Q} \otimes R)[\![x]\!],$$

which is an additive subgroup of $(\mathbb{Q} \otimes R)[\![x]\!]$. We declare that a subset $V \subseteq (\mathbb{Q} \otimes R)[\![x]\!]$ is open iff for all $v(x) \in V$, there exist $r, s \geq 0$ such that $v(x) + U(r,s) \subseteq V$. This gives a topology on $(\mathbb{Q} \otimes R)[\![x]\!]$ with respect to which the ring operations are continuous.

PROPOSITION 14.7. *The elements $p^{-n} f^n(x)$ converge to $\log_{F_f}(x)$ with respect to the above topology.*

PROOF. Put $g_n(x) = p^{-n} f^n(x)$. We will first prove that there is an element $g_\infty(x) \in (\mathbb{Q} \otimes R)[\![x]\!]$ such that $g_m(x) \to g_\infty(x)$ as $m \to \infty$, then we will check separately that $g_\infty(x) = \log_F(x)$.

Our assumptions on $f(x)$ imply that there is a series $e(x)$ with

$$f(x) = px + x^{p^n} + p\, x^2 e(x).$$

Fix $N \geq 0$. Until further notice, all calculations will take place in the ring $Q_N = (\mathbb{Q} \otimes R)[\![x]\!]/x^N$, or the subring $P_N = R[\![x]\!]/x^N$. Note that if $u(x), v(x) \in Q_N$ with $v(0) = 0$ then we have a well-defined composite $u(v(x)) \in Q_N$. From the above expression for $f(x)$ we deduce the following: if $u(x) \in p^k P_N$ for some $k > 0$, then $f(u(x)) \in p^{k+1} P_N$, and $f(u(x)) - p\, u(x) \in p^{2k} P_N$.

Now choose m_0 such that $p^{m_0 n} \geq N$. Using $f(x) = x^{p^n} \pmod{p}$ we see that $f^{m_0}(x) \in p.P_N$. It follows inductively that $f^{(m_0+k)}(x) \in p^{k+1}.P_N$ and $f^{(m_0+k+1)}(x) - p\, f^{(m_0+k)}(x) \in p^{2k}.P_N$. We can now divide by p^{k+1} to get $g_{m_0+k+1}(x) - g_{m_0+k}(x) \in p^{k-1} P_N$. This easily implies that the elements $g_m(x)$ form a Cauchy sequence in the complete metric space Q_N. There is thus a unique polynomial $g_{\infty,N}(x) \in (\mathbb{Q} \otimes R)[x]$ of degree less than N that represents the limit of this Cauchy sequence.

We now let N vary again. From the uniqueness clause above, it follows that $g_{\infty,N+1}(x)$ must reduce to $g_{\infty,N}(x) \bmod x^N$, so there is a unique power series $g_\infty(x) \in (\mathbb{Q} \otimes R)[\![x]\!]$ with $g_\infty(x) = g_{\infty,N}(x) \pmod{x^N}$ for all N. This means that $g_n(x) \to g_\infty(x)$ in $\mathbb{Q}_p[\![x]\!]$ as claimed. It is also easy to see that $g_{\infty,2}(x) = x$ and so $g_\infty(x) = x \pmod{x^2}$.

Now put $h(x) = \log_{F_f}(x) - g_\infty(x)$, so $h(x) = 0 \pmod{x^2}$. Note that $\log_{F_f}(f(x)) = \log_{F_f}([p]_{F_f}(x)) = p \log_{F_f}(x)$, and it is clear by construction that $g_\infty(f(x)) = p\, g_\infty(x)$, so $h(f(x)) = p\, h(x)$. Suppose we have shown that $h(x) = 0 \pmod{x^N}$ for some $N \geq 2$, say $h(x) = a\, x^N \pmod{x^{N+1}}$ for some $a \in \mathbb{Q} \otimes R$. The relation $h(f(x)) = p\, h(x)$ then gives $p^N a\, x^N = p\, a\, x^N \pmod{x^{N+1}}$ so $(p - p^N)a = 0$ so $a = 0$. This means that $h(x) = 0 \pmod{x^{N+1}}$. After applying this inductively we find that $h(x) = 0$, so $\log_F(x) = g_\infty(x)$ as claimed. □

We now explain how to define a formal group G that does not depend on the choice of $f \in \mathcal{F}$.

DEFINITION 14.8. Given any R-algebra A, we define

$$G(A) = (\mathcal{F} \times \mathrm{Nil}(A))/\sim,$$

where $(f, a) \sim (g, b)$ if and only if $u_{f,g}(a) = b$. We define a binary operation on $G(A)$ by

$$[f, a] + [g, b] = [g, F_g(u_{f,g}(a), b)],$$

so in particular we have

$$[f, a] + [f, b] = [f, F_f(a, b)].$$

For $r \in R$ and $[f, a] \in G(A)$ we also define $r.[f, a] = [f, [r]_f(a)]$.

PROPOSITION 14.9. *G is a formal group over* $\mathrm{spec}(R)$*, and the endomorphism ring of G is R.*

PROOF. Fix $h \in \mathcal{F}$ and define $x\colon G \to \widehat{\mathbb{A}}^1$ by $x[f,a] = u_{f,h}(a)$. It is easy to check that this is well-defined and is an isomorphism. This proves that G is a formal group.

Now let E be the endomorphism ring of G. For any $m \in E$, we have an induced map $m^*\colon \omega_G \to \omega_G$ of R-modules, and ω_G is free of rank one over R, so this is multiplication by an element $\delta(m) \in R$. This defines a homomorphism $\delta\colon E \to R$, which is injective by Corollary 9.20. On the other hand, it is easy to see that our definition $r.[f,a] = [f,[r]_f(a)]$ gives a map $\mu\colon R \to E$, with $\delta \circ \mu = 1$. As δ is injective, it follows that δ and μ are mutually inverse isomorphisms. □

15. Moduli schemes of morphisms

Suppose we have two formal groups, say G_0 and G_1, over the same scheme S. As discussed previously, a homomorphism from G_0 to G_1 means a map $f\colon G \to H$ of formal schemes that is compatible with the projections to S and with the group structures. Thus, for any ring R we have a set $S(R)$, and bundles $G(R)$ and $H(R)$ of groups over $S(R)$, and a natural map $f_R\colon G(R) \to H(R)$ of bundles of groups. We will write $\hom(G_0,G_1)$ for the set of homomorphisms in this sense. This is easily seen to be an abelian group under pointwise addition. Also, if we have a third formal group G_2 over S then the composition map

$$\hom(G_1,G_2) \times \hom(G_0,G_1) \to \hom(G_0,G_2)$$

is additive in both variables.

Now suppose we have coordinates x_0 and x_1 on G_0 and G_1, giving rise to formal group laws F_0 and F_1 over $\mathcal{O}_S$, so $x_i(a+b) = F_i(x_i(a),x_i(b))$. There is then a unique power series $m_f(t) = \sum_{i>0} a_i t^i \in \mathcal{O}_S[\![t]\!]$ such that $x_1(f(a)) = m_f(x_0(a))$, and this is a homomorphism of formal group laws from F_0 to F_1.

Rather than just considering the set $\hom(G_0,G_1)$, it is often natural to consider an analogous scheme. Specifically, suppose we have a ring R and a point $a \in S(R)$. This gives formal groups $G_{ia} = \operatorname{spec}(R) \times_S G_i$ over $\operatorname{spec}(R)$ for $i = 0,1$. We put

$$\operatorname{Hom}(G_0,G_1)(R) = \{(a,f) \mid a \in S(R),\ f \in \hom(G_{0a},G_{1a})\}.$$

This defines a functor from rings to sets.

PROPOSITION 15.1. *The functor* $\operatorname{Hom}(G_0,G_1)$ *is a scheme, as is the subscheme* $\operatorname{Iso}(G_0,G_1)$ *of isomorphisms.*

PROOF. For $i = 0,1$ we choose a coordinate x_i on G_i, and let F_i denote the associated formal group law. Put

$$A_0 = \mathcal{O}_S[a_1,a_2,\dots],$$

and define $m(t) = \sum_i a_i t^i \in A_0[\![t]\!]$. Let J be the ideal in A_0 generated by the coefficients of the series

$$m(F_0(s,t)) - F_1(m(s),m(t)) \in A_0[\![s,t]\!].$$

Put $A = A_0/J$. Then it is not hard to identify $\operatorname{Hom}(G_0,G_1)$ with $\operatorname{spec}(A)$, so it is a scheme as claimed. Similarly, we have $\operatorname{Iso}(G_0,G_1) = \operatorname{spec}(A[a_1^{-1}])$. □

EXAMPLE 15.2. Put

$$G = \operatorname{spec}(\mathbb{F}_p) \times \widehat{G}_a = \operatorname{spf}(\mathbb{F}_p[\![x]\!]),$$

and consider this as a formal group over $\mathbb{F}_p$. Then $\operatorname{Hom}(G,G)$ is the scheme A from Definition 12.1. Explicitly, for any $\mathbb{F}_p$-algebra R, the set $A(R)$ is the set of power series $f(t) \in R[\![t]\!]$ of the form $f(t) = \sum_{k\geq 0} a_k t^{p^k}$.

DEFINITION 15.3. In the above context, we note that ω_{G_0} and ω_{G_1} are both free modules of rank one over $\mathcal{O}_S$, as is $\operatorname{Hom}(\omega_{G_1},\omega_{G_0})$, so we have a scheme $\mathbb{A}(\operatorname{Hom}(\omega_{G_1},\omega_{G_0}))$ over S as in Example 5.2. Given a point $(a,f) \in \operatorname{Hom}(G_0,G_1)(R)$ we have a map

$$f^*\colon \omega_{G_{1a}} \to \omega_{G_{0a}},$$

and thus a point $(a,f^*) \in \mathbb{A}(\operatorname{Hom}(\omega_{G_1},\omega_{G_0}))(R)$. This construction gives a map

$$d\colon \operatorname{Hom}(G_0,G_1) \to \mathbb{A}(\operatorname{Hom}(\omega_{G_1},\omega_{G_0})).$$

PROPOSITION 15.4. *If* $\mathcal{O}_S$ *is a* $\mathbb{Q}$*-algebra, then the above map* d *is an isomorphism.*

PROOF. This is essentially a reformulation of Proposition 9.17(a), but we will give an independent argument.

Using Proposition 5.20 we can choose additive coordinates x_0 and x_1 on G_0 and G_1. We note that dx_i is a generator for ω_{G_i}, so there is a unique element u of $\mathrm{Hom}(\omega_{G_1}, \omega_{G_0})$ such that $u(dx_1) = dx_0$.

Now $\mathrm{Hom}(G_0, G_1)$ corresponds to the functor $\mathrm{Alg}_A \to \mathrm{Sets}$ that sends B to the set of power series $f(t) = \sum_{i>0} m_i t^i$ with $f(s+t) = f(s) + f(t)$. As $\mathcal{O}_S$ is a $\mathbb{Q}$-algebra we know that all binomial coefficients are invertible in $\mathcal{O}_S$, and it follows that m_i must vanish for $i > 1$, so $f(t) = m_1 t$. We also see that $d(f) = m_1 u$, and it is clear from this that d is an isomorphism. □

Now suppose we have formal groups G_0 and G_1 over different base schemes S_0 and S_1. We then define

$$\mathrm{Hom}(G_0, G_1)(R) = \{(a_0, a_1, f) \mid a_0 \in S_0(R), a_1 \in S_1(R), f \in \hom(G_{0,a_0}, G_{1,a_1})\}.$$

(In principle this could cause some ambiguity in cases where S_1 happens to be the same as S_0, but we will add clarifying remarks where necessary.) It is easy to see that this is again a scheme, as is the subfunctor

$$\mathrm{Iso}(G_0, G_1)(R) = \{(a_0, a_1, f) \mid a_0 \in S_0(R), a_1 \in S_1(R), f\colon G_{0,a_0} \xrightarrow{\simeq} G_{1,a_1}\}.$$

REMARK 15.5. In topology, these schemes arise as follows. Suppose we have even periodic cohomology theories represented by spectra E_0 and E_1, giving rise to formal groups $G_i = \mathrm{spf}(E_i^0(\mathbb{C}P^\infty))$ over $S_i = \mathrm{spec}(\pi_0(E_i))$. There is then a natural map

$$\mathrm{spec}(\pi_0(E_0 \wedge E_1)) \to \mathrm{Iso}(G_0, G_1),$$

which is an isomorphism under certain natural conditions that are often satisfied. Next, the object $\pi_0(E_0 \wedge (\Omega^\infty E_1)_+)$ has two different products, and the second product induces a ring structure on the group of indecomposables with respect to the first one. It turns out that there is a natural map

$$\mathrm{spec}(\mathrm{Ind}(\pi_0(E_0 \wedge (\Omega^\infty E_1)_+))) \to \mathrm{Hom}(G_0, G_1)$$

which is again often an isomorphism.

16. The Morava stabiliser group

In Example 15.2, we considered the moduli scheme of automorphisms of a formal group of infinite height, and mentioned its importance in algebraic topology. This scheme has natural geometric structure, and so does not behave like an ordinary discrete group.

By contrast, if we have formal groups G_i of height n over base schemes S_i over $\mathrm{spec}(\mathbb{F}_p)$, then the scheme $\mathrm{Hom}(G_0, G_1)$ behaves much more like a discrete set, at least if the rings $\mathcal{O}_{S_i}$ are sufficiently close to being algebraically closed. Moreover, the relevant discrete set does not depend very strongly on the choice of G_0 and G_1. We will postpone any justification of this claim, but we will use it to motivate our approach in this section: we will pick a specific formal group of height n, and investigate its endomorphisms.

DEFINITION 16.1. In this section, we fix a prime p, an integer $n > 0$, and a field k of order p^n. We let F_0 be the formal group law over $\mathbb{Z}_{(p)}$ with logarithm $\log_F(x) = \sum x^{p^{ni}}/p^i$, as in Proposition 8.1, and we let F denote the resulting FGL over $\mathbb{F}_p \subseteq k$. We put $S = \mathrm{spec}(k)$ and $G = S \times \widehat{\mathbb{A}}^1$, with the formal group structure determined by F. We put $D = \mathrm{end}(G)$ and $\Gamma = D^\times = \mathrm{aut}(G)$. We call Γ the *Morava stabiliser group*.

REMARK 16.2. We will show that Γ is a p-adic analytic Lie group of dimension n^2. It turns out that various cohomology groups of Γ are of great importance in chromatic homotopy theory. These cohomology groups are hard to calculate. However, it turns out that there are certain open subgroups of finite index whose cohomology is very simple, and this is a good way to start the calculations.

DEFINITION 16.3. For any $f \in D$, we let $[f](t) \in k[\![t]\!]$ be the power series such that $x(f(a)) = [f](x(a))$ for all $a \in G$. (Elsewhere we have written $m_f(t)$ for $[f](t)$, but here we want to emphasise the fact that

$[f](t) = [n]_F(t)$ when $f = n \in \mathbb{Z} \subseteq D$.) We note that

$$[f+g](t) = F([f](t), [g](t))$$
$$[f \circ g](t) = [f]([g](t))$$
$$[p](t) = [p]_F(t) = t^{p^n}.$$

We also define

$$J_m = \{f \in D \mid [f](t) \in t^{p^m} k[\![t]\!]\}.$$

It is easy to see that this is a two-sided ideal in D, with $J_m J_j \leq J_{m+j}$ and $D = \varprojlim_m D/J_m$.

PROPOSITION 16.4. (a) *There is an element $s \in D$ with $[s](t) = t^p$. This satisfies $s^n = p$ in D.*
(b) *For each $a \in k$ there is an element $\tau(a) \in D$ with $[\tau(a)](t) = at$. These satisfy $\tau(ab) = \tau(a)\tau(b)$ and $\tau(0) = 0$ and $\tau(1) = 1$ and $s\tau(a) = \tau(a^p)s$.*

PROOF. (a) The formal group law F_0 has the form $F_0(t_0, t_1) = \sum_{i,j} a_{ij} t_0^i t_1^j$ with $a_{ij} \in \mathbb{Z}_{(p)}$, which means that $a_{ij}^p = a_{ij} \pmod{p\mathbb{Z}_{(p)}}$. From this it follows that over $\mathbb{F}_p \subseteq k$ we have $F(t_0, t_1)^p = F(t_0^p, t_1^p)$, so the series $[s](t) = t^p$ gives an endomorphism of G, as required. From $[s](t) = t^p$ we get $[s^k](t) = t^{p^k}$ for all k and so $[s^n](t) = t^{p^n} = [p](t)$, so $s^n = p$ in D.

(b) Consider the ring $U = \mathbb{Z}_{(p)}[u]/(u^{p^n} - u)$, and note that in U we have $u^{p^{nk}} = u$ for all $k \geq 0$. In $(\mathbb{Q} \otimes U)[\![t]\!]$ we therefore have

$$\log_F(ut) = \sum_k \frac{u^{p^{nk}} t^{p^{nk}}}{p^k} = \sum_k \frac{u\, t^{p^{nk}}}{p^k} = u \log_F(t).$$

By taking $t = F(t_0, t_1)$ and applying $\log_F^{-1}$ we get $uF(t_0 + t_1) = F(ut_0, ut_1)$, so the series ut gives an endomorphism of F_0 defined over U. For any $a \in k$ we have $a^{p^n} = a$, so there is a unique ring homomorphism $U \to k$ sending u to a. By applying this to the above endomorphism, we conclude that there is an element $\tau(a) \in D$ with $[\tau(a)](s) = as$ as claimed. Clearly $[\tau(a)]([\tau(b)](t)) = abt = [\tau(ab)](t)$ so $\tau(ab) = \tau(a)\tau(b)$. The identities $\tau(0) = 0$ and $\tau(1) = 1$ are also clear. Moreover, we have

$$[s]([\tau(a)](t)) = [s](at) = a^p t^p = [\tau(a^p)]([s](t))$$

so $s\tau(a) = \tau(a^p)s$.

□

PROPOSITION 16.5. *Every element $f \in D$ has a unique expansion $f = \sum_{m=0}^{\infty} \tau(a_m) s^m$ with $a_m \in k$. Moreover, f is invertible iff a_0 is nonzero.*

PROOF. For any $f \in D$, put $a_0 = [f]'(0) \in k$ and $f_0 = f - \tau(a_0)$. Then $f_0'(0) = 0$, so Proposition 9.17 tells us that f_0 factors uniquely through the relative Frobenius map, which is called s in our current notation. In other words, there is a unique $f_1 \in D$ with $f = \tau(a_0) + f_1 s$. An evident induction based on this gives a sequence of elements $a_i \in k$ and $f_i \in D$ with $f = \sum_{j<i} \tau(a_j) s^j + f_i s^i$ and $f_i = \tau(a_i) + f_{i+1} s$. In the limit we get $f = \sum_i \tau(a_i) s^i$ as required. It is clear that the map $f \mapsto [f]'(0)$ gives a ring homomorphism from D to k, so if f is invertible then $a_0 \neq 0$. Conversely, if $a_0 \neq 0$ then we can write f as $\tau(a_0)(1 - g)$ with $g \in Ds = J_1$, and it follows that the sum $\sum_j g^j \tau(a_0^{-1})$ converges in D to an element h with $fh = 1$. A similar construction gives k with $kf = 1$, and then we have $k = k1 = kfh = 1h = h$, so h is a two-sided inverse for f. □

COROLLARY 16.6. *D is a free module of rank n^2 over $\mathbb{Z}_p$.*

PROOF. Let X be the set of sums $\sum_{m=0}^{n-1} \tau(a_m) s^m$ with $a_m \in k$, so $|X| = p^{n^2} < \infty$. As $p = s^n$, the proposition tells us that every element of D has a unique representation $\sum_j x_j p^j$ with $x_j \in X$. It follows that D is generated by X, so in particular it is finitely generated. It also follows that the map $X \to D/p$ is bijective, so $|D/p| = p^{n^2}$, so the rank of D must be n^2. We can thus choose $Y \subseteq X$ with $|Y| = n^2$ such that Y gives a basis for D/p over $\mathbb{Z}/p$. It then follows easily that the resulting map $\mathbb{Z}_p\{Y\} \to D$ is an isomorphism. □

DEFINITION 16.7. We let W denote the subset of D consisting of sums $\sum_j \tau(a_j)p^j$ with $a_j \in k$.

PROPOSITION 16.8. (a) *An element $f \in D$ lies in W iff it commutes with $\tau(a)$ for all $a \in k$.*
(b) *W is a commutative subring of D. It is a free module of rank n over $\mathbb{Z}_p$ with $W/p = k$, so it is an object of the category $\mathcal{W}$ described in Section 13.*
(c) *D is free as a left module over W, with basis $\{s^i \mid 0 \leq i < n\}$. It is also free as a right module, with the same basis.*
(d) *For $a \in W$ we have $sa = \phi(a)s$, where $\phi\colon W \to W$ is the lifted Frobenius map, as in Corollary 13.24.*
(e) *The centre of D is $\mathbb{Z}_p$.*

PROOF. (a) If $f = \sum_i \tau(a_i)s^i$ then

$$\tau(u)^{-1} f \tau(u) = \sum_i \tau(u^{p^i-1}a_i)s^i$$

for all $u \in k^\times$. If u is a generator of $k^\times$ then it has order $p^n - 1$, so u^{p^i-1} is only equal to 1 if i is divisible by n. It follows that f commutes with $\tau(u)$ iff $a_i = 0$ whenever i is not divisible by n, which means that $f = \sum_j a_{nj}s^{nj} = \sum_j a_{nj}p^j \in W$.

(b) From (a) it is clear that W is a subring. Every element of W can be written uniquely as $\sum_i \tau(a_i)p^i$ with $a_i \in k$, so by the method of Corollary 16.6 we see that W is free of rank n over $\mathbb{Z}_p$. We also see that W/p maps isomorphically to k, so $W \in \mathcal{W}$.

(c) We can define $\beta\colon W^n \to D$ by $\beta(w) = \sum_{i=0}^{n-1} w_i s^i$. From what we have said already it is clear that this gives an isomorphism $W^n/p \to D/p$, and both W^n and D are free of rank n^2 over $\mathbb{Z}_p$, so β is an isomorphism. Essentially the same argument shows that we also have a right module basis.

(d) This is clear from the formula $s\tau(a) = \tau(a^p)s$.

(e) If $f \in D$ and f commutes with $\tau(u)$ for all u then we have $f = \sum_i \tau(a_i)p^i$ for some $a_i \in k$. If f also commutes with s then we find that $a_i^p = a_i$ for all i, so $a_i \in \mathbb{F}_p$. From this we see that $f \in \mathbb{Z}_p$. □

DEFINITION 16.9. For $w \in W \setminus \{0\}$, we define $v_p(w)$ to be the largest k such that $w \in p^k W$. We also define $v_p(0) = \infty$.

DEFINITION 16.10. For $f \in D$, we define $\mu(f) \in M_n(W)$ to be the matrix such that

$$fs^i = \sum_{j=0}^{n-1} s^j \mu(f)_{ji}$$

for $0 \leq i < n$. We also define

$$\begin{aligned} MD &= \{m \in M_n(W) \mid m_{ji} \in pW \text{ when } j < i\} \\ &= \{m \in M_n(W) \mid m \text{ is lower triangular mod } p\}. \end{aligned}$$

PROPOSITION 16.11. *The map μ gives an injective ring homomorphism $D \to MD$. Moreover, for any $f \in D$, the characteristic polynomial of $\mu(f)$ lies in $\mathbb{Z}_p[t]$.*

PROOF. First, if $f = \sum_{m=0}^{n-1} a_m s^m$ with $a_i \in W$ we find that

$$fs^i = \sum_{m=0}^{n-1} a_m s^{m+i} = \sum_{m=0}^{n-1} s^{m+i}\phi^{-m-i}(a_m).$$

In cases where $m + i \geq n$, we can write s^{m+i} as $p.s^{m+i-n}$. After reindexing the terms, and noting that $\phi^n = 1$, we obtain

$$\mu(f)_{ji} = \begin{cases} \phi^{-j}(a_{j-i}) & \text{if } i \leq j \\ p\phi^{-j}(a_{j-i+n}) & \text{if } j < i. \end{cases}$$

This shows that $\mu(f) \in MD$. As $\mu(f)_{j0} = \phi^{-j}(a_j)$, it is easy to see that μ is injective. We also have

$$\begin{aligned} fgs^i &= \sum_j fs^j \mu(g)_{ji} = \sum_{m,j} s^m \mu(f)_{mj}\mu(g)_{ji} \\ &= \sum_m s^m (\mu(f)\mu(g))_{mi}, \end{aligned}$$

so $\mu(fg) = \mu(f)\mu(g)$, so μ is a ring homomorphism. Next, a straightforward calculation gives $\det(\mu(s)) = (-1)^n p$, so in particular $\det(\mu(s)) \neq 0$.

Now let $\chi(t)$ be the characteristic polynomial of $\mu(f)$. Let $\phi(\mu(f))$ be the matrix obtained by applying ϕ to each entry in $\mu(f)$. We then find that $\mu(s)\mu(f) = \phi(\mu(f))\mu(s)$. After taking determinants and cancelling $\det(\mu(s))$ we get $\det(\mu(f)) = \phi(\det(\mu(f)))$, so $\det(\mu(f)) \in \mathbb{Z}_p$. After replacing f by $t - f$ with $t \in \mathbb{Z}_p$ we see that $\chi(t) \in \mathbb{Z}_p$ whenever $t \in \mathbb{Z}_p$. From this it follows easily that the coefficients of $\chi(t)$ lie in $\mathbb{Z}_p$. □

Example 16.12. If $n = 4$ and $f = a_0 + a_1 s + a_2 s^2 + a_3 s^3$ then

$$\mu(f) = \begin{bmatrix} a_0 & pa_3 & pa_2 & pa_1 \\ \phi^{-1}(a_1) & \phi^{-1}(a_0) & p\phi^{-1}(a_3) & p\phi^{-1}(a_2) \\ \phi^{-2}(a_2) & \phi^{-2}(a_1) & \phi^{-2}(a_0) & p\phi^{-2}(a_3) \\ \phi^{-3}(a_3) & \phi^{-2}(a_2) & \phi^{-2}(a_1) & \phi^{-3}(a_0) \end{bmatrix}$$

Definition 16.13. For $f \in D$ we define $\mathrm{trace}(f)$ and $\mathrm{norm}(f)$ to be the trace and determinant of the matrix $\mu(f)$. (These lie in $\mathbb{Z}_p$, by the proposition above.) We call them the reduced trace and determinant of f. We put

$$S\Gamma = \ker(\det\colon \Gamma = D^\times \to \mathbb{Z}_p^\times).$$

For $m > 0$ we also put $\Gamma_m = 1 + s^m D = 1 + Ds^m < \Gamma$ and $S\Gamma_m = \Gamma_m \cap S\Gamma$. All these subgroups are easily seen to be normal. The notation $x = y + O(m)$ will mean that $x - y \in s^m D$; if x and y are in Γ this is equivalent to $x\Gamma_m = y\Gamma_m$. We also write $o(m)$ for $O(m+1)$.

Definition 16.14. For $x, y \in D$ we write $[x, y]_a = xy - yx$. If $x, y \in D^\times$ we also write $[x, y]_m = xyx^{-1}y^{-1}$.

Lemma 16.15. *Suppose that $x = 1 + a$ and $y = 1 + b$ with $a \in s^i D$ and $b \in s^j D$ and $i, j > 0$. Then*

$$\begin{aligned} [x, y]_a &= [a, b]_a \in s^{i+j} D \\ xy &= 1 + a + b + O(i + j) = 1 + O(\min(i, j)) \\ xyx^{-1} &= y + [a, b]_a + O(2i + j) \\ [x, y]_m &= 1 + [a, b]_a + O(i + j + \min(i, j)) \\ x^p &= \begin{cases} 1 + a^p + o(pi) & \text{if } i < n/(p-1) \\ 1 + pa + o(i + n) & \text{if } i > n/(p-1). \end{cases} \end{aligned}$$

Note that we have said nothing about x^p in the case where $i(p-1) = n$; this case will be discussed later.

Proof. The following identities can be verified by substituting $x = 1 + a$ and $y = 1 + b$ and expanding out:

$$\begin{aligned} xy - (1 + a + b) &= ab \in s^{i+j} D \\ [x, y]_a &= [a, b]_a \in s^{i+j} D \\ (xyx^{-1} - y - [a, b]_a)x &= -[a, b]_a a \in s^{2i+j} D \\ ([x, y]_m - 1 - [a, b]_a)yx &= [a, b]_a(-a - b - ba) \in s^{i+j+\min(i,j)} D. \end{aligned}$$

As x and y are invertible, our first four claims follow from this. For the last claim, note that

$$x^p - 1 = \sum_{m=1}^{p} \binom{p}{m} a^m.$$

For $m < p$, the binomial coefficient is divisible by $s^n = p$, so the m'th term is divisible by s^{mi+n}. On the other hand, the p'th term is divisible by s^{pi}. If $i < n/(p-1)$ then $mi + n > pi$ for $0 < m < p$ and so $x^p - 1 = a^p + o(pi)$. On the other hand, if $i > n/(p-1)$ then $pi > i + n$ and also $mi + n > i + n$ for $1 < i < p$ so $x^p - 1 = pa + o(i + n)$. □

LEMMA 16.16. *For any positive integer k we have $v_p\binom{p^{-1}}{k} \geq (1 - kp)/(p - 1)$.*

PROOF. Put $m = \binom{p^{-1}}{k}$. From the definitions we have

$$m = (k!)^{-1} p^{-k} \prod_{j=0}^{k-1} (1 - pj),$$

so $v_p(m) = -k - v_p(k!)$. By Lemma 6.5 we have $v_p(k!) \leq (k-1)/(p-1)$ and so $v_p(m) \geq -k - (k-1)/(p-1) = (1 - kp)/(p - 1)$. □

COROLLARY 16.17. (a) *Γ/Γ_1 is isomorphic to $k^\times$*

(b) *For $i > 0$ the quotient Γ_i/Γ_{i+1} is isomorphic to k, considered as a group under addition.*

(c) *$[\Gamma_i, \Gamma_j]_m \leq S\Gamma_{i+j}$*

(d) *The centre of Γ is $\mathbb{Z}_p^\times$*

(e) *If n is not divisible by p then Γ_1 is isomorphic to $(1 + p\mathbb{Z}_p) \times S\Gamma_1$.*

(f) *Suppose that $i > n/(p-1)$. Then the map $x \mapsto x^p$ gives a homeomorphism $\Gamma_i \to \Gamma_{i+n}$. Moreover, this induces a group isomorphism $\Gamma_i/\Gamma_{i+1} \to \Gamma_{i+n}/\Gamma_{i+n+1}$.*

PROOF. (a) Follows from the ring isomorphism $D/sD = k$

(b) The map $a \mapsto 1 + \tau(a)s^i \pmod{\Gamma_{i+1}}$ gives the required isomorphism.

(c) As $S\Gamma$ is the kernel of a homomorphism to the abelian group $\mathbb{Z}_p^\times$, we see that all commutators are contained in $S\Gamma$. From the relation for $[x, y]_m$ in the lemma, we see that $[\Gamma_i, \Gamma_j] \leq \Gamma_{i+j}$.

(d) We saw in Proposition 16.8 that the centre of D is $\mathbb{Z}_p$, and the claim is clear from that.

(e) If n is not divisible by p then the map $u \mapsto u^n$ is bijective on $1 + p\mathbb{Z}_p$, so we can define a map $\mu\colon (1 + p\mathbb{Z}_p) \times S\Gamma_1 \to \Gamma_1$ by $\mu(u, x) = u^{1/n}x$. We find that $\mathrm{norm}(\mu(u, x)) = u$, and using this it is not hard to see that μ is an isomorphism.

(f) Define $\alpha\colon s^iD \to D$ by $\alpha(x) = (1 + x)^p - 1$. This is easily seen to be continuous, with image in $s^{i+n}D$. Now suppose we have $y \in s^{i+n}D$. As $i > n/(p-1)$ we have $i + n = np/(p-1) + \epsilon$ with $\epsilon > 0$. By Lemma 16.16, for $k > 0$ the binomial coefficient $\binom{p^{-1}}{k}$ is a $\mathbb{Z}_p$-multiple of $p^{(1-kp)/(p-1)} = s^{n(1-kp)/(p-1)}$, so $\binom{p^{-1}}{k} y^k \in s^{n/(p-1)+k\epsilon}D$. We can thus define $\beta(y) = \sum_{k>0} \binom{p^{-1}}{k} y^k$ and this lies in $s^{n/(p-1)+\epsilon}D$. A little algebra gives $n/(p-1) + \epsilon = i$, so $\beta\colon s^{i+n}D \to s^iD$. It is now easy to see that β is inverse to α, so α is a homeomorphism as claimed. From the last part of Lemma 16.15 we see that the induced map $\Gamma_i/\Gamma_{i+1} \to \Gamma_{i+n}/\Gamma_{i+n+1}$ is a group isomorphism.

□

LEMMA 16.18. *Suppose that $i \geq n$ (or $i \geq 2n$ in the case $p = 2$). Then the group Γ_i/Γ_{i+n} is elementary abelian, and is central in Γ_n/Γ_{i+n}. Moreover, the map $x \mapsto x^p$ induces a group isomorphism $\Gamma_i/\Gamma_{i+n} \to \Gamma_{i+n}/\Gamma_{i+2n}$.*

PROOF. From Lemma 16.15 we have $[\Gamma_n, \Gamma_i] \leq \Gamma_{i+n}$. This proves that Γ_i/Γ_{i+n} is central in Γ_n/Γ_{i+n}, and so is abelian. We have seen that the p'th power map sends Γ_i to Γ_{i+n}, so Γ_i/Γ_{i+n} is elementary abelian. Now suppose we have $x, y \in \Gamma_i$. We then have $yx = xyz$ for some $z \in \Gamma_{i+n}$. If we work mod Γ_{i+2n} then z becomes central and it is not hard to prove by induction that $(xy)^m = x^m y^m z^{m(m-1)/2}$ for all $m \geq 1$. If p is odd then $p(p-1)/2$ is divisible by p and $z^p \in \Gamma_{i+2n}$ so $(xy)^p = x^p y^p \pmod{\Gamma_{i+2n}}$. It follows that the p'th power map gives a well-defined isomorphism $\Gamma_i/\Gamma_{i+n} \to \Gamma_{i+n}/\Gamma_{i+2n}$. If $p = 2$ we are assuming that $i \geq 2n$ and it follows that z is already in Γ_{i+2n} so we get the same conclusion. □

REMARK 16.19. This lemma means that Γ_i is a powerful pro-p group when $i \geq n$ (or $i \geq 2n$ in the case $p = 2$). Many of our results could be proved more generally for powerful pro-p groups, but we will not develop that theory, and will instead give *ad hoc* arguments for the group Γ.

LEMMA 16.20. *Let $(a_1, \dots, a_{n^2})$ be a basis for D over $\mathbb{Z}_p$. Define $\gamma\colon \mathbb{Z}_p^{n^2} \to \Gamma_n = 1 + pD$ by*

$$\gamma(k) = (1 + pa_1)^{k_1} \cdots (1 + pa_{n^2})^{k_{n^2}}.$$

Then γ is a homeomorphism.

PROOF. It is clear that $\gamma(p^i\mathbb{Z}_p^{n^2}) \leq \Gamma_{(1+i)n}$, and that γ induces a well-defined map

$$\gamma_i\colon \frac{p^i\mathbb{Z}_p^{n^2}}{p^i\mathbb{Z}_p^{n^2}} \to \frac{\Gamma_{(1+i)n}}{\Gamma_{(2+i)n}},$$

which is an isomorphism of elementary abelian p-groups.

Now suppose we have $x \in \Gamma_n$ and we have found $k \in \mathbb{Z}_p^{n^2}$ with $\gamma(k) = x \pmod{\Gamma_{mn}}$. We then have $\gamma(k) = xy^{-1}$ for some $y \in \Gamma_{mn}$. By the above observation, there exists $j \in p^{m-1}\mathbb{Z}_p^{n^2}$ with $\gamma(j) = y \pmod{\Gamma_{(m+1)n}}$. Now each element $(1 + pa_r)^{j_r}$ lies in Γ_{mn} and so is central mod $\Gamma_{(m+1)n}$. Using this we see that $\gamma(i + j)$ agrees with x modulo $\Gamma_{(m+1)n}$. By iterating this, we get a convergent sequence in $\mathbb{Z}_p^{n^2}$ whose image under γ converges to x. By passing to the limit, we see that x is in the image of γ. As x was arbitrary, we see that γ is surjective. A similar inductive argument shows that it is also injective. It is thus a continuous bijection between compact Hausdorff spaces, and therefore a homeomorphism. □

LEMMA 16.21. *Consider elements $a = \sum_{h=0}^{n-1} a_h s^h \in D$ (with $a_h \in W$) and $x = 1 + ap^i s^j \in \Gamma_1$ (with $i, j \geq 0$ and $j < n$). Then the element $\operatorname{norm}(x) \in \mathbb{Z}_p^\times$ can be approximated as follows.*

(a) *If $j > 0$ then $\operatorname{norm}(x) = 1 \pmod{p^{i+1}}$.*
(b) *If $j = 0$ then $\operatorname{norm}(x) = 1 + p^i b \pmod{p^{i+1}}$ where*

$$b = \mathit{trace}_{W/\mathbb{Z}_p}(a_0) = \sum_{r=0}^{m-1} \phi^r(a_0) \in \mathbb{Z}_p.$$

PROOF. We have $as^j = \sum_h a'_h s^h$ for certain elements $a'_h \in W$. If $j > 0$ we find that $a'_0 = pa_{n-j} \in pW$, and it follows that the matrix $\mu(as^j)$ is divisible by p on the diagonal as well as above it. This means that $\mu(x)$ is one mod p^{i+1} on the diagonal, and zero mod p^{i+1} above the diagonal, so $\det(\mu(x)) = 1 \pmod{p^{i+1}}$ as claimed.

Now consider the case where $j = 0$. Put $y = 1 + a_0 p^i$ and $z = y^{-1}x$ so $x = yz$. Then $z \in 1 + p^i sD$, so $\operatorname{norm}(z) = 1 \pmod{p^{i+1}}$ by the previous case, so $\operatorname{norm}(x) = \operatorname{norm}(y) \pmod{p^{i+1}}$. Now $\mu(y)$ is just the diagonal matrix with entries $1 + \phi^{-h}(a_0)p^i$, so $\operatorname{norm}(y)$ is just the product of these entries, which is easily seen to be $1 + p^i b \pmod{p^{i+1}}$ as claimed. □

We have mentioned that the cohomology of the group Γ is important for applications in stable homotopy theory. In order to calculate the cohomology, one needs to know whether Γ has any finite p-subgroups. The following result will help with this.

LEMMA 16.22. *Put $R = \mathbb{Z}_p[v]/(v^{p-1} + p)$ and*

$$\varphi(t) = (t^p - 1)/(t - 1) = \sum_{i=0}^{p-1} t^i.$$

Then R contains an element u with $u = v \pmod{v^2}$ and $\varphi(1 + u) = 0$, and R can also be described as $\mathbb{Z}_p[u]/\varphi(1 + u)$. Moreover, for any $m \in \mathbb{F}_p^\times$ there is an automorphism $\psi^m\colon R \to R$ with $\psi^m(v) = \tau(m)v$, and this satisfies $\psi^m(1 + u) = (1 + u)^m$.

PROOF. Note that R freely generated as a $\mathbb{Z}_p$-module by $\{1, v, \dots, v^{p-2}\}$, and has $R/v = \mathbb{F}_p$. From this it follows that every element of R is a unit multiple of v^i for some i, and that R is an integral domain.

Put $u_0 = v$, and note that

$$(1 + u_0)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} v^i = v(p + v^{p-1}) + \sum_{i=2}^{p-1} \binom{p}{i} v^i = \sum_{i=2}^{p-1} \binom{p}{i} v^i \in R.pv^2 = R.v^{p+1}.$$

Suppose more generally that we have found u_m with $u_m = v \pmod{v^2}$ and $(1+u_m)^p - 1 \in R.v^{p+1+m}$. Let a be such that

$$(1+u_m)^p - 1 = av^{p+1+m} = -pav^{m+2},$$

and put $u_{m+1} = u_m + av^{m+2}$, which is again equal to v mod v^2. We then have

$$(1+u_{m+1})^p - 1 = -1 + \sum_{i=0}^{p} \binom{p}{i} v^{(m+2)i} a^i (1+u_m)^{p-i}.$$

We claim that this is zero mod $v^{p+2+m} = -pv^{m+3}$. Indeed, the term for $i = 0$, together with the -1, gives $-pav^{m+2}$. The term for $i = 1$ is $pav^{m+2}(1+u_m)^{p-1}$, and $u_m = v \pmod{v^2}$, so this all cancels modulo pv^{m+3}, just leaving the terms for $1 < i < p$. Each of these is divisible by $pv^{2(m+2)}$ and $2(m+2) \geq m+3$, so the claim follows. As $u_{m+1} = u_m \pmod{v^{m+2}}$ we see that the elements u_m converge p-adically to an element u with $(1+u)^p = 1$, or equivalently $u\varphi(1+u) = 0$. As $u = v \pmod{v^2}$ we find that u is a unit multiple of v and so u^{p-1} is a unit multiple of $v^{p-1} = -p$ so u is not a zero divisor so $\varphi(1+u) = 0$. Note also that $\varphi(1+u)$ is a monic polynomial of degree $p-1$ in u. Also, as $u = v \pmod{v^2}$ we find that $\{u^i \mid 0 \leq i < p-1\}$ is another basis for R/p over $\mathbb{F}_p$, and thus also for R over $\mathbb{Z}_p$. Using this we can identify R with $\mathbb{Z}_p[u]/\varphi(1+u)$.

Next, as $\varphi(1+u) = 0$ we have $(1+u)^p = 1$ so it is meaningful to write $(1+u)^m$ for $m \in \mathbb{F}_p^\times$. We put $u_m = (1+u)^m - 1$. This has $u_m = mv \pmod{v^2}$, so the elements u_m are distinct and nonzero. We also have $(1+u_m)^p = (1+u)^{mp} = 1$ so $\varphi(1+u_m) = 0$. We thus have $p-1$ distinct roots of $\varphi(t)$, so this must be a complete list of roots.

Next, recall that the map $\tau\colon \mathbb{F}_p \to \mathbb{Z}_p$ is injective and multiplicative, so $\tau(m)^{p-1} = 1$ for all $m \in \mathbb{F}_p^\times$. It is clear from this that there is an automorphism ψ^m sending v to $\tau(m)v$. This must send u to some root of $\varphi(1+t)$, and thus to u_j for some j. As $u = v \pmod{v^2}$ and $u_j = jv \pmod{v^2}$ we find that $j = m$. □

Lemma 16.23. *Let H be a finite subgroup of Γ. Then the subgroup $N = H \cap (1+sD)$ is a p-group and is normal in H, and H/N is a cyclic subgroup of order dividing $p^n - 1$ (and thus coprime to p). Moreover, there is a section of the projection $H \to H/N$, so H is a semidirect product of H/N with N.*

Proof. We have seen that $1+sD$ is normal in Γ with $\Gamma/(1+sD) = k^\times \simeq C_{p^n-1}$. From this it is clear that N is normal and that H/N has the claimed structure. Consider a nontrivial element $x \in N$, so $x = 1 + as^i$ for some $i > 0$ and some $a \in D \setminus sD$. It follows that $x^m = 1 + mas^i \pmod{s^{i+1}}$ for all $m \in \mathbb{Z}$, and thus that $x^m \neq 1$ if p does not divide m. This implies that N must be a p-group.

Now choose an element $h \in H$ that projects to a generator of H/N. Then h generates a cyclic group, which we can split as the product of a p-part and a p'-part. It is then easy to see that the p'-part maps isomorphically to H/N, so H is a semidirect product. □

We now want to understand something about the finite p-sugroups of Γ, which are contained in $1+sD$ by the lemma. For $p = 2$, it is easy to see that the only element of order p in $D^\times$ is -1. For odd primes we have the following:

Proposition 16.24. *Suppose that $p > 2$. If n is not divisible by $p-1$, then the only finite p-subgroup of Γ is the trivial group. If n is divisible by $p-1$ then Γ contains a copy of C_p, but does not contain a copy of C_p^2.*

Proof. We are looking for elements $x \in D$ with $x^p = 1$ but $x \neq 1$. In other words, the element $u = x-1$ should satisfy $\varphi(1+u) = 0$, so we have a ring map from $\mathbb{Z}_p[u]/\varphi(1+u)$ to D. In view of Lemma 16.22, it is equivalent to look for elements $v \in D$ with $v^{p-1} + p = 0$. Note that v cannot be zero, so we have $v = \tau(a)s^i \pmod{s^{i+1}}$ for some $i \geq 0$ and some $a \in k^\times$. This means that v^{p-1} is a unit multiple of $s^{(p-1)i}$, whereas $p = s^n$, so we can only have $v^{p-1} + p = 0$ if $n = (p-1)i$. This proves the first claim.

Now suppose that $n = (p-1)i$. Choose a generator $a \in k^\times \simeq C_{p^n-1}$. We have assumed that $p > 2$ so $(p^n-1)/2 \in \mathbb{N}$ and $a^{(p^n-1)/2}$ is a primitive square root of 1 so it must be equal to -1. Put $b = \tau(a^{(p^i-1)/2})s^i$. One can check by induction that $v^j = \tau(a^{(p^{ij}-1)/2})s^{ij}$, and thus that $v^{p-1} = \tau(a^{(p^n-1)/2})s^n = -p$. Thus, we have a copy of C_p in Γ.

Now suppose we have two commuting elements $u_0, u_1 \neq 1$ with $u_i^p = 1$. These give two commuting elements $v_0, v_1 \in D$ with $v_i^{p-1} = -p$. By our earlier analysis, both v_0 and v_1 must be invertible multiples

of s^i, so $v_1 = zv_0$ for some $z \in D^\times$. As v_0 and v_1 commute, we see that $z^{p-1} = 1$. It follows that the image of z in $D/s = k^\times$ must actually lie in $\mathbb{F}_p^\times$. Thus, we have $z = \tau(c)(1+d)$ for some $c \in \mathbb{F}_p^\times$ and $d \in sD$. As $\tau(c)$ is central and has $\tau(c)^{p-1} = 1$, we see that $(1+d)^{p-1} = 1$. However, we also have $(1+d)^{p-1} = 1 + (p-1)d \pmod{d^2}$ and it follows that we must have $d = 0$. This means that $v_1 = \tau(c)v_0$, and it follows that $1 + u_1 = (1+u_0)^c$. The, the subgroup generated by u_0 and u_1 is just a C_p and not a C_p^2. □

PROPOSITION 16.25. *There is a finite set $A \subset \Gamma$ such that the subgroup generated by A is dense in Γ. In other words, Γ is finitely topologically generated.*

PROOF. Put $N = np/(p-1) = n + n/(p-1)$ (which may or may not be an integer). Let A consist of the elements $\tau(a)$ for $a \in k^\times$, together with the elements $1 + \tau(a)s^j$ with $a \in k$ and $j \leq N$. Let H be the subgroup generated by A. We need to show that H is dense, or equivalently that $H\Gamma_j = \Gamma$ for all $j > 0$, which we will prove by induction. The claim is clear for $j = 1$, because $\Gamma/\Gamma_1 = k^\times$ and $\tau(k^\times) \subseteq A$. For the induction step, it will suffice to show that for all $j > 0$ and all $x \in \Gamma_j$ there exists $y \in H$ with $xy^{-1} \in \Gamma_{j+1}$. If $j \leq N$ then it is clear that we can even take $y \in A$. Suppose instead that $j > N$, and that $x = 1 + a$ with $a \in s^j D$. This means that $x = 1 + pb$ with $b \in s^{j-n}D$, and $j - n > n/(p-1)$. By induction there exists $z \in H$ with $z = 1 + b \pmod{s^{j-n+1}}$. Now $z^p \in H$, and the last part of Lemma 16.15 tells us that $z^p = 1 + a \pmod{s^{j+1}}$, as required. □

17. Divisors

DEFINITION 17.1. A *Weierstrass series* or *W-series* of degree n over a ring R is a power series $f(x) = \sum_k a_k x^k \in R[\![x]\!]$ such that a_n is a unit and a_k is nilpotent for $k < n$. A *Weierstrass polynomial* or *W-polynomial* is a W-series that is also a monic polynomial of degree n.

PROPOSITION 17.2. *Let $f(x)$ be a W-series of degree $n > 0$ over a ring R. Then there is a unique map $\alpha\colon R[\![y]\!] \to R[\![x]\!]$ of R-algebras such that $\alpha(y) = f(x)$, and this makes $R[\![x]\!]$ into a free module over $R[\![y]\!]$ with basis $\{1, x, \dots, x^{n-1}\}$.*

PROOF. Write $f(x) = \sum_k a_k x^k$ and $I = (a_k \mid k < n)$, so I is a nilpotent ideal. After replacing $f(x)$ by $f(x)/a_n$ we may assume that $a_n = 1$. As I is nilpotent it is easy to see that $f(x)$ is nilpotent modulo x^N for any N. Thus, given any series $g(x) = \sum_k b_k y^k \in R[\![y]\!]$ the series $g(f(x)) = \sum_k b_k f(x)^k$ converges in $R[\![x]\!]$. We can thus define $\alpha(g) = g(f(x))$ to get the required map α.

We claim that $\{1, x, \dots, x^{n-1}\}$ is a basis for $R[\![x]\!]$ over $R[\![y]\!]$. To see this, we define elements z_m for $m \geq 0$ as follows. There is a unique way to write $m = nk + j$ with $0 \leq j < n$ and $k \geq 0$, and we put $z_m = f(x)^k x^j$. Our claim is easily equivalent to the statement that any element of $R[\![x]\!]$ can be written uniquely in the form $\sum_m b_m z_m$ for some sequence of elements $b_m \in R$.

To prove this, it is convenient to consider a more general statement. For any R-module M we define a map

$$\theta_M\colon \prod_{m \geq 0} M \to M[\![x]\!]$$

by $\theta(b) = \sum_m b_m z_m$. Thus, our claim is that θ_R is an isomorphism.

Suppose that $IM = 0$, and consider a series $c = \sum_k c_k x^k \in M[\![x]\!]$. For any $b_m \in M$ we have $Ib_m = 0$ so $f(x)^k b_m = x^{nk} b_m \pmod{x^{nk+1}}$ so $z_m b_m = x^m b_m \pmod{x^{m+1}}$. Given this, an easy induction shows that there is a unique sequence of b_m's such that $c = \sum_{j<m} b_j z_j \pmod{x^m}$ for all m. This proves that θ_M is an isomorphism when $IM = 0$.

Now suppose we have a short exact sequence $L \rightarrowtail M \twoheadrightarrow N$ of R-modules, and that θ_L and θ_N are isomorphisms. We then have a diagram

$$\begin{array}{ccccc}
\prod_m L & \rightarrowtail & \prod_m M & \twoheadrightarrow & \prod_m N \\
{\scriptstyle\theta_L}\downarrow{\scriptstyle\simeq} & & {\scriptstyle\theta_M}\downarrow & & {\scriptstyle\simeq}\downarrow{\scriptstyle\theta_N} \\
L[\![x]\!] & \rightarrowtail & M[\![x]\!] & \twoheadrightarrow & N[\![x]\!]
\end{array}$$

It is trivial to check that the rows are exact and a diagram chase shows that θ_M is also an isomorphism. We can now use that short exact sequences $I^k/I^{k+1} \rightarrowtail R/I^{k+1} \twoheadrightarrow R/I^k$ to show that θ_{R/I^k} is an isomorphism for all k. For $k \gg 0$ we have $I^k = 0$ and we conclude that θ_R is an isomorphism as claimed. □

COROLLARY 17.3. *If $f(x) \in R[\![x]\!]$ is a W-series of degree n then $f(x)$ is not a zero-divisor in $R[\![x]\!]$, and $R[\![x]\!]/f(x)$ is a free module over R with basis $\{1, x, \dots, x^{n-1}\}$.* □

COROLLARY 17.4. *If $f(x) \in R[\![x]\!]$ is a W-series of degree n then there is a unique factorisation of the form $f(x) = u(x)g(x)$ where $u(x) \in R[\![x]\!]^\times$ and $g(x)$ is a W-polynomial of degree n.*

PROOF. The previous corollary tells us that there are unique elements $b_j \in R$ such that $-x^n = \sum_{j=0}^{n-1} b_j x^j \pmod{f(x)}$, and it is clear that $g(x) = x^n + \sum_{j=0}^{n-1} b_j x^j$ is the unique monic polynomial of degree n such that $f(x)$ divides $g(x)$, say $g(x) = f(x)v(x)$. As $f(x)$ is not a zero-divisor, the series $v(x)$ is uniquely characterised by this. Modulo I we know that x^n divides $f(x)$ and thus $g(x)$, but $g(x)$ is a monic polynomial of degree n so $g(x) = x^n \pmod{I}$ (which implies that g is a W-polynomial). As $f(x)$ is a unit multiple of x^n modulo I, we see that $v(0) \in R^\times$ and thus $v(x) \in R[\![x]\!]^\times$ so we can take $u(x) = 1/v(x)$. □

LEMMA 17.5. *Let f and g be monic polynomials of degree n and m over a ring R, such that $f(x)g(x) = x^{n+m}$. Then f and g are W-polynomials.*

PROOF. Write $f(x) = \sum_{i \leq n} a_i x^i$ and $g(x) = \sum_{j \leq m} b_j x^j$, so $a_n = b_m = 1$. Fix k with $0 \leq k < n$; we may assume inductively that a_j is nilpotent for $j < k$. It will suffice to show that some power of a_k lies in the nilpotent ideal $I = (a_0, \dots, a_{k-1})$, so we can work modulo I and thus assume that $a_j = 0$ for $j < k$. By considering the coefficient of x^k in the equation $f(x)g(x) = x^{n+m}$ we see that $a_k b_0 = 0$. We claim that more generally we have $a_k^{i+1} b_i = 0$ for $i = 0, \dots, m$. Indeed, if this holds for $i < j$ then $a_k^j g(x) = a_k^j b_j x^j + O(j+1)$, so it also holds for $i = j$ by considering the coefficient of x^{k+i} in the equation $a_k^j g(x) f(x) = a_k^j x^{n+m}$. The case $j = m$ gives $a_k^m = 0$, as required. □

REMARK 17.6. One can make a sharper statement as follows: if the coefficients a_i and b_j have degrees $n-i$ and $m-j$ respectively, then any monomial of total degree greater than nm is zero. We will not explain the proof here.

DEFINITION 17.7. A *formal curve* over a scheme X is a formal scheme C over X of dimension one, so that $C \simeq X \times \widehat{\mathbb{A}}^1$. Of course, a formal group is a formal curve, but in this section we will not need the group structure.

DEFINITION 17.8. Let C be a formal curve over a scheme X.

(a) We define
$$N = \{f \colon C \to \widehat{\mathbb{A}}^1\} < \{f \colon C \to \mathbb{A}^1\} = \mathcal{O}_C.$$
This is clearly an ideal in $\mathcal{O}_C$.

(b) Given an ideal $J \leq \mathcal{O}_C$, we define a functor $V(J) \subset C$ by
$$V(J)(R) = \{c \in C(R) \mid f(c) = 0 \text{ for all } f \in J\}.$$
We also define
$$\sqrt{J} = \{f \in \mathcal{O}_C \mid f^K \in J \text{ for some } K\}.$$

(c) We put
$$D_n^+(C) = \{J \leq \mathcal{O}_C \mid N \leq \sqrt{J} \text{ and } \mathcal{O}_C/J \text{ is free of rank } n \text{ over } \mathcal{O}_X\}.$$

(d) We define $W_n^+(C)$ to be the set of functions $f \in \mathcal{O}_C$ such that the ideal (f) is an element of $D_n^+(C)$. Note that $\mathcal{O}_C^\times$ acts on $W_n^+(C)$ by multiplication and we have a map $W_n^+(C)/\mathcal{O}_C^\times \to D_n^+(C)$ sending f to (f).

PROPOSITION 17.9. *Take $C = X \times \widehat{\mathbb{A}}^1$, write $R = \mathcal{O}_X$, and identify $\mathcal{O}_C$ with $R[\![x]\!]$ in the usual way. Then N is the set of series $f(x) \in R[\![x]\!]$ such that $f(0)$ is nilpotent. Moreover, $W_n^+(C)$ is the set of W-series of degree n over R. Thus, if $P_n(R)$ denotes the set of W-polynomials of degree n over R, we have $W_n^+(C) \simeq P_n(R) \times \mathcal{O}_C^\times$ and $D_n^+(C) = W_n^+(C)/\mathcal{O}_C^\times \simeq P_n(R)$.*

PROOF. The first statement follows from Proposition 5.10, and it follows in turn that $N \leq \sqrt{J}$ if and only if $x \in \sqrt{J}$.

Next, let f be a W-series of degree n. We claim that $J = (f) \in D_n^+(C)$, so that $f \in W_n^+(C)$. In view of Corollary 17.4, we may assume that f is a W-polynomial. As the lower coefficients of f are nilpotent, it is clear that x^n is nilpotent mod J, and thus that x is nilpotent mod J, and thus that $N \leq \sqrt{J}$. We also know from Corollary 17.3 that $R[\![x]\!]/f(x)$ is free of rank n over R, and the claim follows.

Next, suppose that $J \in D_n(R)$. We claim that J is generated by a W-polynomial of degree n. To see this, $A = R[\![x]\!]/J$. By assumption, this is a free module of rank n over R. Moreover, $x \in N \leq \sqrt{J}$ so $x^K = 0$ in A for some K.

For any element $z \in R[\![x]\!]$ we define $\mu_z \colon A \to A$ by $\mu_z(a) = za$. If $p(t)$ is a polynomial over R then clearly $\mu_{p(z)} = p(\mu_z)$.

The map μ_x is an R-linear endomorphism of the free module A, so it has a characteristic polynomial $f(t)$, which is a monic polynomial of degree n over R. The Cayley-Hamilton theorem tells us that $\mu_{f(x)} = f(\mu_x) = 0$, so $f(x) = \mu_{f(x)}(1) = 0$ in A, so $f(x) \in J$. Next, recall that $x^K \in J$ for some K. Write $s = \sum_{j=0}^{K-1} x^j t^{K-j}$, so that $(t-x)s = t^K \in A[t]$. We can regard μ_{t-x}, μ_s and μ_t as $R[t]$-linear endomorphisms of $A[t]$. If we let $g(t)$ be the determinant of μ_s then we find that $f(t)g(t) = t^{nK}$. It follows from Lemma 17.5 that $f(t)$ is a W-polynomial of degree n, so that $R[\![x]\!]/f(x)$ is free of rank n over R. Moreover, A is a quotient of $R[\![x]\!]/f(x)$ and A is also free of rank n, so $A = R[\![x]\!]/f(x)$ and $J = (f)$ (by Lemma 17.10 below). Thus J is generated by a W-polynomial, as claimed.

Now suppose that $g \in W_n^+(C)$. Our previous claim shows that there is a W-polynomial f such that $(g) = (f)$, say $f = ug$ and $g = vf$. Then $f = uvf$ but f is not a zero-divisor so $uv = 1$ so u and v are units. It is not hard to see that any unit multiple of a W-polynomial is a W-series, and we conclude that $W_n^+(C)$ is precisely the set of W-series of degree n. We have also seen that every ideal in $D_n^+(C)$ is generated by a W-polynomial, so the map $W_n^+(C)/\mathcal{O}_C^\times \to D_n^+(C)$ is surjective. As Weierstrass series are not zero divisors, we see easily that any two of them generate the same ideal iff they differ by a unit, so the map $W_n^+(C)/\mathcal{O}_C^\times \to D_n^+(C)$ is actually a bijection. Moreover, Corollary 17.4 tells us that $W_n^+(C) = P_n(R) \times \mathcal{O}_C^\times$, and thus that $D_n^+(C) = P_n(R)$. □

LEMMA 17.10. *Let M and N be free modules of finite rank n over a ring R, and let $\alpha \colon M \to N$ be a surjective homomorphism. Then α is an isomorphism.*

PROOF. We may assume that $M = N = R^n$, and write e_i for the i'th basis vector. As α is surjective we can choose a_i with $\alpha(a_i) = e_i$, and then define $\beta \colon R^n \to R^n$ by $\beta(e_i) = a_i$. We then have $\alpha\beta = 1$ so $\det(\alpha)\det(\beta) = 1$ so $\det(\alpha)$ is a unit in R, so α is an isomorphism. □

COROLLARY 17.11. *Let C be a formal curve over a scheme X.*

(a) *If $J \in D_n^+(C)$ then J is a free module of rank one over $\mathcal{O}_C$.*
(b) *$D_m^+(C) = W_m^+(C)/\mathcal{O}_C^\times$.*
(c) *If also $K \in D_m^+(C)$ then $JK \in D_{n+m}^+(C)$.*
(d) *If also $L \in D_m^+(C)$ and $JK = JL$ then $K = L$.*
(e) *If $f \in W_n^+(C)$ and $g \in W_m^+(C)$ then $fg \in W_{n+m}^+(C)$.*

PROOF. We may assume that $C = X \times \widehat{\mathbb{A}}^1$ and this makes everything fairly clear. Some points to note are as follows. Firstly, if $f \in W_n^+(C)$ and $g \in W_m^+(C)$ then we have a short exact sequence $\mathcal{O}_C/(f) \xrightarrow{\times g} \mathcal{O}_C/(fg) \to \mathcal{O}_C/(g)$, which shows that $\mathcal{O}_C/(fg)$ is free of rank $n+m$ over $\mathcal{O}_X$. Moreover, if $h \in N$ then for large r we have $h^r \in (f)$ and $h^r \in (g)$ so $h^{2r} \in (fg)$. This shows that $fg \in W_{n+m}(C)$, as claimed in (e). Also, for any J and K as above one can check that $K = \{f \mid fJ \subseteq JK\}$, so that J and JK determine K, which proves (d). □

REMARK 17.12. We can summarise this corollary by saying that $D^+(C) = \coprod_{n \geq 0} D_n^+(C)$ and $W^+(C) = \coprod_{n \geq 0} W_n^+(C)$ are commutative monoids under multiplication, in which cancellation is valid.

PROPOSITION 17.13. *Let C be a formal curve over X, with projection map $\pi \colon C \to X$ say. Write $\Gamma(X, C)$ for the set of sections of C, in other words the set of maps $\sigma \colon X \to C$ such that $\pi\sigma = 1$. Then there is a natural isomorphism $\Gamma(X, C) \simeq D_1^+(C)$.*

PROOF. Given a section σ, we define $J_\sigma = \{f\colon C \to \mathbb{A}^1 \mid f \circ \sigma = 0\}$, which is an ideal in $\mathcal{O}_C$. We claim that this lies in $D_1^+(C)$, and that the map $\sigma \mapsto J_\sigma$ is the required bijection. For this, we may assume that $C = X \times \widehat{\mathbb{A}}^1$. The sections are then the maps of the form $\sigma(a) = (a, u(a))$ where $u\colon X \to \widehat{\mathbb{A}}^1$, in other words $u \in \mathrm{Nil}(\mathcal{O}_X)$. We also have $J_\sigma = \{f(x) \in \mathcal{O}_X[\![x]\!] \mid f(u) = 0\}$. It is easy to see that this is generated by the W-polynomial $x - u$. We also know from Proposition 17.9 that every ideal in $D_1^+(C)$ is generated by a unique W-polynomial of degree one, and these clearly all have the form $x - u$. The proposition follows. □

DEFINITION 17.14. Let C be a formal curve over a scheme X. Given a ring R and a point $a \in X(R)$ we have a formal curve $C_a = \mathrm{spec}(R) \times_X C$ over $\mathrm{spec}(R)$, and we define

$$\mathrm{Div}_n^+(C)(R) = \{(a, D) \mid a \in X(R) \text{ and } D \in D_n^+(C_a)\}.$$

This defines a functor $\mathrm{Div}_n^+(C)$ from rings to sets.

REMARK 17.15. It follows from Proposition 17.13 that $\mathrm{Div}_1^+(C) = C$. Also, Corollary 17.11 gives product maps $\mathrm{Div}_n^+(C) \times_X \mathrm{Div}_m^+(C) \to \mathrm{Div}_{n+m}^+(C)$. A choice of coordinate on C gives a natural bijection $D_n^+(C_a) \simeq P_n(R) \simeq \mathrm{Nil}(R)^n$, and thus an isomorphism $\mathrm{Div}_n^+(C) \simeq \widehat{\mathbb{A}}^n \times X$, showing that $\mathrm{Div}_n^+(C)$ is a formal scheme of dimension n over X.

18. Meromorphic functions

DEFINITION 18.1. Let C be a formal curve over a scheme X. We define $\mathcal{M}_C$ to be the ring obtained from $\mathcal{O}_C$ by inverting all the elements of $W_n^+(C)$ for all n. (We shall see shortly that it is equivalent to choose a coordinate x and just invert x.) We write $W_0(C)$ for the subgroup of $\mathcal{M}_C^\times$ consisting of elements f/g where $f, g \in W_n^+(C)$ for some n (the same n for f and g). We also write $D_0(C) = W_0(C)/\mathcal{O}_C^\times$. It is clear that $W_0(C)$ and $D_0(C)$ are groups under multiplication.

REMARK 18.2. You should think of the elements of $\mathcal{M}_C$ as meromorphic functions on C whose poles are infinitesimally close to the origin.

DEFINITION 18.3. A *Weierstrass Laurent series* or *WL-series* of degree n over a ring R is a series $f(x) = \sum_{k\in\mathbb{Z}} a_k x^k$ such that

(1) $a_k = 0$ for $k \ll 0$
(2) a_k is nilpotent for $k < n$
(3) a_n is invertible.

Clearly $f(x)$ is a WL-series of degree n if and only if $x^m f(x)$ is a W-series of degree $m + n$ for $m \gg 0$.

We write $P(R)$ for the set of WL-series of degree 0 such that

(1) $a_k = 0$ for $k > 0$
(2) $a_0 = 1$.

Clearly $f(x) \in P(R)$ if and only if $x^m f(x)$ is a W-polynomial of degree m for $m \gg 0$.

REMARK 18.4. You should again think of $f(x)$ as having poles infinitesimally close to the origin. Recall that a genuine meromorphic function of a complex variable has different Laurent expansions in different annuli, depending on where the poles are. Our formal Laurent series should be thought of as expansions valid outside a small disc that contains all the poles.

PROPOSITION 18.5. *Take $C = X \times \widehat{\mathbb{A}}^1$, write $R = \mathcal{O}_X$, and identify $\mathcal{O}_C$ with $R[\![x]\!]$ in the usual way. Then $\mathcal{M}_C = R[\![x]\!][1/x]$, and $W_0(C)$ is the set of WL-series of degree 0. We also have $W_0(C) = \mathcal{O}_C^\times \times P(R)$ and thus $D_0(C) \simeq P(R)$.*

PROOF. Write $K = R[\![x]\!][1/x]$. We have $P(R) \subset K$ and if $f(x) \in P(R)$ then $1 - f(x)$ is nilpotent, so $f(x)$ is invertible. Thus $P(R) \leq K^\times$. If $g(x)$ is a W-polynomial of degree n then $g(x)/x^n \in P(R)$ so $g(x) \in K^\times$. It now follows from Corollary 17.4 that every W-series becomes invertible in K. In view of Proposition 17.9, this means that $W_n^+(C) \subset K^\times$, and it follows easily that $K = \mathcal{M}_C$. Let V be the set of WL-series of degree 0. If $f(x) \in V$ then for some m we have $x^m f(x) \in W_m^+(C)$, so Corollary 17.4 gives a factorisation $f(x) = u(x)g(x)/x^m$ with $u(x) \in \mathcal{O}_C^\times$ and $g(x)/x^m \in P(R)$. Note that $P(R)$ and $\mathcal{O}_C^\times$ are groups with trivial intersection, and that $P(R).\mathcal{O}_C^\times \subseteq V$. It follows that V is a group and that $V = P(R) \times \mathcal{O}_C^\times$. If

$f(x), g(x) \in W_n^+(C)$ then it is clear that f/x^n and g/x^n lie in V, so $f/g = (f/x^n)/(g/x^n)$ lies in V. This implies that $W_0(C) = V = \mathcal{O}_C^\times \times P(R)$ as claimed. □

DEFINITION 18.6. Let C be a formal curve over a scheme X. Given a ring R and a point $a \in X(R)$ we have a formal curve $C_a = \mathrm{spec}(R) \times_X C$ over $\mathrm{spec}(R)$, and we define

$$\mathrm{Div}_0(C)(R) = \{(a, D) \mid a \in X(R) \text{ and } D \in D_0(C_a)\}.$$

This defines a functor $\mathrm{Div}_0(C)$ from rings to Abelian groups.

REMARK 18.7. A choice of coordinate on C gives a natural bijection

$$D_0(C_a) \simeq P(R) \simeq \bigoplus_{k<0} \mathrm{Nil}(R),$$

and thus an isomorphism $\mathrm{Div}_0(C) \simeq X \times \bigoplus_{k<0} \widehat{\mathbb{A}}^1$. This is not a formal scheme according to our definitions, but one can set up a more general theory of formal schemes which does include $\mathrm{Div}_0(C)$.

19. Elliptic curves

DEFINITION 19.1. A *Weierstrass cubic* over a ring R is a homogeneous polynomial $f(x, y, z)$ of degree three such that $f = y^2 z \pmod{x, z^2}$ and $f = -x^3 \pmod{y, z}$. This means that there are elements $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_6 \in R$ such that

$$f(x, y, z) = y^2 z + \alpha_1 xyz + \alpha_3 yz^2 - x^3 - \alpha_2 x^2 z - \alpha_4 xz^2 - \alpha_6 z^3.$$

REMARK 19.2. If R is an algebraically closed field then every nonzero irreducible homogeneous cubic can be put in this form by a suitable change of coordinates. For more general rings there is a more complicated statement which again essentially reduces the study of all cubics to that of Weierstrass cubics. Such a cubic defines a subscheme C of the projective plane, and there is a coordinate-free description of the schemes that can arise in this way. These are non-affine schemes, but with suitable definitions they can still be regarded as functors from rings to sets. We shall not give details here, however.

As in example 5.9, we can use a Weierstrass cubic $f(x, y, z)$ over $\mathcal{O}_X$ to define a formal curve $\widehat{C}$ over X by

$$\widehat{C}(R) = \{(u, a, c) \in X(R) \times \mathrm{Nil}(R)^2 \mid f(a, 1, c) = 0\}.$$

Our main task in this section is to show that $\widehat{C}$ has a canonical group structure.

REMARK 19.3. The analytic analogy is as follows. If f is a Weierstrass cubic over $\mathbb{C}$ and we write $\mathcal{C} = \{[x : y : z] \in \mathbb{C}P^2 \mid f(x, y, z) = 0\}$ then the classical analytic theory of elliptic curves gives an isomorphism $\mathcal{C} \simeq \mathbb{C}/\Lambda$ for some lattice $\Lambda \leq \mathbb{C}$, with the zero element in $\mathbb{C}/\Lambda$ corresponding to $[0 : 1 : 0]$. This shows that $\mathcal{C}$ has a natural group structure. We next explain a purely algebraic characterisation of this structure, which we can use to generalise the theory to rings other than $\mathbb{C}$. Let $\mathbb{Z}\{\mathcal{C}\}$ be the free Abelian group on the points of $\mathcal{C}$, and let $[c]$ denote the basis element corresponding to a point $c \in \mathcal{C}$. Any nonzero meromorphic function f on C has zeros $\{a_i\}$ with multiplicities $\{n_i\}$, where poles count as zeros of negative multiplicity. This gives an element $\mathrm{div}(f) = \sum_i n_i[a_i] \in \mathbb{Z}\{\mathcal{C}\}$, called the divisor of f. A fundamental result (which can be proved by contour integration, for example) says that an element $\sum_i n_i[a_i]$ arises in this way if and only if we have $\sum_i n_i = 0 \in \mathbb{Z}$ and $\sum_i n_i a_i = 0 \in \mathcal{C}$. On the other hand, if we allow functions that are only meromorphic on an open subset of $\mathcal{C}$, we get all elements of $\mathbb{Z}\{\mathcal{C}\}$, and we only get the zero element if f is an invertible holomorphic function. Thus $\mathbb{Z}\{\mathcal{C}\}$ can be thought of as something like the group of local invertible meromorphic functions modulo local invertible holomorphic functions. We can define $D_0(\mathcal{C})$ to be the subgroup of elements $\sum_i n_i[a_i]$ with $\sum_i n_i = 0$ and $Q(\mathcal{C})$ to be the quotient by the group of divisors of global meromorphic functions. It is then easy to check that the map $c \mapsto [c] - [0]$ gives an isomorphism $\mathcal{C} \simeq Q(\mathcal{C})$ of groups, and this gives the required characterisation of the group structure on $\mathcal{C}$.

We write

$$A = \mathcal{O}_{\widehat{C}} = R[\![x, z]\!]/f(x, 1, z) = R[\![x]\!].$$

Note that

$$f(x, 1, z) = z + \alpha_1 xz + \alpha_3 z^2 - x^3 - \alpha_2 x^2 z - \alpha_4 xz^2 - \alpha_6 z^3,$$

so that $f(x,1,x^3) = 0 \pmod{x^4}$. It follows from Proposition 5.6 and its proof that there is a unique power series $\xi(x) \in R[\![x]\!]$ such that $z = \xi(x)$ in A, and moreover we have $\xi(x) = x^3 \pmod{x^4}$. We may thus write $\xi(x) = \sum_{k\geq 3} \xi_k x^k$, with $\xi_3 = 1$. We also have

$$\widehat{C}(R) = \{(u, a, \xi(a)) \mid u \in X(R) \text{ and } a \in \mathrm{Nil}(R)\}.$$

Next, we write

$$\begin{aligned}
A' &= R[\![z]\!] < A \\
B &= R[X,Y]/f(X,Y,1) \\
B' &= R[Y] \\
U &= \{u \in B \mid u = 1 \bmod \mathrm{Nil}(R)B\} \leq B^\times \\
U_1 &= 1 + \mathrm{Nil}(R) = R^\times \cap U < U \\
K &= A[1/x] = A[1/z] = \mathcal{M}_{\widehat{C}} \\
K' &= A'[1/z] < K.
\end{aligned}$$

We know that z is a unit multiple of x^3 in A, which is why $A[1/x] = A[1/z]$. We see from Proposition 17.2 that A is a free module over A' with basis $\{1, x, x^2\}$, and thus that K is a free module over K' with the same basis. One can also check that $f(X,Y,1)$ can be regarded as a monic polynomial of degree three in X over B', and thus that B is a free module over B' with basis $\{1, X, X^2\}$.

Remark 19.4. The relevant analogies for elliptic curves over the complex numbers are as follows. The ring A is the ring of functions on an formal neighbourhood of the origin. The ring K consists of meromorphic functions on a formal neighbourhood, whose poles are concentrated in an infinitesimal neighbourhood (where "infinitesimal" is smaller than "formal"). The ring B consists of meromorphic functions on the whole curve, whose poles (if any) are concentrated in an infinitesimal neighbourhood of the origin. The group U consists of functions on the whole curve that are very close to 1 away from an infinitesimal neighbourhood of the origin, so all the zeros and poles are contained in such a neighbourhood.

Definition 19.5. We define a map $\alpha\colon B \to K$ by $\alpha(X) = x/z$ and $\alpha(Y) = 1/z$.

Lemma 19.6. *The map α is injective.*

Proof. Note that $\alpha(B') \leq K'$, that B is freely generated over B' by $\{1, X, X^2\}$, and that K is freely generated over K' by $\{\alpha(1), \alpha(X), \alpha(X^2)\}$. It will thus be enough to show that α is injective on B', which is trivial. □

From now on we will allow ourseleves to think of B as a subring of K, and thus of $B^\times$ and U as subgroups of $K^\times$.

Definition 19.7. We write $Q = Q(C) = D_0(\widehat{C})/U = W_0(\widehat{C})/A^\times.U$. We also define a map $\phi\colon \Gamma(X, \widehat{C}) \to Q(C)$ by $\phi(c) = J_c/J_0$, where J_c is as in Proposition 17.13. If we use x as a coordinate to identify $\Gamma(X, \widehat{C})$ with $\mathrm{Nil}(\mathcal{O}_X)$ then we have $(1 - c/x) \in W_0(\widehat{C})$ and our map becomes $\phi(c) = [1 - c/x]$.

Theorem 19.8. *The map $\phi\colon \Gamma(X, \widehat{C}) \to Q(C)$ is a bijection. As $Q(C)$ is a group, this gives a natural group structure on $\Gamma(X, \widehat{C})$.*

Lemma 19.9. *Suppose that $h \in W^+_{3m-1}(\widehat{C})$ for some $m > 0$. Then there exists $u \in U$ such that $z^m u \in Ah$, and u is unique modulo U_1.*

Proof. We know that B has basis $\{X^i Y^j \mid i \geq 0\ ,\ 3 > j \geq 0\}$ over R. Let U' be the subset of U consisting of elements $u = \sum_{i,j} u_{ij} X^i Y^j$ where $u_{00} = 1$ (and necessarily $u_{ij} \in \mathrm{Nil}(R)$ for $(i,j) \neq (0,0)$). This need not be a subgroup but we do have $U = U_1 \times U'$ so it will suffice to show that there is a unique choice of u lying in U'.

Write

$$\begin{aligned}T &= \{(i,j) \mid m-1 > i \geq 0\ ,\ 3 > j \geq 0\} \cup \{(m-1,0),(m-1,1)\}\\ &= \{(i,j) \mid i \geq 0\ ,\ 3 > j \geq 0\ ,\ 3i+j < 3m-1\}\\ &= \{(i,j) \mid m > i \geq 0\ ,\ 3 > j \geq 0\ ,\ i+j \leq m\}.\end{aligned}$$

For each $k \in \{0,\dots,3m-2\}$ there is a unique element $(i,j) \in T$ such that $z^i x^j = x^k \pmod{x^{k+1}}$, and it follows by the method of Proposition 17.2 that $\{z^i x^j \mid (i,j) \in T\}$ is a basis for A/hA over R. Thus, there are unique elements $a_{ij} \in R$ such that $-z^m = \sum_T a_{ij} z^i x^j \pmod{Ah}$. We define

$$u = 1 + \sum_T a_{ij} z^{i-m} x^j = 1 + \sum_T a_{ij} X^i Y^{m-i-j} \in B,$$

so that $z^m u \in Ah$. If h is a unit multiple of x^{3m-1} then clearly $z^m \in Ah$ and so $a_{ij} = 0$ for all (i,j). We can always put ourselves in this situation by working modulo the nilpotent ideal generated by the lower coefficients of h, so we conclude that the elements a_{ij} are always nilpotent. Thus $u \in U'$.

Now suppose we have some other $v \in U'$ such that $z^m v \in Ah$. We can then write $w = v - u = \sum_{i,j} w_{ij} X^j Y^i$ where j runs from 0 to 2 and $w_{00} = 0$, and $z^m w \in Ah$. Note that $z^m w = \sum_{i,j} w_{ij} z^{m-i-j} x^j$. As K is freely generated over K' by $\{1, x, x^2\}$ one can check that $w_{ij} = 0$ when $i + j > m$. We also have $w_{00} = 0$, in other words $w_{ij} = 0$ when $i + j = 0$. If we write $k = m - i - j$ then we find that $w_{ij} = 0$ unless $0 \leq k < m$ and $0 \leq j < 3$ and $j + k = m - i \leq m$. Using our third description of T, we see that $z^m w$ lies in the span of $\{z^i x^j \mid (i,j) \in T\}$ but this set is a basis for A/Ah and $z^m w \in Ah$ so $z^m w = 0$ so $u = v$. □

Proof of Theorem 19.8. Define $Y_m = \{g \in W_0(\widehat{C}) \mid x^{-1} z^m g^{-1} \in A\}$. If $g \in Y_m$ then $x^{-1} z^m g \in W^+_{3m-1}(\widehat{C})$ so the lemma gives an element $u \in U$ such that $z^m u \in z^m x^{-1} g^{-1} A$. Thus $u = x^{-1} g^{-1} k$ for some $k \in A$. As $u, g \in W_0(\widehat{C})$ one can check that $k \in W^+_1(\widehat{C})$, so Corollary 17.4 gives a unique factorisation $k = (x - c)v$ with $c \in \mathrm{Nil}(R)$ and $v \in A^\times$. We define $\psi_m(g) = c$ (it is easy to see that this is well-defined even though u can be multiplied by an element of U_1). It is easy to check that the restriction of ψ_{m+1} to Y_m is ψ_m, and the union of the sets Y_m is $W_0(\widehat{C})$, so we get a map $\psi\colon W_0(\widehat{C}) \to \mathrm{Nil}(R)$.

Now suppose that $g \in Y_m$ as above and $w \in U$ and $t \in A^\times$. Choose n large enough that $z^n w^{-1} \in A$. We then have $uw^{-1} \in U$ and $vt \in A^\times$ and

$$z^{n+m}(uw^{-1}) = z^{n+m} x^{-1} (twg)^{-1} (x - c)(vt),$$

which implies that $\psi_{m+n}(twg) = c$. Thus $\psi(twg) = \psi(g)$, so ψ induces a map $\overline{\psi}\colon Q(C) = W_0(\widehat{C})/UA^\times \to \mathrm{Nil}(R)$.

Now identify $\mathrm{Nil}(R)$ with $\Gamma(X, \widehat{C})$, so that ϕ becomes the map $c \mapsto [1 - c/x]$. If we take $g(x) = 1 - c/x$ then for $m \gg 0$ we have $z^m g^{-1} \in W^+_{3m-1}(\widehat{C})$ and $z^m.1 = z^m x^{-1} g^{-1} (x - c)$ so $\overline{\psi}(g) = c$. Thus $\overline{\psi}\phi = 1$.

On the other hand, if we start with $g \in Y_m$ and define u, v and c as above we find that $g = (1 - c/x) u^{-1} v \in (1 - c/x) UA^\times$, so $[g] = \phi(c)$ in $Q(C)$. Thus $\phi\overline{\psi} = 1$. □

We now consider another characterisation of the group structure on an elliptic curve. The statement is simplest when $X = \mathrm{spec}(k)$ for some algebraically closed field k. We then have a set

$$\mathcal{C} = \{[x : y : z] \in \mathbb{P}^2(k) \mid f(x,y,z) = 0\}.$$

The group structure on this is characterised by the facts that

(a) The identity element is $[0 : 1 : 0]$.
(b) If $P_i = [x_i : y_i : z_i] \in \mathcal{C}$ for $i = 0, 1, 2$ and $P_0 + P_1 + P_2 = 0$ then the P_i's are collinear, or equivalently we have

$$\det \begin{pmatrix} x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{pmatrix} = 0.$$

In our context we need to do something a little more delicate, as many of our elements are nilpotent so we cannot divide by them. A key point is the following lemma:

LEMMA 19.10. *Define*

$$\chi(x_0,x_1,x_2)=\sum_{i,j,k}\xi_{i+j+k+2}x_0^ix_1^jx_2^k,$$

where as usual $\xi(x)=\sum_{k\geq 3}\xi_k x^k$ *is the series such that* $f(x,1,\xi(x))=0$. *Then we have*

$$\det\begin{pmatrix}x_0&x_1&x_2\\1&1&1\\ \xi(x_0)&\xi(x_1)&\xi(x_2)\end{pmatrix}=(x_1-x_0)(x_2-x_1)(x_0-x_2)\chi(x_0,x_1,x_2),$$

and $\chi(x_0,x_1,x_2)=x_0+x_1+x_2+O(2)$.

PROOF. Define $\zeta(x_0,x_1)=\sum_{i,j}\xi_{i+j+1}x_0^ix_1^j$. One can check directly that

$$(x_1-x_0)\zeta(x_0,x_1)=\xi(x_1)-\xi(x_0)$$

$$(x_2-x_1)\chi(x_0,x_1,x_2)=\zeta(x_0,x_2)-\zeta(x_0,x_1).$$

Of course we also have similar identities with the variables permuted. If we subtract the first column of our matrix from the second and third columns and then divide those columns by (x_1-x_0) and (x_0-x_2) respectively, we get the matrix

$$\begin{pmatrix}x_0&1&-1\\1&0&0\\ \xi(x_0)&\zeta(x_0,x_1)&-\zeta(x_0,x_2)\end{pmatrix}.$$

We can now expand with respect to the first column to get the claimed factorisation. As $\xi_k=0$ for $k<3$ and $\xi_3=1$ it is immediate from the definitions that $\chi(x_0,x_1,x_2)=x_0+x_1+x_2+O(2)$. □

PROPOSITION 19.11. *If* $a_0,a_1,a_2\in\Gamma(X,\widehat{C})$ *satisfy* $a_0+a_1+a_2=0$ *(using the group structure coming from Theorem 19.8) then* $\chi(a_0,a_1,a_2)=0$ *and thus*

$$\det\begin{pmatrix}x_0&x_1&x_2\\1&1&1\\ \xi(x_0)&\xi(x_1)&\xi(x_2)\end{pmatrix}=0.$$

PROOF. We need to show that $\phi(a_0)\phi(a_1)\phi(a_2)=1$ in $Q(C)$, or equivalently that $(1-a_0/x)(1-a_1/x)(1-a_2/x)\in UA^\times$. Consider the series $h(x)=\chi(a_0,a_1,x)\in A$. As $\chi(x_0,x_1,x_2)=x_0+x_1+x_2+O(2)$, we see that h is a W-series of degree one, and $h(a_2)=0$ so $h(x)=v(x)(x-a_2)$ for some $v\in A^\times$. Now consider

$$g(x)=(x-a_0)(x-a_1)(x-a_2)v(x)=(x-a_0)(x-a_1)\chi(a_0,a_1,x).$$

On the other hand, if $\zeta(x_0,x_1)$ is as in the proof of Lemma 19.10 we have

$$\begin{aligned}(x-a_0)(x-a_1)\chi(a_0,a_1,x)&=(x-a_0)(\zeta(a_0,x)-\zeta(a_0,a_1))\\&=z-\xi(a_0)-\zeta(a_0,a_1)x+a_0\zeta(a_0,a_1).\end{aligned}$$

This implies easily that $u(x)=g(x)/z\in U$ and of course $w(x)=z/x^3$ lies in $A^\times$, and so

$$(1-a_0/x)(1-a_1/x)(1-a_2/x)=g(x)/(x^3v(x))=u(x)w(x)/v(x)\in UA^\times,$$

as required. □

PROPOSITION 19.12. *If* $a\in\Gamma(X,\widehat{C})$ *then the inverse of* a *is* $-a/(1+\alpha_1a+\alpha_3\xi(a))$, *where the coefficients* α_i *come from the defining Weierstrass cubic*

$$f(x,y,z)=y^2z+\alpha_1xyz+\alpha_3yz^2-x^3-\alpha_2x^2z-\alpha_4xz^2-\alpha_6z^3.$$

PROOF. The basic point is that if a' is the inverse of a then $(a',\xi(a'))$ must lie on the line through the origin containing $(a,\xi(a))$, and it is easy to verify that

$$f(ta,1,t\xi(a))=\xi(a)t(1-t)(1+(1+\alpha_1a+\alpha_3\xi(a))t).$$

If we could divide by $\xi(a)$ and $(1-t)$ we could deduce the result, but these quantities are nilpotent so we need a more delicate argument.

We define $\theta(x) = \sum_k \xi_k x^{k-1}$, so that $\xi(x) = x\theta(x)$. We also define $g(x,t) = f(x,1,tx)/x \in R[x,t]$. It is easy to check that $g(x,\theta(x)) = 0 \in R[\![x]\!]$. Define

$$\begin{aligned} b &= \theta(a) \\ d &= \alpha_1 + \alpha_3 b \\ v &= 1 + ad = 1 + \alpha_1 a + \alpha_3 \xi(a) \\ u &= 1 + \alpha_2 b + \alpha_4 b^2 + \alpha_6 b^3 \\ c &= bdu^{-1} - a \end{aligned}$$

Note that u and v are invertible in R. Clearly $g(a,b) = 0$ and by writing this out we find that $vb = a^2u$. Given this it is easy to verify that $g(x,b) = (x-a)(bd - u(x+a))$ and thus that

$$f(x,1,bx) = xg(x,b) = -ux(x-a)(x-c).$$

Of course we also have $f(x,1,z) = 0$ so modulo $z - bx$ we have $f(x,1,bx) = 0$ so

$$x(x-a)(x-c) = (z-bx)w$$

for some $w \in A$. Modulo nilpotents we have $x^3 = zw$ and it follows easily that $w \in A^\times$. We also have $zx^{-3} \in A^\times$ and

$$(1 - a/x)(1 - c/x) = (1 - bX)w(zx^{-3}) \in UA^\times.$$

This shows that c is the inverse of a in $\Gamma(X, \widehat{C})$. On the other hand we have $vb = a^2$ so $vbd = au.ad = au(v-1) = auv - au$ so $bdu^{-1} = a - av^{-1}$ so $c = bdu^{-1} - a = -av^{-1} = -a/(1 + \alpha_1 a + \alpha_3 \xi(a))$ as claimed. □

20. Additive extensions

Definition 20.1. Let C and D be formal curves over a scheme X. Recall that $\mathcal{O}_C$ is the ring of maps $C \to \mathbb{A}^1$ and let N_C be the ideal of maps $C \to \widehat{\mathbb{A}}^1$. We say that a map $q\colon C \to D$ is an *isogeny of degree d* if the resulting map $q^*\colon \mathcal{O}_D \to \mathcal{O}_C$ makes $\mathcal{O}_C$ a free module of rank d over $\mathcal{O}_D$, and $N_C \leq \sqrt{q^* N_D}$.

Lemma 20.2. *Let $q\colon C \to D$ be a map of formal curves over X, and let x and y be coordinates on C and D respectively. Let f be the unique power series over $\mathcal{O}_X$ such that $q^*y = f(x)$. Then q is an isogeny of degree d if and only if f is a W-series of degree d. If this holds then $\{1, x, \dots, x^{d-1}\}$ is a basis for $\mathcal{O}_C$ over $\mathcal{O}_D$.*

Proof. First note that $N_C = \operatorname{Nil}(\mathcal{O}_X) + x\mathcal{O}_X[\![x]\!]$ so the condition $N_C \leq \sqrt{q^* N_D}$ is equivalent to the condition that $x^N = 0 \pmod{f(x)}$ for $N \gg 0$. It is clear from Proposition 17.2 that if f is a W-series then q is an isogeny, and that $\{1, x, \dots, x^{d-1}\}$ is a basis. Conversely, if q is an isogeny then $\mathcal{O}_C$ is free of rank d over $\mathcal{O}_D$ so $\mathcal{O}_C/f(x)$ is free of rank d over $O_D/y = \mathcal{O}_X$ so $f(x) \in W_d^+(C)$. We conclude from Proposition 17.9 that f is a Weierstrass series of degree d. □

Lemma 20.3. *Let $q\colon C \to D$ be an isogeny of formal curves over X. Then q is an epimorphism in the category of formal schemes over X. In other words, if $r, s\colon D \to E$ are maps of formal schemes over X and $rq = sq$ then $r = s$.*

Proof. Choose coordinates x on C, y on D and $z_1, \dots, z_r$ on E. We then have series f, g_i, h_i such that $q^*y = f(x)$ and $r^*z_i = g_i(y)$ and $s^*z_i = h_i(y)$, so $g_i(f(x)) = h_i(f(x))$ in $\mathcal{O}_X[\![x]\!] = \mathcal{O}_C$. As $q^*\colon \mathcal{O}_D \to \mathcal{O}_C$ is injective we conclude that $g_i = h_i$ so $r = s$. □

Definition 20.4. Let p be a prime, let X be a scheme such that p is nilpotent in $\mathcal{O}_X$, and let G be a formal group over X. We say that G has *Weierstrass height n* (or *W-height n*) if the map $p_G\colon G \to G$ is an isogeny of degree p^n. We say that G is *p-divisible* if it has W-height n for some n (where necessarily $0 < n < \infty$).

Remark 20.5. Write $X_{\mathrm{red}} = \operatorname{spec}(\mathcal{O}_X/\operatorname{Nil}(\mathcal{O}_X)) \subseteq X$, which is a scheme over $\operatorname{spec}(\mathbb{F}_p)$. Write $G_{\mathrm{red}} = G \times_X X_{\mathrm{red}}$, which is a formal group over X_{red}. This has height n for some n with $0 < n \leq \infty$; if $n < \infty$ then in terms of a coordinate we have $[p](x) = ux^{p^n} + O(p^n + 1)$. It is easy to see that G has W-height n if and only if $n < \infty$ and u is invertible.

DEFINITION 20.6. For the rest of this section, X will be a scheme such that p is nilpotent in $\mathcal{O}_X$ and G will be a formal group of W-height n over X. The symbol $\widehat{G}_a$ will really denote $\widehat{G}_a \times X$, considered as a formal group over X.

LEMMA 20.7. *We have* $\mathrm{Hom}(G, \widehat{G}_a) = 0$.

PROOF. Let $s\colon G \to \widehat{G}_a$ be a homomorphism. For $N \gg 0$ we have $p^N = 0$ in $\mathcal{O}_X$ so $p^N = 0$ as an endomorphism of $\widehat{G}_a$. By considering the following square, we see that $s \circ p_G^N = 0$.

$$\begin{array}{ccc} G & \xrightarrow{p_G^N} & G \\ {\scriptstyle s}\downarrow & & \downarrow{\scriptstyle s} \\ \widehat{G}_a & \xrightarrow[p^N=0]{} & \widehat{G}_a \end{array}$$

As p_G^N is an isogeny, it is an epimorphism, so $s = 0$. □

DEFINITION 20.8. An *additive extension* of G is a sequence of formal group schemes and homomorphisms $\widehat{G}_a \xrightarrow{j} E \xrightarrow{q} G$ such that $qj = 0$ and there exist maps $\widehat{G}_a \xleftarrow{r} E \xleftarrow{s} G$ (not necessarily homomorphisms) with $rj = 1_{\widehat{G}_a}$ and $jr + sq = 1_E$ and $qs = 1_G$. Such a pair (r, s) is a *(non-additive) splitting* of the extension.

REMARK 20.9. Let E, j, q, r and s be as above. Note that j and s are monomorphisms and r and q are epimorphisms. Define maps $f\colon \widehat{G}_a \times G \to E$ and $g\colon E \to \widehat{G}_a \times G$ by $f(a, u) = j(a) + s(u)$ and $g(e) = (r(e), q(e))$. Then it is easy to check that $fg = jq + sr = 1_E$. Moreover, as q is a homomorphism with $qj = 0$ and $qs = 1$ we have $qf(a, u) = u$. Also, we have $jrf(a, u) = (1 - sq)f(a, u) = f(a, u) - s(u) = j(a)$ and j is a monomorphism so $rf(a) = a$. We now see that $gf = 1$, so that f and g are mutually inverse isomorphisms.

DEFINITION 20.10. Let E and E' be additive extensions of G. A *morphism* from E to E' is a homomorphism $f\colon E \to E'$ of formal group schemes such that $fj = j'$ and $q'f = q$, so that the following diagram commutes:

$$\begin{array}{ccccc} \widehat{G}_a & \xrightarrow{j} & E & \xrightarrow{q} & G \\ \downarrow & & {\scriptstyle f}\downarrow & & \downarrow \\ \widehat{G}_a & \xrightarrow[j']{} & E' & \xrightarrow[q']{} & G. \end{array}$$

If we choose splittings r, s, r' and s' and define $g = sq' + jr'(1 - fsq')\colon E' \to E$ then one can check that $fg = 1_{E'}$ and $gf = 1_E$ so f is automatically an isomorphism. We write $\mathrm{Ext}(G, \widehat{G}_a)$ for the set of isomorphism classes of additive extensions of G.

LEMMA 20.11. *If E and E' are additive extensions of G then there is at most one morphism from E to E'.*

PROOF. Let $f_0, f_1\colon E \to E'$ be morphisms and put $\delta = f_0 - f_1$, so we need to show that $\delta = 0$. As $f_i j = j'$ and $q' f_i = q$ for $i = 0, 1$ we have $\delta j = 0$ and $q'\delta = 0$. Now put $\zeta = r'\delta s\colon G \to \widehat{G}_a$. As $1_E = sq + jr$ and $1_{E'} = s'q' + j'r'$ we have

$$\delta = (s'q' + j'r')\delta(sq + jr) = j'r'\delta sq = j'\zeta q.$$

As j' is monic and a homomorphism, and q is epic and a homomorphism, and $j'\zeta q$ is a homomorphism, it is not hard to check that ζ is a homomorphism. As $\mathrm{Hom}(G, \widehat{G}_a) = 0$ we see that $\zeta = 0$ so $\delta = 0$ as required. In fact, we do not need to show that ζ is a homomorphism but merely that $\zeta \circ p_G = p_{\widehat{G}_a} \circ \zeta$, as one sees easily from the proof of Lemma 20.7. This is easier so we will give the details. We claim that

$$j'\zeta p_G q = j'\zeta q p_E = p_{E'} j'\zeta q = j' p_{\widehat{G}_a} \zeta q.$$

The three equalities use the fact that q, $j'\zeta q = \delta$ and j' respectively are homomorphisms. As j' is mono and q is epi we conclude that $\zeta p_G = p_{\widehat{G}_a}\zeta$ as required. □

DEFINITION 20.12. We write

$$\begin{aligned} Z(G) = \{\sigma\colon G \times_X G \to \widehat{G}_a \mid \sigma(u,v) = \sigma(v,u)\ ,\ \sigma(u,0) = 0\ ,\\ \sigma(v,w) - \sigma(u+v,w) + \sigma(u,v+w) - \sigma(u,v) = 0\} \\ C(G) = \{\tau\colon G \to \widehat{G}_a \mid \tau(0) = 0\}. \end{aligned}$$

We also define a map $\delta\colon C(G) \to Z(G)$ by

$$\delta(\tau)(u,v) = \tau(u+v) - \tau(u) - \tau(v).$$

We call $Z(G)$ the group of symmetric two-cocycles on G with values in $\widehat{G}_a$.

REMARK 20.13. The case $v = w = 0$ of the cocycle identity $\sigma(v,w) - \sigma(u+v,w) + \sigma(u,v+w) - \sigma(u,v) = 0$ gives $\sigma(u,0) = \sigma(0,0)$. Thus, it would be equivalent to replace the condition $\sigma(u,0) = 0$ by $\sigma(0,0) = 0$ in Definition 20.12.

REMARK 20.14. It is clear that $\delta\colon C(G) \to Z(G)$ is a homomorphism of $\mathcal{O}_X$-modules. The kernel is $\mathrm{Hom}(G, \widehat{G}_a) = 0$, so δ is injective. We may thus think of $\delta C(G)$ as a subgroup of $Z(G)$ and define the quotient module $Z(G)/\delta C(G)$.

DEFINITION 20.15. Given $\sigma \in Z(G)$ we define $E_\sigma = \widehat{G}_a \times G$ with group operation

$$(a,u) + (b,v) = (a + b - \sigma(u,v), u+v).$$

(The inverse of (a,u) is $(-a + \sigma(u,-u), -u)$.) We also define $\widehat{G}_a \xrightarrow{j} E_\sigma \xrightarrow{q} G$ and $\widehat{G}_a \xleftarrow{r} E_\sigma \xleftarrow{s} G$ by

$$\begin{aligned} j(a) &= (a,0) \\ s(u) &= (0,u) \\ q(a,u) &= u \\ r(a,u) &= a. \end{aligned}$$

One can check directly that this gives an additive extension of G. We define a map $\theta\colon Z(G) \to \mathrm{Ext}(G, \widehat{G}_a)$ by $\theta(\sigma) = E_\sigma$.

PROPOSITION 20.16. *The map θ induces a bijection $Z(G)/\delta C(G) \simeq \mathrm{Ext}(G, \widehat{G}_a)$.*

PROOF. First, suppose we have two symmetric cocycles σ and σ' with $\sigma - \sigma' = \delta(\tau)$. One can then check that the map $f(a,u) = (a + \tau(u), u)$ gives an isomorphism of extensions $E_\sigma \simeq E_{\sigma'}$, so that $\theta(\sigma) = \theta(\sigma') \in \mathrm{Ext}(G, \widehat{G}_a)$. Thus, θ induces a map $\overline{\theta}\colon Z(G)/\delta C(G) \to \mathrm{Ext}(G, \widehat{G}_a)$.

Now suppose instead that we have symmetric cocycles σ and σ' and an isomorphism of extensions $f\colon E_\sigma \to E_{\sigma'}$. Define $\tau = r'fs\colon G \to \widehat{G}_a$ (using the usual splittings of E_σ and $E_{\sigma'}$). It is easy to see that $\tau(0) = 0$ so that $\tau \in C(G)$. As $q'f = q$ we have $f(0,u) = (\tau(u), u)$. As $fj = j'$ we have $f(a,0) = (a,0)$. As $(a,u) = (a,0) + (0,u)$ we have $f(a,0) = (a,0) + (\tau(u), u) = (a + \tau(u), u)$. This gives $f((0,u) + (0,v)) = f(-\sigma(u,v), u+v) = (\tau(u+v) - \sigma(u,v), u+v)$. On the other hand we have $f((0,u)+(0,v)) = f(0,u) + f(0,v) = (\tau(u) + \tau(v) - \sigma'(u,v), u+v)$. By comparing these answers we see that $\sigma - \sigma' = \delta(\tau)$. It follows easily that our map $\overline{\theta}\colon Z(G)/\delta C(G) \to \mathrm{Ext}(G, \widehat{G}_a)$ is injective.

Finally, suppose we start with an additive extension E'. Choose splittings r' and s' in the usual way and define $\sigma(u,v) = r'(s'(u+v) - s'(u) - s'(v))$. We know that $q'\colon E' \to G$ is a homomorphism with $q's' = 1$ so $q'(s'(u+v) - s'(u) - s'(v)) = 0$ and $j'r' = 1 - s'q'$ so we see that

$$j'\sigma(u,v) = (1 - s'q')(s'(u+v) - s'(u) - s'(v)) = s'(u+v) - s'(u) - s'(v).$$

From this it follows that $j'\sigma$ satisfies the symmetric cocycle conditions and j' is a monomorphism so σ satisfies the conditions, so $\sigma \in Z(G)$. We define $f\colon E_\sigma \to E'$ by $f(a,u) = j'(a) + s'(u)$. One can check directly that this is an isomorphism of extensions, so that the isomorphism class of E' lies in the image of $\overline{\theta}$. It now follows that $\overline{\theta}$ is an isomorphism. □

REMARK 20.17. If we choose a coordinate x on G (giving a formal group law $F(x,y)$) then $Z(G)$ becomes the set of power series $\sigma(x,y)$ such that $\sigma(x,y) = \sigma(y,x)$ and $\sigma(x,0) = 0$ and

$$\sigma(y,z) - \sigma(x +_F y, z) + \sigma(x, y +_F z) - \sigma(x,y) = 0.$$

LEMMA 20.18. *For any formal group law F over any ring R and any $k \geq 2$ there is a naturally defined symmetric cocycle $\sigma_k(F)(x,y)$ such that $\sigma_k(F)(x,y) = c_k(x,y) + O(k+1)$.*

PROOF. Recall from Theorem 7.2 that the Lazard ring L is a polynomial ring on generators a_j for $j \geq 2$. The formal group law F over R corresponds to a ring map $\phi\colon L \to R$, sending a_j to α_j say. Define $R' = R[\epsilon]/\epsilon^2$. Let $\phi'\colon L \to R'$ be the map that sends a_k to $\alpha_k + \epsilon$ and sends a_j to α_j for $j \neq k$. Let F' be the formal group law over R' coming from ϕ', so $F' = F \pmod{\epsilon}$, so $(x +_{F'} y) -_F x -_F y$ has the form $\epsilon\sigma(x,y)$ for some series $\sigma \in R[\![x,y]\!]$. It is easy to see that this is symmetric and $\sigma(x,0) = 0$. Next note that when $x = x' \pmod{\epsilon}$ we have $\epsilon\sigma(x,y) = \epsilon\sigma(x',y)$, because $\epsilon^2 = 0$. We also have $\epsilon u +_F \epsilon v = \epsilon(u+v)$. It follows that

$$x +_{F'} y +_{F'} z = x +_F y +_F z +_F \epsilon(\sigma(x,y) + \sigma(x +_F y, z)).$$

Using the commutativity and associativity of F and F' it is easy to conclude that σ is a symmetric cocycle. We define $\sigma_k(F) = \sigma$.

We now need to prove that $\sigma(x,y) = c_k(x,y) + O(k+1)$. It will suffice to do this for the universal formal group law over L. We give L its usual grading and then give $L'[\![x,y]\!]$ the grading extending this such that ϵ is homogeneous of degree $k-1$ and x and y are homogeneous of degree -1. With these gradings one can check that $F(x,y)$ and $F'(x,y)$ are homogeneous of degree -1 and thus that $\sigma(x,y)$ is homogeneous of degree $-k$. This means that $\sigma(x,y) = \sum_{ij} b_{ij}x^iy^j$ where $b_{ij} \in L$ is homogeneous of degree $k-i-j$. This means that $b_{ij} = 0$ when $i+j < k$ and that $b_{ij} \in \mathbb{Z}$ when $i+j = k$. Define $\sigma'(x,y) = \sum_{i+j=k} b_{ij}x^iy^j$. All that is left is to show that $\sigma'(x,y) = c_k(x,y)$. For this we note that $\sigma' = \sigma_k(F_a)$, where $F_a(x,y) = x+y$ is the additive formal group law. One can see from the construction in Proposition 6.3 and the definition of a_k that $\sigma_k(F_a) = c_k$ as required. □

We leave the proof of the next two lemmas to the reader.

LEMMA 20.19. *If F is a formal group law over R and $\sigma(x,y)$ is a symmetric cocycle for F and $\sigma(x,y) = 0 + O(k)$ then there is a unique $a \in R$ such that $\sigma(x,y) = ac_k(x,y) + O(k+1)$.* □

LEMMA 20.20. *We have $\delta(x^k) = b_k(x,y) + O(k+1)$, where $b_k(x,y) = (x+y)^k - x^k - y^k = \nu(k)c_k(x,y)$.* □

Now let G be a formal group over X of W-height n. It follows from Theorem 11.11 that we can choose a coordinate x on G_{red} such that the resulting formal group law is additive to order $p^n - 1$. The map $\mathcal{O}_G \to \mathcal{O}_{G_{\mathrm{red}}}$ is clearly surjective, so we can choose a coordinate on G extending x; we call this coordinate x also. If $x +_F y = x + y + \sum_{ij} a_{ij}x^iy^j$ and $I = (p) + (a_{ij} \mid i+j < p^n)$ we find that I is nilpotent and that there is an element $u \in \mathcal{O}_X$ such that $x +_F y = x + y + uc_{p^n}(x,y) + O(p^n+1) \pmod{I}$. We see from Lemma 11.6 that $[p]_F(x) = -ux^{p^n} + O(p^n+1) \pmod{I}$; as G has W-height n we deduce that u is a unit in $\mathcal{O}_X$. We now see that

$$\delta(x^{p^r}) = (x +_F y)^{p^r} - x^{p^r} - y^{p^r} = u^{p^r}c_{p^{n+r}}(x,y) + O(p^{n+r}+1) \pmod{I}.$$

PROPOSITION 20.21. *The group $\mathrm{Ext}(G, \widehat{G}_a)$ is a free module of rank $n-1$ over $\mathcal{O}_X$. If x is a coordinate as above and F is the resulting formal group law then $\{\sigma_{p^r}(F)(x,y) \mid 1 \leq r \leq n-1\}$ is a basis for $\mathrm{Ext}(G, \widehat{G}_a)$.*

PROOF. Write $R = \mathcal{O}_X$, and let $u \in R^\times$ be as in the preceeding discussion. For $k \geq 2$ we define $\tau_k(x,y) \in Z(G)$ by

$$\tau_k(x,y) = \begin{cases} \delta(x^k/\nu(k)) & \text{if } k \text{ is not a power of } p \\ \delta((x/u)^{p^{r-n}}) & \text{if } k = p^r \geq p^n \\ \sigma_{p^r}(F)(x,y) & \text{if } k = p^r < p^n. \end{cases}$$

Note that $\tau_k(x,y) = c_k(x,y) + O(k+1) \pmod{I}$ for all k.

For any R-module M we let $Z(G;M)$ denote the set of formal power series $\sigma(x,y) \in M[\![x,y]\!]$ that satisfy the symmetric cocycle conditions. Define a map $\theta_M\colon \prod_{k\geq 2} M \to Z(G;M)$ by $\theta(m) = \sum_k m_k\tau_k$ (one can

check that this converges, because $\delta(x^k) = 0 + O(k)$ for all k). One can check using Lemma 20.19 that θ_M is an isomorphism when $IM = 0$. As in the proof of Proposition 17.2, we deduce that θ_{R/I^k} is iso for all k and thus that θ_R is iso. This implies that

$$Z(G) = R\{\sigma_p(F), \dots, \sigma_{p^{n-1}}(F)\} \oplus \delta(C(G))$$

and thus that

$$\mathrm{Ext}(G, \widehat{G}_a) = Z(G)/\delta(C(G)) = R\{\sigma_p, \dots, \sigma_{p^{n-1}}\}.$$

□

Definition 20.22. Given a formal group scheme H of dimension d over X, we define $J = J_H = \{f \in \mathcal{O}_H \mid f(0) = 0\}$ and $\omega_H = J/J^2$ and $t_H = \mathrm{Hom}_{\mathcal{O}_X}(\omega_H, \mathcal{O}_X)$. It is easy to see that ω_H and t_H are free modules of rank d over $\mathcal{O}_X$. Moreover, a map $q\colon G \to H$ induces a map $q_*\colon t_G \to t_H$ provided only that $q(0) = 0$; we do not need q to be a homomorphism.

Definition 20.23. Let $\widehat{G}_a \xrightarrow{j} E \xrightarrow{q} G$ be an additive extension. A *rigidification* of this extension is a pair of maps $\mathcal{O}_X = t_{\widehat{G}_a} \xleftarrow{r_0} t_E \xleftarrow{s_0} t_G$ such that $r_0 j_* = 1$ and $q_* s_0 = 1$ and $j_* r_0 + s_0 q_* = 1$.

Exercise 20.24. Show that if $r_0\colon t_E \to \mathcal{O}_X$ satisfies $r_0 j_* = 1$ then there is a unique map $s_0\colon t_G \to t_E$ such that (r_0, s_0) is a rigidification. Similarly, show that if s_0 satisfies $q_* s_0 = 1$ then there is a unique r_0 such that (r_0, s_0) is a rigidification.

Exercise 20.25. Show that if (r_0, s_0) is a rigidification and $u \in \omega_G = \mathrm{Hom}_{\mathcal{O}_X}(t_G, \mathcal{O}_X)$ then $(r_0 + j_* u, s_0 - u q_*)$ is another rigidification, and this construction gives a bijection between ω_G and the set of rigidifications.

Exercise 20.26. Given a rigidification (r_0, s_0), there is a splitting (r, s) such that $r_0 = r_*$ and $s_0 = s_*$.

Definition 20.27. A *rigidified additive extension* of G is an additive extension with a specified rigidification. An *isomorphism of rigidified extensions* is an isomorphism $f\colon E \to E'$ of extensions such that $r'_0 \circ f_* = r_0$ and $f_* \circ s_0 = s'_0$. We write $M(G) = \mathrm{Ext}_{\mathrm{rig}}(G, \widehat{G}_a)$ for the set of isomorphism classes of rigidified additive extensions of G. This is also called the *Dieudonné module* of G.

Exercise 20.28. Prove that there is a natural short exact sequence

$$\omega_G \to \mathrm{Ext}_{\mathrm{rig}}(G, \widehat{G}_a) \to \mathrm{Ext}(G, \widehat{G}_a),$$

so that $\mathrm{Ext}_{\mathrm{rig}}(G, \widehat{G}_a)$ is a free $\mathcal{O}_X$-module of rank n.

Exercise 20.29. Define

$$C_{\mathrm{rig}}(G) = \{\tau\colon G \to \widehat{G}_a \mid \tau(0) = 0 \text{ and } \tau_* = 0\colon t_G \to \mathcal{O}_X\}.$$

Prove that

$$\mathrm{Ext}_{\mathrm{rig}}(G, \widehat{G}_a) = Z(G)/\delta C_{\mathrm{rig}}(G) = \mathcal{O}_X\{\sigma_p(F), \dots, \sigma_{p^n}(F)\}.$$

Definition 20.30. For any $\mathcal{O}_X$-algebra R we put

$$\widetilde{E}(R) = \{(a, u) \in \mathrm{Hom}_{\mathcal{O}_X}(Z(G), \mathrm{Nil}(R)) \times G(R) \mid a(\delta(\tau)) = \tau(u) \text{ for all } \tau \in C(G)\}.$$

We define addition on this set by

$$(a, u) + (b, v) = (a + b + \epsilon(u, v), u + v),$$

where $\epsilon(u, v)\colon Z(G) \to R$ is defined by $\epsilon(u, v)(\sigma) = \sigma(u, v)$.

We will now construct a "universal additive extension" $\widetilde{E}$ of G, from which all additive extensions can be obtained by pushout. Here $\widetilde{E}$ itself is not actually an additive extension of G according to our definitions, because the kernel of the projection $\widetilde{E} \to G$ is not $\widehat{G}_a$ but rather a formal group isomorphic to $\widehat{G}_a^{n-1}$.

THEOREM 20.31. *The above definitions make $\widetilde{E}$ into a formal group scheme of dimension n over X, which fits naturally in an extension*

$$\mathrm{Hom}(\mathrm{Ext}(G,\widehat{G}_a),\widehat{G}_a) \to \widetilde{E} \to G.$$

The resulting short exact sequence of cotangent spaces is naturally identified with the sequence

$$\omega_G \to \mathrm{Ext}_{\mathrm{rig}}(G,\widehat{G}_a) \to \mathrm{Ext}(G,\widehat{G}_a).$$

In particular, this gives $\omega_{\widetilde{E}} \simeq \mathrm{Ext}_{\mathrm{rig}}(G,\widehat{G}_a) = M(G)$.

PROOF. The given rule does indeed give a binary operation on $\widetilde{E}(R)$, because we have

$$\begin{aligned}(a+b+\epsilon(u,v))(\delta(\tau)) &= a(\delta(\tau)) + b(\delta(\tau)) + \epsilon(u,v)(\delta(\tau)) \\ &= \tau(u) + \tau(v) + \delta(\tau(u,v)) = \tau(u+v).\end{aligned}$$

One can check directly from the definitions that this operation gives a commutative group structure on $\widetilde{E}(R)$, with unit element $(0,0)$ and inverses given by $-(a,u) = (-a-\epsilon(u,-u),-u)$. The projection $q\colon \widetilde{E} \to G$ is evidently a homomorphism, and the kernel is

$$\{(a,0) \mid a \in \mathrm{Hom}_{\mathcal{O}_X}(Z(G),\mathrm{Nil}(R)) \mid a(\delta(\tau)) = 0 \text{ for all } \tau \in C(G)\},$$

which is naturally identified with the group

$$\mathrm{Hom}_{\mathcal{O}_X}(Z(G)/\delta C(G),\mathrm{Nil}(R)) = \mathrm{Hom}(\mathrm{Ext}(G,\widehat{G}_a),\mathrm{Nil}(R)) = \mathrm{Hom}(\mathrm{Ext}(G,\widehat{G}_a),\widehat{G}_a)(R).$$

Now choose a coordinate on G, which gives a splitting

$$Z(G) = R\{\sigma_p,\dots,\sigma_{p^{n-1}}\} \oplus \delta(C(G))$$

as in Proposition 20.21. This gives a bijection $\widetilde{E}(R) \to \mathrm{Nil}(R)^{n-1} \times G(R)$ by

$$(a,u) \mapsto (a(\sigma_p(F)),\dots,a(\sigma_{p^{n-1}}(F)),u).$$

We can make the target into a group by the rule

$$(a_1,\dots,a_{n-1},u) + (b_1,\dots,b_{n-1},v) = (a_1+b_1+\sigma_p(F)(u,v),\dots,a_{n-1}+b_{n-1}+\sigma_{p^{n-1}}(F)(u,v),u+v),$$

and then our bijection becomes an isomorphism. Using this it is easy to give a nonadditive splitting of the sequence

$$\mathrm{Hom}(\mathrm{Ext}(G,\widehat{G}_a),\widehat{G}_a) \to \widetilde{E} \to G.$$

All that is left is to identify the cotangent space $\omega_{\widetilde{E}}$. Consider an $\mathcal{O}_X$-linear map $f\colon Z(G)/\delta C_{\mathrm{rig}}(G) \to \mathcal{O}_X$. We define a ring map

$$\chi_f\colon \mathcal{O}_G = \mathcal{O}_X \oplus C(G) \to \mathcal{O}_X[\epsilon]/\epsilon^2$$

by $\chi_f(r,\tau) = r + \epsilon f(\delta(\tau))$. This defines a section u_f of G over $\mathrm{spec}(\mathcal{O}_X[\epsilon]/\epsilon^2)$ which restricts to zero on X. Now let a_f be the composite

$$Z(G) \to Z(G)/\delta C_{\mathrm{rig}}(G) \xrightarrow{f} \mathcal{O}_X \xrightarrow{\times\epsilon} \mathcal{O}_X[\epsilon]/\epsilon^2.$$

For any $\tau \in C(G)$ we have $\tau(u_f) = \chi_f(\tau) = \epsilon f(\delta(\tau)) = a_f(\tau)$, so $(a_f,u_f) \in \widetilde{E}(\mathcal{O}_X[\epsilon]/\epsilon^2)$. This reduces modulo ϵ to zero, so it defines an element $\alpha_f \in t_{\widetilde{E}}$. One can check directly that this construction gives an isomorphism

$$\mathrm{Hom}_{\mathcal{O}_X}(M(G),\mathcal{O}_X) = \mathrm{Hom}_{\mathcal{O}_X}(Z(G)/\delta C_{\mathrm{rig}}(G),\mathcal{O}_X) \to t_{\widetilde{E}}$$

and dually an isomorphism $\omega_{\widetilde{E}} \to M(G)$. □

We now give another description of the module $M(G)$ which is sometimes useful. We will formulate the first step for formal groups of arbitrary dimension, purely so that we can treat $G \times_X G$ on the same footing as G.

DEFINITION 20.32. Given any formal group scheme G of dimension d over X we define $\Omega_{G/X}$ as before (so this is a free module of rank d over $\mathcal{O}_G$). We then let $\Omega^k_{G/X}$ denote the k'th exterior power of $\Omega_{G/X}$ over $\mathcal{O}_G$, and define a formal de Rham differential $d\colon \Omega^k_{G/X} \to \Omega^{k+1}_{G/X}$ by the usual rule

$$d(f_0 df_1 \wedge \cdots \wedge df_k) = df_0 \wedge df_1 \wedge \cdots \wedge df_k.$$

This satisfies $d^2 = 0$ so we can define the cohomology groups $H^*_{dR}(G/X) = H^*(\Omega^\bullet_{G/X})$; these are contravariantly functorial in G. Next, we have natural maps $d_i\colon G \times_X G \to G$ for $i = 0, 1, 2$ given by $d_0(u, v) = v$ and $d_1(u, v) = u + v$ and $d_2(u, v) = u$, which induce map $d_i^*\colon H^*_{dR}(G) \to H^*_{dR}(G \times_X G)$. We say that a class $\alpha \in H^*_{dR}(G)$ is *primitive* if $d_0^*(\alpha) - d_1^*(\alpha) + d_2^*(\alpha) = 0$. We write $\mathrm{Prim}(H^*_{dR}(G/X))$ for the subgroup of primitives (which is naturally an $\mathcal{O}_X$-module).

We now revert to the case where G is a one-dimensional group of Weierstrass height $n < \infty$.

We next want to define a map $\phi\colon Z(G) \to \mathrm{Prim}(H^1_{dR}(G/X))$. Let J be the ideal in $\mathcal{O}_{G\times_X G}$ of functions that vanish on the diagonal, so that $\Omega_{G/X} = J/J^2$. Given $\sigma \in Z(G)$, put $\widetilde{\alpha}(u, u') = \sigma(u, u' - u)$, so $\widetilde{\alpha} \in J$, and let α be the image of $\widetilde{\alpha}$ in $\Omega_{G/X}$.

LEMMA 20.33. *If I is the ideal in $\mathcal{O}_{G\times_X G}$ defining the zero section, then $Z(G) \leq I^2$.*

PROOF. Let I_0 and I_1 be the ideals defining $0 \times G$ and $G \times 0$ respectively. From the definitions it is clear that $Z(G) \leq I_0 \cap I_1$ and $I_0, I_1 \leq I$ so it will suffice to prove that $I_0 \cap I_0 = I_0 I_1$. This is clear after we choose a coordinate giving $\mathcal{O}_{G\times_X G} = \mathcal{O}_X[\![x_0, x_1]\!]$ with $I_0 = (x_0)$ and $I_1 = (x_1)$. □

LEMMA 20.34. *We have $d_0^*\alpha - d_1^*\alpha + d_2^*\alpha = d\sigma \in \Omega_{G\times_X G/X}$. In particular, the left hand side is a coboundary, so $[\alpha] \in \mathrm{Prim}(H^1_{dR}(G/X))$.*

PROOF. Let J' be the ideal of functions f on G^4_X that satisfy $f(u, v, u, v) = 0$, so $\Omega_{G\times_X G/X} = J'/(J')^2$. The form $d\sigma$ is represented by the function $\lambda \in J'$ given by $\lambda(u, v, u', v') = \sigma(u, v) - \sigma(u', v')$, or equivalently

$$\lambda(u, v, u + x, v + y) = \sigma(u, v) - \sigma(u + x, v + y).$$

The form $\sum_j (-1)^j d_j^*\alpha$ is represented by the function $\mu \in J'$ given by

$$\begin{aligned}\mu(u, v, u + x, v + y) &= \widetilde{\alpha}(v, v + y) - \widetilde{\alpha}(u + v, u + v + x + y) - \widetilde{\alpha}(u, u + x)\\ &= \sigma(v, y) - \sigma(u + v, x + y) + \sigma(u, x).\end{aligned}$$

Let $R(a, b, c)$ denote the cocycle identity

$$\sigma(b, c) - \sigma(a + b, c) - \sigma(a, b + c) + \sigma(a, b) = 0.$$

After expanding and cancelling the identity

$$R(u, x, v + y) - R(u, v, x + y) - R(x, v, y) + R(v, x, y)$$

we find that

$$\mu(u, v, u + x, v + y) - \lambda(u, v, u + x, v + y) = \sigma(x, y).$$

Here $\sigma \in I^2$ by Lemma 20.33, and it follows that $\mu - \lambda \in (J')^2$ as required. □

It is now clear that the construction $\sigma \mapsto [\alpha]$ gives a homomorphism $Z(G) \to \mathrm{Prim}(H^1_{dR}(G/X))$. It will be useful to control the target of this map more precisely.

DEFINITION 20.35. We put

$$Z'(G) = \{\alpha \in \Omega_{G/X} \mid \alpha|_X = 0,\ [\alpha] \in \mathrm{Prim}(H^1_{dR}(G))\}.$$

PROPOSITION 20.36. *The construction $\sigma \mapsto \alpha$ gives a homomorphism $\phi\colon Z(G) \to Z'(G)$ fitting into a diagram as follows:*

$$\begin{array}{ccccc} C_{\mathrm{rig}}(G) & \xrightarrow{\delta} & Z(G) & \twoheadrightarrow & \mathrm{Ext}^1_{\mathrm{rig}}(G, \widehat{G}_a) \\ \downarrow{\scriptstyle -1} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ C_{\mathrm{rig}}(G) & \xrightarrow[d]{} & Z'(G) & \twoheadrightarrow & \mathrm{Prim}(H^1_{dR}(G/X)). \end{array}$$

The top row is a splittable short exact sequence, and the bottom row is right exact.

PROOF. We have seen previously that the top row is a splittable short exact sequence. Now consider an element $\sigma \in Z(G)$ and define $\widetilde{\alpha}(u, u+x) = \sigma(u, x)$ and $\phi(\sigma) = \alpha$ as before. Note that $\widetilde{\alpha}(0, x) = \sigma(0, x) = 0$, so $\alpha|_X = 0$. Given this and Lemma 20.34 we see that $\alpha \in Z'(G)$, so we have a homomorphism $\phi\colon Z(G) \to Z'(G)$ as indicated. Now consider the case $\sigma = \delta\tau$ for some $\tau \in C_{\mathrm{rig}}(G)$. We then have $\widetilde{\alpha}(u, u+x) = (\delta\tau)(u, x) = \tau(u+x) - \tau(u) - \tau(x)$, whereas $d\tau$ is represented by the function $(u, u+x) \mapsto \tau(u) - \tau(u+x)$. The condition $\tau \in C_{\mathrm{rig}}(G)$ means that τ vanishes to second order at the identity and thus that the term $\tau(x)$ can be neglected when we project to $\Omega_{G/X}$. It follows that $\phi(\delta(\tau)) = -d\tau$, so the left hand square commutes.

We now prove that the bottom row is right exact. It is clear that $dC_{\mathrm{rig}}(G) \leq Z'(G)$ and that the construction $\alpha \mapsto [\alpha]$ gives a homomorphism $Z'(G)/dC_{\mathrm{rig}}(G) \to \mathrm{Prim}(H^1_{dR}(G/X))$; we claim that this is an isomorphism. For the proof it is convenient to choose a coordinate x on G, and to let Dx denote the unique element in $\mathrm{Prim}(\Omega_{G/X})$ with $(Dx)|_X = (dx)|_X$ (as in Proposition 9.16). Consider an element $c \in \mathrm{Prim}(H^1_{dR}(G/X))$. Choose a representative form $\alpha \in \Omega_{G/X}$, let t be the scalar such that $\alpha|_X = t\,dx|_X$, and put $\alpha' = \alpha - t\,dx$. We find that α' is another representative of c lying in $Z'(G)$, so the map $Z'(G)/dC_{\mathrm{rig}}(G) \to \mathrm{Prim}(H^1_{dR}(G/X))$ is surjective. If $\alpha \in Z'(G)$ and $[\alpha] = 0$ then we must have $\alpha = d\tau$ for some $\tau \in \mathcal{O}_G$, and after subtracting a constant we may assume that $\tau \in C(G)$. The assumption $\alpha|_X = 0$ then forces $\tau \in C_{\mathrm{rig}}(G)$. It follows that our map is also injective.

Finally, as the left square commutes we have an induced map of cokernels, which gives $\phi\colon \mathrm{Ext}_{\mathrm{rig}}(G, \widehat{G}_a) \to \mathrm{Prim}(H^1_{dR}(G/X))$ as required. □

So far we have implicitly worked with a formal group G of finite Weierstrass height over an affine scheme X (which forces p to be nilpotent in $\mathcal{O}_X$). Our results extend more or less automatically to cover the case where X is a formal scheme where p is topologically nilpotent in $\mathcal{O}_X$, but need not be actually nilpotent. In that context it is possible for $\mathcal{O}_X$ to be torsion-free.

PROPOSITION 20.37. *If $\mathcal{O}_X$ is torsion-free then the map $\phi\colon Z(G) \to Z'(G)$ is an isomorphism, as is the induced map $\mathrm{Ext}_{\mathrm{rig}}(G, \widehat{G}_a) \to \mathrm{Prim}(H^1_{dR}(G/X))$.*

PROOF. The key point about the torsion-free case is that if $f \in \mathcal{O}_{G^r_X} \simeq \mathcal{O}_X[\![x_1, \dots, x_r]\!]$ and $df = 0$ then f is constant (i.e. it lies in the subring $\mathcal{O}_X$). This will be used several times.

Suppose that $\sigma \in Z(G)$ satisfies $\phi(\sigma) = 0$. Lemma 20.34 then gives $d\sigma = \sum_j (-1)^j d_j^* \phi(\sigma) = 0$, so σ is constant. We also have $\sigma(0, 0) = 0$ by the definition of $Z(G)$, so $\sigma = 0$. This proves that ϕ is injective.

Now suppose we start with $\alpha \in Z'(G)$. As the class $[\alpha]$ is primitive we must have $\sum_j (-1)^j d_j^* \alpha = d\sigma$ for some function $\sigma \in \mathcal{O}_{G \times_X G}$. After subtracting a constant we may assume that $\sigma(0, 0) = 0$, and then σ is uniquely determined. We claim that $\sigma \in Z(G)$. Indeed, using the uniqueness property we deduce that $\sigma(u, v) = \sigma(v, u)$. We next introduce maps

$$d_i\colon G \times_X G \times_X G \to G \times_X G$$

as follows:

$$d_0(u, v, w) = (v, w) \qquad d_1(u, v, w) = (u + v, w) \qquad d_2(u, v, w) = (u, v + w) \qquad d_3(u, v, w) = (u, v).$$

For the cocycle identity we must show that the function $\rho = \sum_i (-1)^i d_i^* \sigma \in \mathcal{O}_{G \times_X G \times_X G}$ is zero. As $\mathcal{O}_X$ is torsion-free and $\rho(0, 0, 0) = 0$ it will suffice to prove that $d\rho = 0$. Here d commutes with the operators d_i^* and $d\sigma = \sum_j (-1)^j d_j^* \alpha$ so $d\rho = \sum_{i,j} (-1)^{i+j} d_i^* d_j^* \alpha$. This is zero by a standard argument with simplicial identities, which can also be written out more explicitly if desired. Thus, σ satisfies the cocycle identity, and also the identity $\sigma(u, 0) = 0$ by Remark 20.13. Thus $\sigma \in Z(G)$ as claimed.

Now put $\beta = \phi(\sigma) \in Z'(G)$ and $\gamma = \alpha - \beta \in Z'(G)$. By the construction of σ we have $\sum (-1)^j d_j^* \alpha = d\sigma$, but by Lemma 20.34 we have $\sum (-1)^j d_j^* \beta = d\sigma$, so $\sum (-1)^j d_j^* \gamma = 0$. This means that $\gamma \in \mathrm{Prim}(\Omega_{G/X})$. We know from Proposition 9.16 that the map $\theta \mapsto \theta|_X$ gives an isomorphism $\mathrm{Prim}(\Omega_{G/X}) \to \omega_G$, but $\gamma \in Z'(G)$ so $\gamma|_X = 0$, so $\gamma = 0$. This means that $\alpha = \beta = \phi(\sigma)$, so ϕ is surjective and thus an isomorphism. It follows directly from Proposition 20.36 that the induced map $\mathrm{Ext}_{\mathrm{rig}}(G, \widehat{G}_a) \to \mathrm{Prim}(H^1_{dR}(G/X))$ is also an isomorphism. □

21. Curves and their operators

DEFINITION 21.1. Let G be a formal group over a scheme X. A *curve* on G just means a morphism $\gamma\colon \widehat{\mathbb{A}}^1 \times X \to G$ of formal schemes over X that preserves the zero sections. We write $\mathrm{Curves}(G)$ for the set of all curves on G, and we use the group structure of G to make this a group.

DEFINITION 21.2. We say that a curve γ is *basic* if the map $\gamma\colon \widehat{\mathbb{A}}^1 \times X \to G$ is an isomorphism. If so, the inverse map has the form $u \mapsto (x(u), \pi(u))$ for some coordinate x. By a slight abuse of language, we say that γ and x are inverse to each other.

To be explicit, a curve should be written as $\gamma(a,t)$ to indicate the dependence on $a \in X$ and $t \in \widehat{\mathbb{A}}^1$. However, we will often streamline the notation by omitting explicit mention of a.

DEFINITION 21.3. We define maps $\theta_a, v_m, f_n\colon \mathrm{Curves}(G) \to \mathrm{Curves}(G)$ (for $n, m \in \mathbb{N}^+$ and $a \in \mathcal{O}_X$) as follows.

(a) We define $(\theta_a\gamma)(t) = \gamma(at)$, or more explicitly $(\theta_a\gamma)(x,t) = \gamma(x, a(x)t)$ for $x \in X$ and $t \in \widehat{\mathbb{A}}^1$. These are called *homothety* operators.

(b) Similarly, we put $(v_m\gamma)(t) = \gamma(t^m)$, or $(v_m\gamma)(x,t) = \gamma(x,t^m)$. These are called *verschiebung* operators.

(c) The definition of f_n is more complicated. First, we let $f'_m\gamma\colon (\widehat{\mathbb{A}}^m/\Sigma_m) \times X \to G$ be the unique map making the right hand square below commute.

$$\begin{array}{ccccc}
\widehat{\mathbb{A}}^1 \times X & & \widehat{\mathbb{A}}^m \times X & \xrightarrow{\gamma^m} & G_X^m \\
{\scriptstyle i_m}\downarrow & & \downarrow & & \downarrow{\scriptstyle +} \\
\widehat{\mathbb{A}}^m \times X & \xleftarrow[\sigma]{\simeq} & (\widehat{\mathbb{A}}^m/\Sigma_m) \times X & \xrightarrow[f'_m\gamma]{} & G.
\end{array}$$

We then let $\sigma(t_1, \dots, t_m)$ be the list of elementary symmetric functions in the variables t_i, starting with $\sum_i t_i$ and ending with $\prod_i t_i$. This defines an isomorphism σ as shown. Next, we define $i_m(t) = (0, \dots, 0, (-1)^{m+1}t)$ and $f_m\gamma = (f'_m\gamma)\sigma^{-1}i_m$. These are called *frobenius* operators. (The connection with Frobenius morphisms as discussed previously is rather indirect, and will not be discussed until much later.)

REMARK 21.4. Suppose that $\mathcal{O}_X$ contains a primitive m'th root of unity ζ, so that $\prod_{i=0}^{m-1}(1-t\zeta^i) = 1-t^m$ in $\mathcal{O}_X[t]$. This means that the elementary symmetric functions of the vector $\zeta^*(t) = [t, \zeta t, \dots, \zeta^{m-1}t]$ are $0, \dots, 0, (-1)^{m+1}$. We can thus define $\psi^m\colon \widehat{\mathbb{A}}^1 \to \widehat{\mathbb{A}}^1$ by $\psi^m(t) = t^m$ and then enlarge the above diagram as follows:

$$\begin{array}{ccccccc}
\widehat{\mathbb{A}}^1 \times X & \xleftarrow{\psi^m} & \widehat{\mathbb{A}}^1 \times X & \xrightarrow{\zeta^*} & \widehat{\mathbb{A}}^m \times X & \xrightarrow{\gamma^m} & G_X^m \\
{\scriptstyle i_m}\downarrow & & & & \downarrow & & \downarrow{\scriptstyle +} \\
\widehat{\mathbb{A}}^m \times X & & \xleftarrow[\sigma]{\simeq} & & (\widehat{\mathbb{A}}^m/\Sigma_m) \times X & \xrightarrow[f'_m\gamma]{} & G.
\end{array}$$

Using this we find that $(v_m f_m\gamma)(t) = (f_m\gamma)(t^m) = \sum_{i=0}^{m-1}\gamma(\zeta^i t)$. Note that this characterises $f_m\gamma$, because the map ψ^m is an epimorphism of schemes. If $\mathcal{O}_X$ does not have a primitive m'th root of unity then we can just adjoin one by forming the ring $\mathcal{O}_X[\zeta]/\phi_m(\zeta)$ (where ϕ_m is the m'th cyclotomic polynomial) and the corresponding scheme X'. This is faithfully flat over X so most properties of f_m can be proved by changing base to X'.

EXAMPLE 21.5. Consider the case where $G = \widehat{G}_a \times X$, so $\mathrm{Curves}(G) = \{g(t) \in \mathcal{O}_X[\![t]\!] \mid g(0) = 0\}$, with group structure by ordinary addition. If $g(t) = \sum_{i>0} c_i t^i$, then

$$\begin{aligned}
(\theta_a g)(t) &= g(at) = \sum_{i>0} (c_i a^i) t^i \\
(v_n g)(t) &= g(t^n) = \sum_{i>0} c_i t^{ni} \\
(f_n g)(t^n) &= \sum_{i>0} c_i t^i \sum_{j=0}^{n-1} \zeta^{ij} = \sum_{k>0} n\, c_{nk} t^{nk} \\
(f_n g)(t) &= \sum_{k>0} n\, c_{nk} t^k.
\end{aligned}$$

PROPOSITION 21.6. *All the above operators respect addition in* $\mathrm{Curves}(G)$*, and they satisfy the following identities:*

$$\begin{aligned}
\theta_a \theta_b &= \theta_{ab} \\
v_n v_m &= v_{nm} \\
f_n f_m &= f_{nm} \\
f_n v_n &= n \\
f_n v_m &= v_m f_n \text{ if } (n,m) = 1 \\
f_n \theta_a &= \theta_{a^n} f_n \\
\theta_a v_n &= v_n \theta_{a^n}.
\end{aligned}$$

Moreover, we have $\theta_1 = v_1 = f_1 = id$.

PROOF. It is straightforward to check that all operators preserve addition and that $\theta_a\theta_b = \theta_{ab}$ and $v_n v_m = v_{nm}$ and $\theta_a v_n = v_n \theta_{a^n}$. Next, after making a faithfully flat base change if necessary, we may assume that $\mathcal{O}_X$ contains a primitive nm'th root of unity, say ξ. We then have

$$\begin{aligned}
(f_n f_m \gamma)(t^{nm}) &= \sum_{i=0}^{n-1} (f_m\gamma)(\xi^{mi} t^m) = \sum_{i=0}^{n-1} (f_m\gamma)((\xi^i t)^m) \\
&= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \gamma(\xi^{nj} \xi^i t) = \sum_{k=0}^{nm-1} \gamma(\xi^k t) = (f_{nm}\gamma)(t^{nm}).
\end{aligned}$$

It follows that $f_n f_m = f_{nm}$ as claimed. For the remaining identities we use the element $\zeta = \xi^m$, which is a primitive n'th root of unity. Next, we have

$$(f_n v_n \gamma)(t^n) = \sum_{i=0}^{m-1} (v_n\gamma)(\zeta^i t) = \sum_{i=0}^{m-1} \gamma(\zeta^{ni} t^n) = \sum_{i=0}^{m-1} \gamma(t^n) = n\gamma(t^n).$$

This gives $f_n v_n = n$. On the other hand, if m and n are coprime then the map $\zeta^i \mapsto \zeta^{mi}$ is bijective and so

$$(f_n v_m \gamma)(t^n) = \sum_{i=0}^{m-1} (v_m\gamma)(\zeta^i t) = \sum_{i=0}^{m-1} \gamma(\zeta^{mi} t^m) = \sum_{i=0}^{m-1} \gamma(\zeta^i t^m) = (v_m f_n \gamma)(t^n).$$

Finally, we have

$$(\theta_{a^n} f_n \gamma)(t^n) = (f_n\gamma)((at)^n) = \sum_{i=0}^{n-1} \gamma(\zeta^i a t) = \sum_{i=0}^{n-1} (\theta_a\gamma)(\zeta^i t) = (f_n \theta_a \gamma)(t^n).$$

This gives $f_n\theta_a = \theta_{a^n} f_n$ and completes the proof. □

REMARK 21.7. Suppose that n is invertible in $\mathcal{O}_X$. We then find that $n.1_G \colon G \to G$ is an isomorphism, and it follows that multiplication by n is an isomorphism on $\mathrm{Curves}(G)$.

REMARK 21.8. We can regard $\widehat{\mathbb{A}}^1$ as the colimit of the schemes $D_n = \operatorname{spec}(\mathbb{Z}[t]/t^{n+1})$, and this makes $\operatorname{Curves}(G)$ the inverse limit of the groups $\operatorname{Map}^0_X(D_n \times X, G)$. We give these groups the discrete topology, and then we give $\operatorname{Curves}(G)$ the inverse limit topology.

More concretely, we can choose a coordinate x on G. Then, for any curve γ there is a formal power series $g(t) \in \mathcal{O}_X[\![t]\!]$ such that $x(\gamma(t)) = g(t)$; this identifies $\operatorname{Curves}(G)$ with $t\,\mathcal{O}_X[\![t]\!]$, with group operation given by $+_F$. In this picture the topology on $\operatorname{Curves}(G)$ is just the t-adic topology.

We can use this topology to interpret various infinite sums of the operators in Definition 21.3.

DEFINITION 21.9. Let p be a prime number. A curve γ is *p-typical* if $f_m\gamma = 0$ for all $m > 1$ with $m \neq 0 \pmod p$. We write $\operatorname{Curves}_p(G)$ for the subgroup of p-typical curves.

REMARK 21.10. We also say that a curve γ is *additive* if it satisfies $\gamma(s+t) = \gamma(s) + \gamma(t)$. If so, it is easy to check that $f_m\gamma = 0$ for all $m > 1$, so that γ is p-typical for all p.

Until further notice, we will assume that $\mathcal{O}_X$ is a $\mathbb{Z}_{(p)}$-algebra for some prime p.

PROPOSITION 21.11. *The group* $\operatorname{Curves}_p(G)$ *is naturally a summand in* $\operatorname{Curves}(G)$.

PROOF. We define an operator

$$\epsilon = \prod_q (1 - q^{-1}v_q f_q) = \sum_n n^{-1}\mu(n) v_n f_n.$$

Here the product is indexed by all primes q different from p, and the sum is indexed by all positive integers $n \neq 0 \pmod p$. The function μ is the Möbius function, so $\mu(n) = (-1)^j$ if n is a product of j distinct primes, and $\mu(n) = 0$ if n is not square-free. It makes sense to multiply by q^{-1} or m^{-1} because of Remark 21.7. If we identify curves with power series as in Remark 21.8 then v_k is just the operator $g(t) \mapsto g(t^k) = 0 \pmod{t^k}$; it follows that the sum and the product are both convergent, and a straightforward argument shows that they are the same. As $f_q v_q = q$ we see that $q^{-1}v_q f_q$ is idempotent, and therefore the operator $\epsilon_q = 1 - q^{-1}v_q f q_q$ is also idempotent. We also see from Proposition 21.6 that these idempotents commute, and thus that ϵ is also idempotent. It is clear that if γ is p-typical then $\epsilon(\gamma) = \gamma$. Conversely, we have $f_q\epsilon_q = 0$ and so $f_q\epsilon = 0$ for all $q \neq p$, so $\epsilon(\gamma)$ is always p-typical. This shows that ϵ gives a natural retraction $\operatorname{Curves}(G) \to \operatorname{Curves}_p(G)$. □

EXAMPLE 21.12. Consider the case where $G = \widehat{G}_a \times X$ and γ corresponds to a series $g(t) = \sum_i c_i t^i$. Using Example 21.5 we see that $f_q\gamma = 0$ iff $c_{jq} = 0$ for all j, and thus that γ is p-typical iff $c_k = 0$ whenever k is not a power of p. In the general case we find that $(\epsilon g)(t) = \sum_i c_{p^i} t^{p^i}$, so ϵ is just the most obvious projector onto $\operatorname{Curves}_p(G)$.

DEFINITION 21.13. Consider a coordinate $x\colon G \to \widehat{\mathbb{A}}^1$. The map $(x, \pi)\colon G \to \widehat{\mathbb{A}}^1 \times X$ is then an isomorphism, with inverse $\gamma\colon \widehat{\mathbb{A}}^1 \times X \to G$ say. We say that x is a p-typical coordinate iff γ is a p-typical curve. We say that a formal group law F over $\mathcal{O}_X$ is p-typical iff the tautological coordinate on the formal group G_F is p-typical.

PROPOSITION 21.14. *Any formal group G (over a p-local base, by our standing assumption) admits a p-typical coordinate.*

PROOF. Choose any coordinate x, and let γ denote the inverse curve as in Definition 21.13. Put $\delta = \epsilon(\gamma)$, and note that this agrees with γ to first order, so it is also an isomorphism $\widehat{\mathbb{A}}^1 \times X \to G$. We can invert this and project to $\widehat{\mathbb{A}}^1$ to get a new coordinate y on G, which is easily seen to be p-typical. □

PROPOSITION 21.15. *Let x be a p-typical coordinate on G, and let γ be the inverse curve, and let δ be any other p-typical curve. Then there is a unique sequence of coefficients $a_i \in \mathcal{O}_X$ such that $\delta = \sum_{i=0}^{\infty} v_p^i \theta_{a_i}\gamma$, or equivalently $\delta(t) = \sum_{i\geq 0} \gamma(a_i t^{p^i})$.*

PROOF. Put $g(t) = x(\delta(t)) \in \mathcal{O}_X[\![t]\!]$. Suppose that this has the form $g(t) = a\,t^d \pmod{t^{d+1}}$ with $a \neq 0$. We claim that d is a power of p. If not, we can choose a prime $q \neq p$ dividing d and apply x to the identity

$v_q f_q \delta = 0$ to get

$$0 = \sum_{0 \leq i < q}^{F} x(\delta(\zeta^i t)) = \sum_{0 \leq i < q}^{F} g(\zeta^i t) = qat^d \pmod{t^{d+1}},$$

which contradicts the assumption $a \neq 0$. We thus have $d = p^i$ for some i, and it follows that $\delta - v_{p^i}\theta_a\gamma$ vanishes to order strictly greater than d. The proposition follows by a standard argument of successive approximation. □

PROPOSITION 21.16. *Let G be a formal group over a base X such that $\mathcal{O}_X$ is an algebra over $\mathbb{Z}_{(p)}$, and let α be a generator for ω_G. Then there is a canonical additive curve η on G with $\eta^*\alpha = p\, d_0 t$. In terms of a suitable coordinate this is given by $x(\eta(t)) = \exp_F(pt)$.*

PROOF. Choose a coordinate x with $\alpha = d_0 x$, and let γ be the inverse curve, so $\gamma^*\alpha = d_0 t$. Put $\delta = \epsilon(\gamma)$, so δ is p-typical and $\delta^*\alpha = d_0 t$. Put $\eta = (p - v_p f_p)\delta$. We claim that this is additive and independent of the choice of x, and that $\eta^*\alpha = p\, d_0 t$.

To prove this, let y be the p-typical coordinate inverse to δ, and let F be the corresponding formal group law. We then have

$$y(\eta(t)) = [p]_F(y(t)) -_F y((f_p\delta)(t^p)) = pt \pmod{t^2},$$

which gives $\eta^*\alpha = p\,\delta^*\alpha = p\, d_0 t$.

Now let δ' be another p-typical curve with $(\delta')^*\alpha = d_0 t$. By Proposition 21.15 we have $\delta' = \sum_{i=0}^{\infty} v_p^i \theta_{a_i} \delta$ for some list of coefficients a_i, and the condition on α implies that $a_0 = 1$. As $f_p v_p = p$ we see that $(p - v_p f_p) v_p^i \theta_{a_i} \delta = 0$ and so $(p - v_p f_p)\delta' = (p - v_p f_p)\delta$, so η is well-defined.

All that is left is to show that η is additive. If $\mathcal{O}_X$ is a $\mathbb{Q}$-algebra then (by the theory of logarithms) we can take x to be an additive coordinate, and we then find that $\delta = \gamma$ and $f_p\delta = f_p\gamma = 0$ so $\eta = p\,\gamma$, which is certainly additive. For general X we can apply the previous case to see that η becomes additive over $\mathbb{Q} \otimes \mathcal{O}_X$. If $\mathcal{O}_X$ is torsion-free this implies easily that η itself is additive. In particular, as the Lazard ring is torsion-free we see that η is additive in the case of the universal FGL, and it follows by base change that it is additive for any formal group. □

PROPOSITION 21.17. *Let γ be any p-typical basic curve on G, inverse to a coordinate x. Let η be the canonical additive curve such that $\eta^* d_0 x = p\, d_0 t$. Then there is a unique series of elements $u_k \in \mathcal{O}_X$ (for $k > 0$) such that*

$$p\,\gamma(t) = \eta(t) + \sum_{k>0} \gamma(u_k t^{p^k}).$$

PROOF. We have a p-typical curve $\beta(t) = p\,\gamma(t) - \eta(t)$, which satisfies $\beta^*\alpha = 0$. We can use Proposition 21.15 to expand β as $\beta(t) = \sum_k \gamma(u_k t^{p^k})$, and then by considering the effect on $d_0 x$ we get $u_0 = 0$, so this rearranges to give $p\gamma(t) = \eta(t) + \sum_{k>0} \gamma(u_k t^{p^k})$ as claimed. □

REMARK 21.18. If we let F be the formal group law such that $\gamma(s) + \gamma(t) = \gamma(s +_F t)$, and apply x to the equation displayed above, we get

$$[p]_F(t) = \exp_F(pt) +_F \sum_{k>0}^{F} u_k t^{p^k},$$

which is how things are more commonly written in the literature. The elements u_k are called the *Hazewinkel parameters* of (G, γ) or of F.

22. Witt vectors

Let R be a ring. In this section we will define and study a ring $W(R)$ called the *big Witt ring* of R. This is naturally compared with two other rings $NW(R)$ and $GW(R)$ which are easier to define and which have natural maps $NW(R) \xrightarrow{i} W(R) \xrightarrow{w_*} GW(R)$.

DEFINITION 22.1. The *ghost Witt ring* $GW(R)$ is just $\mathrm{Map}(\mathbb{N}^+, R)$ (where $\mathbb{N}^+$ is the set of strictly positive integers). We consider this as a ring under pointwise operations. For each integer $n > 0$ we define $F_n, V_n \colon GW(R) \to GW(R)$ by

$$(F_n u)(m) = u(nm)$$
$$(V_n u)(m) = \begin{cases} n\, u(m/n) & \text{if } n \mid m \\ 0 & \text{otherwise.} \end{cases}$$

REMARK 22.2. It is clear that F_n is a ring map and that $F_n F_m = F_{nm}$ and that $F_n V_n u = n\, u$. However, V_n is not a ring map, but it is additive and satisfies a reciprocity formula $x\, V_n(y) = V_n(F_n(x)y)$.

DEFINITION 22.3. The *naive Witt ring* $NW(R)$ is the free abelian group on elements $\tau(a)$ for $a \in R$, subject only to the relation $\tau(0) = 0$. This has an evident ring structure given by the rule $\tau(a)\tau(b) = \tau(ab)$. For each $n > 0$ there is a natural ring endomorphism $F_n \colon NW(R) \to NW(R)$ given by $F_n\tau(a) = \tau(a^n)$. If R is an algebraically closed field of characteristic 0, then we can also define $V_n \colon NW(R) \to NW(R)$ by $V_n\tau(a) = \sum_{b^n=a} \tau(b)$. This is not a ring map but satisfies a reciprocity formula $x\, V_n(y) = V_n(F_n(x)y)$. We also have a ring map $w_n = w_1 F_n \colon NW(R) \to R$ given by $w_n\tau(a) = a^n$. By combining these we get a ring map $w_* \colon NW(R) \to GW(R)$ defined by $w_*(\tau(a))(n) = w_n(a)$.

The genuine Witt ring $W(R)$ will also have operators V_n and F_n, and maps $R \xrightarrow{\tau} W(R) \xrightarrow{w_n} R$, with formal properties similar to the naive versions (except that V_n will be defined for all rings R, not just for algebraically closed fields of characteristic 0). One can think of $W(R)$ as a kind of completion of a sheafification of $NW(R)$.

DEFINITION 22.4. As a set, $W(R)$ is just $\mathrm{Map}(\mathbb{N}^+, R)$. However, the ring operations are not the obvious ones, and will be introduced later. We give $W(R)$ the product topology deduced from the discrete topology on R.

We define maps

$$R \xrightarrow{\tau} W(R) \xrightarrow{V_n} W(R) \xrightarrow{w_m} R$$

by

$$\tau(u)(n) = \begin{cases} u & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$
$$V_n(a)(m) = \begin{cases} a(m/n) & \text{if } n \mid m \\ 0 & \text{otherwise} \end{cases}$$
$$w_n(a) = \sum_{d \mid n} d\, a(d)^{n/d}.$$

We also define $w_* \colon W(R) \to GW(R)$ by $w_*(a)(n) = w_n(a)$ for all $n > 0$. Maps $F_n \colon W(R) \to W(R)$ will be introduced later.

Now consider a subset $U \subseteq \mathbb{N}^+$. We say that U is *closed under factorisation* if $1 \in U$, and whenever $nm \in U$ we have $n, m \in U$. It will turn out in this case that the set $\mathrm{Map}(U, R)$ inherits a ring structure as a quotient ring of $W(R)$. In particular, we will use the rings

$$W_n(R) = \mathrm{Map}(\{d \mid d \text{ divides } n\}, R)$$
$$W_{p^\infty}(R) = \mathrm{Map}(p^{\mathbb{N}}, R).$$

We will sometimes refer to $W_{p^\infty}(R)$ as the *small Witt ring*.

REMARK 22.5. Let $X \colon \mathrm{Rings} \to \mathrm{Sets}$ be a functor such that $X(R)$ is naturally isomorphic to a finite or countable product of copies of R. It is then clear that X is an affine scheme, with $\mathcal{O}_X$ being a polynomial algebra in a finite or countable set of variables over $\mathbb{Z}$. In particular, this applies if $X = W$ or $X = GW$ or $X = W_n$ or $X = W_{p^\infty}$, or if X is a finite product of functors from this list. Note that in these cases $\mathcal{O}_X$ is torsion-free, so Proposition 4.14 is applicable: to prove that two maps $f, g \colon X \to Y$ are equal, it suffices to check that $f_R = g_R \colon X(R) \to Y(R)$ whenever R is a $\mathbb{Q}$-algebra.

LEMMA 22.6. *The map $w_*\colon W(R) \to GW(R)$ is a bijection when R is a $\mathbb{Q}$-algebra, and is injective when R is torsion-free.*

PROOF. For each $n > 0$ we can define a polynomial f_n (with rational coefficients) in the variables $\{u_d \mid d|n\}$ by the recursive rule

$$f_n(u) = \frac{1}{n}\left[u_n - \sum_{d<n,\ d|n} d\, f_d(u)^{n/d}\right].$$

If R is a $\mathbb{Q}$-algebra we can then define $f_*\colon GW(R) \to W(R)$ by $f_*(u)(n) = f_n(u)$. This is easily seen to be inverse to w_*. Now suppose only that R is torsion-free. By considering the square

$$\begin{array}{ccc} W(R) & \xrightarrow{w_*} & GW(R) \\ \downarrow & & \downarrow \\ W(\mathbb{Q}\otimes R) & \xrightarrow[w_*]{\simeq} & GW(\mathbb{Q}\otimes R) \end{array}$$

we see that w_* is still injective. □

LEMMA 22.7. *There is a bijection $e\colon W(R) \to (1 + t\,R[\![t]\!])$ given by $e(a)(t) = \prod_n (1 - a(n)t^n)$. Moreover, we have*

$$\begin{aligned} e(\tau(u))(t) &= 1 - ut \\ e(V_n(a))(t) &= e(a)(t^n) \\ w_m(\tau(u)) &= u^m \\ w_m(V_n(a)) &= \begin{cases} n\, w_{m/n}(a) & \text{if } n \mid m \\ 0 & \text{otherwise} \end{cases} \\ -t\,\frac{e(a)'(t)}{e(a)(t)} &= \sum_n w_n(a)t^n. \end{aligned}$$

PROOF. The product is clearly t-adically convergent, and thus well-defined. Suppose we have a power series $f(t) \in 1 + t\,R[\![t]\!]$, and we have found $a(d)$ for all $d < n$ such that $\prod_{d<n}(1 - a(d)t^d) = f(t) \pmod{t^{n+1}}$. We then have $f(t)\prod_{d<n}(1 - a(d)t^d)^{-1} = 1 - u\,t^n \pmod{t^{n+1}}$ for some $u \in R$, and we define $a(n) = u$. Extending this recursively gives the unique element $a \in W(R)$ such that $e(a) = f$. Thus, we see that $e\colon W(R) \to (1 + t\,R[\![t]\!])$ is a bijection.

The identities $e(\tau(u))(t) = 1 - at$ and $e(V_n a)(t) = e(a)(t^n)$ and $w_n(\tau(u)) = u^n$ are immediate from the definitions. We also have

$$w_m(V_n(a)) = \sum_{d|m} d\,(V_n a)(d)^{m/d}.$$

Recall that $(V_n a)(d)$ is zero unless $n \mid d$. This means that the sum is zero if n does not divide m. If n does divide m, then we can reindex the sum by $d = nk$, so k must divide m/n and $(V_n a)(d) = a(k)$. We get

$$w_m(V_n(a)) = \sum_{k|m/n} nk\, a(k)^{(m/n)/k} = n\, w_{m/n}(a)$$

as claimed.

Finally, note that the construction $f(t) \mapsto -t\,f'(t)/f(t)$ converts products to sums, and it sends $1 - a(d)t^d$ to the series

$$-t\frac{-d\,a(d)t^{d-1}}{1 - a(d)t^d} = d\frac{a(d)t^d}{1 - a(d)t^d} = \sum_{i>0} d a(d)^i t^{di}.$$

It therefore sends the series $e(a)(t) = \prod_d (1 - a(d)t^d)$ to $\sum_{d,i>0} d\,a(d)^i t^{di}$, which is the same as $\sum_n w_n(a)t^n$, as required. □

DEFINITION 22.8. For $a, b \in W(R)$ we define $a + b = e^{-1}(e(a)e(b))$ and $ab = e^{-1}(f(a,b)(t))$, where

$$f(a,b)(t) = \prod_j \prod_{(r,s)=1} (1 - a(jr)^s b(js)^r t^{jrs})^j.$$

We also define elements $0, 1 \in W(R)$ by $0 = \tau(0)$ and $1 = \tau(1)$.

THEOREM 22.9. *The above operations give a commutative ring structure on $W(R)$. Moreover:*

(a) *There is a unique additive map $i\colon NW(R) \to W(R)$ sending $\tau(a)$ to $\tau(a)$ for all a, and this is a ring map.*
(b) *The map $w_*\colon W(R) \to GW(R)$ is a ring map, and the composite $w_* \circ i$ is the same as the map $w_*\colon NW(R) \to GW(R)$ defined previously.*
(c) *The maps $V_n\colon W(R) \to W(R)$ are additive, and they make the right hand square in the following diagram commute. If R is an algebraically closed field of characteristic zero (so that $V_n\colon NW(R) \to NW(R)$ is defined) then the left hand square also commutes.*

$$\begin{array}{ccccc} NW(R) & \xrightarrow{i} & W(R) & \xrightarrow{w_*} & GW(R) \\ {\scriptstyle V_n}\downarrow & & {\scriptstyle V_n}\downarrow & & \downarrow{\scriptstyle V_n} \\ NW(R) & \xrightarrow[i]{} & W(R) & \xrightarrow[w_*]{} & GW(R) \end{array}$$

We also have $V_n V_m = V_{nm}$ for all $n, m > 0$.

PROOF. First, it follows directly from the definitions that $w_n(\tau(a)) = a^n$ for all $a \in R$ and $n > 0$, and thus that w_* sends the elements $0, 1 \in W(R)$ to the elements $0, 1 \in GW(R)$.

Next, we have $e(a+b) = e(a)e(b)$, so

$$-t\frac{e(a+b)'(t)}{e(a+b)(t)} = -t\frac{e(a)'(t)}{e(a)(t)} - t\frac{e(b)'(t)}{e(b)(t)},$$

and we can combine this with Lemma 22.7 to see that $w_n(a+b) = w_n(a) + w_n(b)$. Similarly, we have

$$-t\frac{f(a,b)'}{f(a,b)} = \sum_{j,k} \sum_{(r,s)=1} j^2 rs\, a(jr)^{ks} b(js)^{kr} t^{jkrs}.$$

Now define a map

$$\{(j,k,r,s) \in (\mathbb{N}^+)^4 \mid (r,s) = 1\} \to \{(n,d,e) \in (\mathbb{N}^+)^3 \mid d \text{ and } e \text{ divide } n\}$$

by $(j,k,r,s) \mapsto (jkrs, jr, js)$. One can check that this is a bijection, and it follows that

$$-t\frac{f(a,b)'}{f(a,b)} = \sum_n \sum_{d|n} \sum_{e|n} de\, a(d)^{n/d} b(e)^{n/e} t^n = \sum_n w_n(a) w_n(b) t^n,$$

so $w_n(ab) = w_n(a)w_n(b)$. Thus, the maps $w_*\colon W(R) \to GW(R)$ preserve addition and multiplication.

Now define $f_R, g_R\colon W(R)^3 \to W(R)$ by $f_R(a,b,c) = a(b+c)$ and $g_R(a,b,c) = ab + ac$. As $GW(R)$ is a commutative ring and w_* preserves addition and multiplication we see that $w_* \circ f = w_* \circ g$. If R is a $\mathbb{Q}$-algebra then $w_*\colon W(R) \to GW(R)$ is a bijection so we see that $f_R = g_R$. It follows using Proposition 4.14 that $f = g$, or in other words that the left distributivity axiom is satisfied in $W(R)$ for all commutative rings R. The other ring axioms for $W(R)$ can be checked in the same way. (Some of the axioms can also be checked easily from the definitions. For example, it is clear that $1 + t\,R[\![t]\!]$ is a group under multiplication, so $W(R)$ is a group under addition.)

We next claim that $\tau(u)\tau(v) = \tau(uv)$ for all $u, v \in R$. Equivalently, we claim that $f(\tau(u), \tau(v))(t) = e(\tau(uv))(t) = 1 + uvt$. This follows directly from Definition 22.8, because almost all terms in the relevant products are equal to 1. Because of this, we have a ring map $i\colon NW(R) \to W(R)$ sending $\tau(u)$ to $\tau(u)$. The maps $w_n\colon NW(R) \to R$ and $w_n \circ i\colon NW(R) \to R$ both send $\tau(u)$ to u^n, and $NW(R)$ is generated additively by elements of the form $\tau(u)$, so $w_* \circ i = w_*$.

From the relation $e(V_n(a))(t) = e(a)(t^n)$ it is clear that V_n is additive and $V_nV_m = V_{nm}$. By differentiating, we get

$$\sum_{k>0} w_k(V_n(a))t^k = -t\frac{e(V_n(a))'(t)}{e(V_n(a))(t)} = -t\frac{n\,t^{n-1}\,e(a)'(t^n)}{e(a)(t^n)} = -n\,t^n\frac{e(a)'(t^n)}{e(a)(t^n} = n\sum_{m>0} w_m(a)t^{nm}.$$

This gives $w_k(V_n(a)) = n\,w_{k/n}(a)$ if n divides k, and $w_k(V_n(a)) = 0$ in all other cases. Thus, in the diagram of claim (c), the right hand square commutes.

For the left hand square, note that $e(V_n(\tau(u)))(t) = e(\tau(u))(t^n) = 1 - ut^n$.

we need to show that $V_n(\tau(u)) = \tau(u^n)$

The remaining properties are less easy to see directly, but we can check them using the map w_*.

It follows that the map $w_*\colon W(R) \to GW(R)$ respects addition and multiplication, if we define these pointwise on $\prod_n R$. It follows, for example, that

$$w((ab)c - a(bc)) = (w(a)w(b))w(c) - w(a)(w(b)w(c)) = 0.$$

If R is torsion-free then w is injective, so $(ab)c = a(bc)$. The other ring axioms can be verified the same way, so $W(R)$ is a ring. Finally, even if R has torsion, we can always find a torsion-free ring R' with a surjective map $\pi\colon R' \to R$. (Indeed, we can just take R' to be a polynomial ring over $\mathbb{Z}$ with one generator x_r for each element $r \in R$, and define $\pi(x_r) = r$.) Now $W(R')$ is a ring and π induces a surjective map $W(R') \to W(R)$ that preserves addition and multiplication, and it follows easily that $W(R)$ also satisfies the commutative ring axioms. □

Remark 22.10. Because $\tau(0) = 0$ and $\tau(1) = 1$ and $\tau(uv) = \tau(u)\tau(v)$, we see that there is a unique ring map $\zeta\colon NW(R) \to W(R)$ satisfying $\zeta\tau(u) = \tau(u)$ for all $u \in R$. For any element $x = \sum_i n_i\tau(u_i) \in NW(R)$, we see that $e(\zeta(x))(t) = \prod_i(1 - a_it)^{n_i}$. The difference between $NW(R)$ and $W(R)$ is that

(a) In $e(W(R))$ we have arbitrary power series, but $e(NW(R))$ only has rational functions, so we have performed a kind of completion.

(b) The rational functions arising from $NW(R)$ are automatically factored into linear factors, but for arbitrary rational functions this kind of factorisation may not be possible without passing to an algebraic extension. This means that we have performed a kind of sheafification.

Lemma 22.11. *Any $a \in W(R)$ can be expressed as $a = \sum_{n>0} V_n(\tau(a(n)))$.*

Proof. It is equivalent to say that $e(a)(t) = \prod_{n>0} e(V_n(\tau(a(n))))(t)$. We have seen that

$$e(V_n(\tau(a(n))))(t) = e(\tau(a(n)))(t^n) = 1 - a(n)t^n,$$

so the claim is immediate from the definition of e. □

Definition 22.12. Consider a power series $f(t) \in 1 + t\,R[\![t]\!]$ and an integer $n > 0$. Put $P_n = R[\![t^n]\!]$, so $R[\![t]\!]$ is free of rank n as a module over P_n, with basis $\{t^i \mid 0 \leq i < n\}$. Multiplication by $f(t)$ gives a P_n-linear endomorphism of $R[\![t]\!]$, which we denote by $\mu_n(f)$. The determinant $\det(\mu(f))$ lies in P_n, so it has the form $(F_nf)(t^n)$ for some series $(F_nf)(t)$. If we take the matrix representing $\mu(f)$ and reduce it modulo the augmentation ideal (t^n) in P_n, it is easy to see that the resulting matrix is upper triangular, with all diagonal entries equal to one. It follows that $(F_nf)(0) = 1$, or in other words $(F_nf)(t) \in 1 + t\,R[\![t]\!]$. This allows us to define $F_n\colon W(R) \to W(R)$ by $F_na = e^{-1}(F_n(e(a)))$.

Proposition 22.13. *The map $F_n\colon W(R) \to W(R)$ is a ring homomorphism, with $F_n(\tau(u)) = \tau(u^n)$ for all $u \in R$, and $w_m(F_n(a)) = w_{nm}(a)$ for all $a \in W(R)$.*

Proof. Multiplicativity of determinants implies that the map $F_n\colon 1 + t\,R[\![t]\!] \to 1 + t\,R[\![t]\!]$ preserves products. As $e(a + b) = e(a)e(b)$, it follows that the map $F_n\colon W(R) \to W(R)$ preserves addition. We next claim that $F_n(\tau(u)) = \tau(u^n)$. We will explain the case $n = 4$; the general case follows the same pattern. Consider the matrix identity

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ a & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & 0 & a & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & -ut^4 \\ -u & 1 & 0 & 0 \\ 0 & -u & 1 & 0 \\ 0 & 0 & -u & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & -ut^4 \\ 0 & 1 & 0 & -u^2t^4 \\ 0 & 0 & 1 & -u^3t^4 \\ 0 & 0 & 0 & 1 - u^4t^4. \end{bmatrix}$$

The second matrix is the matrix of $\mu_4(f)$ with respect to the basis $\{t^i \mid 0 \leq i < 4\}$, where $f(t) = e(\tau(u))(t) = 1 - ut$. The first matrix clearly has determinant 1, and the last matrix clearly has determinant $1 - u^4t^4$, so $\det(\mu_4(f)) = 1 - u^4t^4$, so $F_4(f)(t) = 1 - u^4t$. This is the same as $e(\tau(u^4))(t)$, so $F_4(\tau(u)) = \tau(u^4)$. In exactly the same way, we can prove that $F_n(\tau(u)) = \tau(u^n)$ for all $n > 0$. Now put $Z_{n,m} = \{a \in W(R) \mid w_m(F_n(a)) = w_{mn}(a)\}$. The maps w_m, w_{mn} and F_n preserve addition, so $Z_{n,m}$ is an additive subgroup of $W(R)$. We have $w_{nm}(\tau(u)) = u^{nm}$ and $w_m(F_n(\tau(u))) = w_m(\tau(u^n)) = u^{nm}$ so $\tau(u) \in Z_{n,m}$. It follows that for any $u_1, \dots, u_r \in R$ we have $\sum_i \tau(u_i) \in Z_{n,m}$. A Zariski density argument now shows that $Z_{n,m} = W(R)$, so $w_m(F_n(a)) = w_{mn}(a)$ for all a as claimed **explain in more detail**. It follows in turn that $w_m(F_n(ab) - F_n(a)F_n(b)) = 0$ for all $a, b \in R$ and $n, m > 0$. If R is torsion-free, the maps w_m are jointly injective so we see that F_n preserves multiplication. We saw previously that it also preserves addition, so it is a ring map. For general R we can consider a torsion-free ring with a surjective homomorphism to R, and we deduce by naturality that $F_n \colon W(R) \to W(R)$ is a ring map even if R has torsion. □

COROLLARY 22.14. *The operations F_n and V_m satisfy identities as follows:*

$$\begin{aligned} F_nF_m &= F_{nm} \\ V_nV_m &= V_{nm} \\ F_nV_n &= n \\ F_nV_m &= V_mF_n \text{ if } gcd(n, m) = 1. \end{aligned}$$

PROOF. By the usual reduction to the torsion-free case, it will suffice to check the following:

$$\begin{aligned} w_k(F_n(F_m(a))) &= w_k(F_{nm}(a)) \\ w_k(V_n(V_m(a))) &= w_k(V_{nm}(a)) \\ w_k(F_n(V_n(a))) &= n\, w_k(a) \\ w_k(F_n(V_m(a))) &= w_k(V_m(F_n(a))) \text{ if } \gcd(n, m) = 1. \end{aligned}$$

Recall that $w_k(F_n(b)) = w_{kn}(b)$ and $w_k(V_n(b)) = n\, w_{k/n}(b)$, where we interpret $w_{k/n}(b)$ as zero if k/n is not an integer. The first three identities follow directly from this. For the last identity, the left hand side is $m\, w_{nk/m}(a)$ if nk/m is an integer, and zero otherwise. The right hand side is $m\, w_{nk/m}(a)$ if k/m is an integer, and zero otherwise. Because n and m are coprime, we see that nk/m is an integer iff k/m is an integer, so the two sides are equal. □

LEMMA 22.15. *Suppose that R is a $\mathbb{Z}/p$-algebra, so we have a ring endomorphism $\phi \colon R \to R$ given by $\phi(a) = a^p$, and an induced ring endomorphism $\Phi = W(\phi)$ of $W(R)$. Then we have $V_p\Phi(a) = pa$ for all $a \in W(R)$.*

PROOF. It will suffice to show that $e(V_p\Phi(a))(t) = e(pa)(t)$ in $1 + t\, R[\![t]\!]$. For this we note that

$$\begin{aligned} e(V_p\Phi(a))(t) = e(\Phi(a))(t^p) &= \prod_k (1 - \phi(a(k))t^{pk}) = \prod_k (1 - a(k)^p t^{pk}) \\ &= \left(\prod_k (1 - a(k)t^k)\right)^p = e(a)(t)^p = e(pa)(t). \end{aligned}$$

□

LEMMA 22.16. *If $a(n)b(n) = 0$ for all n, then the Witt sum of a and b is just the ordinary sum, so $(a + b)(n) = a(n) + b(n)$.*

PROOF. Put $c(n) = a(n) + b(n)$. We must show that c is the Witt sum of a and b, or in other words $e(c) = e(a)e(b)$. As $a(n)b(n) = 0$ we have

$$(1 + a(n)t^n)(1 + b(n)t^n) = 1 + a(n)t^n + b(n)t^n + a(n)b(n)t^{2n} = 1 + c(n)t^n,$$

and we can take the product over all n to prove the claim. □

DEFINITION 22.17. Let $U \subseteq \mathbb{N}^+$ be closed under factorisation, and put

$$I_U R = \{a \colon \mathbb{N}^+ \to R \mid a(U) = 0\}$$
$$W_U R = \{a \colon \mathbb{N}^+ \to R \mid a(U^c) = 0\}.$$

We will identify $I_U R$ with $\mathrm{Map}(U^c, R)$ and $W_U R$ with $\mathrm{Map}(U, R)$ where convenient. Given $a \in W(R)$ we define an element $a|_U \in W_U R$ by $(a|_U)(n) = a(n)$ for $n \in U$, and $(a|_U)(n) = 0$ for $n \notin U$. We define $a|_{U^c} \in I_U R$ in a similar way.

PROPOSITION 22.18. *There is a unique ring structure on $W_U R$ for which the map $a \mapsto a|_U$ gives a ring homomorphism $W(R) \to W_U R$. The kernel of this homomorphism is $I_U R$, so we get an induced isomorphism $W(R)/I_U R \to W_U R$. For $n \in U$ the ring map $w_n \colon W(R) \to R$ factors through $W_U R$. These maps taken together give a ring map $w \colon W_U R \to \prod_U R$ which is an isomorphism when R is a $\mathbb{Q}$-algebra, and injective when R is torsion-free.*

The proof will follow after some preliminaries.

LEMMA 22.19. *If $a \in I_U R$ then $w_n(a) = 0$ for all $n \in U$. Conversely, if R is torsion-free and $w_n(a) = 0$ for all $n \in U$, then $a \in I_U R$.*

PROOF. First suppose that $a \in I_U R$. For $n \in U$ we observe that $a(d) = 0$ whenever $d|n$, and thus that $w_n(a) = 0$. Now suppose that R is torsion-free, and that for all $n \in U$ we have $w_n(a) = 0$. We must show that $a(n) = 0$, and we may assume inductively that $a(d) = 0$ for all proper divisors d of n. With that assumption the equation $w_n(a) = 0$ reduces to $n\, a(n) = 0$ and the claim follows. □

COROLLARY 22.20. *$I_U R$ is an ideal in $W(R)$.*

PROOF. This is clear from the lemma in the torsion-free case, and we can recover the general case by writing R as a quotient of a torsion-free ring. □

PROOF OF PROPOSITION 22.18. We have seen that $I_U R$ is an ideal. For $a \in W(R)$ we see using Lemma 22.16 that $a = (a|_U) + (a|_{U^c}) = (a|_U) \pmod{I_U R}$. Thus, if $a|_U = b|_U$ we find that $a = b \pmod{I_U R}$. We next claim that the converse also holds. Indeed, suppose that $a, b \in W(R)$ with $a = b \pmod{I_U R}$. We also have $a = a|_U \pmod{I_U R}$ and $b = b|_U \pmod{I_U R}$ so $a|_U = b|_U + c$ for some $c \in I_U R$. Lemma 22.16 tellus us that the sum $b_U + c$ is just the ordinary pointwise sum, so it commutes with restriction. In particular we can restrict to U^c to see that $c = 0$, so $a|_U = b|_U$ as claimed. We can thus define addition and multiplication on $W_U R$ by

$$a +_U b = (a + b)|_U = \text{ the unique } c \in W_U R \text{ such that } a + b = c \pmod{I_U R}$$
$$a .\!_U b = (ab)|_U = \text{ the unique } d \in W_U R \text{ such that } ab = d \pmod{I_U R}\ .$$

It is straightforward to check that this gives a ring structure for which the restriction map is a homomorphism with kernel $I_U R$. If $n \in U$ it is immediate from the definitions that $w_n(a)$ depends only on $a(d)$ for $d \in U$, so $w_n(a) = w_n(a|_U)$. The rest is now easy. □

DEFINITION 22.21. When discussing $W_{p^\infty}(R)$, we will write F for F_p and V for V_p. Elements of $W_{p^\infty}(R)$ are represented by maps $a \colon p^{\mathbb{N}} \to R$, and we write $a[k]$ for $a(p^k)$. We also write $w_{[k]}(a)$ for $w_{p^k}(a)$.

PROPOSITION 22.22. *Let p be a prime, and let R be a finite $\mathbb{Z}/p$-algebra, with $|R| = p^n$ say. Suppose also that R is reduced, so that the Frobenius map $\phi \colon a \mapsto a^p$ is an automorphism. Then $W_{p^\infty}(R)$ is a free module of rank n over $\mathbb{Z}_p$, and the map $w_{[0]} \colon a \mapsto a_1$ gives an isomorphism $W_{p^\infty}(R)/p \to R$. Thus, the functor W_{p^∞} is inverse to the reduction functor in Theorem 13.15. Moreover, in this context we have $F = W_{p^\infty}(\phi)$, which is an automorphism of $W_{p^\infty}(R)$, and $VF = FV = p$.*

PROOF. Put $\Phi = W_{p^\infty}(\phi) \colon W_{p^\infty}(R) \to W_{p^\infty}(R)$. This is a ring automorphism, which commutes with F and V by naturality. From Lemma 22.15 we see that $V\Phi(a) = pa$ for all a. From the definition of V we see that the sequence $W_{p^\infty}(R) \xrightarrow{V} W_{p^\infty}(R) \xrightarrow{w_{[0]}} R$ is short exact. As $V\Phi = p$ and Φ is an automorphism it follows that the sequence $W_{p^\infty}(R) \xrightarrow{p} W_{p^\infty}(R) \xrightarrow{w_{[0]}} R$ is also short exact, so $W_{p^\infty}(R)$ is torsion-free with $W_{p^\infty}(R)/p = R$.

It is also clear that $\Phi(\tau(u)) = \tau(\phi(u))$. An induction using these facts gives $V^k(\tau(u)) = p^k\tau(\phi^{-k}(u))$. A typical element $a \in W_{p^\infty}(R)$ can be expressed as $a = \sum_{k\geq 0} V^k(\tau(a[k])) = \sum_{k\geq 0} p^k\tau(\phi^{-k}(a[k]))$. It follows that $W_{p^\infty}(R)$ is p-complete and is generated by the finite set $\tau(R)$ as a module over $\mathbb{Z}_p$. As it is finitely generated over $\mathbb{Z}_p$ and torsion-free, it is in fact free. As $W_{p^\infty}(R)/p = R \simeq (\mathbb{Z}/p)^n$, we must have $W_{p^\infty}(R) \simeq \mathbb{Z}_p^n$.

Now note that F and Φ are both $\mathbb{Z}_p$-module endomorphisms of $W_{p^\infty}(R)$, and they are easily seen to agree on the generating set $\tau(R)$, so they are the same. We have noted that Φ commutes with V, so F commutes with V. For any ring we have $FV = p$, but now we can deduce that $VF = p$ as well. □

Definition 22.23. We define $\widehat{W}(R) \subseteq W(R)$ to be the set of maps $a\colon \mathbb{N}^+ \to R$ such that $a(n)$ is nilpotent for all n and is zero for $n \gg 0$. This is easily seen to be an ideal in $W(R)$. We regard the functor $\widehat{W}\colon$ Rings $\to$ Sets as an infinite-dimensional formal scheme, and we note that the map $\tau\colon R \to W(R)$ gives a morphism $\widehat{\mathbb{A}}^1 \to \widehat{W}$ of formal schemes.

Proposition 22.24. *Let G be a formal group over X, and let $\gamma\colon \widehat{\mathbb{A}}^1 \times X \to G$ be a curve. Then there is a unique homomorphism $\widetilde{\gamma}\colon \widehat{W} \times X \to G$ of formal group schemes with $\widetilde{\gamma} \circ \tau = \gamma\colon \widehat{\mathbb{A}}^1 \to G$.*

Proof. We define $\widetilde{\gamma}(a) = \sum_{n>0}(f_n\gamma)(a(n))$. (More precisely, this should be written

$$\widetilde{\gamma}(a, x) = \sum_{n>0}(f_n\gamma)(a(n), x)$$

for all rings R and $a \in W(R)$ and $x \in X(R)$.) We want to prove that $\widetilde{\gamma}(a + b) = \widetilde{\gamma}(a) + \widetilde{\gamma}(b)$. We first treat the case where G is just the additive formal group. We can then write $\gamma(t) = \sum_{i>0} c_i t^i$ for some sequence of coefficients c_i, and Example 21.5 gives $(f_n\gamma)(t) = \sum_{k>0} n\, c_{nk} t^k$. It follows that

$$\widetilde{\gamma}(a) = \sum_{n,k>0} c_{nk} n\, a(n)^k = \sum_{m>0} c_m \sum_{n|m} n\, a(n)^{m/n} = \sum_{m>0} c_m w_m(a).$$

As the maps w_m are additive, we see that the map $\widetilde{\gamma}\colon \widehat{W} \times X \to G$. Is additive in this case. If $\mathcal{O}_X$ is a $\mathbb{Q}$-algebra then every G is isomorphic to the additive group, so we see that $\widetilde{\gamma}$ is always additive. If $\mathcal{O}_X$ is merely torsion-free, then it injects in $\mathbb{Q} \otimes \mathcal{O}_X$ and we deduce again that $\widetilde{\gamma}$ is additive. Finally, we can always write $\mathcal{O}_X$ as a quotient of a torsion-free ring, and by naturality we find that $\widetilde{\gamma}$ is additive in all cases.

Now suppose we have a homomorphism $\alpha\colon \widehat{W} \to G$ with $\alpha \circ \tau = 0$. A Zariski density argument then shows that $\alpha = 0$. **Give more details.** Thus, the above extension $\widetilde{\gamma}$ is uniquely determined. □

Lemma 22.25. *For and $\gamma\colon \widehat{\mathbb{A}}^1 \times X \to G$ as above, and any $u \in \mathcal{O}_X$ and $n \in \mathbb{N}^+$, we have*

$$\widetilde{f_n\gamma}(a) = \widetilde{\gamma}(V_n(a))$$
$$\widetilde{v_n\gamma}(a) = \widetilde{\gamma}(F_n(a))$$
$$\widetilde{\theta_u\gamma}(a) = \widetilde{\gamma}(\tau(u)a).$$

Proof. In each case, we see that the right hand side defines a homomorphism $\widehat{W} \times X \to G$. Thus, in view of the Proposition, it will suffice to prove the following:

$$(f_n\gamma)(t) = \widetilde{\gamma}(V_n(\tau(t)))$$
$$(v_n\gamma)(t) = \widetilde{\gamma}(F_n(\tau(t)))$$
$$(\theta_u\gamma)(t) = \widetilde{\gamma}(\tau(u)\tau(t)).$$

These are all clear from the definitions. □

Corollary 22.26. *A curve $\gamma\colon \widehat{\mathbb{A}}^1 \times X \to G$ is p-typical iff the homomorphism $\widetilde{\gamma}\colon \widehat{W} \times X \to G$ factors through the quotient $\widehat{W}_{p^\infty} \times X$. Thus,* $\mathrm{Curves}_p(G)$ *can be identified with the set of homomorphisms $\widehat{W} \times X \to G$ of formal group schemes over X.*

23. Witt covectors

In this section, we will define an abelian group $CW_{p^\infty}(R)$. To motivate this, consider the case where R is a reduced finite $\mathbb{Z}/p$-algebra. We showed in Proposition 22.22 that $W_{p^\infty}(R)$ is a finitely generated free module over $\mathbb{Z}_p$, with $W_{p^\infty}(R)/p = R$. In this case it will turn out that $CW_{p^\infty}(R) \simeq W_{p^\infty}(R) \otimes (\mathbb{Q}/\mathbb{Z})$, and this can be identified with the Pontrjagin dual of $W_{p^\infty}(R)$. For general R, the group $CW_{p^\infty}(R)$ will again be a module over $W_{p^\infty}(R)$, and will again have a kind of duality relationship with $W_{p^\infty}(R)$, although the details will be more complicated.

Definition 23.1. We define $LW_{p^\infty}(R)$ to be the set of maps $a\colon p^{\mathbb{Z}} \to R$ such that $a(p^{-n}) = 0$ for $n \gg 0$. We write $a[k] = a(p^k)$ for all $k \in \mathbb{Z}$. We identify $W_{p^\infty}(R)$ with the set

$$\{a \in LW_{p^\infty}(R) \mid a[k] = 0 \text{ for all } k < 0\}$$

in the obvious way. We define a bijection $V\colon LW_{p^\infty}(R) \to LW_{p^\infty}(R)$ by $V(a)[k] = a[k-1]$. If $a, b \in LW_{p^\infty}(R)$ then for sufficiently large n we have $V^n(a), V^n(b) \in W_{p^\infty}(R)$ so we can define $a + b = V^{-n}(V^n(a) + V^n(b))$. This is independent of the choice of n because $V\colon W_{p^\infty}(R) \to W_{p^\infty}(R)$ is additive. It is clear that this makes $LW_{p^\infty}(R)$ into a group, with $W_{p^\infty}(R)$ as a subgroup.

We now define $CW_{p^\infty}(R)$ to be the set of maps $a\colon p^{\mathbb{Z}} \to R$ with $a[k] = 0$ for all $k \geq 0$. Using Lemma 22.16 we see that the addition map

$$CW_{p^\infty}(R) \times W_{p^\infty}(R) \to LW_{p^\infty}(R)$$

is bijective, so we can identify $CW_{p^\infty}(R)$ with the quotient $LW_{p^\infty}(R)/W_{p^\infty}(R)$, which gives it a group structure. The automorphism V of $LW_{p^\infty}(R)$ induces a surjective endomorphism of $CW_{p^\infty}(R)$, and for any $a \in CW_{p^\infty}(R)$ we have $V^n(a) = 0$ for $n \gg 0$.

Definition 23.2. For $k \in \mathbb{Z}$ we define $w_{[k]}\colon LW_{p^\infty}(R) \to R[1/p]$ by

$$w_{[k]}(a) = \sum_{j \geq 0} p^{k-j} a[k-j]^{p^j}.$$

(Note that the sum is finite because $a[m] = 0$ for $m \ll 0$.) If $k \geq 0$ and $a \in W_{p^\infty}(R)$ then it is easy to see that this agrees with our earlier definition of $w_{[k]}(a)$. In all cases we find that $w_{[k]}(V(a)) = w_{[k-1]}(a)$. Using this, it follows that $w_{[k]}$ is a homomorphism of additive groups.

Definition 23.3. Let I be an ideal in R. We define

$$W_{p^\infty}(I) = \mathrm{Map}(p^{\mathbb{N}}, I) \subseteq \mathrm{Map}(p^{\mathbb{N}}, R) = W_{p^\infty}(R).$$

It is easy to see that this is an ideal, and is the kernel of the evident surjective homomorphism

$$W_{p^\infty}(\pi)\colon W_{p^\infty}(R) \to W_{p^\infty}(R/I).$$

We define subgroups $LW_{p^\infty}(I) \leq LW_{p^\infty}(R)$ and $CW_{p^\infty}(I) \leq CW_{p^\infty}(R)$ in the same way.

Lemma 23.4. *There is a well-defined homomorphism $\xi\colon CW_{p^\infty}(R/p) \to R[1/p]/R$ given by $\xi(a) = \sum_{j>0} p^{-j}\widetilde{a}[-j]^{p^{j-1}}$ for any $\widetilde{a} \in CW_{p^\infty}(R)$ lifting the element $a \in CW_{p^\infty}(R/p)$.*

Proof. We have a homomorphism $\xi_0 = p^{-1}w_{[-1]}\colon LW_{p^\infty}(R) \to R[1/p]$ given by

$$\xi_0(a) = p^{-1}\sum_{i \geq 0} p^{-i} a[-1-i]^{p^i} = \sum_{j>0} p^{-j} a[-j]^{p^{j-1}}.$$

This is clearly zero on $W_{p^\infty}(R)$ and so induces a homomorphism $\xi_1\colon CW_{p^\infty}(R) \to R[1/p]$. If $j > 0$ and $a[-j]$ is divisible by p then $p^{-j}a[-j]^{p^{j-1}}$ is divisible by p^m where $m = p^{j-1} - j \geq 0$, so $p^{-j}a[-j]^{p^{j-1}} \in R$. This shows that $\xi_1(CW_{p^\infty}(pR)) \leq R$, so we get an induced map $\xi\colon CW_{p^\infty}(R/p) \to R[1/p]/R$ as required. □

Lemma 23.5. *Suppose that R is a finitely generated free module over $\mathbb{Z}_p$ and that R/p is reduced (so that R lies in the category $\mathcal{W}$ from Definition 13.14). Then the map $\xi\colon CW_{p^\infty}(R) \to R[1/p]/R$ is an isomorphism.*

Proof. Using Proposition 13.20(b) we see that any element $b \in R[1/p]/R$ can be expressed uniquely as $\sum_{i<0} \tau(b_i)p^{-i}$ for some system of elements $b_i \in R/p$ with $b_i = 0$ for $i \gg 0$. Recall also that the Frobenius map $\phi\colon R/p \to R/p$ is bijective. We can therefore define $a \in CW_{p^\infty}(R/p)$ by $a[-i] = \phi^{1-i}(b_i)$. It is straightforward to check that this is the only element with $\xi(a) = b$. □