ELSEVIER Journal of Pure and Applied Algebra 121 (1997) 161–208

JOURNAL OF
PURE AND
APPLIED ALGEBRA

Finite subgroups of formal groups[1]

Neil P. Strickland

Trinity College, Cambridge, UK CB2 1TQ

Communicated by E.M. Friedlander; received 26 January 1996

Abstract

We discuss various moduli problems involving the classification of finite subgroups or related structures on formal groups of finite height n. We show that many moduli schemes are smooth or at least Cohen–Macaulay. Moreover, many maps between such schemes are finite and flat, and their degrees can be predicted by thinking of $(\mathbb{Q}_p/\mathbb{Z}_p)^n$ as a "discrete model" for the formal group. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 14L05, 55N22

1. Introduction

In this paper we discuss various moduli problems involving the classification of finite subgroups or related structures on formal groups of finite height. Analogous problems for elliptic curves have of course been widely studied [9]. The moduli spaces which we consider turn out to be surprisingly well-behaved. They are all Cohen–Macaulay, and most of them are smooth. The original motivation for this work came from algebraic topology, in particular the study of power operations in certain homology theories constructed by Morava. I learnt most of what I know about these questions from Mike Hopkins, and a great deal of the theory presented here was developed in discussions with him. See Section 14 for a brief discussion of how moduli problems arise in algebraic topology, and [15] for more details. Some readers may prefer a version of this paper containing rather more exposition of standard algebraic material, which is available from the author.

[1] Partially supported by the N.S.F.

0022-4049/97/$17.00 © 1997 Elsevier Science B.V. All rights reserved

PII S0022-4049(96)00113-2

1.1. Synopsis

In Section 2 we set up our technical context by recalling various results about complete local rings, interpreted in a geometric manner. In Sections 3 and 4, we establish some basic facts about formal groups and divisors. In Section 5 we show that the quotient of a formal group by a finite subgroup is again a formal group. In Section 6 we reformulate the Lubin–Tate deformation theory of formal groups in a coordinate-free way.

For the rest of this synopsis, we consider a formal group $\mathbb{G}_0$ of finite height over a field of positive characteristic, and let $\mathbb{G}/X$ be its universal deformation. The content of subsequent sections is as follows.

Section 7: We define level-A structures on $\mathbb{G}$ (where A is a finite Abelian group). We prove that the moduli space $\mathrm{Level}(A, \mathbb{G})$ is smooth, and that the map $\mathrm{Level}(A, \mathbb{G}) \to X$ is finite and flat.

Section 8: We investigate maps of schemes over X between the schemes Level $(A, \mathbb{G})$; they all arise (contravariantly) from monomorphisms of finite Abelian groups, and are finite and flat.

Section 9: We show how an epimorphism $u: A \to B$ gives rise to a finite flat map $\mathrm{Level}(A, \mathbb{G}) \to \mathrm{Level}(B, \mathbb{G}')$, for a different group $\mathbb{G}'$.

Section 10: We show that the subgroups of $\mathbb{G}$ of degree p^m are classified by a scheme $\mathrm{Sub}_m(\mathbb{G})$ which is finite and flat over X.

Section 11: We consider flags $0 = K_0 < K_1 < \cdots < K_m = \mathbb{G}(1)$, where $\mathbb{G}(1)$ is the kernel of multiplication by p on $\mathbb{G}$ and K_i has given degree p^{λ_i}. We show that such flags are classified by a smooth scheme $\mathrm{Flag}(\lambda, \mathbb{G})$, and that there are finite flat maps $\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G}) \to X$, the first of which is a Galois covering.

Section 12: We consider the orbit scheme $\mathrm{Type}(A, \mathbb{G}) = \mathrm{Level}(A, \mathbb{G}) / \mathrm{Aut}(A)$ (suitably interpreted). We show that $\mathrm{Type}(A, \mathbb{G})$ is smooth and the maps $\mathrm{Level}(A, \mathbb{G}) \to \mathrm{Type}(A, \mathbb{G}) \to X$ are finite and flat. We also show that the normalisation of $\mathrm{Sub}_m(\mathbb{G})$ is a disjoint union of schemes of the form $\mathrm{Type}(A, \mathbb{G})$. Moreover, if the height of $\mathbb{G}_0$ is at most two (but not in general), then the maps $\mathrm{Type}(A, \mathbb{G}) \to \mathrm{Sub}_m(\mathbb{G})$ are closed embeddings.

Section 13: We consider the problem of classifying deformations of a given isogeny of formal groups over a field.

Section 14: We sketch the way in which the problems discussed above arise in algebraic topology.

Section 15: We derive some formulae which help one to construct and compute with formal groups.

Section 16: We present some detailed examples.

2. Geometry of complete local rings

For brevity, a *scheme* will mean a formal scheme of the form $\mathrm{spf}(A)$, where A is a finite product of complete Noetherian local rings of residue characteristic $p > 0$. We shall often assume that A is local, leaving trivial modifications for the semi-local case to the reader. We shall primarily think of schemes as representable functors from the category of complete Noetherian local rings and local homomorphisms to sets, via the definition

$$\mathrm{spf}(A)(B) = \mathrm{Hom}(A,B).$$

If $X = \mathrm{spf}(A)$ we write $\mathcal{O}_X$ for A. Given schemes Y, Z over a base scheme X (which is usually to be understood from the context), a *point of* Y *defined over* Z will mean a map $a\colon Z \rightarrow Y$ of schemes over X. We write $\Gamma(Z,Y)$ for the set of such points. If $f \in \mathcal{O}_Y$ then we write $f(a)$ for $a^*f \in \mathcal{O}_Z$.

If X is connected (i.e. $\mathcal{O}_X$ is local) we write $\kappa_X = \mathcal{O}_X/\mathfrak{m}_X$ for the residue field. We also write $X_0 = \mathrm{spf}(\kappa_X)$ and refer to this as the *special fibre* of X.

We write $\dim(X)$ for the Krull dimension of X and $\mathrm{embdim}(X)$ for the embedding dimension, that is $\mathrm{embdim}(X) = \dim_{\kappa_X}(\mathfrak{m}_X/\mathfrak{m}_X^2)$. We shall say that X is *integral* if $\mathcal{O}_X$ is an integral domain, and *smooth* if $\mathcal{O}_X$ is a regular local ring. If X is integral we write $\mathcal{K}_X$ for the field of fractions of $\mathcal{O}_X$. Suppose we have a map of schemes $f\colon X \rightarrow Y$, and thus a map $f^*\colon \mathcal{O}_Y \rightarrow \mathcal{O}_X$, using which we consider $\mathcal{O}_X$ as a module over $\mathcal{O}_Y$. As usual, we say that f is *flat* (resp. *finite*) if $\mathcal{O}_Y$ is a flat (resp. finitely generated) $\mathcal{O}_X$-module. We also say that f is *dominant* (resp. epi) if the kernel of f^* is nilpotent (resp. zero).

If f is finite and Y is connected we define the *degree* of f to be $\deg(f) = \dim_{\kappa_Y}(\kappa_Y \otimes_{\mathcal{O}_Y} \mathcal{O}_X)$. In our context, if f is also flat then $\mathcal{O}_X$ is actually a free module over $\mathcal{O}_Y$ (see [11, Theorem 7.10]).

We next state in this language some standard facts from commutative algebra.

Lemma 1. *A finite dominant map of smooth schemes is flat.*

Lemma 2. *Let X, Y and Z be integral schemes of the same dimension d, with maps $X \xrightarrow{f} Y \xrightarrow{g} Z$. If gf is finite and dominant, then the same is true of f and g.*

Lemma 3. *If X is smooth and $f\colon X \rightarrow Y$ is finite and flat then Y is smooth.*

Proof. Use the homological criterion [11, Theorem 19.2]. □

Let X be a scheme with an action of a finite group Γ. We shall write X/Γ for the scheme $\mathrm{spf}(\mathcal{O}_X^\Gamma)$. This is of course not a very good construction in general, but it will turn out to be well-behaved in the cases we consider.

Definition 4. A finite extension $R \rightarrow S$ of integral domains is *Galois* if R is the fixed subring for the action of $\mathrm{Aut}_R(S)$ on S and S is free over R. I am not sure whether this definition is standard. Similarly, we say that a map $X \longrightarrow Y$ of integral schemes is a *Galois covering* if $\mathcal{O}_Y \longrightarrow \mathcal{O}_X$ is Galois.

The next two lemmas follow easily from the Galois theory of fields and the fact that regular local rings are integrally closed.

Lemma 5. *If $f : X \longrightarrow Y$ is Galois then $\mathcal{K}_X$ is Galois over $\mathcal{K}_Y$ and*

$$\deg(f) = [\mathcal{O}_X : \mathcal{O}_Y] = [\mathcal{K}_X : \mathcal{K}_Y] = |\operatorname{Aut}_{\mathcal{O}_Y}(\mathcal{O}_X)| = |\operatorname{Aut}_{\mathcal{K}_Y}(\mathcal{K}_X)|.$$

Lemma 6. *A finite dominant map $f : X \longrightarrow Y$ of smooth schemes is a Galois covering if and only if the extension of function fields $\mathcal{K}_Y \longrightarrow \mathcal{K}_X$ is Galois.*

Lemma 7. *Let X be a smooth scheme with a faithful action of a finite group Γ. Suppose that $f : X \longrightarrow Y$ is a finite flat map of degree $d = |\Gamma|$, such that $f \circ g = f$ for all $g \in \Gamma$. Then Y is smooth, f is Galois, and the induced map $X/\Gamma \longrightarrow Y$ is iso.*

Proof. By Lemma 3, we see that Y is smooth. Because $[\mathcal{K}_X : \mathcal{K}_Y] = |\Gamma|$ and $\mathcal{K}_Y \leq \mathcal{K}_X^\Gamma$, Galois theory tells us that $\mathcal{K}_Y = \mathcal{K}_X^\Gamma$ and thus $\mathcal{K}_Y \longrightarrow \mathcal{K}_X$ is Galois. The claim now follows from Lemma 6. □

We next record a few basic facts about norms. Suppose that $f : X \longrightarrow Y$ is a finite flat map of degree m. We can then define a (nonadditive) norm map $N_f = N_{X/Y} : \mathcal{O}_X \longrightarrow \mathcal{O}_Y$, by letting $N_f(u)$ be the determinant of multiplication by u, considered as an $\mathcal{O}_Y$-linear endomorphism of $\mathcal{O}_X$.

Lemma 8. *Suppose we have a pullback diagram*

$$\begin{tikzcd} V \arrow[r, "a"] \arrow[d, "g"'] & X \arrow[d, "f."] \\ W \arrow[r, "b"'] & Y \end{tikzcd}$$

If f is a finite free map then so is g, and $N_g \circ a^* = b^* \circ N_f$.

Proof. For the square to be a pullback means that $\mathcal{O}_V = \mathcal{O}_W \otimes_{\mathcal{O}_Y} \mathcal{O}_X$, and with this identification we have $g^* = 1 \otimes f^*$ and $a^* = b^* \otimes 1$. The claim follows easily by choosing bases. □

Lemma 9. *Suppose that $s : Y \longrightarrow X$ is a section of f, and that $s^*u = 0$. Then $N_f(u) = 0$.*

Proof. We can write $\mathcal{O}_X = f^*\mathcal{O}_Y \oplus I$, where $I = \ker(s^*)$. As $u \in I$, the image of multiplication by u lies in the proper summand I of $\mathcal{O}_X$, so the determinant is zero. □

3. Formal groups

Let $X = \mathrm{spf}(A)$ be a scheme, and $\mathbb{G}$ a one-dimensional commutative formal group over X. In more detail, we have $\mathbb{G} = \mathrm{spf}(B)$ where B is isomorphic to $A[\![x]\!]$ as an augmented A-algebra, and we are given a commutative group law $\mu\colon \mathbb{G} \times_X \mathbb{G} \to \mathbb{G}$ (which we shall write additively). In future, we shall simply say "formal group" instead of "commutative one-dimensional formal group". A *coordinate* on a formal group $\mathbb{G}$ is a choice of generator $x \in \ker(0^* : \mathcal{O}_{\mathbb{G}} \to \mathcal{O}_X)$ such that $\mathcal{O}_{\mathbb{G}} = \mathcal{O}_X[\![x]\!]$. (Here 0^* is the map induced by the zero-section $0\colon X \to \mathbb{G}$).

A *homomorphism* $(f,q)\colon (\mathbb{G},X) \to (\mathbb{H},Y)$ of formal groups consists of maps as follows, which make the obvious diagrams commute.

$$\begin{tikzcd}
\mathbb{G} \arrow[r, "q"] \arrow[d] & \mathbb{H} \arrow[d] \\
X \arrow[r, "f"'] & Y
\end{tikzcd}.$$

We shall say that (q,f) (or just q) is a *fibrewise isomorphism* if the diagram above is a pullback.

Let x be a coordinate on $\mathbb{G}$, and let $x_0,x_1 \in \mathcal{O}_{\mathbb{G}\times_X\mathbb{G}}$ be obtained by pulling back x along the two projections $\mathbb{G} \times_X \mathbb{G} \to \mathbb{G}$. Then $\mathcal{O}_{\mathbb{G}\times_X\mathbb{G}} = \mathcal{O}_X[\![x_0,x_1]\!]$, so we can write $\mu^*x = F(x_0,x_1)$ for a unique power series F over $\mathcal{O}_X$. Equivalently, for any two points $a,b\colon Y \to \mathbb{G}$ we have $x(a+b) = F(x(a),x(b))$. This series is called the formal group law associated to $\mathbb{G}$ and x. It is easily seen to have the following properties:

$$F(y,z) = y + z \pmod{xy}, \qquad F(y,z) = F(z,y)$$
$$F(F(x,y),z) = F(x,F(y,z))$$

We also write $x +_F y$ for $F(x,y)$. Much of the literature on formal groups is written in terms of formal group laws [6, 14, Appendix 2, 7]. However, we shall find it conceptually clearer to take a coordinate-free definition the primary one.

Let $X_0 = \mathrm{spf}(A/\mathfrak{m})$ be the special fibre, and put $\mathbb{G}_0 = \mathbb{G} \times_X X_0$. This is a formal group over X_0.

The following lemma is well-known.

Lemma 10. *Let $q\colon \mathbb{G} \to \mathbb{H}$ be a nonzero homomorphism of formal groups over a base X, and let x and y be coordinates on $\mathbb{G}$ and $\mathbb{H}$. Then there exist $a \in \mathcal{O}_X$ and $n \in \mathbb{N}$ such that $a \neq 0$ and $q^*y = ax^{p^n} \pmod{x^{p^n+1}}$.*

Definition 11. We shall call the integer n described above the *strict height* of q, and define the *height* of q to be the strict height of $q_0 : \mathbb{G}_0 \to \mathbb{H}_0$. We also define the (strict) height of $\mathbb{G}$ to be the (strict) height of the endomorphism $p_{\mathbb{G}} : \mathbb{G} \to \mathbb{G}$, which is just p times the identity map.

From now on, we shall take $\mathbb{G}$ to be a formal group of finite height n over a connected base scheme X.

Proposition 12. *If $q : \mathbb{G} \to \mathbb{H}$ is nonzero, then $m = \mathrm{height}(q)$ is finite and q is flat of degree p^m. Moreover,* $\mathrm{height}(\mathbb{H}) = \mathrm{height}(\mathbb{G})$.

Proof. This is essentially standard. If q has infinite height then $q = 0$; this is an easy generalisation of [6, p. 99] (in which $\mathcal{O}_X$ is assumed to be a DVR). If there is a nonzero map $q : \mathbb{G} \to \mathbb{H}$ then $\mathrm{height}(\mathbb{H}) = \mathrm{height}(\mathbb{G})$ – this is proved as a corollary of the last reference. The Weierstrass preparation Theorem [6, Chapter 1] implies that $\mathcal{O}_{\mathbb{G}}/q^*y$ is freely generated over $\mathcal{O}_X$ by $\{1, x, \ldots, x^{p^m-1}\}$. It is not hard to conclude that these elements also form a basis for $\mathcal{O}_{\mathbb{G}}$ over $q^*\mathcal{O}_{\mathbb{H}}$. □

4. Divisors

By a *divisor* on $\mathbb{G}$ we shall mean a closed subscheme $D \leq \mathbb{G}$ which is finite and flat over X. We briefly record how things work out in our context. The proofs are either easy or parallel to [9, Section 1.1] (for example).

Proposition 13. *If D is a divisor of degree d on $\mathbb{G}$ and x is a coordinate, then there is a unique monic polynomial $f_D(x)$ of degree d such that $\mathcal{O}_D = \mathcal{O}_{\mathbb{G}}/f_D(x)$. Moreover, $f_D(x)$ is the characteristic polynomial of the $\mathcal{O}_X$-linear endomorphism of $\mathcal{O}_D \simeq \mathcal{O}_X^d$ given by multiplication by x, and $f_D(x) = x^d$* $(\mathrm{mod}\, \mathfrak{m})$.

Definition 14. The equation of a divisor D (with respect to a given coordinate x) is the polynomial $f_D(x)$ as above. If $f_D(x) = \sum_{k=0}^{d} c_k x^k$ (with $c_d = 1$) then the *parameters* of D are the coefficients $\{c_0, \ldots, c_{d-1}\}$.

More generally, given a scheme Y over X, a divisor on $\mathbb{G}$ over Y will just mean a divisor on the pulled-back group $\mathbb{G} \times_X Y$.

Because we are assuming that $\mathbb{G}$ has finite height n, the subscheme $\mathbb{G}(m) = \ker(p_{\mathbb{G}}^m : \mathbb{G} \to \mathbb{G}) = \mathrm{spf}(\mathcal{O}_{\mathbb{G}}/(p_{\mathbb{G}}^m)^* x)$ is a divisor of degree p^{mn}.

If a is a section of $\mathbb{G}$ then we write $[a]$ for the associated divisor, which has $f_{[a]}(x) = x - x(a)$. The following lemma provides a useful alternative representation:

Lemma 15. *For any formal group law over any ring A, the power series $x -_F y$ is a unit multiple of $x - y$ in $A[\![x, y]\!]$.*

Proof. $x -_F y$ clearly vanishes mod$(x - y)$. By considering the first few terms, it is easy to see that $(x -_F y)/(x - y)$ must be 1 modulo (x, y), so it is a unit. □

The functor from schemes over X to sets defined by

$$Y \mapsto \{\text{divisors of degree } d \text{ on } \mathbb{G} \text{ over } Y\}$$

is represented by a scheme $\mathrm{Div}_d(\mathbb{G}) = \mathbb{G}^d_X/\Sigma_d$. If x is a coordinate on $\mathbb{G}$ then the ring of functions on this scheme is just the symmetric subring

$$\mathcal{O}_{\mathrm{Div}_d(\mathbb{G})} = \mathcal{O}_X[\![\sigma_1, \dots, \sigma_d]\!] \leq \mathcal{O}_X[\![x_1, \dots, x_d]\!] = \mathcal{O}_{\mathbb{G}^d_X}$$

(where σ_k is the kth elementary symmetric function in the variables x_i). The equation of the universal divisor over this ring is

$$f_D(x) = \prod_k (x - x_k) = \sum_{k=0}^{d} (-1)^k \sigma_k x^{d-k}.$$

The following proposition (taken from [9]) will help us to construct various moduli schemes:

Proposition 16. *Let D, D' be two divisors on $\mathbb{G}$ over X. There is then a closed subscheme $Y \leq X$ such that for any map $a: Z \to X$ we have $a^*D \leq a^*D' \in \Gamma(Z, \mathrm{Div}(\mathbb{G}))$ if and only if a factors through Y.*

Proof. Choose a coordinate x on $\mathbb{G}$, and let d be the degree of D. Then there are unique elements $b_k \in \mathcal{O}_X$ such that

$$f_{D'}(x) = \sum_{k=0}^{d-1} b_k x^k \pmod{f_D(x)}.$$

Put $Y = \mathrm{spf}(\mathcal{O}_X/(b_0, \dots, b_{d-1}))$, and check that this works. □

5. Subgroups and quotient groups

By a *finite subgroup* of $\mathbb{G}$ we shall simply mean a divisor $K < \mathbb{G}$ which is also a subgroup scheme.

Proposition 17. *If K is a finite subgroup of $\mathbb{G}$ then the degree of K is a power of p.*

Proof. It is enough to prove the proposition when $X = X_0 = \mathrm{spec}(\kappa)$, so that $f_K(x) = x^d$. It then follows from the general theory of finite group schemes over a field, but we shall give a direct proof. Let F be the formal group law of $\mathbb{G}$, so that $F(x, y) = x + y \pmod{xy}$. Because K is a subgroup, we have $f_K(F(x, y)) = 0 \pmod{f_K(x),}$

$f_K(y))$. Reading this modulo $(x,y)^{d+1}$, we see that the binomial coefficient $\binom{d}{k}$ is divisible by p when $0 < k < d$. As in Lemma 10, this implies that d is a power of p. □

Proposition 18. *If K is a finite subgroup of $\mathbb{G}$ of degree p^m then $p^m_K = 0$ and thus $K \leq \mathbb{G}(m) = \ker(p^m_{\mathbb{G}})$.*

Proof. This is a special case of a result of Deligne – see [16]. A key point is that one can give a purely equational proof that any element u of a finite Abelian group A of order d has $u^d = 1$. Indeed,

$$\prod_{a\in A} a = \prod_{a\in A} ua = u^d \prod_{a\in A} a. \qquad \square$$

Let K be a finite subgroup of $\mathbb{G}$ of degree p^m. We would like to be able to construct a quotient group $\mathbb{G}/K$. To do this, write μ for the addition map $\mathbb{G} \times_X \mathbb{G} \to \mathbb{G}$ (or any of its restrictions) and $\pi\colon \mathbb{G} \times_X K \to \mathbb{G}$ for the projection. Let $\mathcal{O}_{\mathbb{G}/K}$ be the equaliser

$$\begin{tikzcd} \mathcal{O}_{\mathbb{G}/K} \arrow[r] & \mathcal{O}_{\mathbb{G}} \arrow[r, shift left, "\mu^*"] \arrow[r, shift right, "\pi^*"'] & \mathcal{O}_K \otimes_{\mathcal{O}_X} \mathcal{O}_{\mathbb{G}} \end{tikzcd}$$

Let x be a coordinate on $\mathcal{O}_{\mathbb{G}}$, so that $y = N_\pi \mu^* x \in \mathcal{O}_{\mathbb{G}}$.

Theorem 19. *With K and y as above, we have*

(i) $y = x^{p^m} \pmod{\mathfrak{m}_X}$.

(ii) $\mathcal{O}_{\mathbb{G}/K} = \mathcal{O}_X[\![y]\!]$.

(iii) *$\mathbb{G}/K$ has a natural structure as a formal group.*

(iv) *The projection $\mathbb{G} \to \mathbb{G}/K$ is the categorical cokernel of $K \to \mathbb{G}$.*

(v) *For any map $f\colon Y \to X$ we have $f^*\mathbb{G}/f^*K = f^*(\mathbb{G}/K)$.*

Proof. First, there is a map $\theta\colon \mathbb{G} \times_X K \to \mathbb{G} \times_X K$ defined on points by $\theta(a,b) = (a-b,b)$. This is an automorphism and satisfies $\mu\theta = \pi$. We know that π is a finite flat map, so we conclude that the same is true of μ. Next, let $\pi'\colon \mathbb{G} \times_X K \times_X K \to \mathbb{G} \times_X K$ be the projection on the first two factors, and consider the following commutative squares:

$$\begin{tikzcd} \mathbb{G} \times_X K \times_X K \arrow[r, "1\times\mu"] \arrow[d, "\pi'"'] & \mathbb{G} \times_X K \arrow[d, "\pi"] \\ \mathbb{G} \times_X K \arrow[r, "\pi"'] & \mathbb{G} \end{tikzcd}, \qquad \begin{tikzcd} \mathbb{G} \times_X K \times_X K \arrow[r, "\mu\times 1"] \arrow[d, "\pi'"'] & \mathbb{G} \times_X K \arrow[d, "\pi"] \\ \mathbb{G} \times_X K \arrow[r, "\mu"'] & \mathbb{G} \end{tikzcd}.$$

A diagram chase shows that they are both pullbacks. It follows that all the maps involved are finite flat maps, and that $\pi^* N_\pi = N_{\pi'}(1 \times \mu)^*$, $\mu^* N_\pi = N_{\pi'}(\mu \times 1)^*$. Combining this with the fact that $\mu(1 \times \mu) = \mu(\mu \times 1)$, we see that $y = N_\pi \mu^* x \in \mathcal{O}_{\mathbb{G}}$ actually lies in $\mathcal{O}_{\mathbb{G}/K}$ as claimed. The argument so far follows [3].

Next, write $j\colon K \to \mathbb{G}$ for the inclusion. I claim that $j^*y = 0$. To see this, let $i\colon K \to \mathbb{G} \times_X K$ be the map $a \mapsto (0,a)$, so that $\pi i = 0$ and $\mu i = j$. Thus $j^*\ y = i^*\mu^*y = i^*\pi^*y = 0^*y$. Next consider the diagram

$$\begin{tikzcd}
K \arrow[r, "i"] \arrow[d] & \mathbb{G} \times_X K \arrow[r, "\mu"] \arrow[d, "\pi"] & \mathbb{G} \\
X \arrow[r, "0"'] & \mathbb{G} &
\end{tikzcd}$$

Using Lemma 8 we see that $0^*y = N_{K/X}i^*\mu^*x = N_{K/X}j^*x$. The claim now follows from Lemma 9, using the zero section $X \to K$.

Let f_K be the equation of the divisor K, so that f_K is a monic polynomial of degree p^m and $\ker(j^*) = (f_K(x))$. It thus follows that y is divisible by $f_K(x)$.

From Proposition 13 we know that $\mathcal{O}_K/\mathfrak{m}_X = \kappa[\![x]\!]/x^{p^m}$, so that $\mathcal{O}_{\mathbb{G}\times_X K}/\mathfrak{m}_X = \kappa[\![x,z]\!]/z^{p^m}$. As working mod z is the same as restricting to $\mathbb{G}$, we see that the image of μ^*x in this ring agrees with x mod z. Using the basis $\{1,z,\dots,z^{p^m-1}\}$, we conclude that the norm of μ^*x is just x^{p^m}. However, this norm is just the image of y in $\mathcal{O}_{\mathbb{G}}/\mathfrak{m}_X$, which gives part (i) of the theorem. It follows easily from this that y is a *unit* multiple of $f_K(x)$.

It is not hard to see that there is a commutative diagram

$$\begin{tikzcd}
\mathcal{O}_{\mathbb{G}/K} \arrow[r] \arrow[d, "0^*"'] & \mathcal{O}_{\mathbb{G}} \arrow[r, shift left, "\mu^*"] \arrow[r, shift right, "\pi^*"'] \arrow[d, "j^*"] & \mathcal{O}_K \otimes \mathcal{O}_G \arrow[d, "1\otimes j^*."] \\
\mathcal{O}_X \arrow[r] & \mathcal{O}_K \arrow[r, shift left, "\mu^*"] \arrow[r, shift right, "\pi^*"'] & \mathcal{O}_K \otimes \mathcal{O}_K
\end{tikzcd}$$

Suppose $u \in \mathcal{O}_{\mathbb{G}/K} \leq \mathcal{O}_{\mathbb{G}}$. By the above diagram, $j^*(u - u(0)) = 0$. By the last paragraph, we see that $u - u(0)$ is divisible by y, say $u = u(0) + u'y$ with $u' \in \mathcal{O}_{\mathbb{G}}$. Using the Weierstrass factorisation, we see that π^*y is not a zero divisor in $\mathcal{O}_{\mathbb{G}\times_X K}$. Using this, we can check that $u' \in \mathcal{O}_{\mathbb{G}/K}$. Extending this inductively, we conclude that $\mathcal{O}_{\mathbb{G}/K} = \mathcal{O}_X[\![y]\!]$, giving part (ii) of the theorem.

For part (iii), a diagram chase now shows that $\mathbb{G} \times_X \mathbb{G} \xrightarrow{\mu} \mathbb{G} \xrightarrow{q} \mathbb{G}/K$ factors as $\mathbb{G} \times_X \mathbb{G} \xrightarrow{q\times q} \mathbb{G}/K \times_X \mathbb{G}/K \xrightarrow{v} \mathbb{G}/K$ for a unique map v, which makes $\mathbb{G}/K$ into a formal group with coordinate y. It is easy to see from the definition of $\mathcal{O}_{\mathbb{G}/K}$ that $\mathbb{G}/K$ is the categorical cokernel of j, in other words that a map $r\colon \mathbb{G} \to \mathbb{H}$ of formal groups factors through q if and only if $rj = 0$; this is part (iv). Finally, our construction of y clearly commutes with base change. It follows that $f^*(\mathbb{G}/K) = f^*\mathbb{G}/f^*K$ for any map $f\colon Y \to X$, as claimed in (v). □

6. The universal deformation

Suppose that X_0 is a scheme of the form $\mathrm{spf}(\kappa)$ (where κ is a field of characteristic p), and that $\mathbb{G}_0$ is a formal group over X_0 of finite height n. A *deformation* of $\mathbb{G}_0$ consists of a formal group $\mathbb{H}$ over a scheme Y together with a pullback diagram as follows, exhibiting the restriction of $\mathbb{H}$ to the special fibre of Y as a pullback of $\mathbb{G}_0$.

$$\begin{tikzcd}
\mathbb{H}_0 \arrow[r, "\tilde{f}_0"] \arrow[d] & \mathbb{G}_0 \arrow[d] \\
Y_0 \arrow[r, "f_0"'] & X_0
\end{tikzcd}.$$

Of course, if we start with a group $\mathbb{G}$ over X and define X_0 to be the special fibre of X and $\mathbb{G}_0$ to be the restriction of $\mathbb{G}$ to X_0, then $\mathbb{G}$ is a deformation of $\mathbb{G}_0$ in a tautological way.

A *morphism of deformations* is a pullback square as follows, which is compatible in the obvious sense with the given maps $\mathbb{H}_0 \to \mathbb{G}_0 \leftarrow \mathbb{H}'_0$.

$$\begin{tikzcd}
\mathbb{H} \arrow[r] \arrow[d] & \mathbb{H}' \arrow[d] \\
Y \arrow[r] & Y'
\end{tikzcd}.$$

Recall that the pullback condition means (by definition) that the map $\mathbb{H} \to \mathbb{H}'$ is a fibrewise isomorphism.

In [10] Lubin and Tate construct universal deformations of formal group laws. The following proposition is a simple translation of their result into coordinate-free language.

Proposition 20. *The category of deformations of* $\mathbb{G}_0/X_0$ *has a terminal object* $\mathbb{G}/X$. *Moreover, coordinates can be chosen such that* $\mathcal{O}_X = W[\![u_1,\dots,u_{n-1}]\!]$ (*where* W *is the Witt ring of* κ) *and* $p^*_{\mathbb{G}}x = u_m x^{p^m} \pmod{u_0,\dots,u_{m-1},x^{p^m+1}}$ (*where* $u_0 = p$). *Note that* X *is a smooth scheme of dimension* n, *and* X_0 *is the special fibre of* X. *We refer to* X *as the deformation space of* $\mathbb{G}_0$, *and* $\mathbb{G}$ *as the universal deformation.*

Suppose we start with a group $\mathbb{G}'/X'$, define $X_0 = X'_0$ to be the special fibre of X' and $\mathbb{G}_0 = \mathbb{G}'_0$ the restriction of $\mathbb{G}'$ over X'_0. Let $\mathbb{G}/X$ be the universal deformation of $\mathbb{G}_0/X_0$. There is then a unique map $f : X' \to X$ such that $\mathbb{G}' \simeq f^*\mathbb{G}$. We shall often use only the much weaker corollary that $\mathbb{G}'$ is obtained by pulling back a group over a smooth scheme.

7. Level structures

Let A be a finite Abelian p-group. It is not hard to see that the functor from schemes over X to sets given by $Y \mapsto \mathrm{Hom}(A, \Gamma(Y, \mathbb{G}))$ is represented by a scheme $\mathrm{Hom}(A, \mathbb{G})$ over X. Indeed, we may write A in the form $\bigoplus_{k=0}^{r-1} \mathbb{Z}/p^{d_k}$, and then $\mathrm{Hom}(A, \mathbb{G})$ is isomorphic to the closed subscheme $\prod_k \mathbb{G}(d_k)$ of $\mathbb{G}^r$ (where $\mathbb{G}(d) = \ker(p^d_{\mathbb{G}})$ as usual). If x is a coordinate on $\mathbb{G}$ then $\mathcal{O}_{\mathrm{Hom}(A,\mathbb{G})} = \mathcal{O}_X[\![x_0, \ldots, x_{r-1}]\!]/([p^{d_0}](x_0), \ldots, [p^{d_{r-1}}](x_{r-1}))$. By Proposition 12, this is a finite free module over $\mathcal{O}_X$, in other words the map $\mathrm{Hom}(A, \mathbb{G}) \to X$ is finite and flat. The degree is $|A|^n$.

If $\mathbb{G}$ were a discrete group, it would be natural to write

$$\mathrm{Hom}(A, \mathbb{G}) = \coprod_{B \leq A} \mathrm{Mon}(A/B, \mathbb{G})$$

(where Mon denotes monomorphisms). However, except in trivial cases, there is no scheme $\mathrm{Mon}(A, \mathbb{G})$ over X such that $\mathrm{Mon}(A, \Gamma(Y, \mathbb{G})) = \Gamma(Y, \mathrm{Mon}(A, \mathbb{G}))$. Indeed, by considering the inclusion $\emptyset \to Y$ we see that the left-hand side is not even a functor of Y. The object of the theory of level structures is to approximate the above decomposition as well as possible. The key idea is due to Drinfel'd [5], and some of our results below are parallel to results in [9, Section 1.6].

We write $A(k) = \ker(p^k : A \to A)$. For any map $\phi : A \to \Gamma(Y, \mathbb{G})$ we write $[\phi A]$ for the divisor $\sum_{a \in A} [\phi(a)]$. We also put $\Lambda = (\mathbb{Q}_p/\mathbb{Z}_p)^n$, so that $\Lambda(m) = (\mathbb{Z}/p^m)^n$. Note that $|\mathrm{Hom}(A, \Lambda)| = |A|^n$, which is the same as the degree of $\mathrm{Hom}(A, \mathbb{G}) \to X$. This is the first of many cases in which Λ serves as a "discrete approximation" to $\mathbb{G}$.

Definition 21. A *level-A structure* on $\mathbb{G}$ over an X-scheme Y is a map $\phi : A \to \Gamma(Y, \mathbb{G})$ such that $[\phi A(1)] \leq \mathbb{G}(1)$ as divisors. A level-m structure means a level-$\Lambda(m)$ structure.

The following is very similar to [9, Proposition 1.6.2].

Proposition 22. *The functor from schemes over X to sets given by*

$$Y \mapsto \{\textit{level-}A \textit{ structures on } \mathbb{G} \textit{ over } Y\}$$

is represented by a scheme $\mathrm{Level}(A, \mathbb{G})$ *over X.* (*We will write* $\mathrm{Level}(m, \mathbb{G}) = \mathrm{Level}(\Lambda(m), \mathbb{G})$).

Proof. We can consider $\mathbb{G} \times_X \mathrm{Hom}(A, \mathbb{G})$ as a formal group over $\mathrm{Hom}(A, \mathbb{G})$. On this group we have a tautological map $\phi : A \to \Gamma(\mathrm{Hom}(A, \mathbb{G}), \mathbb{G})$ and thus a divisor $[\phi A(1)] \in \Gamma(\mathrm{Hom}(A, \mathbb{G}), \mathrm{Div}(\mathbb{G}))$. Applying Proposition 16 to this divisor and the divisor $\mathbb{G}(1) \times_X \mathrm{Hom}(A, \mathbb{G})$, we get a closed subscheme $\mathrm{Level}(A, \mathbb{G}) \leq \mathrm{Hom}(A, \mathbb{G})$. It is easy to see that this does the job. □

Suppose that $u\colon A \to B$ is mono, and that $\phi\colon B \to \Gamma(Y, \mathbb{G})$ is a level structure. Then $\phi \circ u$ is clearly a level-A structure, and is thus classified by a map $Y \to \mathrm{Level}(A, \mathbb{G})$. Applying this in the universal case, we obtain a map $u^!\colon \mathrm{Level}(B, \mathbb{G}) \to \mathrm{Level}(A, \mathbb{G})$. This construction is contravariantly functorial.

Theorem 23. $\mathrm{Level}(A, \mathbb{G}) \to X$ *is a finite flat map. If* $\mathbb{G}$ *is the universal deformation of* $\mathbb{G}_0$ *then* $\mathrm{Level}(A, \mathbb{G})$ *is smooth and has dimension* n.

Theorem 24. *If* $\phi\colon A \to \mathbb{G}$ *is a level structure then* $[\phi A]$ *is a subgroup of* $\mathbb{G}$ *and* $[\phi A(k)] \leq \mathbb{G}(k)$ *for all* k. *If* $A = A(m)$ *then* $[\phi A] = \mathbb{G}(m)$.

The proofs of these two theorems will follow after a number of intermediate propositions. Similar results are proved in [5, 9].

Notation. $g_m(x)$ is the Weierstrass polynomial (of degree p^{nm}) which is a unit multiple of $(p^m_{\mathbb{G}})^*(x)$.

Lemma 25. *If* $rank(A) > n$ *then* $\mathrm{Level}(A, \mathbb{G}) = \emptyset$.

Proof. In this case $[\phi A(1)]$ has degree greater than that of $\mathbb{G}(1)$, so we can never have $[\phi A(1)] \leq \mathbb{G}(1)$. □

From now on, we will always assume that A has rank at most n.

Proposition 26. *If* $\mathcal{O}_Y$ *is an integral domain of characteristic zero, then a map* $\phi\colon A \to \Gamma(Y, \mathbb{G})$ *is a level structure if and only if it is injective.*

Proof. Observe that ϕ is injective if and only if $\ker(\phi) \cap A(1) = 0$, so we may assume that $A = A(1)$. Write $x_a = x(\phi(a))$ and

$$y = f_{[\phi A]}(x) = \prod_{a \in A} (x - x_a) \in \mathcal{O}_{\mathbb{G} \times_X Y}.$$

Suppose that ϕ is a level structure. Then for $a \in A \setminus 0$ we have divisibility relations: $x(x - x_a) \mid y \mid p^*_{\mathbb{G}} x = px +$ higher terms. As $p \neq 0$ in R, we must have $x_a \neq 0$ and thus $\phi(a) \neq 0$, as required. Conversely, suppose ϕ is injective. The values x_a as a runs over A are distinct roots of the Weierstrass polynomial $g_1(x)$ defined above. By the usual theory of factorisation over a domain, the product

$$y = \prod_{a \in A} (x - x_a)$$

divides $g_1(x)$, so we have a level structure. □

Proposition 27. *Suppose that* X *is integral. Then there is a prime ideal* $\mathfrak{p} < \mathcal{O}_{\mathrm{Level}(A,\mathbb{G})}$ *with* $\mathfrak{p} \cap \mathcal{O}_X = 0$.

Proof. Let m be large enough that $p^m A = 0$. Let K be the field of fractions of $\mathcal{O}_X$, L the splitting field of g_m over K, and $\mathcal{O}_Y$ the subring of L generated over $\mathcal{O}_X$ by the roots of g_m. These roots are the same as the zeros of $(p^m_{\mathbb{G}})^* x$, so they form a group A' under the operation $+_F$. If we identify a map $a\colon Y \to \mathbb{G}$ over X with the element $x(a) = a^*(x) \in \mathcal{O}_Y$, then $A' = \Gamma(Y, \mathbb{G}(m))$.

Write $y = (p^m_{\mathbb{G}})^* x$. Note that $y = p^m x \pmod{x^2}$, and $p \neq 0$ in L, so y vanishes only to first order at 0. Suppose that a, b are points of $\mathbb{G}$ and $p^m a = 0$. Then $y(a+b) = x(p^m a + p^m b) = y(b)$. It follows that y vanishes only to first order at a. Thus, all the roots of g_m in $\mathcal{O}_Y$ are distinct.

Clearly $A'(1)$ is the set of roots of g_1, and thus has order p^n. Moreover, $p^m A' = 0$ and $|A'| = p^{nm}$. It follows by the structure theory of finite Abelian groups that $A' \simeq (\mathbb{Z}/p^m)^n$, and thus that we can choose an embedding $A \to A'$. By Proposition 26, this is a level structure on $\mathbb{G}$ over Y. It is therefore classified by a map $f\colon Y \to \mathrm{Level}(A, \mathbb{G})$ of schemes over X. We can take $\mathfrak{p}$ to be the kernel of $f^*\colon \mathcal{O}_{\mathrm{Level}(A,\mathbb{G})} \to \mathcal{O}_Y$. □

Remark 28. In geometric language, this says that there is an irreducible component Y of $\mathrm{Level}(A, \mathbb{G})$ such that $Y \to X$ is finite and dominant. We shall see shortly that $Y = \mathrm{Level}(A, \mathbb{G})$.

Corollary 29. *If X is integral then* $\dim(\mathrm{Level}(A, \mathbb{G})) \geq \dim(X)$.

Proposition 30. *If $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$ then* $\mathrm{Level}(A, \mathbb{G})$ *is a smooth scheme of dimension n.*

Proof. Write $E = \mathcal{O}_X = W[\![u_1, \ldots, u_{n-1}]\!]$ (as in Section 6), and $D_A = \mathcal{O}_{\mathrm{Level}(A,\mathbb{G})}$. Suppose that A has rank r, say $A = \langle a_0, \ldots, a_{r-1} \rangle$. Write $x_k = x(\phi(a_k)) \in D_A$. By the proof of Proposition 22, we know that these elements topologically generate D_A over E, so that the u's and x's generate $\mathfrak{m}_{D_A}$. We also put $I = (x_0, \ldots, x_{r-1}, u_r, \ldots, u_{n-1})$. It is enough to show that $D_A/I = \kappa$, for then $\mathrm{embdim}\,\mathrm{Level}(A, \mathbb{G}) \leq n = \dim X \leq \dim \mathrm{Level}(A, \mathbb{G})$. Write $Y = \mathrm{spf}(D_A/I)$. The map $\phi\colon A \to \Gamma(Y, \mathbb{G})$ sends the generators to zero, so it is zero. Thus, $f(x) = f_{[\phi A(1)]}(x) = x^{p^r}$ in $(D_A/I)[x]$. Because ϕ is a level structure, this divides $p^*_{\mathbb{G}} x$. Using the fact (see Section 6) that $p^*_{\mathbb{G}} x = u_m x^{p^m} \pmod{u_0, \ldots, u_{m-1}, x^{p^m+1}}$, we find that $u_0, \ldots, u_{r-1}$ vanish in D_A/I. Of course, the rest of the u's also vanish by definition of I. As the u's and x's generate $\mathfrak{m}_{D_A}$, this implies that $D_A/I = \kappa$ as claimed. □

Proposition 31. *For any $\mathbb{G}$, the projection* $\mathrm{Level}(A, \mathbb{G}) \to X$ *is a finite flat map.*

Proof. We may assume that $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$, as the general case is easily recovered by base change. As $\mathrm{Level}(A, \mathbb{G})$ is a closed subscheme of $\mathrm{Hom}(A, \mathbb{G})$ and $\mathrm{Hom}(A, \mathbb{G}) \to X$ is a finite flat map, we see that $\mathrm{Level}(A, \mathbb{G}) \to X$ is finite. By Propositions 27 and 30, we see that it is also dominant. A finite dominant map of smooth schemes is flat (Lemma 1). □

Proposition 32. *If ϕ is a level structure then $[\phi A(k)]$ is a subgroup scheme contained in $\mathbb{G}(k)$.*

Proof. We may assume that $A = A(k)$, so that $p^kA = 0$. Suppose for the moment that the base scheme X is integral. As in the proof of Proposition 27, we see that the Weierstrass polynomial g_k has distinct roots. By Proposition 26, ϕ is injective, so the polynomials $x - x_a$ for $a \in A$ are distinct factors of $g_k(x)$. It follows that $\prod_a(x - x_a)$ divides $g_k(x)$, so that $[\phi A] \leq \mathbb{G}(k)$ as claimed.

Next, write

$$z = \prod_{a\in A}(x -_F x_a) = (\text{unit}) \times \prod_{a\in A}(x - x_a).$$

In other words, for any point b of $\mathbb{G}$ we have

$$z(b) = \prod_{a\in A} x(b - \phi(a)).$$

Write $\mathbb{H} = \operatorname{spf}(\mathscr{O}_X[\![z]\!])$, so $\mathbb{H}$ is a quotient scheme of $\mathbb{G}$. By the Weierstrass preparation theorem, we see that $q \colon \mathbb{G} \longrightarrow \mathbb{H}$ is flat, of degree $|A|$.

We can let A act on $\mathbb{G}$, with $a \in A$ acting as translation by $\phi(a)$. This action is faithful, because ϕ is injective. The map $q \colon \mathbb{G} \longrightarrow \mathbb{H}$ clearly factors through $\mathbb{G}/A$. It follows from Lemma 7 that $\mathbb{H} = \mathbb{G}/A$ and that q is Galois. Similarly, we find that $(\mathbb{G} \times_X \mathbb{G})/(A \times A) = \mathbb{H} \times_X \mathbb{H}$. Using these descriptions, it is easy to construct a (unique) multiplication on $\mathbb{H}$ such that q is an isogeny of formal groups. The kernel of q is just $\operatorname{spf}(\mathscr{O}_{\mathbb{G}}/z) = [\phi A]$, so $[\phi A]$ is a subgroup scheme as claimed.

Now suppose that X is not integral. Let $\mathbb{G}'/X'$ be the universal deformation of $\mathbb{G}_0$, and ϕ' the universal level structure defined over $\operatorname{Level}(A, \mathbb{G}')$. By Proposition 30, we know that $\operatorname{Level}(A, \mathbb{G}')$ is integral, so the above tells us that $[\phi' A(k)]$ is a subgroup scheme contained in $\mathbb{G}'(k)$. Using the defining properties of X' and $\operatorname{Level}(A, \mathbb{G}')$, we construct a map $f : X \longrightarrow \operatorname{Level}(A, \mathbb{G}')$ such that the pullback of $\mathbb{G}'$ is $\mathbb{G}$ and the pullback of ϕ' is ϕ. It follows that $[\phi A(k)] = f^*[\phi' A(k)]$ is a subgroup scheme of $\mathbb{G}(k)$, as claimed. □

Corollary 33. *It follows from the above proof that $z = \prod_{a\in A}(x -_F x_a)$ is a coordinate on the quotient group $\mathbb{G}/[\phi A]$.*

8. Galois theory of level structures

In this section, we assume that $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$. We write

$$D_A = \mathscr{O}_{\operatorname{Level}(A,\mathbb{G})}, \quad D_m = \mathscr{O}_{\operatorname{Level}(m,\mathbb{G})}, \quad E = D_0 = \mathscr{O}_X,$$

$$K_A = \text{ field of fractions of } D_A.$$

Theorem 34. *Let A and B be finite Abelian p-groups of rank at most n, and $u: A \to B$ a monomorphism. Then*:

(i) $\mathrm{Hom}_E(D_A, D_B) = \mathrm{Hom}_K(K_A, K_B) = \mathrm{Mon}(A, B)$.

(ii) *The map* $u^!: \mathrm{Level}(B, \mathbb{G}) \to \mathrm{Level}(A, \mathbb{G})$ (*which sends* ϕ *to* $\phi \circ u$) *is finite and flat.*

(iii) *If* $B \simeq \Lambda(m)$ *then* $u^!$ *is a Galois covering.*

(iv) *The torsion subgroup of* $\Gamma(\mathrm{Level}(A, \mathbb{G}), \mathbb{G})$ *is* A.

The proof will follow after a number of lemmas.

Lemma 35. $\mathrm{Hom}_K(K_A, K_B) = \mathrm{Hom}_E(D_A, D_B) = \mathrm{Mon}(A, \Gamma(D_B, \mathbb{G}))$.

Proof. By applying Lemma 2 to a sequence of maps $\mathrm{Level}(B, \mathbb{G}) \to \mathrm{Level}(A, \mathbb{G}) \to X$, we see that every E-algebra map $D_A \to D_B$ is a monomorphism, and thus induces a map $K_A \to K_B$ of the fields of fractions. Conversely, consider a K-algebra map $K_A \to K_B$. The image of D_A is integral over E, hence over D_B. As D_B is a unique factorisation domain (by Theorem 23), it is integrally closed in its field of fractions. Thus, the image of D_A is contained in D_B. It follows that $\mathrm{Hom}_K(K_A, K_B) = \mathrm{Hom}_E(D_A, D_B)$. On the other hand, the defining property of D_A implies that $\mathrm{Hom}_E(D_A, D_B) = \{$level-$A$ structures on$\mathbb{G}$ over $D_B\}$. By Proposition 26, this is just $\mathrm{Mon}(A, \Gamma(D_B, \mathbb{G}))$. □

Lemma 36. $\mathrm{Aut}(\Lambda(m))$ *acts transitively on* $\mathrm{Mon}(A, \Lambda(m))$.

Proof. Without loss of generality, we may assume that there is a monomorphism $A \to \Lambda(m)$, and thus think of A as a subgroup of $\Lambda(m)$. Suppose that $\phi: A \to \Lambda(m)$ is a mononomorphism other than the inclusion. Our task is then to find an automorphism ψ of $\Lambda(m)$ extending ϕ. By elementary linear algebra over $\mathbb{F}_p$, the map $\phi_1: A(1) \to \Lambda(1)$ extends to an automorphism of $\Lambda(1)$. This patches with ϕ to give a map $\psi_0: A + \Lambda(1) \to \Lambda(m) \leq \Lambda$. As Λ is a divisible group, it is injective, so ψ_0 extends to a map $\psi: \Lambda(m) \to \Lambda$. The image must be killed by p^m, so we actually have $\psi: \Lambda(m) \to \Lambda(m)$. This is iso on $\Lambda(1)$, so the kernel of ψ contains no points of order p, so ψ itself is mono. By counting, ψ must be iso. Thus $\psi \in \mathrm{Aut}(\Lambda(m))$ and $\psi|_A = \phi$ as required. □

Lemma 37. *Let B be a subgroup of* $\Lambda(m)$, *and set*

$$\Gamma = \{\alpha \in \mathrm{Aut}(\Lambda(m)) \text{ such that } \alpha|_B = 1_B\}.$$

Then the group of fixed points of Γ is just B.

Proof. Suppose that $u \notin B$. We need to construct $\alpha \in \Gamma$ with $\alpha(u) \neq u$. Suppose that u generates a cyclic subgroup C of order p^l, and that $C' = C \cap B$ is generated by $p^k u$ and so has order $p^{l-k} < p^l$. We can then construct an automorphism α of $A = B + C$

by defining $\alpha(b+c) = b + (1 + p^{l-k})\ c$ when $b \in B$ and $c \in C$ (it is not hard to check that this is well-defined). This in turn extends to an automorphism of $A(m)$ by Lemma 36. It sends u to $(1 + p^{l-k})\ u \neq u$. □

Note that K_m is generated over K by roots of the Weierstrass polynomial g_m, which splits completely over K_m. Thus K_m is the splitting field of g_m, and so is Galois over K. We can also see that $A(m)$ is the full group of points of order p^m in $\Gamma(D_m, \mathbb{G})$, as g_m can only have $\deg(g_m) = p^{mn} = |A(m)|$ roots. It follows using Lemma 35 that $\mathrm{Gal}(K_m/K) = \mathrm{Aut}_K(K_m) = \mathrm{Aut}(A(m))$. Moreover, if $p^m A = 0$ then K_A is generated by a subset of the roots of g_m, so that K_m contains a normal closure of K_A. The degree of the extension $K \to K_A$ is just the number of embeddings of K_A in the normal closure, so $[K_A : K] = |\mathrm{Hom}_K(K_A, K_m)| = |\mathrm{Mon}(A, A(m))|$.

Lemma 38. $\mathrm{Hom}_K(K_A, K_B) = \mathrm{Mon}(A, B)$.

Proof. The extension K_m/K_B is Galois as K_m/K is. Moreover, the subgroup of $\mathrm{Gal}(K_m/K)$ fixing K_B is just the group $\Gamma \leq \mathrm{Aut}(A(m))$ of Lemma 37. By the fundamental theorem of Galois theory, the fixed field of Γ is just K_B. Thus $\mathrm{Hom}_K(K_A, K_B)$= $\mathrm{Hom}_K(K_A, K_m)^\Gamma = \mathrm{Mon}(A, A(m))^\Gamma = \mathrm{Mon}(A, B)$, the last equality coming from Lemma 37. □

Corollary 39. *The torsion subgroup of $\Gamma(D_B, \mathbb{G})$ is B.*

Proof. This follows easily by comparing Lemma 38 with Lemma 35. □

Proof of Theorem 34. Part (i) follows immediately from Lemmas 35 and 38. It follows that all the maps $u^!: \mathrm{Level}(B, \mathbb{G}) \to \mathrm{Level}(A, \mathbb{G})$ are dominant. Both the source and target are smooth by Theorem 23, so $u^!$ is flat by Lemma 1. This gives (ii). Now suppose that $B \simeq A(m)$, so without loss of generality $A \leq B = A(m)$. We have seen above that K_m/K_A is Galois, so Lemma 6 tells us that $u^!$ is a Galois covering. This gives (iii). Finally, (iv) is Corollary 39.

We can use the above theory to understand the structure of D_A more explicitly. For simplicity, assume that $A = \mathbb{Z}/p^k \oplus \mathbb{Z}/p^l$, with $k \geq l$ (the extension to groups of larger rank is evident). It is clear that $g_k(x)$ is divisible by $g_{k-1}(x)$, say $g_k(x) = g_{k-1}(x)h_k(x)$ for some Weierstrass polynomial h_k of degree $p^{nk} - p^{n(k-1)}$. Let D' be the subring of D_A generated over E by the root $x_0 = x(\phi(a_0))$ of $h_k(x)$. Over D', the series $h_l(x)$ has $p^l - p^{l-1}$ roots, $\{x(jp^{k-l}a_0) \,|\, 0 < j < p^l,\ j \neq 0 \pmod p\}$. After dividing out the corresponding linear factors, we obtain a Weierstrass polynomial $f(x)$ of degree $p^{nl} - p^{n(l-1)} - p^l + p^{l-1}$. The ring D_A is generated over D' by a root $x_1 = x(\phi(a_1))$ of this polynomial. It is not hard to see that the product of the degrees of h_k and f is the same as the rank $|\mathrm{Mon}(A, A)|$ of D_A over E. It follows that $D_A = E[\![x_0, x_1]\!]/(h_k(x_0), f(x_1))$. □

9. Quotients by level structures

Let $\mathbb{G}_0$ be a formal group of height n over $X_0 = \mathrm{spec}(\kappa)$. For every m, the divisor $p^m[0]$ is a subgroup of $\mathbb{G}_0$. We write $\mathbb{G}_0\langle m\rangle$ for the quotient group $\mathbb{G}_0/p^m[0]$, and $\mathbb{G}\langle m\rangle \to X\langle m\rangle$ for the universal deformation of $\mathbb{G}_0\langle m\rangle \to X_0$. Note that $\mathbb{G}_0(1) = \ker(p_{\mathbb{G}_0}\colon \mathbb{G}_0 \to \mathbb{G}_0) = p^n[0]$. It follows that $p_{\mathbb{G}_0}$ induces an isomorphism $\mathbb{G}_0\langle m+n\rangle \to \mathbb{G}_0\langle m\rangle$. We use this to identify $X\langle m+n\rangle$ with $X\langle m\rangle$ and $\mathbb{G}\langle m+n\rangle$ with $\mathbb{G}\langle m\rangle$.

Proposition 40. *Let $u\colon A \to B$ be an epimorphism of finite Abelian p-groups, with $|\ker(u)| = p^l$ say. Then u induces a map*

$$u_!\colon \mathrm{Level}(A, \mathbb{G}\langle m\rangle) \to \mathrm{Level}(B, \mathbb{G}\langle m+l\rangle).$$

Proof. Let ϕ be the universal level-A structure on $\mathbb{G}\langle m\rangle$, which is defined over the scheme $Y = \mathrm{Level}(A, \mathbb{G}\langle m\rangle)$. Write $K = [\phi \ker(u)]$. This is a subgroup divisor on $\mathbb{G}\langle m\rangle$, whose restriction to the special fibre of Y is $K_0 = p^l[0]$. It follows that $\mathbb{G}\langle m\rangle/K$ is a deformation of $\mathbb{G}_0\langle m+l\rangle$. The composite $\ker(u) \to A \xrightarrow{\phi} \Gamma(Y, \mathbb{G}\langle m\rangle) \to \Gamma(Y, \mathbb{G}\langle m\rangle/K)$ is clearly zero. This gives a map $\psi\colon B \to \Gamma(Y, \mathbb{G}\langle m\rangle/K)$. I claim that this is a level structure. As $\mathcal{O}_Y$ is an integral domain of characteristic zero, it is enough to show that ψ is injective (Proposition 26). Suppose $a \in B \setminus \ker(u)$, and let x be a coordinate on $\mathbb{G}\langle m\rangle$. In view of Corollary 33, we need only check that the following product does not vanish:

$$z(\phi a) = \prod_{c\in\ker(u)} x(\phi a - \phi c) = \prod_{c\in\ker(u)} x(\phi(a-c)).$$

Because ϕ is a level structure, $a - c \neq 0$, and $\mathcal{O}_Y$ is an integral domain, we conclude that $x(\phi(a-c)) \neq 0$. It follows that $z(\phi(a)) \neq 0$ as required.

The level structure ψ is classified by a map $\mathrm{Level}(A, \mathbb{G}\langle m\rangle) \to \mathrm{Level}(B, \mathbb{G}\langle m+l\rangle)$, which we take to be $u_!$. □

In particular, if $|A| = p^l$ then the maps $0 \xrightarrow{0} A \xrightarrow{0} 0$ induce maps

$$0^!\colon \mathrm{Level}(A, \mathbb{G}\langle m\rangle) \to \mathrm{Level}(0, \mathbb{G}\langle m\rangle) = X\langle m\rangle$$

$$0_!\colon \mathrm{Level}(A, \mathbb{G}\langle m\rangle) \to \mathrm{Level}(0, \mathbb{G}\langle m+l\rangle) = X\langle m+l\rangle.$$

The first of these is just the usual projection.

Theorem 41.

(1) *$u_!$ is a covariant functor of u.*

(2) *$u_!$ is a finite flat map.*

(3) *The maps $0 \xrightarrow{0} A(l) \xrightarrow{0} 0$ give the same map*

$$0^! = 0_!\colon \mathrm{Level}(l, \mathbb{G}\langle m\rangle) \to X\langle m\rangle = X\langle m+n\rangle.$$

(4) *Consider a commutative square as follows.*

$$\begin{tikzcd}
A \arrow[r, tail, "r"] \arrow[d, two heads, "u"'] & B \arrow[d, two heads, "v"] \\
C \arrow[r, tail, "s"'] & D
\end{tikzcd}$$

This is a pullback if and only if it is a pushout. If so, then

$$s^! v_! = u_! r^! \colon \mathrm{Level}(B, \mathbb{G}\langle m\rangle) \to \mathrm{Level}(C, \mathbb{G}\langle m+l\rangle)$$

(*where* $|\ker(u)| = p^l = |\ker(v)|$).

(5) *If* u *is iso then* $u_! = (u^!)^{-1} = (u^{-1})^!$.

(6) *If* $A \simeq \Lambda(m)$ *then* $u_!$ *is a Galois covering, with Galois group* $\Gamma = \{\alpha \in \mathrm{Aut}(A) \mid u\alpha = u\}$.

(7) *The maps* $0_! \colon \mathrm{Level}(B, \mathbb{G}\langle m\rangle) \to X\langle m+l\rangle$ *and* $0^! \colon \mathrm{Level}(B, \mathbb{G}\langle m\rangle) \to X$ *have the same degree.*

Proof. We can take $m = 0$ without loss of generality, and assume that $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$.

(1) This is clear.

(2) This will be proved after (3).

(3) The map $0^! \colon \mathrm{Level}(l, \mathbb{G}) \to X$ is just the originally given projection, so the group over $\mathrm{Level}(l, \mathbb{G})$ with which we implicitly start is just $(0^!)^*\mathbb{G}$. We have a universal level structure $\phi \colon \Lambda(l) \to (0^!)^*\mathbb{G}$. By Theorem 24, we have $[\phi\Lambda(l)] = \mathbb{G}(l)$. By the definition of the map $0_!$, we have an isomorphism

$$(0^!)^*\mathbb{G}/\mathbb{G}(l) = (0^!)^*\mathbb{G}/[\phi\Lambda(l)] \to 0_!^*\mathbb{G}\langle nl\rangle$$

whose restriction to the special fibre is just the identity map of $\mathbb{G}_0/p^{nl}[0]$. After using our standard identification of $\mathbb{G}\langle nl\rangle$ with $\mathbb{G}$, we get an isomorphism

$$(0^!)^*\mathbb{G}/\mathbb{G}(l) \to 0_!^*\mathbb{G}$$

whose restriction to the special fibre is the map

$$p^l_{\mathbb{G}_0} \colon \mathbb{G}_0/p^{nl}[0] \to \mathbb{G}_0.$$

Because $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$, the map $0_!$ is uniquely characterised by the existence of such an isomorphism. On the other hand, we have an isomorphism

$$p^l_{\mathbb{G}} \colon (0^!)^*\mathbb{G}/\mathbb{G}(l) \to (0^!)^*\mathbb{G}$$

which has the same effect on the special fibre. It follows that $0_! = 0^!$.

(2) Choose an epimorphism $v \colon \Lambda(l) \longrightarrow A$ (for some large l). We thus have a chain of epimorphisms $\Lambda(l) \xrightarrow{v} A \xrightarrow{u} B \xrightarrow{0} 0$. This gives maps as follows, where the $*$'s refer to various integers:

$$\mathrm{Level}(l, \mathbb{G}\langle *\rangle) \xrightarrow{v_!} \mathrm{Level}(A, \mathbb{G}\langle *\rangle) \xrightarrow{u_!} \mathrm{Level}(B, \mathbb{G}\langle *\rangle) \xrightarrow{0_!} X\langle *\rangle.$$

By (3), we know that the full composite $0_! u_! v_!$ is finite and dominant. All the schemes involved are smooth (and thus integral) and have dimension n. Applying Lemma 2 twice, we see that $u_!$ is finite and dominant. It is therefore flat, by Lemma 1.

(4) Consider the following sequence

$$A \xrightarrow{\binom{r}{u}} B \oplus C \xrightarrow{(v-s)} D.$$

The left hand map is mono (because r is), the right hand map is epi (because v is) and the composite is zero (because the diagram commutes). It is easy to see from this that the sequence is exact if and only if the square is a pushout, if and only if the square is a pullback. If so, we write $E = \ker(u)$ and observe that $r\colon E \simeq \ker(v)$. Write $Y = \mathrm{Level}(B, \mathbb{G})$, so we have a level structure $\phi\colon B \to \Gamma(Y, \mathbb{G})$. We define maps ψ and χ by requiring that the following diagrams commute:

$$\begin{tikzcd}
A \arrow[r, tail, "r"] \arrow[d, "u"'] & B \arrow[r, "\phi"] \arrow[d, "v"] & \Gamma(Y, \mathbb{G}) \arrow[d] \\
C \arrow[r, tail, "s"'] & D \arrow[r, "\psi"'] & \Gamma(Y, \mathbb{G}/[\phi r E])
\end{tikzcd}$$

$$\begin{tikzcd}
A \arrow[r, "\phi r"] \arrow[d, "u"'] & \Gamma(Y, \mathbb{G}) \arrow[d] \\
D \arrow[r, "\chi"'] & \Gamma(Y, \mathbb{G}/[\phi r E])
\end{tikzcd}$$

The two maps $u_! r^!$ and $s^! v_!$ from Y to $\mathrm{Level}(C, \mathbb{G}\langle l\rangle)$ classify the two level structures χ and $\psi \circ s$ on $\mathbb{G}/[\phi r E]$. On the other hand, it is clear from the above diagrams that these level structures are the same.

(5) Apply (4) with $s = u^{-1}$ and $r = v = 1$.

(6) By (3) and Theorem 34, we know that the composite $\mathrm{Level}(A, \mathbb{G}) \xrightarrow{u!}$ $Level(B, \mathbb{G}\langle l\rangle) \xrightarrow{0!} Xnm$ is a Galois covering. Using Lemma 6 to reduce to the case of field extensions, we see that $u_!$ is Galois. Referring again to Theorem 34, we see that the Galois group is $\Gamma = \{\alpha \in \mathrm{Aut}(A) \mid u_! \alpha^! = u_!\}$. Using (5) and the fact that level structures over integral domains in characteristic zero are injective, we conclude that $\Gamma = \{\alpha \in \mathrm{Aut}(A) \mid u = u\alpha\}$.

(7) Choose an epimorphism $u\colon A = \Lambda(l) \to B$, and let Γ be as above. By the Pontrjagin dual of Lemma 36, we see that

$$\deg(0_!) = |\mathrm{Aut}(A)/\Gamma| = |\mathrm{Mon}(A^*, \Lambda(l)^*)| = |\mathrm{Epi}(\Lambda(l), A)|$$

(where $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ etc.). As there are (unnatural) isomorphisms $A \simeq A^*$ and $\Lambda(l) \simeq \Lambda(l)^*$, we see that

$$\deg(0_!) = |\mathrm{Mon}(A, \Lambda(l))| = |\mathrm{Mon}(A, A)|.$$

By Theorem 34, this is the same as the degree of $\deg(0^!)$. □

10. Classification of subgroups

We now fix $m \geq 0$ and study the classification of subgroups of $\mathbb{G}$ of degree p^m.

Theorem 42. *The functor from schemes over X to sets given by*

$$Y \mapsto \{\textit{subgroups of } \mathbb{G} \times_X Y \textit{ of degree } p^m\}$$

is represented by a scheme $\mathrm{Sub}_m(\mathbb{G})$ *over X. Moreover, for any map $X' \to X$ we have*

$$X' \times_X \mathrm{Sub}_m(\mathbb{G}) = \mathrm{Sub}_m(X' \times_X \mathbb{G}).$$

The projection $\mathrm{Sub}_m(\mathbb{G}) \to X$ *is a finite flat map, of degree*

$$d = |\mathrm{Sub}_m(\Lambda)| = \textit{ number of subgroups of } \Lambda \textit{ of order } p^m \ .$$

Formulae for d will be given later. The scheme $\mathrm{Sub}_m(\mathbb{G})$ *is Gorenstein.*

The rest of this section will constitute the proof. The existence and behaviour under pullback of $\mathrm{Sub}_m(\mathbb{G})$ is given by [9, Corollary 1.3.7]. In Section 10.1, we prove some combinatorial formulae. In Section 10.2, we apply these formulae in an argument inspired by the theory of Gröbner bases to give an upper bound for the degree of the map $\mathrm{Sub}_m(\mathbb{G}) \to X$. In Section 10.3, we analyse what happens when we invert p and thus make all finite subgroups étale (cf. [9, Corollary 3.7.2]). In Section 10.4, we assemble these results to prove the theorem, except for the fact that $\mathrm{Sub}_m(\mathbb{G})$ is Gorenstein, which is proved in Section 10.5

10.1. Combinatorics

We write $\Lambda^* = \mathrm{Hom}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Z}_p^n$. Note that $d(m,n)$ is also the number of lattices L of index p^m in Λ^*. Any lattice $L \leq \Lambda^*$ has the form $M.\mathbb{Z}_p^n$ for some matrix $M \in M_n(\mathbb{Z}_p)$ with $\det(M) \neq 0$, and two matrices give the same lattice if and only if they are related by reversible column operations.

Notation. Given a sequence $(\alpha_k, \alpha_{k+1}, \ldots, \alpha_{n-1})$ we write

$$|\alpha| = \sum_j \alpha_j, \quad \|\alpha\| = \sum_j j\alpha_j.$$

If $n = 1$ we allow the empty sequence, with $|\alpha| = \|\alpha\| = 0$.

Lemma 43. *Every matrix in $M \in M_n(\mathbb{Z}_p)$ with* $\det(M) \neq 0$ *can be reduced by reversible column operations to a unique matrix of the following form (we show the* *case $n = 4$, but the generalisation is evident). Equivalently, any lattice $L \leq \Lambda^*$ has a unique basis given by the columns of such a matrix.*

$$\begin{pmatrix} p^{\alpha_0} & 0 & 0 & 0 \\ a_{01} & p^{\alpha_1} & 0 & 0 \\ a_{02} & a_{12} & p^{\alpha_2} & 0 \\ a_{03} & a_{13} & a_{23} & p^{\alpha_3} \end{pmatrix} \qquad 0 \leq a_{kl} < p^{\alpha_l}.$$

The index of such a lattice is $p^{|\alpha|}$.

Proof. We find an element of minimal valuation in the top row and move the corresponding column to the left hand end. We then multiply this column by a unit to get p^{α_0} at the top left, and then perform column operations to clear the rest of the top row. By induction, we can reduce the $(n-1) \times (n-1)$ submatrix at the bottom right to the desired form. A few more evident column operations put the entries in the first column into the stated range. It is now not hard to see that α_k is the minimal valuation of b_k among vectors of the form $(0, \dots, 0, b_k, \dots, b_{n-1})$ in the lattice $L = M.\Lambda^*$. Moreover, the $(k+1)$th column above is the unique such vector with $b_k = p^{\alpha_k}$ and $0 \leq b_l < p^{\alpha_l}$ for $l > k$. This gives uniqueness. It is not hard to see that the vectors $\underline{b}$ with $0 \leq b_k < p^{\alpha_k}$ form a transversal for L in Λ^*, so that $|\Lambda^*/L| = p^{|\alpha|}$. □

Corollary 44. *If α runs over sequences $(\alpha_1, \dots, \alpha_{n-1})$ with $|\alpha| \leq m$ then*

$$d(m,n) = \sum_{\alpha} p^{\|\alpha\|}.$$

It follows that

$$Z_n(t) = \sum_{l} d(m,n)t^m = \prod_{k=0}^{n-1} \frac{1}{1 - p^k t}.$$

Proof. The first statement follows by counting the possible matrices in the lemma in the obvious way. Next, write

$$(1 - p^k t)^{-1} = \sum_{\alpha_k \geq 0} p^{k\alpha_k} t^{\alpha_k}.$$

The second claim follows by expanding out the product. □

We can also give a somewhat more explicit formula for $d(m,n)$. First, we recall the definition of the Gaussian binomial coefficients:

$$\begin{bmatrix} k \\ l \end{bmatrix}_p = \prod_{m=0}^{l-1} \frac{p^k - p^m}{p^l - p^m} = \prod_{m=1}^{l} \frac{p^{k-l+m} - 1}{p^m - 1}.$$

This can also be interpreted as the number of l-dimensional subspaces of a k-dimensional vector space over $\mathbb{F}_p$.

Lemma 45. *The Gaussian binomial coefficients satisfy*

$$\begin{bmatrix} k \\ l \end{bmatrix}_p = \begin{bmatrix} k \\ k-l \end{bmatrix}_p \quad \textit{and} \quad \begin{bmatrix} k \\ l \end{bmatrix}_p = \begin{bmatrix} k-1 \\ l-1 \end{bmatrix}_p + p^l \begin{bmatrix} k-1 \\ l \end{bmatrix}_p .$$

Proof. Suppose $\dim_{\mathbb{F}_p} V = k$. There is an obvious bijection $W \mapsto \operatorname{ann}(W)$ between l-dimensional subspaces of V and $(k-l)$-dimensional subspaces of V^*, which gives the first statement. Now write $V = L \oplus U$ with $\dim L = 1$. Let $W \le V$ have dimension l. If W contains L then it has the form $L \oplus W'$ for a unique $(l-1)$-dimensional subspace of U; there are

$$\begin{bmatrix} k-1 \\ l-1 \end{bmatrix}_p$$

such W's. If W does not contain L then it is the graph of a unique linear map $W'' \to L$ for a unique l-dimensional subspace $W'' \le U$; this occurs

$$p^l \begin{bmatrix} k-1 \\ l \end{bmatrix}_p$$

times. The second claim follows. □

Lemma 46.

$$d(m,n) = \begin{bmatrix} n+m-1 \\ n-1 \end{bmatrix}_p .$$

Proof. We know that

$$Z_n(t) = \sum_m d(m,n)t^m = \prod_{k=0}^{n-1} \frac{1}{1-p^k t}.$$

We want to show that this is the same as

$$W_n(t) = \sum_m \begin{bmatrix} n+m-1 \\ n-1 \end{bmatrix}_p t^m.$$

It is enough to show that $Z_1(t) = W_1(t)$ (which is immediate) and that $(1-p^{n-1}t)$ $W_n(t) = W_{n-1}(t)$. This follows easily from the equation

$$\begin{bmatrix} m+n-1 \\ n-1 \end{bmatrix}_p - p^{n-1} \begin{bmatrix} m+n-2 \\ n-1 \end{bmatrix}_p = \begin{bmatrix} m+n-2 \\ n-2 \end{bmatrix}_p ,$$

which follows in turn from Lemma 45. □

We shall need another auxiliary numerical function. Fix m and n. For $0 \le l \le n$ and $0 \le k$ we define

$$e(k,l) = \sum_\alpha p^{\|\alpha\|} \quad \text{where } \alpha = (\alpha_l, \ldots, \alpha_{n-1}) \text{ and } k + |\alpha| \le m.$$

Of course, we have $e(0,1) = d(m,n)$. If $l = n$ we again allow α to be the empty sequence, with $|\alpha| = \|\alpha\| = 0$. Thus $e(k,n) = 1$ provided that $k \leq m$.

Lemma 47. *$e(k,l)$ is the unique function with the properties*

$$\begin{aligned} e(k,n) &= 1 && \text{if } k \leq m, \\ e(k,l) &= 0 && \text{if } k > m, \\ e(k,l) &= e(k,l+1) + p^l e(k+1,l) && \text{if } l < n. \end{aligned}$$

Proof. It is clear that $e(k,l)$ has the first two properties. For the third, recall that $e(k,l) = \sum\{p^{\|\alpha\|} \mid \alpha = (\alpha_l, \ldots, \alpha_{n-1}) \text{ and } k + |\alpha| \leq m\}$. The sum of the terms with $\alpha_l = 0$ is just $e(k,l+1)$. If $\alpha_l > 0$ then we can write $\beta_l = \alpha_l - 1$ and $\beta_j = \alpha_j$ for $j > l$. Then $|\alpha| = 1 + |\beta|$ and $\|\alpha\| = l + \|\beta\|$. The sum of the terms with $\alpha_l > 0$ is thus $\sum\{p^l p^{\|\beta\|} \mid \beta = (\beta_l, \ldots, \beta_{n-1}) \text{ and } k + 1 + |\beta| \leq m\}$. This is just $p^l e(k+1,l)$. It is easy to see that these properties characterise e uniquely. □

10.2. Infinitesimal theory

In this section, we study the scheme $\mathrm{Sub}_m(\mathbb{G}_0)$ (which is the same as $X_0 \times_X \mathrm{Sub}_m(\mathbb{G})$). We first give a lemma which is slightly more general than what we need in this section, but the extra generality will be useful later.

Lemma 48. *Let B be a finite-dimensional κ-algebra, and suppose that elements $b_0, \ldots, b_m \in B$ satisfy $\prod_i b_i^{n_i} = 0$ with $n_i > 0$ for all i. Then*

$$\dim_\kappa B \leq \sum_i n_i \dim_\kappa B/b_i.$$

Proof. Write $b' = \prod_{i>0} b_i^{n_i}$ (so that $b_0^{n_0} b' = 0$). For $0 \leq j < n_0$, the space Bb_0^j/Bb_0^{j+1} is a cyclic module over B/b_0. Moreover, $Bb_0^{n_0}$ is a cyclic module for B/b'. It follows that $\dim_\kappa B \leq n_0 \dim_\kappa B/b_0 + \dim_\kappa B/b'$. By induction on m, we find that

$$\dim_\kappa B/b' \leq \sum_{i>0} n_i \dim_\kappa B/(b', b_i) = \sum_{i>0} n_i \dim_\kappa B/b_i.$$

The claim follows. □

Proposition 49. $\deg[\mathrm{Sub}_m(\mathbb{G}) \to X] \leq d(m,n)$.

Proof. Write $Y = \mathrm{Sub}_m(\mathbb{G}_0)$ and $E' = \mathcal{O}_Y$ and $\mathbb{H} = \mathbb{G} \times_X Y$. Note that $\mathbb{H}$ has strict height n. We have a universal subgroup $K < \mathbb{H}$ of degree p^m and a quotient map $q\colon \mathbb{H} \to \mathbb{H}/K$. Note that q has height m and $\mathbb{H}/K$ has height n. Let $Y(k,l)$ be the closed subscheme of Y on which q has strict height at least k and $\mathbb{H}/K$ has strict height at least l, and write

$$E'(k,l) = \mathcal{O}_{Y(k,l)}, \quad e'(k,l) = \dim_\kappa E'(k,l).$$

Because $p = 0$ in κ we have $Y = Y(0,1)$. Clearly also $Y(k,l) = \emptyset$ and $e'(k,l) = 0$ if $k > m$.

Next, recall that $Y = \mathrm{Sub}_m(\mathbb{G}_0)$ is a closed subscheme of $\mathrm{Div}_{p^m}(\mathbb{G}_0)$. To see what this means more explicitly, choose coordinates x and y on $\mathbb{H}$ and $\mathbb{H}/K$. By the Weierstrass preparation theorem, we can write $q^*y = f(x)u(x)$ with f a monic polynomial of degree p^m congruent to x^{p^m} modulo $\mathfrak{m}_Y$, and u invertible. It follows that f is just the monic polynomial f_K classifying the divisor K, and thus that the coefficients of f (excluding the top one) generate the maximal ideal of E'. Over $Y(m,l)$ we have $q^*y = 0 \pmod{x^{p^m}}$ from which we see that $f(x) = x^{p^m}$. It follows that the maximal ideal of $E'(m,l)$ is zero, so that $e'(m,l) \leq 1$.

Next, I claim that $e'(k,l) \leq e'(k,l+1) + p^l e'(k+1,l)$ when $l < n$. To see this, we work temporarily over $E'(k,l)$. There are elements $u, v, a \in E'(k,l)$ with u invertible such that

$$p_{\mathbb{H}}^*x = ux^{p^n} + \cdots$$
$$p_{\mathbb{H}/K}^*y = vy^{p^l} + \cdots$$
$$q^*y = ax^{p^k} + \cdots$$

Note that $E'(k,l)/a = E'(k+1,l)$ and $E'(k,l)/v = E'(k,l+1)$. The relation $p_{\mathbb{H}/K} \circ q = q \circ p_{\mathbb{H}}$ gives

$$va^{p^l}x^{p^{k+l}} + \cdots = au^{p^k}x^{p^{k+n}} + \cdots.$$

Because we assume that $l < n$, we find that $va^{p^l} = 0$. The claim now follows from Lemma 48.

We next consider the analogous situation with $l = n$ and $k < m$, so that a lies in the maximal ideal of E'. By the same argument, we find that $va^{p^n} = au^{p^k}$, so that $a(1 - vu^{-p^k}a^{p^n-1}) = 0$. The term in parentheses is a unit, so $a = 0$. This shows that $E'(k,n) = E'(k+1,n)$. By induction, we see that $E'(k,n) = E'(m,n)$, so that $e'(k,n) = e'(m,n) \leq 1$.

From the above and Lemma 47 we see that $e'(k,l) \leq e(k,l)$. In particular, $\dim(E') = e'(0,1) \leq e(0,1) = d(m,n)$ as claimed. □

10.3. Rational theory

In this section, we shall assume that $\mathcal{O}_X$ is an integral domain in which $p \neq 0$, that K is a subgroup of $\mathbb{G}$ of degree p^m, and that we are given a level-m structure $\phi: \Lambda(m) \to \mathbb{G}$. For $a \in \Lambda(m)$ we write $x_a = x(\phi(a)) \in \mathcal{O}_X$.

For any subgroup A of order p^m of Λ (equivalently, of $\Lambda(m)$), we have a subgroup-scheme $[\phi A]$ of $\mathbb{G}$, with degree p^m. This corresponds to a section $\alpha_A : X \to \mathrm{Sub}_m(\mathbb{G})$. Putting these together, we get a map $\mathrm{Sub}_m(\Lambda) \times X \to \mathrm{Sub}_m(\mathbb{G})$, or equivalently $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})} \to F(\mathrm{Sub}_m(\Lambda), \mathcal{O}_X)$. (The target ring $F(\mathrm{Sub}_m(\Lambda), \mathcal{O}_X)$ is the ring of functions from the finite set $\mathrm{Sub}_m(\Lambda)$ to the ring $\mathcal{O}_X$, with pointwise operations.)

Proposition 50. *The resulting map*

$$\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})}[\tfrac{1}{p}] \to F(\mathrm{Sub}_m(\Lambda), \mathcal{O}_X[\tfrac{1}{p}])$$

is surjective with nilpotent kernel.

The proof will be given after some intermediate results. We write $a \sim b$ if and only if a is a unit multiple of b.

Firstly, recall from Theorem 24 that $[\phi\Lambda(m)] = \mathbb{G}(m)$, and hence that

$$(p^m_{\mathbb{G}})^* x \sim \prod_{a \in \Lambda(m)} (x - x_a).$$

On the other hand, for any formal group we have $(p^m_{\mathbb{G}})^* x = p^m x \pmod{x^2}$. It follows that $\prod_{a \neq 0} x_a \sim p^m$. Consider the discriminant

$$\Delta = \prod_{a \neq b} (x_a - x_b).$$

Write $N = |\Lambda(m)| = p^{mn}$. It follows easily from the above and Lemma 15 that

$$\Delta \sim \prod_{a \neq b} x_{a-b} \sim \left(\prod_{a \neq 0} x_a \right)^N \sim p^{mN}.$$

In particular, Δ becomes invertible when we invert p. Now write $E' = \mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})}$, and $\mathfrak{p}_A = \ker(\alpha_A) \lhd E'$. Note that $E'/\mathfrak{p}_A = \mathcal{O}_X$.

Lemma 51. *If $A \neq B$ then p is nilpotent mod $\mathfrak{p}_A + \mathfrak{p}_B$.*

Proof. We may suppose that there exists $a \in A \setminus B$. Modulo $\mathfrak{p}_B$ we have $f_K(x) = \prod_{b \in B}(x - x_b)$, and modulo $\mathfrak{p}_A$ we have $f_K(x_a) = 0$. Thus, using Lemma 15 we get

$$0 = f_K(x_a) = \prod_{b \in B} (x_a - x_b) \sim \prod_b x_{a-b} \pmod{\mathfrak{p}_A + \mathfrak{p}_B}.$$

Each term in the product $\prod_{b \in B}(x_a - x_b)$ divides Δ and thus divides a power of p. Thus p is nilpotent mod $\mathfrak{p}_A + \mathfrak{p}_B$ as claimed. □

Lemma 52. *If $\mathfrak{p}$ is a prime ideal in E' and $p \notin \mathfrak{p}$ then $\mathfrak{p} \geq \mathfrak{p}_A$ for some A.*

Proof. We know that $K \leq \mathbb{G}(m)$, so $f_K(x)$ divides $f_{\mathbb{G}(m)}(x) = \prod_{a \in \Lambda(m)}(x - x_a)$. Now work over the integral domain $E'/\mathfrak{p}$. We know that the discriminant of $f_{\mathbb{G}(m)}$ is nonzero, so the roots are distinct. We must therefore have $f_K(x) = \prod_{a \in A}(x - x_a)$ for some uniquely determined subset $A \subseteq \Lambda(m)$. As K is a subgroup scheme of $\mathbb{G}$, it must be invariant under translation by any of its points. From this, it follows easily that A is a subgroup of $\Lambda(m)$, and that $\mathfrak{p} \geq \mathfrak{p}_A$. □

Proof of Proposition 50. The last two lemmas show that $\mathfrak{p}_A[1/p]+\mathfrak{p}_B[1/p] = E'[1/p]$ and

$$\bigcap_A \mathfrak{p}_A[\tfrac{1}{p}] = \bigcap_{\mathfrak{p}\in\operatorname{spec} E'[\frac{1}{p}]} \mathfrak{p} = \sqrt{0}.$$

The proposition follows by the Chinese remainder theorem. □

Corollary 53. *The map* $\mathrm{Sub}_m(\mathbb{G}) \to X$ *is flat, with degree* $d(m,n)$.

Proof. Write $E = \mathcal{O}_X$ and $d = d(m,n)$. By Proposition 49 we know that there is an E-linear epimorphism $E^d \twoheadrightarrow E'$. It follows that the induced map

$$f' : E[\tfrac{1}{p}]^d \to E'[\tfrac{1}{p}] \to E'[\tfrac{1}{p}]/\sqrt{0}$$

is epi. By Proposition 50, this is an epimorphism between two free modules of the same rank, so it is iso. By assumption E is an integral domain in which $p \neq 0$, so $E^d \to E[\frac{1}{p}]^d$ is mono. By considering the following square, we see that f is mono and thus iso (and thus that $0 = \sqrt{0} \lhd E'$).

$$\begin{tikzcd}
E^d \arrow[r, two heads, "f"] \arrow[d] & E' \arrow[d] \\
E[\frac{1}{p}]^d \arrow[r, two heads, "f'"'] & E'[\frac{1}{p}]/\sqrt{0} \simeq E[\frac{1}{p}]^d
\end{tikzcd}$$

□

10.4. General theory

We can now prove Theorem 42, except for the Gorenstein property, which is treated in the next subsection. Let $\mathbb{G}$ be a formal group of height n over an arbitrary connected base X. Let $\mathbb{G}'/X'$ be the universal deformation of $\mathbb{G}_0/X_0$, and let $\mathbb{G}''$ be the pullback of $\mathbb{G}'$ to $\mathrm{Level}(m,\mathbb{G}')$. We can apply Corollary 53 to conclude that the projection $\mathrm{Sub}_m(\mathbb{G}'') = \mathrm{Level}(m,\mathbb{G}') \times_{X'} \mathrm{Sub}_m(\mathbb{G}') \to \mathrm{Level}(m,\mathbb{G}')$ is flat, with degree $d(m,n)$. As $\mathrm{Level}(m,\mathbb{G}') \to X'$ is faithfully flat, it is not hard to conclde that $\mathrm{Sub}_m(\mathbb{G}') \to X'$ is also flat, with degree $d(m,n)$. As $\mathrm{Sub}_m(\mathbb{G}) = X \times_{X'} \mathrm{Sub}_m(\mathbb{G}')$, we see that $\mathrm{Sub}_m(\mathbb{G}) \to X$ is again flat, with the required degree.

10.5. The Gorenstein property

We next show that the scheme $\mathrm{Sub}_m(\mathbb{G})$ is Gorenstein (I do not know whether it is a complete intersection). We first recall the definition and basic facts about Gorenstein rings.

Definition 54. A Noetherian local ring R is *Gorenstein* if the R-module R admits a finite resolution by injective R-modules.

Proposition 55. (a) *Let R be a Noetherian local ring, and $(x_1,\dots,x_m)$ a regular sequence in R generating an ideal $I \leq \mathfrak{m}$. Then R is Gorenstein if and only if R/I is Gorenstein.*

(b) *A regular Noetherian local ring is Gorenstein.*

(c) *An Artinian local ring R is Gorenstein if and only if the socle* $\operatorname{soc}(R) = \{a \in R \mid a\mathfrak{m} = 0\}$ *has dimension one over $\kappa = R/\mathfrak{m}$.*

Proof. Part (a) is [2, Proposition 3.1.19(b)]. As a field is visibly Gorenstein, part (b) follows. Part (c) is essentially [2, Theorem 3.2.10]. □

Recall the notation used in the proof of Proposition 49. We write Y for the scheme $\operatorname{Sub}_m(\mathbb{G}_0)$ and put $\mathbb{H} = \mathbb{G} \times_X Y$. We have a universal subgroup $K < \mathbb{H}$ of degree p^m and a quotient map $q\colon \mathbb{H} \to \mathbb{H}/K$. We choose coordinates x and y on $\mathbb{H}$ and $\mathbb{H}/K$. There is thus an element $a \in \mathcal{O}_Y$ such that $q^*y = ax \pmod{x^2}$. We can also consider the equation $f_K(x)$ of the divisor K, which is a unit multiple of q^*y in $\mathcal{O}_Y[\![x]\!]$. Thus $f_K(x) = a'x \pmod{x^2}$ for some element $a' \in \mathcal{O}_Y$, which is a unit multiple of a.

Proposition 56. *The ring $\mathcal{O}_{\operatorname{Sub}_m(\mathbb{G})}$ is Gorenstein. The socle of the quotient ring $\mathcal{O}_{\operatorname{Sub}_m(\mathbb{G}_0)}$ is generated by the element $a \uparrow (p + \cdots + p^{n-1})$ (where $a \uparrow N$ means a^N). It is also generated by $a' \uparrow (p + \cdots + p^{n-1})$.*

Proof. First, recall that $\mathcal{O}_{\operatorname{Sub}_m(\mathbb{G}_0)} = \kappa \otimes_X \mathcal{O}_{\operatorname{Sub}_m(\mathbb{G})}$, which is obtained from $\mathcal{O}_{\operatorname{Sub}_m(\mathbb{G})}$ by killing the sequence $(u_0,\dots,u_{n-1})$. This sequence is regular (because $\operatorname{Sub}_m(\mathbb{G}) \to X$ is flat). Thus, by part (a) of Proposition 55, it is enough to show that $\mathcal{O}_{\operatorname{Sub}_m(\mathbb{G}_0)}$ is Gorenstein. Moreover, by part (c) of Proposition 55, it is enough to show that the socle is generated by $a \uparrow (p + \cdots + p^{n-1})$.

To do this, we reuse the notation and ideas of the proof of Proposition 49. It was shown there that

$$e'(k,l) \leq e'(k,l+1) + p^l e'(k+1,l) \quad (l < n).$$

There is a similar relation for the numbers $e(k,l)$, with the inequality replaced by an equality. Moreover, we have

$$e'(k,n) \leq 1 = e(k,n) \quad (k \leq m),$$

$$e'(k,l) = 0 = e(k,l) \quad (k > m).$$

Finally, Theorem 42 implies that $e(0,1) = d(m,n) = e'(0,1)$. It follows easily that $e'(k,l) = e(k,l)$ when $k \leq m$ and $l \leq n$, and thus that $e'(k,l) = e'(k,l+1) + p^l e'(k+1,l)$ when $l < n$. In particular, we have $e'(0,l) = e'(0,l+1) + p^l e'(1,l)$. Recall that the corresponding inequality was derived from the relation $va^{p^l} = 0$, with $E'(0,l)/a = E'(1,l)$ and $E'(0,l)/v = E'(0,l+1)$. Because we are considering the case $k = 0$, the element a here is the same as that in the statement of the proposition. Using Lemma 57 below, we find that multiplication by a^{p^l} gives an isomorphism $\mathrm{soc}(E'(0,l+1)) \simeq \mathrm{soc}(E'(0,l))$. It follows that multiplication by $b = a \uparrow (p + \cdots + p^{n-1})$ gives an isomorphism $\mathrm{soc}(E'(0,n)) \simeq \mathrm{soc}(E'(0,1))$. As $e'(0,n) = e(0,n) = 1$, we see that $E'(0,n) = \kappa$ and thus that $\mathrm{soc}(E'(0,n)) = \kappa$. Moreover, $E'(0,1) = \mathcal{O}_{\mathrm{Sub}_m(\mathbb{G}_0)}$. It follows that $\mathrm{soc}(\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G}_0)})$ is generated by b, as claimed. The last statement of the proposition is trivial. □

We still owe the reader the following lemma.

Lemma 57. *Let R be a finite-dimensional local algebra over a field κ, with maximal ideal $\mathfrak{m}$. Suppose that $v, a \in \mathfrak{m}$ satisfy $va^k = 0$ (for some k) and $\dim(R) = \dim(R/v) + k\dim(R/a)$. Then multiplication by a^k is a monomorphism $R/v \rightarrow R$, whose image is the annihilator of v. Moreover, this map induces an isomorphism $\mathrm{soc}(R/v) \simeq \mathrm{soc}(R)$.*

Proof. As in the proof of Lemma 48, we filter R by the ideals Ra^i (where $0 \leq i \leq k$). The quotients are cyclic modules over R/a, and the last ideal Ra^k is a cyclic module over R/v, so that $\dim(Ra^i/Ra^{i+1}) \leq \dim(R/a)$ and $\dim(Ra^k) \leq \dim(R/v)$. On adding up these inequalities, we obtain the inequality $\dim(R) \leq \dim(R/v) + k\dim(R/a)$, which is by assumption an equality. It follows that all our inequalities are actually equalities, and thus that all our cyclic modules are actually free of rank one. This means that multiplication by a^k gives a monomorphism $R/v \rightarrow R$.

Let J be the annihilator of v, so that the image of the above map is clearly contained in J. On the other hand, we have short exact sequences

$$J \rightarrow R \xrightarrow{v} Rv, \quad Rv \rightarrow R \rightarrow R/v$$

which imply that $\dim(J) = \dim(R/v)$. It follows that our monomorphism $a^k : R/v \rightarrow J$ is actually an isomorphism.

It is immediate that $a^k\,\mathrm{soc}(R/v) \leq \mathrm{soc}(R)$. Conversely, suppose that $x \in \mathrm{soc}(R)$. As $v \in \mathfrak{m}$, we have $xv = 0$, so that $x \in J$. It follows that $x = a^k y$ for some $y \in R/v$. Suppose that $z \in \mathfrak{m}$. Then $a^k(yz) = xz = 0$ because $x \in \mathrm{soc}(R)$. As multiplication by a^k is a monomorphism, we see that $yz = 0$ in R/v. Thus $y \in \mathrm{soc}(R/v)$. This means that a^k gives an isomorphism $\mathrm{soc}(R/v) \simeq \mathrm{soc}(R)$, as claimed. □

11. Flags

Consider a sequence $\lambda = (\lambda_0 = 0 < \lambda_1 < \cdots < \lambda_m = n)$. A *flag of type λ* on $\mathbb{G}$ will mean a sequence of subgroup divisors $0 = K_0 < K_1 < \cdots < K_m = \mathbb{G}(1)$ such that K_k has degree p^{λ_k}. Using Proposition 16 and Theorem 42, we see that the functor from schemes over X to sets given by $Y \mapsto \{\text{flags of type } \lambda \text{ on } \mathbb{G} \times_X Y\}$ is represented by a scheme $\mathrm{Flag}(\lambda, \mathbb{G})$ over X. This is in fact a closed subscheme of $\prod_k \mathrm{Sub}_{\lambda_k}(\mathbb{G})$ and thus is finite over X.

Similarly, we let $\mathrm{Flag}(\lambda, A)$ be the set of sequences $0 = A_0 < A_1 < \cdots < A_m = A(1)$ such that $|A_k| = p^{\lambda_k}$. Let $a_0, \ldots, a_{n-1}$ be the standard basis of $A(1) = (\mathbb{Z}/p)^n$.

Write $A_k = \langle a_i \mid i < \lambda_k \rangle$, so that $\underline{A} = (A_0, \dots, A_m) \in \mathrm{Flag}(\lambda, A)$. Write $\Gamma = \mathrm{Aut}(A(1))$ and let $\Gamma(\lambda)$ be the subgroup which preserves $\underline{A}$. Clearly $\mathrm{Flag}(\lambda, A) \simeq \Gamma/\Gamma(\lambda)$.

If $\phi: A(1) \to \Gamma(X, \mathbb{G})$ is a level structure then by putting $K_k = [\phi A_k]$ we obtain a flag of type λ. This construction gives rise to a map $\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G})$.

Theorem 58. *The maps*

$$\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G}) \to X$$

are flat of degree $|\Gamma(\lambda)|$ *and* $|\mathrm{Flag}(\lambda, A)|$ *respectively. If* $\mathbb{G}$ *is the universal deformation of* $\mathbb{G}_0$ *then* $\mathrm{Flag}(\lambda, \mathbb{G})$ *is a smooth scheme and* $\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G})$ *is Galois.*

We will prove this theorem at the end of this section. First, observe that whenever we have a flag of type λ we have isogenies

$$\mathbb{G} = \mathbb{G}/K_0 \xrightarrow{q_1} \mathbb{G}/K_1 \xrightarrow{q_2} \cdots \xrightarrow{q_{m-1}} \mathbb{G}/K_{m-1} \xrightarrow{q_m} \mathbb{G}.$$

At the last stage, we have identified $\mathbb{G}/K_m = \mathbb{G}/\mathbb{G}(1)$ with $\mathbb{G}$ via the isomorphism $p_{\mathbb{G}}: \mathbb{G}/\mathbb{G}(1) \simeq \mathbb{G}$. With this convention, we have $q_m \circ q_{m-1} \circ \cdots \circ q_1 = p_{\mathbb{G}}: \mathbb{G} \to \mathbb{G}$. Moreover, q_k has height $\lambda_k - \lambda_{k-1}$.

11.1. Combinatorics

Consider a sequence $\mu = (0 = \mu_0 \le \mu_1 \le \cdots \le \mu_m \le n)$. Choose linearly independent subspaces $N_k \le A(1)$ of dimension $\mu_k - \mu_{k-1}$ and put $M_k = \bigoplus_{j=1}^k N_j$ and $M_k' = \bigoplus_{j=k+1}^m N_j$.

Definition 59. $d(\mu)$ is the number of flags of type λ such that $A_k \cap M_m = M_k$ for $0 \le k \le m$. This is clearly independent of the choices made. Note that $d(0, \dots, 0) = |\mathrm{Flag}(\lambda, A)|$, that $d(\mu) = 0$ unless $\mu_{k+1} - \mu_k \le \lambda_{k+1} - \lambda_k$ for $0 \le k < m$, and that $d(\mu) = 1$ if $\mu_k = \lambda_k$ for $0 \le k < m$.

Definition 60. If $\mu_m < n$ and $0 < k \le m$ write

$$\theta_k \mu = (\mu_0, \dots, \mu_{k-1}, \mu_k + 1, \dots, \mu_m + 1).$$

Lemma 61. *If* $\mu_m < n$ *then*

$$d(\mu) = \sum_{k=1}^m p^{\mu_m - \mu_k} d(\theta_k \mu).$$

Proof. Choose $L \le A(1)$ with $\dim_{\mathbb{F}_p} L = 1$ and $L \cap M_m = 0$. Let A be a flag of type λ such that $A_j \cap M_m = M_j$ for all j. There is an exact sequence

$$0 \to M_j \to A_j \cap (M_m \oplus L) \xrightarrow{\pi_j} L.$$

Note that π_m is epi. Let k be the least value of j for which π_j is epi (or equivalently, nonzero). For $j < k$ we have $A_j \cap (M_m \oplus L) = M_j$. For $j \ge k$, there is a unique map

$f_j : L \to M'_j$ such that $A_j \cap (M_m \oplus L) = A_j \cap (M_j \oplus M'_j \oplus L) = M_j \oplus \mathrm{graph}(f_j)$. Moreover, f_{j+1} is just the composite

$$L \xrightarrow{f_j} M'_j = N_{j+1} \oplus M'_{j+1} \to M'_{j+1}.$$

It follows that all the f_j are determined by $f_k \in \mathrm{Hom}(L, M'_k)$. Moreover, any homomorphism $L \to M'_k$ can arise in this way. It follows that the number of A's with a given value of k is $|\mathrm{Hom}(L, M'_k)| d(\theta_k \mu) = p^{\mu_m - \mu_k} d(\theta_k \mu)$. The claim follows. □

11.2. Infinitesimal theory

We next study the scheme $Y = X_0 \times_X \mathrm{Flag}(\lambda, \mathbb{G})$. Consider a sequence μ as above. Write $Y(\mu)$ for the closed subscheme of Y on which q_k has strict height at least $\mu_k - \mu_{k-1}$ for all k. Put $A(\mu) = \mathcal{O}_{Y(\mu)}$ and $e(\mu) = \dim_\kappa A(\mu)$. Note that $e(0, \dots, 0) = \dim_\kappa A$. Recall that we have isogenies

$$\mathbb{G} = \mathbb{G}/K_0 \xrightarrow{q_1} \mathbb{G}/K_1 \xrightarrow{q_2} \cdots \xrightarrow{q_{m-1}} \mathbb{G}/K_{m-1} \xrightarrow{q_m} \mathbb{G}$$

with

$$q_m \circ q_{m-1} \circ \cdots \circ q_1 = p_{\mathbb{G}} : \mathbb{G} \to \mathbb{G}.$$

Proposition 62. $\deg [\mathrm{Flag}(\lambda, \mathbb{G}) \to X] = \dim_\kappa A \leq |\mathrm{Flag}(\lambda, A)|$.

Proof. Note that $e(0, \dots, 0) = \dim_\kappa A = \deg [\mathrm{Flag}(\lambda, \mathbb{G}) \to X]$, and that $d(0, \dots, 0) = |\mathrm{Flag}(\lambda, A)|$, so it is enough to prove that $e(\mu) \leq d(\mu)$ for all μ. It is clear that $e(\mu) = 0$ unless $\mu_{k+1} - \mu_k \leq \lambda_{k+1} - \lambda_k$ for $0 \leq k < m$. Next, suppose that $\mu_k = \lambda_k$ for $0 \leq k < m$. It follows that over $Y(\mu)$ we have $K_k = p^{\lambda_k}[0]$ for $0 \leq k < m$. By construction, the ring A is generated over κ by the parameters of the divisors K_k, so this implies that $\kappa \to A(\mu)$ is epi and $e(\mu) \leq 1$. We now need only prove that when $\mu_m < n$ we have

$$e(\mu) \leq \sum_{k=1}^{m} p^{\mu_{k-1}} e(\theta_k \mu).$$

To see this, we work temporarily over $A(\mu)$. We shall write $a \uparrow n$ for a^n where typographically convenient. Choose coordinates x_k on the formal groups $\mathbb{G}/K_k$. There are elements $b_k \in A(\mu)$ such that $q_k^* x_k = b_k (x_{k-1} \uparrow (p^{\mu_k - \mu_{k-1}})) + \text{higher terms}$. Note that $A(\mu)/b_k = A(\theta_k \mu)$. We also have

$$q_1^* q_2^* \cdots q_m^* x_m = (x_0 \uparrow p^{\mu_m}) \prod_{k=1}^{m} (b_k \uparrow p^{\mu_m - \mu_k}) + \text{higher terms}.$$

On the other hand, $q_1^* \dots q_m^* x_m = p_{\mathbb{G}}^* x_0$, and this is divisible by $x_0^{p^n}$ (because Y lies over X_0). By assumption $\mu_m < n$, so we have

$$\prod_{k=1}^{m} (b_k \uparrow p^{\mu_m - \mu_k}) = 0.$$

It follows by Lemma 48 that

$$\dim_{\kappa} A(\mu) \leq \sum_k p^{\mu_m - \mu_k} \dim_{\kappa} A(\mu)/b_k = \sum_k p^{\mu_m - \mu_k} \dim_{\kappa} A(\theta_k \mu).$$

In other words, $e(\mu) \leq \sum_{k=1}^{m} p^{\mu_{k-1}} e(\theta_k \mu)$ as required. □

11.3. Galois theory

In this subsection we assume that $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$. As mentioned earlier, there is a map $\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G})$, classifying the flag $[\phi A_0] < \cdots < [\phi A_m]$; this clearly factors through $\mathrm{Level}(1, \mathbb{G})/\Gamma(\lambda)$.

Given a subset $S \subseteq A(1)$, we have a divisor $[\phi S] = \sum_{a \in S} [\phi(a)]$ on $\mathbb{G}$ over $\mathrm{Level}(1, \mathbb{G})$. Suppose we have maps $\mathrm{Level}(1, \mathbb{G}) \xrightarrow{f} Y \xrightarrow{g} X$ such that f is epi and gf is the usual map. We shall say that S is defined over Y (or over $\mathcal{O}_Y$) if and only if there is a (unique) divisor D on Y such that $[\phi S] = f^* D$, or equivalently if and only if the polynomial $\prod_{a \in S}(t - x_a)$ lies in the subring $\mathcal{O}_Y[t] \leq \mathcal{O}_{\mathrm{Level}(1,\mathbb{G})}[t]$.

For example, if S is invariant under the action of $\Gamma(\lambda)$ then S is defined over the quotient scheme $\mathrm{Level}(1, \mathbb{G})/\Gamma(\lambda)$. The following facts are evident:

(i) If D_0 and D_1 are defined over Y then so is $D_0 + D_1$.

(ii) If D_0 and $D_0 + D_1$ are defined over Y then so is D_1.

(iii) If the point a and the divisor D are defined over Y then so is the translate $T_a^* D$.

Lemma 63. *Suppose we have epimorphisms* $\mathrm{Level}(1, \mathbb{G}) \to Y \xrightarrow{g} Y' \to X$. *Suppose that $a \in S \subseteq A$, that S is defined over Y', and that $\mathcal{O}_Y$ is generated by x_a over $\mathcal{O}_{Y'}$. Then* $\deg(g) \leq |S|$.

Proof. Consider the polynomial $f(t) = \prod_{b \in S}(t - x_b) \in \mathcal{O}_{Y'}[t]$, which is monic and has degree $|S|$. Clearly $f(x_a) = 0$ so $\mathcal{O}_Y$ is a quotient of $\mathcal{O}_{Y'}[t]/f(t)$ and thus needs at most $|S|$ generators over $\mathcal{O}_{Y'}$. □

Remark 64. Geometrically, this means that Y embeds as a closed subscheme of the divisor $[\phi S]$ over Y'.

Proposition 65. $\deg[\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G})] \leq |\Gamma(\lambda)|$.

Proof. We again write $\{a_0, \ldots, a_{m-1}\}$ for the standard basis of $A(1)$, so that $A_k = \langle a_i \mid i < \lambda_k \rangle$. Put $\Gamma_k = \{\alpha \in \Gamma(\lambda) \mid \alpha(a_i) = a_i \text{ for } i < k\}$. Clearly

$$|\Gamma(\lambda)| = \prod_{k=0}^{n-1} |\Gamma_k / \Gamma_{k+1}| = \prod_{k=1}^{n} |\Gamma_k a_k|.$$

Suppose that $\lambda_j \leq k < \lambda_{j+1}$. A little linear algebra shows that $\Gamma_k a_k = A_{j+1} \backslash \langle a_i \,|\, i < k \rangle$. Write

$$Y_0 = \mathrm{spf}(C_0) = \mathrm{image}(\mathrm{Level}(1, \mathbb{G})/\Gamma(\lambda) \to \mathrm{Flag}(\lambda, \mathbb{G})),$$

$$x_k = x(\phi(a_k)) \in D_1 = \mathscr{O}_{\mathrm{Level}(1,\mathbb{G})},$$

$$C_k = C_0[x_j \,|\, j < k] \leq D_1,$$

$$Y_k = \mathrm{spf}(C_k).$$

We thus have maps $\mathrm{Level}(1, \mathbb{G}) = Y_n \to Y_{n-1} \to \cdots \to Y_0 \to \mathrm{Flag}(\lambda, \mathbb{G})$, the last of which is a closed embedding. The map $\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G})$ is defined so that the pullback of the divisor K_k is precisely $[\phi A_k]$. It follows that A_k is defined over Y_0 for all k.

The point a_k of $\mathbb{G}$ over Y_n is actually defined over Y_{k+1}. Using our description of $\Gamma_k a_k$ above, we see that $\Gamma_k a_k$ is defined over Y_k. Applying Lemma 63, we see that $\deg[Y_{k+1} \to Y_k] \leq |\Gamma_k/\Gamma_{k+1}|$. It follows that

$$\deg[\mathrm{Level}(1, \mathbb{G}) \to \mathrm{Flag}(\lambda, \mathbb{G})] \leq \prod_k |\Gamma_k/\Gamma_{k+1}| = |\Gamma(\lambda)|. \qquad \square$$

Proof of Theorem 58. We may assume that $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$. Write $a = |\Gamma(\lambda)|$ and $b = |\mathrm{Flag}(\lambda, A)|$, and note that $ab = |\Gamma|$. Consider the maps

$$\mathrm{Level}(1, \mathbb{G}) \xrightarrow{f} \mathrm{Level}(1, \mathbb{G})/\Gamma(\lambda) \xrightarrow{g} \mathrm{Flag}(\lambda, \mathbb{G}) \xrightarrow{h} X.$$

By Propositions 62 and 65 we know that $\deg(h) \leq b$ and $\deg(gf) \leq a$; by Theorem 23 we know that gfh is flat of degree ab; and it is clear that $\deg(gfh) \leq \deg(gf)\deg(h)$. It follows that $\deg(gf) = a$ and $\deg(h) = b$. Lemma 7 now tells us that $\mathrm{Flag}(\lambda, \mathbb{G})$ is smooth, f is Galois and g is iso. Finally, Lemmas 2 and 1 tell us that h is flat. □

12. Typed subgroups

Let A be a finite Abelian p-group of order p^m and rank at most n. We write

$$\begin{aligned} \mathrm{Type}(A, A) &= \{\text{subgroups of } A \text{ isomorphic to } A\} \\ &\simeq \mathrm{Mon}(A, A)/\mathrm{Aut}(A) \subseteq \mathrm{Sub}_m(A). \end{aligned}$$

In this section, we investigate what it would mean to replace A with $\mathbb{G}$. We shall define a scheme $\mathrm{Type}(A, \mathbb{G})$ of “finite subgroups of $\mathbb{G}$ of type A”.

Remark 66. This description is somewhat misleading, because it suggests that $\mathrm{Type}(A, \mathbb{G})$ should be a subscheme of $\mathrm{Sub}_m(\mathbb{G})$. There is a natural map

$$\mathrm{Type}(A, \mathbb{G}) \to \mathrm{Sub}_m(\mathbb{G}),$$

but it is not usually an embedding. The smallest case where it fails to be an embedding is $n = 3$, $A = \mathbb{Z}/4 \oplus \mathbb{Z}/2$ – I have proved this by elaborate calculation. See also Theorem 70 below, and the example at the end of Section 16. It would be interesting to have a compelling moduli interpretation of $\text{Type}(A, \mathbb{G})$, but I cannot at present offer one.

Definition 67. If $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$, then we take

$$\text{Type}(A, \mathbb{G}) = \text{Level}(A, \mathbb{G})/\text{Aut}(A).$$

In the general case, we let $\mathbb{H}/Y$ be the universal deformation of $\mathbb{G}_0/X_0$ and take

$$\text{Type}(A, \mathbb{G}) = \text{Type}(A, \mathbb{H}) \times_Y X.$$

Over the course of this section, we shall prove the following theorem.

Theorem 68. *The maps*

$$\text{Level}(A, \mathbb{G}) \to \text{Type}(A, \mathbb{G}) \to X$$

are flat, of degree $|\text{Aut}(A)|$ *and* $|\text{Type}(A, A)|$ *respectively. If* $\mathbb{G}$ *is the universal deformation of* $\mathbb{G}_0$ *then* $\text{Type}(A, \mathbb{G})$ *is smooth.*

We next consider the scheme $\coprod_{(A)} \text{Type}(A, \mathbb{G})$, where the coproduct runs over the isomorphism classes of Abelian groups A of order m and rank at most n.

Theorem 69. *Let f be the evident map*

$$f : \coprod_{(A)} \text{Type}(A, \mathbb{G}) \to \text{Sub}_m(\mathbb{G}).$$

Suppose that $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$. Then the induced map f^* of rings is injective, and becomes iso after inverting p.

Theorem 70. *Suppose that A has the form $\mathbb{Z}/p^{m+l} \oplus (\mathbb{Z}/p^l)^{n-1}$. Then* $\text{Type}(A, \mathbb{G}) \to \text{Sub}_{m+nl}(\mathbb{G})$ *is a closed embedding. In particular, when $n = 2$ (the case arising from a deformation of a supersingular elliptic curve), this holds for all A.*

We now start work on the proofs.

Let A be a finite Abelian p-group. Define

$$U_k(A) = \{a \in A(k) \mid p^{k-1}a \in p^k A\}, \quad T_k(A) = A(k)/U_k(A),$$
$$S_k(A) = A(k) \setminus U_k(A).$$

Note that U_k and T_k are additive functors, and that if $A \simeq \mathbb{Z}/p^l$ is a cyclic group then

$$T_k(A) = \begin{cases} A/p \simeq \mathbb{Z}/p & \text{if } k = l, \\ 0 & \text{otherwise.} \end{cases}$$

Now choose an isomorphism

$$A \simeq \bigoplus_{k\geq 0} (\mathbb{Z}/p^k)^{m_k}.$$

Write a_{kl} (with $0 \leq l < m_k$) for the generators of the cyclic summands. We shall order the pairs (k,l) as follows: $(i,j) < (k,l)$ iff $i > k$ or ($i = k$ and $j < l$). Note that the ordering on the first index is reversed, so that the generators a_{kl} of the largest cyclic summands come first in the ordering.

For $0 \leq l < m_k$ we define

$$V(k,l) = \langle a_{k,0}, \dots, a_{k,l-1}\rangle + U_k(A) \leq A(k),$$

$$\overline{V}(k,l) = V(k,l)/U_k(A) \leq T_k(A),$$

$$S(k,l) = A(k) \setminus V(k,l)$$

so

$$S(k,0) = S(k).$$

We also write

$$\Gamma = \mathrm{Aut}(A), \qquad \Gamma(k,l) = \{\alpha \in \Gamma \mid \alpha(a_{ij}) = a_{ij} \text{ if } (i,j) < (k,l)\}$$

so

$$\Gamma(k, m_k) = \Gamma(k-1, 0) \quad \text{and} \quad \Gamma(k,l)/\Gamma(k,l+1) \simeq \Gamma(k,l)a_{kl}.$$

Lemma 71. *$\Gamma(k,l)a_{kl} = S(k,l)$ and $|\Gamma| = \prod_{k,l} |S(k,l)|$.*

Proof. As $\Gamma(k,l)/\Gamma(k,l+1) \simeq \Gamma(k,l)a_{kl}$, the second statement will follow easily from the first.

Any $\alpha \in \Gamma$ preserves $S(k)$ and induces an automorphism of $T_k(A)$. If $\alpha \in \Gamma(k,l)$ then it is easy to see that $\alpha(a_{kl}) \in S(k,l)$, lest the induced endomorphism of $T_k(A)$ fail to be iso. Conversely, suppose $b \in S(k,l)$. Write

$$A' = (\mathbb{Z}/p^k)^{m_k}, \qquad A'' = \bigoplus_{l \neq k} (\mathbb{Z}/p^l)^{m_l}.$$

Let b' and b'' be the components of b in A' and A''. By linear algebra over $\mathbb{F}_p$ we can find an automorphism α_0 of $T_k(A) = A'/p$ with $\alpha_0(a_{kj}) = a_{kj}$ for $j < l$ and $\alpha_0(a_{kl}) = b' \pmod p$. We can then lift this to get an automorphism α_1 of A' with $\alpha_1(a_{kj}) = a_{kj}$ for $j < l$ and $\alpha_1(a_{kl}) = b'$. Finally, we define an endomorphism α of $A = A' \oplus A''$, with components as follows:

$A' \to A'$	α_1
$A' \to A''$	$a_{kl} \mapsto b''$ other generators $\mapsto 0$
$A'' \to A'$	0
$A'' \to A''$	identity.

It is easy to check that this is iso, and $\alpha(a_{kl}) = b$. Thus $\Gamma(k,l)a_{kl} = S(k,l)$. □

Remark 72. It is neither hard nor apparently helpful to write explicit formulae for $|S(k,l)|$ and $|\Gamma|$.

We assume until further notice that $\mathbb{G}$ is the universal deformation of $\mathbb{G}_0$. As in Section 11.3, we shall say that a subset $S \subseteq A$ is defined over a quotient scheme Y of $\text{Level}(A,\mathbb{G})$ if there is a divisor D on $\mathbb{G}$ over Y whose pullback is $[\phi S]$.

Proof of Theorem 68. We now write $D_A = \mathcal{O}_{\text{Level}(A,\mathbb{G})}$ and $C = D_A^\Gamma = \mathcal{O}_{\text{Type}(A,\mathbb{G})}$. Define

$$x_{ij} = x(\phi(a_{ij})), \qquad C(k,l) = C[x_{ij} \mid (i,j) < (k,l)] \le D_A$$

$$Y(k,l) = \text{spf}(C(k,l)).$$

Note that $Y(k,m_k) = Y(k-1,0)$ and that we have maps $\text{Level}(A,\mathbb{G}) \to Y(k,l+1) \to Y(k,l) \to \text{Type}(A,\mathbb{G})$. Because $U_k(A)$ and $a_{k,0},\dots,a_{k,l-1}$ are defined over $Y(k,l)$, we see that $S(k,l)$ is defined over $Y(k,l)$. Moreover, $a_{kl} \in S(k,l)$ and $C(k,l+1)$ is generated over $C(k,l)$ by x_{kl}. It follows by Lemma 63 that $\deg[Y(k,l+1) \to Y(k,l)] \le |S(k,l)|$. Combining this with Lemma 71, we see that $\deg[\text{Level}(A,\mathbb{G}) \to \text{Type}(A,\mathbb{G})] \le |\Gamma|$. It follows from Lemma 7 that $\text{Level}(A,\mathbb{G}) \to \text{Type}(A,\mathbb{G})$ is Galois and that $\text{Type}(A,\mathbb{G})$ is smooth. Lemmas 2 and 1 now tell us that $\text{Type}(A,\mathbb{G}) \to X$ is flat. As $\deg[\text{Level}(A,\mathbb{G}) \to X] = |\text{Mon}(A,\Lambda)|$, we see that $\deg[\text{Type}(A,\mathbb{G}) \to X] = |\text{Mon}(A,\Lambda)|/|\Gamma| = |\text{Type}(A,\Lambda)|$. □

Proof of Theorem 69. Write $E' = \mathcal{O}_{\text{Sub}_m(\mathbb{G})}$. In Section 10.3, we constructed a map $g: D_m \otimes_E E' \to F(\text{Sub}_m(\Lambda), D_m)$. We proved there that after inverting p, g becomes epi with nilpotent kernel. In the light of Theorem 42, we conclude that g is mono, and becomes iso after inverting p. We now put $\Gamma = \text{Aut}(\Lambda(m))$, and note that g is equivariant for the evident actions of Γ. Passing to fixed points, we obtain a map $g^\Gamma: (D_m \otimes_E E')^\Gamma \to F(\text{Sub}_m(\Lambda), D_m)^\Gamma$ which is again mono, and becomes iso after inverting p.

By Theorem 34, we know that $D_m^\Gamma = E$. Because E' is free over E, we conclude that $(D_m \otimes_E E')^\Gamma = E'$. Next, for each isomorphism class of Abelian p-groups of order m and rank at most n, choose a representative subgroup $A \le \Lambda(m)$. Write S for the set f chosen representatives. For $A \in S$ write $\Gamma_A = \{\alpha \in \Gamma \mid \alpha(A) = A\}$. We have an isomorphism of Γ-sets

$$\text{Sub}_m(\Lambda) \simeq \coprod_{A \in S} \Gamma/\Gamma_A.$$

It is not hard to conclude that

$$F(\text{Sub}_m(\Lambda), D_m)^\Gamma = \prod_{A \in S} D_m^{\Gamma_A}.$$

Lemma 36 implies that $\Gamma_A \to \text{Aut}(A)$ is epi; write Γ'_A for the kernel. Using Theorem 34 we find that

$$D_m^{\Gamma_A} = (D_m^{\Gamma'_A})^{\text{Aut}(A)} = D_A^{\text{Aut}(A)} = C_A.$$

Thus, g^Γ is a map $E' \to \prod_{A\in S} C_A$. One can check that this is the same map as that described in the statement of the theorem. □

Definition 73. Let K be the universal subgroup over $\mathrm{Sub}_m(\mathbb{G})$. We write $p^{-r}K$ for the kernel of the composite

$$\mathbb{G} \xrightarrow{p^r_{\mathbb{G}}} \mathbb{G} \xrightarrow{q} \mathbb{G}/K.$$

Thus $p^{-r}K$ is a subgroup divisor of degree p^{m+nr} defined over $\mathrm{Sub}_m(\mathbb{G})$, and its equation $f_{p^{-r}K}(x)$ is a unit multiple of $f_K((p^r_{\mathbb{G}})^*x)$. The subgroup $p^{-r}K$ is classified by a map

$$p^{-r}\colon \mathrm{Sub}_m(\mathbb{G}) \to \mathrm{Sub}_{m+nr}(\mathbb{G}).$$

Lemma 74. *The map $p^{-r}\colon \mathrm{Sub}_m(\mathbb{G}) \to \mathrm{Sub}_{m+nr}(\mathbb{G})$ is a closed embedding, and identifies $\mathrm{Sub}_m(\mathbb{G})$ with the scheme of subgroups of degree $m+nr$ which contain $\mathbb{G}(r)$.*

Proof. Over $\mathrm{Sub}_{m+nr}(\mathbb{G})$, we have an exact sequence of formal groups

$$\mathbb{G}(r) \to \mathbb{G} \xrightarrow{p^r_{\mathbb{G}}} \mathbb{G}.$$

We know by Proposition 16 that there is a closed subscheme $Z \leq \mathrm{Sub}_{m+nr}(\mathbb{G})$ which is universal for subgroups containing $\mathbb{G}(r)$. Let K' be the universal subgroup over Z and $q'\colon \mathbb{G} \to \mathbb{G}/K'$ the projection. Then the composite $\mathbb{G}(r) \to \mathbb{G} \to \mathbb{G}/K'$ is zero so there is a map (of formal groups over Z) $q\colon \mathbb{G} \to \mathbb{G}/K'$ with $q \circ p^r_{\mathbb{G}} = q'$. The kernel K of q therefore has degree p^m, and is classified by a map $f\colon Z \to \mathrm{Sub}_m(\mathbb{G})$. Clearly $p^{-r}\colon \mathrm{Sub}_m(\mathbb{G}) \to \mathrm{Sub}_{m+nr}(\mathbb{G})$ factors through Z, and the maps $Z \xrightarrow{f} \mathrm{Sub}_m(\mathbb{G}) \xrightarrow{p^{-r}} Z$ are mutually inverse. □

Proposition 75. *Suppose that A is such that $A(r) \simeq \Lambda(r)$ (so that A has rank n and every cyclic factor has length at least r). Write $A' = A/A(r)$ and $|A'| = p^m$. Then there is a canonical isomorphism $\mathrm{Type}(A,\mathbb{G}) \simeq \mathrm{Type}(A',\mathbb{G})$, and the following diagram commutes:*

$$\begin{tikzcd}
\mathrm{Type}(A,\mathbb{G}) \arrow[r] \arrow[d, "\simeq"'] & \mathrm{Sub}_{m+nr}(\mathbb{G}) \\
\mathrm{Type}(A',\mathbb{G}) \arrow[r] & \mathrm{Sub}_m(\mathbb{G}) \arrow[u, "p^{-r}"']
\end{tikzcd}.$$

Proof. It is easy to see that multiplication by p^r induces a bijection between $\mathrm{Type}(A,\Lambda)$ and $\mathrm{Type}(A',\Lambda)$. Thus

$$\frac{|\mathrm{Epi}(\Lambda^*,A)|}{|\mathrm{Aut}(A)|} = |\mathrm{Type}(A,\Lambda)| = |\mathrm{Type}(A',\Lambda)| = \frac{|\mathrm{Epi}(\Lambda^*,A')|}{|\mathrm{Aut}(A')|}.$$

Let $u : A \to A'$ be the projection. Any automorphism α of A induces an automorphism α' of A', with $\alpha' u = u\alpha$. It follows easily that there is a map $u'_!$ making the following diagram commute:

$$\begin{tikzcd}
\mathrm{Level}(A,\mathbb{G}) \arrow[r, "f"] \arrow[d, "u_!"'] & \mathrm{Type}(A,\mathbb{G}) \\
\mathrm{Level}(A',\mathbb{G}) \arrow[r, "f'"'] & \mathrm{Type}(A',\mathbb{G}) \arrow[u, "u'_!"']
\end{tikzcd} .$$

By Theorem 41, we know that $u_!$ is a finite flat map of degree $|\mathrm{Epi}(A^*,A)|/|\mathrm{Epi}(A^*, A')|$. On the other hand, f and f' are finite flat maps of degree $|\mathrm{Aut}(A)|$ and $|\mathrm{Aut}(A')|$ respectively. It follows (using Lemmas 2 and 1) that $u'_!$ is a finite flat map of degree

$$\frac{|\mathrm{Epi}(A^*,A)|}{|\mathrm{Epi}(A^*,A')|}\,\frac{|\mathrm{Aut}(A')|}{|\mathrm{Aut}(A)|} = 1.$$

In other words, $u'_!$ is iso as claimed. It is not hard to see that the diagram commutes. □

Proof of Theorem 70. We may as usual assume that $\mathbb{G}$ is the universal deformation. First, suppose that A is cyclic, say $A \simeq \mathbb{Z}/p^m$ generated by a. We need to prove that C_A is generated by the parameters of the divisor $[\phi A]$. As discussed at the end of Section 8, we can write $(p^m_{\mathbb{G}})^* x = g(x)(p^{m-1}_{\mathbb{G}})^* x$ for a series $g(x) \in E[\![x]\!]$ of Weierstrass degree $s = p^{nm} - p^{n(m-1)}$. Thus, $g(x)$ is a unit multiple of a monic polynomial $h(x)$ of degree s with $h(x) = x^s \pmod{\mathfrak{m}_E}$. Moreover, $D_A = E[x_a]/h(x_a)$, where $x_a = x(\phi(a))$. Write $D'_A = D_A/\mathfrak{m}_E$ and $C'_A = C_A/\mathfrak{m}_E$, so that D'_A is just $\kappa[x_a]/x_a^s$. We shall say that an element of D'_A has valuation t if it is divisible by x_a^t but not by x_a^{t+1}. For $j \in \mathbb{Z}$ we have $x_{ja} = x(\phi(ja)) = jx_a \pmod{x_a^2}$, so this has valuation 1 if $j \neq 0 \pmod{p}$ and valuation greater than 1 otherwise. Now write $r = p^m - p^{m-1}$ (which divides s) and let $u \in C_A$ be the rth symmetric polynomial in $\{x_{ja} \mid 0 \leq j < p^m\}$. This is the rth parameter of the divisor $[\phi A]$, so it lies in the image of $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})} \to C_A$. Let u' be the image of u in D'_A. If we write u' in the usual way as a sum of r-fold products, then there is one term $\prod\{x_{ja} \mid j \neq 0 \pmod{p}\}$ of valuation r, and the other terms have higher valuation. Thus u' itself has valuation r, and the subring of D'_A generated by u' has dimension s/r as a vector space over κ. On the other hand, one can see that $s/r = |\mathrm{Type}(A,A)| = |C_A : E|$. Consider the maps

$$E^{s/r} = E\{1, u, \ldots, u^{s/r-1}\} \xrightarrow{i} C_A \xrightarrow{j} D_A$$

and the resulting maps

$$\kappa^{s/r} = \kappa\{1, u', \ldots, (u')^{s/r-1}\} \xrightarrow{i'} C'_A \xrightarrow{j'} D'_A.$$

We have just seen that $j'i'$ is mono, so i' is mono. By dimension count, i' is iso. It follows that i is epi, and thus that $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})} \to C_A$ is epi as claimed. □

Now suppose that $A \simeq \mathbb{Z}/p^{r+m} \oplus (\mathbb{Z}/p^r)^{n-1}$. Then $A' = A/A(r)$ is cyclic. Proposition 75 gives a commutative diagram as follows:

$$\begin{tikzcd}
\mathrm{Type}(A, \mathbb{G}) \arrow[r] & \mathrm{Sub}_{m+nr}(\mathbb{G}) \arrow[d, "p^{-r}"] \\
\mathrm{Type}(A', \mathbb{G}) \arrow[u, "\simeq"] \arrow[r] & \mathrm{Sub}_m(\mathbb{G})
\end{tikzcd}$$

We have just shown that the bottom map is a closed embedding. The map p^{-r} is a closed embedding by Lemma 74. It follows that the top map is also a closed embedding, as claimed. □

13. Deformation of isogenies

Consider two schemes X_0 and X_0', each of which is spec of a field of characteristic p. Suppose we have a morphism of formal groups as follows:

$$\begin{tikzcd}
\mathbb{G}_0 \arrow[r, "q_0"] \arrow[d] & \mathbb{G}_0' \arrow[d] \\
X_0 \arrow[r, "f_0"'] & X_0'
\end{tikzcd}.$$

We shall suppose that the induced map $\mathbb{G}_0 \to f_0^* \mathbb{G}_0'$ is an isogeny of degree p^m. We would lose little generality by requiring f_0 to be the identity, but in algebraic topology we naturally encounter the case in which f_0 is a power of Frobenius. By a *deformation* of q_0 we shall mean a morphism $q \colon \mathbb{H} \to \mathbb{H}'$ of formal groups over a scheme Y, where $\mathbb{H}$ and $\mathbb{H}'$ are deformations of $\mathbb{G}_0$ and $\mathbb{G}_0'$ respectively, and the restriction of q over Y_0 is compatible with q_0. In more detail, we define $\mathbb{H}_0$ and $\mathbb{H}_0'$ to be the restrictions of $\mathbb{H}$ and $\mathbb{H}'$ to Y_0, and we require a commutative diagram as follows:

$$\begin{tikzcd}
\mathbb{H} \arrow[dr, "q"] \arrow[dd] & & \mathbb{H}_0 \arrow[ll, hook'] \arrow[rr] \arrow[dr] \arrow[dd] & & \mathbb{G}_0 \arrow[dr, "q_0"] \arrow[dd] & \\
& \mathbb{H}' \arrow[dd] & & \mathbb{H}_0' \arrow[ll, hook'] \arrow[rr] \arrow[dd] & & \mathbb{G}_0' \arrow[dd] \\
Y \arrow[dr, "1"'] & & Y_0 \arrow[ll, hook'] \arrow[rr] \arrow[dr, "1"] & & X_0 \arrow[dr, "f_0"'] & \\
& Y & & Y_0 \arrow[ll, hook'] \arrow[rr] & & X_0'
\end{tikzcd}$$

The diagram contains three parallel vertical squares. The middle one is by definition the restriction of the left-hand one over the special fibre $Y_0 \subset Y$. The back face of the right-hand cube is required to be a pullback square, making $\mathbb{H}$ into a deformation of $\mathbb{G}_0$. Similarly for the front face of the right-hand cube. This forces q to be an isogeny of degree p^m.

Our next task is to classify such deformations. First, let $\mathbb{G}/X$ be the universal deformation of $\mathbb{G}_0$. Let $a\colon \mathrm{Sub}_m(\mathbb{G}) \to X$ be the usual projection, and let $K < a^*\mathbb{G}$ be the universal example of a subgroup of degree p^m. As $\mathrm{Sub}_m(\mathbb{G})$ is a closed subscheme of $\mathrm{Div}_{p^m}(\mathbb{G})$ and $\mathrm{Div}_{p^m}(\mathbb{G})_0 = X_0$, we see that $\mathrm{Sub}_m(\mathbb{G})_0 = X_0$. There is a unique subgroup of order p^m of $\mathbb{G}_0$ defined over X_0, viz. the divisor $p^m[0] = \mathrm{spf}(\mathcal{O}_{\mathbb{G}_0}/x^{p^m})$. In particular, $K_0 = p^m[0] = \ker(q_0)$. It follows that there is a pullback diagram as shown below.

$$\begin{tikzcd}
(a^*\mathbb{G}/K)_0 \arrow[r, "\sim"'] \arrow[d] & \mathbb{G}_0/p^m[0] \arrow[r, "\bar{q}_0", "\sim"'] \arrow[d] & \mathbb{G}'_0 \arrow[d] \\
\mathrm{Sub}_m(\mathbb{G})_0 \arrow[r, "\sim", "a_0"'] & X_0 \arrow[r, "\sim", "f_0"'] & X'_0
\end{tikzcd}.$$

Using this, we can consider the projection $a^*\mathbb{G} \to a^*\mathbb{G}/K$ as a deformation of q_0. It is not hard to check that it is the terminal object in the category of deformations.

Now let $\mathbb{G}'/X'$ be the universal deformation of $\mathbb{G}'_0/X'_0$. The above construction also exhibits $a^*\mathbb{G}/K$ as a deformation of $\mathbb{G}'_0$. It is therefore classified by a map $b\colon \mathrm{Sub}_m(\mathbb{G}) \to X'$ extending the map $b_0 = f_0 \circ a_0\colon \mathrm{Sub}_m(\mathbb{G})_0 \to X'_0$.

Proposition 76. *b is a finite flat map, of degree $|\mathrm{Sub}_m(\Lambda)|$.*

Proof. Recall from Theorem 69 that we have a dominant map

$$f\colon \coprod_{(A)} \mathrm{Type}(A,\mathbb{G}) \to \mathrm{Sub}_m(\mathbb{G})$$

(where A runs over isomorphism types of finite Abelian p-groups of order p^m and rank at most n). Moreover, f becomes iso when we invert p. It is easy to see that the composite $\mathrm{Level}(A,\mathbb{G}) \to \mathrm{Type}(A,\mathbb{G}) \to \mathrm{Sub}_m(\mathbb{G}) \xrightarrow{b} X'$ can be identified with the map $0_!$ of Section 9. By part (7) of Theorem 41, this map is flat and has degree $|\mathrm{Mon}(A,\Lambda)|$. Moreover, $\mathrm{Level}(A,\mathbb{G}) \to \mathrm{Type}(A,\mathbb{G})$ is a Galois covering with Galois group $\mathrm{Aut}(A)$. Using Lemmas 2 and 1, we see that $\mathrm{Type}(A,\mathbb{G}) \to X'$ is flat. The degree is clearly $|\mathrm{Mon}(A,\Lambda)|/|\mathrm{Aut}(A)| = |\mathrm{Type}(A,\Lambda)|$. It follows that $b \circ f$ is a flat map of degree $\sum_A |\mathrm{Type}(A,\Lambda)| = |\mathrm{Sub}_m(\Lambda)|$, and thus that $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G})}[1/p]$ is free of this rank over $\mathcal{O}_{X'}[1/p]$.

We next let $Y < \mathrm{Sub}_m(\mathbb{G})$ be the preimage of X'_0 under b, and write $\kappa' = \mathcal{O}_{X'_0}$ and $E' = \mathcal{O}_Y$. I claim that $\dim_{\kappa'} E' = |\mathrm{Sub}_m(\Lambda)|$. The proof is similar to that in Section 10.2. To recall some notation from there: Given a sequence $(\alpha_k, \alpha_{k+1}, \dots, \alpha_{n-1})$

we write $|\alpha| = \sum_j \alpha_j$, $\|\alpha\| = \sum_j j\alpha_j$. If α runs over sequences $(\alpha_1, \dots, \alpha_{n-1})$ with $|\alpha| \leq m$ then $d(m,n) = \sum_\alpha p^{\|\alpha\|}$. Note, however, that E' and Y have different meanings here from those used in Section 10.2. We write $\mathbb{H}$ for the restriction of $a^*\mathbb{G}$ to Y, and K for the evident subgroup of $\mathbb{H}$, so that $\mathbb{H}/K$ is a pullback of $\mathbb{G}'_0$ and thus has strict height n. Let q be the projection $\mathbb{H} \to \mathbb{H}/K$. Choose coordinates x and y on $\mathbb{H}$ and $\mathbb{H}/K$. Let $Y(k,l)$ be the largest closed subscheme of Y over which $\mathbb{H}$ has strict height at least k and q has strict height at least l, and write $E'(k,l) = \mathcal{O}_{Y(k,l)}$ and $f'(k,l) = \dim_{\kappa'} E'(k,l)$. Working over $E'(k,l)$ we see that there are elements u, v, a (with v invertible) such that

$$p_{\mathbb{H}}^* x = u x^{p^k} + \cdots$$

$$p_{\mathbb{H}/K}^* y = v y^{p^n} + \cdots$$

$$q^* y = a x^{p^l} + \cdots$$

Thus $E'(k+1, l) = E'(k,l)/u$ and $E'(k, l+1) = E'(k,l)/a$. Reading the relation $p_{\mathbb{H}/K} \circ q = q \circ p_{\mathbb{H}}$ to lowest order, we find that

$$v a^{p^n} x^{p^{l+n}} + \cdots = a u^{p^l} x^{p^{k+l}} + \cdots.$$

If $k < n$ then we conclude that $a u^{p^l} = 0$, and then Lemma 48 tells us that $f'(k,l) \leq f'(k,l+1) + p^l f'(k+1,l)$. If $k = n$ then u is invertible and we have $a(u^{p^l} - v a^{p^n - 1}) = 0$. If also $l < n$ then a is topologically nilpotent so $u^{p^l} - v a^{p^n-1}$ is invertible so $a = 0$, which shows that $E'(n,l) = E'(n,l+1) = E'(n,m)$. From the construction of $\mathrm{Sub}_m(\mathbb{G})$ one can see that $\kappa' \to E'(n,m)$ is epi, and that $E'(k,l) = 0$ if $k > n$ or $l > m$. To summarise, we have

$$\begin{aligned} &f'(k,l) \leq f'(k,l+1) + p^l f'(k+1,l) \quad \text{if } (k < n), \\ &f'(n,l) \leq 1, \\ &f'(k,l) = 0 \quad \text{if } (l > m). \end{aligned}$$

We next define a function $f(k,l)$ for $0 \leq k \leq n$ and $0 \leq l$ by $f(k,l) = \sum \{ p^{\|\alpha\|} \mid \alpha = (\alpha_1, \dots, \alpha_{n-k}), |\alpha| \leq m\ ,\ \alpha_{n-k} \geq l \}$. We make the usual convention that $f(n,l) = 1$ for $l \leq m$ and $f(k,l) = 0$ for $l > m$. I claim that $f(k,l) \leq f(k,l+1) + p^l f(k+1,l)$ when $k < n$. To see this, consider the sum which defines $f(k,l)$. The sum of the terms with $\alpha_{n-k} > l$ is $f(k,l+1)$. If $\alpha_{n-k} = l$, we define $\beta = (\alpha_1, \dots, \alpha_{n-k-2}, \alpha_{n-k-1} + l)$. Note that $|\beta| = |\alpha|$, that $\beta_{n-(k+1)} \geq l$, and that $\|\alpha\| = \|\beta\| + l$. Using this construction, we see that the sum of $p^{\|\alpha\|}$ for these α's is $p^l f(k+1,l)$, as required. It follows that $f'(k,l) \leq f(k,l)$, and in particular that $\dim_{\kappa'}(E') = f'(1,0) \leq f(1,0) = d(m,n) = |\mathrm{Sub}_m(\Lambda)|$. By an argument very similar to that of Section 10.4, we conclude that the map $b : \mathrm{Sub}_m(\mathbb{G}) \to X'$ is flat and has degree $d(m,n)$. □

14. The connection with algebraic topology

In this section, we make a few brief remarks about how formal groups and moduli problems arise in algebraic topology. Good general references are [1, 14]. However, they are not written from an algebro-geometric point of view, which was first introduced by Morava [12, 13]. This philosophy is developed in [15]. In the discussion below, we shall take a few liberties with technical details.

Let Z be a topological space. A *geometric chain* in Z is a smooth manifold (possibly with boundary) M equipped with a map $M \rightarrow Z$. Geometric chains form a graded Abelian monoid GC_*Z under disjoint union. Restriction to the boundary gives a differential $\partial : \mathrm{GC}_*Z \rightarrow \mathrm{GC}_{*-1}Z$. The homology of this complex is a graded Abelian group MO_*Z. If we require that all manifolds have a given complex structure on the stable normal bundle, we obtain a different group MU_*Z, the *complex bordism group* of Z. We write MU_* for $MU_*(\text{point})$, which is a ring under cartesian product. By a related geometric procedure, we can define a group MU^*Z (which is often but not always the MU_*-dual of MU_*Z). In fact MU^*Z has a natural ring structure. It can be thought of as an analogue of the Chow ring, which some readers may find more familiar. The functor $Z \mapsto MU^*Z$ has a number of formal properties (Mayer-Vietoris sequences, etc.), which can be summarised by saying that it is a multiplicative generalised cohomology theory. It is the most powerful such theory which one has any reasonable chance of computing for popular spaces Z. See [4] for some justification of this claim.

Let $\mathbb{C}P^\infty$ denote the colimit of the finite-dimensional complex projective spaces $\mathbb{C}P^k$, or equivalently the classifying space of the circle group. This is itself (homotopy equivalent to) a topological Abelian group. Moreover, $MU^*\mathbb{C}P^\infty$ is isomorphic to $MU^*[\![x]\!]$. The group structure on $\mathbb{C}P^\infty$ gives rise to a coproduct on $MU^*\mathbb{C}P^\infty$ and hence a formal group law over MU_*. Lazard showed that there is a universal example of a ring L equipped with a formal group law F, and that L is a polynomial algebra over $\mathbb{Z}$ on countably many generators. Quillen proved the fundamental theorem that the classifying map $L \rightarrow MU_*$ is an isomorphism. This is the source of all connections between algebraic topology and formal group theory. If we consider instead manifolds with a splitting of the stable normal bundle as a sum of two complex bundles, we obtain a ring $(MU \wedge MU)^*Z$. If we take Z to be a point, this is the universal example of a ring with two formal group laws and an isomorphism between them. Using these ideas, we can construct descent data making MU^*Z into a sheaf over the stack of formal groups. The cohomology of the dual sheaf MU_*Z is the E_2 term of the Adams–Novikov spectral sequence, which converges to the stable homotopy groups of Z.

A formal group $\mathbb{G}$ over a scheme $X = \mathrm{spf}(E)$ gives rise to a map from X to this stack. By pulling back MU^*Z, we obtain an algebra E^*Z over E, and thus a scheme $Z_E = \mathrm{spf}(E^*Z)$ over X. If the map from X to the stack of formal groups is flat, then the functor $Z \mapsto E^*Z$ defines a generalised cohomology theory. This flatness condition is called Landweber exactness in the topological literature. It holds in particular if $\mathbb{G}/X$ is the universal deformation of a formal group of finite height over a field. If A is a finite Abelian group and BA^* is the classifying space of its dual then $(BA^*)_E = \mathrm{Hom}(A, \mathbb{G})$. For finite non-Abelian groups K, the generalised character theory of [8] establishes a connection between BK_E and schemes of the form $\mathrm{Level}(B, \mathbb{G})$. There is also a map from a certain closed subscheme $\mathrm{spf}(R)$ of $(B\Sigma_{p^m})_E$ to $\mathrm{Sub}_m(\mathbb{G})$, which turns out to be an isomorphism. Theorem 42 is half of the proof of this fact, the other half is topology. A topological calculation shows that the socle element is not in the kernel of the map $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G}_0)} \to R/\mathfrak{m}_E R$; as the source is a Gorenstein ring of dimension zero, we conclude that the map is injective. Another elaborate topological argument computes the dimension of $R/\mathfrak{m}_E R$, showing that it coincides with the dimension of $\mathcal{O}_{\mathrm{Sub}_m(\mathbb{G}_0)}$ given by Theorem 42.

Using this fact, we obtain extra structure on Z_E. Suppose that a, b are two points of X, that $\mathbb{G}_a$ and $\mathbb{G}_b$ are the fibres of $\mathbb{G}$ over a and b, and that $q\colon \mathbb{G}_a \to \mathbb{G}_b$ is an isogeny. A certain topological construction then gives rise to a map $(Z_E)_a \to (Z_E)_b$, which is functorial in q and natural in Z. This gives powerful information about the schemes Z_E. It can be reformulated as saying that a certain kind of generalised Hecke algebra acts on E^*Z, and on certain other topologically defined rings. Certain *Ext* groups over this algebra form the input to spectral sequences that compute homotopy groups of spaces of maps of strictly commutative ring spectra, for example. A conjecture of Mike Hopkins (inspired but not implied by the theory of the Bruhat-Tits building) would mean that this Hecke algebra has finite global dimension; this would be very helpful for the applications. It should be possible to prove the conjecture using the results and methods of this paper.

15. Explicit formulae

Many of the above results were suggested by computer-assisted calculations using explicit examples of formal group laws. In this section, we record some useful formulae which will help the reader to carry out such experiments for herself. We shall assume that $n > 1$ and $p > 2$; some small modifications are needed when in the exceptional cases, but they generally make things easier. We write $a \equiv b$ for $a = b \pmod{p}$.

We first define

$$q = p^n, \qquad l(x) = \sum_{k \geq 0} x^{q^k}/p^k$$

$$e(x) = l^{-1}(x) \quad (\text{so } e(l(x)) = x).$$

Note that $l(px)/p \in \mathbb{Z}[\![x]\!]$, and in fact $l(px)/p = x \pmod{p}$. The composition inverse of this series is $e(px)/p$, so $e(px)/p = x \pmod{p}$. We define a formal group law F_1 over $\mathbb{Q}$ by $F_1(x, y) = e(l(x), l(y))$. It is shown in [7] (for example) that this is actually defined over $\mathbb{Z}_p$ (or even $\mathbb{Z}$, but this is irrelevant for us). We write $F_0(x, y)$ for the resulting formal group over $\mathbb{F}_p$. It is known that any formal group law of height n over a separably closed field of characteristic p is isomorphic to F_0 (see [6, p. 72]).

For any $a \in \mathbb{Z}_p$ we write $[a](x) = e(al(x))$. In other words, if $\mathbb{G}_1$ is the formal group defined by F_1 we have $[a](x) = a^{*}_{\mathbb{G}_1} x$. By applying l one checks that $[p](x) = e(px) +_{F_1} x^q$. We next define $C_{p^m}(x, y) = (x^{p^m} + y^{p^m} - (x + y)^{p^m})/p$.

Lemma 77. $C_p(x, y) \equiv -\sum_{k=1}^{p-1} x^k(-y)^{p-k}/k$.

Proof. This follows easily from Wilson's Theorem (that $(p-1)! \equiv -1$), the equation

$$(p-k)! = \prod_{l=k}^{p-1} (p-l) \equiv (-1)^{p-k}(p-1)!/(k-1)!,$$

and the binomial expansion of $(x+y)^p$. □

Lemma 78. $C_q(x, y) \equiv C_p(x^{q/p}, y^{q/p})$.

Proof. We have $x^{q/p} + y^{q/p} = (x+y)^{q/p} + pz$ for some z. Raising this to the pth power, we find that $(x^{q/p} + y^{q/p})^p = (x+y)^q \pmod{p^2}$. We also have

$$x^q + y^q = (x+y)^q + pC_q(x, y), \quad x^q + y^q = (x^{q/p} + y^{q/p})^p + pC_p(x^{q/p}, y^{q/p}).$$

Subtracting these, we obtain $pC_q(x, y) = pC_p(x^{q/p}, y^{q/p}) \pmod{p^2}$. The claim follows. □

Note that xy divides $C_p(x, y)$, so that $x^{q/p}y^{q/p}$ divides $C_q(x, y)$ mod p. We write $v_p(n)$ for the p-adic valuation of n.

Lemma 79. *If* $0 < l < q^k$ *then*

$$v_p \binom{q^k}{l} = nk - v_p(l).$$

Proof. We can write

$$\binom{q^k}{l} = \frac{q^k}{l} \prod_{j=1}^{l-1} \frac{q^k - j}{j}.$$

The terms in the product are clearly p-adic units; the claim follows. □

Lemma 80. $x +_{F_0} y = x + y + C_p(x^{q/p}, y^{q/p}) \bmod (xy)^q, p)$.

Proof. It is enough to prove this mod y^q, for then by symmetry and unique factorisation it will hold mod $(xy)^q$. For the rest of the proof, we put $y^q = 0$. For some $w \in \mathbb{Z}[\![x, y]\!]$ we have $F_1(x, y) = x + yw$. Applying l, we obtain $l(x) + l(y) = l(x + yw) = l(x) + \sum_{j=1}^{q-1} l^{(j)}(x)(yw)^j/j!$. Because $y^q = 0$, we have $l(y) = y$. We conclude that $y = \sum_{j=1}^{q-1} l^{(j)}(x)(yw)^j/j!$. Lemma 79 implies that the series $l^{(j)}(x)/j!$ for $0 < j < q$

are all integral, and moreover that

$$\frac{l^{(j)}(x)}{j!} \equiv \frac{1}{p}\binom{q}{j}x^{q-j} \quad (1 < j < q)$$

$$l'(x) \equiv 1 \equiv 1 + \frac{1}{p}\binom{q}{1}x^{q-1}.$$

This implies that

$$y \equiv yw + \sum_{j=1}^{q-1}\frac{1}{p}\binom{q}{j}x^{q-j} \equiv yw - C_q(x, yw) \equiv yw - C_p(x^{q/p}, (yw)^{q/p}).$$

Now define z by $yw = y + C_p(x^{q/p}, y^{q/p}) + z$. Note that $y^{q/p}$ divides $C_p(x^{q/p}, y^{q/p})$. As $n \geq 2$, we find that $y^{q^2/p^2} = 0$; it follows that $C_p(x^{q/p}, y^{q/p})^{q/p} = 0$, and thus that $(yw)^{q/p} \equiv y^{q/p} + z^{q/p}$. Feeding this back into our previous equation, we find $y \equiv y + C_p(x^{q/p}, y^{q/p}) + z - C_p(x^{q/p}, y^{q/p} + z^{q/p})$, so $z \equiv C_p(x^{q/p}, y^{q/p} + z^{q/p}) - C_p(x^{q/p}, y^{q/p})$. It follows easily that $z^{q/p}$ divides z mod p. On the other hand, the definition of z implies that y divides z, and thus that z is nilpotent. As z is nilpotent and $z^{q/p}$ divides z, we see that $z = 0$. The claim follows. □

Corollary 81. *There is a power series G over $\mathbb{F}_p$ such that $F_0(x, y) = x + y + G(x^{q/p}, y^{q/p})$.*

Proof. Work in $\mathbb{F}_p[\![x, y, z]\!]/z^{q/p}$. Let k be an integer, and write $k = p^r l$ with $l \not\equiv 0$. We then have $(y+z)^k = (y^{p^r} + z^{p^r})^l = y^k + l y^{k-p^r} z^{p^r} + \cdots$. It follows that $(y+z)^k = y^k$ if q/p divides k. Next, write

$$F_0(x, y) = x + y + \sum_{k>0} a_k(x) y^k.$$

The associativity law says that $F_0(x, F_0(y, z)) = F_0(F_0(x, y), z)$. By the previous lemma, we have $F_0(u, z) = u + z$ for all u. It follows that $F_0(x, y + z) = F_0(x, y) + z$, so

$$\sum_{k>0} a_k(x)(y + z)^k = \sum_{k>0} a_k(x) y^k.$$

We conclude that $a_k(x) = 0$ unless q/p divides k, so that $F_0(x, y) - x - y$ is a function of $y^{q/p}$. By symmetry, it is also a function of $x^{q/p}$. The claim follows. □

Next, we write $W = W\mathbb{F}_q$ for the Witt ring of $\mathbb{F}_q$. Recall that for each $a \in \mathbb{F}_q$ there is a unique element $\hat{a} \in W$ (the Teichmüller representative) such that $\hat{a}^q = \hat{a}$ and $\hat{a} \equiv a$. Any element $a \in W$ can be written uniquely as $\sum_{i \geq 0} a_i p^i$, with $a_i^q = a_i$. There is a Frobenius automorphism F of W defined by $F(\sum a_i p^i) = \sum a_i^p p^i$. For any $a \in \mathbb{F}_q$ we have $l(\hat{a}x) = \hat{a}l(x)$. It follows easily that $e(\hat{a}x) = \hat{a}e(x)$, $F_1(\hat{a}x, \hat{a}y) = \hat{a}F_1(x, y)$. If we write $e(x) = \sum_k m_k x^k$, $F_1(x, y) = \sum_{k,l} a_{kl} x^k y^l$, then we can conclude that $a_{kl} = 0$ unless $k + l = 1 \pmod{q-1}$, and similarly for $e(x)$ etc.

Now suppose that $a \in W$ is arbitrary. We define $[a](x) = e(al(x))$. By expressing a in the form $\sum_i \hat{a}_i p^i$, we can show that this lies in $W[\![x]\!]$. The map $a \mapsto [a](x)$ gives a ring homomorphism $W \to \mathrm{End}(F_1)$. We next put $E = W[\![u_1, \dots, u_{n-1}]\!]$, $u_0 = p$, $u_n = 1$. We also let ϕ denote the endomorphism of E which is the Frobenius on W and sends u_k to u_k^p for $0 < k < n$, so that $a^\phi = a^p \pmod{p}$ for all a.

Over $E[1/p]$ we have a formal power series $\log_F(x) = x + \mathrm{O}(x^2)$ characterised uniquely by either of the two following equations:

$$\log_F(x) = x + \frac{1}{p}\sum_{k=1}^{n} \log_F\left(u_k x^{p^k}\right), \quad \log_F(x) = x + \frac{1}{p}\sum_{k=1}^{n} u_k \log_F^{\phi^k}\left(x^{p^k}\right).$$

From either of these equations, one can see that $F = F_1 \pmod{u_1, \dots, u_{n-1}}$. The following more explicit formulae are given in [14, Section 4.3]. Consider a (possibly empty) sequence $I = (i_1, \dots, i_m)$ with $0 < i_k \leq n$ for all k. Write $|I| = m$ and $\|I\| = \sum_k i_k$ and $j_k = \sum_{l<k} i_l$. Finally, put

$$u_I = \prod_k u_{i_k}^{p^{j_k}}.$$

We then have

$$\log_F(x) = \sum_I \frac{u_I}{p^{|I|}} x^{p^{\|I\|}}.$$

We write $\exp_F(x)$ for the inverse of $\log_F(x)$ (under composition) and set $F(x,y) = x +_F y = \exp_F(\log_F(x) + \log_F(y))$. One can show that this lies in $E[\![x,y]\!]$ (rather that $E[1/p][\![x,y]\!]$), so it defines a formal group law over E.

By applying $\log_F$, one can check that

$$[p]_F(x) = \exp_F(px) +_F u_1 x^p +_F \cdots +_F u_{n-1} x^{p^{n-1}} +_F x^{p^n}.$$

Lemma 82. *If $k > 0$ then*

$$x +_F y = x + y + u_k C_{p^k}(x,y) \quad \mathrm{mod}(u_1, \dots, u_{k-1}) + (x,y)^{p^k+1}.$$

Proof. We work mod $(x,y)^{p^k+1}$ and $(u_1, \dots, u_{k-1})$. This leaves us with a torsion-free ring, so we can still use the logarithm. In this setting, for $w \in (x,y)$ we have $\log_F(w) = w + u_k w^{p^k}/p$ and $wC_{p^k}(x,y) = 0$. For some $z \in (x,y)$ we have $F(x,y) = x + y + u_k C_{p^k}(x,y) + z$. Applying $\log_F$, we get $\log_F(x) + \log_F(y) = \log_F(x + y + u_k C_{p^k}(x,y) + z)$ so

$$x + y + u_k x^{p^k}/p + u_k y^{p^k}/p = x + y + u_k C_{p^k}(x,y) + z + u_k(x + y + z)^{p^k}/p$$

$$z = u_k(x+y)^{p^k}/p - u_k(x+y+z)^{p^k}/p.$$

Thus $z \in (x,y,z)z = (x,y)z$. As the ideal (x,y) is nilpotent, we have $z = 0$ as claimed. □

It follows from this (see [10]) that F is the universal deformation of F_0.

Lemma 83. *$F(x,y)=x+y$ mod(xy) or mod$(y^{q/p},u_0y,u_1y,\dots,u_{n-1}y)$.*

Proof. The first statement holds for any formal group law. Now work mod the second ideal. By the first statement, $F(x,y)-F_1(x,y)$ is divisible by xy. From the definitions, all the coefficients also lie in the ideal $J=(u_1,\dots,u_{n-1})$. Because $Jy=0$, we see that $F(x,y)=F_1(x,y)$. Now consider $F_1(x,y)-x-y$. Using Lemma 80, we see that every term is divisible either by py or by $y^{q/p}$, both of which are zero. Thus $F_1(x,y)=x+y$ as required. □

Next, observe that $(x+_{F_0}y)^{p^k}=x^{p^k}+_{F_0}y^{p^k}$. It follows that $(x+_{F_1}y)^{p^k}-_{F_1}(x^{p^k}+_{F_1}y^{p^k})$ is divisible by p. Thus, there are unique series $\sigma_k(x,y)\in\mathbb{Z}_p[\![x,y]\!]$ such that $(x+_{F_1}y)^{p^k}=x^{p^k}+_{F_1}y^{p^k}+_{F_1}p\sigma_k(x,y)$.

Lemma 84. *$F(x,y)=F_1(x,y)-\sum_{k=1}^{n-1}u_k\sigma_k(x,y) \quad \text{mod}\ (u_0,\dots,u_{n-1})^2$.*

Proof. Write $J=(u_1,\dots,u_{n-1})$ and $I=(p)+J$. For the moment, we work mod J^2. In this setting we have

$$\log_F(x)=x+\sum_{k=1}^{n}u_kl(x^{p^k})/p=l(x)+\sum_{k=1}^{n-1}u_kl(x^{p^k})/p.$$

Next, observe that $x+_Fy-_F(x+_{F_1}y)$ vanishes mod J, so there are unique series $\tau_k(x,y)\in\mathbb{Z}_p[\![x,y]\!]$ such that

$$x+_Fy-_F(x+_{F_1}y)=\sum_{k=1}^{n-1}u_k\tau_k(x,y)(\text{mod}\,J^2).$$

By Lemma 83 we can rewrite the right-hand side as a formal sum. Thus $x+_Fy=(x+_{F_1}y)+_Fu_1\tau_1(x,y)+_F\cdots+_Fu_{n-1}\tau_{n-1}(x,y)$. We now apply $\log_F$ to this equation. The left hand side becomes

$$l(x)+l(y)+\sum_{k=1}^{n-1}\frac{u_k}{p}\left(l(x^{p^k})+l\left(y^{p^k}\right)\right).$$

The right-hand side becomes

$$l(x+_{F_1}y)+\sum\frac{u_k}{p}l\left((x+_{F_1}y)^{p^k}\right)+\sum u_k\tau_k(x,y).$$

Recall that $l(x+_{F_1}y)=l(x)+l(y)$ and $l((x+_{F_1}y)^{p^k})=l(x^{p^k})+l(y^{p^k})+l(p\sigma_k(x,y))$. Using this to simplify the right-hand side further, and rearranging, we conclude that

$$\sum u_k\tau_k(x,y)+\sum_k\frac{u_k}{p}l(p\sigma_k(x,y))=0.$$

Finally, we recall that $l(px)/p=x$ (mod p). This implies that $\tau_k(x,y)=-\sigma_k(x,y)$ (mod p), which proves the lemma. □

16. Examples

In this section we let $\mathbb{G}_1$ be the formal group over $\mathbb{Z}_2$ with logarithm $\log_F(x) = \sum_k x^{4^k}/2^k$, so that $\mathbb{G}_0$ is a formal group of height 2 over $\kappa = \mathbb{F}_2$. Computer calculations give results as follows.

(i) Let $A \simeq \mathbb{Z}/2$ be generated by a. Given a level-A structure ϕ, we shall identify a with $x(\phi(a))$. We then have $\mathrm{Level}(A, \mathbb{G}_0) = \mathrm{spf}(\kappa[a]/a^3)$. A coordinate on the quotient group $\mathbb{G}_0/[\phi A]$ is given by $y = ax + x^2 + a^2x^3$. The associated formal group law is

$$\begin{aligned} y +_{F'} z = {} & y + z + ayz + y^2z^2 + a(y^2z^3 + y^3z^2) \\ & + a^2(y^2z^4 + y^3z^3 + y^4z^2) + \cdots \end{aligned}$$

(ii) Now take $A \simeq (\mathbb{Z}/2)^2$, with generators a and b. Then $\mathrm{Level}(A, \mathbb{G}_0) = \mathrm{spf}(\kappa[a,b]/(a^3, b^3, a^2 + ab + b^2))$. Because $A = A(1)$, the corresponding subgroup divisor is just $\mathbb{G}_0(1)$, and a coordinate on the quotient group is just given by $[2](x) = x^4$.

(iii) Take $A = \mathbb{Z}/4$ generated by a. Then

$$\mathrm{Level}(A, \mathbb{G}_0) = \mathrm{spf}(\kappa[a]/a^{12})$$

$$\mathrm{Type}(A, \mathbb{G}_0) = \mathrm{spf}(\kappa[b]/b^6) \quad b = a^2 + a^5 + a^8 + a^{11}.$$

The equation of the subgroup divisor is

$$\prod_{c \in A} (x - c) = x^4 + b^5x^3 + bx^2 + b^3x.$$

(iv) $\mathrm{Sub}_2(\mathbb{G}_0) = \mathrm{spf}(\kappa[b]/b^7)$. The equation of the subgroup divisor is $x^4 + b^5x^3 + bx^2 + (b^3 + b^6)x$. The map of rings induced by $\mathrm{Type}(A, \mathbb{G}_0) \to \mathrm{Sub}_2(\mathbb{G}_0)$ just sends b to b.

Now let $\mathbb{G}_1$ be the standard height 3 formal group over $\mathbb{Z}_2$, with logarithm $\log_F(x) = \sum_k x^{8^k}/2^k$. Let $A \simeq \mathbb{Z}/4 \oplus \mathbb{Z}/2$ be generated by a and b. Then

$$\mathrm{Level}(A, \mathbb{G}_0) = \mathrm{spf}(\kappa[a,b]/(a^{56}, b^6 + b^5a^8 + b^4a^{16} + \cdots + a^{48}))$$

$$\mathrm{Type}(A, \mathbb{G}_0) = \mathrm{spf}(\kappa[c,d]/(c^{15}, c^{14}d, c^{13}d^2 + c^{14}, d^3 + c^8d + c^{12})).$$

where

$$\begin{aligned} c = {} & a^4 + a^{18} + a^{32} + a^{10}b + a^{17}b \\ & + a^{38}b + a^2b^2 + a^9b^2 + a^{16}b^2 \\ & + a^{37}b^2 + b^4 + a^{14}b^4 + a^{21}b^4 \\ & + a^{35}b^4 + a^{34}b^5 + a^{41}b^5, \\ d = {} & a^8b + b^2 + a^{32}b^5, \end{aligned}$$

The equation of the group divisor is

$$\begin{aligned} f(x) = x^8 & \\ & + (dc^7 + c^3d^2 + c^{10}d^2)x^6 \\ & + c^5d^2x^5 \\ & + cx^4 \\ & + (dc^{13} + c^9d^2)x^3 \\ & + (cd + c^5)x^2 \\ & + (dc^3 + c^{14})x. \end{aligned}$$

Note that $f(x) = x^8 \pmod{c}$; it follows that d does not lie in the subring generated by the coefficients of f, which shows that the map $\mathrm{Type}(A, \mathbb{G}) \to \mathrm{Sub}_8(\mathbb{G})$ is not a closed embedding.

References

[1] J.F. Adams, Stable Homotopy and Generalised Homology (University of Chicago Press, Chicago, 1974).

[2] W. Bruns and J. Herzog, Cohen–Macaulay Rings, Cambridge Studies in Advanced Mathematics, Vol. 39 (Cambridge University Press, Cambridge, 1993).

[3] M. Demazure and P. Gabriel, Groupes Algébriques (North-Holland, Amsterdam, 1970).

[4] E.S. Devinatz, M.J. Hopkins and J.H. Smith, Nilpotence and stable homotopy theory I, Ann. Math., 128 (1988) 207–242.

[5] V.G. Drinfel'd, Elliptic modules, Math. USSR-Sb. 23 (1974) 561–592.

[6] A. Frölich, Formal Groups, Lecture Notes in Mathematics, Vol. 74 (Springer, Berlin, 1968).

[7] M. Hazewinkel, Formal Groups and Applications (Academic Press, New York, 1978).

[8] M.J. Hopkins, N.J. Kuhn and D.C. Ravenel, Generalised group characters and complex oriented cohomology theories, to appear.

[9] N.M. Katz and B. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies, Vol. 108 (Princeton University Press, Princeton, 1985).

[10] J. Lubin and J. Tate, Formal moduli for one parameter formal lie groups, Bull. Soc. Math. France 94 (1966) 49–60.

[11] H. Matsumura, Commutative Ring Theory, Cambridge Studies in Advanced Mathematics, Vol. 8 (Cambridge University Press, Cambridge, 1986).

[12] J. Morava, Completions of complex cobordism, Lecture Notes in Mathematics, Vol. 658 (Springer, Berlin, 1978) 349–361.

[13] J. Morava, Noetherian localisations of categories of cobordism comodules, Ann. Math. 121 (1985) 1–39.

[14] D.C. Ravenel, Complex Cobordism and Stable Homotopy Groups of Spheres (Academic Press, New York, 1986).

[15] N.P. Strickland, Functorial philosophy for formal phenomena, in preparation.

[16] J. Tate and F. Oort, Group schemes of prime order, Ann. Sci. École Norm. Sup. 3 (1970) 1–21.