FINITE SUBGROUPS OF FORMAL GROUPS

NEIL P. STRICKLAND

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.

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 [?] for more details.

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 $G_0$ of finite height over a field of positive characteristic, and let $G/X$ be its universal deformation. The content of subsequent sections is as follows.

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

Section 8:
We investigate maps of schemes over $X$ between the schemes $\text{Level}(A, G)$; 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 $\text{Level}(A, G) \to \text{Level}(B, G')$, for a different group $G'$.

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

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

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

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

If $X = \text{spf}(A)$ 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 $a: Z \to Y$ 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 $\kappa_X = \mathcal{O}_X/m_X$ for the residue field. We also write $X_0 = \text{spf}(\kappa_X)$ and refer to this as the *special fibre* of $X$.

We write $\dim(X)$ for the Krull dimension of $X$ and $\text{embdim}(X)$ for the embedding dimension, that is

$$\text{embdim}(X) = \dim_{\kappa_X}(m_X/m_X^2).$$

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 $\kappa_X$ for the field of fractions of $\mathcal{O}_X$. Suppose we have a map of schemes $f: X \to Y$, and thus a map $f^*: \mathcal{O}_Y \to \mathcal{O}_X$, 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]).

**Lemma 2.1.** A finite dominant map of smooth schemes is flat.

**Proof.** Suppose $X$ and $Y$ are smooth, and $f: X \to Y$ is finite and dominant. Then $f^*: \mathcal{O}_Y \to \mathcal{O}_X$ is injective, and $\mathcal{O}_X$ is a finitely generated module over the regular subring $f^*\mathcal{O}_Y$. Because $\mathcal{O}_X$ is Cohen-Macaulay [11, Theorem 17.8], it is free over any regular subring over which it is finitely generated. \qed

**Lemma 2.2.** 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 $g$.

**Proof.** Write $R = \mathcal{O}_Z$, $S = \mathcal{O}_Y$, $T = \mathcal{O}_X$, so $R \to T$ is mono and $T$ is a finite $R$-module. Let $\mathcal{S}$ denote the image of $S$ in $T$. It is an integral domain and $R \leq \mathcal{S}$ is an integral extension, so $\dim(\mathcal{S}) = d$. Choose a maximal chain $0 = p_0 < \ldots < p_d$ in $\text{spec}(\mathcal{S})$, and denote the preimages in $S$ by $p_0 < \ldots < p_d$. As $\dim(S) = d$, this chain must be maximal, so $p_0 = 0$, so $S = \mathcal{S}$. Thus $S \to T$ is mono, in other words $f$ is dominant. This also makes it clear that $S$ is a finite $R$-module, so $g$ is finite. It is immediate that $f$ is finite and $g$ is dominant. \qed

**Lemma 2.3.** If $X$ is smooth and $f: X \to Y$ is finite and flat then $Y$ is smooth.
Definition 2.4. A finite extension $R \rightarrow S$ of integral domains is Galois iff $R$ is the fixed subring for the action of $\text{Aut}_R(S)$ on $S$ and $S$ is free over $R$. I am not sure whether this definition is standard. Similarly, we say that a map $X \rightarrow Y$ of integral schemes is a Galois covering iff $\mathcal{O}_Y \rightarrow \mathcal{O}_X$ is Galois.

Lemma 2.5. If $f: X \rightarrow Y$ is Galois then $\mathcal{K}_X$ is Galois over $\mathcal{K}_Y$ and
\[
\deg(f) = [\mathcal{O}_X : \mathcal{O}_Y] = [\mathcal{K}_X : \mathcal{K}_Y] = |\text{Aut}_{\mathcal{O}_Y}(\mathcal{O}_X)| = |\text{Aut}_{\mathcal{K}_Y}(\mathcal{K}_X)|
\]

Proof. Write $\Gamma = \text{Aut}_{\mathcal{O}_Y}(\mathcal{O}_X)$ and $d = \deg(f)$. As $\mathcal{O}_Y \rightarrow \mathcal{O}_X$ is a finite extension of integral domains, we see that
\[
\mathcal{K}_X = \mathcal{K}_Y \otimes_{\mathcal{O}_Y} \mathcal{O}_X \simeq \mathcal{K}_Y^d
\]

and also that
\[
\deg(f) = [\mathcal{O}_X : \mathcal{O}_Y] = [\mathcal{K}_X : \mathcal{K}_Y] = d
\]

It follows that
\[
\mathcal{K}_X^\Gamma = \mathcal{K}_Y \otimes_{\mathcal{O}_Y} \mathcal{O}_X^\Gamma = \mathcal{K}_Y
\]

The usual Galois theory of fields now tells us that $\mathcal{K}_Y$ is Galois over $\mathcal{K}_X$, that the Galois group $\text{Aut}_{\mathcal{K}_X}(\mathcal{K}_Y)$ is just $\Gamma$, and that $|\Gamma| = d$.

Lemma 2.6. A finite dominant map $f: X \rightarrow Y$ of smooth schemes is a Galois covering iff the extension of function fields $\mathcal{K}_Y \rightarrow \mathcal{K}_X$ is Galois.

Proof. The forward implication is just the previous lemma. For the converse, suppose that $\mathcal{K}_Y \rightarrow \mathcal{K}_X$ is Galois, with Galois group $\Gamma$. Lemma 2.1 tells us that $f$ is flat, so that $\mathcal{O}_X$ is a free $\mathcal{O}_Y$-module, of rank $d$ say. Clearly $|\Gamma| = |\mathcal{K}_Y : \mathcal{K}_X| = d$. By definition $\Gamma = \text{Aut}_{\mathcal{K}_Y}(\mathcal{K}_X)$; I claim that this is the same as $\Gamma' = \text{Aut}_{\mathcal{O}_Y}(\mathcal{O}_X)$. There is an obvious monomorphism $\Gamma' \rightarrow \Gamma$; to show that it is epi we need only verify that each $\alpha \in \Gamma$ has $\alpha(\mathcal{O}_X) \leq \mathcal{O}_X$. Because $\mathcal{O}_X$ is integral over $\mathcal{O}_Y$, we see that $\alpha(\mathcal{O}_X)$ is integral over $\mathcal{O}_Y = \mathcal{O}_Y$ and therefore also over $\mathcal{O}_X$. However, $\mathcal{O}_X$ is regular and thus integrally closed in $\mathcal{K}_X$, so the claim follows. Finally, we know that $\mathcal{O}_X^{\Gamma'}$ is integral over $\mathcal{O}_Y$ (indeed, $\mathcal{O}_X$ is) and contained in $\mathcal{K}_X^\Gamma = \mathcal{K}_Y$; as $\mathcal{O}_Y$ is integrally closed, this shows that $\mathcal{O}_Y = \mathcal{O}_X^{\Gamma'}$.

Lemma 2.7. Let $X$ be a smooth scheme with a faithful action of a finite group $\Gamma$. Suppose that $f: X \rightarrow Y$ 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 $X/\Gamma \rightarrow Y$ is iso.

Proof. By Lemma 2.3, we see that $Y$ is smooth. Because $[\mathcal{K}_Y : \mathcal{K}_X] = |\Gamma|$ and $\mathcal{K}_Y \leq \mathcal{K}_X^\Gamma$, Galois theory tells us that $\mathcal{K}_Y = \mathcal{K}_X^\Gamma$ and thus $\mathcal{K}_Y \rightarrow \mathcal{K}_X$ is Galois. The claim now follows from Lemma 2.6.

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

Lemma 2.8. Suppose we have a pullback diagram
\[
\begin{array}{ccc}
V & \xrightarrow{a} & X \\
\downarrow{g} & & \downarrow{f} \\
W & \xrightarrow{b} & Y
\end{array}
\]

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

3
Proof. For the square to be a pullback means that \( \mathcal{O}_Y = \mathcal{O}_W \otimes_{\mathcal{O}_X} \mathcal{O}_X \), and with this identification we have \( g^* = 1 \otimes f^* \) and \( a^* = b^* \otimes 1 \). The claim follows easily by choosing bases. \( \square \)

Lemma 2.9. Suppose that \( s: Y \to X \) is a section of \( f \), and that \( s^* u = 0 \). Then \( N_f u = 0 \).

Proof. We can write \( \mathcal{O}_X = f^* \mathcal{O}_Y + I \), 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. \( \square \)

3. Formal Groups

Let \( X = \text{spf}(A) \) be a scheme, and \( \mathbb{G} \) a one-dimensional commutative formal group over \( X \). In more detail, we have \( \mathbb{G} = \text{spf}(B) \) where \( B \) is isomorphic to \( A[[x]] \) as an augmented \( A \)-algebra, and we are given a commutative group law \( \mu: \mathbb{G} \times_X \mathbb{G} \to \mathbb{G} \) (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: \( X \to \mathbb{G} \)).

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

\[
\begin{array}{ccc}
\mathbb{G} & \xrightarrow{q} & \mathbb{H} \\
\downarrow & & \downarrow \\
X & \xrightarrow{f} & Y
\end{array}
\]

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 \( a, b: Y \to \mathbb{G} \) 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:

\[
\begin{align*}
F(y, z) &= y + z \pmod{xy} \\
F(y, z) &= F(z, y) \\
F(F(x,y), z) &= F(x, F(y,z))
\end{align*}
\]

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

Lemma 3.1. Let \( q: \mathbb{G} \to \mathbb{H} \) 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 \( q^* y = ax^n \pmod{m x^{n+1}} \).

Proof. Clearly there exist \( 0 \neq a \in \mathcal{O}_X \) and \( r \in \mathbb{N} \) such that \( q^* y = ax^r \pmod{x^{r+1}} \); we need to show that \( r \) is a power of \( p \). Because \( q \) is a homomorphism, we have

\[
(q \times q)^r \mu_{\mathbb{H} y} = \mu_{\mathbb{G} y} \circ q^* y \in \mathcal{O}_X[[x_0, x_1]]
\]

Using \( \mu_{\mathbb{G} y}(x) = x_0 + x_1 \mod{(x_0, x_1)^2} \) (and similarly for \( \mathbb{H} \)) and working mod \((x_0, x_1)^{r+1} \), we find that

\[
a(x_0^r + x_1^r) = a(x_0 + x_1)^r
\]

Write \( r = p^n m \) where \( m \neq 0 \) (mod \( p \)), and observe that

\[
(x_0 + x_1)^r = (x_0^n + x_1^n)^m = x_0^n + n x_0^{r-p} x_1^n + \cdots \pmod{p}
\]

It follows that the coefficient of \( x_0^{-p} x_1^n \) in \((x_0 + x_1)^r\) is a unit in \( \mathcal{O}_X \). Unless \( m = 1 \), we easily arrive at a contradiction. \( \square \)

Definition 3.2. 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 \( G \) to be a formal group of finite height \( n \) over a connected base scheme \( X \).

**Proposition 3.3.** If \( q : G \to \mathbb{H} \) is nonzero, then \( m = \text{height}(q) \) is finite and \( q \) is flat of degree \( p^m \). Moreover, \( \text{height}(H) = \text{height}(G) \).

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

4. **Divisors**

By a divisor on \( G \) we shall mean a closed subscheme \( D \leq G \) which is finite and flat over \( X \).

**Proposition 4.1.** If \( D \) is a divisor of degree \( d \) on \( G \) and \( x \) is a coordinate, then there is a unique monic polynomial \( f_D(x) \) of degree \( d \) such that \( O_D = O_G/f_D(x) \). Moreover, \( f_D(x) \) is the characteristic polynomial of the \( O_X \)-linear endomorphism of \( O_D \simeq O_X^d \) given by multiplication by \( x \), and \( f_D(x) = x^d \pmod{m} \).

**Proof.** This is again standard. We define \( f_D \) to be the characteristic polynomial as described. By Cayley-Hamilton, this vanishes in \( O_D \), so we have an epimorphism \( O_G/f_D \to O_D \). The coefficient of \( x^k \) for \( k < d \) must be a nonunit, lest \( O_G/f_D \) have rank less than \( d \). Thus \( f_D(x) = x^d \pmod{m} \). Uniqueness is easy. \( \square \)

**Definition 4.2.** 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 \( G \) over \( Y \) will just mean a divisor on the pulled-back group \( G \times_X Y \).

Because we are assuming that \( G \) has finite height \( n \), the subscheme

\[
\mathcal{G}(m) = \ker(p^m : G \to G) = \text{spf}(O_G/(p^m)^*x)
\]

is a divisor of degree \( p^mn \).

If \( a \) is a section of \( G \) 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 4.3.** For any formal group law over any ring \( A \), the power series \( x - y \) is a unit multiple of \( x - y \) in \( A[x, y] \).

**Proof.** \( x - y \) clearly vanishes \( \pmod{(x - y)} \). By considering the first few terms, it is easy to see that \( (x - y)/(x - y) \) must be 1 \( \pmod{(x - y)} \), so it is a unit. \( \square \)

Given two divisors \( D \) and \( D' \), we define a divisor \( D + D' \) by the requirement that \( f_{D+D'}(x) = f_D(x)f_{D'}(x) \). It is not hard to see that this is independent of the coordinate \( x \). The next two lemmas can be proved by elementary manipulation of polynomials.

**Lemma 4.4.** If divisors \( D_i \) on \( G \) over \( Y \) satisfy \( D_0 + D_1 = D_0 + D_2 \) then \( D_1 = D_2 \).

**Lemma 4.5.** Suppose \( f : X \to Y \) is epi. If we have divisors \( D_0, D_1 \) on \( Y \) and \( D'_0, D'_1 \) on \( X \) such that \( f^*D_0 = f^*D_1 + D'_2 \), then there is a unique divisor \( D_2 \) on \( Y \) such that \( f^*D_2 = D'_1 \), and moreover \( D_0 = D_1 + D_2 \). \( \square \)

The functor from schemes over \( X \) to sets defined by

\[
Y \mapsto \{\text{divisors of degree } d \text{ on } G \text{ over } Y\}
\]

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

\[
O_{\text{Div}_d(G)} = O_X[\sigma_1, \ldots, \sigma_d] \leq O_X[x_1, \ldots, x_d] = O_X^d
\]

(\( \text{where } \sigma_k \text{ is the } k\text{'th elementary symmetric function in the variables } x_i \)). 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 4.6.** Let $D, D'$ be two divisors on $\mathbb{G}$ over $X$. There is then a closed subscheme $Y \subseteq X$ such that for any map $\alpha: Z \to X$ we have $\alpha^* D \leq \alpha^* D' \in \Gamma(Z, \text{Div}(\mathbb{G}))$ if and only if $\alpha$ 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

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

Put $Y = \text{spf}(\mathcal{O}_X/(b_0,\ldots,b_{d-1}))$, 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 5.1.** 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 $X = X_0 = \text{spec}(k)$, 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 $F(x, y) = x + y \mod xy$. Because $K$ is a subgroup, we have $f_K(F(x, y)) = 0 \mod f_K(x), f_K(y)$. 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 3.1, this implies that $d$ is a power of $p$. □

**Proposition 5.2.** If $K$ is a finite subgroup of $\mathbb{G}$ of degree $p^m$ then $p_K^p = 0$ and thus $K \leq \mathbb{G}(m) = \ker(p^m_{\mathbb{G}})$.

**Proof.** This is a special case of a result of Deligne — see [15]. 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,

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

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 $\mu$ for the addition map $\mathbb{G} \times_X \mathbb{G} \to \mathbb{G}$ (or any of its restrictions) and $\pi: \mathbb{G} \times_X K \to \mathbb{G}$ for the projection. Let $\mathcal{O}_{\mathbb{G}/K}$ be the equaliser

$$\mathcal{O}_{\mathbb{G}/K} \xrightarrow{\mu^*} \mathcal{O}_{\mathbb{G}} \xrightarrow{\pi^*} \mathcal{O}_K \otimes_{\mathcal{O}_X} \mathcal{O}_{\mathbb{G}}$$

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

**Theorem 5.3.** With $K$ and $y$ as above, we have

1. $y = x^{p^m} \mod m_X$.
2. $\mathcal{O}_{\mathbb{G}/K} = \mathcal{O}_X[y]$.
3. $\mathbb{G}/K$ has a natural structure as a formal group.
4. The projection $\mathbb{G} \to \mathbb{G}/K$ is the categorical cokernel of $K \to \mathbb{G}$.
5. For any map $f: Y \to X$ we have $f^* \mathbb{G}/f^* K = f^*(\mathbb{G}/K)$.

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

$$
\begin{array}{ccc}
\mathbb{G} \times_X K \times_X K & \xrightarrow{\mu \times 1} & \mathbb{G} \times_X K \\
\pi' \downarrow & & \pi \downarrow \\
\mathbb{G} \times_X K \xrightarrow{\pi} \mathbb{G} & & \mathbb{G} \times_X K \xrightarrow{\mu} \mathbb{G}
\end{array}
$$
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 $\mu(1 \times \mu) = (\mu(1) \times 1)$, we see that $y = N_{\pi} \mu^* x \in O_G$ actually lies in $O_{G/K}$ as claimed. The argument so far follows [3].

Next, write $j: K \to G$ for the inclusion. I claim that $j^* y = 0$. To see this, let $i: K \to G \times X K$ 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

$$\begin{array}{ccc}
K & \xrightarrow{i} & G \times X K \\
\downarrow & & \downarrow \pi \\
X & \xrightarrow{0} & G
\end{array}$$

Using Lemma 2.8 we see that $0^* y = N_{K/X} \pi^* x = N_{K/X} j^* x$. The claim now follows from Lemma 2.9, 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 4.1 we know that $O_{K/m X} = \kappa[x]/x^{p^m}$, so that

$$O_{G \times X K/m X} = \kappa[x, z]/z^{p^m}.$$ 

As working mod $z$ is the same as restricting to $G$, we see that the image of $\mu^* x$ in this ring agrees with $x$ mod $z$. Using the basis $\{1, z, \ldots, z^{p^m-1}\}$, we conclude that the norm of $\mu^* x$ is just $x^{p^m}$. However, this norm is just the image of $y$ in $O_{G/m X}$, which gives part (1) 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

$$\begin{array}{ccc}
O_{G/K} & \xrightarrow{\mu^*} & O_K \otimes O_G \\
\downarrow & & \downarrow \pi^* \\
O_X & \xrightarrow{\pi^*} & O_K \otimes O_K
\end{array}$$

Suppose $u \in O_{G/K} \leq O_G$. 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 $u' \in O_G$. Using the Weierstrass factorisation, we see that $\pi^* y$ is not a zero divisor in $O_{G \times X K}$. Using this, we can check that $u' \in O_{G/K}$.

Extending this inductively, we conclude that $O_{G/K} = O_X[y]$, giving part (2) of the theorem.

For part (3), a diagram chase now shows that $G \times X G \xrightarrow{\nu} G \xrightarrow{\rho} G/K$ factors as $G \times X G \xrightarrow{\nu \times \nu} G/K \times X G/K \xrightarrow{\rho} G/K$ for a unique map $\nu$, which makes $G/K$ into a formal group with coordinate $y$. It is easy to see from the definition of $O_{G/K}$ that $G/K$ is the categorical cokernel of $j$, in other words that a map $r: G \to \mathbb{H}$ of formal groups factors through $q$ if and only if if $rj = 0$: this is part (4). Finally, our construction of $y$ clearly commutes with base change. It follows that $f^*(G/K) = f^* G/f^* K$ for any map $f: Y \to X$, as claimed in (5). $\square$

6. The Universal Deformation

Suppose that $X_0$ is a scheme of the form $spf(k)$ (where $k$ is a field of characteristic $p$), and that $G_0$ is a formal group over $X_0$ of finite height $n$. A deformation of $G_0$ 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 $G_0$. 

\[
\begin{array}{c}
H_0 \rightarrowtail \mathcal{G}_0 \\
\downarrow \quad \quad \downarrow \\
Y_0 \rightarrowtail X_0
\end{array}
\]

Of course, if we start with a group $G$ over $X$ and define $X_0$ to be the special fibre of $X$ and $G_0$ to be the restriction of $G$ to $X_0$, then $G$ is a deformation of $G_0$ 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 $H_0 \rightarrowtail G_0 \leftarrowtail H_0$.

\[
\begin{array}{c}
\mathbb{H} \rightarrow \mathbb{H}' \\
\downarrow \quad \quad \downarrow \\
Y \rightarrow Y'
\end{array}
\]

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

In [10] Lubin and Tate construct universal deformations of formal group laws. We can translate their results into coordinate-free language as follows.

**Proposition 6.1.** The category of deformations of $G_0/X_0$ has a terminal object $G/X$. Moreover, $X$ 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 $G_0$, and $G$ as the universal deformation.

**Proof.** Write

\[C_p(x, y) = (x^{p^n} + y^{p^n} - (x + y)^{p^n})/p \in \mathbb{Z}[x, y]\]

Let $W$ be the Witt ring of $\kappa$, which is a complete discrete valuation ring with maximal ideal $(p)$ and residue field $\kappa$. Write

\[X = \text{spf}(E) \quad \quad E = W[[u_1, \ldots, u_{n-1}]\]

We shall take $u_0 = p$ and $u_n = 1$, so that \{u_0, \ldots, u_{n-1}\} is a system of parameters for $E$. Choose a coordinate $x_0$ on $G_0$, and let $F_0 \in \kappa[[x, y]]$ be the resulting formal group law. By proposition 1.1 of [10], there is a formal group law $F$ over $E$ which lifts $F_0$ and has

\[F(x, y) = x + y + u_k C_p(x, y) \mod (u_1, \ldots, u_{k-1}) + (x, y)^{p^k + 1}\]

For particular choices of $F_0$, we can be more explicit — see Section 15. We write $G = \text{spf}(E[[x]])$, and give this the group structure defined by $F$. This makes $G/X$ a deformation of $G_0/X_0$ in a natural way. Now let $\mathbb{H}/Y$ be another deformation. Write $\kappa' = \mathcal{O}_{\mathbb{H}_0}$. By the definition of a deformation, we are given a map $\kappa \rightarrow \kappa'$ (which we think of as an inclusion) and an isomorphism

\[\kappa' \otimes_{\kappa} \mathcal{O}_{G_0} \rightarrow \mathcal{O}_{\mathbb{H}_0}\]

We write $y_0$ for the image of $1 \otimes x_0$, so that $\mathcal{O}_{\mathbb{H}_0} = \kappa'[[y_0]]$. The formal group law corresponding to the coordinate $y_0$ on $\mathbb{H}_0$ is just $F_0$ again. Now choose a coordinate $y$ on $\mathbb{H}$ extending $y_0$, and write $F'$ for the corresponding formal group law. By theorem 3.1 of [10], there is a map $u: E \rightarrow \mathcal{O}_Y$ and a formal power series $\phi \in \mathcal{O}_Y[[t]]$ such that $\phi(t) = t \mod \mathcal{O}_Y$ and

\[F'(\phi(y'), \phi(y'')) = \phi((uF)(y', y''))\]

Moreover, both $u$ and $\phi$ are uniquely determined by this. The map $u: \mathcal{O}_X \rightarrow \mathcal{O}_Y$ extends to a map $\mathcal{O}_G \rightarrow \mathcal{O}_H$ sending $x$ to $\phi(y)$. It is easy to check that this gives a morphism $\mathbb{H}/Y \rightarrow G/X$ of deformations. The uniqueness of $u$ and $\phi$ implies that this morphism is also unique, as claimed. □

Suppose we start with a group $G'/X'$, define $X_0 = X'_0$ to be the special fibre of $X'$ and $G_0 = G'_0$ the restriction of $G'$ over $X'_0$. Let $G/X$ be the universal deformation of $G_0/X_0$. There is then a unique map $f: X' \rightarrow X$ such that $G' \simeq f^*G$. We shall often use only the much weaker corollary that $G'$ is obtained by pulling back a group over a smooth scheme.
We see from the above proof that a coordinate can be chosen on $G$ such that
\[ \phi_{G}^{*} x = u_{m} x^{p^{m}} \pmod{u_{0}, \ldots, u_{m-1}, x^{p^{m}+1}} \]

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
\[ Y \mapsto \text{Hom}(A, \Gamma(Y, G)) \]
is represented by a scheme $\text{Hom}(A, G)$ over $X$. Indeed, we may write $A$ in the form $\bigoplus_{k=0}^{d-1} \mathbb{Z}/p^{k}$, and then $\text{Hom}(A, \mathbb{G})$ is isomorphic to the closed subscheme $\prod_{k} \mathbb{G}(d_{k})$ of $\mathbb{G}^{r}$ (where $\mathbb{G}(d) = \ker(p_{G}^{d})$ as usual). If $x$ is a coordinate on $G$ then
\[ \mathcal{O}_{\text{Hom}(A, G)} = \mathcal{O}_{X}[x_{0}, \ldots, x_{r-1}]/([p^{d_{0}}](x_{0}), \ldots, [p^{d_{r-1}}](x_{r-1})). \]
By Proposition 3.3, this is a finite free module over $\mathcal{O}_{X}$, in other words the map $\text{Hom}(A, G) \to X$ is finite and flat. The degree is $|A|^n$.

If $G$ were a discrete group, it would be natural to write
\[ \text{Hom}(A, G) = \bigoplus_{B \leq A} \text{Mon}(A/B, G) \]
where $\text{Mon}$ denotes monomorphisms). However, except in trivial cases, there is no scheme $\text{Hom}(A, G)$ over $X$ such that
\[ \text{Hom}(A, \Gamma(Y, G)) = \Gamma(Y, \text{Hom}(A, G)). \]
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 $\phi : A \to \Gamma(Y, G)$ 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 $|\text{Hom}(A, \Lambda)| = |A|^n$, which is the same as the degree of $\text{Hom}(A, G) \to X$. This is the first of many cases in which $\Lambda$ serves as a “discrete approximation” to $G$.

**Definition 7.1.** A level-$A$ structure on $G$ over an $X$-scheme $Y$ is a map $\phi : A \to \Gamma(Y, G)$ such that $|\phi A(1)| \leq G(1)$ as divisors. A level-$m$ structure means a level-$\Lambda(m)$ structure.

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

**Proposition 7.2.** The functor from schemes over $X$ to sets given by
\[ Y \mapsto \{ \text{level-A structures on } G \text{ over } Y \} \]
is represented by a scheme $\text{Level}(A, G)$ over $X$. (We will write $\text{Level}(m, G) = \text{Level}(\Lambda(m), G)$).

**Proof.** We can consider $G \times X \text{Hom}(A, G)$ as a formal group over $\text{Hom}(A, G)$. On this group we have a tautological map $\phi : A \to \Gamma(\text{Hom}(A, G), G)$ and thus a divisor $[\phi A(1)] \in \Gamma(\text{Hom}(A, G), \text{Div}(\mathbb{G}))$. Applying Proposition 4.6 to this divisor and the divisor $\mathbb{G}(1) \times X \text{Hom}(A, G)$, we get a closed subscheme $\text{Level}(A, G) \subseteq \text{Hom}(A, G)$. It is easy to see that this does the job. □

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

**Theorem 7.3.** Level$(A, G) \to X$ is a finite flat map. If $G$ is the universal deformation of $G_{0}$ then Level$(A, G)$ is smooth and has dimension $n$. □

**Theorem 7.4.** If $\phi : A \to \mathbb{G}$ is a level structure then $[\phi A]$ is a subgroup of $\mathbb{G}$ and $[\phi A(k)] \leq G(k)$ for all $k$. If $A = \Lambda(m)$ then $[\phi A] = G(m)$. □

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

**Notation.** $g_{m}(x)$ is the Weierstrass polynomial (of degree $p^{nm}$) which is a unit multiple of $(p^{m})^{*}(x)$. 

9
Lemma 7.5. If rank$(A) > n$ then Level$(A, \mathbb{G}) = \emptyset$.

Proof. In this case $[\phi A(1)]$ has degree greater than that of $G(1)$, 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 7.6. If $\mathcal{O}_Y$ is an integral domain of characteristic zero, then a map $\phi : A \rightarrow \Gamma(Y, \mathbb{G})$ is a level structure if and only if it is injective.

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

$$y = f_{[\phi A]}(x) = \prod_{\alpha \in A} (x - x_\alpha) \in \mathcal{O}_{\mathbb{G} \times X Y}.$$  

Suppose that $\phi$ is a level structure. Then for $a \in A \setminus \emptyset$ we have divisibility relationships:

$$x(x - x_\alpha) \mid y \mid p_\mathbb{G}^n x = px + \text{higher terms}.$$  

As $p \neq 0$ in $R$, we must have $x_\alpha \neq 0$ and thus $\phi(a) \neq 0$, as required. Conversely, suppose $\phi$ is injective. The values $x_\alpha$ as $\alpha$ 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

$$y = \prod_{\alpha \in A} (x - x_\alpha)$$

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

Proposition 7.7. Suppose that $X$ is integral. Then there is a prime ideal $p < \mathcal{O}_{\text{Level}(A, \mathbb{G})}$ with $p \cap \mathcal{O}_X = 0$.

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 $(p_\mathbb{G}^m)^* x$, so they form a group $A'$ under the operation $+$. If we identify a map $a : Y \rightarrow \mathbb{G}$ over $X$ with the element $x(a) = a^*(x) \in \mathcal{O}_Y$, then $A' = \Gamma(Y, \mathbb{G}(m))$.

Write $y = (p_\mathbb{G}^m)^* x$. 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 $p^m$. Moreover, $p^m A' = 0$ and $|A'| = p^m$. It follows by the structure theory of finite Abelian groups that $A' \cong (\mathbb{Z}/p^m)^n$, and thus that we can choose an embedding $A \rightarrow A'$. By Proposition 7.6, this is a level structure on $\mathbb{G}$ over $Y$. It is therefore classified by a map $f : Y \rightarrow \text{Level}(A, \mathbb{G})$ of schemes over $X$. We can take $p$ to be the kernel of $f^* : \mathcal{O}_{\text{Level}(A, \mathbb{G})} \rightarrow \mathcal{O}_Y$. □

Remark 7.8. In geometric language, this says that there is an irreducible component $Y$ of $\text{Level}(A, \mathbb{G})$ such that $Y \rightarrow X$ is finite and dominant. We shall see shortly that $Y = \text{Level}(A, \mathbb{G})$.

Corollary 7.9. If $X$ is integral then dim$(\text{Level}(A, \mathbb{G})) \geq $ dim$(X)$.

Proof. Write $E = \mathcal{O}_X = W[u_1, \ldots, u_{n-1}]$ (as in Section 6), and $D_A = \mathcal{O}_{\text{Level}(A, \mathbb{G})}$. Suppose that $A$ has rank $r$, say $A = \langle a_0, \ldots, a_{r-1} \rangle$. Write $x_{\kappa} = x(\phi(a_{\kappa})) \in D_A$. By the proof of Proposition 7.2, we know that these elements topologically generate $D_A$ over $E$, so that the $u$'s and $x$'s generate $m_{D_A}$. We also put

$$I = (x_{\kappa}, \ldots, x_{r-1}, u_r, \ldots, u_{n-1}).$$

It is enough to show that $D_A/I = \kappa$, for then

$$\text{embeddim}(A, \mathbb{G}) \leq n = \text{dim } X \leq \text{dim } (A, \mathbb{G}).$$

Write $Y = \text{spf}(D_A/I)$. The map $\phi : A \rightarrow \Gamma(Y, \mathbb{G})$ sends the generators to zero, so it is zero. Thus, $f(x) = f_{[\phi A(1)]}(x) = x^\kappa$ in $(D_A/I)[x]$. Because $\phi$ is a level structure, this divides $p_\mathbb{G}^n x$. Using the fact (see Section 6) that

$$p_\mathbb{G}^n x = u_m x^m \pmod{u_0, \ldots, u_{m-1}, x^m + 1},$$

we find that $u_0, \ldots, u_{n-1}$ 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 $m_{D_A}$, this implies that $D_A/I = \kappa$ as claimed. □
Proposition 7.11. For any \( G \), the projection \( \text{Level}(A, G) \to X \) is a finite flat map.

Proof. We may assume that \( G \) is the universal deformation of \( G_0 \), as the general case is easily recovered by base change. As \( \text{Level}(A, G) \) is a closed subscheme of \( \text{Hom}(A, G) \) and \( \text{Hom}(A, G) \to X \) is a finite flat map, we see that \( \text{Level}(A, G) \to X \) is finite. By propositions 7.7 and 7.10, we see that it is also dominant. A finite dominant map of smooth schemes is flat (Lemma 2.1).

Proposition 7.12. If \( \phi \) is a level structure then \([\phi A(k)]\) is a subgroup scheme contained in \( G(k) \).

Proof. We may assume that \( A = A(k) \), so that \( p^k A = 0 \). Suppose for the moment that the base scheme \( X \) is integral. As in the proof of Proposition 7.7, we see that the Weierstrass polynomial \( g_k \) has distinct roots. By Proposition 7.6, \( \phi \) 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 \([\phi A] \leq G(k)\) as claimed.

Next, write \( z = \prod_{a \in A} (x - f_a) = (\text{unit}) \times \prod_{a \in A} (x - x_a) \).

In other words, for any point \( b \) of \( G \) we have \( z(b) = \prod_{a \in A} x(b - \phi(a)) \).

Write \( \mathbb{H} = \text{spf}(\mathcal{O}_X[z]) \), so \( \mathbb{H} \) is a quotient scheme of \( G \). By the Weierstrass preparation theorem, we see that \( q: \mathbb{H} \to \mathbb{H} \) is flat, of degree \( |A| \).

We can let \( A \) act on \( \mathbb{H} \), with \( a \in A \) acting as translation by \( \phi(a) \). This action is faithful, because \( \phi \) is injective. The map \( q: \mathbb{H} \to \mathbb{H} \) clearly factors through \( G/A \). It follows from Lemma 2.7 that \( \mathbb{H} = \mathbb{H}/A \) and that \( q \) is Galois. Similarly, we find that \( (G \times X \mathbb{G})/(A \times A) = \mathbb{H} \times X \mathbb{H} \).

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 \( \text{spf}(\mathcal{O}_G/z) = [\phi A] \), so \([\phi A]\) is a subgroup scheme as claimed.

Now suppose that \( X \) is not integral. Let \( G'/X' \) be the universal deformation of \( G_0 \), and \( \phi' \) the universal level structure defined over \( \text{Level}(A, G') \). By Proposition 7.10, we know that \( \text{Level}(A, G') \) is integral, so the above tells us that \([\phi' A(k)]\) is a subgroup scheme contained in \( G'(k) \). Using the defining properties of \( X' \) and \( \text{Level}(A, G') \), we construct a map \( f: X \to \text{Level}(A, G') \) such that the pullback of \( G' \) is \( G \) and the pullback of \( \phi' \) is \( \phi \). It follows that \([\phi A(k)] = f^*[\phi' A(k)]\) is a subgroup scheme of \( G(k) \), as claimed.

Corollary 7.13. It follows from the above proof that \( z = \prod_{a \in A} (x - f_a) \) is a coordinate on the quotient group \( G/[\phi A] \).

8. Galois Theory of Level Structures

In this section, we assume that \( G \) is the universal deformation of \( G_0 \). We write

\[
\begin{align*}
D_A &= \mathcal{O}_{\text{Level}(A, G)} \\
D_m &= \mathcal{O}_{\text{Level}(m, G)} \\
E &= D_0 = \mathcal{O}_X \\
K_A &= \text{field of fractions of } D_A.
\end{align*}
\]

Theorem 8.1. Let \( A \) and \( B \) be finite Abelian \( p \)-groups of rank at most \( n \), and \( u: A \to B \) a monomorphism. Then:

(1) \( \text{Hom}_E(D_A, D_B) = \text{Hom}_K(K_A, K_B) = \text{Mon}(A, B) \).

(2) The map \( u': \text{Level}(B, G) \to \text{Level}(A, G) \) (which sends \( \phi \) to \( \phi \circ u \)) is finite and flat.

(3) If \( B \simeq A(m) \) then \( u' \) is a Galois covering.

(4) The torsion subgroup of \( \Gamma(\text{Level}(A, G), G) \) is \( A \).

The proof will follow after a number of lemmas.

Lemma 8.2. \( \text{Hom}_K(K_A, K_B) = \text{Hom}_E(D_A, D_B) = \text{Mon}(A, \Gamma(D_B, G)) \).
Proof. By applying Lemma 2.2 to a sequence of maps

\[ \text{Level}(B, G) \to \text{Level}(A, G) \to X, \]

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 7.3), it is integrally closed in its field of fractions. Thus, the image of \( D_A \) is contained in \( D_B \). It follows that \( \text{Hom}_K(K_A, K_B) = \text{Hom}_E(D_A, D_B) \).

On the other hand, the defining property of \( D_A \) implies that

\[ \text{Hom}_E(D_A, D_B) = \{ \text{level-}A \text{ structures on } G \text{ over } D_B \}. \]

By Proposition 7.6, this is just \( \text{Mon}(A, \Gamma(D_B, G)) \). □

Lemma 8.3. \( \text{Aut}(\Lambda(m)) \) acts transitively on \( \text{Mon}(A, \Lambda(m)) \).

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 monomorphism other than the inclusion. Our task is then to find an automorphism \( \psi \) of \( \Lambda(m) \) extending \( \phi \). 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 \( \phi \) to give a map \( \psi_0: A + A(1) \to \Lambda(m) \leq \Lambda \). As \( \Lambda \) is a divisible group, it is injective, so \( \psi_0 \) 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 \( \psi \) contains no points of order \( p \), so \( \psi \) itself is mono. By counting, \( \psi \) must be iso. Thus \( \psi \in \text{Aut}(\Lambda(m)) \) and \( \psi|_A = \phi \) as required. □

Lemma 8.4. Let \( B \) be a subgroup of \( \Lambda(m) \), and set

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

Then the group of fixed points of \( \Gamma \) 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 \( p^{l-k} \). We can then construct an automorphism \( \alpha \) of \( A = B + C \) by defining \( \alpha(b + c) = b + (1 + p^{k-l})c \) 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 \( \Lambda(m) \) by Lemma 8.3. 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 \( \Lambda(m) \) is the full group of points of order \( p^m \) in \( \Gamma(D_m, G) \), as \( g_m \) can only have \( \deg(g_m) = p^m = |\Lambda(m)| \) roots. It follows using Lemma 8.2 that \( \text{Gal}(K_m/K) = \text{Aut}_K(K_m) = \text{Aut}(\Lambda(m)) \). 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

\[ [K_A : K] = |\text{Hom}_K(K_A, K_m)| = |\text{Mon}(A, \Lambda(m))|. \]

Lemma 8.5. \( \text{Hom}_K(K_A, K_B) = \text{Mon}(A, B) \).

Proof. The extension \( K_m/K \) is Galois as \( K_m/K \) is. Moreover, the subgroup of \( \text{Gal}(K_m/K) \) fixing \( K_B \) is just the group \( \Gamma \leq \text{Aut}(\Lambda(m)) \) of Lemma 8.4. By the fundamental theorem of Galois theory, the fixed field of \( \Gamma \) is just \( K_B \). Thus

\[ \text{Hom}_K(K_A, K_B) = \text{Hom}_K(K_A, K_m)^\Gamma = \text{Mon}(A, \Lambda(m))^\Gamma = \text{Mon}(A, B), \]

the last equality coming from Lemma 8.4. □

Corollary 8.6. The torsion subgroup of \( \Gamma(D_B, G) \) is \( B \).

Proof. This follows easily by comparing Lemma 8.5 with Lemma 8.2 □
Proof of Theorem 8.1. Part (1) follows immediately from lemmas 8.2 and 8.5. It follows that all the maps $u'$: Level($B, G$) → Level($A, G$) are dominant. Both the source and target are smooth by Theorem 7.3, so $u'$ is flat by Lemma 2.1. This gives (2). Now suppose that $B \cong \Lambda(m)$, so without loss of generality $A \cong B = \Lambda(m)$. We have seen above that $K_m/K_A$ is Galois, so Lemma 2.6 tells us that $u'$ is a Galois covering. This gives (3). Finally, (4) is Corollary 8.6. □

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, $\{x(p^{l-1}a_0) \mid 0 < j < p^l, j \neq 0 \mod p\}$. After dividing out the corresponding linear factors, we obtain a Weierstrass polynomial $f(x)$ of degree $p^{nl} - 2p^{n(l-1)} = p^l + p^l - 1$. 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 $|\text{Mon}(A, \Lambda)|$ 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 $G_0$ be a formal group of height $n$ over $X_0 = \text{spec}(\kappa)$. For every $m$, the divisor $p^m[0]$ is a subgroup of $G_0$. We write $G_0(m)$ for the quotient group $G_0/p^m[0]$, and $G(m) → X(m)$ for the universal deformation of $G_0(m) → X_0$. Note that

$$G_0(1) = \text{ker}(p_{G_0}: G_0 → G_0) = p^0[0].$$

It follows that $p_{G_0}$ induces an isomorphism $G_0(m+n) → G_0(m)$. We use this to identify $X(m+n)$ with $X(m)$ and $G(m+n)$ with $G(m)$.

Proposition 9.1. Let $u: A → B$ be an epimorphism of finite Abelian $p$-groups, with $|\text{ker}(u)| = p^l$ say. Then $u$ induces a map

$$u': \text{Level}(A, G(m)) → \text{Level}(B, G(m+l)).$$

Proof. Let $\phi$ be the universal level-$A$ structure on $G(m)$, which is defined over the scheme $Y = \text{Level}(A, G(m))$. Write $K = [\phi \text{ker}(u)]$. This is a subgroup divisor on $G(m)$, whose restriction to the special fibre of $Y$ is $K_0 = p^0[0]$. It follows that $G(m)/K$ is a deformation of $G_0(m+l)$. The composite

$$\text{ker}(u) → A \xrightarrow{\phi} \Gamma(Y, G(m)) → \Gamma(Y, G(m)/K)$$

is clearly zero. This gives a map

$$\psi: B → \Gamma(Y, G(m)/K).$$

I claim that this is a level structure. As $O_Y$ is an integral domain of characteristic zero, it is enough to show that $\psi$ is injective (Proposition 7.6). Suppose $a ∈ B \setminus \text{ker}(u)$, and let $x$ be a coordinate on $G(m)$. In view of Corollary 7.13, we need only check that the following product does not vanish:

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

Because $\phi$ is a level structure, $a - c \neq 0$, and $O_Y$ 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 $\psi$ is classified by a map Level($A, G(m)$) → Level($B, G(m+l)$), which we take to be $u'$.

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

$$0': \text{Level}(A, G(m)) → \text{Level}(0, G(m)) = X(m)$$

$$0: \text{Level}(A, G(m)) → \text{Level}(0, G(m+l)) = X(m+l).$$

The first of these is just the usual projection.

Theorem 9.2.

1. $u'$ is a covariant functor of $u$.
2. $u'$ is a finite flat map.
(3) The maps \(0 \overset{\varphi}{\rightarrow} \Lambda(l) \overset{\alpha}{\rightarrow} 0\) give the same map
\[0^l = 0 : \text{Level}(l, \mathbb{G}(m)) \rightarrow X(m) = X(m + n)\.

(4) Consider a commutative square as follows.

\[
\begin{array}{ccc}
A & \overset{r}{\rightarrow} & B \\
\downarrow{u} & & \downarrow{v} \\
C & \overset{s}{\rightarrow} & D
\end{array}
\]

This is a pullback if and only if it is a pushout. If so, then
\[s^l v^l = u_0 r^l : \text{Level}(B, \mathbb{G}(m)) \rightarrow \text{Level}(C, \mathbb{G}(m + l))\]
(where \(\ker(u) = p^l = \ker(v)\)).

(5) If \(u\) is iso then \(u_0 = (u^{-1})^l\).

(6) If \(A \simeq \Lambda(m)\) then \(u_0\) is a Galois covering, with Galois group \(\Gamma = \{\alpha \in \text{Aut}(A) | u_0 \alpha = u\}\).

(7) The maps \(0_0 : \text{Level}(B, \mathbb{G}(m)) \rightarrow X(m + l)\) and \(0^l : \text{Level}(B, \mathbb{G}(m)) \rightarrow X\) 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 \(0^l : \text{Level}(l, \mathbb{G}) \rightarrow X\) is just the originally given projection, so the group over \(\text{Level}(l, \mathbb{G})\) with which we implicitly start is just \((0^l)^*\mathbb{G}\). We have a universal level structure \(\phi : \Lambda(l) \rightarrow (0^l)^*\mathbb{G}\). By Theorem 7.4, we have \([\phi \Lambda(l)] = \mathbb{G}(l)\). By the definition of the map \(0_0\), we have an isomorphism
\[(0^l)^*\mathbb{G}/\phi(\mathbb{G}(l)) = (0^l)^*\mathbb{G}/[\phi \Lambda(l)] \rightarrow 0^l \mathbb{G}(nl)\]
whose restriction to the special fibre is just the identity map of \(\mathbb{G}_0/p^{nl}[0]\). After using our standard identification of \(\mathbb{G}(nl)\) with \(\mathbb{G}\), we get an isomorphism
\[(0^l)^*\mathbb{G}/\phi(\mathbb{G}(l)) \rightarrow 0^l \mathbb{G}\]
whose restriction to the special fibre is the map
\[p_{\mathbb{G}_0}^l : \mathbb{G}_0/p^{nl}[0] \rightarrow \mathbb{G}_0\].

Because \(\mathbb{G}\) is the universal deformation of \(\mathbb{G}_0\), the map \(0_0\) is uniquely characterised by the existence of such an isomorphism. On the other hand, we have an isomorphism
\[p_{\mathbb{G}}^l : (0^l)^*\mathbb{G}/\phi(\mathbb{G}(l)) \rightarrow (0^l)^*\mathbb{G}\]
which has the same effect on the special fibre. It follows that \(0_0 = 0^l\).

(2) Choose an epimorphism \(v : \Lambda(l) \rightarrow A\) (for some large \(l\)). We thus have a chain of epimorphisms
\[\Lambda(l) \overset{\nu}{\rightarrow} A \overset{\alpha}{\rightarrow} B \overset{0}{\rightarrow} 0\].

This gives maps as follows, where the \(s\)'s refer to various integers:
\[
\text{Level}(l, \mathbb{G}(\ast)) \overset{\nu}{\rightarrow} \text{Level}(A, \mathbb{G}(\ast)) \overset{\alpha}{\rightarrow} \text{Level}(B, \mathbb{G}(\ast)) \overset{0_0}{\rightarrow} X(\ast).
\]

By (3), we know that the full composite \(0_0 u v\) is finite and dominant. All the schemes involved are smooth (and thus integral) and have dimension \(n\). Applying Lemma 2.2 twice, we see that \(u_0\) is finite and dominant. It is therefore flat, by Lemma 2.1.

(4) Consider the following sequence
\[A \overset{\nu}{\rightarrow} B \oplus C \overset{v - s}{\rightarrow} D\]

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 pullback, if and only if the square is a pullback. If so, we write \(E = \ker(u)\) and...
observe that \( r: E \simeq \ker(v) \). Write \( Y = \text{Level}(B, G) \), so we have a level structure \( \phi: B \to \Gamma(Y, G) \).

We define maps \( \psi \) and \( \chi \) by requiring that the following diagrams commute:

\[
\begin{array}{ccc}
A & \xrightarrow{r} & B \\
\downarrow{u} & & \downarrow{v} \\
C & \xrightarrow{s} & D \\
\end{array}
\]

\[
\begin{array}{ccc}
\Gamma(Y, G) \\
\downarrow{\phi} \\
\Gamma(Y, G/\phi r E) \\
\end{array}
\]

\[
\begin{array}{ccc}
\Gamma(Y, G) \\
\downarrow{\psi} \\
\Gamma(Y, G/\phi r E) \\
\end{array}
\]

The two maps \( ur\psi \) and \( s\chi \) from \( Y \) to \( \text{Level}(C, G(l)) \) classify the two level structures \( \chi \) and \( \psi \circ s \) on \( G/[\phi r E] \). 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 8.1, we know that the composite \( \text{Level}(A, G) \xrightarrow{u} \text{Level}(B, G(l)) \xrightarrow{0_l} X(nm) \) is a Galois covering. Using Lemma 2.6 to reduce to the case of field extensions, we see that \( u_l \) is Galois. Referring again to Theorem 8.1, we see that the Galois group is

\[ \Gamma = \{ \alpha \in \text{Aut}(A) \mid u_l \alpha = u_l \} \].

Using (5) and the fact that level structures over integral domains in characteristic zero are injective, we conclude that

\[ \Gamma = \{ \alpha \in \text{Aut}(A) \mid u = u \alpha \} \].

(7) Choose an epimorphism \( u: A = \Lambda(l) \to B \), and let \( \Gamma \) be as above. By the Pontrjagin dual of Lemma 8.3, we see that

\[ \deg(0_l) = |\text{Aut}(A)/\Gamma| = |\text{Mon}(A^*, \Lambda(l)^*)| = |\text{Epi}(\Lambda(l), A)| \]

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

\[ \deg(0_l) = |\text{Mon}(A, \Lambda(l))| = |\text{Mon}(A, \Lambda)| \].

By Theorem 8.1, this is the same as the degree of \( \deg(0_l) \).

\[ \square \]

10. Classification of Subgroups

We now fix \( m \geq 0 \) and study the classification of subgroups of \( G \) of degree \( p^m \).

**Theorem 10.1.** The functor from schemes over \( X \) to sets given by

\[ Y \mapsto \{ \text{subgroups of } G \times_X Y \text{ of degree } p^m \} \]

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

\[ X' \times_X \text{Sub}_m(G) = \text{Sub}_m(X' \times_X G) \].

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

\[ d = |\text{Sub}_m(A)| = \text{number of subgroups of } A \text{ of order } p^m \].

Formulae for \( d \) will be given later. The scheme \( \text{Sub}_m(G) \) is Gorenstein.
The rest of this section will constitute the proof. In Subsection 10.1, we construct $\operatorname{Sub}_m(G)$ and show that it behaves well under pullback (cf. [9, Corollary 1.3.7]). In Subsection 10.2, we prove some combinatorial formulae. In 10.3, 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 $\operatorname{Sub}_m(G) \to X$. In 10.4, we analyse what happens when we invert $p$ and thus make all finite subgroups étale (cf. [9, Corollary 3.7.2]). In 10.5, we assemble these results to prove the theorem, except for the fact that $\operatorname{Sub}_m(G)$ is Gorenstein, which is proved in 10.6.

10.1. Construction of $\operatorname{Sub}_m(G)$. Let $D$ be the universal divisor defined over $Y = \operatorname{Div}_{p^m}(G)$, with equation $f_D(x) = \sum_{k=0}^{m} c_k x^k$. There are unique elements $a_{ij} \in \mathcal{O}_Y$ such that

$$f(x + fy) = \sum_{i,j=0}^{p^m-1} a_{ij} x^i y^j \pmod{f(x), f(y)}$$

Define $E' = \mathcal{O}_Y/(c_0, a_{ij} \ | \ 0 \leq i, j < p^n)$ and $\operatorname{Sub}_m(G) = \operatorname{spf}(E')$.

If $Z$ is a scheme over $X$ and $K$ is a divisor of degree $p^m$ on $G$ over $Z$, then $K$ is classified by a map $f: Z \to Y = \operatorname{Div}_{p^m}(G)$. It is easy to see that this factors (uniquely) through $\operatorname{Sub}_m(G)$ iff $K$ is a subgroup scheme. Thus, $\operatorname{Sub}_m(G)$ represents the functor

$$Z \mapsto \{ \text{subgroups of } G \times_X Z \text{ of degree } p^m \}$$

as required. One can see from this construction that $X' \times_X \operatorname{Sub}_m(G) = \operatorname{Sub}_m(X' \times_X G)$.

10.2. Combinatorics. We write $\Lambda^* = \operatorname{Hom}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p) = \mathbb{Z}_p^n$. Note that $d(m, n)$ is also the number of lattices $L$ of index $p^m$ in $\Lambda^*$. 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 $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ we write

$$|\alpha| = \sum_j \alpha_j$$

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

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

Lemma 10.2. 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.

$$\begin{pmatrix} p^{a_0} & 0 & 0 & 0 \\ a_{01} & p^{a_1} & 0 & 0 \\ a_{02} & a_{12} & p^{a_2} & 0 \\ a_{03} & a_{13} & a_{23} & p^{a_3} \end{pmatrix} \quad 0 \leq a_{kl} < p^{a_l}$$

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 $p^{a_0}$ 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 $\alpha_0$ is the minimal valuation of $b_k$ among vectors of the form $(0, \ldots, 0, b_k, \ldots, b_{n-1})$ in the lattice $L = M, \Lambda^*$. Moreover, the $(k + 1)$'th column above is the unique such vector with $b_k = p^{a_k}$ and $0 \leq b_l < p^{a_l}$ for $l > k$. This gives uniqueness. It is not hard to see that the vectors $b$ with $0 \leq b_k < p^{a_k}$ form a transversal for $L$ in $\Lambda^*$, so that $|\Lambda^*/L| = p^{|\alpha|}$. \hfill $\square$
**Corollary 10.3.** If \( \alpha \) runs over sequences \((\alpha_1, \ldots, \alpha_{n-1})\) with \(|\alpha| \leq m\) then
\[
d(m, n) = \sum_{\alpha} p^{||\alpha||}.
\]

It follows that
\[
Z_n(t) = \sum_m d(m, n)t^m = \prod_{k=0}^{n-1} \frac{1}{1 - p^{kt}}.
\]

**Proof.** The first statement follows by counting the possible matrices in the lemma in the obvious way. Next, write
\[
(1 - p^{kt})^{-1} = \sum_{\alpha_k \geq 0} p^{k\alpha_k} t^{\alpha_k}.
\]
The second claim follows by expanding out the product. \(\square\)

We can also give a somewhat more explicit formula for \(d(m, n)\). First, we recall the definition of the Gaussian binomial coefficients:
\[
\left[ \begin{array}{c} k \\ l \end{array} \right]_p = \prod_{m=0}^{l-1} \frac{p^k - p^m}{p^l - p^m} = \prod_{m=1}^{l} \frac{p^{k-1+m} - 1}{p^m - 1}.
\]
This can also be interpreted as the number of \(l\)-dimensional subspaces of a \(k\)-dimensional vector space over \(F_p\).

**Lemma 10.4.** The Gaussian binomial coefficients satisfy
\[
\left[ \begin{array}{c} k \\ l \end{array} \right]_p = \left[ \begin{array}{c} k \\ k-l \end{array} \right]_p
\]
and
\[
\left[ \begin{array}{c} k \\ l \end{array} \right]_p = \left[ \begin{array}{c} k-1 \\ l-1 \end{array} \right]_p + p^l \left[ \begin{array}{c} k-1 \\ l \end{array} \right]_p.
\]

**Proof.** Suppose \(\dim_{F_p} V = k\). There is an obvious bijection \(W \mapsto \text{ann}(W)\) 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 \(W \leq V\) 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 \(\left[ \begin{array}{c} k-1 \\ l-1 \end{array} \right]_p\) 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 \(W'' \leq U\); this occurs \(p^l \left[ \begin{array}{c} k-1 \\ l \end{array} \right]_p\) times. The second claim follows. \(\square\)

**Lemma 10.5.** \(d(m, n) = \left[ \begin{array}{c} n+m-1 \\ n-1 \end{array} \right]_p\).

**Proof.** We know that
\[
Z_n(t) = \sum_m d(m, n)t^m = \prod_{k=0}^{n-1} \frac{1}{1 - p^{kt}}.
\]
We want to show that this is the same as
\[
W_n(t) = \sum_m \left[ \begin{array}{c} n+m-1 \\ n-1 \end{array} \right]_p t^m.
\]
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
\[
\left[ \begin{array}{c} m+n-1 \\ n-1 \end{array} \right]_p = p^{n-1} \left[ \begin{array}{c} m+n-2 \\ n-1 \end{array} \right]_p = \left[ \begin{array}{c} m+n-2 \\ n-2 \end{array} \right]_p,
\]
which follows in turn from Lemma 10.4. \(\square\)
We shall need another auxiliary numerical function. Fix $m$ and $n$. For $0 \leq l \leq n$ and $0 \leq k$ we define
\[
e(k,l) = \sum_{\alpha} p^{l|\alpha|} \quad \text{where} \quad \alpha = (\alpha_1, \ldots, \alpha_{n-1}) \text{ and } k + |\alpha| \leq m.
\]

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

**Lemma 10.6.** $e(k,l)$ is the unique function with the properties
\[
\begin{align*}
e(k,n) &= 1 & & \text{if } k \leq m \\
e(k,l) &= 0 & & \text{if } k > m \\
e(k,l) &= e(k,l+1) + p^l e(k+1,l) & & \text{if } l < n.
\end{align*}
\]

**Proof.** It is clear that $e(k,l)$ has the first two properties. For the third, recall that
\[
e(k,l) = \sum \{ p^{l|\alpha|} | \alpha = (\alpha_1, \ldots, \alpha_{n-1}) \text{ and } k + |\alpha| \leq m \}.
\]

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
\[
\sum \{ p^l p^{\|\beta\|} | \beta = (\beta_1, \ldots, \beta_{n-1}) \text{ and } k + 1 + |\beta| \leq m \}.
\]

This is just $p^l e(k+1,l)$. It is easy to see that these properties characterise $e$ uniquely. \hfill \Box

### 10.3. Infinitesimal Theory

In this section, we study the scheme $\text{Sub}_m(G_0)$ (which is the same as $X_0 \times_X \text{Sub}_m(G)$). 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 10.7.** Let $B$ be a finite-dimensional $k$-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
\[
\dim_k B \leq \sum_i n_i \dim_k B/b_i.
\]

**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
\[
\dim_k B \leq n_0 \dim_k B/b_0 + \dim_k B / b'.
\]

By induction on $m$, we find that
\[
\dim_k B / b' \leq \sum_{i > 0} n_i \dim_k B / (b', b_i) = \sum_{i > 0} n_i \dim_k B / b_i.
\]

The claim follows. \hfill \Box

**Proposition 10.8.** $\deg [\text{Sub}_m(G) \to X] \leq d(m,n)$.

**Proof.** Write $Y = \text{Sub}_m(G_0)$ and $E' = \mathcal{O}_Y$ and $\mathbb{H} = G \times_X Y$. Note that $\mathbb{H}$ has strict height $n$. We have a universal subgroup $K < \mathbb{H}$ of degree $p^m$ and a quotient map $q: \mathbb{H} \to \mathbb{H}/K$. 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
\[
E'(k,l) = \mathcal{O}_{Y(k,l)}
\]
\[
e'(k,l) = \dim_k E'(k,l).
\]

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

Next, recall that $Y = \text{Sub}_m(G_0)$ is a closed subscheme of $\text{Div}_p^m(G_0)$. 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 $m_Y$, 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 $e'(m,l) \leq 1$. 

18
Next, I claim that $\epsilon'(k,l) \leq \epsilon'(k,l+1) + p^i \epsilon'(k+1,l)$ 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
\[
p^{\epsilon'}_{k,l} x = ux^{\epsilon'} + \ldots \\
p^{\epsilon'}_{k,l} y = vy^{\epsilon'} + \ldots \\
q^i y = ax^{\epsilon'} + \ldots
\]
Note that $E'(k,l)/a = E'(k+1,l)$ and $E'(k,l)/v = E'(k,l+1)$. The relation $p^{\epsilon'}_{K} \circ q = q \circ p^{\epsilon'}_{K}$ gives
\[
va^{\epsilon'}x^{p^{\epsilon'} + i} + \ldots = au^{\epsilon'}x^{p^{\epsilon'} + n} + \ldots.
\]
Because we assume that $l < n$, we find that $va^{\epsilon'} = 0$. The claim now follows from Lemma 10.7.

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 $va^{\epsilon'} = au^{\epsilon'}$, so that
\[
a(1 - vu^{-1}a^{p^{\epsilon'} - 1}) = 0.
\]
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 $\epsilon'(k,n) = \epsilon'(m,n) \leq 1$.

From the above and Lemma 10.6 we see that $\epsilon'(k,l) \leq \epsilon(k,l)$. In particular, $\text{dim}(E') = \epsilon'(0,1) \leq (0,1) = d(m,n)$ as claimed. □

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

**Proposition 10.9.** The resulting map
\[
\mathcal{O}_{\text{Sub}_m(G)}[\frac{1}{p}] \to F(\text{Sub}_m(\Lambda), \mathcal{O}_X[\frac{1}{p}])
\]
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 7.4 that $[\phi \Lambda(m)] = G(m)$, and hence that
\[
(p_G^m)^*x \sim \prod_{a \in \Lambda(m)} (x - x_a).
\]
On the other hand, for any formal group we have $(p_G^m)^*x = p^m x \pmod{x^2}$. 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 4.3 that
\[
\Delta \sim \prod_{a \neq b} (x_a - x_b) \sim \left( \prod_{a \neq 0} x_a \right)^N \sim p^{mn}.\]
In particular, $\Delta$ becomes invertible when we invert $p$.

Now write $E' = \mathcal{O}_{\text{Sub}_m(G)}$, and $p_A = \text{ker}(\alpha_A) \subseteq E'$. Note that $E'/p_A = \mathcal{O}_X$.

**Lemma 10.10.** If $A \neq B$ then $p$ is nilpotent mod $p_A + p_B$. 

19
Proof. We may suppose that there exists $a \in A \setminus B$. Modulo $p_B$ we have $f_K(x) = \prod_{b \in B}(x - x_b)$, and modulo $p_A$ we have $f_K(x_a) = 0$. Thus, using Lemma 4.3 we get

$$0 = f_K(x_a) = \prod_{b \in B}(x_a - x_b) \sim \prod_b x_{a-b} \pmod{p_A + p_B}.$$ 

Each term in the product $\prod_{b \in B}(x_a - x_b)$ divides $\Delta$ and thus divides a power of $p$. Thus $p$ is nilpotent mod $p_A + p_B$ as claimed. \hfill \Box

**Lemma 10.11.** If $p$ is a prime ideal in $E'$ and $p \not\subset p$ then $p \geq p_A$ for some $A$.

**Proof.** We know that $K \leq G(m)$, so $f_K(x)$ divides $f_G(x) = \prod_{a \in A}(x - x_a)$. Now work over the integral domain $E'/p$. We know that the discriminant of $f_G$ 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 $A \subseteq A(m)$. As $K$ is a subgroup scheme of $G$, it must be invariant under translation by any of its points. From this, it follows easily that $A$ is a subgroup of $A(m)$, and that $p \geq p_A$. \hfill \Box

**Proof of Proposition 10.9.** The last two lemmas show that $p_A[\frac{1}{p}] + p_B[\frac{1}{p}] = E'[\frac{1}{p}]$ and

$$\bigcap_A p_A[\frac{1}{p}] = \bigcap_{p \in \text{spec } E'[\frac{1}{p}]} p = \sqrt{0}.$$ 

The proposition follows by the Chinese remainder theorem. \hfill \Box

**Corollary 10.12.** The map $\text{Sub}_m(G) \to X$ is flat, with degree $d(m, n)$.

**Proof.** Write $E = O_X$ and $d = d(m, n)$. By Proposition 10.8 we know that there is an $E$-linear epimorphism $E^d \to E'$. It follows that the induced map

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

is epi. By Proposition 10.9, 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 $0 = \sqrt{0} \triangleleft E'$).

$$\begin{array}{ccc}
E^d & \xrightarrow{f} & E' \\
\downarrow & & \downarrow \\
E[\frac{1}{p}]^d & \xrightarrow{f'} & E'[\frac{1}{p}] / \sqrt{0} \cong E[\frac{1}{p}]^d
\end{array}$$

\hfill \Box

**10.5. General Theory.** We can now prove Theorem 10.1, except for the Gorenstein property, which is treated in the next subsection. Let $G$ be a formal group of height $n$ over an arbitrary connected base $X$. Let $G'/X'$ be the universal deformation of $G_0/X_0$, and let $G''$ be the pullback of $G'$ to $\text{Level}(m, G')$. We can apply Corollary 10.12 to conclude that the projection

$$\text{Sub}_m(G'') = \text{Level}(m, G') \times_X \text{Sub}_m(G') \to \text{Level}(m, G')$$

is flat, with degree $d(m, n)$. As $\text{Level}(m, G') \to X'$ is faithfully flat, it is not hard to conclude that $\text{Sub}_m(G') \to X'$ is also flat, with degree $d(m, n)$. As $\text{Sub}_m(G) = X \times_X \text{Sub}_m(G')$, we see that $\text{Sub}_m(G) \to X$ is again flat, with the required degree.
10.6. The Gorenstein property. We next show that the scheme \( \text{Sub}_{m}(G) \) is Gorenstein (I do not know whether it is a complete intersection). We first recall the definition and basic facts about Gorenstein rings.

**Definition 10.13.** A Noetherian local ring \( R \) is Gorenstein if the \( R \)-module \( R \) admits a finite resolution by injective \( R \)-modules.

**Proposition 10.14.**

(a) Let \( R \) be a Noetherian local ring, and \((x_1, \ldots, x_m)\) a regular sequence in \( R \) generating an ideal \( I \leq m \). 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 \( \text{soc}(R) = \{a \in R \mid am = 0\} \) has dimension one over \( \kappa = R/m \).

**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 10.8. We write \( Y \) for the scheme \( \text{Sub}_{m}(G_0) \) and put \( \mathbb{H} = G \times_X Y \). We have a universal subgroup \( K < \mathbb{H} \) of degree \( p^m \) and a quotient map \( q: \mathbb{H} \to \mathbb{H}/K \). 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 \( q^*y = ax \) (mod \( x^2 \)). 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 \( f_K(x) = a'x \) (mod \( x^2 \)) for some \( a' \in \mathcal{O}_Y \), which is a unit multiple of \( a \).

**Proposition 10.15.** The ring \( \mathcal{O}_{\text{Sub}_{m}(G)} \) is Gorenstein. The socle of the quotient ring \( \mathcal{O}_{\text{Sub}_{m}(G_0)} \) is generated by the element \( a \uparrow (p + \ldots + p^{n-1}) \) (where \( a \uparrow N \) means \( a^N \)). It is also generated by \( a' \uparrow (p + \ldots + p^{n-1}) \).

**Proof.** First, recall that \( \mathcal{O}_{\text{Sub}_{m}(G_0)} = \kappa \otimes_X \mathcal{O}_{\text{Sub}_{m}(G)} \), which is obtained from \( \mathcal{O}_{\text{Sub}_{m}(G)} \) by killing the sequence \((u_0, \ldots, u_{n-1})\). This sequence is regular (because \( \text{Sub}_{m}(G) \to X \) is flat). Thus, by part (a) of Proposition 10.14, it is enough to show that \( \mathcal{O}_{\text{Sub}_{m}(G_0)} \) is Gorenstein. Moreover, by part (c) of Proposition 10.14, it is enough to show that the socle is generated by \( a \uparrow (p + \ldots + p^{n-1}) \).

To do this, we reuse the notation and ideas of the proof of Proposition 10.8. It was shown there that

\[
\epsilon'(k,l) \leq \epsilon'(k,l + 1) + p^l \epsilon'(k + 1,l) \quad (l < n).
\]

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 10.1 implies that \( \epsilon(0,1) = d(m,n) = \epsilon'(0,1) \). 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 \( va^l = 0 \), with \( E'(0,l)/a = E'(1,l) \) and \( E'(0,l)/va = E'(0,l+1) \). 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 10.16 below, we find that multiplication by \( a^l \) gives an isomorphism \( \text{soc}(E'(0,l+1)) \cong \text{soc}(E'(0,l)) \). It follows that multiplication by \( b = a \uparrow (p + \ldots + p^{n-1}) \) gives an isomorphism \( \text{soc}(E'(0,n)) \cong \text{soc}(E'(0,1)) \). As \( \epsilon'(0,n) = \epsilon(0,n) = 1 \), we see that \( E'(0,n) = \kappa \) and thus that \( \text{soc}(E'(0,n)) = \kappa \). Moreover, \( E'(0,1) = \mathcal{O}_{\text{Sub}_{m}(G_0)} \). It follows that \( \text{soc}(\mathcal{O}_{\text{Sub}_{m}(G_0)}) \) is generated by \( b \), as claimed. The last statement of the proposition is trivial.

We still owe the reader the following lemma.

**Lemma 10.16.** Let \( R \) be a finite-dimensional local algebra over a field \( \kappa \), with maximal ideal \( m \). Suppose that \( v, a \in m \) 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 \( R/v \to R \), whose image is the annihilator of \( v \). Moreover, this map induces an isomorphism \( \text{soc}(R/v) \cong \text{soc}(R) \).

**Proof.** As in the proof of Lemma 10.7, 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 \( R/v \to R \).

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

\[
J \to R \xrightarrow{v} Rv, \\
Rv \to R \to R/v
\]

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

It is immediate that \( a^k \text{soc}(R/v) \leq \text{soc}(R) \). Conversely, suppose that \( x \in \text{soc}(R) \). 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 \( x \in \text{soc}(R) \). As multiplication by \( a^k \) is a monomorphism, we see that \( yz = 0 \) in \( R/v \). Thus \( y \in \text{soc}(R/v) \). This means that \( a^k \) gives an isomorphism \( \text{soc}(R/v) \simeq \text{soc}(R) \), as claimed. \( \Box \)

11. Flags

Consider a sequence \( \lambda = (\lambda_0 = 0 < \lambda_1 < \ldots < \lambda_m = n) \). A flag of type \( \lambda \) on \( \mathbb{G} \) will mean a sequence of subgroup divisors \( 0 = K_0 < K_1 < \ldots < K_m = \mathbb{G}(1) \) such that \( K_k \) has degree \( p^{\lambda_k} \). Using Proposition 4.6 and Theorem 10.1, 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 \( \text{Flag}(\lambda, \mathbb{G}) \) over \( X \). This is in fact a closed subscheme of \( \prod_k \text{Sub}_{\lambda_k}(\mathbb{G}) \) and thus is finite over \( X \).

Similarly, we let \( \text{Flag}(\lambda, \Lambda) \) be the set of sequences \( 0 = A_0 < A_1 < \ldots < A_m = \Lambda(1) \) such that \( |A_k| = p^{\lambda_k} \). Let \( a_0, \ldots, a_{n-1} \) be the standard basis of \( \Lambda(1) = (\mathbb{Z}/p)^n \). Write \( \Lambda_k = \langle a_i \mid i < \lambda_k \rangle \), so that \( \Lambda = (\Lambda_0, \ldots, \Lambda_m) \in \text{Flag}(\lambda, \Lambda) \). Write \( \Gamma = \text{Aut}(\Lambda(1)) \) and let \( \Gamma(\lambda) \) be the subgroup which preserves \( \Lambda \). Clearly \( \text{Flag}(\lambda, \Lambda) \simeq \Gamma/\Gamma(\lambda) \).

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

**Theorem 11.1.** The maps

\[
\text{Level}(1, \mathbb{G}) \to \text{Flag}(\lambda, \mathbb{G}) \to X
\]

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

We will prove this theorem at the end of this section.

First, observe that whenever we have a flag of type \( \lambda \) we have isogenies

\[
\mathbb{G} = \mathbb{G}/K_0 \xrightarrow{q_1} \mathbb{G}/K_1 \xrightarrow{q_2} \ldots \xrightarrow{q_{m-1}} \mathbb{G}/K_{m-1} \xrightarrow{q_m} \mathbb{G}.
\]

At the last stage, we have identified \( \mathbb{G}/K_m = \mathbb{G}/\mathbb{G}(1) \) with \( \mathbb{G} \) via the isomorphism \( p_G: \mathbb{G}/\mathbb{G}(1) \simeq \mathbb{G} \). With this convention, we have

\[
q_m \circ q_{m-1} \circ \cdots \circ q_1 = p_G: \mathbb{G} \to \mathbb{G}.
\]

Moreover, \( q_k \) has height \( \lambda_k - \lambda_{k-1} \).

11.1. Combinatorics. Consider a sequence \( \mu = (0 = \mu_0 \leq \mu_1 \leq \ldots \leq \mu_m \leq n) \). Choose linearly independent subspaces \( N_k \leq \Lambda(1) \) 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 11.2.** \( d(\mu) \) is the number of flags of type \( \lambda \) such that \( A_k \cap M_m = M_k \) for \( 0 \leq k \leq m \). This is clearly independent of the choices made. Note that \( d(0, \ldots, 0) = |\text{Flag}(\lambda, \Lambda)| \), that \( d(\mu) = 0 \) unless \( \mu_{k+1} - \mu_k \leq \lambda_{k+1} - \lambda_k \) for \( 0 \leq k < m \), and that \( d(\mu) = 1 \) if \( \mu_k = \lambda_k \) for \( 0 \leq k < m \).

**Definition 11.3.** If \( \mu_m < n \) and \( 0 < k \leq m \) write \( \theta_k \mu = (\mu_0, \ldots, \mu_{k-1}, \mu_k + 1, \ldots, \mu_m + 1) \).

**Lemma 11.4.** If \( \mu_m < n \) then

\[
d(\mu) = \sum_{k=1}^{m} p^{\mu_{m-k} - \mu_k} d(\theta_k \mu).
\]
Proof. Choose $L \leq \Lambda(1)$ with $\dim \frac{G}{K_0} = 1$ and $L \cap M_m = 0$. Let $A$ be a flag of type $\lambda$ 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 $\pi_m$ is epi. Let $k$ be the least value of $j$ for which $\pi_j$ is epi (or equivalently, nonzero). For $j < k$ we have $A_j \cap (M_m \oplus L) = M_j$. For $j \geq k$, there is a unique map $f_j : L \to M'_j$ such that

$$A_j \cap (M_m \oplus L) = A_j \cap (M_j \oplus M'_j \oplus L) = M_j \oplus \text{graph}(f_j).$$

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 $f_k \in \text{Hom}(L, M'_k)$. 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 $|\text{Hom}(L, M'_k)| d(\theta_{k\mu}) = p^{\mu_k - \mu_k} d(\theta_{k\mu})$. The claim follows.

11.2. **Infinite Theory.** We next study the scheme $Y = X_0 \times_X \text{Flag}(\lambda, G)$. Consider a sequence $\mu$ 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 $e(0, \ldots, 0) = \dim_\kappa A$. Recall that we have isogenies

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

with

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

**Proposition 11.5.** $\deg [\text{Flag}(\lambda, G) \to X] = \dim_\kappa A = |\text{Flag}(\lambda, \Lambda)|$.

**Proof.** Note that

$$e(0, \ldots, 0) = \dim_\kappa A = \deg [\text{Flag}(\lambda, G) \to X],$$

and that

$$d(0, \ldots, 0) = |\text{Flag}(\lambda, \Lambda)|,$$

so it is enough to prove that $e(\mu) \leq d(\mu)$ for all $\mu$. 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 $\kappa$ by the parameters of the divisors $K_k$, so this implies that $\kappa \to A(\mu)$ is epi and $\kappa(\mu) \leq 1$. 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 $\mathcal{G}/K_k$. 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, $q_1^* \cdots q_m^* x_m = p_G^m x_0$, and this is divisible by $x_0^p$ (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 10.7 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. \hfill \square

11.3. **Galois Theory.** In this subsection we assume that \( G \) is the universal deformation of \( G_0 \). As mentioned earlier, there is a map \( \text{Level}(1, G) \to \text{Flag}(\lambda, G) \), classifying the flag \([\phi \Lambda_0] < \ldots < [\phi \Lambda_m]; \) these clearly factors through \( \text{Level}(1, G)/\Gamma(\lambda) \).

Given a subset \( S \subseteq \Lambda(1) \), we have a divisor \([\phi S] = \sum_{a \in S} [\phi(a)] \) on \( G \) over \( \text{Level}(1, G) \). Suppose we have epimorphisms \( \text{Level}(1, G) \to Y \to X \) 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 \( \mathcal{O}_Y[t] \leq \mathcal{O}_{\text{Level}(1, G)}[t] \).

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

1. If \( D_0 \) and \( D_1 \) are defined over \( Y \) then so is \( D_0 + D_1 \).
2. If \( D_0 \) and \( D_0 + D_1 \) are defined over \( Y \) then so is \( D_1 \).
3. If the point \( a \) and the divisor \( D \) are defined over \( Y \) then so is the translate \( T_a D \).

**Lemma 11.6.** Suppose we have epimorphisms \( \text{Level}(1, G) \to Y \to Y' \to X \). 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 \( \deg(a) \leq |S| \).

**Proof.** Consider the polynomial \( f(t) = \prod_{a \in S} (t - x_a) \in \mathcal{O}_Y[t] \), which is monic and has degree \( |S| \). It follows that \( f(x_a) = 0 \) 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 11.7.** Geometrically, this means that \( Y \) embeds as a closed subscheme of the divisor \([\phi S]\) over \( Y' \).

**Proposition 11.8.** \( \deg(\text{Level}(1, G) \to \text{Flag}(\lambda, G)) \leq |\Gamma(\lambda)| \).

**Proof.** We again write \( \{a_0, \ldots, a_{m-1}\} \) for the standard basis of \( \Lambda(1) \), so that \( \Lambda_k = \langle a_i \mid i < \lambda_k \rangle \). 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
\[ \Gamma_k a_k = \Lambda_{j+1} \setminus \langle a_i \mid i < k \rangle. \]

Write
\[ Y_0 = \text{spf}(C_0) = \text{image}(\text{Level}(1, G)/\Gamma(\lambda) \to \text{Flag}(\lambda, G)) \]
\[ x_k = x(\phi(a_k)) \in D_1 = \mathcal{O}_{\text{Level}(1, G)} \]
\[ C_k = C_0[x_j \mid j < k] \leq D_1 \]
\[ Y_k = \text{spf}(C_k). \]

We thus have maps
\[ \text{Level}(1, G) = Y_0 \to Y_{n-1} \to \ldots \to Y_0 \to \text{Flag}(\lambda, G), \]
the last of which is a closed embedding.

The map \( \text{Level}(1, G) \to \text{Flag}(\lambda, G) \) is defined so that the pullback of the divisor \( K_k \) is precisely \( [\phi \Lambda_k] \). It follows that \( \Lambda_k \) is defined over \( Y_0 \) for all \( k \).

The point \( a_k \) of \( G \) 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 11.6, we see that \( \deg(Y_{k+1} \to Y_k) \leq |\Gamma_k/\Gamma_{k+1}| \). It follows that
\[ \deg(\text{Level}(1, G) \to \text{Flag}(\lambda, G)) \leq \prod_k |\Gamma_k/\Gamma_{k+1}| = |\Gamma(\lambda)|. \]

\( \square \)
Proof of Theorem 11.1. We may assume that $G$ is the universal deformation of $G_0$. Write $a = |\Gamma(\lambda)|$ and $b = |\Flag(\lambda, \Lambda)|$, and note that $ab = |\Gamma|$. Consider the maps

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

By propositions 11.5 and 11.8 we know that $\deg(h) \leq b$ and $\deg(gf) \leq a$; by Theorem 7.3 we know that $gfh$ is flat of degree $ab$; and it is clear that $\deg(gfh) \leq \deg(gf) \deg(h)$. It follows that $\deg(gfh) = a$ and $\deg(h) = b$. Lemma 2.7 now tells us that $\Flag(\lambda, G)$ is smooth, $f$ is Galois and $g$ is iso. Finally, lemmas 2.2 and 2.1 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

$$\text{Type}(A, \Lambda) = \{ \text{subgroups of } \Lambda \text{ isomorphic to } A \} \cong \text{Mon}(A, \Lambda)/\text{Aut}(A) \subseteq \text{Sub}_m(\Lambda).$$

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

**Remark 12.1.** This description is somewhat misleading, because it suggests that $\text{Type}(A, G)$ should be a subscheme of $\text{Sub}_m(G)$. There is a natural map

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

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 12.5 below, and the example at the end of Section 16. It would be interesting to have a compelling moduli interpretation of $\text{Type}(A, G)$, but I cannot at present offer one.

**Definition 12.2.** If $G$ is the universal deformation of $G_0$, then we take

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

In the general case, we let $H/Y$ be the universal deformation of $G_0/X_0$ and take

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

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

**Theorem 12.3.** The maps

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

are flat, of degree $|\text{Aut}(A)|$ and $|\text{Type}(A, A)|$ respectively. If $G$ is the universal deformation of $G_0$ then $\text{Type}(A, G)$ is smooth. □

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

**Theorem 12.4.** Let $f$ be the evident map

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

Suppose that $G$ is the universal deformation of $G_0$. Then the induced map $f^*$ of rings is injective, and becomes iso after inverting $p$. □

**Theorem 12.5.** Suppose that $A$ has the form $\mathbb{Z}/p^{m+l} \oplus (\mathbb{Z}/p^l)^{n-1}$. Then

$$\text{Type}(A, G) \to \text{Sub}_{m+n}(G)$$

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

\[
U_k(A) = \{ a \in A(k) \mid p^{k-1}a \in p^kA \}
\]

\[
T_k(A) = A(k)/U_k(A)
\]

\[
S_k(A) = A(k) \setminus U_k(A).
\]

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

\[
A \simeq \bigoplus_{k \geq 0} \left( \mathbb{Z}/p^k \right)^{m_k}
\]

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:

\[
(i, j) < (k, l) \text{ if } i > k \text{ or } (i = k \text{ and } j < l).
\]

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

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

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

and

\[
S(k, l) = A(k) \setminus V(k, l)
\]

so

\[
S(k, 0) = S(k).
\]

We also write

\[
\Gamma = \text{Aut}(A)
\]

and

\[
\Gamma(k, l) = \{ \alpha \in \Gamma \mid \alpha(a_{ij}) = a_{ij} \text{ if } (i, j) < (k, l) \}
\]

so

\[
\Gamma(k, m_k) = \Gamma(k - 1, 0)
\]

and

\[
\Gamma(k, l)/\Gamma(k, l + 1) \simeq \Gamma(k, l)a_{kl}.
\]

**Lemma 12.6.** $\Gamma(k, l)a_{kl} = S(k, l)$ 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

\[
A' = \left( \mathbb{Z}/p^k \right)^{m_k}
\]

\[
A'' = \bigoplus_{l \neq k} \left( \mathbb{Z}/p^l \right)^{m_l}.
\]

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 $\alpha_0$ 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 $\alpha_1$ of $A'$ with $\alpha_1(a_{kj}) = a_{kj}$ for $j < l$ and $\alpha_1(a_{kl}) = b'$. Finally, we define an endomorphism $\alpha$ of $A = A' \oplus A''$, with components as follows:

\[
\begin{align*}
A' &\rightarrow A' & \alpha_1 \\
A' &\rightarrow A'' & a_{kl} \mapsto b'' \\
A'' &\rightarrow A' & 0 \\
A'' &\rightarrow A'' & \text{identity}
\end{align*}
\]

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

$$\Gamma(k,l)a_{kl} = S(k,l).$$

\[\square\]

Remark 12.7. It is neither hard nor apparently helpful to write explicit formulae for $|S(k,l)|$ and $|\Gamma|$.

We assume until further notice that $G$ is the universal deformation of $G_0$. As in Subsection 11.3, we shall say that a subset $S \subseteq A$ is defined over a quotient scheme $Y$ of Level$(A, G)$ if there is a divisor $D$ on $G$ over $Y$ whose pullback is $[\phi S]$.

Proof of Theorem 12.3. We now write $D_A = \mathcal{O}_{\text{Level}(A,G)}$ and $C = D_A^G = \mathcal{O}_{\text{Type}(A,G)}$. Define

$$x_{ij} = x(\phi(a_{ij})),\
C(k,l) = C[x_{ij} | (i,j) < (k,l)] \leq D_A\
Y(k,l) = \text{spf}(C(k,l)).$$

Note that $Y(k, m_k) = Y(k-1,0)$ and that we have maps

$$\text{Level}(A, G) \rightarrow Y(k, l+1) \rightarrow Y(k, l) \rightarrow \text{Type}(A, G).$$

Because $U_k(A)$ and $a_{k,0}, \ldots, a_{k,l-1}$ 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 11.6 that

$$\deg [Y(k, l+1) \rightarrow Y(k, l)] \leq |S(k,l)|.$$

Combining this with Lemma 12.6, we see that

$$\deg [\text{Level}(A, G) \rightarrow \text{Type}(A, G)] \leq |\Gamma|.$$

It follows from Lemma 2.7 that $\text{Level}(A, G) \rightarrow \text{Type}(A, G)$ is Galois and that $\text{Type}(A, G)$ is smooth. Lemmas 2.2 and 2.1 now tell us that $\text{Type}(A, G) \rightarrow X$ is flat. As $\deg [\text{Level}(A, G) \rightarrow X] = |\text{Mon}(A, A)|$, we see that

$$\deg [\text{Type}(A, G) \rightarrow X] = |\text{Mon}(A, A)|/|\Gamma| = |\text{Type}(A, A)|.$$

\[\square\]

Proof of Theorem 12.4. Write $E' = \mathcal{O}_{\text{Sub}_m(G)}$. In Subsection 10.4, we constructed a map

$$g: D_m \otimes E' \rightarrow F(\text{Sub}_m(A), D_m).$$

We proved there that after inverting $p$, $g$ becomes epi with nilpotent kernel. In the light of Theorem 10.1, we conclude that $g$ is mono, and becomes iso after inverting $p$. We now put $\Gamma = \text{Aut}(A(m))$, and note that $g$ is equivariant for the evident actions of $\Gamma$. Passing to fixed points, we obtain a map

$$g^\Gamma: (D_m \otimes E')^\Gamma \rightarrow F(\text{Sub}_m(A), D_m)^\Gamma$$

which is again mono, and becomes iso after inverting $p$.

By Theorem 8.1, we know that $D_m^\Gamma = E$. Because $E'$ is free over $E$, we conclude that $(D_m \otimes E')^\Gamma = E'$. Next, for each isomorphism class of Abelian $p$-groups of order $m$ and rank at most $n$, choose a representative subgroup $A \leq A(m)$. Write $S$ for the set of chosen representatives. For $A \in S$ write $\Gamma_A = \{ \alpha \in \Gamma | \alpha(A) = A \}$. We have an isomorphism of $\Gamma$-sets

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

\[\square\]
Let

\[ F(\text{Sub}_m(A), D_m)^\Gamma = \prod_{A \in S} D_{m, A}^\Gamma. \]

Lemma 8.3 implies that \( \Gamma_A \to \text{Aut}(A) \) is epi; write \( \Gamma_A' \) for the kernel. Using Theorem 8.1 we find that

\[ D_{m, A}^\Gamma = (D_{m, A})^{\text{Aut}(A)} = D_{\text{Aut}(A)} = C_A. \]

Thus, \( g^\Gamma \) 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. \( \square \)

**Definition 12.8.** Let \( K \) be the universal subgroup over \( \text{Sub}_m(G) \). We write \( p^{-r}K \) for the kernel of the composite

\[ G \xrightarrow{p^r} G \xrightarrow{q} G/K. \]

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

\[ p^{-r} : \text{Sub}_m(G) \to \text{Sub}_{m+nr}(G). \]

**Lemma 12.9.** The map \( p^{-r} : \text{Sub}_m(G) \to \text{Sub}_{m+nr}(G) \) is a closed embedding, and identifies \( \text{Sub}_m(G) \) with the scheme of subgroups of degree \( m + nr \) which contain \( G(r) \).

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

\[ G(r) \to G \xrightarrow{p^r} G. \]

We know by Proposition 4.6 that there is a closed subscheme \( Z \leq \text{Sub}_{m+nr}(G) \) which is universal for subgroups containing \( G(r) \). Let \( K' \) be the universal subgroup over \( Z \) and \( q' : G \to G/K' \) the projection. Then the composite \( G(r) \to G \to G/K' \) is zero so there is a map (of formal groups over \( Z \)) \( q : G \to G/K' \) with \( q \circ p_G^r = q' \). The kernel \( K \) of \( q \) therefore has degree \( p^m \), and is classified by a map \( f : Z \to \text{Sub}_m(G) \).

Clearly \( p^{-r} : \text{Sub}_m(G) \to \text{Sub}_{m+nr}(G) \) factors through \( Z \), and the maps \( Z \xrightarrow{f} \text{Sub}_m(G) \xrightarrow{p^{-r}} Z \) are mutually inverse. \( \square \)

**Proposition 12.10.** 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 \( \text{Type}(A, G) \simeq \text{Type}(A', G) \), and the following diagram commutes:

\[ \begin{array}{ccc} 
\text{Type}(A, G) & \xrightarrow{\simeq} & \text{Sub}_{m+nr}(G) \\
\downarrow & & \downarrow p^{-r} \\
\text{Type}(A', G) & \xrightarrow{\simeq} & \text{Sub}_m(G) 
\end{array} \]

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

\[ \frac{|\text{Epi}(A^*, A)|}{|\text{Aut}(A)|} = |\text{Type}(A, \Lambda)| = |\text{Type}(A', \Lambda)| = \frac{|\text{Epi}(A^*, A')|}{|\text{Aut}(A')|}. \]

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

\[ \begin{array}{ccc} 
\text{Level}(A, G) & \xrightarrow{f} & \text{Type}(A, G) \\
\downarrow u & & \downarrow u' \\
\text{Level}(A', G) & \xrightarrow{f'} & \text{Type}(A', G) 
\end{array} \]
By Theorem 9.2, we know that \( u \) is a finite flat map of degree
\[
|\text{Epi}(A^*, A)|/|\text{Epi}(A^*, A')|.
\]
On the other hand, \( f \) and \( f' \) are finite flat maps of degree \(|\text{Aut}(A)|\) and \(|\text{Aut}(A')|\) respectively. It follows (using lemmas 2.2 and 2.1) that \( u' \) is a finite flat map of degree
\[
|\text{Epi}(A^*, A)|/|\text{Aut}(A')| = 1.
\]
In other words, \( u' \) is iso as claimed. It is not hard to see that the diagram commutes. \( \square \)

**Proof of Theorem 12.5.** We may as usual assume that \( G \) 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 \((p^m_0)^*x = g(x)(p^m_0 - 1)^*x\) for a series \( g(x) \in E[x] \) of Weierstrass degree \( s = p^n - p^{n-1} \). Thus, \( g(x) \) is a unit multiple of a monic polynomial \( h(x) \) of degree \( s \) with \( h(x) = x^s \) (mod \( m_E \)). Moreover, \( D_A = E[x_a]/h(x_a) \), where \( x_a = x(\phi(a)) \). Write \( D'_A = D_A/m_E \) and \( C'_A = C_A/m_E \), 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 \( x_ja = x(\phi(ja)) = jx_a \) (mod \( x_a^2 \)), so this has valuation 1 if \( j \neq 0 \) (mod \( p \)) 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 \( r \)th symmetric polynomial in \( \{x_{ja} \mid 0 \leq j < p^m \} \). This is the \( r \)th parameter of the divisor \([\phi A]\), so it lies in the image of \( \mathcal{O}_{\text{Sub}_u(G)} \rightarrow C_A \). Let \( u' \) be the image of \( u \) in \( D'_A \). If we write \( u' \) in the usual way as a sum of \( r \)th-fold products, then there is one term \( \prod (x_{ja} \mid j \neq 0 \) (mod \( p \)) \) 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 \( \kappa \). On the other hand, one can see that \( s/r = |\text{Type}(A, \Lambda)| = |C_A : E| \).

Consider the maps

\[
E^{s/r} = E\{1, u, \ldots, u^{s/r-1}\} \xrightarrow{i} C_A \xrightarrow{\lambda} D_A
\]

and the resulting maps

\[
\kappa^{s/r} = \kappa\{1, u', \ldots, (u')^{s/r-1}\} \xrightarrow{i'} C'_A \xrightarrow{\lambda'} D'_A
\]

We have just seen that \( i' \) is mono, so \( i' \) is mono. By dimension count, \( i' \) is iso. It follows that \( i \) is epi, and thus that \( \mathcal{O}_{\text{Sub}_u(G)} \rightarrow C_A \) 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 12.10 gives a commutative diagram as follows:

\[
\begin{array}{ccc}
\text{Type}(A, \mathbb{G}) & \xrightarrow{=} & \text{Sub}_{m+n}(\mathbb{G}) \\
& | & \\
\text{Type}(A', \mathbb{G}) & \xrightarrow{p^{-r}} & \text{Sub}_m(\mathbb{G})
\end{array}
\]

We have just shown that the bottom map is a closed embedding. The map \( p^{-r} \) is a closed embedding by Lemma 12.9. It follows that the top map is also a closed embedding, as claimed. \( \square \)

**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:

\[
\begin{array}{ccc}
G_0 & \xrightarrow{q_0} & G'_0 \\
\downarrow & & \downarrow \\
X_0 & \xrightarrow{f_0} & X'_0
\end{array}
\]

We shall suppose that the induced map \( G_0 \rightarrow G'_0 \) 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 \( q: \mathbb{H} \to \mathbb{H}' \) 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:

\[
\begin{array}{ccc}
\mathbb{H} & \xrightarrow{q} & \mathbb{H}' \\
\downarrow & & \downarrow \\
\mathbb{H}_0 & \xrightarrow{q_0} & \mathbb{H}'_0 \\
\downarrow & & \downarrow \\
Y & \xrightarrow{f_0} & X_0 \\
\end{array}
\]

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 \( a: \text{Sub}_m(\mathbb{G}) \to X \) be the usual projection, and let \( K < a^*\mathbb{G} \) be the universal example of a subgroup of degree \( p^m \). As \( \text{Sub}_m(\mathbb{G}) \) is a closed subscheme of \( \text{Div}_{p^m}(\mathbb{G}) \) and \( \text{Div}_{p^m}(\mathbb{G})_0 = X_0 \), we see that \( \text{Sub}_m(\mathbb{G})_0 = X_0 \).

There is a unique subgroup of order \( p^m \) of \( \mathbb{G}_0 \) defined over \( X_0 \), viz. the divisor \( p^m[0] = \text{spf}(\mathcal{O}_{\mathbb{G}_0}/p^m) \). In particular, \( K_0 = p^m[0] = \ker(q_0) \). It follows that there is a pullback diagram as shown below.

\[
(a^*\mathbb{G}/K)_0 \xrightarrow{\sim} \mathbb{G}_0/p^m[0] \xrightarrow{\sim} \mathbb{G}_0' \\
\text{Sub}_m(\mathbb{G})_0 \xrightarrow{\sim} X_0 \xrightarrow{\sim} X_0'
\]

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 \( b: \text{Sub}_m(\mathbb{G}) \to X' \) extending the map \( b_0 = f_0 \circ a_0: \text{Sub}_m(\mathbb{G})_0 \to X_0' \).

**Proposition 13.1.** \( b \) is a finite flat map, of degree \( |\text{Sub}_m(\mathbb{A})| \).

**Proof.** Recall from Theorem 12.4 that we have a dominant map

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

(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

\[
\text{Level}(A, \mathbb{G}) \to \text{Type}(A, \mathbb{G}) \to \text{Sub}_m(\mathbb{G}) \to X'
\]

can be identified with the map \( \theta_0 \) of Section 9. By part (7) of Theorem 9.2, this map is flat and has degree \( |\text{Mon}(A, \mathbb{A})| \). Moreover, \( \text{Level}(A, \mathbb{G}) \to \text{Type}(A, \mathbb{G}) \) is a Galois covering with Galois group \( \text{Aut}(A) \). Using lemmas 2.2 and 2.1, we see that \( \text{Type}(A, \mathbb{G}) \to X' \) is flat. The degree is clearly \( |\text{Mon}(A, \mathbb{A})|/|\text{Aut}(A)| = |\text{Type}(A, \mathbb{A})| \). It follows that \( b \circ f \) is a flat map of degree \( \sum_A |\text{Type}(A, \mathbb{A})| = |\text{Sub}_m(\mathbb{A})| \), and thus that \( \mathcal{O}_{\text{Sub}_m(\mathbb{G})}[\frac{1}{p}] \) is free of this rank over \( \mathcal{O}_{X'}[\frac{1}{p}] \).
We next let $Y < \text{Sub}_{m}(G)$ be the preimage of $X_{0}'$ under $b$, and write $\kappa' = \mathcal{O}_{X_{0}'}$ and $E' = \mathcal{O}_{Y}$. I claim that $\dim_{\kappa'} E' = |\text{Sub}_{m}(A)|$. The proof is similar to that in Subsection 10.3. To recall some notation from there: Given a sequence $(\alpha_{k}, \alpha_{k+1}, \ldots, \alpha_{n-1})$ we write

$$|\alpha| = \sum_{j} \alpha_{j}$$

$$\|\alpha\| = \sum_{j} j\alpha_{j}.$$ 

If $\alpha$ runs over sequences $(\alpha_{1}, \ldots, \alpha_{n-1})$ 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 Subsection 10.3. We write $\mathbb{H}$ for the restriction of $\alpha^*G$ to $Y$, and $K$ for the evident subgroup of $\mathbb{H}$, so that $\mathbb{H}/K$ is a pullback of $G_0'$ 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

$$p_{\mathbb{H}}^{p}x = ux^{p} + \cdots$$

$$p_{\mathbb{H}/K}^{p}y = vy^{p} + \cdots$$

$$q^{*}y = ax^{p} + \cdots.$$ 

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

$$va^{p}x^{p^j} + \cdots = au^{p}x^{p^{j+1}} + \cdots.$$ 

If $k < n$ then we conclude that $aw^{p} = 0$, and then Lemma 10.7 tells us that $f'(k, l) \leq f'(k, l + 1) + p^{f}(k + 1, l)$.

If $k = n$ then $u$ is invertible and we have $a(u^{p} - va^{p - 1}) = 0$. If also $l < n$ then $a$ is topologically nilpotent so $u^{p} - va^{p - 1}$ is invertible so $a = 0$, which shows that $E'(n, l) = E'(n, l + 1) = E'(n, m)$. From the construction of $\text{Sub}_{m}(G)$ 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

$$f'(k, l) \leq f'(k, l + 1) + p^{f}(k + 1, l)$$

if $(k < n)$

$$f'(n, l) \leq 1$$

if $(l > m)$

$$f'(k, l) = 0$$

if $(l > m)$

We next define a function $f(k, l)$ for $0 \leq k \leq n$ and $0 \leq l \leq l$ by

$$f(k, l) = \sum \{p^{\|\alpha\|} : \alpha = (\alpha_{1}, \ldots, \alpha_{n-k}), |\alpha| \leq m, \alpha_{n-k} \geq l\}.$$ 

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

$$f(k, l) \leq f(k, l + 1) + p^{f}(k + 1, l)$$

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

$$\beta = (\alpha_{1}, \ldots, \alpha_{n-k-2}, \alpha_{n-k-1} + l).$$ 

Note that $|\beta| = |\alpha|$, that $\beta_{n-(k+1)} \geq l$, and that $\|\beta\| = |\beta| + l$. Using this construction, we see that the sum of $p^{\|\beta\|}$ for these $\alpha$’s is $p^{f}(k + 1, l)$, as required. It follows that $f'(k, l) \leq f(k, l)$, and in particular that

$$\dim_{\kappa'}(E') = f'(1, 0) \leq f(1, 0) = d(m, n) = |\text{Sub}_{m}(A)|.$$ 

By an argument very similar to that of Subsection 10.5, we conclude that the map

$$b : \text{Sub}_{m}(G) \to X'$$ 

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] and [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 [?]. 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 $M \to Z$. Geometric chains form a graded Abelian monoid $GC_\ast Z$ under disjoint union. Restriction to the boundary gives a differential $\partial: GC_\ast Z \to GC_{\ast -1} Z$. The homology of this complex is a graded Abelian group $MO_\ast Z$. If we require that all manifolds have a given complex structure on the stable normal bundle, we obtain a different group $MU_\ast Z$, the complex bordism group of $Z$. We write $MU_\ast$ for $MU_\ast(\text{point})$, which is a ring under cartesian product. By a related geometric procedure, we can define a group $MU^\ast Z$ (which is often but not always the $MU_\ast$-dual of $MU_\ast Z$). In fact $MU^\ast Z$ has a natural circle ring structure. It can be thought of as an analogue of the Chow ring, which some readers may find more familiar.

Moreover, \( \text{BA}_G \) is the classifying space of its dual then \( (\text{BA}_G)^\ast \) is a polynomial algebra over \( \mathbb{Z} \). This is the source of all connections between algebraic topology and formal group theory. If we consider \( \text{BA}_G \) over a scheme \( X \) of dimension \( d \), then a group \( \text{BA}_G \langle a \rangle \) of \( \mathbb{Z} \)-points gives rise to a coproduct on \( \text{BA}_G \langle a \rangle^\ast Z \). If we require that all manifolds have a given complex structure on the stable normal bundle, we obtain a ring \( (\text{BA}_G \langle a \rangle^\ast Z)_{\text{point}} \). 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 $MU^\ast Z$ into a sheaf over the stack of formal groups. The cohomology of the dual sheaf $MU^\ast Z$ is the $E_2$ term of the Adams-Novikov spectral sequence, which converges to the stable homotopy groups of $Z$.

A formal group $G$ over a scheme $X = \text{spf}(E)$ gives rise to a map from $X$ to this stack. By pulling back $MU^\ast Z$, we obtain an algebra $E^\ast Z$ over $E$, and thus a scheme $Z_E = \text{spf}(E^\ast Z)$ over $X$. If the map from $X$ to the stack of formal groups is flat, then the functor $Z \mapsto E^\ast Z$ defines a generalised cohomology theory. This flatness condition is called Landweber exactness in the topological literature. It holds in particular if $G/X$ is the universal deformation of a formal group of finite height over a field. If $A$ is a finite Abelian group and $BA^\ast$ is the classifying space of its dual then $(BA^\ast)_E = \text{Hom}(A, G)$. For finite non-Abelian groups $K$, the generalised character theory of [8] establishes a connection between $BK_E$ and schemes of the form $\text{Level}(B, G)$. There is also a map from a certain closed subscheme $\text{spf}(R)$ of $(BS_{\text{pm}})_E$ to $\text{Sub}_{\text{an}}(G)$, which turns out to be an isomorphism. Theorem 10.1 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 $O_{\text{Sub}_{\text{an}}(G)} \to R/m_E R$; 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 $R/m_E R$, showing that it coincides with the dimension of $O_{\text{Sub}_{\text{an}}(G)}$ given by Theorem 10.1.

Using this fact, we obtain extra structure on $Z_E$. Suppose that $a, b$ are two points of $X$, that $G_a$ and $G_b$ are the fibres of $G$ over $a$ and $b$, and that $g: G_a \to G_b$ is an isogeny. A certain topological construction then gives rise to a map $(Z_E)_a \to (Z_E)_b$, which is functorial in $g$ 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 $E^\ast Z$, 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.

32
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 \( a \equiv b \pmod{p} \) for \( a = b \pmod{p} \).

We first define

\[
q = p^n, \\
l(x) = \sum_{k \geq 0} x^{k^2} / p^k, \\
e(x) = t^{-1}(x) \quad (\text{so } e(l(x)) = x).
\]

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 \( F \) 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 \( G_1 \) is the formal group defined by \( F_1 \) we have \([a](x) = a^*_G x \). By applying \( l \) one checks that

\[
[p](x) = e(px) + r, \quad x^q.
\]

We next define

\[
C_{p^m}(x, y) = (x^m + y^m - (x + y)^m)/p.
\]

**Lemma 15.1.** \( C_p(x, y) \equiv -\sum_{k=1}^{p-1} x^k (-y)^{p-k}/k \)

**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 \((x + y)^p\). \( \square \)

**Lemma 15.2.** \( C_q(x, y) \equiv C_p(x^{q/p}, y^{q/p}) \)

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

\[
x^q + y^q = (x + y)^q + pC_q(x, y)
\]

\[
x^q + y^q = (x^{q/p} + y^{q/p})^p + pC_p(x^{q/p}, y^{q/p}).
\]

Subtracting these, we obtain

\[
pC_q(x, y) = pC_p(x^{q/p}, y^{q/p}) \pmod{p^2}.
\]

The claim follows. \( \square \)

Note that \( xy \) divides \( C_p(x, y) \), so that \( x^{q/p}y^{q/p} \) divides \( C_q(x, y) \pmod{p} \).

We write \( v_p(n) \) for the \( p \)-adic valuation of \( n \).

**Lemma 15.3.** If \( 0 < l < q^k \) then

\[
v_p \left( \frac{q^k}{l} \right) = nk - v_p(l).
\]
Proof. We can write
\[ \left( \frac{q^k}{l} \right) = \frac{q^k}{l} \prod_{j=1}^{l-1} \frac{q^k - j}{j}. \]
The terms in the product are clearly p-adic units; the claim follows. \qed

Lemma 15.4. \( x + y \equiv x + y + C_p(x^{q/p}, y^{q/p}) \pmod{(xy)^q}. \)

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 \( l(y) = 0 \). We conclude that
\[ y = \sum_{j=1}^{q-1} l(j)(x)(yw)^j/j!. \]
Lemma 15.3 implies that the series \( l(j)(x)/j! \) for \( 0 < j < q \) are all integral, and moreover that
\[ \frac{l(j)(x)}{j!} \equiv \frac{1}{p} \binom{q}{j} x^{q-j} \quad (1 < j < q) \]
\[ l'(x) \equiv 1 + \frac{1}{p} \binom{q}{1} x^{q-1}. \]
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. \qed

Corollary 15.5. 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 \( k = p^l \) with \( l \neq 0 \). We then have
\[ (y + z)^k = (y^{p^r} + z^{p^r})^l = y^k + ly^{k-p^r}z^{p^r} + \ldots. \]
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
\[ F_0(F_0(x, y), z) = F_0(F_0(x, y), z). \]
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. \( \square \)

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 \( \sum_{i \geq 0} a_ip^i \), with \( a_i^q = a_i \). There is a Frobenius automorphism \( F \) of \( W \) defined by \( F(\sum a_ip^i) = \sum a_i^p p^i \).

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 \( k + l = 1 \) (mod \( q - 1 \)), 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 \( \sum \hat{a}_i p^i \), we can show that this lies in \( W[x] \). The map \( a \mapsto [a](x) \) gives a ring homomorphism \( W \to \text{End}(F_1) \).

We next put
\[
E = W[u_1, \ldots, u_{n-1}]
\]
\[
u_0 = p, u_n = 1.
\]
We also let \( \phi \) 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 \( a^\phi = a^p \) (mod \( p \)) for all \( a \).

Over \( E[\frac{1}{p}] \) we have a formal power series \( \log_F(x) = x + O(x^2) \) characterised uniquely by either of the two following equations:
\[
\log_F(x) = x + \frac{1}{p} \sum_{k=1}^n \log_F(u_kx^{p^k})
\]
\[
\log_F(x) = x + \frac{1}{p} \sum_{k=1}^n u_k \log_F(x^{p^k})
\]
From either of these equations, one can see that \( F = F_1 \) (mod \( u_1, \ldots, u_{n-1} \)). The following more explicit formulæ are given in [14, Section 4.3]. Consider a (possibly empty) sequence \( I = (i_1, \ldots, i_m) \) 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
\[
u_l = \prod_k u_k^{-j_k}.
\]
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 than \( E[\frac{1}{p}][x, y] \)), so it defines a formal group law over \( E \).
By applying \( \log_F \), one can check that
\[
[p]_F(x) = \exp_F(px) + F u_1 x^p + F \cdots + F u_{n-1} x^{p^{n-1}} + F x^n.
\]

**Lemma 15.6.** If \( k > 0 \) then
\[
x + F y = x + y + u_k C_{p^k}(x, y) \mod (u_1, \ldots, u_{k-1}) + (x, y)^{p^k+1}.
\]

*Proof.* We work \( \mod (x, y)^{p^k+1} \) and \( (u_1, \ldots, u_{k-1}) \). 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 \( u C_{p^k}(x, y) = 0 \). 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
\[
x + y + u_k x^{p^k}/p + u_k y^{p^k}/p = x + y + u_k C_{p^k}(x, y) + z + u_k (x + y + z)^{p^k}/p
\]
\[
z = u_k (x + y + z)^{p^k}/p - u_k (x + y + z)^{p^k}/p.
\]
Thus \( z \in (x, y) z = (x, y)z \). 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 15.7.** \( F(x, y) = x + y \mod (x, y) \) or \( \mod (y^{p^k}, u_0 y, u_1 y, \ldots, u_{n-1} y) \).

*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 \( J = (u_1, \ldots, u_{n-1}) \). Because \( Jy = 0 \), we see that \( F(x, y) = F_1(x, y) \). Now consider \( F_1(x, y) - x - y \). Using Lemma 15.4, we see that every term is divisible either by \( p^k \) or by \( y^{p^k} \), both of which are zero. Thus \( F_1(x, y) = x + y \) as required.

Next, observe that \((x + F_i y)^{p^k} = x^{p^k} + \sum_{k=1}^{n} u_k x^{p^k}/p = x + \sum_{k=1}^{n} u_k (x^{p^k}/p)\). It follows that \((x + F_i y)^{p^k} - F_i (x^{p^k} + F_i y^{p^k})\) is divisible by \( p \).

Thus, there are unique series \( \sigma_k(x, y) \in \mathbb{Z}_p[y][x] \) such that
\[
\sigma_k(x, y) = \sum_{k=1}^{n} u_k (x^{p^k}/p)\]

**Lemma 15.8.** \( F(x, y) = F_1(x, y) - \sum_{k=1}^{n-1} u_k \sigma_k(x, y) \mod (u_0, \ldots, u_{n-1})^2 \)

*Proof.* Write \( J = (u_1, \ldots, u_{n-1}) \) and \( I = (p) + J \). For the moment, we work \( \mod J^2 \). In this setting we have
\[
\log_F(x) = x + \sum_{k=1}^{n} u_k l(x^{p^k})/p = l(x) + \sum_{k=1}^{n-1} u_k l(x^{p^k})/p.
\]
Next, observe that \( x + F y - F (x + F_i y) \) vanishes \( \mod J \), so there are unique series \( \tau_k(x, y) \in \mathbb{Z}_p[y][x] \) such that
\[
x + F y - F (x + F_i y) = \sum_{k=1}^{n-1} u_k \tau_k(x, y) \mod J^2.
\]
By Lemma 15.7 we can rewrite the right hand side as a formal sum. Thus
\[
x + F y = (x + F_i y) + F u_1 \tau_1(x, y) + F \cdots + F u_{n-1} \tau_{n-1}(x, y).
\]
We now apply \( \log_F \) to this equation. The left hand side becomes
\[
l(x) + l(y) + \sum_{k=1}^{n-1} u_k/l(x^{p^k}) + l(y^{p^k}).
\]
The right hand side becomes
\[
l(x + F_i y) + \sum_{k=1}^{n-1} u_k l(x + F_i y^{p^k}) + \sum_{k=1}^{n} u_k \tau_k(x, y).
\]
Recall that \( l(x + F_1, y) = l(x) + l(y) \) and 
\[
\ell((x + F_1, y)^{p^k}) = \ell(x^{p^k}) + \ell(y^{p^k}) + \ell(p\sigma_k(x, y)).
\]
Using this to simplify the right hand side further, and rearranging, we conclude that
\[
\sum u_k\tau_k(x, y) + \sum \frac{u_k}{p}\ell(p\sigma_k(x, y)) = 0.
\]
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 \( G_1 \) be the formal group over \( \mathbb{Z}_2 \) with logarithm \( \log_F(x) = \sum_k x^{2^k}/2^k \), so that \( G_0 \) is a formal group of height 2 over \( \kappa = F_2 \). Computer calculations give results as follows.

(1) Let \( A \simeq \mathbb{Z}/2 \) be generated by \( a \). Given a level-\( A \) structure \( \phi \), we shall identify \( a \) with \( x(\phi(a)) \). We then have
\[
\text{Level}(A, G_0) = \text{spf}(\kappa[a]/a^3).
\]
A coordinate on the quotient group \( G_0/\phi[A] \) is given by
\[
y = ax + x^2 + a^2x^3.
\]
The associated formal group law is
\[
y + F^r\ z \ = \ y + z + ayz + y^2z^2 + a(y^2z^3 + y^3z^2) + a^2(y^2z^4 + y^3z^3 + y^4z^2) + \cdots.
\]
(2) Now take \( A \simeq (\mathbb{Z}/2)^2 \), with generators \( a \) and \( b \). Then
\[
\text{Level}(A, G_0) = \text{spf}(\kappa[a, b]/(a^3, b^3, a^2 + ab + b^2)).
\]
Because \( A = \Lambda(1) \), the corresponding subgroup divisor is just \( G_0(1) \), and a coordinate on the quotient group is just given by \( [2](x) = x^4 \).
(3) Take \( A = \mathbb{Z}/4 \) generated by \( a \). Then
\[
\text{Level}(A, G_0) = \text{spf}(\kappa[a]/a^{12})
\]
\[
\text{Type}(A, G_0) = \text{spf}(\kappa[b]/b^{12}) \quad b = a^2 + a^3 + a^8 + a^{11}.
\]
The equation of the subgroup divisor is
\[
\prod_{c \in A} (x - c) = x^4 + b^5x^3 + bx^2 + b^3x.
\]
(4)
\[
\text{Sub}_2(G_0) = \text{spf}(\kappa[b]/b^7).
\]
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 \( \text{Type}(A, G_0) \rightarrow \text{Sub}_2(G_0) \) just sends \( b \) to \( b \).

Now let \( G_1 \) 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
\[
\text{Level}(A, G_0) = \text{spf}(\kappa[a, b]/(a^{56}, b^9 + b^5a^8 + b^4a^{16} + \cdots + a^{48}))
\]
\[
\text{Type}(A, G_0) = \text{spf}(\kappa[c, d]/(c^{15}, c^{14}d, c^{13}d^2 + c^{14}, a^3 + c^8d + c^{12})).
\]
where
\[ c = a^4 + a^{18} + a^{32} + a^{10}b + a^{17}b + a^{38}b + a^2b^2 + a^{10}b^2 + a^{37}b^2 + b^4 + a^{14}b^4 + a^{21}b^4 + a^{35}b^4 + a^{34}b^5 + a^{41}b^5 \]
\[ d = a^8b + b^2 + a^{32}b^5. \]

The equation of the group divisor is
\[
 f(x) = x^8 + (dc^7 + c^3d^2 + c^{10}d^2)x^6 + c^5d^2x^5 + cx^4 + (dc^{13} + c^9d^2)x^3 + (cd + c^7)x^2 + (dc^3 + c^{14})x.
\]

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 \( \text{Type}(A, G) \rightarrow \text{Sub}_8(G) \) is not a closed embedding.

**References**


