THE POWER OPERATION STRUCTURE ON MORAVA E-THEORY OF HEIGHT 2 AT THE PRIME 3

A DISSERTATION
SUBMITTED TO THE FACULTY OF THE GRADUATE SCHOOL
OF THE UNIVERSITY OF MINNESOTA
BY

YIFEI ZHU

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

TYLER LAWSON

JUNE, 2013

Acknowledgements

I thank Charles Rezk for his encouragement on this work, and for his observation (4.4.21) which led to Proposition 4.4.7, Corollary 4.4.8, and eventually an approach to Adem relations as in the proof of Proposition 5.2.3 (iv).

I thank Kyle Ormsby for helpful discussions on the calculations in Chapter 4, and for directing me to places in the literature, including [1]. The computation in Example 4.4.13 is out of his suggestion.

I thank Tyler Lawson for the sustained support from him I received as a student.

Finally, I am grateful to everyone who helped me over the years—I feel very fortunate to have been able to study mathematics at the University of Minnesota.

Abstract

Dyer-Lashof theories organize power operations in cohomology. We give an overview of the structure of the Dyer-Lashof theories associated to Morava E-theories. When the E-theory is an elliptic cohomology theory, this structure enables us to compute power operations by doing calculations with elliptic curves. We give explicit computations of the Dyer-Lashof theory for a specific E-theory spectrum and its $K(1)$-localization.

Contents

Chapter 1

Introduction

1.1 Motivation

Algebraic topology is a field that solves topological or geometric problems by translating them into algebra. The problem of vector fields on spheres asks: What is the maximum integer $k(n)$ for which there exist k continuous vector fields on the unit sphere in Euclidean n-space, linearly independent everywhere? This was solved by Adams [2] as a classic application of algebraic topology to geometry. The solution was built upon the study of cohomology operations—the work of Steenrod and Whitehead [3] which used the Steenrod squares to study the same problem, and Adams' original attempt to replace the Steenrod squares by "cohomology operations of higher kinds."[1] These led to the construction of the Adams operations which were the key tool for solving the vector-field problem for spheres.

The Steenrod squares and the Adams operations are operations in ordinary cohomology with $\mathbb{Z}/2$-coefficients and in K-theory respectively, and both are examples of an important family of cohomology operations called *power operations*. Foundational work on the Steenrod operations and the *Steenrod algebra* A^* established a model for studying power operations in other cohomology theories, as encapsulated in [5, Section 1]: "Steenrod constructed a family of elements of A^*, ... [6], Adem found some relations between them [7], Serre showed that Steenrod's elements generated A^* and

[1] Cf. [2, Section 2]. Adams used secondary cohomology operations to solve the Hopf invariant one problem [4].

Adem's relations implied all relations [8] and Milnor elucidated the full structure of A^* [9]. Nonetheless much remains to be understood about A^* and it is an active area of research."

Following earlier work for ordinary cohomology and K-theory, the study of power operations for other cohomology theories has been carried out by tom Dieck and Quillen for complex cobordism [10, 11], by McClure for p-adic K-theory [12, 13], by Voevodsky for motivic cohomology [14], and by Ando, Hopkins, and Strickland for Morava E-theories [15], among others. In particular, complex cobordism, p-adic K-theory, and Morava E-theories, together with ordinary cohomology, all fit into *the chromatic filtration*, an organizing principle for understanding large-scale phenomena in modern stable homotopy theory (cf. [16, 17, 18]). Under this framework, cohomology theories are organized according to the *heights* of their associated *formal group laws*, and also prime by prime: ordinary cohomology with rational coefficients at height 0, p-adic K-theory at height 1, complex cobordism and ordinary cohomology with $\mathbb{Z}/p$-coefficients at height ∞, and Morava E-theories as a family of cohomology theories at height n for each n—with $n = 2$ including elliptic cohomology theories [19, 20, 21]—and at all primes. The chromatic filtration has an intimate connection with algebraic geometry and number theory, and studying power operations from this viewpoint brings in new tools and insight from beyond the range of classical algebraic topology.

In elliptic cohomology, the study of power operations is aided by a "bridge" connecting homotopy theory and the theory of elliptic curves (see [22, Theorem B] and [23, 2.9.1]), and is based on work of Ando, Hopkins, and Strickland for the case of supersingular curves (see [15]), and work of Ando and Ganter for the case of the Tate curve (see [24, 25]). Thanks to the correspondence across this bridge, explicit constructions and computations for power operations flow from calculations with isogenies of elliptic curves (cf. [26]). With concrete formulas, we hope to study the structure underlying power operations in elliptic cohomology, along the lines of understanding the Steenrod algebra A^* for ordinary cohomology. Moreover, as explained at the beginning of [27], we hope to learn about the conjectural geometric interpretation of Morava E-theories (at height $n = 2$) by examining power operations, analogous to vector bundles and representation theory as encoded in the Adams operations for K-theory (cf. [2, 28] and see Example 2.1.1 for details).

1.2 Statement of results

The power operation structure on Morava E-theory of height 2 at the prime 3

Let p be a prime, and q be a power of p. We use the symbols $\mathbb{F}_q$ and $\mathbb{Z}_q$ to denote a field with q elements and the ring of p-typical Witt vectors over $\mathbb{F}_q$ respectively. In particular $\mathbb{Z}_p$ is the ring of p-adic integers.

For a Morava E-theory, the analog of the Steenrod algebra in ordinary cohomology is the *Dyer-Lashof algebra* as the collection of all power operations. In [26] Rezk explicitly computes the Dyer-Lashof algebra for a specific E-theory of height 2 at the prime 2. Following his work, at height 2 for the prime 3, we studied the power operation structure on an E-theory E with homotopy groups

$$\pi_* E = E_* \cong \mathbb{Z}_9[\![h]\!][u^{\pm 1}]$$

where h and u are in degrees 0 and 2 respectively.

As in [26], our computation of power operations follows the approach of [6]: one first defines a total power operation, and then uses the computation of the cohomology of the classifying space $B\Sigma_m$ for the symmetric group Σ_m to obtain individual power operations. By doing calculations with elliptic curves associated to E, we get formulas for a total power operation ψ^3 on E_0 and a ring S_3 which represents a corresponding moduli problem. Based on the computation of $E^* B\Sigma_m$ in [29] as reflected in the formula for S_3, we then define individual power operations Q_k, and derive the relations they satisfy—action on scalars, additivity, commutation relations, Adem relations, Cartan formulas, and the Frobenius congruence (see Proposition 5.2.3). In view of the general structures studied in [22], we get an explicit description of the corresponding Dyer-Lashof algebra Γ as below.

Definition 1.2.1 (Definition 5.3.1)**.**

(i) Let i be an element generating $\mathbb{Z}_9$ over $\mathbb{Z}_3$ with $i^2 = -1$. Define Γ to be the associative ring generated over $\mathbb{Z}_9[\![h]\!]$ by elements Q_0, Q_1, Q_2, and Q_3 subject to the following relations: the Q_k's commute with elements in $\mathbb{Z}_3 \subset \mathbb{Z}_9[\![h]\!]$, and

satisfy *commutation relations*

$$\begin{aligned}
Q_0 h &= (h^3 - 27h^2 + 201h - 342)Q_0 + (3h^2 - 54h + 171)Q_1 + (9h - 81)Q_2 \\
&\quad + 24Q_3, \\
Q_1 h &= (-6h^2 + 108h - 334)Q_0 + (-18h + 171)Q_1 + (-72)Q_2 + (h - 9)Q_3, \\
Q_2 h &= (3h - 27)Q_0 + 8Q_1 + 9Q_2 + (-24)Q_3, \\
Q_3 h &= (h^2 - 18h + 57)Q_0 + (3h - 27)Q_1 + 8Q_2 + 9Q_3, \\
Q_k i &= (-i)Q_k \text{ for all } k,
\end{aligned}$$

and *Adem relations*

$$\begin{aligned}
Q_1 Q_0 &= (-6)Q_0 Q_1 + 3Q_2 Q_1 + (6h - 54)Q_0 Q_2 + 18Q_1 Q_2 + (-9)Q_3 Q_2 \\
&\quad + (-6h^2 + 108h - 369)Q_0 Q_3 + (-18h + 162)Q_1 Q_3 + (-54)Q_2 Q_3, \\
Q_2 Q_0 &= 3Q_3 Q_1 + (-3)Q_0 Q_2 + (3h - 27)Q_0 Q_3 + 9Q_1 Q_3, \\
Q_3 Q_0 &= Q_0 Q_1 + (-h + 9)Q_0 Q_2 + (-3)Q_1 Q_2 + (h^2 - 18h + 63)Q_0 Q_3 \\
&\quad + (3h - 27)Q_1 Q_3 + 9Q_2 Q_3.
\end{aligned}$$

(ii) Write $\omega \coloneqq \pi_2 E$, viewed as a free module with one generator u over $E_0 \cong \mathbb{Z}_9[\![h]\!]$. Define ω as a left Γ-module, compatible with its E_0-module structure, such that

$$Q_k \cdot u \coloneqq \begin{cases} u, & \text{if } k = 1, \\ 0, & \text{if } k \neq 1. \end{cases}$$

The relations in Definition 1.2.1 (i), together with additivity, Cartan formulas, and a natural grading, describe explicitly the structure of Γ as that of a *graded twisted bialgebra over* E_0 (see Section 3.2).

Our computation is motivated by Rezk's result [30, 22] on the general pattern of power operations for Morava E-theory spectra. The formulas in Definition 1.2.1 give the following concrete version of his theorem, at height 2 for the prime 3. (See Section 3.2 for details about the notation and terminology.)

Theorem 1.2.2 (Theorem 5.3.2)**.** *Let A be a $K(2)$-local commutative E-algebra. Let Γ be the graded twisted bialgebra over E_0 in Definition 1.2.1* (i)*, and ω be the Γ-module*

in Definition 1.2.1 (ii)*. Then A_* has the structure of an ω-twisted $\mathbb{Z}/2$-graded amplified Γ-ring. In particular, for a free commutative E-algebra $\mathbb{P}_E(\Sigma^d E)$,*

$$\pi_* L_{K(2)} \mathbb{P}_E(\Sigma^d E) \cong \big(R_d\big)^{\wedge}_{(3,h)}$$

where R_d is the free graded amplified Γ-ring with one generator in dimension d.

Power operations on the $K(1)$-localization

On the $K(1)$-localization F of our Morava E-theory E, the power operation structure is simpler: the Dyer-Lashof algebra has a single generator ψ^3_F over the ring

$$F_0 = \mathbb{Z}_9[\![h]\!][h^{-1}]^{\wedge}_3 = \left\{ \sum_{n=-\infty}^{\infty} k_n h^n \;\middle|\; k_n \in \mathbb{Z}_9, \lim_{n\to-\infty} k_n = 0 \right\}.$$

We derive formulas for this $K(1)$-local power operation ψ^3_F from the calculations for the total power operation ψ^3 above. Based on [31, Sections 2.4 and 8.2], it boils down to interpreting the $K(1)$-local power operations in terms of the elliptic curve and formal group data related to our construction of ψ^3. Here are the formulas.

Proposition 1.2.3 (cf. Corollary 5.2.1 and Section 5.4)**.** *The total power operation*

$$\psi^3\colon\ E^0 \longrightarrow E^0[\alpha]/\big(w(\alpha)\big)$$

is given by

$$\begin{aligned}\psi^3(h) &= h^3 + (\alpha^3 - 6\alpha - 27)h^2 + 3(-6\alpha^3 + \alpha^2 + 36\alpha + 67)h \\ &\quad + 57\alpha^3 - 27\alpha^2 - 334\alpha - 342, \\ \psi^3(i) &= -i,\end{aligned}$$

where

$$\alpha \equiv 0 \mod 3 \qquad \text{and} \qquad w(\alpha) = \alpha^4 - 6\alpha^2 + (h-9)\alpha - 3.$$

Correspondingly the $K(1)$-local power operation

$$\psi^3_F\colon\ F^0 \longrightarrow F^0$$

is given by

$$\psi_F^3(h) = h^3 - 27h^2 + 183h - 180 + 186h^{-1} + 1674h^{-2} + (\textit{lower-order terms}),$$
$$\psi_F^3(i) = -i.$$

1.3 Outline of the thesis

As explained in Section 1.1, our computational results stated in Section 1.2 are made possible by the "bridge" between homotopy theory and the theory of elliptic curves, with power operations corresponding to deformations of Frobenius isogenies. Thus naturally this thesis consists of two parts: on one side of the bridge, the discussions in Chapters 2 and 3 lead to the structure of power operations in Morava E-theories; on the other side, the topics in Chapter 4 are centered around cyclic isogenies of elliptic curves. Finally, in Chapter 5, the bridge connects the two sides, and we get an explicit description of the power operation structure on Morava E-theory at height 2 for the prime 3.

More details for each Chapter are as follows.

In Chapter 2, we introduce the general theory of power operations for cohomology theories represented by commutative ring spectra. Section 2.1 begins with an intuitive description of the power operation construction, with power operations in K-theory as an example, and then discusses the construction systematically using the functors of extended powers. Based on the structure of the extended powers, Section 2.2 introduces the organizing principle of algebraic theories for power operations, in particular, the Dyer-Lashof theory associated to a commutative ring spectrum R which models all homotopy operations on commutative R-algebra spectra.

In Chapter 3, we discuss the theory of power operations for Morava E-theories, specifically, the foundational connection to deformations of Frobenius isogenies. Section 3.1 introduces Morava E-theories in the context of the chromatic filtration which relates stable homotopy theory and one-dimensional commutative formal groups. Section 3.2 describes the general pattern of power operations in any Morava E-theory E. Section 3.3 translates from the E-Dyer-Lashof theory and related categories to categories arising from the formal group and its finite flat subgroups associated to E, and Section 3.4 describes the structure within the latter categories.

In Chapter 4, we present some of the basics about elliptic curves that are relevant

to our computations, and illustrate the theory by a specific example built through each section. Section 4.1 discusses Weierstrass equations, rigidity, dual isogenies, and the group law algorithm. Section 4.2 discusses the structure of torsion subgroups and division polynomials, and contains one of our main calculations (Proposition 4.2.3). Section 4.3 discusses p-divisible groups, the Serre-Tate theorem on deformation theory, and the Hasse invariant and supersingular elliptic curves. Section 4.4 discusses cyclic isogenies (with another main calculation in Proposition 4.4.2) and their compositions, the Lubin isogeny construction, and Vélu's formulas. Section 4.5 introduces basic moduli problems for elliptic curves, discusses their representability and morphisms, and presents examples of how the representing moduli schemes look and how they behave under morphisms; in particular, via the Serre-Tate theorem, we produce a Morava E-theory spectrum in Example 4.5.12.

In Chapter 5, we connect the calculations with elliptic curves in Chapter 4 to the theory of power operations in Chapters 2 and 3. Section 5.1 recapitulates our main example developed in Chapter 4, and collects the calculations scattered therein. Section 5.2 gives formulas for the total power operation ψ^3, and then defines the individual power operations Q_k and derives the relations they satisfy. Based on these formulas, Section 5.3 gives an explicit description of the Dyer-Lashof theory in terms of an associative ring generated by the Q_k's. Section 5.4 discusses the relationship between the total power operation ψ^3, at height 2, and the corresponding $K(1)$-local power operations, and derives formulas for the latter from the calculations in Section 5.2.

1.4 Conventions

All formal groups mentioned in this thesis will be commutative and one-dimensional.

Let p be a prime, and q a power of p. We use the following list of symbols.

$\mathbb{Z}_{(p)}$	the localization of $\mathbb{Z}$ with respect to the ideal (p)
$\mathbb{F}_q$	a field with q elements
$\mathbb{Z}_q$	the ring of p-typical Witt vectors over $\mathbb{F}_q$
$\mathbb{Q}_q$	the fraction field of $\mathbb{Z}_q$
$\mathbb{W}(k)$	the ring of p-typical Witt vectors over a perfect field k of characteristic p
$\mathbb{Z}/m$	the additive group of integers modulo m

Σ_m	the symmetric group on m letters
$R^\times$	the group of units of a ring R
$R^\wedge_I$	the completion of a ring R with respect to an ideal I
$R[\![x]\!]$	the ring of formal power series over a ring R in a variable x
$R(\!(x)\!)$	the ring of formal Laurent series over a ring R in a variable x
$[n]$	the multiplication-by-n map on a group scheme
	(and also the induced map on the coordinate ring)
$G[n]$	the kernel of $[n]$ on a group scheme G
$\underline{\mathbb{Z}/m}$	the constant group scheme associated to $\mathbb{Z}/m$
μ_m	the group scheme of m'th roots of unity,
	i.e., the kernel of $[m]$ on the multiplicative group scheme
$\widehat{E}$	the formal completion of an elliptic curve E at the identity
Set	the category of sets
Sch	the category of schemes
Sch$/S$	the category of schemes over a scheme S

Chapter 2

Extended powers and power operations

2.1 How a power operation arises

Let $h^*(-)$ be a multiplicative cohomology theory, so that we have maps

$$h^c(X) \otimes h^d(X) \longrightarrow h^{c+d}(X)$$

for spaces X and integers c and d. In particular, for each $m \geq 0$, we have the m'th-power map

$$\begin{aligned} h^d(X) &\longrightarrow h^{md}(X) \\ a &\mapsto a^m. \end{aligned}$$

As we will see below, if $h^*(-)$ is represented by a structured commutative ring spectrum, the m'th-power map lifts to a map P^m, called *the m'th total power operation*, fitting into the diagram

$$\begin{array}{ccc} & & h^0(X \times B\Sigma_m) \\ & \overset{P^m}{\nearrow} & \big\downarrow \\ h^0(X) & \xrightarrow[a \mapsto a^m]{} & h^0(X) \end{array} \tag{2.1.1}$$

where the vertical map is induced by (the homotopy class of) a map from a point to $B\Sigma_m$. Moreover, for each α in the homology group $h_0(B\Sigma_m)$, pairing with α (taking the slant product) gives an operation

$$Q_\alpha\colon\ h^0(X) \xrightarrow{P^m} h^0(X \times B\Sigma_m) \xrightarrow{/\alpha} h^0(X).$$

The total power operations P^m are multiplicative, but not additive in general; the individual operations Q_α may not be additive or multiplicative.

Example 2.1.1. Take complex K-theory $K(-)$ as $h^0(-)$ (it is an even-periodic generalized cohomology theory). Let $R(\Sigma_m)$ be the complex representation ring of Σ_m. Its completion, in the topology induced by the ideal of virtual representations of degree 0, is isomorphic to $K(B\Sigma_m)$ by the Atiyah-Segal completion theorem [32].

For each $\alpha \in \mathrm{Hom}\big(R(\Sigma_m), \mathbb{Z}\big)$, we can build Q_α as a composite

$$K(X) \xrightarrow{P^m} K_{\Sigma_m}(X^m) \xrightarrow{\Delta^*} K_{\Sigma_m}(X) \cong K(X) \otimes R(\Sigma_m) \xrightarrow{\mathrm{id}\otimes\alpha} K(X) \otimes \mathbb{Z} \cong K(X),$$

which we explain as follows. The total power operation P^m sends a representative V of an isomorphism class of complex vector bundles over X to its m'th external tensor product $V^{\boxtimes m}$ over X^m, naturally a Σ_m-equivariant bundle ($K_{\Sigma_m}(-)$ denotes the Σ_m-equivariant K-theory). It then pulls back along the diagonal map $\Delta\colon\ X \to X^m$ to be a Σ_m-equivariant bundle over X representing an element in $K_{\Sigma_m}(X)$. This ring is isomorphic to $K(X) \otimes R(\Sigma_m)$ by [33, Proposition 2.2], and composing with α the map lands back in $K(X)$.

In particular, the non-additivity of P^m and Q_α boils down to the distributive law of tensor products over direct sums for vector spaces. Operations of this type turn out to generate all the operations in K-theory (cf. Example 3.4.1). Their properties have a close interaction with vector bundles and linear representations of finite symmetric groups (see [2, 28] and [34, Sections 1-4]).

In the above example, complex K-theory is represented by an E_∞-ring spectrum KU (see [35, Theorem VIII.4.3]). In general, the category of modules over an E_∞-ring spectrum R has a symmetric monoidal smash product $\wedge_R$. Taking R as the sphere spectrum S, we have the stable homotopy category of spectra. With a symmetric monoidal smash product, we can construct total power operations and individual power

operations systematically via the extended powers.

We work in the category of S-modules, in the sense of [35], as the basic category of spectra. Let R be a commutative S-algebra, i.e., an E_∞-ring spectrum which is an S-module (see [35, Lemma II.3.4]). Consider the *m'th extended power* functor

$$\mathbb{P}^m_R(-) \coloneqq (-)^{\wedge_R m}/\Sigma_m \colon \mathrm{Mod}_R \to \mathrm{Mod}_R$$

on the category of R-modules, which sends an R-module to its m-fold smash product over R modulo the action by Σ_m. The $\mathbb{P}^m_R(-)$'s assemble together to give the *free commutative R-algebra* functor

$$\mathbb{P}_R(-) \coloneqq \bigvee_{m\geq 0} \mathbb{P}^m_R(-) \colon \mathrm{Mod}_R \to \mathrm{Alg}_R$$

from the category of R-modules to the category of commutative R-algebras. In particular, $\mathbb{P}_R$ is a monad in Mod_R, and a commutative R-algebra is precisely an algebra for this monad.

The above functors descend to homotopy categories, where power operations for a commutative R-algebra A arise as follows. Let

$$\mu \colon \mathbb{P}_R(A) \longrightarrow A$$

be the structure map of A as a $\mathbb{P}_R$-algebra. Denote by $A^{B\Sigma^+_m}$ the spectrum of functions from $B\Sigma^+_m \coloneqq \Sigma^\infty_+ B\Sigma_m$ to A. For each $m \geq 0$, we have a total power operation

$$P^m \colon \pi_0 A \longrightarrow \pi_0\big(A^{B\Sigma^+_m}\big)$$

sending an element $x \in \pi_0 A$, represented by an R-module map

$$f_x \colon R \longrightarrow A,$$

to the element represented by the composite

$$R \wedge B\Sigma^+_m \cong \mathbb{P}^m_R(R) \xrightarrow{\mathbb{P}^m_R(f_x)} \mathbb{P}^m_R(A) \hookrightarrow \mathbb{P}_R(A) \xrightarrow{\mu} A. \tag{2.1.2}$$

Composed with the inclusion of a basepoint in $B\Sigma_m$, P^m gives the m'th-power map

$$\pi_0 A \xrightarrow{P^m} \pi_0\big(A^{B\Sigma_m^+}\big) \to \pi_0 A, \qquad x \mapsto x^m.$$

For each $\alpha \in \pi_0 \mathbb{P}_R^m(R)$ represented by an R-module map

$$f_\alpha \colon\ R \longrightarrow \mathbb{P}_R^m(R),$$

precomposing (2.1.2) by f_α gives an operation

$$Q_\alpha \colon\ \pi_0 A \longrightarrow \pi_0 A$$

which sends an element $x \in \pi_0 A$ to the element represented by the entire composite

$$R \xrightarrow{f_\alpha} \mathbb{P}_R^m(R) \xrightarrow{\mathbb{P}_R^m(f_x)} \mathbb{P}_R^m(A) \hookrightarrow \mathbb{P}_R(A) \xrightarrow{\mu} A. \tag{2.1.3}$$

More generally, for each $\alpha \in \pi_{d+i} \mathbb{P}_R^m(\Sigma^d R)$ with d, $i \in \mathbb{Z}$, we have an operation

$$Q_\alpha \colon\ \pi_d A \longrightarrow \pi_{d+i} A$$

from a representative

$$f_\alpha \colon\ \Sigma^{d+i} R \longrightarrow \mathbb{P}_R^m(\Sigma^d R) \cong R \wedge B\Sigma_m^{dV_m} \tag{2.1.4}$$

where $B\Sigma_m^{dV_m}$ is the Thom spectrum of a virtual bundle with $V_m = \mathbb{R}^m$ equipped with the Σ_m-action given by permuting coordinates.

As before, the total power operations P^m are multiplicative, but not additive in general; the individual power operations Q_α may not be additive or multiplicative. To build additive operations, we take quotients by the transfer ideal

$$I \coloneqq \bigoplus_{0<i<m} \operatorname{image}\Big(\pi_0\big(A^{B(\Sigma_i \times \Sigma_{m-i})^+}\big) \xrightarrow{\text{transfer}} \pi_0\big(A^{B\Sigma_m^+}\big)\Big), \tag{2.1.5}$$

that is, we define additive total power operations as ring homomorphisms

$$\psi^m \colon\ \pi_0 A \xrightarrow{P^m} \pi_0\big(A^{B\Sigma_m^+}\big) \to \pi_0\big(A^{B\Sigma_m^+}\big)/I. \tag{2.1.6}$$

From these we can then define additive individual power operations as above. In particular, for any space X, taking $A = R^{(\Sigma^\infty_+ X)}$ we get operations on R-cohomology of spaces.

2.2 How power operations fit together

Let R be a commutative S-algebra. For a commutative R-algebra A, we have seen that

$$\mathbb{P}_R(-) = \bigvee_{m\geq 0} \mathbb{P}^m_R(-)$$

is a monad in Mod_R over which A is an algebra. In particular, for any integers d and i, each $\alpha \in \pi_{d+i}\mathbb{P}^m_R(\Sigma^d R) \cong R_{d+i}(B\Sigma^{dV_m}_m)$ gives rise to a power operation

$$Q_\alpha \colon \pi_d A \longrightarrow \pi_{d+i} A.$$

Under the action of power operations, the homotopy groups $\pi_* A = A_*$ is an algebra over an operad[1] in R_*-modules involving the structure of $R_* B\Sigma_m$ for all m. This operad, traditionally called a *Dyer-Lashof algebra*, encodes all power operations on the homotopy groups of commutative R-algebras. It can be thought of as coming from the operad underlying the monad $\mathbb{P}_R$, as we take homotopy groups of the algebras over the latter. For a specific R, the structure maps of an algebra over this Dyer-Lashof algebra can be described explicitly in terms of generators and relations (see Example 2.2.9).

Following [34], instead of operads, we use *algebraic theories* (see [37] and [38, Chapter 3]) as an organizing principle for understanding the structure among power operations. They are amenable to the treatment of gradings (see [22]) and also to the study of homological-algebra properties of the collection of power operations (see [39]).

Definition 2.2.1. An *(algebraic) theory* is a category T with object set $\{T^0, T^1, T^2, \ldots\}$, together with a canonical map $T^0 \to T^1$, and *projection maps* $\pi_i \colon T^n \to T^1$ for all $n \geq 1$, $1 \leq i \leq n$ such that

$$T(T^k, T^n) \xrightarrow{\pi_i} \prod_{i=1}^{n} T(T^k, T^1)$$

[1] See, for example, [36, Sections 1.1.2-3] for an exposition of operads and monads.

is a bijection for all k and n, i.e., T^n is the n-fold product of T^1.

A *morphism of theories* is a functor $\phi\colon R \to T$ which preserves the product structure of a theory, i.e.,

$$\phi(R^k) = T^k \qquad \text{and} \qquad \phi(R^k \xrightarrow{\pi_i} R^1) = T^k \xrightarrow{\pi_i} T^1.$$

Definition 2.2.2. A *model* of a theory T (or *T-model*) is a functor $A\colon T \to \mathrm{Set}$ which preserves finite products.

We can think of a model of T as an underlying set $X = A(T^1)$ together with operations $P_f\colon X^k \to X$ for each $f \in T(T^k, T^1)$ (these determine all the other operations $X^k \to X^n$ with $n > 1$). In particular, a *free model* with n generators is the model $F_T(n)$ defined on objects by

$$F_T(n)(T^m) \coloneqq T(T^n, T^m).$$

We write Model_T for the category of models of T.

Example 2.2.3. Let R be a commutative ring. Let F be the full subcategory of the category of commutative R-algebras having as objects $\{F_0, F_1, F_2, \ldots\}$ where $F_0 = R$ and $F_n = R[x_1, \ldots, x_n]$ for $n \geq 1$. We then have the theory of commutative R-algebras $C_R = F^{\mathrm{op}}$, with projection maps

$$\begin{aligned} \pi_i\colon R[x_1, \ldots, x_n] &\longrightarrow R[x_1] \\ x_i &\mapsto x_1, \\ x_j &\mapsto 0, \qquad j \neq i. \end{aligned}$$

Definition 2.2.4. A *commutative operation theory* (COT) is a triple (T, R, ϕ) consisting of a theory T, a commutative ring R, and a morphism $\phi\colon C_R \to T$ of theories, such that the induced functor $\phi^*\colon \mathrm{Model}_T \to \mathrm{Model}_{C_R}$ commutes with finite coproducts.

In other words, if T is a COT, every T-model has an underlying structure of a commutative R-algebra, and coproducts in Model_T are computed as tensor products over R (we will use $\otimes$ when writing coproducts). We denote by $R\{x_1, \ldots, x_n\}$ a free T-model with n generators, and we have

$$R\{x_1, \ldots, x_n\} \cong R\{x_1\} \otimes_R \cdots \otimes_R R\{x_n\}.$$

We next introduce grading to a theory.

Definition 2.2.5. Let C be a fixed set, called the set of *colors*. Let $\mathbb{N}[C]$ be the free commutative monoid on C. A *C-graded theory* T is a category with object set $\{T^n\}_{n\in\mathbb{N}[C]}$, together with, for each $n = \sum_{c\in C} n_c[c] \in \mathbb{N}[C]$, a specified identification of T^n with the product $\prod_{c\in C}(T^{[c]})^{n_c}$.

In particular, given a $\mathbb{Z}$-graded theory T and a graded-commutative ring R_*, we can define a graded COT as a triple (T, R_*, ϕ) similarly as above (the theory C_{R_*} of graded-commutative R_*-algebras is equipped with the graded tensor product). Given a T-model A, we write A_c for the piece in grading c of the model.

For a graded COT (T, R_*, ϕ), and free models $R_*\{x\}$ and $R_*\{x_1, x_2\}$ with $|x| = |x_1| = |x_2| = c$, let $\mathcal{A}(c, d)$ be the set of elements $f \in R_*\{x\}_d = T(T^{[c]}, T^{[d]})$ which are primitive under the comultiplication

$$R_*\{x\} \xrightarrow{x \mapsto x_1+x_2} R_*\{x_1, x_2\},$$

that is,

$$f \longmapsto f \otimes 1 + 1 \otimes f. \tag{2.2.1}$$

Such $f \in \mathcal{A}(c, d)$ give rise to additive maps $A_c \to A_d$ natural in A. In particular $x \in R_*\{x\}_c$ corresponds to the identity map on A_c. Thus we obtain a category $\mathcal{A}$ of additive operations whose object set is $\mathbb{Z}$, the set of colors of our graded COT.

Example 2.2.6. Let $O_{H\mathbb{F}_p}$ be the $\mathbb{Z}$-graded COT T given by

$$\begin{aligned} &T(T^{[c_1]+\cdots+[c_m]}, T^{[d_1]+\cdots+[d_n]}) \\ \coloneqq\ &[K(\mathbb{F}_p, c_1) \times \cdots \times K(\mathbb{F}_p, c_m), K(\mathbb{F}_p, d_1) \times \cdots \times K(\mathbb{F}_p, d_n)], \end{aligned}$$

the set of homotopy classes of maps between products of Eilenberg-Mac Lane spaces, where by convention $K(\mathbb{F}_p, c) = *$ for $c < 0$. Then $\mathrm{Model}_{O_{H\mathbb{F}_p}}$ is the category of unstable algebras over the mod-p Steenrod algebra (this is a restatement of results of Serre [8] and Cartan [40]; see [6, Section II.5]). We have $\mathcal{A}(c, d)$ as the set of additive operations $H^c(-; \mathbb{F}_p) \to H^d(-; \mathbb{F}_p)$. In particular, for $p = 2$, the additive operations $H^c(-; \mathbb{F}_2) \to H^*(-; \mathbb{F}_2)$ are linear combinations of monomials which are admissible

composites of Steenrod operations Sq^i having excess less than c (see [8, Theorem 2 of Section 4] and [41, Chapters 3 and 9]).

Having the COT describing cohomology operations for spaces, we next consider one describing operations for spectra.

Definition 2.2.7. Given a commutative S-algebra R, the *Dyer-Lashof theory* DL_R is the $\mathbb{Z}$-graded theory T defined by

$$\begin{aligned} &T(T^{[c_1]+\cdots+[c_m]}, T^{[d_1]+\cdots+[d_n]}) \\ &\coloneqq h\mathrm{Alg}_R\Big(\mathbb{P}_R\big(R\wedge(S^{d_1}\vee\cdots\vee S^{d_n})\big), \mathbb{P}_R\big(R\wedge(S^{c_1}\vee\cdots\vee S^{c_m})\big)\Big) \end{aligned}$$

where $h\mathrm{Alg}_R$ denotes the homotopy category of commutative R-algebras.

Free DL_R-models are given by

$$F_T([c_1]+\cdots+[c_m])_d = \pi_d\mathbb{P}_R\big(R\wedge(S^{c_1}\vee\cdots\vee S^{c_m})\big).$$

If $\pi_*\mathbb{P}_R(R\wedge S^c)$ are flat as π_*R-modules, DL_R turns out to be a COT (see [34, Lemma 7.5]).

Remark 2.2.8. The significance of DL_R is that it describes *all* homotopy operations on commutative R-algebras (as natural transformations of the functors $\pi_i(-)$):

$$T(T^{[c]}, T^{[d]}) = h\mathrm{Alg}_R\big(\mathbb{P}_R(R\wedge S^d), \mathbb{P}_R(R\wedge S^c)\big) = \{\pi_c(-)\to\pi_d(-)\}.$$

In particular, as in Section 2.1, the R-cohomology of a space X admits the structure of a DL_R-model via taking homotopy groups of the commutative R-algebra $R^{(\Sigma^\infty_+X)}$. More examples of DL_R-models are discussed in [34, Section 9.1].

Example 2.2.9. Let P be a ring containing $\mathbb{F}_p$, and $R = HP$ be the corresponding Eilenberg-Mac Lane spectrum. By a calculation, $\pi_*\mathbb{P}_R(R\wedge S^c)$ is a free graded P-module for all c (see [34, pp 33-34] for $p=2$, and [34, Section 12] for p odd). Thus DL_R is a COT.

For $p=2$, we can describe DL_R explicitly as follows (cf. [13, VIII.3.3 and IX.2.1] and [34, Section 10]). A DL_R-model is a graded-commutative P-algebra A_* equipped

with functions

$$Q^i\colon\ A_d \longrightarrow A_{d+i}$$

for all d, $i \in \mathbb{Z}$ such that the following relations hold:

(i) $Q^i(x) = x^2$ if $i = d$, and $Q^i(x) = 0$ if $i < d$;

(ii) $Q^i(x) = 0$ if $x \in P$ and $i \neq 0$;

(iii) $Q^i(x + y) = Q^i(x) + Q^i(y)$ for all i;

(iv) Adem relations

$$Q^iQ^j(x) = \sum_k \binom{k-j-1}{2k-i} Q^{i+j-k}Q^k(x)$$

for $i > 2j$;[2]

(v) Cartan formula

$$Q^i(xy) = \sum_k Q^{i-k}(x)Q^k(y).$$

The above relations turn out to characterize DL_R so that any theory whose models are described by these relations is isomorphic to DL_R (see [34, Sections 10 and 11]). In particular, for a space X, taking $R = H\mathbb{F}_2$ we recover on $H^*(X;\mathbb{F}_2) \cong \pi_{-*}\big(R^{(\Sigma^\infty_+ X)}\big)$ the Steenrod squares

$$\mathrm{Sq}^i = Q^{-i}\colon\ H^*(X;\mathbb{F}_2) \longrightarrow H^{*+i}(X;\mathbb{F}_2)$$

(cf. Example 2.2.6).

[2] The right-hand side of the above identity is a finite sum in view of (i).

Chapter 3

Power operations and subgroups of formal groups

3.1 Morava E-theories associated to formal groups

Recall from Section 1.1 that one organizing principle for understanding large-scale phenomena in modern stable homotopy theory is through the chromatic filtration. It corresponds to a stratification of the moduli stack of one-dimensional commutative formal groups into layers according to height. For complex-oriented cohomology theories, such as ordinary cohomology and complex K-theory, the formal groups arise in terms of formal group laws. These are formal power series that express the first Chern class of the tensor product of two line bundles in terms of the first Chern classes of the individual line bundles (see [42, Section 1]).

For each formal group law F of height $n < \infty$ over a perfect field k of characteristic p, there is a complete local ring $\mathrm{LT}(k, F)$, called the *Lubin-Tate ring*. It is universal among complete local rings with residue field k carrying a formal group law whose reduction to k is F. As k is perfect, we have an isomorphism

$$\mathrm{LT}(k, F) \cong \mathbb{W}(k)[\![u_1, \ldots, u_{n-1}]\!]$$

(see [43] and [44, Sections 4.3 and 4.5]). There is an E_∞-ring spectrum $E_n(k, F)$ whose homotopy groups are $\mathrm{LT}(k, F)[u^{\pm 1}]$ with $|u| = 2$ (see [45, Corollary 7.6]). This is the

Morava E-theory spectrum associated to F, and we call it a Morava E-theory spectrum *of height n at the prime p.*

Closely related to Morava E-theories are *Johnson-Wilson theories* $E(n)$ and *Morava K-theories* $K(n)$ for all $n \geq 0$, with

$$\pi_* E(n) \cong \mathbb{Z}_{(p)}[v_1, \ldots, v_n, v_n^{-1}] \qquad \text{and} \qquad \pi_* K(n) \cong \mathbb{F}_p[v_n, v_n^{-1}]$$

where $|v_i| = 2(p^i - 1)$ and by convention $v_0 = p$. They are particularly useful when we study specific layers in the chromatic filtration through *Bousfield localization* (see [17, Chapter 7] and [46, Lectures 20-23]). In [47], for each generalized homology theory E, Bousfield defines an idempotent functor L_E on the stable homotopy category whose image is equivalent to the category of fractions defined by Adams in [48, Section III.14].

Given the connection to the moduli stack of formal groups via formal group laws, we can think of the stable homotopy category as approximated by a category of quasi-coherent sheaves on a moduli stack $\mathcal{M}$ which has a sequence of open substacks $\mathcal{M}(n)$. The Bousfield localization $L_{E(n)}$ can be thought of as restricting to the open substack $\mathcal{M}(n)$. The difference $\mathcal{M}(n) \setminus \mathcal{M}(n-1)$ between two adjacent layers is a closed substack of $\mathcal{M}(n)$, and $L_{K(n)}$ acts as completing along this closed substack. Roughly speaking, $L_{K(n)}$ has the effect of isolating height-n phenomena, and $L_{E(n)}$ sees all phenomena of height n and lower. Thus to understand the stable homotopy category, we can first examine one chromatic layer at a time and do specific calculations for $K(n)$-localizations. Then we need to understand how to patch these together into the $E(n)$-localizations, and we need to understand the "chromatic convergence," that is, how to take the limit as n goes to infinity.

In the chromatic filtration, ordinary cohomology with rational coefficients lives over the open substack $\mathcal{M}(0)$, and p-adic K-theory lives over $\mathcal{M}(1)$. The open substack $\mathcal{M}(2)$ is where elliptic cohomology theories are concentrated. An elliptic cohomology theory has its associated formal group equipped with a chosen isomorphism to the formal completion of an elliptic curve at the identity. More precisely we have the following definition (cf. [49, Definition 1.2] and [21, Definition 1.2]).

Definition 3.1.1. An *elliptic cohomology theory* consists of the following data:

(i) a commutative ring S,

(ii) an elliptic curve C over S,

(iii) a multiplicative cohomology theory E which is even and weakly periodic, i.e., the natural map

$$E^2(*) \otimes_{E^0(*)} E^n(*) \longrightarrow E^{n+2}(*)$$

is an isomorphism for all $n \in \mathbb{Z}$,

(iv) an isomorphism $E^0(*) \cong S$ and an isomorphism $\operatorname{Spf} E^0(\mathbb{CP}^\infty) \cong \widehat{C}$ of formal groups over $E^0(*) \cong S$.

As an algebraic invariant attached to topological spaces, an elliptic cohomology theory records information about elliptic curves and integral modular forms (cf. [50, Section 2]). In particular, as we will see in Chapter 5, power operations in such a cohomology theory encode moduli problems of elliptic curves, specifically cyclic isogenies of the corresponding power.

3.2 The Dyer-Lashof theories associated to Morava E-theories

For a commutative S-algebra R, we have seen in Section 2.2 that the Dyer-Lashof theory DL_R models all the algebraic structure naturally adhering to the homotopy groups of commutative R-algebras (cf. Remark 2.2.8). For a Morava E-theory spectrum E, we modify Definition 2.2.7 of its associated Dyer-Lashof theory by applying a certain localization to have good values of $E_*B\Sigma_m$ (cf. [34, Sections 13-15] and [22, Section 3]). The free model with one generator is

$$E_*\{x_c\} \coloneqq \bigoplus_{m\geq 0} E_*^\wedge(B\Sigma_m^{cV_m}) \tag{3.2.1}$$

where $E_*^\wedge(-)$ reflects the localization. We need to be slightly careful about this localization, as it does not preserve homotopy colimits; see [29, Sections 2-3], [51, Section 8], and [52] for details. Henceforth the Dyer-Lashof theory DL_E associated to a Morava E-theory E will refer to this modified version.

When E represents a Morava E-theory at the prime p, it is a theorem of Rezk [22, Theorem A] that under a congruence criterion, p-torsion-free commutative monoid

objects in graded modules over a certain associative ring Γ_E can be identified with DL_E-models. We may call Γ_E a "Dyer-Lashof algebra" as a workable object for organizing power operations in Morava E-theories. Based on this theorem, Rezk gives a description of the general pattern of power operations for Morava E-theories as below (cf. [30, 22]).

Let E be a Morava E-theory spectrum of height n at the prime p, and A be a $K(n)$-local[1] commutative E-algebra. The Dyer-Lashof algebra Γ associated to E has the structure of a *twisted bialgebra over* E_0, defined as follows, which can be thought of as a Hopf algebra over E_0 without E_0 being central.

Definition 3.2.1. Let R be a commutative ring. A *twisted bialgebra over* R consists of the following data:

(i) an associative ring Γ,

(ii) a map $\eta\colon R \to \Gamma$ of rings,

(iii) a map $\epsilon\colon \Gamma \to R$ of left R-modules such that $\epsilon\big(\eta(r)\big) = r$ for all $r \in R$ and $\epsilon(xy) = \epsilon\big(x \cdot \eta\epsilon(y)\big)$ for all $x, y \in \Gamma$,

(iv) a *2-multimorphism* $\Delta\colon \Gamma \to {}_R\Gamma \otimes {}_R\Gamma$ *of* R*-bimodules*[2] which is coassociative and cocommutative with counit ϵ such that

$$\Delta(xy) = \sum x'_i y'_j \otimes x''_i y''_j$$

where $\Delta(x) = \sum_i x'_i \otimes x''_i$ and $\Delta(y) = \sum_j y'_j \otimes y''_j$.

Let Γ be a twisted bialgebra over a commutative ring R. By Γ-*module*, we mean a left Γ-module. It is automatically an R-module via the ring homomorphism $\eta\colon R \to \Gamma$. The category of Γ-modules is symmetric monoidal, with the Γ-module structure on a tensor product $M \otimes_\Gamma N$ given by a Cartan formula

$$x \cdot (m \otimes_\Gamma n) \coloneqq \sum_i x'_i m \otimes_R x''_i n$$

[1] We need A to be $K(n)$-local due to the localization applied in the E-Dyer-Lashof theory mentioned above.

[2] Here ${}_R\Gamma \otimes {}_R\Gamma \coloneqq (\Gamma \otimes \Gamma)/(rx \otimes y \sim x \otimes ry)$. It admits a left R-module structure given by $r \cdot (x \otimes y) \coloneqq rx \otimes y = x \otimes ry$ and two right R-module structures given by $(x \otimes y) \cdot r \coloneqq xr \otimes y$ and $(x \otimes y) \cdot r \coloneqq x \otimes yr$. A *2-multimorphism* $\Gamma \to {}_R\Gamma \otimes {}_R\Gamma$ is a map which respects all these R-module structures.

for $m \in M$, $n \in N$, and $x \in \Gamma$ with $\Delta(x) = \sum_i x'_i \otimes x''_i$.

Definition 3.2.2. Let Γ be a twisted bialgebra over a commutative ring R. A Γ-*ring* is a commutative monoid object in the symmetrical monoidal category of Γ-modules. More explicitly, it is a commutative R-algebra M equipped with a Γ-module structure compatible with the R-module structure via $\eta\colon\ R \to \Gamma$ and satisfying

$$x \cdot (mn) = \sum_i (x'_i m)(x''_i n)$$

for m, $n \in M$ and $x \in \Gamma$ with $\Delta(x) = \sum_i x'_i \otimes x''_i$.

Definition 3.2.3. Let Γ be a twisted bialgebra over E_0. An *amplified* Γ-*ring* is a Γ-ring B equipped with a map $\theta\colon\ B \to B$ such that

$$\phi(b) = b^p + p\theta(b) \tag{3.2.2}$$

for all $b \in B$, where $\phi \in \Gamma$ is a representative of the *Frobenius class*.[3] Moreover, we require that all the identities necessarily satisfied by θ on a p-torsion-free Γ-ring, imposed via (3.2.2) by the Γ-module structure on B, remain true for B not necessarily p-torsion free.

With the above definitions, A_0 can be described as an amplified Γ-ring with Γ a twisted bialgebra over E_0. This Dyer-Lashof algebra Γ accounts for power operations on A_0. To get power operations in higher-degree E-cohomology and a description of the power operation structure on A_*, recall from Section 3.1 that Morava E-theories are even-periodic ($E_* \cong \mathrm{LT}(k, F)[u^{\pm 1}]$ with $|u| = 2$). We use this property and follow the treatment of gradings in [22, Section 2].

Let $(\mathcal{C}, \otimes, \kappa)$ be an additive tensor category, i.e., an additive category $\mathcal{C}$ equipped with a symmetric monoidal tensor product $\otimes$ and a unit object κ such that $\otimes$ distributes over finite sums. Given objects M and N of $\mathcal{C}$, let $\tau_{M,N}\colon\ M \otimes N \to N \otimes M$ denote the interchange isomorphism of the symmetric monoidal structure on $\mathcal{C}$. We say that an object ω of $\mathcal{C}$ is *symmetric* if $\tau_{\omega,\omega} = \mathrm{id}_{\omega\otimes\omega}$.

[3] This is a conjugacy class in $\Gamma/p\Gamma$ corresponding to the homomorphism $\phi^*\colon\ E^0 B\Sigma_p/I \to E^0/pE^0$, with I the transfer ideal, which represents a universal Frobenius isogeny (cf. (3.4.1) below, and see [22, 10.3-5]). Examples are given in [26, 2.6] and Proposition 5.2.3 (vi).

Let ω be a symmetric object of $\mathcal{C}$. We define the *ω-twisted $\mathbb{Z}/2$-graded category associated to $\mathcal{C}$* as follows.

Definition 3.2.4. Let $\mathcal{C}^*$ be the category whose objects are pairs $M^* = \{M^0, M^1\}$ of objects of $\mathcal{C}$, and whose morphisms are given componentwise, i.e., a morphism $f\colon\ M^* \to N^*$ is a pair $\{f^i\colon\ M^i \to N^i,\ i = 0, 1\}$ of morphisms of $\mathcal{C}$.

There is an induced additive tensor category structure on $\mathcal{C}^*$, twisted by ω, with a symmetric monoidal tensor product $\circledast$ given by

$$(M^* \circledast N^*)^0 \coloneqq (M^0 \otimes N^0) \oplus (M^1 \otimes N^1 \otimes \omega),$$
$$(M^* \circledast N^*)^1 \coloneqq (M^0 \otimes N^1) \oplus (M^1 \otimes N^0),$$

and a unit object $\kappa^* \coloneqq \{\kappa, 0\}$.

Example 3.2.5. Let $\mathcal{C}$ be the category of E_0-modules, and ω be $\pi_2 E \cong \widetilde{E}^0 S^2$ viewed as a free E_0-module with one generator u. Since u is invertible in E_*, ω is invertible in $\mathcal{C}$ with respect to the symmetric monoidal tensor product. Thus there is an equivalence between the category of E_*-modules and the ω-twisted $\mathbb{Z}/2$-graded category $\mathcal{C}^*$: it associates to a $\mathbb{Z}$-graded E_*-module M_* the object $\{M_0, M_{-1}\}$ of $\mathcal{C}^*$ (see [22, 2.9-10]).

Now let $\mathcal{C}$ be the category of Γ-modules, and ω be $\pi_2 E \cong \widetilde{E}^0 S^2$. Since ω is free of rank 1 as an E_0-module, it is a symmetric object in $\mathcal{C}$. The following theorem of Rezk describes the general pattern of power operations for a Morava E-theory E of height n at the prime p.

Theorem 3.2.6 (Rezk, cf. [30, 22])**.** *Let A be a $K(n)$-local commutative E-algebra. Then A_* has the structure of an ω-twisted $\mathbb{Z}/2$-graded amplified Γ-ring.*

We will give a proof of this theorem, at height 2 for the prime 3, in Section 5.3 (see Theorem 5.3.2). Below is an explicit description of Γ and ω for a Morava E-theory E of height 2 at the prime 2 given by Rezk [26, Section 2].

Example 3.2.7. Define Γ to be the associative ring generated over $\mathbb{Z}[a]$ by elements Q_0, Q_1, and Q_2 subject to the following relations: the Q_i's commute with elements in

$\mathbb{Z} \subset \mathbb{Z}[a]$, and satisfy *commutation relations*

$$\begin{aligned} Q_0 a &= a^2 Q_0 - 2aQ_1 + 6Q_2, \\ Q_1 a &= 3Q_0 + aQ_2, \\ Q_2 a &= -aQ_0 + 3Q_1, \end{aligned}$$

and *Adem relations*

$$\begin{aligned} Q_1 Q_0 &= 2Q_2 Q_1 - 2Q_0 Q_2, \\ Q_2 Q_0 &= Q_0 Q_1 + aQ_0 Q_2 - 2Q_1 Q_2. \end{aligned}$$

Define ω as a Γ-module, compatible with its E_0-module structure, such that

$$\begin{aligned} Q_0 \cdot u &\coloneqq 0, \\ Q_1 \cdot u &\coloneqq -u, \\ Q_2 \cdot u &\coloneqq 0. \end{aligned}$$

In general, for a Morava E-theory E associated to a formal group $\mathbb{G}$, it turns out that $\mathbb{G}$ produces Γ, in a sense which we will make precise in the next section. In particular, this leads to calculations of the explicit formulas in the above example, to be continued in Example 3.4.2.

3.3 From power operations to deformations of Frobenius

Let E be the Morava E-theory spectrum associated to a formal group $\mathbb{G}$ of height $n < \infty$ over a perfect field k of characteristic p.

Based on knowledge of E, we study the structure of the Dyer-Lashof theory DL_E. We restrict our attention to the degree-0 part DL_{E_0} of DL_E. We can translate operations in higher degree E-cohomology to degree 0 by working with higher sphere spectra (cf. (2.1.4)); even better, Morava E-theories are even-periodic, so that a lot of operations are already determined by those in degree 0 (cf. Theorem 3.2.6).

To understand the structure of DL_{E_0}, the main input comes from deformations of Frobenius. In particular, when the E-theory is an elliptic cohomology theory, deformations of Frobenius are parametrized by finite flat subgroups of the formal group of the

associated elliptic curve, and thus we may study power operations by doing calculations with elliptic curves. Also the Serre-Tate theorem (Theorem 4.3.1) states that p-adically the deformation theory of an elliptic curve is equivalent to the deformation theory of its p-divisible group. As Morava E-theories are associated to the latter, this important result enables our approach to power operations in elliptic cohomology.

First we consider additive power operations.

Let $\mathcal{A}$ be the set of additive elements (see (2.2.1)) in

$$E_0\{x\} = \bigoplus_{m\geq 0} E_0^\wedge B\Sigma_m,$$

the free DL_{E_0}-model with one generator (cf. (3.2.1)). Write $\mathcal{A}_{[m]} \subset E_0^\wedge B\Sigma_m$ for the summand of $\mathcal{A}$, and write $\mathcal{A}_r \coloneqq \mathcal{A}_{[p^r]}$. It turns out that $\mathcal{A}_{[m]} = 0$ unless $m = p^r$ for some r (cf. [29, Lemma 8.10]). Thus $\mathcal{A} = \bigoplus_{r\geq 0} \mathcal{A}_r$ is an associative (not necessarily commutative) graded ring with respect to the product given by "composition of operations," with the unit element given by the generator $x \in E_0\{x\}$ representing the identity operation. Moreover, the category $\mathrm{Mod}_{\mathcal{A}}$ of left $\mathcal{A}$-modules naturally admits a tensor product which makes it into a symmetric monoidal category (see [34, Proposition 7.6]).

We formulate a category equivalent to $\mathrm{Mod}_{\mathcal{A}}$, which is specific to Morava E-theories, using deformations of Frobenius.

Let R be a complete local ring containing $\mathbb{F}_p$. Given an R-algebra A, let $\mathrm{Frob}^*\colon\ \sigma^*A \to A$ be the unique map of R-algebras that fits into the diagram

$$\begin{array}{ccccc} R & \xrightarrow{\sigma} & R & = & R \\ \downarrow & & \downarrow & & \downarrow \\ A & \longrightarrow & \sigma^*A & \xrightarrow{\mathrm{Frob}^*} & A \end{array} \qquad (3.3.1)$$

where σ sends an element to its p'th power, and the left-hand square is a pushout of rings. In particular, if G is a formal group over R, there is an isogeny $\mathrm{Frob}\colon\ G \to \sigma^*G$ of formal

groups over R defined by $\mathrm{Frob}^*\colon \mathcal{O}_{\sigma^*G} = \sigma^*\mathcal{O}_G \to \mathcal{O}_G$ which is the R-homomorphism

$$\begin{aligned} R[\![y]\!] &\longrightarrow R[\![x]\!] \\ y &\mapsto x^p. \end{aligned}$$

The Frobenius can be defined more generally for any complete local ring R with maximal ideal $\mathfrak{m}$ (and R-algebras), by imposing the above commutative diagram on their mod-p reductions. This is indeed the generality we will be working with henceforth. Our restricted first definition is simply for the clarity of exposition.

Let $\pi\colon R \to R/\mathfrak{m}$ be the natural quotient map. A *deformation of* $\mathbb{G}$ *to* R is a triple (G, i, α) consisting of a formal group G over R, an inclusion $i\colon k \to R/\mathfrak{m}$, and an isomorphism $\alpha\colon \pi^*G \to i^*\mathbb{G}$ of formal groups over $R/\mathfrak{m}$. Thus we have a diagram

$$\begin{array}{ccccccc} G & \longleftarrow & \pi^*G & \xrightarrow[\sim]{\alpha} & i^*\mathbb{G} & \longrightarrow & \mathbb{G} \\ \downarrow & \urcorner & \downarrow & & \downarrow & \ulcorner & \downarrow \\ \operatorname{Spec} R & \xleftarrow{\pi} & \operatorname{Spec} R/\mathfrak{m} & = & \operatorname{Spec} R/\mathfrak{m} & \xrightarrow{i} & \operatorname{Spec} k. \end{array}$$

We will simply write π^*G as G_0, i.e., the special fiber of G as a formal scheme over R. Similarly, given an isogeny ϕ of formal groups, we write ϕ_0 for the induced isogeny on the special fibers. A $\star$-*isomorphism* $(G, i, \alpha) \to (G', i', \alpha')$ is an isomorphism $\phi\colon G \to G'$ of formal groups over R such that $i' = i$ and $\alpha' \circ \phi_0 = \alpha$.

We define the *category of deformations of Frobenius over* R as follows.

Definition 3.3.1. Let $\mathrm{DefFrob}_{\mathbb{G}}(R)$ be the category whose objects are deformations of $\mathbb{G}$ to R, and whose morphisms are isogenies which are *deformations of Frobenius*, i.e., a morphism $(G, i, \alpha) \to (G', i', \alpha')$ is an isogeny $\phi\colon G \to G'$ such that $i' = \sigma^r \circ i$ and $\alpha' \circ \phi_0 = \mathrm{Frob}^r \circ \alpha$ for some $r \geq 0$.

Remark 3.3.2. In the above definition, when $r = 0$, a morphism $(G, i, \alpha) \to (G', i', \alpha')$ is precisely a $\star$-isomorphism.

We then consider the category of sheaves of modules on $\mathrm{DefFrob}_{\mathbb{G}} \coloneqq \{\mathrm{DefFrob}_{\mathbb{G}}(R)\}$.

Definition 3.3.3. Define a category $\mathrm{Mod}_{\mathrm{DefFrob}_{\mathbb{G}}}$ as follows. An object $\mathcal{F}$ of this category consists of the following data:

(i) for each complete local ring R, a functor

$$\mathcal{F}_R\colon \operatorname{DefFrob}_{\mathbb{G}}(R)^{\mathrm{op}} \longrightarrow \operatorname{Mod}_R,$$

(ii) for each local homomorphism $f\colon R \to S$, a natural isomorphism

$$\mathcal{F}_f\colon f^*\mathcal{F}_R \longrightarrow \mathcal{F}_S\, f^*$$

where the first f^* is the functor $\operatorname{Mod}_R \to \operatorname{Mod}_S$ of extending scalars along f, and the second $f^*\colon \operatorname{DefFrob}_{\mathbb{G}}(R)^{\mathrm{op}} \to \operatorname{DefFrob}_{\mathbb{G}}(S)^{\mathrm{op}}$ is induced by f ($\operatorname{DefFrob}_{\mathbb{G}}(-)$ is a functor),

together with natural isomorphisms

$$\mathcal{F}_{\mathrm{id}} \cong \mathrm{id} \qquad \text{and} \qquad \mathcal{F}_{gf} \cong \mathcal{F}_g(f^*) \circ g^*(\mathcal{F}_f)$$

for all local homomorphisms $\mathrm{id}\colon R \to R$, $f\colon R \to S$, and $g\colon S \to T$.

A morphism $\eta\colon \mathcal{F} \to \mathcal{G}$ in this category is a collection of natural transformations

$$\eta_R\colon \mathcal{F}_R \longrightarrow \mathcal{G}_R$$

together with natural isomorphisms

$$\mathcal{G}_f \circ f^*(\eta_R) \cong \eta_S(f^*) \circ \mathcal{F}_f.$$

Example 3.3.4. There is an object $\mathcal{O}$ of $\operatorname{Mod}_{\operatorname{DefFrob}_{\mathbb{G}}}$ described as follows. The functor $\mathcal{O}_R$ sends deformations to their base ring R, and sends morphisms between deformations to the identity map of R. The natural isomorphism $\mathcal{O}_f$ is determined by the isomorphism

$$\begin{aligned} R \otimes_R{}^f S &\longrightarrow S \\ r \otimes s &\mapsto f(r)s. \end{aligned}$$

The natural isomorphisms

$$\mathcal{O}_{\mathrm{id}} \cong \mathrm{id} \qquad \text{and} \qquad \mathcal{O}_{gf} \cong \mathcal{O}_g(f^*) \circ g^*(\mathcal{O}_f)$$

are determined respectively by the isomorphisms

$$\begin{array}{ccc} R \otimes_R{}^{\mathrm{id}} R \longrightarrow R & \text{and} & R \otimes_R{}^{gf} T \longrightarrow (R \otimes_R{}^{f} S) \otimes_S{}^{g} T. \\ r_1 \otimes r_2 \ \mapsto \ r_1 r_2 & & r \otimes t \ \mapsto \ (r \otimes 1) \otimes t \end{array}$$

Remark 3.3.5. The category $\mathrm{Mod}_{\mathrm{DefFrob}_{\mathbb{G}}}$ is symmetric monoidal with the tensor product $\mathcal{F} \otimes \mathcal{G}$ given by $(\mathcal{F} \otimes \mathcal{G})_R(G) \coloneqq \mathcal{F}_R(G) \otimes_R \mathcal{G}_R(G)$. The unit object is $\mathcal{O}$ in the above example.

Theorem 3.3.6 ([34, Pre-Theorem 16.4])**.** *There is an equivalence of symmetric monoidal categories*

$$\mathrm{Mod}_{\mathcal{A}} \xrightarrow{\sim} \mathrm{Mod}_{\mathrm{DefFrob}_{\mathbb{G}}}.$$

Next we consider $\mathrm{Model}_{\mathrm{DL}_{E_0}}$, the category of models for the theory DL_{E_0}, on which $\mathcal{A}$ acts. By [34, Proposition 7.6], there is a forgetful functor $\mathrm{Model}_{\mathrm{DL}_{E_0}} \to \mathrm{Mod}_{\mathcal{A}}$ along which the coproduct of DL_{E_0}-models and the tensor product of $\mathrm{Mod}_{\mathcal{A}}$ agree.

Definition 3.3.7. Define a category $\mathrm{Alg}_{\mathrm{DefFrob}_{\mathbb{G}}}$ as follows. An object $\mathcal{B}$ of this category is a ring object in $\mathrm{Mod}_{\mathrm{DefFrob}_{\mathbb{G}}}$ satisfying the *Frobenius congruence*, i.e., the diagram

$$\begin{array}{ccc} \sigma^* \mathcal{B}_R(G) & \xrightarrow[\sim]{\mathcal{B}_\sigma(G)} & \mathcal{B}_R \sigma^*(G) \\ & {\scriptstyle \mathrm{Frob}^*} \searrow & \downarrow {\scriptstyle \mathcal{B}_R(\mathrm{Frob})} \\ & & \mathcal{B}_R(G) \end{array}$$

commutes for all complete local rings R and deformations G of $\mathbb{G}$ to R.

Morphisms in this category are maps of ring objects.

An object $\mathcal{B}$ is said to be *torsion free* if $\mathcal{B}_R(G)$ is p-torsion free for every p-torsion-free R and every deformation G to R. We denote by $\mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_{\mathbb{G}}}$ the full subcategory of $\mathrm{Alg}_{\mathrm{DefFrob}_{\mathbb{G}}}$ consisting of torsion-free objects.

Remark 3.3.8. We note as in [22, 11.18] that roughly speaking, the Frobenius congruence is the requirement that $\mathcal{B}$ carry the (relative) Frobenius on formal groups to the (relative) Frobenius on algebras.

Here is the key result bridging power operations and deformations of Frobenius (cf. [22, Theorem B]).

Theorem 3.3.9 ([34, Pre-Theorem 16.5])**.** *There is a functor*

$$\mathrm{Model}_{\mathrm{DL}_{E_0}} \longrightarrow \mathrm{Alg}_{\mathrm{DefFrob}_{\mathbb{G}}}.$$

It restricts to an equivalence

$$\mathrm{Model}^{\mathrm{tf}}_{\mathrm{DL}_{E_0}} \xrightarrow{\sim} \mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_{\mathbb{G}}}$$

of full subcategories of torsion-free objects.

3.4 Deformations of Frobenius are parametrized by subgroups

Having identified the categories, we now analyze the essential data that are encoded in $\mathrm{Mod}_{\mathrm{DefFrob}_{\mathbb{G}}}$ and $\mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_{\mathbb{G}}}$, by studying the structure of the category $\mathrm{DefFrob}_{\mathbb{G}}(R)$ of deformations of Frobenius. This turns out to be parametrized by the finite flat subgroups of deformations of $\mathbb{G}$ to R, as we explain below.

Let x be a coordinate on a formal group G over R. A *degree-d subgroup K of G* is an effective Cartier divisor on G with $\mathcal{O}_K = R[\![x]\!]/\big(f(x)\big)$ for some monic polynomial $f(x)$ of order d such that

$$f(x_1 +_G x_2) \in \big(f(x_1),\ f(x_2)\big) \qquad \text{and} \qquad f(x) \in (x),$$

i.e., the group law of G restricts to K and K contains the identity. In particular K is finite and flat over R (we will assume finiteness and flatness of subgroups even when we do not mention their degrees). We have the *quotient group* G/K which is again a formal group (see [53, Section 5]).

One can show that the homomorphism $[d]\colon G \to G$ restricts to zero on K (see [54, Section 1]), i.e., $f(x)$ divides $[d](x)$. Thus subgroups of a formal group over a p-local ring must have degree p^r for some $r \geq 0$. In particular, if G is a formal group over a field k of characteristic p, there is exactly one subgroup of degree p^r, given by $f(x) = x^{p^r}$,

which is the kernel of the r-fold Frobenius isogeny Frob^r.

We have seen in Remark 3.3.2 that in $\mathrm{DefFrob}_{\mathbb{G}}(R)$ the degree-1 morphisms (when $r = 0$) are precisely the $\star$-isomorphisms of deformations. In general, with morphisms corresponding to all $r \geq 0$, $\mathrm{DefFrob}_{\mathbb{G}}(R)$ is equivalent to the following category (see [34, Proposition 16.9]). The objects of this category are $\star$-isomorphism classes of deformations $[G]$. The morphisms are $\star$-isomorphism classes of pairs $[G > K]$: the source of $[G > K]$ is $[G]$, and the target of $[G > K]$ is $[G/K]$ where G/K is a deformation of $\mathbb{G}$ with $i_{G/K} = \sigma^r \circ i_G$ (p^r being the degree of K). Moreover, by the Lubin-Tate theorem (see [43, Theorem 3.1] and [44, Section 4.3]), there is at most one $\star$-isomorphism between any two deformations. If $[G/K] = [G']$, then

$$[G' > K'] \circ [G > K] = [G > K'']$$

where K'' is the kernel of the composite

$$G \to G/K \cong G' \to G'/K'.$$

Thus we see that deformations of Frobenius with source (G, i, α) correspond precisely to subgroups of G.

Example 3.4.1. Let $\mathbb{G}$ be the multiplicative formal group over $\mathbb{F}_p$ (of height 1). For the multiplicative formal group $\widehat{\mathbb{G}}_m$ over a p-local ring R, since the formal group law is defined by

$$1 + (x_1 +_{\widehat{\mathbb{G}}_m} x_2) \coloneqq (1 + x_1)(1 + x_2),$$

we have

$$[p^r](x) = (1 + x)^{p^r} - 1,$$

which is a monic polynomial of order p^r. Thus the only subgroups of $\widehat{\mathbb{G}}_m$ are $\widehat{\mathbb{G}}_m[p^r]$ with $\mathcal{O}_{\widehat{\mathbb{G}}_m[p^r]} = \mathcal{O}_{\widehat{\mathbb{G}}_m}/\big([p^r](x)\big)$. Moreover, by the Lubin-Tate theorem (see [43, Theorem 3.1] and [44, Section 4.3]), every object of $\mathrm{DefFrob}_{\mathbb{G}}(R)$ is $\star$-isomorphic to $\widehat{\mathbb{G}}_m$, and the set of $\star$-isomorphism classes of deformations of $\mathbb{G}$ to R is classified by the ring $\mathcal{O}_{\mathrm{univ}} \coloneqq \mathbb{Z}_p$. In particular we can take the universal deformation G_{univ} to be the multiplicative formal group over $\mathbb{Z}_p$. Thus by functoriality, to describe an object $\mathcal{B}$ of $\mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_{\mathbb{G}}}$, it is enough to give the following data:

(i) a p-torsion free $\mathbb{Z}_p$-algebra $B = \mathcal{B}_{\mathbb{Z}_p}(\widehat{\mathbb{G}}_m)$,

(ii) maps $\psi^{p^r}\colon B \to B$ of $\mathbb{Z}_p$-algebras (corresponding to the isogenies $[p^r]\colon \widehat{\mathbb{G}}_m \to \widehat{\mathbb{G}}_m$) such that

- $\psi^1 = \mathrm{id}_B$ and $\psi^{p^r} \circ \psi^{p^s} = \psi^{p^{r+s}}$,
- $\psi^p(b) \equiv b^p \mod pB$ (the Frobenius congruence).

We note as in [22, Example 1.3] that the above is a "p-typicalization" of Wilkerson's theorem [55, Proposition 1.2] which characterizes torsion-free λ-rings in terms of the Adams operations satisfying the Frobenius congruences at all primes. More concretely, consider the complex K-theory spectrum KU (cf. Example 2.1.1). For $B = \pi_0 A$, where A is a p-complete KU-algebra (i.e., a commutative KU-algebra such that $A \cong A^\wedge_p$), ψ^p recovers the p'th Adams operation studied by McClure (see [13, Chapters VIII and IX]).

In general, consider the functor X_r which associates to a ring R the set of $\star$-isomorphism classes of pairs $[G > K]$ with K a degree-p^r subgroup of G. By [29, Theorem 9.2], it is represented by the complete local ring

$$\mathcal{O}_{X_r} \coloneqq E^0 B\Sigma_{p^r}/I$$

where

$$I \coloneqq \bigoplus_{0<i<p^r} \mathrm{image}\big(E^0 B(\Sigma_i \times \Sigma_{p^r-i}) \xrightarrow{\text{transfer}} E^0 B\Sigma_{p^r}\big)$$

is the transfer ideal (cf. (2.1.5)). This can be viewed as a generalization of the Lubin-Tate theorem for $\mathcal{O}_{\mathrm{univ}} = \mathcal{O}_{X_0}$. Moreover there are two ring homomorphisms

$$s^*,\ t^*\colon \mathcal{O}_{\mathrm{univ}} \longrightarrow \mathcal{O}_{X_r}$$

where s^* represents the source map $[G > K] \mapsto [G]$, and t^* represents the target map $[G > K] \mapsto [G/K]$. Thus to describe an object $\mathcal{B}$ of $\mathrm{Alg}^{\mathrm{tf}}_{\mathrm{DefFrob}_{\mathbb{G}}}$, it is enough to give the following data (subject to a set of formal properties):

(i) a p-torsion-free $\mathcal{O}_{\mathrm{univ}}$-algebra $B = \mathcal{B}_{\mathcal{O}_{\mathrm{univ}}}(G_{\mathrm{univ}})$,

(ii) maps $\psi^{p^r}\colon B \to B \otimes^{s^*}_{\mathcal{O}_{\text{univ}}} \mathcal{O}_{X_r}$ of $\mathcal{O}_{\text{univ}}$-algebras as the composites

$$B \to B \otimes^{t^*}_{\mathcal{O}_{\text{univ}}} \mathcal{O}_{X_r} \overset{\mathcal{B}_f}{\cong} \mathcal{B}_{\mathcal{O}_{X_r}}(t^*G_{\text{univ}}) \xrightarrow{\mathcal{B}_{\mathcal{O}_{X_r}}(\psi)} \mathcal{B}_{\mathcal{O}_{X_r}}(s^*G_{\text{univ}}) \overset{\mathcal{B}_g}{\cong} B \otimes^{s^*}_{\mathcal{O}_{\text{univ}}} \mathcal{O}_{X_r}$$

where $f = t^*$ and $g = s^*$ are local homomorphisms, and $\psi\colon s^*G_{\text{univ}} \to t^*G_{\text{univ}}$ is the universal deformation of Frob^r (see [53, Section 13]).

In particular, if we denote by ϕ^* the map

$$\mathcal{O}_{X_1} \longrightarrow \mathcal{O}_{\text{univ}}/p\mathcal{O}_{\text{univ}} \tag{3.4.1}$$

which represents a universal Frobenius isogeny, the Frobenius congruence amounts to requiring that

$$B \xrightarrow{\psi^p} B \otimes^{s^*}_{\mathcal{O}_{\text{univ}}} \mathcal{O}_{X_1} \xrightarrow{\text{id}\otimes\phi^*} B \otimes_{\mathcal{O}_{\text{univ}}} (\mathcal{O}_{\text{univ}}/p\mathcal{O}_{\text{univ}}) \cong B/pB \tag{3.4.2}$$

be the p'th-power map

$$B \to B/pB \xrightarrow{\sigma} B/pB$$

which sends b to $\overline{b}^p$.

In Example 3.4.1, $\mathcal{O}_{X_r} \cong \mathcal{O}_{\text{univ}}$ for all r, that is,

$$E^0 B\Sigma_{p^r}/I \cong E^0,$$

so that $s^* = t^* = \text{id}$. In fact this is true for any complex-oriented cohomology theory whose formal group is of height 1, as a height-1 formal group $\mathbb{G}$ has a unique degree-p^r subgroup $\mathbb{G}[p^r]$ (classified by $\mathcal{O}_{X_r}$) for each r. Thus by Theorem 3.3.9, the power operation structure on a $K(1)$-local Morava E-theory at the prime p is simple: the operation $\psi^p\colon E^0 \to E^0$, which is a lift of the Frobenius map, determines the other ψ^{p^r} with $r > 1$ by iterated composition. In particular, when E_* is p-torsion free, ψ^p determines *all* the power operations so that E_* has the structure of a *free Frobenius algebra with one generator* on which ψ^p acts (cf. [56, Section 4]).

Here is an example for $\mathbb{G}$ of height 2 studied by Rezk [26].

Example 3.4.2. Consider the elliptic curve[4] $C_0 \subset \mathbb{P}^2_{\mathbb{F}_2}$ defined by

$$Y^2Z + YZ^2 = X^3,$$

which is supersingular so that its formal group $\widehat{C}_0$ is of height 2. It has a universal deformation C over the Lubin-Tate ring $\mathbb{W}(\mathbb{F}_2)[\![u_1]\!] \cong \mathbb{Z}_2[\![a]\!]$ given by

$$Y^2Z + aXYZ + YZ^2 = X^3$$

where a is the Hasse invariant (cf. [50, Proposition 3.2] and [23, 2.2.10]). Setting $a = 0$ we recover the supersingular elliptic curve C_0. Let E be the Morava E-theory spectrum associated to $\widehat{C}_0/\mathbb{F}_2$, so that

$$E_* \cong \mathbb{Z}_2[\![a]\!][u^{\pm 1}]$$

with $|u| = 2$.

By studying degree-2 subgroups of C, i.e., subgroups generated by 2-torsion points on C, Rezk identifies that

$$\mathcal{O}_{X_1} \cong \mathbb{Z}_2[\![a, d]\!]/(d^3 - ad - 2),$$

i.e., in the affine coordinate chart $\{u = X/Y, v = Z/Y\}$, degree-2 subgroups are generated by points Q of the form $\big(u(Q), v(Q)\big) = (d, -d^3)$ with $d^3 - ad - 2 = 0$. Thus there is a power operation

$$\psi^2 \colon E^0 \longrightarrow E^0[\![d]\!]/(d^3 - ad - 2).$$

Moreover, by studying the universal isogeny with source C and kernel the degree-2 subgroup generated by Q (cf. [57, Theorem 1.4]), Rezk computes that

$$t^*(a) = \psi^2(a) = a^2 + 3d - ad^2.$$

He also gives formulas for individual power operations Q_0, Q_1, and Q_2 which express

$$\psi^2(x) = Q_0(x) + Q_1(x)d + Q_2(x)d^2$$

[4] See, for example, Chapter 4 for some of the basics about elliptic curves.

(see Example 3.2.7). In particular the Frobenius congruence takes the form

$$Q_0(x) \equiv x^2 \mod 2.$$

Chapter 4

Subgroups of elliptic curves

We have seen in Section 3.1 that there is a connection between complex-oriented cohomology theories and one-dimensional commutative formal groups, via Chern classes of line bundles, which gives rise to the chromatic filtration. In particular the formal groups for ordinary cohomology and complex K-theory turn out to be the additive formal group $\widehat{\mathbb{G}}_a$ and the multiplicative formal group $\widehat{\mathbb{G}}_m$ respectively (see [42, Example 2.14, and Sections 1 and 7], and cf. Example 3.4.1). These are formal completions of one-dimensional group schemes. Apart from the additive and multiplicative groups, the only other possibility of a one-dimensional group scheme over an algebraically closed field is an elliptic curve (see [58, IV.1.6], and cf. [18, Section 12]).

Throughout this chapter we will use a specific example (starting as Example 4.1.5) to illustrate the theory related to subgroups of elliptic curves. Via the bridge discussed in Chapter 3 (particularly Theorem 3.3.9), the calculations we do with this example will be used for computing power operations in Chapter 5.

4.1 The group structure

Let S be a scheme. By a *smooth curve* E/S, we mean a smooth morphism

$$\pi\colon E \longrightarrow S$$

of relative dimension one which is separated and of finite presentation. An *elliptic curve* E/S is a proper smooth curve with geometrically connected fibers all of genus one together with a section $O \in E(S)$. There is a unique structure of commutative S-group scheme on E/S for which O is the identity (see [23, 2.1.2 and 2.5.1]), and thus the formal completion $\widehat{E}$ of E at O is a one-dimensional commutative formal group. As with subgroups of formal groups in Section 3.4, by a *degree-d subgroup* of an elliptic curve E/S we mean a closed subgroup scheme which is finite locally free of rank d over S (see [23, 1.2]).

Visibly (a fiber of) such a (relative) curve, with the group law on it, is depicted on the front cover of [59, second ed.]; the interested reader might also seek out Bryan Birch's birthday card. More concretely, we can describe an elliptic curve and do calculations with its group law using a *Weierstrass equation*.

Weierstrass equations

Locally on some affine open subset $\operatorname{Spec} R \subset S$, any elliptic curve E/S has a presentation as the locus in $\mathbb{P}^2_R$ of a Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{4.1.1}$$

where $a_i \in R$, with $O = [0, 1, 0]$. In the affine coordinate chart $\{x = X/Z, y = Y/Z\}$, this becomes

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.1.2}$$

with O at the infinity. Associated to E/R given as above, we have the following quantities (see Caution 4.1.1 below):

$$\begin{aligned} b_2 &\coloneqq a_1^2 + 4a_2, \\ b_4 &\coloneqq 2a_4 + a_1a_3, \\ b_6 &\coloneqq a_3^2 + 4a_6, \\ b_8 &\coloneqq a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta &\coloneqq -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ \omega &\coloneqq -\frac{dx}{2y + a_1x + a_3} = \frac{dy}{a_1y - 3x^2 - 2a_2x - a_4}. \end{aligned} \tag{4.1.3}$$

Here Δ is invertible in R so that E is smooth. The one-form ω is nowhere vanishing, and is invariant under translation by the group law on E. Locally it is an R-basis of the invertible sheaf

$$\underline{\omega}_{E/S} \coloneqq \pi_* \Omega_{E/S},$$

the pushforward along the structure morphism $\pi\colon E \to S$ of the relative cotangent sheaf $\Omega_{E/S}$, on which the multiplicative group $\mathbb{G}_m \coloneqq \operatorname{Spec} R[\lambda^{\pm 1}]$ acts by

$$\omega \longmapsto \lambda\omega. \tag{4.1.4}$$

This action lifts to one on E/R with

$$(x, y) \mapsto (\lambda^{-2}x, \lambda^{-3}y) \qquad \text{and} \qquad a_i \mapsto \lambda^{-i}a_i \ \text{ for all } \ i,$$

and we have a compatible grading with

$$|x| = 2, \qquad |y| = 3, \qquad \text{and} \qquad |a_i| = i.$$

Keeping track of this grading is helpful in calculations with elliptic curves. The only change of variables fixing O and preserving the form of (4.1.2) is

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + u^2sx' + t$$

where r, s, $t \in R$ and $u \in R^\times$.

When we study the formal completion of E at O, it is convenient to work in the affine coordinate chart $\{u = X/Y, v = Z/Y\}$ so that $O = (0, 0)$. In uv-coordinates, the Weierstrass equation (4.1.1) becomes

$$v + a_1uv + a_3v^2 = u^3 + a_2u^2v + a_4uv^2 + a_6v^3,$$

and we have

$$u = \frac{x}{y}, \quad v = \frac{1}{y}, \qquad \text{or} \qquad x = \frac{u}{v}, \quad y = \frac{1}{v},$$

with

$$|u| = -1 \qquad \text{and} \qquad |v| = -3.$$

In particular, the formal group $\widehat{E}$ has u as a coordinate which is *adapted to* ω in the sense that

$$\omega|_{\widehat{E}} = \big(1 + (\text{higher-order terms})\big)du \tag{4.1.5}$$

(cf. [59, IV.1]).

Caution 4.1.1. In some sources (e.g., [59, IV.1] and [60, Section 9]) the formulas for u and v, as well as that for ω, differ from ours by a minus sign.

Rigidity and duality

As a geometric manifestation of the group structure, the following rigidity property of elliptic curves is important to our later discussion (see Remark 4.1.4 and the proof of Proposition 4.4.7).

Theorem 4.1.2 ([23, 2.4.2])**.** *Let S be a scheme, E_1 and E_2 two elliptic curves over S, and $\phi\colon E_1 \to E_2$ an S-homomorphism. Then Zariski-locally on S, either $\phi = 0$ or ϕ is an* isogeny*, i.e., ϕ is finite locally free.*

Corollary 4.1.3. *Hypotheses and notations as in the above theorem, suppose S is connected. If $\phi_x\colon (E_1)_x \to (E_2)_x$ is zero for some $x \in S$ where $(-)_x$ denotes the fiber over x along the structure morphism, then $\phi = 0$.*

Remark 4.1.4. Some of the formulas involved in our later calculations with elliptic curves are in fact valid only fiber by fiber over the base scheme (for example, the group law algorithm in Example 4.1.5, the division polynomial ψ_3 in the proof of Proposition 4.2.3, Vélu's formulas in Example 4.4.13, and the changes of variables in Example 4.4.13 and in the proof of Proposition 4.5.11). As our base scheme is connected, the statements for elliptic curves over the entire base scheme follow by rigidity. We will write those formulas formally to streamline the exposition.

As a consequence of rigidity (essentially of the group structure), every isogeny $\phi\colon E_1 \to E_2$ of degree d over a connected base scheme S has a *dual isogeny* $\widehat{\phi}\colon E_2 \to E_1$ of the same degree such that $\widehat{\phi} \circ \phi = [d]$ (see [23, 2.6.1]). In particular, if $\phi\colon E \to E$ is an endomorphism, then in the endomorphism ring of E, ϕ is a root of the polynomial

$$X^2 - \operatorname{trace}(\phi) \cdot X + d = 0 \tag{4.1.6}$$

with $\mathrm{trace}(\phi) \coloneqq \phi + \widehat{\phi}$ an integer satisfying

$$\big(\mathrm{trace}(\phi)\big)^2 - 4d \leq 0$$

(see [23, 2.6.2.2 and 2.6.3]).

Calculations

Example 4.1.5. Consider the curve in $\mathbb{P}^2$ given by the affine equation

$$C\colon\ y^2 + axy + aby = x^3 + bx^2 \tag{4.1.7}$$

over $\mathbb{Z}[a,b]$. Not knowing if it is an elliptic curve, we compute formally according to (4.1.3) that

$$\begin{aligned} &b_2 = a^2 + 4b, \quad b_4 = a^2 b, \quad b_6 = a^2 b^2, \quad b_8 = a^2 b^3, \\ &\Delta = a^2 b^4 (a^2 - 16b), \\ &\omega = \ -dx/(2y + ax + ab) = dy/(ay - 3x^2 - 2bx). \end{aligned}$$

Thus C is an elliptic curve over the graded ring

$$S^\bullet \coloneqq \mathbb{Z}[1/4][a, b, \Delta^{-1}]$$

where $|a| = 1$ and $|b| = 2$. The invertibility of 4 in $S^\bullet$ allows us to characterize 4-torsion points on C as below.

Let $P_0 \coloneqq (0,0)$. Since from the formula for ω we have

$$\frac{dy}{dx} = \frac{3x^2 + 2bx - ay}{2y + ax + ab},$$

the tangent line of C at P_0 is $y = 0$. By the group law as geometrically depicted, $2P_0$ is then the other point where $y = 0$ and C intersect, namely, $(-b, 0)$. We compute that the tangent line at $2P_0$ is $x = -b$, and thus $4P_0$ is the identity O at the infinity. Conversely, as 4 is invertible in $S^\bullet$, any 4-torsion point P has the above property: the tangent line at P passes through a point P' such that the tangent line at P' is vertical.

In uv-coordinates, the equation (4.1.7) of C becomes

$$v + auv + abv^2 = u^3 + bu^2v. \tag{4.1.8}$$

In terms of an algorithm, the group law on C satisfies:

- given $P(u, v)$, the coordinates of $-P$ are

$$\left(-\frac{v}{u(u+bv)}, -\frac{v^2}{u^2(u+bv)}\right);$$

- given $P_1(u_1, v_1)$ and $P_2(u_2, v_2)$, the coordinates of $-(P_1 + P_2)$ are

$$u_3 \coloneqq ak - \frac{bm}{1+bk} - u_1 - u_2 \qquad \text{and} \qquad v_3 \coloneqq ku_3 + m$$

where

$$k = \frac{v_1 - v_2}{u_1 - u_2} \qquad \text{and} \qquad m = \frac{u_1v_2 - u_2v_1}{u_1 - u_2}.$$

Given $P(u, v)$ and $Q(d, e)$, with the above notations and formulas, we then have:

- set

$$(u_1, v_1) = \left(-\frac{v}{u(u+bv)}, -\frac{v^2}{u^2(u+bv)}\right) \qquad \text{and} \qquad (u_2, v_2) = (d, e)$$

so that

$$P - Q = (u_3, v_3);$$

- set

$$(u_1, v_1) = (u, v) \qquad \text{and} \qquad (u_2, v_2) = (d, e)$$

so that

$$P + Q = \left(-\frac{v_3}{u_3(u_3+bv_3)}, -\frac{v_3^2}{u_3^2(u_3+bv_3)}\right).$$

4.2 Torsion subgroups

In Example 4.1.5 we looked at a 4-torsion point P_0 on an elliptic curve C over a ring $S^\bullet$ where 4 is invertible. Here is the general structure of the subgroup of m-torsion points

on an elliptic curve (cf. [23, 2.3.2 and 12.2.6]).

Theorem 4.2.1 ([23, 2.3.1])**.** *Let S be a scheme, E/S an elliptic curve, and $m \geq 1$ an integer. Then the* multiplication-by-m *homomorphism*

$$[m]\colon E \longrightarrow E$$

over S is finite locally free of rank m^2. If m is invertible on S, its kernel $E[m]$ is finite étale over S, locally for the étale topology on S isomorphic to $\underline{\mathbb{Z}/m} \times \underline{\mathbb{Z}/m}$.

To compute an m-torsion point on an elliptic curve E over a field in the Weierstrass equation (4.1.2), with the quantities b_i as in (4.1.3), we introduce *division polynomials* (cf. [59, Exercise 3.7] and [61, 13(9.2-4)]).

Definition 4.2.2. Define polynomials $\psi_m \in \mathbb{Z}[a_1, \ldots, a_4, a_6, x, y]$, $m \geq 0$, using the initial values

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1x + a_3,\\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8,\\
\psi_4 &= \psi_2\big(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2\big),
\end{aligned}$$

and then inductively by the formulas

$$\begin{aligned}
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, && \text{for } m \geq 2,\\
\psi_2\psi_{2m} &= \psi_{m-1}^2\psi_m\psi_{m+2} - \psi_{m-2}\psi_m\psi_{m+1}^2, && \text{for } m \geq 3.
\end{aligned}$$

Define polynomials ϕ_m, $\omega_m \in \mathbb{Z}[a_1, \ldots, a_4, a_6, x, y]$, $m \geq 2$, by

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
2\psi_2\omega_m &= \psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

By [59, Exercise 3.7d and f], for $m \geq 2$ and any point $P(x, y)$ on E, we have

$$[m](x, y) = \left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right), \tag{4.2.1}$$

and ψ_m vanishes at precisely the nonzero m-torsion points.

Calculations

As a continuation of Example 4.1.5, we compute the nonzero 3-torsion points on the elliptic curve C.

Proposition 4.2.3. *On the elliptic curve C over $S^\bullet$, the uv-coordinates (d, e) of any nonzero 3-torsion point satisfy the identities*

$$f(d) = 0 \tag{4.2.2}$$

and

$$e = g(d) \tag{4.2.3}$$

where f, $g \in S^\bullet[u]$ are given by

$$\begin{aligned} f(u) &= b^4u^8 + 3ab^3u^7 + 3a^2b^2u^6 + (a^3b + 7ab^2)u^5 + (6a^2b - 6b^2)u^4 + 9abu^3 \\ &\quad + (-a^2 + 8b)u^2 - 3au - 3, \\ g(u) &= -\frac{1}{a(a^2 - 16b)}\big(ab^3u^7 + (3a^2b^2 - 2b^3)u^6 + (3a^3b - 6ab^2)u^5 + (a^4 + a^2b \\ &\quad + 2b^2)u^4 + (4a^3 - 15ab)u^3 + 18bu^2 - 12au - 18\big). \end{aligned}$$

Proof. [1] Given the elliptic curve C with equation (4.1.7), a nonzero point Q is 3-torsion if and only if the polynomial

$$\psi_3(x) = 3x^4 + (a^2 + 4b)x^3 + 3a^2bx^2 + 3a^2b^2x + a^2b^3 \tag{4.2.4}$$

in Definition 4.2.2 vanishes at Q. Substituting $x = u/v$ and clearing the denominators, we get a polynomial

$$\widetilde{\psi}_3(u, v) \coloneqq 3u^4 + (a^2 + 4b)u^3v + 3a^2bu^2v^2 + 3a^2b^2uv^3 + a^2b^3v^4.$$

[1] See Appendix A.1 for explicit formulas for the polynomials $\widetilde{f}$, Q_1, R_1, Q_2, R_2, K, L, M, and N that appear in the proof.

As $Q = (d, e)$ in uv-coordinates, we then have

$$\widetilde{\psi}_3(d, e) = 0. \tag{4.2.5}$$

To get the polynomial f, we take v as variable and rewrite (4.1.8) as a quadratic equation

$$abv^2 + (-bu^2 + au + 1)v - u^3 = 0, \tag{4.2.6}$$

where the leading coefficient ab is invertible in $S^\bullet = \mathbb{Z}[1/4][a, b, \Delta^{-1}]$ as $\Delta = a^2b^4(a^2 - 16b)$. Define

$$\widetilde{f}(u) \coloneqq \widetilde{\psi}_3(u, v)\widetilde{\psi}_3(u, \bar{v}) \tag{4.2.7}$$

where v and $\bar{v}$ are formally the conjugate roots of (4.2.6) so that we compute $\widetilde{f}$ in terms of u by substituting

$$v + \bar{v} = \frac{bu^2 - au - 1}{ab} \qquad \text{and} \qquad v\bar{v} = -\frac{u^3}{ab}.$$

We then factor $\widetilde{f}$ over $S^\bullet$ as

$$\widetilde{f}(u) = -\frac{u^4 f(u)}{a^2 b} \tag{4.2.8}$$

with f the stated polynomial of order 8. We check that f is irreducible by applying Eisenstein's criterion to the homogeneous prime ideal $(3, H)$ of $S^\bullet$.

We have $\widetilde{f}(d) = 0$ by (4.2.7) and (4.2.5). To see $f(d) = 0$, consider the closed subscheme $D \subset C[3]$ of nonzero 3-torsion points. By Theorem 4.2.1 it is finite locally free of rank 8 over $S^\bullet$. By the Cayley-Hamilton theorem, as a global section of D, u locally satisfies a homogeneous monic equation of order 8, and this equation locally defines the rank-8 scheme D. Since D is affine, it is then globally defined by such an equation. In view of $\widetilde{f}(d) = 0$ and (4.2.8), we determine this equation, and (up to a unit in $S^\bullet$) get the first stated identity (4.2.2).

To get the polynomial g, we note that both the quartic polynomial

$$A(v) \coloneqq \widetilde{\psi}_3(d, v)$$

and the quadratic polynomial

$$B(v) \coloneqq abv^2 + (-bd^2 + ad + 1)v - d^3$$

defined from (4.2.6) vanish at e, and thus so does their greatest common divisor (gcd). Applying the Euclidean algorithm (see Appendix A.1 for explicit expressions), we have

$$A(v) = Q_1(v)B(v) + R_1(v),$$
$$B(v) = Q_2(v)R_1(v) + R_2,$$

where

$$R_1(v) = K(d)v + L(d)$$

for some polynomials K and L, and $R_2 = 0$ in view of (4.2.2). Thus $R_1(v)$ is the gcd of $A(v)$ and $B(v)$, and hence

$$K(d)e + L(d) = R_1(e) = 0.$$

To write e in terms of d from the above identity, we apply the Euclidean algorithm to f and K. Their gcd turns out to be 1, and thus there are polynomials M and N with

$$M(u)f(u) + N(u)K(u) = 1.$$

By (4.2.2) we then have $N(d)K(d) = 1$, and thus

$$e = -N(d)L(d) = g(d)$$

where g is as stated. □

4.3 The formal group

The p-divisible group and deformation theory

In Section 4.2 we looked at the torsion subgroups $E[m]$ of an elliptic curve E/S. In particular, for a prime p, consider

$$E[p^\infty] := \bigcup_{n\geq 0} E[p^n].$$

It is a *p-divisible group of height 2* in the sense of [62, Section 2.1]. The following theorem of Serre and Tate states that p-adically the deformation theory of an elliptic curve is equivalent to the deformation theory of its p-divisible group.

Theorem 4.3.1 (Serre-Tate, see [23, 2.9.1])**.** *Let R be a ring, I an ideal of R, and p a prime number. Suppose that the ideal (I, p) is nilpotent. Denote by R_0 the ring R/I. Consider the following two categories:*

$\mathcal{A}$: *objects are elliptic curves E/R, morphisms are R-homomorphisms;*

$\mathcal{C}$: *objects are triples $(E_0/R_0, \mathbb{G}/R, i)$ with*

E_0/R_0 an elliptic curve,

$\mathbb{G}/R$ a p-divisible group, and

i an R_0-isomorphism $E_0[p^\infty] \xrightarrow{\sim} \mathbb{G} \otimes_R R_0$ of p-divisible groups,

morphisms are pairs (ϕ_0, ϕ) with

ϕ_0 an R_0-homomorphism of elliptic curves,

ϕ an R-homomorphism of p-divisible groups, such that

ϕ_0 and $\phi \otimes_R R_0$ agree (via i) on the p-divisible groups over R_0.

Then the functor $\mathcal{A} \to \mathcal{C}$ defined on objects by

$$E/R \longmapsto \big((E \otimes_R R_0)/R_0, E[p^\infty], \mathrm{id}\big)$$

is an equivalence of categories.

We will come back to this theorem when we discuss a universal deformation of a

specific elliptic curve in Example 4.5.12.

Associated to any p-divisible group $\mathbb{G}$ over a complete noetherian local ring R there is an exact sequence

$$0 \to \mathbb{G}^0 \to \mathbb{G} \to \mathbb{G}^{\text{et}} \to 0 \tag{4.3.1}$$

of p-divisible groups over R, natural in $\mathbb{G}$, where $\mathbb{G}^0$ is formal and $\mathbb{G}^{\text{et}}$ is étale, and the sum of their heights equals the height of $\mathbb{G}$ (see [62, Section 2.2]). In particular, when $\mathbb{G} = E[p^\infty]$ with E an elliptic curve over a field k of characteristic p, $\mathbb{G}^0$ coincides with $\widehat{E}$, and the height of $\mathbb{G}^0$ as a p-divisible group agrees with the *height* of $\widehat{E}$ as a formal group (the latter notion we will recall below). With motivation from algebraic topology, we are particularly interested in the case when $\widehat{E}$ is of height 2, so that $E[p^\infty]$ is all formal, i.e., there is no étale component in (4.3.1).

Let Γ be a formal group over a perfect field k of characteristic p. Recall that the *height of* Γ, denoted by $\mathrm{ht}(\Gamma)$, is defined to be the largest integer n such that

$$[p](u) = f(u^{p^n})$$

for some $f(u) \in k[\![u]\!] = \mathcal{O}_\Gamma$ (if $[p] = 0$, we set $\mathrm{ht}(\Gamma) \coloneqq \infty$). In particular, for an elliptic curve E/k, $\mathrm{ht}(\widehat{E})$ is either 1 or 2 (see [59, IV.7.5]), and correspondingly the elliptic curve is said to be *ordinary* or *supersingular*. This dichotomy of elliptic curves has a geometric characterization as below (cf. [23, 12.4.1]).

The Hasse invariant and supersingularity

Let $E/S/\mathbb{F}_p$ be an elliptic curve over an $\mathbb{F}_p$-scheme. Recall that the absolute Frobenius of E, affine-locally given by the ring homomorphism $x \mapsto x^p$, has a canonical factorization through the relative Frobenius F (cf. (3.3.1) and (2.1.1)):

$$\begin{array}{ccccc}
 & & x^p \leftarrow\!\shortmid x & & \\
 & \overset{F}{\nearrow} & & \searrow & \\
E & \longrightarrow & E^{(p)} & \longrightarrow & E \\
\downarrow & & \downarrow & & \downarrow \\
S & = & S & \xrightarrow[s^p \leftarrow\!\shortmid s]{} & S.
\end{array}$$

Denote by $V\colon E^{(p)} \to E$ the Verschiebung dual to F so that $V \circ F = [p]$. Define *the Hasse invariant* H as a modular form of weight $p-1$ given by the tangent map of V:

$$\begin{aligned} V_* &\in \mathrm{Hom}_S\big(\mathcal{L}ie(E^{(p)}/S), \mathcal{L}ie(E/S)\big) \\ &= \mathrm{Hom}_S\big(\mathcal{L}ie(E/S)^{\otimes p}, \mathcal{L}ie(E/S)\big) \\ &= \mathrm{Hom}_S\big(\mathcal{O}_S, (\underline{\omega}_{E/S})^{\otimes(p-1)}\big) \\ &= H^0\big(S, (\underline{\omega}_{E/S})^{\otimes(p-1)}\big) \end{aligned}$$

where the $\mathcal{O}_S$-module $\mathcal{L}ie(E/S) \cong (\underline{\omega}_{E/S})^\vee$ is the pushforward to S of the relative tangent sheaf on E/S along the structure morphism.

Locally on $\operatorname{Spec} R \subset S$ pick an R-basis ω as we did in Section 4.1. In terms of the bases of $\mathcal{L}ie(E^{(p)}/S)$ and $\mathcal{L}ie(E/S)$ dual to ω, the Hasse invariant $H(E,\omega)$ is then an element in R. In particular, for the formal group $\widehat{E}$ with a coordinate u adapted to ω (see (4.1.5)), since

$$[p](u) = V \circ F(u) = V(u^p),$$

we see that $H(E,\omega)$ is the coefficient of u^p in $[p](u)$. Thus $\widehat{E}$ is of height 2 if and only if $H(E,\omega) = 0$. The following theorem of Igusa gives a precise description of the vanishing of the Hasse invariant.

Theorem 4.3.2 (Igusa, see [23, 12.4.3])**.** *The Hasse invariant has simple zeros, i.e., if k is a perfect field of characteristic p, and R an artinian local k-algebra with residue field k, then for any elliptic curve E/R, the following conditions are equivalent:*

(i) the Verschiebung $V\colon E^{(p)} \to E$ has tangent map $V_* = 0$;

(ii) there exists a supersingular elliptic curve E_0/k together with an R-isomorphism $E_0 \otimes_k R \cong E$.

The next theorem gives a numerical criterion for supersingularity.

Theorem 4.3.3 ([59, V.4.1a])**.** *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$. Let $E/\mathbb{F}_q$ be an elliptic curve given by a Weierstrass equation*

$$E\colon\ y^2 = f(x)$$

where $f(x) \in \mathbb{F}_q[x]$ is a cubic polynomial with distinct roots in $\overline{\mathbb{F}}_q$. Then E is supersingular if and only if the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ is zero.

The dichotomy between ordinary and supersingular elliptic curves also appears in the structure of torsion subgroups. Over a field k of characteristic p, if E is supersingular, then the torsion subgroup

$$E[p^n] = \ker(F^{2n} \colon E \to E^{(p^{2n})}), \tag{4.3.2}$$

and thus it is connected so that the group of k-points $E[p^n](k) = 0$; if E is ordinary, then there is an exact sequence

$$0 \to \mu_{p^n} \to E[p^n] \to \underline{\mathbb{Z}/p^n} \to 0, \tag{4.3.3}$$

and it splits if k is perfect so that $E[p^n](k) = \mathbb{Z}/p^n$ (see [23, 12.3.3-4 and 12.2.7]).

Example 4.3.4. Continuing Example 4.1.5, we compute the supersingular locus at the prime 3 for the elliptic curve $C/S^\bullet$. By Theorem 4.3.3, over a finite field of characteristic 3, C is supersingular precisely when the quantity

$$H \coloneqq a^2 + b \tag{4.3.4}$$

vanishes. This is indeed the Hasse invariant $H(C, \omega)$ by a calculation of the formal power series $[3](u)$ (cf. [60, Section 9.1]). By Theorem 4.3.2, as $(3, H)$ is a homogeneous maximal ideal of $S^\bullet$ corresponding to the closed subscheme $\operatorname{Spec} \mathbb{F}_3 \subset \operatorname{Proj} S^\bullet$, the supersingular locus consists of a single closed point. We compute that C restricts to $\mathbb{F}_3$ as

$$C_0 \colon y^2 + xy - y = x^3 - x^2. \tag{4.3.5}$$

The formula for f in Proposition 4.2.3 satisfies a congruence

$$f(u) \equiv u^2(b^4u^6 + abHu^3 - H) \mod 3. \tag{4.3.6}$$

Over the supersingular locus where $H = 0$, the eight roots of f (counted with multiplicity), together with $u = 0$ as the identity, correspond to the group scheme $C_0[3]$ which is connected. When $H \not\equiv 0 \mod 3$, the two roots of f which reduce to zero modulo 3

correspond to the two nonzero points in the unique connected degree-3 subgroup of C isomorphic to μ_3 (cf. (4.3.3)).

4.4 Isogenies

Cyclicity

With motivation from algebraic topology, we are particularly interested in isogenies of elliptic curves that correspond to power operations in elliptic cohomology theories via deformations of Frobenius (see Section 3.3). Such isogenies are *cyclic*. We give a precise definition of cyclicity in the sense of Drinfeld (cf. [23, 1.4.1]).

Definition 4.4.1. Let S be a scheme, E/S an elliptic curve, and $m \geq 1$ an integer.

(i) We say that a point $P \in E(S)$ has *exact order* m if the effective Cartier divisor

$$D \coloneqq [P] + [2P] + \cdots + [mP]$$

is a subgroup scheme of E/S. We call this subgroup scheme *the cyclic subgroup of degree* m *generated by* P.

(ii) We say that a closed subgroup scheme $G \subset E$ which is finite locally free of rank m over S is *cyclic* if

$$G = \sum_{i=1}^{m} [iP]$$

holds locally with respect to the f.p.p.f. topology for some generator P.

(iii) An isogeny is *cyclic* if its kernel is a cyclic group scheme.

Using the calculations in Proposition 4.2.3, we can explicitly compute a cyclic isogeny with source the elliptic curve C in Example 4.1.5.

Proposition 4.4.2.

(i) The universal degree-3 isogeny ψ with source C is defined over the graded ring

$$S_3^\bullet \coloneqq S^\bullet[\kappa]/\big(W(\kappa)\big)$$

where $|\kappa| = -2$ *and*

$$W(\kappa) = \kappa^4 - \frac{6}{b^2}\ \kappa^2 + \frac{a^2 - 8b}{b^4}\ \kappa - \frac{3}{b^4}, \tag{4.4.1}$$

and has target the elliptic curve

$$C' \colon\ v + a'uv + a'b'v^2 = u^3 + b'u^2v$$

where

$$\begin{aligned} a' &= \frac{1}{a}\big((a^2b^4 - 4b^5)\kappa^3 + 4b^4\kappa^2 + (-6a^2b^2 + 20b^3)\kappa + a^4 - 12a^2b \\ &\quad + 12b^2\big), \\ b' &= b^3. \end{aligned} \tag{4.4.2}$$

(ii) The kernel of ψ *is generated by a point* Q *of exact order 3 with coordinates* (d, e) *satisfying*

$$\begin{aligned} \kappa &= -\frac{1}{a^2 - 16b}\big(ab^3d^7 + (3a^2b^2 - 2b^3)d^6 + (3a^3b - 6ab^2)d^5 + (a^4 \\ &\quad + a^2b + 2b^2)d^4 + (4a^3 - 15ab)d^3 + (a^2 + 2b)d^2 - 12ad - 18\big) \\ &= ae - d^2. \end{aligned} \tag{4.4.3}$$

(iii) The restriction of ψ *to the supersingular locus at the prime 3 is the 3-power Frobenius endomorphism.*

(iv) The induced map ψ^* *on the relative cotangent space of* C' *at the identity sends* du *to* κdu*.*

Proof. [2] Let $P = (u, v)$ be a point on C, and $Q = (d, e)$ be a nonzero 3-torsion point. Rewriting (4.1.8) as

$$v = u^3 + bu^2v - auv - abv^2,$$

we express v as a power series in u by substituting this equation into itself recursively.

[2] See Appendix A.2 for the power series expansion of v and explicit formulas for (4.4.5) that appear in the proof.

For the purpose of our calculations, we take this power series up to u^{12} as an expression for v, and write $e = g(d)$ as in (4.2.3).

Define functions u' and v' by

$$\begin{aligned} u' &\coloneqq u(P) \cdot u(P-Q) \cdot u(P+Q), \\ v' &\coloneqq v(P) \cdot v(P-Q) \cdot v(P+Q). \end{aligned} \tag{4.4.4}$$

By the group law algorithm in Example 4.1.5, we express u' and v' as power series in u:

$$\begin{aligned} u' &= \kappa u + (\text{higher-order terms}), \\ v' &= \lambda u^3 + (\text{higher-order terms}), \end{aligned} \tag{4.4.5}$$

where the coefficients (κ, λ, etc.) involve a, b, and d. In particular, in view of (4.2.2), we compute that κ satisfies $W(\kappa) = 0$ with $|\kappa| = -2$ as stated in (i).

Now define the isogeny $\psi\colon C \to C'$ by

$$u\big(\psi(P)\big) \coloneqq u' \qquad \text{and} \qquad v\big(\psi(P)\big) \coloneqq \frac{\kappa^3}{\lambda} \cdot v', \tag{4.4.6}$$

where we introduce the factor κ^3/λ so that the equation of C' will be in the Weierstrass form. Using (4.4.5) (see Appendix A.2 for explicit expressions), we then determine the coefficients in a Weierstrass equation and get the stated equation of C'.

We next check the statement of (ii). In view of (4.4.6) and (4.4.4), the kernel of ψ is the degree-3 subgroup generated by Q. In (4.4.3), the first identity is computed in (4.4.5); we then compare it with (4.2.3) and get the second identity.

For (iii), recall from Example 4.3.4 that the supersingular locus at the prime 3 is $\operatorname{Spec} \mathbb{F}_3$. Over $\mathbb{F}_3$, since $C[3](\mathbb{F}_3) = 0$ by (4.3.2), Q coincides with the identity, and thus

$$u\big(\psi(P)\big) = u(P) \cdot u(P-Q) \cdot u(P+Q) = \big(u(P)\big)^3.$$

As the u-coordinate is a local uniformizer at the identity, ψ then restricts to $\mathbb{F}_3$ as the 3-power Frobenius endomorphism.

The statement of (iv) follows by definition of κ in (4.4.5). □

Remark 4.4.3. In view of Proposition 4.4.2 (iii), the formal completion of $\psi\colon C \to C'$ at the identity of C is a deformation of Frobenius (see Definition 3.3.1). When it is clear from the context, we will simply call ψ itself a deformation of Frobenius.

Remark 4.4.4. From (4.4.4) and (4.4.5) we have

$$u(P-Q)\cdot u(P+Q) = \kappa + u\cdot(\text{higher-order terms}). \tag{4.4.7}$$

In particular $u(-Q)\cdot u(Q) = \kappa$. The analog of κ at the prime 2 coincides with d as studied in [26, Section 3] (see Example 3.4.2).

Cyclic in standard order

We have seen in Section 4.3 that for an elliptic curve $E/S/\mathbb{F}_p$ there are dual isogenies $F\colon E \to E^{(p)}$ and $V\colon E^{(p)} \to E$. It turns out that both are cyclic of degree p, and their composite $V\circ F = [p]$ is also cyclic (see [23, 12.2.1, 12.2.3, and 12.2.5]). In general the composite of two cyclic isogenies need not be cyclic. The above is an example of two isogenies being *cyclic in standard order* (cf. [23, 6.7.7]).

Definition 4.4.5. Over a scheme S, suppose we are given a pair of composable isogenies

$$E \xrightarrow{\phi_1} E' \xrightarrow{\phi_2} E''$$

with ϕ_1 and ϕ_2 of degrees d_1 and d_2 respectively. We say that the pair (ϕ_1, ϕ_2) is *cyclic in standard order* if both of the following conditions hold:

(i) the composite $\phi_2\circ\phi_1$ is cyclic;

(ii) f.p.p.f.-locally on S, in terms of any generator P of $\ker(\phi_2\circ\phi_1)$, $\ker\phi_1$ is the cyclic subgroup of degree d_1 generated by d_2P.

Example 4.4.6. Let ψ_0 be the restriction to the supersingular locus of the universal degree-3 isogeny ψ in Proposition 4.4.2. By (iii) of the proposition $\psi_0\colon C_0 \to C_0$ is the 3-power Frobenius endomorphism, and thus (ψ_0, ψ_0) is cyclic in standard order by [23, 12.2.4(1)].

To study compositions of power operations, we want to lift $\psi_0 \circ \psi_0$ to a composite of deformations of Frobenius. In the situation of Definition 4.4.5 we have

$$\ker \phi_2 = \phi_1\big(\ker(\phi_2 \circ \phi_1)\big) = \big(\ker(\phi_2 \circ \phi_1)\big)\big/ \ker \phi_1.$$

In Proposition 4.4.2 we have $\psi\colon\ C \to C' = C/G$ where G is a degree-3 subgroup of C. Let

$$G' \coloneqq C[3]/G,$$

which is a degree-3 subgroup of C'. Since $C_0/\mathbb{F}_3$ is supersingular, $C_0[3]$ is connected by (4.3.2). Thus over a formal neighborhood of the supersingular locus, if G is the unique connected degree-3 subgroup of C, G' is then the unique connected degree-3 subgroup of C'. As in the proof of Proposition 4.4.2, we define

$$\psi'\colon\ C' \longrightarrow C'/G'$$

using a nonzero point in G' (see (4.4.4) and (4.4.6)), and ψ' is then also a deformation of Frobenius.

Proposition 4.4.7. *The following diagram of elliptic curves over $S_3^\bullet$ commutes:*

$$\begin{array}{ccc} C & \xrightarrow{\quad\psi\quad} & C/G = C' \\ & \searrow^{[-3]} & \big\downarrow{\scriptstyle \psi'} \\ & & C/C[3] \cong \frac{C/G}{C[3]/G} = \frac{C'}{G'}. \end{array} \tag{4.4.8}$$

Proof. By Corollary 4.1.3, since $\operatorname{Proj} S_3^\bullet$ is connected, we need only show that the locus over which $\psi' \circ \psi = [-3]$ is not empty, where by abuse of notation $[-3]$ denotes the map $[-3]$ on C composed with the canonical isomorphism from $C/C[3]$ to C'/G'.

We have seen in Example 4.4.6 that both ψ and ψ' restrict as the 3-power Frobenius endomorphism ψ_0 of C_0. By (4.1.6), in the endomorphism ring of C_0, ψ_0 is a root of the polynomial

$$X^2 - \operatorname{trace}(\psi_0) \cdot X + 3 \tag{4.4.9}$$

with $\mathrm{trace}(\psi_0)$ an integer satisfying

$$\big(\mathrm{trace}(\psi_0)\big)^2 \leq 12. \tag{4.4.10}$$

Moreover by (4.3.2), since C_0 is supersingular, we have

$$\psi_0 \circ \psi_0 \equiv 0 \mod 3,$$

and thus by [23, 12.3.3(1)]

$$\widehat{\psi}_0 \circ \widehat{\psi}_0 \equiv 0 \mod 3.$$

We then have

$$\begin{aligned}\big(\mathrm{trace}(\psi_0)\big)^2 &= (\psi_0 + \widehat{\psi}_0) \circ (\psi_0 + \widehat{\psi}_0) \\ &= \psi_0 \circ \psi_0 + \widehat{\psi}_0 \circ \psi_0 + \psi_0 \circ \widehat{\psi}_0 + \widehat{\psi}_0 \circ \widehat{\psi}_0 \\ &= \psi_0 \circ \psi_0 + 3 + 3 + \widehat{\psi}_0 \circ \widehat{\psi}_0 \\ &\equiv 0 \mod 3.\end{aligned}$$

This congruence and (4.4.10) imply that $\mathrm{trace}(\psi_0) = 0$, 3, or -3. We exclude the latter two possibilities by checking the action of ψ_0 at the 2-torsion point $(1, 0)$ on

$$C_0 \colon\ y^2 + xy - y = x^3 - x^2.$$

It then follows from (4.4.9) that $\psi_0 \circ \psi_0$ agrees with $[-3]$ on C_0 over $\mathbb{F}_3$. □

Analogous to Proposition 4.4.2 (iv), let κ' be the element in $S_3^\bullet$ such that $(\psi')^*$ sends du to $\kappa' du$. Note that $|\kappa'| = -6$.

Corollary 4.4.8. *The following relations hold in $S_3^\bullet$:*

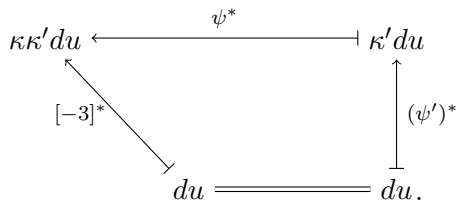
$$b^4 \kappa \kappa' + 3 = 0$$

and

$$\kappa' = -\kappa^3 + \frac{6}{b^2}\ \kappa - \frac{a^2 - 8b}{b^4}.$$

Proof. The isogenies in (4.4.8) induce maps on relative cotangent spaces at the identity.

By Proposition 4.4.2 (iv) we then have a commutative diagram



Thus for the first stated relation we need only show that $[3]^*$ sends du to $3du/b^4$.

Let $P = (u, v)$ be a point on C. For $i = 1$, 2, 3, and 4, let Q_i be a generator for each of the four degree-3 subgroups of C. Each Q_i can be chosen as Q in (4.4.4), and we denote the corresponding quantity κ in (4.4.5) by κ_i. Define an isogeny Ψ with source C by

$$\begin{aligned} u\big(\Psi(P)\big) &\coloneqq u(P) \prod_{i=1}^{4} \big(u(P - Q_i) \cdot u(P + Q_i)\big), \\ v\big(\Psi(P)\big) &\coloneqq v(P) \prod_{i=1}^{4} \big(v(P - Q_i) \cdot v(P + Q_i)\big). \end{aligned} \tag{4.4.11}$$

In view of (4.4.7), since [3] has the same kernel as Ψ, we have

$$[3]^*(du) = s \cdot \kappa_1\kappa_2\kappa_3\kappa_4 \cdot du \tag{4.4.12}$$

where s is a degree-0 unit in $S^\bullet$ coming from an automorphism of C over $S^\bullet$. In view of (4.4.1) we have

$$\kappa_1\kappa_2\kappa_3\kappa_4 = -\frac{3}{b^4}.$$

We compute that $s = -1$ by comparing the restrictions of the two sides of (4.4.12) to the point corresponding to the homogeneous maximal ideal $(5, H)$ of $S^\bullet$, and then comparing the restrictions to the point corresponding to $(7, H)$. Over both points, $[3]^*$ becomes the multiplication-by-3 map, and $-3/b^4$ becomes -3. Thus $[3]^*$ sends du to $3du/b^4$.

The second stated relation follows by a computation from the first relation and the relation $W(\kappa) = 0$ as in Proposition 4.4.2 (i). □

Remark 4.4.9. As noted in Remark 4.4.4, the (local) analog of κ at the prime 2 coincides

with the parameter d in [26, Section 3]. In particular, with the notations there and the equation in [50, Proposition 3.2], d and d' satisfy an analogous relation $A_3 dd' + 2 = 0$ which locally reduces to $dd' + 2 = 0$. These arise as examples of [63, Lemma 3.21].

Remark 4.4.10. In view of (4.4.8), $-\psi'$ (composed with the canonical isomorphism on the target) turns out to be the dual isogeny of ψ (cf. the proof of [23, 2.9.4]). If G is the unique degree-3 subgroup of C in a formal neighborhood of the identity, then

$$\kappa \equiv 0 \mod 3 \tag{4.4.13}$$

by (4.3.6) and (4.4.3). Thus in view of Corollary 4.4.8 and (4.3.4) we have

$$-\kappa' = \kappa^3 - \frac{6}{b^2}\,\kappa + \frac{a^2 - 8b}{b^4} \equiv \frac{H}{b^4} \mod 3.$$

This congruence agrees with the interpretation of H as defined by the tangent map of the Verschiebung isogeny over $\mathbb{F}_3$ (see Section 4.3).

Isogenies as studied by Lubin and Vélu

The isogeny Ψ in the proof of Corollary 4.4.8 above and the isogeny ψ in Proposition 4.4.2 (cf. (4.4.11) and (4.4.4)) are examples of a construction used by Lubin in his study of finite isogenies of formal groups.

Theorem 4.4.11 (Lubin, see [57, Theorem 1.4])**.** *Let p be a prime number. Let k be a finite extension of $\mathbb{Q}_p$, and K a finite extension of k. Denote by $\mathcal{O}_k$ and $\mathcal{O}_K$ the rings of integers in k and K respectively. Let Γ be a formal group law over $\mathcal{O}_k$, and G a finite subgroup of $\Gamma(\mathcal{O}_K)$. Then there is a formal group law Γ' defined over $\mathcal{O}_K$ and a $\phi \in \mathrm{Hom}_{\mathcal{O}_K}(\Gamma, \Gamma')$ with $\ker \phi = G$. Moreover, if G is stable under the action of $\mathrm{Aut}(\overline{k}/k)$, then Γ' can be defined over $\mathcal{O}_k$.*

In the proof of this theorem, Lubin gives explicitly the function ϕ as

$$\phi(x) = \prod_{g \in G} (x +_\Gamma g) \in \mathcal{O}_K[\![x]\!]. \tag{4.4.14}$$

Remark 4.4.12. In [27] Ando constructs coordinates on certain Lubin-Tate formal groups which are preserved under isogenies (see [27, Theorem 2.5.7]). The problem addressed

by his theorem arose in the study of cohomology operations in elliptic cohomology and Morava E-theories. In particular, with notations as in Theorem 4.4.11, his coordinate x is determined by requiring that the corresponding formal group law Γ satisfy

$$\phi(x) = [p](x)$$

for G the subgroup of p-torsion points (see [27, Theorem 2.6.4]). When the formal group is $\widehat{C}$ and $p = 3$, with notations as in the proof of Corollary 4.4.8, the above identity becomes

$$x\big(\Psi(P)\big) = x\big([3](P)\big),$$

which our coordinate u does not satisfy (recall that we have $s = -1$). On the other hand, in the prime-2 case studied by Rezk in [26], this holds for the analogous coordinate u.

Constructions similar to (4.4.14) appear in the study of finite subgroups and isogenies of elliptic curves. For an elliptic curve E over a field of characteristic not equal to 2 or 3, the division polynomials in Definition 4.2.2 are given by

$$\psi_m(x) = \prod_{Q \in (E[m] - \{O\})/\{\pm 1\}} \big(x - x(Q)\big) \tag{4.4.15}$$

(see [61, 13(9.2)]). Since $E[m] - \{O\}$ is stable under the automorphism $[-1]$ on E which fixes x, it is defined by the equation $\psi_m(x) = 0$.

Using a polynomial in x that defines a finite subgroup, we can compute an isogeny whose kernel is this subgroup. The formulas are given by Vélu [64].

Let E be an elliptic curve over an algebraically closed field given by a Weierstrass equation (4.1.2) in xy-coordinates. Let $P = (x, y)$ be a point on E. Let G be a finite subgroup of E, and denote by E' the quotient curve E/G. Define an isogeny $\Phi\colon\ E \to E'$ by

$$\begin{aligned} x\big(\Phi(P)\big) &\coloneqq x(P) + \sum_{Q \in G - \{O\}} \big(x(P+Q) - x(Q)\big), \\ y\big(\Phi(P)\big) &\coloneqq y(P) + \sum_{Q \in G - \{O\}} \big(y(P+Q) - y(Q)\big). \end{aligned} \tag{4.4.16}$$

Vélu gives an explicit Weierstrass equation of E' with coefficients in terms of the coordinates of the points Q in $G - \{O\}$.

Below we follow the presentation of Vélu's formulas in [1, Section 2.4] in terms of a polynomial $\psi(x)$ defining $G - \{O\}$ (cf. [65]). As we mentioned above for $\psi_m(x)$ in (4.4.15) defining $E[m]-\{O\}$, such a polynomial exists as x is fixed by the automorphism $[-1]$ on E. We discuss only the case when the degree d of G is odd and the base field is of characteristic not equal to 2.

Write $d = 2n+1$ and s_i the i'th elementary symmetric function in the roots of $\psi(x)$ so that

$$\psi(x) = x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n.$$

Write $\psi_2 = 2y + a_1 x + a_3$ as in Definition 4.2.2. The isogeny Φ is given by

$$\Phi(x,y) = \left(\frac{\phi(x)}{\psi(x)^2}, \frac{\omega(x,y)}{\psi(x)^3} \right)$$

(cf. (4.2.1)) where

$$\begin{aligned} \phi(x) &= (4x^3 + b_2 x^2 + 2b_4 x + b_6)\big(\psi'(x)^2 - \psi''(x)\psi(x)\big) \\ &\quad - (6x^2 + b_2 x + b_4)\psi'(x)\psi(x) + (dx - 2s_1)\psi(x)^2, \\ \omega(x,y) &= \phi'(x)\psi(x)\psi_2/2 - \phi(x)\psi'(x)\psi_2 - \big(a_1\phi(x) + a_3\psi(x)^2\big)\psi(x)/2. \end{aligned}$$

The equation of the quotient curve E' is given by

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + (a_4 - 5t)x + a_6 - b_2 t - 7w$$

where

$$\begin{aligned} t &= 6(s_1^2 - 2s_2) + b_2 s_1 + nb_4, \\ w &= 10(s_1^3 - 3s_1 s_2 + 3s_3) + 2b_2(s_1^2 - 2s_2) + 3b_4 s_1 + nb_6. \end{aligned}$$

As an application of Vélu's formulas, we give an alternate computation, in xy-coordinates, of the universal degree-3 isogeny ψ in Proposition 4.4.2.

Example 4.4.13. We continue with the notations in Proposition 4.4.2 and Vélu's formulas above. Let s be the x-coordinate of the 3-torsion point Q on C, with $|s| = 2$. As in

(4.2.4), it satisfies

$$\widetilde{W}(s) \coloneqq 3s^4 + (a^2 + 4b)s^3 + 3a^2bs^2 + 3a^2b^2s + a^2b^3 = 0. \tag{4.4.17}$$

Since the x-coordinate of any point on C is fixed by $[-1]$, which is the only nontrivial automorphism of any degree-3 subgroup, we then have

$$S_3^\bullet \cong S^\bullet[s]/\big(\widetilde{W}(s)\big).$$

Let G be the subgroup generated by Q. The universal degree-3 isogeny

$$\psi\colon\ C \longrightarrow C' = C/G$$

is determined up to an isomorphism by the polynomial (with an abuse of notation)

$$\psi(x) \coloneqq x - s,$$

as the point $-Q$ has the same x-coordinate as Q. We have $d = 3$ and $n = 1$, and in the identity

$$\psi(x) = x^n - s_1x^{n-1} + \cdots + (-1)^n s_n$$

we have

$$s_1 = s, \qquad \text{and} \qquad s_i = 0 \quad \text{for} \quad i > 1.$$

We then compute that

$$\begin{aligned}
\phi(x) &= x^3 - 2sx^2 + (7s^2 + a^2s + 4bs + a^2b)x - 2s^3 + a^2bs + a^2b^2,\\
\omega(x,y) &= \big(x^3 - 3sx^2 + (-3s^2 - a^2s - 4bs - a^2b)x - 3s^3 - a^2s^2 - 4bs^2 - 3a^2bs\\
&\quad - 2a^2b^2\big)y + (-6as^2 - a^3s - 4abs - a^3b)x^2 + (3as^3 - 3abs^2 - 2a^3bs\\
&\quad - 2ab^2s - 2a^3b^2)x - as^4 - abs^3 - 2ab^2s^2 - a^3b^2s - a^3b^3.
\end{aligned}$$

In view of (4.4.17), the 4-torsion point $(0,0)$ on C (see Example 4.1.5) then maps to

$$(x_0, y_0) \coloneqq \left(\frac{\phi(0)}{\psi(0)^2}, \frac{\omega(0,0)}{\psi(0)^3}\right)$$

where

$$\begin{aligned} x_0 &= 6b^{-2}s^3 + (2a^2b^{-2} + 5b^{-1})s^2 + (5a^2b^{-1} - 6)s + 3a^2, \\ y_0 &= (-9ab^{-2} - 6a^{-1}b^{-1})s^3 + (-3a^3b^{-2} - 8ab^{-1} - 8a^{-1})s^2 - 7a^3b^{-1}s \\ &\quad - 4a^3 - 9ab. \end{aligned}$$

The equation of the quotient curve is given by

$$y^2 + axy + aby = x^3 + bx^2 - 5tx - (a^2 + 4b)t - 7w$$

where

$$\begin{aligned} t &= 6s^2 + (a^2 + 4b)s + a^2b, \\ w &= 10s^3 + (2a^2 + 8b)s^2 + 3a^2bs + a^2b^2. \end{aligned}$$

We normalize this equation into the form of (4.1.7) by making two changes of variables, where x' and y' are the variables after each change:

- set
$$x = x' + x_0 \qquad \text{and} \qquad y = y' + y_0;$$
- set
$$x = x' \qquad \text{and} \qquad y = y' + kx$$
where
$$k = -6a^{-1}b^{-2}s^3 + (-2ab^{-2} - 8a^{-1}b^{-1})s^2 - 6ab^{-1}s - 5a.$$

We then have

$$C' \colon\ y^2 + a'xy + a'b'y = x^3 + b'x^2$$

where

$$\begin{aligned} a' &= -\frac{1}{ab^2}\big(12s^3 + (4a^2 + 16b)s^2 + 12a^2bs + 9a^2b^2\big), \\ b' &= \frac{1}{b}\big(3s^2 + (a^2 - 2b)s + a^2b + b^2\big). \end{aligned}$$

Since $|a'| = |a| = 1$ and $|b'| = |b| = 2$ (cf. (4.4.2)), the isogeny $C \to C'$ computed above

cannot be a deformation of the 3-power Frobenius endomorphism over the supersingular locus at the prime 3 (see Remark 4.4.3). To get a deformation of Frobenius, we need a further change of variables:

- set
$$x = \lambda^{-2}x' \qquad \text{and} \qquad y = \lambda^{-3}y'$$
where
$$\lambda = -s - b.$$

We will write the equation of the resulting curve in terms of a new parameter $\tau \coloneqq 1/s$, with $|\tau| = -2$ and

$$a^2b^3\tau^4 + 3a^2b^2\tau^3 + 3a^2b\tau^2 + (a^2+4b)\tau + 3 = 0 \tag{4.4.18}$$

in $S_3^\bullet$ (cf. (4.4.17)). In view of Proposition 4.2.3, since $\tau = e/d$, we compute that

$$\begin{aligned}\tau = \frac{1}{a(a^2-16b)}\big(&6b^4d^7 + 17ab^3d^6 + (15a^2b^2+2b^3)d^5 + (3a^3b\\ &+ 48ab^2)d^4 + (-a^4+35a^2b-38b^2)d^3 + (-4a^3+69ab)d^2\\ &+ (-6a^2+30b)d - 6a\big).\end{aligned} \tag{4.4.19}$$

In particular, if Q is in a formal neighborhood of the identity, then by (4.3.6) we have

$$\tau \equiv 0 \mod 3.$$

Now, after the final change of variables, a' and b' become

$$\begin{aligned}a' &= a\big(a^2b^3\tau^3 + 3a^2b^2\tau^2 + (3a^2b-4b^2)\tau + a^2 - 3b\big),\\ b' &= b^3,\end{aligned} \tag{4.4.20}$$

which reduce to $a' = a^3$ and $b' = b^3$ over the supersingular locus, and thus we get a deformation of Frobenius. In view of (4.4.3), (4.4.19), and (4.2.2), we have a relation

$$(b\kappa + 1)(b\tau + 1) = 1$$

in the ring $S^\bullet[d]/\big(f(d)\big)$. We then check that (4.4.2) and (4.4.20) agree via this relation. Thus we recover the computation of the universal degree-3 isogeny $\psi\colon C \to C'$ in Proposition 4.4.2 using Vélu's formulas and the parameter τ.

Remark 4.4.14. As the group law on the elliptic curve is encoded in Vélu's formulas, the computation of ψ in Example 4.4.13 above is considerably easier than the one in Proposition 4.4.2. However, for our purpose of studying power operations, this second approach is less convenient, as the construction (4.4.16) is not a priori a deformation of Frobenius. In fact we have to compose an isomorphism as in the changes of variables toward the end of the computation. In general, Lubin's and Vélu's constructions define isogenies which have the same kernel but differ by an isomorphism.

In Vélu's construction, the invariant one-form ω defined in (4.1.3) on E' pulls back along Φ to that on E (see [64, Remarque 2]). This property does not hold in Lubin's construction. In fact, over the supersingular locus the induced map on the relative cotangent space at the identity is zero (see Theorem 4.3.2).

An important property of Lubin's and Vélu's constructions is that they are both functorial under composition of isogenies (see [27, Proposition 2.2.6] and [1, Section 2.4]).

Remark 4.4.15. We can rewrite (4.4.18) as

$$b^4\tau\tau' + 3 = 0 \tag{4.4.21}$$

where

$$\tau' = \frac{a^2}{b}\,\tau^3 + \frac{3a^2}{b^2}\,\tau^2 + \frac{3a^2}{b^3}\,\tau + \frac{a^2+4b}{b^4}.$$

However, unlike in Corollary 4.4.8, τ' is not the parameter analogous to τ for the isogeny ψ'. In particular, the relation (4.4.18) no longer holds in $S_3^\bullet$ if we substitute a, b, and τ by a', b', and τ' respectively.

4.5 Moduli problems

Individual finite subgroups and isogenies of elliptic curves determine various types of "level structures" on the elliptic curves. We can study them systematically, each type as a whole, by studying the corresponding moduli problems. Based on Definitions 4.4.1

and 4.4.5, we first define these level structures in the sense of Drinfeld (cf. [23, 3.1-4 and 7.9.4]).

Definition 4.5.1. Let S be a scheme, E/S an elliptic curve, and $m \geq 1$ an integer.

(i) A $\Gamma(m)$-*structure* on E/S is a pair of points (P, Q) on E which generate $E[m]$, i.e., we have an equality of effective Cartier divisors in E:

$$E[m] = \sum_{i,\ j \bmod m} [iP + jQ].$$

(ii) A $\Gamma_1(m)$-*structure* on E/S is a point P on E which has exact order m, i.e., the effective Cartier divisor

$$\sum_{i \bmod m} [iP]$$

is a subgroup scheme of E.

(iii) A *balanced* $\Gamma_1(m)$-*structure* on E/S is a diagram

$$P \quad E \underset{\widehat{\phi}}{\overset{\phi}{\rightleftarrows}} E' \quad P'$$

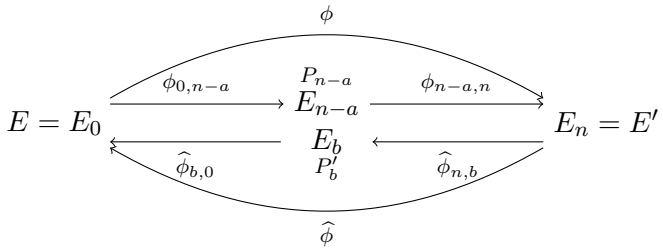
where E' is an elliptic curve over S, ϕ is a degree-m isogeny, $\widehat{\phi}$ is the dual isogeny, $P \in (\ker \phi)(S)$ is a generator of $\ker \phi$, and $P' \in (\ker \widehat{\phi})(S)$ is a generator of $\ker \widehat{\phi}$.

(iv) A $\Gamma_0(m)$-*structure* on E/S is a degree-m isogeny

$$E \xrightarrow{\phi} E' = E/G$$

of elliptic curves over S where $G = \ker \phi$ is cyclic.

(v) Suppose $m = p^n$ for some prime p and integer n. Let $0 \leq a, b \leq n$ be integers. A $[\Gamma_0(p^n); a, b]$-*structure* on E/S is a diagram



where E' is an elliptic curve over S, ϕ is a degree-p^n isogeny, $\widehat{\phi}$ is the dual isogeny, $(\phi_{0,n-a}, \phi_{n-a,n})$ is a pair of isogenies cyclic in standard order with $\phi_{n-a,n}$ of degree p^a, $(\widehat{\phi}_{n,b}, \widehat{\phi}_{b,0})$ is a pair of isogenies cyclic in standard order with $\widehat{\phi}_{b,0}$ of degree p^b, $P_{n-a} \in (\ker \phi_{n-a,n})(S)$ is a generator of $\ker \phi_{n-a,n}$, and $P'_b \in (\ker \widehat{\phi}_{b,0})(S)$ is a generator of $\ker \widehat{\phi}_{b,0}$.

The notion of a moduli problem for elliptic curves provides a way to parametrize these structures. To introduce the definition, we note that our setting here is comparable, and indeed related, to that for deformations of Frobenius in Section 3.3.

Definition 4.5.2 (cf. Definition 3.3.1)**.** For any scheme S, let $\mathrm{Ell}(S)$ be the category whose objects are elliptic curves over S, and whose morphisms are S-homomorphisms. In particular, for any ring R, we write $\mathrm{Ell}(R) \coloneqq \mathrm{Ell}(\operatorname{Spec} R)$.

Note that for a fixed ring R, $\mathrm{Ell}(R)$ is the category $\mathcal{A}$ in Theorem 4.3.1, and is different from the category Ell/R in Definition 4.5.9 below.

Definition 4.5.3 (cf. Definition 3.3.3)**.** We write $\mathrm{Ell} \coloneqq \{\mathrm{Ell}(S)\}$. Precisely, Ell is the category whose objects are elliptic curves

$$\begin{array}{c} E \\ \big\downarrow{\scriptstyle \pi} \\ S \end{array}$$

over variable base schemes, and whose morphisms are cartesian squares

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E \\ {\scriptstyle \pi_1}\downarrow & & \downarrow{\scriptstyle \pi} \\ S_1 & \xrightarrow{f} & S\,, \end{array}$$

i.e., commutative squares such that the induced morphism of S_1-schemes

$$E_1 \xrightarrow{(\phi,\pi_1)} E \times_S S_1$$

is an isomorphism of elliptic curves over S_1.

A *moduli problem* $\mathcal{P}$ *(over* Ell*)* is a functor

$$\mathcal{P}\colon \mathrm{Ell}^{\mathrm{op}} \longrightarrow \mathrm{Set}.$$

Morphisms between moduli problems are natural transformations.

We denote the moduli problems associated to the level structures in Definition 4.5.1 by

$$[\Gamma(m)], \quad [\Gamma_1(m)], \quad [\mathrm{bal.}\,\Gamma_1(m)], \quad [\Gamma_0(m)], \quad [\Gamma_0(p^n); a, b]. \tag{4.5.1}$$

In general, given a moduli problem $\mathcal{P}$ and an elliptic curve E/S, an element in the set $\mathcal{P}(E/S)$ is called a *(level)* $\mathcal{P}$*-structure on* E/S.

Definition 4.5.4 ([23, 4.2])**.** A moduli problem $\mathcal{P}$ is said to be *relatively representable (over* Ell*)* if for every elliptic curve E/S, the functor on $(\mathrm{Sch}/S)^{\mathrm{op}}$ defined on objects by

$$T \longmapsto \mathcal{P}\big((E \times_S T)/T\big)$$

is representable by an S-scheme denoted by $\mathcal{P}_{E/S}$.

Theorem 4.5.5 ([23, 5.1.1, 7.9.6, and 7.1.3(1)])**.** *Each of the five moduli problems* (4.5.1) *is relatively representable over* Ell.

Definition 4.5.6. A moduli problem $\mathcal{P}$ is said to be *representable* if it is representable as a functor, i.e., if there exists an elliptic curve over a scheme denoted by

$$\begin{array}{c} \mathbb{E} \\ \big\downarrow \\ \mathcal{M}(\mathcal{P}) \end{array}$$

together with a functorial isomorphism

$$\mathcal{P}(E/S) \cong \mathrm{Hom}_{\mathrm{Ell}}\big(E/S, \mathbb{E}/\mathcal{M}(\mathcal{P})\big).$$

Any representable moduli problem is relatively representable (see [23, 4.3.2]).

Given moduli problems $\mathcal{P}$ and $\mathcal{P}'$, the *simultaneous moduli problem* $(\mathcal{P}, \mathcal{P}')$ is the moduli problem defined on objects by

$$E/S \longmapsto \mathcal{P}(E/S) \times \mathcal{P}'(E/S).$$

If $\mathcal{P}$ is representable and $\mathcal{P}'$ is relatively representable, then $(\mathcal{P}, \mathcal{P}')$ is representable, and we have

$$\mathcal{M}(\mathcal{P}, \mathcal{P}') = \mathcal{P}'_{\mathbb{E}/\mathcal{M}(\mathcal{P})}$$

where $\mathbb{E}/\mathcal{M}(\mathcal{P})$ represents $\mathcal{P}$.

Given a representable moduli problem $\mathcal{P}$, the scheme $\mathcal{M}(\mathcal{P})$ represents the functor on Sch which sends a scheme S to the set

$$\left\{ \begin{array}{l} \text{isomorphism classes of pairs } (E/S, x) \text{ with} \\ \quad E \text{ an elliptic curve over } S \text{ and} \\ \quad x \in \mathcal{P}(E/S) \text{ a } \mathcal{P}\text{-structure on } E/S \end{array} \right\}.$$

Motivated by this, we give the following definition of a more general class of morphisms between moduli problems. It allows the flexibility to consider isomorphism classes, rather than individual objects, of elliptic curves equipped with level structures. In particular, such a morphism between two representable moduli problems induces a morphism of their representing moduli schemes, free of reference to the universal elliptic curves over these schemes (see Examples 4.5.16 and 4.5.18).

Definition 4.5.7. An *exotic morphism* $\mathcal{P} \to \mathcal{P}'$ *of moduli problems* is a rule which to

every scheme S and every elliptic curve E/S with $\mathcal{P}$-structure $x \in \mathcal{P}(E/S)$, assigns an elliptic curve E'/S with $\mathcal{P}'$-structure $x' \in \mathcal{P}'(E'/S)$, and which to every morphism

$$\begin{array}{ccc} {\scriptstyle x_1=(\phi,\ f)^*(x)\in\mathcal{P}(E_1/S_1)}\ E_1 & \xrightarrow{\phi} & E\ {\scriptstyle x\in\mathcal{P}(E/S)} \\ \downarrow & & \downarrow \\ S_1 & \xrightarrow{f} & S \end{array}$$

in Ell assigns a morphism

$$\begin{array}{ccc} {\scriptstyle (x_1)'\in\mathcal{P}'(E_1'/S_1)}\ E_1' & \xrightarrow{\phi'} & E'\ {\scriptstyle x'\in\mathcal{P}'(E'/S)} \\ \downarrow & & \downarrow \\ S_1 & \xrightarrow{f} & S \end{array}$$

with the same f, such that

$$(x_1)' = (\phi',\ f)^*(x'),$$

and such that the assignment $(\phi,\ f) \mapsto (\phi',\ f)$ is compatible with composition of morphisms in Ell.

In particular, the rule of an exotic morphism $\mathcal{P} \to \mathcal{P}'$ sends an isomorphism

$$\begin{array}{ccc} {\scriptstyle x_1=(\phi,\ \mathrm{id}_S)^*(x)\in\mathcal{P}(E_1/S)}E_1 & \underset{\phi^{-1}}{\overset{\phi}{\rightleftarrows}} & E{\scriptstyle x=(\phi^{-1},\ \mathrm{id}_S)^*(x_1)\in\mathcal{P}(E/S)} \\ \downarrow & & \downarrow \\ S & = & S \end{array}$$

to an isomorphism

$$\begin{array}{ccc} {\scriptstyle (x_1)'=(\phi',\ \mathrm{id}_S)^*(x')\in\mathcal{P}'(E_1'/S)}E_1' & \underset{(\phi')^{-1}}{\overset{\phi'}{\rightleftarrows}} & E'{\scriptstyle x'=\left((\phi')^{-1},\ \mathrm{id}_S\right)^*\left((x_1)'\right)\in\mathcal{P}'(E'/S)} \\ \downarrow & & \downarrow \\ S & = & S\,. \end{array}$$

Thus, if both $\mathcal{P}$ and $\mathcal{P}'$ are representable, passing to isomorphism classes the exotic morphism $\mathcal{P} \to \mathcal{P}'$ then induces a morphism $\mathcal{M}(\mathcal{P}) \to \mathcal{M}(\mathcal{P}')$ of schemes.

Remark 4.5.8. A morphism $\mathcal{P} \to \mathcal{P}'$ (see Definition 4.5.3) is an exotic morphism which to every scheme S and every elliptic curve E/S with $\mathcal{P}$-structure $x \in \mathcal{P}(E/S)$, assigns the *same* E/S with $\mathcal{P}'$-structure $x' \in \mathcal{P}'(E/S)$, and which to every morphism $(\phi,\ f)$ in Ell assigns the *same* $(\phi,\ f)$.

The definition of a moduli problem over the category Ell in Definition 4.5.3 and the related notions we have discussed thereafter generalize to the following category.

Definition 4.5.9 (cf. Definition 4.5.3)**.** For any ring R, let Ell/R be the category of elliptic curves over variable R-schemes, with morphisms the cartesian squares whose bottom arrow is R-linear.

Theorem 4.5.10 ([23, 3.7.1, 7.9.6, and 7.1.3(2)])**.** *Each of the five moduli problems* (4.5.1)*, as a relatively representable moduli problem over* $\mathrm{Ell}/\mathbb{Z}[1/m]$ *via the forgetful map* $\mathrm{Ell}/\mathbb{Z}[1/m] \to \mathrm{Ell}$*, is finite étale over* $\mathrm{Ell}/\mathbb{Z}[1/m]$*, i.e., for every elliptic curve* $E/S/\mathbb{Z}[1/m]$*, the morphism*

$$\begin{array}{c} \mathcal{P}_{E/S} \\ \big\downarrow \\ S \end{array}$$

is finite étale if $\mathcal{P}$ *is any of these moduli problems.*

Representability of the moduli problems (4.5.1) is more delicate. It involves the *rigidity* of a moduli problem, i.e., the property that the automorphism group of any elliptic curve acts freely on the set of level structures on the elliptic curve (see [23, 4.4, 4.7, and 2.7]). For example, $[\Gamma_1(m)]$ over $\mathrm{Ell}/\mathbb{Z}[1/m]$ is rigid if $m \geq 4$ by [23, 2.7.3], and thus combined with its relative representability from Theorem 4.5.5 and affineness from Theorem 4.5.10 it is representable over $\mathrm{Ell}/\mathbb{Z}[1/m]$ by [23, 4.7.0].

Another example is the moduli problem $[\omega]$ defined on objects by

$$[\omega](E/S) \coloneqq \{\text{nowhere-vanishing invariant one-forms on } E/S\}.$$

It is relatively representable over Ell, but not representable (see [23, 8.1.7.1]).

In practice, even if we know by general representability results that a moduli problem $\mathcal{P}$ is representable, we may not be able to work with $\mathcal{M}(\mathcal{P})$ explicitly. It is often interesting to consider simultaneous moduli problems $(\mathcal{P}, \mathcal{P}')$ and restrictions of $\mathcal{P}$ over certain Ell/R, and, when $\mathcal{P}$ is not representable, to consider a *coarse* moduli scheme as the best approximation to a representing object (see [23, Chapter 8]).

The moduli problem $[\Gamma_1(4)]$

We denote by

$$\mathcal{S} \coloneqq \big([\Gamma_1(4)], [\omega]\big) \quad \text{over} \quad \mathrm{Ell}/\mathbb{Z}[1/4] \tag{4.5.2}$$

the simultaneous moduli problem which carries the data of a point of exact order 4 and a nowhere-vanishing invariant one-form on each elliptic curve over a $\mathbb{Z}[1/4]$-scheme. It is representable, as we have seen above that over $\mathrm{Ell}/\mathbb{Z}[1/4]$, $[\Gamma_1(4)]$ is representable and $[\omega]$ is relatively representable. Explicitly we have the following (cf. [61, 4(4.6a)] and [50, Proposition 3.2 and Corollary 3.3]).

Proposition 4.5.11. *Notations as in Example 4.1.5, the moduli problem $\mathcal{S}$ over $\mathrm{Ell}/\mathbb{Z}[1/4]$ is represented by*

$$\begin{array}{c} C, \quad (P_0, \omega) \in \mathcal{S}(C/S^\bullet) \\ \big\downarrow \\ \operatorname{Proj} S^\bullet. \end{array}$$

Proof. Let $E/S/\mathbb{Z}[1/4]$ be an elliptic curve with $(Q, \eta) \in \mathcal{S}(E/S)$, locally on $\operatorname{Spec} R \subset S$ given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $Q = (x_0, y_0)$. We need only show that there is a unique R-isomorphism from E to $C \otimes_{S^\bullet} R$ which sends (Q, η) to (P_0, ω), where the map $S^\bullet \to R$ in $C \otimes_{S^\bullet} R$ is given by $a \mapsto a_1'$ and $b \mapsto a_2'$ for some a_1', $a_2' \in R$ uniquely determined below.

Recall from Section 4.1 that the only change of variables fixing the identity and preserving the form of a Weierstrass equation is

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + u^2sx' + t \tag{4.5.3}$$

where r, s, $t \in R$ and $u \in R^\times$. We make a sequence of changes of variables, where x' and y' are the variables after each change satisfying a Weierstrass equation with adjusted coefficients (cf. Example 4.4.13):

- set
$$x = x' + x_0 \qquad \text{and} \qquad y = y' + y_0$$
which sends Q to $P_0 = (0, 0)$, and x' and y' satisfy
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x$$
with
$$\dot{y}(0, 0) \coloneqq \frac{dy}{dx}(0, 0) = \frac{a_4}{a_3}$$
(the fact that Q has exact order 4 forces a_3 to be invertible);

- set
$$x = x' \qquad \text{and} \qquad y = y' + \frac{a_4}{a_3} \cdot x$$
which fixes P_0 and makes $\dot{y}(0, 0) = 0$, and x' and y' satisfy
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2$$
with $(-a_2, 0) = 2P_0$ a 2-torsion point so that $a_3 = a_1a_2$ (we have formally $\dot{y}(-a_2, 0) = a_2^2/(a_3 - a_1a_2)$);

- set
$$x = u^2x' \qquad \text{and} \qquad y = u^3y'$$
for some $u \in R^\times$ to scale the image of η under the previous changes of variables into ω.

These steps exhaust the coefficients in (4.5.3) and give a unique R-isomorphism from E

to an elliptic curve with Weierstrass equation

$$y^2 + a_1' xy + a_1' a_2' y = x^3 + a_2' x^2$$

for some a_1', $a_2' \in R$. This is $C/S^\bullet$ along the base change

$$\begin{aligned} S^\bullet &\longrightarrow R \\ a &\mapsto a_1', \\ b &\mapsto a_2'. \end{aligned}$$

□

From Proposition 4.5.11 above, we see that $\mathcal{M}(\mathcal{S}) = \operatorname{Proj} S^\bullet$ where

$$S^\bullet = \mathbb{Z}[1/4][a, b, \Delta^{-1}]$$

with $|a| = 1$, $|b| = 2$, and $\Delta = a^2 b^4 (a^2 - 16b)$. To work with this moduli scheme, we consider the weighted projective space

$$\operatorname{Proj} \mathbb{Z}[1/4][a, b].$$

For every element f homogeneous of positive degree in $\mathbb{Z}[1/4][a, b]$, there is a distinguished open subset

$$\operatorname{Proj} \mathbb{Z}[1/4][a, b][f^{-1}] \cong \operatorname{Spec} \left(\mathbb{Z}[1/4][a, b][f^{-1}]\right)^0.$$

In particular, taking $f = \Delta$, we see that $\mathcal{M}(\mathcal{S})$ is an affine open subscheme of the weighted projective space $\operatorname{Proj} \mathbb{Z}[1/4][a, b]$. Moreover, in the étale topology, this weighted projective space is covered by two affine coordinate charts: the first one is

$$\operatorname{Proj} \mathbb{Z}[1/4][a, b][a^{-1}] \cong \operatorname{Spec} \mathbb{Z}[1/4]\left[\frac{b}{a^2}\right],$$

which is open and contains $\mathcal{M}(\mathcal{S})$ (inverting Δ automatically inverts a); the second one

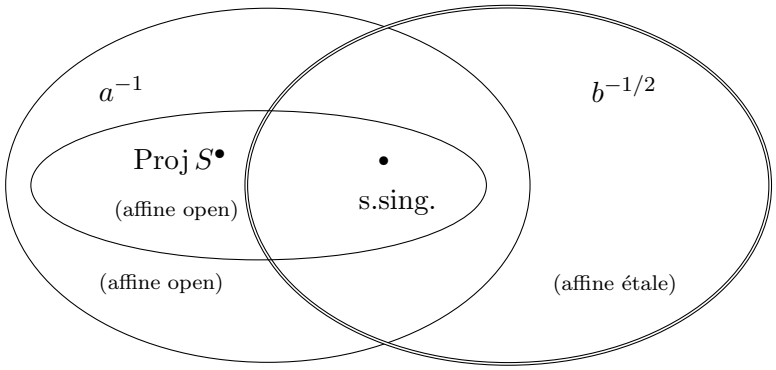
is

$$\operatorname{Proj} \mathbb{Z}[1/4][a,b][u^{-1}] \cong \operatorname{Spec} \mathbb{Z}[1/4]\left[\frac{a}{u}\right]$$

with u an adjoined element such that $u^2 = b$, which is finite étale with Galois group $\{\pm 1\}$ (2 is invertible on $\operatorname{Proj} \mathbb{Z}[1/4][a,b]$). Both coordinate charts contain the supersingular locus at the prime 3 which we identified in Example 4.3.4 as a single closed point

$$\operatorname{Proj} S^\bullet/(3,H) \cong \operatorname{Spec} \mathbb{F}_3$$

where $H = a^2 + b$. We summarize the above in a diagram.



(4.5.4)

In view of Proposition 4.5.11, $C/S^\bullet$ is a universal deformation of the supersingular elliptic curve $C_0/\mathbb{F}_3$ (see (4.3.5)). Recall from Section 3.1 that the formal group associated to a Morava E-theory is the universal deformation of a formal group over a perfect field to the corresponding Lubin-Tate ring. We can now produce a Morava E-theory spectrum from the above universal deformation of a supersingular elliptic curve via the Serre-Tate theorem (Theorem 4.3.1).

Example 4.5.12. We follow the convention that elements in algebraic degree n lie in topological degree $2n$, and work in the affine étale coordinate chart "$b^{-1/2}$" in (4.5.4). Write $c \coloneqq a/u$ so that

$$a = uc \qquad \text{and} \qquad b = u^2.$$

Consider the graded ring

$$S^\bullet[u^{-1}] \cong \mathbb{Z}[1/4][a, \Delta^{-1}][u^{\pm 1}]$$

where $|u| = 1$, and write

$$S \coloneqq \left(S^\bullet[u^{-1}]\right)^0 \cong \mathbb{Z}[1/4][c, \delta^{-1}]$$

where $\delta = u^{-12}\Delta = c^2(c^2 - 16)$. Thus $\operatorname{Spec} S$ is the restriction of $\mathcal{M}(\mathcal{S})$ to this affine étale coordinate chart.

Write

$$\widehat{S} \coloneqq \mathbb{Z}_9[\![h]\!]$$

where

$$h \coloneqq u^{-2}H = c^2 + 1. \tag{4.5.5}$$

Let i be an element generating $\mathbb{Z}_9$ over $\mathbb{Z}_3$ with $i^2 = -1$. Henceforth we fix an isomorphism $\mathbb{Z}_9 \cong \mathbb{Z}_3[i]$, and it induces $\mathbb{F}_9 \cong \mathbb{F}_3(i)$. We may choose

$$c \equiv i \mod (3, h)$$

and we have

$$\delta \equiv -1 \mod (3, h)$$

where $(3, h)$ is the maximal ideal of the complete local ring $\widehat{S}$. Then by Hensel's lemma, both c and δ lie in $\widehat{S}$, and both are invertible. Thus

$$\widehat{S} \cong S^\wedge_{(3,h)}.$$

Now C restricts to S as

$$y^2 + cxy + cy = x^3 + x^2, \tag{4.5.6}$$

and $\widehat{C}$ is a formal group over $\widehat{S}$. In view of (4.5.5) and (4.3.4), its reduction to $\widehat{S}/(3, h) \cong \mathbb{F}_9$ is $\widehat{C}_0$, which is a formal group of height 2. By Theorem 4.3.1 and Proposition 4.5.11, $C[3^\infty]$ is the universal deformation of $C_0[3^\infty]$ as 3-divisible groups. Since $\operatorname{ht}(\widehat{C}_0) = 2$, $C_0[3^\infty]$ is all formal (see Section 4.3), i.e.,

$$C_0[3^\infty] = \left(C_0[3^\infty]\right)^0 \cong \widehat{C}_0.$$

Thus $\widehat{C} \cong \big(C[3^\infty]\big)^0$ is the universal deformation of $\widehat{C}_0$ as formal groups. Let E be the Morava E-theory spectrum associated to $\widehat{C}_0/\mathbb{F}_9$. Then

$$E_* \cong \mathbb{Z}_9[\![h]\!][u^{\pm 1}]$$

where u is in topological degree 2, and it corresponds to a local uniformizer at the identity of C.

Remark 4.5.13. In view of (4.1.4), $[\omega]$ is a $\mathbb{G}_m$-torsor over Ell, and the induced action of $\mathbb{G}_m$ on $C/S^\bullet$ fixes $P_0(0,0) \in [\Gamma_1(4)](C/S^\bullet)$. Thus over $\mathrm{Ell}/\mathbb{Z}[1/4]$ we have

$$\mathcal{M}\big([\Gamma_1(4)]\big) \cong \mathcal{M}\big([\Gamma_1(4)], [\omega]\big)/\mathbb{G}_m$$

(cf. [23, 7.1.3] and [66, Theorem 1.10]). As $S = \big(S^\bullet[u^{-1}]\big)^0$ consists of the $\mathbb{G}_m$-invariants of $S^\bullet[u^{-1}]$, locally over $\mathcal{M}\big([\Gamma_1(4)]\big)$ the universal elliptic curve with a $\Gamma_1(4)$-structure is then given by (4.5.6).

The moduli problem $[\Gamma_0(3)]$

We denote by

$$\mathcal{S}_3 \coloneqq \big([\Gamma_0(3)], \mathcal{S}\big) \quad \text{over} \quad \mathrm{Ell}/\mathbb{Z}[1/4]$$

the simultaneous moduli problem which carries the data of a cyclic subgroup of degree 3 (cf. Definition 4.5.1 (iv)) together with the data of $\mathcal{S}$ (see (4.5.2)) on each elliptic curve over a $\mathbb{Z}[1/4]$-scheme. It is representable, as $[\Gamma_0(3)]$ is relatively representable and $\mathcal{S}$ is representable (see Theorem 4.5.5 and Proposition 4.5.11).

Recall from Proposition 4.4.2 (i) that we constructed the universal degree-3 isogeny ψ with source C over the graded ring $S_3^\bullet$. In view of [23, 6.8.7] we then have

$$\mathcal{M}(\mathcal{S}_3) \cong [\Gamma_0(3)]_{C/S^\bullet} \cong \operatorname{Proj} S_3^\bullet.$$

As $S_3^\bullet = S^\bullet[\kappa]/\big(W(\kappa)\big)$ is an $S^\bullet$-module of rank 4, $\operatorname{Proj} S_3^\bullet$ is affine and is covered by two affine coordinate charts which are extensions of those in (4.5.4).

Example 4.5.14. Notations as in Example 4.5.12, the restriction of this moduli scheme

$\mathcal{M}(\mathcal{S}_3)$ to the affine étale coordinate chart "$b^{-1/2}$" is $\operatorname{Spec} S_3$ where

$$S_3 \coloneqq S[\alpha]/\big(w(\alpha)\big) \tag{4.5.7}$$

with

$$w(\alpha) = \alpha^4 - 6\alpha^2 + (c^2 - 8)\alpha - 3.$$

In particular, we have

$$[\Gamma_0(3)]_{\widehat{C}/\,\widehat{S}} \cong \operatorname{Spec} \mathbb{Z}_9[\![h, \alpha]\!]/\big(\alpha^4 - 6\alpha^2 + (h-9)\alpha - 3\big),$$

which exhibits the moduli problem $[\Gamma_0(3)]$ as an *open arithmetic surface* with two parameters h and α (we have $3 = \alpha^4 - 6\alpha^2 + (h-9)\alpha$). More precisely, we have seen in Example 4.5.12 that $\widehat{C}/\mathbb{Z}_9[\![h]\!]$ is the universal formal deformation of the supersingular elliptic curve $C_0/\mathbb{F}_9$ with u a local uniformizer. The first parameter $h = H(C/S, \omega)$ (see (4.5.5) and (4.3.4)) arises as a parameter for this deformation (cf. [23, 12.4.4]). We have seen in Remark 4.4.4 that

$$\kappa = u(Q) \cdot u(-Q)$$

where Q is a nonzero 3-torsion point on C generating the universal degree-3 subgroup G. Thus, as the restriction of κ over S_3, the second parameter α arises as the norm

$$N\big(u(Q)\big) \coloneqq \prod_{\sigma \in \operatorname{Aut}(G)} u(\sigma \cdot Q).$$

There is a second parametrization for $[\Gamma_0(3)]$ given by α and α' where α' is the restriction of κ' over S_3 (see Corollary 4.4.8). We have

$$[\Gamma_0(3)]_{\widehat{C}/\,\widehat{S}} \cong \operatorname{Spec} \mathbb{Z}_9[\![\alpha, \alpha']\!]/(\alpha\alpha' + 3)$$

and

$$\alpha' = -h - \alpha^3 + 6\alpha + 9.$$

These are examples of the two parametrizations for $[\Gamma_0(p^n)]$ listed in [23, 7.7].

Remark 4.5.15. Another viewpoint for the moduli scheme $\mathcal{M}(\mathcal{S}_3)$ is that (4.5.7) exhibits the moduli problem $\mathcal{S}_3$ as a *relative curve over* $\operatorname{Spec}\mathbb{Z}$. Its *compactification* $\overline{\mathcal{M}}(\mathcal{S}_3)[1/6]$ is a proper smooth curve over $\mathbb{Z}[1/6]$ with geometrically connected fibers, in which the *scheme of cusps* is finite étale over $\mathbb{Z}[1/6]$ (see [23, 8.6 and 10.9.5]). This is an example of the moduli problem $\big([\Gamma_1(N_1)], [\Gamma_0(N_2)]\big)$, with N_1 and N_2 relatively prime and $N_1 \geq 4$, listed in [23, 10.9.6].

Exotic endomorphisms of $[\Gamma_1(4)]$ and $[\Gamma_0(3)]$

Recall from Definition 4.5.7 that an exotic morphism $\mathcal{P} \to \mathcal{P}'$ of moduli problems sends each pair $\big(E/S,\ x \in \mathcal{P}(E/S)\big)$ to $\big(E'/S,\ x' \in \mathcal{P}'(E'/S)\big)$. The constructions in Propositions 4.4.2 and 4.4.7 each gives rise to an example of an exotic endomorphism.

Example 4.5.16. We continue with the notations in Example 4.5.14 and work in the affine étale coordinate chart "$b^{-1/2}$." By Proposition 4.4.2 (i), in xy-coordinates, C' restricts to S_3 as

$$y^2 + c'xy + c'y = x^3 + x^2$$

where

$$c' = \frac{1}{c}\big((c^2-4)\alpha^3 + 4\alpha^2 + (-6c^2+20)\alpha + c^4 - 12c^2 + 12\big).$$

Since this equation is in the form of (4.5.6), the isogeny ψ determines an assignment

$$\big(C/S_3,\quad P_0(0,0) \in [\Gamma_1(4)](C/S_3)\big) \longmapsto \big(C'/S_3,\quad P_0(0,0) \in [\Gamma_1(4)](C'/S_3)\big). \tag{4.5.8}$$

By Proposition 4.5.11 and Remark 4.5.13, over the affine étale coordinate chart "$b^{-1/2}$," we have a universal pair

$$\big(C/S,\quad P_0(0,0) \in [\Gamma_1(4)](C/S)\big)$$

for the moduli problem $[\Gamma_1(4)]$ over $\mathrm{Ell}/\mathbb{Z}[1/4]$. However, in (4.5.8), S_3 is an extension of S, and C' is not defined over S. To get an exotic endomorphism of $[\Gamma_1(4)]$, we consider its restriction over $\mathbb{F}_9$ to a formal neighborhood of the supersingular locus, where we have $\alpha = 0$ (cf. (4.4.13)). The above assignment then sends

$$C\colon\ y^2 + cxy + cy = x^3 + x^2, \qquad P_0(0,0)$$

to

$$C' \colon\ y^2 + c^3xy + c^3y = x^3 + x^2, \qquad P_0(0,0).$$

In particular, under this further restriction, locally we have an induced endomorphism of the moduli scheme $\mathcal{M}([\Gamma_1(4)]) \cong \operatorname{Spec} S$ which sends c to c^3.

Remark 4.5.17. In contrast, over the affine open coordinate chart "a^{-1}," although the assignment analogous to (4.5.8) locally induces an endomorphism of the moduli scheme near the supersingular locus, it does not lift to an assignment *within* the chart. Precisely, if we denote by $\tilde{c}$ and $\tilde{\alpha}$ the analogs of c and α respectively, we have

$$C \colon\ y^2 + xy + \tilde{c}y = x^3 + \tilde{c}x^2$$

and

$$C' \colon\ y^2 + rxy + r\tilde{c}^3y = x^3 + \tilde{c}^3x^2$$

where

$$\begin{aligned} r &= (-4\tilde{c}^5 + \tilde{c}^4)\tilde{\alpha}^3 + 4\tilde{c}^4\tilde{\alpha}^2 + (20\tilde{c}^3 - 6\tilde{c}^2)\tilde{\alpha} + 12\tilde{c}^2 - 12\tilde{c} + 1 \\ &\neq 1. \end{aligned}$$

This makes the chart less convenient for the purpose of studying power operations (cf. the proof of Corollary 5.2.1 below), particularly their compositions.

Example 4.5.18. In [23, 11.3.1] (cf. [67, Lemmas 7-10]), for every integer $m \geq 1$, the *involution* W_m *of* $[\Gamma_0(m)]$ is defined as an exotic endomorphism of $[\Gamma_0(m)]$ which sends

$$(E/S, \quad \text{cyclic subgroup } G \text{ of degree } m) \quad \text{to} \quad \big(E'/S \coloneqq (E/G)/S, \quad G' \coloneqq E[m]/G\big)$$

(the subgroup G' is cyclic of degree m by Theorem 4.2.1 and [23, 12.2.5]).

By construction of ψ' in Proposition 4.4.7, locally over the affine étale coordinate chart "$b^{-1/2}$," we have an involution of the moduli problem $\big([\Gamma_0(3)], [\Gamma_1(4)]\big)$ which sends

$$(C/S_3, \quad \psi, \quad P_0) \qquad \text{to} \qquad (C'/S_3, \quad \psi', \quad P_0).$$

In particular, by Proposition 4.4.2 (i) and Corollary 4.4.8, the induced endomorphism t

of the moduli scheme $\operatorname{Spec} S_3$ is given by

$$\begin{aligned} c &\longmapsto \frac{1}{c}\big((c^2-4)\alpha^3+4\alpha^2+(-6c^2+20)\alpha+c^4-12c^2+12\big), \\ \alpha &\longmapsto -\alpha^3+6\alpha-c^2+8, \end{aligned}$$

and we have $t \circ t = \mathrm{id}$ (cf. [50, Section 5]).

Chapter 5

An example of the power operation structure on an elliptic cohomology theory

5.1 Summary of the main example in Chapter 4

Recall from Section 3.1 that a Morava E-theory of height 2 at the prime 3 has its formal group as the universal deformation of a height-2 formal group over a perfect field of characteristic 3. In Example 4.5.12 we produced such an E-theory spectrum from a universal deformation of a supersingular elliptic curve over $\mathbb{F}_9$.

Proposition 5.1.1 (cf. Proposition 4.5.11 and Remark 4.5.13)**.** *Over $\mathbb{Z}[1/4]$, the moduli problem of elliptic curves with a choice of a point of exact order 4 is representable. Locally for the étale topology on the moduli scheme, the universal elliptic curve is given by*

$$C\colon\ y^2 + cxy + cy = x^3 + x^2, \tag{5.1.1}$$

with chosen point $(0,0)$, over the ring

$$S = \mathbb{Z}[1/4][c, \delta^{-1}]$$

where $\delta = c^2(c^2 - 16)$.

Let C_0 be the restriction of C to the supersingular locus

$$\operatorname{Spec} \mathbb{F}_9 \cong \operatorname{Spec} S/(3,h)$$

where $h = c^2 + 1$ (see Examples 4.3.4 and 4.5.12). The Morava E-theory spectrum E associated to $\widehat{C}_0/\mathbb{F}_9$ has homotopy groups

$$E_* \cong \mathbb{Z}_9[\![h]\!][u^{\pm 1}]$$

where $|h| = 0$ and $|u| = 2$. In particular,

$$E_0 \cong \mathbb{Z}_9[\![h]\!] \cong S^{\wedge}_{(3,h)}. \tag{5.1.2}$$

In Section 4.4 we first constructed a deformation of Frobenius from the following.

Proposition 5.1.2 (cf. Proposition 4.4.2 and Example 4.5.16)**.**

(i) The universal degree-3 isogeny ψ with source C is defined over the ring

$$S_3 = S[\alpha]\big/\big(w(\alpha)\big) \tag{5.1.3}$$

where

$$w(\alpha) = \alpha^4 - 6\alpha^2 + (c^2 - 8)\alpha - 3,$$

and has target the elliptic curve

$$C'\colon\ y^2 + c'xy + c'y = x^3 + x^2 \tag{5.1.4}$$

where

$$c' = \frac{1}{c}\big((c^2-4)\alpha^3 + 4\alpha^2 + (-6c^2+20)\alpha + c^4 - 12c^2 + 12\big).$$

(ii) The kernel G of ψ is generated by a point Q of exact order 3 with coordinates (d, e)

satisfying

$$\begin{aligned}\alpha = &-\frac{1}{c^2-16}\big(cd^7+(3c^2-2)d^6+(3c^3-6c)d^5+(c^4+c^2+2)d^4\\ &+(4c^3-15c)d^3+(c^2+2)d^2-12cd-18\big)\\ &= ce-d^2.\end{aligned} \tag{5.1.5}$$

(iii) The restriction of ψ to the supersingular locus at the prime 3 is the 3-power Frobenius endomorphism.

(iv) The induced map ψ^* on the relative cotangent space of C' at the identity sends du to αdu.

We then constructed a composite of deformations of Frobenius from the following.

Proposition 5.1.3 (cf. Proposition 4.4.7, Corollary 4.4.8, and Example 4.5.18)**.** *Notations as in the above proposition, let*

$$\psi' \colon C' \longrightarrow C'/G'$$

be the degree-3 isogeny over S_3 with kernel $G' = C[3]/G$. Then the following diagram of elliptic curves over S_3 commutes:

$$\begin{array}{ccc} C & \xrightarrow{\quad\psi\quad} & C/G = C' \\ & \searrow^{[-3]} & \downarrow{\scriptstyle \psi'} \\ & & C/C[3] \cong \frac{C/G}{C[3]/G} = \frac{C'}{G'}. \end{array} \tag{5.1.6}$$

Moreover the isogenies in this diagram induce maps on relative cotangent spaces at the identity, and we have a commutative diagram

$$\begin{array}{ccc} -3du = \alpha\alpha' du & \xleftarrow{\quad\psi^*\quad} & \alpha' du \\ & \nwarrow^{[-3]^*} & \uparrow{\scriptstyle (\psi')^*} \\ & du = du & \end{array}$$

where

$$\alpha' = -\alpha^3 + 6\alpha - c^2 + 8. \tag{5.1.7}$$

In the next section, via the bridge of Theorem 3.3.9 between deformations of Frobenius and power operations, we will compute power operations for the Morava E-theory E from Propositions 5.1.2 and 5.1.3 above.

5.2 $K(2)$-local power operations

Total power operations

Recall from Section 2.1 (cf. (2.1.6)) that there is an additive total power operation

$$\psi^3\colon\ E^0 \longrightarrow E^0 B\Sigma_3/I$$

where

$$I = \bigoplus_{0<i<3} \operatorname{image}\big(E^0 B(\Sigma_i \times \Sigma_{3-i}) \xrightarrow{\text{transfer}} E^0 B\Sigma_3\big).$$

The source of ψ^3 is

$$E^0 \cong \mathbb{Z}_9[\![h]\!] \cong S^{\wedge}_{(3,h)}$$

(cf. (5.1.2)), in which c and i are elements with $c^2 + 1 = h$ and $i^2 = -1$. The target of ψ^3 is

$$E^0 B\Sigma_3/I \cong \big(S_3\big)^{\wedge}_{(3,h)} \tag{5.2.1}$$

by Strickland's computation of Morava E-theory of symmetric groups (cf. [29, Theorem 1.1]). In view of (5.1.3) we then have

$$E^0 B\Sigma_3/I \cong E^0[\alpha]/\big(w(\alpha)\big). \tag{5.2.2}$$

Corollary 5.2.1. *The total power operation*

$$\psi^3\colon\ E^0 \longrightarrow E^0 B\Sigma_3/I \cong E^0[\alpha]/\big(w(\alpha)\big)$$

is given by

$$\begin{aligned}\psi^3(h) &= h^3 + (\alpha^3 - 6\alpha - 27)h^2 + 3(-6\alpha^3 + \alpha^2 + 36\alpha + 67)h \\ &\quad + 57\alpha^3 - 27\alpha^2 - 334\alpha - 342, \\ \psi^3(c) &= c^3 + (\alpha^3 - 6\alpha - 12)c - 4(\alpha+1)^2(\alpha-3)c^{-1}, \\ \psi^3(i) &= -i,\end{aligned}$$

where

$$\alpha \equiv 0 \mod 3. \tag{5.2.3}$$

Proof. By Theorem 3.3.9 there is a correspondence between the universal degree-3 isogeny ψ over S_3, which is a deformation of Frobenius, and the total power operation ψ^3. In particular, in view of (5.1.1) and (5.1.4), $\psi^3(c)$ is given by c'. As ψ^3 is a ring homomorphism, we then get the formula for $\psi^3(h) = \psi^3(c^2+1)$. We also have

$$\big(\psi^3(i)\big)^2 = \psi^3(-1) = -1,$$

which implies $\psi^3(i) = i$ or $-i$. We exclude the former possibility in view of the Frobenius congruence

$$\psi^3(i) \equiv i^3 \mod 3$$

(see Definition 3.3.7 and (3.4.2)). The congruence (5.2.3) follows from (4.3.6) and (5.1.5) (cf. (4.4.13)). □

More generally, let A be a $K(2)$-local commutative E-algebra. From Corollary 5.2.1 we have a total power operation

$$\psi^3\colon\ A_0 \longrightarrow A_0 \otimes_{E_0} (E^0 B\Sigma_3/I) \cong A_0[\alpha]/\big(w(\alpha)\big).$$

We also have a composite of total power operations

$$\begin{aligned} A_0 \xrightarrow{\psi^3} A_0 \otimes_{E_0} (E^0 B\Sigma_3/I) &\xrightarrow{\psi^3} \big(A_0 \otimes_{E_0} (E^0 B\Sigma_3/I)\big) \,{}^{\psi^3}\!\otimes_{E_0[\alpha]} (E^0 B\Sigma_3/I) \\ &\cong \Big(A_0[\alpha]/\big(w(\alpha)\big)\Big) \,{}^{\psi^3}\!\otimes_{E_0[\alpha]} \Big(E^0[\alpha]/\big(w(\alpha)\big)\Big) \end{aligned} \tag{5.2.4}$$

where the elements in the target $M \,{}^{\psi^3}\!\otimes_R N$ are subject to the equivalence relation

$$m \otimes (r \cdot n) \sim \big(m \cdot \psi^3(r)\big) \otimes n$$

for $m \in M$, $n \in N$, and $r \in R$, with

$$\psi^3(\alpha) = -\alpha^3 + 6\alpha - h + 9$$

by (5.1.7), as well as other relations in a usual tensor product.

Individual power operations

Recall from Section 2.1 (cf. (2.1.3)) that for each $\alpha \in \pi_0 \mathbb{P}^3_E(E) \cong E_0 B\Sigma_3$ there is an individual power operation Q_α given by pairing with α the total power operation P^3. In view of (5.2.2) we have additive individual power operations from the total power operation ψ^3 as follows.

Definition 5.2.2. Let A be a $K(2)$-local commutative E-algebra. Define the individual power operations

$$Q_k \colon A_0 \longrightarrow A_0$$

for $k = 0$, 1, 2, and 3 by

$$\psi^3(x) = Q_0(x) + Q_1(x)\alpha + Q_2(x)\alpha^2 + Q_3(x)\alpha^3.$$

Proposition 5.2.3. *The following relations hold among the individual power operations Q_0, Q_1, Q_2, and Q_3:*

(i) $Q_0(1) = 1, \quad Q_1(1) = Q_2(1) = Q_3(1) = 0$;

(ii) $Q_k(x + y) = Q_k(x) + Q_k(y)$ *for all* k;

(iii) Commutation relations

$$\begin{aligned} Q_0(hx) = {} & (h^3 - 27h^2 + 201h - 342)Q_0(x) + (3h^2 - 54h + 171)Q_1(x) \\ & + (9h - 81)Q_2(x) + 24Q_3(x), \end{aligned}$$

$$
\begin{aligned}
Q_1(hx) &= (-6h^2+108h-334)Q_0(x)+(-18h+171)Q_1(x)+(-72)Q_2(x)\\
&\quad +(h-9)Q_3(x),\\
Q_2(hx) &= (3h-27)Q_0(x)+8Q_1(x)+9Q_2(x)+(-24)Q_3(x),\\
Q_3(hx) &= (h^2-18h+57)Q_0(x)+(3h-27)Q_1(x)+8Q_2(x)+9Q_3(x),\\
Q_0(cx) &= (c^3-12c+12c^{-1})Q_0(x)+(3c-12c^{-1})Q_1(x)+(12c^{-1})Q_2(x)\\
&\quad +(-12c^{-1})Q_3(x),\\
Q_1(cx) &= (-6c+20c^{-1})Q_0(x)+(-20c^{-1})Q_1(x)+(-c+20c^{-1})Q_2(x)\\
&\quad +(4c-20c^{-1})Q_3(x),\\
Q_2(cx) &= (4c^{-1})Q_0(x)+(-4c^{-1})Q_1(x)+(4c^{-1})Q_2(x)+(-c-4c^{-1})Q_3(x),\\
Q_3(cx) &= (c-4c^{-1})Q_0(x)+(4c^{-1})Q_1(x)+(-4c^{-1})Q_2(x)+(4c^{-1})Q_3(x),\\
Q_k(ix) &= (-i)Q_k(x) \textit{ for all } k;
\end{aligned}
$$

(iv) Adem relations

$$
\begin{aligned}
Q_1Q_0(x) &= (-6)Q_0Q_1(x)+3Q_2Q_1(x)+(6h-54)Q_0Q_2(x)+18Q_1Q_2(x)\\
&\quad +(-9)Q_3Q_2(x)+(-6h^2+108h-369)Q_0Q_3(x)\\
&\quad +(-18h+162)Q_1Q_3(x)+(-54)Q_2Q_3(x),\\
Q_2Q_0(x) &= 3Q_3Q_1(x)+(-3)Q_0Q_2(x)+(3h-27)Q_0Q_3(x)+9Q_1Q_3(x),\\
Q_3Q_0(x) &= Q_0Q_1(x)+(-h+9)Q_0Q_2(x)+(-3)Q_1Q_2(x)\\
&\quad +(h^2-18h+63)Q_0Q_3(x)+(3h-27)Q_1Q_3(x)+9Q_2Q_3(x);
\end{aligned}
$$

(v) Cartan formulas

$$
\begin{aligned}
Q_0(xy) &= Q_0(x)Q_0(y)+3\big(Q_3(x)Q_1(y)+Q_2(x)Q_2(y)+Q_1(x)Q_3(y)\big)\\
&\quad +18Q_3(x)Q_3(y),\\
Q_1(xy) &= \big(Q_1(x)Q_0(y)+Q_0(x)Q_1(y)\big)\\
&\quad +(-h+9)\big(Q_3(x)Q_1(y)+Q_2(x)Q_2(y)+Q_1(x)Q_3(y)\big)\\
&\quad +3\big(Q_3(x)Q_2(y)+Q_2(x)Q_3(y)\big)+(-6h+54)Q_3(x)Q_3(y),
\end{aligned}
$$

$$\begin{aligned}
Q_2(xy) = {} & \big(Q_2(x)Q_0(y) + Q_1(x)Q_1(y) + Q_0(x)Q_2(y)\big) \\
& + 6\big(Q_3(x)Q_1(y) + Q_2(x)Q_2(y) + Q_1(x)Q_3(y)\big) \\
& + (-h+9)\big(Q_3(x)Q_2(y) + Q_2(x)Q_3(y)\big) + 39Q_3(x)Q_3(y), \\
Q_3(xy) = {} & \big(Q_3(x)Q_0(y) + Q_2(x)Q_1(y) + Q_1(x)Q_2(y) + Q_0(x)Q_3(y)\big) \\
& + 6\big(Q_3(x)Q_2(y) + Q_2(x)Q_3(y)\big) + (-h+9)Q_3(x)Q_3(y);
\end{aligned}$$

(vi) The Frobenius congruence

$$Q_0(x) \equiv x^3 \mod 3.$$

Proof. The relations in (i), (ii), (iii), and (v) follow computationally from the formulas in Corollary 5.2.1 together with the fact that ψ^3 is a ring homomorphism.

For (iv), there is a canonical isomorphism $C/C[3] \cong C$ of elliptic curves over $S \subset S_3$. Given the correspondence between deformations of Frobenius and power operations in Theorem 3.3.9, the commutativity of (5.1.6) then implies that the composite (5.2.4) lands in A_0. In terms of formulas, we have

$$\begin{aligned}
\psi^3\big(\psi^3(x)\big) &= \psi^3\big(Q_0(x) + Q_1(x)\alpha + Q_2(x)\alpha^2 + Q_3(x)\alpha^3\big) \\
&= \sum_{k=0}^{3} \psi^3\big(Q_k(x)\big)\big(\psi^3(\alpha)\big)^k \\
&= \sum_{k=0}^{3}\sum_{j=0}^{3} Q_jQ_k(x)\alpha^j(-\alpha^3 + 6\alpha - h + 9)^k \\
&\equiv \Psi_0(x) + \Psi_1(x)\alpha + \Psi_2(x)\alpha^2 + \Psi_3(x)\alpha^3 \mod \big(w(\alpha)\big)
\end{aligned}$$

where each Ψ_i is an E_0-linear combination of the Q_jQ_k's. The vanishing of $\Psi_1(x)$, $\Psi_2(x)$, and $\Psi_3(x)$ gives the three relations in (iv).

The congruence in (vi) follows from (5.2.3) and the Frobenius congruence

$$\psi^3(x) \equiv x^3 \mod 3$$

satisfied by ψ^3 (see Definition 3.3.7 and (3.4.2)). □

Example 5.2.4. We have $E^0S^2 \cong \mathbb{Z}_9[\![h]\!][u]/(u^2)$. By definition of κ in (4.4.5), the Q_k's

act canonically on $u \in E^0S^2$:

$$Q_k(u) = \begin{cases} u, & \text{if } k = 1, \\ 0, & \text{if } k \neq 1. \end{cases}$$

We then get the values of the Q_k's on elements in E^0S^2 from Proposition 5.2.3 (i)-(iii).

5.3 The $K(2)$-local Dyer-Lashof algebra

Definition 5.3.1.

(i) Let i be an element generating $\mathbb{Z}_9$ over $\mathbb{Z}_3$ with $i^2 = -1$. Define γ to be the associative ring generated over $\mathbb{Z}_9[\![h]\!]$ by elements q_0, q_1, q_2, and q_3 subject to the following relations: the q_k's commute with elements in $\mathbb{Z}_3 \subset \mathbb{Z}_9[\![h]\!]$, and satisfy *commutation relations*

$$\begin{aligned}
q_0h &= (h^3 - 27h^2 + 201h - 342)q_0 + (3h^2 - 54h + 171)q_1 + (9h - 81)q_2 \\
&\quad + 24q_3, \\
q_1h &= (-6h^2 + 108h - 334)q_0 + (-18h + 171)q_1 + (-72)q_2 + (h - 9)q_3, \\
q_2h &= (3h - 27)q_0 + 8q_1 + 9q_2 + (-24)q_3, \\
q_3h &= (h^2 - 18h + 57)q_0 + (3h - 27)q_1 + 8q_2 + 9q_3, \\
q_ki &= (-i)q_k \text{ for all } k,
\end{aligned}$$

and *Adem relations*

$$\begin{aligned}
q_1q_0 &= (-6)q_0q_1 + 3q_2q_1 + (6h - 54)q_0q_2 + 18q_1q_2 + (-9)q_3q_2 \\
&\quad + (-6h^2 + 108h - 369)q_0q_3 + (-18h + 162)q_1q_3 + (-54)q_2q_3, \\
q_2q_0 &= 3q_3q_1 + (-3)q_0q_2 + (3h - 27)q_0q_3 + 9q_1q_3, \\
q_3q_0 &= q_0q_1 + (-h + 9)q_0q_2 + (-3)q_1q_2 + (h^2 - 18h + 63)q_0q_3 \\
&\quad + (3h - 27)q_1q_3 + 9q_2q_3.
\end{aligned}$$

(ii) Write $\omega \coloneqq \pi_2E$, viewed as a free module with one generator u over $E_0 \cong \mathbb{Z}_9[\![h]\!]$.

Define ω as a left γ-module, compatible with its E_0-module structure, such that

$$q_k \cdot u \coloneqq \begin{cases} u, & \text{if } k = 1, \\ 0, & \text{if } k \neq 1. \end{cases}$$

In the above definition, an element $s \in \mathbb{Z}_9[\![h]\!] \cong E_0$ corresponds to the multiplication-by-s operation, and each q_k corresponds to the individual power operation Q_k in Section 5.2. Under this correspondence, the relations in Proposition 5.2.3 (ii)-(v) describe explicitly the structure of γ as that of a twisted bialgebra over E_0 (cf. Definition 3.2.1).

There is a grading on γ coming from the number of the q_k's in a monomial. For example, commutation relations are in degree 1, and Adem relations are in degree 2. Under these relations, γ has an *admissible basis*: it is free as a left E_0-module on the elements of the form

$$q_0^m q_{k_1} \cdots q_{k_n} \tag{5.3.1}$$

where $m, n \geq 0$ ($n = 0$ gives q_0^m), and $k_i = 1$, 2, or 3. If we write $\gamma[r]$ for the degree-r part of γ, then $\gamma[r]$ is of rank $1 + 3 + \cdots + 3^r$.

We now identify γ with the Dyer-Lashof algebra of power operations on $K(2)$-local commutative E-algebras.

Theorem 5.3.2 (cf. Theorem 3.2.6)**.** *Let A be a $K(2)$-local commutative E-algebra. Let γ be the graded twisted bialgebra over E_0 in Definition 5.3.1* (i)*, and ω be the γ-module in Definition 5.3.1* (ii)*. Then A_* has the structure of an ω-twisted $\mathbb{Z}/2$-graded amplified γ-ring. In particular,*

$$\pi_* L_{K(2)} \mathbb{P}_E(\Sigma^d E) \cong \big(R_d\big)^{\wedge}_{(3,h)}$$

where R_d is the free graded amplified γ-ring with one generator in dimension d.

Proof. Let Γ be the graded twisted bialgebra of power operations on E_0 in [22, Section 6]. We need only identify Γ with γ.

There is a direct sum decomposition $\Gamma = \bigoplus_{r \geq 0} \Gamma[r]$ where the summands come from the completed E-homology of $B\Sigma_{3^r}$ (see [22, 6.2]). We have a degree-preserving ring

homomorphism

$$\begin{aligned} \phi\colon \gamma &\longrightarrow \Gamma \\ q_k &\mapsto Q_k, \end{aligned}$$

which is an isomorphism in degrees 0 and 1. We need to show that ϕ is both surjective and injective in all degrees.

For the surjectivity of ϕ, we use a transfer argument. We have

$$\nu_3(|\Sigma_3^{\wr r}|) = \nu_3(|\Sigma_{3^r}|) = (3^r - 1)/2$$

where $\nu_3(-)$ is the 3-adic valuation, and $(-)^{\wr r}$ is the r-fold wreath product. Thus following the proof of [22, Proposition 3.17], we see that Γ is generated in degree 1, and hence ϕ is surjective.

By (5.3.1) and (the E_0-linear dual of) [29, Theorem 1.1], $\gamma[r]$ and $\Gamma[r]$ are of the same rank $1 + 3 + \cdots + 3^r$ as free modules over E_0. Hence ϕ is also injective. □

5.4 $K(1)$-local power operations

Recall from Section 3.4 that the power operation structure on a $K(1)$-local Morava E-theory at the prime p (with p-torsion-free homotopy groups) is determined by a single power operation corresponding to the unique degree-p subgroup of the formal group. We now compute power operations on the $K(1)$-localization of E from our calculations of $K(2)$-local power operations in Section 5.2.

Let $F \coloneqq L_{K(1)}E$ be the $K(1)$-localization of E. The following diagram describes the relationship between $K(1)$-local power operations on F^0 and the power operation on E^0 in Corollary 5.2.1:

$$\begin{array}{ccc} E^0 & \xrightarrow{\psi^3} & E^0 B\Sigma_3/I \\ \downarrow & & \downarrow \\ F^0 & \xrightarrow{\psi_F^3} & F^0 B\Sigma_3/J \cong F^0. \end{array}$$

Here ψ_F^3 is the $K(1)$-local power operation induced by ψ^3, and $J \cong F^0 \otimes_{E^0} I$ is the

transfer ideal. Recall from Proposition 5.1.2 (i), (5.2.1), and Corollary 5.2.1 that ψ^3 arises from the universal degree-3 isogeny which is parametrized by the ring S_3 with

$$\big(S_3\big)^{\wedge}_{(3,h)} \cong E^0 B\Sigma_3/I.$$

The vertical maps are induced by the $K(1)$-localization $E \to F$. In terms of homotopy groups, this is obtained by inverting the generator h and completing at the prime 3 (see [68, Corollary 1.5.5]):

$$E_* = \mathbb{Z}_9[\![h]\!][u^{\pm 1}] \qquad \text{and} \qquad F_* = \mathbb{Z}_9[\![h]\!][h^{-1}]^{\wedge}_3[u^{\pm 1}]$$

with

$$F_0 = \mathbb{Z}_9(\!(h)\!)^{\wedge}_3 = \left\{ \sum_{n=-\infty}^{\infty} k_n h^n \;\middle|\; k_n \in \mathbb{Z}_9, \lim_{n\to-\infty} k_n = 0 \right\}.$$

The formal group $\widehat{C}$ over E^0 has a unique degree-3 subgroup after being pulled back to F^0, and the map

$$E^0 B\Sigma_3/I \to F^0 B\Sigma_3/J \cong F^0$$

classifies this subgroup. Along the base change

$$E^0 B\Sigma_3/I \to F^0 \otimes_{E^0} (E^0 B\Sigma_3/I) \cong (F^0 \otimes_{E^0} E^0 B\Sigma_3)/J \cong F^0 B\Sigma_3/J,$$

the special fiber of the 3-divisible group of $\widehat{C}$ which consists solely of a formal component may split into formal and étale components (see Section 4.3). We want to take the formal component so as to keep track of the unique degree-3 subgroup of the formal group over F^0. This subgroup gives rise to the $K(1)$-local power operation ψ^3_F.

Recall from (5.1.3) that $S_3 = S[\alpha]/\big(w(\alpha)\big)$. Since

$$w(\alpha) = \alpha^4 - 6\alpha^2 + (h-9)\alpha - 3 \equiv \alpha(\alpha^3 + h) \mod 3,$$

the equation $w(\alpha) = 0$ has a unique root $\alpha = 0$ in $\mathbb{F}_9(\!(h)\!)$ (cf. (5.2.3)). By Hensel's lemma this unique root lifts to a root in $\mathbb{Z}_9(\!(h)\!)^{\wedge}_3$; it corresponds to the unique degree-3 subgroup of $\widehat{C}$ over F^0. Plugging this specific value of α into the formulas for ψ^3 in Corollary 5.2.1, we then get an endomorphism of the ring F^0. This endomorphism

is the $K(1)$-local power operation ψ_F^3, and it determines the other $K(1)$-local power operations by iterated composition.

Explicitly, with h invertible in F^0, we solve for α from $w(\alpha) = 0$ by first writing

$$\alpha = (3 + 6\alpha^2 - \alpha^4)/(h - 9) = (3 + 6\alpha^2 - \alpha^4) \sum_{n=1}^{\infty} 9^{n-1} h^{-n}$$

and then substituting this equation into itself recursively. We plug the power series expansion for α into $\psi^3(h)$ and get

$$\psi_F^3(h) = h^3 - 27h^2 + 183h - 180 + 186h^{-1} + 1674h^{-2} + (\text{lower-order terms}).$$

Similarly, writing h as $c^2 + 1$ in $w(\alpha) = 0$, we solve for α in terms of c and get

$$\psi_F^3(c) = c^3 - 12c - 6c^{-1} - 84c^{-3} - 933c^{-5} - 10956c^{-7} + (\text{lower-order terms}).$$

References

[1] David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields*. ProQuest LLC, Ann Arbor, MI, 1996. Thesis (Ph.D.)–University of California, Berkeley.

[2] J. F. Adams. Vector fields on spheres. *Ann. of Math. (2)*, 75:603–632, 1962.

[3] N. E. Steenrod and J. H. C. Whitehead. Vector fields on the n-sphere. *Proc. Nat. Acad. Sci. U. S. A.*, 37:58–63, 1951.

[4] J. F. Adams. On the non-existence of elements of Hopf invariant one. *Ann. of Math. (2)*, 72:20–104, 1960.

[5] J. P. C. Greenlees. How blind is your favourite cohomology theory? *Exposition. Math.*, 6(3):193–208, 1988.

[6] N. E. Steenrod. *Cohomology operations*. Lectures by N. E. Steenrod written and revised by D. B. A. Epstein. Annals of Mathematics Studies, No. 50. Princeton University Press, Princeton, N.J., 1962.

[7] José Adem. The iteration of the Steenrod squares in algebraic topology. *Proc. Nat. Acad. Sci. U. S. A.*, 38:720–726, 1952.

[8] Jean-Pierre Serre. Cohomologie modulo 2 des complexes d'Eilenberg-MacLane. *Comment. Math. Helv.*, 27:198–232, 1953.

[9] John Milnor. The Steenrod algebra and its dual. *Ann. of Math. (2)*, 67:150–171, 1958.

[10] Tammo tom Dieck. Steenrod-Operationen in Kobordismen-Theorien. *Math. Z.*, 107:380–401, 1968.

[11] Daniel Quillen. Elementary proofs of some results of cobordism theory using Steenrod operations. *Advances in Math.*, 7:29–56 (1971), 1971.

[12] James E. McClure. Dyer-Lashof operations in K-theory. *Bull. Amer. Math. Soc. (N.S.)*, 8(1):67–72, 1983.

[13] R. R. Bruner, J. P. May, J. E. McClure, and M. Steinberger. *H_∞ ring spectra and their applications*, volume 1176 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1986.

[14] Vladimir Voevodsky. Reduced power operations in motivic cohomology. *Publ. Math. Inst. Hautes Études Sci.*, (98):1–57, 2003.

[15] Matthew Ando, Michael J. Hopkins, and Neil P. Strickland. The sigma orientation is an H_∞ map. *Amer. J. Math.*, 126(2):247–334, 2004.

[16] Daniel Quillen. On the formal group laws of unoriented and complex cobordism theory. *Bull. Amer. Math. Soc.*, 75:1293–1298, 1969.

[17] Douglas C. Ravenel. *Nilpotence and periodicity in stable homotopy theory*, volume 128 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1992. Appendix C by Jeff Smith.

[18] Tyler Lawson. An overview of abelian varieties in homotopy theory. In *New topological contexts for Galois theory and algebraic geometry (BIRS 2008)*, volume 16 of *Geom. Topol. Monogr.*, pages 179–214. Geom. Topol. Publ., Coventry, 2009.

[19] Jack Morava. Forms of K-theory. *Math. Z.*, 201(3):401–428, 1989.

[20] Mike Hopkins and Mark Mahowald. From elliptic curves to homotopy theory. preprint, available at http://hopf.math.purdue.edu//Hopkins-Mahowald/eo2homotopy.pdf.

[21] J. Lurie. A survey of elliptic cohomology. In *Algebraic topology*, volume 4 of *Abel Symp.*, pages 219–277. Springer, Berlin, 2009.

[22] Charles Rezk. The congruence criterion for power operations in Morava E-theory. *Homology, Homotopy Appl.*, 11(2):327–379, 2009.

[23] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[24] Matthew Ando. Power operations in elliptic cohomology and representations of loop groups. *Trans. Amer. Math. Soc.*, 352(12):5619–5666, 2000.

[25] Nora Ganter. Stringy power operations in Tate K-theory. preprint, available at arXiv:0701565.

[26] Charles Rezk. Power operations for Morava E-theory of height 2 at the prime 2. preprint, available at arXiv:0812.1320.

[27] Matthew Ando. Isogenies of formal group laws and power operations in the cohomology theories E_n. *Duke Math. J.*, 79(2):423–485, 1995.

[28] M. F. Atiyah. Power operations in K-theory. *Quart. J. Math. Oxford Ser. (2)*, 17:165–193, 1966.

[29] N. P. Strickland. Morava E-theory of symmetric groups. *Topology*, 37(4):757–779, 1998.

[30] Charles Rezk. Power operations in Morava E-theory: a survey. slides for a talk at the Midwest Topology Seminar (Minneapolis, MN, 2009), available at http://www.math.uiuc.edu/~rezk/midwest-2009-power-ops-handout.pdf.

[31] Tyler Lawson and Niko Naumann. Commutativity conditions for truncated Brown-Peterson spectra of height 2. *J. Topol.*, 5(1):137–168, 2012.

[32] M. F. Atiyah and G. B. Segal. Equivariant K-theory and completion. *J. Differential Geometry*, 3:1–18, 1969.

[33] Graeme Segal. Equivariant K-theory. *Inst. Hautes Études Sci. Publ. Math.*, (34):129–151, 1968.

[34] Charles Rezk. Lectures on power operations. course notes, available at http://www.math.uiuc.edu/~rezk/power-operation-lectures.dvi.

[35] A. D. Elmendorf, I. Kriz, M. A. Mandell, and J. P. May. *Rings, modules, and algebras in stable homotopy theory*, volume 47 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997. With an appendix by M. Cole.

[36] Nathalie Wahl. Ribbon Braids and related operads. Thesis (Ph.D.)–University of Oxford, 2001, available at http://www.math.ku.dk/~wahl/wahlthesis.ps, 2001.

[37] F. William Lawvere. Functorial semantics of algebraic theories. *Proc. Nat. Acad. Sci. U.S.A.*, 50:869–872, 1963.

[38] Francis Borceux. *Handbook of categorical algebra. 2*, volume 51 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994. Categories and structures.

[39] Charles Rezk. Rings of power operations for Morava E-theories are Koszul. preprint, available at arXiv:1204.4831.

[40] Henri Cartan. Sur les groupes d'Eilenberg-Mac Lane. II. *Proc. Nat. Acad. Sci. U. S. A.*, 40:704–707, 1954.

[41] Robert E. Mosher and Martin C. Tangora. *Cohomology operations and applications in homotopy theory*. Harper & Row Publishers, New York, 1968.

[42] Mike Hopkins. Complex oriented cohomology theories and the language of stacks. course notes, available at http://www.math.rochester.edu/people/faculty/doug/otherpapers/coctalos.pdf.

[43] Jonathan Lubin and John Tate. Formal moduli for one-parameter formal Lie groups. *Bull. Soc. Math. France*, 94:49–59, 1966.

[44] Charles Rezk. Notes on the Hopkins-Miller theorem. In *Homotopy theory via algebraic geometry and group representations (Evanston, IL, 1997)*, volume 220 of *Contemp. Math.*, pages 313–366. Amer. Math. Soc., Providence, RI, 1998.

[45] P. G. Goerss and M. J. Hopkins. Moduli spaces of commutative ring spectra. In *Structured ring spectra*, volume 315 of *London Math. Soc. Lecture Note Ser.*, pages 151–200. Cambridge Univ. Press, Cambridge, 2004.

[46] Jacob Lurie. Chromatic homotopy theory. course notes, available at http://www.math.harvard.edu/~lurie/252x.html.

[47] A. K. Bousfield. The localization of spectra with respect to homology. *Topology*, 18(4):257–281, 1979.

[48] J. F. Adams. *Stable homotopy and generalised homology*. University of Chicago Press, Chicago, Ill., 1974. Chicago Lectures in Mathematics.

[49] M. Ando, M. J. Hopkins, and N. P. Strickland. Elliptic spectra, the Witten genus and the theorem of the cube. *Invent. Math.*, 146(3):595–687, 2001.

[50] Mark Mahowald and Charles Rezk. Topological modular forms of level 3. *Pure Appl. Math. Q.*, 5(2, Special Issue: In honor of Friedrich Hirzebruch. Part 1):853–872, 2009.

[51] Mark Hovey and Neil P. Strickland. Morava K-theories and localisation. *Mem. Amer. Math. Soc.*, 139(666):viii+100, 1999.

[52] Mark Hovey. Morava E-theory of filtered colimits. *Trans. Amer. Math. Soc.*, 360(1):369–382 (electronic), 2008.

[53] Neil P. Strickland. Finite subgroups of formal groups. *J. Pure Appl. Algebra*, 121(2):161–208, 1997.

[54] John Tate and Frans Oort. Group schemes of prime order. *Ann. Sci. École Norm. Sup. (4)*, 3:1–21, 1970.

[55] Clarence Wilkerson. Lambda-rings, binomial domains, and vector bundles over $\mathbf{C}P(\infty)$. *Comm. Algebra*, 10(3):311–328, 1982.

[56] M. J. Hopkins. $K(1)$-local E_∞ ring spectra. unpublished notes, available at http://www.math.rochester.edu/people/faculty/doug/otherpapers/knlocal.pdf.

[57] Jonathan Lubin. Finite subgroups and isogenies of one-parameter formal Lie groups. *Ann. of Math. (2)*, 85:296–302, 1967.

[58] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[59] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[60] Paul Pearson. Calculating formal group laws. unpublished notes, available at http://www.math.rochester.edu/people/faculty/pearson/papers/fgls-2up.pdf.

[61] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[62] J. T. Tate. p-Divisible groups. In *Proc. Conf. Local Fields (Driebergen, 1966)*, pages 158–183. Springer, Berlin, 1967.

[63] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127(6):1325–1387, 2005.

[64] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[65] L. Dewaghe. Isogénie entre courbes elliptiques. *Util. Math.*, 55:123–127, 1999.

[66] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)]*. Springer-Verlag, Berlin, third edition, 1994.

[67] A. O. L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[68] Mark A. Hovey. v_n-Elements in ring spectra and applications to bordism theory. *Duke Math. J.*, 88(2):327–356, 1997.

Appendix A

Long formulas

Here we list long formulas whose appearance in the main body might affect readability. The calculations involve power series expansions and manipulations of long polynomials with large coefficients (division, factorization, and finding greatest common divisors). They are done using the software *Wolfram Mathematica 8*. The commands `Reduce` and `Solve` are used to extract relations out of given identities.

A.1 Formulas in the proof of Proposition 4.2.3

$$\begin{aligned}
\widetilde{f}(u) =& -\frac{u^4}{a^2b}\big(b^4u^8+3ab^3u^7+3a^2b^2u^6+(a^3b+7ab^2)u^5+(6a^2b-6b^2)u^4\\
&+9abu^3+(-a^2+8b)u^2-3au-3\big),\\
Q_1(v) =& \, ab^2v^2+(b^2d^2+2abd-b)v+\frac{b^2d^4}{a}+2bd^3+ad^2-\frac{2bd^2}{a}-d+\frac{1}{a},\\
R_1(v) =& \, (\frac{b^3d^6}{a}+2b^2d^5+abd^4-\frac{3b^2d^4}{a}+2bd^3+\frac{3bd^2}{a}-\frac{1}{a})v+\frac{b^2d^7}{a}+2bd^6\\
&+ad^5-\frac{2bd^5}{a}+2d^4+\frac{d^3}{a},\\
Q_2(v) =& \, \frac{a}{(b^3d^6+2ab^2d^5+a^2bd^4-3b^2d^4+2abd^3+3bd^2-1)^2}\big((ab^4d^6+2a^2b^3d^5\\
&+a^3b^2d^4-3ab^3d^4+2a^2b^2d^3+3ab^2d^2-ab)v-b^4d^8-2ab^3d^7-a^2b^2d^6\\
&+4b^3d^6-ab^2d^5+a^2bd^4-6b^2d^4+4abd^3+4bd^2-ad-1\big),
\end{aligned}$$

$$
\begin{aligned}
R_2 = &-\frac{ad^4}{(b^3d^6+2ab^2d^5+a^2bd^4-3b^2d^4+2abd^3+3bd^2-1)^2}(b^4d^8+3ab^3d^7\\
&+3a^2b^2d^6+a^3bd^5+7ab^2d^5+6a^2bd^4-6b^2d^4+9abd^3-a^2d^2+8bd^2\\
&-3ad-3),\\
K(u) = &\frac{b^3u^6}{a}+2b^2u^5+(ab-\frac{3b^2}{a})u^4+2bu^3+\frac{3bu^2}{a}-\frac{1}{a},\\
L(u) = &\frac{b^2u^7}{a}+2bu^6+(a-\frac{2b}{a})u^5+2u^4+\frac{u^3}{a},\\
M(u) = &\frac{b}{a^2(a^2-16b)^2}\big((10a^3b^3-112ab^4)u^5+(19a^4b^2-217a^2b^3-16b^4)u^4\\
&+(8a^5b-126a^3b^2+304ab^3)u^3+(-a^6+34a^4b-266a^2b^2+32b^3)u^2\\
&+(28a^3b-384ab^2)u-4a^4+51a^2b-16b^2\big),\\
N(u) = &-\frac{1}{a(a^2-16b)^2}\big((10a^3b^5-112ab^6)u^7+(29a^4b^4-329a^2b^5-16b^6)u^6\\
&+(27a^5b^3-313a^3b^4-48ab^5)u^5+(7a^6b^2-15a^4b^3-837a^2b^4-16b^5)u^4\\
&+(-a^7b+66a^5b^2-714a^3b^3+528ab^4)u^3+(-4a^6b+137a^4b^2\\
&-1147a^2b^3+80b^4)u^2+(-12a^5b+237a^3b^2-1200ab^3)u+a^6-44a^4b\\
&+409a^2b^2-48b^3\big).
\end{aligned}
$$

A.2 Formulas in the proof of Proposition 4.4.2

The power series expansion of v in terms of u up to u^{12} is

$$
\begin{aligned}
v = &\,u^3-au^4+(a^2+b)u^5+(-a^3-3ab)u^6+(a^4+6a^2b+b^2)u^7+(-a^5-10a^3b\\
&-6ab^2)u^8+(a^6+15a^4b+20a^2b^2+b^3)u^9+(-a^7-21a^5b-50a^3b^2\\
&-10ab^3)u^{10}+(a^8+28a^6b+105a^4b^2+50a^2b^3+b^4)u^{11}+(-a^9-36a^7b\\
&-196a^5b^2-175a^3b^3-15ab^4)u^{12}.
\end{aligned}
$$

Using the formulas of the group law on C in Example 4.1.5, we plug the coordinates of $P-Q$ and $P+Q$ into (4.4.4). In view of (4.2.2), we then have in (4.4.5)

$$
\begin{aligned}
\kappa = &-\frac{1}{a^2-16b}\big(ab^3d^7+(3a^2b^2-2b^3)d^6+(3a^3b-6ab^2)d^5+(a^4+a^2b+2b^2)d^4\\
&+(4a^3-15ab)d^3+(a^2+2b)d^2-12ad-18\big),
\end{aligned}
$$

$$\lambda = -\frac{1}{a^2b^2(a^2-16b)}\big((a^3b^3-11ab^4)d^7+(3a^4b^2-33a^2b^3-4b^4)d^6+(3a^5b$$
$$-33a^3b^2-15ab^3)d^5+(a^6-4a^4b-96a^2b^2-4b^3)d^4+(6a^5-80a^3b$$
$$+31ab^2)d^3+(10a^4-153a^2b+20b^2)d^2+(3a^3-117ab)d-6a^2-12b\big).$$

More extended power series expansions in u for u' (up to u^6) and v' (up to u^9) are needed in (4.4.5) to determine the coefficients in the equation of C':

$$u' = -\frac{1}{a^2-16b}\big((ab^3d^7+3a^2b^2d^6-2b^3d^6+3a^3bd^5-6ab^2d^5+a^4d^4+a^2bd^4$$
$$+2b^2d^4+4a^3d^3-15abd^3+a^2d^2+2bd^2-12ad-18)u+(-a^2b^3d^7$$
$$+12b^4d^7-3a^3b^2d^6+36ab^3d^6-3a^4bd^5+36a^2b^2d^5+4b^3d^5-a^5d^4$$
$$+5a^3bd^4+94ab^2d^4-6a^4d^3+85a^2bd^3-76b^2d^3-9a^3d^2+136abd^2+60bd$$
$$+6a)u^2+(a^3b^3d^7-17ab^4d^7+3a^4b^2d^6-50a^2b^3d^6-8b^4d^6+3a^5bd^5$$
$$-48a^3b^2d^5-27ab^3d^5+a^6d^4-7a^4bd^4-150a^2b^2d^4-16b^3d^4+7a^5d^3$$
$$-113a^3bd^3+9ab^2d^3+16a^4d^2-258a^2bd^2+56b^2d^2+15a^3d-237abd$$
$$+2a^2-32b)u^3+(-a^4b^3d^7+16a^2b^4d^7+12b^5d^7-3a^5b^2d^6+46a^3b^3d^6$$
$$+64ab^4d^6-3a^6bd^5+42a^4b^2d^5+121a^2b^3d^5+4b^4d^5-a^7d^4+3a^5bd^4$$
$$+209a^3b^2d^4+122ab^3d^4-8a^6d^3+114a^4bd^3+248a^2b^2d^3-76b^3d^3$$
$$-24a^5d^2+384a^3bd^2-4ab^2d^2-33a^4d+519a^2bd+60b^2d-18a^3$$
$$+282ab)u^4+(a^5b^3d^7-9a^3b^4d^7-117ab^5d^7+3a^6b^2d^6-24a^4b^3d^6$$
$$-396a^2b^4d^6-24b^5d^6+3a^7bd^5-18a^5b^2d^5-484a^3b^3d^5-111ab^4d^5+a^8d^4$$
$$+7a^6bd^4-307a^4b^2d^4-1038a^2b^3d^4+9a^7d^3-73a^5bd^3-1181a^3b^2d^3$$
$$+573ab^3d^3+33a^6d^2-451a^4bd^2-1236a^2b^2d^2+72b^3d^2+54a^5d$$
$$-807a^3bd-873ab^2d+36a^4-570a^2b-48b^2)u^5+(-a^6b^3d^7-5a^4b^4d^7$$
$$+337a^2b^5d^7+12b^6d^7-3a^7b^2d^6-19a^5b^3d^6+1064a^3b^4d^6+204ab^5d^6$$
$$-3a^8bd^5-27a^6b^2d^5+1164a^4b^3d^5+638a^2b^4d^5+4b^5d^5-a^9d^4-24a^7bd^4$$
$$+441a^5b^2d^4+3195a^3b^3d^4+182ab^4d^4-10a^8d^3-22a^6bd^3+2956a^4b^2d^3$$
$$-645a^2b^3d^3-76b^4d^3-43a^7d^2+403a^5bd^2+4594a^3b^2d^2-544ab^3d^2$$
$$-78a^6d+996a^4bd+4014a^2b^2d+60b^3d-57a^5+852a^3b+942ab^2)u^6\big),$$

$$
\begin{aligned}
v' = &-\frac{1}{a^2b^2(a^2-16b)}\big((a^3b^3d^7 - 11ab^4d^7 + 3a^4b^2d^6 - 33a^2b^3d^6 - 4b^4d^6 \\
&+ 3a^5bd^5 - 33a^3b^2d^5 - 15ab^3d^5 + a^6d^4 - 4a^4bd^4 - 96a^2b^2d^4 - 4b^3d^4 \\
&+ 6a^5d^3 - 80a^3bd^3 + 31ab^2d^3 + 10a^4d^2 - 153a^2bd^2 + 20b^2d^2 + 3a^3d \\
&- 117abd - 6a^2 - 12b)u^3 + (-2a^4b^3d^7 + 28a^2b^4d^7 - 6a^5b^2d^6 + 82a^3b^3d^6 \\
&+ 28ab^4d^6 - 6a^6bd^5 + 78a^4b^2d^5 + 90a^2b^3d^5 - 2a^7d^4 + 8a^5bd^4 + 294a^3b^2d^4 \\
&+ 20ab^3d^4 - 14a^6d^3 + 202a^4bd^3 + 72a^2b^2d^3 - 32a^5d^2 + 510a^3bd^2 \\
&- 124ab^2d^2 - 30a^4d + 546a^2bd - 6a^3 + 204ab)u^4 + (3a^5b^3d^7 - 38a^3b^4d^7 \\
&- 107ab^5d^7 + 9a^6b^2d^6 - 108a^4b^3d^6 - 409a^2b^4d^6 - 4b^5d^6 + 9a^7bd^5 \\
&- 96a^5b^2d^5 - 590a^3b^3d^5 - 47ab^4d^5 + 3a^8d^4 + a^6bd^4 - 646a^4b^2d^4 \\
&- 912a^2b^3d^4 - 4b^4d^4 + 24a^7d^3 - 292a^5bd^3 - 1249a^3b^2d^3 + 639ab^3d^3 \\
&+ 70a^6d^2 - 1057a^4bd^2 - 849a^2b^2d^2 + 20b^3d^2 + 93a^5d - 1512a^3bd \\
&- 597ab^2d + 48a^4 - 870a^2b - 12b^2)u^5 + (-4a^6b^3d^7 + 24a^4b^4d^7 + 583a^2b^5d^7 \\
&- 12a^7b^2d^6 + 60a^5b^3d^6 + 1923a^3b^4d^6 + 156ab^5d^6 - 12a^8bd^5 + 36a^6b^2d^5 \\
&+ 2268a^4b^3d^5 + 639a^2b^4d^5 - 4a^9d^4 - 40a^7bd^4 + 1256a^5b^2d^4 + 5128a^3b^3d^4 \\
&+ 140ab^4d^4 - 36a^8d^3 + 229a^6bd^3 + 5409a^4b^2d^3 - 2227a^2b^3d^3 - 127a^7d^2 \\
&+ 1597a^5bd^2 + 6835a^3b^2d^2 - 748ab^3d^2 - 201a^6d + 2952a^4bd + 5277a^2b^2d \\
&- 129a^5 + 2130a^3b + 708ab^2)u^6 + (5a^7b^3d^7 + 35a^5b^4d^7 - 1754a^3b^5d^7 \\
&- 275ab^6d^7 + 15a^8b^2d^6 + 125a^6b^3d^6 - 5511a^4b^4d^6 - 1833a^2b^5d^6 - 4b^6d^6 \\
&+ 15a^9bd^5 + 165a^7b^2d^5 - 5988a^5b^3d^5 - 4312a^3b^4d^5 - 103ab^5d^5 + 5a^{10}d^4 \\
&+ 130a^8bd^4 - 2183a^6b^2d^4 - 17022a^4b^3d^4 - 2940a^2b^4d^4 - 4b^5d^4 + 50a^9d^3 \\
&+ 159a^7bd^3 - 15035a^5b^2d^3 + 179a^3b^3d^3 + 1703ab^4d^3 + 206a^8d^2 \\
&- 1708a^6bd^2 - 25304a^4b^2d^2 + 1431a^2b^3d^2 + 20b^4d^2 + 363a^7d - 4398a^5bd \\
&- 23694a^3b^2d - 1437ab^3d + 258a^6 - 3816a^4b - 7026a^2b^2 - 12b^3)u^7 \\
&+ (-6a^8b^3d^7 - 164a^6b^4d^7 + 3864a^4b^5d^7 + 3365a^2b^6d^7 - 18a^9b^2d^6 \\
&- 522a^7b^3d^6 + 11837a^5b^4d^6 + 13701a^3b^5d^6 + 448ab^6d^6 - 18a^{10}bd^5 \\
&- 582a^8b^2d^5 + 12275a^6b^3d^5 + 21828a^4b^4d^5 + 2395a^2b^5d^5 - 6a^{11}d^4 \\
&- 296a^9bd^4 + 3283a^7b^2d^4 + 43960a^5b^3d^4 + 30290a^3b^4d^4 + 424ab^5d^4
\end{aligned}
$$

$$
\begin{aligned}
&- 66a^{10}d^3 - 1099a^8bd^3 + 32246a^6b^2d^3 + 30529a^4b^3d^3 - 17045a^2b^4d^3 \\
&- 310a^9d^2 + 679a^7bd^2 + 66726a^5b^2d^2 + 24833a^3b^3d^2 - 2192ab^4d^2 - 588a^8d \\
&+ 4809a^6bd + 73578a^4b^2d + 23685a^2b^3d - 444a^7 + 5316a^5b + 30936a^3b^2 \\
&+ 1704ab^3)u^8 + (7a^9b^3d^7 + 392a^7b^4d^7 - 6863a^5b^5d^7 - 17458a^3b^6d^7 \\
&- 515ab^7d^7 + 21a^{10}b^2d^6 + 1218a^8b^3d^6 - 20647a^6b^4d^6 - 61745a^4b^5d^6 \\
&- 6709a^2b^6d^6 - 4b^7d^6 + 21a^{11}bd^5 + 1302a^9b^2d^5 - 20664a^7b^3d^5 \\
&- 81924a^5b^4d^5 - 22146a^3b^5d^5 - 183ab^6d^5 + 7a^{12}d^4 + 567a^{10}bd^4 \\
&- 3982a^8b^2d^4 - 97733a^6b^3d^4 - 158644a^4b^4d^4 - 8392a^2b^5d^4 - 4b^6d^4 \\
&+ 84a^{11}d^3 + 2878a^9bd^3 - 57242a^7b^2d^3 - 160981a^5b^3d^3 + 59447a^3b^4d^3 \\
&+ 3223ab^5d^3 + 442a^{10}d^2 + 2563a^8bd^2 - 142138a^6b^2d^2 - 189134a^4b^3d^2 \\
&+ 18323a^2b^4d^2 + 20b^5d^2 + 885a^9d - 2382a^7bd - 179958a^5b^2d \\
&- 164688a^3b^3d - 2637ab^4d + 696a^8 - 5400a^6b - 92938a^4b^2 - 29078a^2b^3 \\
&- 12b^4)u^9\big).
\end{aligned}
$$