ELLIPTIC SPECTRA, THE WITTEN GENUS AND THE THEOREM OF THE CUBE

M. ANDO, M. J. HOPKINS, AND N. P. STRICKLAND

Contents

1. Introduction

This paper is part of a series ([HMM98, HM98] and other work in progress) getting at some new aspects of the topological approach to elliptic genera. Most of these results were announced in [Hop95].

In [Och87] Ochanine introduced the *elliptic genus*—a cobordism invariant of oriented manifolds taking its values in the ring of (level 2) modular forms. He conjectured and proved half of the *rigidity theorem*—that the elliptic genus is multiplicative in bundles of spin manifolds with connected structure group.

Ochanine defined his invariant strictly in terms of characteristic classes, and the question of describing the elliptic genus in more geometric terms naturally arose—especially in connection with the rigidity theorem.

In [Wit87, Wit88] Witten interpreted Ochanine's invariant in terms of index theory on loop spaces and offered a proof of the rigidity theorem. Witten's proof was made mathematically rigorous by Bott and Taubes [BT89], and since then there have been several new proofs of the rigidity theorem [Liu95, Ros98].

In the same papers Witten described a variant of the elliptic genus now known as the *Witten genus.* There is a characteristic class λ of Spin manifolds, twice which is the first Pontrjagin class, p_1. The Witten genus is a cobordism invariant of Spin-manifolds for which $\lambda = 0$, and it takes its values in modular forms (of level 1). It has exhibited a remarkably fecund relationship with geometry (see [Seg88], and [HBJ92]).

Rich as it is, the theory of the Witten genus is not as developed as are the invariants described by the index theorem. One thing that is missing is an understanding of the Witten genus of a family. Let S be a space, and M_s a family of n-dimensional Spin-manifolds (with $\lambda = 0$) parameterized by the points of S. The family M_s defines an element in the cobordism group

$$MO\langle 8\rangle^{-n}S,$$

where $MO\langle 8\rangle$ denotes the cobordism theory of "Spin-manifolds with $\lambda = 0$." The Witten genus of this family should be some kind of "family of modular forms" parameterized by the points of S. Motivated by the index theorem, we should regard this family of modular forms as an element in

$$E^{-n}S$$

for some (generalized) cohomology theory E. From the topological point of view, the Witten genus of a family is thus a multiplicative map of generalized cohomology theories

$$MO\langle 8\rangle \to E,$$

and the question arises as to which E to choose, and how, in this language, to express the modular invariance of the Witten genus. One candidate for E, *elliptic cohomology*, was introduced by Landweber, Ravenel, and Stong in [LRS95].

To keep the technicalities to a minimum, we focus in this paper on the restriction of the Witten genus to stably almost complex manifolds with a trivialization of the Chern classes c_1 and c_2 of the tangent bundle. The bordism theory of such manifolds is denoted $MU\langle 6\rangle$. We will consider generalized cohomology theories (or, more precisely, homotopy commutative ring spectra) E which are *even* and *periodic*. In the language of generalized cohomology, this means that the cohomology groups

$$\tilde{E}^0(S^n)$$

are zero for n odd, and that for each pointed space X, the map

$$\tilde{E}^0(S^2) \underset{E^0(\mathrm{pt})}{\otimes} \tilde{E}^0(X) \to \tilde{E}^0(S^2 \wedge X)$$

is an isomorphism. In the language of spectra the conditions are that

$$\pi_{\mathrm{odd}} E = 0$$

and that $\pi_2 E$ contains a unit. Our main result is a convenient description of *all* multiplicative maps

$$MU\langle 6\rangle \to E.$$

In another paper in preparation we will give, under more restrictive hypotheses on E, an analogous description of the multiplicative maps

$$MO\langle 8\rangle \to E.$$

These results lead to a useful homotopy theoretic explanation of the Witten genus, and to an expression of the modular invariance of the Witten genus of a family. To describe them it is necessary to make use of the language of formal groups.

The assumption that E is even and periodic implies that the cohomology ring

$$E^0\mathbb{C}P^\infty.$$

is the ring of functions on a formal group P_E over $\pi_0 E = E^0(\mathrm{pt})$ [Qui69, Ada74]. From the point of view of the formal group, the result [Ada74, Part II, Lemma 4.6] can be interpreted as saying that the set of multiplicative maps

$$MU \to E$$

is naturally in one to one correspondence with the set of rigid sections of a certain rigid line bundle $\Theta^1(\mathcal{L})$ over P_E. Here a line bundle is said to be *rigid* if it has a specified trivialization at the zero element, and a section is said to be *rigid* if it takes the specified value at zero. Our line bundle $\mathcal{L}$ is the one whose sections are functions that vanish at zero, or in other words $\mathcal{L} = \mathcal{O}(-\{0\})$. The fiber of $\Theta^1(\mathcal{L})$ at a point $a \in P_E$ is defined to be $\mathcal{L}_0 \otimes \mathcal{L}_a^*$; it is immediate that $\Theta^1(\mathcal{L})$ has a canonical rigidification.

Similarly, given a line bundle $\mathcal{L}$ over a commutative group A, let $\Theta^3(\mathcal{L})$ be the line bundle over A^3 whose fiber at (a, b, c) is

$$\Theta^3(\mathcal{L})_{(a,b,c)} = \frac{\mathcal{L}_{a+b}\mathcal{L}_{b+c}\mathcal{L}_{a+c}\mathcal{L}_0}{\mathcal{L}_{a+b+c}\mathcal{L}_a\mathcal{L}_b\mathcal{L}_c}.$$

In this expression the symbol "+" refers to the group law of A, and multiplication and division indicate the tensor product of lines and their duals. A *cubical structure* on $\mathcal{L}$ is a nowhere vanishing section s of $\Theta^3(\mathcal{L})$ satisfying (after making the appropriate canonical identifications of line bundles)

$$\begin{array}{lrcl}
\text{(rigid)} & s(0,0,0) & = & 1 \\
\text{(symmetry)} & s(a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}) & = & s(a_1, a_2, a_3) \\
\text{(cocycle)} & s(b,c,d)s(a,b+c,d) & = & s(a+b,c,d)s(a,b,d).
\end{array}$$

(See [Bre83], and Remark 2.42 for comparison of conventions.) Our main result (2.50) asserts that the set of multiplicative maps

$$MU\langle 6\rangle \to E$$

is naturally in one to one correspondence with the set of cubical structures on $\mathcal{L} = \mathcal{O}(-\{0\})$.

We have chosen a computational approach to the proof of this theorem partly because it is elementary, and partly because it leads to a general result. In [AS98], the first and third authors give a less computational proof of this result (for formal groups of finite height in positive characteristic), using ideas from [Mum65, Gro72, Bre83] on the algebraic geometry of biextensions and cubical structures.

On an *elliptic curve* the line bundle $\mathcal{O}(-\{0\})$ has a unique cubical structure. Indeed, for fixed x and y, there is by Abel's theorem a rational function $f(x,y,z)$ with divisor $\{-x-y\}+\{0\}-\{-x\}-\{-y\}$. Any two such functions have a constant ratio, so the quotient $s(x,y,z) = f(x,y,0)/f(x,y,z)$ is well-defined and is easily seen to determine a trivialization of $\Theta^3(\mathcal{O}(-\{0\}))$. Since the only global functions on an elliptic curve are constants, the requirement $s(0,0,0) = 1$ determines the section uniquely, and shows that it satisfies the "symmetry" and "cocycle" conditions. In fact the "theorem of the cube" (see for example [Mum70]) shows more generally that *any* line bundle over *any abelian variety* has a unique cubical structure.

Over the complex numbers, a transcendental formula for $f(x,y,z)$ is

$$\frac{\sigma(x+y+z)\,\sigma(z)}{\sigma(x+y)\,\sigma(x+z)},$$

where σ is the Weierstrass σ function. It follows that the unique cubical structure is given by

$$\frac{\sigma(x+y)\,\sigma(x+z)\,\sigma(y+z)\,\sigma(0)}{\sigma(x+y+z)\,\sigma(x)\,\sigma(y)\,\sigma(z)}. \tag{1.1}$$

Putting all of this together, if the formal group P_E can be identified with the formal completion of an elliptic curve, then there is a canonical multiplicative map

$$MU\langle 6\rangle \to E$$

corresponding to the unique cubical structure which extends to the elliptic curve.

Definition 1.2. An *elliptic spectrum* consists of

i. an even, periodic, homotopy commutative ring spectrum E with formal group P_E over $\pi_0 E$;
ii. a generalized elliptic curve C over $E^0(\mathrm{pt})$;
iii. an isomorphism $t\colon P_E \to \widehat{C}$ of P_E with the formal completion of C.

For an elliptic spectrum $\mathbf{E} = (E, C, t)$, the σ*-orientation*

$$\sigma_{\mathbf{E}}\colon MU\langle 6\rangle \to E$$

is the map corresponding to the unique cubical structure extending to C.

Note that this definition involves generalized elliptic curves over arbitrary rings. The relevant theory is developed in [KM85, DR73]; we give a summary in Appendix B.

A *map* of elliptic spectra $\mathbf{E_1} = (E_1, C_1, t_1) \to \mathbf{E_2} = (E_2, C_2, t_2)$ consists of a map $f\colon E_1 \to E_2$ of multiplicative cohomology theories, together with an isomorphism of elliptic curves

$$(\pi_0 f)^* C_2 \to C_1,$$

extending the induced map of formal groups. Given such a map, the uniqueness of cubical structures over elliptic curves shows that

$$\begin{tikzcd} & MU\langle 6\rangle \arrow[dl, "\sigma_{\mathbf{E_1}}"'] \arrow[dr, "\sigma_{\mathbf{E_2}}"] & \\ E_1 \arrow[rr, "f"'] & & E_2 \end{tikzcd} \tag{1.3}$$

commutes. We will refer to the commutativity of this diagram as the *modular invariance* of the σ-orientation.

By way of illustration, let's consider examples derived from elliptic curves over $\mathbb{C}$, and ordinary cohomology (for which the formal group is the additive group).

An elliptic curve over $\mathbb{C}$ is of the form $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. The map of formal groups derived from

$$\mathbb{C} \longrightarrow \mathbb{C}/\Lambda$$

gives an isomorphism t_Λ, from the additive formal group to the formal completion of the elliptic curve. Let R_Λ be the graded ring $\mathbb{C}[u_\Lambda, u_\Lambda^{-1}]$ with $|u_\Lambda| = 2$, and define an elliptic spectrum $H_\Lambda = (E_\Lambda, C_\Lambda, t_\Lambda)$ by taking E_Λ to be the spectrum representing

$$H_*(\,-\,; R_\Lambda),$$

C_Λ the elliptic curve $\mathbb{C}/\Lambda$, and t_Λ the isomorphism described above.

The abelian group of cobordism classes of $2n$-dimensional stably almost complex manifolds with a trivialization of c_1 and c_2 is

$$MU\langle 6\rangle_{2n}(\mathrm{pt}).$$

The σ-orientation for H_Λ thus associates to each such M, an element of $(E_\Lambda)_{2n}(\mathrm{pt})$ which can be written

$$\Phi(M;\Lambda)\cdot u_\Lambda^n,$$

with

$$\Phi(M;\Lambda) \in \mathbb{C}.$$

Suppose that $\Lambda' \subset \mathbb{C}$ is another lattice, and that λ is a non-zero complex number for which $\lambda \cdot \Lambda = \Lambda'$. Then multiplication by λ gives an isomorphism $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$. This extends to a map $H_{\Lambda'} \longrightarrow H_\Lambda$, of elliptic spectra, which, in order to induce the correct map of formal groups, must send $u_{\Lambda'}$ to λu_Λ (this is explained in example 2.3). The modular invariance of the σ-orientation then leads to the equation

$$\Phi(M; \lambda\cdot\Lambda) = \lambda^{-n}\Phi(M;\Lambda).$$

This can be put in a more familiar form by choosing a basis for the lattice Λ. Given a complex number τ with positive imaginary part, let $\Lambda(\tau)$ be the lattice generated by 1 and τ, and set

$$f(M,\tau) = \Phi(M, \Lambda(\tau)).$$

Given

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

set

$$\begin{aligned} \Lambda &= \Lambda(\tau) \\ \Lambda' &= \Lambda\left((a\,\tau + b)/(c\,\tau + d)\right) \\ \lambda &= (c\,\tau + d)^{-1}. \end{aligned}$$

The above equation then becomes

$$f(M;(a\tau+b)/(c\tau+d))=(c\tau+d)^n f(M;\tau),$$

which is the functional equation satisfied by a modular form of weight n. It can be shown that $f(M,\tau)$ is a holomorphic function of τ by considering the elliptic spectrum derived from the family of elliptic curves

$$\mathfrak{H}\times\mathbb{C}/\langle 1,\tau\rangle\to\mathfrak{H}$$

parameterized by the points of the upper half plane $\mathfrak{H}$, and with underlying homology theory

$$H_*\left(-;\mathcal{O}[u,u^{-1}]\right),$$

where $\mathcal{O}$ is the ring of holomorphic functions on $\mathfrak{H}$. Thus the σ-orientation associates a modular form of weight n to each $2n$-dimensional $MU\langle 6\rangle$-manifold. Using an elliptic spectrum constructed out of K-theory and the Tate curve, one can also show that the modular forms that arise in this manner have integral q-expansions (see §2.8).

In fact, it follows from formula (1.1) (for details see §2.7) that the q-expansion of this modular form is the Witten genus of M. The σ-orientation can therefore be viewed as a topological refinement of the Witten genus, and its modular invariance (1.3), an expression of the modular invariance of the Witten genus of a family.

All of this makes it clear that one can deduce special properties of the Witten genus by taking special choices of E. But it also suggests that the really natural thing to do is to consider *all* elliptic curves at once. This leads to some new torsion companions to the Witten genus, some new congruences on the values of the Witten genus, and to the ring of topological modular forms. It is the subject of the papers [HMM98, HM98].

1.1. **Outline of the paper.** In §2, we state our results and the supporting definitions in more detail. In §2.3 we give a detailed account of our algebraic model for $E_0BU\langle 2k\rangle$. In §2.4 we describe our algebraic model for $E_0MU\langle 2k\rangle$. We deduce our results about $MU\langle 2k\rangle$ from the results about $BU\langle 2k\rangle$ and careful interpretation of the Thom isomorphism; the proof of the main result about $E_0BU\langle 2k\rangle$ (Theorem 2.29) is the subject of §4.

In §2.5 we give in more detail the argument sketched in the introduction that there is a unique cubical structure on any elliptic curve. We give an argument with explicit formulae which works when the elliptic curves in question are allowed to degenerate to singular cubics ("generalized elliptic curves"), and also gives some extra insight even in the non-degenerate case. The proof of the main formula (Proposition 2.55) is given in appendix B.

In §2.6, we give a formula for the cubical structure on the Tate curve, inspired by the transcendental formula involving the σ-function that was mentioned in the introduction. In §2.7, we interpret this formula as describing the σ-orientation for the elliptic spectrum K_{Tate}, and we show that its effect on homotopy rings is the Witten genus. In §2.8, we deduce the modularity of the Witten genus from the modular invariance of the σ-orientation.

The rest of the main body of the paper assembles a proof of Theorem 2.29. In §3 we study a set $\underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)(R)$ of formal power series in k variables over a ring R with certain symmetry and cocycle properties. This is a representable functor of R, in other words $\underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)$ is an affine group scheme. For $0\leq k\leq 3$ we will eventually identify $\underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)$ with $\operatorname{spec}(H_*BU\langle 2k\rangle)$. For $k=3$ we use a small fragment of the theory of Weil pairings associated to cubical structures; this forms the heart of an alternative proof of our results [AS98] which works for p-divisible formal groups but not for the formal group of an arbitrary generalized elliptic curve.

In §4 we first check that our algebraic model coincides with the usual description of $\operatorname{spec}(E_0BU)$. We then compare our algebraic calculations to the homology of the fibration

$$BSU\to BU\to\mathbb{C}P^\infty$$

to show that $\operatorname{spec}(H_*BSU)\cong\underline{C}^2(\widehat{\mathbb{G}}_a,\mathbb{G}_m)$.

We then recall Singer's analysis of the Serre spectral sequence of the fibration

$$K(\mathbb{Z},3) \to BU\langle 6\rangle \to BSU.$$

By identifying the even homology of $K(\mathbb{Z},3)$ with the scheme of Weil pairings described in §3.7, we show that $\operatorname{spec}(H_*BU\langle 6\rangle) \cong \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$. Finally we deduce Theorem 2.29 for all E from the case of ordinary homology.

The paper has two appendices. The first proves some results about the group of *additive* cocycles $\underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(A)$, which are used in §3. The second gives an exposition of the theory of generalized elliptic curves, culminating in a proof of Proposition 2.55. We have tried to make things as explicit as possible rather than relying on the machinery of algebraic geometry, and we have given a number of examples.

2. More detailed results

2.1. **The algebraic geometry of even periodic ring spectra.** Let $BU\langle 2k\rangle \to \mathbb{Z}\times BU$ be the $(2k-1)$–connected cover, and let $MU\langle 2k\rangle$ be the associated bordism theory. For an even periodic ring spectrum E and for $k \leq 3$, the map

$$\mathrm{RingSpectra}(MU\langle 2k\rangle, E) \to \mathrm{Alg}_{\pi_0 E}(E_0 MU\langle 2k\rangle, \pi_0 E)$$

is an isomorphism. In other words, the multiplicative maps $MU\langle 2k\rangle \to E$ are in one-to-one correspondence with $\pi_0 E$-valued points of $\operatorname{spec}(\pi_0 E \wedge MU\langle 2k\rangle)$. If E is an elliptic spectrum, then the Theorem of the Cube endows this scheme with a canonical point. In order to connect the topology to the algebraic geometry, we shall express some facts about even periodic ring spectra in the language of algebraic geometry.

2.1.1. *Formal schemes and formal groups.* Following [DG70], we will think of an *affine scheme* as a representable covariant functor from rings to sets. The functor (co-)represented by a ring A is denoted $\operatorname{spec} A$. The ring (co-)representing a functor X will be denoted O_X.

A *formal scheme* is a filtered colimit of affine schemes. For example, the functor $\widehat{\mathbb{A}}^1$ associating to a ring R its set of nilpotent elements is the colimit of the schemes $\operatorname{spec}(\mathbb{Z}[x]/x^k)$ and thus is a formal scheme.

The category of formal schemes has finite products: if $X = \operatorname{colim} X_\alpha$ and $Y = \operatorname{colim} Y_\beta$ then $X \times Y = \operatorname{colim} X_\alpha \times Y_\beta$. The formal schemes in this paper will all be of the form $\widehat{\mathbb{A}}^n \times Z = \widehat{\mathbb{A}}^1 \times \ldots \times \widehat{\mathbb{A}}^1 \times Z$ for some affine scheme Z. If $X = \operatorname{colim}_\alpha X_\alpha$ is a formal scheme, then we shall write $\mathcal{O}_X$ for $\lim_\alpha \mathcal{O}_{X_\alpha}$; in particular we have $\mathcal{O}_{\widehat{\mathbb{A}}^1} = \mathbb{Z}[\![x]\!]$. We write $\widehat{\otimes}$ for the completed tensor product, so that for example

$$\mathcal{O}_{X\times Y} = \mathcal{O}_X \widehat{\otimes} \mathcal{O}_Y.$$

If $X \to S$ is a morphism of schemes with a section $j\colon S \to X$, then $\widehat{X}$ will denote the completion of X along the section. Explicitly, the section j defines an augmentation

$$\mathcal{O}_X \xrightarrow{j^*} \mathcal{O}_S.$$

If J denotes the kernel of j^*, then

$$\widehat{X} = \operatorname*{colim}_N \operatorname{spec}(\mathcal{O}_X / J^N).$$

For example, the zero element defines a section $\operatorname{spec}(\mathbb{Z}) \to \mathbb{A}^1$, and the completion of $\mathbb{A}^1$ along this section is the formal scheme $\widehat{\mathbb{A}}^1$.

A *commutative one-dimensional formal group* over S is a commutative group G in the category of formal schemes over S which, locally on S, is isomorphic to $S \times \widehat{\mathbb{A}}^1$ as a pointed formal scheme over S. We shall often omit "commutative" and "one-dimensional", and simply refer to G as a formal group.

We shall use the notation $\mathbb{G}_a$ for the additive group, and $\mathbb{G}_m$ for the multiplicative group. As functors we have $\mathbb{G}_a(R) = R$ and $\mathbb{G}_m(R) = R^\times$. Thus $\widehat{\mathbb{G}}_a$ is the additive formal group, and $\widehat{\mathbb{G}}_a(R)$ is the additive group of nilpotent elements of R.

If the group scheme $\mathbb{G}_m$ acts on a scheme X, we have a map $\alpha\colon \mathbb{G}_m \times X \to X$, corresponding to a map $\alpha^*\colon \mathcal{O}_X \to \mathcal{O}_{\mathbb{G}_m \times X} = \mathcal{O}_X[u, u^{-1}]$. We put $(\mathcal{O}_X)_n = \{f \mid \alpha(f) = u^n f\}$. This makes $\mathcal{O}_X$ into a graded ring.

A graded ring R_* is said to be of finite type over $\mathbb{Z}$ if each R_n is a finitely generated abelian group.

2.1.2. *Even ring spectra and schemes.* If E is an even periodic ring spectrum, then we write

$$S_E \overset{\text{def}}{=} \operatorname{spec}(\pi_0 E).$$

If X is a space, we write E^0X and E_0X for the unreduced E-(co)homology of X. If A is a spectrum, we write E^0A and E_0A for its spectrum (co)homology. These are related by the formula $E^0X = E^0\Sigma^\infty X_+$.

Let X be a CW-complex. If $\{X_\alpha\}$ is the set of finite subcomplexes of X then we write X_E for the formal scheme $\operatorname{colim}_\alpha \operatorname{spec}(E^0 X_\alpha)$. This gives a covariant functor from spaces to formal schemes over S_E.

We say that X is *even* if H_*X is a free abelian group, concentrated in even degrees. If X is even and E is an even periodic ring spectrum, then E_0X is a free module over E_0, and E^0X is its dual. The restriction to even spaces of the functor $X \mapsto X_E$ preserves finite products. For example the space $P \overset{\text{def}}{=} \mathbb{C}P^\infty$ is even, and P_E is (non-canonically) isomorphic to the formal affine line. The multiplication $P \times P \to P$ classifying the tensor product of line bundles makes the scheme P_E into a (one-dimensional commutative) formal group over S_E.

The formal group P_E is not quite the same as the one introduced by Quillen [Qui69]. The ring of functions on Quillen's formal group is $E^*(P)$, while the ring of functions on P_E is $E^0(P)$. The homogeneous parts of $E^*(P)$ can interpreted as sections of line bundles over P_E. For example, let I be the ideal of functions on P_E which vanish along the identity section. The natural map

$$I/I^2 \to \tilde{E}^0(S^2) = \pi_2 E \tag{2.1}$$

is an isomorphism. Now I/I^2 is, by definition, the Zariski cotangent space to the group P_E at the identity, and defines a line bundle over $\operatorname{spec} \pi_0 E$. This line bundle is customarily denoted ω, and can be regarded as the sheaf of invariant 1-forms on P_E. In this way we will identify $\pi_2 E$ with invariant 1-forms on P_E. More generally, $\pi_{2n}E$ can be identified with the module of sections of ω^n (i.e., invariant differentials of degree n on P_E).

Note that for any space X, the map

$$\tilde{E}^0(X) \otimes_{\pi_0 E} \pi_{-2n}(E) \longrightarrow \tilde{E}^{2n}(X)$$

is an isomorphism, and so $E^{2n}(X)$ can be identified with the module of sections of the pull-back of the line bundle ω^{-n} to X_E.

Let E be an even ring spectrum, which need not be periodic. Let $EP = \bigvee_{n\in\mathbb{Z}} \Sigma^{2n} E$. There is an evident way to make this into a commutative ring spectrum with the property that $\pi_* EP = E_*[u, u^{-1}]$ with $u \in \pi_2 EP$. With this structure, EP becomes an even periodic ring spectrum. Note that when X is finite we just have $EP^0X = \bigoplus_n E^{2n}X$, so the ring EP^0X has a natural even grading. If X is an infinite, even CW-complex then EP^0X is the completed direct sum (with respect to the topology defined by kernels of restrictions to finite subcomplexes) of the groups $E^{2n}X$ and so again has a natural even grading.

We write HP for the 2-periodic integer Eilenberg-MacLane spectrum $H\mathbb{Z}P$, and MP for $MUP = MU\langle 0\rangle$. The formal group of HP is the additive group $\widehat{\mathbb{G}}_a$; and we may choose an additive coordinate z on $\widehat{\mathbb{G}}_a$ for which $u = dz$. By Quillen's theorem [Qui69], the formal group of MP is Lazard's universal formal group law.

If X is an even, homotopy commutative H-space, then X_E is a (commutative but in general not one-dimensional) formal group. In that case E_0X is a Hopf algebra over E_0 and we write $X^E = \operatorname{spec}(E_0X)$ for the corresponding group scheme. It is the *Cartier dual* of the formal group X_E. We recall (from [Dem72, §II.4], for example; see also [Str99a, Section 6.4] for a treatment adapted to the present situation) that the Cartier dual of a formal group G is the functor from rings to groups

$$\underline{\mathrm{Hom}}(G, \mathbb{G}_m)(A) = \{(u, f) \mid u\colon \operatorname{spec}(A) \to S\ ,\ f \in (\text{Formal groups})(u^*G, u^*\mathbb{G}_m)\}.$$

Let $b \in E_0X \widehat{\otimes} E^0X$ be the adjoint of the identity map $E_0X \to E_0X$. Given a ring homomorphism $g\colon E_0X \to A$ we get a map $u\colon \operatorname{spec}(A) \to S_E$ and an element $g(b) \in (A \widehat{\otimes} E^0X)^\times = (A \widehat{\otimes} \mathcal{O}_{X_E})^\times$, which corresponds to a map of schemes

$$f\colon u^*X_E \to u^*\mathbb{G}_m.$$

One shows that it is a group homomorphism, and so gives a map of group schemes

$$X^E \to \underline{\mathrm{Hom}}(X_E, \mathbb{G}_m), \tag{2.2}$$

which turns out to be an isomorphism.

2.2. **Constructions of elliptic spectra.** Recall that an elliptic spectrum is a triple (E, C, t) consisting of an even, periodic, homotopy commutative ring spectrum E, a generalized elliptic curve C over $E^0(\mathrm{pt})$, and an isomorphism formal groups

$$t\colon P_E \to \widehat{C}.$$

Here are some examples.

Example 2.3. As discussed in the introduction, if $\Lambda \subset \mathbb{C}$ is a lattice, then the quotient $\mathbb{C}/\Lambda$ is an elliptic curve C_Λ over $\mathbb{C}$. The covering map $\mathbb{C} \to \mathbb{C}/\Lambda$ gives an isomorphism $t_\Lambda\colon \widehat{C}_\Lambda \cong \widehat{\mathbb{G}}_a$. Let E_Λ be the spectrum representing the cohomology theory $H^*(\,-\,; \mathbb{C}[u_\Lambda, u_\Lambda^{-1}])$. Define H_Λ to be the elliptic spectrum $(E_\Lambda, C_\Lambda, t_\Lambda)$. Note that u_Λ can be taken to correspond to the invariant differential dz on $\mathbb{C}$ under the isomorphism (2.1).

Given a non-zero complex number λ, consider the map

$$\begin{aligned} f\colon E_{\lambda\Lambda} &\to E_\Lambda \\ u_{\lambda\Lambda} &\mapsto \lambda u_\Lambda \end{aligned}$$

(i.e. $\pi_2 f$ scales the invariant differential by λ). The induced map of formal groups is simply multiplication by λ, and so extends to the isomorphism

$$C_\Lambda \xrightarrow{\lambda\cdot} C_{\lambda\Lambda}$$

of elliptic curves. Thus f defines a map of elliptic spectra

$$f\colon H_{\lambda\Lambda} \to H_\Lambda.$$

Example 2.4. Let C_{HP} be the cuspidal cubic curve $y^2z = x^3$ over $\operatorname{spec}(\mathbb{Z})$. In §B.1.4, we give an isomorphism $s\colon (C_{HP})_{\mathrm{reg}} \cong \mathbb{G}_a$ and so $\hat{s}\colon \widehat{C}_{HP} \cong \widehat{\mathbb{G}}_a = P_{HP}$. Thus the triple $(HP, C_{HP}, \hat{s})$ is an elliptic spectrum.

Example 2.5. Let $C = C_K$ be the nodal cubic curve $y^2z + xyz = x^3$ over $\operatorname{spec}(\mathbb{Z})$. In §B.1.4, we give an isomorphism $t\colon (C_K)_{\mathrm{reg}} \cong \mathbb{G}_m$ so $\widehat{C}_K \cong \widehat{\mathbb{G}}_m = P_K$. The triple $(K, C_K, \hat{t})$ is an elliptic spectrum.

Example 2.6. Let C/S be an untwisted generalized elliptic curve (see Definition B.2) with the property that the formal group $\widehat{C}$ is Landweber exact (For example, this is automatic if $\mathcal{O}_S$ is a $\mathbb{Q}$-algebra). Landweber's exact functor theorem gives an even periodic cohomology theory $E^*(\,-\,)$, together with an isomorphism of formal groups $t\colon P_E \to \widehat{C}$. This is the classical construction of elliptic cohomology; and gives rise to many examples. In fact, the construction identifies a representing spectrum E up to canonical isomorphism, since Franke [Fra92] and Strickland [Str99a, Proposition 8.43] show that there are no phantom maps between Landweber exact elliptic spectra.

Example 2.7. In §2.6, we describe an elliptic spectrum based on the Tate elliptic curve, with underlying spectrum $K[\![q]\!]$.

2.3. **The complex-orientable homology of $BU\langle 2k\rangle$ for $k \leq 3$.** Let E be an even periodic ring spectrum with a coordinate $x \in \widetilde{E}^0 P$, giving rise to a formal group law F over E_0. Let $\rho\colon P^3 \to BU\langle 6\rangle$ be the map (see (2.24)) such that the composition

$$P^3 \xrightarrow{\rho} BU\langle 6\rangle \to BU$$

classifies the virtual bundle $\prod_i (1 - L_i)$. Let $f = f(x_1, x_2, x_3)$ be the power series which is the adjoint of $E_0\rho$ in the ring $E^0 P^3 \widehat{\otimes} E_0 BU\langle 6\rangle \cong E_0 BU\langle 6\rangle[\![x_1, x_2, x_3]\!]$. It is easy to check that f satisfies the following three conditions.

$$f(x_1, x_2, 0) = 1 \tag{2.8a}$$

$$f(x_1, x_2, x_3) \text{ is symmetric in the } x_i \tag{2.8b}$$

$$f(x_1, x_2, x_3) f(x_0, x_1 +_F x_2, x_3) = f(x_0 +_F x_1, x_2, x_3) f(x_0, x_1, x_3). \tag{2.8c}$$

We will eventually prove the following result.

Theorem 2.9. *$E_0 BU\langle 6\rangle$ is the universal example of an E_0-algebra R equipped with a formal power series $f \in R[\![x_1, x_2, x_3]\!]$ satisfying the conditions* (2.8).

In this section we will reformulate this statement (as the case $k = 3$ of Theorem 2.29) in a way which avoids the choice of a coordinate.

2.3.1. *The functor C^k.*

Definition 2.10. If A and T are abelian groups, we let $C^0(A, T)$ be the group

$$C^0(A, T) \overset{\text{def}}{=} (\text{Sets})(A, T),$$

and for $k \geq 1$ we let $C^k(A, T)$ be the subgroup of $f \in (\text{Sets})(A^k, T)$ such that

$$f(a_1, \dots, a_{k-1}, 0) = 0; \tag{2.11a}$$

$$f(a_1, \dots, a_k) \text{ is symmetric in the } a_i; \tag{2.11b}$$

$$f(a_1, a_2, a_3, \dots, a_k) + f(a_0, a_1 + a_2, a_3, \dots, a_k) = f(a_0 + a_1, a_2, a_3, \dots, a_k) + f(a_0, a_1, a_3, \dots, a_k). \tag{2.11c}$$

We refer to (2.11c) as the *cocycle condition* for f. It really only involves the first two arguments of f, with the remaining arguments playing a dummy rôle. Of course, because f is symmetric, we have a similar equation for any pair of arguments of f.

Remark 2.12. We leave it to the reader to verify that the condition (2.11a) can be replaced with the weaker condition

$$f(0, \dots, 0) = 0 \tag{2.11a'}$$

Remark 2.13. Let $\mathbb{Z}[A]$ denote the group ring of A, and let $I[A]$ be its augmentation ideal. For $k \geq 0$ let

$$C_k(A) \overset{\text{def}}{=} \operatorname{Sym}^k_{\mathbb{Z}[A]} I[A]$$

be the k^{th} symmetric tensor power of $I[A]$, considered as a module over the group ring. One has $C_0(A) = \mathbb{Z}[A]$ and $C_1(A) = I[A]$. For $k \geq 1$, the abelian group $C_k(A)$ is the quotient of $\operatorname{Sym}^k_{\mathbb{Z}} I[A]$ by the relation

$$([c] - [c + a_1]) \otimes ([0] - [a_2]) \otimes \dots \otimes ([0] - [a_k]) = ([0] - [a_1]) \otimes ([c] - [c + a_2]) \otimes \dots \otimes ([0] - [a_k])$$

for $c \in A$. After some rearrangement and reindexing, this relation may be expressed in terms of generators of the form $\langle a_1, \dots, a_k\rangle \overset{\text{def}}{=} ([0] - [a_1]) \otimes \dots \otimes ([0] - [a_k])$ by the formula

$$\langle a_1, a_2, a_3, \dots, a_k\rangle - \langle a_0 + a_1, a_2, a_3, \dots, a_k\rangle + \langle a_0, a_1 + a_2, a_3, \dots, a_k\rangle - \langle a_0, a_1, a_3, \dots, a_k\rangle = 0.$$

It follows that the map of sets

$$\begin{gathered}A^k \to C_k(A)\\(a_1,\dots,a_k) \mapsto \langle a_1,\dots,a_k\rangle\end{gathered}$$

induces an isomorphism

$$(\text{Abelian groups})(C_k(A),T) \cong C^k(A,T).$$

Remark 2.14. Definition 2.10 generalizes to give a subgroup $C^k(A,B)$ of the group of maps $f\colon A^k \to B$, if A and B are abelian groups in any category with finite products.

Definition 2.15. If G and T are formal groups over a scheme S, and we wish to emphasize the rôle of S, we will write $C^k_S(G,T)$. For any ring R, we define

$$\underline{C}^k(G,T)(R) = \{(u,f) \mid u\colon \operatorname{spec}(R) \to S\ ,\ f \in C^k_{\operatorname{spec}(R)}(u^*G,u^*T)\}.$$

This gives a covariant functor from rings to groups. We shall abbreviate $\underline{C}^k(G,\mathbb{G}_m \times S)$ to $\underline{C}^k(G,\mathbb{G}_m)$.

Remark 2.16. It is clear from the definition that, for all maps of schemes $S' \to S$, the natural map

$$\underline{C}^k(G \times_S S', \mathbb{G}_m) \to \underline{C}^k(G,\mathbb{G}_m) \times_S S'$$

is an isomorphism.

Proposition 2.17. *Let G be a formal group over a scheme S. For all k, the functor $\underline{C}^k(G,\mathbb{G}_m)$ is an affine commutative group scheme.*

Proof. We assume that $k > 0$, leaving the modifications for the case $k = 0$ to the reader. It suffices to work locally on S, and so we may choose a coordinate x on G. Let F be the resulting formal group law of G. We let A be the set of multi-indices $\alpha = (\alpha_1,\dots,\alpha_k)$, where each α_i is a nonnegative integer. We define $R = \mathcal{O}_S[b_\alpha \mid \alpha \in A][b_0^{-1}]$, and $f(x_1,\dots,x_k) = \sum_\alpha b_\alpha x^\alpha \in R[\![x_1,\dots,x_k]\!]$. Thus, f defines a map $\operatorname{spec}(R) \times_S G^k \to \mathbb{G}_m$, and in fact $\operatorname{spec}(R)$ is easily seen to be the universal example of a scheme over S equipped with such a map. We define power series $g_0,\dots,g_k$ by

$$g_i = \begin{cases} i = 0 & f(0,\dots,0)\\ i < k & f(x_1,\dots,x_{i-1},x_{i+1},x_i,\dots,x_k)f(x_1,\dots,x_k)^{-1}\\ i = k & f(x_1,\dots,x_k)f(x_0 +_F x_1, x_2,\dots)^{-1} f(x_0, x_1 +_F x_2,\dots) f(x_0,x_1,x_3,\dots)^{-1}\end{cases}$$

We then let I be the ideal in R generated by all the coefficients of all the power series $g_i - 1$. It is not hard to check that $\operatorname{spec}(R/I)$ has the universal property that defines $\underline{C}^k(G,\mathbb{G}_m)$. □

Remark 2.18. A similar argument shows that $\underline{C}^k(G,T)$ is a group scheme when T is a formal group, or when T is the additive group $\mathbb{G}_a$.

Remark 2.19. If G is a formal group and $k > 0$ then the inclusion $\underline{C}^k(G,\widehat{\mathbb{G}}_m) \to \underline{C}^k(G,\mathbb{G}_m)$ is an isomorphism, so we shall not distinguish between these two schemes. Indeed, we can locally identify $\underline{C}^k(G,\mathbb{G}_m)(R)$ with a set of power series f as in the above proof. One of the conditions on f is that $f(0,\dots,0) = 1$, so when $x_1,\dots,x_k$ are nilpotent we see that $f(x_1,\dots,x_n) = 1$ mod nilpotents, so $f(x_1,\dots,x_n) \in \widehat{\mathbb{G}}_m \subset \mathbb{G}_m$. This does not work for $k = 0$, as then we have

$$C^0(G,\mathbb{G}_m) = \operatorname{Map}(G,\mathbb{G}_m) \neq \operatorname{Map}(G,\widehat{\mathbb{G}}_m) = C^0(G,\widehat{\mathbb{G}}_m).$$

2.3.2. *The maps* $\delta\colon C^k(G,T) \to C^{k+1}(G,T)$. We now define maps of schemes that will turn out to correspond to the maps $BU\langle 2k+2\rangle \longrightarrow BU\langle 2k\rangle$ of spaces.

Definition 2.20. If G and T are abelian groups, and if $f\colon G^k \to T$ is a map of sets, then let $\delta(f)\colon G^{k+1} \to T$ be the map given by the formula

$$\delta(f)(a_0,\dots,a_k) = f(a_0,a_2,\dots,a_k) + f(a_1,a_2,\dots,a_k) - f(a_0+a_1,a_2,\dots,a_k). \tag{2.21}$$

It is clear that δ generalizes to abelian groups in any category with products. We leave it to the reader to verify the following.

Lemma 2.22. *For $k \geq 1$, the map δ induces a homomorphism of groups*

$$\delta\colon C^k(G,T) \to C^{k+1}(G,T).$$

Moreover, if G and T are formal groups over a scheme S, then δ induces a homomorphism of group schemes $\delta\colon \underline{C}^k(G,T) \to \underline{C}^{k+1}(G,T)$. □

Remark 2.23. When A and T are discrete abelian groups, the group $H^2(A;T) \overset{\text{def}}{=} \operatorname{cok}(\delta\colon C^1(A,T) \to C^2(A,T))$ classifies central extensions of A by T. The next map $\delta\colon C^2(A,T) \to C^3(A,T))$ can also be interpreted in terms of biextensions [Mum65, Gro72, Bre83].

2.3.3. *Relation to $BU\langle 2k\rangle$.* For any space X, we write $K^*(X)$ for the periodic complex K-theory groups of X; in the case of a point we have $K^* = \mathbb{Z}[v,v^{-1}]$ with $v \in K^{-2}$. We have $K^{2t}(X) = [X, \mathbb{Z}\times BU]$ for all t. We also consider the connective K-theory groups $bu^*(X)$, so $bu^* = \mathbb{Z}[v]$ and $bu^{2t}(X) = [X, BU\langle 2t\rangle]$. To make this true when $t=0$, we adopt the convention that $BU\langle 0\rangle = \mathbb{Z}\times BU$. Multiplication by $v^t\colon \Sigma^{2t}bu \to bu$ gives an identification of the 0-space of $\Sigma^{2t}bu$ with $BU\langle 2t\rangle$. Under this identification, the projection $BU\langle 2t+2\rangle \longrightarrow BU\langle 2t\rangle$ is derived from multiplication by v mapping $\Sigma^{2t+2}bu \to \Sigma^{2t}bu$.

For $t \geq 0$ we define a map

$$\rho_t\colon P^t = (\mathbb{C}P^\infty)^t \to BU\langle 2t\rangle \tag{2.24}$$

as follows. The map $\rho_0\colon P \to 1\times BU \subset BU\langle 0\rangle$ is just the map classifying the tautological line bundle L. For $t>0$, let $L_1,\dots,L_2$ be the obvious line bundles over P^t. Let $x_i \in bu^2(P^t)$ be the bu-theory Euler class, given by the formula

$$vx_i = 1 - L_i.$$

Then we have the isomorphisms

$$\begin{aligned} bu^*(P^t) &\cong \mathbb{Z}[v][\![x_1,\dots,x_t]\!] \\ K^*(P^t) &\cong \mathbb{Z}[v,v^{-1}][\![x_1,\dots,x_t]\!]. \end{aligned}$$

The class $\prod_i x_i \in bu^{2t}(P^t)$ gives the map ρ_t. Note that the composition

$$P^t \xrightarrow{\rho_t} BU\langle 2t\rangle \to BU$$

classifies the bundle $\prod_i(1-L_i)$.

Since P and $BU\langle 2t\rangle$ are abelian group objects in the homotopy category of topological spaces, we can define

$$C^t(P, BU\langle 2t\rangle) \subset [P^t, BU\langle 2t\rangle] = bu^{2t}(P^t).$$

Then we have the following.

Proposition 2.25. *The map ρ_t is contained in the subgroup $C^t(P,BU\langle 2t\rangle)$ of $bu^{2t}(P^t)$ and satisfies*

$$v_*\rho_{t+1} = \delta(\rho_t) \in C^{t+1}(P, BU\langle 2t\rangle).$$

Proof. It suffices to check that f_t gives an element of $C^t(P, BU\langle 0\rangle)$. As the group structure of P corresponds to the tensor product of line bundles, while the group structure of $BU\langle 0\rangle$ corresponds to the Whitney sum of vector bundles, the cocycle condition (2.11c) amounts to the equation

$$(1-L_2)(1-L_3)+(1-L_1)(1-L_2L_3)=(1-L_1L_2)(1-L_3)+(1-L_1)(1-L_2)$$

in $K^0(P^3)$. The other conditions for membership in C^t are easily verified. Similarly, the equation $v_*\rho_{t+1}=\delta(\rho_t)$ follows from the equation

$$(1-L_1)+(1-L_2)-(1-L_1L_2)=(1-L_1)(1-L_2).$$

□

Now let E be an even periodic ring spectrum. Applying E-homology to the map ρ_k gives a homomorphism

$$E_0\rho_k\colon E_0P^k\to E_0BU\langle 2k\rangle.$$

For $k\le 3$, $BU\langle 2k\rangle$ is even ([Sin68] or see §4), and of course the same is true of P, and so we may consider the adjoint $\hat\rho_k$ of $E_0\rho_k$ in $E_0BU\langle 2k\rangle\widehat{\otimes}E^0P^k$. Proposition 2.25 then implies the following.

Corollary 2.26. *The element $\hat\rho_k\in E_0BU\langle 2k\rangle\widehat{\otimes}E^0P^k$ is an element of $\underline{C}^k(P_E,\mathbb{G}_m)(E_0BU\langle 2k\rangle)$.* □

Definition 2.27. For $k\le 3$, let $f_k\colon BU\langle 2k\rangle^E\to\underline{C}^k(P_E,\mathbb{G}_m)$ be the map classifying the cocycle $\hat\rho_k$.

Corollary 2.28. *The map f_k is a map of group schemes. For $k\le 2$, the diagram*

$$\begin{tikzcd}
BU\langle 2k+2\rangle^E \arrow[r, "v^E"] \arrow[d, "f_{k+1}"'] & BU\langle 2k\rangle^E \arrow[d, "f_k"] \\
\underline{C}^{k+1}(P_E,\mathbb{G}_m) \arrow[r, "\delta"'] & \underline{C}^k(P_E,\mathbb{G}_m)
\end{tikzcd}$$

commutes.

Proof. The commutativity of the diagram follows easily from the Proposition. To see that f_k is a map of group schemes, note that the group structure on $BU\langle 2k\rangle^E$ is induced by the diagonal map $\Delta\colon BU\langle 2k\rangle\to BU\langle 2k\rangle\times BU\langle 2k\rangle$. The commutative diagram

$$\begin{tikzcd}
P^k \arrow[r, "\Delta"] \arrow[d, "\rho_k"'] & P^k\times P^k \arrow[d, "\rho_k\times\rho_k"] \\
BU\langle 2k\rangle \arrow[r, "\Delta"] & BU\langle 2k\rangle\times BU\langle 2k\rangle
\end{tikzcd}$$

shows that

$$BU\langle 2k\rangle^E\times BU\langle 2k\rangle^E\to BU\langle 2k\rangle^E$$

pulls the function $\hat\rho_k$ back to the multiplication of $\hat\rho_k\otimes 1$ and $1\otimes\hat\rho_k$ as elements of the ring $E_0(BU\langle 2k\rangle^2)\widehat{\otimes}E^0P^k$ of functions on $P^k_E\times(BU\langle 2k\rangle^E\times BU\langle 2k\rangle^E)$. The result follows, since the group structure of $\underline{C}^k(P_E,\mathbb{G}_m)$ is induced by the multiplication of functions in $\mathcal{O}_{P^k_E}$. □

Our main calculation, and the promised coordinate-free version of Theorem 2.9, is the following.

Theorem 2.29. *For $k\le 3$, the map of group schemes*

$$BU\langle 2k\rangle^E\xrightarrow{f_k}\underline{C}^k(P_E,\mathbb{G}_m)$$

is an isomorphism.

This is proved in §4. The cases $k \leq 1$ are essentially well-known calculations. For $k = 2$ and $k = 3$ we can reduce to the case $E = MP$, using Quillen's theorem that $\pi_0 MP$ carries the universal example of a formal group law. Using connectivity arguments and the Atiyah-Hirzebruch spectral sequence, we can reduce to the case $E = HP$. After these reductions, we need to compare $H_* BU\langle 2k\rangle$ with $\mathcal{O}_{\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)}$. We analyze $H^*(BU\langle 2k\rangle; \mathbb{Q})$ and $H^*(BU\langle 2k\rangle; \mathbb{F}_p)$ using the Serre spectral sequence, and we analyze $\mathcal{O}_{\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)}$ by direct calculation, one prime at a time. For the case $k = 3$ we also give a model for the scheme associated to the polynomial subalgebra of $H^*(K(\mathbb{Z}, 3); \mathbb{F}_p)$, and by fitting everything together we show that the map $BU\langle 2k\rangle^E \to \underline{C}^k(P_E, \mathbb{G}_m)$ is an isomorphism.

Remark 2.30. As $BU\langle 2k\rangle^E = \underline{\mathrm{Hom}}(BU\langle 2k\rangle_E, \mathbb{G}_m) = \underline{C}^k(P_E, \mathbb{G}_m)$, it is natural to hope that one could

i. define a formal group scheme $C_k(P_E)$ which could be interpreted as the k'th symmetric tensor power of the augmentation ideal in the group ring of the formal group P_E;
ii. show that $\underline{C}^k(P_E, \mathbb{G}_m) = \underline{\mathrm{Hom}}(C_k(P_E), \mathbb{G}_m)$; and
iii. prove that $BU\langle 2k\rangle_E = C_k(P_E)$.

This would have advantages over the above theorem, because the construction $X \mapsto X_E$ is functorial for all spaces and maps, whereas the construction $X \mapsto X^E$ is only functorial for commutative H-spaces and H-maps. It is in fact possible to carry out this program, at least for $k \leq 3$. It relies on the apparatus developed in [Str99a], and the full strength of the present paper is required even to prove that $C_3(G)$ (as defined by a suitable universal property) exists. Details will appear elsewhere.

2.4. The complex-orientable homology of $MU\langle 2k\rangle$ for $k \leq 3$.

We now turn our attention to the Thom spectra $MU\langle 2k\rangle$. We first note that when $k \leq 3$, the map $BU\langle 2k\rangle \to BU\langle 0\rangle = \mathbb{Z} \times BU$ is a map of commutative, even H-spaces. The Thom isomorphism theorem as formulated by [MR81] implies that $E_0 MU\langle 2k\rangle$ is an $E_0 BU\langle 2k\rangle$-comodule algebra; and a choice of orientation $MU\langle 0\rangle \to E$ gives an isomorphism

$$E_0 MU\langle 2k\rangle \cong E_0 BU\langle 2k\rangle$$

of comodule algebras. In geometric language, this means that the scheme $MU\langle 2k\rangle^E$ is a principal homogeneous space or "torsor" for the group scheme $BU\langle 2k\rangle^E$.

In this section, we work through the Thom isomorphism to describe the object which corresponds to $MU\langle 2k\rangle^E$ under the isomorphism $BU\langle 2k\rangle^E \cong \underline{C}^k(P_E, \mathbb{G}_m)$ of Theorem 2.29. Whereas the schemes $BU\langle 2k\rangle^E$ are related to functions on the formal group P_E of E, the schemes $MU\langle 2k\rangle^E$ are related to the sections of the ideal sheaf $\mathcal{I}(0)$ on P_E. In §2.4.4, we describe the analogue $\underline{C}^k(G; \mathcal{I}(0))$ for the line bundle $\mathcal{I}(0)$ of the functor $\underline{C}^k(G, \mathbb{G}_m)$. In §2.4.5, we give the map

$$g_k \colon MU\langle 2k\rangle^E \to \underline{C}^k(P_E; \mathcal{I}(0))$$

which is our description of $MU\langle 2k\rangle^E$.

2.4.1. *Torsors.* We begin with a brief review of torsors in general and the Thom isomorphism in particular.

Definition 2.31. Let S be a scheme and G a group scheme over S. A (right) *G-torsor* over S is an S-scheme X with a right action

$$X \times G \xrightarrow{\mu} X$$

of the group G, with the property that there exists a faithfully flat S-scheme T and an isomorphism

$$G \times T \to X \times T$$

of T-schemes, compatible with the action of $G \times T$. (All the products here are to be interpreted as fiber products over S.) Any such isomorphism is a *trivialization* of X over T. A map of G-torsors is just an equivariant map of schemes. Note that a map of torsors is automatically an isomorphism.

When $G = \operatorname{spec}(H)$ is affine over $S = \operatorname{spec}(A)$, a G-torsor works out to consists of an affine S-scheme $T = \operatorname{spec}(M)$ and a right coaction

$$M \xrightarrow{\mu^*} M \otimes_A H$$

with the property that over some faithfully flat A-algebra B there is an isomorphism

$$H \otimes_A B \to M \otimes_A B$$

of rings which is a map of right $H \otimes_A B$-comodules.

For example, consider the relative diagonal

$$MU\langle 2k\rangle \xrightarrow{\Delta} MU\langle 2k\rangle \wedge BU\langle 2k\rangle_+.$$

If E is an even periodic ring spectrum and $k \leq 3$, then by the Künneth and universal coefficient theorems, the map Δ induces an action

$$MU\langle 2k\rangle^E \times BU\langle 2k\rangle^E \xrightarrow{\mu} MU\langle 2k\rangle^E.$$

of the group scheme $BU\langle 2k\rangle^E$ on $MU\langle 2k\rangle^E$. The scheme $MU\langle 2k\rangle^E$ is in fact a torsor for $BU\langle 2k\rangle^E$. Indeed, a complex orientation $MU\langle 0\rangle \to E$ restricts to an orientation $\Phi\colon MU\langle 2k\rangle \to E$ which induces an isomorphism

$$E_0 MU\langle 2k\rangle \xrightarrow{\Delta} E_0 MU\langle 2k\rangle \wedge BU\langle 2k\rangle_+ \xrightarrow{\Phi\wedge BU\langle 2k\rangle_+} E_0 BU\langle 2k\rangle_+ \tag{2.32}$$

of $E_0 BU\langle 2k\rangle$-comodule algebras.

2.4.2. *The line bundle $\mathcal{I}(0)$.* Another source of torsors is line bundles. If $\mathcal{L}$ is a line bundle (invertible sheaf of $\mathcal{O}_X$-modules) over X, let $\Gamma^\times(\mathcal{L})$ be the functor of rings

$$\Gamma^\times(\mathcal{L})(R) = \{(u, s) \mid u\colon \operatorname{spec}(R) \to X\ ,\ s \text{ a trivialization of } u^*\mathcal{L}\}.$$

Then $\Gamma^\times(\mathcal{L})$ is a $\mathbb{G}_m$-torsor over X, and $\Gamma^\times$ is an equivalence between the category of line bundles (and isomorphisms) and the category of $\mathbb{G}_m$ torsors. We will often not distinguish in notation between $\mathcal{L}$ and the associated $\mathbb{G}_m$-torsor $\Gamma^\times(\mathcal{L})$.

Let G be a formal group over a scheme S. The ideal sheaf $\mathcal{I}(0)$ associated to the zero section $S \subset G$ defines a line bundle over G. Indeed, the set of global sections of $\mathcal{I}(0)$ is the set of functions $f \in \mathcal{O}_G$ such that $f|_S = 0$. Locally on S, a choice of coordinate x gives an isomorphism $\mathcal{O}_G = \mathcal{O}_S[\![x]\!]$, and the module of sections is the ideal (x), which is free of rank 1.

If C is a generalized elliptic curve over, then we again let $\mathcal{I}(0)$ denote the ideal sheaf of $S \subset C$. Its restriction to the formal completion $\widehat{C}$ is the same as the line bundle over $\widehat{C}$ constructed above.

2.4.3. *The Thom sheaf.* Suppose that X is a finite complex and V is a complex vector bundle over X. We write X^V for its Thom spectrum, with bottom cell in degree equal to the real rank of V. This is the suspension spectrum of the usual Thom space. Now let E be an even periodic ring spectrum. The E^0X-module E^0X^V is the sheaf of sections of a line bundle over X_E. We shall write $\mathbb{L}(V)$ for this line bundle, and $\mathbb{L}$ defines a functor from vector bundles over X to line bundles over X_E. If V and W are two complex vector bundles over X then there is a natural isomorphism

$$\mathbb{L}(V \oplus W) \cong \mathbb{L}(V) \otimes \mathbb{L}(W), \tag{2.33}$$

and so $\mathbb{L}$ extends to the category of virtual complex vector bundles by the formula $\mathbb{L}(V - W) = \mathbb{L}(V) \otimes \mathbb{L}(W)^{-1}$. Moreover, if $f\colon Y \to X$ is a map of spaces, then there is a natural isomorphism $(\operatorname{spec} E^0 f)^*\mathbb{L}(V) \cong \mathbb{L}(f^*V)$ of line bundles over Y_E. This construction extends naturally to infinite complexes by taking suitable (co)limits.

Example 2.34. For example, if L is the tautological line bundle over $P = \mathbb{C}P^\infty$ then the zero section $P \to P^L$ induces an isomorphism $\widetilde{E}^0 P^L \cong \widetilde{E}^0 P = \ker(E^0 P \to E^0)$, and thus gives an isomorphism

$$\mathbb{L}(L) \cong \mathcal{I}(0) \tag{2.35}$$

of line bundles over P_E.

2.4.4. *The functors Θ^k (after Breen* [Bre83]*).* We recall that the category of line bundles or $\mathbb{G}_m$-torsors is a strict Picard category, or in other words a symmetric monoidal category in which every object $\mathcal{L}$ has an inverse $\mathcal{L}^{-1}$, and the twist map of $\mathcal{L} \otimes \mathcal{L}$ is the identity. This means that the procedures we use below to define line bundles give results that are well-defined up to coherent canonical isomorphism.

Suppose that G is a formal group over a scheme S and $\mathcal{L}$ is a line bundle over G.

Definition 2.36. A *rigid* line bundle over G is a line bundle $\mathcal{L}$ equipped with a specified trivialization of $\mathcal{L}|_S$ at the identity $S \to G$. A *rigid section* of such a line bundle is a section s which extends the specified section at the identity. A *rigid isomorphism* between two rigid line bundles is an isomorphism which preserves the specified trivializations.

Definition 2.37. Suppose that $k \geq 1$. Given a subset $I \subseteq \{1, \dots, k\}$, we define $\sigma_I \colon G^k_S \to G$ by $\sigma_I(a_1, \dots, a_k) = \sum_{i \in I} a_i$, and we write $\mathcal{L}_I = \sigma_I^* \mathcal{L}$, which is a line bundle over G^k_S. We also define the line bundle $\Theta^k(\mathcal{L})$ over G^k_S by the formula

$$\Theta^k(\mathcal{L}) \overset{\text{def}}{=} \bigotimes_{I \subset \{1,\dots,k\}} (\mathcal{L}_I)^{(-1)^{|I|}}. \tag{2.38}$$

Finally, we define $\Theta^0(\mathcal{L}) = \mathcal{L}$.

For example we have

$$\begin{aligned} \Theta^0(\mathcal{L})_a &= \mathcal{L}_a \\ \Theta^1(\mathcal{L})_a &= \frac{\mathcal{L}_0}{\mathcal{L}_a} \\ \Theta^2(\mathcal{L})_{a,b} &= \frac{\mathcal{L}_0 \otimes \mathcal{L}_{a+b}}{\mathcal{L}_a \otimes \mathcal{L}_b} \\ \Theta^3(\mathcal{L})_{a,b,c} &= \frac{\mathcal{L}_0 \otimes \mathcal{L}_{a+b} \otimes \mathcal{L}_{a+c} \otimes \mathcal{L}_{b+c}}{\mathcal{L}_a \otimes \mathcal{L}_b \otimes \mathcal{L}_c \otimes \mathcal{L}_{a+b+c}}. \end{aligned}$$

We observe three facts about these bundles.

i. $\Theta^k(\mathcal{L})$ has a natural rigid structure for $k > 0$.
ii. For each permutation $\sigma \in \Sigma_k$, there is a canonical isomorphism
$$\xi_\sigma : \pi_\sigma^* \Theta^k(\mathcal{L}) \cong \Theta^k(\mathcal{L}),$$
where $\pi_\sigma \colon G^k_S \to G^k_S$ permutes the factors. Moreover, these isomorphisms compose in the obvious way.
iii. There is a canonical identification (of rigid line bundles over G^{k+1}_S)
$$\Theta^k(\mathcal{L})_{a_1,a_2,\dots} \otimes \Theta^k(\mathcal{L})^{-1}_{a_0+a_1,a_2,\dots} \otimes \Theta^k(\mathcal{L})_{a_0,a_1+a_2,\dots} \otimes \Theta^k(\mathcal{L})^{-1}_{a_0,a_1,\dots} \cong 1. \tag{2.39}$$

Definition 2.40. A Θ^k–structure on a line bundle $\mathcal{L}$ over a group G is a trivialization s of the line bundle $\Theta^k(\mathcal{L})$ such that

i. for $k > 0$, s is a rigid section;
ii. s is symmetric in the sense that for each $\sigma \in \Sigma_k$, we have $\xi_\sigma \pi_\sigma^* s = s$;
iii. the section $s(a_1, a_2, \dots) \otimes s(a_0+a_1, a_2, \dots)^{-1} \otimes s(a_0, a_1+a_2, \dots) \otimes s(a_0, a_1, \dots)^{-1}$ corresponds to 1 under the isomorphism (2.39).

A Θ^3–structure is known as a *cubical structure* [Bre83]. We write $C^k(G; \mathcal{L})$ for the set of Θ^k-structures on $\mathcal{L}$ over G. Note that $C^0(G; \mathcal{L})$ is just the set of trivializations of $\mathcal{L}$, and $C^1(G; \mathcal{L})$ is the set of rigid trivializations of $\Theta^1(\mathcal{L})$. We also define a functor from rings to sets by

$$\underline{C}^k(G; \mathcal{L})(R) = \{(u, f) \mid u \colon \operatorname{spec}(R) \to S\ ,\ f \in C^k_{\operatorname{spec}(R)}(u^*G; u^*\mathcal{L})\}.$$

Remark 2.41. Note that for the trivial line bundle $\mathcal{O}_G$, the set $C^k(G; \mathcal{O}_G)$ reduces to that of the group $\mathbb{C}^k(G, \mathbb{G}_m)$ of cocycles introduced in §2.3.1.

Remark 2.42. There are some differences between our functors Θ^k and Breen's functors Λ and Θ [Bre83]. Let $\mathcal{L}' = \Theta^1(\mathcal{L})^{-1}$ be the line bundle $\mathcal{L}_a/\mathcal{L}_0$. Then there are natural isomorphisms

$$\begin{aligned}\Lambda(\mathcal{L}') &\cong \Theta^2(\mathcal{L}) \\ \Theta(\mathcal{L}') &\cong \Theta^3(\mathcal{L})^{-1}.\end{aligned}$$

Breen also uses the notation $\Theta_1(M)$ for $\Theta(\mathcal{L}')$ [Bre83, Equation 2.8.1]. As the trivializations of $\mathcal{L}$ biject with those of $\mathcal{L}^{-1}$ in an obvious way, our definition of cubical structures is equivalent to Breen's.

Proposition 2.43. *If G is a formal group over S, and $\mathcal{L}$ is a trivializable line bundle over G, then the functor $\underline{C}^k(G;\mathcal{L})$ is a scheme, whose formation commutes with change of base. Moreover, $\underline{C}^k(G;\mathcal{L})$ is a trivializable torsor for $\underline{C}^k(G,\mathbb{G}_m)$.*

Proof. There is an evident action of $\underline{C}^k(G,\mathbb{G}_m)$ on $\underline{C}^k(G;\mathcal{L})$, and a trivialization of $\mathcal{L}$ clearly gives an equivariant isomorphism of $\underline{C}^k(G;\mathcal{L})$ with $\underline{C}^k(G;\mathcal{O}_G) = \underline{C}^k(G,\mathbb{G}_m)$. Given this, the Proposition follows from the corresponding statements for $\underline{C}^k(G,\mathbb{G}_m)$, which were proved in Proposition 2.17. □

The following lemmas can easily be checked from Definitions 2.37 and 2.40.

Lemma 2.44. *If $\mathcal{L}$ is a line bundle over a formal group G, then there is a canonical isomorphism*

$$\Theta^k(\mathcal{L})_{a_0,a_2,\dots} \otimes \Theta^k(\mathcal{L})_{a_1,a_2,\dots} \otimes \Theta^k(\mathcal{L})^{-1}_{a_0+a_1,a_2,\dots} \cong \Theta^{k+1}(\mathcal{L})_{a_0,\dots,a_k}. \qquad \square$$

Lemma 2.45. *There is a natural map $\delta\colon \underline{C}^k(G;\mathcal{L}) \to \underline{C}^{k+1}(G;\mathcal{L})$, given by*

$$\delta(s)(a_0,\dots,a_k) = s(a_0,a_2,\dots)s(a_1,a_2,\dots)s(a_0+a_1,a_2,\dots)^{-1},$$

where the right hand side is regarded as a section of $\Theta^{k+1}(\mathcal{L})$ by the isomorphism of the previous lemma. □

2.4.5. *Relation to $MU\langle 2k\rangle$.* For $1 \le i \le k$, let L_i be the line bundle over the i factor of P^k. Recall from (2.24) that the map $\rho_k\colon P^k \to BU\langle 2k\rangle$ pulls the tautological virtual bundle over $BU\langle 2k\rangle$ back to the bundle

$$V = \bigotimes_i (1 - L_i).$$

Passing to Thom spectra gives a map

$$(P^k)^V \to MU\langle 2k\rangle$$

which determines an element s_k of $E_0 MU\langle 2k\rangle \widehat{\otimes} E^0((P^k)^V)$.

We recall from (2.35) that there is an isomorphism of line bundles $\mathbb{L}(L) \cong \mathcal{I}(0)$ over P_E, where $\mathcal{I}(0)$ is the ideal sheaf of the zero section; and that the functor $\mathbb{L}$ (from virtual vector bundles to line bundles over X_E) sends direct sums to tensor products. Together these observations give an isomorphism

$$\mathbb{L}(V) \cong \Theta^k(\mathcal{I}(0)) \tag{2.46}$$

of line bundles over P_E^k. With this identification, s_k is a section of the pull-back of $\Theta^k(\mathcal{I}(0))$ along the projection $MU\langle 2k\rangle^E \to S_E$.

Lemma 2.47. *The section s_k is a Θ^k-structure.*

Proof. This is analogous to Corollary 2.26. □

Let

$$MU\langle 2k\rangle^E \xrightarrow{g_k} \underline{C}^k(P_E;\mathcal{I}(0))$$

be the map classifying the Θ^k-structure s_k. We note that the isomorphism $BU\langle 2k\rangle^E \cong \underline{C}^k(P_E,\mathbb{G}_m)$ gives $\underline{C}^k(P_E;\mathcal{I}(0))$ the structure of a torsor for the group scheme $BU\langle 2k\rangle^E$.

Theorem 2.48. *For $k \leq 3$, the map g_k is a map of torsors for the group $BU\langle 2k\rangle^E$ (and so an isomorphism). Moreover, the map $MU\langle 2k+2\rangle \longrightarrow MU\langle 2k\rangle$ induces the map $\delta\colon \underline{C}^k(P_E;\mathcal{I}(0)) \to \underline{C}^{k+1}(P_E;\mathcal{I}(0))$.*

Proof. Let us write μ for the action

$$\underline{C}^k(P_E;\mathcal{I}(0)) \times \underline{C}^k(P_E,\mathbb{G}_m) \to \underline{C}^k(P_E;\mathcal{I}(0)).$$

If f_{univ} is the universal element of $\underline{C}^k(P_E,\mathbb{G}_m)$ and s_{univ} is the universal element of $\underline{C}^k(P_E;\mathcal{I}(0))$, then μ is characterized by the equation

$$\mu^* s_{univ} = f_{univ} s_{univ}, \tag{2.49}$$

as elements of $\underline{C}^k(P_E;\mathcal{I}(0))(\mathcal{O}_{\underline{C}^k(P_E;\mathcal{I}(0))\times\underline{C}^k(P_E,\mathbb{G}_m)})$.

Now consider the commutative diagram

$$\begin{tikzcd}
(P^k)^V \arrow[r, "\Delta"] \arrow[d] & (P^k)^V \wedge (P^k)_+ \arrow[d] \\
MU\langle 2k\rangle \arrow[r, "\Delta"'] & MU\langle 2k\rangle \wedge BU\langle 2k\rangle_+.
\end{tikzcd}$$

Applying E-homology and then taking the adjoint in $E_0(BU\langle 2k\rangle_+ \wedge MU\langle 2k\rangle)\widehat{\otimes}E^0(P^k)^V$ gives a section of $\Theta^k(\mathcal{I}(0))$ over $BU\langle 2k\rangle^E \times MU\langle 2k\rangle^E$. The counterclockwise composition identifies this section as the pull-back of the section s_k under the action

$$MU\langle 2k\rangle^E \times BU\langle 2k\rangle^E \xrightarrow{\Delta^E} MU\langle 2k\rangle^E$$

as in §2.4.1. Via the isomorphism $BU\langle 2k\rangle^E \cong \underline{C}^k(P_E,\mathbb{G}_m)$ of Theorem 2.29, the clockwise composition is $f_{univ}s_k$. From the description of μ (2.49) it follows that g_k is a map of torsors, as required.

Another diagram chase shows that the map $MU\langle 2k+2\rangle \to MU\langle 2k\rangle$ is compatible with the map $\delta\colon \underline{C}^k(G_E;\mathcal{I}(0)) \to \underline{C}^{k+1}(G_E;\mathcal{I}(0))$. □

Corollary 2.50. *For $0 \leq k \leq 3$, maps of ring spectra $MU\langle 2k\rangle \to E$ are in bijective correspondence with Θ^k-structures on $\mathcal{I}(0)$ over G_E.*

Proof. Since $E_*MU\langle 2k\rangle$ is torsion free and concentrated in even degrees, one has

$$[MU\langle 2k\rangle, E] = E^0 MU\langle 2k\rangle = \operatorname{Hom}_{\pi_0 E}(E_0 MU\langle 2k\rangle, \pi_0 E).$$

One checks that maps of ring spectra correspond to ring homomorphisms, so

$$\operatorname{RingSpectra}(MU\langle 2k\rangle, E) = \operatorname{Alg}_{\pi_0 E}(E_0 MU\langle 2k\rangle, \pi_0 E).$$

This is just the set of global sections of $MU\langle 2k\rangle^E$ over S_E, which is the set of Θ^k-structures on $\mathcal{I}(0)$ over G_E by the theorem. □

Example 2.51. Maps of ring spectra $MP = MU\langle 0\rangle \to E$ are in bijective correspondence with global trivializations of the sheaf $\mathcal{I}(0) \cong \mathbb{L}(L)$, that is, with generators x of the augmentation ideal $E^0P \to E^0(pt)$.

Example 2.52. Maps of ring spectra $MU = MU\langle 2\rangle \to E$ are in bijective correspondence with rigid sections of $\omega \otimes \mathcal{I}(0)^{-1}$, or equivalently with rigid sections of $\omega^{-1} \otimes \mathcal{I}(0)$. The isomorphism (2.46) identifies sections of $\omega^{-1} \otimes \mathcal{I}(0)$ with elements of $E^0(P^{L-1})$, and the rigid sections are those which restrict to the identity under the inclusion

$$S^0 \to P^{L-1}$$

of the bottom cell. It is equivalent to give a class $x \in \tilde{E}^2(P)$ whose restriction to $\tilde{E}^2(S^2)$ is the suspension of $1 \in \tilde{E}^0 S^0$; this is the description of maps $MU \to E$ in [Ada74].

2.5. The σ–orientation of an elliptic spectrum.

2.5.1. *Elliptic spectra and the Theorem of the Cube.* Let C be a generalized elliptic curve over an affine scheme S. To begin, note that the smooth locus C_{reg} is a group scheme over S, so we can define $\Theta^3(\mathcal{I}(0))$ over C_{reg}. We define a cubical structure on C to be a cubical structure on $\mathcal{I}(0)|_{C_{\text{reg}}}$; and we write $\underline{C}^3(C;\mathcal{I}(0))$ for $\underline{C}^3(C_{\text{reg}};\mathcal{I}(0))$.

Theorem 2.53. *For any (nonsingular) elliptic curve C over a normal scheme S, there is a unique cubical structure $s(C/S) \in \underline{C}^3(C;\mathcal{I}(0))$. It has the following properties:*

i. *If C'/S' is obtained from C/S by base change along $f\colon S' \longrightarrow S$, then*
$$s(C'/S') = f^*s(C/S)$$

ii. *If $t\colon C' \longrightarrow C$ is an isomorphism over S, then*
$$s(C'/S) = (t^3)^*s(C/S).$$

Proof. The first claim follows from [Gro72, Exposé VIII, Cor. 7.5] (see also [Bre83, Proposition 2.4]); the argument was sketched in the introduction. The other claims are immediate by uniqueness. □

We would like to extend this to the case where S need not be normal and C is allowed to have singularities. In this generality there may be many cubical structures (for example when C is a cuspidal cubic over spec$(\mathbb{Z})$, with $C_{\text{reg}} = \mathbb{G}_a$) but nonetheless there will be a canonical choice of one. To prove this, we will exhibit a formula which gives the unique cubical structure on the universal elliptic curve over $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6][\Delta^{-1}]$ and give a density argument to show that this formula works in general.

Definition 2.54. Let $C = C(a_1, a_2, a_3, a_4, a_6)$ be a Weierstrass curve (see Appendix B for definitions and conventions). A typical point of $(C_{\text{reg}})^3_S$ will be written as (c_0, c_1, c_2). We define $s(\underline{a})$ by the following expression:

$$s(\underline{a})(c_0, c_1, c_2) = \begin{vmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix}^{-1} \begin{vmatrix} x_0 & z_0 \\ x_1 & z_1 \end{vmatrix} \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix} \begin{vmatrix} x_2 & z_2 \\ x_0 & z_0 \end{vmatrix} (z_0 z_1 z_2)^{-1} d(x/y)_0.$$

(Compare [Bre83, Equation 3.13.4], bearing in mind the isomorphism $x \mapsto [\wp(x) : \wp'(x) : 1]$ from $\mathbb{C}/\Lambda$ to $\mathcal{E}$; Breen cites [FS80, Jac] as sources.)

Proposition 2.55. *$s(\underline{a})$ is a meromorphic section of the line bundle $p^*\omega_C$ over $(C_{\text{reg}})^3_S$ (where $p\colon C^3_S \longrightarrow S$ is the projection). It defines a rigid trivialization of*
$$(p^*\omega_C) \otimes \mathcal{I}_{-D_1+D_2-D_3} = \Theta^3(\mathcal{I}(0))$$
(in the notation of §B.4.2).

The proof is given in §B.4 of the appendix.

Corollary 2.56. *There is a unique way to assign to a generalized elliptic curve C over a scheme S a cubical structure $s(C/S) \in \underline{C}^3(C;\mathcal{I}(0))$, such that the following conditions are satisfied.*

i. *If C'/S' is obtained from C/S by base change along $f\colon S' \longrightarrow S$, then*
$$s(C'/S') = f^*s(C/S)$$

ii. *If $t\colon C' \longrightarrow C$ is an isomorphism over S, then*
$$s(C'/S) = (t^3)^*s(C/S).$$

Proof. Over the locus $WC_{\text{ell}} \subset WC$ where Δ is invertible, there is only one rigid trivialization of $\Theta^3(\mathcal{I}(0))$, and it is a cubical structure (by Theorem 2.53). Thus $s(\underline{a})$ satisfies the equations for a cubical structure when restricted to the dense subscheme $C^3_{\text{reg}} \times_{WC} WC_{\text{ell}} \subset C^3_{\text{reg}}$, so it must satisfy them globally. Similarly, the uniqueness clause in the theorem implies that $s(\underline{a})|_{WC_{\text{ell}}}$ is invariant under the action of the group WR, and thus $s(\underline{a})$ itself is invariant.

Now suppose we have a generalized elliptic curve C over a general base S. At least locally, we can choose a Weierstrass parameterization of C and then use the formula $s(\underline{a})$ to get a cubical structure. Any other Weierstrass parameterization is related to the first one by the action of WR, so it gives the same cubical structure by the previous paragraph. We can thus patch together our local cubical structures to get a global one. The stated properties follow easily from the construction. □

Theorem 2.57. *For any elliptic spectrum* $\mathbf{E} = (E, C, t)$ *there is a canonical map of ring spectra*

$$\sigma_{\mathbf{E}} \colon MU\langle 6\rangle \to E.$$

This map is natural in the sense that if $f \colon \mathbf{E} \to \mathbf{E}' = (E', C', t')$ *is a map of elliptic spectra, then the diagram*

$$\begin{tikzcd} & MU\langle 6\rangle \arrow[dl, "\sigma_{\mathbf{E}}"'] \arrow[dr, "\sigma_{\mathbf{E}'}"] & \\ E \arrow[rr, "f"'] & & E' \end{tikzcd}$$

commutes (up to homotopy).

Proof. This is now very easy. Let $s(C/S_E)$ be the cubical structure constructed in Corollary 2.56, and let $s(\widehat{C}/S_E)$ be the restriction of $s(C/S)$ to $\widehat{C}_E$. The orientation is the map $\sigma_{\mathbf{E}} : MU\langle 6\rangle \to E$ corresponding to $t^* s(\widehat{C}/S)$ via Corollary 2.50. The functoriality follows from the functoriality of s in the corollary. □

2.6. The Tate curve.

In this section we describe the Tate curve C_{Tate}, and give an explicit formula for the cubical structure $s(\widehat{C}_{\mathrm{Tate}})$. For further information about the Tate curve, the reader may wish to consult for example [Sil94, Chapter V] or [Kat73].

By way of motivation, let's work over the complex numbers. Elliptic curves over $\mathbb{C}$ can be written in the form

$$\mathbb{C}^\times/(u \sim qu)$$

for some q with $0 < |q| < 1$. This is the Tate parameterization, and as is customary, we will work with all q at once by considering the family of elliptic curves

$$C'_{\mathrm{an}}/D' = D' \times \mathbb{C}^\times/(q, u) \sim (q, qu),$$

parameterized by the punctured open unit disk

$$D' = \{q \in \mathbb{C} \mid 0 < |q| < 1\}.$$

In this presentation, meromorphic functions on C'_{an} are naturally identified with meromorphic functions $f(q, u)$ on $D' \times \mathbb{C}^\times$ satisfying the functional equation

$$f(q, qu) = f(q, u). \tag{2.58}$$

Sections of line bundles on C'_{an} admit a similar description, but with (2.58) modified according to the descent datum of the line bundle.

Let $\mathcal{I}(0)$ be the ideal sheaf of the origin on C'_{an}. The pullback of $\mathcal{I}(0)$ to $D' \times \mathbb{C}^\times$ is the line bundle whose holomorphic sections are functions vanishing at the points (q, q^n), with $n \in \mathbb{Z}$. One such function is

$$\tilde{\theta}(q, u) = (1 - u) \prod_{n>0} (1 - q^n u)(1 - q^n u^{-1}),$$

which has simple zeroes at the powers of q, and so gives a trivialization of the pullback of $\mathcal{I}(0)$ to $\mathbb{C}^\times$. The function $\tilde{\theta}(q, u)$ does not descend to a trivialization of $\mathcal{I}(0)$ on C'_{an}, but instead satisfies the functional equation

$$\tilde{\theta}(q, qu) = -u^{-1}\tilde{\theta}(q, u). \tag{2.59}$$

However, as one can easily check,

$$\delta^3\tilde{\theta}(q,u)$$

does descend to a rigid trivialization of $\Theta^3(\mathcal{I}(0))$, and hence gives the unique cubical structure.

The curve C'_{an} has the following presentation as a Weierstrass curve. Set

$$\begin{aligned}\sigma_k(n) &= \sum_{d|n} d^k \\ \alpha_k &= \sum_{n>0} \sigma_k(n) q^n \\ a_4 &= -5\alpha_3 \\ a_6 &= -(5\alpha_3 + 7\alpha_5)/12\end{aligned}$$

(The coefficients of a_6 are in fact integers). Consider the Weierstrass cubic

$$y^2 + xy = x^3 + a_4 x + a_6 \tag{2.60}$$

over D'.

Proposition 2.61. *The formulae*

$$\begin{aligned}x &= \frac{u}{(1-u)^2} + \sum_{n>0} q^n \sum_{d|n} d(u^d - 2 + u^{-d}) \\ y &= \frac{u^2}{(1-u)^3} + \sum_{n>0} q^n \sum_{d|n} \frac{d}{2}((d-1)u^d + 2 - (d+1)u^{-d}).\end{aligned}$$

give an analytic isomorphism between the projective plane curve defined by (2.60) *and* C'_{an}.

Proof. See for example [Sil94, Chapter V §1]. □

Equation (2.60) makes sense for $q = 0$ and defines a family C_{an} of generalized elliptic curves over the open unit disk

$$D = \{q \in \mathbb{C} \mid |q| < 1\}.$$

The fiber of C_{an} over $q = 0$ is the twisted cubic curve

$$y^2 = x^3.$$

The invariant differential of C_{an} is given by

$$\frac{dx}{2y+x} = \frac{du}{u}.$$

By continuity and Corollary 2.56, the expression $\delta^3\tilde{\theta}(q,u)$ determines the cubical structure on C_{an}.

Let $A \subset \mathbb{Z}[\![q]\!]$ be the subring consisting of power series which converge absolutely on the open unit disk

$$\{q \in \mathbb{C} \mid |q| < 1\}.$$

The series a_4 and a_6 are in fact elements of A, and so (2.60) defines a generalized elliptic curve C over $\operatorname{spec} A$. The curve C_{an} is obtained by change of base from A to the ring of holomorphic functions on D. The *Tate curve* C_{Tate} is the generalized elliptic curve over

$$D_{\mathrm{Tate}} = \operatorname{spec} \mathbb{Z}[\![q]\!]$$

obtained by change of base along the inclusion $A \subset \mathbb{Z}[\![q]\!]$. Since the map from the meromorphic sections of $\Theta^3(\mathcal{I}(0))$ on C^3 to meromorphic sections on C^3_{an} is a monomorphism, one can interpret the expression

$$s(C^3_{\mathrm{an}}) = \delta^3\tilde{\theta}(q,u)$$

as a formula for the cubical structure on the sheaf $\mathcal{I}(0)$ over C, and thus by base change, for C_{Tate}.

Now the map

$$D' \times \mathbb{C}^\times = D' \times \mathbb{G}_m \to C'_{\mathrm{an}}$$

is a local analytic isomorphism, and restricts to an isomorphism of formal groups

$$D' \times \widehat{\mathbb{G}}_m \to \widehat{C}'_{\mathrm{an}}.$$

This, in turn, extends to an analytic isomorphism

$$D \times \widehat{\mathbb{G}}_m \to \widehat{C}_{\mathrm{an}}. \tag{2.62}$$

Although $\tilde{\theta}(q,u)$ does not descend to a meromorphic function on C_{an}, it does extend to a function on the formal completion $\widehat{C}_{\mathrm{an}}$. In fact it can be taken to be a coordinate on $\widehat{C}_{\mathrm{an}}$. We have therefore shown

Proposition 2.63. *The pullback of the canonical cube structure $s(C_{an})$ to $\widehat{C}^3_{an}$, is given by*

$$s(\widehat{C}_{an}) = \delta^3\tilde{\theta}(q,u),$$

where $\tilde{\theta}(q,u)$ is interpreted as a coordinate on $\widehat{C}_{an}$ via (2.62). □

We now have three natural coordinates on $\widehat{C}'_{\mathrm{an}}$:

$$t = x/y, \quad \tilde{\theta}(q,u), \quad \text{and} \quad 1-u.$$

Of these, only the function t gives an algebraic coordinate on C'_{an} (and in fact on C_{an}). Let's write each of the above as formal power series in t:

$$\begin{aligned}\tilde{\theta}(q,u) = \tilde{\theta}(t) = t + O(t^2)\\ 1-u = 1-u(t) = t + O(t^2).\end{aligned}$$

By definition, the coefficients of the powers of t in the series $\tilde{\theta}(t)$ and $u(t)$ are holomorphic functions on the punctured disc D'. It is also easy to check that they in fact extend to holomorphic functions on D (set $q = 0$) and have integer coefficients (work over the completion of $\mathbb{Z}[u^{\pm 1}][\![q]\!]$ at $(1-u)$). Thus $\tilde{\theta}(t)$ and $u(t)$ actually lie in $A[\![t]\!]$, and in this way can be interpreted as functions on the formal completion of $\widehat{C}$ of C (and hence, after change of base, on the completion $\widehat{C}_{\mathrm{Tate}}$ of C_{Tate}). The function $1-u(t)$ gives an isomorphism

$$s_{\mathrm{Tate}} \overset{\mathrm{def}}{=} 1-u(t)\colon \widehat{C} \to \widehat{\mathbb{G}}_m \tag{2.64}$$

Moreover, the restriction of the cubical structure $s(C)$ to $\widehat{C}^3$ is given by

$$s(\widehat{C}) = \delta^3\tilde{\theta}(t),$$

since the map from the ring of formal functions on $\widehat{C}$ to the ring of formal functions on $\widehat{C}_{\mathrm{an}}$ is a monomorphism. Thus we have proved

Proposition 2.65. *The canonical cubical structure $s(\widehat{C}/A) \in \underline{C}^3(\widehat{C};\mathcal{I}(0))$ is given by the formula*

$$s(\widehat{C}/A) = \delta^3\tilde{\theta}(t),$$

where $t = x/y$, and $\tilde{\theta}(t)$ is the series defined above. □

2.7. **The elliptic spectrum $K_{\mathbf{Tate}}$ and its σ-orientation.** The multiplicative cohomology theory underlying K_{Tate} is simply $K[\![q]\!]$, so $\pi_0 K_{\text{Tate}} = \mathbb{Z}[\![q]\!]$. The formal group comes from that of K-theory via the inclusion

$$K \hookrightarrow K[\![q]\!],$$

and is just the multiplicative formal group. The elliptic curve is the Tate elliptic curve C_{Tate}. The triple $(K[\![q]\!], C_{\text{Tate}}, s_{\text{Tate}})$ is the Tate elliptic spectrum, which we shall denote simply K_{Tate}.

By Proposition 2.65 and Theorem 2.48, the σ-orientation is the composite

$$MU\langle 6\rangle \to MP \xrightarrow{\tilde{\theta}} K[\![q]\!],$$

with the map labeled $\tilde{\theta}$ corresponding to the coordinate $\tilde{\theta}(t)$ on $\widehat{C}_{\text{Tate}}$ in the isomorphism of Theorem 2.48. In this section, we express the map

$$\pi_* MU \to \pi_* MP \xrightarrow{\pi_* \tilde{\theta}} \pi_* K[\![q]\!]$$

in terms of characteristic classes, and identify the corresponding bordism invariant with the Witten genus.

According to Theorem 2.48, maps

$$MP \to E$$

are in one-to-one correspondence with coordinates f on the formal group. The restriction

$$MU \to MP \to E$$

sends the coordinate f to the rigid section δf of $\Theta^1(\mathcal{I}(0)) = \mathcal{I}(0)_0 \otimes \mathcal{I}(0)^{-1}$. The most straightforward formula for δf is

$$\delta f = \frac{f(0)}{f}$$

which can be misleading, because it is tempting to write $f(0) = 0$. (The point is that it is not so when regarded as a section of $\mathcal{I}(0)_0$.) It seems clearer to express δf in terms of the isomorphism

$$\mathcal{I}(0)_0 \otimes \mathcal{I}(0)^{-1} \cong \omega \otimes \mathcal{I}(0)^{-1}$$

as in §2.1.2. Sections of ω can be identified with invariant one-forms on P_E. If x is a coordinate on P_E, and $f(x)$ is a trivialization of $\mathcal{I}(0)$, then

$$\delta f = \frac{f'(0) Dx}{f(x)}$$

where Dx is the invariant differential with value dx at 0.

The K-theory orientation of complex vector bundles

$$MP \to K \tag{2.66}$$

constructed by Atiyah-Bott-Shapiro [ABS64] corresponds to the coordinate $1-u$ on the formal completion of $\mathbb{G}_m = \operatorname{spec} \mathbb{Z}[u, u^{-1}]$. The invariant differential is

$$D(1-u) = -\frac{du}{u},$$

and the restriction of (2.66) to $MU \to K$ is classified by the Θ^1-structure

$$\delta(1-u) = \frac{1}{1-u}\left(-\frac{du}{u}\right).$$

The map

$$MU \to MP \xrightarrow{\tilde{\theta}} K_{\text{Tate}}$$

factors as

$$MU \to MU \wedge BU_+ \xrightarrow{\delta(1-u)\wedge(\theta')} K_{\text{Tate}},$$

where θ' is the element of $BU^{K_{\mathrm{Tate}}} \cong C^1(\widehat{C}_{\mathrm{Tate}}, \mathbb{G}_m)$ given by the formula

$$\theta' = \prod_{n\geq 1} \frac{(1-q^n)^2}{(1-q^n\, u)(1-q^n\, u^{-1})}.$$

In geometric terms, the homotopy groups

$$\pi_* MU \wedge BU_+$$

are the bordism groups of pairs (M, V) consisting of a stably almost complex manifold M, and a virtual complex vector bundle V over M of virtual dimension 0. The map

$$\pi_* MU \to \pi_* MU \wedge BU_+$$

sends a manifold M to the pair (M, ν) consisting of M and its reduced stable normal bundle.

The map $\pi_*\delta(1-u)$ sends a manifold M of dimension $2n$ to

$$f_! 1 \in K^{-2n}(\mathrm{pt}) \approx \tilde{K}^0(S^{2n}),$$

where

$$f : M \to \mathrm{pt}$$

is the unique map. One has

$$f_! 1 = \mathrm{Td}(M) \left(-\frac{du}{u}\right)^n,$$

where $\mathrm{Td}(M)$ is the Todd genus of M, and it is customary to suppress the grading and write simply

$$f_! 1 = \mathrm{Td}(M).$$

The map θ' is the stable exponential characteristic class taking the value

$$\prod_{n\geq 1} \frac{(1-q^n)^2}{(1-q^n L)(1-q^n L^{-1})}$$

on the reduced class of a line bundle $(1-L)$. This stable exponential characteristic class can easily be identified with

$$V \mapsto \bigotimes_{n\geq 1} \mathrm{Sym}_{q^n}(-\bar{V}_{\mathbb{C}}),$$

where $V_{\mathbb{C}} = V \otimes_{\mathbb{R}} \mathbb{C}$, $\bar{V}_{\mathbb{C}} = V_{\mathbb{C}} - \mathbb{C}^{\dim V}$, and $\mathrm{Sym}_t(W)$ is defined for (complex) vector bundles W by

$$\mathrm{Sym}_t(W) = \bigoplus_{n\geq 0} \mathrm{Sym}^n(V)\, t^n \in K(M)[\![t]\!],$$

and extended to virtual bundles using the exponential rule

$$\mathrm{Sym}_t(W_1 \oplus W_2) = \mathrm{Sym}_t(W_1)\, \mathrm{Sym}_t(W_2).$$

The effect on homotopy groups of the the σ-orientation therefore sends an almost complex manifold M of dimension $2n$ to

$$(\pi_* \sigma_{K_{\mathrm{Tate}}})(M) = f_! \left(\bigotimes_{n\geq 1} \mathrm{Sym}_{q^n}(\bar{T}_{\mathbb{C}}) \right) \in \tilde{K}[\![q]\!]^0(S^{2n}).$$

This is often written as

$$f_! \left(\bigotimes_{n\geq 1} \mathrm{Sym}_{q^n}(\bar{T}_{\mathbb{C}}) \right) = \mathrm{Td}\left(M; \bigotimes_{n\geq 1} \mathrm{Sym}_{q^n}(\bar{T}_{\mathbb{C}}) \right) \left(-\frac{du}{u}\right)^n$$

or simply as

$$f_! \left(\bigotimes_{n \geq 1} \operatorname{Sym}_{q^n}(\bar{T}_{\mathbb{C}}) \right) = \operatorname{Td}\left(M; \bigotimes_{n \geq 1} \operatorname{Sym}_{q^n}(\bar{T}_{\mathbb{C}}) \right).$$

The σ-orientation of K_{Tate} determines an invariant of *Spin*–manifolds, by insisting that the diagram

$$\begin{tikzcd}
MSU \arrow[r] \arrow[d] & MU \arrow[d] \\
MSpin \arrow[r] & K_{\text{Tate}}
\end{tikzcd}$$

commute. To explain this invariant in classical terms, let M be a spin manifold of dimension $2n$, and, by the splitting principle, write

$$TM \cong L_1 + \cdots + L_n$$

for complex line bundles L_i. The *Spin* structure gives a square root of $\prod L_i$, but it is conventional to regard each L_i as having square root.

Since, for each i, the $O(2)$ bundles underlying $L_i^{1/2}$ and $L_i^{-1/2}$ are isomorphic, we can write

$$TM \cong \sum L_i + L_i^{-1/2} - L_i^{1/2},$$

which is a sum of SU-bundles.

Using this, one easily checks that the σ-orientation of M gives

$$\widehat{A}\left(M; \bigotimes_{n \geq 1} \operatorname{Sym}_{q^n}(\bar{T}_{\mathbb{C}}) \right) \left(-\frac{du}{u} \right)^n,$$

where the $\widehat{A}$ genus is the push-forward in KO-theory associated to the unique orientation $MSpin \to KO$ making the diagram

$$\begin{tikzcd}
MSU \arrow[r] \arrow[d] & MU \arrow[r] & K \arrow[d, equal] \\
MSpin \arrow[r] & KO \arrow[r] & K
\end{tikzcd}$$

commute. As above, it is customary to suppress the grading and write

$$\widehat{A}\left(M; \bigotimes_{n \geq 0} \operatorname{Sym}_{q^n}(\bar{T}_{\mathbb{C}}) \right),$$

which is formula (27) in [Wit87].

We have proved

Proposition 2.67. *The invariant*

$$\pi_* MSpin \to \mathbb{Z}[\![q]\!]$$

associated to the σ-orientation on K_{Tate} is the Witten genus. □

2.8. Modularity.

Proposition 2.68. *For any element $[M] \in \pi_{2n} MU\langle 6 \rangle$, the series*

$$(\pi_{2n}\sigma_{K_{Tate}})(M) \left(-\frac{du}{u} \right)^{-n} \in \pi_0 K_{Tate} = \mathbb{Z}[\![q]\!]$$

is the q-expansion of a modular form.

Proof. Let us write

$$\Phi(M) = (\pi_{2n}\sigma_{K_{\mathrm{Tate}}})(M)\left(-\frac{du}{u}\right)^{-n}.$$

The discussion in the preceding section shows that $\Phi(M)$ defines holomorphic function on D, with integral q-expansion coefficients. It suffices to show that, if $\pi\colon \mathfrak{H} \to D$ is the map

$$\pi(\tau) = e^{2\pi i\tau},$$

then $\pi^*\Phi(M)$ transforms correctly under the action of $SL_2\mathbb{Z}$. This follows from the discussion of H_Λ in the introduction. □

3. Calculation of $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$

In this section, we calculate the structure of the schemes $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ for $1 \leq k \leq 3$, so as to be able to compare them to $BU\langle 2k\rangle^{HP}$ in §4.

3.1. The cases $k = 0$ and $k = 1$.

The group $\underline{C}^0(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ is just the group of invertible formal power series $f \in R[\![x]\!]$; and $\underline{C}^1(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ is the group of formal power series $f \in R[\![x]\!]$ with $f(0) = 1$. Let $R_0 = \mathbb{Z}[b_0, b_0^{-1}, b_1, b_2, \dots]$, and let $R_1 = \mathbb{Z}[b_1, b_2, b_3, \dots]$. If $F_k \in \underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R_k)$ are the power series

$$F_0 = \sum_{i\geq 0} b_i x^i$$
$$F_1 = 1 + \sum_{i\geq 1} b_i x^i,$$

then the following is obvious.

Proposition 3.1. *For $k = 0$ and $k = 1$, the ring R_k represents the functor $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$, with universal element F_k.* □v

Note that F_0 has a unique product expansion

$$F_0 = a_0 \prod_{n\geq 1}(1 - a_n x^n) \tag{3.2}$$

The a_i give a different polynomial basis for R_0 and R_1.

3.2. The strategy for $k = 2$ and $k = 3$.

For $k \geq 2$, the group $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ is the group of symmetric formal power series $f \in R[\![x_1, \dots, x_k]\!]$ such that $f(x_1, \dots, x_{k-1}, 0) = 1$ and

$$f(x_1, x_2, \dots)f(x_0 + x_1, \dots)^{-1} f(x_0, x_1 + x_2, \dots) f(x_0, x_1, \dots)^{-1} = 1.$$

In the light of Remark 2.12, we can replace the normalization $f(x_1, \dots, x_{k-1}, 0) = 1$ by $f(0, \dots, 0) = 1$. Alternatively, by symmetry, we can replace it by the condition that $f(x_1, \dots, x_k) = 1 \pmod{\prod_j x_j}$.

Similarly, the group $\underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(R)$ is the group of symmetric formal power series $f \in R[\![x_1, \dots, x_k]\!]$ such that $f(x_1, \dots, x_{k-1}, 0) = 0$ and

$$f(x_1, x_2, \dots) - f(x_0 + x_1, \dots) + f(x_0, x_1 + x_2, \dots) - f(x_0, x_1, \dots) = 0.$$

We write $\underline{C}^k_d(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(R)$ for the subgroup consisting of polynomials of homogeneous degree d.

Our strategy for constructing the universal 2 and 3-cocycles is based on the following simple observation.

Lemma 3.3. *Suppose that $h \in \underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$, and that $h = 1 \bmod (x_1, \dots, x_k)^d$. Then there is a unique cocycle $c \in \underline{C}^k_d(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)$ such that $h = 1 + c \bmod (x_1, \dots, x_k)^{d+1}$. If g and h are two elements of $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ of the form $1 + c \bmod (x_1, \dots, x_k)^{d+1}$, then g/h is an element of $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ of the form $1 \bmod (x_1, \dots, x_k)^{d+1}$.* □

We call c the *leading term* of h. We first calculate a basis of homogeneous polynomials for the group of additive cocycles. Then we attempt construct multiplicative cocycles with study with our homogeneous additive cocycles as leading term. The universal multiplicative cocycle is the product of these multiplicative cocycles. Much of the work in the case $k = 3$ is showing how additive cocycles can occur as leading multiplicative cocycles.

In the cases $k = 0$ and $k = 1$, this procedure leads to the product description (3.2) of invertible power series.

We shall use the notation

$$\delta_\times : \underline{C}^{k-1}(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \to \underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$$

for the map given in Definition 2.20, and reserve δ for the map

$$\delta\colon \underline{C}^{k-1}(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a) \to \underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a).$$

Definition 2.20 gives these maps for $k \geq 2$; for $f \in \underline{C}^0(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ we define

$$\delta_\times f(x_1) = f(0)f(x_1)^{-1}$$

and similarly for $\underline{C}^0(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)$.

3.3. **The case** $k = 2$**.** Although we shall see (Proposition 3.12) that the ring $\mathcal{O}_{\underline{C}^2(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$ is polynomial over $\mathbb{Z}$, the universal 2-cocycle F_2 does not have a product decomposition

$$F_2 = \prod_{d\geq 2} g_2(d, b_d),$$

with $g_2(d, b_d)$ having leading term of degree d, until one localizes at a prime p. The analogous result for H_*BSU is due to Adams [Ada76].

Fix a prime p. For $d \geq 2$, let $c(d) \in \mathbb{Z}[x_1, x_2]$ be the polynomial

$$c(d) = \begin{cases} \frac{1}{p}(x_1^d + x_2^d - (x_1 + x_2)^d) & d = p^s \text{ for some } s \geq 1 \\ x_1^d + x_2^d - (x_1 + x_2) & \text{otherwise} \end{cases} \tag{3.4}$$

The following calculation of $\underline{C}^2(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)$ is due to Lazard; it is known as the "symmetric 2-cocycle lemma". A proof may be found in [Ada74].

Lemma 3.5. *Let A be a $\mathbb{Z}_{(p)}$-algebra. For $d \geq 2$, the group $\underline{C}^2_d(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(A)$ is the free A-module on the single generator $c(d)$.* □

Let

$$E(t) = \exp\left(\sum_{k\geq 0} \frac{t^{p^k}}{p^k}\right) \tag{3.6}$$

be the Artin-Hasse exponential (see for example [Haz78]). It is of the form 1 mod (t), and it has coefficients in $\mathbb{Z}_{(p)}$.

For $d \geq 2$, let $g_2(d, b) \in \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(\mathbb{Q}[b])$ be the power series

$$g_2(d, b) = \begin{cases} \delta_\times^2(E(bx^d)^{-p}) & \text{if } d \text{ is a power of } p \\ \delta_\times^2(E(bx^d)) & \textit{otherwise.} \end{cases} \tag{3.7}$$

Using the formulae for the polynomials $c(d)$ and the Artin-Hasse exponential, it is not hard to check that $g_2(d, b)$ belongs to the ring $\mathbb{Z}_{(p)}[b][\![x_1, x_2]\!]$, and that it is of the form

$$g_2(d, b) = 1 + bc(d) \bmod (x_1, x_2)^{d+1}. \tag{3.8}$$

We give the proof as Corollary 3.22.

Now let R_2 be the ring

$$R_2 = \mathbb{Z}_{(p)}[a_2, a_3, \dots],$$

and $F_2 \in \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R_2)$ be the the cocycle

$$F_2 = \prod_{d \geq 2} g_2(d, a_d).$$

Proposition 3.9. *The ring R_2 represents $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec}(\mathbb{Z}_{(p)})$, with universal element F_2.*

Proof. Let A be a $\mathbb{Z}_{(p)}$-algebra, and let $h \in \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(A)$ be a cocycle. By Lemma 3.5 and the equation (3.8), there is a unique element $a_2 \in A$ such that

$$\frac{h}{g_2(2, a_2)} = 1 \bmod (x_1, x_2)^3$$

in $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(A)$. Proceeding by induction yields a unique homomorphism from R_2 to A, which sends the cocycle F_2 to h. □

3.4. **The case $k = 3$: statement of results.** The analysis of $\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ is more complicated than that of of $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ for two reasons. First, the structure of $\underline{C}^3(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)$ is more complicated; in addition, it is a more delicate matter to prolong some of the additive cocycles c into multiplicative ones of the form $1 + bc + \dots$. This is reflected in the answer: although the ring representing $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ is polynomial, the ring representing $\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec}(\mathbb{Z}_{(p)})$ contains divided polynomial generators.

Definition 3.10. We write $D[x]$ for the divided-power algebra on x over $\mathbb{Z}$. It has a basis consisting of the elements $x^{[m]}$ for $m \geq 0$; the product is given by the formula

$$x^{[m]} x^{[n]} = \frac{(m+n)!}{m!n!} x^{[m+n]}.$$

If R is a ring then we write $D_R[x]$ for the ring $R \otimes D[x]$.

We summarize some well-known facts about divided-power algebras in §3.4.1.

Fix a prime p. Let R_3 be the ring

$$R_3 = \mathbb{Z}_{(p)}[a_d | d \geq 3 \text{ not of the form } 1 + p^t] \otimes \bigotimes_{t \geq 1} D_{\mathbb{Z}_{(p)}}[a_{1+p^t}].$$

In §3.6.1, we construct an element $F_3 \in \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$. In Proposition 3.28, we show that the map classifying F_3 gives an isomorphism

$$Z_3 = \operatorname{spec} R_3 \underset{\cong}{\longrightarrow} \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec}(\mathbb{Z}_{(p)}). \tag{3.11}$$

The plan of the rest of this section is as follows. In §3.5, we describe the scheme $\underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)$. We calculate $\underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a) \times \operatorname{spec} \mathbb{Q}$ for all k, and we calculate $\underline{C}^3(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a) \times \operatorname{spec} \mathbb{F}_p$. The proofs of the main results are given in Appendix A.

In §3.6, we construct multiplicative cocycles with our additive cocycles as leading terms. This will allow us to write a cocycle Z_3 over R_3 in §3.6.1. For some of our additive cocycles in characteristic p (precisely, those we call $c'(d)$), we are only able to write down a multiplicative cocycle of the form $1 + ac'(d)$ by assuming that $a^p = 0 \pmod p$; these correspond to the divided-power generators in R_3.

In §3.7, we show that the condition $a^p = 0 \pmod p$ is universal, completing the proof of the isomorphism (3.11).

3.4.1. *Divided powers.* For convenience we recall some facts about divided-power rings.

i. A *divided power sequence* in a ring R is a sequence
$$(1 = a^{[0]}, a = a^{[1]}, a^{[2]}, a^{[3]}, \dots)$$
such that
$$a^{[m]}a^{[n]} = \frac{(m+n)!}{m!n!}a^{[m+n]}$$
for all $m, n \geq 0$. It follows that $a^m = m!a^{[m]}$. We write $\mathbb{D}^1(R)$ for the set of divided power sequences in R. It is clear that $\mathbb{D}^1 = \operatorname{spec} D[x]$.

ii. An *exponential series* over R is a series $\alpha(x) \in R[\![x]\!]$ such that $\alpha(0) = 1$ and $\alpha(x+y) = \alpha(x)\alpha(y)$. We write $\operatorname{Exp}(R)$ for the set of such series. It is a functor from rings to abelian groups.

iii. Given $\underline{a} \in \mathbb{D}^1(R)$, we define $\exp(\underline{a})(x) = \sum_{m\geq 0} a^{[m]}x^m \in R[\![x]\!]$. By a mild abuse, we allow ourselves to write $\exp(ax)$ for this series. It is an exponential series, and the correspondence $\underline{a} \mapsto \exp(\underline{a})(x)$ gives an isomorphism of functors $\mathbb{D}^1 \cong \operatorname{Exp}$. In particular both are group schemes.

iv. The map $\mathbb{Q}[x] \to D_{\mathbb{Q}}[x]$ sending x to x has inverse $x^{[m]} \mapsto x^m/m!$, and this gives an isomorphism
$$\mathbb{D}^1 \times \operatorname{spec}(\mathbb{Q}) \cong \mathbb{A}^1 \times \operatorname{spec}(\mathbb{Q}).$$

v. We write $T_p[x]$ for the truncated polynomial ring $T_p[x] = \mathbb{F}_p[x]/x^p$, and we write $\alpha_p = \operatorname{spec} T_p[x]$. Thus $\alpha_p(R)$ is empty unless R is an $\mathbb{F}_p$-algebra, and in that case $\alpha_p(R) = \{a \in R \mid a^p = 0\}$.

vi. Given a $\mathbb{Z}_{(p)}$-algebra R and an element $a \in R$, we define $\operatorname{texp}(ax) = \sum_{k=0}^{p-1} a^k x^k/k!$. Here we can divide by $k!$ because it is coprime to p.

vii. Over $\mathbb{F}_p$ the divided power ring decomposes as a tensor product of truncated polynomial rings
$$D_{\mathbb{F}_p}[x] \cong \bigotimes_{r\geq 0} T_p[x^{[p^r]}]$$
Moreover there is an equation
$$\exp(ax) = \prod_{r\geq 0} \operatorname{texp}(a^{[p^r]}x^{p^r}) \pmod{p}.$$
Each factor on the right is separately exponential: if $a \in \alpha_p(R)$ then
$$\operatorname{texp}(a(x+y)) = \operatorname{texp}(ax)\operatorname{texp}(ay).$$
In other words, the map
$$\underline{a} \mapsto (a^{[1]}, a^{[p]}, a^{[p^2]}, \dots)$$
gives an isomorphism
$$\mathbb{D}^1 \times \operatorname{spec}(\mathbb{F}_p) = \prod_{m\geq 0} \alpha_p,$$
and the resulting isomorphism
$$\prod_{m\geq 0} \alpha_p \cong \operatorname{Exp} \times \operatorname{spec}(\mathbb{F}_p)$$
is given by
$$\underline{b} \mapsto \prod_{m\geq 0} \operatorname{texp}(b_m x^{p^m}).$$

3.4.2. *Grading.* It will be important to know that the maps $\mathcal{O}_{\underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)} \to R_k$ we construct may be viewed as maps of connected graded rings of finite type: a graded ring R_* is said to be of finite type over $\mathbb{Z}$ if each R_n is a finitely generated abelian group.

We let $\mathbb{G}_m$ act on the scheme $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ by

$$(u.h)(x_1, \dots , x_k) = h(ux_1, \dots , ux_k),$$

and give $\mathcal{O}_{\underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$ the grading associated to this action. One checks that the coefficient of $x^\alpha = \prod_i x_i^{\alpha_i}$ in the universal cocycle has degree $|\alpha| = \sum_i \alpha_i$. If $k > 0$ then the constant term is 1 and the other coefficients have strictly positive degrees tending to infinity, so the homogeneous components of $\mathcal{O}_{\underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$ have finite type over $\mathbb{Z}$.

The divided power ring $D[x]$ can be made into a graded ring by setting $|x^{[m]}| = m|x|$. We can then grade our rings R_k by setting the degree of a_d to be d. It is clear that R_1 is a connected graded ring of finite type over $\mathbb{Z}$, and R_k is a connected graded ring of finite type over $\mathbb{Z}_{(p)}$ for $k > 1$.

This can be described in terms of an action of $\mathbb{G}_m$ on $Z_k = \operatorname{spec} R_k$. We have

$$\begin{aligned} Z_0 &\cong \mathbb{G}_m \times \prod_{d\geq 1} \mathbb{A}^1 \\ Z_1 &\cong \prod_{d\geq 1} \mathbb{A}^1 \\ Z_2 &\cong \prod_{d\geq 2} \mathbb{A}^1 \times \operatorname{spec} \mathbb{Z}_{(p)} \\ Z_3 &\cong \prod_{d\geq 3} Z_{3,d} \end{aligned}$$

where

$$Z_{3,d} = \begin{cases} \mathbb{A}^1 \times \operatorname{spec} \mathbb{Z}_{(p)} & d \neq 1 + p^t \\ \mathbb{D}^1 \times \operatorname{spec} \mathbb{Z}_{(p)} & d = 1 + p^t. \end{cases}$$

We let $\mathbb{G}_m$ act on $\mathbb{A}^1$ or $\mathbb{G}_m$ by $u.a = ua$, and on $\mathbb{D}^1$ by $(u.a)^{[k]} = u^k a^{[k]}$. We then let $\mathbb{G}_m$ act on Z_k by

$$u.(a_k, a_{k+1}, \dots) = (u^k.a_k, u^{k+1}.a_{k+1}, \dots).$$

The resulting grading on R_k is as described. For $k \leq 2$, it is easy to check that the map $Z_k \to \underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ classifying F_k is $\mathbb{G}_m$-equivariant.

As an example of the utility of the gradings, we have the following.

Proposition 3.12. *The ring $\mathcal{O}_{C^2(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$ is polynomial over $\mathbb{Z}$ on countably many homogeneous generators.*

Proof. As $\mathcal{O}_{C^2(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$ is a connected graded ring of finite type over $\mathbb{Z}$, it suffices by well-known arguments to check that $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{C^2(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$ is polynomial on homogeneous generators for all primes p. By Proposition 3.9, we have an isomorphism of rings $\mathbb{Z}_{(p)} \otimes \mathcal{O}_{C^2(\widehat{\mathbb{G}}_a,\mathbb{G}_m)} \cong \mathcal{O}_{Z_2} = \mathbb{Z}_{(p)}[a_d \mid d \geq 2]$, and it is easy to check that a_d is homogeneous of degree d. □

3.5. **Additive cocycles.** In this section we describe the group $\underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(A)$ for various k and A. The results provide the list of candidates for leading terms of multiplicative cocycles. Proofs are given in the appendix A.

Fix an integer $k \geq 1$. We write $C^k(A)$ for $\underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(A)$, and we write $C^k_d(A)$ for the subgroup $\underline{C}^k_d(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)$ of series which are homogeneous of degree d. Note that $C^k_d(A) = 0$ for $d < k$.

Given a set $I \subseteq \{1, \dots, k\}$ we write $x_I = \sum_{i \in I} x_i$. One can easily check that for $g \in A[\![x]\!] = C^0(A)$ we have

$$(\delta^k g)(x_1, \dots, x_k) = \sum_I (-1)^{|I|} g(x_I).$$

For example, if $g(x) = x^d$ then

$$\begin{aligned}(\delta^2 g)(x, y) &= (x + y)^d - x^d - y^d \\ (\delta^3 g)(x, y, z) &= -(x + y + z)^d + (x + y)^d + (x + z)^d + (y + z)^d - x^d - y^d - z^d.\end{aligned}$$

3.5.1. *The rational case.* Rationally, the cocycles $\delta^k x^d$ for $d \geq k$ are a basis for the additive cocycles.

Proposition 3.13 (A.1)**.** *If A is a $\mathbb{Q}$-algebra, then for $d \geq k$ the group $C^k_d(A)$ is the free abelian group on the single generator $\delta^k x^d$.*

3.5.2. *Divisibility.* Now we fix an integer $k \geq 2$ and a prime p.

Definition 3.14. For all n let $\nu_p(n)$ denote the p-adic valuation of n. For $d \geq k$ we let $u(d)$ be the greatest common divisor of the coefficients of the polynomial $\delta^k(x^d)$. We write $v(d)$ for the p-adic valuation $\nu_p(u(d))$. Let $c(d)$ be the polynomial $c(d) = ((-\delta)^k(x^d))/p^{v(d)} \in \mathbb{Z}[x_1, \dots, x_k]$ (We have put a sign in the definition to ensure that $c(d)$ has positive coefficients). It is clear that

$$c(d) \in C^k_d(\mathbb{Z}).$$

If we wish to emphasize the dependence on k, we write $u_k(d)$, $c_k(d)$, and $v_k(d)$.

We will need to understand the integers $v(d)$ more explicitly.

Definition 3.15. For any nonnegative integer d and any prime p, we write $\sigma_p(d)$ for the sum of the digits in the base p expansion of d. In more detail, there is a unique sequence of integers d_i with $0 \leq d_i < p$ and $\sum_i d_i p^i = d$, and we write $\sigma_p(d) = \sum_i d_i$.

The necessary information is given by the following result, which will be proved in Appendix A.

Proposition 3.16 (A.10)**.** *For any $d \geq k$ we have*

$$v(d) = \max\left(0, \left\lceil \frac{k - \sigma_p(d)}{p - 1} \right\rceil\right).$$

The important examples of Proposition 3.16 for the present paper are $k = 2$ and $k = 3$:

Corollary 3.17.

$$v_2(d) = \begin{cases} 1 & \sigma_p(d) = 1 \\ 0 & \textit{otherwise} \end{cases}$$

$$v_3(d) = \begin{cases} 2 & \sigma_2(d) = 1 \textit{ and } p = 2 \\ 1 & \sigma_p(d) = 1 \textit{ and } p > 2 \\ 1 & \sigma_p(d) = 2 \\ 0 & \sigma_p(d) > 2. \end{cases}$$

In other words, $v_2(d) = 1$ if d is a power of p, and 0 otherwise. We have $v_3(d) = 2$ if $p = 2$ and d has the form 2^t with $t > 1$, and $v_3(d) = 1$ if $p = 2$ and d has the form $2^s(1 + 2^t)$. On the other hand, when $p > 2$ we have $v_3(d) = 1$ if d has the form p^t or $2p^t$ or $p^s(1 + p^t)$ (with $s \geq 0$ and $t > 0$). In all other cases we have $v_3(d) = 0$. □

In particular, the calculation of $v_2(d)$ shows that the cocycle $c_2(d)$ in Definition 3.14 coincides with the cocycle $c(d)$ in the formula (3.4).

3.5.3. *The modular case.* We continue to fix an integer $k \geq 2$ and a prime p, and we analyze $C^k(A)$ when $p = 0$ in A.

For any ring A we define an endomorphism ϕ of $A[\![x_1, \dots, x_k]\!]$ by $\phi(x_i) = x_i^p$. If $p = 0$ in A one checks that this sends $C^k(A)$ to $C^k(A)$ and $C^k_d(A)$ to $C^k_{dp}(A)$. Moreover, if $A = \mathbb{F}_p$ then $a^p = a$ for all $a \in \mathbb{F}_p$ and thus $\phi(h) = h^p$.

In particular, we can consider the element $\phi^j c(d) \in \mathbb{Z}[x_1, \dots, x_k]$, whose reduction mod p lies in $C^k_{p^j d}(\mathbb{F}_p)$. The following proposition shows that this rarely gives anything new.

Proposition 3.18. *If $\nu_p(d) \geq v(d)$ then*

$$c(p^j d) = c(d)^{p^j} = \phi^j c(d) \pmod{p^{\nu_p(d) - v(d) + 1}}.$$

It is clear from Proposition 3.16 that $v(pd) = v(d)$, so even if the above proposition does not apply to d, it does apply to $p^i d$ for large i.

Proof. We can reduce easily to the case $j = 1$. Write $v = v(pd) = v(d)$, so that $c(d) = (-\delta)^k (x^d)/p^v$ and $c(pd) = (-\delta)^k (x^{pd})/p^v$. Write $w = v_p(d)$, so the claim is equivalent to the assertion that

$$\phi(-\delta)^k (x^d) = (-\delta)^k (x^{pd}) \pmod{p^{w+1}}.$$

The left hand side is $\sum_I \pm\phi(x_I^d) = \sum_I \pm\phi(x_I)^d$. It is well-known that $\phi(x_I) = (x_I)^p \pmod{p}$, and that whenever we have $a = b \pmod{p}$ we also have $a^{p^i} = b^{p^i} \pmod{p^{i+1}}$. It follows easily that $\phi(x_I)^d = (x_I)^{pd} \pmod{p^{w+1}}$. As the right hand side of the displayed equation is just $\sum_I \pm(x_I)^{pd}$, the claim follows. □

3.5.4. *The case $k = 3$.* In this section we set $k = 3$, and we give basis for the group of additive three-cocycles over an $\mathbb{F}_p$-algebra. In order to describe the combinatorics of the situation, it will be convenient to use the following terminology.

Definition 3.19. We say that an integer $d \geq 3$ has *type*

I if d is of the form $1 + p^t$ with $t > 0$.
II if d is of the form $p^s(1 + p^t)$ with $s, t > 0$.
III otherwise.

If $d = p^s(1 + p^t)$ has type I or II we define $c'(d) = \phi^s c(1 + p^t) \in C^3_d(\mathbb{F}_p)$. Note that d has type I precisely when $\sigma_p(d - 1) = 1$, and in that case we have $c'(d) = c(d)$.

Proposition 3.20 (A.12). *If A is an $\mathbb{F}_p$-algebra then $C^3(A)$ is a free module over A generated by the elements $c(d)$ for $d \geq 3$ and the elements $c'(d)$ for d of type II.*

3.6. **Multiplicative cocycles.** We fix a prime p and an integer $k \geq 1$. In this section we write down the basic multiplicative cocycles. We need the following integrality lemma; many similar results are known (such as [Haz78, Lemma 2.3.3]) and this one may well also be in the literature but we have not found it.

Lemma 3.21. *Let A be a torsion-free p-local ring, and $\phi\colon A \longrightarrow A$ a ring map such that $\phi(a) = a^p \pmod{p}$ for all $a \in A$. If $(b_k)_{k>0}$ is a sequence of elements such that $\phi(b_k) = b_{k+1} \pmod{p^{k+1}}$ for all k, then the series $\exp(\sum_k b_k x^{p^k}/p^k) \in (\mathbb{Q} \otimes A)[\![x]\!]$ actually lies in $A[\![x]\!]$.*

Proof. Write $f(x) = \exp(\sum_k b_k x^{p^k}/p^k)$. Clearly $f(0) = 1$, so there are unique elements $a_j \in \mathbb{Q} \otimes A$ such that $f(x) = \prod_{j>0} E(a_j x^j)$, and it is enough to show that $a_j \in A$ for all j. By taking logs we find that

$$\sum_k b_k x^{p^k}/p^k = \sum_{i,j} a_j^{p^i} x^{jp^i}/p^i.$$

It follows that $a_j = 0$ unless j is a power of p, and that $b_k = \sum_{k=i+j} p^i a_{p^i}^{p^j}$. We may assume inductively that $a_1, a_p, \dots, a_{p^{j-1}}$ are integral. It follows that for $i < j$ we have $\phi(a_{p^i}) = a_{p^i}^p \pmod p$, and thus (by a well-known lemma) that

$$\phi(a_{p^i}^{p^{j-i-1}}) = \phi(a_{p^i})^{p^{j-i-1}} = a_{p^i}^{p^{j-i}} \pmod{p^{j-i}}.$$

It follows that

$$\begin{aligned} p^j a_{p^j} &= b_j - \sum_{i=0}^{j-1} p^i a_{p^i}^{p^{j-i}} \\ &= b_j - \sum_{i=0}^{j-1} p^i \phi(a_{p^i})^{p^{j-i-1}} \pmod{p^j} \\ &= b_j - \phi(b_{j-1}) \\ &= 0 \pmod{p^j}, \end{aligned}$$

or in other words that a_{p^j} is integral. □

Recall from (3.6) that $E(t) \in \mathbb{Z}_{(p)}[\![t]\!]$ denotes the Artin-Hasse exponential.

Corollary 3.22. *If d is such that $\nu_p(d) \geq v(d)$, then $\delta_\times^k E(bx^d)^{p^{-v(d)}} \in \mathbb{Q}[b][\![x_1, \dots, x_k]\!]$ actually lies in $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(\mathbb{Z}_{(p)}[b]) \subseteq \mathbb{Z}_{(p)}[b][\![x_1, \dots, x_k]\!]$. It has leading term $bc(d)$.*

Proof. The symmetric cocycle conditions are clear, so we need only check that the series is integral. Using the exp in the Artin-Hasse exponential gives the formula

$$\delta_\times^k E(bx^d)^{p^{-v(d)}} = \exp\left(\sum_{i\geq 0} \frac{b^{p^i} \delta^k(x^{dp^i})}{p^{i+v(d)}}\right) = \exp\left(\sum_{i\geq 0} \frac{b^{p^i} c(dp^i)}{p^i}\right).$$

In view of Lemma 3.21, it suffices to check that $\phi(c(dp^i)) = c(dp^{i+1}) \pmod{p^{i+1}}$, where ϕ is the endomorphism of $\mathbb{Z}_{(p)}[\![x_1, \dots, x_k]\!]$ given by $\phi(x_i) = x_i^p$. This follows from Proposition 3.18. □

Definition 3.23. If R is a $\mathbb{Z}_{(p)}$-algebra, b is an element of R, and if d is such that $\nu_p(d) \geq v(d)$, we define

$$E(k, d, b) \overset{\text{def}}{=} \delta_\times^k E(bx^d)^{p^{-v(d)}}$$

to be the element of $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ given by the corollary.

In order to analyze the map $\delta_\times$, we need the following calculation.

Lemma 3.24. *If $\nu_p(d) \geq v(d)$ we have*

$$E(k, d, b)^p = E(k, pd, b^p) \pmod p.$$

Proof. We can work in the universal case, where $A = \mathbb{Z}_{(p)}[b]$ is torsion-free, so it makes sense to use exponentials. We have

$$E(k, d, b) = \exp(\sum_k b^{p^k} c(p^k d)/p^k),$$

and it follows easily that $E(k, d, b)^p / E(k, pd, a^p) = \exp(pac(d))$. One checks easily that the series $\exp(pt) - 1$ has coefficients in $p\mathbb{Z}_{(p)}$, and the claim follows. □

We need one other family of cocycles, given by the following result.

Proposition 3.25. *Let B be the divided-power algebra on one generator b over $\mathbb{Z}_{(p)}$. Then the series $\delta_\times^k \exp(bx^d/p^{v(d)}) = \exp((-1)^k b\, c(d))$ lies in $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(B) \subseteq B[\![x_1, \dots, x_k]\!]$.* □

3.6.1. *The case $k = 3$.* Suppose that $d \geq 3$ is not of the form $1 + p^t$. Then Corollary 3.17 shows that $\nu_p(d) \geq v(d)$, and so Definition 3.23 gives cocycles

$$g_3(d, a_d) \overset{\text{def}}{=} E(3, d, a_d) \in \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(\mathbb{Z}_{(p)}[a_d]). \tag{3.26}$$

For $d = 1 + p^t$ and $t \geq 1$, let

$$g_3(d, a_d) \overset{\text{def}}{=} \exp(-a_d\, c(d)) \in \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(D_{\mathbb{Z}_{(p)}}[a_d])$$

be the cocycle given by Proposition 3.25.

Note that if $d = 1 + p^t$ then in $\mathbb{F}_p \otimes D_{\mathbb{Z}_{(p)}}[a_d]$ we have an equation

$$g_3(d, a_d) = \prod_{s \geq 0} \operatorname{texp}(-a_d^{[p^s]} c'(dp^s)) \tag{3.27}$$

as in §3.4.1, and each factor on the right is separately an element of $\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(T_p[a_d^{[p^s]}])$.

Let F_3 be the cocycle

$$F_3 = \prod_{d \geq 3} g_3(d, a_d)$$

over

$$Z_3 = \operatorname{spec} \mathbb{Z}_{(p)}[a_d \mid d \neq 1 + p^t] \otimes \bigotimes_{t \geq 1} D_{\mathbb{Z}_{(p)}}[a_{1+p^t}].$$

Proposition 3.28. *The map $Z_3 \to \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec}(\mathbb{Z}_{(p)})$ classifying F_3 is an isomorphism.*

Proof. Let h denote this map. It is easy to check that it is compatible with the $\mathbb{G}_m$-actions described in §3.4.2, so the induced map of rings preserves the gradings.

We will show that the map $h(R)\colon Z_3(R) \longrightarrow \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ is an isomorphism when R is a $\mathbb{Q}$-algebra or an $\mathbb{F}_p$-algebra. This means that the map $h^*\colon \mathcal{O}_{\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)} \otimes \mathbb{Z}_{(p)} \longrightarrow \mathcal{O}_{Z_3}$ becomes an isomorphism after tensoring with $\mathbb{Q}$ or $\mathbb{F}_p$. As both sides are connected graded rings of finite type over $\mathbb{Z}_{(p)}$, it follows that h is itself an isomorphism.

Suppose that R is a $\mathbb{Q}$-algebra. In this case we get divided powers for free, and an element of $Z_3(R)$ is just a list of elements $(a_3, a_4, \dots)$. According to Proposition 3.13, the additive cocycle $c(d)$ generates $\underline{C}^3_d(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(R)$. Since g_d has leading term $a_d c(d)$, the process of successive approximation suggested by Lemma 3.3 shows that $h(R)$ is an isomorphism.

We now suppose instead that R is an $\mathbb{F}_p$-algebra. As $D_{\mathbb{F}_p}[x] = T_p[x^{[p^i]} \mid i \geq 0]$, we see that a point of $Z_3(R)$ is just a sequence of elements $a_d \in R$ for $d \geq 3$, with additional elements $a_{d,i} = a_d^{[p^i]}$ when d has type I, such that $a_{d,0} = a_d$ and $a_{d,i}^p = 0$. We write $a'_{dp^i} = a_{d,i}$. With this reindexing, an element of $Z_3(R)$ is a system of elements a_d (where d has type II or III) together with a system of elements a'_d (where d has type I or II) subject only to the condition $(a'_d)^p = 0$.

On the other hand, suppose that $f \in C^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ is a cocycle with leading term c of degree d. If d has type III, then Proposition 3.20 shows that $c = a_d c(d)$ for a unique c in R. If d has type I, then $c = a'_{d,0} c'(d)$ for some unique $a'_{d,0}$ in R. Finally, if d has type II, then $c = a_d c(d) + a'_d c'(d)$ for some unique a_d and a'_d in R. We shall show in Proposition 3.29 that in fact $(a'_d)^p = 0$. The process of successive approximation gives a point of $Z_3(R)$ which clearly maps to f under the map $h(R)$. □

In the course of the proof, we used the following result, whose proof will be given in §3.7.

Proposition 3.29. *Suppose that R is an $\mathbb{F}_p$-algebra and that $f \in C^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ has leading term $ac'(d)$ (so that d has type I or II). Then $a^p = 0$.*

Corollary 3.30. *The ring $\mathcal{O}_{C^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)}$ is a graded free abelian group of finite type.*

Proof. Proposition 3.28 shows that this is true p-locally for every prime p, so it is true integrally. □

3.7. The Weil pairing: cokernel of $\delta_\times \colon \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \to \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$.

The first result of this section is a proof of Proposition 3.29, which completes the calculation in Proposition 3.28. The analysis which leads to this result also gives a description of the cokernel of the map

$$\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \xrightarrow{\delta_\times} \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m),$$

which we shall use to compare $\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ to $BU\langle 6\rangle^{HP}$.

More precisely, the scheme Z_3 decomposes as a product of schemes

$$Z_3 = Z_3' \times \mathbb{Z}_3''$$

where

$$\begin{aligned} Z_3' &= \operatorname{spec} D_{\mathbb{Z}_{(p)}}[a_{1+p^t} \mid t \geq 1] \\ Z_3'' &= \operatorname{spec} \mathbb{Z}_{(p)}[a_d \mid d \text{ not of the form } 1+p^t]. \end{aligned}$$

We shall show that $\delta_\times$ maps $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec} \mathbb{F}_p$ surjectively onto $Z_3'' \times \operatorname{spec} \mathbb{F}_p$, and that the cokernel $\mathbb{Z}_3' \times \operatorname{spec} \mathbb{F}_p$ has a natural description as the scheme $\mathrm{Weil}(\widehat{\mathbb{G}}_a)$ of *Weil pairings*. In §4.5.1, we shall see that this scheme is isomorphic to the scheme associated to the even homology of $K(\mathbb{Z}, 3)$. In this paper we give a bare-bones account of Weil pairings. The reader can consult [Bre83, Mum65, AS98] for a more complete treatment.

Definition 3.31. Let R be any ring, and h an element of $\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$. We define a series $e(h) \in R[\![x, y]\!]$ by the formula

$$e(h)(x, y) = \prod_{k=1}^{p-1} \frac{h(x, kx, y)}{h(x, ky, y)}.$$

In §3.7.1, e will be interpreted as giving a map of group schemes

$$\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec} \mathbb{F}_p \to \mathrm{Weil}(\widehat{\mathbb{G}}_a).$$

Proposition 3.32. *We have*

$$\begin{aligned} e(h)(x, y)\, e(h)(x, z) &= e(h)(x, y+z)\, \frac{h(px, y, z)}{h(x, py, pz)} \\ &= e(h)(x, y+z) \pmod{p}, \end{aligned}$$

and $e(h)(x, y)^p = 1 \pmod{p}$.

Proof. Recall the cocycle relation $R(w, x, y, z) = 1$, where

$$R(w, x, y, z) = \frac{h(x, y, z) h(w, x+y, z)}{h(w+x, y, z) h(w, x, z)}.$$

By brutally expanding the relation

$$R(y, z, k(y+z), x) R(ky, (k+1)z, y, x) R((k+1)z, y, ky, x) \\ R(ky, kz, z, x) R(kx, x, y, z) R(x, y, z, kx) = 1,$$

and using the symmetry of h, we find that

$$\frac{h(x, kx, y)}{h(x, ky, y)} . \frac{h(x, kx, z)}{h(x, kz, z)} = \frac{h(x, kx, y+z)}{h(x, ky+kz, y+z)} . \frac{h(x, ky, kz)}{h(x, (k+1)y, (k+1)z)} . \frac{h((k+1)x, y, z)}{h(kx, y, z)}$$

We now take the product from $k = 1$ to $p-1$. We note that the second term on the right has the form $f(k)/f(k+1)$, so the product gives $f(1)/f(p)$. After dealing with the last term in a similar way and doing some cancellation, we find that

$$e(h)(x, y)\, e(h)(x, z) = e(h)(x, y+z)\, h(px, y, z)\, h(x, py, pz)^{-1},$$

as claimed. For any cocycle h we have $h = 1 \pmod{xyz}$, so our expression reduces to $e(h)(x, y+z)$ modulo p. This means that $e(h)$ behaves exponentially in the second argument, so $e(h)(x,y)^p = e(h)(x, py) = 1 \pmod{p}$. □

We can also consider an additive analogue of the above construction. Given $c \in C^3(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(R)$, we write

$$e_+(c)(x,y) = \sum_{k=1}^{p-1} (c(x, kx, y) - c(x, ky, y)).$$

By applying the definitions and canceling in a simple-minded manner we find that

$$e_+(\delta^3 f)(x,y) = f(x) - f(x+py) - f(y) + f(y+px) - f(px) + f(py).$$

Thus $e_+(\delta^3 f) = 0 \pmod{p}$.

The following calculation is the key to the proof of Proposition 3.29, and it also permits the identification of $\mathbb{Z}'_3$ with the scheme of Weil pairings.

Lemma 3.33. *Let $d = p^s(1+p^t)$ with $s \geq 0$ and $t \geq 1$. Then*

$$e_+(c'(d)) = x^{p^s} y^{p^{s+t}} - x^{p^{s+t}} y^{p^s} \pmod{p}.$$

Proof. As $c'(p^s(1+p^t))^p = c(1+p^t)^{p^{s+1}}$, it suffices to calculate $e_+(c(1+p^t)) \pmod{p}$. Let $n = 1 + p^t$. By Corollary 3.17, we have $c(n) = \delta^3(x^n)/p$, so that

$$\begin{aligned} pe_+(c(n)) &= x^n - (x+py)^n - y^n + (y+px)^n - p^n x^n + p^n y^n \\ &= -pnx^{n-1}y + pnxy^{n-1} \pmod{p^2} \\ &= p(xy^{p^t} - x^{p^t} y) \pmod{p^2}. \end{aligned}$$

Thus $e_+(c(1+p^t)) = xy^{p^t} - yx^{p^t} \pmod{p}$ as required. □

We can now give the

Proof of Proposition 3.29. Suppose that R is an $\mathbb{F}_p$-algebra and that $h \in C^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ has leading term $ac'(d)$ (so that d has type I or II).

It is easy to see that $e(h) = 1 + ae_+(c'(d)) \pmod{(x,y,z)^{d+1}}$, and thus that $e(h)^p = 1 + a^p e_+(c'(d))^p \pmod{(x,y,z)^{pd+1}}$. On the other hand, we know from Proposition 3.32 that $e(h)^p = 1$. Lemma 3.33 shows that $e_+(c'(d))^p$ is a nonzero polynomial over $\mathbb{F}_p$ which is homogeneous of degree pd. It follows that $a^p = 0$. □

3.7.1. *The scheme of Weil pairings.* In this section we work implicitly over $\operatorname{spec}(\mathbb{F}_p)$. We note that a faithfully flat map of schemes is an epimorphism.

We also recall [DG70, III,§3,n. 7] that the category of affine commutative group schemes over $\mathbb{F}_p$ is an abelian category, in which $\operatorname{spec} f\colon \operatorname{spec} A \to \operatorname{spec} B$ is an epimorphism if and only if $f\colon B \to A$ is injective.

Let R be an $\mathbb{F}_p$-algebra. We write $\operatorname{Weil}(\widehat{\mathbb{G}}_a)(R)$ for the group (under multiplication) of formal power series $f(x,y) \in R[\![x,y]\!]$ such that

$$\begin{aligned} f(x,x) &= 1 \\ f(x,y)f(x,z) &= f(x, y+z) \\ f(x,z)f(y,z) &= f(x+y, z). \end{aligned} \tag{3.34}$$

Note that this implies $f(x,y)f(y,x) = 1$ by a polarization argument. We write $\operatorname{Weil}(\widehat{\mathbb{G}}_a)(R) = \emptyset$ if R is not an $\mathbb{F}_p$-algebra.

Proposition 3.32 shows that, if R is an $\mathbb{F}_p$-algebra and $h \in \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ is a three-cocycle, then $e(h)$ is a Weil pairing. In other words, e may be viewed as a natural transformation

$$e\colon \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \to \operatorname{Weil}(\widehat{\mathbb{G}}_a).$$

In this section, we show that there is a commutative diagram

$$\begin{tikzcd}
\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, "\delta_\times"] \arrow[d, two heads] & \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, two heads, "e"] & \operatorname{Weil}(\widehat{\mathbb{G}}_a) \\
Z_3'' \arrow[r, tail] & Z_3' \times Z_3'' \arrow[r, two heads] \arrow[u, "\cong"] & Z_3' \arrow[u, "\cong"]
\end{tikzcd} \tag{3.35}$$

of group schemes over $\operatorname{spec} \mathbb{F}_p$, with exact rows and with epi, mono, and isomorphisms as indicated. In §4.5, we compare the top row to a sequence arising from the fibration $K(\mathbb{Z}, 3) \to BU\langle 6\rangle \to BSU$.

To begin, we note that $\operatorname{Weil}(\widehat{\mathbb{G}}_a)$ is an affine group scheme over $\mathbb{F}_p$. The representing ring $\mathcal{O}_{\operatorname{Weil}(\widehat{\mathbb{G}}_a)}$ is the quotient of the ring $\mathbb{F}_p[a_{kl} \mid k, l \geq 0]$ by the ideal generated by the coefficients of the series $\tilde{f}(x, x) - 1$ and $\tilde{f}(x + y, z) - \tilde{f}(x, z)\tilde{f}(y, z)$ and $\tilde{f}(x, y + z) - \tilde{f}(x, y)\tilde{f}(x, z)$, where $\tilde{f}$ is the power series

$$\tilde{f}(x, y) = \sum a_{kl} x^k y^l.$$

We let $\mathbb{G}_m$ act on $\operatorname{Weil}(\widehat{\mathbb{G}}_a)$ by $(u.f)(x, y) = f(ux, uy)$, and this gives a grading on $\mathcal{O}_{\operatorname{Weil}(\widehat{\mathbb{G}}_a)}$ making it into a graded connected Hopf algebra over $\mathbb{F}_p$. If

$$f(x, y) = \sum_{i,j} a_{ij} x^i y^j$$

is the universal Weil pairing, then the degree of a_{ij} is $i + j$.

Lemma 3.36. *The ring $\mathcal{O}_{\operatorname{Weil}(\widehat{\mathbb{G}}_a)}$ is a tensor product of rings of the form $\mathbb{F}_p[a]/a^p$. If $f = \sum a_{ij} x^i y^j$ is the universal Weil pairing, then elements of the form a_{p^m, p^n} with $m < n$ are a basis for* $\operatorname{Ind}(\mathcal{O}_{\operatorname{Weil}(\widehat{\mathbb{G}}_a)})$.

Proof. Let us temporarily write A for $\mathcal{O}_{\operatorname{Weil}(\widehat{\mathbb{G}}_a)}$. Note that if $f(x, y) \in \operatorname{Weil}(\widehat{\mathbb{G}}_a)(R)$ we have $f(x, y)^p = f(x, py) = f(x, 0) = 1$, and it follows that the Frobenius map for A is trivial. It follows from the structure theory of connected graded Hopf algebras over $\mathbb{F}_p$ that A is a tensor product of rings of the form $\mathbb{F}_p[a]/a^p$.

The dual of the group of indecomposables in A is easily identified with the kernel of the map

$$\operatorname{Weil}(\widehat{\mathbb{G}}_a)(\mathbb{F}_p[\epsilon]/\epsilon^2) \to \operatorname{Weil}(\widehat{\mathbb{G}}_a)(\mathbb{F}_p)$$

that is induced by the augmentation map $\mathbb{F}_p[\epsilon]/\epsilon^2 \to \mathbb{F}_p$. This kernel is the set of power series of the form $1 + \epsilon g(x, y)$ (with $g \in \mathbb{F}_p[\![x, y]\!]$) such that $1 + \epsilon g(x, x) = 0$ and $(1 + \epsilon g(x, y))(1 + \epsilon g(x, z)) = 1 + \epsilon g(x, y + z)$ and $(1 + \epsilon g(x, z))(1 + \epsilon g(y, z)) = 1 + \epsilon g(x + y, z)$. This reduces to the requirement that $g(x, y)$ be additive in both arguments, with $g(x, x) = 0$. The additivity means that $g(x, y)$ must have the form $\sum_{m,n} b_{mn} x^{p^m} y^{p^n}$. Because $g(x, x) = 0$ we must have $b_{mm} = 0$ (even if $p = 2$) and $b_{mn} = -b_{nm}$ if $m > n$. □

Let j denote the splitting map

$$Z_3' \to \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m).$$

Note that Z_3' is a group scheme, because

$$Z_3' \cong \prod \mathbb{D}^1 \times \operatorname{spec}(\mathbb{Z}_{(p)}) \cong \prod \operatorname{Exp} \times \operatorname{spec}(\mathbb{Z}_{(p)}).$$

It is easy to check that j is a map of group schemes (even over $\operatorname{spec}(\mathbb{Z}_{(p)})$). The first step in the analysis of the diagram 3.35 is the following.

Proposition 3.37. *The map of group schemes*

$$ej\colon Z_3' \to \mathrm{Weil}(\widehat{\mathbb{G}}_a)$$

is an isomorphism.

Proof. First, when R is an $\mathbb{F}_p$-algebra we can identify $Z_3'(R)$ with $\prod_d \{a \in R \mid a^p = 0\}$, where d runs over integers $d \geq 3$ of type I or II, and according to (3.27), $j(\underline{a})$ is the cocycle

$$j(\underline{a}) = \coprod_d \mathrm{texp}(-a_d c'(d)).$$

Lemma 3.33 shows that if $d = p^s(1+p^t)$ then

$$e(\mathrm{texp}(-a_d c'(d)) = 1 - a_d(x^{p^s} y^{p^{s+t}} - x^{p^{s+t}} y^{p^s}) \pmod{(x,y)^{d+1}}.$$

It follows that ej induces an isomorphism of indecomposables. Moreover, ej induces a map of graded rings if $\mathcal{O}_{Z_3'}$ is given the grading with a_d' in dimension d. We thus a map of connected graded algebras, both of which are tensor products of polynomial algebras truncated at height p, and our map gives an isomorphism on indecomposables. It follows that the map is an isomorphism. □

To show that Z_3'' is the kernel of e, we first observe that $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ maps to the kernel.

Lemma 3.38. *If R is an $\mathbb{F}_p$-algebra and $g \in \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$ then $e(\delta_\times g) = 1$.*

Proof. By definition we have $\delta_\times g(x, kx, y) = g(x,y)g(kx,y)/g((k+1)x, y)$. As $\delta_\times g$ is symmetric, we have $\delta_\times g(x, ky, y) = g(x,y)g(x,ky)/g(x,(k+1)y)$. By substituting these equations into the definition of $e(\delta_\times g)$ and canceling, we obtain $e(\delta_\times g)(x,y) = g(x,py)/g(px,y)$, which is 1 because $p = 0$ in R. □

Next we show that $\delta_\times$ actually factors through the inclusion $Z_3'' \to \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$. Let w and θ be given by the formulae

$$\begin{aligned} w(2) &= 1 \\ w(d) &= v_3(d) - v_2(d) && d \geq 3 \\ \theta(d) &= p^{w(d)} d. \end{aligned}$$

By Corollary 3.17, it is equivalent to set $w(d) = 1$ if d is of the form $p^s(1+p^r)$ with $r \geq 0$, and $w(d) = 0$ otherwise. It follows also that θ gives a bijection from $\{d \mid d \geq 2\}$ to $\{d \mid d \geq 3 \text{ and } d \text{ is not of the form } 1+p^t\}$.

Let $r\colon Z_2 = \operatorname{spec} R_2 \to Z_3''$ be given by the formula

$$r^* a_{\theta(d)} = a_d^{p^{w(d)}}.$$

It is clear that r is faithfully flat.

Lemma 3.39. *The diagram*

$$\begin{tikzcd}
\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, "\delta_\times"] & \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \\
Z_2 \arrow[u, "\cong"] \arrow[r, "r"] & Z_3'' \arrow[u]
\end{tikzcd}$$

commutes over $\operatorname{spec}(\mathbb{F}_p)$. *In particular, over* $\operatorname{spec}(\mathbb{F}_p)$, $\delta_\times$ *factors through a faithfully flat map* $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \to Z_3''$.

Proof. This follows from the equations

$$\delta_\times g_2(d,a) = \delta_\times^3 E(ax^d)^{p^{-v_2(()d)}} = E(3,d,a)^{p^{w(d)}} = E(3, \theta(d), a^{p^{w(d)}}) = g_3(\theta(d), a^{p^{w(d)}}).$$

The only equation which is not a tautology is the third, which is Lemma 3.24. Actually the lemma does not apply in the case $d = 2$, but the result is valid anyway. One can see this directly from the definitions, using the fact that $\delta^3(x^2) = 0$. □

Proposition 3.40. *The kernel of the map*

$$e\colon \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \to \mathrm{Weil}(\widehat{\mathbb{G}}_a)$$

is Z_3'' (which is thus a subgroup scheme). Moreover, we have $\underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) = Z_3' \times Z_3''$ as group schemes.

Proof. We know from Lemma 3.38 that $e\delta_\times = 1$, and faithfully flat maps are epimorphisms of schemes, so Lemma 3.39 implies that $Z'' \leq \ker(e)$. As the map $(f', f'') \mapsto f'f''$ gives an isomorphism $Z' \times Z'' \to \underline{C}^3$, and $e\colon Z' \to \mathrm{Weil}(\widehat{\mathbb{G}}_a)$ is an isomorphism, it follows that $Z'' = \ker(e)$. This means that Z'' is a subgroup scheme, and we have already observed before Proposition 3.37 that the same is true of Z'. It follows that $\underline{C}^3 = Z' \times Z''$ as group schemes. □

We summarize the discussion in this section as the following.

Corollary 3.41. *If we work over* $\mathrm{spec}(\mathbb{F}_p)$ *then the following sequence of group schemes is exact:*

$$\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \xrightarrow{\delta} \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \xrightarrow{e} \mathrm{Weil}(\widehat{\mathbb{G}}_a) \to 0.$$

□

3.8. The map $\delta_\times : \underline{C}^1(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \to \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$.

In the course of comparing BSU^{HP} to $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ in §4, we shall use the following analogue of Corollary 3.41.

Proposition 3.42. *For each prime p, the map*

$$\underline{C}^1(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \mathrm{spec}(\mathbb{F}_p) \xrightarrow{\delta_\times} \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \mathrm{spec}(\mathbb{F}_p)$$

is faithfully flat.

Proof. In order to calculate $\delta_\times$, it is useful to use the model for $\underline{C}^1$ which is analogous to our model Z_2 for $\underline{C}^2$. Let Z_1 be the scheme

$$Z_1 = \mathrm{spec}\,\mathbb{Z}_{(p)}[a_d \mid d \geq 1],$$

and let

$$\begin{aligned} F_1 &\overset{\mathrm{def}}{=} \prod_{d\geq 1} E(1, d, a_d) \\ &= \prod_{d\geq 1} E(a_d x^d) \end{aligned}$$

be the resulting cocycle over $\mathcal{O}_{Z_1}$. It is clear that the map

$$Z_1 \to \underline{C}^1(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \mathrm{spec}(\mathbb{Z}_{(p)})$$

classifying F_1 is an isomorphism. Thus if $k = 1$ or 2, and if R is a $\mathbb{Z}_{(p)}$-algebra, then $Z_k(R)$ is the set of sequences $(a_k, a_{k+1}, \dots)$ of elements of R.

For $d \geq 1$ let $\theta(d) = p^{v_2(d)} d$, with the convention that $v_2(1) = 1$. The calculation of $v_2(d)$ in Corollary 3.17 shows that θ induces a bijection from the set $\{d \mid d \geq 1\}$ to the set $\{d \mid d \geq 2\}$. Let $r\colon Z_1 \to Z_2$ be the map which sends a sequence $\underline{a} = (a_1, a_2, \dots) \in \mathbb{Z}_1(R)$ to the sequence

$$r(\underline{a})_{\theta(d)} = a_d^{p^{v_2(d)}}.$$

Thus r is a product of copies of the identity map $\mathbb{A}^1 \to \mathbb{A}^1$ (indexed by $\{d \mid v(d) = 0\}$), together with some copies of the Frobenius map $\mathbb{A}^1 \to \mathbb{A}^1$ (indexed by $\{d \mid v(d) = 1\}$). These maps are faithfully flat, and so r is faithfully flat. The Proposition then follows once we know that the diagram

$$\begin{tikzcd}
\underline{C}^1(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec}(\mathbb{F}_p) \arrow[r, "\delta_\times"] & \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec}(\mathbb{F}_p) \\
Z_1 \times \operatorname{spec}(\mathbb{F}_p) \arrow[u, "\cong"] \arrow[r, "r"] & Z_2 \times \operatorname{spec}(\mathbb{F}_p) \arrow[u, "\cong"']
\end{tikzcd}$$

commutes. The commutativity of the diagram follows from the equations (modulo p)

$$\begin{aligned}
\delta_\times E(ax^d) &= E(2,d,a)^{p^{v_2(d)}} \\
&= E(2,\theta(d),a^{p^{v_2(d)}}) \\
&= g_2(\theta(d),a^{p^{v_2(d)}}).
\end{aligned}$$

The first and last equations are tautologies; the middle equation follows from Lemma 3.24. □

3.9. **Rational multiplicative cocycles.** Given $k > 0$, let $Y_k(R)$ be the set of formal power series $f(x) \in R[\![x]\!]$ such that $f(x) = 1 \pmod{x^k}$. This clearly defines a closed subscheme $Y_k \subset \underline{C}^0(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$

Proposition 3.43. *Over* $\operatorname{spec}(\mathbb{Q})$*, the map* $\delta_\times^k : Y_k \to \underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ *is an isomorphism.*

Proof. Let R be a $\mathbb{Q}$-algebra, and let $g \in R[\![x_1, \dots, x_k]\!]$ be an element of $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$. We need to show that $g = \delta_\times^k(f)$ for a unique element $f \in Y_k(R)$. If $I = (x_1, \dots, x_k)$ then $g = 1 \pmod{I}$ so the series $\log(g) = -\sum_{m>0}(1-g)^m/m$ is I-adically convergent. One checks that it defines an element of $\underline{C}^k(\widehat{\mathbb{G}}_a, \mathbb{G}_a)(R)$, so Proposition 3.13 tells us that there is a unique $h \in R[\![x]\!]$ with $h = 0 \pmod{x^k}$ and $\delta^k(h) = \log(g)$. The series $\exp(h) = \sum_m h^m/m!$ is x-adically convergent to an element of $Y_k(R)$, which is easily seen to be the required f. □

4. Topological calculations

In this section we will compare our algebraic calculations with known topological calculations of E_*BU, H_*BSU, and $H_*BU\langle 6\rangle$, and we deduce that $BU\langle k\rangle^E = \underline{C}^k(P_E, \mathbb{G}_m)$ for $k \leq 3$. We start with the cases $k = 0$ and $k = 1$, which are merely translations of very well-known results. We then prove the result for all k when $E = HP\mathbb{Q}$ (the rational periodic Eilenberg-MacLane spectrum); this is an easy calculation.

Next, we prove the case $k = 2$ with $E = HP$. It suffices to do this with coefficients in the field $\mathbb{F}_p$, and then it is easy to compare our analysis of the scheme $\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ to the short exact sequence

$$P^{HP} \to BU^{HP} \to BSU^{HP}.$$

For $BU\langle 6\rangle$ we recall Singer's calculation of $H^*(BU\langle 6\rangle; \mathbb{F}_p)$, which is based on the fibration

$$K(\mathbb{Z}, 3) \to BU\langle 6\rangle \to BSU.$$

Most of the work in this section is to produce the topological analogue of the exact sequence

$$\begin{tikzcd}
\underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, "\delta_\times"] & \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, "e"] & \operatorname{Weil}(\widehat{\mathbb{G}}_a) \arrow[r] & 0
\end{tikzcd}$$

of Corollary 3.41; see (4.9). Having done so, we can easily prove the isomorphism $BU\langle 6\rangle^E \cong \underline{C}^3(P_E, \mathbb{G}_m)$ for $E = HP\mathbb{F}_p$. The isomorphism for integral homology follows from the cases $E = HP\mathbb{Q}$ and $E = HP\mathbb{F}_p$. Using a collapsing Atiyah-Hirzebruch spectral sequence and its algebraic analogue, we deduce the case $E = MP$, and we find that $MP_0 BU\langle 6\rangle$ is free over MP_0. It is then easy to deduce the isomorphism for arbitrary E.

4.1. **Ordinary cohomology.** We begin with a brief recollection of the ordinary cohomology of BU, in order to fix notation.

It is well-known that H^*BU is a formal power series algebra generated by the Chern classes. It follows easily that the corresponding thing is true for HP^0BU: we can define Chern classes $c_k \in HP^0BU$ for $k > 0$ and we find that $HP^0BU = \mathbb{Z}[\![c_k \mid k > 0]\!]$. We also put $c_0 = 1$. We define a series $c(t) \in HP^0[\![t]\!]$ by $c(t) = \sum_{k\geq 0} c_k t^k$. We then define elements q_k by the equation $tc'(t)/c(t) = \sum_k q_k t^k$. The group of primitives is

$$\operatorname{Prim} HP^0BU = \{\sum_i n_i q_i \mid n_i \in \mathbb{Z}\} \cong \prod_{i>0} \mathbb{Z}.$$

There is an inclusion $S^1 = U(1) \xrightarrow{j} U$ and a determinant map $U \xrightarrow{\det} S^1$ with $\det \circ j = 1$. These give maps $P \xrightarrow{Bj} BU \xrightarrow{B\det} P$ with $B\det \circ Bj = 1$, and the fiber of $B\det$ is $BU\langle 4\rangle = BSU$. In fact, if $i\colon BSU \longrightarrow BU$ is the inclusion then one sees easily that $i + j\colon BSU \times P \longrightarrow BU$ induces an isomorphism of homotopy groups, so it is an equivalence.

We have $HP^0P = \mathbb{Z}[\![x]\!]$ with $B\det^* x = c_1$ and $Bj^*c_1 = x$ and $Bj^*c_k = 0$ for $k > 1$. It follows (as is well-known) that the inclusion $BSU \longrightarrow BU$ gives an isomorphism $HP^0BSU = HP^0BU/c_1 = \mathbb{Z}[\![c_k \mid k > 1]\!]$.

In particular, both BU and BSU are even spaces.

The Hopf algebra HP_0BU is again a polynomial algebra, with generators b_k for $k > 0$. We also put $b_0 = 1$. The pairing between this ring and HP^0BU satisfies

$$\langle c_k, \prod_i b_i^{\alpha_i}\rangle = \begin{cases} 1 & \text{if } \prod_i b_i^{\alpha_i} = b_1^k \\ 0 & \text{otherwise.}\end{cases}$$

The group of primitives in HP_0BU is generated by elements r_k, which are characterized by the equation

$$t\,d\log(b(t))/dt = t\,b'(t)/b(t) = \sum_k r_k t^k.$$

4.2. **The isomorphism for $BU\langle 0\rangle$ and $BU\langle 2\rangle$.**

Proposition 4.1. *For $k = 0$ and $k = 1$ and for any even periodic ring spectrum E, the natural map*

$$BU\langle 2k\rangle^E \longrightarrow \underline{C}^k(P_E, \mathbb{G}_m)$$

is an isomorphism.

Proof. We treat the case $k = 1$, leaving the case $k = 0$ for the reader. A coordinate x on P_E gives isomorphisms

$$\begin{aligned} \mathcal{O}_{P_E} &= E^0P \cong E^0[\![x]\!] \\ \mathcal{O}^\vee_{P_E} &= \widetilde{E}_0P \cong E_0\{\beta_1, \beta_2, \dots\} \\ E_0(BU) &\cong E^0[b_1, b_2, \dots] \\ \mathcal{O}_{C^1(P_E,\mathbb{G}_m)} &\cong E^0[b'_1, b'_2, \dots]. \end{aligned}$$

Here the $\beta_i \in \widetilde{E}_0P$ are defined so $\langle x^i, \beta_j\rangle = \delta_{ij}$, and $b_i = (E_0\rho_1)(\beta_i)$, where $\rho_1\colon P \longrightarrow BU$ classifies the virtual bundle $1 - L$. The b'_i are defined by writing the universal element of $\underline{C}^1(P_E, \mathbb{G}_m)$ as $1 + \sum_{i\geq 1} b'_i x^i$.

By Definition 2.27, the map $BU^E \longrightarrow \underline{C}^1(P_E, \mathbb{G}_m)$ classifies the element $b \in E_0BU\widehat{\otimes}E^0P \cong E_0BU[\![x]\!]$ which is the adjoint of the map $E_0\rho_1$. It is easy to see that $b = \sum_i b_i x^i$. □

Recall that Cartier duality (2.2) gives an isomorphism

$$P^E \cong \underline{\mathrm{Hom}}(P_E, \mathbb{G}_m).$$

The construction $f \mapsto 1/f$ gives a map

$$\underline{\mathrm{Hom}}(P_E, \mathbb{G}_m) \xrightarrow{i} \underline{C}^1(P_E, \mathbb{G}_m).$$

Corollary 4.2. *The diagram*

$$\begin{tikzcd}
P^E \arrow[r, "(B\det)^E"] \arrow[d, "\cong"'] & BU^E \arrow[d, "\cong"] \\
\underline{\mathrm{Hom}}(P_E, \mathbb{G}_m) \arrow[r, "i"] & \underline{C}^1(P_E, \mathbb{G}_m)
\end{tikzcd}$$

commutes.

Proof. It will be enough to show that the dual diagram of rings commutes. As E_0BU is generated over E_0 by $(E_0\rho_1)(\widetilde{E}_0P)$, it suffices to check commutativity after composing with $E_0\rho_1$. It is then clear, because $B\det\circ\rho_1$ classifies $\det(1-L)\cong L^{-1}$, and so has degree -1. □

4.3. **The isomorphism for rational homology and all k.**

Proposition 4.3. *For any $k>0$ we have*

$$HP^0(BU\langle 2k\rangle;\mathbb{Q}) = HP^0(BU;\mathbb{Q})/(c_1,\dots,c_{k-1}) = \mathbb{Q}[\![c_n \mid n\geq k]\!].$$

We also have an isomorphism

$$BU\langle 2k\rangle^{HP\mathbb{Q}} \cong \underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)\times \mathrm{spec}(\mathbb{Q}).$$

Proof. We have fibrations $BU\langle 2k+2\rangle \longrightarrow BU\langle 2k\rangle \longrightarrow K(\mathbb{Z},2k)$. It is well-known that

$$H^*(K(\mathbb{Z},2k);\mathbb{Q}) = \mathbb{Q}[u_{2k}]$$

with $|u_{2k}|=2k$. We know that the map $BU\langle 2k\rangle \longrightarrow K(\mathbb{Z},2k)$ induces an isomorphism on $\pi_{2k}(-)$ and we may assume inductively that $H^*(BU\langle 2k\rangle;\mathbb{Q}) = \mathbb{Q}[\![c_n \mid n\geq k]\!]$, so the Hurewicz theorem tells us that u_{2k} hits a nontrivial multiple of c_k. It now follows from the Serre spectral sequence that

$$H^*(BU\langle 2k+2\rangle;\mathbb{Q}) = \mathbb{Q}[\![c_n \mid n\geq k+1]\!] = H^*(BU;\mathbb{Q})/(c_1,\dots,c_k).$$

Dually, we know that $H_*(BU;\mathbb{Q})$ is generated by primitive elements r_i such that r_i is dual to c_i, and we find that $H_*(BU\langle 2k\rangle;\mathbb{Q}) = \mathbb{Q}[r_i \mid i\geq k]$. These are precisely the functions on $C^1(\widehat{\mathbb{G}}_a,\mathbb{G}_m)$ that are unchanged when we replace $f\in C^1(\widehat{\mathbb{G}}_a,\mathbb{G}_m)(R)$ by $f\exp(g)$ for some polynomial g of degree less than k, as we see from the definition of the r_i. We see from the proof of Proposition 3.43 that these are the same as the functions that depend only on $\delta_\times^{k-1}(f)$, and thus that $BU\langle 2k\rangle^{HP\mathbb{Q}}$ can be identified with $\underline{C}^k(\widehat{\mathbb{G}}_a,\mathbb{G}_m)\times\mathrm{spec}(\mathbb{Q})$, as claimed. □

4.4. **The ordinary homology of BSU.**

Proposition 4.4. *The natural map*

$$BSU^{HP} \longrightarrow \underline{C}^2(\widehat{\mathbb{G}}_a,\mathbb{G}_m)$$

is an isomorphism.

Proof. It is enough to prove this modulo p for all primes p, so fix one. Consider the diagram of affine commutative group schemes (in which everything is taken implicitly over $\mathbb{F}_p$)

$$\begin{tikzcd}
P^{HP} \arrow[r] \arrow[d, "\cong"'] & BU^{HP} \arrow[r] \arrow[d, "\cong"'] & BSU^{HP} \arrow[d] \\
\underline{\mathrm{Hom}}(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r] & \underline{C}^1(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, "\delta_\times"] & \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m).
\end{tikzcd}$$

The diagram commutes by Corollaries 2.28 and 4.2. The splitting $BU = BSU \times P$ implies that the top row is a short exact sequence. It is clear that $\underline{\mathrm{Hom}}(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ is the kernel of $\delta_\times$, so it remains to show that $\delta_\times$ is an epimorphism. That is precisely the content of Proposition 3.42. □

4.5. **The ordinary homology of $BU\langle 6\rangle$.** The mod p cohomology of $BU\langle 2k\rangle$ was computed (for all $k \geq 0$) by Singer [Sin68]. We next recall the calculation for $k = 3$. Note that $BU\langle 6\rangle$ is the fiber of a map $BSU \to K(\mathbb{Z}, 4)$ and $\Omega K(\mathbb{Z}, 4) = K(\mathbb{Z}, 3)$ so we have a fibration

$$K(\mathbb{Z}, 3) \xrightarrow{\gamma} BU\langle 6\rangle \xrightarrow{v} BSU.$$

In this section we give an algebraic model for the ordinary homology of this fibration, in terms of the theory of symmetric cocycles and Weil pairings.

Classical calculations show that for $p > 2$ we have

$$H^*(K(\mathbb{Z}, 3); \mathbb{F}_p) = E[u_0, u_1, \ldots] \otimes \mathbb{F}_p[\beta u_1, \beta u_2, \ldots],$$

where $|u_k| = 2p^k + 1$ and $u_{k+1} = P^{p^k} u_k$ and $\beta u_0 = 0$. We write A^* for the polynomial subalgebra generated by the elements βu_k for $k > 0$. We also write $A = \prod_{k \geq 0} A^{2k}$, which is an ungraded formal power series algebra over $\mathbb{F}_p$. In the case $p = 2$ we have

$$H^*(K(\mathbb{Z}, 3); \mathbb{F}_2) = \mathbb{F}_2[u_0, u_1, \ldots],$$

with $|u_k| = 2^{k+1} + 1$ and $u_{k+1} = Sq^{2^{k+1}} u_k$, and we let A^* be the subalgebra generated by the elements u_k^2. We write $A^\vee_*$ for the vector space dual $\mathrm{Hom}(A^*, \mathbb{F}_p)$.

Lemma 4.5. *In the Serre spectral sequence*

$$H^*(BSU; H^*(K(\mathbb{Z}, 3); \mathbb{F}_p)) \Longrightarrow H^*(BU\langle 6\rangle; \mathbb{F}_p)$$

the class u_t survives to E_{2p^t+2}, and then there is a differential $d_{2p^t+2}(u_t) = q_{1+p^t}$, up to a unit in $\mathbb{F}_p$.

Proof. We treat the case $p > 2$ and leave the (small) modifications for $p = 2$ to the reader. As $BU\langle 6\rangle$ is 5-connected, we must have a transgressive differential $d_4(u_0) = c_2$ (up to a unit in $\mathbb{F}_p$). We can think of $H^*(BU; \mathbb{F}_p)$ as a ring of symmetric functions in the usual way, so we have $c_2 = \sum_{i<j} x_i x_j$. One checks by induction that

$$P^{p^{t-1}} \ldots P^p P^1(c_2) = \sum_{i \neq j} x_i x_j^{p^t} = q_1^{1+p^t} - q_{1+p^t}$$

for $t > 0$. We also have $q_1 = c_1$ (which vanishes on BSU) and thus $P^{p^{t-1}} \ldots P^p P^1(c_2) = -q_{1+p^t}$ in $H^*(BSU; \mathbb{F}_p)$. It follows from the Kudo transgression theorem and our knowledge of the action of the Steenrod algebra that u_t survives to E_{2p^t+2} and $d_{2p^t+2}(u_t) = q_{1+p^t}$. □

Proposition 4.6. *We have a short exact sequence of Hopf algebras*

$$H^*(BSU; \mathbb{F}_p)/(c_2, q_{1+p^t} \mid t > 0) \rightarrowtail H^*(BU\langle 6\rangle; \mathbb{F}_p) \twoheadrightarrow A^*.$$

Moreover, $H^*(BU\langle 6\rangle; \mathbb{F}_p)$ is a polynomial ring over $\mathbb{F}_p$, concentrated in even degrees, with the same Poincaré series as $\mathbb{F}_p[c_k \mid k \geq 3]$.

Proof. Note that $q_k = kc_k$ modulo decomposables, so we can take q_{1+p^t} as a generator of $H^{2(1+p^t)}(BSU)$ p-locally when $t > 0$. Thus

$$H^*(BSU;\mathbb{F}_p) = \mathbb{F}_p[q_{1+p^t} \mid t > 0] \otimes \mathbb{F}_p[c_k \mid k \geq 2 \text{ is not of the form } 1+p^t]$$

Using this, one can check that Lemma 4.5 gives all the differentials in the spectral sequence, and that

$$\begin{aligned} E_\infty &= H^*(BU;\mathbb{F}_p)/(c_2, q_{1+p^t} \mid t > 0) \otimes A^* \\ &= \mathbb{F}_p[c_k \mid k \geq 2 \text{ is not of the form } 1+p^t] \otimes \\ &\quad \mathbb{F}_p[\beta u_k \mid k > 0]. \end{aligned}$$

By thinking about the edge homomorphisms of the spectral sequence, we obtain the claimed short exact sequence of Hopf algebras. As the two outer terms are polynomial rings in even degrees, the same is true of the middle term. As $|\beta u_k| = |q_{1+p^k}|$, we have the claimed equality of Poincaré series. □

Corollary 4.7. *$BU\langle 6\rangle$ is a even space, and $H^*BU\langle 6\rangle$ is a polynomial algebra of finite type over $\mathbb{Z}$.*

Proof. It is easy to see that $BU\langle 6\rangle$ has finite type. The remaining statements are true p-locally for all p by the Proposition, and the integral statement follows because everything has finite type. □

Corollary 4.8. *The sequence of group schemes over $\mathbb{F}_p$*

$$BSU^{HP\mathbb{F}_p} \longrightarrow BU\langle 6\rangle^{HP\mathbb{F}_p} \longrightarrow \operatorname{spec}(A^\vee) \longrightarrow 0$$

is exact.

4.5.1. *The Weil scheme and $HP_0K(\mathbb{Z},3)$.* In this section, we work over $\mathbb{F}_p$ unless otherwise specified. In particular, homology is taken with coefficients in $\mathbb{F}_p$.

We now have the solid arrows of the diagram

$$\begin{tikzcd} BSU^{HP} \arrow[r] \arrow[d, "f_2"', "\cong"] & BU\langle 6\rangle^{HP} \arrow[r] \arrow[d, "f_3"'] & \operatorname{spec}(A^\vee) \arrow[r] \arrow[d, dashed, "\cong"', "\lambda"] & 0 \\ \underline{C}^2(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, "\delta_\times"] & \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \arrow[r, "e"] & \operatorname{Weil}(\widehat{\mathbb{G}}_a) \arrow[r] & 0. \end{tikzcd} \tag{4.9}$$

The diagram commutes by Corollary 2.28. Moreover the rows are exact (by Corollaries 3.41 and 4.8), and the map f_2 is an isomorphism by Proposition 4.4. It follows that there is a map λ making the diagram commute. Our next task is to show that this map is an isomorphism.

We can give an explicit formula for this map. Recall from §2.3.3 that f_3 classifies the 3-cocycle $\hat{\rho}_3 \in HP^0P\hat{\otimes}HP_0BU\langle 6\rangle$. Here $\hat{\rho}_3$ is the adjoint of $HP_0\rho_3$, where ρ_3 is the map

$$P^3 \xrightarrow{\rho_3} BU\langle 6\rangle$$

whose composite to BU classifies the bundle $\prod_i(1-L_i)$. Let $W\colon P^2 \to BU\langle 6\rangle$ be the map whose composite to BU classifies the virtual bundle

$$\sum_{k=1}^{p-1}\big((1-L_1)(1-L_1^k)(1-L_2) - (1-L_1)(1-L_2^k)(1-L_2)\big) \cong (1-L_1)(1-L_2)\sum_{k=1}^{p-1} L_2^k - L_1^k. \tag{4.10}$$

Let $\hat{W}$ be the adjoint in $HP^0P^2\hat{\otimes}HP_0BU\langle 6\rangle$ of the map HP_0W. Let $x = -c_1L_1$ and $y = -c_1L_2$ be the indicated generators of HP^0P^2. Then $\hat{W}$ gives a power series

$$\hat{W}(x,y) \in HP_0(BU\langle 6\rangle)[\![x,y]\!] \cong HP^0P^2\hat{\otimes}HP_0BU\langle 6\rangle.$$

Lemma 4.11. *The power series* $\hat{W}(x,y)$ *has coefficients in the subring* $A^\vee[\![x,y]\!]$. *As such it is an element of* $\mathrm{Weil}(\widehat{\mathbb{G}}_a)(A^\vee)$. *The map* $\lambda\colon \mathrm{spec}(A^\vee) \to \mathrm{Weil}(\widehat{\mathbb{G}}_a)$ *classifying* $\hat{W}(x,y)$ *makes the diagram* (4.9) *commute.*

Proof. Recall that the map $e\colon \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \to \mathrm{Weil}(\widehat{\mathbb{G}}_a)$ takes the power series $f(x,y,z)$ to the power series

$$e(f)(x,y) = \prod_{k=1}^{p-1} \frac{f(x,kx,y)}{f(x,ky,y)}.$$

Recall also that the H-space structure of $BU\langle 6\rangle$ corresponds on the algebraic side to the multiplication of power series and on the topological side to addition of line bundles. The H-space structure of P corresponds on the algebraic side to addition in the group $\widehat{\mathbb{G}}_a$ and on the topological side to the tensor product of line bundles.

Putting these observations together shows that

$$\hat{W} = e(\hat{\rho}_3).$$

The lemma follows from this equation and the structure of the solid diagram (4.9). □

Lemma 4.12. *For* $s \geq 1$, *we have an equation*

$$W^* q_{1+p^s} = p(xy^{p^s} - x^{p^s} y) \mod p^2$$

in the integral *cohomology* HP^0P^2.

Proof. As $x = -c_1L_1$ and $y = -c_1L_2$, the total Chern class of the bundle (4.10) is given by the formula

$$W^*c(t) = \frac{(1-yt)(1-pxt)(1-(x+py)t)}{(1-xt)(1-pyt)(1-(px+y)t)}.$$

We have $q(t) = td\log c(t)$. Modulo p^2 we have equations

$$\begin{aligned} td\log(1-xt) =& -tx(1+xt+(xt)^2+\dots) \\ td\log(1-pxt) =& -pxt \\ td\log(1-(x+py)t) =& \frac{(x+py)t}{(1-(x+py)t)} \\ =& -pyt(1+xt+(xt)^2+\dots) - xt(1+xt+(xt)^2+\dots) \\ & -pxyt^2(1+2xt+3(xt)^2+\dots). \end{aligned}$$

With these formulae it is easy to verify the assertion. □

Note that Lemma 4.11 implies that the map (of $\mathbb{F}_p$–modules)

$$HP_0W\colon HP_0P^2 \to HP_0BU\langle 6\rangle$$

factors through the inclusion of $A^\vee$ in $HP_0BU\langle 6\rangle$.

Proposition 4.13. *The map of group schemes* $\lambda\colon \mathrm{spec}(A^\vee) \to \mathrm{Weil}(\widehat{\mathbb{G}}_a)$ *is an isomorphism.*

Proof. First note that A is a formal power series algebra on primitive generators (because u_0 is primitive and the Steenrod action preserves primitives). It follows that $A^\vee$ is a divided power algebra over $\mathbb{F}_p$ and thus a tensor product of rings of the form $\mathbb{F}_p[y]/y^p$. We know from Lemma 3.36 that $\mathcal{O}_{\mathrm{Weil}(\widehat{\mathbb{G}}_a)}$ also has this structure. It will thus suffice to show that the map $\mathrm{Ind}(\mathcal{O}_{\mathrm{Weil}(\widehat{\mathbb{G}}_a)}) \to \mathrm{Ind}(A^\vee) = \mathrm{Prim}(A)^\vee$ is an isomorphism, or equivalently that the resulting pairing of $\mathrm{Ind}(\mathcal{O}_{\mathrm{Weil}(\widehat{\mathbb{G}}_a)})$ with $\mathrm{Prim}(A)$ is perfect.

Define elements $b_i \in H_*P$ by setting $\langle b_i, x^j\rangle = \delta_{ij}$, and define elements $b_{ij} \in A^\vee$ by setting

$$b_{ij} = H_*W(b_i \otimes b_j).$$

It is clear that the Weil pairing $g(x,y)$ associated to HP_0W is given by the formula

$$g(x,y) = \sum_{ij} b_{ij} x^i y^j.$$

Let $f(x,y) = \sum_{i,j} a_{ij} x^i y^j$ be the universal Weil pairing defined over $\mathcal{O}_{\mathrm{Weil}(\widehat{\mathbb{G}}_a)}$, so our map sends f to g and thus a_{ij} to b_{ij}. We know from Lemma 3.36 that the elements a_{p^i,p^j} (with $i<j$) form a basis for $\mathrm{Ind}(\mathcal{O}_{\mathrm{Weil}(\widehat{\mathbb{G}}_a)})$. On the other hand, the elements $(\beta u_k)^{p^m}$ (with $k>0$ and $m \geq 0$) are easily seen to form a basis for $\mathrm{Prim}(A)$.

The calculation of the Serre spectral sequence in Lemma 4.5 and the characteristic class calculation in Lemma 4.12 together imply that

$$W^* \beta u_k = \epsilon (x y^{p^k} - x^{p^k} y)$$

in $H^*(P^2)$, where ϵ is a unit in $\mathbb{F}_p$. It follows that the inner product $\langle b_{p^i,p^j}, (\beta u_k)^{p^m} \rangle$ in A is the same (up to a unit) as the inner product $\langle b_{p^i,p^j}, x^{p^m} y^{p^{k+m}} - x^{p^{k+m}} y^{p^m} \rangle$ in $H^*(P^2)$, and this inner product is just $\delta_{im}\delta_{jk}$. This proves that the pairing is perfect, as required. □

Corollary 4.14. *For periodic* integral *homology, the map* $BU\langle 6\rangle^{HP} \to \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)$ *is an isomorphism.*

Proof. It is enough to prove this mod p for all p. We can chase the diagram 4.9 to see that the map $BU\langle 6\rangle^{HP\mathbb{F}_p} \to \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \mathrm{spec}(\mathbb{F}_p)$ is an epimorphism. We see from Propositions 4.3 and 3.28 that the corresponding graded rings have the same Poincaré series, so the map must actually be an isomorphism. □

4.6. *BSU* and *BU*⟨6⟩ for general *E*.

Let FGL be the scheme of formal group laws and let $G = \widehat{\mathbb{A}}^1 \times FGL$. There is a canonical group structure $\sigma\colon G \times_{FGL} G = \widehat{\mathbb{A}}^2 \times FGL \to \widehat{\mathbb{A}}^1 \times FGL = G$ given by the formula $\sigma(a,b,F) = (a +_F b, F)$. We define an action of $\mathbb{G}_m$ on FGL by $(u.F)(x,y) = u^{-1}F(ux,uy)$. This gives a grading on $\mathcal{O}_{FGL}$; explicitly, if $F(x,y) = \sum_{i,j} a_{ij} x^i y^j$ is the universal formal group law, then a_{ij} is a homogeneous element of $\mathcal{O}_{FGL}$ of degree $i+j-1$. It is clear that $\mathcal{O}_{FGL}$ is generated (subject to many relations) by the elements a_{ij}. It is a theorem of Lazard (see [Ada74] for example) that $\mathcal{O}_{FGL}$ is a graded polynomial algebra with one generator in each degree $i > 0$.

The scheme $C = \underline{C}^3(G, \mathbb{G}_m)$ is the functor that assigns to each ring R the set of pairs (F,f), where F is a formal group law over R and $f \in R[\![x_1,x_2,x_3]\!]$ is symmetric, congruent to 1 modulo $x_1x_2x_3$, and satisfies the cocycle condition

$$f(x_1,x_2,x_3) f(x_0 +_F x_1, x_2, x_3)^{-1} f(x_0, x_1 +_F x_2, x_3) f(x_0,x_1,x_3)^{-1} = 1.$$

The action of $\mathbb{G}_m$ on FGL extends to an action on C by the formula $u.(F,f) = (u.F, u.f)$, where

$$(u.f)(x_1,x_2,x_3) = f(ux_1,ux_2,ux_3)$$

and

$$(u.F)(x,y) = u^{-1}F(ux,uy).$$

This gives $\mathcal{O}_C$ the structure of a graded $\mathcal{O}_{FGL}$-algebra. If $f(x_1,x_2,x_3) = \sum_{i,j,k\geq 0} b_{ijk} x_1^i x_2^j x_3^k$ then b_{ijk} can be thought of as a homogeneous element of $\mathcal{O}_C$ with degree $i+j+k$. Moreover, we have $b_{000} = 1$.

It is clear that $\mathcal{O}_C$ is generated over $\mathcal{O}_{FGL}$ by the elements b_{ijk}, and thus that $\mathcal{O}_C$ is a connected graded ring of finite type over $\mathbb{Z}$.

Lemma 4.15. *The ring* $\mathcal{O}_C$ *is a graded free module over* $\mathcal{O}_{FGL}$*. In particular, it is free of finite type over* $\mathbb{Z}$*.*

Proof. Let I be the ideal in $\mathcal{O}_C$ generated by the elements of positive degree in $\mathcal{O}_{\mathrm{FGL}}$, so the associated closed subscheme $V(I) \cong \operatorname{spec}(\mathbb{Z}) \subset \mathrm{FGL}$ just consists of the additive formal group law. It follows that $\mathcal{O}_C/I = \mathcal{O}_{\underline{C}^3(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$, which is a free abelian group by Corollary 3.30. We choose a homogeneous basis for $\mathcal{O}_C/I$ and lift the elements to get a system of homogeneous elements in $\mathcal{O}_C$. Using these, we can construct a graded free module M over $\mathcal{O}_{\mathrm{FGL}}$ and a map $M \xrightarrow{\alpha} \mathcal{O}_C$ of $\mathcal{O}_{\mathrm{FGL}}$-modules that induces an isomorphism $M/IM \cong \mathcal{O}_C/I\mathcal{O}_C$. It is easy to check by induction on the degrees that α is surjective. Also, M is free over $\mathcal{O}_{\mathrm{FGL}}$, which is free over $\mathbb{Z}$, so M is free over $\mathbb{Z}$. Now, if we have a surjective map $f\colon A \longrightarrow B$ of finitely generated Abelian groups such that A is free and $A \otimes \mathbb{Q} \cong B \otimes \mathbb{Q}$, it is easy to see that f is an isomorphism. Thus, if we can show that M has the same rational Poincaré series as $\mathcal{O}_C$, we can deduce that α is an isomorphism.

If (F, f) is a point of C over a rational ring R, then we can define a series $\exp_F$ in the usual way and get a series $g = f \circ (\exp_F^3)$ defined by $g(x_1, x_2, x_3) = f(\exp_F(x_1), \exp_F(x_2), \exp_F(x_3))$. Clearly we have $g \in \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m)(R)$, and this construction gives an isomorphism $C \times \operatorname{spec}(\mathbb{Q}) \longrightarrow \mathrm{FGL} \times \underline{C}^3(\widehat{\mathbb{G}}_a, \mathbb{G}_m) \times \operatorname{spec}(\mathbb{Q})$. It follows that the Poincaré series of $\mathcal{O}_C$ is the same as that of $\mathcal{O}_{\mathrm{FGL}} \otimes \mathcal{O}_{\underline{C}^3(\widehat{\mathbb{G}}_a,\mathbb{G}_m)}$, which is the same as that of M by construction. □

Proposition 4.16. *For any even periodic ring spectrum E, the natural maps*

$$BSU^E \longrightarrow \underline{C}^2(P_E, \mathbb{G}_m)$$

and

$$BU\langle 6\rangle^E \longrightarrow \underline{C}^3(P_E, \mathbb{G}_m)$$

are isomorphisms.

Proof. Let $k = 2$ or 3. Because $BU\langle 2k\rangle$ is even, we know that the Atiyah-Hirzebruch spectral sequence

$$H_*(BU\langle 2k\rangle; E_*) \Longrightarrow E_*BU\langle 2k\rangle$$

collapses, and thus that $E_1BU\langle 2k\rangle = 0$ and $E_0BU\langle 2k\rangle$ is a free module over E_0. If we have a ring map $E' \longrightarrow E$ between even periodic ring spectra then we get a map $E_0 \otimes_{E'_0} E'_0BU\langle 2k\rangle \longrightarrow E_0BU\langle 2k\rangle$, and a comparison of Atiyah-Hirzebruch spectral sequences shows that this is an isomorphism, so $BU\langle 2k\rangle^E = BU\langle 2k\rangle^{E'} \times_{S_{E'}} S_E$. On the other hand, because the formation of $\underline{C}^k$ commutes with base change, we have

$$\underline{C}^k(P_E, \mathbb{G}_m) = \underline{C}^k(P_{E'} \times_{S_{E'}} S_E, \mathbb{G}_m) = \underline{C}^k(P_{E'}, \mathbb{G}_m) \times_{S_{E'}} S_E.$$

It follows that if the theorem holds for E' then it holds for E. It holds for $E = HP$ by Proposition 4.4 or Corollary 4.14, and we have ring maps

$$HP \longrightarrow HP\mathbb{Q} \longrightarrow HP\mathbb{Q} \wedge MU = MP\mathbb{Q},$$

so the theorem holds for $MP\mathbb{Q}$.

For any E, we can choose a coordinate on E and thus a map $MP \longrightarrow E$ of even periodic ring spectra, so it suffices to prove the theorem when $E = MP$, in which case $S_E = \mathrm{FGL}$. In this case we have a map of graded rings $\mathcal{O}_C \longrightarrow MP_0BU\langle 2k\rangle = MU_*BU\langle 2k\rangle$, both of which are free of finite type over $\mathbb{Z}$. This map is a rational isomorphism by the previous paragraph, so it must be injective, and the source and target must have the same Poincaré series. It will thus suffice to prove that it is surjective. Recall that I denotes the kernel of the map $MP_0 \longrightarrow \mathbb{Z} = HP_0$ that classifies the additive formal group law, or equivalently the ideal generated by elements of strictly positive dimension in MU_*. By induction on degrees, it will suffice to prove that the map $\mathcal{O}_C/I \longrightarrow MP_0BU\langle 2k\rangle/I$ is surjective. Base change and the Atiyah-Hirzebruch sequence identifies this map with the map $\mathcal{O}_{\underline{C}^3(\widehat{\mathbb{G}}_a,\mathbb{G}_m)} \longrightarrow HP_0BU\langle 2k\rangle$, in other words the case $E = HP$ of the proposition. This case was proved in Proposition 4.4 ($k = 2$) or Corollary 4.14 ($k = 3$). □

Appendix A. Additive cocycles

The main results of this section are proofs of Propositions 3.13, 3.16, and 3.20. We use the notation of §3. In particular, we abbreviate $C^k(A)$ for $\underline{C}^k(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)$, and for $d \geq 1$ we write $C^k_d(A)$ for the subgroup of polynomials which are homogeneous of degree d.

For $d \geq 1$ let x^d be considered as an element of $C^0(\widehat{\mathbb{G}}_a, \widehat{\mathbb{G}}_a)(\mathbb{Z})$. Then we have polynomials $\delta^k(x_d) \in \mathbb{Z}[x_1, \dots, x_k]$ giving elements of $C^k(\mathbb{Z})$. For example

$$\begin{aligned}\delta^2(x_d) &= x_1^d + x_2^d - (x_1 + x_2)^d \\ \delta^3(x_d) &= x_1^d + x_2^d + x_3^d - (x_1 + x_2)^d - (x_1 + x_2)^d - (x_2 + x_3)^d + (x_1 + x_2 + x_3)^d.\end{aligned}$$

A.1. **Rational additive cocycles.**

Proposition A.1 (3.13)**.** *If A is a $\mathbb{Q}$-algebra, then for $d \geq k$ the group $C^k_d(A)$ is the free abelian group on the single generator $\delta^k x^d$.*

Proof. If $h \in C^k(A)$ then there is a unique series $f(x)$ such that $h(x, \epsilon, \dots, \epsilon) = \epsilon^{k-1} f(x) \pmod{\epsilon^k}$, and moreover $f(0) = 0$. It follows that there is a unique series $g \in C^0_{\geq k}(A)$ whose $(k-1)$'st derivative is f. We can thus define an A-linear map $\pi\colon C^k(A) \to C^0_{\geq k}(A)$ by $\pi(h) = (-1)^k g$. We claim that this is the inverse of δ^k.

To see this, suppose that $g \in C^0_{\geq k}(A)$, so that $g^{(k-1)}(0) = 0$. From the definitions, we have

$$\begin{aligned}(\delta^k g)(x, \epsilon, \dots, \epsilon) &= \sum_I (-1)^{|I|} (g(|I|\epsilon) - g(x + |I|\epsilon)) \\ &= \sum_{j=0}^{k-1} (-1)^j \begin{pmatrix} k-1 \\ j \end{pmatrix} (g(j\epsilon) - g(x + j\epsilon)),\end{aligned}$$

where I runs over subsets of $\{2, \dots, k\}$. To understand this, we introduce the operators $(Tf)(x) = f(x + \epsilon)$ and $(Df)(x) = f'(x)$. Taylor's theorem tells us that $T = \exp(\epsilon D)$. It is clear that

$$\begin{aligned}\sum_{j=0}^{k-1} (-1)^j \begin{pmatrix} k-1 \\ j \end{pmatrix} g(x + j\epsilon) &= ((1 - T)^{k-1} g)(x) \\ &= ((1 - \exp(\epsilon D))^{k-1} g)(x) \\ &= (-\epsilon)^{k-1} g^{(k-1)}(x) \pmod{\epsilon^k}.\end{aligned}$$

If we feed this twice into our earlier expression and use the fact that $g^{(k-1)}(0) = 0$, we find that

$$(\delta^k g)(x, \epsilon, \dots, \epsilon) = (-1)^k \epsilon^{k-1} g^{(k-1)}(x) \pmod{\epsilon^k}.$$

This shows that $\pi \delta^k = 1$.

To complete the proof, it suffices to show that π is injective. Suppose that $h \in C^k(A)$ and that $\pi(h) = 0$, so that $h(x, \epsilon, \dots, \epsilon) = 0 \pmod{\epsilon^k}$. If $k = 2$ we consider the cocycle condition

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

If we substitute $z = \epsilon$ and work modulo ϵ^2 then the first two terms become zero and we have $h(x, y + \epsilon) = h(x, y)$, or equivalently $\partial h(x, y)/\partial y = 0$. By symmetry we also have $\partial h(x, y)/\partial x = 0$, and as A is rational we can integrate so h is constant. We also know that $h(0, 0) = 0$ so $h = 0$ as required.

Now suppose that $k > 2$. We know that h has the form $g(x_1, \dots, x_k) x_k$ for some series g. By assumption, ϵ^k divides $h(x, \epsilon, \dots, \epsilon) = \epsilon g(x, \epsilon, \dots, \epsilon)$ so $g(x, \epsilon, \dots, \epsilon) = 0 \pmod{\epsilon^{k-1}}$. On the other hand, $x_2, \dots, x_{k-1}$ also divide g so it is not hard to see that $g(x, \epsilon, \dots, \epsilon, 0) = g(x, \epsilon, \dots, \epsilon) = 0 \pmod{\epsilon^{k-1}}$. Moreover, the series $g(x_1, \dots, x_{k-1}, 0)$ lies in $C^{k-1}(A)$, so by induction on k we find that $g(x_1, \dots, x_{k-1}, 0) = 0$. This shows that $h(x_1, \dots, x_{k-1}, \epsilon) = 0 \pmod{\epsilon^2}$. The argument of the $k = 2$ case now shows that $h = 0$. □

A.2. **Divisibility.** Recall that u_d is the greatest common divisor of the coefficients of the polynomial $\delta^k x^d$. Let

$$\mathbf{c}(k,d) = \frac{\delta^k x^d}{u_d}.$$

It is clear that $C^k(\mathbb{Z}) = C^k(\mathbb{Q}) \cap \mathbb{Z}[\![x_1, \dots, x_k]\!]$, so Proposition A.1 has the following corollary.

Corollary A.2. *For $d \geq k$, the group $C^k_d(\mathbb{Z})$ is a free abelian group on the single generator $\mathbf{c}(k,d)$* □

We fix a prime p and an integer $k \geq 1$. In §3 it is convenient work p-locally, and then to use the cocycles

$$c(d) = \frac{(-\delta)^k(x^d)}{p^{v(d)}},$$

which locally at p are unit multiples of $\mathbf{c}(k,d)$ (see Definition 3.14). In this section we study $v(d) = \nu_p(u(d))$.

It is clear that $u(d)$ is the greatest common divisor of the multinomial coefficients

$$\frac{d}{a_1! \cdot \dots \cdot a_k!},$$

where $a_i \geq 1$ and $\sum a_i = d$.

We start with some auxiliary definitions.

Definition A.3. For any nonnegative integer d, we write $\sigma_p(d)$ for the sum of the digits in the base p expansion of d. In more detail, there is a unique sequence of integers d_i with $0 \leq d_i < p$ and $\sum_i d_i p^i = d$, and we write $\sigma_p(d) = \sum_i d_i$. Given a sequence $\alpha = (\alpha_1, \dots, \alpha_k)$ of nonnegative integers, we write

$$\begin{aligned} |\alpha| &= \sum_i \alpha_i \\ x^\alpha &= \prod_i x_i^{\alpha_i} \\ \alpha! &= \prod_i \alpha_i! \\ \operatorname{supp}(\alpha) &= \{i \mid \alpha_i > 0\}. \end{aligned}$$

Lemma A.4. *We have*

$$v(d) = \inf\{\nu_p(d!/\alpha!) \mid |\alpha| = d \textit{ and } \alpha_i > 0 \textit{ for all } i\}. \quad \square$$

To exploit this, we need some well-known formulae involving multinomial coefficients.

Lemma A.5. *We have $v_p(n!) = (n - \sigma_p(n))/(p-1)$.*

Proof. The number of integers in $\{1, \dots, n\}$ that are divisible by p is $\lfloor n/p \rfloor$. Of these, precisely $\lfloor n/p^2 \rfloor$ are divisible by a further power of p, and so on. This leads easily to the formula $v_p(n!) = \sum_k \lfloor n/p^k \rfloor$. If n has expansion $\sum_i n_i p^i$ in base p, then $\lfloor n/p^k \rfloor = \sum_{i \geq k} n_i p^{i-k}$. A little manipulation gives $v_p(n!) = \sum_i n_i(p^i - 1)/(p-1) = (n - \sigma_p(n))/(p-1)$ as claimed. □

Corollary A.6. *For any multi-index α we have*

$$v_p(|\alpha|!/\alpha!) = \left(\sum_i \sigma_p(\alpha_i) - \sigma_p(|\alpha|) \right) / (p-1).$$

Thus

$$v(d) = \inf \left\{ \frac{\sum_i \sigma_p(\alpha_i) - \sigma_p(d)}{p-1} \;\middle|\; |\alpha| = d \textit{ and } \alpha_i > 0 \textit{ for all } i \right\}. \quad \square$$

It is not hard to check the following description of the minimum in Corollary A.6.

Lemma A.7. *The minimum in Corollary A.6 is achieved by the multi-index α such that summing*

$$d = \alpha_1 + \cdots + \alpha_k$$

in base p involves "carrying" the fewest number of times; and $v(d)$ is equal to the number of carries. □

The proof of Proposition 3.16 involves working out this number of carries. To make the argument precise, we introduce a few definitions.

Definition A.8. We let $A(p, k, d)$ denote the set of doubly indexed sequences $\alpha = (\alpha_{ij})$, where i runs from 1 to k, j runs over all nonnegative integers, and the following conditions are satisfied:

i. For each i, j we have $0 \leq \alpha_{ij} \leq p - 1$.
ii. We have $\sum_{i,j} \alpha_{ij} p^j = d$.
iii. For each i there exists j such that $\alpha_{ij} > 0$.

By writing multi-indices in base p, we see that $v(d)$ is the minimum value of $(\sum_{ij} \alpha_{ij} - \sigma_p(d))/(p-1)$ as α runs over $A(p, k, d)$.

Definition A.9. We let $B = B(p, k, d)$ be the set of sequences $\beta = (\beta_j)$ (where j runs over nonnegative integers) such that

i. For each j we have $0 \leq \beta_j \leq k(p-1)$.
ii. We have $\sum_j \beta_j p^j = d$.
iii. We have $\sum_j \beta_j \geq k$.

We also write $\widetilde{B} = \widetilde{B}(p, k, d)$ for the larger set of sequences satisfying only conditions i and ii. Given $\beta \in \widetilde{B}$ we write $\tau(\beta) = \sum_j \beta_j$, so $\beta \in B$ if and only if $\tau(\beta) \geq k$. If d has expansion $d = \sum_k \tilde{\beta}_k p^k$ in base p, then $\tilde{\beta} = (\tilde{\beta}_0, \tilde{\beta}_1, \dots)$ is an element of $\widetilde{B}$, with $\tau(\tilde{\beta}) = \sigma_p(d)$.

Proposition A.10 (3.16)**.** *For any $d \geq k$ we have*

$$v(d) = \max\left(0, \left\lceil \frac{k - \sigma_p(d)}{p-1} \right\rceil\right).$$

Alternatively, $v(d)$ is equal to the minimum number of "carries" in base-p arithmetic, when d is calculated as the sum of k integers $a_1, \dots, a_k$ with $a_i \geq 1$.

Proof. Consider the map $\rho\colon A(p, k, d) \longrightarrow B(p, k, d)$ defined by $\rho(\alpha)_j = \sum_i \alpha_{ij}$. It is easily seen that ρ is surjective and that $\tau\rho(\alpha) = \sum_{ij} \alpha_{ij}$. It follows that $v(p, k, d) = \inf\{(\tau(\beta) - \sigma_p(d))/(p-1) \mid \beta \in B\}$. If $k \leq \sigma_p(d) = \tau(\tilde{\beta})$ then $\tilde{\beta} \in B$ and this makes it clear that $v(d) = 0$. From now on we assume that $k > \sigma_p(d)$.

We define a map $\theta\colon \widetilde{B} \setminus B \longrightarrow \widetilde{B}$ as follows. If $\beta \in \widetilde{B} \setminus B$ then $\sum_j \beta_j < k$ and $\sum_j \beta_j p^j = d$. As $d \geq k$ this clearly cannot happen unless there exists some $i > 0$ with $\beta_i > 0$. We let j denote the largest such i. We then define

$$\theta(\beta)_i = \begin{cases} i = j & \beta_j - 1 \\ i = j-1 & \beta_{j-1} + p \\ i \neq j-1, j & \beta_i. \end{cases}$$

We claim that the resulting sequence lies in $\widetilde{B}$. The only way this could fail would be if $\beta_{j-1} + p > k(p-1)$, but as $\beta_j > 0$ this would imply

$$\tau(\beta) \geq \beta_j + \beta_{j-1} \geq 1 + (k-1)(p-1) \geq k,$$

contradicting the assumption that $\beta \notin B$.

Note that $\tau\theta(\beta) = \tau(\beta) + (p-1)$. It follows that for some i, the sequence $\beta = \theta^i(\tilde{\beta})$ is defined, lies in B, and satisfies $k \leq \tau(\beta) = \sigma_p(d) + i(p-1) < k + p - 1$. It follows that

$$i = \frac{\tau(\beta) - \sigma_p(d)}{p-1} = \left\lceil \frac{k - \sigma_p(d)}{p-1} \right\rceil,$$

and thus that $v(d) \leq \lceil (k - \sigma_p(d))/(p-1) \rceil$. By definition we have $\tau(\gamma) \geq k$ for all $\gamma \in B$, and this implies the reverse inequality. Thus $v(d) = \lceil (k - \sigma_p(d))/(p-1) \rceil$. □

A.3. **Additive cocycles: The modular case.** In this section we give the description of $C^3(A)$ when A is an $\mathbb{F}_p$-algebra, as promised in Proposition 3.20. For convenience, we recall what we need to prove.

Let ϕ be the endomorphism of $A[\![x_1, \dots, x_k]\!]$ defined by $\phi(x_i) = x_i^p$, and we observed that if $p = 0$ in A then this sends $C^k(A)$ to $C^k(A)$ and $C^k_d(A)$ to $C^k_{dp}(A)$. Moreover, if $A = \mathbb{F}_p$ then $a^p = a$ for all $a \in \mathbb{F}_p$ and thus $\phi(h) = h^p$.

Definition A.11. We say that an integer $d \geq 3$ has *type*

I if d is of the form $1 + p^t$ with $t > 0$.
II if d is of the form $p^s(1 + p^t)$ with $s, t > 0$.
III otherwise.

If $d = p^s(1+p^t)$ has type I or II we define $c'(d) = \phi^s c(1 + p^t) \in C^3_d(\mathbb{F}_p)$. Note that d has type I precisely when $\sigma_p(d-1) = 1$, and in that case we have $c'(d) = c(d)$.

Proposition A.12 (3.20)**.** *If A is an $\mathbb{F}_p$-algebra then $C^3(A)$ is a free module over A generated by the elements $c(d)$ for $d \geq 3$ and the elements $c'(d)$ for d of type II.*

The proof will be given at the end of this section. It is based on the observation that a cocycle $h = h(x, y, z) \in C^3_d(A)$ can be written uniquely in the form $\sum_i h_i(x, y) z^i$. Each h_i must be a two-cocycle, and so a multiple of $c_2(d - i)$. The symmetry of h restricts how the h_i can occur.

It is convenient to have the following description of the image of ϕ.

Lemma A.13. *If $p = 0$ in A and $h \in C^k(A)$ and $h(x_1, \dots, x_{k-1}, \epsilon) = 0 \pmod{\epsilon^2}$ then $h = \phi(g)$ for some $g \in C^k(A)$. Moreover, if h is homogeneous of degree d, then g is homogeneous of degree d/p, which means that $h = 0$ if p does not divide d.*

Proof. The cocycle condition gives

$$h(x_1, \dots, x_k) - h(x_1, \dots, x_{k-1}, x_k + \epsilon) + h(x_1, \dots, x_{k-1} + x_k, \epsilon) - h(x_1, \dots, x_{k-2}, x_k, \epsilon) = 0.$$

Modulo ϵ^2, the last two terms vanish and we conclude that $\partial h/\partial x_k = 0$. This shows that powers x_k^j can only occur in h if p divides j, or in other words that h is a function of x_k^p. By symmetry it is a function of x_i^p for all i, or in other words it has the form $\phi(g)$ for some g. It is easy to check that g lies again in $C^k(A)$. The extra statements for when h is homogeneous are clear. □

Definition A.14. Given an integer $d \geq 3$ and a prime p, we let $\tau = \tau(d)$ be the unique integer such that $p^\tau + 1 < d \leq p^{\tau+1} + 1$.

Definition A.15. We define a map $\pi \colon C^3_d(A) \longrightarrow A$ as follows. Given a cocycle $h \in C^3_d(A)$, write

$$h(x, y, z) = \sum_{i=0}^{d} h_i(x, y) z^i.$$

Then we can write $h(x, y, z)$ uniquely in the form $\sum_{i=0}^d h_i(x, y) z^i$. It is easy to check that h_i is a two-cocycle, and so Lemma 3.5 implies that $h_i = a_i c_2(d - i)$ for a unique element $a_i \in A$. Set $\pi(h) = a_{p^{\tau(d)}}$.

Lemma A.16. *There is a unit $\lambda \in {\mathbb{F}_p}^{\times}$ such that $\pi(ac(d)) = \lambda a$, so π is always surjective. If d is not divisible by p then $\pi\colon C^3_d(A) \longrightarrow A$ is an isomorphism. If d is divisible by p then the kernel of π is contained in the image of the map $\phi\colon C^3_{d/p}(A) \longrightarrow C^3_d(A)$.*

Proof. For the first claim we need only check that when $A = \mathbb{F}_p$, the element $\lambda = \pi(c(d))$ is nonzero. Equivalently, we claim that some term $x^i y^j z^{p^\tau}$ (with $i + j + p^\tau = d$) occurs nontrivially in $c(d)$. Given Corollary A.6 and Proposition 3.16, it is enough to show that there exist integers $i, j > 0$ with $i + j + p^\tau = d$ and

$$\frac{\sigma_p(i) + \sigma_p(j) + 1 - \sigma_p(d)}{p-1} = \max\left(\left\lceil \frac{3 - \sigma_p(d)}{p-1} \right\rceil, 0\right).$$

If $\sigma_p(d) \geq 3$ then this reduces to the requirement that $\sigma_p(i) + \sigma_p(j) = \sigma_p(d) - 1$. We cannot have $d = p^{\tau+1}$ or $d = p^{\tau+1} + 1$ because in those cases $\sigma_p(d) < 3$, so we must have $p^\tau + 1 < d < p^{\tau+1}$. It follows that in the base-p expansion $d = \sum_{i=0}^{\tau} d_i p^i$ we have $d_\tau > 0$, and thus that $\sigma_p(d - p^\tau) = \sigma_p(d) - 1 \geq 2$. It is now easy to find numbers $i, j > 0$ such that $i + j = d - p^\tau$ and the sum can be computed in base p without carrying, which implies that $\sigma_p(i) + \sigma_p(j) = \sigma_p(d - p^\tau)$ as required.

We now suppose that $\sigma_p(d) \leq 2$. In this case, we need to find $i, j > 0$ such that $i + j + p^\tau = d$ and

$$3 - \sigma_p(d) \leq \sigma_p(i) + \sigma_p(j) + 1 - \sigma_p(d) < 3 - \sigma_p(d) + p - 1,$$

or equivalently

$$2 \leq \sigma_p(i) + \sigma_p(j) < p + 1.$$

Assuming that $p > 2$, the possible values of d, together with appropriate values of i and j, are as follows.

$$\begin{array}{ll} d = p^{\tau+1} & i = j = \frac{1}{2}(p-1)p^\tau \\ d = 1 + p^{\tau+1} & i = 1\ ,\ j = (p-1)p^\tau \\ d = p^s + p^\tau\ \ (0 < s \leq \tau) & i = p^{s-1}\ ,\ j = (p-1)p^{s-1} \end{array}$$

In the case $p = 2$, the possibilities are as follows.

$$\begin{array}{ll} d = 2^{\tau+1}\ \ (\tau > 0) & i = j = 2^{\tau-1} \\ d = 1 + 2^{\tau+1} & i = 1\ ,\ j = 2^\tau \\ d = 2^s + 2^\tau\ \ (0 < s < \tau) & i = j = 2^{s-1} \end{array}$$

This completes the proof that $\lambda = \pi(c(d))$ is nonzero. For general A we have $\pi(ac(d)) = \lambda a$, and it follows immediately that π is surjective.

We next show that the kernel of π is contained in the image of ϕ (and thus is zero if p does not divide d). Suppose that $h \in C^3_d(A)$ and $\pi(h) = 0$. Let a_i be as in Definition A.15, so that $a_{p^\tau} = \pi(h) = 0$. By Lemma A.13, it suffices to check that h is divisible by x^2. We already know that it is divisible by x, so we just need to know that $a_1 = 0$. Let $\lambda_{i,j} \in \mathbb{F}_p$ be the coefficient of $x^i y^j$ in $c_2(()i + j)$, so we have

$$h = \sum_{i+j+k=d} \lambda_{i,j} a_k x^i y^j z^k.$$

As h is symmetric in x, y, and z, we conclude that $\lambda_{i,j} a_k = \lambda_{i,k} a_j$. In particular, we have

$$a_1 \lambda_{p^\tau, d-p^\tau-1} = a_{p^\tau} \lambda_{1, d-p^\tau-1} = 0.$$

It is thus enough to check that $\lambda_{p^\tau, d-p^\tau-1}$ is a unit in $\mathbb{F}_p$. In the case $d = p^{\tau+1} + 1$ we have $c(2, p, p^{\tau+1}) = ((x+y)^{p^{\tau+1}} - x^{p^{\tau+1}} - y^{p^{\tau+1}})/p$ and thus $\lambda_{p^\tau, d-p^\tau-1} = \binom{p^{\tau+1}}{p^\tau}/p$. Corollary A.6 tells us that this integer has p-adic valuation 0, so it becomes a unit in $\mathbb{F}_p$. In the case when $d < p^{\tau+1} + 1$, we have $c(p, 2, d-1) = (x+y)^{d-1} - x^{d-1} - y^{d-1}$ and thus $\lambda_{p^\tau, d-1-p^\tau} = \binom{d-1}{p^\tau}$.

It is not hard to see that we have a base-p expansion $d-1=\sum_{i=0}^{\tau} d_i p^i$ in which $d_\tau > 0$. Given this, Corollary A.6 again tells us that $\lambda_{p^\tau, d-1-p^\tau}$ is a unit, as required. □

Lemma A.17. *If d has type II then $\pi(c'(d))=0$.*

Proof. We have $d=p^s(1+p^t)$ with $s>0$ and $1+p^t\geq 3$. As $s>0$ we have $1+p^{s+t}<p^s+p^{s+t}\leq 1+p^{s+t+1}$, so $\tau(p^s+p^{s+t})=s+t$. We thus have to prove that there are no terms of the form $x^iy^jz^{p^{s+t}}$ in $c(1+p^t)^{p^s}$, or equivalently that there are no terms of the form $x^iy^jz^{p^t}$ in $c(1+p^t)$. This is clear because $c(1+p^t)$ has the form $xyz\,f(x,y,z)$, where f is homogeneous of degree p^t-2. □

Proof of Proposition A.12. It is clear from Lemma A.16 that $C^3(A)$ is generated over A by the elements $\phi^s c(d)$ for all s and d. However, Proposition 3.18 and Corollary 3.17 tell us that $\phi^s c(d) = c(p^s d)$ unless $\nu_p(d) < v(d)$, where

$$v(d)=\begin{cases} 2 & \sigma_2(d)=1 \text{ and } p=2 \\ 1 & \sigma_p(d)=1 \text{ and } p>2 \\ 1 & \sigma_p(d)=2 \\ 0 & \sigma_p(d)>2. \end{cases}$$

Suppose that d is one of these exceptional cases. We clearly cannot have $\sigma_p(d)>2$. If $\sigma_p(d)=1$ then $d=p^t$ for some t. The inequality $\nu_p(d)<v(d)$ means that $t<2$ if $p=2$ and $t<1$ if $p>2$. We also must have $d\geq 3$, so $t>0$, and $t>1$ if $p=2$. These requirements are inconsistent, so we cannot have $\sigma_p(d)=1$. This only leaves the possibility $\sigma_p(d)=2$, so $d=p^r(1+p^t)$ with $t\geq 0$, and $t>0$ if $p=2$. The inequality $\nu_p(d)<v(d)$ now means that $r=0$. The inequality $d\geq 3$ means that the case $t=0$ is excluded even when $p>2$.

In other words, $\phi^s c(d)=c(dp^s)$ unless $s>0$ and d has the form $1+p^t$ with $t>0$, so $p^s d$ has type II. Thus $C^3(A)$ is spanned by the elements $c(d)$ for $d\geq 3$ and $c'(d)$ for d of type II.

It is easy to see that $C^3_d(A)=C^3_d(\mathbb{F}_p)\otimes A$, and in the case $A=\mathbb{F}_p$ we know from Lemmas A.16 and A.17 that our spanning set is linearly independent. The proposition follows. □

Appendix B. Generalized elliptic curves

In this appendix, we outline the theory of generalized elliptic curves. We have tried to give an elementary account, with explicit formulae wherever possible. This has both advantages and disadvantages over the other available approaches, which make more use of the apparatus of schemes and sheaf cohomology. For more information, and proofs of results merely stated here, see [Del75, KM85, Sil94, DR73]. Note, however, that our definition is not quite equivalent to that of [DR73]: their generalized elliptic curves are more generalized than ours, so what we call a generalized elliptic curve is what they would call a stable curve of genus 1 with a specified section in the smooth locus.

We shall again think of non-affine schemes as functors from rings to sets. The basic example is the projective scheme $\mathbb{P}^n$, where $\mathbb{P}^n(R)$ is the set of submodules $L\leq R^{n+1}$ such that L is a summand and has rank one. If we have elements $a_0,\dots,a_n\in R$ such that $\sum_i Ra_i=R$ then the vector $(a_0,\dots,a_n)\in R^{n+1}$ generates such a submodule, which we denote by $[a_0:\dots:a_n]$. This is of course a free module. In general, L may be a non-free projective module, so it need not have the form $[a_0:\dots:a_n]$, but nonetheless it is usually sufficient to consider only points of that form. For more details, and a proof of equivalence with more traditional approaches, see [Str99a, Section 3].

Definition B.1. A *Weierstrass curve* over a scheme S is a (non-affine) scheme of the form

$$\begin{aligned} C &= C(a_1,a_2,a_3,a_4,a_6) \\ &= \{([x:y:z],s)\in\mathbb{P}^2\times S \mid y^2z+a_1(s)xyz+a_3(s)yz^2 = x^3+a_2(s)x^2z+a_4(s)xz^2+a_6(s)z^3\} \end{aligned}$$

for some system of functions $a_1, \dots, a_6 \in \mathcal{O}_S$. (Whenever we write $(a_1, \dots, a_6)$, it is to be understood that there is no a_5.) For any such curve, there is an evident projection $p\colon C \longrightarrow S$ and a section $0\colon S \longrightarrow C$ given by $s \mapsto ([0:1:0], s)$. We write $WC(R)$ for the set of 5-tuples $(a_1, \dots, a_6) \in R^5$, which can clearly be identified with the set of Weierstrass curves over $\operatorname{spec}(R)$. Thus, $WC = \operatorname{spec}(\mathbb{Z}[a_1, \dots, a_6])$ is a scheme. We define various auxiliary functions as follows:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= a_1a_3 + 2a_4 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\
j &= c_4^3/\Delta
\end{aligned}$$

The function $\Delta \in \mathcal{O}_S$ is called the discriminant. We say that a Weierstrass curve C is *smooth* if its discriminant is a unit in $\mathcal{O}_S$.

Definition B.2. A *generalized elliptic curve* over S is a scheme C equipped with maps $S \xrightarrow{0} C \xrightarrow{p} S$ such that S can be covered by open subschemes S_i such that $C_i = C \times_S S_i$ is isomorphic to a Weierstrass curve, by an isomorphism preserving p and 0. An *elliptic curve* is a generalized elliptic curve that is locally isomorphic to a smooth Weierstrass curve. We shall think of S as being embedded in C as the zero-section. We write $\omega_{C/S}$ for the cotangent space to C along S, or equivalently $\omega_{C/S} = \mathcal{I}_S/\mathcal{I}_S^2$, where $\mathcal{I}_S$ is the ideal sheaf of S. One checks that this is a line bundle on S. We say that C/S is *untwisted* if $\omega_{C/S}$ is trivializable.

It is possible to give an equivalent coordinate-free definition, but this requires rather a lot of algebro-geometric machinery.

Let C be a Weierstrass curve. Note that if we put $z = 0$ then the defining equation becomes $x^3 = 0$, so the locus where $z = 0$ is an infinitesimal thickening of the locus $x = z = 0$, which is our embedded copy of S. Thus, the complementary open subscheme $C_1 = C \setminus S$ is just the locus where z is invertible. This can be identified with the curve in the affine plane with equation

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

Weierstrass curves are often described by giving this sort of inhomogeneous equation.

A given generalized elliptic curve can be isomorphic to two different Weierstrass curves, and it is important to understand the precise extent to which this can happen. For this, we define a group scheme WR of "Weierstrass reparameterizations": for any ring R, $WR(R)$ is the group of matrices of the form

$$M(u, r, s) = \begin{pmatrix} u^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}$$

with $u \in R^\times$. Such a matrix acts by multiplication on $\mathbb{P}^2 \times \operatorname{spec}(R)$ in the obvious way, and one checks that it carries $C(a_1, \dots, a_6)$ to $C(a'_1, \dots, a'_6)$, where

$$\begin{aligned}
a'_1 &= a_1u - 2s \\
a'_2 &= a_2u^2 + a_1su - 3r - s^2 \\
a'_3 &= a_3u^3 - a_1ru + 2rs - 2t \\
a'_4 &= a_4u^4 + a_3su^3 - 2a_2ru^2 + a_1(t - 2rs)u + 3r^2 + 2rs^2 - 2st \\
a'_6 &= a_6u^6 - a_4ru^4 + a_3(t - rs)u^3 + a_2r^2u^2 + a_1(r^2s - rt)u + 2rst - t^2 - r^2s^2 - r^3
\end{aligned}$$

(These equations are equivalent to [Del75, Equations 1.6] with a_i and a'_i exchanged.)

We therefore have an action of WR on WC, and a map from $WR\times WC$ to the scheme of triples (C,C',f) where C and C' are Weierstrass curves and f is an isomorphism $C\longrightarrow C'$ of pointed curves. One can check that this map is an isomorphism.

If we define c'_4, c'_6, Δ' and j' in the obvious way then we have

$$\begin{aligned} c'_4 &= c_4u^4 \\ c'_6 &= c_6u^6 \\ \Delta' &= \Delta u^{12} \\ j' &= j. \end{aligned}$$

Definition B.3. Let C be a generalized elliptic curve over S. We will define various things as though C were a Weierstrass curve; one can check that the definitions are local on S and invariant under reparameterization, so they are well-defined in general. We write

$$\begin{aligned} S_{\text{ell}} &= D(\Delta) \\ S_{\text{sing}} &= V(\Delta) \\ S_{\text{mult}} &= D(c_4)\cap V(\Delta) \\ S_{\text{add}} &= V(c_4)\cap V(\Delta), \end{aligned}$$

and call these the elliptic, singular, multiplicative and additive loci in S, respectively. Here as usual, $D(a)$ is the locus where a is invertible and $V(a)$ is the locus where $a=0$. Let f be a standard Weierstrass equation for C, and write $f_x=\partial f/\partial x$ and so on. Let C_{sing} be the closed subscheme of C where $f_x=f_y=f_z=0$, and let C_{reg} be the complementary open subscheme.

It turns out that C_{reg} has a unique structure as an abelian group scheme over S such that the map $0\colon S\longrightarrow C_{\text{reg}}$ is the zero section. If C is a Weierstrass curve, then any three sections c_0,c_1,c_2 of C_{reg} with $c_0+c_1+c_2=0$ are collinear in $\mathbb{P}^2$, or equivalently the matrix formed by the coordinates of the c_i has determinant zero. Any map of generalized elliptic curves (compatible with the projections and the zero-sections) is automatically a homomorphism. One can check that the negation map is given by

$$-[x:y:z]=[x:-a_1x-y-a_3z:z].$$

The formal completion of C along S is written $\widehat{C}$. If C is defined by a Weierstrass equation $f=0$ then we have

$$\widehat{C}(R)=\{(x,z,s)\in \operatorname{Nil}(R)^2\times S(R)\mid f(x,1,z)=0\},$$

where $\operatorname{Nil}(R)$ is the set of nilpotent elements in R. One checks using the formal implicit function theorem that there is a unique power series $\xi(x)=\sum_{k>0}\xi_kx^k\in\mathcal{O}_S[\![x]\!]$ such that $\xi(x)=x^3 \pmod{x^4}$, and $(x,z,s)\in\widehat{C}(R)$ if and only if $z=\xi(x)$. This proves that $\widehat{C}\cong S\times\widehat{\mathbb{A}}^1$, so that $\widehat{C}$ is a formal curve over S. The rational function x/y gives a coordinate; we normally work in the affine piece $y=1$ so this just becomes x. The group structure on C thus makes $\widehat{C}$ into a formal group over S (i.e. a commutative, one-dimensional, smooth formal group). If we define

$$\chi(x_0,x_1,x_2)=\sum_{i,j,k\geq 0}\xi_{i+j+k+2}x_0^ix_1^jx_2^k$$

then one can check that $\chi(x_0,x_1,x_2)=x_0+x_1+x_2 \bmod (x_0,x_1,x_2)^2$ and

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

One can deduce from this that $\chi(x_0,x_1,x_2)$ is a unit multiple of $x_0+_Fx_1+_Fx_2$, and that the series $G(x_0,x_1)=[-1]_F(x_0+_Fx_1)$ is uniquely characterized by the equation $\chi(x_0,x_1,G(x_0,x_1))=0$.

We also have

$$[-1]_F(x) = -x/(1 + a_1 x + a_3 \xi(x)).$$

More generally, if C is an untwisted generalized elliptic curve then $\widehat{C}$ is still a formal group, although we do not have such explicit formulae in this case.

B.0.1. *Modular forms.*

Definition B.4. A *modular form of weight* k over $\mathbb{Z}$ is a rule g that assigns to each generalized elliptic curve C/S a section $g(C/S)$ of $\omega_{C/S}^{\otimes k}$ over S, in such a way that for each pull-back square

$$\begin{tikzcd} C \arrow[r, "\tilde{f}"] \arrow[d, "p"'] & C' \arrow[d, "p'"] \\ S \arrow[r, "f"'] & S' \end{tikzcd}$$

of generalized elliptic curves, we have $f^*g(C'/S') = g(C/S)$. (We will shortly compare this with the classical, transcendental definition.) We write MF_k for the group of modular forms of weight k over $\mathbb{Z}$. More generally, for any ring R, we define modular forms over R by the same procedure, except that S is required to be a scheme over $\operatorname{spec}(R)$.

Let $C = C(a_1, \dots, a_6)$ be the obvious universal Weierstrass curve over the scheme

$$WC = \operatorname{spec}(\mathbb{Z}[a_1, \dots, a_6]).$$

We have a projection map $\pi\colon WR \times WC \longrightarrow WC$ and also an action map $\alpha\colon WR \times WC \longrightarrow WC$ defined by

$$\alpha(a_1, \dots, a_6, r, s, t, u) = (a_1', \dots, a_6'),$$

where the elements a_i' are as in the previous section.

We can regard $WR \times C$ as a generalized elliptic curve over $WR \times WC$, and we have maps

$$\tilde{\pi}, \tilde{\alpha}\colon WR \times C \longrightarrow C \tag{B.5}$$

covering π and α. The first of these is just the projection, and the second is given by the usual action of $WR < GL_3$ on $\mathbb{P}^2$. It is clear that the group of modular forms of weight k over $\mathbb{Z}$ is precisely the set of sections $g(C/WC)$ of $\omega_{C/WC}^{\otimes k}$ such that

$$\alpha^* g(C/WC) = \pi^* g(C/WC). \tag{B.6}$$

More explicitly, there is the following.

Proposition B.7. *The space MF_k can be identified with the set of functions $h \in \mathcal{O}_{WC} = \mathbb{Z}[a_1, \dots, a_6]$ such that $\alpha^* h = u^k h$. Moreover, we have an isomorphism of graded rings*

$$MF_* = \mathbb{Z}[c_4, c_6, \Delta]/(1728\Delta - c_4^3 + c_6^2),$$

where $c_4 \in MF_4$, $c_6 \in MF_6$ and $\Delta \in MF_{12}$. (The prime factorization of 1728 *is* $2^6\,3^3$*.)*

Proof. To understand the condition (B.6) more explicitly, we notice that x/y defines a function on a neighborhood of the zero-section in C, so we have a section $d(x/y)_0$ of $\omega_{C/WC}$, which is easily seen to be a basis. Moreover, we have $\pi^* d(x/y)_0 = d(x/y)_0$ and $\alpha^* d(x/y)_0 = u^{-1} d(x/y)_0$. Thus, a section $g(C/WC)$ of $\omega_{C/WC}^{\otimes k}$ is of the form $g(C/WC) = h\, d(x/y)_0^k$ for a unique $h \in \mathcal{O}_{WC} = \mathbb{Z}[a_1, \dots, a_6]$; and equation (B.6) is equivalent to the equation $\alpha^* h = u^k \pi^* h$ (and we implicitly identify $\pi^* h$ with h). It follows that c_4, c_6 and Δ correspond to modular forms of the indicated weights, and one checks directly from the definitions that $c_4^3 - c_6^2 = 1728\Delta$. The proof that MF_* is precisely $\mathbb{Z}[c_4, c_6, \Delta]/(1728\Delta - c_4^3 + c_6^2)$ can be found in [Del75] and will not be reproduced here. □

Definition B.8. The *q-expansion* of a modular form g is the series $h(q) \in \mathbb{Z}[\![q]\!] = \mathcal{O}_{D_{\mathrm{Tate}}}$ such that $g(C_{\mathrm{Tate}}/D_{\mathrm{Tate}}) = h(q)d(x/y)_0^k$.

Note that if τ lies in the upper half plane then the analytic variety $C_\tau = \mathbb{C}/\mathbb{Z}\{1,\tau\}$ has a canonical structure as a scheme over $\operatorname{spec}(\mathbb{C})$, which makes it an elliptic curve. Moreover, if z is the obvious coordinate on $\mathbb{C}$, then the form dz on $\mathbb{C}$ gives an invariant differential on C_τ. Thus, for any modular form g of weight k we have a complex number $f(\tau)$ such that $g(C_\tau/\operatorname{spec}(\mathbb{C})) = f(\tau)(dz)^k$. If $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and $\tau' = (a\tau+b)/(c\tau+d)$ then multiplication by $(c\tau+d)^{-1}$ gives an isomorphism $C_\tau \longrightarrow C_{\tau'}$. The pull-back of dz along this is $(dz)/(c\tau+d)$, so we conclude that $f(\tau') = (c\tau+d)^k f(\tau)$. One can check that this construction gives an isomorphism of $\mathbb{C}\otimes MF_*$ with the more classical ring of holomorphic functions on the upper half plane, satisfying the functional equation $f(\tau') = (c\tau+d)^k f(\tau)$ and a growth condition at infinity. Moreover, if g has q-expansion $h(q)$ then the power series $h(e^{2\pi i\tau})$ converges to $f(\tau)$.

B.0.2. *Invariant differentials.* As C_{reg} is a group scheme, the sections of $\omega_{C/S}$ over S biject with the sections of $\Omega^1_{C/S}$ over C_{reg} that are invariant under translation. This is proved by the same argument as the corresponding fact for Lie groups. Another way to say this is as follows. A section of $\Omega^1_{C/S}$ is the same as a section of $\mathcal{I}_\Delta/\mathcal{I}_\Delta^2$, where Δ is the diagonal in $C_{\mathrm{reg}} \times_S C_{\mathrm{reg}}$, and $\mathcal{I}_\Delta$ is the associated ideal sheaf. In other words, it is a function $\alpha(c_0,c_1)$ that is defined when c_0 is infinitesimally close to c_1, such that $\alpha(c,c) = 0$. In these terms, a section of the form $g\,dh$ becomes the function $(c_0,c_1) \mapsto g(c_0)(h(c_0)-h(c_1))$. A section of $\Omega^1_{C/S}$ is invariant if and only if $\alpha(c+c_0,c+c_1) = \alpha(c_0,c_1)$. On the other hand, a section of $\omega_{C/S}$ is a function $\beta(c)$ that is defined when c is infinitesimally close to 0, such that $\beta(0) = 0$. These biject with invariant sections of $\Omega^1_{C/S}$ by $\beta(c) = \alpha(c,0)$ and $\alpha(c_0,c_1) = \beta(c_0-c_1)$.

We refer to invariant sections of $\Omega^1_{C/S}$ as invariant differentials on C. We next exhibit such a section when C is a Weierstrass curve. Suppose that C is given by an equation $f=0$, where

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

We write $f_x = \partial f/\partial x$ and so on. Next, observe that a point that is infinitesimally close to $0 = [0:1:0]$ has the form $[\epsilon:1:0]$ with $\epsilon^2 = 0$. We need to calculate $[x:1:z]+[\epsilon:1:0]$. We know that $-[x:1:z] = [-x:1+a_1x+a_3z:-z]$ and $-[\epsilon:1:0] = [-\epsilon:1+a_1\epsilon:0]$, and one checks that

$$\begin{vmatrix} -\epsilon & 1+a_1\epsilon & 0 \\ -x & 1+a_1x+a_3z & -z \\ x+\epsilon f_z & 1 & z-\epsilon f_x \end{vmatrix} = 0 \pmod{\epsilon^2}$$

and

$$f(x+\epsilon f_z, 1, z-\epsilon f_x) = 0 \pmod{\epsilon^2}.$$

This shows that

$$[x:1:z]+[\epsilon:1:0] = [x+\epsilon f_z:1:z-\epsilon f_x] \pmod{\epsilon^2}.$$

Thus, if we define a section β_0 of $\omega_{C/S}$ by $\beta_0([\epsilon:1:0]) = \epsilon$, then the corresponding invariant differential α_0 satisfies

$$\alpha_0([x+\epsilon f_z:1:z-\epsilon f_x],[x:1:z]) = \epsilon,$$

and thus $\alpha_0 = dx/f_z$. It is convenient to rewrite this in terms of homogeneous coordinates: it becomes $\alpha_0 = y^2\,d(x/y)/f_z$. We rewrite this again, and also introduce two further forms α_1 and α_2, as follows:

$$\begin{aligned} \alpha_0 &= y^2d(x/y)/f_z = (y\,dx - x\,dy)/f_z \\ \alpha_1 &= z^2d(y/z)/f_x = (z\,dy - y\,dz)/f_x \\ \alpha_2 &= x^2d(z/x)/f_y = (x\,dz - z\,dx)/f_y. \end{aligned}$$

We claim that any two of these forms agree wherever they are both defined. Indeed, one can check directly that

$$\begin{aligned}\alpha_0 - \alpha_1 &= (y\, df - 3f\, dy)/(f_x f_z)\\ \alpha_1 - \alpha_2 &= (z\, df - 3f\, dz)/(f_y f_x)\\ \alpha_2 - \alpha_0 &= (x\, df - 3f\, dx)/(f_z f_y),\end{aligned}$$

and the right hand sides are zero because $f = 0$ on C and thus $df = 0$ on C. Thus, we get a well-defined differential form α on the complement of the closed subscheme C_{sing} where $f_x = f_y = f_z = 0$. We have seen that α_0 is invariant wherever it is defined, and it follows by an evident density argument that α is invariant on all of C_{reg}.

B.1. **Examples of Weierstrass curves.** In this section, we give a list of examples of Weierstrass curves with various universal properties or other special features. We devote the whole of the next section to the Tate curve.

B.1.1. *The standard form where six is invertible.* Consider the curve $C = C(0, 0, 0, a_4, a_6)$ over the base scheme $S = \mathrm{spec}(\mathbb{Z}[\frac{1}{6}, a_4, a_6])$ given by the equation

$$y^2 z = x^3 + a_4 x z^2 + a_6 z^3,$$

equipped with the invariant differential

$$\alpha = \frac{-z\, dx + x\, dz}{2yz} = \frac{y\, dz - z\, dy}{3x^2 + a_4 z^2} = \frac{y\, dx - x\, dy}{y^2 - 2a_4 xz - 3a_6 z^2}.$$

We have

$$\begin{aligned}c_4 &= -2^4 3 a_4\\ c_6 &= -2^5 3^3 a_6\\ \Delta &= -2^4(4a_4^3 + 27a_6^2)\\ j &= 2^8 3^3 a_4^3/(4a_4^3 + 27a_6^2)\end{aligned}$$

This is the universal example of a generalized elliptic curve over a base where six is invertible, equipped with a generator α of $\omega_{E/S}$. More precisely, suppose we have a scheme S' where six is invertible in $\mathcal{O}_{S'}$, and a generalized elliptic curve $C' \longrightarrow S'$. Suppose that the line bundle $\omega_{C'/S'}$ over S' is trivial, and that α' is a generator. Then there is a map $f\colon S' \longrightarrow S$, and an isomorphism $g\colon C' \cong f^*C$, such that the image of α under the evident map induced by f and g, is α'. Moreover, the pair (f, g) is unique.

Here is an equivalent statement: there is a unique quadruple (x', y', a_4', a_6') with the following properties:

i. x' and y' are functions on $C_1' = C' \setminus S'$.
ii. a_4 and a_6 are functions on S'.
iii. The functions x' and y' induce an isomorphism of C_1' with the curve $(y')^2 = (x')^3 + a_4 x' + a_6$ in $\mathbb{A}^2 \times S$.
iv. The form $\alpha'|_{C_1'}$ is equal to $-dx'/(2y')$.

B.1.2. *The Jacobi quartic.* The Jacobi quartic is given by the equation

$$Y^2 = 1 - 2\delta X^2 + \epsilon X^4$$

over $\mathbb{Z}[\frac{1}{6}, \delta, \epsilon]$. The projective closure of this curve is singular, so instead we consider the closure in $\mathbb{P}^3$ of its image under the map $[1, X, Y, X^2]$. This closure (which we will call C) is defined by the equations

$$\begin{aligned}Y^2 &= W^2 - 2\delta WZ + \epsilon Z^2\\ WZ &= X^2.\end{aligned}$$

For generic δ and ϵ, the curve C is smooth and is the normalization of the projective closure of the Jacobi quartic. In all cases, C is isomorphic to the Weierstrass curve

$$y^2z = (x - 12\delta z)((x + 6\delta z)^2 - 324\epsilon)$$

via

$$\begin{aligned} x &= \frac{6((3\epsilon - \delta^2)X^2 + 2\delta(Y - 1))}{Y + \delta X^2 - 1} \\ y &= \frac{2^2 3^3(\delta^2 - \epsilon)X}{Y + \delta X^2 - 1} \\ X &= 6(12\delta - x)/y \\ Y &= (2^5 3^4 \delta(\delta^2 - 3\epsilon) + 2^3 3^3(\delta^2 + 3\epsilon)x - 36\delta x^2 + y^2)/y^2. \end{aligned}$$

The standard invariant differential is as follows

$$\alpha = -dX/(6Y) = -dx/(2y) = dy/(2^2 3^3(\delta^2 + 3\epsilon) - 3x^2).$$

The zero section corresponds to the point

$$[W : X : Y : Z] = [1 : 0 : 1 : 0].$$

There is also a distinguished point P of order two, given by

$$[W : X : Y : Z] = [1 : 0 : -1 : 0] \qquad \text{or} \qquad [x : y : z] = [12\delta : 0 : 1].$$

The curve C is the universal example of an elliptic curve with a given generator of ω_E and a given point of order two, over a base scheme where six is invertible. Indeed, given such a curve, the last example tells us that there is a unique quadruple (x, y, a_4, a_6) giving an isomorphism of C with the curve $y^2 = x^3 + a_4x + a_6$, such that the given differential is $d(x/y)_0$. The points of exact order two correspond to the points where the tangent line is vertical. It follows that we must have $y(P) = 0$ and $x(P) = 12\delta$ for some δ, so that $12^3\delta^3 + 12a_4\delta + a_6 = 0$, so $x - 12\delta$ divides $x^3 + a_4x + a_6$. As the coefficient of x in this polynomial is zero, one checks that the remaining term has the form $x^2 + 12\delta + \eta$ for some η, or equivalently the form $(x + 6\delta)^2 + 324\epsilon$ for some ϵ. The claim follows easily from this.

The modular forms for the Jacobi curve are

$$\begin{aligned} c_4 &= 2^6 3^4(\delta^2 + 3\epsilon) \\ c_6 &= 2^9 3^6 \delta(\delta^2 - 9\epsilon) \\ \Delta &= 2^{12} 3^{12}(\epsilon - \delta^2)^2\epsilon \\ j &= 2^6 \frac{(\delta^2 + 3\epsilon)^3}{\epsilon(\epsilon - \delta^2)^2}. \end{aligned}$$

B.1.3. *The Legendre curve.* Consider the Weierstrass curve over $\mathbb{Z}[\frac{1}{2}, \lambda]$ given by

$$y^2z = x(x - z)(x - \lambda z).$$

The modular forms are

$$\begin{aligned} c_4 &= 2^4(1 - \lambda + \lambda^2) \\ c_6 &= 2^5(\lambda - 2)(\lambda + 1)(2\lambda - 1) \\ \Delta &= 2^4\lambda^2(\lambda - 1)^2 \\ j &= 2^8(1 - \lambda + \lambda^2)^3/((\lambda - 1)^2\lambda^2) \end{aligned}$$

If we restrict to the open subscheme where λ and $(1 - \lambda)$ are invertible, then the kernel of multiplication by 2 is a constant group scheme, with points

$$0 = [0 : 1 : 0] \qquad P = [0 : 0 : 1] \qquad Q = [1 : 0 : 1] \qquad P + Q = [\lambda : 0 : 1].$$

B.1.4. *Singular fibers.* The curve $y^2z + xyz = x^3$ is a nodal cubic, with multiplicative formal group. There is a birational map f from $\mathbb{P}^1$ to the curve, with inverse g:

$$f[s : t] = [st(s - t) : t^2s : (s - t)^3]$$

$$g[x : y : z] = [x + y : y].$$

The map f sends 1 to $[0 : 1 : 0]$, and sends both 0 and infinity to the singular point $[0 : 0 : 1]$. If $s_0s_1s_2 = 1$ then the points $f[s_0 : 1]$, $f[s_1 : 1]$ and $f[s_2 : 1]$ are collinear, which shows that the restriction to $\mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\}$ is a homomorphism. The discriminant is zero and the j invariant is infinite.

The curve $y^2z = x^3$ is a cuspidal cubic, with additive formal group. There is a birational map f from $\mathbb{P}^1$ to the curve, with inverse g:

$$f[s : t] = [t^2s : t^3 : s^3]$$

$$g[x : y : z] = [x : y].$$

This sends infinity to the singular point $[0 : 0 : 1]$ with multiplicity two, and sends 0 to $[0 : 1 : 0]$. If $s_0 + s_1 + s_2 = 0$ then the points $f[s_0 : 1]$, $f[s_1 : 1]$ and $f[s_2 : 1]$ are collinear, which shows that the restriction to $\mathbb{G}_a = \mathbb{P}^1 \setminus \{\infty\}$ is a homomorphism. The discriminant is zero and the j invariant is undefined.

B.1.5. *Curves with prescribed j invariant.* If a and $b = a - 1728$ are invertible in R then we have a smooth Weierstrass curve C over $\operatorname{spec}(R)$ with equation

$$y^2z + xyz = x^3 - 36xz^2/b - z^3/b.$$

The associated modular forms are

$$\begin{aligned} c_4 = -c_6 &= a/b \\ \Delta &= a^2/b^3 \\ j &= a. \end{aligned}$$

If 6 is invertible in R we can put $a = 0$ and get the singular curve $(y + x/2)^2 = (x + 1/12)^3$, which has $c_4 = \Delta = 0$ so that j is undefined.

B.2. **Elliptic curves over $\mathbb{C}$.** Let C be an elliptic curve over $\mathbb{C}$. It is well-known that there exists a complex number τ in the upper half plane and a complex-analytic group isomorphism $C \cong C_\tau = \mathbb{C}/\Lambda$, where Λ is the lattice generated by 1 and τ. We collect here a number of formulae, which are mostly proved in [Sil94, Chapter V] (for example). We write $q = e^{2\pi i\tau}$, so the map $z \mapsto u = e^{2\pi iz}$ gives an analytic isomorphism $\mathbb{C}_\tau \cong \mathbb{C}^\times/q^{\mathbb{Z}}$. We also have an analytic isomorphism of C_τ with the curve

$$Y^2Z = 4X^3 - g_2XZ - g_3Z^3,$$

where $g_k = \sum_{\omega\in\Lambda\setminus 0} \omega^{-2k}$. The isomorphism is given by $(z \bmod \Lambda) \mapsto [\wp(z) : \wp'(z) : 1]$, where

$$\wp(z) = z^{-2} + \sum_{\omega\in\Lambda\setminus 0} ((z - \omega)^{-2} - \omega^{-2}).$$

This is to be interpreted as $[0 : 1 : 0]$ if z lies in Λ. We also have an analytic isomorphism of C_τ with the Weierstrass curve

$$y^2z + xyz = x^3 + a_4xz^2 + a_6z^3,$$

where a_4 and a_6 are given by the same formulae as for the Tate curve in §2.6. This isomorphism sends $u = e^{2\pi iz}$ to $[x : y : 1]$, where x and y are again given by the same formulae as for the Tate curve. We have the following identities.

$$\begin{aligned} X &= (2\pi i)^2(x+1/12) \\ Y &= (2\pi i)^3(2y+x) \\ a_4 &= -(2\pi i)^{-4}g_2/4+1/48 \\ a_6 &= -(2\pi i)^{-6}g_3/4-(2\pi i)^{-4}g_2/48+1/1728. \end{aligned}$$

B.3. **Singularities.**

Proposition B.9. *Let C be a generalized elliptic curve over S. Then C is flat over S.*

Proof. We can work locally on S and thus assume that S is affine and that C is a Weierstrass curve. Let C_0 be the locus where z is invertible, which is isomorphic to the affine curve where $z=1$, which has equation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$. Thus, the ring of functions on C_0 is a free module of rank 2 over $\mathcal{O}_S[x]$, or of rank 3 over $\mathcal{O}_S[y]$. Either description makes it clear that $\mathcal{O}_{C_0}$ is free as a module over $\mathcal{O}_S$, so C_0 is flat over S. Similar arguments show that the locus C_1 (where y is invertible) is also flat. The union of C_0 and C_1 is the complement of the closed subscheme where $y=z=0$. On this locus the defining equation gives $x^3=0$, which is impossible as x, y and z are assumed to generate the unit ideal. It follows that $C_0\cup C_1=C$, and thus that C is flat over S. □

Proposition B.10. *The singular locus C_{sing} is contained in the open subscheme $C_0=C\setminus S$. The projection $p\colon C\longrightarrow S$ sends C_{sing} into S_{sing}.*

Proof. Our claims are local on S so we may assume that C is a Weierstrass cubic, defined by an equation $f=0$ in the usual way. On $S\subset C$ we have $x=z=0$ and y is invertible, so we can take $y=1$. We then have $f_z=y^2=1$, so clearly $S\subseteq C_{\mathrm{reg}}$ and $C_{\mathrm{sing}}\subseteq C_0$.

Now consider a point $P=[x:y:z]$ of C. If $z=0$ then the defining equation gives $x^3=0$, so P lies in an infinitesimal thickening of $S\subset C$. It follows that C_0 is the same as the complementary open locus where z is invertible.

Now consider a point $P=[x:y:z]$ of C_{sing}. By the above, z is invertible so we may assume $z=1$. We can then shift our coordinates so that $x=y=0$. This changes f but does not change Δ, as we see from the standard transformation formulae. Let the new f be

$$f(x,y,1)=(y^2+a_1xy+a_3y)-(x^3+a_2x^2+a_4x+a_6).$$

We must have $f(0,0,1)=f_x(0,0,1)=f_y(0,0,1)=0$, so $a_3=a_4=a_6=0$. It follows that the parameters b_k are given by $b_2=a_1^2+4a_2$ and $b_4=b_6=b_8=0$, and thus that $\Delta=0$. In other words, P lies over S_{sing} as claimed. □

B.4. **The cubical structure for the line bundle $\mathcal{I}(0)$ on a generalized elliptic curve.** In this section we give a proof of Proposition 2.55.

B.4.1. *Divisors and line bundles.* We will need to understand the relationship between divisors and line bundles in a form which is valid for non-Noetherian schemes. An account of divisors on curves is given in [KM85], but we need to genera-Lise this slightly to deal with divisors on $C\times_S C\times_S C$ over S, for example. The issues involved are surely well-known to algebraic geometers, but it seems worthwhile to have a self-contained and elementary account.

Definition B.11. Let X be a scheme over a scheme S. An *effective divisor* on X over S is a closed subscheme $Y\subseteq X$ such that the ideal sheaf $\mathcal{I}_Y$ is invertible and the map $Y\longrightarrow S$ is flat.

Suppose that $S=\mathrm{spec}(A)$ and $X=\mathrm{spec}(B)$ for some A-algebra B, and that $Y=\mathrm{spec}(B/b)$ for some element b that is not a zero-divisor. Then $\mathcal{I}_Y$ corresponds to the principal ideal $Bb\cong B$ in B, and it is easy to see that Y is a divisor if and only if B/b is a flat A-module.

Conversely, if Y is a divisor then one can cover S by open sets of the form $S' = \mathrm{spec}(A)$ and the preimage X' of S' by sets of the form $\mathrm{spec}(B)$ in such a way that $Y \cap \mathrm{spec}(B)$ has the form $\mathrm{spec}(B/b)$ as above.

Proposition B.12. *Let Y and Z be effective divisors on X over S. Then there is a unique effective divisor $Y + Z$ with $\mathcal{I}_{Y+Z} = \mathcal{I}_Y \mathcal{I}_Z = \mathcal{I}_Y \otimes_{\mathcal{O}_X} \mathcal{I}_Z$. The effective divisors form an abelian monoid* $\mathrm{Div}^+(X/S)$ *under this operation. Moreover, this monoid has cancellation.*

Proof. We define $Y + Z$ to be the closed subscheme defined by the ideal sheaf $\mathcal{I}_Y \mathcal{I}_Z < \mathcal{O}_X$. We claim that the product map $\mathcal{I}_Y \otimes_{\mathcal{O}_X} \mathcal{I}_Z \longrightarrow \mathcal{I}_{Y+Z} = \mathcal{I}_Y \mathcal{I}_Z$ is an isomorphism. Indeed, the question is local, and locally it translates to the claim that $Bb \otimes_B Bc$ maps isomorphically to Bbc when b and c are not zero-divisors, and this claim is obvious. All that is left is to check that $Y + Z$ is flat over S. Locally, we have a short exact sequence

$$\begin{tikzcd} B/b \arrow[r, tail, "c"] & B/bc \arrow[r, two heads] & B/c \end{tikzcd}$$

with B/b and B/c flat over A, so B/bc is also flat over A. The rest is clear. □

Definition B.13. We write $\mathrm{Div}(X/S)$ for the group completion of the monoid $\mathrm{Div}^+(X/S)$, and refer to its elements as divisors. The proposition implies that the natural map $\mathrm{Div}^+(X/S) \longrightarrow \mathrm{Div}(X/S)$ is injective. It also implies that given a divisor $Y = Y_+ - Y_-$, we can define a line bundle $\mathcal{I}_Y = \mathcal{I}_{Y_+} \mathcal{I}_{Y_-}^{-1}$ and this is well-defined up to canonical isomorphism.

Proposition B.14. *Let $f \colon X' \longrightarrow X$ be a flat map. Then the pull-back along f gives a homomorphism* $\mathrm{Div}^+(X/S) \longrightarrow \mathrm{Div}^+(X'/S)$*, with $\mathcal{I}_{f^*Y} = f^*\mathcal{I}_Y$ as line bundles over X'. This extends to give an induced homomorphism $f^* \colon$* $\mathrm{Div}(X/S) \longrightarrow \mathrm{Div}(X'/S)$.

Proof. Let $Y \subset X$ be a divisor, and write $Y' = f^*Y = Y \times_X X'$. It is clear that this is a closed subscheme of X'. The induced map $f' \colon Y' \longrightarrow Y$ is a pull-back of a flat map so it is again flat. The map $Y \longrightarrow S$ is flat because Y is a divisor, so the composite $Y' \longrightarrow S$ is flat. Let $j \colon Y \longrightarrow X$ and $j' \colon Y' \longrightarrow X'$ be the inclusion maps. Essentially by definition we have $f^*\mathcal{O}_X = \mathcal{O}_{X'}$ and $f^* j_* \mathcal{O}_Y = j'_*(f')^* \mathcal{O}_Y = j'_* \mathcal{O}_{Y'}$. We have a short exact sequence of sheaves $\mathcal{I}_Y \longrightarrow \mathcal{O}_X \longrightarrow j_*\mathcal{O}_Y$, where $j \colon Y \longrightarrow X$ is the inclusion. As f is flat, the functor f^* is exact, so we have a short exact sequence $f^*\mathcal{I}_Y \longrightarrow \mathcal{O}_{X'} \longrightarrow j'_*\mathcal{O}_{Y'}$. It follows that $\mathcal{I}_{Y'} = f^*\mathcal{I}_Y$, and $f^*\mathcal{I}_Y$ is clearly a line bundle. Thus, Y' is a divisor, as required. It is easy to see that f^* is a homomorphism, and it follows by general nonsense that it induces a map of group completions. □

Proposition B.15. *Let $g \colon S' \longrightarrow S$ be an arbitrary map, and write $X' = g^*X$. Then pull-back along g gives a homomorphism* $\mathrm{Div}^+(X/S) \longrightarrow \mathrm{Div}^+(X'/S')$*, with $\mathcal{I}_{g^*Y} = g^*\mathcal{I}_Y$ as line bundles over X'. This extends to give an induced homomorphism $f^* \colon$* $\mathrm{Div}(X/S) \longrightarrow \mathrm{Div}(X'/S)$.

Proof. The proof is similar to that of the previous result. □

Definition B.16. Let $\mathcal{L}$ be a line bundle over X, and u a section of $\mathcal{L}$. Then there is a largest closed subscheme Y of X such that $u|_Y = 0$. If this is a divisor, we say that u is *divisorial* and write $\mathrm{div}(u) = Y$. If so, then u is a trivialization of the line bundle $\mathcal{L} \otimes \mathcal{I}_Y$, so $\mathcal{L} \cong \mathcal{I}_Y^{-1}$.

If v is a divisorial section of another line bundle $\mathcal{M}$ then one can check that $u \otimes v$ is a divisorial section of $\mathcal{L} \otimes \mathcal{M}$ with $\mathrm{div}(u \otimes v) = \mathrm{div}(u) + \mathrm{div}(v)$. One can also check that the formation of $\mathrm{div}(u)$ is compatible with the two kinds of base change discussed in Propositions B.14 and B.15.

Definition B.17. A *meromorphic divisorial section* u of a line bundle $\mathcal{L}$ is an expression of the form u_+/u_-, where u_+ and u_- are divisorial sections of line bundles $\mathcal{L}_+$ and $\mathcal{L}_-$ with a given isomorphism $\mathcal{L} = \mathcal{L}_+/\mathcal{L}_-$. These expressions are subject to the obvious sort of equivalence relation. We define $\mathrm{div}(u) = \mathrm{div}(u_+) - \mathrm{div}(u_-)$, which is well-defined by the above remarks. We again have $\mathcal{L} \cong \mathcal{I}_{\mathrm{div}(u)}^{-1}$.

Lemma B.18. *Let C be a subscheme of $\mathbb{P}^2 \times S$ defined by a single homogeneous equation $f = 0$ of degree m, such that the coefficients of f generate the unit ideal in $\mathcal{O}_S$. Let C_{reg} be the open subscheme $D(f_x) \cup D(f_y) \cup D(f_z)$ of C, where f_x, f_y and f_z are the partial derivatives of f. Let σ be a section of C_{reg} over S. Then $\sigma S \subset C$ is a divisor.*

Proof. Let U, V and W be the open subschemes of S where $f_x \circ \sigma$, $f_y \circ \sigma$ and $f_z \circ \sigma$ are invertible. Because σ is a section of C_{reg} we know that $S = U \cup V \cup W$. We restrict attention to U; a similar argument can be given for V and W. After replacing S by U, we may assume that $f_x \circ \sigma$ is invertible. Let C_1 and C_2 be the open subschemes where y and z are invertible. Because f is homogeneous of degree m we have $xf_x + yf_y + zf_z = mf$ and $f \circ \sigma = 0$ so $x = -yf_y/f_x - zf_z/f_x$ on the image of σ. Thus, on the closed subscheme where $y = z = 0$ we also have $x = 0$, so this subscheme is empty, which implies that $C = C_1 \cup C_2$. Write $U_i = \sigma^{-1}C_i$, so that $U = U_1 \cup U_2$. We restrict attention to U_2; a similar argument can be given for U_1. In this context we can work with the affine plane where $z = 1$, and x, y and f can be considered as genuine functions. Write $x_0 = x \circ \sigma$ and $y_0 = y \circ \sigma$. As $f \circ \sigma = 0$ we have $f = (x - x_0)g + (y - y_0)h$ for some functions g and h. Clearly, $g(x_0, y_0) = f_x(x_0, y_0)$ and this is assumed invertible, so $D(g)$ is an open subscheme of C_2 containing σU_2. On this scheme we have $f = 0$ and thus $x = x_0 - (y - y_0)h/g$. Thus

$$D(g) \cap V(y - y_0) = D(g) \cap V(x - x_0, y - y_0) = D(g) \cap \sigma S.$$

Thus, in the open set $D(g)$, our subscheme σS is defined by a single equation $y = y_0$, so the corresponding ideal sheaf is generated by $y - y_0$.

We still need to verify that $y - y_0$ is not a zero-divisor on $D(g) \cap C_2$. It is harmless to shift coordinates so that $y_0 = x_0 = 0$. Suppose that $r \in \mathcal{O}_S[x, y]$ is such that $ry = 0$ on $D(g) \cap C_2$; we need to show that $r = 0$ on $D(g) \cap C_2$. We have $g^k ry = sf$ in $\mathcal{O}_S[x, y]$ for some k and s. It follows that $g^{k+1}rx = g^k r(f - hy) = (g^k r - hs)f$ and thus $(g^k r - hs)yf = g^{k+1}rxy = gsxf$. As the coefficients of f generate $\mathcal{O}_S$ we know that f is not a zero-divisor in $\mathcal{O}_S[x, y]$ so $(g^k r - hs)y = gsx$. It follows easily that y divides gs, say $gs = ty$, and then $g^{k+1}ry = gsf = tfy$ so $g^{k+1}r = tf$. On C_2 we have $f = 0$ and thus $g^{k+1}r = 0$, so on $D(g) \cap C_2$ we have $r = 0$ as required.

This shows that the intersection of σS with $D(g) \cap C_2$ is a divisor. Similar arguments cover the rest of σS with open subschemes of C in which σS is a divisor. Trivially, the (empty) intersection of σS with the open subscheme $C \setminus \sigma S$ is a divisor. This covers the whole of C, as required. □

Corollary B.19. *If C is a generalized elliptic curve over S then the zero section of C is a divisor.* □

B.4.2. *The line bundle $\mathcal{I}(0)$.* Let C be a generalized elliptic curve over S, and let $\mathcal{I}(0)$ denote the ideal sheaf of $S \subset C$. The smooth locus C_{reg} is a group scheme over S, so we can define $\Theta^3(\mathcal{I}(0))$ over C_{reg} and thus the notion of a cubical structure. In this section we give a divisorial formula for $\Theta^3(\mathcal{I}(0))$.

Consider the scheme $C_S^3 = C \times_S C \times_S C$. A typical point of C_S^3 will be written as (c_0, c_1, c_2). We write $[c_0 = c_1]$ for the largest closed subscheme of $(C_{\mathrm{reg}})_S^3$ on which $c_0 = c_1$, and so on. This is the pull-back of the divisor $S \subset C_{\mathrm{reg}}$ under the map $g\colon (c_0, c_1, c_2) \mapsto c_0 - c_1$. This map is the composite of the isomorphism $(c_0, c_1, c_2) \to (c_0 - c_1, c_1, c_2)$ with the projection map $(C_{\mathrm{reg}})_S^3 \to C_{\mathrm{reg}}$, and the projection is flat because C is flat over S (Proposition B.9). Thus, g is flat. It follows from Proposition B.14 that $[c_0 = c_1]$ is a divisor, and the associated ideal sheaf is $g^*\mathcal{I}(0)$. Similar arguments show that the subschemes $[c_i = 0]$, $[c_i = c_j]$, $[c_i + c_j = 0]$ and $[c_0 + c_1 + c_2 = 0]$ are all divisors (assuming that $i \neq j$). We can thus define divisors

$$\begin{aligned}
D_1 &= [c_0 = 0] + [c_1 = 0] + [c_2 = 0] \\
D_2 &= [c_0 + c_1 = 0] + [c_1 + c_2 = 0] + [c_2 + c_0 = 0] \\
D_3 &= [c_0 + c_1 + c_2 = 0] \\
D_4 &= [c_0 = c_1] + [c_1 = c_2] + [c_2 = c_0].
\end{aligned}$$

There is (almost by definition) a canonical isomorphism of line bundles

$$\Theta^3(\mathcal{I}(0)) = \mathcal{I}(0)_0\mathcal{I}_{-D_1+D_2-D_3} = \omega_C\mathcal{I}_{D_2}\mathcal{I}_{D_1+D_3}^{-1}.$$

B.4.3. *A formula for the cubical structure.*

Definition B.20. Let $C = C(a_1, a_2, a_3, a_4, a_6)$ be a Weierstrass curve. A typical point of $(C_{\mathrm{reg}})^3_S$ will be written as (c_0, c_1, c_2), with $c_i = [x_i : y_i : z_i]$. We define $s(\underline{a})$ by the following expression:

$$s(\underline{a})(c_0, c_1, c_2) = \begin{vmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix}^{-1} \begin{vmatrix} x_0 & z_0 \\ x_1 & z_1 \end{vmatrix} \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix} \begin{vmatrix} x_2 & z_2 \\ x_0 & z_0 \end{vmatrix} (z_0z_1z_2)^{-1}d(x/y)_0.$$

Proposition B.21 (2.55). *$s(\underline{a})$ is a meromorphic divisorial section of the line bundle $p^*\omega_C$ over $(C_{\mathrm{reg}})^3_S$ (where $p\colon C^3_S \longrightarrow S$ is the projection). Its divisor is $-D_1 + D_2 - D_3$ (in the notation of §B.4.2), so it defines a trivialization of*

$$(p^*\omega_C) \otimes \mathcal{I}_{-D_1+D_2-D_3} = \Theta^3(\mathcal{I}(0)),$$

which is equal to $s(C/S)$.

Proof. By an evident base-change, we may assume that C is the universal Weierstrass curve over $S = \mathrm{spec}(\mathbb{Z}[a_1, a_2, a_3, a_4, a_6])$, and thus that S is a Noetherian, integral scheme.

We have a bundle $\mathcal{O}(1)$ over C, whose global sections are homogeneous linear forms in x, y and z. We can take the external tensor product of three copies of $\mathcal{O}(1)$ to get a bundle $\mathcal{L}$ over $C \times_S C \times_S C$. We define a section u of $\mathcal{L}$ by

$$u(c_0, c_1, c_2) = \begin{vmatrix} x_0 & y_0 & z_0 \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix}.$$

We claim that this is divisorial, and that $\mathrm{div}(u) = D_4 + D_3$. This is plausible, because one can easily check that $u = 0$ on the divisors $[c_i = c_j]$ (whose sum is D_3) and also on the divisor $[c_0 + c_1 + c_2 = 0]$ (because any three points that sum to zero are collinear). Let U_0 be the open subscheme of $(C_{\mathrm{reg}})^3_S$ where $c_1 \neq c_2$, and define U_1 and U_2 similarly. Then the complement of $U = U_0 \cup U_1 \cup U_2$ is the locus where $c_0 = c_1 = c_2$, which has codimension 2. Given this, it is enough to check that $u|_{U_i}$ is divisorial and that $\mathrm{div}(u|_{U_i}) = (D_4 + D_3) \cap U_i$ for $0 \leq i \leq 2$ (see [Har77, Proposition II.6.5]). By symmetry, we need only consider the case $i = 0$. Let V_0 be the complement of the diagonal in $(C_{\mathrm{reg}})^2_S$, so that $U_0 = C_{\mathrm{reg}} \times_S V_0$, which we can think of as the regular part of a generalized elliptic curve over V_0. The diagonal is defined by the vanishing of the quantities $x_1y_2 - x_2y_1$, $y_1z_2 - y_2z_1$, and $z_1x_2 - z_2x_1$, so on V_0 these quantities generate the unit ideal. It follows from this that the map

$$h\colon [s_1 : s_2] \mapsto [s_1x_1 + s_2x_2 : s_1y_1 + s_2y_2 : s_1z_1 + s_2z_2]$$

gives an isomorphism of $\mathbb{P}^1$ with the locus in $\mathbb{P}^2$ where the determinant vanishes. The addition law on C is defined by the requirement that the intersection of $h(\mathbb{P}^1)$ with $C \times_S V_0$ is $[c_0 = c_1] + [c_0 = c_2] + [c_0 = -c_1 - c_2]$. Moreover, we have $[c_1 = c_2] \cap U_0 = \emptyset$. Thus, $\mathrm{div}(u) \cap U_0 = (D_4 + D_3) \cap U_0$ as required.

We now define sections v and w of $\mathcal{L}$ and $\mathcal{L}^2$ by

$$v(c_0, c_1, c_2) = z_0z_1z_2$$

$$w(c_0, c_2, c_2) = \begin{vmatrix} x_0 & z_0 \\ x_1 & z_1 \end{vmatrix} \begin{vmatrix} x_1 & z_1 \\ x_2 & z_2 \end{vmatrix} \begin{vmatrix} x_2 & z_2 \\ x_0 & z_0 \end{vmatrix}.$$

By methods similar to the above, we find that

$$\mathrm{div}(z_0) = 3[c_0 = 0]$$

$$\mathrm{div}(x_0z_1 - x_1z_0) = [c_0 = 0] + [c_1 = 0] + [c_0 = c_1] + [c_0 + c_1 = 0]$$

and thus

$$\begin{aligned}\operatorname{div}(v) &= 3D_1\\ \operatorname{div}(w) &= 2D_1 + D_2 + D_4.\end{aligned}$$

We also have $s(\underline{a}) = u^{-1}wv^{-1}d(x/y)_0$ so as claimed this is a meromorphic divisorial section of $p^*\omega_C$, with divisor $-D_1 + D_2 - D_3$. As explained earlier, it therefore gives rise to a trivialization of $\Theta^3(\mathcal{I}(0))$.

Recall that $\Theta^3(\mathcal{I}(0))$ is canonically trivialized on the locus where $c_2 = 0$. In terms of our picture of $\Theta^3(\mathcal{I}(0))$ involving rational one-forms, this isomorphism sends a one-form to its residue at $c_2 = 0$. To calculate this for $s(\underline{a})$, we may as well restrict attention to the affine piece where $y_0 = y_1 = y_2 = 1$, and let x_2 tend to zero. The 3×3 determinant in the definition of $s(\underline{a})$ approaches $-\left|\begin{smallmatrix} x_0 & z_0 \\ x_1 & z_1 \end{smallmatrix}\right|$. The defining cubic gives the relation

$$z_2(1 + a_1x_2 - a_2x_2^2 + a_3z_2 - a_4x_2z_2 - a_6z_2^2) = x_2^3,$$

which shows that z_2 is asymptotic to x_2^3 and thus that $\left|\begin{smallmatrix} x_1 & z_1 \\ x_2 & z_2 \end{smallmatrix}\right|$ is asymptotic to $-x_2z_1$ and $\left|\begin{smallmatrix} x_2 & z_2 \\ x_0 & z_0 \end{smallmatrix}\right|$ is asymptotic to x_2z_0. (Here we say that two functions f and g are *asymptotic* if there is a function h on a neighborhood of the locus $c_2 = 0$ such that $f = gh$ and $h = 1$ when $c_2 = 0$). It follows that $s(\underline{a})(c_0, c_1, c_2)$ is asymptotic to $x_2^{-1}d(x)_0$, and this means that $s(\underline{a})$ has residue 1, as required.

We now see that $s(\underline{a})$ is a rigid section of $\Theta^3(\mathcal{I}(0))$, so that $f = s(\underline{a})/s(C/S)$ is an invertible function on $(C_{\text{reg}})^3_S$, whose restriction to S is 1. It follows that $f = 1$ on the open subscheme $p^{-1}S_{\text{ell}}$, which is dense in $(C_{\text{reg}})^3_S$, so $f = 1$ everywhere. Thus $s(\underline{a}) = s(C/S)$. □

References

[ABS64] Michael F. Atiyah, Raoul Bott, and Arnold Shapiro. Clifford modules. *Topology*, 3 suppl. 1:3–38, 1964.

[Ada76] J. Frank Adams. Primitive elements in the K-theory of BSU. *Quart. J. Math. Oxford Ser. (2)*, 27(106):253–262, 1976.

[Ada74] J. Frank Adams. *Stable Homotopy and Generalised Homology.* University of Chicago Press, Chicago, 1974.

[AS98] Matthew Ando and Neil P. Strickland. Weil pairings and Morava K-theory. 23 pp., To appear in Topology, 1998.

[Bre83] L. Breen. *Fonctions Théta et Théorème du Cube*, volume 980 of *Lecture Notes in Mathematics.* Springer–Verlag, 1983.

[BT89] Raoul Bott and Clifford Taubes. On the rigidity theorems of Witten. *J. Amer. Math. Soc.*, 2(1):137–186, 1989.

[Del75] Pierre Deligne. Courbes elliptiques: formulaire (d'après J. Tate). In *Modular Functions of One Variable III*, volume 476 of *Lecture Notes in Mathematics*, pages 53–73. Springer–Verlag, 1975.

[Dem72] Michel Demazure. *Lectures on p-divisible groups.* Springer-Verlag, Berlin, 1972. Lecture Notes in Mathematics, Vol. 302.

[DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs.* Masson & Cie, Éditeur, Paris, 1970. Avec un appendice *Corps de classes local* par Michiel Hazewinkel.

[DR73] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In *Modular Functions of One Variable II*, volume 349 of *Lecture Notes in Mathematics*, pages 143–316. Springer–Verlag, 1973.

[EKMM96] A. D. Elmendorf, I. Kriz, M. A. Mandell, and J. P. May. *Rings, Modules and Algebras in Stable Homotopy Theory*, volume 47 of *Amer. Math. Soc. Surveys and Monographs.* American Mathematical Society, 1996.

[Fra92] J. Franke. On the construction of elliptic cohomology. *Math. Nachr.*, 158:43–65, 1992.

[FS80] G. Frobenius and L. Stickelberger. Uber die Addition und Multiplication der elliptischen Functionen. *J. für die reine u. angewandte Math.*, 88:146–184, 1880. Reproduced in Frobenius, *Oeuvres Complètes*, Springer 1968.

[Gro72] *Groupes de monodromie en géométrie algébrique. I.* Springer-Verlag, Berlin, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim, Lecture Notes in Mathematics, Vol. 288.

[Har77] Robin H. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics.* Springer–Verlag, 1977.

[Haz78] Michiel Hazewinkel. *Formal Groups and Applications.* Academic Press, 1978.

[HBJ92] Friedrich Hirzebruch, Thomas Berger, and Rainer Jung. *Manifolds and modular forms.* Aspects of Mathematics, E20. Friedr. Vieweg & Sohn, Braunschweig, 1992. With appendices by Nils-Peter Skoruppa and by Paul Baum.

[HM98] M. J. Hopkins and M. Mahowald. Elliptic curves and stable homotopy theory II. in preparation, 1998.

[HMM98] M. J. Hopkins, M. Mahowald, and H. R. Miller. Elliptic curves and stable homotopy theory I. in preparation, 1998.

[Hop95] Michael J. Hopkins. Topological modular forms, the Witten genus, and the theorem of the cube. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*, pages 554–565, Basel, 1995. Birkhäuser.

[Hus75] Dale Husemoller. *Fibre Bundles*, volume 33 of *Graduate Texts in Mathematics.* Springer–Verlag, 1975.

[Jac] C. G. J. Jacobi. Formulae novae in theoria transcendentium ellipticarum fundamentales. *Crelle J. für die reine u. angewandte Math.*, 15:199–204. Reproduced in *Gesammelte Werke* Vol. I 335-341, Verlag von G. Reimer, Berlin 1881.

[Kat73] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350, Berlin, 1973. Springer.

[KM85] N. M. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*, volume 108 of *Annals of Mathematics Studies.* Princeton University Press, 1985.

[Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.

[Liu95] Kefeng Liu. On modular invariance and rigidity theorems. *J. Differential Geom.*, 41(2):343–396, 1995.

[LRS95] Peter S. Landweber, Douglas C. Ravenel, and Robert E. Stong. Periodic cohomology theories defined by elliptic curves. In *The Čech centennial (Boston, MA, 1993)*, volume 181 of *Contemp. Math.*, pages 317–337. Amer. Math. Soc., Providence, RI, 1995.

[MR81] Mark Mahowald and Nigel Ray. A note on the Thom isomorphism. *Proc. Amer. Math. Soc.*, 82(2):307–308, 1981.

[MM65] John W. Milnor and John C. Moore. On the structure of Hopf algebras. *Annals of Mathematics*, 81(2):211–264, 1965.

[Mor89] Jack Morava. Forms of K-theory. *Math. Z.*, 201(3):401–428, 1989.

[Mum65] David Mumford. Biextensions of formal groups. In *Arithmetic algebraic geometry (proceedings of Purdue conference).* Harper, 1965.

[Mum70] David Mumford. *Abelian Varieties*, volume 5 of *Tata institute of fundamental research series in mathematics.* Oxford University Press, 1970.

[Och87] S. Ochanine. Sur les genres multiplicatifs définis par des intégrals elliptiques. *Topology*, 26:143–151, 1987.

[Qui69] Daniel G. Quillen. On the formal group laws of unoriented and complex cobordism. *Bulletin of the American Mathematical Society*, 75:1293–1298, 1969.

[Qui71] Daniel G. Quillen. The spectrum of an equivariant cohomology ring, I and II. *Annals of Mathematics*, 94:549–602, 1971.

[Ros98] Ioanid Rosu. *Equivariant elliptic cohomology and rigidity.* PhD thesis, MIT, 1998.

[RW77] Douglas C. Ravenel and W. Stephen Wilson. The Hopf ring for complex cobordism. *Journal of Pure and Applied Algebra*, 9:241–280, 1977.

[Seg88] Graeme Segal. Elliptic cohomology. In *Séminaire Bourbaki 1987/88*, volume 161-162 of *Astérisque*, pages 187–201. Societe Mathematique de France, Février 1988.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer–Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics.* Springer–Verlag, New York, 1994.

[Sin68] William M. Singer. Connective fiberings over BU and U. *Topology*, 7, 1968.

[Str99a] Neil P. Strickland. Formal schemes and formal groups. In J.P. Meyer, J. Morava, and W.S. Wilson, editors, *Homotopy-invariant algebraic structures: in honor of J.M. Boardman*, Contemporary Mathematics. American Mathematical Society, 1999. 75 pp., To Appear.

[Str99b] Neil P. Strickland. Products on MU-modules. *Transactions of the American Mathematical Society*, 351:2569–2606, 1999.

[Tat74] John T. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.

[Wit87] Edward Witten. Elliptic genera and quantum field theory. *Comm. Math. Physics*, 109:525–536, 1987.

[Wit88] Edward Witten. The index of the Dirac operator in loop space. In P. S. Landweber, editor, *Elliptic Curves and Modular Forms in Algebraic Topology*, volume 1326 of *Lecture Notes in Mathematics*, pages 161–181, New York, 1988. Springer–Verlag.

Department of Mathematics, The University of Illinois at Urbana-Champaign, Urbana IL 61801, USA

E-mail address: `mando@math.uiuc.edu`

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: `mjh@math.mit.edu`

Department of Pure Mathematics, University of Sheffield, Sheffield S3 7RH, England

E-mail address: `N.P.Strickland@sheffield.ac.uk`