Constructing Elliptic Cohomology

Matthew Greenberg

Department of Mathematics and Statistics, McGill University

805 rue Sherbrooke Ouest, Montréal, Québec, H3A 2K6 Canada

July, 2002

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the degree of Master of Science

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisisitons et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 0-612-85790-5
Our file Notre référence
ISBN: 0-612-85790-5

Acknowledgement

There are many people to whom I owe a debt of thanks for their support over the last two years. First, I would like to sincerely acknowledge my supervisor Eyal Goren for suggesting I study elliptic cohomology and patiently guiding me through the mathematics involved. Even though he has, in my opinion, the busiest schedule of any professor I have met, he always found adequate time to oversee my studies and to share his knowledge and expertise with me. I took many excellent courses during my Masters program from which I learned a great deal. I would like to thank the professors of these courses for their dedication and time.

On a personal note I would like to thank my family and friends for putting up with my erratic mood and (I hope) occassional irritability over the past two years. In particular, I would like to thank my parents and sister for never cutting me off during my marathon complaining/venting sessions. Finally, I would like to thank Kristina for all of her support. I credit her intolerance of laziness and self pity for rescuing my motivation and work ethic on several occassions.

Institutionally, I would like to thank the Mathematics department at McGill University and the Natural Sciences and Engineering Research Council (NSERC) for their financial support.

Abstract

In 1986, Landweber, Ravenel, and Stong introduced a new family of generalized cohomology theories. As these theories are in a sense defined by elliptic curves, they were dubbed *elliptic cohomology theories.* In this thesis, we survey the mathematics behind the construction of elliptic cohomology. Topics treated include the theory of universal formal group laws and the Lazard ring, the formal group law of an elliptic curve, the group law (up-to-homotopy) on $\mathbb{CP}^\infty$, oriented and complex cobordism theories, the universal elliptic genus, and Landweber's exact functor theorem.

Résumé

En 1986, Landweber, Ravenel, et Stong ont introduits une nouvelle famille de théories cohomologique généralisés. Comme ces théories sont, d'une certaine manière, définies par des courbes elliptiques, elles furent appelées *théories de cohomologie elliptique*. Nous couvrons, dans cette thèse, les mathématiques soutenant la construction de la cohomologie elliptique. Les sujets traités incluent la théorie des lois de groupe formel universelles et l'anneau de Lazard, la loi de groupe formel d'une courbe elliptique, la loi de groupe (à homotopie près) sur $\mathbb{CP}^\infty$, les théories de cobordisme orienté et complexe, le genre elliptique universel, et le théorème du fonctor exact de Landweber.

Contents

Notation, in order of appearance

Page	Notation	Description
1	$\mathcal{G}_a$	formal additive group law
1	$\mathcal{G}_m$	formal multiplicative group law
3	$\mathrm{Hom}(F_1, F_2)$	formal group law homomorphisms from F_1 to F_2
5	$[m]_F$	formal multiplication-by-m in F
6	$\log_F$	logarithm of the formal group law F
23	$\mathrm{ht}\, F$	height of the formal group law F
24	$\mathcal{O}_{E,O}$	local ring of E at O
24	$\widehat{\mathcal{O}}_{E,O}$	the completion of $\mathcal{O}_{E,O}$ at its unique maximal ideal
24	$\widehat{\otimes}$	completed tensor product
26	$\mathrm{Hom}(E_1, E_2)$	elliptic curve isogenies from E_1 to E_2
27	$[m]_E$	multiplication-by-m map on E
31	$\wp(z, \Lambda)$	Weierstrass $\wp$-function of the lattice Λ
32	$\mathcal{H}$	Poincaré upper half plane
32	Λ_τ	the lattice $\mathbb{Z} + \mathbb{Z}\tau$
33	$\sigma(z)$	the elliptic function $-2(\wp(z) - e_3)/\wp'(z)$
34	$\mathrm{div}\, f$	divisor of the meromorphic function, f
42	$\mathbb{F}$	either $\mathbb{R}$ or $\mathbb{C}$
42	$\mathbb{FP}^n$	n-dimensional projective space over $\mathbb{F}$
42	$\mathbb{F}^\infty$	$\varinjlim_n \mathbb{F}^n$
42	$\mathbb{FP}^\infty$	$\varinjlim_n \mathbb{FP}^n$
42	$\mathrm{G}(n, \mathbb{F}^{n+k})$	Grassmann manifold of n-planes in $\mathbb{F}^{n+k}$

Page	Notation	Description
43	$\mathrm{G}^{\circlearrowleft}(n, \mathbb{R}^{n+k})$	oriented Grassmann manifold of oriented n-planes in $\mathbb{R}^{n+k}$
43	$\mathrm{G}(n, \mathbb{F}^{\infty})$	$\varinjlim_k \mathrm{G}(n, \mathbb{F}^{n+k})$
43	$\mathrm{G}^{\circlearrowleft}(n, \mathbb{R}^{\infty})$	$\varinjlim_k \mathrm{G}^{\circlearrowleft}(n, \mathbb{R}^{n+k})$
44	$\mathrm{H}^n(X, R)$	n-th cohomology group of X with coefficients in R
46	$B(\xi)$	base space of the vector bundle ξ
46	$E(\xi)$	total space of the vector bundle ξ
46	$\mathrm{Fib}_b\, \xi$	fibre of ξ over b
46	$\mathbf{VB}$	category of $\mathbb{F}$-vector bundles
46	$\mathbf{VB}_B$	category of $\mathbb{F}$-vector bundles on the base space B
47	$\gamma_{n,k}(\mathbb{F})$	tautological n-plane bundle over $\mathrm{G}(n, \mathbb{F}^{n+k})$
47	$\gamma_n(\mathbb{F})$	tautological n-plane bundle over $\mathrm{G}(n, \mathbb{F}^{\infty})$
49	$f^*\xi$	pullback by f of the bundle ξ
49	$\mathbf{VS}$	category of $\mathbb{F}$-vector spaces
55	$\mathrm{O}(n)$	group of $n \times n$ orthogonal matrices
55	$\mathrm{U}(n)$	group of $n \times n$ unitary martices
55	$[X, Y]$	homotopy classes of maps from X to Y
56	$\mathrm{BO}(n)$	classifying space for real n-plane bundles
56	$\mathrm{BU}(n)$	classifying space for complex n-plane bundles
59	$w_k(\xi)$	k-th Stiefel-Whitney class of the bundle ξ
61	$c_k(\xi)$	k-th Chern class of the bundle ξ
61	$p_k(\xi)$	k-th Pontryatin class of the bundle ξ
63	μ_X	fundamental homology class of the manifold X
63	$w_I[X]$	I-th Stiefel-Whitney number of X
64	$c_I[X]$	I-th Chern number of X
64	$p_I[X]$	I-th Pontryatin number of X
64	τ_X	tangent bundle of the manifold X
67	$\mathbb{HP}^n$	n-dimensional quaternionic projective space

Page	Notation	Description
68	$\star$	a one point space
72	Ω_*	unoriented bordism ring
74	Ω_*^{O}	oriented bordism ring
76	$T(\xi)$	Thom space of ξ
77	Ω_*^{U}	complex bordism ring
82	ΣX	reduced suspension of X
83	$\mathrm{MSO}^*(X)$	oriented cobordism ring of X
83	$\mathrm{MU}^*(X)$	complex cobordism ring of X
83	F^{MU}	formal group law of complex cobordism
87	F^{MSO}	formal group law of oriented cobordism
87	$\log_\varphi$	logarithm of the genus φ
88	ψ^{O}	universal elliptic oriented genus
88	ψ^{U}	universal elliptic complex genus
93	$\mathrm{SL}(2,\mathbb{Z})$	2×2 integral matrices with determinant 1
93	$\Gamma_0(2)$	2×2 integral matrices which are upper triangular modulo 2
95	$\mathrm{M}_k(\Gamma)$	modular forms of weight k for Γ
95	$\mathrm{M}_*(\Gamma)$	ring of modular forms for Γ
102	$\mathbf{j}$	multi-index

Introduction

In 1986, Landweber, Ravenel, and Stong introduced a new family of generalized cohomology theories called *elliptic cohomology theories*. This terminology is appropriate as these theories are in a sense defined by elliptic curves. In this thesis, we seek to survey some of the mathematics invloved in the construction of these elliptic cohomology theories.

At the moment, there is no intrinsic, geometric description of elliptic cohomology. It is defined by as a specialization of another generalized cohomology theory called *complex cobordism theory*. Both complex cobordism theory and the elliptic cohomology theories are examples of *complex-oriented cohomology theories*. These complex-oriented cohomology theories have *formal group laws* associated to them in a natural way. That the specialization of complex cobordism theory to the elliptic cohomology theories works relies heavily on properties of formal group laws of elliptic curves, which turn out to be the formal group laws associated to elliptic cohomology theories.

In Chapter 1, we discuss the basic theory of (1-dimensional, commutative) formal group laws, including Lazard's construction of a universal formal group law defined over the polynomial ring $\mathbb{Z}[u_2, u_3, \ldots]$.

In Chapter 2, we discuss how one may obtain a formal group law which represents the addition law on a given elliptic curve in a neighbourhood of its neutral element. We construct specific formal group laws corresponding to elliptic curves given by the equations $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and $y^2 = 1 - 2\delta x^2 + \varepsilon x^4$.

Having discussed instances where formal group laws appear in algebraic geometry, we turn our attention to formal group laws arising in topology. The appearance of formal group laws in topology is a consequence of the fact that $\mathbb{CP}^\infty$, the infinite-dimensional complex projective space, is a group-up-to-homotopy. This fact is proved in Chapter 3 using the theory of classifying spaces of vector bundles. Chapter 3 closes with a discussion of characteristic (Stiefel-Whitney, Chern, and Pontryagin) classes of vector bundles.

Chapter 4 begins with the definition of a generalized cohomology theory, and continues with a brief discussion of complex-oriented cohomology theories. Loosely speaking, these are generalized cohomology theories which behave well on the complex projective spaces $\mathbb{CP}^n$. We then explain how the group law up-to-homotopy on $\mathbb{CP}^\infty$ allows us to attach a formal group law to each complex-oriented cohomology theory. Next, we treat in some detail several important complex-oriented cohomology theories: *oriented cobordism* and *complex cobordism* theories. Our treatment of these includes geometric descriptions of the oriented and complex bordism rings. Complex cobordism theory is in a sense universal among complex-oriented cohomology theories. Its formal group law is universal. It therefore seems feasible to attempt the construction of other complex-oriented theories by somehow specializing complex cobordism.

This specialization process is discussed in Chapter 5. The notions of oriented and complex elliptic genera are introduced, and Landweber's condition under which a specialization of complex cobordism yields a generalized cohomology theory is stated. This condition is phrased in terms of formal group laws. We then use special properties of formal group laws of elliptic curves to verify that the particular specializations of complex cobordism yielding the elliptic cohomology theories works. We then proceed to discuss how the oriented and complex elliptic genera may be viewed as functions assigning modular forms to manifolds. We are also able to interpret the rings of coefficients of the elliptic cohomology theories as rings of modular forms.

In Appendix A, we generalize Lazard's construction of a 1-dimensional, universal formal group law over $\mathbb{Z}[u_2, u_3, \ldots]$ to the case of higher dimensions.

CHAPTER 1

One-dimensional formal group laws

1. Basic definitions

Let R be a commutative ring and let $R[\![x_1, \ldots, x_n]\!]$ denote the ring of formal power series in indeterminates $x_1 \ldots x_n$ with coefficients from R.

DEFINITION 1.1. A one-dimensional, commutative formal group law with coefficients from R (or more briefly, a formal group law defined over R), is a formal power series $F(x, y) \in R[\![x, y]\!]$ satisfying

(i) $F(x, F(y, z)) = F(F(x, y), z)$

(ii) $F(x, y) = F(y, x)$

(iii) $F(x, 0) = x$ and $F(0, y) = y$

(iv) there exists a power series $i(x) \in R[\![x]\!]$ such that $F(x, i(x)) = 0$.

The power series $i(x)$ of property (iv) is called the *formal inverse.*

Notice that if we write $F(x, y) = \sum_{m,n \geq 0} a_{mn} x^m y^n$, then properties (ii) and (iii) imply that $F(x, y)$ has the form

$$F(x, y) = x + y + \sum_{\ell \geq 1} a_{\ell\ell} x^\ell y^\ell + \sum_{n > m \geq 1} a_{mn}(x^m y^n + x^n y^m). \tag{1.1}$$

EXAMPLE 1.2. The *formal additive group law* is given by the power series $\mathcal{G}_a(x, y) = x + y$. The formal inverse is given by $i(x) = -x$.

EXAMPLE 1.3. The *formal multiplicative group law* is given by the power series $\mathcal{G}_m(x, y) = x + y + xy$. The formal inverse is given by $i(x) = -x + x^2 - x^3 + \cdots$. That $\mathcal{G}_m$ satisfies properties (i)-(iv) of Definition 1.1 is a routine verification.

2. Manufacturing groups subordinate to formal group laws

Formal group laws resemble "group laws without any group elements". Properties (i)-(iv) of Definition 1.1 assert (formal) associativity, commutativity, existence of 0, and existence of additive inverses, respectively.

Sometimes, it is possible to evaluate a formal group law on a collection of elements, turning that collection into a group. Let $F(x, y)$ be a formal group law with coefficients in R, and suppose A is a commutative, topological R-algebra such that for every $a, b \in A$, $F(a, b)$ and $i(a)$ converge. If we define new addition and inversion laws on A by

$$a +_F b = F(a, b) \text{ and } -_F a = i(a),$$

the fact that $(A, +_F, -_F)$ is an abelian group follows immediately from properties (i)-(iv) of Definition 1.1.

EXAMPLE 1.4. Let A be a commutative R-algebra and let $N(A)$ denote the collection of nilpotent elements of A. Then for any formal group law $F(x, y)$ with coefficients in R, and for any $a, b \in N(A)$, $F(a, b)$ and $i(a)$ exist and are in $N(A)$. Thus, the above construction may be applied to define a new group law $+_F$ on $N(A)$.

EXAMPLE 1.5. Let R be a complete local ring ($R = \mathbb{Z}_p$, for instance) with maximal ideal $\mathfrak{m}$, and let $F(x, y)$ be a formal group law with coefficients in R. For any $a, b \in \mathfrak{m}$, both $F(a, b)$ and $i(a)$ converge to an element of $\mathfrak{m}$, by the completeness of R. Thus, $F(x, y)$ induces a new group structure on $\mathfrak{m}$. This group will be denoted $\mathfrak{m}_F$. Notice that

$$\mathfrak{m}_F \cong \varprojlim_n (\mathfrak{m}/\mathfrak{m}^n)_F, \quad \text{and} \quad \mathfrak{m}/\mathfrak{m}^n = N(R/\mathfrak{m}^n).$$

3. Homomorphisms and Logarithms

DEFINITION 1.6. Let $F(x, y)$ and $G(x, y)$ be formal group laws with coefficients in R, and let A be an R-algebra. A *homomorphism* $\varphi : F \to G$ defined over A is a power series $\varphi(x) \in A[\![x]\!]$ such that $\varphi(F(x, y)) = G(\varphi(x), \varphi(y))$. We will say that φ

is an *isomorphism* (defined over A) if there exists a homomorphism $\psi : G \to F$, also defined over A, such that $\psi(\varphi(x)) = \varphi(\psi(x)) = x$. If $\varphi : F \to G$ and $\psi : G \to H$ are homomorphisms, then the composition of φ and ψ, $\psi\varphi : F \to H$ defined by $\psi\varphi(x) = \psi(\varphi(x))$ is a homomorphism from F to H. We say φ is *strict* if $\varphi(x) = x + \cdots$.

This definition is natural in the following sense. Suppose A is an R-algebra on which the formal group laws $F(x, y)$ and $G(x, y)$ can be imposed (in the sense of Section 2), yielding abelian groups A_F and A_G. Let $\varphi : F \to G$ be a homorphism defined over R with the property that for each $a \in A$, $\varphi(a)$ converges to an element of A. Then φ induces a homomorphism $\varphi_\sharp : A_F \to A_G$ of abelian groups by the rule $\varphi_\sharp(a) = \varphi(a)$. If $\psi\colon G \to H$ is another homomorphism of formal group laws, then we have the identity $(\psi\varphi)_\sharp = \psi_\sharp\varphi_\sharp$. Thus, if F and G are isomorphic formal group laws, then A_F and A_G are isomorphic abelian groups.

Let F and G be formal group laws defined over R and let $\mathrm{Hom}(F, G)$ be the set of homomorphisms from F to G. One can verify directly that the addition law $(\varphi(x), \psi(x)) \mapsto G(\varphi(x), \psi(x))$ endows the set $\mathrm{Hom}(F, G)$ with the structure of an abelian group. As usual, set $\mathrm{End}\, F = \mathrm{Hom}(F, F)$. One can show that $\mathrm{End}\, F$ has a ring structure where the addition operation is as above, and multiplication is given by composition of power series.

EXAMPLE 1.7 (Continuation of Example 1.4). Now that we have the appropriate notion of morphism, we observe that the correspondence $A \mapsto (N(A), +_F)$ of Example 1.4 can be viewed as a functor $\mathcal{F}$ from the category of R-algebras to the category of abelian groups. Suppose F and G are formal group laws defined over R, and $\varphi\colon F \to G$ is a homomorphism, and let $\mathcal{F}$ and $\mathcal{G}$ be the corresponding abelian group valued functors. Then φ induces a natural transformation $T_\varphi\colon \mathcal{F} \to \mathcal{G}$; for an R-algebra A, the map $a \mapsto \varphi(a)$ is a well defined homomorphism from $\mathcal{F}(A)$ to $\mathcal{G}(A)$. One can check that the transformation so defined is natural.

We can in fact show that *all* natural transformations between functors obtained in the above manner are induced by homomorphisms of formal group laws. Let

$T\colon \mathcal{F} \to \mathcal{G}$ be a natural transformation. We shall produce a homomorphism $\varphi\colon F \to G$ such that $T = T_\varphi$. Let $f\colon A \to B$ be a homomorphism of R-algebras. Then the naturality of T gives us a commutative diagram of the form

$$\begin{array}{ccc} \mathcal{F}(A) & \xrightarrow{T_A} & \mathcal{G}(A) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathcal{F}(B) & \xrightarrow[T_B]{} & \mathcal{G}(B). \end{array} \tag{1.2}$$

We construct a power series $\varphi(x) \in R[\![x]\!]$ such that $T_A(a) = \varphi(a)$, for each $a \in N(A)$. Let $A_n = R[x]/(x^n)$, and for $1 \le k < n$, define $\alpha_k^{(n)} \in R$ by the relations

$$T_{A_n}(x) \equiv \sum_{k=1}^{n-1} \alpha_k^{(n)} x^k \pmod{x^n}.$$

Let $\pi\colon A_{n+1} \to A_n$ be the unique R-algebra homomorphism sending x to x. Replacing A, B, and f in (1.2) by A_{n+1}, A_n, and π, respectively, one sees that $\alpha_k^{(n)} = \alpha_k^{(n+1)}$ when $1 \le k < n$. Letting $\alpha_k = \alpha_k^{(k+1)}$ and $\varphi(x) = \sum_{k\ge 1} \alpha_k x^k$, we have that $T_{A_n}(x) = \varphi(x)$, for all n.

Let B be an R-algebra, and let $b \in N(B)$. We claim that $T_B(b) = \varphi(b)$. Let $n \ge 1$ be such that $b^n = 0$. Then there exists a unique $f\colon A_n \to B$ sending x to b. By the naturality of T, we have

$$T_B(b) = T_B(f(x)) = f(T_{A_n}(x)) = f(\varphi(x)) = \varphi(f(x)) = \varphi(b).$$

Note that $f(\varphi(x)) = \varphi(f(x))$ since f is an R-algebra homomorphism and $\varphi(x)$ is a *polynomial* in the nilpotent element x of A_n.

It remains to show that φ is a homomorphism from F to G. For $n \ge 1$, define $R-$*algebras* $C_n = R[x,y]/(x^k y^{n-k} \mid k = 0, \ldots n)$. Computing in C_n, we see that

$$\varphi(F(x,y)) \equiv T_{C_n}(x +_F y) = T_{C_n}(x) +_G T_{C_n}(y) \equiv G(\varphi(x), \varphi(y)) \pmod{\text{degree } n}.$$

Thus, the identity $\varphi(F(x,y)) = G(\varphi(x), \varphi(y))$ holds in $R[\![x,y]\!]$, and we have produced a homomorphism φ such that $T = T_\varphi$.

Viewed slightly differently, we have essentially shown that the correspondence $F \mapsto \mathcal{F}$ embeds the category of formal group laws defined over R into the category of abelian group valued functors of R-algebras.

EXAMPLE 1.8. Let $F(x, y)$ be a formal group law with coefficients in R. For each integer m, we define a homomorphism $[m] : F \to F$ called the *formal multiplication-by-m* map. We define $[0](x) = 0$, $[m](x) = F(x, [m-1](x))$ for $m \geq 1$, and $[m](x) = i([-m](x))$ for $m \leq -1$. It is easy to verify that $[m]$ is in fact a homomorphism of formal group laws defined over R and that the map from $\mathbb{Z}$ to $\operatorname{End} F$ given by $m \mapsto [m]_F$ is a ring homomorphism.

If A is an R-algebra on which the formal group law $F(x, y)$ can be imposed yielding an abelian group A_F, the the induced map $[m]_\sharp$ is the usual multiplication-by-m map on A_F.

The following result, although trivial to prove, is important.

LEMMA 1.9. *For $m \in \mathbb{Z}$, $[m](x) = mx +$ (higher order terms).*

EXAMPLE 1.10. If $F(x, y)$ is a formal group law with coefficients in R, a ring of characteristic $p > 0$, then the *Frobenius map* $\varphi : F \to F$ defined by $\varphi(x) = x^p$ is a homomorphism of formal group laws defined over R.

EXAMPLE 1.11. Let R be a ring of characteristic 0 containing $\mathbb{Q}$ as a subring. Define $\log : \mathcal{G}_m \to \mathcal{G}_a$ by $x \mapsto \log(1 + x)$ where $\log(1 + x)$ is defined by the formal Taylor series

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots .$$

This in fact defines a homomorphism, as

$$\begin{aligned} \log(1 + \mathcal{G}_m(x, y)) &= \log[(1 + x)(1 + y)] \\ &= \log(1 + x) + \log(1 + y) \\ &= \mathcal{G}_a(\log(1 + x), \log(1 + y)). \end{aligned}$$

The log map is actually an isomorphism; one may similarly define an exponential $x \mapsto \exp x - 1$ map $x \mapsto \exp x - 1$ which acts as the inverse to log.

Example 1.11 can actually be generalized.

THEOREM 1.12. *Let R be a $\mathbb{Q}$-algebra, and let $F(x, y)$ be a formal group law with coefficients in R. Then there is a power series $f(x) \in R[\![x]\!]$ of the form $f(x) = x + \cdots$, such that*

$$f(F(x, y)) = f(x) + f(y).$$

PROOF. Let

$$f(x) = \int_0^x \frac{dt}{F_2(t, 0)} \tag{1.3}$$

where $F_2(x, y) = \partial F/\partial y$. That $f(x)$ has leading term x is immediate from equation (1.3). Let $w(x, y) = f(F(x, y)) - f(x) - f(y)$. We want to show that $w = 0$. Differentiating the identity $F(F(x, y), z) = F(x, F(y, z))$ with respect to z and evaluating the derivative at $z = 0$, we get

$$F_2(F(x, y), 0) = F_2(x, F(y, 0))F_2(y, 0). \tag{1.4}$$

On the other hand,

$$\begin{aligned} \frac{\partial w}{\partial y} &= f'(F(x, y))F_2(x, y) - f'(y) \\ &= \frac{F_2(x, y)}{F_2(F(x, y), 0)} - \frac{1}{F_2(y, 0)} \quad \text{(by Equation 1.3)} \\ &= 0 \qquad\qquad\qquad\qquad\quad \text{(by Equation 1.4).} \end{aligned}$$

Symmetrically, $\partial w/\partial x = 0$, so w is constant. Noting that $w(0, 0) = 0$, the proof is complete. □

NOTATION 1.13. We will denote the power series $f(x)$ of Theorem 1.12 by $\log_F(x)$.

COROLLARY 1.14. *Let $F(x, y)$ be a formal group law with coefficients in R, a ring of characteristic 0. Then F is strictly isomorphic to $\mathcal{G}_a$ over $R \otimes \mathbb{Q}$.*

PROOF. By the previous theorem, $\log_F : F \to \mathcal{G}_a$ is a strict isomorphism. □

4. Universal formal group laws

Let R and S be rings and $\varphi : R \to S$ be a ring homomorphism. Then φ induces a map $\varphi_* : R[\![x, y]\!] \to S[\![x, y]\!]$ by applying φ to each coefficient of a given power series in $R[\![x, y]\!]$.

DEFINITION 1.15. Let R be a ring and A be an R-algebra. A *universal formal group law over A relative to the base ring R* is a formal group law $F^u(x, y)$ with coefficients in A such that for any R-algebra B and formal group law $G(x, y)$ defined over B, there is a unique R-algebra homomorphism $\varphi : A \to B$ such that $\varphi_* F^u(x, y) = G(x, y)$.

Suppose that $F_1^u(x, y)$ and $F_2^u(x, y)$ formal group laws defined over R-algebras A_1 and A_2, respectively. Further, suppose that $F_1^u(x, y)$ and $F_2^u(x, y)$ are both universal relative to the base ring R. By the universality of F_1^u and F_2^u, there exist unique R-algebra homomorphisms $\varphi\colon A_1 \to A_2$ and $\psi\colon A_2 \to A_1$ such that $\varphi_* F_1^u = F_2^u$ and $\psi_* F_2^u = F_1^u$. The standard argument shows that φ and ψ are mutually inverse isomorphisms. That is, the pair $(F^u(x, y), A)$ is unique, up to unique isomorphism.

PROPOSITION 1.16. *Let R be a ring. Then there is an R-algebra L_R and a universal formal group law over L_R, relative to the base ring R.*

PROOF. We construct an R-algebra L_R and a formal group law $F^{R,u}(x, y)$ over L_R, universal relative to the base ring R. Let $L'_R = R[\alpha_{mn} \mid m, n \geq 0]$ where the α_{mn} are indeterminates. Let $F(x, y) = \sum_{m,n \geq 0} \alpha_{mn} x^m y^n \in L'_R[\![x, y]\!]$. To say that $F(x, y)$ is a formal group law is to say that the coefficients α_{mn} satisfy a collection of *polynomial* identities $P_\beta(\{\alpha_{mn}\})$, β running over some index set, coming from the associativity and commutativity axioms. Let I be the ideal of L'_R generated by the $P_\beta(\{\alpha_{mn}\})$, $L_R = L'_R/I$ and $\pi : L'_R \to L_R$ be the canonical projection. We claim that $F^{R,u}(x, y) = \pi_* F(x, y)$ is a universal formal group law over L_R. Let A be an R-algebra

and $G(x,y) = \sum_{m,n\geq 0} b_{mn}x^m y^n$ be a formal group law with coefficients in A. Define an R-algebra homomorphism $\varphi' : L'_R \to A$ by $\varphi'(\alpha_{mn}) = b_{mn}$. As $G(x,y)$ is a formal group law, the b_{mn} satisfy the identities $P_\beta(\{b_{mn}\})$. Thus, $I \subseteq \operatorname{Ker}\varphi'$, and φ' induces an R-algebra homomorphism $\varphi : L_R \to A$ which satisfies $\varphi_* F^{R,u}(x,y) = G(x,y)$. The uniqueness of the map φ is a consequence of the fact that the set $\{\pi(\alpha_{mn})\}$ generates L_R. □

The ring L_R (unique up to R-algebra isomorphism) is called the *Lazard ring for R-algebras*, after M. Lazard, one of the originators of the theory of formal group laws. The Lazard ring for $\mathbb{Z}$-algebras will be refered to simply as the Lazard ring and denoted by L.

The following remarkable theorem, which we prove in the next section, determines the isomorphism class of L. This theorem is due to Lazard, see [**22**].

THEOREM 1.17. *There exists a universal formal group law (relative to the base ring $\mathbb{Z}$) defined over the polynomial ring $\mathbb{Z}[u_2, u_3, \ldots]$.*

COROLLARY 1.18. *Let R be any ring. Then there exists a universal formal group law, relative to the base ring R, defined over the ring $R[u_2, u_3, \ldots] \cong L \otimes_{\mathbb{Z}} R$.*

PROOF. Let $F^u(x,y)$ a universal formal group law defined over $\mathbb{Z}[u_2, u_3, \ldots]$. Let $h : \mathbb{Z}[u_2, u_3, \ldots] \to R[u_2, u_3, \ldots]$ be the unique ring homomorphism fixing each u_i and define $F^{R,u}(x,y) = h_* F^u(x,y)$. We claim that $F^{R,u}(x,y)$ is universal formal group law relative to the base ring R. Let $G(x,y)$ be a formal group law defined over an R-algebra A. By the universality of the formal group law $F^u(x,y)$, there exists a unique ring homomorphism $\varphi : \mathbb{Z}[u_2, u_3, \ldots] \to A$ such that $G(x,y) = \varphi_* F^u(x,y)$. Let $\overline{\varphi}$ be the unique R-algebra homomorphism from $R[u_2, u_3, \ldots]$ into A such that $h\overline{\varphi} = \varphi$. Then it is clear that $\overline{\varphi}_* F^{R,u}(x,y) = G(x,y)$. Suppose ψ: $R[u_2, u_3, \ldots] \to A$ was another R-algebra homomorphism such that $\psi_* F^{R,u} = G$. Then $(\psi h)_* F^u = \psi_* h_* F^u = \psi_* F^{R,u} = G$. As φ is the unique ring homomorphism with that property,

we have $\psi h = \varphi$. It thus follows from the uniqueness property of $\overline{\varphi}$ that $\psi = \overline{\varphi}$. Therefore, $\overline{\varphi}$ is the unique R-algebra homomorphism such that $\overline{\varphi}_* F^{R,u} = G$. □

REMARK 1.19. Using logarithms, it is easy to show directly that $L_{\mathbb{Q}}$ is isomorphic to $\mathbb{Q}[u_2, u_3, \dots]$. Let $F(x, y)$ be the formal group law over $\mathbb{Q}[u_2, u_3, \dots]$ with logarithm $f(x) = x + u_2 x^2 + u_3 x^3 + \cdots$. We claim that $F(x, y)$ is universal with respect to the base ring $\mathbb{Q}$. To see this, let $G(x, y)$ be a formal group law defined over a $\mathbb{Q}$-algebra A. Let $g(x) = x + b_2 x^2 + b_3 x^3 + \cdots$ be its logarithm and note that $g(x)$ is also defined over A (as A is a $\mathbb{Q}$-algebra). Then the $\mathbb{Q}$-algebra homomorphism $\varphi : \mathbb{Q}[u_2, u_3, \dots] \to A$ defined by $\varphi(u_i) = b_i$, $i \geq 2$, is clearly the unique map sending $F(x, y)$ into $G(x, y)$. This observation may serve to motivate Theorem 1.17.

5. Structure of the Lazard Ring

Our ultimate goal in this section is to prove Theorem 1.17, that the Lazard ring, L, is isomorphic to $\mathbb{Z}[u_2, u_3, \dots]$. We do this by constructing a universal formal group law over $\mathbb{Z}[u_2, u_3, \dots]$. The material in this section is from [**22**]. Other treatments are given in [**23**], [**1**, Chapter II, §7], and [**34**, Appendix 2]. A more explicit method for constructing universal formal group laws over $\mathbb{Z}[u_2, u_3, \dots]$ is given in [**15**, Ch. I]

To facilitate this construction, we introduce more primitive structures – formal group law buds of order n (more briefly, n-buds). An *n-bud* is simply a formal power series which satisfies the axioms of a formal group law, modulo degree $n+1$. We will show that for each $n \geq 2$, one may construct (inductively) a universal n-bud $F_n(x, y)$ over the ring $\mathbb{Z}[u_2, \dots, u_n]$. This construction can be carried out in such a way that $F_{n+1}(x, y)$ extends $F_n(x, y)$, so that the limit $F(x, y) = \lim_{n \to \infty} F_n(x, y)$ make sense. $F(x, y)$ is our universal group law defined over $\mathbb{Z}[u_2, u_3, \dots]$.

The key tool in our arguments is a result known as the Lazard Comparison Lemma, stated below as Theorem 1.25. This lemma regulates how the process of extending an n-bud can proceed.

5.1. Buds.

DEFINITION 1.20. Let R be a ring and let $F(x,y) \in R[\![x,y]\!]$ and $n \geq 1$. We say that $F(x,y)$ is a *formal group law bud*[1] *of order* n defined over R (or briefly, an n-bud) if $F(x,y)$ satisfies the defining properties of a formal group law, mod degree $n+1$. That is,

(i) $F(x,0) = x$ and $F(0,y) = y$,

(ii) $F(x,y) \equiv F(y,x) \pmod{\text{degree } n+1}$,

(iii) $F(F(x,y),z) \equiv F(x,F(y,z)) \pmod{\text{degree } n+1}$.

A formal group law $G(x,y)$ is an n-bud, for any n. We often think of an n-bud as a polynomial of degree n by ignoring terms of higher degree. Let $F(x,y)$ and $G(x,y)$ be m and n-buds, respectively, with $m < n$. We say that $G(x,y)$ extends $F(x,y)$ if $F(x,y) \equiv G(x,y) \pmod{\text{degree } m+1}$.

Most of the notions which we have discussed for formal group laws have natural bud analogues. In particular, we have the notion of a *universal* n*-bud.* We say that an n-bud $F_n^u(x,y)$ defined over a ring R is universal if for any n-bud $G(x,y)$ defined over a ring S, there is a unique ring homomorphism $\varphi\colon R \to S$ such that

$$G(x,y) \equiv \varphi_* F_n^u(x,y) \pmod{\text{degree } n+1}.$$

Our strategy for constructing a universal formal group law is as follows. We construct inductively a sequence F_n^u of universal n-buds, where F_n^u is defined over a ring A_n. This construction is performed in such a way that $A_n \subseteq A_{n+1}$ and F_{n+1}^u extends F_n^u. Consequently, the limit $F^u(x,y) = \lim_{n\to\infty} F_n^u(x,y)$ exists and is a universal formal group law defined over the ring $A = \varinjlim A_n$. For suppose G is a formal group law defined over a ring B. Since G may be viewed as an n-bud for each n, there exist unique maps $\varphi_n\colon A_n \to B$ such that $(\varphi_n)_* F_n^u \equiv G \pmod{\text{degree } n+1}$. The map φ_{n+1} extends φ_n by the uniqueness of φ_n. Therefore, we may let $\varphi = \lim_{n\to\infty} \varphi_n\colon A \to B$. If is clear from its construction that $\varphi_* F^u = G$.

[1] *French: bourgeon*

To successfully execute this strategy, we must first describe the extension process. To ease the notation, let

$$\Delta F(x,y,z) = F(F(x,y),z) - F(x,F(y,z)),$$

and $\Delta_k F$ be the homogeneous component of ΔF of degree k.

LEMMA 1.21. *Let $F(x,y)$ be an n-bud over R. Then $F(x,y)$ can be extended to an $(n+1)$-bud over R if and only if there exists a homogeneous polynomial $H(x,y) \in R[x,y]$ of degree $n+1$ such that $\delta H = \Delta_{n+1}F(x,y,z)$, where*

$$\delta H = H(y,z) - H(x+y,z) + H(x,y+z) - H(x,y).$$

PROOF. We may assume that $F(x,y)$ is a polynomial of degree n. $F(x,y)$ can be extended to an $(n+1)$-bud if and only if we can find a symmetric polynomial $H(x,y)$, homogeneous of degree $n+1$, such that $\Delta_{n+1}(F+H) = 0$. Set $F'(x,y) = F(x,y) + H(x,y)$. A direct computation reveals that

$$\Delta_{n+1}F'(x,y,z) = \Delta_{n+1}F(x,y,z) - \delta H(x,y,z).$$

The lemma follows. □

Let Q be an $(n-1)$-bud, and suppose F and G are n-buds extending Q. Must F and G be related in any nice way? The following corollary to Lemma 1.21 answers this question affirmatively; it describes the restrictions involved in the extension process. This result will be refined later.

COROLLARY 1.22. *Let F and G be n-buds defined over a ring R with $F(x,y) \equiv G(x,y)$ (mod degree n). Then there exists a homogeneous polynomial $H(x,y) \in R[x,y]$ of degree n satisfying*

(i) $\delta H(x,y,z) = H(y,z) - H(x+y,z) + H(x,y+z) - H(x,y) = 0$,

(ii) $H(x,y) = H(y,x)$,

such that

$$F(x,y) \equiv G(x,y) + H(x,y) \pmod{\text{degree } n+1}.$$

PROOF. View $G(x,y)$ as an $(n-1)$-bud. Since $F(x,y)$ is an n-bud extending $G(x,y)$, Lemma 1.21 asserts the existence of a homogeneous polynomial $H(x,y) \in R[x,y]$ of degree n with

$$F(x,y) \equiv G(x,y) + H(x,y) \pmod{\text{degree } n+1}$$

and $\delta H = \Delta_n G$. But since $G(x,y)$ is an n-bud, $\Delta_n G = 0$. The above congruence also shows that $H(x,y) = H(y,x)$. This completes the proof. □

DEFINITION 1.23. We say that a homogeneous polynomial H satisfies *Lazard's conditions* if H satisfies conditions (i) and (ii) in the statement of Corollary 1.22.

We wish to prove a result, due to Lazard, which describes completely (and simply!) all polynomials which satisfy Lazard's conditions. This result gives us the control we need to proceed with our construction of universal n-buds and formal group laws. We treat the one-dimensional and N-dimensional cases separately.

5.2. The Lazard comparison lemma. In this section, we give a complete description of all polynomials $H(x,y)$ satisfying Lazard's conditions. This will allow us to deduce the Lazard Comparison Lemma.

Let $\nu(n)$ be p if n is a power of p, and 1 otherwise. For $n \geq 1$, we define the polynomials

$$B_n(x,y) = (x+y)^n - x^n - y^n,$$
$$C_n(x,y) = \frac{1}{\nu(n)} B_n(x,y) = \frac{1}{\nu(n)}[(x+y)^n - x^n - y^n].$$

THEOREM 1.24. *Let $H(x,y) \in R[x,y]$ be a homogeneous polynomial of degree n satisfying Lazard's conditions. The there exists some $\alpha \in R$ such that*

$$H(x,y) = \alpha C_n(x,y).$$

Combining this result with Corollary 1.22, we obtain the following pleasing result.

THEOREM 1.25 (1-Dimensional Lazard Comparison Lemma). *Let $F(x,y)$ and $G(x,y)$ be n-buds over R with $F(x,y) \equiv G(x,y)$* (mod degree n). *Then there exists some $a \in R$ with*

$$F(x,y) \equiv G(x,y) + aC_n(x,y) \pmod{\text{degree } n+1}.$$

The proof of Theorem 1.24 which we give is due to Fröhlich, [**12**, Chapter 3, §1]. In this proof, most of the computations take place under the assumption that the ring R is in fact a field. The characteristic zero case is easy; the case of a field of positive characteristic requires a bit more analysis.

Let H be a homogeneous polynomial of degree n; write

$$H(x,y) = \sum_{\ell=0}^{n} a_\ell x^\ell y^{n-\ell}.$$

It is easy to check that H satisfies Lazard's conditions if and only if $a_\ell = a_{n-\ell}$, $a_0 = a_n = 0$, and for any i, j, $k > 0$ with $i+j+k = n$, we have

$$a_{i+j}\binom{i+j}{j} = a_{j+k}\binom{j+k}{k}. \tag{1.5}$$

We derive a useful formula. Suppose H satisfies Lazard's conditions. Then setting $i = 1$ and $k = n-1-j$ in (1.5), we see that

$$a_{1+j}(1+j) = a_1\binom{n-1}{j}, \tag{1.6}$$

for $j = 1, \ldots, n-2$.

5.2.1. *Fields of characteristic zero.* Theorem 1.24 can be deduced easily in the case where $R = F$, a field of characteristic zero. Let H be as above. Equation (1.6) (with $\ell = j+1$) implies that for $\ell = 0, \ldots, n-1$,

$$a_\ell = \frac{a_1}{\ell}\binom{n-1}{\ell-1} = \frac{a_1}{n}\binom{n}{\ell}. \tag{1.7}$$

Thus, $H = \frac{a_1}{n}C_n$, so verifying the theorem for fields of characteristic zero.

5.2.2. *Fields of positive characteristic.* Let $R = F$, a field of characteristic $p > 0$, and let H be as above, satisfying Lazard's conditions. The following observation about the polynomial C_n, modulo p, is crucial.

LEMMA 1.26. *Let $m \geq 2$. Then*

$$C_{pm}(x, y) \equiv C_m(x^p, y^p) \pmod{p}.$$

PROOF. First, suppose m is not a power of p. Then $C_{mp} = B_{mp}$ and $C_m = B_m$. Therefore, working modulo p, we have

$$\begin{aligned} B_{mp}(x, y) &= (x + y)^{pm} - x^{pm} - y^{pm} \\ &\equiv (x^p + y^p)^m - (x^p)^m - (y^p)^m \\ &= B_m(x^p, y^p). \end{aligned}$$

It remains to show that for $r \geq 2$, the congruence

$$C_{p^r}(x, y) \equiv C_{p^{r-1}}(x^p, y^p) \pmod{p}$$

holds. We have

$$\begin{aligned} B_{p^{r-1}}(x^p, y^p) &= [(x + y)^p - B_p(x, y)]^{p^{r-1}} - x^{p^r} - y^{p^r} \\ &= B_{p^r}(x, y) + \sum_{k=1}^{p^{r-1}} (-1)^k \binom{p^{r-1}}{k} B_p(x, y)^k (x + y)^{p(p^{r-1}-k)}. \end{aligned}$$

As $r \geq 2$, the binomial coefficient $\binom{p^{r-1}}{k}$ is divisible by p, for $k = 1, \ldots, p^{r-1}$. Also, each coefficient of $B_p(x, y)$ is divisible by p. Therefore,

$$B_{p^r}(x, y) \equiv B_{p^{r-1}}(x^p, y^p) \pmod{p^2}.$$

Dividing by $p = \nu(p^r) = \nu(p^{r-1})$, we obtain the desired congruence. □

In light of the above lemma, the following lemma must hold if Theorem 1.24 does.

LEMMA 1.27. *Let H be a homogeneous polynomial over F of degree pm which satisfies Lazards conditions. Then there exists a homogeneous polynomial h over F of degree m such that*

$$H(x,y) = h(x^p, y^p).$$

Further, h satisfies Lazard's conditions.

PROOF. Write

$$H(x,y) = \sum_{i=0}^{pm} a_i x^i y^{pm-i}.$$

Suppose $p \nmid i$; we will show that $a_i = 0$. Write $i = rp + s$ where $1 \leq s \leq p-1$. Since $a_i = a_{pm-i}$, we may assume without loss of generality that $r \geq 1$. The polynomial H satisfies Lazard's conditions, so setting $i = rp$, $j = s$, and $k = p(m-r)$,

$$a_{rp+s}\binom{rp+s}{s} = a_{p(m-r)}\binom{p(m-r)}{s}.$$

As $1 \leq s \leq p-1$, the binomial coefficient $\binom{p(m-r)}{s}$ is divisible by p. On the other hand,

$$\binom{rp+s}{s} = \frac{(rp+s)(rp+s-1)\cdots(rp+1)}{s(s-1)\cdots 1}$$

is evidently not divisible by p. Therefore, we must have $a_i = a_{rp+s} = 0$. Consequently, h exists and is given by the formula

$$h(x,y) = \sum_{i=1}^{m} a_{pi} x^i y^{m-i}.$$

To say that h satisfies Lazard's conditions is to say that the coefficients a_{pi} satisfy various identities. That these identities are satisfied follows from the fact that the coefficients of H satisfy those identities. □

We may now prove Theorem 1.24 for $R = F$, a field of characteristic $p > 0$. We will initially consider several special cases. Assume first that $p \nmid n$. Let $\ell \in \{1, \ldots, n-1\}$.

If $p \nmid \ell$, then equation (1.7) is still valid. If $p \mid \ell$, then as we assume $p \nmid n$, we must have $p \nmid n - \ell$. Thus, by equation (1.7) with ℓ replaced by $n - \ell$, we have

$$a_\ell = a_{n-\ell} = \frac{a_1}{n}\binom{n}{n-\ell} = \frac{a_1}{n}\binom{n}{\ell}.$$

Therefore, in the case $p \nmid n$, we still have $H = \frac{a_1}{n}C_n$.

The final special case we consider is the case $n = p$. In this case, for each $\ell = 1, \ldots, n-1$, we have $p \nmid i$, so

$$a_\ell = \frac{a_1}{i}\binom{n-1}{i-1}.$$

Therefore,

$$H(x,y) = a_1 \sum_{\ell=1}^{n-1} \frac{1}{\ell}\binom{n-1}{\ell-1} x^\ell y^{n-\ell} = a_1 \widetilde{C}_n(x,y),$$

where the polynomial $\widetilde{C}_n$ is defined by the above equation. It is clear that $\widetilde{C}_n$ satisfies Lazard's conditions.

It follows from our argument that any homogeneous polynomial of degree n defined over F which satisfies Lazard's conditions is a multiple of $\widetilde{C}_n$. Thus, in particular, $C_n = \beta\widetilde{C}_n$ for some $\beta \in F$. We conclude that $H = a_1\beta^{-1}C_n$.

For the remaining case $n = mp$, with $m \geq 2$, we proceed by induction. By Lemma 1.27, there is a homogeneous polynomial h of degree $m = n/p$ satisfying Lazard's conditions such that $H(x,y) = h(x^p, y^p)$. But by induction, there is some $\gamma \in F$ such that $h = \alpha C_m$. An application of Lemma 1.26 gives $C_n(x,y) = C_m(x^p, y^p)$ in F. Thus, we have $H = \alpha C_n$, completing the argument.

5.2.3. *Completion of the proof: General ring R.* Let R be a ring and let H be a homogeneous polynomial over R of degree n which satisfies Lazard's conditions. Notice that Lazard's conditions involve the multiplicative structure of R only to the extent of its $\mathbb{Z}$-module structure. We thus treat H as a "polynomial over R^+", the additive group of R, where by definition, a polynomial (in two variables) over an abelian group A is an element of $A \otimes \mathbb{Z}[x,y]$.

We translate Theorem 1.24 into the language of polynomials over abelian groups so that we may invoke the structure theory of finitely generated abelian groups.

THEOREM 1.28. *Let H be a homogeneous polynomial of degree n over an abelian group A which satisfies Lazard's conditions. Then there is some $\alpha \in A$ such that $H = \alpha C_n$.*

REMARK 1.29. Note that since C_n has integer coefficients, the expression αC_n makes sense in the abelian group $A \otimes \mathbb{Z}[x, y]$.

PROOF. Since H is defined over the subgroup of A generated by its coefficients, we may assume A is finitely generated.

Since the theorem holds for polynomials defined over $\mathbb{Q}$, and the polynomials C_n are primitive polynomials with coefficients in $\mathbb{Z}$, the theorem holds for polynomials defined over $\mathbb{Z}$. That it also holds for polynomials defined over $\mathbb{Z}/p^r\mathbb{Z}$ follows from the following lemma.

LEMMA 1.30. *Let H be a homogeneous polynomial of degree n defined over the abelian group $\mathbb{Z}/p^r\mathbb{Z}$. Suppose H satisfies Lazard's conditions. Then there exists some $\alpha \in \mathbb{Z}/p^r\mathbb{Z}$ such that $H = \alpha C_n$.*

PROOF. We proceed by induction on r. The $r = 1$ case holds by the above lemma, as $\mathbb{Z}/p\mathbb{Z}$ is a field. Suppose the conclusion of the lemma holds for r, that is,

$$H(x, y) \equiv \alpha C_n(x, y) + p^r K(x, y) \pmod{p^{r+1}}.$$

Writing this congruence as

$$p^r K(x, y) \equiv H(x, y) - \alpha C_n(x, y) \pmod{p^{r+1}},$$

it is evident that K satisfies Lazard's conditions, modulo p. Thus, we may find some β such that

$$K(x, y) \equiv \beta C_n(x, y) \pmod{p}.$$

Therefore,

$$H(x,y) \equiv (\alpha + p^r\beta)C_n(x,y) \pmod{p^{r+1}},$$

completing the proof. □

It is obvious that if the theorem holds for abelian groups A and B, it also holds for their direct sum. Therefore, by invoking the structure theory of finitely generated abelian groups, we are done. □

5.3. Construction of a universal, one-dimensional formal group law. The following lemma describes the inductive construction of universal formal group law buds of order n, defined over $\mathbb{Z}[u_2, \ldots, u_n]$. By a limiting process, this can be extended to construction of a universal formal group law over the ring $\mathbb{Z}[u_2, u_3, \ldots]$. We introduce the shorthand

$$A = \mathbb{Z}[u_2, u_3, \ldots], \quad A_n = \mathbb{Z}[u_2, \ldots, u_n] \quad \text{for } n \geq 2.$$

LEMMA 1.31. *One may construct two sequences of power series, $F_n(x,y)$ and $f_n(x)$, satisfying the following conditions for all $n \geq 2$:*

(i) $F_n(x,y) \in A_n[\![x,y]\!], \quad f_n(x) \in (A_n \otimes \mathbb{Q})[\![x]\!]$

(ii) $F_n(x,y) \equiv F_{n+1}(x,y)$ *and* $f_n(x) \equiv f_{n+1}(x) \pmod{\text{degree } n+1}$

(iii) $f_n(F_n(x,y)) \equiv f_n(x) + f_n(y) \pmod{\text{degree } n+1}$

(iv) $F_n(x,y) - u_n C_n(x,y) \in A_{n-1}[\![x,y]\!]$

REMARK 1.32. Conditions (ii) and (iii) say that $F_n(x,y)$ is an increasing sequence of formal group law buds with given by the increasing sequence of "logarithm buds" $f_n(x)$ (by 'increasing', we mean that the $(n+1)$-st series extends the n-th). The purpose of condition (iv) is to ensure that $F(x,y)$ is "free enough" to satisfy the universality property.

PROOF. We proceed by induction on n. Define

$$F_2(x,y) = x + y + u_2xy, \quad f_2(x,y) = x - \frac{u_2}{2}x^2.$$

One may show directly that $F_2(x,y)$ and $f_2(x,y)$ satisfy (i)-(iv).

Now assume we have constructed $F_2(x,y),\dots,F_n(x,y)$ and $f_2(x),\dots,f_n(x)$ satisfying (i)-(iv). We may assume that each $F_r(x,y)$ and $f_r(x)$, $2 \le r \le n$, is a polynomial of (total) degree r.

Let $\Phi_n(x,y)$ be the formal group law with logarithm $f_n(x)$, that is,

$$\Phi_n(x,y) = f_n^{-1}(f_n(x) + f_n(y)). \tag{1.8}$$

By (iii) and our assumption that $F_n(x,y)$ is a polynomial of degree n,

$$\Phi_n(x,y) \equiv F_n(x,y) + H(x,y) \pmod{\text{degree } n+2}, \tag{1.9}$$

where $H(x,y)$ is the homogeneous component $\Phi_n(x,y)$ of degree $n+1$. By Lemma 1.21,

$$\delta H(x,y,z) = \Delta_{n+1}F(x,y,z) \in A_n[x,y,z].$$

From the fact that $\Phi_n(x,y)$ is a formal group law, it follows that, that $H(x,y) = H(y,x)$. Although $H(x,y)$ may not be defined over A_n (Φ_n is defined over $A_n \otimes \mathbb{Q}$, not necessarily over A_n), we may find a positive integer k such that $K(x,y) := kH(x,y)$ has coefficients in A_n. Let $\overline{A}_n = A_n/kA_n$, and let $\overline{K}(x,y)$ denote the image of $K(x,y)$ in $\overline{A}_n$. From the above discussion, it follows that $\delta\overline{K}(x,y,z) = 0$ and $\overline{K}(x,y) = \overline{K}(y,x)$. Thus, by Theorem 1.24, we may find some $\overline{a} \in \overline{A}_n$ with

$$\overline{K}(x,y) = \overline{a}C_{n+1}(x,y).$$

Let $a \in A_n$ be a lift of $\overline{a}$. Then the above relation says that there exists some $H'(x,y) \in A_n[x,y]$ with

$$kH(x,y) = aC_{n+1}(x,y) + kH'(x,y). \tag{1.10}$$

Define $F_{n+1}(x,y)$ and $f_{n+1}(x)$ by

$$F_{n+1}(x,y) = F_n(x,y) + H'(x,y) + u_{n+1}C_{n+1}(x,y), \tag{1.11}$$

$$f_{n+1}(x) = f_n(x) - \frac{1}{\nu(n+1)}(u_{n+1} - \frac{a}{k})x^{n+1}. \tag{1.12}$$

It is clear that with the above definitions, F_{n+1} and $f_{n+1}(x)$ satisfy conditions (i), (ii), and (iv) of the lemma. It remains to verify (iv):

Let $\beta = u_{n+1} - a/k$. Combining (1.9), (1.10), and (1.11) we see that

$$F_{n+1}(x,y) \equiv \Phi_n(x,y) + \beta C_{n+1}(x,y) \pmod{\text{degree } n+2}. \tag{1.13}$$

Replacing x by $F_{n+1}(x,y)$ in (1.12), we get

$$f_{n+1}(F_{n+1}(x,y)) = f_n(F_{n+1}(x,y)) - \frac{\beta}{\nu(n+1)} F_{n+1}(x,y)^{n+1}. \tag{1.14}$$

Computing (mod degree $n+2$), we see that

$$\begin{aligned} f_n(F_{n+1}(x,y)) &\equiv f_n(\Phi_n(x,y) + \beta C_{n+1}(x,y)) && \text{by (1.13)} \\ &\equiv f_n(\Phi_n(x,y)) + \beta C_{n+1}(x,y) \\ &\equiv f_n(x) + f_n(y) + \beta C_{n+1}(x,y) && (1.15) \end{aligned}$$

$$\begin{aligned} \text{and } F_{n+1}(x,y)^{n+1} &\equiv (x+y)^{n+1} \\ &= x^{n+1} + y^{n+1} + B_{n+1}(x,y). && (1.16) \end{aligned}$$

Combining (1.14), (1.15), and (1.16), we have, mod degree $n+2$,

$$\begin{aligned} f_{n+1}(F_{n+1}(x,y)) &\equiv f_n(x) - \frac{\beta}{\nu(n+1)} x^{n+1} + f_n(y) - \frac{\beta}{\nu(n+1)} y^{n+1} \\ &\quad + \beta C_{n+1}(x,y) - \beta \frac{B_{n+1}(x,y)}{\nu(n+1)} \\ &= f_{n+1}(x) + f_{n+1}(y). \end{aligned}$$

So (iv) holds for $F_{n+1}(x,y)$ and $f_{n+1}(x)$. This completes the proof of the lemma. □

We now verify that we have in fact constructed universal objects.

THEOREM 1.33. *Let $n \geq 2$. Then the $F_n(x,y)$ (as constructed above) is a universal formal group law bud of order n. More precisely, if $G(x,y)$ is a formal group law bud of order n defined over a ring R, there is a unique ring homomorphism $\varphi_n : \mathbb{Z}[u_2, \ldots, u_n] \to R$ such that $G(x,y) \equiv (\varphi_n)_* F_n(x,y)$ (mod degree $n+1$).*

PROOF. Again, we proceed by induction on n. Let $G(x,y)$ be a 2-bud defined over a ring R. Then

$$G(x,y) \equiv x + y + bxy \pmod{\text{degree } 3},$$

for some $b \in R$. Defining φ_2 by the rule $\varphi_2(u_2) = b$, we have $G(x,y) \equiv (\varphi_2)_* F_2(x,y)$ (mod degree 3).

Now suppose that the theorem holds for an arbitrary $n \geq 2$. Let $G(x,y)$ be an $(n+1)$-bud defined over R. Treating $G(x,y)$ as an n-bud, our induction hypothesis asserts the existence of a ring homomorphism $\varphi_n : \mathbb{Z}[u_2, \ldots, u_n] \to R$ such that $G(x,y) \equiv (\varphi_n)_* F_n(x,y)$ (mod degree $n+1$).

Extend φ_n to a map $\varphi'_n : \mathbb{Z}[u_2, \ldots u_{n+1}] \to R$ by defining $\varphi'_n(u_{n+1}) = 0$. It is easy to see that

$$(\varphi'_n)_* F_{n+1}(x,y) \equiv G(x,y) \pmod{\text{degree } n+1}.$$

Since both $(\varphi'_n)_* F_{n+1}(x,y)$ and $G(x,y)$ are $(n+1)$-buds, the Lazard Comparison Lemma asserts the existence of some $a \in R$ such that

$$G(x,y) \equiv (\varphi'_n)_* F_{n+1}(x,y) + aC_{n+1}(x,y) \pmod{\text{degree } n+2}. \tag{1.17}$$

By its construction (see (1.11)),

$$F_{n+1}(x,y) = F_n(x,y) + H'(x,y) + u_{n+1}C_{n+1}(x,y),$$

where $H'(x,y) \in \mathbb{Z}[u_2, \ldots, u_n]$ is homogeneous of degree $n+1$. Thus,

$$(\varphi'_n)_* F_{n+1}(x,y) = (\varphi'_n)_*(F_n(x,y) + H'(x,y)). \tag{1.18}$$

Let φ_{n+1} extend φ_n to a map from $\mathbb{Z}[u_2, \ldots, u_{n+1}]$ to R by setting $\varphi_{n+1}(u_{n+1}) = a$. Noting that φ_{n+1} and φ'_n agree on $\mathbb{Z}[u_2, \ldots, u_n]$, we see that

$$\begin{aligned}
(\varphi_{n+1})_* F_{n+1}(x,y) &= (\varphi_{n+1})_*(F_n(x,y) + H'(x,y)) + \varphi_{n+1}(u_{n+1})C_{n+1}(x,y) \\
&= (\varphi'_n)_* F_{n+1}(x,y) + aC_{n+1}(x,y) \quad \text{by (1.18)} \\
&\equiv G(x,y) \pmod{\text{degree } n+2} \quad \text{by (1.17)}.
\end{aligned}$$

This completes the argument. □

COROLLARY 1.34. *Let $F_n(x,y)$ be as above and let $F(x,y) = \lim_{n\to\infty} F_n(x,y)$. Then $F(x,y)$ is a universal formal group law defined over $\mathbb{Z}[u_2, u_3, \ldots]$.*

PROOF. Let $G(x,y)$ be a formal group law defined over a ring R. Treating $G(x,y)$ as an n-bud for each $n \geq 2$, we obtain a sequence of mappings φ_n as in the above theorem. Letting $\varphi = \lim_{n\to\infty} \varphi_n$ (limit corresponding to the chain of inclusions $\mathbb{Z}[u_2, \ldots, u_n] \subseteq \mathbb{Z}[u_2, \ldots, u_{n+1}]$), it is clear that $\varphi_* F(x,y) = G(x,y)$. □

Since the universal n-bud extends to the universal $(n+1)$-bud, the following becomes clear.

COROLLARY 1.35. *Let G be an n-bud defined over a ring R. Then G can be extended to an $(n+1)$-bud, and in fact to a formal group law defined over R.*

6. Formal group laws in characteristic p

In this section, we introduce an important invariant of formal group laws defined over rings of characteristic p called *height*. We begin by making the following observation.

LEMMA 1.36. *Let $f\colon F \to G$ be a homomorphism of formal group laws defined over a ring R of characteristic p. Then there exists a unique integer $h \geq 0$ and a power series $g(x) \in R[\![x]\!]$ satisfying $g'(0) \neq 0$ such that $f(x) = g(x^{p^h})$.*

PROOF. Write $f(x) = a_1 x + a_2 x^2 + \cdots$. If $f'(0) \neq 0$, take $h = 0$ and $g = f$. Suppose that $f'(0) = 0$. Differentiating the relation $f(F(x,y)) = G(f(x), f(y))$ with respect to y and setting $y = 0$, we obtain

$$f'(x)\frac{\partial F}{\partial y}(x,0) = \frac{\partial G}{\partial y}(f(x),0)f'(0) = 0.$$

Note that $(\partial F/\partial y)(x,0) = 1 + \cdots$, so it is a unit in $R[\![x]\!]$. Therefore, $f'(x)$ is identically zero, that is, $na_n = 0$ for all $n \geq 1$. As R has characteristic p, if $p \nmid n$, we must have $a_n = 0$. Letting $f_1(x) = \sum_{n\geq 0} a_{pn} x^n$, it follows that $f(x) = f_1(x^p)$. We

now interpret f_1 as a homomorphism of formal group laws. Let $\varphi\colon R \to R$ be the p-th power Frobenius endomorphism, and let $F^{(p^h)} = \varphi_* F$. Then the power series x^p defines a homomorphism from F to $F^{(p)}$. We claim that f_1 is a homomorphism from $F^{(p)}$ to G. Indeed,

$$\begin{aligned} f_1(F^{(p)}(x^p, y^p)) &= f_1(F(x,y)^p) = f(F(x,y)) \\ &= G(f(x), f(y)) = G(f_1(x^p), f_1(y^p)). \end{aligned}$$

If $f_1'(0) \neq 0$, then take $h = 1$ and $g = f_1$. Otherwise, repeat the above argument replacing f by f_1 and F by $F^{(p)}$. □

REMARK 1.37. Thus, a homomorphism $f\colon F \to G$ can be expressed as the composition $F \to F^{(p^h)} \to G$ of a Frobenius map and a map g with $g'(0) \neq 0$.

DEFINITION 1.38. Let $f\colon F \to G$ be a homomorphism of formal group laws defined over a ring R of characteristic p. As in Lemma 1.36, write $f(x) = g(x^{p^h})$, with $g'(0) \neq 0$. The integer h is called the *height of* f, and denoted $\operatorname{ht} f$. We define the height of a formal group law F to be the height $\operatorname{ht}[p]_F$ of its multiplication-by-p endomorphism. We denote the height of F by $\operatorname{ht} F$. If $[p]_F \equiv 0 \pmod{p}$, we define $\operatorname{ht} F$ to be ∞. Note that $\operatorname{ht} F \geq 1$.

EXAMPLE 1.39. Consider the additive group $\mathcal{G}_a(x,y) = x+y$. Then $[p]_{\mathcal{G}_a} = px$, so $\operatorname{ht} \mathcal{G}_a = \infty$. Consider the multiplicative group, which we write in the form $\mathcal{G}_m(x,y) = (1+x)(1+y) - 1$. An easy induction verifies that $[m]_{\mathcal{G}_m}(x) = (1+x)^m - 1$, and consequently, one has $[p]_{\mathcal{G}_m} \equiv x^p \pmod{p}$. Therefore, $\operatorname{ht} \mathcal{G}_m = 1$.

It is easy to see that $\operatorname{ht} F$ is an isomorphism invariant of F. In fact, it a complete isomorphism invariant for formal group laws defined over a separably closed field of characteristic p.

THEOREM 1.40. *Let F and G be formal group laws defined over the separably closed field k of characteristic p. Then F and G are isomorphic (over k) if and only if* $\operatorname{ht} F = \operatorname{ht} G$.

For a proof of this theorem, see [**12**, Chapter III, §2].

CHAPTER 2

The formal group law of an elliptic curve

In this section, we investigate how the addition law on an elliptic curve may be described locally by a formal group law.

1. Theoretical considerations

Let E be an elliptic curve defined over a field K, with additive structure given by the rule $\alpha : E \times E \to E$ and the neutral element O. Pick a uniformizer z for E at O. Then by the Cohen Structure Theorem, the completed local ring $\widehat{\mathcal{O}}_{E,O}$ is isomorphic to the power series ring $K[\![z]\!]$. Noting the isomorphism

$$\widehat{\mathcal{O}}_{E\times E,(O,O)} \cong \widehat{\mathcal{O}}_{E,O} \underset{K}{\widehat{\otimes}} \widehat{\mathcal{O}}_{E,O} \cong K[\![1 \mathbin{\widehat{\otimes}} z, z \mathbin{\widehat{\otimes}} 1]\!], \tag{2.1}$$

we may view $\alpha^* z$ as a power series $F(1 \mathbin{\widehat{\otimes}} z, z \mathbin{\widehat{\otimes}} 1)$ in $K[\![1 \mathbin{\widehat{\otimes}} z, z \mathbin{\widehat{\otimes}} 1]\!]$. We claim that F is a formal group law. We show how F inherits the required associativity property from the associativity of α. The verification of the other axioms proceeds similarly. By associativity of addition on E, the diagram

$$\begin{array}{ccc} E \times E \times E & \xrightarrow{\alpha \times \mathrm{id}} & E \times E \\ {\scriptstyle \mathrm{id}\times\alpha}\downarrow & & \downarrow{\scriptstyle \alpha} \\ E \times E & \xrightarrow[\alpha]{} & E \end{array}$$

commutes.

Passing to local rings at the neutral elements and using the isomorphism (2.1), we obtain the following commutative diagram.

$$\begin{array}{ccc} K[\![1\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}z, 1\mathbin{\widehat{\otimes}}z\mathbin{\widehat{\otimes}}1, z\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}1]\!] & \xleftarrow{\alpha^*\widehat{\otimes}\mathrm{id}} & K[\![1\mathbin{\widehat{\otimes}}z, z\mathbin{\widehat{\otimes}}1]\!] \\ {\scriptstyle \mathrm{id}\widehat{\otimes}\alpha^*}\uparrow & & \uparrow{\scriptstyle \alpha^*} \\ K[\![1\mathbin{\widehat{\otimes}}z, z\mathbin{\widehat{\otimes}}1]\!] & \xleftarrow[\alpha^*]{} & K[\![z]\!]. \end{array}$$

Computing, we see that

$$\begin{aligned} (\alpha^*\mathbin{\widehat{\otimes}}\mathrm{id})(\alpha^* z) &= (\alpha^*\mathbin{\widehat{\otimes}}\mathrm{id})(F(1\mathbin{\widehat{\otimes}}z, z\mathbin{\widehat{\otimes}}1)) \\ &= F(1\mathbin{\widehat{\otimes}}\alpha^* z, z\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}1) \\ &= F(1\mathbin{\widehat{\otimes}}F(1\mathbin{\widehat{\otimes}}z, z\mathbin{\widehat{\otimes}}1), z\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}1) \\ &= F(F(1\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}z, 1\mathbin{\widehat{\otimes}}z\mathbin{\widehat{\otimes}}1), z\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}1). \end{aligned}$$

One verifies similarly that

$$(\mathrm{id}\mathbin{\widehat{\otimes}}\alpha^*)(\alpha^* z) = F(1\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}z, F(1\mathbin{\widehat{\otimes}}z\mathbin{\widehat{\otimes}}1, z\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}1)).$$

It follows from the commutativity of the above diagram that

$$F(F(1\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}z, 1\mathbin{\widehat{\otimes}}z\mathbin{\widehat{\otimes}}1), z\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}1) = F(1\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}z, F(1\mathbin{\widehat{\otimes}}z\mathbin{\widehat{\otimes}}1, z\mathbin{\widehat{\otimes}}1\mathbin{\widehat{\otimes}}1)),$$

verifying the associativity condition for F.

REMARK 2.1. Let G be an algebraic group of dimension n defined over a field K. One can show by arguments analogous to those presented above, that the group law on G can also be described locally by an n-dimensional formal group law over K. This formal group law need not be commutative in general (cf. Example A.6).

The above correspondence from elliptic curves to formal group laws is actually functorial. Let $\varphi\colon E_1 \to E_2$ be an isogeny of elliptic curves defined over K. Let F_i be the formal group law attached to E_i as above by choosing uniformizers $z_i \in \mathcal{O}_{E_i,O}$, for $i = 1, 2$. We will show how φ induces a homomorphism $f\colon F_1 \to F_2$. The map φ is an isogeny, so $\varphi(O) = O$. Thus, we have an induced map $\varphi^*\colon \widehat{\mathcal{O}}_{E_2,O} \to \widehat{\mathcal{O}}_{E_1,O}$. Now

$\widehat{\mathcal{O}}_{E_1,O} \cong K[\![z_1]\!]$, so we may view $\varphi^* z_2$ as a power series $f(z_1) \in K[\![z_1]\!]$. We claim that f is actually a homomorphism from F_1 to F_2.

Let α_1 and α_2 denote the addition laws on E_1 and E_2, respectively. As φ is an isogeny, the diagram

$$\begin{array}{ccc} E_1 \times E_1 & \xrightarrow{\alpha_1} & E_1 \\ {\scriptstyle \varphi\times\varphi}\downarrow & & \downarrow{\scriptstyle \varphi} \\ E_2 \times E_2 & \xrightarrow{\alpha_2} & E_2 \end{array}$$

commutes. Passing to the local rings, we obtain the commutative diagram

$$\begin{array}{ccc} \widehat{\mathcal{O}}_{E_1,O} \underset{K}{\widehat{\otimes}} \widehat{\mathcal{O}}_{E_1,O} & \xleftarrow{\alpha_1^*} & \widehat{\mathcal{O}}_{E_1,O} \\ {\scriptstyle \varphi^*\widehat{\otimes}\varphi^*}\uparrow & & \uparrow{\scriptstyle \varphi^*} \\ \widehat{\mathcal{O}}_{E_2,O} \underset{K}{\widehat{\otimes}} \widehat{\mathcal{O}}_{E_2,O} & \xleftarrow[\alpha_2^*]{} & \widehat{\mathcal{O}}_{E_1,O}. \end{array}$$

Computing, we see that

$$\begin{aligned} \alpha_1^*(\varphi^* z_2) &= \alpha_1^* f(z_1) \\ &= f(\alpha_1^* z_1) \\ &= f(F_1(1 \mathbin{\widehat{\otimes}} z_1, z_1 \mathbin{\widehat{\otimes}} 1)), \\ (\varphi^* \mathbin{\widehat{\otimes}} \varphi^*)(\alpha_2^* z_2) &= (\varphi^* \mathbin{\widehat{\otimes}} \varphi^*)(F_2(1 \mathbin{\widehat{\otimes}} z_2, z_2 \mathbin{\widehat{\otimes}} 1)) \\ &= F_2(1 \mathbin{\widehat{\otimes}} \varphi^* z_2, \varphi^* z_2 \mathbin{\widehat{\otimes}} 1) \\ &= F_2(f(1 \mathbin{\widehat{\otimes}} z_2), f(z_2 \mathbin{\widehat{\otimes}} 1)). \end{aligned}$$

By the commutativity of the above diagram, we have

$$f(F_1(1 \mathbin{\widehat{\otimes}} z_1, z_1 \mathbin{\widehat{\otimes}} 1)) = F_2(f(1 \mathbin{\widehat{\otimes}} z_2), f(z_2 \mathbin{\widehat{\otimes}} 1)),$$

implying that f is a homomorphism, as claimed. Thus, given elliptic curves E_1 and E_2 with corresponding formal group laws F_1 and F_2, one has a map from $\mathrm{Hom}(E_1, E_2)$ into $\mathrm{Hom}(F_1, F_2)$, where $\mathrm{Hom}(E_1, E_2)$ is the group of isogenies from E_1 to E_2. By applying the definition, one may show that this map is a group homomorphism.

Further, one verifies easily that if E_3 is a another elliptic curve with formal group law F_3, then the diagram

$$\begin{array}{ccc} \mathrm{Hom}(E_1, E_2) \times \mathrm{Hom}(E_2, E_3) & \longrightarrow & \mathrm{Hom}(F_1, F_2) \times \mathrm{Hom}(F_2, F_3) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(E_1, E_3) & \longrightarrow & \mathrm{Hom}(F_1, F_3) \end{array}$$

commutes, where the vertical arrows are given by composition. Thus, the map from $\mathrm{End}\, E_1$ to $\mathrm{End}\, F_1$ is a ring homomorphism.

EXAMPLE 2.2. Let E be an elliptic curve, and let F be the formal group law obtained from E by choosing a uniformizer $z \in \mathcal{O}_{E,O}$. Let $[m]_E \colon E \to E$ denote the multiplication-by-m endomorphism of E. Since the map from $\mathrm{End}\, E$ to $\mathrm{End}\, F$ is a ring homomorphism, it follows that the isogeny $[m]_E$ induces the formal multiplication-by-m map $[m]_F$ on F.

EXAMPLE 2.3. Let E be an elliptic curve defined over a field K of characteristic p, and let $\varphi \colon E \to E^{(p^r)}$ be the p^r-th power Frobenius map (see [**37**, Chapter II, §2]). Then one can show that the induced homomorphism of formal group laws is given by the power series $f(x) = x^{p^r}$.

One can show that the height of the formal group law of an elliptic curve is 1 or 2. This will be discussed in more detail in §4.

2. More explicitly

Let E be an elliptic curve given by the Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

It is convenient to introduce the change of variables

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}, \tag{2.3}$$

under which the equation of E becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 := f(z, w). \tag{2.4}$$

We attempt to express w as a power series in z by substituting equation (2.4) into itself again and again. The first substitution gives

$$\begin{aligned} w = f(z,w) &= f(z, f(z,w)) \\ &= z^3 + a_1 z^4 + a_2 z^5 + a_3 z^6 + a_4 z^7 + a_6 z^9 + (\text{terms involving } w). \end{aligned}$$

We want this process to converge to a power series $w(z) \in \mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$ such that $w(z) = f(z, w(z))$. For the rest of this section, let R denote $\mathbb{Z}[a_1, \ldots, a_6][\![z]\!]$.

To prove this, we need to give a more precise description of our algorithm. Define a sequence of polynomials inductively by

$$f_1(z,w) = f(z,w), \quad f_{n+1}(z,w) = f(z, f(z,w)) \text{ for } n \geq 1.$$

The n-th approximation to our desired power series $w(z)$ is $f_n(z,0)$. It is clear that each $f_n(z,0)$ is a polynomial with coefficients in R. We claim that the sequence $f_n(z,0)$ converges to a limit $w(z) \in R[\![z]\!]$ in the obvious sense – that is, if we let $\alpha_k^{(n)}$ be the coefficient of z^k in $f_n(z,0)$, then the sequence $(\alpha_k^{(n)})_{n \geq 1}$ is eventually constant. The convergence of the sequence $f_n(z,0)$ is a consequence of a variant of Hensel's Lemma; see [**37**, Ch. IV, Lemma 1.2]. We obtain

LEMMA 2.4. *The sequence $f_n(z,0)$ converges to a power series*

$$w(z) = z^3(1 + \alpha_1 z + \alpha_2 z^2 + \cdots) \in R[\![z]\!]$$

satisfying $w(z) = f(z, w(z))$.

Thus, by Equations (2.3), x and y have formal Laurent expansions of the form

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} + \cdots, \quad y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + \cdots, \tag{2.5}$$

yielding formal solutions (i.e., solutions in the ring of formal Laurent series) to Equation (2.2).

We now use Equations (2.5), together with the group law on E, to derive a power series $F(z_1, z_2) \in R[\![z_1, z_2]\!]$ series describing this group law. In fact, it is convenient to begin by developing a power series $i(z) \in R[\![z]\!]$ describing the inversion operation

on E. Let z be an indeterminate and let $P = (z, w(z))$ represent a point on E. If we represent P in the (x, y)-plane by $(x(z), y(z))$, then $-P$ is given formally by $(x(z), -y(z) - a_1x(z) - a_3)$. Therefore, the value of z corresponding to $-P$ is

$$i(z) = \frac{x(z)}{y(z) + a_1x(z) + a_3} = \frac{z^{-2} + \cdots}{-z^{-3} + \cdots} \in R[\![z]\!], \tag{2.6}$$

yielding a formal power series describing inversion on E.

Let z_1 and z_2 be indeterminates, and let $w_i = w_i(z_i)$ and $P_i = (z_i, w_i)$ for $i = 1, 2$. The line joining P_1 and P_2 has slope

$$\begin{aligned}\lambda = \frac{w_1 - w_2}{z_1 - z_2} &= \sum_{n\geq 3} \alpha_{n-3} \frac{z_1^n - z_2^n}{z_1 - z_2} \qquad (\alpha_0 := 1) \\ &= (z_1^2 + z_1z_2 + z_2^2) + \alpha_1(z_1^2 + z_1^2z_2 + z_1z_2^2 + z_1^3) + \cdots \in R[\![z_1, z_2]\!].\end{aligned}$$

Letting $\nu = w_1 - \lambda z_1$, we have the line through P_1 and P_2 is given by $w = \lambda z + \nu$. Substituting this expression into equation (2.4), we see that that the points of intersection of $w = \lambda z + \nu$ and E are given by solutions of

$$\begin{aligned}0 &= z^3 + a_1z(\lambda z + \nu) + a_2z^2(\lambda z + \nu) + +a_3(\lambda z + \nu)^2 \\ &\quad + a_4z(\lambda z + \nu)^2 + a_6(\lambda z + \nu)^3 - (\lambda z + \nu) \\ &= (1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3)z^3 + \\ &\quad + (a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu)z^2 + Az + B.\end{aligned}$$

By construction, z_1 and z_2 are roots of this cubic; let $z_3 = z_3(z_1, z_2)$ be the other one. By examining the quadratic term, we get

$$\begin{aligned}-(z_1 + z_2 + z_3) &= \frac{a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \\ \iff z_3 &= -z_1 - z_2 - \frac{a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \in R[\![z_1, z_2]\!].\end{aligned}$$

So by the definition of addition on E, the value of z corresponding to $P_1 + P_2$ is given by

$$F(z_1, z_2) := i(z_3(z_1, z_2)) \in R[\![z_1, z_2]\!]. \tag{2.7}$$

One can compute that the first few terms of $F(z_1, z_2)$ are given by

$$F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - \\ - 2a_3(z_1^3 z_2 + z_1 z_2^3) - (a_1 a_2 - 3a_3) z_1^2 z_2^2 + \cdots .$$

It follows from the corresponding properties of the group law on E, that the power series $F(z_1, z_2)$ of equation (2) and $i(z)$ of equation (2.6) satisfy all the properties of Definition 1.1. Thus, $F(z_1, z_2)$ is a formal group law with coefficients in $R = \mathbb{Z}[a_1, \ldots, a_6]$.

REMARK 2.5. Suppose E be is an elliptic curve defined over a complete local field K with ring of integers R and maximal ideal $\mathfrak{m}$. Let $F(z_1, z_2)$ be the formal group law obtained from E as described above and form the group $\mathfrak{m}_F$ as described in Example 1.5. Then the map

$$\varphi : \mathfrak{m}_F \to E(K) \text{ defined by } \varphi(a) = (x(a), y(a))$$

is clearly a homomorphism as the group law on $\mathfrak{m}_F$ is induced by the group law on $E(K)$. The map φ is actually one-to-one, its inverse being given by the correspondence $(x(a), y(a)) \mapsto -x(a)/y(a)$. One can show that

$$\operatorname{Im}\varphi = \{\, (x, y) \in E(K) \mid 1/x \in \mathfrak{m} \,\},$$

see [**37**, p. 114]. These observations allow one to use the theory of formal group laws to analyse elliptic curves defined over local fields.

3. Elliptic curves given by Jacobi quartics

3.1. Euler's formal group law. For some applications to topology, it is often more convenient to coordinatize elliptic curves in the form

$$E\colon y^2 = R(x) = 1 - 2\delta x^2 + \varepsilon x^4, \tag{2.8}$$

where the discriminant $\Delta := \varepsilon(\delta^2 - \varepsilon)^2$ is nonzero. The polynomial $R(x)$ is called a *Jacobi quartic*. One may obtain a formal group law $F(x, y)$ from this equation which

represents the group law on E around its neutral element $O = (0, 1)$. We will show that this formal group law has the pleasing form

$$F(x, y) = \frac{x\sqrt{R(y)} + y\sqrt{R(x)}}{1 - \varepsilon x^2 y^2}. \tag{2.9}$$

This is actually for the addition formula for the elliptic integral $\int dt/R(t)^{1/2}$. That is,

$$\int_0^x \frac{dt}{\sqrt{R(t)}} + \int_0^y \frac{dt}{\sqrt{R(t)}} = \int_0^{F(x,y)} \frac{dt}{\sqrt{R(t)}}.$$

This formula is due to Euler, and thus the formal group law (2.9) is often called *Euler's formal group law*. The origins of these formulae lie in the classical problem of doubling the arc of the lemniscate. For an elementary exposition of this issue, see [**36**, Chapter 1]; for a higher powered account see [**31**, Chapter 2].

We prove that (2.9) is in fact a formal group law using complex analytic techniques. We show that for complex number x_1, x_2, and x_3 of small enough modulus, the power series $F(F(x_1, x_2), x_3)$ and $F(x_1, F(x_2, x_3))$ converge to the same value. Thus, the corresponding coefficients of their power series expansions, given by the usual formluas, are the same.

Of course, the elliptic curve E is isomorphic to one given by a Weierstrass cubic. We will show that Euler's formal group law is strictly isomorphic to an elliptic formal group law of the form given in the previous section. This isomorphism is induced by a change of variable converting quartics to cubics.

3.2. The Weierstrass $\wp$-function. We need to recall a few facts about the Weierstrass $\wp$-function. For proofs of the assertions below and basic facts concerning elliptic functions, see [**31**, Chapter 2] or [**37**, Chapter VI]. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$, and let $\Lambda' = \Lambda - \{0\}$. Defering to tradition, we define the Weierstrass $\wp$-function $\wp(z, \Lambda)$ of the lattice Λ by the formula

$$\wp(z) = \wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left[\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right].$$

The function $\wp(z)$ defines an even, meromorphic function, elliptic (doubly periodic) with respect to the lattice Λ, with a double pole at each lattice point. The derivative $\wp'(z)$ is given by

$$\wp'(z) = -2\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}.$$

The function $\wp'(z)$ is an odd, meromorphic function, also elliptic with respect to Λ, with a pole of order three at each lattice point. One can show that in the set

$$\{\, r_1\omega_1 + r_2\omega_2 \mid 0 \le r_1, r_2 \le 1 \,\},$$

the *fundamental parallelogram* of Λ, the function $\wp'(z)$ has simple zeros at

$$\lambda_1 := \frac{\omega_1}{2}, \quad \lambda_2 := \frac{\omega_2}{2}, \quad \text{and} \quad \lambda_3 := \frac{\omega_1+\omega_2}{2}.$$

Let $e_i = \wp(\lambda_i)$, for $i = 1, 2, 3$.

Further, the $\wp$-function satisfies the differential equation

$$\begin{aligned}\wp'(z)^2 &= 4\wp(z)^3 - g_2\wp(z) - g_3\\ &= 4(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3),\end{aligned}$$

where g_2 and g_3 are defined by the Eisenstein series

$$g_2 = g_2(\Lambda) = 60\sum_{\omega\in\Lambda'}\frac{1}{\omega^4}, \quad g_3 = g_3(\Lambda) = 140\sum_{\omega\in\Lambda'}\frac{1}{\omega^6}.$$

Therefore, the correspondence $z \mapsto (\wp(z), \wp'(z))$ is parameterization of the elliptic curve

$$y^2 = 4x^3 - g_2x - g_3.$$

In fact, the above correspondence is an analytic isomorphism of Lie groups between the torus $\mathbb{C}/\Lambda$ and the above elliptic curve, see [**37**, Ch. VI, Proposition 3.6].

Conversely, given an elliptic curve in the form

$$y^2 = 4x^3 - Ax - B, \tag{2.10}$$

with A, $B \in \mathbb{C}$ and $A^3 - 27B^2 \neq 0$, we can find a lattice Λ with $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$. Thus, any elliptic curve in the form (2.10) can be parameterized using the Weierstrass $\wp$-function. This is the content of the celebrated *Uniformization Theorem* [**37**, Chapter VI, Theorem 5.1]. Above, we interpreted g_2 and g_3 as complex value functions of lattices in $\mathbb{C}$. One may also view g_2 and g_3 as complex valued functions defined on the Poincaré upper half plane, $\mathcal{H}$. For $\tau \in \mathcal{H}$, let $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. As noted above, the Weierstrass $\wp$-function $\wp(z, \tau) := \wp(z, \Lambda_\tau)$ satisfies the differential equation, depending on the parameter τ,

$$(\wp')^2 = 4\wp^3 - g_2(\tau)\wp - g_3(\tau),$$

where $g_i(\tau) = g_i(\Lambda_\tau)$. In Chapter 5, we will interpret $g_2(\tau)$ and $g_3(\tau)$ as modular forms.

Using the group law on the elliptic curve which it parameterizes, one can show that the Weierstrass $\wp$-function admits the algebraic addition formula

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left[\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right]^2.$$

3.3. Parameterization of Jacobi quartics. In order to understand elliptic curves given in the form

$$y^2 = 1 - 2\delta x^2 + \varepsilon x^4, \quad \delta, \varepsilon \in \mathbb{C} \tag{2.11}$$

we describe a parameterization analogous to the one given above for elliptic curves in Weierstrass normal form. To ensure the curves given by 2.11 are nonsingular, we insist that the discriminant $\Delta := \varepsilon(\delta^2 - \varepsilon)^2$ be nonzero. One can parameterize elliptic curves defined by such Jacobi quartics as follows (see [**21**, §5] and [**45**] for details). We shall use the notation of the previous section.

THEOREM 2.6. *Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the unique lattice with*

$$g_2(\Lambda) = \frac{1}{3}(\delta^2 + 3\varepsilon), \quad g_3(\Lambda) = \frac{1}{27}\delta(\delta^2 - 9\varepsilon),$$

and $\wp(z)$ be its associated $\wp$-function. Define

$$\sigma(z) = \sigma(z, \Lambda) = -2\frac{\wp(z, \Lambda) - e_3}{\wp'(z, \Lambda)}, \tag{2.12}$$

where e_3 is defined as in §3.2. Then σ satisfies the differential equation

$$(\sigma'(z))^2 = 1 - 2\delta\sigma(z)^2 + \varepsilon\sigma(z)^4,$$

and therefore the correspondence $z \mapsto (\sigma(z), \sigma'(z))$ is a complex parameterization of the elliptic curve (2.11).

One may view the parameters δ and ε as complex valued functions on $\mathcal{H}$. As before, let $\tau \in \mathcal{H}$ and define $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. Then $\sigma(z, \tau) := \sigma(z, \Lambda_\tau)$ satisfies a differential equation, depending on the parameter τ, of the form

$$(\sigma')^2 = 1 - 2\delta(\tau)\sigma^2 + \varepsilon(\tau)\sigma^4.$$

In Chapter 5, we will interpret the functions $\delta(\tau)$ and $\varepsilon(\tau)$ as modular forms.

We list a few properties of the function $\sigma(z)$ and its derivative, $\sigma'(z)$ which may be deduced directly from (2.12) and properties of the Weierstrass $\wp$-function.

(i) $\sigma(z)$ is an odd function with simple poles at λ_1 and λ_2, and simple zeros 0 and λ_3, that is,

$$\operatorname{div}\sigma(z) = (0) + (\lambda_3) - (\lambda_1) - (\lambda_2).$$

(ii) $\sigma(z)$ satisfies the identities

$$\sigma(z + \lambda_3) = -\sigma(z), \quad \sigma(\lambda_3 - z) = \sigma(z).$$

(iii) $\sigma'(z)$ is an even elliptic function satisfying $\sigma'(0) = 1$. Letting $\theta = \lambda_3/2$, we have

$$\operatorname{div}\sigma'(z) = (\theta) + (-\theta) + (\theta + \lambda_1) + (\theta + \lambda_2) - 2(\lambda_1) - 2(\lambda_2).$$

(iv) The function $\sigma(z + \lambda_1)$ has poles where $\sigma(z)$ has zeros, and zeros where $\sigma(z)$ has poles. Therefore, $\operatorname{div}\sigma(z + \lambda_1) = -\operatorname{div}\sigma(z)$, or $\sigma(z + \lambda_1)\sigma(z) = c$, for some $c \in \mathbb{C}$.

(v) Replacing z by $z+\lambda_2$ in (iv) and using (ii), we see that $\sigma(z+\lambda_2)\sigma(z) = -c$.

We may actually identify the constant c appearing in (iv) and (v). By (iii), and the differential equation for $\sigma(z)$,

$$\sigma(\theta), \quad \sigma(-\theta), \quad \sigma(\theta+\lambda_1), \quad \sigma(\theta+\lambda_2)$$

are zeros of the polynomial $1-2\delta x+\varepsilon x^4$. Examining the constant term in the identity

$$1 - 2\delta x^2 + \varepsilon x^4 = \varepsilon(x-\sigma(\theta))(x-\sigma(-\theta))(x-\sigma(\theta+\lambda_1))(x-\sigma(\theta+\lambda_2))$$

and using the fact that $\sigma(z)$ is odd, we conclude that $\varepsilon = 1/c^2$.

As $\sigma(z)$ parameterizes an elliptic curve, it is not surprising that it satisfies an addition formula.

THEOREM 2.7 ([**21**, Appendix]). *The function $\sigma(z)$ and its derivative $\sigma'(z)$ satisfy the addition formula*

$$\sigma(z+w) = \frac{\sigma(z)\sigma'(w)+\sigma(w)\sigma'(z)}{1-\varepsilon\sigma(z)^2\sigma(w)^2}. \tag{2.13}$$

PROOF. Fix a complex number w with $\sigma(w) \neq 0$. It suffices to verify (2.13) for such w. Let

$$A(z) = \sigma(z+w)\left(1-\frac{1}{c^2}\sigma(z)^2\sigma(w)^2\right),$$

$$B(z) = \sigma(z)\sigma'(w)+\sigma(w)\sigma'(z).$$

Since $A(0) = \sigma(w) = B(0)$, and A and B are elliptic, it suffices to show that $A(z)$ and $B(z)$ have the same divisor.

To compute $\operatorname{div} A(z)$, we identify the zeros and poles of each factor in the expression

$$A(z) = \sigma(z+w)\left(1-\frac{1}{c}\sigma(z)\sigma(w)\right)\left(1+\frac{1}{c}\sigma(z)\sigma(w)\right).$$

It follows immediately from (i) that

$$\operatorname{div}\sigma(z+w) = (-w)+(\lambda_3-w)-(\lambda_1-w)-(\lambda_2-w).$$

To compute $\operatorname{div}(1-\sigma(z)\sigma(w)/c)$, we first note that the function $1-\sigma(z)\sigma(w)/c$ has the same poles as $\sigma(z)$, that is, simple poles at λ_1 and λ_2. From the formula $\sigma(z+\lambda_1)\sigma(z)=c$ of (iv), it follows that λ_1+w is a zero of $1-\sigma(z)\sigma(w)/c$. Also, by the oddness of $\sigma(z)$ and (v), we obtain

$$\sigma(w)\sigma(\lambda_2-w)=-\sigma(-w)\sigma(\lambda_2+(-w))=c.$$

Therefore, λ_2-w is also a zero of $1-\sigma(z)\sigma(w)/c$. Since it has only two poles, we conclude that

$$\operatorname{div}\left(1-\frac{1}{c}\sigma(z)\sigma(w)\right)=(\lambda_1+w)+(\lambda_2-w)-(\lambda_1)-(\lambda_2).$$

In like manner, one shows that

$$\operatorname{div}\left(1+\frac{1}{c}\sigma(z)\sigma(w)\right)=(\lambda_1-w)+(\lambda_2+w)-(\lambda_1)-(\lambda_2).$$

Therefore,

$$\operatorname{div}A(z)=(-w)+(\lambda_3-w)+(\lambda_1+w)+(\lambda_2+w)-2(\lambda_1)-2(\lambda_2).$$

To compute the divisor of $B(z)$, we first note that its poles are precisely the poles of $\sigma'(z)$, that is, double poles at λ_1 and λ_2. We proceed to show the four zeros of $A(z)$ are also zeros of $B(z)$. As $\sigma(z)$ is odd and $\sigma'(z)$ is even, we see that $B(-w)=0$. It follows easily from (ii) that λ_3-w is a zero of $B(z)$. Differentiating the relations $\sigma(z+\lambda_1)\sigma(z)=c$ and $\sigma(z+\lambda_2)\sigma(z)=-c$ of (iv) and (v), respectively, we see that $B(\lambda_1+w)=B(\lambda_2+w)=0$. This completes the verification that $B(z)$ has the same zeros and poles, and hence the same divisor, as $A(z)$. This completes the argument. □

3.4. Elliptic formal group laws, revisited. Using the addition formula proved above, it is easy to deduce that Euler's addition formula for the elliptic integral is in fact a formal group law.

THEOREM 2.8. *Let δ and ε be indeterminates, let $R(x) = 1 - 2\delta x^2 + \varepsilon x^4$, and let*

$$F(x,y) = \frac{x\sqrt{R(y)} + y\sqrt{R(x)}}{1 - \varepsilon x^2 y^2}.$$

The $F(x,y)$ defines a formal group law with coefficients in the ring $\mathbb{Z}[1/2, \delta, \varepsilon]$.

PROOF. That the power series expansion of $F(x,y)$ has coefficients in the ring $\mathbb{Z}[1/2, \delta, \varepsilon]$ follows from the binomial expansion. It is clear that as formal power series, $F(x,0) = x$, $F(0,y) = y$, and $F(x,y) = F(y,x)$. It remains to verify the formal power series identity

$$F(F(x_1,x_2),x_3) = F(x_1,F(x_2,x_3)). \tag{2.14}$$

Suppose that (2.14) held for all complex numbers δ and ε with $\varepsilon(\delta^2 - \varepsilon)^2 \neq 0$. This would say that the corresponding coefficients of the power series expansions of each side of (2.14) define the same polynomial function of δ and ε. This implies that the corresponding coefficients are equal as formal polynomials in δ and ε. Thus, it suffices to verify (2.14) for all complex numbers δ and ε.

Let δ and ε be complex numbers with $\varepsilon(\delta^2 - \varepsilon)^2 \neq 0$. As mentioned on page 31 it suffices to show that the functions $F(F(x_1,x_2),x_3)$ and $F(x_1,F(x_2,x_3))$ have the same value for complex numbers x_1, x_2, and x_3 with sufficiently small modulus. Now $\sigma(z)$ is analytic at 0, so we may find neighbourhoods U and V of 0 in $\mathbb{C}$ such that $\sigma(U) = V$, and $\sigma(z)$ has no poles in $U + U + U$. Let x_1, x_2, $x_3 \in V$, and find u_1, u_2, $u_3 \in U$ such that $x_i = \sigma(u_i)$ for $i = 1,2,3$. Then

$$\begin{aligned} F(F(x_1,x_2),x_3) &= F(F(\sigma(u_1),\sigma(u_2)),\sigma(u_3)) \\ &= F(\sigma(u_1+u_2),\sigma(u_3)) \\ &= \sigma(u_1+u_2+u_3) < \infty, \end{aligned}$$

by two applications of Theorem 2.7. Symmetrically,

$$F(x_1,F(x_2,x_3)) = \sigma(u_1+u_2+u_3) < \infty.$$

Thus, $F(F(x_1, x_2), x_3)$ and $F(x_1, F(x_2, x_3))$ agree on V, completing the proof. □

To relate the above discussion to that of §1, we point out explicitly how Euler's formal group law does indeed come from the expansion of the group law of an elliptic curve around its neutral element with respect to an appropriate uniformizer. Let δ, $\varepsilon \in \mathbb{C}$ with $\Delta = \varepsilon(\delta^2 - \varepsilon)^2 \neq 0$ and consider the elliptic curve given by $E : y^2 = 1 - 2\delta x^2 + \varepsilon x^4$. Let Λ be a lattice which parameterizes E via

$$(x, y) = (x(z), y(z)) = (\sigma(z), \sigma'(z)).$$

Since σ has a simple zero at 0, the function x is a uniformizer for the local ring of E at $O = (0, 1)$. By Theorem 2.7, one has

$$x(z_1 + z_2) = \sigma(z_1 + z_2) = F(\sigma(z_1), \sigma(z_2)) = F(x(z_1), x(z_2)),$$

where F is Euler's formal group law. Thus, F represents the expansion of the group law on E around $O = (0, 1)$ with respect to the uniformizer $x \in \mathcal{O}_{E,O}$.

Given an elliptic curve E, we have defined for it two different formal group laws – one formal group law, $F_W(x, y)$, corresponding to its Weierstrass cubic representation, and another, $F_J(x, y)$, corresponding to its Jacobi quartic representation. Since they both these formal group laws represent the group law on E locally at O, they should certainly be isomorphic. We verify this fact.

Setting notation explicitly, let δ and ε be such that $\Delta = \varepsilon(\delta^2 - \varepsilon)^2 \neq 0$, and let E be the curve given by the Jacobi quartic (2.8), and let $F_J(x, y)$ ('J' for Jacobi) be Euler's formal group law. Let E' be the curve

$$y^2 = 4x^3 - g_2 x - g_3,$$

given in Weierstrass form, where g_2 and g_3 are given in terms of δ and ε as in the statement of Theorem 2.6. The change of variable

$$x = \frac{z}{w}, \quad y = \frac{-2}{w} \iff z = \frac{-2x}{y}, \quad w = \frac{-2}{y} \tag{2.15}$$

puts the above curve into the form

$$w = z^3 - \frac{g_2}{4}zw^2 - \frac{g_3}{4}w^3.$$

Thus, we may use the methods of the previous section, we may express w as a power series $w(z)$ in z, and thereby construct a formal group law $F_W(x,y)$ ('W' for Weierstrass) representing the group law on E' in a neighbourhood of O.

THEOREM 2.9 ([**21**, Theorem 4]). *The formal group laws $F_J(x,y)$ and $F_W(x,y)$ are strictly isomorphic over the ring $\mathbb{Z}[1/6,\varepsilon,\delta]$.*

PROOF. Guided by (2.12) and (2.15), we define our perspective isomorphism of $F_W(x,y)$ onto $F_J(x,y)$ by the formula

$$f(z) = z - \frac{\delta}{3}w(z).$$

As $w(z)$ has coefficients in $\mathbb{Z}[1/2,\delta,\varepsilon]$, it is clear that $f(z)$ has coefficients in $\mathbb{Z}[1/6,\delta,\varepsilon]$.

By arguments similar to those presented in the proof of the previous theorem, to show that the power series identity

$$f(F_W(x,y)) = F_J(f(x),f(y)),$$

holds, it suffices to verify the above for complex variables δ and ε in $\mathbb{C}$ with $\varepsilon(\delta^2-\varepsilon)^2 \neq 0$. Still guided by (2.15), define elliptic functions

$$z(s) = \frac{-2\wp(s)}{\wp'(s)}, \quad w(s) = \frac{-2}{\wp'(s)}.$$

By the definition of $\sigma(s)$, we have

$$\sigma(s) = z(s) - \frac{\delta}{3}w(s) = f(z(s)).$$

We also have

$$\sigma(s_1+s_2) = F_J(\sigma(s_1),\sigma(s_2)), \quad z(s_1+s_2) = F_W(z(s_1),z(s_2)).$$

Therefore,

$$\begin{aligned} f(F_W(z(s_1), z(s_2))) &= f(z(s_1 + s_2)) \\ &= \sigma(s_1 + s_2) \\ &= F_J(\sigma(s_1), \sigma(s_2)). \end{aligned}$$

The desired conclusion follows. □

4. Heights of elliptic formal group laws

In this section we prove the following description of elliptic formal group laws.

THEOREM 2.10. *Let F be the formal group law of an elliptic curve E defined over a field of characteristic p. Then* $\operatorname{ht} F = 1$ *or* 2.

This theorem is a consequence of the following result.

LEMMA 2.11 ([**37**, Chapter IV, Theorem 7.4]). *Let k be a field of characteristic p, and let $\varphi\colon E_1 \to E_2$ be a nonzero isogeny of elliptic curves defined over k. Let f denote the homomorphism of formal group laws induced by φ. Then*

$$p^{\operatorname{ht} f} = \deg_i \varphi,$$

where $\deg_i \varphi$ *denotes the degree of inseparability of* φ.

SKETCH OF PROOF. We begin by considering two special cases. First, suppose φ is the p^r-th power Frobenius map. Then $f(x) = x^{p^r}$ (see Example 2.3), and $p^{\operatorname{ht} f} = p^r = \deg_i \varphi$. Now suppose φ is separable. In this case, one can show that the height of the corresponding homomorphism of formal group laws is zero. One completes the proof using the following facts.

- A nonzero isogeny of elliptic curves can be written as the composition of a Frobenius map and a separable isogeny (cf. Remark 1.37).
- The assignment of a formal group law to an elliptic curve is functorial (see §1).

- If $f\colon F \to G$ and $g\colon G \to H$ are homomorphisms of formal group laws, then $\operatorname{ht} f \circ g = \operatorname{ht} f + \operatorname{ht} g$.

□

PROOF OF THEOREM 2.10. By definition, $\operatorname{ht} F = \operatorname{ht}[p]_F$. Now $[p]_F$ is the homomorphism induced by the multiplication-by-p endomorphism $[p]_E$ of E (see Example 2.2), which has degree p^2 (see [**37**, Chapter III, Theorem 6.4(a)]). Therefore, $\deg_i [p]_E = 1$, p, or p^2. Now $[p]_F(x)$ is nonzero and has the form $[p]_F(x) = px + \cdots$, so $\operatorname{ht}[p]_F \neq 0$. The theorem follows. □

DEFINITION 2.12. An elliptic curve E defined over a field k of characteristic p is called *supersingular* if the height of its formal group law is 2. It is called *ordinary* otherwise.

For a lengthy list of conditions equivalent to supersingularity, see [**37**, Chapter V, Theorem 3.1].

CHAPTER 3

Vector bundles and $\mathbb{CP}^\infty$

1. Projective spaces and Grassmann manifolds

1.1. Definitions and basic properties. We begin by discussing the ubiquitous projective spaces and their generalizations, the Grassmann manifolds. Let V be a vector space. We shall refer to a 1-dimensional subspace of V as a *line* in V, and to an n-dimensional subspace of V as an *n-plane* in V. If $a = (a_0, \ldots, a_{n-1}) \in \mathbb{F}^n$, we let $(a_0 : \cdots : a_{n-1})$ denote the line through a. An *n-frame* in V is defined to be an n-tuple of linearly independent vectors of V. Let $\mathbb{F}$ denote either of the fields $\mathbb{R}$ or $\mathbb{C}$. For positive integers n, we let $\mathbb{FP}^n$ be the set of all lines in $\mathbb{F}^{n+1}$. We give $\mathbb{FP}^n$ the quotient topology induced by the map $q : \mathbb{F}^{n+1} - \{0\} \to \mathbb{FP}^n$ defined by $q(u) = \mathbb{F}u$. The space $\mathbb{FP}^n$ is called *n-dimensional* (*real* or *complex*) *projective space.* One may easily show that $\mathbb{RP}^n$ (respectively, $\mathbb{CP}^n$), can be given the structure of a smooth n-dimensional (respectively, $2n$-dimensional), compact manifold.

There is a chain of topological embeddings, $\mathbb{FP}^1 \subseteq \mathbb{FP}^2 \subseteq \cdots$, induced by the inclusion $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, 0)$ of $\mathbb{F}^n$ into $\mathbb{F}^{n+1}$. We may therefore define the *infinite dimensional* (*real* or *complex*) *projective space*, denoted $\mathbb{FP}^\infty$, to be the topological direct limit of the spaces $\mathbb{FP}^n$. A subset U of $\mathbb{FP}^\infty$ of is open if and only if $U \cap \mathbb{FP}^n$ is open for each positive integer n. Letting $\mathbb{F}^\infty$ be the union of the spaces $\mathbb{F}^n$, one sees that $\mathbb{FP}^\infty$ can be identified with the set of lines in $\mathbb{F}^\infty = \bigoplus_{i \geq 0} \mathbb{F}$.

Let $\mathrm{V}(n, \mathbb{F}^{n+k})$ denote the set of all n-frames in $\mathbb{F}^{n+k}$. The collection $\mathrm{V}(n, \mathbb{F}^{n+k})$ is an open subset of $\mathbb{F}^{n(n+k)}$ called the *Stiefel manifold.* We define the (*real* or *complex*) *Grassmann manifold* $\mathrm{G}(n, \mathbb{F}^{n+k})$ to be the set of n-planes in $\mathbb{F}^{n+k}$. Give $\mathrm{G}(n, \mathbb{F}^{n+k})$

the quotient topology induced by the map from $\mathrm{V}(n, \mathbb{F}^{n+k})$ to $\mathrm{G}(n, \mathbb{F}^{n+k})$ taking an n-frame to the n-plane which it spans. By definition, we have

$$\mathbb{FP}^n = \mathrm{G}(1, \mathbb{F}^{n+1}).$$

so the Grassmann manifolds are in fact a generalization of the projective spaces.

We briefly recall the definition of an oriented vector space. Let V be an n-dimensional real vector space. We define an equivalence relation on the set bases of V by declaring two bases equivalent if the determinant of the transition matrix between them is positive. Evidently, this equivalence relation partitions the set of bases of V into two parts. Each equivalence class is called an orientation of V; thus each real vector space has two distinct orientations. An *oriented vector space* V is simply the space V, together with a choice of orientation for V. A basis of V contained is called *positively oriented* if it is contained in the orientation of V, and *negatively oriented* otherwise. One may modify the above construction by considering oriented n-planes in $\mathbb{R}^{n+k}$. Let $\mathrm{G}^\circlearrowleft(n, \mathbb{R}^{n+k})$ be the set of oriented n-planes in $\mathbb{R}^{n+k}$. Define $q\colon \mathrm{V}(n, \mathbb{R}^{n+k}) \to \mathrm{G}^\circlearrowleft(n, \mathbb{R}^{n+k})$ by mapping a given n-tuple to the unique oriented n-plane for which it is a positively oriented basis. Give $\mathrm{G}^\circlearrowleft(n, \mathbb{R}^{n+k})$ the quotient topology induced by q. The space $\mathrm{G}^\circlearrowleft(n, \mathbb{R}^{n+k})$ is called an *oriented Grassmann manifold*. It is a fact that if V is a complex vector space, then its underlying real vector space has a preferred orientation. Therefore, we do not consider a complex analogue of this construction.

As their name implies, the Grassmann manifolds may be given a manifold structure.

LEMMA 3.1 ([**25**, Lemma 5.1]). *The space* $\mathrm{G}(n, \mathbb{R}^{n+k})$ *(respectively,* $\mathrm{G}(n, \mathbb{C}^{n+k})$*) can be given the structure of a smooth, compact manifold of dimension* nk *(respectively,* $2nk$*). The oriented Grassmann manifold* $\mathrm{G}^\circlearrowleft(n, \mathbb{R}^{n+k})$ *is a smooth, compact, oriented manifold of dimension* nk*).*

As before, the inclusion of $\mathbb{F}^n$ into $\mathbb{F}^{n+1}$ induces a chain of inclusions $\mathrm{G}(n,\mathbb{F}^{n+1}) \subseteq \mathrm{G}(n,\mathbb{F}^{n+2}) \subseteq \mathrm{G}(n,\mathbb{F}^{n+3}) \cdots$. Therefore, we may define the infinite (real or complex) Grassmann manifold $\mathrm{G}(n,\mathbb{F}^\infty)$ as the direct limit (with respect to k) of the spaces $\mathrm{G}(n,\mathbb{F}^{n+k})$. In like manner, one constructs the infinite oriented Grassmann manifold $\mathrm{G}^\circlearrowleft(n,\mathbb{R}^\infty)$.

1.2. Cohomology of projective spaces and Grassmann manifolds. One computes the cohomology of the projective spaces and Grassmann manifolds by representing them as CW-complexes. For basic definitions of and theorems about CW-complexes, consult [**26**, §38]. The complex projective spaces have a very simple cell structure.

THEOREM 3.2. *The complex projective space $\mathbb{CP}^n$ has the structure of a CW-complex with exactly one $2k$-cell, for each $k = 0,\ldots,n$. The infinite dimensional complex projective space $\mathbb{CP}^\infty$ has the structure of a CW-complex with one $2k$-cell for each $k \geq 0$.*

PROOF. We proceed by induction on n. The theorem holds trivially for $n = 0$, as $\mathbb{CP}^0$ is just a single point. Suppose the theorem holds for $\mathbb{CP}^{n-1}$. Let B^{2n} denote the closed, real, unit $2n$-ball, and let $e_{2n} = \mathbb{CP}^n - \mathbb{CP}^{n-1}$. Define $f\colon B^{2n} \to \mathbb{CP}^n$ by the rule

$$f(x_0,y_0,\ldots,x_{n-1},y_{n-1}) = \left(x_0+iy_0 : \cdots : x_{n-1}+iy_{n-1} : \left[1-\sum_{k=0}^{n-1}(x_k^2+y_k^2)\right]^{1/2}\right)$$

Then f maps $\operatorname{Int} B^{2n}$ homeomorphically onto e_{2n}, and maps the boundary of B^{2n} onto $\mathbb{CP}^{n-1}$, which by our induction hypothesis is a union of cells of lower dimension. The assertion about the cell structure of $\mathbb{CP}^\infty$ follows from the fact that it is the union of the spaces $\mathbb{CP}^n$. □

Thus, the cellular cochain complex of $\mathbb{CP}^n$ is

$$\mathbb{Z} \to 0 \to \mathbb{Z} \to 0 \to \cdots \to \underset{(2n-1)}{0} \to \underset{(2n)}{\mathbb{Z}} \to 0 \to 0 \to 0 \to \cdots.$$

Therefore, $H^{2k}(\mathbb{CP}^n, \mathbb{Z}) = \mathbb{Z}$, $0 \leq k \leq n$, and all of its other cohomology groups vanish. The cellular cochain complex of $\mathbb{CP}^\infty$ is

$$\mathbb{Z} \to 0 \to \mathbb{Z} \to 0 \to \cdots .$$

Therefore, $H^{2k}(\mathbb{CP}^\infty, \mathbb{Z}) = \mathbb{Z}$, $k \geq 0$, and all of its other cohomology groups vanish. To determine the ring structure of the complex projective spaces, one uses Poincaré duality; see [**26**, §68].

For a description of a cell structure for Grassmann manifolds and a computation of their cohomology, see [**25**, Chapter 6].

We summarize the results which we shall need. When discussing complex or oriented Grassman manifolds, we shall consider cohomology with coefficients in $\mathbb{Z}$. When discussing real (unoriented) Grassmann manifolds, we shall use $\mathbb{Z}/2\mathbb{Z}$ as our coefficient ring.

- The i-th cohomology group $H^i(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z})$ of real projective n-space is cyclic of order two for $0 \leq i \leq n$, and zero otherwise. If g denotes the non-zero element of $H^1(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z})$, then $H^i(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z})$ is generated by the i-fold cup product g^i. Further the cohomology ring $H^*(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z})$ is generated as a $\mathbb{Z}/2\mathbb{Z}$-algebra by g, that is,

  $$H^*(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z}) \cong (\mathbb{Z}/2\mathbb{Z})[g]/(g^{n+1}),$$

  where g has weight 1.
- The cohomology ring of $H^*(\mathbb{RP}^\infty, \mathbb{Z}/2\mathbb{Z}) = \varprojlim H^*(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z})$ is isomorphic to the power series ring $(\mathbb{Z}/2\mathbb{Z})[\![x]\!]$.
- The $2i$-th cohomology group $H^{2i}(\mathbb{CP}^n, \mathbb{Z})$ is infinite cyclic if $0 \leq i \leq n$; all other cohomology groups of $\mathbb{CP}^n$ vanish. In fact, if g is a generator of $H^2(\mathbb{CP}^n, \mathbb{Z})$, then $H^{2i}(\mathbb{CP}^n, \mathbb{Z})$ is generated by the i-fold cup product g^i. The cohomology ring $H^*(\mathbb{CP}^n, \mathbb{Z})$ is generated as a $\mathbb{Z}$-algebra by g, that is,

  $$H^*(\mathbb{CP}^n, \mathbb{Z}) \cong \mathbb{Z}[g]/(g^{n+1}),$$

where g has weight 2.

- The cohomology ring $\mathrm{H}^*(\mathbb{CP}^\infty, \mathbb{Z}) = \varprojlim \mathrm{H}^*(\mathbb{CP}^n, \mathbb{Z}/2\mathbb{Z})$ is isomorphic to the power series ring $\mathbb{Z}[\![x]\!]$.
- The cohomology ring $\mathrm{H}^*(\mathrm{G}(n, \mathbb{R}^\infty), \mathbb{Z}/2\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})[\![x_1, \ldots, x_n]\!]$.
- The cohomology ring $\mathrm{H}^*(\mathrm{G}(n, \mathbb{C}^\infty), \mathbb{Z})$ is isomorphic to $\mathbb{Z}[\![x_1, \ldots, x_n]\!]$.

2. Vector bundles

2.1. Definition and examples.

DEFINITION 3.3. Let E and B be topological spaces and $\pi\colon E \to B$ be a continuous surjection. The triple $\xi = (E, \pi, B)$ is called a *vector bundle of dimension* n, or an $\mathbb{F}^n$-bundle if the following conditions are satisfied:

(i) For each $b \in B$, the set $\pi^{-1}(b)$ has the structure of an n-dimensional $\mathbb{F}$-vector space.

(ii) There is an open cover $\mathcal{U}$ of B such that for each $U \in \mathcal{U}$, there is homeomorphism

$$h_U : U \times \mathbb{F}^n \to \pi^{-1}(U)$$

which restricts to a vector space isomorphism $h_{U,b} : \{b\} \times \mathbb{F}^n \to \pi^{-1}(b)$, for each $b \in U$. This condition is called the *local triviality condition.*

A vector bundle of dimension one will be refered to as a *line bundle.*

We call B and E the *base space* and *total space*, respectively. To avoid ambiguity, we will sometimes write $B(\xi)$ and $E(\xi)$ for the base and total spaces of a vector bundle ξ. For $b \in B$, we call the set $\pi^{-1}(b)$ the *fibre* (of π) over b and denote it by $\mathrm{Fib}_b\, \xi$.

REMARK 3.4. There are standard ways to convert complex vector bundles into real ones, and vice versa. It is clear that one may treat a $\mathbb{C}^n$-bundle as a $\mathbb{R}^{2n}$-bundle by simply forgetting about its complex structure. Conversely, if ξ is a real vector bundle, one obtains its complexification $\xi \otimes \mathbb{C}$ by tensoring each fibre with $\mathbb{C}$.

In order to turn the class of class vector bundles into a category, we must define a notion of morphism.

DEFINITION 3.5. Let ξ and η be complex vector bundles. A morphism or bundle map from ξ to η is a continuous map $f : E(\xi) \to E(\eta)$ such that f maps each fibre $\mathrm{Fib}_b\,\xi$ isomorphically onto some fibre $\mathrm{Fib}_{b'}\,\eta$. We write $f : \xi \to \eta$.

We let $\mathbf{VB}$ denote the category of vector bundles and bundle maps. If B is a topological space, we denote by $\mathbf{VB}_B$ the subcategory of vector bundles over the base space B.

Since points of the Grassmann manifolds are by definition vector spaces, it is not surprising that there exist canonical constructions of vector bundles over these spaces. To construct an n-dimensional vector bundle $\gamma_{n,k}(\mathbb{F})$ over the Grassmann manifold $\mathrm{G}(n, \mathbb{F}^{n+k})$, let

$$E(\gamma_{n,k}(\mathbb{F})) = \{\, (H, x) \in \mathrm{G}(n, \mathbb{F}^{n+k}) \times \mathbb{F}^{n+k} \mid x \in H \,\},$$

and define $\pi : E(\gamma_{n,k}(\mathbb{F})) \to \mathrm{G}(n, \mathbb{F}^{n+k})$ by the rule $\pi(H, x) = H$. The bundle $\gamma_{n,k}(\mathbb{F})$ does indeed satisfy the local triviality condition; for details see [**25**, §6].

We may construct an n-dimensional bundle $\gamma_n(\mathbb{F})$ over the infinite Grassmann manifold $\mathrm{G}(n, \mathbb{F}^\infty)$ by taking the direct limit (with respect to k) of the bundles $\gamma_{n,k}(\mathbb{F})$. The total space of $\gamma_n(\mathbb{F})$ may be identified with the set

$$\{\, (H, x) \in \mathrm{G}(n, \mathbb{F}^\infty) \times \mathbb{F}^\infty \mid x \in H \,\},$$

with the projection map π defines as above.

Oriented vector bundles. Fix an orientation of $\mathbb{R}^n$, and let ξ be a real n-bundle. An *orientation of* ξ is a choice of orientation of each fibre of ξ such that the following compatibility condition is satisfied:

There exists a trivialization $\mathcal{U}$ of ξ with coordinate charts h_U, $U \in \mathcal{U}$ such that the map $x \mapsto h_U(b, x)$ is an orientation-preserving[1] isomorphism of $\mathbb{R}^n$ with $\mathrm{Fib}_b\, \xi$ whenever $b \in U$.

Using the fact that points of $\mathrm{G}^{\circlearrowleft}(n, \mathbb{R}^{n+k})$ are oriented n-planes, there exists a tautological construction of an oriented n-plane bundle over $\mathrm{G}^{\circlearrowleft}(n, \mathbb{R}^{n+k})$. This construction is completely analogous to that in the non-oriented case. We denote this bundle by $\gamma^{\circlearrowleft}_{n,k}$. Taking direct limits, we may also define a tautological oriented n-plane bundle $\gamma^{\circlearrowleft}_n$ over the infinite oriented Grassmann manifold $\mathrm{G}^{\circlearrowleft}(n, \mathbb{R}^\infty)$. Again, the details of this construction are the same as in the non-oriented case.

There is another way of looking at vector bundles which is often illuminating. Suppose ξ is an $\mathbb{F}^n$-bundle, with open cover $\mathcal{U}$ and coordinate charts h_U as in Definition 3.3(ii). Suppose elements U and V of $\mathcal{U}$ intersect nontrivially. Then the map

$$h_{UV} \colon (U \cap V) \times \mathbb{F}^n \to (U \cap V) \times \mathbb{F}^n$$

defined by $h_{UV} = h_U \circ h_V^{-1}$ (suitably restricting domains) is a homeomorphism. Further, for any $b \in U \cap V$, the map $h_{UV}|_{\{b\} \times \mathbb{F}^n}$ may be naturally identified with an element of $\mathrm{GL}(n, \mathbb{F})$. It is easy to see that the map

$$g_{UV} \colon U \cap V \to \mathrm{GL}(n, \mathbb{F})$$

defined by $g_{UV}(b) = h_{UV}|_{\{b\} \times \mathbb{F}^n}$ is continuous. The maps g_{UV} are called *transition maps*.

In fact, the transition maps g_{UV} determine ξ up to isomorphism. Let

$$E = \coprod_{U \in \mathcal{U}} U \times \mathbb{F}^n \Big/ \sim$$

where the equivalence relation $\sim$ identifies points $(b, x) \in U \times \mathbb{F}^n$ and $(b, y) \in V \times \mathbb{F}^n$ if $g_{UV}(b)(x) = y$. One may easily show that E is the total space of a vector bundle

[1] i.e., the map sends positively oriented bases of $\mathbb{R}^n$ to positively oriented bases of $\mathrm{Fib}_b\, \xi$

isomorphic to ξ. One calls the group $\mathrm{GL}(n, \mathbb{F})$ the *structural group* of $\mathbb{F}^n$-bundles, and thinks of the maps g_{UV} as specifying some sort of "glueing data". For more details on this point of view, see [**17**, Chapter 5].

One can show that a real n-plane bundle ξ is orientable (i.e. can be given an orientation) if and only if one may find a trivialization $\mathcal{U}$ of ξ with coordinate charts h_U, $U \in \mathcal{U}$, such that the corresponding transtition functions g_{UV} take values in the subgroup of $\mathrm{GL}(n, \mathbb{R})$ consisting of matrices with positive determinant.

2.2. Operations on vector bundles. There are many ways to make new vector bundles out of old ones. For instance, if ξ is a vector bundle, and $A \subseteq B(\xi)$, there is an obvious way to restict ξ to a bundle $\xi|_A$ over A. Also, if η is another bundle, then there is a canonical construction of a product bundle $\xi \times \eta$ over the base space $B(\xi) \times B(\eta)$.

Somewhat more exotic is the construction of the pullback of a vector bundle. Suppose η is a vector bundle with projection $\pi\colon E(\eta) \to B(\eta)$, and f is a continuous map from a space B into $B(\eta)$. Then we may pull back the bundle η to construct a bundle $f^*\eta$ over B with total space

$$E = \{\, (b, e) \in B \times E(\eta) \mid f(b) = \pi(e) \,\},$$

and projection map p sending $(b, e) \in E$ to $b \in B$. Again, one must verify the local triviality condition. If we define $\widehat{f}\colon E \to E(\eta)$ by $\widehat{f}(b, e) = e$, then it follows that $\widehat{f}$ is a bundle map and that the following diagram is cartesian:

$$\begin{array}{ccc} E & \xrightarrow{\widehat{f}} & E(\eta) \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle \pi} \\ B & \xrightarrow[f]{} & B(\eta) \end{array}$$

The vector bundle $f^*\eta$ constructed above is called the *pullback of η by f*.

Conversely, suppose $g : \xi \to \eta$ is a bundle map. Let $\overline{g}\colon B(\xi) \to B(\eta)$ be defined such that the formula $g(\mathrm{Fib}_b\, \xi) = \mathrm{Fib}_{\overline{g}(b)}\, \eta$ holds. Then one can show that ξ is

isomorphic to $\overline{g}^*\eta$. This illustrates the intimate relationship between pullbacks and bundle maps.

One often thinks of a vector bundle as a continuous family of vector spaces lying over a topological space. For this reason, it seems natural to attempt to define analogues of popular vector space constructions (direct sum, tensor product, dual, ...) for vector bundles. Below, we indicate how this may be accomplished.

Let $\mathbf{VS}$ denote the category of vector spaces over $\mathbb{F}$. To unify (and simplify) our presentation, we make the following definition.

DEFINITION 3.6. Let T be a functor from the product category $\mathbf{VS}^n$ to $\mathbf{VS}$. We say that T is continuous if for any vector spaces $V_1, \ldots, V_n$, $W_1, \ldots, W_n$ in $\mathbf{VS}$, the map

$$\mathrm{Hom}(V_1, W_1) \times \cdots \times \mathrm{Hom}(V_n, W_n) \to \mathrm{Hom}(T(V_1, \ldots, V_n), T(W_1, \ldots, W_n))$$

induced by T is continuous. In other words, the map $T(f_1, \ldots, f_n)$ depends continuously on $f_1, \ldots, f_n$.

The functors $\oplus$, $\otimes$, and $^\vee$ (dual) are easily seen to be continuous.

THEOREM 3.7 ([**25**, §3(f)]). *Let $\xi_1, \ldots, \xi_n$ be vector bundles over the common base space B, and let $T\colon \mathbf{VS}^n \to \mathbf{VS}$ be a continuous functor. Then there is a vector bundle $\xi = T(\xi_1, \ldots, \xi_n)$ over B such that for all $b \in B$, the fibre $\mathrm{Fib}_b\, \xi$ is equal to $T(\mathrm{Fib}_b\, \xi_1, \ldots, \mathrm{Fib}_b\, \xi_n)$.*

PROOF. Let

$$E = \coprod_{b \in B} T(\mathrm{Fib}_b\, \xi_1, \ldots, \mathrm{Fib}_b\, \xi_n)$$

(we the symbol $\coprod$ for disjoint union). Define $\pi : E \to B$ by the rule

$$\pi(T(\mathrm{Fib}_b\, \xi_1, \ldots, \mathrm{Fib}_b\, \xi_n)) = b,$$

and set $\xi = (E, \pi, B)$.

For each $i \leq n$, find a local coordinate system (U, h_i) for ξ_i. Writing m_i for the dimension of (each fibre of) ξ_i and π_i for the projection from $E(\xi_i)$ to B, we have that the map h_i is a homeomorphism from $U \times \mathbb{F}^{m_i}$ onto $\pi_i^{-1}(U)$ mapping $\{b\} \times \mathbb{F}^{m_i}$ isomorphically onto $\mathrm{Fib}_b\, \xi_i$. Let $h_{i,b} = h_i | \{b\} \times \mathbb{F}^{m_i}$. By the functoriality of T, the map

$$T(h_{1,b}, \ldots, h_{n,b}) : T(\mathbb{F}^{m_1}, \ldots, \mathbb{F}^{m_n}) \to T(\mathrm{Fib}_b\, \xi_1, \ldots, \mathrm{Fib}_b\, \xi_n)$$

is an isomorphism. By the continuity of T, the map $h_U : U \times T(\mathbb{F}^{m_1}, \ldots, \mathbb{F}^{m_n}) \to \pi^{-1}(U)$ defined by the rule

$$h_U|_{\{b\} \times T(\mathbb{F}^{m_1}, \ldots, \mathbb{F}^{m_n})} = T(h_{1,b}, \ldots, h_{n,b})$$

is a homeomorphism.

If U and U' are coordinate neighbourhoods for all the ξ_i, then it is clear that the map $h_{U'}^{-1} \circ h_U$ is a homeomorphism of $(U \cap U') \times T(\mathbb{F}^{m_1}, \ldots, \mathbb{F}^{m_n})$ onto itself. Therefore, there is a unique topology on E such that each map h_U constructed above is continuous.

Letting $\mathcal{U}$ be the collection of all open $U \subseteq B$ such that U is a coordinate neighbourhood of each ξ_i, we have shown that $\mathcal{U}$ is a trivialization of ξ. This completes the proof. □

It is easy to show that the correspondence

$$(\xi_1, \ldots, \xi_n) \mapsto T(\xi_1, \ldots, \xi_n)$$

extends to a functor from $(\mathbf{VB}_B)^n$ to $\mathbf{VB}$.

A continuous functor unique to the category of complex vector spaces is the complex conjugation functor. Given a complex vector space V, we let $\overline{V}$ denote the vector space whose underlying abelian group is V, and whose scalar multiplication is defined by twisting that of V by complex conjugation. That is, if $s\colon \mathbb{C} \times V \to V$ represents scalar multiplication in V, and $c\colon \mathbb{C} \to \mathbb{C}$ is complex conjugation, then scalar multiplication in $\overline{V}$ is given by $s \circ (c \times \mathrm{id})$.

Let ω be a complex vector bundle. We denote by $\overline{\omega}$ the vector bundle obtained from ω by applying the complex conjugation functor. We call it the *conjugate* of ω. A fibre $\mathrm{Fib}_b\,\overline{\omega}$ of $\overline{\omega}$ is naturally identified with the vector space $\overline{\mathrm{Fib}_b\,\omega}$.

Note that even though $V \cong \overline{V}$ for any vector space V (they have the same dimension), it is *not* true in general that a complex vector bundle ω is isomorphic to its conjugate $\overline{\omega}$. This is because there is generally no canonical $\mathbb{C}$-vector space isomorphism between V and $\overline{V}$ (complex conjugation is not $\mathbb{C}$-linear). One may construct bundle isomorphisms $\omega|_U \cong \overline{\omega}|_U$ for suitable sets U, but the lack of a natural choice for these isomorphisms may prevent them from being mutually compatible.

We show, for example, that the tangent bundle τ of $\mathbb{CP}^1$ is not isomorphic to its conjugate bundle, $\overline{\tau}$. Observe that if V is a 1-dimensional complex vector space, and $\varphi\colon V \to \overline{V}$ is a linear isomorphism, then φ is given by reflecting V across some line. Suppose there was an isomorphism f from τ to $\overline{\tau}$. Let $T_P\mathbb{CP}^1$ denote the tangent space to $\mathbb{CP}^1$ at the point P. Then f induces a linear isomorphism $f_P\colon T_P\mathbb{CP}^1 \to \overline{T_P\mathbb{CP}^1}$, which must be given by reflection across a line ℓ_P. We may identify $\mathbb{CP}^1$ with the 2-sphere S^2 and view ℓ_P as a line in $\mathbb{R}^3$ tangent to S^2 at P. Since f is a bundle morphism, it follows that the lines ℓ_P vary continuously, and cut out a 1-dimensional subbundle of the tangent bundle of the 2-sphere, S^2. Let

$$X = \{\, (P, v) \mid P \in S^2,\, v \in \ell_P, \text{ and } \|v\| = 1 \,\}.$$

Since the lines ℓ_P vary continuously, the space X is naturally a double covering of the 2-sphere S^2. But S^2 is simply connected, so X must be the trivial double covering. Each branch of the covering X represents a nonvanishing vector field on S^2. It is well known that such a vector field does exist; see for instance, [**26**, Corollary 21.6]. Thus, the tangent bundle of $\mathbb{CP}^1$ is not isomorphic to its conjugate.

Continuous functors interact very nicely with pullbacks.

LEMMA 3.8. *Let B and B' be topological spaces, $\xi_1, \ldots, \xi_n$ be vector bundles over B and $f\colon B' \to B$ be continuous. Suppose that $T\colon \mathbf{VS}^n \to \mathbf{VS}$ is a continuous*

functor. Then

$$T(f^*\xi_1, \ldots, f^*\xi_n) \cong f^*T(\xi_1, \ldots, \xi_n).$$

There is another way in which we may mutate continuous functors of vector spaces into functors of vector bundles. Let $B_1, \ldots, B_n$ be topological spaces and $T\colon \mathbf{VS}^n \to \mathbf{VS}$ be a continuous functor. Then one can show using arguments analogous to those presented above that T induces a functor

$$\widetilde{T}\colon \mathbf{VB}_{B_1} \times \cdots \times \mathbf{VB}_{B_n} \to \mathbf{VB}_{B_1 \times \cdots \times B_n}.$$

One proves this fact using the following theorem.

THEOREM 3.9. *Let $\xi_1, \ldots, \xi_n$ be vector bundles over base spaces $B_1, \ldots, B_n$, respectively, and let $T\colon \mathbf{VS}^n \to \mathbf{VS}$ be a continuous functor. Then there is a vector bundle $\widetilde{\xi} = \widetilde{T}(\xi_1, \ldots, \xi_n)$ over $B_1 \times \cdots \times B_n$ such that for all $b = (b_1, \ldots, b_n) \in B_1 \times \cdots \times B_n$, the fibre $\operatorname{Fib}_b \xi$ is equal to $T(\operatorname{Fib}_b \xi_1, \ldots, \operatorname{Fib}_b \xi_n)$.*

It is traditional to denote the functor $\widetilde{\otimes}\colon \mathbf{VB}_{B_1} \times \mathbf{VB}_{B_2} \to \mathbf{VB}_{B_1 \times B_2}$ by $\boxtimes$.

The above constructions are related in the following way.

LEMMA 3.10. *Let $\xi_1, \ldots, \xi_n$ be vector bundles over the common base space B. Let $T\colon \mathbf{VS}^n \to \mathbf{VS}$ be a continuous functor, $d\colon B \to B^n$ be the diagonal map, and $p_i\colon B^n \to B$ be the i-th projection map. Then*

(i) $T(\xi_1, \ldots, \xi_n) \cong d^*\widetilde{T}(\xi_1, \ldots, \xi_n)$,

(ii) $\widetilde{T}(\xi_1, \ldots, \xi_n) \cong T(p_1^*\xi_1, \ldots, p_n^*\xi_n)$.

Both isomorphisms are canonical.

For vector spaces U, V, and W, we know that $U \oplus V \cong V \oplus U$, $U \otimes V \cong V \otimes U$, $U \otimes (V \otimes W) \cong (U \otimes V) \otimes W$, and $U \otimes (V \oplus W) \cong (U \otimes V) \oplus (U \otimes W)$. The following result shows that analogues of these identities hold for vector bundles ξ, η, and ζ. The proof is a just diagram chase.

LEMMA 3.11. *Let B, B_1, ..., B_n be a topological spaces, and let S and T be naturally equivalent continuous functors from the n-fold cartesian product $\mathbf{VS}^n$ into*

VS. *Then S and T remain naturally equivalent when viewed as functors from $(\mathbf{VB}_B)^n$ into $\mathbf{VB}_B$. Also, the functors $\widetilde{S}$ and $\widetilde{T}$ from $\mathbf{VB}_{B_1} \times \cdots \times \mathbf{VB}_{B_n}$ to $\mathbf{VB}_{B_1 \times \cdots \times B_n}$ are naturally equivalent.*

2.3. Euclidean and Hermitian metrics on vector bundles. One may also study vector bundles in which each fibre has the structure of an inner product space. A *Euclidean metric* on a real vector bundle ξ is a continuous map

$$E(\xi \oplus \xi) \to \mathbb{R}, \quad (e_1, e_2) \mapsto \langle e_1, e_2 \rangle \in \mathbb{R}$$

such that for each $b \in B$, its restriction to $\mathrm{Fib}_b(\xi \oplus \xi)$ defines a Euclidean inner product on $\mathrm{Fib}_b \xi$. A *Hermitian metric* on a complex vector bundle ω is defined in like manner, except one insists that the metric endows each fibre of ω with a Hermitian inner product.

One shows that any vector bundle over a "reasonable" base space admits a metric.

DEFINITION 3.12. A topological space X is said to be *paracompact* if any open cover of X has an open, locally finite refinement. That is, if $\mathcal{U}$ is any open cover of X, there exists another open cover $\mathcal{V}$ of X such that

(i) For each $V \in \mathcal{V}$, there is some $U \in \mathcal{U}$ with $V \subseteq U$.
(ii) Each point of X has a neighbourhood that meets only finitely many elements of $\mathcal{V}$.

Most non-pathological spaces, including all metric spaces and all manifolds, are paracompact. We will deduce the existence of metrics on vector bundles over paracompact base spaces using the notion of a Gauss map. Let ξ be an n-dimensional vector bundle. A continuous map of $f\colon E(\xi) \to \mathbb{F}^{n+k}$ is called a *Gauss map* if f is linear and injective on each fibre of ξ. One may prove the following result, which we will use again later. For details, see [**17**, Chapter 3, §5] or [**25**, Lemma 5.3, Theorem 5.6].

THEOREM 3.13. *Any vector bundle over a paracompact base space admits a Gauss map.*

COROLLARY 3.14. *Any real (respectively, complex) vector bundle over a paracompact base space admits a Euclidean (respectively, Hermitian) metric.*

PROOF. Let ξ be a real, n-dimensional vector bundle over the paracompact base space B, and let $f\colon E(\xi) \to \mathbb{R}^{n+k}$ be a Gauss map. Letting $\langle -, - \rangle$ denote the standard Euclidean inner product on $\mathbb{R}^{n+k}$, one verifies easily that the correspondence $(e_1, e_2) \mapsto \langle f(e_1), f(e_2) \rangle$ defines a Euclidean metric on ξ. Hermitian metrics on complex vector bundles are constructed similarly. □

REMARK 3.15. One may also prove the above corollary using a standard partition of unity argument.

The existence of metrics allows us to relate vector bundles with their duals.

LEMMA 3.16.

(i) *Let ξ be a finite dimensional, real vector bundle with Euclidean metric $\langle -, - \rangle$. Then the correspondence $e \mapsto \langle -, e \rangle$ defines an isomorphism between ξ and its dual, $\xi^\vee$.*

(ii) *Let ω be a finite dimensional, complex vector bundle with Hermitian metric $\langle -, - \rangle$. Then the correspondence $e \mapsto \langle -, e \rangle$ defines an isomorphism between its conjugate bundle $\overline{\omega}$, and its dual bundle, $\omega^\vee$.*

The proof of this lemma is an easy generalization of the standard argument from linear algebra. Using a vector bundle analogue of the Graham-Schmidt orthogonalization algorithm, one may prove the following lemma, which asserts that one may always find orthogonal gluing data. For details, see [**17**, Chapter 3, §9].

LEMMA 3.17. *Let ξ be a real (respectively, complex) vector bundle with a Euclidean (respectively, Hermitian) metric. Then there exists an open cover $\mathcal{U}$ of $B(\xi)$ with coordinate charts h_U, $U \in \mathcal{U}$, such that the corresponding transition maps g_{UV} (see*

§2.1) take values in the group $\mathrm{O}(n)$ *of orthogonal matrices (respectively, the group* $\mathrm{U}(n)$ *of unitary matrices).*

Thus the existence of a Euclidean (respectively, Hermitian) metric facilitates a reduction of the structural group of a real (respectively, complex) vector bundle from $\mathrm{GL}(n,\mathbb{R})$ (respectively, $\mathrm{GL}(n,\mathbb{C})$) to the group $\mathrm{O}(n)$ (respectively, $\mathrm{U}(n)$). Similarly, the existence of a Euclidean metric allows one to reduce the structural group of an oriented $\mathbb{R}^n$-bundle to the group $\mathrm{SO}(n)$ of orthogonal matrices with determinant 1.

2.4. Classification of vector bundles. In §2.1, we constructed canonical vector bundles over the Grassmann manifolds. As it turns out, these bundles classify all finite dimensional vector bundles over paracompact spaces, in a sense to be made precise below. One may prove the following:

THEOREM 3.18 ([**25**, Theorem 5.6]). *Any* $\mathbb{F}^n$*-bundle* ξ *over a paracompact base space admits a bundle map into the canonical* n*-plane bundle* $\gamma_n(\mathbb{F})$ *over the infinite Grassmann manifold,* $\mathrm{G}(n,\mathbb{F}^\infty)$. *Thus, every such bundle* ξ *determines a map* $f\colon B(\xi) \to \mathrm{G}(n,\mathbb{F}^\infty)$ *such that* $\xi = f^*\gamma_n(\mathbb{F})$.

PROOF. Let $\widehat{g}\colon E(\xi) \to \mathbb{F}^{n+k} \subseteq \mathbb{F}^\infty$ be a Gauss map, the existence of which was asserted in Theorem 3.13. Define $g\colon E(\xi) \to E(\gamma_n(\mathbb{F}))$ by the rule

$$g(e) = (\widehat{g}(\text{fibre through } e), \widehat{g}(e)).$$

One may verify the continuity of g using the local triviality of ξ. It is clear that g is fibre preserving. Therefore, g is a bundle map. □

This result may be strengthened:

THEOREM 3.19 ([**17**, Chapter 3, Theorem 7.2]). *Two* $\mathbb{F}^n$*-bundles* ξ *and* η *over the same base space* B *are isomorphic if and only if the determine homotopic maps from* B *to* $\mathrm{G}(n,\mathbb{F}^\infty)$.

Thus, the isomorphism classes of $\mathbb{F}^n$ bundles over a paracompact base space B are in one-to-one correspondence with the set $[B, \mathrm{G}(n,\mathbb{F}^\infty)]$ of homotopy classes of

maps from B into the infinite Grassmann manifold $\mathrm{G}(n, \mathbb{F}^\infty)$. For this reason, the space $\mathrm{G}(n, \mathbb{F}^\infty)$ is often called the *classifying space*, or *universal base space* for $\mathbb{F}^n$-bundles. Topologists denote the classifying spaces $\mathrm{G}(n, \mathbb{R}^\infty)$ and $\mathrm{G}(n, \mathbb{C}^\infty)$ by $\mathrm{BO}(n)$ and $\mathrm{BU}(n)$, respectively. The 'B' stands for 'base space'; the 'O' and 'U' stand for 'orthogonal' and 'unitary', respectively. The notation $\mathrm{BO}(n)$ is appropriate since it is the universal base space for vector bundles with $\mathrm{O}(n)$ as structural group (see Lemma 3.17). A similar remark holds for $\mathrm{BU}(n)$. We make special note of the fact that $\mathrm{BU}(1) = \mathbb{CP}^\infty$.

Analogously, one may show that the infinite oriented Grassmann manifold $\mathrm{G}^\circlearrowleft(n, \mathbb{R}^\infty)$ is the classifying space for oriented $\mathbb{R}^n$-bundles. This space is often denote $\mathrm{BSO}(n)$ because it is the universal base space for bundles with structural group $\mathrm{SO}(n)$.

3. A group law on $\mathbb{CP}^\infty$ (almost)

We briefly digress from our general discussion of vector bundles to discuss an important application of the notions discussed above. Borrowing notation from algebraic geometry, we let $\operatorname{Pic} B$ be the set of isomorphism classes of line bundles over the paracompact topological space B. The following theorem is fundamental to understanding the structure of $\operatorname{Pic} B$.

THEOREM 3.20. *The function $(\xi, \eta) \mapsto \xi \otimes \eta$ is an abelian group law on the set $\operatorname{Pic} B$. The neutral element for this group law is the trivial line bundle, ε (with total space $B \times \mathbb{F}$), and the inverse of a bundle ξ is given by its dual bundle, $\xi^\vee$.*

PROOF. The tensor product operation on vector bundles is associative and commutative by Lemma 3.11, and it is easy to check that $\xi \otimes \varepsilon \cong \xi$. That $\xi^\vee$ serves as an inverse of ξ follows easily from the fact that for a one dimensional vector space V, the tensor product $V \otimes V^\vee$ is canonically isomorphic to the field of scalars $\mathbb{F}$. □

REMARK 3.21. By Lemma 3.16(i), the group of *real* line bundles over a given paracompact base space B has exponent two. By Lemma 3.16(ii), the bundle conjugation

acts as inversion on the group of *complex* line bundles over a given paracompact base space B.

Using the universal property of the space $\mathbb{CP}^\infty$ in conjunction with the above theorem, we can show that $\mathbb{CP}^\infty$ actually has the structure of a "group up to homotopy". Let the symbol $\sim$ denote the homotopy relation.

DEFINITION 3.22. Let X be a topological space and $m\colon X \to X$ be a continuous map. We say that m is an abelian group law up to homotopy if there exist continuous maps $e\colon X \to X$ and $i\colon X \to X$ such that

(i) (Associativity) $m \circ (m, \mathrm{id}_X) \sim m \circ (\mathrm{id}_X, m)$,
(ii) (Commutativity) $m \circ s \sim m$ where $s\colon X \times X \to X \times X$ be given by $s(x, y) = (y, x)$,
(iii) (Identity) $m \circ (\mathrm{id}_X, e) \sim \mathrm{id}_X$,
(iv) (Inverse) $m \circ (\mathrm{id}_X, i) \sim e$.

Let $\gamma = \gamma_1(\mathbb{C})$ and ε be the universal and trivial line bundles over $\mathbb{CP}^\infty$, respectively, and consider the line bundle $\gamma \boxtimes \gamma$ (in the sense of Theorem 3.9) over the product $\mathbb{CP}^\infty \times \mathbb{CP}^\infty$. By Theorem 3.19, applicable as $\mathbb{CP}^\infty \times \mathbb{CP}^\infty$ is paracompact, there exists a continuous map $m\colon \mathbb{CP}^\infty \times \mathbb{CP}^\infty \to \mathbb{CP}^\infty$, unique up to homotopy, such that $\gamma \boxtimes \gamma \cong m^*\gamma$. Let e and i be the continuous maps from $\mathbb{CP}^\infty$ to $\mathbb{CP}^\infty$, unique up to homotopy, such that $\varepsilon \cong e^*\gamma$ and $\gamma^\vee \cong i^*\gamma$.

THEOREM 3.23. *The map m gives $\mathbb{CP}^\infty$ the structure of an abelian group, up to homotopy, with identity map e and inverse map i.*

PROOF. We must verify (i)-(iv) of Definition 3.22. We will verify (iv), the rest being similar. Let $p_1, p_2 : \mathbb{CP}^\infty \times \mathbb{CP}^\infty \to \mathbb{CP}^\infty$ be the projection maps. Then

$$\begin{aligned}
(m \circ (\mathrm{id}, i))^*\gamma &\cong (\mathrm{id}, i)^* m^* \gamma \\
&= (\mathrm{id}, i)^*\gamma \boxtimes \gamma && \text{by the above,} \\
&= (\mathrm{id}, i)^*(p_1^*\gamma \otimes p_2^*\gamma) && \text{by Lemma 3.10,} \\
&= ((\mathrm{id}, i)^* p_1^*\gamma) \otimes ((\mathrm{id}, i)^* p_2^*\gamma) && \text{by Lemma 3.8,} \\
&= (p_1 \circ (\mathrm{id}, i))^*\gamma \otimes (p_2 \circ (\mathrm{id}, i))^*\gamma \\
&= \mathrm{id}^*\gamma \otimes i^*\gamma \\
&\cong \gamma \otimes \gamma^\vee \\
&\cong \varepsilon && \text{by Theorem 3.20.}
\end{aligned}$$

We have shown that the map $m \circ (\mathrm{id}, i)$ pulls back γ to ε. Therefore, by the uniqueness of e up to homotopy, we must have $m \circ (\mathrm{id}, i) \sim e$. □

We can actually give explicit formulas for the maps e, i, and m. Let $a = (a_0, a_1, \ldots)$ and $b = (b_0, b_1, \ldots)$ be elements of $\mathbb{C}^\infty$. We let A and B denote the lines through a and b, respectively. View A and B as elements of $\mathbb{CP}^\infty$. Define a bilinear composition law $*$ on $\mathbb{C}^\infty$ by the rule

$$a * b = (c_0, c_1, \ldots), \quad \text{where} \quad c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Notice that if we identify $\mathbb{C}^\infty$ with the polynomial ring $\mathbb{C}[x]$ by identifying a with the polynomial $a_0 + a_1 x + \cdots$, then the composition law $*$ corresponds to polynomial multiplication. Therefore, if a and b are nonzero, then $a * b$ is also nonzero. It is also clear that $(\lambda a) * (\kappa b) = \lambda\kappa(a * b)$ for all complex numbers λ and κ. Therefore, $*$ descends to a map from $\mathbb{CP}^\infty \times \mathbb{CP}^\infty \to \mathbb{CP}^\infty$. With this point of view, we have that $a * b \in A * B$

THEOREM 3.24. *Let $e\colon \mathbb{CP}^\infty \to \mathbb{CP}^\infty$ be any constant map, $i\colon \mathbb{CP}^\infty \to \mathbb{CP}^\infty$ be induced by complex conjugation, and $m\colon \mathbb{CP}^\infty \times \mathbb{CP}^\infty \to \mathbb{CP}^\infty$ be defined by the formula $m(A,B) = A * B$. Then $e^*\gamma \cong \varepsilon$, $i^*\gamma \cong \gamma^\vee$, and $m^*\gamma \cong \gamma \boxtimes \gamma$.*

PROOF. It is clear that $e^*\gamma \cong \varepsilon$. By Lemma 3.16(ii), we may show instead that $i^*\gamma \cong \overline{\gamma}$. To demonstrate this, it suffices to produce a bundle map $I\colon E(\overline{\gamma}) \to E(\gamma)$ such that the diagram

$$\begin{array}{ccc} E(\overline{\gamma}) & \xrightarrow{I} & E(\gamma) \\ \downarrow & & \downarrow \\ \mathbb{CP}^\infty & \xrightarrow[i]{} & \mathbb{CP}^\infty \end{array}$$

commutes (see §2.2). Define $I\colon E(\overline{\gamma}) \to E(\gamma)$ by the rule $I(A,a) = (\overline{A}, \overline{a})$, where $\overline{a} = (\overline{a}_0, \overline{a}_1, \ldots)$, and $\overline{A}$ is the line through $\overline{a}$. One verifies directly that I is a bundle map which completes the above diagram.

Let A, $B \in \mathbb{CP}^\infty$, and consider the mapping from $(\mathrm{Fib}_A\,\gamma) \times (\mathrm{Fib}_B\,\gamma)$ to $\mathrm{Fib}_{A*B}\,\gamma$ given by

$$((A,a),(B,b)) \mapsto (A * B, a * b).$$

This is a well defined, bilinear map. Therefore, it induces a bundle map $M\colon E(\gamma \boxtimes \gamma) \to E(\gamma)$ defined by

$$M((A,a) \otimes (B,b)) = (A * B, a * b).$$

It is clear that the diagram,

$$\begin{array}{ccc} E(\gamma \boxtimes \gamma) & \xrightarrow{M} & E(\gamma) \\ \downarrow & & \downarrow \\ \mathbb{CP}^\infty \times \mathbb{CP}^\infty & \xrightarrow[m]{} & \mathbb{CP}^\infty \end{array}$$

commutes, so we may conclude that $m^*\gamma \cong \gamma \boxtimes \gamma$. □

4. Characteristic classes of vector bundles

We continue our discussion of vector bundles by introducing a family invariants of known as *characteristic classes.* These characteristic classes are special cohomology classes of the base space of a bundle which contain much useful information. For details on the constructions of these characteristic classes, see [**25**].

We first introduce the *Stiefel-Whitney classes.* One may show that for any real vector bundle ξ, there exists a unique sequence of cohomology classes $w_i(\xi) \in \mathrm{H}^i(B(\xi), \mathbb{Z}/2\mathbb{Z})$, $i \geq 0$, with the following properties:

(i) The class $w_0(\xi)$ is the unit element of $\mathrm{H}^0(B(\xi), \mathbb{Z}/2\mathbb{Z})$, and $w_i(\xi)$ is zero for $i > \dim_{\mathbb{R}} \xi$.

(ii) If $f : \xi \to \eta$ is a bundle map, then $w_i(\xi) = f^* w_i(\eta)$.

(iii) If ξ and η are vector bundles over the same base space, then

$$w_k(\xi \oplus \eta) = \sum_{i=0}^{k} w_i(\xi) \cup w_{k-i}(\eta).$$

(iv) Letting $\gamma_{1,1}(\mathbb{R})$ denote the canonical (Hopf) line bundle over $\mathbb{RP}^1$ (see page 46), the class $w_1(\gamma_{1,1}(\mathbb{R}))$ is nonzero.

The cohomology class $w_i(\xi)$ is called the *i-th Stiefel-Whitney class* of the vector bundle ξ. Letting

$$w(\xi) = w_0(\xi) + w_1(\xi) + \cdots \in \mathrm{H}^*(B(\xi), \mathbb{Z}/2\mathbb{Z}),$$

we express property (iii) in the form $w(\xi \oplus \eta) = w(\xi) \cup w(\eta)$. We call $w(\xi)$ the *total Stiefel-Whitney class* of ξ.

One may compute the Stiefel-Whitney classes of a cartesian product of vector bundles in terms of the Stiefel-Whitney classes of the factors.

LEMMA 3.25. *Let ξ and η be vector bundles. Then*

$$w_k(\xi \times \eta) = \sum_{i=0}^{k} w_i(\xi) \times w_{k-i}(\eta).$$

Here, $w_i(\xi) \times w_{k-i}(\eta)$ denotes the *cohomology cross product* $w_i(\xi)$ and $w_{k-i}(\eta)$. For its definition and properties, see [**26**, p. 355ff].

PROOF. Let π_1 and π_2 be the projection maps from $B(\xi) \times B(\eta)$ onto $B(\xi)$ and $B(\eta)$, respectively. Then $\xi \times \eta \cong (\pi_1^*\xi) \oplus (\pi_2^*\eta)$. Computing, using the naturality of characteristic classes and a standard fact relating cup and cross products in cohomology, we see that

$$\begin{aligned} w_k(\xi \times \eta) &= w_k((\pi_1^*\xi) \oplus (\pi_2^*\eta)) \\ &= \sum_{i=0}^{k} w_i(\pi_1^*\xi) \cup w_{k-i}(\pi_2^*\eta) \\ &= \sum_{i=0}^{k} (\pi_1^* w_i(\xi)) \cup (\pi_2^* w_{k-i}(\eta)) \\ &= \sum_{i=0}^{k} w_i(\xi) \times w_{k-i}(\eta). \end{aligned}$$

□

One may use the Stiefel-Whitney classes to derive interesting non-embedding results for manifolds (see, for instance, [**25**, Theorem 4.8]), and important theorems concerning the existence of real division algebras (see, for instance, [**25**, Theorem 4.7]). The fact we have chosen our coefficient ring to be $\mathbb{Z}/2\mathbb{Z}$ makes Stiefel-Whitney classes ideally suited to studying non-oriented manifolds. They will come up again later when we discuss non-oriented cobordism.

We now introduce the *Chern classes*, characteristic classes of complex vector bundles. For every complex vector bundle ω, there is a unique sequence of cohomology classes $c_i(\omega) \in \mathrm{H}^{2i}(B(\omega), \mathbb{Z})$ satisfying properties completely analogous to properties (i)-(iv) of the Stiefel-Whitney classes.

(i) The class $c_0(\omega)$ is the unit element of $\mathrm{H}^0(B(\omega), \mathbb{Z})$, and $c_i(\omega)$ is zero for $i > \dim_{\mathbb{C}} \omega$.

(ii) If $f : \omega \to \zeta$ is a bundle map, then $c_i(\omega) = f^* c_i(\zeta)$.

(iii) If ω and ζ are vector bundles over the same base space, then

$$c_k(\omega \oplus \zeta) = \sum_{i=0}^{k} c_i(\omega) \cup c_{k-i}(\zeta).$$

(iv) Letting $\gamma_{1,1}(\mathbb{C})$ denote the canonical (Hopf) line bundle over $\mathbb{CP}^1$ (see page 46), the class $c_1(\gamma_{1,1}(\mathbb{C}))$ is nonzero.

The class $w_i(\omega)$ is called the *i-th Chern class* of ω. We define the *total Chern class* of ω to be the sum

$$c(\omega) = c_0(\omega) + c_1(\omega) + c_2(\omega) + \cdots \in \mathrm{H}^*(B(\omega), \mathbb{Z}).$$

One can prove the following relationship between a complex bundle and its conjugate.

LEMMA 3.26 ([**25**, Lemma 14.9]). *Let ω be a complex n-bundle. Then the total Chern class of $\overline{\omega}$ is given by*

$$c(\overline{\omega}) = 1 - c_1(\omega) + c_2(\omega) - \cdots + (-1)^n c_n(\omega).$$

For what shall follow, we will require one more family of characteristic classes, the Pontryagin classes. These classes are actually defined in terms of the Chern classes. Let ξ be a real, n-dimensional vector bundle. Then the complexification $\xi \otimes \mathbb{C}$ of ξ is an n-dimensional complex vector bundle. The i-th Pontryagin class of ξ, denoted $p_i(\xi)$, is defined in terms of the $2i$-th Chern class of its complexification by the formula

$$p_i(\xi) = (-1)^i c_{2i}(\xi \otimes \mathbb{C}) \in \mathrm{H}^{4i}(B(\xi), \mathbb{Z}).$$

We define the total Pontryagin class of ξ to be the sum

$$p(\xi) = p_0(\xi) + p_1(\xi) + p_2(\xi) + \cdots \in \mathrm{H}^*(B(\xi), \mathbb{Z}).$$

The Pontryagin classes satisfy properties formally similar to those satisfied by the Stiefel-Whitney and Chern classes. These properties may derived from the corresponding properties of the Chern classes. The following relationship between Chern and Pontryagin classes is useful.

LEMMA 3.27 ([**25**, Corollary 15.5]). *Let ω be a complex n-plane bundle and $\omega_{\mathbb{R}}$ the real vector bundle obtained by ignoring its complex structure. Then*

$$1-p_1(\omega_{\mathbb{R}})+\cdots+(-1)^n p_n(\omega_{\mathbb{R}}) = (1-c_1(\omega)+\cdots+(-1)^n c_n(\omega))(1+c_1(\omega)+\cdots+c_n(\omega)).$$

PROOF. By the definition of Pontryagin classes, we have

$$1 - p_1(\omega) + p_2(\omega) - \cdots + (-1)^n p_n(\omega) = 1 + c_2(\omega_{\mathbb{R}} \otimes \mathbb{C}) + \cdots + c_{2n}(\omega_{\mathbb{R}} \otimes \mathbb{C}).$$

But $\omega_{\mathbb{R}} \otimes \mathbb{C} \cong \omega \oplus \overline{\omega}$, so by Lemma 3.26,

$$\begin{aligned} c(\omega_{\mathbb{R}} \otimes \mathbb{C}) &= 1 + c_1(\omega_{\mathbb{R}} \otimes \mathbb{C}) + \cdots + c_{2n}(\omega_{\mathbb{R}} \otimes \mathbb{C}) \\ &= c(\omega \oplus \overline{\omega}) = c(\omega)c(\overline{\omega}) \\ &= (1 + c_1(\omega) + \cdots + c_n(\omega))(1 - c_1(\omega) + \cdots + (-1)^n c_n(\omega)). \end{aligned}$$

It follows that if k is odd, then

$$c_k(\omega_{\mathbb{R}} \otimes \mathbb{C}) = \sum_{i=0}^{k} ((-1)^{k-i} + (-1)^i) c_i(\omega) c_{k-i}(\omega) = 0,$$

since $(-1)^{k-i} + (-1)^i = 0$ for each $i = 0, \ldots, k$. Therefore,

$$\begin{aligned} 1 - p_1(\omega) + p_2(\omega) - \cdots + (-1)^n p_n(\omega) &= c(\omega_{\mathbb{R}} \otimes \mathbb{C}) \\ &= (1 + c_1(\omega) + \cdots + c_n(\omega))(1 - c_1(\omega) + \cdots + (-1)^n c_n(\omega)). \end{aligned}$$

□

One has an analogue of Lemma 3.25 for Chern and Pontryagin classes. Since the arguments in the proof of Lemma 3.25 were purely formal, the proof remains unchanged.

LEMMA 3.28.

(i) *Let ω and ζ be complex vector bundles. Then*

$$c_k(\omega \times \zeta) = \sum_{i=0}^{k} c_i(\omega) \times c_{k-i}(\zeta).$$

(ii) *Let ξ and η be real vector bundles. Then*

$$p_k(\xi \times \eta) = \sum_{i=0}^{k} p_i(\xi) \times p_{k-i}(\eta).$$

Let X be an n-dimensional, smooth manifold. One defines its Stiefel-Whitney classes $w_i(X)$ (respectively, its Pontryagin classes, $p_i(X)$) to be the Stiefel-Whitney classes (respectively, Pontryagin classes) of its tangent bundle. To make a similar definition for Chern classes, we introduce a piece of terminology. We call a complex structure on the tangent bundle of X an *almost-complex structure* on X. An *almost-complex manifold* is defined to be a manifold together with an almost-complex structure. Consequently, the tangent bundle of an almost-complex manifold can be viewed as a complex vector bundle. We may therefore define the Chern classes $c_i(X)$ of the almost-complex manifold X to be the Chern classes of its tangent bundle.

One may use these characteristic classes to define numerical invariants of manifolds. Let X be a smooth, compact, n-dimensional manifold, and let $\mu_X \in \mathrm{H}_n(X, \mathbb{Z}/2\mathbb{Z})$ denote the fundamental homology class of X. Then for any cohomology class $u \in \mathrm{H}^n(X, \mathbb{Z}/2\mathbb{Z})$, the Kronecker product $\langle u, \mu_X \rangle$ is a well defined element of $\mathbb{Z}/2\mathbb{Z}$. Let $I = (i_1, \ldots, i_r)$ be a partition of the integer n (i.e. $i_1 \leq \cdots \leq i_r$ and $i_1 + \cdots + i_r = n$). Then the cohomology class $w_{i_1}(X) \cup \cdots \cup w_{i_r}(X)$ is in $\mathrm{H}^n(X, \mathbb{Z}/2\mathbb{Z})$. Therefore, we may define

$$w_I[X] = \langle w_{i_1}(X) \cup \cdots \cup w_{i_r}(\xi), \mu_{B(X)} \rangle \in \mathbb{Z}/2\mathbb{Z}.$$

The integer $w_I[X]$ is called the *I-th Stiefel-Whitney number* of X. If X is an oriented manifold, then X has a fundamental homology class $\mu_X \in \mathrm{H}_n(X, \mathbb{Z})$, and the *Pontryagin numbers* $p_I[X]$ may be defined in an analogous manner. In addition, *Chern numbers* $c_I[X]$ may be constructed under the assumption that X is almost complex (which implies that X has a preferred orientation). If X is an n-dimensional complex manifold, one can show that the Chern number $c_n[X]$ is equal to the Euler characteristic $\chi(X)$ of X; see [**25**, Corollary 11.2].

EXAMPLE 3.29. To illustrate the above points, we discuss the characteristic classes and numbers of the projective spaces. We begin with the Stiefel-Whitney classes of real projective space. There is an obvious bundle map f from the canonical line bundle $\gamma_{1,1}(\mathbb{R})$ over $\mathbb{RP}^1$ to $\gamma_{1,n}(\mathbb{R})$ over $\mathbb{RP}^n$. By properties (ii) and (iv) of Stiefel Whitney classes, we have

$$0 \neq w_1(\gamma_{1,1}(\mathbb{R})) = f^* w_1(\gamma_{1,n}(\mathbb{R})).$$

Therefore, $w_1(\gamma_{1,n}(\mathbb{R})) = g$, where g is the unique nonzero element of $\mathrm{H}^1(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z})$. Applying property (i) of Stiefel-Whitney classes, it follows that $w(\gamma_{1,n}) = 1 + g$.

Let $\tau_{\mathbb{RP}^n}$ be the tangent bundle of $\mathbb{RP}^n$, and let ε be the trivial line bundle over $\mathbb{RP}^n$. One may show (see [**25**, Proof of Theorem 4.5]) that

$$\tau_{\mathbb{RP}^n} \oplus \varepsilon \cong \underbrace{\gamma_{1,n}(\mathbb{R}) \oplus \cdots \oplus \gamma_{1,n}(\mathbb{R})}_{n+1 \text{ summands}}.$$

This is an example of the *splitting principle* for vector bundles. Therefore, by property (iii) of Stiefel-Whitney classes,

$$\begin{aligned} w(\mathbb{RP}^n) = w(\tau_{\mathbb{RP}^n}) = w(\tau_{\mathbb{RP}^n} \oplus \varepsilon) &= (1+g)^{n+1} \\ &= 1 + \binom{n+1}{1} g + \binom{n+1}{2} g^2 + \cdots + \binom{n+1}{n} g^n. \end{aligned}$$

This formula can be used to show that all of the Stiefel-Whitney numbers of $\mathbb{RP}^n$ vanish if and only if n is odd. If n is even, then it follows from the above formula that $w_n(\mathbb{RP}^n) = (n+1)g^n$, implying that $w_n[\mathbb{RP}^n] \equiv 1 \pmod 2$. Now suppose n is odd, and write $n = 2k - 1$. Then

$$w(\mathbb{RP}^n) = (1+g)^{2k} \equiv (1+g^2)^k = \sum_{i=0}^{k} \binom{k}{i} g^{2k} \pmod 2.$$

Since the above sum contains no terms of even weight, it follows that $w_j(\mathbb{RP}^n) = 0$ if j is odd. Consequently, all the Stiefel-Whitney numbers of $\mathbb{RP}^n$ vanish.

One may use similar ideas to compute the Chern classes of complex projective n-space, $\mathbb{CP}^n$. In this case, one begins by showing that

$$\begin{aligned}\tau_{\mathbb{CP}^n} &\cong \mathrm{Hom}(\gamma_{1,n}(\mathbb{C}), \varepsilon \oplus \cdots \oplus \varepsilon) \\ &\cong \underbrace{\overline{\gamma}_{1,n}(\mathbb{C}) \oplus \cdots \oplus \overline{\gamma}_{1,n}(\mathbb{C})}_{n+1 \text{ summands}};\end{aligned}$$

for details, see [**25**, Proof of Theorem 14.10]. Therefore,

$$c(\mathbb{CP}^n) = c(\overline{\gamma}_{1,n}(\mathbb{C}))^{n+1} = (1 - c_1(\gamma_{1,n}(\mathbb{C})))^{n+1}.$$

Letting $g = -c_1(\gamma_{1,n}(\mathbb{C}))$, it follows that

$$c(\mathbb{CP}^n) = 1 + \binom{n+1}{1} g + \binom{n+1}{2} g^2 + \cdots + \binom{n+1}{n} g^n.$$

It can be shown that g is the generator of $\mathrm{H}^2(\mathbb{CP}^n, \mathbb{Z})$ such that $g^n \in \mathrm{H}^{2n}(\mathbb{CP}^n, \mathbb{Z})$ is compatible with the preferred orientation of $\mathbb{CP}^n$, (i.e., $\langle \mu_{\mathbb{CP}^n}, g^n \rangle = 1$). It follows that for any partition $I = (i_1, \ldots, i_r)$ of the integer n, we have

$$c_I[\mathbb{CP}^n] = \binom{n+1}{i_1} \cdots \binom{n+1}{i_r}. \tag{3.1}$$

For example,

$$c_1[\mathbb{CP}^1] = 2, \quad c_1^2[\mathbb{CP}^2] = 9, \quad c_2[\mathbb{CP}^2] = 3. \tag{3.2}$$

From Lemma 3.27, it follows that the total Pontryagin class $p(\mathbb{CP}^n)$ is given by $(1 + g^2)^{n+1}$. Its Pontryagin nmbers are given by

$$p_I[\mathbb{CP}^n] = \binom{2n+1}{i_1} \cdots \binom{2n+1}{i_r},$$

where I is a partition of n. Therefore,

$$p_1[\mathbb{CP}^2] = 3, \quad p_1^2[\mathbb{CP}^4] = 25, \quad p_2[\mathbb{CP}^4] = 10 \tag{3.3}$$

EXAMPLE 3.30. Let C_1 and C_2 be complex curves, and define the surface $S = C_1 \times C_2$. Computing using Lemma 3.28, one obtains

$$c_2(S) = c_1(C_1) \times c_1(C_2), \quad c_1^2(S) = 2c_1(C_1) \times c_1(C_2).$$

Let μ_S be the homology class which determines the preferred orientation of S. One can show that $\mu_S = \mu_{C_1} \times \mu_{C_2}$. Therefore,

$$c_2[S] = \langle c_2(S), \mu_{C_1} \times \mu_{C_2} \rangle = \langle c_1(C_1), \mu_{C_1} \rangle \langle c_1(C_2), \mu_{C_2} \rangle = c_2[C_1]c_2[C_2],$$

$$c_1^2[S] = 2c_1[C_1]c_1[C_2].$$

Since, by (3.2), $c_1(\mathbb{CP}^1) = 2$, we have

$$c_2[\mathbb{CP}^1 \times \mathbb{CP}^1] = 4, \quad c_1^2[\mathbb{CP}^1 \times \mathbb{CP}^1] = 8. \tag{3.4}$$

Using the above style of argument, one may prove results relating the Pontryagin numbers of a product of manifolds to the Pontryagin numbers of the factors. In particular, one may show that if M and N are 4-dimensional oriented manifolds, then

$$p_2[M \times N] = p_1[M]p_1[N], \quad p_1^2[M \times N] = 2p_1[M]p_1[N].$$

Consequently,

$$p_2[\mathbb{CP}^2 \times \mathbb{CP}^2] = 9, \quad p_1^2[\mathbb{CP}^2 \times \mathbb{CP}^2] = 18. \tag{3.5}$$

We summarize in tabular form some manifolds and their characteristic numbers:

	c_1^2	c_2
$\mathbb{CP}^1 \times \mathbb{CP}^1$	8	4
$\mathbb{CP}^2$	9	3

	p_1^2	p_2
$\mathbb{CP}^2 \times \mathbb{CP}^2$	18	9
$\mathbb{CP}^4$	25	10

EXAMPLE 3.31. Let X be a complex surface, and let $\widetilde{X}$ be the blow-up of X at a point P. There is a nice relationship between the Chern numbers of X and $\widetilde{X}$. It is a fact (see for instance [**14**, Appendix A, Example 4.1.2]) that for any surface Y, we have $c_1(Y) = -K_Y$, where K_Y is the canonical divisor on Y. Further, by [**14**, Chapter V, Proposition 3.3], one has the relationship $K_{\widetilde{X}}^2 = K_X^2 - 1$. Therefore, $c_1^2[\widetilde{X}] = c_1^2[X] - 1$.

Let E denote the special fibre of the blow-up $\widetilde{X} \to X$. It can be shown (see [**13**, p.473-474]) that

$$\mathrm{H}_i(\widetilde{X}) = \mathrm{H}_i(X) \oplus \mathrm{H}_i(E), \quad i > 0.$$

Since $E \cong \mathbb{CP}^1$, it follows that $\dim \mathrm{H}_i(\widetilde{X}) = \dim \mathrm{H}_i(X)$, if $i > 0$ and $i \neq 2$, and $\dim \mathrm{H}_2(\widetilde{X}) = \dim \mathrm{H}_2(X) + 1$. Since the top Chern number of a manifold is equal to its Euler characteristic (this was mentioned on page 64), we have $c_2[\widetilde{X}] = c_2[X] + 1$.

EXAMPLE 3.32. In this example, we describe the Pontryagin classes of the quaternionic projective spaces $\mathbb{HP}^n$. For proofs of the assertions made below, see [**16**, §1.3]. Using an appropriate cell decomposition, one can show that $\mathrm{H}^*(\mathbb{HP}^n, \mathbb{Z}) = \mathbb{Z}[u]/(u^{n+1})$, where u is a generator of $\mathrm{H}^4(\mathbb{HP}^n, \mathbb{Z})$.

Let u be the generator of $\mathrm{H}^4(\mathbb{HP}^n, \mathbb{Z})$ which is compatible with the orientation an $\mathbb{HP}^n$. Then the Pontryagin classes of $\mathbb{HP}^n$ are given by

$$\begin{aligned} p(\mathbb{HP}^n) &= (1+u)^{2n+2}(1+4u)^{-1} \\ &= (1+u)^{2n+2}(1-4u+16u^2-64u^3+\cdots). \end{aligned}$$

As an illustration, we compute the Pontryagin numbers of $\mathbb{HP}^2$. Let $u \in \mathrm{H}^4(\mathbb{HP}^2, \mathbb{Z})$ be as above. Then since $u^3 = 0$, the above formula reduces to

$$p(\mathbb{HP}^2) = (1+u)^6(1-4u+16u^2) = 1+2u+7u^2.$$

That is, $p_1(\mathbb{HP}^2) = 2u$ and $p_2(\mathbb{HP}^2) = 7u^2$. As $\langle u, \mu_{\mathbb{HP}^2} \rangle = 1$, we have

$$p_1^2[\mathbb{HP}^2] = 4, \quad p_2[\mathbb{HP}^2] = 7. \tag{3.6}$$

CHAPTER 4

Bordism and cobordism

1. Generalized cohomology theories

1.1. The Eilenberg-Steenrod axioms. We begin by recalling the Eilenberg-Steenrod axioms defining generalized cohomology theories; see [**10**]. If (X, A) and (Y, B) are pairs of topological spaces with $A \subseteq X$ and $B \subseteq Y$, then a map $f\colon (X, A) \to (Y, B)$ is a continuous map $f\colon X \to Y$ with $f(A) \subseteq B$. Let $\mathcal{A}$ be a category of pairs (X, A) of topological spaces with $A \subseteq X$ such that:

- If the pair (X, A) is in $\mathcal{A}$, then so are the pairs (X, X), $(X, \varnothing)$, (A, A), and $(A, \varnothing)$.
- If (X, A) is in $\mathcal{A}$, then so is $(X \times I, A \times I)$.
- There is a one-point space $\star$ with $(\star, \varnothing)$ in $\mathcal{A}$.

Such a category is called *admissable*. We shall often identify the pair $(X, \varnothing)$ with the set X. A *generalized cohomology theory on* $\mathcal{A}$ consists of the following data:

- A sequence h^n, $n \geq 0$, of contravariant functors from $\mathcal{A}$ to the category of abelian groups. If $f\colon (X, A) \to (Y, B)$ is a continuous map between admissable pairs, we let f^* denote the induced map $h^n(f)\colon h^n(Y, B) \to h^n(X, A)$.
- A *coboundary map* $\delta\colon h^{n-1}(A) \to h^n(X, A)$ for each admissable pair (X, A) and each n.

Further, we require that the following axioms be satisfied.

(1) If $f\colon (X,A) \to (Y,B)$, then the diagram

$$\begin{array}{ccc} h^{n-1}(B) & \xrightarrow{\delta} & h^n(Y,B) \\ {\scriptstyle (f|_A)^*}\downarrow & & {\scriptstyle f^*}\downarrow \\ h^{n-1}(A) & \xrightarrow[\delta]{} & h^n(X,A) \end{array}$$

commutes.

(2) (Exactness) If $i\colon A \to X$ and $j\colon X \to (X,A)$ are inclusion maps, then the sequence of homomorphisms

$$\cdots \xrightarrow{i^*} h^{n-1}(A) \xrightarrow{\delta} h^n(X,A) \xrightarrow{j^*} h^n(X) \xrightarrow{i^*} h^n(A) \xrightarrow{\delta} \cdots$$

is exact.

(3) (Homotopy) If f and g are homotopic maps from (X,A) to (Y,B), then $f^* = g^*$.

(4) (Excision) Let (X,A) be in $\mathcal{A}$, and let U be an open subset of X such that $\overline{U} \subseteq \operatorname{Int} A$. If $(X-U, A-U)$ is in $\mathcal{A}$, then inclusion induces an isomorphism

$$h^n(X-U, A-U) \cong h^n(X,A).$$

In addition to satisfying the above, ordinary cohomology theory H^n also satisfies the following *dimension axiom.*

If $\star$ is a one point space then $\mathrm{H}^n(\star) = 0$ for $n \geq 1$, and $\mathrm{H}^0(\star) = \mathbb{Z}$.

One can show that on a sufficiently nice admissable category (for example, the category of simplicial complexes and simplicial maps), Axioms (1)-(4) together with the dimension axiom characterize ordinary cohomology theory [**10**]. Later, we shall come across generalized cohomology theories, the cobordism theories, for instance, which do not satisfy the dimension axiom.

A generalized cohomology theory h^n is said to have products if for each admissable pair (X,A) and integers m and n, there is a pairing

$$h^m(X,A) \times h^n(X,A) \to h^{m+n}(X,A)$$

which endows the direct sum $h^*(X,A) := \bigoplus_{n\geq 0} h^n(X,A)$ with a ring structure. We note that $h^*(X,A)$ is always a graded module over $h^*(\star)$.

1.2. Complex-oriented cohomology theories. For our purposes, one of the crucial properties of the space $\mathbb{CP}^\infty$ is that its cohomology ring is a power series ring in one variable. We thus define a class of generalized cohomology theories, the complex-oriented cohomology theories (see [**40**, §2.2], or [**15**, §31.1.1]), which share that property.

Let h^* be a generalized cohomology theory with products such that 2 is invertible in the ring of coefficients $h^*(\star)$. We call h^* complex-oriented if there is a cohomology class $t \in h^2(\mathbb{CP}^\infty)$ (called an orientation) such that:

- t maps to $-t$ under the endomorphism of $h^2(\mathbb{CP}^\infty)$ induced by complex conjugation,
- t restricts to the canonical generator of $h^2(S^2)$.

Suppose h^* is a complex-oriented cohomology theory. Then one may deduce using only the above properties and the Eilenberg-Steenrod axioms that

$$h^*(\mathbb{CP}^\infty) \cong h^*(\star)[\![x]\!].$$

Ordinary cohomology is a complex-oriented theory. Representing the 2-sphere S^2 as $\mathbb{C}\cup\{\infty\}$, one observes that complex conjugation induces a reflection of S^2 about an equator. Such a reflection induces multiplication by -1 on $\mathrm{H}^2(S^2,\mathbb{Z})$.

Now suppose h^* is a complex-oriented cohomology theory. Let $R = h^*(\star)$ be its ring of coefficients. For each space X, $h^*(X)$ is a module over $h^*(\star)$. As h^* is contravariant, the map $m\colon \mathbb{CP}^\infty \to \mathbb{CP}^\infty$ induces a co-multiplication map

$$\mu\colon h^*(\mathbb{CP}^\infty) \to h^*(\mathbb{CP}^\infty \times \mathbb{CP}^\infty) \cong h^*(\mathbb{CP}^\infty) \underset{R}{\widehat{\otimes}} h^*(\mathbb{CP}^\infty),$$

where the isomorphism in the above formula is a consequence of the Künneth theorem. Note that since h^* is well defined modulo homotopy equivalence, the map μ is

independent of our choice of m. As h^* is complex-oriented,

$$h^*(\mathbb{CP}^\infty) \cong R[\![z]\!], \quad \text{and} \quad h^*(\mathbb{CP}^\infty) \underset{R}{\widehat{\otimes}} h^*(\mathbb{CP}^\infty) \cong R[\![z]\!] \otimes R[\![z]\!] \cong R[\![x, y]\!].$$

Therefore, we may view μ as a map from $R[\![z]\!]$ into $R[\![x, y]\!]$. A purely formal argument, essentially identical to the one presented in Chapter 2, §1, proves the following consequence of the group law property of the map m.

THEOREM 4.1. *Let $F(x, y) = \mu(z) \in R[\![x, y]\!]$. Then $F(x, y)$ is a formal group law with coefficients in the ring $R = h^*(point)$.*

In summary, using the group property of the classifying space $\mathbb{CP}^\infty = \mathrm{BU}(1)$, we may attach a formal group law to each complex-oriented cohomology theory.

2. Bordism

Bordism theory, initiated by L. Pontryagin and V. A. Rohlin and brought to maturity by J. Milnor and R. Thom, was developed to answer questions like the following:

> Given a manifold, how may we determine if it is the boundary of another manifold?

Considering the central role played by the notion of boundary in homology theory, it comes as no surprise that homological tools have been vital in investigations related to the above question. In fact, our answer is phrased in terms of characteristic cohomology classes.

Assume all manifolds appearing in this section are smooth and compact. By a closed manifold, we mean a manifold without boundary. Let $\mathcal{M}$ be the set of diffeomorphism classes of closed (smooth, compact) manifolds. For manifolds X_1 and X_2, we let $X_1 + X_2$ denote their disjoint union. The empty manifold $\varnothing$ serves as a neutral element for $+$. The cartesian product operation on $\mathcal{M}$ distributes over disjoint union. In fact, $(\mathcal{M}, +, \times)$ has satisfies all axioms of a commutative ring except for the existence of additive inverse.

2.1. Non-oriented bordism. We define an equivalence relation on $\mathcal{M}$ by declaring X_1 and X_2 equivalent if and only if there is a manifold Y such that ∂Y is diffeomorphic to $X_1 + X_2$. This is an equivalence relation: Symmetry is obvious; reflexitivity follows from the fact that for any closed manifold X, the disjoint union $X + X$ is the boundary of the cartesian product $X \times [0, 1]$. Transitivity follows from the following theorem, which allows us to glue two manifolds together along a common boundary.

THEOREM 4.2 (Collar neighbourhood theorem). *Let X be a smooth, compact manifold with boundary ∂X. Then there exists a neighbourhood of ∂X in X which is diffeomorphic to $\partial X \times [0, 1)$.*

We call this relation non-oriented bordism, and say that two related manifolds are *bordant*. Let Ω_* be the set of equivalence classes of $\mathcal{M}$, modulo the non-oriented bordism relation.

We claim that Ω_* is a ring under $+$ and $\times$. That addition is well defined follows from the identity $\partial(Y_1 + Y_2) = \partial Y_1 + \partial Y_2$. A closed manifold X is its own additive inverse in Ω_*, as $X + X = \partial X \times [0, 1]$ is a boundary. That $\times$ is well defined on Ω_* follows from the fact that if X is closed and ∂Y is a boundary, then $X \times \partial Y = \partial(X \times Y)$. We call Ω_* the *non-oriented bordism ring*. The ring Ω_* is graded by dimension. The set Ω_n of equivalence classes of closed, n-dimensional manifolds under the non-oriented bordism relation is an abelian group, and

$$\Omega_* = \bigoplus_{n \geq 0} \Omega_n.$$

It is clear that the cartesian product induces a bilinear map $\times : \Omega_m \times \Omega_n \to \Omega_{m+n}$. The structure of Ω_* is given by the following theorem.

THEOREM 4.3 (Thom [**39**]). *The non-oriented cobordism ring Ω_* is isomorphic to a polynomial ring*

$$(\mathbb{Z}/2\mathbb{Z})[X_2, X_4, X_5, X_6, X_8, X_9, \ldots],$$

with one generator $X_n \in \Omega_n$ for all $n \neq 2^m - 1$. If n is even, then we may take X_n to be the bordism class of real, n-dimensional projective space.

A proof is also given in [**38**].

The Stiefel-Whitney numbers, discussed earlier, are complete invariants of non-oriented bordism.

THEOREM 4.4 (Pontryagin [**30**], Thom [**39**]). *Let X be a smooth, compact, closed manifold. Then X is the boundary of a smooth, compact manifold Y if and only if all of its Stiefel-Whitney numbers $w_I[X]$ are zero.*

These issues are treated in detail in [**38**]. From the discussion of Example 3.29, we see that $\mathbb{RP}^n$ bounds if and only if n is odd. Observing that

$$\mathrm{H}^n(X_1 + X_2, \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{H}^n(X_1, \mathbb{Z}/2\mathbb{Z}) \oplus \mathrm{H}^n(X_1, \mathbb{Z}/2\mathbb{Z}),$$

it follows that for any partition I of the integer n, we have $w_I[X_1 + X_2] = w_I[X_1] + w_I[X_2]$ in $\mathbb{Z}/2\mathbb{Z}$. We therefore obtain the following corollary.

COROLLARY 4.5. *Two smooth, compact, closed, n-dimensional manifolds X_1 and X_2 are cobordant if and only if X_1 and X_2 have the same Stiefel-Whitney numbers.*

2.2. Oriented bordism. We also wish to determine necessary and sufficient conditions for an oriented manifold to be an oriented boundary. For an oriented manifold X, we let $-X$ denote the manifold X with the opposite orientation. Let $\mathcal{M}^{\mathcal{O}}$ denote the set of isomorphism (i.e. orientation preserving[1] diffeomorphism) classes of closed, oriented manifolds. The set $\mathcal{M}^{\mathcal{O}}$ satisfies all the axioms of a ring except for the existence of additive inverse. Unlike in the non-oriented case though, the cartesian product operation on $\mathcal{M}^{\mathcal{O}}$ is not commutative in usual sense. It is, however, commutative in the following graded sense. If we view $\mathcal{M}^{\mathcal{O}}$ as being graded by dimension, and let X and Y be oriented manifolds of dimension m and n, respectively, then $X \times Y$ is

[1]Let $\varphi\colon X \to Y$ be a diffeomorphism between oriented manifolds X and Y. We say that φ is *orientation preserving* if the induced map $d\varphi$ on tangent spaces sends positively oriented bases to positively oriented bases.

isomorphic to $(-1)^{mn}Y \times X$. The reason for this is as follows. Let $\varphi\colon X \times Y \to Y \times X$ be defined by $\varphi(x, y) = (y, x)$ Let $e = (e_1, \ldots, e_m)$ and $f = (f_1, \ldots, f_n)$ be bases for the tangent spaces of X and Y at points x and y, respectively. Then

$$e \times f := ((e_1, 0), \ldots, (e_m, 0), (0, f_1), \ldots, (0, f_n)) \quad \text{and}$$
$$f \times e := ((f_1, 0), \ldots, (f_n, 0), (0, e_1), \ldots, (0, e_m))$$

are positively oriented bases for the tangent spaces of $X \times Y$ and $Y \times X$ at (x, y) and (y, x), respectively. Let $d\varphi$ denote the map on tangent spaces induced by φ. As $d\varphi(e_i, 0) = (0, e_i)$ and $d\varphi(0, f_i) = (f_i, 0)$, it follows that $d\varphi$ sends the basis $e \times f$ to the basis

$$d\varphi(e \times f) = ((0, e_1), \ldots, (0, e_m), (f_1, 0), \ldots, (f_n, 0)).$$

One sees directly that the determinant of the change of basis from $f \times e$ to $d\varphi(e \times f)$ is $(-1)^{mn}$. Therefore, the assertion that $X \times Y \cong (-1)^{mn}Y \times X$ follows.

We define a relation on the class of oriented manifolds by declaring X_1 and X_2 equivalent if $X_1 + (-X_2)$ is the boundary of another oriented manifold. The proof that this defines an equivalence relation proceeds essentially as in the non-oriented case. Note that as oriented manifolds, $\partial X \times [0, 1] \cong X + (-X)$. This relation is called the *oriented bordism relation*, and again, two related manifolds are said to be (*oriented*) *bordant*. Let $\Omega_*^{\mathcal{O}}$ be the corresponding set of equivalence classes. Then as in the non-oriented case, $\Omega_*^{\mathcal{O}}$ is a ring, with the additive inverse of and oriented manifold X being $-X$. Letting $\Omega_n^{\mathcal{O}}$ denote the set of equivalence classes of oriented n-dimensional manifolds under the oriented bordism relation, it follows easily from the above that

$$\Omega_*^{\mathcal{O}} = \bigoplus_{n \geq 0} \Omega_n^{\mathcal{O}}$$

is a graded ring, commutative in the graded sense.

The structure of this oriented bordism ring, modulo 2-torsion, is given by the following theorem:

THEOREM 4.6 (Thom [39], Milnor [24]).

(i) *The tensor product* $\Omega_*^O \otimes \mathbb{Z}[1/2]$ *is isomorphic to a polynomial ring*

$$\mathbb{Z}[1/2][X_4, X_8, \ldots]$$

with one generator in each positive dimension divisible by 4.

(ii) *Let* $[\mathbb{CP}^n]$ *denote the oriented bordism class of* $\mathbb{CP}^n$. *Then killing all torsion, we may take* $X_{4n} = [\mathbb{CP}^{2n}]$. *That is,*

$$\Omega_* \otimes \mathbb{Q} \cong \mathbb{Q}[\,[\mathbb{C}P^2], [\mathbb{C}P^4], \ldots].$$

Note that since all the generators of $\Omega_*^O \otimes \mathbb{Z}[1/2]$ have even weight, the graded commutativity inherited from Ω_*^O is just commutativity. For a description of the 2-torsion in Ω_*^O, see [41].

Together, the Pontryagin and Stiefel-Whitney numbers constitute complete invariants of oriented bordism.

THEOREM 4.7 (Pontryagin [30], Milnor [24], Wall [41]). *Two oriented manifolds* X *and* Y *are oriented bordant if and only if all of their corresponding Pontryagin and Stiefel-Whitney numbers coincide. Consequently, a compact, oriented manifold* X *is a the boundary of another compact, oriented manifold if and only if all of its Pontryagin numbers and Stiefel-Whitney numbers are zero.*

The Pontryagin numbers of an oriented manifold completely determine the image of an oriented manifold in $\Omega_*^O \otimes \mathbb{Q}$.

THEOREM 4.8 (Thom [39]). *Two oriented manifolds have the same image in* $\Omega_*^O \otimes \mathbb{Q}$ *if and only if all of their Pontryagin numbers coincide.*

EXAMPLE 4.9. Let $X = 3(\mathbb{CP}^2 \times \mathbb{CP}^2) - 2\mathbb{CP}^4$. We claim that X and $\mathbb{HP}^2$ have the same image in $\Omega_*^O \otimes \mathbb{Q}$. We must show that their have the same Pontryagin numbers.

Consulting (3.6) and the tables on page 66, we see that

$$\begin{aligned} p_1^2[X] &= 3p_1^2[\mathbb{CP}^2 \times \mathbb{CP}^2] - 2p_1^2[\mathbb{CP}^4] \\ &= 3 \cdot 18 - 2 \cdot 25 = 4 \\ &= p_1^2[\mathbb{HP}^2], \\ p_2[X] &= 3p_2[\mathbb{CP}^2 \times \mathbb{CP}^2] - 2p_2[\mathbb{CP}^4] \\ &= 3 \cdot 9 - 2 \cdot 10 = 7 \\ &= p_2[\mathbb{HP}^2]. \end{aligned}$$

So our claim holds.

Thom determined the structure of the oriented bordism groups by interpreting them as certain stable homotopy groups. To each vector bundle ξ, Thom attached a space $T(\xi)$, called the *Thom space* of ξ, with the following property:

- If $n < k - 1$, then the homotopy group $\pi_{n+k}(T(\gamma_n^{\mathcal{O}}))$ is isomorphic to the n-th oriented bordism group $\Omega_n^{\mathcal{O}}$, where $\gamma_n^{\mathcal{O}}$ is the universal oriented n-plane bundle over the oriented Grassmann manifold $\mathrm{G}^{\mathcal{O}}(n, \mathbb{R}^\infty)$.

For an accessible discussion of Thom spaces, see [**25**, §18]. We shall refer to these Thom spaces again when discussing the construction of cobordism theories.

2.3. Complex bordism. Somewhat less intuitive, although essential for our purposes, is the notion of *complex bordism*. Before we give the definition, we must introduce some terminology.

Let ξ and η be vector bundles over the common base space B, and let ε be the trivial line bundle over B. We say that ξ and η are *stably equivalent* if there exist integers m and n such that $\xi \oplus \varepsilon^m \cong \eta \oplus \varepsilon^n$. For example, by the discussion in Example 3.29, the tangent bundle $\tau_{\mathbb{RP}^n}$ of $\mathbb{RP}^n$ is stably equivalent to $\gamma_{1,n} \oplus \cdots \oplus \gamma_{1,n}$ ($n+1$ summands). If ξ is stably equivalent to a trivial bundle (that is, $\xi \oplus \varepsilon^m \cong \varepsilon^n$, for some integers m and n), we say that ξ is *stably trivial*. It is clear that stable

equivalence is an equivalence relation on the class of vector bundles over B. In fact, the set of stable equivalence classes of vector bundles over B form an abelian group under the operation of $\oplus$. The existence of additive inverses is a consequence of the following result:

LEMMA 4.10. *Let ξ be an $\mathbb{F}$-vector bundle over the paracompact base space B. Then there exists another $\mathbb{F}$-vector bundle η over B such that the direct sum $\xi \oplus \eta$ is (stably) trivial.*

PROOF. Let $g\colon E(\xi) \to \mathbb{F}^N$ be a Gauss map. Since B is paracompact, such a map exists by Theorem 3.13. Define $\widehat{g}\colon E(\xi) \to B \times \mathbb{F}^N$ by $e \in \mathrm{Fib}_b\, \xi \mapsto (b, g(e))$. Then $\widehat{g}$ embeds ξ as a subbundle of the trivial N-bundle ε^N. Choosing a metric on ε^N (here, we need the paracompactness of B), we may find a complementary subbundle η for ξ. □

The notions of oriented and non-oriented bordism discussed above do not generalize readily to the case of complex or even almost-complex manifolds (see page 63). This is because complex or almost-complex manifolds have even real dimension, and thus the boundary of a complex or almost-manifold cannot be complex or almost-complex. The notion of stable equivalence allows us to circumvent this difficulty.

Let X be a manifold, and let τ be its tangent bundle. Let ω be a complex vector bundle whose underlying real vector bundle is stably equivalent to τ. The stable equivalence class $[\omega]$ of the complex vector bundle ω is called a *complex structure on the stable tangent bundle* of X. A *stably almost-complex* manifold is defined to be a pair $(X, [\omega])$, where X is a manifold and $[\omega]$ is a complex structure on its stable tangent bundle.

We define the complex bordism relation for stably almost-complex manifolds. We first note that if $[\omega_1]$ and $[\omega_2]$ are complex structures on the stable tangent bundles of manifolds X_1 and X_2, respectively, there is an obvious way to define a complex structure on $X_1 + X_2$ induced by $[\omega_1]$ and $[\omega_2]$. For a stably almost-complex manifold

$(X, [\omega])$, we define its boundary, $\partial(X, [\omega])$, by the formula

$$\partial(X, [\omega]) = (\partial X, [\omega|_{\partial X}]).$$

Let $(X, [\omega])$ be a stably almost-complex manifold. We wish to define $-(X, [\omega])$. Let $\varepsilon_{\mathbb{R}}$ and $\varepsilon_{\mathbb{C}}$ be the trivial real and complex line bundles over X, and let $\overline{\varepsilon}_{\mathbb{C}}$ be the conjugate bundle. Note that the underlying real bundles of $\varepsilon_{\mathbb{C}}$ and $\overline{\varepsilon}_{\mathbb{C}}$ are both isomorphic to $\varepsilon_{\mathbb{R}} \oplus \varepsilon_{\mathbb{R}}$. We define $-(X, [\omega])$ to be the stably almost-complex manifold $(X, [\omega \oplus \overline{\varepsilon}_{\mathbb{C}}])$. It now makes sense to declare two stably almost-complex manifolds $(X_1, [\omega_1])$ and $(X_2, [\omega_2])$ *complex-bordant* if there exists another stably almost-complex manifold $(Y, [\zeta])$ such that

$$(X_1, [\omega_1]) + (X_2, [\omega_2]) = \partial(Y, [\zeta]).$$

As before, one can check that this does in fact define an equivalence relation on the class of stably almost-complex manifolds. We denote the quotient by Ω^{U}_*. One defines the cartesian product of $(X, [\omega])$ and $(Y, [\zeta])$ to be $(X \times Y, [\omega \times \zeta])$. To show that this makes sense, we verify that the underlying real bundle $(\omega \times \zeta)_{\mathbb{R}}$ is stably equivalent to $\tau_X \times \tau_Y$. Suppose $\omega_{\mathbb{R}} \cong \tau_X \oplus \varepsilon^m$ and $\zeta_{\mathbb{R}} \cong \tau_Y \oplus \varepsilon^n$, and let π_1 and π_2 denote the projection maps from $X \times Y$. Then

$$\begin{aligned}
(\omega \times \zeta)_{\mathbb{R}} &\cong \omega_{\mathbb{R}} \times \zeta_{\mathbb{R}} \\
&\cong \pi_1^*(\tau_X \oplus \varepsilon^m) \oplus \pi_2^*(\tau_Y \oplus \varepsilon^n) \\
&\cong (\pi_1^*\tau_X) \oplus (\pi_1^*\varepsilon^m) \oplus (\pi_2^*\tau_Y) \oplus (\pi_2^*\varepsilon^n) \\
&\cong (\pi_1^*\tau_X) \oplus (\pi_2^*\tau_Y) \oplus \varepsilon^{n+m} \\
&\cong (\tau_X \times \tau_Y) \oplus \varepsilon^{n+m}.
\end{aligned}$$

As before, the operations $+$ and $\times$ give Ω^{U}_* the structure of a graded ring. That $+$ is well defined, modulo bordism, follows from the additivity of $+$. To check that multiplication in Ω^{U}_* makes sense, we must verify that the set of boundaries is closed

under multiplication by arbitrary closed manifolds. Computing, we see that,

$$\begin{aligned}(\partial M, [\zeta|_{\partial M}]) \times (X, [\omega]) &= (\partial M \times X, [\zeta|_{\partial M} \times \omega]) \\ &\cong (\partial(M \times X), [(\zeta \times \omega)_{\partial(M \times X)}]) \\ &= \partial(M \times X, [\zeta \times \omega]).\end{aligned}$$

Thus, Ω_*^{U} is a ring. The structure of this *complex bordism ring* was determined by Milnor, and independently by Novikov.

THEOREM 4.11 ([**24**], [**28**]). *The complex bordism ring Ω_*^{U} has the structure of a polynomial ring $\mathbb{Z}[X_2, X_4, \ldots]$, with one generator in each real dimension divisible by 4.*

A system of generators for Ω_*^{U} can be described as follows. Let $H_{ij} \subseteq \mathbb{CP}^i \times \mathbb{CP}^j$ be the smooth hypersurface defined by the relation $x_0 y_0 + \cdots x_k y_k = 0$, where $k = \min\{i, j\}$. The manifold H_{ij} has real dimension $2(i + j - 1)$. One can show (see [**16**, §4.1]) that the manifolds H_{ij} are polynomial generators of Ω_*^{U}.

We note that two stably equivalent vector bundles have the same characteristic classes, since the characteristic classes of the trivial bundle are trivial. Therefore, the Chern classes and numbers of a stably almost-complex manifold are well defined. These Chern numbers are complete invariants for complex bordism theory.

THEOREM 4.12 (Milnor [**24**], Novikov [**28**]). *Two stably, almost complex manifolds are complex-bordant if and only if all of their corresponding Chern numbers coincide.*

EXAMPLE 4.13. Let X be a smooth, projective, complex, algebraic surface, and let $\widetilde{X}$ be the blow-up of X at a point P. We claim that $\widetilde{X} - X$ and $\mathbb{CP}^1 \times \mathbb{CP}^1 - \mathbb{CP}^2$ are complex-bordant. We compute their Chern numbers, referring to Example 3.31

and the tables on page 66.

$$\begin{aligned} c_1^2[\mathbb{CP}^1 \times \mathbb{CP}^1 - \mathbb{CP}^2] &= c_1^2[\mathbb{CP}^1 \times \mathbb{CP}^1] - c_1^2[\mathbb{CP}^2] \\ &= 8 - 9 = -1 \\ &= c_1^2[\widetilde{X}] - c_1^2[X] = c_1^2[\widetilde{X} - X] \\ c_2[\mathbb{CP}^1 \times \mathbb{CP}^1 - \mathbb{CP}^2] &= 4 - 3 = 1 \\ &= c_2[\widetilde{X} - X] \end{aligned}$$

As their Chern numbers coincide, they are complex-cobordant.

We have remarked before that every almost-complex manifold is oriented. Therefore, there is a natural 'forgetful' homomorphism $\varphi\colon \Omega_*^{\mathrm{U}} \to \Omega_*^{\mathrm{O}}$. This follows from the fact that an orientation of a vector bundle stably equivalent to the tangent bundle τ of X induces an orientation of the n-dimensional manifold X. For let $\xi = \tau \oplus \varepsilon_{\mathbb{R}}^k$, and $e_1, \ldots, e_k$ be the standard basis of $\mathbb{R}^k$. Let $x \in X$. We say that an ordered basis $(v_1, \ldots, v_n)$ is a positively oriented basis for $\mathrm{Fib}_x\, \tau$ if and only if $(v_1, \ldots, v_n, e_1, \ldots, e_k)$ is a positively oriented basis if $\mathrm{Fib}_x\, \xi \cong (\mathrm{Fib}_x\, \tau) \oplus \mathbb{R}^k$. One can easily verify that this is well defined. Thus, a complex structure on the stable tangent bundle of X induces an orientation of X. One can check directly that the complex structures $[\omega]$ and $[\omega \oplus \bar{\varepsilon}_{\mathbb{C}}]$ induce opposite orientations on the underlying manifold. It is known, see [**38**, Chapter IX], that φ is onto, modulo torsion.

3. Bordism theories as homology theories

Our construction of the bordism groups may be generalized. We describe this generalization for oriented bordism, since it will be important for us later. Fix an oriented manifold, X. We shall consider pairs (M, f), where M is a manifold and $f\colon M \to X$ is an orientation preserving (see footnote, page 73), smooth map. Declare two such pairs (M_1, f_1) and (M_2, f_2) equivalent if there exists a pair (N, g) such that

- ∂N is diffeomorphic to $M_1 + (-M_2)$,

- $f_1 = g|_{M_1}$ and $f_2 = g|_{M_2}$.

Let $\mathrm{MSO}_n(X)$ be the set of equivalence classes of such pairs (M, f), where M has dimension n. Let $\star$ be a one point space. One observes immediately that $\mathrm{MSO}_n(\star)$ is just the n-th oriented bordism ring, Ω_n^{O}. It is clear that the disjoint union operation endows the set $\mathrm{MSO}_n(X)$ with an abelian group structure. Let

$$\mathrm{MSO}_*(X) = \bigoplus_{n \geq 0} \mathrm{MSO}_n(X).$$

The cartesian product does not induce a ring structure in a natural way on $\mathrm{MSO}_*(X)$. However, $\mathrm{MSO}_*(X)$ does have the structure of a $\mathrm{MSO}_*(\star)$-module. For oriented manifolds X and Y, there is an obvious pairing

$$\mathrm{MSO}_*(X) \times \mathrm{MSO}_*(Y) \to \mathrm{MSO}_*(X \times Y)$$

defined by the correspondence $((M_1, f_1), (M_2, f_2)) \mapsto (M_1 \times M_2, f_1 \times f_2)$. We obtain our module structure by taking $Y = \{\star\}$, and noticing that $X \times \{\star\}$ can be naturally identified with X.

The correspondence $X \mapsto \mathrm{MSO}_n(X)$ is covariantly functorial. If $\theta\colon X \to Y$ is an orientation preserving diffeomorphism, then there is an induced map $\theta_*\colon \mathrm{MSO}_n(X) \to \mathrm{MSO}_n(Y)$ defined by $\theta_*(M, f) = (M, \theta \circ f)$. In fact, one can show that the correspondence $X \mapsto \mathrm{MSO}_n(X)$ defines a generalized homology theory in the sense of [**10**]. We verify invariance under homotopy; for other details, see [**2**].

LEMMA 4.14. *Two homotopic maps from X to Y induce the same homomorphism from $\mathrm{MSO}_n(X)$ to $\mathrm{MSO}_n(Y)$.*

PROOF. Let $H : X \times [0,1] \to Y$ be a smooth map, and let $H_t(x) = H(x,t)$, for $t \in [0,1]$. We must show that $H_{0*} = H_{1*}$. By definition,

$$H_{0*}(M, f) = (M, H_0 \circ f), \quad H_{1*}(M, f) = (M, H_1 \circ f).$$

Let $g = F \circ (f \times \mathrm{id})$, and consider the pair $(M \times [0,1], g)$. Then we have

$$\partial(M \times I) = M \times \{1\} + (-M) \times \{0\} \cong M + (-M),$$
$$g|_{M\times\{0\}} = H_0 \circ f,$$
$$g|_{M\times\{1\}} = H_1 \circ f.$$

Therefore, $(M, H_0 \circ f)$ and $(M, H_1 \circ f)$ represent the same element of $\mathrm{MSO}_n(X)$. □

One may make analogous definitions for complex bordism. One defines functors $X \mapsto \mathrm{MU}_n(X)$ and $X \mapsto \mathrm{MU}_*(X)$ such that $\mathrm{MU}_*(\star) = \Omega^{\mathrm{U}}_*$, and that these functors actually define a generalized homology theory. Considering the intimate relationship between the oriented and complex bordism rings, it is not surprising that the homology theories MSO_* and MU_* are related. It is known that the forgetful natural transformation from MU_* to MSO_* induces an isomorphism

$$\mathrm{MU}_*(-) \underset{\Omega^{\mathrm{U}}_*}{\otimes} \Omega^{\mathrm{O}}_*[1/2] \xrightarrow{\sim} \mathrm{MSO}_*(-)[1/2].$$

For details, see [**18**].

4. Cobordism

4.1. Spectra. Before we indicate how one may construct cobordism theory, the generalized cohomology theory dual to the bordism theory introduced above, we introduce some terminology. Let X be a pointed topological space with base point x_0, and let I denote the unit interval. We denote by ΣX the quotient space of $X \times I$ obtained by identifying the subset $(X \times \{0\}) \cup (\{x_0\} \times I) \cup (X \times \{1\})$ to a point. We call the space ΣX the *reduced suspension* of X.

REMARK 4.15. The suspension operator Σ is a natural object to consider. Let ΩX denote the set of loops based at x_0 with the compact-open topology, the so-called loop space. One may show that Σ and Ω are actually adjoint functors in the sense that $[\Sigma X, Y] \cong [X, \Omega Y]$.

We define a *spectrum* E to be a sequence of pointed spaces $E(n)$, $n \geq 0$, together with pointed maps $\alpha_n \colon \Sigma E(n) \to E(n+1)$. Let $E = (E(n), \alpha_n)$ be a spectrum and let X be any space. Then for any i and j, there is a natural map from $[\Sigma^i X, E(j)]$ to $[\Sigma^{i+1} X, E(j+1)]$, which one constructs as follows. Let $f \colon \Sigma^i X \to E(j)$, and let $f_* \colon \Sigma^{i+1} X \to \Sigma E(j)$ be the map induced by the functoriality of Σ. Let $f \mapsto \alpha_j \circ f_*$.

According to a theorem of G. W. Whitehead, given a spectrum $E = (E(n), \alpha_n)$, one may construct from it a generalized cohomology theory $X \mapsto E^n(X)$,

$$E^n(X) = \varinjlim_k [\Sigma^k X, E(n+k)], \tag{4.1}$$

where the transition maps are as above.

4.2. Oriented and complex cobordism. Earlier, we mentioned the Thom spaces $T(\gamma_n^{\mathcal{O}})$, where $\gamma_n^{\mathcal{O}}$ is the universal oriented n-plane bundle over the oriented Grassmann manifold $\mathrm{G}^{\mathcal{O}}(n, \mathbb{R}^\infty) = \mathrm{BSO}(n)$, and the crucial role they play in the determination of the structure of the bordism groups. Defering to topological tradition, we shall begin using the notation $\mathrm{MSO}(n)$ for the space $T(\gamma_n^{\mathcal{O}})$. One may define the Thom space $\mathrm{MSO}(n)$ as the quotient $E(\gamma_n^{\mathcal{O}})/A$, where $E(\gamma_n^{\mathcal{O}})$ is the total space of the bundle $\gamma_n^{\mathcal{O}}$ and A is the collection of all vectors in $E(\gamma_n^{\mathcal{O}})$ of length greater than or equal to 1. Thus, $\mathrm{MSO}(n)$ comes equipped with a natural choice of base point, the image of A. By the universal property of $\gamma_{n+1}^{\mathcal{O}}$, the Whitney sum $\gamma_n^{\mathcal{O}} \oplus \varepsilon^1$ admits a bundle map into $\gamma_{n+1}^{\mathcal{O}}$, where ε^1 denotes the trivial line bundle over $\mathrm{BSO}(n)$. This map, in turn, induces a pointed map $\alpha_n \colon \Sigma \mathrm{MSO}(n) \to \mathrm{MSO}(n+1)$. Thus, the Thom spaces $\mathrm{MSO}(n)$, together with the transition maps α_n, form a spectrum which we call the *Thom spectrum* and denote by MSO. We define the *n-th oriented cobordism group* of X by

$$\mathrm{MSO}^n(X) = \varinjlim_k [\Sigma^k X, \mathrm{MSO}(n+k)],$$

and by Whitehead's theorem, the correspondence $X \mapsto \mathrm{MSO}^n(X)$ defines a generalized cohomology theory which we call *oriented cobordism*.

We construct complex cobordism via its spectrum. One defines spaces $\mathrm{MU}(n)$ as we defined $\mathrm{MSO}(n)$ above, but with complex Grassmannians and the corresponding complex bundles in place of their oriented counterparts. Essentially due to the fact that $\dim_{\mathbb{R}} \mathbb{C} = 2$, the universal property of the canonical bundle over $\mathrm{G}(n, \mathbb{C}^\infty) = \mathrm{BU}(n)$ induces a natural map from $\Sigma^2\mathrm{MU}(n)$ to $\mathrm{MU}(n+1)$ (not from $\Sigma\mathrm{MU}(n)$ to $\Sigma\mathrm{MU}(n+1)$). Thus, we define a spectrum MU whose constituent spaces are

$$0,\ 0,\ \mathrm{MU}(1),\ \mathrm{MU}(1),\ \mathrm{MU}(2),\ \mathrm{MU}(2),\ \mathrm{MU}(3),\ \mathrm{MU}(3),\ \ldots.$$

From Whitehead's theorem, we obtain the generalized cohomology theory of complex cobordism, MU^* defined by formula 4.1. For a nice geometric description of complex cobordism theory, see [**33**, §1].

4.3. Quillen's theorem. One can show that complex cobordism is in fact a canonically complex-oriented cohomology theory; see [**1**, Part II, §2]. Therefore, we can attach to complex cobordism theory a formal group law F^{MU} defined over the ring $\mathrm{MU}^*(\star) = \Omega^{\mathrm{U}}_*$. By a remarkable theorem of Quillen [**32**], this formal group law is actually universal. We state this important result as a theorem.

THEOREM 4.16. *Let F^{MU} be the formal group law of complex cobordism, defined over the complex bordism ring Ω^{U}_*. Then F^{MU} is a universal, one-dimensional formal group law.*

Note that this result is consistent with Milnor's determination of the structure of the complex bordism ring Ω^{U}_*; see Theorem 4.11. We can also give a very pleasing formula for the logarithm of F^{MU}.

THEOREM 4.17 (Mischenko, Appendix 1 in [**28**]). *The logarithm of the formal group law of complex cobordism is given by*

$$\log_{F^{\mathrm{MU}}}(x) = \sum_{n \geq 0} \frac{[\mathbb{CP}^n]}{n+1} x^{n+1}.$$

Not only is the formal group law universal, but complex cobordism theory is actually a universal object in the category of complex oriented cobordism theories.

It is known that if h^* is another complex oriented cobordism theory, then there is a natural transformation from MU^* to h^* sending the complex orientation of MU^* to that of h^*; for details, see [**33**].

CHAPTER 5

Elliptic genera and elliptic cohomology theories

We have seen in Chapter 4, §1.2 that complex-oriented cohomology theories have associated formal group laws. It is natural to ponder the converse of this observation:

> *Do all formal group laws arise from complex-oriented cohomology theories?*

Since the universal formal group law is the formal group law of complex cobordism theory, this seems to be a reasonable thing to ask.

Although this question is still very much open, some special cases are known. The additive and multiplicative group laws arise from ordinary cohomology and K-theory, respectively. We shall show that Euler's formal group law,

$$F(x,y) = \frac{x\sqrt{R(y)} + y\sqrt{R(x)}}{1 - \varepsilon x^2 y^2}, \quad R(x) = 1 - 2\delta x^2 + \varepsilon x^4, \tag{5.1}$$

defined over the ring $\mathbb{Z}[1/2, \delta, \varepsilon]$, arises from a complex oriented cohomology theory, a so-called "elliptic cohomology theory". The proof of this fact uses in an essential way the theory of elliptic curves.

1. Genera

Let G be a formal group law, defined over a ring A of characteristic zero. Since the formal group law, F^{MU}, of complex cobordism is universal, one is tempted to attempt the construction of a cohomolgy theory yielding G by somehow "specializing" complex cobordism theory. One could proceed as follows.

Let Ω_*^{U} denote the complex cobordism ring, which we recall is isomorphic to the Lazard ring. By universality, there exists a unique ring homomorphism $\varphi\colon \Omega_*^{\mathrm{U}} \to A$

such that $\varphi_* F^{\mathrm{MU}} = G$. The map φ induces a Ω^{U}_*-module structure on A in the standard way. Define a ring valued functor on topological spaces by the rule

$$X \mapsto \mathrm{MU}^*(X) \underset{\Omega^{\mathrm{U}}_*}{\otimes} A. \tag{5.2}$$

One proves the following lemma by tracing through the construction of the formal group law of a complex-oriented cohomology theory.

LEMMA 5.1. *Suppose (5.2) defines a generalized cohomology theory. Then its formal group law is G.*

PROOF. Let h^* denote the generalized cohomology theory given by (5.2). Note that

$$h^*(\star) = \mathrm{MU}^*(\star) \underset{\Omega^{\mathrm{U}}_*}{\otimes} A = \Omega^{\mathrm{U}}_* \underset{\Omega^{\mathrm{U}}_*}{\otimes} A \cong A.$$

Also, we have

$$\begin{aligned} h^*(\mathbb{CP}^\infty) &= h^*(\varinjlim \mathbb{CP}^n) = \varprojlim h^*(\mathbb{CP}^n) \\ &= \varprojlim (\Omega^{\mathrm{U}}_*(\star)[x]/(x^{n+1})) \underset{\Omega^{\mathrm{U}}_*}{\otimes} A \\ &\cong \varprojlim (\Omega^{\mathrm{U}}_*(\star) \underset{\Omega^{\mathrm{U}}_*}{\otimes} A)[x]/(x^{n+1}) \\ &\cong A[\![x]\!], \end{aligned}$$

from which follows,

$$h^*(\mathbb{CP}^\infty \times \mathbb{CP}^\infty) \cong A[\![x_1, x_2]\!].$$

Let $m\colon \mathbb{CP}^\infty \times \mathbb{CP}^\infty \to \mathbb{CP}^\infty$ be the multiplication map of Chapter 3, §3. Arguing as in Chapter 4, §1.2, m induces a comultiplication map,

$$\mu\colon A[\![x]\!] \to A[\![x_1, x_2]\!]$$

which can be described as follows. Let $F^{\mathrm{MU}}(x_1, x_2) = \sum_{i,j} a_{ij} x_1^i x_2^j$ be the formal group law of complex cobordism. Then the map μ is given by

$$\mu(x) = \sum_{i,j} (a_{ij} \otimes 1) x_1^i x_2^j = \sum_{i,j} (1 \otimes \varphi(a_{ij})) x_1^i x_2^j.$$

Note that $\mu(x)$ is the formal group law of h^*. Under the natural isomorphism of $\Omega_*^{\mathrm{U}} \underset{\Omega_*^{\mathrm{U}}}{\otimes} A$ with A, the formal group law $\sum_{i,j}(1 \otimes \varphi(a_{ij})) x_1^i x_2^j$ is identified with G. □

One would certainly like to know when (5.2) defines a generalized cohomology theory. We shall discuss this issue in the next section. First, though, we introduce some useful terminology. Let A be a $\mathbb{Q}$-algebra, and let B be a ring.

DEFINITION 5.2. An *oriented genus* with values in A is a $\mathbb{Q}$-algebra homomorphism from $\Omega^{\mathrm{O}} \otimes \mathbb{Q}$ into A. A *complex genus* with values in B is a ring homomorphism from the complex bordism ring Ω_*^{U} into B.

REMARK 5.3. In the literature, an oriented genus is usually referred to simply as a *genus*.

Let F^{MU} and F^{MSO} be the formal group laws of the complex and oriented cobordism theories, respectively, constructed as in Chapter 4, §1.2. By Quillen's Theorem 4.16, the formal group law F^{MU} is universal. As all formal group laws over B can be obtained from F^{MU} via base change, complex genera with values in B are in one-to-one correspondence with formal group laws defined over B. If $\varphi\colon \Omega_*^{\mathrm{U}} \to \Omega_*^{\mathrm{O}} \otimes \mathbb{Q}$ is the forgetful homomorphism, then one has $F^{\mathrm{MSO}} = \varphi_* F^{\mathrm{MU}}$. Therefore, by Theorems 4.17 and 4.6, the logarithm of F^{MSO} is given by

$$\log_{F^{\mathrm{MSO}}}(x) = \sum_{n \geq 0} \frac{[\mathbb{CP}^{2n}]}{2n+1} x^{2n+1}.$$

Since every formal group law over a $\mathbb{Q}$-algebra admits a logarithm, and $\Omega_*^{\mathrm{O}} \otimes \mathbb{Q}$ is free on the $[\mathbb{CP}^{2n}]$ by Theorem 4.6, it follows that oriented genera with values in A are in one-to-one correspondence with formal group laws over A whose logarithms are odd power series of the form $x + \cdots$.

We define the logarithm of an oriented or complex genus φ with values in a ring A of characteristic 0 to be the power series

$$\log_\varphi(x) = \sum_{n\geq 0} \frac{\varphi([\mathbb{CP}^n])}{n+1} x^{n+1} \in (A \otimes \mathbb{Q})[\![x]\!].$$

If F_φ is the formal group law corresponding to φ, then by Theorems 4.16 and 4.17, the logarithms of φ and F_φ coincide.

DEFINITION 5.4. An oriented or complex genus φ with values a $\mathbb{Z}[1/2]$-algebra A is said to be *elliptic* if its logarithm is given by an elliptic integral of the form

$$\log_\varphi(x) = \int_0^x \frac{1}{\sqrt{1-2\delta t^2+\varepsilon t^4}} dt, \quad \delta, \varepsilon \in A. \tag{5.3}$$

Its formal group law F_φ is given by Euler's formula (5.1), and is defined over $\mathbb{Z}[1/2, \delta, \varepsilon]$. Let ψ^{O} (respectively, ψ^{U}) be the elliptic oriented (respectively, complex) genus with values in the ring free polynomial ring $\mathbb{Q}[\delta, \varepsilon]$ whose logarithm is given by (5.3). We call ψ^{O} (respectively, ψ^{U}) the *universal* elliptic oriented (respectively, complex) genus. This terminology is justified since every elliptic oriented (respectively, complex) genus can be obtained from ψ^{O} (respectively, ψ^{U}) by specializing δ and ε.

REMARK 5.5. Let X be a stably, almost-complex manifold. We know that in this case, X has a preferred orientation and thus may also be viewed as an oriented manifold. In such a situation, one has $\psi^{\mathrm{O}}([X]) = \psi^{\mathrm{U}}([X])$.

Let ψ denote either ψ^{O} or ψ^{U}. Using the binomial expansion, we may write $\log_\psi$ in the form

$$\log_\psi(x) = \sum_{n\geq 0} \frac{P_n(\delta, \varepsilon)}{2n+1} x^{2n+1},$$

where the polynomials $P_n(\delta, \varepsilon)$ lie in $\mathbb{Z}[1/2, \delta, \varepsilon]$. These polynomials are related to the classical Legendre polynomials $P_n(\delta)$ defined by the generating series

$$\frac{1}{\sqrt{1-2\delta x+\varepsilon x^2}} = \sum_{n\geq 0} P_n(\delta) x^n.$$

One can verify that $P_n(\delta,1) = P_n(\delta)$ and $P_n(\delta,\varepsilon) = P_n(\delta/\sqrt{\varepsilon})\varepsilon^{n/2}$. For example,

$$P_0(\delta,\varepsilon) = 1, \quad P_1(\delta,\varepsilon) = \delta, \quad P_2(\delta,\varepsilon) = \frac{1}{2}(3\delta^2 - \varepsilon).$$

We can actually be more precise about the images $\psi^{\mathcal{O}}$ and ψ^{U}.

LEMMA 5.6.

(i) *The universal elliptic complex genus ψ^{U} maps Ω^{U}_* into the subring $\mathbb{Z}[1/2,\delta,\varepsilon]$ of $\mathbb{Q}[\delta,\varepsilon]$.*

(ii) *The image of the composite $\Omega^{\mathcal{O}}_* \to \Omega^{\mathcal{O}}_* \otimes \mathbb{Q} \xrightarrow{\psi^{\mathcal{O}}} \mathbb{Q}[\delta,\varepsilon]$ is contained in the subring $\mathbb{Z}[1/2,\delta,\varepsilon]$ of $\mathbb{Q}[\delta,\varepsilon]$.*

PROOF. (i) Since Ω^{U}_* is generated as a ring by the coefficients of F^{MU}, the image of ψ^{U} is contained in the subring of $\mathbb{Q}[\delta,\varepsilon]$ generated by the coefficients of Euler's formal group law, $\psi^{\mathrm{U}}_* F^{\mathrm{MU}}$. We noticed earlier, however, that Euler's formal group law is defined over $\mathbb{Z}[1/2,\delta,\varepsilon]$.

(ii) By (i), the image of the composite

$$\Omega^{\mathrm{U}}_* \to \Omega^{\mathcal{O}}_* \to \Omega^{\mathcal{O}}_* \otimes \mathbb{Q} \xrightarrow{\psi^{\mathcal{O}}} \mathbb{Q}[\delta,\varepsilon]$$

is contained in $\mathbb{Z}[1/2,\delta,\varepsilon]$, where $\Omega^{\mathrm{U}}_* \to \Omega^{\mathcal{O}}_*$ is the forgetful homomorphism. We remarked on page 79 that this forgetful homomorphism is onto, modulo torsion. Since $\mathbb{Q}[\delta,\varepsilon]$ has no torsion, the images of $\Omega^{\mathcal{O}}_*$ and Ω^{U}_* in $\mathbb{Q}[\delta,\varepsilon]$ are equal. □

For geometric characterizations of elliptic genera, see [**29**] or [**16**, Chapter 4].

Let us compute the images under $\psi^{\mathcal{O}}$ and ψ^{U} of various manifolds.

EXAMPLE 5.7. Let ψ denote either $\psi^{\mathcal{O}}$ or ψ^{U} We have two expressions for the logarithm of ψ:

$$\log_\psi(x) = \sum_{n\geq 0} \frac{\psi([\mathbb{CP}^{2n}])}{n+1} x^{n+1} = \sum_{n\geq 0} \frac{P_n(\delta,\varepsilon)}{2n+1} x^{2n+1}.$$

Comparing coefficients, we see that

$$\psi([\mathbb{CP}^{2n}]) = P_n(\delta,\varepsilon), \quad \psi([\mathbb{CP}^{2n+1}]) = 0.$$

In particular, $\psi([\mathbb{CP}^1]) = 0$ and $\psi([\mathbb{CP}^2]) = \delta$.

EXAMPLE 5.8. Let us compute the image of $\mathbb{HP}^2$ under ψ^{O}. In Example 4.9, we showed that $3(\mathbb{CP}^2 \times \mathbb{CP}^2) - 2\mathbb{CP}^4$ and $\mathbb{HP}^2$ have the same image in $\Omega^{\mathrm{O}}_* \otimes \mathbb{Q}$. Therefore,

$$\begin{aligned}\psi^{\mathrm{O}}([\mathbb{HP}^2]) &= 3\psi^{\mathrm{O}}([\mathbb{CP}^2 \times \mathbb{CP}^2]) - 2\psi^{\mathrm{O}}([\mathbb{CP}^4]) \\ &= 3P_1(\delta, \varepsilon) - 2P_2(\delta, \varepsilon) \\ &= 3\delta^2 - 2 \cdot \frac{1}{2}(3\delta^2 - \varepsilon) \\ &= \varepsilon.\end{aligned}$$

EXAMPLE 5.9. Let X be a smooth, projective, complex, algebraic surface, and let $\widetilde{X}$ be the blow-up of X at a point P. We compute the difference between $\psi^{\mathrm{U}}([X])$ and $\psi^{\mathrm{U}}([\widetilde{X}])$. In Example 4.13, we showed that $\widetilde{X} - X$ and $\mathbb{CP}^1 \times \mathbb{CP}^1 - \mathbb{CP}^2$ are complex-bordant. Therefore,

$$\psi^{\mathrm{U}}([\widetilde{X}]) - \psi^{\mathrm{U}}([X]) = \psi^{\mathrm{U}}([\widetilde{X} - X]) = \psi^{\mathrm{U}}([\mathbb{CP}^1 \times \mathbb{CP}^1]) - \psi^{\mathrm{U}}([\mathbb{CP}^2]) = 0^2 - \delta = -\delta,$$

or alternatively, $\psi^{\mathrm{U}}([\widetilde{X}]) = \psi^{\mathrm{U}}([X]) - \delta$.

2. Landweber's exact functor theorem

Let A be a ring and let $\varphi\colon \Omega^{\mathrm{U}}_* \to A$ be a complex genus with values in A. We wish to specialize complex cobordism via φ in order to obtain a new generalized cohomology theory given by the rule

$$X \mapsto \mathrm{MU}^*(X) \underset{\Omega^{\mathrm{U}}_*}{\otimes} A.$$

A condition under which this construction works was formulated by Landweber in [18]. Before we formulate this condition we introduce a piece of terminology. A sequence $a_1, a_2, \ldots$ of elements of a ring A is called *regular* if multiplication by a_1 is injective on A, and multiplication by a_n is injective on $A/(a_1, \ldots, a_{n-1})$, for $n \geq 2$. Suppose $a_1, \ldots, a_{n-1}$ is a regular sequence, and a_n is a unit in $A/(a_1, \ldots, a_{n-1})$.

Then $a_1, \ldots, a_{n-1}, a_n, a_{n+1}, \ldots$ is regular for any choice of elements $a_{n+1}, a_{n+2} \ldots$, as $A/(a_1, \ldots, a_n) = 0$.

Let F be the formal group law over A specified by the genus φ. For each prime p, we consider the formal multiplication-by-p endomorphism of F. Let u_n be the coefficient of x^{p^n} in $[p]_F$.

$$[p]_F(x) = px + \cdots + u_1 x^p + \cdots + u_n x^{p^n} + \cdots . \tag{5.4}$$

THEOREM 5.10 (Landweber [18]). *Suppose that for each prime p, the sequence $p, u_1, u_2, \ldots$ is regular in A. Then the functor $X \mapsto \mathrm{MU}_*(X) \otimes_{\Omega^{\mathrm{U}}_*} A$ defines a generalized homology theory.*

For our purposes, we require a version of this theorem for cohomology.

COROLLARY 5.11. *For finite CW-complexes, the associated cohomology is given by*

$$X \mapsto \mathrm{MU}^*(X) \underset{\Omega^{\mathrm{U}}_*}{\otimes} A.$$

For details on the derivation of this corollary from Theorem 5.10, see the paragraph following the statement of Theorem 2 in [11]. Since the complex projective spaces $\mathbb{CP}^n$ are finite CW-complexes, it follows from the above corollary that the cohomology theories arising from genera satisfying Landweber's condition are complex-oriented.

3. Elliptic cohomology theories

Let $R = \mathbb{Z}[1/2, \delta, \varepsilon]$, and let $\psi^{\mathrm{U}} \colon \Omega^{\mathrm{U}}_* \to R$ be the universal elliptic genus. The corresponding formal group law F is given by Euler's formula (5.1). We claim that if we invert $\Delta = \varepsilon(\delta^2 - \varepsilon)^2$, Landweber's conditions will be satisfied. We must verify that for each prime p, the sequence $p, u_1, u_2, \ldots$ (as in (5.4)) is regular in $R[\Delta^{-1}]$. The verification relies heavily on the theory of elliptic curves.

Since 2 is invertible in $R[\Delta^{-1}]$, the case $p = 2$ is trivial. Therefore, suppose $p \neq 2$. It is clear that multiplication by p is injective on $R[\Delta^{-1}]$. To show that multiplication

by u_1 is injective on $R[\Delta^{-1}] \cong \mathbb{F}_p[\delta, \varepsilon, \Delta^{-1}]$, it suffices to show that u_1 is nonzero, modulo p. Find δ_0, $\varepsilon_0 \in \overline{\mathbb{F}}_p$ such that the elliptic curve

$$E_0 \colon y^2 = 1 - 2\delta_0 x^2 + \varepsilon_0 x^4$$

defined over $\overline{\mathbb{F}}_p$ is ordinary (i.e., not supersingular). Why do such parameters exist? There is a one-to-one correspondence between isomorphism classes of elliptic curves defined over $\overline{\mathbb{F}}_p$ and elements of $\overline{\mathbb{F}}_p$ given by associating to an elliptic curve its j-invariant (see [**37**, Chapter III, Proposition 1.4(b)(c)]). The set of j-invariants corresponding to supersingular elliptic curves over $\overline{\mathbb{F}}_p$ is finite (see [**37**, Theorem 4.1(b), Proof of (c)]). But the j-invariant of an elliptic curve of the form $y^2 = 1 - 2\delta x^2 + \varepsilon x^4$ is a rational function of δ and ε (see (5.7) on page 96). Therefore, there are infinitely many j-invariants corresponding to curves of that form, and the desired parameters δ_0 and ε_0 can be found.

Let F_0 be the formal group law of the curve E_0 obtained by choosing x as a uniformizer at $O = (0, 1)$. By the discussion following Theorem 2.8, F_0 is given by Euler's formula,

$$F_0(x, y) = \frac{x\sqrt{R(y)} + y\sqrt{R(x)}}{1 - \varepsilon x^2 y^2} \in \mathbb{F}_p[\delta_0, \varepsilon_0][\![x, y]\!], \quad R(x) = 1 - 2\delta_0 x^2 + \varepsilon_0 x^4.$$

The map $\theta \colon \mathbb{Z}[1/2, \delta, \varepsilon] \to \mathbb{F}_p[\delta_0, \varepsilon_0]$ specializes F to F_0. Let v_1 be the coefficient of x^p in the multiplication-by-p endomorphism of F_0. Since the elliptic curve E_0 is ordinary, it follows that $v_1 \neq 0$. As $\theta_* F = F_0$, we have $\theta(u_1) = v_1 \neq 0$. Therefore, u_1 is nonzero, modulo p.

We now claim that u_2 is a unit in $R_1 := R[\Delta^{-1}]/(p, u_1)$. If we can verify this claim, we are done, for all subsequent quotients will be trivial. Suppose u_2 is not a unit in R_1. Then we may find a maximal ideal $\mathfrak{m} \subseteq R_1$ with $u_2 \in \mathfrak{m}$. Let $\overline{\delta}$ and $\overline{\varepsilon}$ be the images of δ and ε, respectively, in the field $R_1/\mathfrak{m}$, and consider the curve

$$\overline{E} \colon y^2 = 1 - 2\overline{\delta} x^2 + \overline{\varepsilon} x^4.$$

Since Δ is invertible in R_1, it follows that Δ is nonzero, modulo $\mathfrak{m}$. Therefore, $\overline{E}$ is an elliptic curve. Letting w_n be the coefficient of x^{p^n} in the multiplication-by-p endomorphism of the formal group law of $\overline{E}$. If follows immediately that $w_1 = w_2 = 0$, implying that the height of the formal group law of $\overline{E}$ is greater than two. But this contradicts the fact that the height of the formal group law of an elliptic curve is 1 or 2 (cf. Chapter 2, §4). Therefore, u_2 is a unit in R_1. We have proved the following theorem:

THEOREM 5.12. *Let $\psi^{\mathrm{U}}\colon \Omega^{\mathrm{U}}_* \to \mathbb{Z}[1/2, \delta, \varepsilon]$ be the universal elliptic genus. Then the functor*

$$X \mapsto \mathrm{MU}_*(X) \underset{\Omega^{\mathrm{U}}_*}{\otimes} \mathbb{Z}[1/2, \delta, \varepsilon, \Delta^{-1}]$$

defines a generalized homology theory. The formal group law associated to its (complex-oriented) cohomology theory is given by Euler's formula,

$$F(x, y) = \frac{x\sqrt{R(y)} + y\sqrt{R(x)}}{1 - \varepsilon x^2 y^2}, \quad R(x) = 1 - 2\delta x^2 + \varepsilon x^4.$$

REMARKS 5.13.

(i) One can show that for p odd, we have

$$u_1 \equiv P_{(p-1)/2}(\delta, \varepsilon) \pmod{p},$$

where $P_n(\delta, \varepsilon)$ is as in §1. That u_1 is nonzero modulo p follows from the fact that $P_n(1,1) = 1$ for all n. For details, see [**21**, §2].

(ii) That u_2 is a unit in $R[\Delta^{-1}]$ follows from the congruence

$$u_2 \equiv \left(\frac{-1}{p}\right) \Delta^{(p^2-1)/4} \pmod{p, u_1}.$$

This is proved in [**21**, §3]. Landweber attributes this result to B.H. Gross.

(iii) It is proved in [**11**] that Landweber's condition is still satisfied if instead of inverting Δ, one inverts another element $\rho \in \mathbb{Z}[1/2, \delta, \varepsilon]$ of positive degree. This approach yields cohomology theories whose values on a one point space is $\mathbb{Z}[1/2, \delta, \varepsilon, \rho^{-1}]$. These cohomology theories are known as *elliptic cohomology theories.*

(iv) One can construct an elliptic cohomology theory with coefficient ring $\mathbb{Z}[1/2, \delta, \varepsilon]$ using a construction of "bordism with singularities". For more details on this approach, see [**19**, §3.5].

4. Elliptic genera and modular forms

In this section, we show that one may view the universal elliptic genus as taking its values in a ring on modular forms. We begin by setting ideas, notation, and terminology relating to modular forms. For more details, consult [**35**, Chapter VII], [**16**, Appendix I], or [**8**, Chapter 1].

Let $\mathcal{H}$ denote the Poincaré upper half-plane. The group $\mathrm{SL}(2, \mathbb{Z})$ will be referred to as the modular group. Let $\Gamma_0(2)$ denote the subgroup of $\mathrm{SL}(2, \mathbb{Z})$ consisting of all 2×2 matrices which are upper-triangular, modulo 2. The subgroup $\Gamma_0(2)$ of $\mathrm{SL}(2, \mathbb{Z})$

is non-normal of index 3. The subgroups of the modular group act on $\mathcal{H}$ by fractional-linear transformations. View $\mathcal{H}$ as a subset of $\mathbb{CP}^1 = \mathbb{C} \cup \{\infty\}$. Then subgroups of the modular group also act on the extended upper half-plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{QP}^1$ by fractional-linear transformations.

Let Γ be a subgroup of the modular group. An open subset F_Γ of $\mathcal{H}$ is called a *fundamental domain* for Γ if $\overline{F}_\Gamma$ contains a representative of each orbit of Γ, and F_Γ contains at most one representative of each orbit. Fundamental domains of $\mathrm{SL}(2,\mathbb{Z})$ and $\Gamma_0(2)$ are given by

$$F_{\mathrm{SL}(2,\mathbb{Z})} = \{\, z \in \mathcal{H} \mid -\frac{1}{2} < \Re z < \frac{1}{2}, \quad |z| > 1 \,\}, \tag{5.5}$$

$$F_\Gamma = \{\, z \in \mathcal{H} \mid -\frac{1}{2} < \Re z < \frac{1}{2}, \quad |z-1| > 1, \quad |z+1| > 1 \,\}. \tag{5.6}$$

For proofs, see [**8**, Proposition 1.2.2] and [**16**, p. 79].

The *cusps* of Γ are defined to be the orbits of Γ in $\mathbb{QP}^1$. The points where a fundamental domain of F_Γ meets the boundary of $\mathcal{H}$ in $\mathbb{CP}^1$ constitutes a set of representatives for the cusps of Γ. Abusing terminology, these points will also be referred to as the cusps of Γ. From (5.5) and (5.6), it is evident that $\mathrm{SL}(2,\mathbb{Z})$ has a single cusp at ∞, while $\Gamma_0(2)$ has cusps at 0 and ∞.

Let Γ denote either $\mathrm{SL}(2,\mathbb{Z})$ or $\Gamma_0(2)$. We say that a function $f\colon \mathcal{H} \to \mathbb{C}$ is a *modular function of weight k for Γ* if

(i) f is meromorphic on $\mathcal{H}$,

(ii) for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and all $\tau \in \mathcal{H}$, we have

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau),$$

(iii) f is meromorphic at the cusps of Γ.

Since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$, we have $f(\tau+1) = f(\tau)$ for all modular functions f for Γ. Therefore, any such f can be expanded in a Fourier series of the form $\sum a_n q^n$, where $q = e^{2\pi i \tau}$.

That f must be meromorphic at ∞ says that this Fourier series actually has the form

$$f(\tau) = \sum_{n \geq n_0} a_n q^n$$

for some $n_0 \in \mathbb{Z}$.

A function $f\colon \mathcal{H} \to \mathbb{C}$ is said to be a *modular form of weight k for Γ* if f is a modular function of weight k for Γ, and f is holomorphic at the cusps of Γ. Such a function f has a Fourier expansion of the form $f(\tau) = \sum_{n \geq 0} a_n q^n$. We let $\mathrm{M}_k(\Gamma)$ denote the complex vector space of modular forms of weight k, and let $\mathrm{M}_*(\Gamma) := \bigoplus_k \mathrm{M}_k(\Gamma)$ be be the corresponding graded ring.

We proceed by giving some examples of modular forms. Let Λ be a lattice in $\mathbb{C}$. The *Eisenstein series of weight $2k$* is the series

$$G_{2k}(\Lambda) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^{2k}}.$$

For $\tau \in \mathcal{H}$, we let $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$, and set $G_{2k}(\tau) = G_{2k}(\Lambda_\tau)$. One can show that $G_{2k}(\tau)$ is a modular form of weight $2k$ for $\mathrm{SL}(2,\mathbb{Z})$. Its Fourier expansion is given by

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} + \sum_{n \geq 1} \Big(\sum_{d|n} d^{2k-1} \Big) q^n,$$

where ζ is the Riemann zeta function and $q = e^{2\pi i \tau}$ (see [**37**, Appendix C, Proposition 12.4]). One can show that G_4 and G_6 are algebraically independent generators of the ring $\mathrm{M}_*(\mathrm{SL}(2,\mathbb{Z}))$, that is, $\mathrm{M}_*(\mathrm{SL}(2,\mathbb{Z})) = \mathbb{C}[G_4, G_6]$. For proofs of the above assertions, refer to [**35**, Chapter VII].

One may construct other popular modular functions from these Eisenstein series. Define

$$\Delta = \frac{1}{1728}(G_4^3 - G_6^2), \quad j = G_4^3/\Delta.$$

The function Δ is a modular form of weight 12 for $\mathrm{SL}(2,\mathbb{Z})$, while j is a modular *function* of weight 0 for $\mathrm{SL}(2,\mathbb{Z})$ (j has a simple pole at ∞). Their Fourier expansions

have the form

$$\Delta(\tau) = q - 24q^2 + 252q^3 - 1427q^4 + 4830q^5 + \cdots,$$
$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots.$$

The j-function gives a complex embedding of $\mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}$ into $\mathbb{CP}^1$ which extends to an isomorphism of extended quotient $\mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}^*$ with $\mathbb{CP}^1$. For details, see [**37**, Chapter VII, Proposition 5 and remarks following].

Elliptic curves and modular forms are intimately connected. We first consider elliptic curves given in the standard cubic form $y^2 = 4x^3 - g_2x - g_3$. Recall from Chapter 2, §3.2 that the Weierstrass $\wp$-function $\wp(z,\tau)$ of the lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ parameterizes the elliptic curve

$$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau),$$

where $g_2(\tau) = 60G_4(\tau)$ and $g_3(\tau) = 60G_6(\tau)$. Thus, the coefficients g_2 and g_3 are modular forms of weight 4 and 6, respectively, for $\mathrm{SL}(2,\mathbb{Z})$.

Similarly, the function $\sigma(z,\tau)$, introduced in Chapter 2, §3.3, parameterizes the elliptic curve

$$y^2 = 1 - 2\delta(\tau)x^2 + \varepsilon(\tau)x^4.$$

It can be shown (see [**45**]) that $\delta(\tau)$ and $\varepsilon(\tau)$ are modular forms of weight 2 and 4, respectively, for the group $\Gamma_0(2)$, and that

$$g_2(\tau) = \frac{1}{3}(\delta(\tau)^2 + 3\varepsilon(\tau)) \quad \text{and} \quad g_3(\tau) = \frac{\delta}{27}(\delta(\tau^2) - 9\varepsilon(\tau)).$$

Using these identities, one deduces that

$$j = \frac{g_2^3}{60^3\Delta} = \frac{1}{3^3 \cdot 60^3}\frac{(\delta^2 - 3\varepsilon)^3}{\varepsilon(\delta^2 - \varepsilon)}. \tag{5.7}$$

The modular forms δ and ε are algebraically independent generators of the polynomial ring $\mathrm{M}_*(\Gamma_0(2))$, that is, $\mathrm{M}_*(\Gamma_0(2)) = \mathbb{C}[\delta,\varepsilon]$. The Fouier expansions of δ and ε are

given by

$$\delta(\tau) = -\frac{1}{8} - 3\sum_{n\geq 0}\Big(\sum_{\substack{d|n\\ d \text{ odd}}} d\Big)q^n, \tag{5.8}$$

$$\varepsilon(\tau) = \sum_{n\geq 1}\Big(\sum_{\substack{d|n\\ n/d \text{ odd}}} d^3\Big)q^n, \tag{5.9}$$

where $q = e^{2\pi i\tau}$. These issues are treated in detail in [**16**, Appendix I] and in [**45**].

One can use the modular forms δ and ε to construct a complex embedding of the Riemann surface $\Gamma_0(2)\backslash\mathcal{H}^*$. We claim that the map $\theta\colon \Gamma_0(2)\backslash\mathcal{H}^* \to \mathbb{CP}^1$ given by $\theta(\tau) = (\delta(\tau)^2 : \varepsilon(\tau))$ is an embedding. To see this, define $\gamma\colon \mathbb{CP}^1 \to \mathbb{CP}^1$ by the rule

$$\gamma(x : y) = ((x - 3y)^3 : 3^3 \cdot 60^3\varepsilon(\delta^2 - \varepsilon)^2),$$

and consider the diagram

$$\begin{array}{ccc} \Gamma_0(2)\backslash\mathcal{H}^* & \xrightarrow{\theta} & \mathbb{CP}^1 \\ {\scriptstyle \tau\mapsto\tau}\big\downarrow & & \big\downarrow{\scriptstyle \gamma} \\ \mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}^* & \xrightarrow[j]{} & \mathbb{CP}^1. \end{array}$$

By (5.7), this diagram commutes. Since $\Gamma_0(2)$ has index 3 in $\mathrm{SL}(2,\mathbb{Z})$, the map $\theta\colon \Gamma_0(2)\backslash\mathcal{H}^* \to \mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}$ is a triple covering. The map γ is also a triple covering, as it is described by polynomials of degree 3. As we mentioned before, j is an isomorphism. Therefore, the composite $\gamma \circ \theta$ is a triple covering. It follows that θ is one-to-one, and being a morphism of compact Riemann surfaces, must be an isomorphism.

From Lemma 5.6, we know that ψ^{U} and ψ^{O} map Ω^{U}_* and Ω^{O}_*, respectively, into $\mathbb{Z}[1/2, \delta, \varepsilon]$. Since these elliptic genera are in fact graded homomorphisms, ψ^{U} (respectively, ψ^{O}) assigns to each stably almost-complex manifold (respectively, oriented manifold) of real dimension $2n$ a modular form of weight n in $\mathbb{Z}[1/2, \delta, \varepsilon]$. These modular forms can be described as follows.

THEOREM 5.14.

(i) *The ring* $\mathbb{Z}[1/2, \delta, \varepsilon]$ *consists of all modular forms for* $\Gamma_0(2)$ *whose Fourier coefficients lie in the ring* $\mathbb{Z}[1/2]$.

(ii) *The localization* $\mathbb{Z}[1/2, \delta, \varepsilon][\Delta^{-1}]$ *can be identified with the ring of modular functions for* $\Gamma_0(2)$ *which are holomorphic on* $\mathcal{H}$.

PROOF. (i) View $\mathbb{Z}[1/2, \delta, \varepsilon]$ as a subring of $\mathrm{M}_*(\Gamma_0(2))$. For any ring R with $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$, let $\mathrm{M}_*^R(\Gamma_0(2))$ denote the set of modular forms for $\Gamma_0(2)$ whose Fourier coefficients lie in R. The proof of (i) will follow from the following claim.

For any ring R with $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$, we have

$$\mathrm{M}_*^R(\Gamma_0(2)) = R[8\delta, \varepsilon].$$

The inclusion "$\supseteq$" follows from the above (5.8) and (5.9). Conversely, suppose $f \in \mathrm{M}_{2k}^R(\Gamma_0(2))$. Let $c_n \in R$ denote its n-th Fourier coefficient. Since δ and ε generate $\mathrm{M}_*(\Gamma_0(2))$, we may write

$$f = \sum_{\ell \leq k/2} a_\ell (-8\delta)^{k-2\ell} \varepsilon^\ell,$$

where $a_\ell \in \mathbb{C}$. It follows again from (5.8) and (5.9) that

$$a_\ell (-8\delta)^{2k-\ell} \varepsilon^\ell = a_\ell q^\ell + \sum_{n > \ell} a_\ell b_n^{(\ell)} q^n,$$

where $b_n^{(\ell)} \in \mathbb{Z}$. Collecting terms, we obtain

$$\sum_{\ell \leq k/2} a_\ell (-8\delta)^{k-2\ell} \varepsilon^\ell = \sum_{n \geq 0} \Big(\sum_{\ell < n} a_\ell b_n^{(\ell)} + a_n \Big) q^n.$$

Comparing terms, see that

$$a_n = c_n - \sum_{\ell < n} a_\ell b_n^{(\ell)}.$$

In particular, $a_0 = c_0$. Suppose, for the purposes of induction, that $a_1, \ldots, a_n$ are in R. Then since c_{n+1} is also in R and each $b_{n+1}^{(\ell)}$ is an integer, it follows from the above identity that $a_{n+1} \in R$. Therefore, by induction, the proof of (i) is complete.

(ii) Recall that $\Delta = \varepsilon(\delta^2 - \varepsilon)^2$. From the fact that δ and ε are holomorphic on $\mathcal{H} \cup \{\infty\}$ and nonvanishing on $\mathcal{H}$, it follows that Δ is a modular function for $\Gamma_0(2)$ which is holomorphic on $\mathcal{H}$. Conversely, we note that Δ has a zero at ∞, as ε does. Therefore, if f is a modular function for $\Gamma_0(2)$ which is holomorphic on $\mathcal{H}$, then $f\Delta^N$ is a modular form for sufficiently large N. If, in addition, the Fourier coefficients of f lie in $\mathbb{Z}[1/2]$, it follows from (i) and the fact that the Fourier coefficients of Δ lie in $\mathbb{Z}[1/2]$ that $f\Delta^N \in \mathbb{Z}[1/2, \delta, \varepsilon]$. Thus, $f \in \mathbb{Z}[1/2, \delta, \varepsilon][\Delta^{-1}]$, and (ii) is proved. □

Thus, the universal elliptic genus assigns a modular form to each manifold! Two cobordant manifolds are assigned the same modular form. Also, the rings of coefficients of the elliptic cohomology theories can be viewed as rings of modular forms.

5. Conclusion

In this text, we have barely scratched the surface of the theories of elliptic cohomology and elliptic genera; much research has been done on these topics and many tantilizing questions remain.

There is a body of work by A. Baker [**3**, **4**] establishing precisely the relationship between operations in elliptic cohomology and isogenies of supersingular elliptic curves. In particular, Baker proves in [**3**] the "supersingular congruence"

$$(E_{p+1})^{p-1} \equiv -\left(\frac{-1}{p}\right)\Delta^{(p^2-1)/12} \pmod{p, E_{p-1}}$$

between the Eisenstein functions E_{p+1} and E_{p-1}, and the modular form Δ. This congruence is intimately related to the congruence of Gross mentioned in Remark 5.13(ii).

Much research is also being done in the field of elliptic genera. In [**16**], Hirzebruch develops generalized elliptic genera which take values in rings of modular forms of higher level. We observed earlier that the universal elliptic genus assigns to each manifold a modular form. There are many papers devoted to investigating this correspondence in various specific cases. A striking result of [**9**] computes the elliptic genus on a symmetric power of a manifold X in terms of its value on X itself. Elliptic

genera of Calabi-Yau manifolds have also been computed, and relations with mirror symmetry have been noted. In [7], it is shown that the elliptic genus of a Calabi-Yau manifold is a Jacobi form and that the elliptic genera of Calabi-Yau hypersurfaces in toric varieties and their mirrors coincide up to sign.

Properties of families of modular forms attached to families of manifolds have also been studied. In [5], Borisov and Gunnels investigate a subring of the ring of modular forms for $\Gamma_1(\ell)$ which is naturally associated to the family of toric varieties. They show that this family of "toric modular forms" has many nice properties – it is a finitely generated ring over $\mathbb{C}$, and it is stable under the Hecke operators and the Fricke involution. In [6], they characterize the space of weight two toric forms as a vector space generated by cusp eigenforms whose L-functions satisfy a nonvanishing condition.

Elliptic genera are also of interest to mathematical physicists. In [43, 44], E. Witten discusses how one may view the elliptic genus as the index of a certain Dirac-like operator on loop space. He also presents connections between elliptic genera and quantum field theory.

Perhaps the most fundamental outstanding issue in the theory of elliptic cohomology at present is the lack of an intrinsic, geometric description of this cohomology theory in general. There are specific instances of elliptic cohomology, though, in which one does have a geometric description to work with. Moonshine phenomena allow one to describe geometrically the elliptic cohomology groups of the classifying spaces of finite groups; see [40]. It is perceived that it is the lack of an intrinsic description of elliptic cohomology that is currently limiting its application. In words of Thomas [40, p. v], "With more geometric input, elliptic cohomology may resolve some of the open questions which seem just beyond the reach of K-theory".

APPENDIX A

N-dimensional formal group laws

1. Definition and examples

DEFINITION A.1. An N-dimensional, commutative formal group law with coefficients from R (or more briefly, a formal group law over R) is an N-tuple of power series

$$F_1(x_1,\dots,x_N,y_1,\dots,y_N),\dots,F_N(x_1,\dots,x_N,y_1,\dots,y_N)$$

in $R[\![x_1,\dots,x_N,y_1,\dots,y_N]\!]$ satisfying:

(i) For $i=1,\dots,N$, we have the identity

$$\begin{aligned}&F_i(x_1,\dots,x_N,F_1(y_1,\dots,y_N,z_1,\dots,z_N),\dots,F_N(y_1,\dots,y_N,z_1,\dots,z_N))\\ =&F_i(F_1(x_1,\dots,x_N,y_1,\dots,y_N),\dots,F_N(x_1,\dots,x_N,y_1,\dots,y_N),z_1,\dots,z_N)\end{aligned}$$

in the power series ring $R[\![x_1,\dots,x_N,y_1,\dots,y_N,z_1,\dots,z_N]\!]$.

(ii) For $i=1,\dots,N$, we have

$$F_i(x_1,\dots,x_N,y_1,\dots,y_N)=F_i(y_1,\dots,y_N,x_1,\dots,x_N).$$

(iii) For $i=1,\dots,N$, we have $F_i(x_1,\dots,x_N,0,\dots,0)=x_i$ and $F_i(0,\dots,0,y_1,\dots,y_N)=y_i$.

(iv) There exists an N-tuple of power series $\iota_1(x_1,\dots,x_N),\dots,\iota_N(x_1,\dots x_N)$ such that for each $i=1,\dots,N$,

$$F_i(x_1,\dots,x_N,\iota_1(x_1,\dots,x_N),\dots,\iota_N(x_1,\dots x_N))=0.$$

REMARK A.2. By using the formal implicit function theorem, one may actually deduce (iv) from (i)-(iii). Thus, any N-tuple of power series satisfying (i)-(iii) is a formal group law.

The above notation is quite cumbersome; we introduce the following shorthand. We will often write x (respectively, y) for the list $x_1, \ldots, x_N$ (respectively, $y_1, \ldots, y_N$). Also, we may write F for the list $F_1, \ldots, F_n$. With these conventions, conditions (i)-(iv) take on a more pleasing form.

(i) $F(x, F(y, z)) = F(F(x, y), z)$,
(ii) $F(x, y) = F(y, x)$,
(iii) $F(x, 0) = x$ and $F(0, y) = y$,
(iv) There exists an N-tuple of power series $\iota = (\iota_1, \ldots, \iota_N)$ in $R[\![x]\!]$ such that $F(x, \iota(x)) = F(\iota(y), y) = 0$.

The N-tuple ι is known as the formal inverse.

NOTATION A.3 (Multi-index notation). We introduce a convenient notational device. An infinite sequence of nonnegative integers $\mathbf{j} = (j_1, j_2, \ldots)$ with only finitely many nonzero terms will be called a *multi-index*. We let $\mathbf{0} = (0, 0, \ldots)$. Partially order the collection of all multi-indices by saying $\mathbf{j} \leq \mathbf{k}$ if $j_i \leq k_i$ for all i. We write $\mathbf{j} < \mathbf{k}$ if $\mathbf{j} \leq \mathbf{k}$ but $\mathbf{j} \neq \mathbf{k}$, that is, there is strict inequality in at least one component. We let $\mathbf{e}_i$ be the multi-index with 1 in the i-th component and zero in every other component. We add multi-indices componentwise. If $x_1, \ldots, x_N$ are indeterminates and $\mathbf{j}$ is a multi-index, we let $x^{\mathbf{j}}$ denote the monomial $x_1^{j_1} x_2^{j_2} \cdots x_N^{j_N}$.

Using this notation, we see that a formal group law F must have the form

$$F_i(x, y) = x_i + y_i + \sum_{\mathbf{j}>\mathbf{k}>\mathbf{0}} a_{\mathbf{jk}}(x^{\mathbf{j}} y^{\mathbf{k}} + x^{\mathbf{k}} y^{\mathbf{j}}) + \sum_{\mathbf{l}>\mathbf{0}} a_{\mathbf{l}\mathbf{l}} x^{\mathbf{l}} y^{\mathbf{l}}. \tag{A.1}$$

For completeness, we mention a few standard examples.

EXAMPLE A.4. The *N-dimensional formal additive group law* is given by the N-tuple of power series $\mathcal{G}_a^N$ where

$$\mathcal{G}_{a,i}^N(x,y) = x_i + y_i.$$

The formal inverse is given by $\iota(x) = -x$.

EXAMPLE A.5. The *N-dimensional formal multiplicative group law* is given by N power series

$$\mathcal{G}_m^N(x,y) = x_i + y_i + x_i y_i.$$

Its formal inverse is given by $\iota(x) = -x + x^2 - x^3 + \cdots$.

EXAMPLE A.6. Let K be a field and let A/K be an abelian variety of dimension n with neutral element O. We obtain an n-dimensional formal group law from A by expanding the group law on A around O. We will only sketch the details of the construction, as they are quite similar to the one-dimensional (elliptic curve) case. Let $\alpha\colon A \times A \to A$ be the group law on A. Then α induces a map between the local rings,

$$\alpha^*\colon \widehat{\mathcal{O}}_{A,O} \to \widehat{\mathcal{O}}_{A,O} \mathop{\widehat{\otimes}}_K \widehat{\mathcal{O}}_{A,O}.$$

By the Cohen structure theorem, $\widehat{\mathcal{O}}_{A,O} \cong K[\![x_1, \ldots, x_n]\!]$. Noting that

$$K[\![x_1, \ldots, x_n]\!] \mathop{\widehat{\otimes}}_K K[\![x_1, \ldots, x_n]\!] \cong K[\![x_1 \mathbin{\widehat{\otimes}} 1, \ldots, x_n \mathbin{\widehat{\otimes}} 1, 1 \mathbin{\widehat{\otimes}} x_1, \ldots, 1 \mathbin{\widehat{\otimes}} x_n]\!],$$

we may view α^* as a map from $K[\![x_1, \ldots, x_n]\!]$ into $K[\![x_1 \mathbin{\widehat{\otimes}} 1, \ldots, x_n \mathbin{\widehat{\otimes}} 1, 1 \mathbin{\widehat{\otimes}} x_1, \ldots, 1 \mathbin{\widehat{\otimes}} x_n]\!]$. For $i = 1, \ldots, n$, let

$$F_i(x_1 \mathbin{\widehat{\otimes}} 1, \ldots, x_n \mathbin{\widehat{\otimes}} 1, 1 \mathbin{\widehat{\otimes}} x_1, \ldots, 1 \mathbin{\widehat{\otimes}} x_n) = \alpha^* x_i.$$

Then $F = (F_1, \ldots, F_n)$ is an n-dimensional formal group law defined over K.

2. Logarithms

One can produce many formal group laws using the following construction. Let $f = (f_1, \ldots, f_n)$ be an N-tuple of power series from $R[\![x_1, \ldots, x_N]\!]$ with no constant terms. Let $Df = (\partial f_i/\partial x_j)$ be the $N \times N$ Jacobian matrix of f, and suppose that $Df(0)$ is the identity matrix. Then by the formal inverse function theorem, f is invertible (with respect to composition), and the rule

$$F(x, y) = f^{-1}(f(x) + f(y)) \tag{A.2}$$

defines a formal group law. The N-tuple f is called the *logarithm* of F, and is often denoted $\log_F$. It will follow from our construction of an N-dimensional formal group law that each formal group law $F(x, y)$ defined over a ring R of characteristic zero admits a logarithm defined over $R \otimes \mathbb{Q}$.

3. The N-dimensional comparison lemma

The relevant definitions and results about buds carry over, mutatis mutandis, to the N-dimensional case.

Theorem 1.24 and the Lazard Comparison Lemma 1.25 were our main tools in the construction of a universal one-dimensional formal group law over the ring $\mathbb{Z}[u_2, u_3, \ldots]$. In order to generalize our arguments to N dimensions, we must first appropriately generalize these results.

Let $\mathbf{n}$ and $\mathbf{k}$ be multi-indices (see Notation A.3). We define

$$|\mathbf{n}| = n_1 + n_2 + \cdots + n_N,$$
$$\binom{\mathbf{n}}{\mathbf{k}} = \binom{n_1}{k_1} \cdots \binom{n_N}{k_N},$$
$$\nu(\mathbf{n}) = \gcd\{ \binom{\mathbf{n}}{\mathbf{k}} \mid 0 < \mathbf{k} < \mathbf{n} \}.$$

Our first task is to define the family of polynomials which will play the role of the (one-dimensional) polynomials $C_n(x, y)$. We define the polynomial

$$\begin{aligned} C_{\mathbf{n}}(x, y) &= \frac{1}{\nu(\mathbf{n})}[(x_1 + y_1)^{n_1} \cdots (x_N + y_N)^{n_N} - x_1^{n_1} \cdots x_N^{n_N} - y_1^{n_1} \cdots y_N^{n_N}] \\ &= \frac{1}{\nu(\mathbf{n})}[(x + y)^{\mathbf{n}} - x^{\mathbf{n}} - y^{\mathbf{n}}]. \end{aligned}$$

It is clear that $C_{\mathbf{n}}$ satisfies Lazard's conditions (see Definition 1.23). It is these polynomials which will play the role of the C_n (in fact, they are a generalization of the C_n). Note that $C_{\mathbf{n}}$ is a primitive polynomial in $\mathbb{Z}[x, y]$.

We wish to prove the following theorem characterizing N-dimensional Lazard polynomials.

THEOREM A.7. *Let B be an abelian group and $H(x, y) \in A[x, y]$ be a polynomial satisfying Lazard's conditions. Then $H(x, y)$ can be written as a B-linear combination of polynomials $C_{\mathbf{n}}$, $|\mathbf{n}| = \deg H(x, y)$.*

This theorem combined with Corollary 1.22 give the N-dimensional analogue of the one-dimensional Lazard Comparison Lemma. We define an N-dimensional n-bud to be an N-tuple of power series F which satisfies the axioms of an N-dimensional formal group law, mod degree $n + 1$.

THEOREM A.8 (N-dimensional Lazard Comparison Lemma). *Let F and G be two N-dimensional n-buds defined over a ring R with $F(x, y) \equiv G(x, y)$* (mod degree n). *Then for $i = 1, \ldots, N$ and multi-indices $\mathbf{j}$ with $|\mathbf{j}| = n$ there exist elements $a(i, \mathbf{j}) \in R$ such that*

$$F_i(x, y) \equiv G_i(x, y) + \sum_{|\mathbf{j}|=n} a(i, \mathbf{j}) C_{\mathbf{j}}(x, y) \quad (\text{mod degree } n + 1).$$

We will prove Theorem A.7 essentially by reduction to the 1-dimensional case.

Let B be an abelian group and $H(x,y) \in B[x,y]$ be a symmetric polynomial of degree m with $H(x,0) = H(0,y) = 0$. Then $H(x,y)$ may be written in the form

$$H(x,y) = \sum_{|\mathbf{n}|=m} \sum_{0<\mathbf{k}<\mathbf{n}} c(\mathbf{n},\mathbf{k}) x^{\mathbf{k}} y^{\mathbf{n}-\mathbf{k}}.$$

One checks that $H(x,y)$ satisfies Lazard's conditions if and only if $c(\mathbf{n},\mathbf{k}) = c(\mathbf{n},\mathbf{n}-\mathbf{k})$ for all $\mathbf{n},\mathbf{k}$, and

$$\text{(A.3)} \qquad \binom{\mathbf{i}+\mathbf{j}}{\mathbf{j}} c(\mathbf{n},\mathbf{i}+\mathbf{j}) = \binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} c(\mathbf{n},\mathbf{j}+\mathbf{k}) \quad \text{for } \mathbf{i},\mathbf{j},\mathbf{k} > 0 \text{ with } \mathbf{i}+\mathbf{j}+\mathbf{k} = \mathbf{n}$$

(cf. Equation (1.5)). To prove Theorem A.7, we show that for each $\mathbf{n}$ with $|\mathbf{n}| = m$, we can find some $b_{\mathbf{n}} \in B$ with

$$\sum_{0<\mathbf{k}<\mathbf{n}} c(\mathbf{n},\mathbf{k}) x^{\mathbf{k}} y^{\mathbf{n}-\mathbf{k}} = b_{\mathbf{n}} C_{\mathbf{n}}(x,y).$$

The above relations, combined with the fact that we can work 'one $\mathbf{n}$ at a time', leads us naturally to consider the following object.

Fix a multi-index $\mathbf{n}$ with $|\mathbf{n}| = m$, and let $A_{\mathbf{n}}$ be the abelian group generated freely by the set $\{\, u(\mathbf{n},\mathbf{k}) \mid 0 < \mathbf{k} < \mathbf{n} \,\}$ subject to the relations $u(\mathbf{n},\mathbf{k}) = u(\mathbf{n},\mathbf{n}-\mathbf{k})$ and

$$\binom{\mathbf{i}+\mathbf{j}}{\mathbf{j}} u(\mathbf{n},\mathbf{i}+\mathbf{j}) = \binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} u(\mathbf{n},\mathbf{j}+\mathbf{k}) \quad \text{for } \mathbf{i},\mathbf{j},\mathbf{k} > 0 \text{ with } \mathbf{i}+\mathbf{j}+\mathbf{k} = \mathbf{n}.$$

With notation as above, it is clear that there is a unique homomorphism $\psi : A_{\mathbf{n}} \to B$ with $\psi u(\mathbf{n},\mathbf{k}) = c(\mathbf{n},\mathbf{k})$ for all $\mathbf{k}$ with $0 < \mathbf{k} < \mathbf{n}$, or equivalently,

$$\psi_* \sum_{0<\mathbf{k}<\mathbf{n}} u(\mathbf{n},\mathbf{k}) x^{\mathbf{k}} y^{\mathbf{n}-\mathbf{k}} = \sum_{0<\mathbf{k}<\mathbf{n}} c(\mathbf{n},\mathbf{k}) x^{\mathbf{k}} y^{\mathbf{n}-\mathbf{k}}.$$

The following lemma describes the structure of $A_{\mathbf{n}}$ is some cases.

LEMMA A.9. *Let $\mathbf{n}$ be a multi-index, and suppose $\mathbf{n}$ has more than one nonzero component. Let i be the smallest index such that n_i is nonzero. Then $A_{\mathbf{n}}$ is generated by the single element $u(\mathbf{n}, n_i \mathbf{e}_i)$.*

PROOF. We show how to express each generator $u(\mathbf{n}, \mathbf{k})$ as an integer multiple of the element $u(\mathbf{n}, n_i\mathbf{e}_i)$. We consider two cases.

Case 1. Let $\mathbf{j} = j\mathbf{e}_i$. Define $\mathbf{k} = (n_i - j)\mathbf{e}_i$ and $\mathbf{l} = \mathbf{n} - \mathbf{j} - \mathbf{k}$. Then

$$u(\mathbf{n}, \mathbf{j}) = u(\mathbf{n}, \mathbf{n} - \mathbf{j}) = u(\mathbf{n}, \mathbf{l} + \mathbf{k}), \quad \binom{\mathbf{l}+\mathbf{k}}{\mathbf{l}} = 1, \quad u(\mathbf{n}, \mathbf{j} + \mathbf{k}) = u(\mathbf{n}, n_i\mathbf{e}_i).$$

Therefore,

$$u(\mathbf{n}, \mathbf{j}) = \binom{\mathbf{l}+\mathbf{k}}{\mathbf{l}} u(\mathbf{n}, \mathbf{l} + \mathbf{k}) = \binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} u(\mathbf{n}, \mathbf{j} + \mathbf{k}) = \binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} u(\mathbf{n}, n_i\mathbf{e}_i).$$

Case 2. Suppose $\mathbf{r}$ is not of the form $j\mathbf{e}_i$. We may without loss of generality assume that $0 < r_i \leq n_i$, for otherwise replace $\mathbf{r}$ with $\mathbf{n} - \mathbf{r}$ and use the fact that $u(\mathbf{n}, \mathbf{r}) = u(\mathbf{n}, \mathbf{n} - \mathbf{r})$. Let $\mathbf{j} = r_i\mathbf{e}_i$, $\mathbf{k} = \mathbf{r} - \mathbf{j}$, and $\mathbf{l} = \mathbf{n} - \mathbf{j} - \mathbf{k}$. Then

$$u(\mathbf{n}, \mathbf{r}) = u(\mathbf{n}, \mathbf{j} + \mathbf{k}), \quad \binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} = 1, \quad u(\mathbf{n}, \mathbf{k} + \mathbf{l}) = u(\mathbf{n}, \mathbf{j}) = u(\mathbf{n}, r_i\mathbf{e}_i).$$

Therefore,

$$u(\mathbf{n}, \mathbf{r}) = \binom{\mathbf{j}+\mathbf{k}}{\mathbf{k}} u(\mathbf{n}, \mathbf{j} + \mathbf{k}) = \binom{\mathbf{l}+\mathbf{k}}{\mathbf{l}} u(\mathbf{n}, \mathbf{l} + \mathbf{k}) = \binom{\mathbf{l}+\mathbf{k}}{\mathbf{l}} u(\mathbf{n}, r_i\mathbf{e}_i).$$

By Case 1, $u(\mathbf{n}, r_i\mathbf{e}_i)$ is in the subgroup generated by $u(\mathbf{n}, n_i\mathbf{e}_i)$, so we are done. □

We are now in a position to complete the proof of Theorem A.7.

PROOF OF THEOREM A.7. Let

$$G_{\mathbf{n}}(x, y) = \sum_{\mathbf{0}<\mathbf{k}<\mathbf{n}} u(\mathbf{n}, \mathbf{k}) x^{\mathbf{k}} y^{\mathbf{n}-\mathbf{k}} \in A_{\mathbf{n}}[x, y].$$

It suffices to show that $G_{\mathbf{n}}(x, y) = b_{\mathbf{n}} C_{\mathbf{n}}(x, y)$ for some $\mathbf{n} \in A_{\mathbf{n}}$. If $\mathbf{n}$ has only one nonzero component, then this is just the one dimensional case. Thus assume $\mathbf{n}$ has more that one nonzero component and i is the smallest index with n_i nonzero.

Since $C_{\mathbf{n}}$ is a Lazard polynomial over $\mathbb{Z}$ and $\nu(\mathbf{n}) = 1$, the map $\psi : A_{\mathbf{n}} \to \mathbb{Z}$ defined by the rule

$$\psi u(\mathbf{n}, \mathbf{k}) = \binom{\mathbf{n}}{\mathbf{k}}$$

is a well defined homomorphism (this is the unique homomorphism satisfying $\psi_* G_{\mathbf{n}} = C_{\mathbf{n}}$). By the above lemma, we may find, for each $\mathbf{k}$, some $a_{\mathbf{k}} \in \mathbb{Z}$ with

$$u(\mathbf{n}, \mathbf{k}) = a_{\mathbf{k}} u(\mathbf{n}, n_i \mathbf{e}_i).$$

Applying ψ to this equation, we obtain

$$\binom{\mathbf{n}}{\mathbf{k}} = a_{\mathbf{k}} \binom{\mathbf{n}}{n_i \mathbf{e}_i} = a_{\mathbf{k}}.$$

Substituting, we have

$$G_{\mathbf{n}}(x, y) = u(\mathbf{n}, n_i \mathbf{e}_i) \sum_{0<\mathbf{k}<\mathbf{n}} \binom{\mathbf{n}}{\mathbf{k}} x^{\mathbf{k}} y^{\mathbf{n}-\mathbf{k}} = u(\mathbf{n}, n_i \mathbf{e}_i) C_{\mathbf{n}}(x, y).$$

□

4. Construction of a universal, N-dimensional formal group law

The logical structure of our construction of an N-dimensional formal group law is the same as that in the one-dimensional case. Due to the increased volume of notation, we recapitulate much of the argument.

For each $i = 1, \ldots, N$ and each multi-index $\mathbf{j}$ of length N, we introduce an indeterminate $u(i, \mathbf{j})$. We introduce the shorthand

$$A = \mathbb{Z}[u(i, \mathbf{j}) \mid i = 1, \ldots, N \text{ and } |\mathbf{j}| \geq 2],$$

$$A^{(n)} = \mathbb{Z}[u(i, \mathbf{j}) \mid i = 1, \ldots, N \text{ and } 2 \leq |\mathbf{j}| \leq n], \quad n \geq 2.$$

We also let $A^{(1)} = \mathbb{Z}$.

LEMMA A.10. *One may inductively construct two sequences of N-tuples of power series, $F^{(n)}(x_1, \ldots, x_N, y_1, \ldots, y_N)$ and $f^{(n)}(x_1, \ldots, x_N)$,*

$$F^{(n)}(x, y) = (F_1^{(n)}(x, y), \ldots, F_N^{(n)}(x, y))$$

$$f^{(n)}(x) = (f_1^{(n)}(x), \ldots, f_N^{(n)}(x)),$$

satisfying the following conditions for all $n \geq 1$.

(i) $F_i^{(n)}(x, y) \in A^{(n)}[\![x, y]\!], \quad f_i^{(n)}(x) \in (A^{(n)} \otimes \mathbb{Q})[\![x]\!],$

(ii) $F^{(n+1)}(x,y) \equiv F^{(n)}(x,y)$ *and* $f^{(n+1)}(x) \equiv f^{(n)}(x) \pmod{\text{degree } n+1}$,

(iii) $f^{(n)}(F^{(n)}(x,y)) \equiv f^{(n)}(x) + f^{(n)}(y) \pmod{\text{degree } n+1}$,

(iv) *If* $n \geq 2$, *then for each* $i = 1, \ldots, N$,

$$F_i^{(n)}(x,y) - \sum_{|\mathbf{j}|=n} u(i,\mathbf{j}) C_{\mathbf{j}}(x,y) \in A^{(n-1)}[\![x,y]\!].$$

PROOF. We proceed by induction on n. For $n = 1$, we define $F_i^{(1)}(x,y) = x_i + y_i$ and $f_i^{(1)}(x) = x_i$ for $i = 1, \ldots, N$. Defined in this way, $F^{(1)}$ and $f^{(1)}$ clearly satisfy the required conditions.

Now suppose we have have constructed $F^{(1)}, \ldots, F^{(n)}$ and $f^{(1)}, \ldots, f^{(n)}$ satisfying conditions (i)-(iv) of the lemma. We wish to construct $F^{(n+1)}$ and $f^{(n+1)}$.

Let $\Phi^{(n)}$ be the formal group law with logarithm $f^{(n)}$. By an argument analogous to that presented in the one-dimensional case, we may find an N-tuple $H = (H_1, \ldots, H_n)$ of homogeneous polynomials of degree $n+1$ in $(A^{(n)} \otimes \mathbb{Q})[x,y]$, such that

$$\Phi^{(n)}(x,y) \equiv F^{(n)}(x,y) + H(x,y) \pmod{\text{degree } n+2} \tag{A.4}$$

Essentially by clearing denominators, we may find a positive integer k such that $kH_i(x,y) \in A^{(n)}[x,y]$ for $i = 1, \ldots, N$, and each kH_i satisfies Lazard's conditions, modulo k. More precisely, $H(x,y) = H(x,y)$ and $\delta(kH) \equiv 0 \pmod{k}$. Therefore, by Theorem A.7, for $i = 1, \ldots, N$ and each multi-index $\mathbf{j}$ with $|\mathbf{j}| = n+1$, we may find some $a(i,\mathbf{j}) \in A^{(n)}$ such that

$$kH_i(x,y) \equiv \sum_{|\mathbf{j}|=n+1} a(i,\mathbf{j}) C_{\mathbf{j}}(x,y) \pmod{k}.$$

Thus, we may find polynomials $H_1'(x,y), \ldots, H_N'(x,y) \in A^{(n)}[x,y]$ such that

$$kH_i(x,y) = \sum_{|\mathbf{j}|=n+1} a(i,\mathbf{j}) C_{\mathbf{j}}(x,y) + kH_i'(x,y), \tag{A.5}$$

for $i = 1, \ldots, N$.

We may now define, for $i = 1, \ldots, N$,

$$F_i^{(n+1)}(x,y) = F_i^{(n)}(x,y) + H_i'(x,y) + \sum_{|\mathbf{j}|=n+1} u(i,\mathbf{j})C_{\mathbf{j}}(x,y), \tag{A.6}$$

$$f_i^{(n+1)} = f_i^{(n+1)}(x) - \sum_{|\mathbf{j}|=n+1} \frac{1}{\nu(\mathbf{j})}\left[u(i,\mathbf{j}) - \frac{a(i,\mathbf{j})}{k}\right] x^{\mathbf{j}}. \tag{A.7}$$

It is clear that $F^{(n+1)}$ and $f^{(n+1)}$ satisfy conditions (i), (ii), and (iv) of the lemma; it remains to verify (iii).

Let $\beta(i,\mathbf{j}) = u(i,\mathbf{j}) - a(i,\mathbf{j})/\nu(\mathbf{j})$. If follows from Equations A.4, A.5, and A.6 that for $i = 1, \ldots, N$,

$$F_i^{(n+1)}(x,y) \equiv \Phi_i^{(n)} + \sum_{|\mathbf{j}|=n+1} \beta(i,\mathbf{j})C_{\mathbf{j}}(x,y) \pmod{\text{degree } n+2}. \tag{A.8}$$

By Equation A.7, for $i = 1, \ldots, N$,

$$\begin{aligned} f_i^{(n+1)}(F^{(n+1)}(x,y)) &= f_i^{(n)}(F^{(n+1)}(x,y)) \\ &\quad - \sum_{|\mathbf{j}|=n+1} \frac{\beta(i,\mathbf{j})}{\nu(\mathbf{j})} F_1^{(n+1)}(x,y)^{j_1} \cdots F_N^{(n+1)}(x,y)^{j_N}. \end{aligned} \tag{A.9}$$

We wish to approximate each term on the right hand side of the above equation modulo degree $n+2$. We accomplish this using the following easy lemma.

LEMMA A.11. *Let f be a polynomial of the form*

$$f(x_1, \ldots, x_N) = x_i + \textit{higher order terms.}$$

Let $g_1, \ldots, g_N$ be polynomials with no constant term, and let $h_1, \ldots, h_N$ be homogeneous polynomials of degree m. Then

$$f(g_1 + h_1, \ldots, g_N + h_N) \equiv f(g_1, \ldots, g_N) + h_i \pmod{\text{degree } m+1}.$$

Working modulo degree $n+2$, we have for $i = 1, \ldots, N$,

$$\begin{aligned} f_i^{(n)}(F^{(n+1)}(x,y)) &\equiv f_i^{(n)}(\Phi_1^{(n)}(x,y) + \sum_{|\mathbf{j}|=n+1} \beta(1,\mathbf{j})C_{\mathbf{j}}(x,y), \cdots \\ &\qquad \cdots, \Phi_N^{(n)}(x,y) + \sum_{|\mathbf{j}|=n+1} \beta(N,\mathbf{j})C_{\mathbf{j}}(x,y)) \\ &\equiv f_i^{(n)}(\Phi_1^{(n)}(x,y), \ldots, \Phi_N^{(n)}(x,y)) + \\ &\qquad + \sum_{|\mathbf{j}|=n+1} \beta(i,\mathbf{j})C_{\mathbf{j}}(x,y), \end{aligned} \tag{A.10}$$

by the above lemma with $f = f_i^{(n)}$, $g_r = \Phi_r^{(n)}$, and $h_r = \sum_{|\mathbf{j}|=n+1} \beta(r,\mathbf{j})C_{\mathbf{j}}(x,y)$. But by its definition, $f^{(n)}$ is the logarithm of $\Phi^{(n)}$. It therefore follows that working modulo degree $n+2$,

$$f_i^{(n)}(F^{(n+1)}(x,y)) \equiv f_i^{(n)}(x) + f_i^{(n)}(y) + \sum_{|\mathbf{j}|=n+1} \beta(i,\mathbf{j})C_{\mathbf{j}}(x,y). \tag{A.11}$$

Since $F_i^{(n+1)} = x_i + y_i +$higher order terms, it is easy to see that for any multi-index $\mathbf{j}$ with $|\mathbf{j}| = n+1$,

$$\begin{aligned} F_1^{(n+1)}(x,y)^{j_1} \cdots F_N^{(n+1)}(x,y)^{j_N} &\equiv (x_1+y_1)^{j_1} \cdots (x_N+y_N)^{j_N}, \\ &= \nu(\mathbf{j})C_{\mathbf{j}}(x,y) + x^{\mathbf{j}} + y^{\mathbf{j}} \pmod{\text{degree } n+2}. \end{aligned} \tag{A.12}$$

Plugging (A.11) and (A.12) into Equation A.9, we obtain for each $i = 1, \ldots, N$,

$$\begin{aligned} f_i^{(n+1)}(F^{(n+1)}(x,y)) &\equiv f_i^{(n)}(x) + f_i^{(n)}(y) + \sum_{|\mathbf{j}|=n+1} \beta(i,\mathbf{j})C_{\mathbf{j}}(x,y) - \\ &\quad - \sum_{|\mathbf{j}|=n+1} \frac{\beta(i,\mathbf{j})}{\nu(\mathbf{j})}(\nu(\mathbf{j})C_{\mathbf{j}}(x,y) + x^{\mathbf{j}} + y^{\mathbf{j}}) \\ &= f_i^{(n)}(x) - \sum_{|\mathbf{j}|=n+1} \frac{\beta(i,\mathbf{j})}{\nu(\mathbf{j})}x^{\mathbf{j}} + \\ &\quad + f_i^{(n)}(y) - \sum_{|\mathbf{j}|=n+1} \frac{\beta(i,\mathbf{j})}{\nu(\mathbf{j})}y^{\mathbf{j}} \\ &= f_i^{(n+1)}(x) + f_i^{(n+1)}(y) \pmod{\text{degree } n+2}. \end{aligned}$$

This completes the proof of property (iv) and the lemma. □

As in the one-dimensional case, we verify that we have in fact constructed universal objects. The proof is a straight generalization of the proof of the corresponding one-dimensional theorem.

THEOREM A.12. *Let n be a positive integer. Then $F^{(n)}$ (as constructed above) is a universal, N-dimensional n-bud.*

PROOF. We proceed by induction on n. The $n = 1$ case is trivial. Suppose the theorem holds for some n, and let G be an N-dimensional $(n+1)$-bud defined over a ring R.

Treating G as an n-bud, our inductive hypothesis our inductive hypothesis asserts the existence of a unique ring homomorphism $\varphi^{(n)} \colon A^{(n)} \to R$ such that $\varphi_*^{(n)} F^{(n)}(x,y) \equiv G(x,y) \pmod{\text{degree } n+1}$. Extend $\varphi^{(n)}$ to a map $\widetilde{\varphi}^{(n)} \colon A^{(n+1)} \to R$ by setting $\widetilde{\varphi}^{(n)} u(i,\mathbf{j}) = 0$ for all $i = 1, \ldots, N$ and all multi-indices $\mathbf{j}$ with $|\mathbf{j}| = n+1$. It is easy to see that

$$\widetilde{\varphi}_*^{(n)} F^{(n+1)}(x,y) \equiv G(x,y) \pmod{\text{degree } n+1}.$$

Since $\widetilde{\varphi}_*^{(n)} F^{(n+1)}$ and G are both $(n+1)$-buds over R which agree, modulo degree $n+1$, the N-dimensional Lazard Comparison Lemma asserts the existence of elements

$a(i,\mathbf{j}) \in R$, $i = 1,\dots,N$, $|\mathbf{j}| = n+1$, such that

$$G_i(x,y) \equiv \widetilde{\varphi}_*^{(n)} F_i(x,y) + \sum_{|\mathbf{j}|=n+1} a(i,\mathbf{j}) C_{\mathbf{j}}(x,y).$$

Recalling Equation A.6, we have

$$F_i^{(n+1)}(x,y) = F_i^{(n)}(x,y) + H_i'(x,y) + \sum_{|\mathbf{j}|=n+1} u(i,\mathbf{j}) C_{\mathbf{j}}(x,y),$$

where $H_i \in A^{(n)}[x,y]$ is a homogeneous polynomial of degree $n+1$. Thus,

$$\widetilde{\varphi}_*^{(n+1)} F_i^{(n+1)}(x,y) = \widetilde{\varphi}_*^{(n)}(F_i^{(n)}(x,y) + H_i'(x,y)).$$

Let $\varphi^{(n)}$ extend $\varphi^{(n)}$ to a map from $A^{(n+1)}$ to R by setting $\varphi^{(n+1)} u(i,\mathbf{j}) = a(i,\mathbf{j})$ for all $i = 1,\dots,N$ and all multi-indices $\mathbf{j}$ with $|\mathbf{j}| = n+1$. Noting that $\widetilde{\varphi}^{(n)}$ and $\varphi^{(n+1)}$ agree on $A^{(n)}$, we see that

$$\begin{aligned}
\varphi_*^{(n+1)} F^{(n+1)}(x,y) &= \varphi_*^{(n+1)}(F_i^{(n)}(x,y) + H_i'(x,y)) + \sum_{|\mathbf{j}|=n+1} \varphi^{(n+1)} u(i,\mathbf{j}) C_{\mathbf{j}}(x,y) \\
&= \widetilde{\varphi}_*^{(n)} F_i^{n+1}(x,y) + \sum_{|\mathbf{j}|=n+1} a(i,\mathbf{j}) C_{\mathbf{j}}(x,y) \\
&\equiv G_i(x,y) \pmod{\text{degree } n+2}.
\end{aligned}$$

□

We obtain the following the following corollaries just like in the one-dimensional case.

COROLLARY A.13. *Let $F^{(n)}$ be as above and let $F(x,y) = \lim_{n\to\infty} F^{(n)}(x,y)$. The F is a universal, N-dimensional formal group law defined over the ring A.*

COROLLARY A.14. *Let G be an N-dimensional n-bud defined over a ring R. Then G can be extended to an N-dimensional $(n+1)$-bud, and in fact to an N-dimensional formal group law defined over R.*

COROLLARY A.15. *Let F be an N-dimensional formal group law defined over a ring R of characteristic zero. Then F admits a logarithm defined over the ring $R \otimes \mathbb{Q}$.*

Bibliography

[1] Adams, J.F., *Stable Homotopy and Generalised Homology*, Chicago Lectures in Mathematics, The University of Chicago Press, Chicago, 1974.

[2] Atiyah, M.F., *Bordism and cobordism*, Proc. Cambridge Phil. Soc. 57, 1961, pp. 200-208.

[3] Baker, A., *A supersingular congruence for modular forms*, Acta Arith. 86, 1998, pp. 91-100.

[4] Baker, A., *Isogenies of supersingular elliptic curves over finite fields and operations in elliptic cohomology*, Glasgow University Mathematics Department preprint 98/39.

[5] Borisov, L.A., Gunnells, P.E., *Toric varieties and modular forms*, Invent. Math. 144, 2001, pp. 297-325.

[6] Borisov, L.A., Gunnells, P.E., *Toric modular forms and nonvanishing of L-functions*, J. Reine Angew Math. 539, 2001, pp. 149-165.

[7] Borisov, L.A., Libgober, A., *Elliptic genera of toric varieties and applications to mirror symmetry*, Invent. Math. 140, 2001, pp. 453-485.

[8] Bump, D., *Automorphic Forms and Representations*, Cambridge Studies in Advanced Mathematics 55, Cambridge University Press, 1998.

[9] Dijkgraff, R., Moore, D., Verlinde E., Verlinde, H., *Elliptic genera of symmetric products and second quantized strings*, Comm. Math. Phys. 185, 1997, pp. 197-209.

[10] Eilenberg, S., Steenrod, N., *Foundations of Algebraic Topology*, Princeton University Press, Princeton, N.J., 1952.

[11] Franke, Jens, *On the construction of elliptic cohomology*, Math. Nachr. 158, 1992, pp. 43-65.

[12] Frölich, A., *Formal Groups*, Lecture Notes in Mathematics 74, Springer Verlag, Berlin, 1968.

[13] Griffiths, P., Harris, J., *Principles of Algebraic Geometry*, John Wiley and Sons, New York, 1978.

[14] Hartshorne, R., *Algebraic geometry*, Graduate texts in mathematics 52, Springer-Verlag, New York, 1977.

[15] Hazewinkel, M., *Formal Groups and Applications*, Pure and Applied Mathematics Vol. 78, Academic Press, New York, 1978.

[16] Hirzebruch, F., Berger, T., Rainer, J., *Manifolds and Modular Forms*, Aspects of Mathematics Vol. E20, Max Planck Institute, Bonn, 1992.

[17] Husemoller, D., *Fibre Bundles*, Graduate Texts in Mathematics 78, Springer-Verlag, New York, 1975.

[18] Landweber, P.S., *Homological properties of comodules over MU_*MU and BP_*BP*, American Journal of Mathematics 98, 1976, pp. 591-610.

[19] Landweber, P.S., Ravenel, D.C., Stong, R.E., *Periodic cohomology theories defined by elliptic curves*, Contemporary Mathematics 181, 1995, pp. 317-337.

[20] Landweber, P.S., *Elliptic Curves and Modular Forms in Algebraic Topology: Proceedings, Princeton 1986*, Lecture Notes in Mathematics 1326, Springer-Verlag, Berlin, 1986.

[21] Landweber, P.S., *Supersingular elliptic curves and congruences for Legendre polynomials*, In [**20**], pp.69-93.

[22] Lazard, M., *Sur les groups Lie formels a un paramètre*, Bull. Soc. Math. France 83, 1955, pp. 251-274.

[23] Lazard, M., *Commutative Formal Groups*, Lecture Notes in Mathematics 443, Springer-Verlag, New York, 1975.

[24] Milnor, J.M., *On the cobordism ring Ω^* and a complex analogue, Part I*, American Journal of Mathematics 82, 1960, pp. 505-521.

[25] Milnor, J.W., Stasheff, J.D., *Characteristic Classes*, Annals of Mathematical Studies, No. 76, Princeton University Press, Princeton, N.J., Tokyo, 1974.

[26] Munkres, J.R., *Elements of Algebraic Topology*, Perseus books, Cambridge, Massachusetts, 1984.

[27] Newlander, A., Nirenberg, L., *Complex analytic coordinates in almost complex manifolds*, Annals of Mathematics 65, 1957, pp. 391-404.

[28] Novikov, S.P., *Methods of algebraic topology from the viewpoint of cobordism theories* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 31, 1967, pp. 855-951; translation, Math. USSR – Izv., 1967, pp. 827-913.

[29] Ochanine, S., *Sur les genres multiplicatifs definis par des integrales elliptiques*, Topology 26, 1987, pp. 143-151.

[30] Pontryagin, L.S., *Characteristic cycles of differentiable manifolds*, Mat. Sbornik 21, 1947, pp. 233-284.

[31] Prasolov, V., Solovyev, Y., *Elliptic Functions and Elliptic Integrals*, Translations of Mathematical Monographs Vol. 170, American Mathematical Society, Providence, 1991.

[32] Quillen, D., *On the formal group laws of unoriented and complex cobordism theory*, Bull. Amer. Math. Soc. 75, 1969, pp. 1293-1298.

[33] Quillen, D., *Elementary proofs of some results of cobordism theory using Steenrod operations*, Advances in Mathematics 7, 1971, pp. 29-56.

[34] Ravenel, D.C., *Complex Cobordism and Stable Homotopy Groups of Spheres*, Academic Press, Inc., Orlando, 1986.

[35] Serre, J.-P., *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, Berlin, 1973.

[36] Siegel, C.L., *Topics in Complex Function Theory I: Elliptic Functions and Uniformization Theory*, Wiley-Interscience, New York, 1969.

[37] Silverman, J. H., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, New York, 1986.

[38] Stong, R.E., *Notes on cobordism theory*, Princeton University Press, Princeton, NJ, 1968.

[39] Thom, R, *Quelques propriétés des variétés différentiables*, Comm. Math. Helv 28, 1954, pp. 17-86.

[40] Thomas, C.B., *Elliptic Cohomology*, Kluwer Academic, New York, 1999.

[41] Wall, C.T.C., *Determination of the cobordism ring*, Annals of Mathematics 72, 1960, pp. 292-311.

[42] Whitehead, G.W., *Generalized homology theories*, Trans. Amer. Math. Soc. 102, 1962, pp. 227-283.

[43] Witten, E., *The index of the Dirac operator in loop space*, In [**20**], pp.161-181.

[44] Witten, E., *Elliptic genera and quantum field theory*, Comm. Math. Phys. 109, 1987, pp. 525-536.

[45] Zagier, D., *Note on the Landweber-Stong elliptic genus*, In [**20**], pp.216-224.