# COMPUTATION OF THE CLASSIFYING RING OF FORMAL MODULES

A. SALCH

Abstract. In this paper, we develop general machinery for computing the classifying ring $L^A$ of one-dimensional formal $A$-modules, for various commutative rings $A$. We then apply the machinery to obtain calculations of $L^A$ for various number rings and cyclic group rings $A$. This includes the first full calculations of the ring $L^A$ in cases in which it fails to be a polynomial algebra. We also derive consequences for the solvability of some lifting and extension problems.

Contents



## 1. Introduction and review of some known facts

1.1. **Introduction.** This paper is about the computation of the classifying rings $L^A$ of formal $A$-modules. We offer some relevant definitions: when $A$ is a commutative ring, a *formal $A$-module* is a formal group law $F$ over a commutative $A$-algebra $R$, which is additionally equipped with a ring map $\rho : A \to \mathrm{End}(F)$ such that $\rho(a)(X) \equiv aX$ modulo $X^2$. Higher-dimensional formal modules exist and arise naturally from abelian varieties of dimension $> 1$, but in this paper we restrict our attention to the moduli of formal modules of dimension 1. From now on, all formal groups and formal modules are implicitly assumed to be one-dimensional.

Formal modules arise in number theory and arithmetic geometry, for example, in Lubin and Tate's famous $p$-adic version [11] of the Kronecker-Weber theorem; in Drinfeld's elliptic modules [4]; in Drinfeld's $p$-adic symmetric domains [5], which are deformation spaces of certain formal modules; and as the formal parts of Barsotti-Tate modules, as in [15]. Formal $A$-modules also arise in algebraic topology, by using the natural map from the moduli stack of formal $A$-modules to the moduli

stack of formal groups to detect certain classes in the cohomology of the latter, particularly in order to resolve certain differentials in spectral sequences used to compute the Adams-Novikov $E_2$-term and stable homotopy groups of spheres; for example, see [16], [12], [19], and [20].

A straightforward algebraic argument (see [4]) shows that there exists a classifying ring $L^A$ for formal $A$-modules, i.e., a commutative $A$-algebra $L^A$ such that $\hom_{A-alg}(L^A, R)$ is in natural bijection with the set of formal $A$-modules over $R$. It remains an open problem to explicitly compute $L^A$ for a general commutative ring $A$. The ring $L^A$ has been computed for only a few classes of rings $A$, described in the next paragraph. In each case, *the ring $L^A$ has turned out to be a polynomial $A$-algebra*. One reason this matters is that certain qualitative features of formal $A$-modules follow as a consequence of the calculation of $L^A$. As an example, in [4] Drinfeld obtained the following results, under the assumption that $A$ is the ring of integers in a nonarchimedean local field:

**Extension:** Every formal $A$-module $n$-bud extends to a formal $A$-module. (A *formal module $n$-bud* is what one gets by reducing the entire definition of a formal module modulo $(X,Y)^{n+1}$, so that $F(X,Y)$ is a power series in $R[[X,Y]]/(X,Y)^{n+1}$, and it is only required to satisfy the axioms for a formal module modulo $(X,Y)^{n+1}$.)

**Lifting:** If $R$ is a commutative $A$-algebra and $I$ is an ideal of $R$, then every formal $A$-module over $R/I$ is the modulo-$I$ reduction of a formal $A$-module over $R$.

These two qualitative features of formal $A$-modules follow immediately from $L^A$ being a polynomial $A$-algebra, and that is *how these properties are proven*: one calculates $L^A$, and the extension and lifting properties follow as a consequence.

Consequently it is of some value to have calculations of the ring $L^A$ for various rings $A$, particularly Dedekind domains, since formal $A$-modules of interest in number theory often have $A$ the ring of integers in a (local or global) number field. There are three cases of rings $A$ for which $L^A$ is already calculated:

(1) In [10], M. Lazard proved that

$$L^A \cong A[x_1, x_2, \dots], \tag{1.1}$$

a polynomial algebra on countably infinitely many generators, when $A = \mathbb{Z}$. As a consequence, the ring $L^{\mathbb{Z}}$ is often called the Lazard ring.

(2) In [4], V. Drinfeld proved that there is also an isomorphism of the form (1.1) when $A$ is the ring of integers in a local nonarchimedean field (e.g. the ring of integers in a finite extension of $\mathbb{Q}_p$).

(3) Finally, M. Hazewinkel proved in [9] that there is an isomorphism of the form (1.1) when $A$ is a discrete valuation ring or a global number ring of class number one.

One cannot expect an isomorphism of the form (1.1) for an arbitrary (global) number ring $A$. As far as the author knows, this was first observed by Hazewinkel, who showed that, in the case when $A$ is the ring of integers in the field $\mathbb{Q}(\sqrt[4]{-18})$, the sub-$A$-module of $L^A$ consisting of elements of degree 2 is not a free $A$-module, and consequently $L^A$ cannot be a polynomial $A$-algebra. This observation appears in 21.3.3A of [9], but no attempt is made there to compute the ring $L^A$.

In the present paper we compute the ring $L^A$ for certain classes of commutative ring $A$. These are apparently the first known full computations of $L^A$ in which $L^A$ fails to be polynomial. Specifically, the computations we make are as follows:

- In Theorem 2.3.3, we prove the following: let $A$ be a torsion-free commutative ring, and let $S$ be a set of prime numbers such that the ring $A[S^{-1}]$ is hereditary. (If, for example, $A$ is already hereditary, then we can let $S$ be the empty set.)

  Then the commutative graded ring $L^A$ is, after inverting $S$, isomorphic to a tensor product of (graded) Rees algebras[1], and also isomorphic to a tensor product of graded symmetric algebras:

$$\begin{aligned} L^A[S^{-1}] &\cong \big(\mathrm{Rees}_A^2(I_2^A) \otimes_A \mathrm{Rees}_A^4(I_3^A) \otimes_A \mathrm{Rees}_A^6(I_4^A) \\ &\qquad \otimes_A \mathrm{Rees}_A^8(I_5^A) \otimes_A \mathrm{Rees}_A^{10}(I_6^A) \otimes_A \dots\big)\,[S^{-1}] \\ &\cong \big(\mathrm{Sym}_A^2(I_2^A) \otimes_A \mathrm{Sym}_A^4(I_3^A) \otimes_A \mathrm{Sym}_A^6(I_4^A) \\ &\qquad \otimes_A \mathrm{Sym}_A^8(I_5^A) \otimes_A \mathrm{Sym}_A^{10}(I_6^A) \otimes_A \dots\big)\,[S^{-1}] \end{aligned}$$

  where $I_n^A$ is the ideal in $A$ generated by $\nu(n)$ and by all elements of the form $a^n - a$, and where $\nu(n)$ is defined to be $p$ if $n$ is a power of a prime number $p$, and $\nu(n) = 1$ if $n$ is not a prime power.

  In particular, the ring $L^A[S^{-1}]$ is a polynomial $A$-algebra if and only if each of the ideals $I_n^A$ is nonprincipal in $A[S^{-1}]$.
- In Theorem 3.1.1, we prove the following: let $A$ be the ring of integers in a finite extension $K/\mathbb{Q}$, let $1, \alpha_1, \dots, \alpha_j$ be a $\mathbb{Z}$-linear basis for $A$, and let $J_n^A$ be the ideal $(\nu(n), \alpha_1^n - \alpha_1, \alpha_2^n - \alpha_2, \dots, \alpha_j^n - \alpha_j)$ of $A$. Let $P$ denote the set of integers $> 1$ which are prime powers, and let $R$ denote the set of integers $> 1$ which are not prime powers. Then we have isomorphisms of commutative graded $A$-algebras:

$$\begin{aligned} L^A &\cong \left(\bigotimes_A^{n\in P} \mathrm{Rees}_A^{2n-2}(J_n^A)\right) \otimes_A A[x_{n-1} : n \in R] \\ &\cong \left(\bigotimes_A^{n\in P} \mathrm{Sym}_A^{2n-2}(J_n^A)\right) \otimes_A A[x_{n-1} : n \in R], \end{aligned}$$

  with $x_{n-1}$ in degree $2(n-1)$. To be clear, the notation $A[x_{n-1} : n \in R]$ denotes the polynomial $A$-algebra on the set of indeterminates $\{x_{n-1} : n \in R\}$.
- For quadratic number rings, we prove Theorem 3.1.5: let $K$ be a quadratic extension of the rational numbers, and let $A = \mathbb{Z}[\alpha]$ be the ring of integers of $K$. Let $\Delta$ denote the discriminant of $K/\mathbb{Q}$. For each prime number $p$ which divides $\Delta$, let $\mathfrak{m}_p$ be the unique maximal ideal of $A$ over $p$. Let $R$ be the set of prime numbers $p$ which divide $\Delta$ and which have the property that $J_{p^m}^A = (p, \alpha^{p^m} - \alpha)$ is nonprincipal for some positive integer $m$. Let $S$

[1]The *Rees algebra* of an ideal $I$ in a commutative ring $A$, written $\mathrm{Rees}_A(I)$, is the commutative $A$-algebra $\coprod_{n\geq 0} I^n\{t^n\} \subseteq A[t]$. The notation $\mathrm{Rees}_A^n(I)$ denotes $\mathrm{Rees}_A(I)$ as a graded $A$-algebra, graded so that $I^m$ is in degree $mn$.

Similarly, here and throughout this paper, $\mathrm{Sym}_A^n(I)$ does *not* denote the $n$th symmetric power of $I$. Rather, it denotes the symmetric $A$-algebra of $A$, equipped with the grading in which the $m$th symmetric power of $I$ is concentrated in degree $mn$. See Definition 2.1.5.

be the set of integers $> 1$ which are not powers of primes contained in $R$. Then we have an isomorphism of commutative graded $A$-algebras:

$$L^A \cong A[x_{n-1} : n \in S] \otimes_A \bigotimes_A^{p \in R} \left( \mathrm{Rees}_A^{2p-2}(J_p^A) \otimes_A \mathrm{Rees}_A^{2p^2-2}(J_{p^2}^A) \otimes_A \mathrm{Rees}_A^{2p^3-2}(J_{p^3}^A) \otimes_A \dots \right)$$

with each polynomial generator $x_{n-1}$ in degree $2(n-1)$.

Consequently, we have an isomorphism of commutative graded $A[R^{-1}]$-algebras $L^A[R^{-1}] \cong A[R^{-1}][x_1, x_2, \dots]$, with each $x_i$ in degree $2i$.

- As an example computation, in Theorem 3.1.10 we fully work out the ring $L^A$ in the case where $A$ is the ring of integers in the number field $\mathbb{Q}(\sqrt[4]{-18})$. This was Hazewinkel's original example of a number ring $A$ in which $L^A$ could not possibly be a polynomial ring (but Hazewinkel's computation stopped at grading degree 2). The full result is: let $S$ denote the set of all integers $> 1$ which are not powers of 2 or of 3. Then we have an isomorphism of commutative graded $A$-algebras

$$\begin{aligned} L^A \cong A[x_{n-1} : n \in S] &\otimes_A A[x_1, y_1]/(2x_1 - (\alpha^2 - \alpha)y_1) \\ &\otimes_A \bigotimes_A^{m \geq 2} (A[x_{2^m-1}, y_{2^m-1}]/(2x_{2^m-1} - \alpha y_{2^m-1})) \\ &\otimes_A \bigotimes_A^{m \geq 1} (A[x_{3^m-1}, y_{3^m-1}]/(3x_{3^m-1} - \alpha y_{3^m-1})), \end{aligned}$$

  where $\alpha = \sqrt[4]{-18} \in A$, and where the polynomial generators $x_i$ and $y_i$ are each in degree $2i$.

  Consequently the ring $L^A$ is not isomorphic to a polynomial algebra, but we have an isomorphism of commutative graded $A[\frac{1}{6}]$-algebras $L^A\left[\frac{1}{6}\right] \cong A\left[\frac{1}{6}\right][x_1, x_2, \dots]$, with each $x_i$ in degree $2i$.
- Let $C_m$ be the cyclic group of order $m$, let $P$ be the set of integers $> 1$ which are prime powers relatively prime to $m$, and let $S$ be the set of integers $> 1$ not contained in $P$. Write $R$ for the group $\mathbb{Z}\left[\frac{1}{m}\right]$-algebra $\mathbb{Z}\left[\frac{1}{m}\right][C_m]$ of $C_m$. Theorem 3.2.1 establishes an isomorphism of graded rings

$$\begin{aligned} L^{\mathbb{Z}[C_m]}\left[\frac{1}{m}\right] \cong \bigotimes_R^{n \in P} &(R[x_{n-1}, y_{n-1}]/(\nu(n)x_{n-1} - (1-\sigma)y_{n-1})) \\ &\otimes_R R[x_{n-1} : n \in S], \end{aligned}$$

  where $\sigma$ denotes a generator of $C_m$, and where the polynomial generators $x_{n-1}$ and $y_{n-1}$ are each in degree $2(n-1)$.
- In each of the above cases, $L^A$ is a tensor product of Rees rings, so even when $L^A$ fails to be a polynomial algebra, $L^A$ *is still a subalgebra of a polynomial algebra.* Furthermore, in each of the above cases, $L^A$ is also a symmetric algebra on a projective module. As a consequence, we get Corollary 2.3.4, a generalization of Drinfeld's lifting and extension theorems: for all of the hereditary rings $A$ described above, every formal $A$-module $n$-bud over a commutative $A$-algebra extends to a formal $A$-module. Furthermore, if $R$ is a commutative $A$-algebra and $I$ is an ideal of $R$, then every formal

$A$-module over $R/I$ is the modulo-$I$ reduction of a formal $A$-module over $R$.

It is well-known that the classifying ring $L^A B$ for formal $A$-modules is always a polynomial algebra over $L^A$, and the Hopf algebroid $(L^A, L^A B)$ is isomorphic to $(L^A, L^A[b_1, b_2, \dots])$. The stack associated to the groupoid scheme $(\operatorname{Spec} L^A, \operatorname{Spec} L^A B)$ is the moduli stack of formal $A$-modules, so the reader who is so inclined can regard the computations in this paper as computations of presentations for this moduli stack.

Producing these computations of $L^A$ for various rings $A$ requires some preliminary work. In section 2 we define a certain homology theory on rings, "$U$-homology." Proposition 2.1.4 shows that, in homological degrees 0 and 1, $U$-homology is the obstruction to $L^A$ being a polynomial algebra. These and other general properties of $U$-homology are worked out in section 2.1.

In section 2.2 we use a theorem of Pirashvili, and a comparison to Hochschild homology with twisted coefficients, to show that $U$-homology is, in fact, *acyclic*: it vanishes in all positive degrees!

In section 2.3, we derive the various consequences of these results on $U$-homology. Most importantly, Corollary 2.3.2 establishes that, for a torsion-free ring $A$ such that the ideal $I_n^A = (\nu(n), a^n - a \ \forall a \in A) \subseteq A$ is a projective $A$-module for all integers $n > 1$, $L^A$ is a tensor product of suspended Rees algebras. We then prove Theorem 2.3.3, which similarly identifies $L^A[S^{-1}]$ for any torsion-free commutative ring $A$ and any multiplicatively-closed subset $S \subseteq A$ such that $A[S^{-1}]$ is hereditary. All of the above calculations of $L^A$ are enabled by Theorem 2.3.3.

The author is grateful to D. Ravenel for teaching him a great deal about formal modules and homotopy theory when the author was a graduate student. The author also found the SAGE and MAGMA computer algebra systems, [21] and [1], quite helpful while preparing the number-theoretic results in section 3.1. Finally, the author is grateful to the editor and referee for their tremendous patience with an author who has taken a remarkably long time to make revisions.

**Conventions 1.1.1.** Here are a few conventions which are in force throughout this paper.

- Given a ring $A$, we write $A\{x\}$ for the free $A$-module on a generator $x$.
- All graded rings considered in this paper are $\mathbb{N}$-graded, and concentrated in even degrees. Consequently there is no question about whether the Koszul sign convention is in effect: all our commutative graded rings are genuinely commutative, i.e., commutative as ungraded rings.
- For every commutative ring $A$, we equip the classifying ring $L^A$ of formal $A$-modules with the grading in which the homogeneous elements of degree $2d-2$ are those elements which parameterize the total degree $d$ terms in a formal $A$-module, regarded as a power series $F(X,Y) \in A[[X,Y]]$. This grading is chosen for compatibility with the appearance of formal groups in algebraic topology. Specifically, with our chosen grading, Quillen's isomorphism [14] of $L^{\mathbb{Z}}$ with the coefficient ring $MU_*$ of complex bordism is an isomorphism of graded rings.
- Occasionally (e.g. in Theorem 3.1.5 and in Theorem 3.1.10) we refer to a tensor product of *infinitely many* commutative algebras. In every case, these are tensor products of commutative *graded* algebras, trivial in negative degrees, and in which only finitely many tensor factors have nonzero

homogeneous elements in any given degree. The upshot is that there are no special subtleties or surprises in these infinitary tensor products: these infinitary tensor products behave just as ordinary finite tensor products behave.

- If $n$ is a positive integer, we let $\nu(n)$ stand for the integer 1 if $n$ is not a prime power, and we let $\nu(n) = p$ if $n$ is a power of the prime number $p$.

1.2. **Review of some known facts.** Proposition 1.2.1 appears as Proposition 1.1 in [4].

**Proposition 1.2.1. (Drinfeld.)** *Let $A$ be a commutative ring, and let $n$ be an integer. Let $\nu(n)$ be defined as in Convention 1.1.1. Let $D^A$ denote the homogeneous ideal in $L^A$ generated by all products of elements $xy$ with $x, y \in L^A$ each homogeneous of positive degree. Let $\overline{L}^A$ denote the quotient ring $L^A/D^A$. The ring $\overline{L}^A$ is graded, so we may consider its degree $n$ summand $\overline{L}^A_n$ for various integers $n$. If $n \geq 2$, then $\overline{L}^A_{2n-2}$ is isomorphic to the $A$-module generated by symbols $d$ and $\{c_a : a \in A\}$, that is, one generator $c_a$ for each element $a$ of $A$ along with one additional generator $d$, modulo the relations:*

$$d(a^n - a) = \nu(n)c_a \quad \text{for all } a \in A \tag{1.2}$$

$$c_{a+b} - c_a - c_b = d\frac{(a+b)^n - a^n - b^n}{\nu(n)} \quad \text{for all } a, b \in A \tag{1.3}$$

$$ac_b + b^n c_a = c_{ab} \quad \text{for all } a, b \in A. \tag{1.4}$$

We will refer to the presentation described in Proposition 1.2.1 as *Drinfeld's presentation for $\overline{L}^A_{2n-2}$*.

Our gradings are twice those found in [4], for the reason explained in Conventions 1.1.1.

One fairly easy application of Proposition 1.2.1 is Proposition 1.2.2, which is proven in [4].

**Proposition 1.2.2.** *Let $A$ be a commutative $\mathbb{Q}$-algebra. Then the classifying ring $L^A$ of formal $A$-modules is isomorphic, as a graded $A$-algebra, to $A[x_1, x_2, \dots]$. The polynomial generator $x_n$ is in degree $2n$, and it corresponds to the generator $d$ of $A \cong \overline{L}^A_{2n}$ in the Drinfeld presentation for $\overline{L}^A_{2n}$.*

Theorem 1.2.3 appears in Hazewinkel's excellent book [9] (see the proof of Theorem 21.3.5 there). A more fully explained proof also appears in the preprint [17].

**Theorem 1.2.3.** *Let $A$ be a commutative ring and let $S$ be a multiplicatively closed subset of $A$. Then the homomorphism of graded rings $L^A[S^{-1}] \to L^{A[S^{-1}]}$ is an isomorphism.*

Definition-Proposition 1.2.4 first appeared, with proof, in a version of the preprint [17]. For the sake of the self-containedness of the present paper, we have elected to remove the proof of Definition-Proposition 1.2.4 from [17], and to include it in the present paper instead.

**Definition-Proposition 1.2.4.** *Let $n$ be a positive integer, let $\nu(n)$ be as defined in Conventions 1.1.1, and let $A$ be a commutative ring which is $\nu(n)$-torsion-free. Recall from Proposition 1.2.1 that $\overline{L}^A_{2n-2}$ is generated, as an $A$-module, by elements $d$ and $\{c_a\}_{a \in A}$, subject to the relations* (1.2), (1.3), *and* (1.4).

*Let $M_{2n-2}^A$ denote the $A$-module generated by elements $d$ and $\{c_a\}_{a\in A}$, subject only to the relations* (1.2)*. Let $q_{2n-2} : M_{2n-2}^A \to \overline{L}_{2n-2}^A$ denote the $A$-module quotient map which enforces the additional relations* (1.3) *and* (1.4)*.*

*By the* degree $2n-2$ fundamental functional of $A$*, we mean the $A$-module homomorphism*

$$\sigma_{2n-2} : \overline{L}_{2n-2}^A \to A$$

*given by*

$$\sigma_{2n-2}(d) = \nu(n),$$
$$\sigma_{2n-2}(c_a) = a^n - a.$$

*If $n > 1$, then the kernel of the composite map $\sigma_{2n-2} \circ q_{2n-2} : M_{2n-2}^A \to A$ is exactly the set of $\nu(n)$-torsion elements of $M_{2n-2}^A$. Furthermore, the kernel of $\sigma_{2n-2}$ and the kernel of $q_{2n-2}$ are each annihilated by multiplication by $\nu(n)$. Furthermore, if $n$ is not a prime power, then $\sigma_{2n-2}$ and $q_{2n-2}$ are each isomorphisms of $A$-modules.*

*Proof.* By the definition of $M_{2n-2}^A$, the top row in the commutative diagram of $A$-modules

$$\begin{array}{ccccccc} \coprod_{a\in A} A\{r_a\} & \xrightarrow{\delta_0} & A\{d\} \oplus \coprod_{a\in A} A\{c_a\} & \xrightarrow{\delta_{-1}} & M_{2n-2}^A & \longrightarrow & 0 \\ & & & \searrow^{\tilde{\sigma}_{2n-2}} & \downarrow{\scriptstyle \sigma_{2n-2}\circ q_{2n-2}} & & \\ & & & & A & & \end{array}$$

is exact, where $\tilde{\sigma}_{2n-2}$ is the map given by $\tilde{\sigma}_{2n-2}(d) = \nu(n)$ and $\tilde{\sigma}_{2n-2}(c_a) = a^n - a$, where $\delta_0$ is the map given by $\delta_0(r_a) = (a^n - a)d - \nu(n)c_a$, and where $\delta_{-1}$ sends $d$ to $d$ and sends $c_a$ to $c_a$. Suppose that $x = \beta d + \sum_{a\in A} \alpha_a c_a$ is in the kernel of $\tilde{\sigma}_{2n-2}$, where $\beta \in A$ and $\alpha_a \in A$ for all $a \in A$. Then:

$$\begin{aligned} 0 &= \tilde{\sigma}_{2n-2}(x) \\ &= \beta\nu(n) + \sum_{a\in A} \alpha_a(a^n - a), \end{aligned}$$

so $\beta\nu(n) = -\sum_{a\in A} \alpha_a(a^n - a)$. Continuing, we have

$$\begin{aligned} \delta_0\left(\sum_{a\in A} -\alpha_a r_a\right) &= \left(\sum_{a\in A} -\alpha_a(a^n - a)\right) d + \sum_{a\in A} \alpha_a \nu(n) c_a \\ &= \beta\nu(n)d + \sum_{a\in A} \alpha_a \nu(n) c_a \\ &= \nu(n)x, \end{aligned}$$

so $\nu(n)x \in \text{im } \delta_0$. Hence every element in the kernel of $\sigma_{2n-2} \circ q_{2n-2}$ is killed by $\nu(n)$.

Conversely, since the codomain of $\sigma_{2n-2} \circ q_{2n-2}$ is $A$, and since $A$ is $\nu(n)$-torsion-free, every element in $M_{2n-2}^A$ killed by $\nu(n)$ is also in the kernel of $\sigma_{2n-2} \circ q_{2n-2}$.

By its construction, $q_{2n-2}$ is a surjection, and so we have a short exact sequence

$$0 \to \ker q_{2n-2} \to \ker \sigma_{2n-2} \circ q_{2n-2} \to \ker \sigma_{2n-2} \to 0.$$

We have just shown that every element in $\ker \sigma_{2n-2} \circ q_{2n-2}$ is killed by multiplication by $\nu(n)$. Since $\ker \sigma_{2n-2}$ and $\ker q_{2n-2}$ are subquotients of $\ker \sigma_{2n-2} \circ q_{2n-2}$, they too are killed by multiplication by $\nu(n)$, as claimed.

Now suppose that $n$ is not a prime power. We have just shown that the kernel of $\sigma_{2n-2}$ is killed by multiplication by $\nu(n)$, so if $n$ is not a prime power then $\sigma_{2n-2}$ is injective. Furthermore, $\nu(n) = 1$ implies that $\sigma_{2n-2}(d) = 1 \in A$, so $\sigma_{2n-2}$ is surjective. Hence $\sigma_{2n-2}$ is an isomorphism. One also checks easily that, when $\nu(n) = 1$, the relations (1.3) and (1.4) can be derived from the relation (1.2), so $q_{2n-2}$ is also an isomorphism. □

Below, in Theorem 2.3.1, we will show that the fundamental functional is injective whenever $A$ is $\nu(n)$-torsion-free. It is the injectivity of the fundamental functional which makes the computation of $L^A$ possible using the methods of this paper. The entire apparatus of $U$-homology, which is defined and developed starting in the next section, is not much more than a tool for showing that the fundamental functional is injective.

## 2. $U$-HOMOLOGY

2.1. **$U$-homology as the obstruction to $L^A$ being a polynomial algebra.** In this subsection we introduce "$U$-homology," an invariant of commutative rings. In Proposition 2.1.4 and in Proposition 2.1.11 we demonstrate the main properties of $U$-homology:

- in dimension 1, it is the obstruction to injectivity of the fundamental functional,
- in dimension 0, it is the obstruction to surjectivity of the fundamental functional,
- and the vanishing of $U_0^A(n)$ and $U_1^A(n)$ for all $n$ is equivalent to $L^A$ being isomorphic to a polynomial algebra by a certain fundamental comparison map.

**Definition 2.1.1.** *When $A$ is a commutative ring and $n > 1$ an integer, let $F_n(A)$ denote the free $A/\nu(n)$-module generated by the underlying abelian group of $A$, i.e., $F_n(A)$ is the $A/\nu(n)$-module with one generator $c_a$ for each element $a \in A$, and subject to the relation $c_0 = 0$ and the relation $c_{a+b} = c_a + c_b$ for each $a, b \in A$.*

To be clear, in Definition 2.1.1 and throughout this paper, $A/\nu(n)$ denotes the quotient of $A$ by the ideal generated by the integer $\nu(n)$.

**Definition-Proposition 2.1.2.** *Suppose $A$ is a commutative ring and $n > 1$ an integer which is a power of a prime number (which is necessarily $\nu(n)$). Given an element $a \in A$, we will write $\overline{a}$ for the reduction of $a$ modulo $\nu(n)$. Let $\mathcal{U}^A(n)_\bullet$ denote the simplicial $A/\nu(n)$-module given as follows:*

- *$\mathcal{U}^A(n)_0 = A/\nu(n)$.*
- *$\mathcal{U}^A(n)_m = F_n(A)^{\otimes_{A/\nu(n)} m}$, i.e., the $m$-fold tensor product, over $A/\nu(n)$, of $F_n(A)$ with itself. This definition holds for $m \geq 0$, and is consistent with the case $m = 0$ given above.*
- *The face map $d_0 : \mathcal{U}^A(n)_1 = F_n(A) \to A/\nu(n) = \mathcal{U}^A(n)_0$ is given by letting $d_0(c_a) = \overline{a}$.*
- *The face map $d_1 : \mathcal{U}^A(n)_1 = F_n(A) \to A/\nu(n) = \mathcal{U}^A(n)_0$ is given by letting $d_1(c_a) = \overline{a}^n$.*

- *If $m \geq 1$, the face map*

  $$d_0 : \mathcal{U}^A(n)_{m+1} = F_n(A)^{\otimes_{A/\nu(n)} m+1} \to F_n(A)^{\otimes_{A/\nu(n)} m} = \mathcal{U}^A(n)_m$$

  *is given by* $d_0(c_{a_1} \otimes \cdots \otimes c_{a_{m+1}}) = \overline{a}_1(c_{a_2} \otimes \cdots \otimes c_{a_{m+1}})$.
- *If $m \geq 1$ and $1 \leq i \leq m$, the face map*

  $$d_i : \mathcal{U}^A(n)_{m+1} = F_n(A)^{\otimes_{A/\nu(n)} m+1} \to F_n(A)^{\otimes_{A/\nu(n)} m} = \mathcal{U}^A(n)_m$$

  *is given by*

  $$d_i(c_{a_1} \otimes \cdots \otimes c_{a_{m+1}}) = c_{a_1} \otimes \cdots \otimes c_{a_{i-1}} \otimes c_{a_i a_{i+1}} \otimes c_{a_{i+2}} \otimes \cdots \otimes c_{a_{m+1}}.$$
- *If $m \geq 1$, the face map*

  $$d_{m+1} : \mathcal{U}^A(n)_{m+1} = F_n(A)^{\otimes_{A/\nu(n)} m+1} \to F_n(A)^{\otimes_{A/\nu(n)} m} = \mathcal{U}^A(n)_m$$

  *is given*[2] *by* $d_{m+1}(c_{a_1} \otimes \cdots \otimes c_{a_{m+1}}) = \overline{a}^n_{m+1}(c_{a_1} \otimes \cdots \otimes c_{a_m})$.
- *The degeneracy map $s_0 : A/\nu(n) = \mathcal{U}^A(n)_0 \to \mathcal{U}^A(n)_1 = F_n(A)$ is given by* $s_0(b) = bc_1$.
- *If $m \geq 1$ and $0 \leq i \leq m$, the degeneracy map*

  $$s_i : \mathcal{U}^A(n)_m = F_n(A)^{\otimes_{A/\nu(n)} m} \to F_n(A)^{\otimes_{A/\nu(n)} m+1} = \mathcal{U}^A(n)_{m+1}$$

  *is given by* $s_i(c_{a_1} \otimes \cdots \otimes c_{a_m}) = c_{a_1} \otimes \cdots \otimes c_{a_i} \otimes c_1 \otimes c_{a_{i+1}} \otimes \cdots \otimes c_{a_m}$.

*Let $U^A(n)_\bullet$ denote the Moore/alternating sum chain complex of $\mathcal{U}^A(n)_\bullet$, i.e., the chain complex whose $i$-chain group is $\mathcal{U}^A(n)_i$ and whose boundary map $\mathcal{U}^A(n)_i \to \mathcal{U}^A(n)_{i-1}$ is $\sum_{j=0}^{i}(-1)^j d_j$. Let $U^A_i(n)$ denote the $i$th homology group $H_i(U^A(n)_\bullet)$ of the chain complex of $A/\nu(n)$-modules $U^A(n)_\bullet$. We will call these homology groups* $U$-homology.

*Proof.* One ought to show that $\mathcal{U}^A(n)_\bullet$ is actually a simplicial $A/\nu(n)$-module, i.e., that the simplicial identities are satisfied. This is routine and left as an exercise for the interested reader, who has at least two reasonable approaches:

- explicitly write out the simplicial identities and verify that they hold, or
- observe that $\mathcal{U}^A(n)_\bullet$ is levelwise isomorphic to the Hochschild bar construction of $A/\nu(n)$ with coefficients in a certain bimodule, whose definition is given below in Definition 2.2.1, and the levelwise isomorphisms commute with the face and degeneracy maps. Since the face and degeneracy maps in the Hochschild bar construction satisfy the simplicial identities, so must the face and degeneracy maps in $\mathcal{U}^A(n)_\bullet$. This argument appears more explicitly below, in the proof of Theorem 2.2.2.

□

For example, in low degrees, the chain complex $U^A(n)_\bullet$ is

$$\cdots \to F_n(A) \otimes_{A/\nu(n)} F_n(A) \xrightarrow{\delta_1} F_n(A) \xrightarrow{\delta_0} A/\nu(n) \to 0 \tag{2.5}$$

[2]The formulas for $d_{m+1}$ and for $d_1$ each involve an $n$th power of $\overline{a}$. Taking an $n$th power is, in general, not a group homomorphism. However, the entire simplicial module we are defining is a simplicial $A/\nu(n)$-module. When $\nu(n)$ is not a prime power, $A/\nu(n)$ is the zero ring. Consequently it is only in the case that $n$ is a prime power that one needs to be sure that the face and degeneracy maps are indeed well-defined module homomorphisms. When $n$ is a prime power, $A/\nu(n)$ is a commutative ring of characteristic $p$, and $n$ is a power of $p$, so the $n$th power map indeed commutes with addition.

with $\delta_0$ and $\delta_1$ defined by:

$$\delta_0(c_a) = a - a^n,$$
$$\delta_1(c_a \otimes c_b) = ac_b - c_{ab} + b^n c_a.$$

In the rest of this paper, we do not need any of the $U$-homology groups except $U_0^A(n)$ and $U_1^A(n)$, so in fact the complex (2.5) suffices for our needs, and the rest of the simplicial module $\mathcal{U}^A(n)_\bullet$ is not really needed for anything that follows in this paper.

**Definition-Proposition 2.1.3.** *Let $n > 1$ be an integer. Let $P^A_{2n-2}$ denote the cokernel of the $A$-module homomorphism $A \to \overline{L}^A_{2n-2}$ sending 1 to $d$ (see Proposition 1.2.1 for the element $d$). Clearly $P^A_{2n-2}$ is functorial in the choice of commutative ring $A$.*

*For any commutative ring $A$, the natural map of $A$-modules*

$$P^A_{2n-2} \to P^{A/\nu(n)}_{2n-2}$$

*is an isomorphism.*

*Proof.* After reducing modulo $d$, the Drinfeld relations (1.2), (1.3), and (1.4) become

$$\begin{aligned} 0 &= \nu(n)c_a, \\ c_{a+b} &= c_a + c_b, \\ c_{ab} &= ac_b + b^n c_a. \end{aligned} \tag{2.6}$$

In particular, filling in 1 for $a$ and $b$ in (2.6) gives us that $c_1 = 0$. Hence $c_{\nu(n)} = \nu(n)c_1 = 0$, and so $c_{\nu(n)a} = \nu(n)c_a + a^n c_{\nu(n)} = 0$. Hence $P^A_{2n-2}$ is isomorphic, as an $A$-module, to the $A/\nu(n)$-module with one generator $c_a$ for each $a \in A/\nu(n)$, subject to the modulo $d$ Drinfeld relations above; this is exactly the modulo $d$ Drinfeld presentation for $\overline{L}^{A/\nu(n)}_{2n-2}$, i.e., a presentation for $P^{A/\nu(n)}_{2n-2}$. □

**Proposition 2.1.4.** *Let $A$ be a commutative ring and let $n > 1$ be an integer. Suppose that $A$ is $\nu(n)$-torsion-free. Then $U_1^A(n) \cong 0$ if and only if the fundamental functional $\sigma_{2n-2} : \overline{L}^A_{2n-2} \to A$ is injective. Furthermore, $U_0^A(n)$ is isomorphic to the cokernel of $\sigma_{2n-2}$.*

*Proof.* We will write $\delta_1, \delta_0$ for the differentials in the chain complex $U^A(n)_\bullet$, defined in Definition-Proposition 2.1.2 and more explicitly in (2.5). Clearly (see the proof of Definition-Proposition 2.1.3) the cokernel of $\delta_1$ is $P^A_{2n-2}$, since $\operatorname{coker}\delta_1$ and $P^A_{2n-2}$ are $A/\nu(n)$-modules with the same set of generators as one another, and the same set of relations as one another. We have a commutative diagram of $A$-modules with exact rows

$$\begin{array}{ccccccccc} & & A & \xrightarrow{d} & \overline{L}^A_{2n-2} & \longrightarrow & P^A_{2n-2} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \sigma_{2n-2}} & & \downarrow{\scriptstyle \tilde{\delta}_0} & & \downarrow \\ 0 & \longrightarrow & A & \xrightarrow{\nu(n)} & A & \longrightarrow & A/\nu(n) & \longrightarrow & 0, \end{array} \tag{2.7}$$

where $\tilde{\delta}_0$ is the $A/\nu(n)$-module map sending each $c_a$ to $a^n - a$. We furthermore have the commutative diagram with exact rows and columns

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \operatorname{im}\delta_1 & \xrightarrow{\mathrm{id}} & \operatorname{im}\delta_1 & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \ker\delta_0 & \longrightarrow & F_n(A) & \xrightarrow{-\delta_0} & A/\nu(n) & & \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\
0 & \longrightarrow & U_1^A(n) & \longrightarrow & P_{n-1}^A & \xrightarrow{\tilde{\delta}_0} & A/\nu(n) & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & 0 & & 0, & & & &
\end{array}$$

so vanishing of $U_1^A(n)$ is equivalent to injectivity of $\tilde{\delta}_0$. The "four lemma" from homological algebra, applied to diagram (2.7), then tells us that injectivity of $\tilde{\delta}_0$ is equivalent to injectivity of $\sigma_{2n-2}$.

For the claim about $U_0^A(n)$: we have the commutative square of $A$-modules with exact columns and rows

$$\begin{array}{ccccccc}
A\{d\} \oplus \coprod_{a\in A} A\{c_a\} & \xrightarrow{-\tilde{\sigma}_{2n-2}} & A & \longrightarrow & \operatorname{coker}\sigma_{2n-2} & \longrightarrow & 0 \\
\downarrow{\scriptstyle \pi'} & & \downarrow{\scriptstyle \pi} & & \downarrow & & \downarrow \\
F_n(A) & \xrightarrow{\delta_0} & A/\nu(n) & \longrightarrow & U_0^A(n) & \longrightarrow & 0
\end{array} \tag{2.8}$$

where $\pi'(d) = 0$, and $\pi'(\alpha c_a) = \overline{\alpha} c_a$ (using the notation of Definition-Proposition 2.1.2), and $\pi$ is the modulo $\nu(n)$ reduction map. The map $\tilde{\sigma}_{2n-2}$ is the composite of the Drinfeld presentation $A\{d\} \oplus \coprod_{a\in A} A\{c_a\} \twoheadrightarrow \overline{L}^A_{2n-2}$ with the fundamental functional $\sigma_{2n-2} : \overline{L}^A_{2n-2} \to A$. Hence the bottom row in diagram (2.8) is the reduction, modulo $\nu(n)$ (and also modulo $d \in A\{d\} \oplus \coprod_{a\in A} A\{c_a\}$), of the top row. In particular, $U_0^A(n)$ is the reduction modulo $\nu(n)$ of $\operatorname{coker}\sigma_{2n-2}$. But $\nu(n)$ is already zero in $\operatorname{coker}\sigma_{2n-2}$ since $\sigma_{2n-2}(d) = \nu(n)$, and consequently $\operatorname{coker}\sigma_{2n-2} \cong U_0^A(n)$. □

This is an opportune time to introduce the symmetric algebras and the Rees algebras. Both are classical constructions. We will need graded versions as well, which are slightly less classical:

**Definition 2.1.5.** *Let $A$ be a commutative ring, $I$ an ideal of $A$.*

- *By the* Rees algebra of $I$, *written* $\operatorname{Rees}_A(I)$, *we mean the commutative $A$-algebra* $\coprod_{n\geq 0} I^n\{t^n\} \subseteq A[t]$.
- *Let $j$ be an integer. By the* $j$-suspended Rees algebra of $I$, *written* $\operatorname{Rees}^j_A(I)$, *we mean the commutative graded $A$-algebra whose underlying commutative $A$-algebra is* $\operatorname{Rees}_A(I)$, *and which is equipped with the grading in which the summand $I^n\{t^n\}$ is in grading degree $jn$.*

*Now, more generally, let $A$ be a commutative ring and let $M$ be an $A$-module.*

- *By the* symmetric algebra of $M$*, written* $\mathrm{Sym}_A(M)$*, we mean the commutative $A$-algebra* $\coprod_{n\geq 0}(M^{\otimes_A n})_{\Sigma_n}$*, where* $(M^{\otimes_A n})_{\Sigma_n}$ *is the module of coinvariants under the action of the symmetric group* $\Sigma_n$ *on* $M^{\otimes_A n}$ *given by permuting the tensor factors.*
- *Let $j$ be an integer. By the* $j$-suspended symmetric algebra of $M$*, written* $\mathrm{Sym}^j_A(M)$*, we mean the commutative graded $A$-algebra whose underlying commutative $A$-algebra is* $\mathrm{Sym}_A(M)$*, and which is equipped with the grading in which the summand* $(M^{\otimes_A n})_{\Sigma_n}$ *is in degree* $jn$*.*

In this paper, $\mathrm{Rees}^j_A(I)$ only occurs in cases where $j$ is even, so $\mathrm{Rees}^j_A(I)$ is both graded-commutative and commutative. That is, as explained in Convention 1.1.1, we do not have to deal with the Koszul sign convention.

**Definition 2.1.6.** *Let $A$ be a commutative ring. we will say that $A$* satisfies the fundamental comparison condition *if the $A$-module $\overline{L}^A_{2n-2}$ is projective for all integers $n > 1$.*

If $A$ satisfies the fundamental comparison condition, then the projection $A$-module map $L^A_{2n-2} \to \overline{L}^A_{2n-2}$ splits for all integers $n > 1$. Choose such a splitting $A$-module map $i_{2n-2} : \overline{L}^A_{2n-2} \to L^A_{2n-2}$ for each integer $n > 1$, and let $i : \coprod_{n>1} \overline{L}^A_{2n-2} \to L^A$ be the $A$-module coproduct of the maps $i_{2n-2}$. Then the adjunction between $\mathrm{Sym}_A$ and the forgetful functor from commutative $A$-algebras to $A$-modules yields a choice of commutative graded $A$-algebra homomorphism $i^\sharp : \mathrm{Sym}_A\left(\coprod_{n>1} \overline{L}^A_{2n-2}\right) \to L^A$.

**Definition 2.1.7.** *Let $A$ be a commutative ring satisfying the fundamental comparison condition. By the* fundamental comparison triangle for $A$ *we mean the diagram of commutative graded $A$-algebra homomorphisms*

(2.9)
$$\begin{array}{ccc} & \mathrm{Sym}_A\left(\coprod_{n>1} \overline{L}^A_{2n-2}\right) & \\ {\scriptstyle i^\sharp}\swarrow & & \searrow{\scriptstyle s} \\ L^A & & \mathrm{Sym}_A\left(\coprod_{n>1} A\right) \xrightarrow{\cong} A[x_1, x_2, \dots] \end{array}$$

*where $s$ is $\mathrm{Sym}_A\left(\coprod_{n>1} \sigma_{2n-2}\right)$, the symmetric algebra functor applied to the coproduct (in the category of graded $A$-modules) of the fundamental functionals $\sigma_{2n-2}$ for all $n$.*

Note that we need $A$ to satisfy the fundamental comparison condition in order to define the fundamental comparison triangle.

**Definition 2.1.8.** *Let $A$ be a commutative ring satisfying the fundamental comparison condition. Choose a splitting $A$-module map for $L^A_{2n-2} \to \overline{L}^A_{2n-2}$ for each integer $n > 1$. We will say that $L^A$* is polynomial by the fundamental comparison (with respect to the given family of splitting maps) *if each $A$-algebra homomorphism in the fundamental comparison triangle is an isomorphism.*

**Remark 2.1.9.** The fundamental comparison triangle is, at least *a priori*, not natural in the choice of $A$, since it involves making choices of the splitting maps

$\{i_{2n-2}\}$, and when one has a homomorphism from one split short exact sequence to another, there is an (often nontrivial) obstruction to the existence of a *compatible* splitting of the two short exact sequences. See [18], for example.

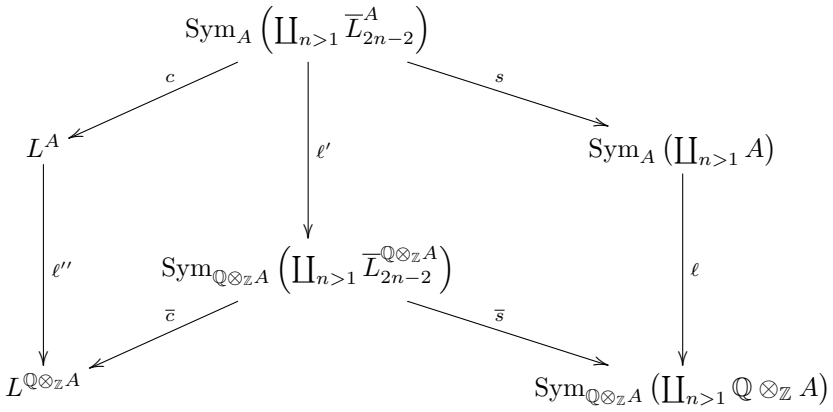
**Remark 2.1.10.** Although $\mathrm{Sym}_A$ preserves epimorphisms, it typically does not preserve monomorphisms; see section 6.2 of chapter III of [2].

**Proposition 2.1.11.** *Suppose that $A$ is a torsion-free commutative ring satisfying the fundamental comparison condition. Then the following are equivalent:*

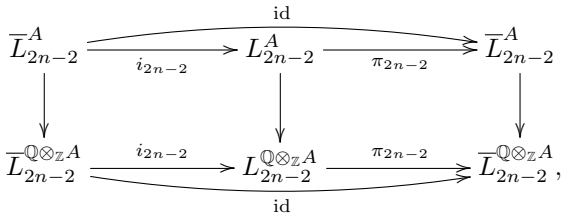
1. *The groups $U_1^A(n)$ and $U_0^A(n)$ are both trivial for all integers $n > 1$.*
2. *$L^A$ is polynomial by the fundamental comparison, with respect to every family of splitting maps.*
3. *$L^A$ is polynomial by the fundamental comparison, with respect to some family of splitting maps.*

*Proof.* From Theorem 1.2.3 we know that the natural commutative graded $\mathbb{Q} \otimes_{\mathbb{Z}} A$-algebra homomorphism $\mathbb{Q} \otimes_{\mathbb{Z}} L^A \to L^{\mathbb{Q}\otimes_{\mathbb{Z}} A}$ is an isomorphism. It is automatic that $\mathbb{Q} \otimes_{\mathbb{Z}} A$ satisfies the fundamental comparison condition, since Proposition 1.2.2 ensures that the $A$-module $\overline{L}^{\mathbb{Q}\otimes_{\mathbb{Z}} A}_{2n-2}$ is free, hence projective. After choosing a family of splitting maps, we can fit the fundamental comparison triangle for $A$ together with the fundamental comparison triangle for $\mathbb{Q} \otimes_{\mathbb{Z}} A$ to get the diagram

(2.10)




In light of Remark 2.1.9, we ought to explain why we have a map of fundamental comparison triangles in this situation. The reason is that, when we choose a splitting $i_{2n-2}$ of the projection $\pi_{2n-2} : L^A_{2n-2} \to \overline{L}^A_{2n-2}$, we can tensor that splitting map over $A$ with $\mathbb{Q} \otimes_{\mathbb{Z}} A$ to get a splitting map $\mathbb{Q} \otimes_{\mathbb{Z}} L^A_{2n-2} \to \mathbb{Q} \otimes_{\mathbb{Z}} \overline{L}^A_{2n-2}$, and hence, using Theorem 1.2.3, a commutative diagram of $A$-modules




which is all we need in order to get the commutativity of the left-hand trapezoid in diagram (2.10).

**1 implies 2:** Suppose that $U_0^A(n) \cong 0 \cong U_1^A(n)$ for all integers $n > 1$. Then $\sigma_{2n-2}$ is an isomorphism for all $n > 1$ by Proposition 2.1.4, hence the homomorphism $s$ in diagram (2.9) is an isomorphism. Since $A$ is torsion-free, the localization map $A \to \mathbb{Q} \otimes_{\mathbb{Z}} A$ is injective, hence the map marked $\ell$ in diagram (2.10) is injective[3]. Consequently $\ell \circ s = \overline{s} \circ \ell'$ is injective, so $\ell'$ is injective as well. The map marked $\overline{c}$ in diagram (2.10) is an isomorphism by Proposition 1.2.2, so $\overline{c} \circ \ell' = \ell'' \circ c$ is injective, hence $c$ is injective. The map $c$ is also surjective since every element in $L^A$ is a sum of products of indecomposables. Hence $c$ is an isomorphism. Hence $c$ and $s$ are both isomorphisms, so $L^A$ is polynomial by the fundamental comparison.

**2 implies 3:** Trivial.

**3 implies 1:** If $L^A$ is polynomial by the fundamental comparison, then the map $s$ in diagram (2.10) is an isomorphism. Since the map of $A$-modules $\coprod_{n>1} \sigma_{2n-2} : \coprod_{n>1} \overline{L}^A_{2n-2} \to \coprod_{n>1} A$ is the summand consisting of rank 1 tensors in the map of $A$-modules $s : \mathrm{Sym}_A\left(\coprod_{n>1} \overline{L}^A_{2n-2}\right) \to \mathrm{Sym}_A\left(\coprod_{n>1} A\right)$, we then have that $\coprod_{n>1} \sigma_{2n-2}$ is an isomorphism of $A$-modules, and hence that each $\sigma_{2n-2}$ is an isomorphism of $A$-modules. Now Proposition 2.1.4 implies that $U_0^A(n) \cong 0 \cong U_1^A(n)$ for all integers $n > 1$.

□

**Definition 2.1.12.** *Let $A$ be a commutative ring, and let $n$ be a positive integer. We write $I_n^A$ for the ideal in $A$ generated by $\nu(n)$ and by all elements of the form $a^n - a \in A$.*

When $n$ is not a prime power, it is easy to see that the ideal $I_n^A$ is the trivial ideal (1). For a prime power $n = p^m$, the ideal $I_{p^m}^A$ has a certain universal property: it is the largest among all ideals in $A$ which are contained in the kernel of every ring homomorphism $A \to \mathbb{F}_{p^m}$. For that reason, the ideal $I_{p^m}^A$ is called *the universal $\mathbb{F}_{p^m}$-point-detecting ideal of $A$* in the preprint [17]. See [17] for further discussion of the relationship between $I_{p^m}^A$, counting $\mathbb{F}_{p^m}$-points, and the zeta-function of Spec $A$.

**Remark 2.1.13.** It is occasionally useful (e.g. in Corollary 3.1.2, below) to have a smaller presentation of the ideal $I_n^A$. Suppose that $A$ is generated as a commutative ring by a single element $t \in A$, i.e., the ring homomorphism $\mathbb{Z}[t] \to A$, sending $t$ to $t$, is surjective. Then $I_n^A = (\nu(n), t^{\nu(n)} - t)$. The proof is elementary, and left to the interested reader.

**Theorem 2.1.14.** *Suppose that $A$ is a torsion-free commutative ring, and suppose that the fundamental functional $\sigma_{2n-2}$ is injective for all $n > 1$. Suppose that, for each $n > 1$, the ideal $I_n^A$ is projective when regarded as an $A$-module. Then the following statements are all true:*

- *$A$ satisfies the fundamental comparison condition.*

[3]This *isn't* due to Sym preserving injections, since in general, Sym does not preserve injections—see Remark 2.1.10. Instead this is simply due to the observation that $\mathrm{Sym}_A(\coprod_{n>1} A)$ is a polynomial algebra over $A$, and $\mathrm{Sym}_{\mathbb{Q}\otimes_{\mathbb{Z}} A}\left(\mathbb{Q} \otimes_{\mathbb{Z}} \coprod_{n>1} A\right)$ is a polynomial algebra over $\mathbb{Q} \otimes_{\mathbb{Z}} A$ on the same set of polynomial generators.

- *Of the fundamental comparison maps*

$$s : \mathrm{Sym}_A\left(\coprod_{n>1} \overline{L}^A_{2n-2}\right) \to \mathrm{Sym}_A\left(\coprod_{n>1} A\right)$$

*and*

$$i^\sharp : \mathrm{Sym}_A\left(\coprod_{n>1} \overline{L}^A_{2n-2}\right) \to L^A,$$

*the map $s$ is injective and $i^\sharp$ is an isomorphism. Consequently $L^A$ is isomorphic to a sub-$A$-algebra of a polynomial $A$-algebra.*

- *$L^A$ is isomorphic, as a graded $A$-algebra, to the tensor product of the suspended symmetric algebras of the ideals $I^A_2, I^A_3, \dots$ of $A$:*

$$\begin{aligned} L^A &\cong \bigotimes_{n>1} \mathrm{Sym}_A^{2n-2)}\left(I^A_n\right) \\ &\cong \mathrm{Sym}^2_A(I^A_2) \otimes_A \mathrm{Sym}^4_A(I^A_3) \otimes_A \mathrm{Sym}^6_A(I^A_4) \otimes_A \dots. \end{aligned} \tag{2.11}$$

- *$L^A$ is isomorphic, as a graded $A$-algebra, to the tensor product of the suspended Rees algebras of the ideals $I^A_2, I^A_3, \dots$ of $A$:*

$$\begin{aligned} L^A &\cong \bigotimes_{n>1} \mathrm{Rees}_A^{2n-2}\left(I^A_n\right) \\ &\cong \mathrm{Rees}^2_A(I^A_2) \otimes_A \mathrm{Rees}^4_A(I^A_3) \otimes_A \mathrm{Rees}^6_A(I^A_4) \otimes_A \dots. \end{aligned} \tag{2.12}$$

*Proof.*

- Since $\sigma_{2n-2}$ is assumed injective for all $n$, the $A$-module $\overline{L}^A_{2n-2}$ is isomorphic to $\mathrm{im}\ \sigma_{2n-2} = I^A_n$, which is projective for all $n > 1$, by assumption. Hence $A$ satisfies the fundamental comparison condition.
- We claim that the inclusion $I^A_n \subseteq A$, regarded as an $A$-module map, induces a monomorphism

$$\mathrm{Sym}_A(I^A_n) \to \mathrm{Sym}_A(A) \tag{2.13}$$

after applying $\mathrm{Sym}_A$. The injectivity of (2.13) uses the assumption that $I^A_n$ is projective, and is not generally true if we relax the projectivity assumption on $I^A_n$; see Remark 2.1.10.

The argument for injectivity of (2.13) is general, classical, and quite simple: since $I^A_n$ is projective, tensoring the $A$-module monomorphism $I^A_n \to A$ with $I^A_n$ yields that the multiplication map $I^A_n \otimes_A I^A_n \to I^A_n$ is monic. A similar argument together with a straightforward induction yields that the multiplication map $(I^A_n)^{\otimes_A j} \to A^{\otimes_A j} \cong A$ is monic for all positive integers $j$. Hence we have a commutative square of $A$-modules

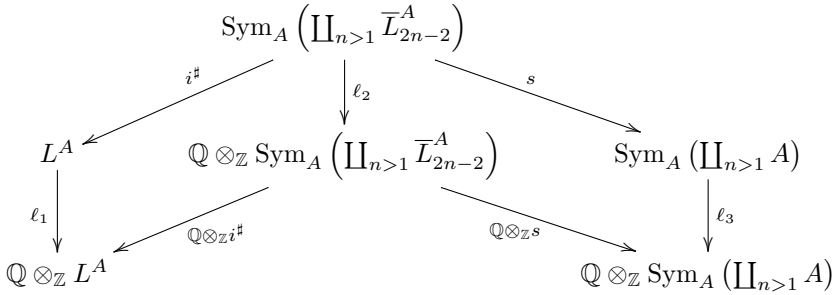
$$\begin{array}{ccc} (I^A_n)^{\otimes_A j} & \longrightarrow & A^{\otimes_A j} \\ \downarrow & & \downarrow \\ \left((I^A_n)^{\otimes_A j}\right)_{\Sigma_j} & \longrightarrow & \left(A^{\otimes_A j}\right)_{\Sigma_j} \end{array}$$

whose top horizontal map is injective. The right-hand vertical map is an isomorphism, hence the composite from upper-left to lower-right is injective. This tells us that the left-hand vertical map must be injective as well. It is

also surjective, since it is projection to the module of coinvariants. Hence the left-hand vertical map is an isomorphism, hence the bottom horizontal map is injective. The direct sum of the bottom horizontal map, over all nonnegative integers $j$, is precisely the map $\mathrm{Sym}_A(I_n^A) \to \mathrm{Sym}_A(A)$. Hence (2.13) is injective, as claimed.

The map $s$ is, up to isomorphism, a tensor product of copies of the map (2.13), taken across all integers $n > 1$. This map is injective by an induction completely analogous to that described in the previous paragraph, again using the projectivity of $I_n^A$, and the resulting projectivity of $\mathrm{Sym}_A(I_n^A)$, as an $A$-module. Hence $s$ is injective, as claimed.

Now we need to know why the map $i^\sharp$ is an isomorphism. We have the commutative diagram

(2.14)



in which the vertical maps $\ell_1, \ell_2, \ell_3$ are the canonical localization maps. The map $\mathbb{Q} \otimes_{\mathbb{Z}} i^\sharp$ is an isomorphism by Proposition 1.2.2 and Theorem 1.2.3. The map $\ell_2$ is injective, since we already showed that

$$\mathrm{Sym}_A\left(\coprod_{n>1}\overline{L}^A_{2n-2}\right) \cong \mathrm{Sym}_A\left(\coprod_{n>1} I_n^A\right) \to \mathrm{Sym}_A\left(\coprod_{n>1} A\right)$$

is injective, $\mathrm{Sym}_A\left(\coprod_{n>1} A\right)$ is a free $A$-module, and $A$ is torsion-free. Hence $\left(\mathbb{Q} \otimes_{\mathbb{Z}} i^\sharp\right) \circ \ell_2 = \ell_1 \circ i^\sharp$ is injective, and consequently $i^\sharp$ is injective.

The map $i^\sharp$ is also surjective since every element of $L^A$ is a product of (lifts of) indecomposables. Hence $i^\sharp$ is an isomorphism, as claimed.

- The fact that $i^\sharp$ is an isomorphism gives us the claimed isomorphism of $L^A$ with a tensor product of suspended symmetric algebras. We already showed that, for each $j$, the $j$th symmetric power of $I_n^A$ coincides with the $j$th power $(I_n^A)^j$ of the ideal $I_n^A$, i.e., the $j$th summand in the Rees algebra $\mathrm{Rees}_A(I_n^A)$. Consequently the symmetric algebras of the ideals $I_n^A$ coincide with their Rees algebras, giving us the claimed isomorphism of $L^A$ with a tensor product of suspended Rees algebras.

  The degree $2n-2$ of the suspensions on the right-hand side of (2.11) and of (2.12) arises because $I_n^A \subseteq A$ is the image of the fundamental functional $\sigma_{2n-2} : \overline{L}^A_{2n-2} \to A$, and $\overline{L}^A_{2n-2}$ is the $A$-module of degree $2n-2$ indecomposables in the graded $A$-algebra $L^A$.

□

**Corollary 2.1.15. (Lifting and extensions.)** *Suppose that $A$ is a torsion-free commutative ring, and suppose that the fundamental functional $\sigma_{2n-2}$ is injective, and has image a projective module, for all $n$. Then every formal $A$-module $n$-bud*

*extends to a formal $A$-module. Furthermore, if $R$ is a commutative $A$-algebra and $I$ is an ideal in $R$, then every formal $A$-module over $R/I$ is the reduction modulo $I$ of a formal $A$-module over $R$.*

*Proof.* Let $L^A_{\leq n}$ be the classifying ring of formal $A$-module $n$-buds, and let $\iota : L^A_{\leq n} \to L^A$ be the map classifying the formal $A$-module $n$-bud of the universal formal $A$-module. Then from Theorem 2.1.14 we have a commutative square

$$\begin{array}{ccc} L^A_{\leq n} & \xrightarrow{\quad\iota\quad} & L^A \\ \downarrow\cong & & \downarrow\cong \\ \mathrm{Sym}_A\left(\coprod_{1<m\leq n} I^A_m\right) & \xrightarrow{\mathrm{Sym}_A(\kappa)} & \mathrm{Sym}_A\left(\coprod_{1<m} I^A_m\right) \end{array}$$

where $\kappa$ is the inclusion of the summand $\kappa : \coprod_{1<m\leq n} I^A_m \hookrightarrow \coprod_{1<m} I^A_m$. By the universal property of $\mathrm{Sym}_A$, every morphism of commutative $A$-algebras $L^A_{\leq n} \to R$ extends over $\iota$ to a morphism of commutative $A$-algebras $L^A \to R$, hence every formal $A$-module $n$-bud extends to a formal $A$-module.

Furthermore, by the universal property of $\mathrm{Sym}_A$ and the lifting property of projective modules, every morphism of commutative $A$-algebras $L^A \to R/I$ lifts to a morphism $L^A \to R$. Hence every formal $A$-module over $R/I$ is the reduction modulo $I$ of a formal $A$-module over $R$. □

The fundamental comparison works especially well for hereditary rings $A$:

**Corollary 2.1.16.** *Suppose that $A$ is a torsion-free hereditary commutative ring, and suppose that the fundamental functional $\sigma_{2n-2}$ is injective for all $n$. Then the conclusions of Theorem 2.1.14 and of Corollary 2.1.15 all hold.*

## 2.2. **Calculation of $U$-homology.**

**Definition 2.2.1.** *Let $p$ be a prime number, and let $B$ be a commutative algebra over the field $\mathbb{F}_p$ with $p$ elements. If $n$ is a power of $p$, let $\Phi^n(B)$ denote the $B$-bimodule whose underlying right $B$-module is $B$ itself, and whose left $B$ action is twisted by the $n$th power map. That is, if $x \in \Phi^n(B)$ and $b \in B$, then $xb \in \Phi^n(B)$ is the product of $x$ and $b$ in the ring $B$, and $bx \in \Phi^n(B)$ is the product of $b^n$ and $x$ in the ring $B$.*

An alert reader may have noticed that the definition of the chain complex $\mathcal{U}^A(n)_\bullet$ in Definition-Proposition 2.1.2 resembles the construction of a Hochschild chain complex. Indeed, we have the following identification of $U$-homology with Hochschild homology with appropriate coefficients:

**Theorem 2.2.2.** *Let $A$ be a commutative ring, and let $n > 1$ be an integer.*

- *If $n$ is not a prime power, then the $U$-homology group $U^A_i(n)$ vanishes for all $i$.*
- *If $n$ is a power of a prime number $p$, then write $A/p$ for the ring $A$ reduced modulo the ideal generated by $p$. The $U$-homology group $U^A_i(n)$ is isomorphic to the Hochschild homology group $HH_i(A/p; \Phi^n(A/p))$.*

*Proof.* In the case that $n$ is not a prime power, $A/\nu(n)$ is the zero ring, so the chain complex of $A/\nu(n)$-modules $\mathcal{U}^A(n)_\bullet$ is zero. The nontrivial case is when we instead suppose that $n$ is a power of $p = \nu(n)$. By Definition 2.1.1, the $A/p$-module $F_n(A)$

is obtained by forgetting the $A$-module structure on $A$, retaining only the abelian group structure, and then taking the free $A/p$-module on this abelian group. In other words, $F_n(A)$ is $A/p \otimes_{\mathbb{Z}} A$. Of course this $A/p$-module is, in turn, isomorphic to $A/p \otimes_{\mathbb{F}_p} A/p$. Consequently the $A/p$-module of $m$-simplices $\mathcal{U}^A(n)_m$ in $\mathcal{U}^A(n)_\bullet$, defined in Definition-Proposition 2.1.2, is

$$\begin{aligned}\mathcal{U}^A(n)_m &= F_n(A)^{\otimes_{A/p} m} \\ &\cong (A/p \otimes_{\mathbb{Z}} A)^{\otimes_{A/p} m} \\ &\cong \left(A/p \otimes_{\mathbb{F}_p} A/p\right)^{\otimes_{A/p} m} \\ &\cong A/p \otimes_{\mathbb{F}_p} \left(A/p^{\otimes_{\mathbb{F}_p} m}\right)\end{aligned}$$

via the isomorphism

$$\begin{gathered}F_n(A)^{\otimes_{A/p} m} \xrightarrow{\psi_m} A/p \otimes_{\mathbb{F}_p} \left(A/p^{\otimes_{\mathbb{F}_p} m}\right) \\ a_1 c_{b_1} \otimes a_2 c_{b_2} \otimes \cdots \otimes a_m c_{b_m} \mapsto a_1 a_2 \ldots a_m \otimes b_1 \otimes \cdots \otimes b_m.\end{gathered}$$

We claim that the isomorphisms $\psi_0, \psi_1, \ldots$ fit together with the face and degeneracy maps to yield an isomorphism of simplicial $A/p$-modules

(2.15)

$$\begin{array}{ccccc} F_n(A)^{\otimes_{A/p} 0} & \rightleftarrows & F_n(A)^{\otimes_{A/p} 1} & \substack{\leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow} & F_n(A)^{\otimes_{A/p} 2} \substack{\leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow} \ldots \\ \cong \downarrow \psi_0 & & \cong \downarrow \psi_1 & & \cong \downarrow \psi_2 \\ A/p \otimes_{\mathbb{F}_p} \left(A/p^{\otimes_{\mathbb{F}_p} 0}\right) & \rightleftarrows & A/p \otimes_{\mathbb{F}_p} \left(A/p^{\otimes_{\mathbb{F}_p} 1}\right) & \substack{\leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow} & A/p \otimes_{\mathbb{F}_p} \left(A/p^{\otimes_{\mathbb{F}_p} 2}\right) \substack{\leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow\\ \leftarrow} \ldots \end{array}$$

The top row of (2.15) is the simplicial $A/p$-module $\mathcal{U}^A(n)_\bullet$, while the bottom row is the Hochschild bar construction of $A/p$, as a $\mathbb{F}_p$-algebra, with coefficients in the bimodule $\Phi^n(A/p)$. Verifying that the maps $\psi_0, \psi_1, \ldots$ indeed define a morphism of simplicial $A/p$-modules is a matter of verifying that they commute with the face and degeneracy maps, which is routine.

Since each $\psi_i$ is an isomorphism, $\mathcal{U}^A(n)_\bullet$ is isomorphic to the Hochschild bar construction of $A/p$ with coefficients in $\Phi^n(A/p)$. Taking Moore complexes and then homology, we get the desired isomorphism $U_i^A(n) \cong HH_i(A/p; \Phi^n(A/p))$ for each $i$. □

The following 2007 theorem of Pirashvili, the main result of [13], is now extremely useful:

**Theorem 2.2.3. (Pirashvili.)** *Let $n$ be a positive power of a prime number $p$, let $B$ be a commutative $\mathbb{F}_p$-algebra, and let $\Phi^n(B)$ be the $B$-bimodule defined in Definition 2.2.1. Then $HH_i(B; \Phi^n(B))$ vanishes for all $i > 0$.*

Putting Theorems 2.2.2 and 2.2.3 together, we have:

**Corollary 2.2.4.** *All $U$-homology groups vanish in all positive homological degrees. That is, $U_i^A(n)$ vanishes whenever $A$ is a commutative ring, and $i, n$ are integers with $i > 0$ and $n > 1$.*

*Furthermore, the group $U_0^A(n)$ if trivial if $n$ is not a prime power. If $n$ is a power of a prime number $p$, then $U_0^A(n) \cong HH_0(A/p; \Phi^n(A/p)) \cong A/I_n^A$.*

2.3. **Consequences for the structure of $L^A$.** Now we are ready to combine the calculation of $U$-homology in Corollary 2.2.4 with the relationship between $U$-homology and $L^A$, proven in Proposition 2.1.4, yielding the following theorem:

**Theorem 2.3.1.** *Let $A$ be a commutative ring and let $n > 1$ be an integer. Suppose that $A$ is $\nu(n)$-torsion-free. Then the fundamental functional $\sigma_{2n-2} : \overline{L}^A_{2n-2} \to A$ is injective. The image of $\sigma_{2n-2}$ is the ideal $I^A_n$ generated by $\nu(n)$ and by all elements of the form $a^n - a \in A$.*

Applying Theorem 2.1.14 now yields:

**Corollary 2.3.2.** *Let $A$ be a torsion-free commutative ring. Suppose that, for each integer $n$, the ideal $I^A_n = (\nu(n), a^n - a \ \forall a \in A)$ of $A$ is projective as an $A$-module. Then $L^A$ is isomorphic to the tensor product of suspended symmetric algebras, and also isomorphic to the tensor product of suspended Rees algebras:*

$$L^A \cong \bigotimes_{n>1} \mathrm{Sym}^{2n-2}_A \left(I^A_n\right) \cong \bigotimes_{n>1} \mathrm{Rees}^{2n-2}_A \left(I^A_n\right).$$

In particular, by assuming that the ring $A$ is hereditary, we can force the projectivity hypothesis on the ideals $I^A_n$ to be satisfied:

**Theorem 2.3.3.** *Let $A$ be a torsion-free commutative ring. Let $S$ be a set of prime numbers such that the ring $A[S^{-1}]$ is hereditary. (If, for example, $A$ is already hereditary, then we can let $S$ be the empty set.)*

*Then the commutative graded ring $L^A$ is, after inverting $S$, isomorphic to a tensor product of ("suspended," i.e., graded) Rees algebras:*

$$L^A[S^{-1}] \cong \left(\mathrm{Rees}^2_A(I^A_2) \otimes_A \mathrm{Rees}^4_A(I^A_3) \otimes_A \mathrm{Rees}^6_A(I^A_4) \otimes_A \mathrm{Rees}^8_A(I^A_5) \otimes_A \dots\right)[S^{-1}]$$

*where $I^A_n$, for each positive integer $n$, is the ideal of $A$ defined in Definition 2.1.12 and again in Corollary 2.3.2.*

*Proof.* Theorem 1.2.3 ensures that $L^A[S^{-1}]$ coincides with $L^{A[S^{-1}]}$. The claim now follows from Corollary 2.3.2. □

**Corollary 2.3.4.** *Let $A$ be a commutative ring and $S$ a set of prime numbers such that $A$ and $S$ satisfy the assumptions of Theorem 2.3.3. Then the following statements are all true:*

- *$L^A[S^{-1}]$ is a commutative graded sub-$A$-algebra of the polynomial algebra $A[S^{-1}][x_1, x_2, \dots]$, with $x_i$ in degree $2i$.*
- *$L^A[S^{-1}]$ is not Noetherian, but for every integer $n$, the sub-$A$-algebra of $L^A[S^{-1}]$ generated by all elements of degree $\leq n$ is Noetherian.*
- *If $A[S^{-1}]$ is an integral domain, then the underlying $A[S^{-1}]$-module of $L^A[S^{-1}]$ is torsion-free.*
- *If $U^A_0(n)[S^{-1}]$ is trivial for all $n$, then $L^A[S^{-1}]$ is polynomial by the fundamental comparison condition, so $L^A[S^{-1}] \cong A[S^{-1}][x_1, x_2, \dots]$.*
- **All formal module buds extend:** *Every formal $A$-module $n$-bud over a commutative $A[S^{-1}]$-algebra extends to a formal $A$-module.*
- **All formal modules lift:** *If $R$ is a commutative $A[S^{-1}]$-algebra and $I$ is an ideal of $R$, then every formal $A$-module over $R/I$ is the modulo-$I$ reduction of a formal $A$-module over $R$.*

*Proof.* Theorem 2.3.3 together with Corollary 2.1.15. □

**Corollary 2.3.5.** *Let $K/\mathbb{Q}$ be a finite field extension with ring of integers $A$. Then every formal $A$-module $n$-bud extends to a formal $A$-module. Furthermore, if $R$ is a commutative $A$-algebra and $I$ is an ideal in $R$, then every formal $A$-module over $R/I$ is the reduction modulo $I$ of a formal $A$-module over $R$.*

## 3. Computations of $L^A$ for certain classes of ring $A$

### 3.1. **Number rings.**

**Theorem 3.1.1.** *Let $A$ be the ring of integers in a finite field extension $K/\mathbb{Q}$, let $1, \alpha_1, \ldots, \alpha_j$ be a $\mathbb{Z}$-linear basis for $A$, and let $J_n^A$ be the ideal $(\nu(n), \alpha_1^n - \alpha_1, \alpha_2^n - \alpha_2, \ldots, \alpha_j^n - \alpha_j)$ of $A$. Let $P$ denote the set of integers $> 1$ which are prime powers, and let $R$ denote the set of integers $> 1$ which are not prime powers. Then we have an isomorphism of commutative graded $A$-algebras:*

$$L^A \cong \left( \bigotimes_A^{n \in P} \mathrm{Rees}_A^{2n-2}(J_n^A) \right) \otimes_A A[x_{n-1} : n \in R],$$

*with $x_{n-1}$ in degree $2(n-1)$.*

*Proof.* We use Theorem 2.3.3. If $n$ is not a prime power, then the ideal $I_n^A$ is principal, and hence $\mathrm{Rees}_A^{2n-2}(I_n^A) \cong A[x_{n-1}]$. If $n = p^m$ for some prime number $p$, then recall that $I_n^A$ is the ideal generated by $p$ and by all elements of the form $a^{p^m} - a$ with $a \in A$. One checks easily that, if an ideal contains $p$ as well as $\alpha^{p^m} - \alpha$ for every element $\alpha$ in some $\mathbb{Z}$-linear basis for $A$, then that ideal contains $a^{p^m} - a$ for all $a \in A$. Hence $J_n^A = I_n^A$. □

Some (but not all) number fields have the property that their ring of integers can be written in the form $A = \mathbb{Z}[\alpha]$ for some element $\alpha$. Such number fields are said to be *monogenic*. Remark 2.1.13 gives us an even more compact description of $L^A$ in that case:

**Corollary 3.1.2.** *Let $A = \mathbb{Z}[\alpha]$ be the ring of integers in a monogenic finite extension $K/\mathbb{Q}$, and let $J_n^A$ be the ideal $(\nu(n), \alpha^n - \alpha)$ of $A$. Then we have an isomorphism of commutative graded $A$-algebras:*

$$L^A \cong \mathrm{Rees}_A^2(J_2^A) \otimes_A \mathrm{Rees}_A^4(J_3^A) \otimes_A \mathrm{Rees}_A^6(J_4^A) \otimes_A \mathrm{Rees}_A^8(J_5^A) \otimes_A \ldots.$$

*Proof.* This is just Theorem 3.1.1 together with Remark 2.1.13 to get a small set of generators for the ideals $I_n^A$. □

Here is another corollary of Theorem 3.1.1:

**Corollary 3.1.3.** *Let $A$ be the ring of integers in a finite extension $K/\mathbb{Q}$. Let $P$ denote the set of integers $> 1$ which are prime powers, and let $R$ denote the set of integers $> 1$ which are not prime powers. Then we have an isomorphism of commutative graded $A$-algebras:*

$$L^A \cong \left( \bigotimes_A^{n \in P} A[x_{n-1}, y_{n-1}] / \left( f_{n-1}(x_{n-1}, y_{n-1}) \right) \right) \otimes_A A[x_{n-1} : n \in R],$$

*for some set of polynomials $\{f_{n-1}\}_{n \in P}$, with each $f_{n-1} \in A[x, y]$, and with $x_{n-1}$ and $y_{n-1}$ in degree $2(n-1)$.*

*Proof.* Every ideal in $A$ can be generated by two elements, so the ideals $J_n^A$ appearing in Theorem 3.1.1 can each be generated by two elements, and with a single relation between them. Hence $\mathrm{Rees}_A(J_n^A) \cong A[x,y]/f(x,y)$ with $f(x,y)$ the relation between the two generators of $J_n^A$. □

**Remark 3.1.4.** It seems have already been known to Hazewinkel in 1978 that, when $A$ is the ring of integers in a finite extension of $\mathbb{Q}$, the $A$-module $\overline{L}_{2n-2}^A$ is isomorphic to the ideal of $A$ generated by $\nu(n)$ and by all elements of the form $a^n - a$; see Example 21.3.3A of [9], where this is almost (but not quite) stated in these terms. The full description of $L^A$ given in Theorem 3.1.2 is, on the other hand, new.

The rest of this subsection consists of special cases, examples, and observations about them. All of that material is in, in a way, routine: it follows from using elementary techniques in algebraic number theory to identify the structures of the ideals $I_n^A$ arising in Theorem 3.1.1, in order to calculate $L^A$ for various number rings $A$. The author finds these examples illuminating, as illustrations of how Theorem 3.1.1 is fruitfully applied to make calculations, what kinds of observations fall out easily from the calculations, and what kinds of phenomena one encounters. Since part of the audience for this paper may consist of topologists (like the author) who may not be accustomed to arguments involving class groups or using reciprocity laws to deduce the pattern of splitting of primes in a number field, we have elected to leave in some of the details of how these arguments go, although they are very standard arguments in number theory. The reader who does not care for examples will want to skip the rest of this subsection.

**Theorem 3.1.5.** *Let $K$ be a quadratic extension of the rational numbers, and let $A = \mathbb{Z}[\alpha]$ be the ring of integers of $K$. Let $\Delta$ denote the discriminant of $K/\mathbb{Q}$. For each prime number $p$ which divides $\Delta$, let $\mathfrak{m}_p$ be the (unique, since $p$ ramifies totally in $A$) maximal ideal of $A$ over $p$. Let $R$ be the set of prime numbers $p$ which divide $\Delta$ and which have the property that $I_{p^m}^A = (p, \alpha^{p^m} - \alpha)$ is nonprincipal for some positive integer $m$, and let $S$ be the set of integers $> 1$ which are not powers of primes contained in $R$. Then we have an isomorphism of commutative graded $A$-algebras:*

$$\begin{aligned} L^A \cong & A[x_{n-1} : n \in S] \\ & \otimes_A \bigotimes_A^{p \in R} \left( \mathrm{Rees}_A^{2p-2}(I_p^A) \otimes_A \mathrm{Rees}_A^{2p^2-2}(I_{p^2}^A) \otimes_A \mathrm{Rees}_A^{2p^3-2}(I_{p^3}^A) \otimes_A \dots \right) \end{aligned}$$

*with each polynomial generator $x_{n-1}$ in degree $2(n-1)$.*

*Consequently, we have an isomorphism of commutative graded $A[R^{-1}]$-algebras:*

$$L^A[R^{-1}] \cong A[R^{-1}][x_1, x_2, \dots],$$

*with each $x_n$ in degree $2n$.*

*Proof.* If we can show that the ideal $I_n^A$ is principal for all integers $n \in S$, then $I_n^A$ is projective as an $A$-module, so the claims all follow from Theorem 3.1.2. If $n$ is not a prime power, then $1 = \nu(n) \in I_n^A$, so $I_n^A$ is certainly principal in that case. Consequently, assume that $n = p^m$ for some prime $p \notin R$. Our goal is to show that the ideal $I_{p^m}^A$ is principal.

Every quadratic extension $K$ of $\mathbb{Q}$ can be written as $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer $d$. We now break into three cases:

**If $d$ is congruent to 2 or 3 modulo 4:** Then $A = \mathbb{Z}[\sqrt{d}]$, and by Remark 2.1.13, $I^A_{p^m} = (p, \sqrt{d} - \sqrt{d}^{p^m})$. In case $d \equiv 2$ or 3 modulo 4, the primes dividing the discriminant $\Delta$ are 2 and the primes dividing $d$. Hence the condition $p \notin R$ implies that $p$ is odd and does not divide $d$. Consequently the ideal $I^A_{p^m}$ contains $(\sqrt{d} - \sqrt{d}^{p^m})^2 = d(1 - d^{\frac{p^m-1}{2}})^2$.

Now we consider two possibilities: either $p$ divides $1 - d^{\frac{p^m-1}{2}}$, or it doesn't. If $p$ *doesn't* divide $1 - d^{\frac{p^m-1}{2}}$, then $p$ is coprime to $d(1 - d^{\frac{p^m-1}{2}})^2$ and hence $I^A_{p^m} = (1)$, which is certainly a principal ideal. On the other hand, if $p$ *does* divide $1 - d^{\frac{p^m-1}{2}}$, then

$$I^A_{p^m} = (p, \sqrt{d} - \sqrt{d}^{p^m}) = (p, \sqrt{d}(1 - d^{\frac{p^m-1}{2}})) = (p),$$

which is again principal.

We conclude that, if $d \equiv 2$ or 3 modulo 4, then $I^A_{p^m}$ is principal.

**If $p$ is odd and $d$ is congruent to 1 modulo 4:** If we write $\alpha = \frac{1}{2} + \frac{\sqrt{d}}{2}$, then $A = \mathbb{Z}[\alpha]$, and the primes dividing the discriminant $\Delta$ are exactly the primes dividing $d$. It is still the case that $\sqrt{d} \in A$, even though $A$ is not equal to $\mathbb{Z}[\sqrt{d}]$. Consequently the ideal $I^A_{p^m}$ still contains $(\sqrt{d} - \sqrt{d}^{p^m})^2$. From here the argument for the principalness of $I^A_{p^m}$ is exactly the same as in the case $d \equiv 2$ or 3 modulo 4.

**If $p = 2$ and $d$ is congruent to 1 modulo 4:** The minimal polynomial of $\alpha \in A$ is $\alpha^2 - \alpha + \frac{1-d}{4} = 0$, so modulo 2, we have

$$\begin{aligned}
\alpha - \alpha^{2^m} &\equiv \alpha - \left(\alpha + \frac{d-1}{4}\right)^{2^{m-1}} \\
&\equiv -\left(\frac{d-1}{4}\right)^{2^{m-1}} + \alpha - \alpha^{2^{m-1}} \\
&\equiv -\left(\frac{d-1}{4}\right)^{2^{m-1}} + \alpha - \left(\alpha + \frac{d-1}{4}\right)^{2^{m-2}} \\
&\equiv \dots \\
&\equiv -\sum_{i=0}^{m-1} \left(\frac{d-1}{4}\right)^{2^i},
\end{aligned}$$

which is an integer, consequently is either 0 or 1 modulo 2. If it is congruent to 0 modulo 2, then $A/I^A_{2^m} \cong A/(2)$ and hence $I^A_{2^m} = (2)$, which is principal. On the other hand, if it is congruent to 1 modulo 2, then $A/I^A_{2^m} \cong 0$ and hence $I^A_{2^m} = (1)$, which is still principal.

We conclude that, when $p \notin R$, the ideal $I^A_{p^m}$ is principal, as desired. □

**Corollary 3.1.6.** *Let $K$ be a quadratic extension of the rational numbers, let $A$ be the ring of integers of $K$, and let $\Delta$ denote the discriminant of $K/\mathbb{Q}$. Then we*

*have an isomorphism of commutative graded $A[R^{-1}]$-algebras:*

$$L^A\left[\frac{1}{\Delta}\right] \cong A\left[\frac{1}{\Delta}\right][x_1, x_2, \dots],$$

*with each $x_i$ in degree $2i$.*

**Example 3.1.7.** Let $A$ be the ring of integers in $\mathbb{Q}(\sqrt{-5})$. By Theorem 3.1.5, the only primes $p$ such that $I^A_{p^m}$ is possibly nonprincipal are those primes $p$ that ramify in $A$, i.e., 2 and 5. Let $\alpha$ denote a square root of $-5$ in $A$. By direct computation one finds that $I^A_{2^m} = (2, \alpha - 1)$ for all $m$, which is nonprincipal, and that $I^A_{5^m} = (\alpha)$ for all $m$, which is of course principal. Consequently:

$$L^A \cong \frac{A[x_1, y_1, x_3, y_3, x_7, y_7, x_{15}, y_{15}, \dots]}{((\alpha - 1)x_{2^i-1} - 2y_{2^i-1}\ \forall i \geq 1)} \otimes_A A[x_j : j \neq 2^i - 1]$$

where each $x_j$ and each $y_j$ is in degree $2j$.

**Remark 3.1.8.** Corollary 3.1.6 does *not* remain true if we simply remove the word "quadratic" from its statement; it is not the case that, for the ring of integers $A$ in an arbitrary finite extension $K/\mathbb{Q}$, the ring $L^A$ becomes polynomial after inverting the discriminant of $K/\mathbb{Q}$. For example, the cubic field $\mathbb{Q}(\sqrt[3]{7})$ has the property that, in its ring of integers $\mathbb{Z}[\sqrt[3]{7}]$, the ideals

$$I_2^{\mathbb{Z}[\sqrt[3]{7}]}, I_3^{\mathbb{Z}[\sqrt[3]{7}]}, I_5^{\mathbb{Z}[\sqrt[3]{7}]}, I_{11}^{\mathbb{Z}[\sqrt[3]{7}]}, I_{17}^{\mathbb{Z}[\sqrt[3]{7}]}, I_{23}^{\mathbb{Z}[\sqrt[3]{7}]}, I_{47}^{\mathbb{Z}[\sqrt[3]{7}]}, I_{53}^{\mathbb{Z}[\sqrt[3]{7}]}, I_{59}^{\mathbb{Z}[\sqrt[3]{7}]},$$

and probably $I_p^{\mathbb{Z}[\sqrt[3]{7}]}$ for many other $p$, are nonprincipal, as one can verify with a few lines of SAGE [21] or Magma [1]. However, 3 and 7 are the only primes dividing the discriminant of $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$, so inverting the discriminant does not make $L^{\mathbb{Z}[\sqrt[3]{7}]}$ isomorphic to a polynomial algebra. There is no finite collection of primes one can invert to make $L^{\mathbb{Z}[\sqrt[3]{7}]}$ isomorphic to a polynomial algebra. This is a consequence of the Galois closure of $\mathbb{Q}(\sqrt[3]{7})/\mathbb{Q}$ being a *nonabelian* extension of $\mathbb{Q}$, so there is no straightforward reciprocity law which establishes that how primes split, and whether they are principal, is governed simply by the congruence class of the prime modulo some conductor. A fuller discussion of these ideas requires a much longer excursion into number theory than fits within the scope of this paper.

**Remark 3.1.9.** In the proof of Theorem 3.1.5, we show that the ideal $I^A_{p^m}$ in $A$ is principal for all $p$ not ramifying in $A$. It is worth mentioning that this means that $I^A_{p^m}$ is often principal even when the factors of $(p)$ in $A$ are not principal. For example, in the case of Example 3.1.7 (i.e., $A = \mathbb{Z}[\sqrt{-5}]$), the class number is 2, and the prime numbers $3, 7, 23, 43, 47, 67, 83, 103$, and many others, all split as products of distinct nonprincipal primes. But $I^A_{p^m} \subseteq \mathbb{Z}[\sqrt{-5}]$ is still principal for those primes $p$ and for all positive integers $m$.

Something similar happens in the case of Theorem 3.1.10, i.e., $A$ the ring of integers in $\mathbb{Q}(\sqrt[4]{-18})$: the prime numbers $17, 41, 59, 107, 137, 179, 227$, and many others split in $A$ and have nonprincipal prime factors, but $I^A_{p^m} \subseteq A$ is still principal for those primes $p$ and for all positive integers $m$.

In 21.3.3A of [9], Hazewinkel explains that the extension $K = \mathbb{Q}(\sqrt[4]{-18})$ of $\mathbb{Q}$ has the property that the ideal $I^A_2$ of $A$ is nonprincipal, and consequently $L^A$ could not be a polynomial $A$-algebra. Hazewinkel does not attempt a computation of $L^A$, however. We now compute $L^A$ explicitly:

**Theorem 3.1.10.** *Let $K = \mathbb{Q}(\sqrt[4]{-18})$, and let $A$ be the ring of integers of $K$. Let $S$ denote the set of all integers $> 1$ which are not powers of 2 or of 3. Then we have an isomorphism of commutative graded $A$-algebras*

$$\begin{aligned} L^A \cong A[x_{n-1} : n \in S] \otimes_A A[x_1, y_1]/(2x_1 - (\alpha^2 - \alpha)y_1) \\ \otimes_A \bigotimes_A^{m \geq 2} (A[x_{2^m-1}, y_{2^m-1}]/(2x_{2^m-1} - \alpha y_{2^m-1})) \\ \otimes_A \bigotimes_A^{m \geq 1} (A[x_{3^m-1}, y_{3^m-1}]/(3x_{3^m-1} - \alpha y_{3^m-1}))\,, \end{aligned}$$

*where $\alpha = \sqrt[4]{-18} \in A$, and where the polynomial generators $x_i$ and $y_i$ are in degree $2i$.*

*Consequently, we have an isomorphism of commutative graded $A[\frac{1}{6}]$-algebras:*

$$L^A\left[\frac{1}{6}\right] \cong A\left[\frac{1}{6}\right][x_1, x_2, \dots]\,,$$

*with each $x_i$ in degree $2i$.*

*Proof.* Write $\alpha$ for $\sqrt[4]{-18}$. It is routine to calculate that the ring of integers of $A$ is the ring of $\mathbb{Z}$-linear combinations of $1, \alpha, \frac{1}{3}\alpha^2$, and $\frac{1}{3}\alpha^3$. Consequently

$$I^A_{p^m} = \left(p,\ \alpha - \alpha^{p^m},\ \left(\frac{1}{3}\alpha^2\right) - \left(\frac{1}{3}\alpha^2\right)^{p^m},\ \frac{1}{3}\alpha^3 - \left(\frac{1}{3}\alpha^3\right)^{p^m}\right).$$

If $p \neq 3$, then $\frac{1}{3}\alpha^2 - \left(\frac{1}{3}\alpha^2\right)^{p^m}$ and $\frac{1}{3}\alpha^3 - \left(\frac{1}{3}\alpha^3\right)^{p^m}$ are already in the ideal generated by $p$ and $\alpha - \alpha^{p^m}$. Hence, if $p \neq 3$, then $I^A_{p^m} = (p, \alpha - \alpha^{p^m})$.

We will handle the primes $p = 2$ and 3 shortly, but for now, let $p > 3$ be a prime number and let $m$ be a positive integer. We claim that the ideal $I^A_{p^m}$ is principal. To prove this claim, we break into cases:

**If $p^m - 1$ is congruent to 0 modulo 4:** Then:

$$\alpha - \alpha^{p^m} = \alpha\left(1 - (-18)^{\frac{p^m-1}{4}}\right), \tag{3.16}$$

and consequently $\left(\alpha - \alpha^{p^m}\right)^4 = -18\left(1 - (-18)^{\frac{p^m-1}{4}}\right)^4$.

If $p$ *does not* divide $1 - (-18)^{\frac{p^m-1}{4}}$ then $p$ is coprime to the integer $\left(\alpha - \alpha^{p^m}\right)^4 \in I^A_{p^m}$. Hence $I^A_{p^m}$ contains two coprime integers, hence $I^A_{p^m} = (1)$, which is principal. If $p$ instead *does* divide $1 - (-18)^{\frac{p^m-1}{4}}$, then $\alpha - \alpha^{p^m} \in (p)$, by equality (3.16), so $I^A_{p^m} = (p)$, which is again principal.

**If $p^m - 1$ is congruent to 2 modulo 4:** We have

$$\alpha - \alpha^{p^m} = \alpha\left(1 - 3\sqrt{-2}(-18)^{\frac{p^m-3}{4}}\right). \tag{3.17}$$

Since $p > 3$, the ideal $(\alpha)$ is coprime to $(p)$. Consequently $(p, \alpha - \alpha^{p^m}) = (p, 1 - 3\sqrt{-2}(-18)^{\frac{p^m-3}{4}})$, which is extended up from the subring $\mathbb{Z}[\sqrt{-2}]$ of $A$. The class number of $\mathbb{Q}(\sqrt{-2})$ is 1, so $I_A^{p^m} = (p, 1 - 3\sqrt{-2}(-18)^{\frac{p^m-3}{4}})$ is principal.

Since $p^m$ is odd, the cases $p^m - 1 \equiv 0$ and $p^m - 1 \equiv 2$ modulo 4 are all the possible cases. Hence, if $p > 3$, then $I^A_{p^m}$ is principal.

Now for the primes $p = 2$ and $p = 3$. For $p = 2$, we have $I^A_2 = (2, \alpha^2 - \alpha)$, which is nonprincipal by elementary calculation. If $m > 1$, then

$$I^A_{2^m} = (2, \alpha - \alpha^{2^m}) = (2, \alpha - (-18)^{2^{m-2}}) = (2, \alpha),$$

so $I^A_{2^m}$ is nonprincipal as well.

For $p = 3$, we claim that $I^A_{3^m} = (3, \alpha)$ for all $m \geq 1$, which is again nonprincipal. The proof is as follows: first, since $-2 \equiv 1$ modulo 3, clearly $1 - (-2)^{\frac{3^m-1}{2}}$ is divisible by 3. Consequently we have equalities in $A$

$$\begin{aligned}\frac{\alpha^2}{3} - \left(\frac{\alpha^2}{3}\right)^{3^m} &= \frac{\alpha^2}{3}\left(1 - \left(\frac{\alpha^2}{3}\right)^{3^m-1}\right) \\ &= \sqrt{-2}\left(1 - (-2)^{\frac{3^m-1}{2}}\right),\end{aligned}$$

hence equalities of ideals

$$\begin{aligned}\left(3, \alpha - \alpha^{3^m}, \frac{\alpha^2}{3} - \left(\frac{\alpha^2}{3}\right)^{3^m}\right) &= \left(3, \alpha\left(1 - (3\sqrt{-2})^{\frac{3^m-1}{2}}\right), \sqrt{-2}\left(1 - (-2)^{\frac{3^m-1}{2}}\right)\right) \\ &= (3, \alpha).\end{aligned}$$

It is elementary to verify that $\frac{\alpha^3}{3} - \left(\frac{\alpha^3}{3}\right)^{3^m} \in (3, \alpha)$ as well. This yields the desired equality of ideals $I^A_{3^m} = (3, \alpha)$.

The theorem as stated now follows from Theorem 3.1.2. □

3.2. **Group rings.** Let $C_m$ be the cyclic group with $m$ elements. In Theorem 3.2.1 we compute the classifying ring $L^{\mathbb{Z}[C_m]}$ of formal $\mathbb{Z}[C_m]$-modules, after inverting $m$, so that $\mathbb{Z}[C_m]\left[\frac{1}{m}\right]$ is hereditary and Theorem 2.3.3 applies. The resulting ring $L^{\mathbb{Z}[C_m]}\left[\frac{1}{m}\right]$ is not a polynomial algebra but nevertheless has a tractable presentation.

**Theorem 3.2.1.** *Let $C_m$ be the cyclic group of order $m$. Let $P$ be the set of integers $> 1$ which are prime powers relatively prime to $m$. Let $S$ be the set of integers $> 1$ not contained in $P$. Write $R$ for the group $\mathbb{Z}\left[\frac{1}{m}\right]$-algebra $\mathbb{Z}\left[\frac{1}{m}\right][C_m]$ of $C_m$. Then we have an isomorphism of graded $\mathbb{Z}\left[\frac{1}{m}\right]$-algebras*

$$\begin{aligned}L^{\mathbb{Z}[C_m]}\left[\frac{1}{m}\right] \cong \bigotimes_R^{n\in P} &(R[x_{n-1}, y_{n-1}]/(\nu(n)x_{n-1} - (1-\sigma)y_{n-1})) \\ &\otimes_R R[x_{n-1} : n \in S],\end{aligned}$$

*where $\sigma$ denotes a generator of $C_m$, and where the polynomial generators $x_{n-1}$ and $y_{n-1}$ are each in degree $2(n-1)$.*

*Proof.* This is another special case of Theorem 2.3.3, since $\mathbb{Z}[C_m]$ is torsion-free and since the ring $R$ is hereditary. If $p$ divides $m$, then clearly the ideal $I^{\mathbb{Z}[C_m]}_{p^i}$ becomes principal after inverting $m$, hence $\mathrm{Rees}_{\mathbb{Z}[C_m]}(I^{\mathbb{Z}[C_m]}_{p^i})\left[\frac{1}{m}\right] \cong R[x]$ if $p$ divides $m$.

Now suppose that $p$ does not divide $m$. By Remark 2.1.13, the two elements $p$ and $\sigma^{p^i} - \sigma$ suffice to generate the ideal $I^A_{p^i}$. The projection $\mathbb{Z}[C_m] \to \mathbb{Z}[C_m]/(p, \sigma^{p^i} - \sigma)$ sends $p$ to zero and $\sigma$ to 1, i.e., the kernel of the projection is the ideal $(p, \sigma - 1)$. Hence $I^{\mathbb{Z}[C_n]}_{p^i} = (p, \sigma - 1)$. Now the claim follows from Theorem 2.3.3 and the

standard presentation for the Rees algebra of a two-generator ideal, as in the proof of Corollary 3.1.3. □

**Remark 3.2.2.** Suppose $G$ is a finite abelian group. In [3] (see also [6] for a nice survey) a theory of "$G$-equivariant formal group" is developed, which is designed to admit a classifying ring $L^G$ for $G$-equivariant formal groups with a canonical comparison map with the $G$-equivariant complex bordism ring $MU^G_*$. It is a highly nontrivial fact that the comparison map is an isomorphism: this was *Greenlees' conjecture*, proven in the case $G = \mathbb{Z}/2\mathbb{Z}$ in [7] and for an arbitrary compact abelian Lie group $G$ in [8].

A $G$-equivariant formal group is a more complicated gadget than just a formal group $F$ equipped with a choice of group homomorphism $G \to \mathrm{Aut}(F)$. Even the definition of a $G$-equivariant formal group is rather involved, and since it is only tangentially related to the present paper, we refer the reader to [3] for the definition. One expects that $G$-equivariant formal groups ought to have some relationship with the simple notion of a formal group equipped with an action by the group $G$, which is nearly the same thing as a formal $\mathbb{Z}[G]$-module. Clearly, to specify the structure map $\rho : \mathbb{Z}[G] \to \mathrm{End}(F)$ of a formal $\mathbb{Z}[G]$-module, we could just as well have specified a group homomorphism $G \to \mathrm{Aut}(F)$; the only point to mention here is the tangency axiom in the definition of a formal module, i.e., that $\rho(g)(X) \equiv gX \mod X^2$, meaning that we need to have an action of $G$ on the coefficient ring of $F$. But if we begin with a group homomorphism $G \to \mathrm{Aut}(F)$, we can typically choose an action of $G$ on the coefficient ring of $F$ so that the tangency axiom is satisfied. Hence the distinction between a $\mathbb{Z}[G]$-module and a formal group with an action by $G$ is slight.

The author hopes that Theorem 3.2.1 will turn out to be useful in a comparison between the moduli of formal $\mathbb{Z}[G]$-modules and the moduli of $G$-equivariant formal group laws, after inverting the order of $G$. Such a comparison is not within the scope of this paper, though.

## References


[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Nicolas Bourbaki. *Algebra I. Chapters 1–3*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation [ MR0979982 (90d:00002)].

[3] Michael Cole, J. P. C. Greenlees, and I. Kriz. Equivariant formal group laws. *Proc. London Math. Soc. (3)*, 81(2):355–386, 2000.

[4] V. G. Drinfel′d. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[5] V. G. Drinfel′d. Coverings of $p$-adic symmetric domains. *Funkcional. Anal. i Priložen.*, 10(2):29–40, 1976.

[6] J. P. C. Greenlees. Equivariant formal group laws and complex oriented cohomology theories. *Homology Homotopy Appl.*, 3(2):225–263, 2001. Equivariant stable homotopy theory and related areas (Stanford, CA, 2000).

[7] Bernhard Hanke and Michael Wiemeler. An equivariant Quillen theorem. *Adv. Math.*, 340:48–75, 2018.

[8] Markus Hausmann. Global group laws and equivariant bordism rings. *Ann. of Math. (2)*, 195(3):841–910, 2022.

[9] Michiel Hazewinkel. *Formal groups and applications*, volume 78 of *Pure and Applied Mathematics*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[10] Michel Lazard. *Commutative formal groups*. Lecture Notes in Mathematics, Vol. 443. Springer-Verlag, Berlin, 1975.
[11] Jonathan Lubin and John Tate. Formal complex multiplication in local fields. *Ann. of Math. (2)*, 81:380–387, 1965.
[12] Austin Pearlman. *Algebraic extensions of the Brown-Peterson spectrum*. PhD in Mathematics, University of Washington, 1986.
[13] Teimuraz Pirashvili. Hochschild homology, Frobenius homomorphism and Mac Lane homology. *Algebr. Geom. Topol.*, 7:1071–1079, 2007.
[14] Daniel Quillen. On the formal group laws of unoriented and complex cobordism theory. *Bull. Amer. Math. Soc.*, 75:1293–1298, 1969.
[15] M. Rapoport and Th. Zink. *Period spaces for p-divisible groups*, volume 141 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1996.
[16] Douglas C. Ravenel. Formal $A$-modules and the Adams-Novikov spectral sequence. *J. Pure Appl. Algebra*, 32(3):327–345, 1984.
[17] Andrew Salch. Structure and cohomology of moduli of formal modules. *available on arXiv*.
[18] Andrew Salch. Obstructions to compatible splittings. *Comm. Algebra*, 44(8):3592–3610, 2016.
[19] Andrew Salch. Moduli of formal $A$-modules under change of $A$. *Algebr. Geom. Topol.*, 18(2):797–826, 2018.
[20] Andrew Salch. Height four formal groups with quadratic complex multiplication. *Algebr. Geom. Topol.*, 21(5):2141–2173, 2021.
[21] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 6.6)*, 2015. `https://www.sagemath.org`.