An Elementary Classification of Symmetric 2-Cocycles *

Adam Hughes, JohnMark Lau, Eric Peterson

November 25, 2008

Abstract

We present a classification of the so-called “additive symmetric 2-cocycles” of arbitrary degree and dimension over \( \mathbb{Z}_p \), along with a partial result and some conjectures for \( m \)-cocycles over \( \mathbb{Z}_p \), \( m > 2 \). This expands greatly on a result originally due to Lazard and more recently investigated by Ando, Hopkins, and Strickland, which together with their work culminates in a complete classification of 2-cocycles over an arbitrary commutative ring. The ring classifying these polynomials finds application in algebraic topology, including generalizations of formal group laws and of cubical structures.

Contents

1 Overview

2 Applications
  2.1 The Functor \( \text{spec} H_\ast BU \langle 2k \rangle \)
  2.2 Formal Group Laws
  2.3 Split Extensions and Higher Cubical Structures

3 Characterization of Additive Cocycles
  3.1 Preliminaries
  3.2 Basic Results
  3.3 Gathering
  3.4 Integral Projection
  3.5 Counting Additive 2-Cocycles
  3.6 The Generalized Lazard Ring
  3.7 For Higher \( m \)

A Tables of Modular Additive 2-Cocycles
  A.1 Characteristic 2
  A.2 Characteristic 3
  A.3 Characteristic 5

B Notation

*The authors were supported by NSF grant DMS-0705233.
1. Overview

An additive symmetric 2-cocycle in $k$-variables over a commutative ring $A$ (or simply “a cocycle”) is a symmetric polynomial $f \in A[x_1, \ldots, x_k]$ that satisfies the following equation:

$$f(x_1, x_2, x_3, \ldots, x_k) - f(x_0 + x_1, x_2, x_3, \ldots, x_k) + f(x_0, x_1 + x_2, x_3, \ldots, x_k) - f(x_0, x_1, x_2, \ldots, x_k) = 0.$$  

When $k = 2$, these polynomials were classified by Lazard in [Laz55] in the context of formal group laws, where he exhibited a countable basis for the space of cocycles of the form

$$f_n(x, y) = \left(\gcd_{0 < i < n} \binom{n}{i}\right)^{-1} ((x + y)^n - x^n - y^n),$$

one for each $n \in \mathbb{N}$.

An extension of Lazard’s work was considered by Ando, Hopkins, and Strickland in [AHS01] to explore $BU(2k)$ (see [2.1]). They accomplished a complete classification of the $k$-variable rational cocycles for all $k$, where they found that they were generated by a unique polynomial in each homogenous degree given by

$$\zeta^n_k = d^{-1} \sum_{I \subseteq \{1, \ldots, k\}, I \neq \emptyset} (-1)^{|I|} \left(\sum_{i \in I} x_i\right)^n,$$

where $d$ is the gcd of the coefficients of the right-hand sum. The form of these cocycles is a relatively straightforward generalization of Lazard’s cocycles; note that

$$\zeta^n_2 = d^{-1} \sum_{I \subseteq \{1, 2\}, I \neq \emptyset} (-1)^{|I|} \left(\sum_{i \in I} x_i\right)^n \stackrel{d^{-1}}{=} d^{-1} ((x_1 + x_2)^n - x_1^n - x_2^n) = f_n(x_1, x_2).$$

The authors also found a classification for $A$-cocycles in three-variable case for any commutative ring $A$. In the particular case when $A = \mathbb{Z}_p$, they found generators in each homogenous degree given by one or both of $\zeta_3^n$ and $(\zeta_3^{n/p})^p$ under the projection $\pi_p : \mathbb{Z} \rightarrow \mathbb{Z}_p$, the second considered precisely when $p \mid n$.

This modular classification is what we complete for higher $k$. What separates our approach from past classifications is that we construct the classification for all $k$ in concert; indeed, the classification for $k$ variable often depends upon the classification for $r$ variables, $r > k$.

First, to each integer partition $\lambda$ of $n$, we associate a symmetric polynomial $\tau_\lambda$ given by

$$\tau_\lambda = d^{-1} \sum_{\sigma \in S_k} x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_k^{\lambda_k} \in \mathbb{Z}[x],$$

where $S_k$ acts on an ordered partition $\lambda$ by permuting its elements. For instance, we have

$$\tau(2, 1, 1) = x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2,$$
$$\tau(2, 2, 2) = x_1^2 x_2^2 x_3^2,$$
$$\tau(1, 2, 3) = x_1 x_2^2 x_3^3 + x_1 x_2 x_3^2 x_4 + x_1^2 x_2 x_3^2 + x_1^3 x_2 x_3 + x_1^2 x_2^3 x_3 + x_1^3 x_2^2 x_3.$$  

We say such a partition is power-of-$p$ when all its entries are integer powers of $p$. It’s not difficult to show that $\tau_\lambda$ is a cocycle over $\mathbb{Z}_p$ when $\lambda$ is power-of-$p$. The first step in our classification is then

**Theorem 1.1:** Let $n, k$ be such that a power-of-$p$ partition of $n$ of length $k$ exists. Then the symmetrized monomials corresponding to power-of-$p$ partitions of $n$ of length $k$ are the only 2-cocycles of that homogenous degree, number of variables, and characteristic.
This alone gives the vast majority of the classification in $\mathbb{Z}_2$; if for a power-of-2 partition $\lambda$ we can pick $x \in \lambda$ not equal to one, then we can construct the partition $\lambda' = (\lambda \setminus \{x\}) \cup (2^{-1}x, 2^{-1}x)$, where $\cup$ denotes partition concatenation and \ denotes deletion. $\lambda'$ is a power-of-2 partition of length one greater than $\lambda$, and we can then simply apply $\Box$ again. Of course, when $n = 13$, our smallest power-of-2 partition is given by $(8, 4, 1)$, and so $\Box$ tells us nothing about the 2-cocycles in two variables here. This problem becomes even more exaggerated in odd prime characteristics; the partition $(9, 3)$ gives rise to the power-of-3 partitions $(9, 1, 1, 1)$ and $(3, 3, 3, 3)$ by a similar splitting procedure, and now we find that we’ve skipped over the cocycles in three variables. To highlight the non-power-of-$p$ cases we’ve left undescribed, we provide the following excerpt from the table of cocycle bases over $\mathbb{Z}_3$ contained in $\Box$ as obtained by raw computation:

| dim | 2 | 3 | 4 | 5 | 6 |
|-----|---|---|---|---|---|
|     |   |   |   |   |   |
| deg 8 | $\tau(6, 2)+$ | $\tau(6, 1, 1)-$ | $\tau(3, 3, 1, 1)$ | $\tau(3, 2, 1, 1, 1)+$ | $\tau(3, 1, 1, 1, 1)$ |
|       | $\tau(4, 4)-$ | $\tau(4, 3, 1)+$ |               | $\tau(4, 1, 1, 1, 1)$ |               |
|       | $\tau(7, 1)-$ | $\tau(3, 3, 2)$ |               |               |               |
|       | $\tau(5, 3)$ |               |               |               |               |
| 12   | $\tau(9, 3)$ | $\tau(6, 3, 3)$ | $\tau(3, 3, 3, 3)$ | $\tau(6, 3, 1, 1, 1)-$ | $\tau(3, 3, 3, 1, 1, 1)$ |
|       | $\tau(9, 2, 1)-$ | $\tau(9, 1, 1, 1)$ |               | $\tau(4, 3, 3, 1, 1)+$ |               |
|       | $\tau(10, 1, 1)$ |               |               | $\tau(3, 3, 3, 2, 1)$ |               |
|       |               |               |               |               |               |

To explain these other entries, we define $G_{i,j}$, called a gathering operator, to act on partitions by

$$G_{i,j} : \lambda \mapsto (\lambda_i + \lambda_j) \cup (\lambda \setminus (\lambda_i, \lambda_j)).$$

Following the above example, we compute

$$G_{1,2}(9, 1, 1, 1) = (10, 1, 1),$$
$$G_{2,3}(9, 1, 1, 1) = (9, 2, 1),$$
$$G_{1,2}(3, 3, 3, 3) = (6, 3, 3).$$

Our main result is that in all degree, dimension, characteristic triples not covered by $\Box$ the following theorem completes the classification:

**Theorem 1.2:** Select a power-of-$p$ partition $\lambda$ of $n$ with length $k$. Let $T^m \lambda$ denote the set of all possible partitions of the form $G_{i_1, j_1} \cdots G_{i_m, j_m} \lambda$. Then, if $m \leq p - 2$ or if $\lambda$ is the shortest power-of-$p$ partition of $n$, the polynomial

$$\sum_{\mu \in T^m \lambda} c_\mu \cdot (\tau \mu)$$

will be a cocycle, where $c_\mu$ is the coefficient of $\tau \mu$ in $\pi_p \zeta_k^\mu$. In addition, cocycles formed in this manner give a basis for the space of modular cocycles.

First note that by setting $m = 0$, this subsumes theorem $\Box$. The theorem then applies in two cases, one corresponding to a limit on the number of gathering operators we apply and another to having picked a very particular $\lambda$. To illustrate the first case, we continue our example of $n = 12, k = 3, p = 3$ by computing the requisite intermediates

$$T^1(9, 1, 1, 1) = \{(9, 2, 1), (10, 1, 1)\},$$
$$T^1(3, 3, 3, 3) = \{(6, 3, 3)\},$$
$$\pi_3 \zeta_3^{12} = \tau(9, 2, 1) - \tau(10, 1, 1) + \tau(6, 3, 3).$$
Since \( m = 1 \leq 1 = p - 2 \), the above theorem then states that \( (\tau(9, 2, 1) - \tau(10, 1, 1)) \) and \( \tau(6, 3, 3) \) are cocycles that form a basis for this subspace. The second case applies in essence when \( \lambda \) corresponds to the base-\( p \) representation of \( n \); for instance, if \( p = 3 \) and \( n = 8 = 2 \cdot 3^1 + 2 \cdot 3^0 \), then \( \lambda = (3, 3, 1, 1) \) is the smallest power-of-3 partition of 8. We can use the following information to form cocycle bases of dimensions 2 and 3:

\[
T^1(3, 3, 1, 1) = \{ (6, 1, 1), (4, 3, 1), (3, 3, 2) \}
\]

\[
\pi_3 \zeta_8^2 = \tau(4, 3, 1) - \tau(6, 1, 1) - \tau(3, 3, 2)
\]

\[
T^2(3, 3, 1, 1) = \{ (7, 1), (6, 2), (5, 3), (4, 4) \}
\]

\[
\pi_3 \zeta_8^3 = \tau(7, 1) - \tau(6, 2) + \tau(5, 3) - \tau(4, 4)
\]

Theorem 1.2 then states that \( \pi_3 \zeta_8^2 \) and \( \pi_3 \zeta_8^3 \) span the spaces of characteristic 3 cocycles of homogenous degree 8 in dimensions 2 and 3 respectively.

To emphasize the interdimensional relationship that \( T^m \lambda \) illuminates, we present the following stratifications of the first few cocycles of degrees 8 and 12 in characteristic 3:

Figure 1: Cocycles over \( \mathbb{Z}_3 \) of homogenous degree 8.

Figure 2: Cocycles over \( \mathbb{Z}_3 \) of homogenous degree 12.
Here arrows with triangular tails denote cocycles discovered by splitting a power-of-$p$ partition, while those with circular tails denote cocycles discovered by our gathering operations and theorem 1.2. Under the conditions employed in 1.2, $T_m\mu$ and $T_m\lambda$ are disjoint for distinct $\mu$ and $\lambda$, which gives us a way to count the cocycles of a particular degree and dimension. It is well known that the coefficients $C_{nk}^p$ of the generating function

$$
\prod_{i=0}^{\infty} \left(1 - tx^p\right)^{-1} = \sum_{n,k} C_{nk}^p x^n t^k
$$

count the number of ways to write $n$ as a sum of $k$ powers of $p$. Then, as a corollary,

**Theorem 1.3:** The number of cocycles in degree $n$ and dimension $k$ is $C_{nk'}^p$, where $k'$ is the smallest number greater than $k$ such that $C_{nk'}^p$ is nonzero.

We begin the paper in §2 by motivating the study of these 2-cocycles and investigating loosely where they arise in other fields. We then spend §3.1 introducing the notations and conventions used in our proofs, including multi-indices and the relevant cochain complex. We break down the problem into smaller parts in §3.2, then work up to a version of 1.1 and the definition of $\zeta_n^k$. In §3.3 we produce a variety of results about carry minimality and carry’s behavior under our gathering and splitting operations, culminating in a proof of the first half of 1.2. We then spend §3.4 on demonstrating that the cocycles we constructed in §3.3 form a basis, corresponding to the second half of 1.2. We wrap up the paper by giving a few corollaries of our classification in sections §3.5 and §3.6 along with conjectures for higher cocycle conditions in §3.7.

2. Applications

2.1. The Functor $\text{spec} H_*BU\langle 2k \rangle$

Let $\{L_i\}_{i=1}^{k+1}$ be $(k + 1)$ copies of the line bundle over $CP^\infty$ inherited from $C^\infty \to CP^\infty$ and denote the trivial line bundle on $CP^\infty$ by 1. Vector bundles over a fixed space $X$ form a commutative semiring with addition given by direct sum and multiplication by tensor product. Applying the Grothendieck construction to this semiring (which effectively adjoins formal additive inverses) produces what is called the ring of virtual bundles, denoted $K(X)$ or $K_0(X)$. In this context we can consider the virtual bundle

$$
\xi_k = \prod_{i=1}^{k} (1 - \mathbb{L}_i) = \sum_{I \subseteq \{1, \ldots, k\}} (-1)^{|I|} \left( \prod_{i \in I} \mathbb{L}_i \right),
$$

taken over the product space $(CP^\infty)^k$.

The virtual bundle $\xi_k$ is important because it illuminates a correspondence between ring maps

$$
H_*BU\langle 2k \rangle \to A
$$

and multiplicative 2-cocycles in $k$ variables with coefficients in $A$ (here $X\langle n \rangle$ is the $(n - 1)$-connected cover of $X$). This arises in short because $\xi_k$ is a virtual bundle of rank zero, so there’s a map $(CP^\infty)^k \to BU$ classifying it. Because $\xi_k$ has vanishing Chern classes $c_1, \ldots, c_k$ this classifying map lifts to $f : (CP^\infty)^k \to BU(2k)$ in such a way that the following diagram commutes:
This induces a map in homology \( H_* f : H_* (\mathbb{C}P^\infty)^k \to H_* BU(2k) \), which by the universal coefficient theorem corresponds to an element

\[
f' \in H^* (\mathbb{C}P^\infty)^k ; H_* BU(2k))
\]

An application of the Künneth formula and the calculation \( H^* \mathbb{C}P^\infty = \mathbb{Z}[x] \) gives that

\[
H^* (\mathbb{C}P^\infty)^k; H_* BU(2k)) = \bigotimes_{i=1}^{k} H^*(\mathbb{C}P^\infty; H_* BU(2k))
\]

and so \( f' \) can be viewed as a power series, an idea we further explore. To start, there are also two standard classes of maps:

- \( \pi_i : (\mathbb{C}P^\infty)^{k+1} \to (\mathbb{C}P^\infty)^k \), given by dropping the \( i \)th copy of \( \mathbb{C}P^\infty \).
- \( m_{ij} : (\mathbb{C}P^\infty)^{k+1} \to (\mathbb{C}P^\infty)^k \), given by applying the multiplication map \( \mathbb{C}P^\infty \times \mathbb{C}P^\infty \to \mathbb{C}P^\infty \) to the \( i \)th and \( j \)th components, corresponding to tensor product of line bundles.

We can then compute the pullback bundles along these maps:

\[
\pi_i^* \xi_k = \prod_{1 \leq i \leq k \atop i \neq s} (1 - \mathbb{L}_i),
\]

\[
m_{st}^* \xi_k = (1 - L_sL_t) \cdot \prod_{1 \leq i \leq k \atop i \neq s,t} (1 - \mathbb{L}_i).
\]

Next, we make note of the following isomorphism (where \( s \neq t \)):

\[
(m_{st}^* - \pi_s^* - \pi_t^*)\xi_k = (1 - L_sL_t) \cdot \prod_{1 \leq i \leq k+1 \atop i \neq s,t} (1 - \mathbb{L}_i) - \prod_{1 \leq i \leq k+1 \atop i \neq s} (1 - \mathbb{L}_i) - \prod_{1 \leq i \leq k+1 \atop i \neq t} (1 - \mathbb{L}_i)
\]

\[
= ((1 - L_sL_t) - (1 - L_s) - (1 - L_t)) \prod_{1 \leq i \leq k+1 \atop i \neq s,t} (1 - \mathbb{L}_i)
\]

\[
= \prod_{1 \leq i \leq k+1} (1 - \mathbb{L}_i) = \xi_{k+1}.
\]

In particular, this means the following class of isomorphisms hold for all choices of \( s \neq t, s' \neq t' \):

\[
(m_{st}^* - \pi_s^* - \pi_t^*)\xi_k \cong (m_{s't'}^* - \pi_{s'}^* - \pi_{t'}^*)\xi_k.
\]

Selecting \( s = 1, t = s' = 2, \) and \( t' = 3 \) gives the following identity in terms of our power series \( f' \):

\[
\frac{f'(x_1, \ldots, x_k)}{f'(x_0 + x_1, x_2, \ldots, x_k)} \cdot \frac{f'(x_0, x_1 + x_2, x_3, \ldots, x_k)}{f'(x_0, x_1, x_3, \ldots, x_k)} = 1.
\]

We call this the multiplicative 2-cocycle condition in \( k \) variables.

In addition, there are maps \( t_{ij} : (\mathbb{C}P^\infty)^k \to (\mathbb{C}P^\infty)^k \) that act by transposing the \( i \)th and \( j \)th coordinates, and the isomorphism of virtual bundles \( t_{ij}^* \xi_k \cong \xi_k \) means that \( f' \) is symmetric as a power series. The map \( i_s : (\mathbb{C}P^\infty)^{k-1} \hookrightarrow (\mathbb{C}P^\infty)^k \) that includes away from the \( s \)th factor can be composed with \( \pi_s \) to give a pullback bundle

\[
(i_s \pi_s)^* \xi_k = (1 - 1) \prod_{1 \leq i \leq k \atop i \neq s} (1 - \mathbb{L}_i) = 0,
\]
which in turn forces $f'$ to be a rigid power series (i.e., $f'(\ldots,0,\ldots) = 1$). This guarantees the existence of the power series $(f')^{-1}$ used above.

For $k \leq 3$, theorems due to Ando, Hopkins, and Strickland state that multiplicative 2-cocycles over an arbitrary ring $A$ are selected by this universal multiplicative 2-cocycle $f'$ via some ring map $H_*BU(2k) \to A$ and the induced map $(H_*BU(2k))[x_1, \ldots, x_k] \to A[x_1, \ldots, x_k]$. In addition, the action of a ring map $H_*BU(2k) \to A$ is determined by the image of $f'$, effectively giving a polite description of the correspondence is not known.

It is easy to check that these power series must be of the form $1 + g +$ higher order terms, where $g$ is a $k$-variable additive 2-cocycle as described in 2.2. Formal Group Laws

2.2. Formal Group Laws

Let $E^*$ be a multiplicative cohomology theory and $E = E^*(pt)$ be its coefficient ring. $E^*$ is said to be complex orientable when it admits a notion of Chern classes; given a vector bundle $\xi/X$, the Chern classes associated to $E^*$ are a sequence of elements $c^E_i(\xi) \in E^{2i}(X)$ satisfying the following properties:

- **Naturality:** Given a map $f : Y \to X$, we have $f^*(c^E_i\xi) = c^E_i(f^*\xi)$, where the first use of $f^*$ denotes the induced map in cohomology and the second use denotes the pullback bundle construction.

- **Additivity:** For vector bundles $\xi/X$ and $\eta/X$, we have

  $$c^E_n(\xi \oplus \eta) = \sum_{i=0}^n c^E_i(\xi)c^E_{n-i}(\eta).$$

If we write the “total Chern class” as the formal power series $c^E(\xi) = \sum_i c^E_i(\xi)$, this can be expressed as $c^E(\xi \oplus \eta) = c^E(\xi)c^E(\eta)$.

- **Normalization:** We require the cohomology theory to provide an element $x \in E^2\mathbb{C}P^\infty$ such that $E^*\mathbb{C}P^\infty = E[\![x]\!]$ and $E^*\mathbb{C}P^k = E[\![x]\!]/(x)^{k+1}$, and we require the first Chern class to behave as $c^E_1(L) = x$. As in [2.1], $L$ is the line bundle over $\mathbb{C}P^\infty$ inherited from the quotient map $\mathbb{C}^\infty \to \mathbb{C}P^\infty$.

Let $f : \mathbb{C}P^\infty \times \mathbb{C}P^\infty \to \mathbb{C}P^\infty$ be the map classifying the line bundle $(L \otimes L)/((\mathbb{C}P^\infty \times \mathbb{C}P^\infty)$. $f$ induces a map in cohomology of the form

$$f^* : E^*(\mathbb{C}P^\infty) \to E^*(\mathbb{C}P^\infty \times \mathbb{C}P^\infty) = E[\![x,y]\!]$$

Applying the axioms above, we find that the first Chern class of the product bundle takes the form

$$c^E_1(L \otimes L) = c^E_1(f^*L) = f^*(x) = F(x,y)$$

for some bivariate power series $F$. Various properties of the tensor product of line bundles force the following three properties upon $F$:

$$\xi \otimes \eta \cong \eta \otimes \xi \implies F(x,y) = F(y,x),$$

$$\xi \otimes 1 \cong 1 \otimes \xi \implies F(x,0) = F(0,x) = x,$$

$$(\xi \otimes \eta) \otimes \nu \cong \xi \otimes (\eta \otimes \nu) \implies F(F(x,y),z) = F(x,F(y,z)).$$

Any $F$ satisfying these three properties we call a (commutative, one-dimensional) “formal group law.” As examples, the FGL associated in this way to ordinary cohomology theory is $G_a(x,y) = x + y$, the FGL associated to complex K-theory is $G_m(x,y) = x + y + xy$, and the FGL associated to complex cobordism
is \( U(x, y) = \sum_i a_i \cdot f_i(x, y) \), where \( f_i \) are Lazard’s cocycles from \([8]\) and the \( a_i \) are the adjoined elements in \( MU^*(pt) \cong \mathbb{Z}[a_1, a_2, \ldots] \). The cocycle condition also manifests in this context. Given a ring \( A \), we define an \( n \)-bud (sometimes called an \( n \)-chunk) to be a polynomial \( f \in A[[x, y]]/(x, y)^{n+1} \) also satisfying the above three conditions, a sort of truncated formal group law. Now let \( f' \in A[[x, y]]/(x, y)^{n+2} \) be an \((n+1)\)-bud extending \( f \) (i.e., \( f' = f \mod (x, y)^{n+1} \)). We seek to classify the polynomials \( g \in A[[x, y]]/(x, y)^{n+2} \) such that \( f' + g \) is again an \((n+1)\)-bud extension of \( f \) (the motivation here is that two \((n+1)\)-buds extending \( f \) will differ by such a \( g \)).

To begin, \( g \) must be of homogenous degree \((n+1)\) since it must vanish under the map
\[
A[[x, y]]/(x, y)^{n+1} \to A[[x, y]]/(x, y)^n.
\]

In addition, since \( f' + g \) is an \((n+1)\)-bud, their sum must satisfy the three FGL axioms, and in particular
\[
(f' + g)((f' + g)(x, y), z) = (f' + g)(x, (f' + g)(y, z)).
\]

After noting that \( G_a(x, y) \) is simple and trivially both an \( n \)-bud and an \((n+1)\)-bud, we set \( f = f' = G_a \) for ease of computation. Keeping careful track of truncation degree we see:
\[
(f' + g)((f' + g)(x, y), z) = (f' + g)(x, y) + z + g((f' + g)(x, y), z)
= x + y + z + g(x, y) + g(x + y + g(x, y), z)
= x + y + z + g(x, y) + g(x + y, z),
\]
\[
(f' + g)(x, (f' + g)(y, z)) = x + (f' + g)(y, z) + g(x, (f' + g)(y, z))
= x + y + z + g(y, z) + g(x, y + z + g(y, z))
= x + y + z + g(y, z) + g(x, y + z).
\]

Equating these two expansions forces the relation
\[
g(x, y) - g(z + x, y) + g(z, x + y) - g(z, x) = 0,
\]
and \( g \) is then said to be a symmetric additive \( 2 \)-cocycle.

### 2.3. Split Extensions and Higher Cubical Structures

In this section, all groups are assumed abelian. Let \( A \) and \( C \) be groups. A group \( B \) with homomorphisms \( \pi, i \) and set map \( s \) is said to be a “split extension” of \( C \) by \( A \) if the sequence
\[
0 \to A \xrightarrow{i} B \xrightarrow{\pi} C \to 0
\]
is exact and \( s \) satisfies both \( \pi \circ s = id_C \) and \( s(0_C) = 0_B \). It is fairly obvious that \( B \cong A \times C \) as sets; we can explicitly construct the two halves of the set isomorphism:
\[
\gamma : (a, c) \mapsto a + sc,
\]
\[
\gamma^{-1} : b \mapsto (b - s\pi b, \pi b).
\]

For brevity we have identified \( A \) with its embedding in \( B \), and we will shorthand the \( A \) component of \( \gamma^{-1} \) as \( a : b \mapsto b - s\pi b \).

We can then investigate the group structure induced on \( A \times C \):
\[
\gamma^{-1} b_1 + \gamma^{-1} b_2 = \gamma^{-1}(b_1 + b_2)
\]
\[
\gamma(ab_1, \pi b_1) + \gamma(ab_2, \pi b_2) = \gamma(a(b_1 + b_2), \pi(b_1 + b_2))
\]
\[
= \gamma(b_1 + b_2 - s\pi(b_1 + b_2), \pi(b_1 + b_2))
\]
\[
= \gamma(ab_1 + s\pi b_1 + ab_2 + s\pi b_2 - s\pi(b_1 + b_2), \pi(b_1 + b_2))
\]
\[
= \gamma(ab_1 + ab_2 + (s\pi b_1 + s\pi b_2 - s\pi(b_1 + b_2)), \pi(b_1 + b_2))
\]
If we rename these elements as \((a_1, c_1) = \gamma^{-1}b_1, (a_2, c_2) = \gamma^{-1}b_2\), then the last equality takes the form
\[
(a_1, c_1) +_B (a_2, c_2) = (a_1 + a_2 + f_s(c_1, c_2), c_1 + c_2),
\]
\[
f_s(c_1, c_2) = sc_1 + sc_2 - s(c_1 + c_2).
\]
As in the formal group law computation in \([2.2]\), checking associativity and commutativity of \(+_B\) forces the 2-cocycle and symmetry conditions on \(f\).

It is important to note that we’ve converted a section \(s : C \to B\) into a map \(f : C^2 \to A\). If we define a map of split extensions to be a map of short exact sequences such that the sections also commute, then it is easy to check that two split extensions are isomorphic if and only if their associated cocycles differ by a coboundary (i.e., for \(f\) and \(f'\) the associated 2-cocycles, we can find \(g : C \to A\) such that \((f - f')(c_1, c_2) = g(c_1 + c_2) - g(c_1) - g(c_2)\)). Again, this associated cochain complex in no way involves the extension \(B\) groups themselves.

This can all be restated by letting \(B\) be an \(A\)-torsor over \(C\) (we’ll change notation to \(\mathcal{B}\) to emphasize the change of setting); the section \(s\) then “trivializes” the torsor. In this light, we can use various standard constructions to build new torsors out of these old ones, including:

- **Pullback:** Given a \(G\)-torsor \(\mathcal{B} \to Y\) and a set map \(f : X \to Y\), we can construct the pullback torsor \(f^*\mathcal{B} \to X\) whose fibers are given by \((f^*\mathcal{B})_x = \mathcal{B}_{f(x)}\).

- **Dual:** Given a \(G\)-torsor \(\mathcal{B} \to X\) we can construct a torsor \(\mathcal{B}^{-1} \to X\), called the dual of \(\mathcal{B}\), whose fiber over \(x \in X\) is given by \(G\)-equivariant maps \(\mathcal{B}_x \to G\).

- **Tensor product:** Given two \(G\)-torsors \(\mathcal{A}, \mathcal{B} \to X\) we can construct a torsor \(\mathcal{A} \otimes \mathcal{B} \to X\) whose fibers are given by \((\mathcal{A} \otimes \mathcal{B})_x = \mathcal{A}_x \otimes \mathcal{B}_x\). Denoting the trivial torsor \(G \times X \to X\) by \(1\), the notation for the dual is then motivated by the relations \(\mathcal{A} \otimes \mathcal{B} \cong \mathcal{B} \otimes \mathcal{A}\), \(\mathcal{A} \otimes (\mathcal{B} \otimes C) \cong (\mathcal{A} \otimes \mathcal{B}) \otimes C\), \(\mathcal{A} \otimes 1 \cong \mathcal{A}\), and \(\mathcal{A} \otimes \mathcal{A}^{-1} \cong 1\).

In the case that \(X\) is a group, we have a number of projection and multiplication maps \(X^{m+1} \to X^m\) analogous to those given in \([2.1]\). We use this information to define a symmetric biextension of \(C\) by \(A\) to be an \(A\)-torsor \(\mathcal{B} \to C\), along with a section \(t\) of the torsor \(\mathcal{B}^{-1} \otimes t^*\mathcal{B} \to C^2\), \(\tau : C^2 \to C^2\) the flip map, and sections \(s_{ij}\) of the following family torsors for each \(1 \leq i \leq 2, j = i + 1:\)

\[
\chi_{ij}\mathcal{B} = \frac{m^i_j \mathcal{B}}{\pi^*_i \mathcal{B} \otimes \pi^*_j \mathcal{B}} \to C^3.
\]

Because these sections trivialize these torsors, we can translate these into the fiber relations \(\mathcal{B}_{c+d} \cong \mathcal{B}_{c,d} \otimes \mathcal{B}_{c,d}, \mathcal{B}_{c,d+e} \cong \mathcal{B}_{c,d} \otimes \mathcal{B}_{c,e}\), and \(\mathcal{B}_{c,d} \cong \mathcal{B}_{d,c}\). These fiber relations express a sort of partial group law defined on \(\mathcal{B}\) whenever the two operands share a \(C\)-component. Such a \(\mathcal{B}\) equipped with a section \(s : C^2 \to \mathcal{B}\) is called a split symmetric biextension, and as in the split extension case we can explicitly write out the (partial) group laws as

\[
(a, x, y) + (b, x', y) = (a + b + f(y)(x, x'), x + x', y),
\]
\[
(a, x, y) + (b, x, y') = (a + b + f(x)(y, y'), x, y + y'),
\]
where each \(f(x)(-, -)\) is a symmetric 2-cocycle.

Now, given a torsor \(\mathcal{B} \to C\), we can construct the two torsors \(\Lambda \mathcal{B} \to C^2\) and \(\Theta \mathcal{B} \to C^3\), called the first and second differences of \(\mathcal{B}\) respectively, whose fibers are given by the formulas

\[
(\Lambda \mathcal{B})_{x,y} = \frac{\mathcal{B}_{x+y}}{\mathcal{B}_x \otimes \mathcal{B}_y}, (\Theta \mathcal{B})_{x,y,z} = \frac{\mathcal{B}_{x+y+z} \otimes \mathcal{B}_x \otimes \mathcal{B}_y \otimes \mathcal{B}_z}{\mathcal{B}_{x+y} \otimes \mathcal{B}_{x+z} \otimes \mathcal{B}_{y+z}}.
\]

A torsor is said to be rigid when we equip it with a section of the fiber \(\mathcal{B}_0\); a section of \(\Theta \mathcal{B}\) then automatically gives a rigidification of \(\mathcal{B}\), \(\Lambda \mathcal{B}\), and \(\Theta \mathcal{B}\). The section of \(\Theta \mathcal{B}\) itself is said to be rigid when the rigidification
section agrees with the induced sections of $i_s^*(\Theta B) \cong (\pi \circ 0)^*(\Theta B)$, where $i_s : C^2 \to C^3$ includes away from the $s$th component. A rigid section of $\Theta B$ corresponds to a kind of symmetric biextension structure on $\Lambda B$ called a cubical structure. We pick first fiber relation given in the previous paragraph to derive as an example:

$$\Theta B = \frac{B_{x+y+z} \otimes B_x \otimes B_y \otimes B_z}{B_{x+y} \otimes B_{x+z} \otimes B_{y+z}} \cong 1$$

Thus, since giving a section of $\Theta B$ trivializes it, we get a biextension structure on $\Lambda B$ because of it, and the biextension structure is automatically symmetric by definition of $\Lambda B$. In fact, because the maps $(\Lambda B)_{x,z} \otimes (\Lambda B)_{y,z} \to (\Lambda B)_{x+y,z}$ and $(\Lambda B)_{x,y} \otimes (\Lambda B)_{z,y} \to (\Lambda B)_{x+z,y}$ are both determined by the same section of $(\Theta B)_{x,y,z}$ ("same" in the sense that the section is rigid, and so it won’t matter which we choose), we have that the two evaluations of $f$ in the following two calculations are equal:

$$(g, x, z) +_L (h, y, z) = (g + h + f(z)(x, y), x + y, z)$$

$$(g, x, y) +_L (h, z, y) = (g + h + f(y)(x, z), x + z, y),$$

where $+_L$ denotes the action of the isomorphisms $B_{x,z} \otimes B_{y,z} \to B_{x+y,z}$ given by the biextension structure. Similar equalities occur for other permutations of $x, y,$ and $z$, resulting in symmetry of $f$ as a function $C^3 \to G$. This material has all been examined in detail before; see for instance [Bre83] for a thorough treatment of cubical structures in general and $[AS01]$ for their application as in $[2.1]$

We can use a variation of this construction to form $m$-variable 2-cocycles $f : C^m \to A$. Given an $A$-torsor $B \to C$, let $\Theta^m B \to C^m$ be defined by the formula

$$(\Theta^m B)_x = \bigotimes_{I \subseteq \{1, \ldots, m\}, I \neq \emptyset} (B_{\sum_{i \in I} x_i})^{(-1)^{|I|}}.$$ 

It’s worth noting the following correspondences:

$$\Theta^0 B = 1,$$

$$\Theta^1 B = B,$$

$$\Theta^2 B = \Lambda B,$$

$$\Theta^3 B = \Theta B.$$ 

Generalizing the previous definitions in the obvious way, an $m$-extension is a $B \to C^m$ with sections of $\chi_{ij} B \to X^{m+1}$ for $1 \leq i \leq m, j = i + 1$, and a symmetric $m$-extension is an $m$-extension where $B_x \cong B_{\sigma x}$ for every $\sigma \in S_m$. Then, a section $s$ of $\Theta^m B \to C^{m+1}$ (a sort of higher cubical structure) satisfying $\pi_A(s(x)) = \pi_A(s(\sigma x))$ induces a symmetric $m$-extension structure on $\Theta^m B \to C^m$ in a manner identical to the biextension case. Again as in the previous cases, the symmetric $m$-extension structure gives rise to a function $f : C^{m-2} \to (C^2 \to A)$ which parameterizes a family of symmetric 2-cocycles, and as in the biextension case because the same fiber section of $\Theta^{m+1} B$ determines the action of both $f(x)$ (here interpreted as a function $f : C^m \to A$ and $f(\sigma x)$, we find that $f(x) = f(\sigma x)$.

We can recast this again, this time in the light of affine schemes: to give a split extension of the group scheme $Z$ by the group scheme $X$ is to give a split extension $Y(R)$ of the groups $Z(R)$ by $X(R)$ naturally in $R$. This is to say that for every ring map $f : R \to S$ we should have the following corresponding commutative
In addition, we require that the diagram:

\[\begin{array}{ccc}
0 & \rightarrow & X(R) \rightarrow Y(R) \rightarrow Z(R) \rightarrow 0 \\
| & \downarrow{X(f)} & \downarrow{Y(f)} & \downarrow{Z(f)} \\
0 & \rightarrow & X(S) \rightarrow Y(S) \rightarrow Z(S) \rightarrow 0
\end{array}\]

In addition, we require that \(Y(f) \circ s(R) = s(S) \circ Z(f)\), where \(s(R) : Z(R) \rightarrow Y(R)\) is the section associated to the split extension \(Y(R)\) of \(Z(R)\) by \(X(R)\).

Let \(\mathbb{G}_a\) denote the functor that sends a \(k\)-algebra \(R\) to its underlying additive group \(R_+\), representable by \(k[x]\). If we fix a split extension \(Y\) of \(\mathbb{G}_a\) by \(\mathbb{G}_a\) and pick a \(k\)-algebra \(R\), then the split extension \(Y(R)\) associated to \(R\) is set isomorphic to \(R_+ \times R_+\), and the multiplication map \(Y(R) \times Y(R) \rightarrow Y(R)\) then corresponds to a map \((R_+ \times R_+)^2 \rightarrow R_+ \times R_+\). We have seen already that the multiplication in \(Y(R)\) is determined by its action on elements with zero left-component, say \((0, r)\) and \((0, s)\). These elements are, by construction of \(\mathbb{G}_a(R) = X(R) = Z(R)\), selected by the map

\[f : k[a] \otimes_k k[b] = k[a, b] \rightarrow (R_+)^2,\]

\[f : a \mapsto r, f : b \mapsto s.\]

By naturality of the scheme assignment,

\[(0, r) +_{Y(R)} (0, s) = (f(0), f(a)) +_{Y(R)} (f(0), f(b)) = f((0, a) +_{Y(k[a, b])} (0, b)) = f((g(a, b), a + b)),\]

where \(g\) is the symmetric 2-cocycle corresponding to the split extension. Most importantly, \(g\) is a map with target \(k[a, b]\), and so \(g(a, b)\) will be a polynomial over \(k\) that universally determines the action of the split scheme extension. \(g\) is easily seen to be symmetric and to satisfy the 2-cocycle condition. This same construction can be made for split multiextensions of \(\mathbb{G}_a\) by \(\mathbb{G}_a\), where the \(k\)-variable symmetric 2-cocycle again has a polynomial representation.

3. Characterization of Additive Cocycles

3.1. Preliminaries

We first introduce the central constructs and notations we will use throughout the paper, most importantly that of multi-indices and number theoretic functions on them, in particular the notion of carry-count.

**Definition 3.1.1:** A multi-index of weight \(n\) and length \(k\) is a \(k\)-tuple of elements of \(\mathbb{N}_0 = \mathbb{N} \cup \{0\}\) of the form \(\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)\) that satisfies \(\sum \lambda_i = n\). We further say that \(\lambda\) is a power-of-\(p\) multi-index when there exist \(a_i \in \mathbb{N}\) such that \(\lambda_i = p^{a_i}\) for all \(i\). We denote the length as \(\ell(\lambda) = k\) and the weight as \(|\lambda| = n\).

We define the following operations over multi-indices:

- **Exponentiation:** \(x^\lambda = x_1^{\lambda_1}x_2^{\lambda_2} \cdots x_k^{\lambda_k}\), where \(x = (x_1, x_2, \ldots, x_k)\).
- **Permutation:** \(\sigma \lambda = (\lambda_{(\sigma1)}, \lambda_{(\sigma2)}, \ldots, \lambda_{(\sigma k)})\), for \(\sigma \in S_k\).
- **Membership:** We write \(a \in \lambda\) when there is some \(i\) for which \(a = \lambda_i\).
- **Concatenation:** \(\lambda \cup \mu = (\lambda_1, \ldots, \lambda_i, \mu_1, \ldots, \mu_j)\).
• **Difference:** \( \lambda \setminus \mu = \lambda' \) is defined to be the unique unordered multi-index such that \( \mu \cup \lambda' = \lambda \) (again up to reordering). For example, \( (2, 2, 1) \setminus (2, 1) = (2) \).

• **Ring extension:** \( A[x] = A[x_1, \ldots, x_k] \) for \( x = (x_1, \ldots, x_k) \).

• **Map to monomials:** We define \( \tau(\lambda) \) to be the polynomial \( \sum_{\sigma \in S_k} x^{\sigma \lambda} \) once divided by the gcd of the coefficients. For example, we provide these expansions:

\[
\tau(2, 1, 1) = x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2 \\
\tau(2, 2, 2) = x_1^2 x_2^2 x_3^2 \\
\tau(1, 2, 3) = x_1 x_2^2 x_3^3 + x_1 x_2 x_3^2 + x_1^2 x_2 x_3^3 + x_1^2 x_2^2 x_3 + x_1^3 x_2 x_3 + x_1^3 x_2^2 x_3
\]

• **Factorial:** We define \( \lambda! = \prod_{i} \lambda_i! \).

In addition, there are a handful of useful number-theoretic constructs that can be formulated in terms of multi-indices:

• **Partitions:** When all entries of a multi-index of weight \( n \) are positive and listed in descending order, it is called a *partition of \( n \)* and is denoted \( \lambda \vdash n \).

• **Multinomial coefficients:** For a multi-index \( \lambda \), let \( \binom{\lambda}{\lambda} \) denote the integer \( (|\lambda|)!/(\lambda)!^{-1} \). Note that

\[
\binom{n + m}{(m, n)} = \binom{n + m}{m} = \binom{n + m}{n}
\]

corresponds with the usual binomial coefficients.

• **Carry count:** The number of times one carries when calculating the base \( p \) sum \( \sum \lambda_i \) is denoted \( \alpha_p(\lambda) \). It is well known that this can be formalized as the number of times \( \binom{\lambda}{\lambda} \) is divisible by \( p \). This is a straightforward generalization of a result due to Kummer, originally found in [Kum85]. A particularly useful property is that for two multi-indices \( \lambda, \mu \) we have \( \alpha_p(\lambda \cup \mu) = \alpha_p(|\lambda| \cup \mu) + \alpha_p(\lambda) \), corresponding to associativity of addition.

• **Digital sum:** The digital sum of a number \( n \) in base \( p \) is denoted \( \sigma_p(n) \). Explicitly, if \( n = \sum_{i=0}^{\infty} a_i p^i \) for \( 0 \leq a_i < p \), then \( \sigma_p(n) = \sum_{i=0}^{\infty} a_i \).

• **Base-\( p \) representation:** Given \( n \in \mathbb{N} \), let \( \rho_p(n) \) be the power-of-\( p \) multi-index such that \( |\rho_p(n)| = n \) and \( \rho_p(n) \) has minimal length (i.e., \( \sigma_p(n) = \ell(\rho_p(n)) \)). For example, we can compute \( \rho_3(16) = (9, 3, 3, 1) \). \( (9, 3, 1, 1, 1, 1) \) is another power-of-3 multi-index with weight 16, but it does not have minimal length. This corresponds in an obvious way to the base-\( p \) expansion of \( n \) given by \( n = \sum_{i=0}^{\infty} a_i p^i \) for \( 0 \leq a_i < p \), where \( p^i \) appears \( a_i \) many times in \( \rho_p(n) \).

**Definition 3.1.2:** We say that a partition \( \lambda \) of weight \( n \) and length \( k \) has carry-minimal sum in base \( p \) or is \( p \)-carry minimal when \( \alpha_p(\lambda) \) is minimal in the sense of \( \alpha_p(\lambda') = \min \{ \alpha_p(\lambda') \mid \lambda' \vdash n, \ell(\lambda') = k \} \). For example, \( \alpha_3(9, 2, 1) = 1 \), and is \( 3 \)-carry minimal. \( \alpha_3(8, 3, 1) = 2 \), and so because \( (8, 3, 1) \) is of the same weight and length as \( (9, 2, 1) \), it is not \( 3 \)-carry minimal.

**Definition 3.1.3:** Throughout this paper, we will use *ring* to mean commutative ring with unit. Given a ring \( A \) and an ideal \( I \subseteq A \) we will use \( \pi_I : A \to A/I \) to denote the natural homomorphism with kernel \( I \). In the event \( I = \langle a \rangle \), \( a \in A \), we denote \( \pi_I \) by \( \pi_a \).

**Definition 3.1.4:** We say an \( k \)-variable polynomial is *symmetric* if \( f(x) = f(\sigma x) \) for all \( \sigma \in S_k \).

**Remark 3.1.5:** The \( A \)-algebra of symmetric multivariate polynomials has two natural gradations, one corresponding to degree and one corresponding to number of variables.
**Definition 3.1.6:** $\tau$ surjects onto a basis for symmetric polynomials. When restricted to $k$-variable polynomials of homogenous degree $n$, we call it the monomial symmetric basis on $k$ variables, and denote it as $B_k^n$.

**Definition 3.1.7:** The $m$-coboundary map, denoted $\delta_m$, is a map of modules that operates on polynomials of $k \geq m$ variables and is defined by

$$\delta_m(f) = f(x_1, \ldots, x_k) + \sum_{i=1}^{m} (-1)^i f(x_0, x_1, \ldots, x_{i-2}, x_{i-1} + x_i, x_{i+1}, \ldots, x_k) + (-1)^{m+1} f(x_0, x_1, \ldots, x_{m-1}, x_{m+1}, \ldots, x_k).$$

It is easy to see that $\delta_m$ sends polynomials of homogenous degree $n$ in $k$ variables to polynomials of homogenous degree $n$ in $(k+1)$ variables. In addition, $\delta_m \circ \delta_{m-1} = 0$, or $\delta$ is a differential. We define the $(m)$-cocycle condition as applied to a polynomial $f$ to mean $\delta_m f = 0$, and say that "$f$ satisfies the $(m)$-cocycle condition" or "$f$ is an $(m)$-cocycle".

We also define a number of one-time use functions. We will reuse the symbol $\theta$ for all of them to save naming clutter. Which $\theta$ we intend will be clear, since a definition will be given in the theorem statement.

### 3.2. Basic Results

Beginning at this point, we strongly suggest that the reader frequently refer to appendix A where we list bases for ker $\delta_2$ restricted to particular degrees and dimensions with coefficients in $\mathbb{Z}_2$, $\mathbb{Z}_3$, and $\mathbb{Z}_5$. The structure of the data guides the structure of the proofs to follow, and to reinforce this we will provide some examples inlined with the body of the text.

Given that $\delta_m$ is a graded map of modules, we then seek to further decompose the problem into more workable pieces. There is a basis for the module of all polynomials $A[x]$ given by $\{x^\lambda\}_\lambda$ for all multi-indices $\lambda$. We would like to have the additional ability to consider our monomial symmetric basis elements one monomial at a time, but we run into the complication that there exist monomials shared between different monomial symmetric basis elements depending upon the dimension of the grading – for instance, $\tau(1,1,0)$ and $\tau(1,1)$ share the term $x_1x_2$. To eliminate this problem, we show in general that symmetrized monomials with terms not mixed in every variable cannot participate in polynomials in ker $\delta_m$.

**Lemma 3.2.1:** If $\lambda$ is of the form $(0, \lambda_2, \lambda_3, \ldots, \lambda_k)$, then $x^\lambda$ cannot contribute to a linear combination of monomials in the kernel of $\delta$.

**Proof.** The application $\delta_m(x^\lambda)$ yields the following sum:

$$\delta_m(x^\lambda) = x_2^{\lambda_2}x_3^{\lambda_3} \cdots x_k^{\lambda_k} - x_2^{\lambda_2}x_3^{\lambda_3} \cdots x_k^{\lambda_k} + (x_1 + x_2)^{\lambda_2}x_3^{\lambda_3} \cdots x_k^{\lambda_k} + \sum_{i=3}^{m} (-1)^i x_1^{\lambda_2} \cdots x_{i-2}^{\lambda_{i-2}}(x_{i-1} + x_i)^{\lambda_i}x_{i+1}^{\lambda_{i+1}} \cdots x_k^{\lambda_k} + (-1)^{m+1} x_1^{\lambda_2} \cdots x_{m-1}^{\lambda_{m-1}}x_m^{\lambda_m} \cdots x_k^{\lambda_k}.$$

Ignoring the monomials with terms mixed in $x_1$ and $x_2$ (equivalently, working modulo the ideal $\langle x_0 \cdots x_k \rangle$), we see that we have a residual term of $x_2^{\lambda_2}x_3^{\lambda_3} \cdots x_k^{\lambda_k}$. Any other choice of $\lambda$ will yield summands distinct from this monomial, therefore $x^\lambda$'s image cannot be completely cancelled by any other monomial's image under $\delta_m$. Thus no linear combination of monomials containing $x^\lambda$ can lie in the kernel of $\delta_m$. \(\square\)

**Corollary 3.2.2:** If $0 \in \lambda$, then $\tau \lambda$ cannot contribute to any symmetric cocycle.

**Proof.** Select a $\sigma \in S_k$ such that $\sigma \lambda$ is of the form $(0, \lambda_2, \ldots, \lambda_k)$ and apply Lemma 3.2.1 \(\square\)
We can then restrict our attention to multi-indices \( \lambda \) that satisfy \( 0 \not\in \lambda \). Since the presence of a zero was the only thing that prevented the entire sum from telescoping in 3.2.1, we also note that any unmixed terms in the naïve expansion of \( \delta_m \tau \lambda \) will vanish.

**Lemma 3.2.3:** Let \( \lambda \) be a multi-index with \( 0 \not\in \lambda \), \( \ell(\lambda) = k \). Then \( \delta_m(x^\lambda) \) will contain only monomials mixed in all of \( x_0, \ldots, x_k \).

**Proof.** Again working modulo the ideal \( \langle x_0 \cdots x_k \rangle, \delta_m(x^\lambda) \) can be rewritten as:

\[
x_1^{\lambda_1} \cdots x_k^{\lambda_k} + \sum_{i=1}^{m} (-1)^i x_0^{\lambda_1} \cdots x_{i-1}^{\lambda_{i-1}} x_{i+1}^{\lambda_{i+1}} \cdots x_k^{\lambda_k}
\]

\[
+ \sum_{i=1}^{m} (-1)^i x_0^{\lambda_1} \cdots x_{i-2}^{\lambda_{i-2}} x_i^{\lambda_i} \cdots x_k^{\lambda_k}
\]

\[
+ (-1)^{m+1} x_0^{\lambda_1} \cdots x_{m-1}^{\lambda_{m-1}} x_{m+1}^{\lambda_{m+1}} \cdots x_k^{\lambda_k}.
\]

The \( i \)th term of the first sum cancels with the \((i+1)\)th term of the second, so the expression telescopes and all unmixed terms vanish.

If we can find polynomials for which \( f(a+b) = f(a) + f(b) \), then we can immediately apply 3.2.3 to demonstrate that these polynomials do in fact lie in ker \( \delta_m \). If we restrict our attention to working in a ring of characteristic \( p \neq 0 \), then there are a few obvious examples of such polynomials.

**Corollary 3.2.4:** Asymmetric monomials associated to multi-indices of the form \((p^{a_1}, \ldots, p^{a_m}, b_{m+1}, \ldots, b_k)\) are \( m \)-cocycles in a coefficient ring of characteristic \( p \).

**Proof.** For any \( a, b \) in a ring of characteristic \( p \), recall that \((a+b)^p = a^p + b^p \). This then follows immediately from 3.2.3.

**Corollary 3.2.5:** The symmetrized polynomial \( \tau(\lambda) \) for \( \lambda \) a power-of-\( p \) multi-index is a cocycle under \( \delta_m : \mathbb{Z}_p[x] \rightarrow \mathbb{Z}_p[x_0, x] \).

**Proof.** Each element of this sum is a cocycle by 3.2.4 and \( \delta_m \) is a linear map.

We thus have a few critical examples of symmetric cocycles in the modular case of \( \mathbb{Z}_p[x] \). We will also require some rational cocycles, which have been classified previously in [AHS01]. We reconstruct what we will need here.

**Definition 3.2.6:** \( \zeta_k^n \in \mathbb{Z}[x] \) denotes the polynomial \( (i\delta_1)^{k-1} x^n \) when divided by the gcd of the resultant monomial coefficients, where \( i : \mathbb{Z}[x_0, \ldots] \rightarrow \mathbb{Z}[x_1, \ldots] \) acts by \( i : x_i \mapsto x_{i+1} \) and exponentiation denotes repeated application. Because \( \delta \) is a differential, this is a 2-cocycle.

The authors of [AHS01] go on to demonstrate that ker \( \delta_2 \) (for \( \delta_2 : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x_0, x] \)) is in fact generated by these \( \zeta_k^n \); the reader interested in a classification of the integral cocycles can find a proof at the beginning of [AHS01]'s appendix A. \( \zeta_k^n \) is an interesting polynomial on its own; when we expand the \( \delta_1 \) applications in 3.2.6 we find the expression takes the form:

\[
\zeta_k^n = d^{-1} \sum_{X \subseteq \{x_1, \ldots, x_k\}} \left( \frac{\delta_1}{\gcd_{0 \not\in \lambda} \left( \begin{array}{c} n \\ \lambda \end{array} \right)} \right)^{-1} \sum_{\lambda \not\in \lambda} \left( \begin{array}{c} n \\ \lambda \end{array} \right) \tau(\lambda),
\]

for some \( d \in \mathbb{Z} \). When the sums are expanded, we find

\[
\zeta_k^n = \left( \frac{\gcd_{0 \not\in \lambda} \left( \begin{array}{c} n \\ \lambda \end{array} \right)}{\lambda \geq \lambda_{i+1}} \right)^{-1} \sum_{\lambda \not\in \lambda} \left( \begin{array}{c} n \\ \lambda \end{array} \right) \tau(\lambda).
\]
Using this second expansion, we see immediately from the formal definition of $p$-carry-count that monomial summands of $\zeta^n_k$ of the form $c_\lambda x^\lambda$ belonging to non-carry-minimal $\lambda$ will vanish under $\pi_p$, while carry-minimal $c_\lambda$ will remain non-zero.

### 3.3. Gathering

Beginning with the symmetric polynomials guaranteed to us to be cocycles by 3.2.5, we investigate how to modify and extend these to form new cocycles. Looking to previous classifications for clues, [AHS01] employs the fact that their integral cocycles $\zeta^n_k$ form modular cocycles when their coefficient ring $\mathbb{Z}$ is projected down to $\mathbb{Z}_p$. It is obvious that the following diagram commutes for a general coefficient ring $A$ and ideal $I \subseteq A$:

$$
\begin{array}{c}
A[x] \xrightarrow{\delta_m} A[x, x_0] \\
\downarrow \pi_I \quad \downarrow \pi_I \\
(A/I)[x] \xrightarrow{\delta_m} (A/I)[x, x_0]
\end{array}
$$

Noting that the $m$-coboundary map when applied to $A[x]$, $\ell(x) = k$ leaves the remaining $k - m$ variables undisturbed (i.e., for $i > m$ the evaluation maps in $\delta_m$ act on $x_i$ by sending it to $x_1$), we can decompose the polynomial ring $A[x_1, \ldots, x_k]$ into the ring extension $(A[x_{m+1}, \ldots, x_k])[x_1, \ldots, x_m]$, bringing the variables undisturbed by the cocycle condition into the coefficient ring. This effectively rewrites a $k$-variable $m$-cocycle $f$ as

$$
f = \sum_{\ell(I) = k-m} (x_{m+1}, \ldots, x_k)^I \cdot f_I(x_1, \ldots, x_m),
$$

where each $f_I$ is an $m$-variable $m$-cocycle.

In this new coefficient ring we have a wide range of nontrivial ideals to select; picking ideals of the form $I = \langle x_i - x_j \rangle$ with $m < i < j \leq k$ will take $k$-variable symmetric cocycles to $(k-1)$-variable asymmetric cocycles, in effect giving us approximate information about the lower dimensional cases. $\pi_I$ is the operation that we call “gathering.” Denoting $k$-dimensional $m$-cocycles over $A$ as $Z^k(A)$ and their symmetric subset as $Z^k_s(A)$, the following (noncommutative) diagram paints a portrait of what we have so far:

$$
\begin{array}{c}
Z^{n+1}_s(\mathbb{Z}) \xrightarrow{\delta_1} Z^{n+2}_s(\mathbb{Z}) \xrightarrow{\delta_1} Z^{n+3}_s(\mathbb{Z}) \xrightarrow{\pi_p} Z^{n+1}_s(\mathbb{Z}_p) \\
\downarrow \pi_p \quad \downarrow \pi_p \quad \downarrow \pi_p \\
\cdots \quad \cdots \quad \cdots
\end{array}
$$

In this section we seek to construct the dashed maps, and to do so understanding the exact nature of $\pi_I$’s action will help. Selecting $\tau(9, 1, 1, 1)$ as an example in the case $k = 4$ and $p = 3$, its gathering is

$$
\pi_I \tau(9, 1, 1, 1) = x_1^9 x_2 x_3 + x_1 x_2^9 x_3 + 2x_1 x_2 x_3^{10}
$$

for $I = \langle x_3 - x_4 \rangle \subseteq (\mathbb{Z}_3[x_3, x_4])[x_1, x_2]$. Obviously this polynomial is no longer symmetric, and so we seek to find an appropriate symmetrization (i.e., an action for the dashed map). It is almost immediately obvious
that the naïve symmetrization \( \sum_{\sigma \in S_{k-1}} (\pi f)(\sigma x) \) will not be sufficient in general (see appendix A.3 for a plethora of complicated low-dimensional examples), and we must be more creative.

The other information we have at this point in dimension \( k-1 \) is that \( \pi_p \zeta^p_{k-1} \) is a symmetric cocycle. As we will shortly prove, gathering cocycles sufficiently “near” a power-of-\( p \) cocycle \( \tau \lambda \) yields a sum of monomials \( \sum \lambda \) for an indexed set of multi-indices \( S \) where each \( S_i \) is carry-minimal. (For example, this holds true in the above case; both \( (9, 2, 1) \) and \( (10, 1, 1) \) have minimal 3-carry.) This means that these monomials appear as summands of \( \zeta^p_i \) (for instance, \( \zeta^3_2 = \tau(9, 2, 1) - \tau(10, 1, 1) + \tau(6, 3, 3) \)), and so we may be able to use the information contained there to recover symmetric cocycles corresponding to the gathered cocycles. We begin by formalizing the notion of “nearness.”

**Definition 3.3.1:** Define the function \( \phi_p \) from multi-indices to \( \mathbb{N}_0 \) by

\[
\phi_p : \lambda \mapsto \ell(\lambda) - \ell(\lambda) = \ell \left( \bigcup_{i=1}^{\ell(\lambda)} \rho_p(\lambda_i) \right) - \ell(\lambda),
\]

which corresponds to the fewest number of gathering operations required to reach \( \lambda \) from a power-of-\( p \) multi-index. \( \phi_p(\lambda) \) is called the *splitting distance* of \( \lambda \).

For example, working in \( p = 3 \), we have

\[
\phi_3(9, 1, 1, 1) = 0, \\
\phi_3(9, 2, 1) = 1, \\
\phi_3(10, 2) = 2, \\
\phi_3(9, 3) = 0.
\]

**Theorem 3.3.2:** If \( \lambda \) is a multi-index such that \( \phi_p(\lambda) > p - 2 \) and \( \alpha_p(\lambda) > 0 \), then \( \lambda \) is not carry minimal.

*Proof.* We define a gathering operator, \( G_{ij} \), of a multi-index \( \lambda \), \( 1 \leq i < j \leq \ell(\lambda) \), to be

\[
G_{ij} \lambda = (\lambda_i + \lambda_j) \cup (\lambda \setminus (\lambda_i, \lambda_j)).
\]

Note that \( \alpha_p(G_{ij} \lambda) \leq \alpha_p(\lambda) \) for all gathering operators \( G_{ij} \).

Let \( \hat{\lambda} = \bigcup \rho_p(\lambda_i) \). Because \( \alpha_p(\hat{\lambda}) = \alpha_p(\lambda) > 0 \) and \( \hat{\lambda} \) is a power-of-\( p \) multi-index, \( \hat{\lambda} \) contains \( p \) many copies of some \( p^k \). These \( p^k \) can be gathered in \( p - 1 \) steps to form a multi-index \( \mu \) that satisfies \( \alpha_p(\mu) < \alpha_p(\lambda) \).

We can then apply any gathering operations we like to \( \mu \) to achieve a multi-index \( \mu' \) with \( \ell(\mu') = \ell(\lambda) \), and we are still guaranteed that \( \alpha_p(\mu') \leq \alpha_p(\mu) < \alpha_p(\lambda) \), which means that \( \lambda \) cannot be \( p \)-carry minimal. \( \square \)

This technique of forming an alternative gathering guides the structure of many of the remaining proofs. Using it, we can immediately gain various facts about the carry-minimality of power-of-\( p \) multi-indices and their gatherings.

**Corollary 3.3.3:** For \( n, k, p \) such that there exists a power-of-\( p \) partition \( \mu \vdash n \) with \( \ell(\mu) = k \), then any \( \lambda \) of the same weight and length that is not power-of-\( p \) will not be carry minimal.

*Proof.* First, note that all partitions can be reached via “gathering” (i.e., applying raising operators to) the trivial partition

\[
\underbrace{(1, \ldots, 1)}_{n \text{ times}} = \bigcup_{i=1}^{n}(1) = (1^n)
\]

of weight and length \( n \), and that in particular we require exactly \( p - 1 \) gathering operations to collect \( p \) copies of any \( p^k \) to form an instance of \( p^{k+1} \). Thus all power-of-\( p \) partitions occur at regular intervals of length \( p - 1 \).

Now, let \( \lambda \) be a non-power-of-\( p \) multi-index, and \( \mu \) be power-of-\( p \) with equal weight and length. Then \( \hat{\lambda} = \bigcup \rho_p(\lambda_i) \) is power-of-\( p \) with \( \ell(\hat{\lambda}) > \ell(\mu) \), and so \( \phi_p(\lambda) \geq p - 1 \). We can then apply 3.3.2. \( \square \)
Corollary 3.3.4: Iteratively gathering a power-of-$p$ monomial $\tau(\lambda)$ results in a sum of carry-minimal exponent monomials when done fewer than $p-1$ times.

Proof. Clearly gathering power-of-$p$ partitions fewer than $p-1$ times will result in partitions of the same carry-count; the question is whether this count is still minimal for the length. There are two cases: one where $\alpha_p(\lambda) = 0$ and one where $\alpha_p(\lambda) > 0$. For the first, all gatherings of $\lambda$ will also have carry-count 0, and so they are trivially carry minimal. Now, let $\alpha_p(\lambda) > 0$, let $\mu$ be the result of fewer than $p-1$ gathering operations applied to $\lambda$, and assume $\nu$ is a carry-minimal with the same weight and length as $\mu$ such that $\alpha_p(\nu) < \alpha_p(\mu)$. $\nu$ cannot arise as a gathering of anything which is power-of-$p$ and the same weight and length as $\lambda$ (since then $\alpha_p(\nu) = \alpha_p(\lambda) = \alpha_p(\mu)$), and so $\ell(\bigcup_i \rho_p(\nu_i)) > \ell(\lambda)$, which implies $\phi_p(\nu) > p-1$.

We can then apply Lemma 3.3.6 so $\nu$ is not carry minimal, a contradiction. 

Corollary 3.3.5: Let $\lambda, \mu$ be two power-of-$p$ partitions of equal length and weight. Then $\alpha_p(\lambda) = \alpha_p(\mu)$.

Proof. By Lemma 3.3.4 all power-of-$p$ partitions are carry minimal, hence if $\lambda, \mu$ are power-of-$p$ of equal length and weight, $\alpha_p(\lambda) \leq \alpha_p(\mu)$ and vice-versa.

Now we return to symmetrizing $m$-fold gatherings of $\tau\lambda$, for $\lambda$ power-of-$p$ and $m < p-1$. We begin with something slightly weaker: we find a symmetric cocycle in which all our symmetrized monomials appear as carry-minimal, hence if $\lambda, \mu$ are power-of-$p$ of equal length and weight, $\alpha_p(\lambda) \leq \alpha_p(\mu)$ and vice-versa.

Lemma 3.3.6: Let $\lambda$ be a power-of-$p$ partition and either $m < p-1$ or $\lambda = \rho_p(|\lambda|)$.

This is not quite enough to meet our original goal, since we may be forced to add other symmetrized monomials beyond what we expect from gathering. Consider, again, gatherings of $(9,1,1,1)$. We find $\pi_3\zeta_3^2 = \tau(9,2,1) - \tau(10,1,1) + \tau(6,3,3)$, and so $\tau(6,3,3)$ is an unwanted extension. $\tau(6,3,3)$, however, occurs as the 1-fold gathering of $\tau(3,3,3,3)$, which is a distinct power-of-$p$ monomial of the same degree and dimension as $\tau(9,1,1,1)$. We turn our attention toward using this observation to separate out parts of the projected integral cocycle, each of which on its own is a modular cocycle.

Fix natural $n$ and $k$ where a power-of-$p$ multi-index $\lambda$ of weight $n$ and length $k$ exists. Let $T^0(n,k) = \{\{\lambda\} \mid \lambda \vdash n \text{ is power-of-$p$, } \ell(\lambda) = k\}$. Let $\theta$ be a map from sets of partitions to sets of their single-step gatherings, and let $T^m(n,k)$ be inductively defined as $\{\theta M \mid M \in T^{m-1}(n,k)\}$. When the context is clear, we drop $(n,k)$ and write only $T^m$. We then seek to decompose $\mathbb{Z}_p[x_0,x]$ into a sum of submodules $\bigoplus_i A_i$ such that there is a one-to-one correspondence between the $A_i$ and the elements of our particular $T^m$. The decomposition must satisfy that for each $M_i \in T^m$ with associated component $A_i$, we have $\delta_{2\tau\mu} \in A_i$ for each $\mu \in M_i$, which guarantees linear independence of the gatherings of the various power-of-$p$ symmetrized monomials.

For $(9,1,1,1)$, we have $n = 12, k = 4$, and $p = 3$. Here, we compute

$$T^0 = \{\{(9,1,1,1)\}, \{3,3,3,3\}\},$$

$$T^1 = \theta T^0 = \{\{(9,2,1), (10,1,1)\}, \{6,3,3\}\}.$$ Ordering $T^1$ as written above, one choice of $A_1$ is span$\{\tau(9,1,1,1)\}$. A matching choice for $A_2$ is span$(B^1_{3} \setminus \{\tau(9,1,1,1)\})$, which has span$\{\tau(3,3,3,3)\}$ as a subspace, and the relation to preimages by $\theta$ is not coincidental. To use this observation, we must first demonstrate that distinct sets of gatherings $M_i, M_j \in T^m$ are
disjoint for $m < p - 1$, and then we may use our knowledge of basic polynomial arithmetic in $\mathbb{Z}_p[x]$ to show that such extensions are not necessary.

**Lemma 3.3.7:** Given two distinct power-of-$p$ multi-indices $\lambda$ and $\mu$ both of weight $n$ and length $k$, gathering must be applied at least $p - 1$ times before their gatherings have nonempty intersection.

**Proof.** Let $\lambda$ be a carry-minimal multi-index with gathered from $\hat{\lambda} = \bigcup_i \rho_p(\lambda_i)$, and let $\mu$ be some other gathering parent of $\lambda$ of the same weight and length as $\lambda$. We know by Lemma 3.3.3 that $\alpha_p(\mu) = \alpha_p(\lambda) = \alpha_p(\lambda)$, and so gathering cannot combine $p$ copies of $p^k$ into any single entry of $\lambda$. Hence $\mu$ contains as many copies of $p^k$ for any particular $k$ as $\hat{\lambda}$. Since every $\mu$ and $\hat{\lambda}$ are contain only powers of $p$, $\mu = \hat{\lambda}$. \qed

In $\delta_2\tau(10, 1, 1)$, we see summands such as $(x_0 + x_1)^{10}x_2x_3$. These, in turn, have expansions of the form $x_0^{10}x_2x_3 + x_0^9x_1x_2x_3 + x_0x_2^9x_2x_3 + x_2^{10}x_2x_3$ in $\mathbb{Z}_3[x]$. The unmixed terms cancel, hence we need only consider the middle two summands, which take the remarkable form of previous gatherings of $\tau(10, 1, 1)$’s power-of-$p$ parent.

**Theorem 3.3.8:** Under the same conditions as 3.3.6 monomials in the image of gathering of $\tau\lambda m$-many times can be resymmetrized and assigned non-zero coefficients such that the result is a 2-cocycle.

**Proof.** This monomial can be gathered into monomials $m'_1, m'_2, \ldots, m'_l$ with symmetrizations $m_1, \ldots, m_l$. By 3.3.6 these can be assigned non-zero coefficients $c_1, \ldots, c_l$ and extended by some $f$ such that $c_1m_1 + \cdots + c_lm_l + f$ forms a $(k - 1)$-dimension cocycle and $f$ contains no monomials that appear in $m_i$. We argue that $f$ can always be chosen to be 0.

Recall that if $c$’s base-$p$ representation is $\rho_p(c) = (c_1, \ldots, c_l)$, then for all $a, b \in \mathbb{Z}_p$ we have

$$(a + b)^c = \prod_{i \in \{1, \ldots, l\}} (a + b)^{c_i} = \prod_{i \in \{1, \ldots, l\}} (a^{c_i} + b^{c_i}) = \sum_{S \subseteq \{1, \ldots, l\}} a^{\sum_{i \in S} c_i} b^{\sum_{i \in S} c_i}. $$

Using this, the cocycle condition applied to a carry-minimal $\lambda$ with parent $\hat{\lambda} = \bigcup_i \rho_p(\lambda_i)$ will then result in a sum of monomials of the form $\sum_{\mu} c_{\mu}x^\mu$, $c_{\mu} \neq 0$, whose exponents $\mu$ are either a reordering of the multi-index $\lambda \cup \{0\}$ or a gathering of $\hat{\lambda}$ whose length is $\ell(\lambda) + 1$. The $f$ given by the residual terms of $\pi_p c^\mu$ is composed of $(\phi(\lambda) - 1)$-fold gatherings of other power-of-$p$ symmetrized monomials of the same weight and length as $\hat{\lambda}$. By 3.3.7 we then have that the images generated by each power-of-$p$ cocycle are linearly independent under $\delta_2$, and so $\delta_2(c_1m_1 + \cdots + c_lm_l + f) = 0$ implies that $\delta_2(c_1m_1 + \cdots + c_lm_l) = 0$. \qed

### 3.4. Integral Projection

In §3.3 we demonstrated the existence of a wide variety of modular cocycles, using power-of-$p$ multi-indices and the existence of a particular rational cocycle as input. We now show that this exhausts all possible 2-cocycles. Such a statement has two parts: there are no cocycles that do not occur via this process, and cocycles that do occur as part of this process cannot be written as the sum of two “smaller” cocycles for an appropriate interpretation of the word “smaller.” These will actually be proven nearly simultaneously, but we must first frame the question appropriately, beginning by precisely communicating a notion of “smallness,” which we more suggestively name “indecomposable.”

**Definition 3.4.1:** A $k$-variable $m$-cocycle $f$ of degree $n$ is called *indecomposable* if there exists a set partition $\{B_1, B_2\}$ of $B^k_\ell$ with some $f_1 \in \text{span } B_1, f_2 \in \text{span } B_2$ such that $f_1 + f_2 = f$ and $f_1, f_2 \in \ker \delta_m$. $f$ is called *indecomposable* otherwise.

**Lemma 3.4.2:** The set of indecomposable cocycles is a basis for the kernel of $\delta_m$ taken over any field.

**Proof.** First, homogenous $f \in \ker \delta_m$ can be written as the sum of indecomposable cocycles. Note first that for indecomposable $f$ and for symmetrized monomials this is trivially true. Assume instead that $f$ is decomposable, let $B_f \subseteq B^k_\ell$ be such that $f \in \text{span } B_f$, and assume that the lemma holds for all $B_{f'}, \subseteq B_f$. Let
$B_1, B_2, f_1, f_2$ be as in 3.4.1. The inductive hypothesis gives us the existence of $f_1 = \sum_i f_{1,i}$ and $f_2 = \sum_j f_{2,j}$, where $f_{1,i}, f_{2,j}$ are indecomposable cocycles. The desired decomposition is then $f = \sum_i f_{1,i} + \sum_j f_{2,j}$, and inducting over the size of $B_f$ shows that the set of indecomposables spans ker $\delta_m$.

In addition, the set of indecomposables is linearly independent. Assume instead that two indecomposable cocycles $f_1, f_2$ share a particular monomial $f = \sum_{\sigma \in S_k} x^\mu$ with coefficient $b_1$ in $f_1$ and $b_2$ in $f_2$. Then $b_2 f_1 - b_1 f_2$ is a cocycle with a zero coefficient on $f$, and $b_2^{-1} (b_2 f_1 - b_1 f_2) + b_1 f$ is a decomposition of $f_1$. □

When we apply $\delta_m$ to a particular symmetrized monomial $\tau \lambda$ with $\lambda$ not power-of-$p$, we see a sum of image monomials. In order for $\tau \lambda$ to participate in a cocycle, we must include other symmetrized monomials with which we might cancel the image of $\tau \lambda$ to achieve zero. Given an image monomial $x^{(\lambda_0, \ldots, \lambda_k)}$, in the general case of $\delta_m$, the possible parent monomials must be of the form (we will prove this in a moment) $x^{(\lambda_0, \ldots, \lambda_i + \lambda_{i+1}, \ldots, \lambda_k)}$ for some $0 \leq i < m \leq k$. When $m = 2$, we do not have a choice; one of the two parents belongs to the symmetrized monomial we are trying to cancel, and so the other parent is our only choice and we are forced to include it. We can iterate this process on this new summand, and the collection of such multi-indices we call the annihilating set of $\lambda$, which is formally defined as follows:

**Definition 3.4.3:** We define the map $\theta$ from partitions to sets of partitions by the following rule: if $\lambda$ is a partition of length $k$, then for any permutation $\sigma \in S_k$ and corresponding reordering $\sigma \lambda = \lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$, we have $(\lambda_1', \lambda_2', \lambda_3', \ldots, \lambda_k') \in \theta(\lambda)$ exactly when $p_\sigma(\lambda_1') \cup p_\sigma(\lambda_2') = p_\sigma(\lambda_1)$. Define $\Theta(S) = \bigcup_{\lambda \in S} \theta(\lambda)$. The sequence $\Theta^n((\lambda))$ is nondecreasing and bounded, and is thus eventually constant with value denoted Ann $\lambda$, called the annihilating set of $\lambda$.

This definition takes into account our observation from 3.3.8 concerning $(a + b)^c$ for $a, b \in \mathbb{Z}_p$; we need not consider splittings $\lambda_1' + \lambda_2' = \lambda_1$ that do not occur as $p_\sigma(\lambda_1') \cup p_\sigma(\lambda_2') = p_\sigma(\lambda_1)$. We compute some sample annihilator sets of degree 12, dimension 3, and characteristic 3 below:

- $\text{Ann}(9, 2, 1) = \{(9, 2, 1), (10, 1, 1)\}$
- $\text{Ann}(6, 3, 3) = \{(6, 3, 3)\}$
- $\text{Ann}(4, 4, 4) = \{(4, 4, 4), (5, 4, 3), (6, 4, 2), (6, 5, 1), (7, 3, 2), (7, 4, 1), (8, 3, 1)\} \cup \text{Ann}(9, 2, 1) \cup \text{Ann}(6, 3, 3)$
- $\text{Ann}(5, 5, 2) = \{(5, 5, 2), (8, 2, 2)\} \cup \text{Ann}(4, 4, 4)$

Now, we demonstrate that these sets actually capture what we want:

**Lemma 3.4.4:** Any linear combination of symmetrized monomials lying in ker $\delta_2$ containing $\tau(\lambda)$ for some partition $\lambda$ will also contain each of $\tau(\lambda')$ for $\lambda' \in \text{Ann } \lambda$.

*Proof.* $\delta_2(\tau \lambda)$ will contain $x^{\mu, \mu} = (\lambda_1', \lambda_2', \lambda_3, \ldots, \lambda_k)$ for every $p_\sigma(\lambda_1') \cup p_\sigma(\lambda_2') = p_\sigma(\lambda_1)$ by the reduced binomial expansion noted in 3.3.8. The preimage of $x^{\mu}$ by $\delta_2$ contains at most $\lambda$ and the partition $$(\lambda_1', \lambda_2', \lambda_3, \ldots, \lambda_k) \in \nu,$$the latter when $\alpha_p(\lambda_1') = 0$. This is because the third term of $\delta_2(\tau(\lambda'))$ will be of the form $$x_{\lambda_1'}^\lambda (x_1 + x_2)^{\lambda_1'}, x_3^{\lambda_2}, x_4^{\lambda_3}, \ldots x_k^{\lambda_k}.$$Therefore if $x^{\mu}$ is to vanish then $\tau \nu$ must appear in linear combination with $\tau \lambda$. This is exactly the definition of $\nu \in \text{Ann } \lambda$. □

Problems arise when $p_\sigma(\lambda_1') \cup p_\sigma(\lambda_2') \neq p_\sigma(\lambda_1' + \lambda_2')$, since then $\nu$ cannot contribute the requisite cancelling monomial to the image. This happens when $\alpha_p(\lambda_1') \cdot \alpha_p(\lambda_2') > 0$, or equivalently when $\alpha_p(\nu) < \alpha_p(\lambda)$. This happens strikingly often; suppose we begin with the partition $(4, 4, 4)$ and set $\nu = 3$. Then we can split $p_\sigma(4) = (3, 1)$ as $\{1\} \cup \{3\}$ and form an element $(1, 3 + 4, 4) = (1, 7, 4) \in \theta(4, 4, 4) \subseteq \Theta^1(\{(4, 4, 4)\})$. $(1, 7, 4)$ can be reordered as $(4, 7, 1)$ and then $p_\sigma(4)$ can again be split as $\{1\} \cup \{3\}$, giving an element $(1, 3 + 7, 1) = (1, 10, 1) \in \theta(4, 7, 1) \subseteq \Theta^2(\{(4, 4, 4)\}) \subseteq \text{Ann}(4, 4, 4)$. Since $\alpha_3(10, 1, 1) = 1$ and $\alpha_3(4, 4, 4) = 2$, we have constructed our desired $\nu$ with $\alpha_p(\nu) < \alpha_p(\lambda)$ and $\nu \in \text{Ann } \lambda$. This same game can actually be played with every non-carry-minimal partition, which gives us the first half of our exhaustiveness argument:
Theorem 3.4.5: If $\lambda$ is a non-carry-minimal partition in base $p$ and has carry-count $\alpha_p(\lambda)$, there exists an $\lambda' \in \text{Ann} \lambda$ with $\alpha_p(\lambda') < \alpha_p(\lambda)$.

Proof. The nearest (in terms of splitting distance) power-of-$p$ partition for which $\lambda$ may be gathered is given by $\bigcup \rho_p(\lambda) = \lambda$. Because $\lambda$ is not carry minimal, there exists–as in the proof of 3.3.2–a partition $\mu$ which is power-of-$p$ with $\ell(\lambda) \leq \ell(\mu) < \ell(\lambda)$ and $|\lambda| = |\mu|$ that is a $(p - 1)$-fold gathering of $\lambda$. Let $p^k$ be a power of $p$ disturbed in the gathering process to form $\mu$ from $\lambda$. Noting that there must be at least $p$ copies of $p^k$ present in $\lambda$, we can iteratively separate out the copies of $p^k$ in our original partition, $\lambda$.

Borrowing the notation of the construction from 3.4.4, we begin by permuting $\lambda$ such that $\lambda^k \in \rho_p(\lambda_{\sigma_1})$, then $\lambda'$ to be all the copies of $\lambda$ in $\rho_p(\lambda_{\sigma_1})$ and $\lambda''$ to be everything else (i.e., $\lambda'_1 + \lambda'' = \lambda_{\sigma_1}$), then $\lambda^k$ to be everything else (i.e., $\lambda'_1 + \lambda'' = \lambda_{\sigma_1}$) and then permuting by the cycle $\sigma = (1 2)$, we then call this freshly constructed partition $\lambda$.

At each step we select some $\sigma ∈ S_{\ell(\lambda)}$ such that $2$ is undisturbed and $p^k \in \rho_p((\sigma \lambda)_1)$. We then reverse the above construction, splitting the sum of all copies of $p^k$ present into $(\sigma \lambda)_1$ with $\ell(\lambda)$ and the remainder into $\lambda'_1$, then collecting $\lambda''$ with the $p^k$ accumulating in $\lambda_2$, each time generating a new multi-index $(\lambda'_1, \lambda'' + \lambda_2, \ldots, \lambda_k)$ that lies in $\text{Ann} \lambda$ (with the same caveat about $\lambda_1 = \bigcup_{k=1}^p(p^k)$ for some $j$). After at most $p$ many steps, $\lambda_2 \geq p^k + 1$, which constructs a partition in $\text{Ann} \lambda$ with carry-count reduced by 1. \hfill □

The second half of the argument lies in noting the following invariant of $\delta_m$:

Lemma 3.4.6: Let $\lambda$ be a partition, and select $\mu$ such that the coefficient $c_{\mu}$ is nonzero in

$$\delta_m(\tau \lambda) = \sum_{\mu} c_{\mu} \cdot (\tau \mu).$$

Then $\alpha_p(\lambda) = \alpha_p(\mu)$.

Proof. Let $\lambda'_1, \lambda''$ be such that $\mu = (\lambda \setminus (\lambda_1)) \cup (\lambda'_1, \lambda''')$.

Then,

$$\alpha_p(\mu) = \alpha_p(\lambda'_1, \lambda''', \lambda_2, \ldots, \lambda_k) = \alpha_p(\lambda'_1, \lambda'') + \alpha_p(\lambda_1, \ldots, \lambda_k) = 0 + \alpha_p(\lambda),$$

where the last equality stems from noticing that $\rho_p(\lambda'_1) \cup \rho_p(\lambda'') = \rho_p(\lambda_1)$, as remarked upon in 3.3.8 \hfill □

Theorem 3.4.7: If $\lambda$ is not a $p$-carry-minimal partition, then $\tau \lambda$ cannot participate in a cocycle.

Proof. By 3.4.5, we have that each non-carry-minimal partition's annihilating set contains another of strictly lower carry-count. If we follow the construction of $\text{Ann} \lambda$ using definition 3.4.3, there must exist partitions $\lambda', \lambda'' \in \text{Ann} \lambda$ such that $\lambda''$ is required to cancel an image monomial of $\lambda'$, and $\alpha_p(\lambda'') < \alpha_p(\lambda')$. Since by 3.4.6, all of the monomials in $\delta_2 \tau \lambda' \lambda''$ have carry-counts distinct from those of $\delta_2 \tau \lambda'$, they cannot cancel each other, and in turn $\tau \lambda$ cannot participate in a cocycle. \hfill □

Corollary 3.4.8: Let $\{\beta_i\}_i$ be the indecomposable basis associated to the subspace of cocycles of dimension $k$, degree $n$, and characteristic $p$. Then $\pi_p(\zeta_k^n) = \sum_i a_i \beta_i$, where the $a_i$ are all non-zero.

Proof. Immediate from the alternative expansions of $\zeta_k^n$ noted after 3.2.6 and its decomposition into a sum of indecomposables. \hfill □

In addition to the exhaustiveness above, we can also use these annihilating sets to achieve indecomposability of symmetrized gatherings of 3.3.8.

Theorem 3.4.9: Let $T$ be a set in $T^m(n, k)$ (as defined in 3.3.8), where $m$, $n$, and $k$ satisfy the conditions of 3.3.8. Then for every $\lambda \in T$, $\text{Ann} \lambda = T$. 

20
Proof. For a fixed weight $n$ and length $k$, we define a function $d$ on unordered partitions of this type that takes a pair $(\lambda, \mu)$ to the number of slots in which $\lambda$ and $\mu$ differ. Then, for distinct $\lambda, \mu \in T$, it suffices to show that there is a $\lambda' \in T \cap \text{Ann} \lambda$ such that $d(\lambda', \mu)$ is strictly less than $d(\lambda, \mu)$. Under the conditions imposed in 3.3.8 which mean to prevent any $p$ copies of a particular $p^k$ from being summed together during the gathering procedure used to form $T$, this is obvious. Induction then yields that $\mu \in \text{Ann} \lambda$ and $\text{Ann} \lambda = T$.

Corollary 3.4.10: The cocycles resulting from 3.3.8 are indecomposable.

Proof. Immediate from 3.4.9, 3.4.4, and 3.3.7.

3.5. Counting Additive 2-Cocycles

In the end, we are studying additive cocycles with intent to eventually investigate the multiplicative cocycles, so that we may in turn apply these results to maps in algebraic topology. The rank of these maps is related to the number of multiplicative cocycles present in a particular degree and dimension, which is in turn bounded from above by the number of additive cocycles present in the same degree and dimension (a statement made precise in §2.1). The number-theoretic properties of the additive cocycles suggests a particular way to count them using generating functions, for which we give a construction below.

Definition 3.5.1: We define $C_{nk}^p \in \mathbb{Z}$ to be the coefficients of the generating function

$$\prod_{i=0}^{\infty} (1 - tx^{p^i})^{-1} = \sum_{n,k} C_{nk}^p x^n t^k.$$

Lemma 3.5.2: $C_{nk}^p$ equals the number of ways to write $n$ as a sum of $k$ many powers of $p$.

Proof. A factor of the product looks like

$$\left(1 - tx^{p^i}\right)^{-1} = \sum_{j=0}^{\infty} t^j x^{jp^i}.$$

Expanding these products reveals that for particular $n$ and $k$, the summands contributing to $C_{nk}^p$ have the form $t^k x^n$ with $n = \sum_{m=1}^{k} a_m p^m$ for $a_m \in \mathbb{N}_0$.

These summations indeed correspond to cocycles, the proof of which is merely a summation of everything that’s led to this point.

Theorem 3.5.3: In a particular degree $n$ and number of variables $k$, if a power-of-$p$ multi-index exists, the restriction of $\delta_2$ to $k$-variable $n$-degree symmetric polynomials has kernel spanned by

$$\{\tau(\lambda) \mid \lambda \text{ is a power-of-}p \text{ multi-index}, \ell(\lambda) = k, |\lambda| = n\}.$$

Proof. Using 3.3.3 and 3.3.5, we have that exactly the power-of-$p$ multi-indices are $p$-carry minimal. By our classification in 3.4.8 we have that they are exhaustive of all 2-cocycles in the degree and dimension to which they belong, and because they are composed of single symmetrized monomials, they are trivially indecomposable.

Corollary 3.5.4: $C_{nk}^p$ count the number of $n$-degree $k$-dimensional cocycles when $C_{nk}^p \neq 0$.

Proof. Immediate from 3.5.2 and 3.5.3.

When working in $\mathbb{Z}_2$, the generating function is especially nice, since every number $n$ has a power-of-2 representation of length $k$ for every $\sigma_2(n) \leq k \leq n$.

Lemma 3.5.5: For $\sigma_2(n) \leq k \leq n$, $C_{nk}^2$ is always non-zero.
Proof. As discussed in the proof of 3.3.3, power-of-p multi-indices for a particular degree \( n \) begin in dimension \( n \) and occur for every dimension \( n - c(p-1), \) \( c \in \mathbb{N}_0. \) For \( p = 2, \) this means a power-of-2 multi-index occurs in every dimension in the range \( \sigma_2(n), \ldots, n. \)

However, the general case does not appear to be so well off, since there are lengths and weights for which no sum of powers of 3 can be written. For instance, \((3, 1, 1, 1)\) and \((3, 3)\) have lengths 4 and 2 respectively and both has weight 6, but there exists no power-of-3 multi-index of weight 6 and length 3. Pleasantly enough, because the gathering operation allows us to determine the presence of these intermediate cocycles knowing only what the kernel looks like in locations where power-of-p multi-indices do exist, we can extend \( C_{nk}^p \) to cover these middle cases as well.

**Theorem 3.5.6:** Define \( D_{nk}^p \) to be \( C_{nk}^p \) when \( C_{nk}^p \) is non-zero, to be \( D_{n(k+1)}^p \) when \( C_{nk}^p \) is zero and \( k < n, \) and 0 otherwise. Then \( D_{nk}^p \) counts the number of cocycles in \( \mathbb{Z}_p \) of degree \( n \) and dimension \( k. \)

Proof. This is just successive application of the results 3.3.7, 3.4.8 and 3.4.10.

### 3.6. The Generalized Lazard Ring

Lazard demonstrated a ring isomorphism between the universal representing ring for two variable 2-cocycles and a polynomial ring on countably many generators, a celebrated result in the theory of formal group laws. Here we provide a similar result for the representing ring of \( k \)-variable 2-cocycles.

To begin, since the representing ring selects cocycles over an arbitrary ring \( A, \) we must demonstrate that our knowledge about the \( \mathbb{Q} \) and \( \mathbb{Z}_p \) cases is sufficient to determine the rest of the story for arbitrary commutative rings.

**Theorem 3.6.1:** Let \( A \) be an abelian group and let \( f \in A \otimes \mathbb{Z}[x] \) be a \( k \)-variable symmetric 2-cocycle of homogenous degree \( n. \) Then \( f \) is of the form

\[
    f = \sum_i a_i \otimes \beta_i(x),
\]

where \( a_i \in A \) and \( \beta_i \) is the relevant indecomposable basis of 3.4.2.

Proof. We begin by making a number of standard reductions. First, since only finitely many terms will appear in \( f, \) it is sufficient to prove the theorem when \( A \) is finitely generated. Then, for two abelian groups \( A \subseteq B, \) if the theorem is true for \( B \) then it is also true for \( A. \) This implies in addition that if the theorem is true for arbitrary \( A \) and \( B \) if and only if it is true for \( A \oplus B. \) Using the structure theorem for finitely generated abelian groups, we have reduced to the cases \( A = \mathbb{Z} \) and \( A = \mathbb{Z}_p \) for a prime \( p \) and positive \( l. \)

Using the inclusion property, we can produce the result for \( \mathbb{Z} \) by proving it for \( \mathbb{Q} \supseteq \mathbb{Z}. \) The authors of \[AHS01\] have shown that all symmetric \( k \)-variable 2-cocycles over \( \mathbb{Q} \) of homogenous degree \( n \) are of the form \( a \cdot \zeta^k_n \) for \( a \in \mathbb{Q}, \) and \( \zeta^k_n \) has a decomposition into indecomposables by 3.4.8. We then can decompose the \( \mathbb{Z}_p \) case inductively; we have demonstrated a classification for \( l = 1 \) above, and so we assume that we have accomplished the classification up to some \( l \geq 1. \) An \( f \) with coefficients in \( \mathbb{Z}_{p^{l+1}} \) must be of the form

\[
    f = \sum_i a_i \otimes \beta_i + p^l f'
\]

for some \( f', \) which we can think of as a symmetric 2-cocycle over \( \mathbb{Z}_p. \) We can then again decompose \( f' \) into a sum of indecomposables and collect coefficients, giving the desired decomposition of \( f. \)

Since we have now shown that all cocycles take our prescribed form, the only piece of the puzzle left is to actually construct the ring, and we do so in steps.

**Theorem 3.6.2:** The representing ring for symmetric \( k \)-variable 2-cocycles is a tensor of polynomial rings, corrected for torsion.
Proof. Fix a homogenous degree \( n \) and number of variables \( k \). Then the representing ring for symmetric 2-cocycles in \( k \) variables of this homogenous degree are selected by the coefficients \( a_i \) in \ref{3.6.1}. If we denote the coefficient of \( \zeta^n_k \) as \( b_n \) and the coefficient of the polynomial \( \beta_i \) in the characteristic \( p \) indecomposable basis as \( c_{p,i} \), where \( i \) ranges over the integers \( \{0, \ldots, l_{n,p}\} \), then our representing ring is given by

\[
L^n_k = \mathbb{Z}[b_n] \otimes \left( \bigotimes_{\text{prime } p} \mathbb{Z}_p[c_{p,i}] \langle pc_{p,i} \rangle \right).
\]

Here we drop the zeroth indecomposable basis element because, as noted in \ref{3.4.8}, \( \beta_0 = \zeta^n_k - \sum_{i\neq 0} \beta_i \).

These rings \( L^n_k \) can then be tensored together to form \( L_k = \bigotimes_n L^n_k \), the representing ring for symmetric 2-cocycles in \( k \) variables.

It is worth noting that when \( k = 2 \) we cover the classic result \( L_2 = \mathbb{Z}[b_2, b_3, b_4, \ldots] \), since the innermost tensor product vanishes.

3.7. For Higher \( m \)

Many of the results in this paper were presented in the context of \( \delta_2 \), but in fact yield results for \( \delta_m \) with \( m > 2 \) as well.

**Lemma 3.7.1:** If \( f \), a symmetric \( k \)-variable polynomial, is both an \( n \)-cocycle and an \( m \)-cocycle, then \( f \) is also an \( n+ m \)-cocycle (provided \( n+ m < k \)) and an \( |n- m| \)-cocycle (provided \( n \neq m \)).

**Proof.** Assume \( n + m < k \), and consider the unreduced sum \( \delta_{n+m} f \). The first \( n + 1 \) terms of this sum can be reduced to \( f(x_0, \ldots, x_{n-1}, x_{n+1}, \ldots, x_k) \) by applying the \( n \)-cocycle condition. Then, the remaining \( m + 2 \) summands can be reduced to zero using the \( m \)-cocycle condition.

Take \( m < n \) for simplicity, so \( n - m > 0 \). First, we know that \( \delta_n f = 0 \), and again we work with the unreduced sum of \( \delta_n f \). We can replace the last \( m + 1 \) terms of the sum with \( f(x_0, \ldots, x_{n-1}, x_{n-m}, \ldots, x_k) \), and the residual sum forms exactly \( \delta_{n-m} f \). Transitivity shows that \( f \in \ker \delta_{n-m} \).

**Corollary 3.7.2:** If \( f \) is a symmetric \( k \)-variable \( m \)-cocycle, then it is a symmetric \((cm)\)-cocycle for all \( c \) with \( c \cdot m \leq k \).

**Proof.** Take \( n = m \) and apply the first part of \ref{3.7.1} inductively. \( \Box \)

In particular, \ref{3.4} relies on \( m = 2 \), which allows us to limit the number of parents an image monomial has and make the annihilating set construction (see \ref{3.4.4}). This means that the exhaustivity of our classification here cannot be directly generalized to all \( m \) that satisfy \( 2 \mid m \), though the existence of these gathered cocycles is guaranteed by \ref{3.7.2}.

Using Mathematica, we’ve been able to explore \( m > 2 \) for relatively small \( m \); because \( \delta_m \) only applies to polynomials of dimension at least \( m \), the calculations grow unreasonably slow fairly quickly. Nonetheless, it is our conjecture that the exhaustiveness of gathering is in fact true for all even \( m \). In addition, these gathered cocycles appear to vanish for odd \( m \), leaving only the power-of-\( p \) symmetrized monomials behind.
## A. Tables of Modular Additive 2-Cocycles

Here we provide comma delimited lists of modular symmetric 2-cocycles, ordered in rows by degree and in columns by dimension.

### A.1. Characteristic 2

| deg 2 | dim 2 | 3   | 4   | 5   | 6   |
|-------|-------|-----|-----|-----|-----|
| τ(1, 1) | τ(1, 1, 1) | 0  | 0  | 0  | 0  |
| τ(2, 1) | τ(2, 1, 1) | τ(1, 1, 1) | 0  | 0  | 0  |
| τ(2, 2) | τ(2, 1, 1) | τ(1, 1, 1, 1) | τ(1, 1, 1, 1) | 0  | 0  |
| τ(4, 1) | τ(2, 2, 1) | τ(2, 1, 1, 1) | τ(2, 1, 1, 1, 1) |
| τ(4, 2) | τ(4, 1, 1) | τ(2, 2, 1, 1) | τ(2, 1, 1, 1, 1) |
| τ(4, 3) | τ(4, 1, 1) | τ(2, 2, 1, 1) | τ(2, 1, 1, 1, 1) |
| τ(4, 4) | τ(4, 2, 1) | τ(2, 2, 1, 1) | τ(2, 2, 2, 1, 1) |
| τ(8, 1) | τ(4, 3, 1) | τ(1, 1, 1, 1) | τ(1, 1, 1, 1, 1) |
| τ(8, 2) | τ(4, 4, 1) | τ(2, 2, 2, 1, 1) | τ(2, 2, 2, 1, 1) |
| τ(8, 3) | τ(8, 1, 1) | τ(2, 2, 2, 1, 1) | τ(4, 1, 1, 1, 1) |
| τ(8, 4) | τ(8, 2, 1) | τ(2, 2, 2, 1, 1) | τ(4, 1, 1, 1, 1) |
| τ(12, 1) | τ(8, 3, 1) | τ(2, 2, 2, 1, 1) | τ(4, 1, 1, 1, 1) |
| τ(12, 2) | τ(8, 4, 1) | τ(2, 2, 2, 1, 1) | τ(4, 1, 1, 1, 1) |
| τ(12, 3) | τ(8, 4, 2) | τ(2, 2, 2, 1, 1) | τ(4, 1, 1, 1, 1) |
| τ(12, 4) | τ(8, 4, 3) | τ(2, 2, 2, 1, 1) | τ(4, 1, 1, 1, 1) |
| τ(14, 1) | τ(8, 4, 4) | τ(2, 2, 2, 1, 1) | τ(4, 1, 1, 1, 1) |
### A.2. Characteristic 3

| deg 2 | dim 2 | 3      | 4      | 5      | 6      |
|-------|-------|--------|--------|--------|--------|
| τ(1,1) | 0     | 0      | 0      | 0      | 0      |
| τ(2,1) | τ(1,1,1) | 0     | 0      | 0      | 0      |
| τ(3,1) | τ(2,1,1) | τ(1,1,1) | 0      | 0      | 0      |
| τ(3,2) | τ(3,1,1) | τ(2,1,1,1) | τ(1,1,1,1) | 0      |        |
| τ(3,3) | τ(3,2,1) | τ(3,1,1) | τ(2,1,1,1) | τ(1,1,1,1) | 0      |
| τ(4,1) | τ(4,1,1) | τ(3,2,1,1) | τ(1,1,1,1) | τ(2,1,1,1) | 0      |
| τ(6,1) | τ(4,1,1) | τ(3,2,1,1) | τ(3,1,1,1) | τ(2,1,1,1) | 0      |
| τ(6,2) | τ(6,1,1) | τ(3,3,1,1) | τ(3,2,1,1) | τ(3,1,1,1) | τ(2,1,1,1) |
| τ(4,4) | τ(4,3,1) | τ(3,3,1,1) | τ(3,2,1,1) | τ(3,1,1,1) | τ(2,1,1,1) |
| τ(7,1) | τ(3,3,2) | τ(3,3,1,1) | τ(3,2,1,1) | τ(3,1,1,1) | τ(2,1,1,1) |
| τ(5,3) | τ(3,3,3) | τ(3,1,1,1) | τ(3,2,1,1) | τ(3,1,1,1) | τ(2,1,1,1) |
| τ(9,1) | τ(4,3,3) | τ(3,3,3) | τ(6,1,1,1) | τ(4,1,1,1) | τ(3,1,1,1) |
| τ(10,1) | τ(6,3,1) | τ(3,3,3) | τ(3,3,3,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(9,2) | τ(9,1,1) | τ(6,1,1,1) | τ(4,3,3,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(10,2) | τ(10,1) | τ(4,3,3,1) | τ(3,3,3,2) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(9,3) | τ(6,3,3) | τ(9,2,1) | τ(6,3,1,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(10,3) | τ(6,3,3) | τ(9,1,1) | τ(4,3,3,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(9,4) | τ(9,2,1) | τ(10,1) | τ(3,3,3,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(10,4) | τ(9,3,1) | τ(4,3,3) | τ(3,3,3,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(12,1) | τ(9,3,1) | τ(9,3,1) | τ(6,3,1,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(12,2) | τ(12,1) | τ(4,3,3,1) | τ(3,3,3,2) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(13,1) | τ(11,3) | τ(10,3,1) | τ(9,2,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(11,3) | τ(10,4) | τ(9,4,1) | τ(9,1,1) | τ(3,3,3,1) | τ(3,3,3,1) |
| τ(9,5) | τ(9,6) | τ(6,3,3) | τ(3,3,3,3) | τ(3,3,3,3) | τ(3,3,3,3) |
| τ(12,3) | τ(9,3,3) | τ(9,3,3) | τ(6,3,3,3) | τ(3,3,3,3) | τ(3,3,3,3) |
| τ(12,2) | τ(12,1) | τ(9,3,3) | τ(9,3,3) | τ(6,3,3,3) | τ(3,3,3,3) |
| τ(13,2) | τ(9,6) | τ(9,6) | τ(6,3,3,3) | τ(9,3,3) | τ(9,3,3) |
| τ(12,4) | τ(10,3,3) | τ(10,6) | τ(9,4,3) | τ(9,4,3) | τ(9,4,3) |
### A.3. Characteristic 5

| deg | dim 2 | 3       | 4       | 5       | 6       |
|-----|-------|---------|---------|---------|---------|
| 2   | 1·τ(1,1) | 0       | 0       | 0       | 0       |
| 3   | 1·τ(2,1) | 1·τ(1,1,1) | 0 | 0       | 0       |
| 4   | 1·τ(2,2)+ 4·τ(3,1) | 1·τ(2,1,1) | 1·τ(1,1,1) | 0       |
| 5   | 1·τ(3,2)+ 3·τ(4,1) | 1·τ(2,1,1) | 1·τ(1,1,1,1) | 0       |
| 6   | 1·τ(5,1) | 1·τ(2,2,2)+ 2·τ(4,1,1)+ 4·τ(3,2,1) | 1·τ(2,1,1,1) | 1·τ(1,1,1,1,1) | 0       |
| 7   | 1·τ(5,2)+ 2·τ(6,1) | 1·τ(2,2,1)+ 2·τ(4,1,1)+ 4·τ(3,2,1) | 1·τ(2,1,1,1,1) | 0       |
| 8   | 1·τ(5,3)+ 3·τ(6,2)+ 3·τ(7,1) | 1·τ(5,1,1,1) | 1·τ(2,2,1,1,1)+ 1·τ(2,1,1,1,1,1)+ 4·τ(3,1,1,1,1) | 0       |
| 9   | 1·τ(5,4)+ 1·τ(7,2)+ 4·τ(6,3)+ 4·τ(8,1) | 1·τ(5,2,1,1)+ 2·τ(4,1,1,1,1)+ 4·τ(3,2,1,1,1) | 0       |
| 10  | 1·τ(5,5) | 1·τ(5,3,2)+ 2·τ(6,3,1)+ 2·τ(8,1,1)+ 3·τ(5,4,1)+ 3·τ(6,2,2)+ 3·τ(7,2,1) | 1·τ(5,2,1,1,1)+ 2·τ(6,1,1,1,1) | 0       |
| 11  | 1·τ(6,5)+ 3·τ(10,1) | 1·τ(5,2,2,2)+ 2·τ(6,2,1,1)+ 2·τ(7,1,1,1)+ 4·τ(5,3,1,1) | 1·τ(5,2,1,1,1)+ 2·τ(6,1,1,1,1) | 0       |
| 12  | 1·τ(6,6)+ 1·τ(7,5)+ 3·τ(11,1)+ 4·τ(10,2) | 1·τ(5,5,2)+ 1·τ(10,1,1)+ 2·τ(6,5,1) | 1·τ(5,2,2,1)+ 2·τ(6,2,1,1,1)+ 2·τ(7,1,1,1,1)+ 4·τ(5,3,1,1,1) | 0       |

...
B. Notation

\[ \mathbb{N}_0 = \mathbb{N} \cup \{0\} \quad \{0, 1, 2, 3, \ldots\} \]

\[ \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} \quad \text{the field with } p \text{ elements.} \]

\[ S_k \quad \text{the symmetric group on } k \text{ symbols.} \]

\[ \lambda \cup \mu \quad \text{the multi-index } (\lambda, \mu) \]

\[ \lambda \setminus \mu \quad \text{the unique operation satisfying } (\lambda \setminus \mu) \cup \mu = \lambda \text{ up to order} \]

\[ x = (x_1, \ldots, x_k) \quad \text{a } k\text{-tuple of variables.} \]

\[ A[x] \quad \text{the ring of polynomials in the } x_i \in x \text{ over } A. \]

\[ A[[x]] \quad \text{the ring of power-series in the } x_i \in x \text{ over } A. \]

\[ \lambda! = \prod \lambda_i! \quad \text{the partition factorial} \]

\[ \binom{n}{\lambda} = \frac{n!}{\lambda!} \quad \text{the multinomial coefficient of } \lambda. \]

\[ \lambda \vdash n \quad \lambda \text{ is a partition of } n. \]

\[ \zeta_k^n \quad \text{the unique rational } 2\text{-cocycle of degree } n \text{ in } k \text{ variables.} \]

\[ \tau\lambda, \tau(\lambda) \quad \text{the monomial symmetric function associated to } \lambda. \]

\[ \delta_m \quad \text{the (additive) } m\text{-coboundary map.} \]

References

[AHS01] Ando, M. et al., *Elliptic spectra, the Witten genus and the theorem of the cube*. Inventiones Mathematicae, 2001.

[AS01] Ando, M., Strickland, N., *Weil pairings and Morava K-theory*. Topology, 2001.

[Bre83] Breen, L., *Fonctions thêta et théorème du cube*. Springer Lectures Notes in Mathematics v. 980, 1983.

[Kum852] Kummer, E. E. *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*. J. Reine Angew. Math., 1852.

[Laz55] Lazard, M. *Sur les groupes de Lie formels à un paramètre*. Bull. Soc. Math., 1955.

[Tate57] Tate, J. *Homology of Noetherian Rings and Local Rings*. Ill. J. of Math., 1957.