An A_∞-structure on the cohomology ring of the symmetric group S_p with coefficients in $\mathbb{F}_p$

Bachelor thesis

in partial fullfillment of the requirement for the degree of
Bachelor of Science in Mathematics

Universität Stuttgart

Stephan Schmid
November 2012

Contents

0.1. Introduction

A_∞-algebras Let R be a commutative ring. Let A be a $\mathbb{Z}$-graded R-module. Let $m_1 : A \to A$ be a graded map of degree 1 with $m_1^2 = 0$, i.e. a differential on A. Let $m_2 : A \otimes A \to A$ be a graded map of degree 0 satisfying the Leibniz rule, i.e.

$$m_1 \circ m_2 = m_2 \circ (m_1 \otimes 1 + 1 \otimes m_1).$$

The map m_2 is in general not required to be associative. Instead, we require that for a morphism $m_3 : A^{\otimes 3} \to A$, the following identity holds.

$$m_2 \circ (m_2 \otimes 1 - 1 \otimes m_2) = m_1 \circ m_3 + m_3 \circ (m_1 \otimes 1^{\otimes 2} + 1 \otimes m_1 \otimes 1 + 1^{\otimes 2} \otimes m_1)$$

Following Stasheff, cf. [21], this can be continued in a certain way with higher multiplication maps to obtain a tuple of graded maps $(m_n : A^{\otimes n} \to A)_{n\geq 1}$ of certain degrees satisfying the Stasheff identities, cf. (11). The tuple $(A, (m_n)_{n\geq 1})$ is then called an A_∞-algebra.

A morphism of A_∞-algebras from $(A', (m'_n)_{n\geq 1})$ to $(A, (m_n)_{n\geq 1})$ is a tuple of graded maps $(f_n : A'^{\otimes n} \to A)_{n\geq 1}$ of certain degrees satisfying the identities (12). The first two of these are

$$\begin{array}{ll} (12)[1]: & f_1 \circ m_1' = m_1 \circ f_1 \\ (12)[2]: & f_1 \circ m_2' - f_2 \circ (m_1' \otimes 1 + 1 \otimes m_1') = m_1 \circ f_2 + m_2 \circ (f_1 \otimes f_1). \end{array}$$

The specific form of the Stasheff identities and of (12) is motivated by the bar construction. It relates the A_∞-structures on a $\mathbb{Z}$-graded R-module A bijectively to the coalgebra differentials of degree 0 on the graded tensor coalgebra TA. It relates morphisms of A_∞-algebras from $(A', (m_n')_{n\geq 1})$ to $(A, (m_n)_{n\geq 1})$ bijectively to the morphisms of graded differential coalgebras from TA' to TA of degree 0.

A morphism $f = (f_n)_{n\geq 1}$ of A_∞-algebras from $(A', (m_n')_{n\geq 1})$ to $(A, (m_n)_{n\geq 1})$ contains a morphism of complexes $f_1 : (A', m_1') \to (A, m_1)$. We say that f is a quasi-isomorphism of A_∞-algebras if f_1 is a quasi-isomorphism. Furthermore, there is a concept of homotopy for A_∞-morphisms, cf. e.g. [12, 3.7] and [16, Définition 1.2.1.7].

History The history of A_∞-algebras is outlined in [12] and [13].

As already mentioned, Stasheff introduced A_∞-algebras in 1963.

If R is a field, we have the following basic results on A_∞-algebras, which are known since the early 1980s.

- Each quasi-isomorphism of A_∞-algebras is a homotopy equivalence, cf. [20], [10], ...
- The minimality theorem: Each A_∞-algebra $(A, (m_n)_{n\geq 1})$ is quasi-isomorphic to an A_∞-algebra $(A', \{m_n'\}_{n\geq 1})$ with $m_1' = 0$, cf. [9], [8], [20], [5], [7], [18], ... The A_∞-algebra A' is then called a minimal model of A.

Keller established a connection between A_∞-algebras and representation theory in the early 2000s, cf. [11], [12, 7.7] and also [16, §7]: Given an $\mathbb{F}$-algebra B over a field $\mathbb{F}$ and B-modules $M_1, \ldots, M_n$, consider the full subcategory of B-modules given by the B-modules which have a finite filtration such that all quotients are isomorphic to some M_i. Set $M = \oplus_{i=1}^n M_i$ and choose a projective resolution $\mathrm{PRes}\, M$ of M. The homology of the dg-algebra $\mathrm{Hom}_B^*(\mathrm{PRes}\, M, \mathrm{PRes}\, M)$ is the Yoneda algebra $\mathrm{Ext}_B^*(M, M)$. Construct an A_∞-structure on $\mathrm{Ext}_B^*(M, M)$ such that $\mathrm{Ext}_B^*(M, M)$ becomes a minimal model of the dg-algebra $\mathrm{Hom}_B^*(\mathrm{PRes}\, M, \mathrm{PRes}\, M)$. Now $\mathrm{Ext}_B^*(M, M)$ together with its A_∞-structure is all that is necessary for reconstructing the subcategory mentioned above.

For the purpose of this introduction, we will call such an A_∞-structure on $\mathrm{Ext}_B^*(M, M)$ the canonical A_∞-structure on $\mathrm{Ext}_B^*(M, M)$, which is unique up to isomorphisms of A_∞-algebras, cf. [12, 3.3].

This structure has been calculated or partially calculated in several cases.

Let p be a prime.

For an arbitrary field $\mathbb{F}$, Madsen computed the canonical A_∞-structure on $\mathrm{Ext}^*_{\mathbb{F}[\alpha]/(\alpha^n)}(\mathbb{F}, \mathbb{F})$, where $\mathbb{F}$ is the trivial $\mathbb{F}[\alpha]/(\alpha^n)$-module, cf. [17, Appendix B.2]. This can be used to compute the canonical A_∞-structure on the group cohomology $\operatorname{Ext}^*_{\mathbb{F}_p\mathrm{C}_m}(\mathbb{F}_p, \mathbb{F}_p)$, where $m \in \mathbb{Z}_{\geq 1}$ and C_m is the cyclic group of order m, cf. [22, Theorem 4.3.8].

Vejdemo-Johansson developed algorithms for the computation of minimal models, cf. [22]. He applied these algorithms to compute large enough parts of the canonical A_∞-structures of the group cohomologies $\operatorname{Ext}^*_{\mathbb{F}_2\mathrm{D}_8}(\mathbb{F}_2, \mathbb{F}_2)$ and $\operatorname{Ext}^*_{\mathbb{F}_2\mathrm{D}_{16}}(\mathbb{F}_2, \mathbb{F}_2)$ to distinguish them, where D_8 and D_{16} denote dihedral groups. He stated a conjecture on the complete A_∞-structure on $\operatorname{Ext}^*_{\mathbb{F}_2\mathrm{D}_8}(\mathbb{F}_2, \mathbb{F}_2)$. Furthermore, he computed parts of the canonical A_∞-structure on $\operatorname{Ext}^*_{\mathbb{F}_2\mathrm{Q}_8}(\mathbb{F}_2, \mathbb{F}_2)$ for the quaternion group Q_8. He conjecturally stated the minimal complexity of such a structure. Based on this work, there are now built-in algorithms for the Magma computer algebra system. These are capable of computing partial A_∞-structures on the group cohomology of p-groups.

In [23] and [22] (note the comments at [22, p. 41]), Vejdemo-Johansson examined the canonical A_∞-structure $(m_n)_{n\geq 1}$ on the group cohomology $\operatorname{Ext}^*_{\mathbb{F}_p(\mathrm{C}_k\times\mathrm{C}_l)}(\mathbb{F}_p, \mathbb{F}_p)$ of the abelian group $\mathrm{C}_k \times \mathrm{C}_l$ for $k, l \geq 4$ such that k, l are multiples of p. He showed that the multiplication maps m_2, m_k, m_l, m_{k+l-2}, $m_{2(k-2)+l}$ and $m_{2(l-2)+k}$ are non-zero, cf. [22, Theorem 3.3.3].

In [14], Klamt investigated canonical A_∞-structures in the context of the representation theory of Lie-algebras. In particular, given certain direct sums M of parabolic Verma modules, she examined the canonical A_∞-structure $(m'_k)_{k\geq 1}$ on $\operatorname{Ext}^*_{\mathcal{O}^\mathfrak{p}}(M, M)$. She proved upper bounds for the maximal $k \in \mathbb{Z}_{\geq 1}$ such that m'_k is non-vanishing and computed the complete A_∞-structure in certain cases.

The result For $n \in \mathbb{Z}_{\geq 1}$, we denote by S_n the symmetric group on n elements.

The group cohomology $\operatorname{Ext}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathbb{F}_p, \mathbb{F}_p)$ is well-known. For example, in [1, p. 74], it is calculated using group cohomological methods.

In this document, we will construct the canonical A_∞-structure on $\operatorname{Ext}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathbb{F}_p, \mathbb{F}_p)$.

We obtain homogeneous elements $\iota, \chi \in \operatorname{Hom}^*_{\mathbb{F}_p\mathrm{S}_p}(\operatorname{PRes}\mathbb{F}_p, \operatorname{PRes}\mathbb{F}_p) =: A$ of degree $|\iota| = 2(p-1) =: l$ and $|\chi| = l-1$ such that $\iota^j, \chi\circ\iota^j =: \chi\iota^j$ are cycles for all $j \in \mathbb{Z}_{\geq 0}$ and such that their set of homology classes $\{\overline{\iota^j} \mid j \in \mathbb{Z}_{\geq 0}\} \sqcup \{\overline{\chi\iota^j} \mid j \in \mathbb{Z}_{\geq 0}\}$ is an $\mathbb{F}_p$-basis of $\operatorname{Ext}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathbb{F}_p, \mathbb{F}_p) = \mathrm{H}^*A$, cf. Proposition 35.

For all primes p, the obtained A_∞-structure $(m'_n : (\mathrm{H}^*A)^{\otimes n} \to \mathrm{H}^*A)_{n\geq 1}$ on H^*A still has a simple description. In fact, we have $m'_n = 0$ for all $n \in \mathbb{Z}_{\geq 1} \setminus \{2, p\}$:

On the elements $\overline{\chi^{a_1}\iota^{j_1}} \otimes \cdots \otimes \overline{\chi^{a_n}\iota^{j_n}}$, $n \in \mathbb{Z}_{\geq 1}$, $a_i \in \{0, 1\}$ and $j_i \in \mathbb{Z}_{\geq 0}$ for $i \in \{1, \ldots, n\}$, the maps m'_n are given as follows, cf. Definition 38 and Remark 52.

If there is an $i \in \{1, \ldots, n\}$ such that $a_i = 0$, then

$$\begin{aligned} m'_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \cdots \otimes \overline{\chi^{a_n}\iota^{j_n}}) &= 0 \qquad\qquad \text{for } n \neq 2 \text{ and} \\ m'_2(\overline{\chi^{a_1}\iota^{j_1}} \otimes \overline{\chi^{a_2}\iota^{j_2}}) &= \overline{\chi^{a_1+a_1}\iota^{j_1+j_2}}. \end{aligned}$$

If all a_i equal 1, then

$$\begin{aligned} m'_n(\overline{\chi\iota^{j_1}} \otimes \cdots \otimes \overline{\chi\iota^{j_n}}) &= 0 && \text{for } n \neq p \text{ and} \\ m'_p(\overline{\chi\iota^{j_1}} \otimes \cdots \otimes \overline{\chi\iota^{j_p}}) &= (-1)^p \overline{\iota^{p-1+j_1+\ldots+j_p}}. \end{aligned}$$

0.2. Outline

Section 1 The goal of section 1 is to obtain a projective resolution of the trivial $\mathbb{F}_p\mathrm{S}_p$-Specht module $\mathbb{F}_p$. A well-known method for that is "Walking around the Brauer tree", cf. [4]. Instead, we use locally integral methods to obtain a projective resolution in an explicit and straightforward manner.

Over $\mathbb{Q}$, the Specht modules are absolutely simple. Therefore we have a morphism of $\mathbb{Z}_{(p)}$-algebras $r : \mathbb{Z}_{(p)}\mathrm{S}_p \to \prod_{\lambda \dashv p} \mathrm{End}_{\mathbb{Z}_{(p)}} S^\lambda_{\mathbb{Z}_{(p)}} =: \Gamma$ induced by the operation of the elements of $\mathbb{Z}_{(p)}\mathrm{S}_p$ on the Specht modules S^λ for partitions λ of p, which becomes an Wedderburn isomorphism when tensoring with $\mathbb{Q}$. So Γ is a product of matrix rings over $\mathbb{Z}_{(p)}$. There is a well-known description of $\mathrm{im}\, r =: \Lambda$, of which we will give an explicit version in section 1.1.

For $p \geq 3$, we use this description of Λ in section 1.2 to obtain projective Λ-modules $\tilde{P}_k \subseteq \Lambda$, $k \in [1, p-1]$, and to construct the indecomposible projective resolution $\mathrm{PRes}\, \mathbb{Z}_{(p)}$ of the trivial $\mathbb{Z}_{(p)}\mathrm{S}_p$-Specht module $\mathbb{Z}_{(p)}$. The non-zero parts of $\mathrm{PRes}\, \mathbb{Z}_{(p)}$ are periodic with period length $l = 2(p-1)$. In section 1.3, we reduce $\mathrm{PRes}\, \mathbb{Z}_{(p)}$ modulo p to obtain a projective resolution $\mathrm{PRes}\, \mathbb{F}_p$ of the trivial $\mathbb{F}_p\mathrm{S}_p$-Specht module $\mathbb{F}_p$.

Section 2 and appendix A The goal of section 2 is to compute a minimal model of the dg-algebra $\mathrm{Hom}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathrm{PRes}\, \mathbb{F}_p, \mathrm{PRes}\, \mathbb{F}_p) =: A$ by equipping its homology $\mathrm{Ext}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathbb{F}_p, \mathbb{F}_p) = \mathrm{H}^*A$ with a suitable A_∞-structure and finding a quasi-isomorphism of A_∞-algebras from H^*A to A.

Towards that end, we recall the basic definitions concerning A_∞-algebras and present a formulation of the minimality theorem in section 2.1. Furthermore, in appendix A, we present the bar construction in detail as well as a proof of the minimality theorem using Kadeishvili's algorithm.

While there does not seem to be a substantial difference between the cases $p = 2$ and $p \geq 3$, we separate them to simplify notation and argumentation. Consider the case $p \geq 3$. In section 2.2, we obtain a set of cycles $\{\iota^j \mid j \in \mathbb{Z}_{\geq 0}\} \cup \{\chi\iota^j \mid j \in \mathbb{Z}_{\geq 0}\}$ in A such that their homology classes are a graded basis of H^*A. In section 2.3, we obtain a suitable A_∞-structure on H^*A and a quasi-isomorphism of A_∞-algebras from H^*A to A. For the prime 2, both steps are combined in the short section 2.4.

0.3. Notations and conventions

Stipulations

- **For the remainder of this document, p will be a prime with $p \geq 3$.**
- **Write $l := 2(p-1)$.** This will give the period length of the constructed projective resolution of $\mathbb{F}_p$ over $\mathbb{F}_p \mathrm{S}_p$, cf. e.g. (6), Theorem 14 and Lemma 18.

Miscellaneous

- Concerning "∞", we assume the set $\mathbb{Z} \cup \{\infty\}$ to be ordered in such a way that ∞ is greater than any integer, i.e. $\infty > z$ for all $z \in \mathbb{Z}$, and that the integers are ordered as usual.
- For $a \in \mathbb{Z}$, $b \in \mathbb{Z} \cup \{\infty\}$, we denote by $[a, b] := \{z \in \mathbb{Z} \mid a \leq z \leq b\} \subseteq \mathbb{Z}$ the integral interval. In particular, we have $[a, \infty] = \{z \in \mathbb{Z} \mid z \geq a\} \subseteq \mathbb{Z}$ for $a \in \mathbb{Z}$.
- For $n \in \mathbb{Z}_{\geq 0}$, $k \in \mathbb{Z}$, let the binomial coefficient $\binom{n}{k}$ be defined by the number of subsets of the set $\{1, \dots, n\}$ that have cardinality k. In particular, if $k < 0$ or $k > n$, we have $\binom{n}{k} = 0$. Then the formula $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ holds for all $k \in \mathbb{Z}$.
- Rings are unital rings.
- For a commutative ring R, an R-module M and $a, b \in M$, $c \in R$, we write

  $$b \equiv_c a \qquad :\Longleftrightarrow \qquad a - b \in cM.$$

  Often we have $M = R$ as module over itself.
- For a prime q, we denote by $\mathbb{Z}_{(q)}$ the localization of the integers $\mathbb{Z}$ at the prime ideal $(q) := q\mathbb{Z}$, that is $\mathbb{Z}_{(q)} := \{z \in \mathbb{Q} \mid \exists x \in \mathbb{Z} \setminus q\mathbb{Z} \colon xz \in \mathbb{Z}\} \subseteq \mathbb{Q}$, that is the quotients of integers such that the denominator is coprime to q.
- For a prime q, let $\mathbb{F}_q$ denote the finite field containing q elements.
- Let R be a commutative ring. An R-algebra (A, ρ) is a ring A together with a ring morphism $\rho : R \to A$ such that $\rho(R)$ is a subset of the center of A. By abuse of notation, we often just write A for (A, ρ). A is an R-module via $r \cdot a := \rho(r) \cdot a$ for $r \in R$, $a \in A$.

  For R-algebras (A, ρ) and (B, τ), a morphism of R-algebras $g : (A, \rho) \to (B, \tau)$ is a ring morphism $g : A \to B$ such that $g \circ \rho = \tau$.
- Morphisms will be written on the left.
- Modules are right-modules unless otherwise specified. For a ring A, we denote by $\texttt{Mod-}A$ the category of right A-modules.
- We denote a tuple by enclosing it in parentheses. I.e. for a set M and $a_i \in M$, $i \in [1, n]$, $n \geq 0$, we have the tuple $(a_1, a_2, \dots, a_n) = a$. In particular, $()$ is the empty tuple.

For a map $g : M \to N$ from M to another set N, we define

$$g(a) := (g(x)\colon x \in a) := (g(a_1), g(a_2), \ldots, g(a_n)).$$

For another set M', by abuse of notation, we denote by $M' \setminus a$ the set difference between M' and the set of elements of a. Similarly, we write $a \subseteq M'$ if each entry of a is an element of M'.

We will express ordered bases of finite-rank free modules as tuples of pairwise distinct elements.

- For sets, we denote by $\sqcup$ the disjoint union of sets. For tuples $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_m)$, we denote by $\sqcup$ the concatenation:

$$a \sqcup b := (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m)$$

- $|\cdot|$: For a homogeneous element x of a graded module or a graded map g between graded modules, we denote by $|x|$ resp. $|g|$ their degrees (This is not unique for $x = 0$ resp. $g = 0$). For y a real number, $|y|$ denotes its absolute value. For $a = (a_1, \ldots, a_n)$ a tuple, $|a| := n$ is the number of its entries.

Symmetric Groups Let $n \in \mathbb{Z}_{\geq 1}$.

- We write $\lambda \dashv n$ to indicate that λ is a partition of n.
- By S_n, we denote the symmetric group on n elements.
- Concerning the representations of the symmetric groups, we use the notation given in [6] by JAMES. In particular for $\lambda \dashv n$, we denote the corresponding Specht module by S^λ.

Complexes Let R be a commutative ring and B an R-algebra.

- For a complex of B-modules

$$\cdots \to C_{k+1} \xrightarrow{d_{k+1}} C_k \xrightarrow{d_k} C_{k-1} \to \cdots ,$$

its k-th boundaries, cycles and homology groups are defined by $\mathrm{B}^k := \operatorname{im} d_{k+1}$, $\mathrm{Z}^k := \ker d_k$ and $\mathrm{H}^k := \mathrm{Z}^k/\mathrm{B}^k$.

For a cycle $x \in \mathrm{Z}^k$, we denote by $\overline{x} := x + \mathrm{B}^k \in \mathrm{H}^k$ its equivalence class in homology.

- For a complex of B-modules $C = (\cdots \to C_{k+1} \xrightarrow{d_{k+1}} C_k \xrightarrow{d_k} C_{k-1} \to)$ and $z \in \mathbb{Z}$, the shifted complex $C[z] =: \tilde{C}$ is defined by $\tilde{C}_k := C_{k+z}$, $\tilde{d}_k := (-1)^z d_{k+z}$.
- Let

$$C = (\cdots \to C_{k+1} \xrightarrow{d_{k+1}} C_k \xrightarrow{d_k} C_{k-1} \to \cdots)$$

$$C' = (\cdots \to C'_{k+1} \xrightarrow{d'_{k+1}} C'_k \xrightarrow{d'_k} C'_{k-1} \to \cdots)$$

be two complexes of B-modules.

Given $z \in \mathbb{Z}$, let

$$\mathrm{Hom}_B^z(C, C') := \prod_{i \in \mathbb{Z}} \mathrm{Hom}_B(C_{i+z}, C'_i).$$

For an additional complex $C'' = (\cdots \to C''_{k+1} \xrightarrow{d''_{k+1}} C''_k \xrightarrow{d''_k} C''_{k-1} \to \cdots)$ and maps $h = (h_i)_{i\in\mathbb{Z}} \in \mathrm{Hom}_B^m(C, C')$, $h' = (h'_i)_{i\in\mathbb{Z}} \in \mathrm{Hom}_B^n(C', C'')$, $m, n \in \mathbb{Z}$, we define the composition by component-wise composition as

$$h' \circ h := (h'_i \circ h_{i+n})_{i\in\mathbb{Z}} \in \mathrm{Hom}_B^{m+n}(C, C'').$$

We will assemble elements of $\mathrm{Hom}_B^z(C, C')$ as sums of their non-zero components, which motivates the following notations regarding "extensions by zero" and sums.

For a map $g : C_x \to C'_y$, we define $\lfloor g \rfloor_x^y \in \mathrm{Hom}_B^{x-y}(C, C')$ by

$$(\lfloor g \rfloor_x^y)_i := \begin{cases} g & \text{for } i = y \\ 0 & \text{for } i \in \mathbb{Z} \setminus \{y\} \end{cases}.$$

Let $k \in \mathbb{Z}$. Let I be a (possibly infinite) set. Let $g_i = (g_{i,j})_j \in \mathrm{Hom}_B^k(C, C')$ for $i \in I$ such that $\{i \in I \mid g_{i,j} \neq 0\}$ is finite for all $j \in \mathbb{Z}$.
We define the sum $\sum_{i\in I} g_i \in \mathrm{Hom}_B^k(C, C')$ by

$$\left(\sum_{i\in I} g_i\right)_j := \sum_{i\in I, g_{i,j}\neq 0} g_{i,j}\,.$$

The graded R-module $\mathrm{Hom}_B^*(C, C') := \bigoplus_{k\in\mathbb{Z}} \mathrm{Hom}_B^k(C, C')$ becomes a complex via the differential $d_{\mathrm{Hom}_B^*(C,C')}$, which is defined on elements $g \in \mathrm{Hom}_B^k(C, C')$, $k \in \mathbb{Z}$ by

$$d_{\mathrm{Hom}_B^*(C,C')}(g) := d' \circ g - (-1)^k g \circ d \in \mathrm{Hom}_B^{k+1}(C, C'),$$

where $d := (d_{i+1})_{i\in\mathbb{Z}} = \sum_{i\in\mathbb{Z}} \lfloor d_{i+1} \rfloor_{i+1}^i \in \mathrm{Hom}_B^1(C, C)$ and analogously $d' := (d'_{i+1})_{i\in\mathbb{Z}} = \sum_{i\in\mathbb{Z}} \lfloor d'_{i+1} \rfloor_{i+1}^i \in \mathrm{Hom}_B^1(C', C')$.

An element $h \in \mathrm{Hom}_B^0(C, C')$ is called a complex morphism if it satisfies $d_{\mathrm{Hom}_B^*(C,C')}(h) = 0$, i.e. $d' \circ g = g \circ d$.

0.4. Acknowledgements

I would like to thank Matthias Künzer for his advice and patient reading of the text. His many comments helped to greatly improve the quality of the text. I would like to thank my family for their constant support.

1. The projective resolution of $\mathbb{F}_p$ over $\mathbb{F}_p\mathrm{S}_p$

1.1. A description of $\mathbb{Z}_{(p)}\mathrm{S}_p$

In this paragraph, we review results found e.g. in [15, Chapter 4.2]. We use the notation of [6].

Let $n \in \mathbb{Z}_{\geq 1}$.

A partition of the form $\lambda^k := (n-k+1, 1^{k-1})$, $k \in [1,n]$ is called a *hook partition* of n.

Suppose $\lambda \dashv n$, i.e. λ is a partition of n.

Let S^λ be the corresponding integral Specht module, which is a right $\mathbb{Z}\mathrm{S}_n$-module, cf. [6, 4.3]. Then S^λ is finitely generated free over $\mathbb{Z}$, cf. [6, 8.1, proof of 8.4], having a standard $\mathbb{Z}$-basis consisting of the standard λ-polytabloids. We write n_λ for the rank of S^λ.

For a tuple $b = (b_2, b_3, \ldots, b_k)$, $k \in [1,n]$, of pairwise distinct elements of $[1,n]$, let $\langle\!\langle b \rangle\!\rangle$ be the λ^k-polytabloid generated by the λ^k-tabloid

$$\begin{array}{l} \overline{\underline{* \cdots *}} \\ \underline{b_2} \\ \underline{b_3} \\ \vdots \\ \underline{b_n} \end{array} \qquad ,$$

where $* \cdots *$ are the elements of $[1,n] \setminus b$. Any polytabloid of S^{λ^k} can be expressed this way.

For such a tuple b and distinct elements $y_1, \ldots, y_s \in [1,n] \setminus b$, we denote by $(b, y_1, \ldots, y_s)$ the tuple $(b_2, b_3, \ldots, b_k, y_1, \ldots, y_s)$. Recall the notations for manipulation of tuples from section 0.3.
The λ^k-polytabloid $\langle\!\langle b \rangle\!\rangle$ is standard iff $2 \leq b_2 < b_3 < \cdots < b_k \leq n$, cf. [6, 8.1]. This entails the following lemma.

Lemma 1. *For $k \in [1,n]$, the rank of S^{λ^k} is given by $n_{\lambda^k} = \binom{n-1}{k-1}$.*

Lemma 2 (cf. e.g. [15, Proposition 4.2.3])**.** *Let $k \in [1, n-1]$. We have the $\mathbb{Z}$-linear box shift morphisms for hooks*

$$\begin{array}{ccc} S^{\lambda^k} & \xrightarrow{f_k} & S^{\lambda^{k+1}} \\ \langle\!\langle b \rangle\!\rangle & \longmapsto & \sum_{s \in [2,n] \setminus b} \langle\!\langle (b, s) \rangle\!\rangle . \end{array}$$

For $x \in S^{\lambda^k}$ and $\rho \in \mathrm{S}_n$, we have

$$f_k(x \cdot \rho) \equiv_n f_k(x) \cdot \rho. \tag{1}$$

I.e. the composite $(S^{\lambda^k} \xrightarrow{f_k} S^{\lambda^{k+1}} \xrightarrow{\pi} S^{\lambda^{k+1}}/nS^{\lambda^{k+1}})$, where π is residue class map, is $\mathbb{Z}\mathrm{S}_n$-linear.

Lemma 3 (cf. [19, Lemma 2], [15, Proposition 4.2.4]). *The following sequence of $\mathbb{Z}$-linear maps is exact.*

$$0 \to S^{\lambda^1} \xrightarrow{f_1} S^{\lambda^2} \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} S^{\lambda^n} \to 0$$

Proof. We show that $\operatorname{im} f_k \subseteq \ker f_{k+1}$ for $k \in [1, n-2]$, i.e. that $f_{k+1} \circ f_k = 0$. Let $\langle\!\langle b \rangle\!\rangle \in S^{\lambda^k}$ be a polytabloid. We obtain

$$\begin{aligned} f_{k+1} f_k(\langle\!\langle b \rangle\!\rangle) &= f_{k+1}\left(\sum_{s\in[2,n]\setminus b} \langle\!\langle (b,s) \rangle\!\rangle\right) = \sum_{\substack{s,t\in[2,n]\setminus b,\\ s\neq t}} \langle\!\langle (b,s,t) \rangle\!\rangle \\ &= \sum_{\substack{s,t\in[2,n]\setminus b,\\ s<t}} \big(\langle\!\langle (b,s,t) \rangle\!\rangle + \langle\!\langle (b,t,s) \rangle\!\rangle\big) \overset{\text{cf. [6, 4.3]}}{=} 0. \end{aligned}$$

Now we show the exactness of the sequence. For convenience, we set $f_0 \colon 0 \to S^{\lambda^1}$ and $f_n \colon S^{\lambda^n} \to 0$. We define T^k for $k \in [1, n]$ to be the tuple of all tuples $b = (b_2, \ldots, b_k)$ such that $2 \le b_2 < b_3 < \ldots < b_k \le n-1$, where T^k is ordered, say, lexicographically. Then we set $B_{\mathrm{b}}^k := (\langle\!\langle b \rangle\!\rangle \colon b \in T^k)$, which consists of standard λ^k-polytabloids. We set $B_{\mathrm{c}}^1 := ()$, which is the empty tuple, and for $k \in [2, n]$,

$$\begin{aligned} B_{\mathrm{c}}^k &:= (f_{k-1}(x) \colon x \in B_{\mathrm{b}}^{k-1}) \\ &= \left(\sum_{s\in[2,n]\setminus b} \langle\!\langle (b,s) \rangle\!\rangle \colon b \in T^{k-1}\right) = \left(\langle\!\langle (b,n) \rangle\!\rangle + \sum_{s\in[2,n-1]\setminus b} \langle\!\langle (b,s) \rangle\!\rangle \colon b \in T^{k-1}\right). \end{aligned}$$

So $B_{\mathrm{c}}^k \subseteq \operatorname{im} f_{k-1}$ and thus $f_k(B_{\mathrm{c}}^k) \subseteq \{0\}$ for $k \in [1, n]$.

By comparing $B_{\mathrm{c}}^k \sqcup B_{\mathrm{b}}^k$ with the standard basis, we observe that $B_{\mathrm{c}}^k \sqcup B_{\mathrm{b}}^k$ is a $\mathbb{Z}$-basis of S^{λ^k} for $k \in [1, n]$.

For $k \in [1, n]$, we have

$$\begin{aligned} n_{\mathrm{b}}^k &:= |B_{\mathrm{b}}^k| = \binom{n-2}{k-1} \\ n_{\mathrm{c}}^k &:= |B_{\mathrm{c}}^k| = \left\{ \begin{array}{ll} |B_{\mathrm{b}}^{k-1}| = \binom{n-2}{k-2} & \text{for } k \in [2,n] \\ 0 = \binom{n-2}{1-2} & \text{for } k = 1 \end{array} \right\} = \binom{n-2}{k-2}. \end{aligned}$$

For $k \in [1, n-1]$, the morphism f_k maps $\langle B_{\mathrm{b}}^k \rangle_{\mathbb{Z}}$ bijectively to $\langle B_{\mathrm{c}}^{k+1} \rangle_{\mathbb{Z}}$ and $\langle B_{\mathrm{c}}^k \rangle_{\mathbb{Z}}$ to zero. So $\ker f_k = \langle B_{\mathrm{c}}^k \rangle_{\mathbb{Z}}$ and $\operatorname{im} f_k = \langle B_{\mathrm{c}}^{k+1} \rangle_{\mathbb{Z}}$. As $B_{\mathrm{c}}^1 = () = B_{\mathrm{b}}^n$, we have also $\operatorname{im} f_0 = \langle B_{\mathrm{c}}^1 \rangle_{\mathbb{Z}}$ and $\ker f_n = \langle B_{\mathrm{c}}^n \rangle_{\mathbb{Z}}$. So the sequence in question is exact. $\square$

We equip the Specht modules S^{λ^k} of hook type with the ordered $\mathbb{Z}$-basis $B_{\mathrm{c}}^k \sqcup B_{\mathrm{b}}^k$. We equip all other Specht modules with the standard $\mathbb{Z}$-basis with an arbitrarily chosen total order. From now on each of these bases will be referred to as *the* basis of the respective Specht module. We define the $\mathbb{Z}$-algebra

$$\Gamma^{\mathbb{Z}} := \prod_{\lambda \dashv n} \mathbb{Z}^{n_\lambda \times n_\lambda}.$$

Let $\lambda \dashv n$ and let $B = (b_1, \ldots, b_{n_\lambda})$ be the basis of S^λ. For the multiplication with matrices, we identify S^λ with $\mathbb{Z}^{1\times n_\lambda}$ via B.

Then S^λ becomes a right $\Gamma^{\mathbb{Z}}$-module via $x \cdot \rho := x \cdot \rho^\lambda$ for $x \in S^\lambda$ and $\rho \in \Gamma^{\mathbb{Z}}$, where ρ^λ is the λ-th component of ρ. I.e. $\rho \in \Gamma^{\mathbb{Z}}$ operates by multiplication with the matrix ρ^λ on the right with respect to the basis B.

Similarly, $\bigoplus_{\lambda \dashv n} S^\lambda$ becomes a right $\Gamma^{\mathbb{Z}}$-module. Each $\mathbb{Z}$-endomorphism of $\bigoplus_{\lambda \dashv n} S^\lambda$ is represented by the operation of a unique element of $\Gamma^{\mathbb{Z}}$. As the operation of $\mathbb{Z}\mathrm{S}_n$ defines such endomorphisms (cf. [6, Corollary 8.7]), we obtain a $\mathbb{Z}$-algebra morphism $r^{\mathbb{Z}} : \mathbb{Z}\mathrm{S}_n \to \Gamma^{\mathbb{Z}}$ such that $y \cdot r^{\mathbb{Z}}(x) = y \cdot x$ for all $\lambda \dashv n$, $y \in S^\lambda$, $x \in \mathbb{Z}\,\mathrm{S}_n$.

As the Specht modules give all irreducible ordinary representations of S_n, the map $r^{\mathbb{Z}}$ is injective. Because of (1), the image of $r^{\mathbb{Z}}$ is contained in

$$\Lambda^{\mathbb{Z}} := \{\rho \in \Gamma^{\mathbb{Z}} \mid f_k(x\rho) \equiv_n f_k(x)\rho \;\forall_{k\in[1,n-1]}\, \forall_{x \in S^{\lambda^k}}\} \subseteq \Gamma^{\mathbb{Z}}.$$

As the basis $B_{\mathrm{c}}^k \sqcup B_{\mathrm{b}}^k$ of S^{λ^k}, $k \in [1,n]$, consists of two parts, we may split each ρ^{λ^k} for a $\rho \in \Gamma^{\mathbb{Z}}$ into four blocks corresponding to the parts B_{c}^k and B_{b}^k:

$$\rho^{\lambda^k} = \begin{array}{cc} \begin{array}{cc} n_{\mathrm{c}}^k & n_{\mathrm{b}}^k \end{array} & \\ \left(\begin{array}{c|c} \rho_{\mathrm{cc}}^{\lambda^k} & \rho_{\mathrm{bc}}^{\lambda^k} \\ \hline \rho_{\mathrm{cb}}^{\lambda^k} & \rho_{\mathrm{bb}}^{\lambda^k} \end{array}\right) & \begin{array}{l} \}\, n_{\mathrm{c}}^k \\ \}\, n_{\mathrm{b}}^k \end{array} \end{array} \tag{2}$$

Suppose given $k \in [1, n-1]$. We represent f_k by a matrix M_{f_k} with respect to the bases of S^{λ^k} and $S^{\lambda^{k+1}}$, i.e. $f_k(x) = x \cdot M_{f_k}$ for $x \in S^{\lambda^k}$. As $f_k(B_{\mathrm{b}}^k) = B_{\mathrm{c}}^{k+1}$ and $f_k(B_{\mathrm{c}}^k) \subseteq \{0\}$, the matrix M_{f_k} has the following block form:

$$M_{f_k} = \begin{array}{cc} \begin{array}{cc} n_{\mathrm{c}}^{k+1} & n_{\mathrm{b}}^{k+1} \end{array} & \\ \left(\begin{array}{c|c} 0 & 0 \\ \hline E_{n_{\mathrm{b}}^k} & 0 \end{array}\right) & \begin{array}{l} \}\, n_{\mathrm{c}}^k \\ \}\, n_{\mathrm{b}}^k \end{array} \end{array}$$

Here E_i is the $i \times i$-identity matrix for $i \in \mathbb{Z}_{\geq 1}$.

So for $x \in S^{\lambda^k}$, $\rho \in \Gamma^{\mathbb{Z}}$ we have

$$f_k(x) \cdot \rho = x \cdot M_{f_k} \cdot \rho^{\lambda^{k+1}} = x \cdot \left(\begin{array}{c|c} 0 & 0 \\ \hline E_{n_{\mathrm{b}}^k} & 0 \end{array}\right) \cdot \left(\begin{array}{c|c} \rho_{\mathrm{cc}}^{\lambda^{k+1}} & \rho_{\mathrm{bc}}^{\lambda^{k+1}} \\ \hline \rho_{\mathrm{cb}}^{\lambda^{k+1}} & \rho_{\mathrm{bb}}^{\lambda^{k+1}} \end{array}\right) = x \cdot \left(\begin{array}{c|c} 0 & 0 \\ \hline \rho_{\mathrm{cc}}^{\lambda^{k+1}} & \rho_{\mathrm{bc}}^{\lambda^{k+1}} \end{array}\right)$$

$$f_k(x\cdot\rho) = x\cdot\rho^{\lambda^k}\cdot M_{f_k} = x\cdot\left(\begin{array}{c|c}\rho^{\lambda^k}_{\mathrm{cc}} & \rho^{\lambda^k}_{\mathrm{bc}}\\ \hline \rho^{\lambda^k}_{\mathrm{cb}} & \rho^{\lambda^k}_{\mathrm{bb}}\end{array}\right)\cdot\left(\begin{array}{c|c}0 & 0\\ \hline E_{n^k_{\mathrm{b}}} & 0\end{array}\right) = x\cdot\left(\begin{array}{c|c}\rho^{\lambda^k}_{\mathrm{bc}} & 0\\ \hline \rho^{\lambda^k}_{\mathrm{bb}} & 0\end{array}\right).$$

This way we have $f_k(x\cdot\rho)\equiv_n f_k(x)\cdot\rho$ for all $x\in S^{\lambda^k}$ if and only if $\rho^{\lambda^k}_{\mathrm{bb}}\equiv_n\rho^{\lambda^{k+1}}_{\mathrm{cc}}$, $\rho^{\lambda^k}_{\mathrm{bc}}\equiv_n 0$ and $\rho^{\lambda^{k+1}}_{\mathrm{bc}}\equiv_n 0$. So

$$\Lambda^{\mathbb{Z}} = \{\rho\in\Gamma^{\mathbb{Z}} \mid (\rho^{\lambda^k}_{\mathrm{bb}}\equiv_n\rho^{\lambda^{k+1}}_{\mathrm{cc}} \text{ for } k\in[1,n-1]) \text{ and } (\rho^{\lambda^k}_{\mathrm{bc}}\equiv_n 0 \text{ for } k\in[1,n])\}. \tag{3}$$

We have (cf. e.g. [15, Corollary 4.2.6])

$$|\Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}| = n^{\frac{1}{2}\sum_{k\in[1,n]}\binom{n-1}{k-1}^2},$$

which is proven by counting the congruences in (3):

$$\begin{aligned}|\Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}| &= n^{\sum_{k=1}^{n-1}(n^k_{\mathrm{b}})^2+\sum_{k=1}^{n}n^k_{\mathrm{b}}\cdot n^k_{\mathrm{c}}}\\ &\overset{n^n_{\mathrm{b}}=0}{=} n^{\sum_{k\in[1,n]}((n^k_{\mathrm{b}})^2+n^k_{\mathrm{b}}\cdot n^k_{\mathrm{c}})} = n^{\sum_{k\in[1,n]}n^k_{\mathrm{b}}(n^k_{\mathrm{b}}+n^k_{\mathrm{c}})}\end{aligned}$$

$$\begin{aligned}\sum_{k\in[1,n]} n^k_{\mathrm{b}}(n^k_{\mathrm{c}}+n^k_{\mathrm{b}}) &= \sum_{k\in[1,n]}\tbinom{n-2}{k-1}\left(\tbinom{n-2}{k-2}+\tbinom{n-2}{k-1}\right)\\ &= \frac{1}{2}\sum_{k\in[1,n]}\left(\tbinom{n-2}{k-1}\tbinom{n-2}{k-2}+\tbinom{n-2}{k-1}^2\right)+\frac{1}{2}\sum_{k\in[1,n]}\left(\tbinom{n-2}{k-1}\tbinom{n-2}{k-2}+\tbinom{n-2}{k-2}^2\right)\\ &= \frac{1}{2}\sum_{k\in[1,n]}\tbinom{n-2}{k-1}\left(\tbinom{n-2}{k-2}+\tbinom{n-2}{k-1}\right)+\tbinom{n-2}{k-2}\left(\tbinom{n-2}{k-1}+\tbinom{n-2}{k-2}\right)\\ &= \frac{1}{2}\sum_{k\in[1,n]}\tbinom{n-2}{k-1}\tbinom{n-1}{k-1}+\tbinom{n-2}{k-2}\tbinom{n-1}{k-1} = \frac{1}{2}\sum_{k\in[1,n]}\tbinom{n-1}{k-1}^2\end{aligned}$$

Recall that $p\geq 3$ is a prime. Let $n=p$. We have the commutative diagram of $\mathbb{Z}$-modules

$$\begin{tikzcd}
\mathbb{Z}\,\mathrm{S}_p \arrow[r, hook, "\iota^{\mathbb{Z}}\circ r^{\mathbb{Z}}"] \arrow[d, hook, "r^{\mathbb{Z}}"] & \Gamma^{\mathbb{Z}} \arrow[r, two heads] \arrow[d, "||"] & \Gamma^{\mathbb{Z}}/(\iota^{\mathbb{Z}}\circ r^{\mathbb{Z}}(\mathbb{Z}\,\mathrm{S}_p)) \arrow[d, "s^{\mathbb{Z}}"] \\
\Lambda^{\mathbb{Z}} \arrow[r, hook, "\iota^{\mathbb{Z}}"] & \Gamma^{\mathbb{Z}} \arrow[r, two heads] & \Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}
\end{tikzcd} \tag{4}$$

The map $\iota^{\mathbb{Z}}$ is the inclusion of $\Lambda^{\mathbb{Z}}$ in $\Gamma^{\mathbb{Z}}$. The maps from $\Gamma^{\mathbb{Z}}$ to $\Gamma^{\mathbb{Z}}/(\iota^{\mathbb{Z}}\circ r^{\mathbb{Z}}(\mathbb{Z}\,\mathrm{S}_p))$ and to $\Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}$ are the residue class maps. As $r^{\mathbb{Z}}(\mathbb{Z}\,\mathrm{S}_p)\subseteq\Lambda^{\mathbb{Z}}$, we have an unique surjective map $s^{\mathbb{Z}}:\Gamma^{\mathbb{Z}}/(\iota^{\mathbb{Z}}\circ r^{\mathbb{Z}}(\mathbb{Z}\,\mathrm{S}_p))\to\Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}$ such that the right rectangle is commutative. By construction, the rows of the diagram are short exact sequences. Note that the morphisms of the left rectangle are in fact $\mathbb{Z}$-algebra morphisms.

We will need the following result on the localization of rings.

Lemma 4 (cf. [2, chap. II Localisation, §2, n° 3, Théorème 1])**.** *Let A be a commutative ring. Let $P \subseteq R$ a prime ideal of A. Let A_P be the localization of A at P. Then A_P is a flat A-module, that is, the functor $- \underset{A}{\otimes}{}_A(A_P)_{A_P}$ from the category of A-modules to the category of A_P-modules is exact.*

We denote by $\mathbb{Z}_{(p)}$ the localization of $\mathbb{Z}$ at the prime ideal $(p) := p\mathbb{Z}$. We apply the functor $- \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}$ to obtain a commutative diagram (4) of the following form:

$$\begin{tikzcd}
\mathbb{Z}_{(p)}\mathrm{S}_p \arrow[r, hook, "\iota\circ r"] \arrow[d, hook, "r"] & \Gamma \arrow[r, two heads] \arrow[d, "||"] & \Gamma/(\iota \circ r(\mathbb{Z}_{(p)}\mathrm{S}_p)) \arrow[d, two heads, "s"] \\
\Lambda \arrow[r, hook, "\iota"] & \Gamma \arrow[r, two heads] & \Gamma/\Lambda
\end{tikzcd} \tag{5}$$

By Lemma 4, the functor $- \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}$ is exact, so the short exact sequences are mapped to short exact sequences, monomorphisms to monomorphisms and epimorphisms to epimorphisms. So the rows of diagram (5) are exact and we have mono-/epimorphism as indicated by the arrows. We identify $\mathbb{Z}\,\mathrm{S}_p \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}$ with $\mathbb{Z}_{(p)}\mathrm{S}_p$. We identify $\Gamma^{\mathbb{Z}} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}$ with

$$\Gamma := \prod_{\lambda \dashv n} \mathbb{Z}_{(p)}^{n_\lambda \times n_\lambda}.$$

The map ι realizes $\Lambda := \Lambda^{\mathbb{Z}} \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}$ as the following subset of Γ, for which we will use notation analogous to (2):

$$\Lambda = \{\rho \in \Gamma \mid (\rho_{\mathrm{bb}}^{\lambda^k} \equiv_p \rho_{\mathrm{cc}}^{\lambda^{k+1}} \text{ for } k \in [1, p-1]) \text{ and } (\rho_{\mathrm{bc}}^{\lambda^k} \equiv_p 0 \text{ for } k \in [1, p])\}$$

As the rows are exact, we identify $(\Gamma^{\mathbb{Z}}/(\iota^{\mathbb{Z}} \circ r^{\mathbb{Z}}(\mathbb{Z}\,\mathrm{S}_p))) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}$ with $\Gamma/(\iota \circ r(\mathbb{Z}_{(p)}\mathrm{S}_p)$ and $(\Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}$ with Γ/Λ.

By the classification of finitely generated $\mathbb{Z}$-modules, each finite $\mathbb{Z}$-module M is isomorphic to a finite direct sum of modules of the form $\mathbb{Z}/q^a\mathbb{Z}$, where q is a prime and $a \in \mathbb{Z}_{\geq 0}$. If $q \neq p$ then $(\mathbb{Z}/q^a\mathbb{Z}) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)} \cong (0)$. Otherwise $(\mathbb{Z}/p^a\mathbb{Z}) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)} \cong \mathbb{Z}_{(p)}/p^a\mathbb{Z}_{(p)}$ and $|(\mathbb{Z}/p^a\mathbb{Z}) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}| = p^a = |\mathbb{Z}/p^a\mathbb{Z}|$. For $x = p^{a_p} \cdot \prod_{\substack{q \text{ prime} \\ q \neq p}} q^{a_q} \in \mathbb{Z}_{\geq 1}$, we set

$$(x)_p := p^{a_p}.$$

So for finite M, we have $|M \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_{(p)}| = (|M|)_p$.

By the total index formula (cf. e.g. [15, Proposition 1.1.4]), we have

$$|\Gamma^{\mathbb{Z}}/(\iota^{\mathbb{Z}} \circ r^{\mathbb{Z}}(\mathbb{Z}\,\mathrm{S}_p))| = \sqrt{\frac{p!^{p!}}{\prod_{\lambda \dashv p} n_\lambda^{n_\lambda^2}}}\,.$$

By the hook formula (cf. [6, 20.1], [15, Lemma 4.2.7]), we have for $\lambda \dashv p$

$$(n_\lambda)_p = \begin{cases} 1 & \text{if } \lambda \text{ is a hook-partition} \\ p & \text{otherwise} \end{cases}.$$

So

$$\begin{aligned} |\Gamma/(i\circ r(\mathbb{Z}_{(p)}\mathrm{S}_p))| &= \left(\sqrt{\frac{p!^{p!}}{\prod_{\lambda\dashv p} n_\lambda^{n_\lambda^2}}}\right)_p = \sqrt{\frac{p^{p!}}{\prod_{\substack{\lambda\dashv p \\ \lambda \text{ not a hook}}} (n_\lambda)_p^{n_\lambda^2}}} \\ &= \sqrt{\frac{\prod_{\lambda\dashv p} p^{n_\lambda^2}}{\prod_{\substack{\lambda\dashv p \\ \lambda \text{ not a hook}}} p^{n_\lambda^2}}} = \sqrt{\prod_{k\in[1,n]} p^{n_{\lambda^k}^2}} = p^{\frac{1}{2}\sum_{k\in[1,n]}\binom{p-1}{k-1}^2} \\ &= |\Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}| = (|\Gamma^{\mathbb{Z}}/\Lambda^{\mathbb{Z}}|)_p = |\Gamma/\Lambda|. \end{aligned}$$

By the pigeon-hole-principle, s is an isomorphism as it is surjective. As (5) has exact rows, r needs to be an isomorphism as well. Note that the functor $-\underset{\mathbb{Z}}{\otimes}\mathbb{Z}_{(p)}$ transforms morphisms of $\mathbb{Z}$-algebras into morphisms of $\mathbb{Z}_{(p)}$-algebras. In particular, the left rectangle in (5) consists of morphisms of $\mathbb{Z}_{(p)}$-algebras and $r : \mathbb{Z}_{(p)}\mathrm{S}_p \to \Lambda$ is an isomorphism of $\mathbb{Z}_{(p)}$-algebras. We have proven the

Proposition 5 (cf. e.g. [15, Corollary 4.2.8])**.** *Recall that $p \geq 3$ is a prime. Recall $\Lambda \subset \Gamma$. We have the isomorphism of $\mathbb{Z}_{(p)}$-algebras*

$$r : \ \mathbb{Z}_{(p)}\mathrm{S}_p \ \xrightarrow{\sim} \ \Lambda.$$

We recall the occurring notations:

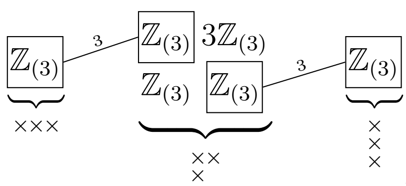
$$\Gamma := \prod_{\lambda\dashv p} \mathbb{Z}_{(p)}^{n_\lambda\times n_\lambda}$$

$$\Lambda := \{\rho\in\Gamma \mid \rho_{\mathrm{bb}}^{\lambda^k} \equiv_p \rho_{\mathrm{cc}}^{\lambda^{k+1}} \textit{ for } k\in[1,p-1] \textit{ and } \rho_{\mathrm{bc}}^{\lambda^k}\equiv_p 0 \textit{ for } k\in[1,p]\}.$$

We have $n_\lambda := \dim S^\lambda$, $n_{\mathrm{b}}^k = \binom{p-2}{k-1}$, $n_{\mathrm{c}}^k = \binom{p-2}{k-2}$ and $n_{\mathrm{b}}^k + n_{\mathrm{c}}^k = \binom{p-1}{k-1} = n_{\lambda^k}$. For $\rho\in\Gamma$, we write (cf. (2))

$$\rho^{\lambda^k} = \begin{array}{c} \overbrace{n_{\mathrm{c}}^k}\ \overbrace{n_{\mathrm{b}}^k} \\ \left(\begin{array}{c|c} \rho_{\mathrm{cc}}^{\lambda^k} & \rho_{\mathrm{bc}}^{\lambda^k} \\ \hline \rho_{\mathrm{cb}}^{\lambda^k} & \rho_{\mathrm{bb}}^{\lambda^k} \end{array}\right) \end{array} \begin{array}{l} \\ \}\, n_{\mathrm{c}}^k \\ \}\, n_{\mathrm{b}}^k \end{array}.$$

Example 6. For $p = 3$, the ring $\mathbb{Z}_{(3)}\,\mathrm{S}_3$ is isomorphic to the subring Λ of $\Gamma = \mathbb{Z}_{(3)}^{1\times1} \times \mathbb{Z}_{(3)}^{2\times2} \times \mathbb{Z}_{(3)}^{1\times1}$ described as



.

An entry in this tuple of matrices indicates that an element of Λ must have its corresponding entry in the indicated set. A relation " $\overset{p}{\text{———}}$ " between (equal sized) subblocks indicates that these subblocks are equivalent modulo p, i.e. the difference of corresponding entries is an element of $p\mathbb{Z}_{(p)}$. The blocks are labeled with the diagrams of the corresponding partitions. Alternatively, Λ is the $\mathbb{Z}_{(3)}$-span of

$$\left(3, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, 0\right) =: \beta^{\Leftarrow}_{1,1,1}, \quad \left(1, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, 0\right) =: \beta^{\Leftrightarrow}_{1,1,1} =: \tilde{e}_1, \quad \left(0, \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix}, 0\right) =: \beta^{\rightarrow}_{2,1,1},$$
$$\left(0, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, 0\right) =: \beta^{\leftarrow}_{2,1,1}, \quad \left(0, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 1\right) =: \beta^{\Leftrightarrow}_{2,1,1} =: \tilde{e}_2, \quad \left(0, \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}, 0\right) =: \beta^{\Leftarrow}_{2,1,1}.$$

The names of these elements were chosen in anticipation of the definitions in section 1.2. We have an orthogonal decomposition $1 = \tilde{e}_1 + \tilde{e}_2$ into primitive idempotents. Thus we have a decomposition $\Lambda = \tilde{P}_1 \oplus \tilde{P}_2$ into indecomposable projective right modules, where

$$\tilde{P}_1 := \tilde{e}_1\Lambda = \langle \beta^{\Leftarrow}_{1,1,1}, \tilde{e}_1, \beta^{\rightarrow}_{2,1,1} \rangle_{\mathbb{Z}_{(3)}}, \qquad \tilde{P}_2 := \tilde{e}_2\Lambda = \langle \beta^{\leftarrow}_{2,1,1}, \tilde{e}_2, \beta^{\Leftarrow}_{2,1,1} \rangle_{\mathbb{Z}_{(3)}}.$$

In this case all partitions of 3 are of hook-type. Thus there appear no full matrix algebras as direct factors of Λ.

Example 7. $\mathbb{Z}_{(5)}\,\mathrm{S}_5$ is isomorphic to the subring Λ of $\Gamma = \mathbb{Z}_{(5)}^{1\times 1} \times \mathbb{Z}_{(5)}^{4\times 4} \times \mathbb{Z}_{(5)}^{6\times 6} \times \mathbb{Z}_{(5)}^{4\times 4} \times \mathbb{Z}_{(5)}^{1\times 1} \times \mathbb{Z}_{(5)}^{5\times 5} \times \mathbb{Z}_{(5)}^{5\times 5}$ described as

$$\underbrace{\begin{array}{c}\mathbb{Z}_{(5)}\end{array}}_{\times\times\times\times\times}
\quad
\underbrace{\begin{array}{cccc}
\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)}
\end{array}}_{\begin{array}{l}\times\times\times\times\\ \times\end{array}}
\quad
\underbrace{\begin{array}{cccccc}
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)}
\end{array}}_{\begin{array}{l}\times\times\times\\ \times\\ \times\end{array}}
\quad
\underbrace{\begin{array}{cccc}
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & 5\mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)}
\end{array}}_{\begin{array}{l}\times\times\\ \times\\ \times\\ \times\end{array}}
\quad
\underbrace{\begin{array}{c}\mathbb{Z}_{(5)}\end{array}}_{\begin{array}{l}\times\\ \times\\ \times\\ \times\\ \times\end{array}}$$

$$\underbrace{\begin{array}{ccccc}
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)}
\end{array}}_{\begin{array}{l}\times\times\\ \times\times\\ \times\end{array}}
\quad
\underbrace{\begin{array}{ccccc}
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} \\
\mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)} & \mathbb{Z}_{(5)}
\end{array}}_{\begin{array}{l}\times\times\times\\ \times\times\end{array}}\ .$$

For this tuple of matrices, we use the same conventions as in Example 6.

1.2. A projective resolution of $\mathbb{Z}_{(p)}$ over $\mathbb{Z}_{(p)}\mathrm{S}_p$

Recall that $p \geq 3$ is a prime.

Recall from Proposition 5 that Λ is a subring of $\Gamma = \prod_{\lambda \dashv p} \mathbb{Z}_{(p)}^{n_\lambda \times n_\lambda}$. We shall construct two $\mathbb{Z}_{(p)}$-bases of Λ.

For $\lambda \dashv p$ and $i, j \in [1, n_\lambda]$, we set $\eta_{\lambda,i,j}$ to be the element of Γ such that $(\eta_{\lambda,i,j})^{\tilde{\lambda}} = 0$ for $\tilde{\lambda} \neq \lambda$ and $(\eta_{\lambda,i,j})^{\lambda} \in \mathbb{Z}^{n_\lambda \times n_\lambda}$ has entry 1 at position (i, j) and zeros elsewhere. Then let

(1) $\mathscr{B}^{\Leftrightarrow} := \{\beta^{\Leftrightarrow}_{k,x,y} \mid k \in [1, p-1], x, y \in [1, n^k_{\mathrm{b}}]\}$, where $\beta^{\Leftrightarrow}_{k,x,y} := \eta_{\lambda^k, n^k_{\mathrm{c}}+x, n^k_{\mathrm{c}}+y} + \eta_{\lambda^{k+1},x,y}$.

(2) $\mathscr{B}^{\Leftarrow} := \{\beta^{\Leftarrow}_{k,x,y} \mid k \in [1, p-1], x, y \in [1, n^k_{\mathrm{b}}]\}$, where $\beta^{\Leftarrow}_{k,x,y} := p\eta_{\lambda^k, n^k_{\mathrm{c}}+x, n^k_{\mathrm{c}}+y}$.

(3) $\mathscr{B}^{\Rightarrow} := \{\beta^{\Rightarrow}_{k,x,y} \mid k \in [1, p-1], x, y \in [1, n^k_{\mathrm{b}}]\}$, where $\beta^{\Rightarrow}_{k,x,y} := p\eta_{\lambda^{k+1},x,y}$.

(4) $\mathscr{B}^{\leftarrow} := \{\beta^{\leftarrow}_{k,x,y} \mid k \in [1, p], x \in [1, n^k_{\mathrm{b}}], y \in [1, n^k_{\mathrm{c}}]\}$, where $\beta^{\leftarrow}_{k,x,y} := \eta_{\lambda^k, n^k_{\mathrm{c}}+x, y}$.

(5) $\mathscr{B}^{\rightarrow} := \{\beta^{\rightarrow}_{k,x,y} \mid k \in [1, p], x \in [1, n^k_{\mathrm{c}}], y \in [1, n^k_{\mathrm{b}}]\}$, where $\beta^{\rightarrow}_{k,x,y} := p\eta_{\lambda^k, x, n^k_{\mathrm{c}}+y}$.

(6) $\mathscr{B}^{*} := \{\eta_{\lambda,x,y} \mid \lambda \dashv p \text{ not a hook partition}, x, y \in [1, n_\lambda]\}$.

We have two $\mathbb{Z}_{(p)}$-bases $\mathscr{B}^{\Leftrightarrow} \sqcup \mathscr{B}^{\Leftarrow} \sqcup \mathscr{B}^{\leftarrow} \sqcup \mathscr{B}^{\rightarrow} \sqcup \mathscr{B}^{*}$ and $\mathscr{B}^{\Leftrightarrow} \sqcup \mathscr{B}^{\Rightarrow} \sqcup \mathscr{B}^{\leftarrow} \sqcup \mathscr{B}^{\rightarrow} \sqcup \mathscr{B}^{*}$ of Λ.

Example 8 ($p = 3$, continuation of Example 6)**.** The only of the $\beta^d_{a,b,c}$ that are defined above and that are not shown in Example 6 are the following elements.

$$\left(0, \begin{pmatrix} 3 & 0 \\ 0 & 0 \end{pmatrix}, 0\right) = \beta^{\Rightarrow}_{1,1,1}, \qquad \left(0, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, 3\right) = \beta^{\Rightarrow}_{2,1,1}$$

$\mathscr{B}^{*}$ is empty since all partitions are hook partitions.

Let $k \in [1, p-1]$. We obtain the idempotent

$$\tilde{e}_k := \beta^{\Leftrightarrow}_{k,1,1} = \eta_{\lambda^k, n^k_{\mathrm{c}}+1, n^k_{\mathrm{c}}+1} + \eta_{\lambda^{k+1},1,1} \in \Lambda.$$

We define corresponding projective right Λ-modules

$$\tilde{P}_k := \tilde{e}_k \Lambda \qquad \text{for } k \in [1, p-1].$$

Once more, see Example 6 for an illustration of the case $p = 3$.

Let

(1) $\mathscr{B}^{\Leftrightarrow}_k := (\beta^{\Leftrightarrow}_{k,1,y} \colon y \in (1, \ldots, n^k_{\mathrm{b}})) = (\eta_{\lambda^k, n^k_{\mathrm{c}}+1, n^k_{\mathrm{c}}+y} + \eta_{\lambda^{k+1},1,y} \colon y \in (1, \ldots, n^k_{\mathrm{b}}))$

(2) $\mathscr{B}^{\Leftarrow}_k := (\beta^{\Leftarrow}_{k,1,y} \colon y \in (1, \ldots, n^k_{\mathrm{b}})) = (p\eta_{\lambda^k, n^k_{\mathrm{c}}+1, n^k_{\mathrm{c}}+y} \colon y \in (1, \ldots, n^k_{\mathrm{b}}))$

(3) $\mathscr{B}^{\Rightarrow}_k := (\beta^{\Rightarrow}_{k,1,y} \colon y \in (1, \ldots, n^k_{\mathrm{b}})) = (p\eta_{\lambda^{k+1},1,y} \colon y \in (1, \ldots, n^k_{\mathrm{b}}))$

(4) $\mathscr{B}^{\leftarrow}_k := (\beta^{\leftarrow}_{k,1,y} \colon y \in (1, \ldots, n^k_{\mathrm{c}})) = (\eta_{\lambda^k, n^k_{\mathrm{c}}+1, y} \colon y \in (1, \ldots, n^k_{\mathrm{c}}))$

(5) $\mathscr{B}^{\rightarrow}_k := (\beta^{\rightarrow}_{k+1,1,y} \colon y \in (1, \ldots, n^{k+1}_{\mathrm{b}})) = (p\eta_{\lambda^{k+1},1,n^{k+1}_{\mathrm{c}}+y} \colon y \in (1, \ldots, n^{k+1}_{\mathrm{b}}))$

Remark 9. Similarly to the bases of Λ, the tuples $\mathscr{B}_k^{\Leftrightarrow} \sqcup \mathscr{B}_k^{\Leftarrow} \sqcup \mathscr{B}_k^{\leftarrow} \sqcup \mathscr{B}_k^{\rightarrow}$ and $\mathscr{B}_k^{\Leftrightarrow} \sqcup \mathscr{B}_k^{\Rightarrow} \sqcup \mathscr{B}_k^{\leftarrow} \sqcup \mathscr{B}_k^{\rightarrow}$ are $\mathbb{Z}_{(p)}$-bases of $\tilde{P}_k$.

Remark 10. Let $k \in [1, p-1]$. The idempotent $\tilde{e}_k$ is actually a primitive idempotent and thus $\tilde{P}_k$ is an indecomposable projective Λ-right module: Assume $\tilde{e}_k = c + c'$ for some idempotents $0 \neq c, c' \in \Lambda$ that are orthogonal, that is $c \cdot c' = c' \cdot c = 0$. Then $\tilde{e}_k \cdot c = (c + c')c = c^2 = c = c(c + c') = c \cdot \tilde{e}_k$. Similarly, we have $\tilde{e}_k \cdot c' = c' = c' \cdot \tilde{e}_k$. Thus $c, c' \in \tilde{e}_k \Lambda \tilde{e}_k$. The $\mathbb{Z}_{(p)}$-algebra

$$\tilde{e}_k \Lambda \tilde{e}_k = \langle e_k, \beta^{\Leftarrow}_{k,1,1} \rangle_{\mathbb{Z}_{(p)}} = \langle e_k, \beta^{\Rightarrow}_{k,1,1} \rangle_{\mathbb{Z}_{(p)}}$$

is isomorphic to the $\mathbb{Z}_{(p)}$-algebra

$$J := \mathbb{Z}_{(p)} \overset{p}{\text{———}} \mathbb{Z}_{(p)}$$

consisting of elements $\{(a, b) \in \mathbb{Z}_{(p)} \times \mathbb{Z}_{(p)} \mid a \equiv_p b\}$. The only idempotents in $\mathbb{Z}_{(p)} \times \mathbb{Z}_{(p)}$ are $(0,0) \in J$, $(1,1) \in J$, $(1,0) \notin J$ and $(0,1) \notin J$. Thus the identity element $(1,1)$ of J cannot be decomposed into non-trivial idempotents and the same holds for $\tilde{e}_k$.

Remark 11. Let A be an R-algebra and let $e, e' \in A$ be two idempotents. For the right modules eA, $e'A$, we have the isomorphism of R-Modules

$$\begin{array}{rcl} \mathrm{Hom}_A(eA, e'A) & \xrightarrow[\sim]{T_{e',e}} & e'Ae \\ f & \longmapsto & T_{e',e}(f) := f(e) \\ T^{-1}_{e',e}(e'be) := (ea \mapsto e'bea) & \longleftarrow & e'be \end{array} .$$

Thus given $m \in e'Ae$, the morphism $T^{-1}_{e',e}(m)$ acts on elements $x \in eA$ by the multiplication of m on the left: $(T^{-1}_{e',e}(m))(x) = m \cdot x$.

Given idempotents $e, e', e'' \in A$, and elements $f \in \mathrm{Hom}_A(eA, e'A)$, $g \in A(e'A, e''A)$, we have $T_{e'',e}(g \circ f) = g(f(e)) = g(e'f(e)) = g(e') \cdot f(e) = T_{e'',e'}(g) \cdot T_{e',e}(f)$.

Definition 12. For well-definedness of the definitions below, we check $n_{\mathrm{c}}^1 = 0$, $n_{\mathrm{b}}^1 = 1$, $n_{\mathrm{c}}^{p-1+1} = 1$, $n_{\mathrm{b}}^{p-1+1} = 0$, and for $k \in [1, p-2]$, we check $n_{\mathrm{c}}^{k+1}, n_{\mathrm{b}}^{k+1} \geq 1$.
We have $\beta^{\Leftarrow}_{1,1,1} = p\eta_{\lambda^1,1,1} \in \tilde{e}_1 \Lambda \tilde{e}_1$, $\beta^{\Rightarrow}_{p-1,1,1} = p\eta_{\lambda^p,1,1} \in \tilde{e}_{p-1} \Lambda \tilde{e}_{p-1}$. For $k \in [1, p-2]$, we have $\beta^{\leftarrow}_{k+1,1,1} = \eta_{\lambda^{k+1}, n_{\mathrm{c}}^{k+1}+1,1} \in \tilde{e}_{k+1} \Lambda \tilde{e}_k$ and $\beta^{\rightarrow}_{k+1,1,1} = p\eta_{\lambda^{k+1},1,n_{\mathrm{c}}^{k+1}+1} \in \tilde{e}_k \Lambda \tilde{e}_{k+1}$. For $k \in [1, p-1]$, we have $\tilde{e}_k \in \tilde{e}_k \Lambda \tilde{e}_k$. Then we define via Remark 11

$$\begin{array}{lcll} \hat{e}_k & := & T^{-1}_{\tilde{e}_k,\tilde{e}_k}(\tilde{e}_k) & \in \mathrm{Hom}_\Lambda(\tilde{P}_k, \tilde{P}_k) \quad \text{for } k \in [1, p-1] \\ \hat{e}_{1,1} & := & T^{-1}_{\tilde{e}_1,\tilde{e}_1}(p\eta_{\lambda^1,1,1}) & \in \mathrm{Hom}_\Lambda(\tilde{P}_1, \tilde{P}_1) \\ \hat{e}_{p-1,p-1} & := & T^{-1}_{\tilde{e}_{p-1},\tilde{e}_{p-1}}(p\eta_{\lambda^p,1,1}) & \in \mathrm{Hom}_\Lambda(\tilde{P}_{p-1}, \tilde{P}_{p-1}) \\ \hat{e}_{k+1,k} & := & T^{-1}_{\tilde{e}_{k+1},\tilde{e}_k}(\eta_{\lambda^{k+1},n_{\mathrm{c}}^{k+1}+1,1}) & \in \mathrm{Hom}_\Lambda(\tilde{P}_k, \tilde{P}_{k+1}) \quad \text{for } k \in [1, p-2] \\ \hat{e}_{k,k+1} & := & T^{-1}_{\tilde{e}_k,\tilde{e}_{k+1}}(p\eta_{\lambda^{k+1},1,n_{\mathrm{c}}^{k+1}+1}) & \in \mathrm{Hom}_\Lambda(\tilde{P}_{k+1}, \tilde{P}_k) \quad \text{for } k \in [1, p-2]. \end{array}$$

Note that $\hat{e}_k$ is the identity map on $\tilde{P}_k$ for $k \in [1, p-1]$.

Lemma 13. *We have*

(a) $\ker \hat{e}_{k+1,k} = \langle \mathscr{B}_k^{\leftarrow} \sqcup \mathscr{B}_k^{\Leftarrow} \rangle_{\mathbb{Z}_{(p)}}$, $\quad \operatorname{im} \hat{e}_{k+1,k} = \langle \mathscr{B}_{k+1}^{\leftarrow} \sqcup \mathscr{B}_{k+1}^{\Leftarrow} \rangle_{\mathbb{Z}_{(p)}}$ *for* $k \in [1, p-2]$,

(b) $\ker \hat{e}_{k,k+1} = \langle \mathscr{B}_{k+1}^{\rightarrow} \sqcup \mathscr{B}_{k+1}^{\Rightarrow} \rangle_{\mathbb{Z}_{(p)}}$, $\quad \operatorname{im} \hat{e}_{k,k+1} = \langle \mathscr{B}_k^{\rightarrow} \sqcup \mathscr{B}_k^{\Rightarrow} \rangle_{\mathbb{Z}_{(p)}}$ *for* $k \in [1, p-2]$,

(c) $\ker \hat{e}_{p-1,p-1} = \langle \mathscr{B}_{p-1}^{\leftarrow} \sqcup \mathscr{B}_{p-1}^{\Leftarrow} \rangle_{\mathbb{Z}_{(p)}}$, $\quad \operatorname{im} \hat{e}_{p-1,p-1} = \langle \mathscr{B}_{p-1}^{\Rightarrow} \sqcup \mathscr{B}_{p-1}^{\rightarrow} \rangle_{\mathbb{Z}_{(p)}}$,

(d) $\ker \hat{e}_{1,1} = \langle \mathscr{B}_1^{\Rightarrow} \sqcup \mathscr{B}_1^{\rightarrow} \rangle_{\mathbb{Z}_{(p)}}$, $\quad \operatorname{im} \hat{e}_{1,1} = \langle \mathscr{B}_1^{\Leftarrow} \sqcup \mathscr{B}_1^{\leftarrow} \rangle_{\mathbb{Z}_{(p)}}$.

Proof. (a):

$$\begin{aligned}
\hat{e}_{k+1,k}(\mathscr{B}_k^{\Leftrightarrow}) &\stackrel{\text{R.11}}{=} (\eta_{\lambda^{k+1},n_\mathrm{c}^{k+1}+1,1}\eta_{\lambda^{k+1},1,y} \colon y \in (1,\ldots,n_\mathrm{b}^k)) \\
&= (\eta_{\lambda^{k+1},n_\mathrm{c}^{k+1}+1,y} \colon y \in (1,\ldots,n_\mathrm{c}^{k+1})) = \mathscr{B}_{k+1}^{\leftarrow} \\
\hat{e}_{k+1,k}(\mathscr{B}_k^{\rightarrow}) &\stackrel{\text{R.11}}{=} (\eta_{\lambda^{k+1},n_\mathrm{c}^{k+1}+1,1}\, p\,\eta_{\lambda^{k+1},1,n_\mathrm{c}^{k+1}+y} \colon y \in (1,\ldots,n_\mathrm{b}^{k+1})) \\
&= (p\eta_{\lambda^{k+1},n_\mathrm{c}^{k+1}+1,n_\mathrm{c}^{k+1}+y} \colon y \in (1,\ldots,n_\mathrm{b}^{k+1})) = \mathscr{B}_{k+1}^{\Leftarrow} \\
\hat{e}_{k+1,k}(\mathscr{B}_k^{\leftarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\} \\
\hat{e}_{k+1,k}(\mathscr{B}_k^{\Leftarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\}
\end{aligned}$$

Thus by Remark 9, assertion (a) holds.

(b):

$$\begin{aligned}
\hat{e}_{k,k+1}(\mathscr{B}_{k+1}^{\Leftrightarrow}) &\stackrel{\text{R.11}}{=} (p\eta_{\lambda^{k+1},1,n_\mathrm{c}^{k+1}+1}\eta_{\lambda^{k+1},n_\mathrm{c}^{k+1}+1,n_\mathrm{c}^{k+1}+y} \colon y \in (1,\ldots,n_\mathrm{b}^{k+1})) \\
&= (p\eta_{\lambda^{k+1},1,n_\mathrm{c}^{k+1}+y} \colon y \in (1,\ldots,n_\mathrm{b}^{k+1})) = \mathscr{B}_k^{\rightarrow} \\
\hat{e}_{k,k+1}(\mathscr{B}_{k+1}^{\leftarrow}) &\stackrel{\text{R.11}}{=} (p\eta_{\lambda^{k+1},1,n_\mathrm{c}^{k+1}+1}\eta_{\lambda^{k+1},n_\mathrm{c}^{k+1}+1,y} \colon y \in (1,\ldots,n_\mathrm{c}^{k+1})) \\
&= (p\eta_{\lambda^{k+1},1,y} \colon y \in (1,\ldots,n_\mathrm{b}^{k})) = \mathscr{B}_k^{\Rightarrow} \\
\hat{e}_{k,k+1}(\mathscr{B}_{k+1}^{\rightarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\} \\
\hat{e}_{k,k+1}(\mathscr{B}_{k+1}^{\Rightarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\}
\end{aligned}$$

Thus by Remark 9, assertion (b) holds.

(c):

$$\begin{aligned}
\hat{e}_{p-1,p-1}(\mathscr{B}_{p-1}^{\Leftrightarrow}) &\stackrel{\text{R.11}}{=} (p\eta_{\lambda^p,1,1}\eta_{\lambda^{(p-1)+1},1,y} \colon y \in (1,\ldots,n_\mathrm{b}^{p-1})) \\
&= (p\eta_{\lambda^{(p-1)+1},1,y} \colon y \in (1,\ldots,n_\mathrm{b}^{p-1})) = \mathscr{B}_{p-1}^{\Rightarrow} \\
\mathscr{B}_{p-1}^{\rightarrow} &= () \text{ as } n_\mathrm{b}^p = 0 \\
\hat{e}_{p-1,p-1}(\mathscr{B}_{p-1}^{\leftarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\} \\
\hat{e}_{p-1,p-1}(\mathscr{B}_{p-1}^{\Leftarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\}
\end{aligned}$$

Thus by Remark 9, assertion (c) holds.

(d):

$$\begin{aligned}
\hat{e}_{1,1}(\mathscr{B}_1^{\Leftrightarrow}) &\stackrel{\text{R.11}}{=} (p\eta_{\lambda^1,1,1}\eta_{\lambda^1,n_\mathrm{c}^1+1,n_\mathrm{c}^1+y} \colon y \in (1,\ldots,n_\mathrm{b}^1)) \\
&\stackrel{n_\mathrm{c}^1=0}{=} (p\eta_{\lambda^1,n_\mathrm{c}^1+1,n_\mathrm{c}^1+y} \colon y \in (1,\ldots,n_\mathrm{b}^1)) = \mathscr{B}_1^{\Leftarrow} \\
\mathscr{B}_1^{\leftarrow} &= () \text{ as } n_\mathrm{c}^1 = 0 \\
\hat{e}_{1,1}(\mathscr{B}_1^{\Rightarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\} \\
\hat{e}_{1,1}(\mathscr{B}_1^{\rightarrow}) &\stackrel{\text{R.11}}{\subseteq} \{0\}
\end{aligned}$$

Thus by Remark 9, assertion (d) holds. □

The trivial $\mathbb{Z}_{(p)}\mathrm{S}_p$-module $\mathbb{Z}_{(p)}$ becomes a Λ-module via the isomorphism of $\mathbb{Z}_{(p)}$-algebras $r : \mathbb{Z}_{(p)}\mathrm{S}_p \to \Lambda$ described in Proposition 5. We want to construct a projective resolution of $\mathbb{Z}_{(p)}$ over Λ.

Γ is a right Λ-module as Λ is a subalgebra of Γ. The set $\Gamma^{\lambda^1} := \{\rho \in \Gamma \mid \rho^\lambda = 0 \text{ for } \lambda \neq \lambda^1\}$ is a right Λ-submodule of Γ. As $n_{\mathrm{c}}^k = 0$ and $n_{\mathrm{b}}^k = 1$, Γ^{λ^1} is free over $\mathbb{Z}_{(p)}$ with basis $\{\eta_{\lambda^1,1,1}\}$.

Given a partition $\lambda \dashv p$, the operation of an element $x \in \mathbb{Z}_{(p)}\mathrm{S}_p$ on the Specht module corresponding to λ is multiplication with the matrix $r(x)^\lambda$ with respect to a certain basis of that Specht module, cf. the definition of $r^{\mathbb{Z}}$ in the proof of Proposition 5.

As $\mathbb{Z}_{(p)}$ is the Specht module corresponding to the trivial partition λ^1 of p, and as $\mathbb{Z}_{(p)}$ is one-dimensional, the operation of $x \in \mathbb{Z}_{(p)}\mathrm{S}_p$ on $\mathbb{Z}_{(p)}$ is multiplication with the scalar $r(x)^{\lambda^1}$. Thus an element $\rho \in \Lambda$ operates on $\mathbb{Z}_{(p)}$ via multiplication with the scalar ρ^{λ^1} and we haven an isomorphism of right Λ-modules by

$$\begin{array}{rccl} \hat{\varepsilon}^1 : & \Gamma^{\lambda^1} & \longrightarrow & \mathbb{Z}_{(p)} \\ & \eta_{\lambda^1,1,1} & \longmapsto & 1. \end{array}$$

We have the morphism of right Λ-modules

$$\begin{array}{rccl} \hat{\varepsilon}^0 : & \tilde{P}_1 & \longrightarrow & \Gamma^{\lambda^1} \\ & \tilde{e}_1 x & \longmapsto & \eta_{\lambda^1,1,1}\tilde{e}_1 x = \eta_{\lambda^1,1,1} x \quad \text{for } x \in \Lambda \end{array}$$

We have $\hat{\varepsilon}^0(\tilde{e}_1) = \hat{\varepsilon}^0(\eta_{\lambda^1,1,1} + \eta_{\lambda^2,1,1}) = \eta_{\lambda^1,1,1}$, thus $\hat{\varepsilon}^0$ is surjective as $\{\eta_{\lambda^1,1,1}\}$ is a $\mathbb{Z}_{(p)}$-basis of Γ^{λ^1}. Given $x \in \tilde{P}_1$, we have $\hat{e}_{1,1}(x) = p\hat{\varepsilon}^0(x)$ as elements of Γ. Thus the maps $\hat{e}_{1,1}$ and $\hat{\varepsilon}^0$ have the same kernel. Concatenation with the isomorphism $\hat{\varepsilon}^1$ yields the surjective morphism of right Λ-modules

$$\hat{\varepsilon} := \hat{\varepsilon}^1 \circ \hat{\varepsilon}^0 : \tilde{P}_1 \longrightarrow \mathbb{Z}_{(p)},$$

for which we have $\ker \hat{\varepsilon} = \ker \hat{e}_{1,1}$.

With these properties of $\hat{\varepsilon}$ and Lemma 13, we are able to directly formulate a projective resolution of $\mathbb{Z}_{(p)}$:

We set

$$\tilde{\mathrm{Pr}}_i := \begin{cases} \tilde{P}_{\omega(i)} & i \geq 0 \\ 0 & i < 0 \end{cases},$$

where the integer $\omega(i)$ is given by the following construction: Recall the stipulation $l := 2(p-1)$. We have $i = jl + r$ for some $j \in \mathbb{Z}$ and $0 \leq r \leq l-1$. Then

$$\omega(i) := \begin{cases} r+1 & \text{for } 0 \leq r \leq p-2 \\ l - r = 2(p-1) - r & \text{for } p-1 \leq r \leq 2(p-1)-1 = l-1 \end{cases}. \tag{6}$$

So $\omega(i)$ increases by steps of one from 1 to $p-1$ as i runs from jl to $jl+(p-2)$ and $\omega(i)$ decreases from $p-1$ to 1 as i runs from $jl+(p-1)$ to $jl+(l-1)$. Finally we set

$$\hat{d}_i := \begin{cases} \hat{e}_{\omega(i-1),\omega(i)} : \tilde{P}_{\omega(i)} \to \tilde{P}_{\omega(i-1)} & i \geq 1 \\ 0 & i \leq 0 \end{cases}.$$

Now Lemma 13 gives the projective resolution of $\mathbb{Z}_{(p)}$

$$\cdots \xrightarrow{\hat{d}_3} \tilde{\mathrm{Pr}}_2 \xrightarrow{\hat{d}_2} \tilde{\mathrm{Pr}}_1 \xrightarrow{\hat{d}_1} \tilde{\mathrm{Pr}}_0 \xrightarrow{0=\hat{d}_0} 0 \to \cdots , \tag{7}$$

written more explicitly as

$$\begin{aligned} \cdots \to \tilde{P}_2 \xrightarrow{\hat{e}_{1,2}} \tilde{P}_1 \xrightarrow{\hat{e}_{1,1}} \tilde{P}_1 \xrightarrow{\hat{e}_{2,1}} \tilde{P}_2 \to \ldots \to \tilde{P}_{p-2} \xrightarrow{\hat{e}_{p-1,p-2}} \tilde{P}_{p-1} \\ \xrightarrow{\hat{e}_{p-1,p-1}} \tilde{P}_{p-1} \xrightarrow{\hat{e}_{p-2,p-1}} \tilde{P}_{p-2} \to \ldots \to \tilde{P}_2 \xrightarrow{\hat{e}_{1,2}} \tilde{P}_1 \to 0 \to \cdots . \end{aligned}$$

The corresponding extended projective resolution is

$$\begin{aligned} \cdots \to \tilde{P}_2 \xrightarrow{\hat{e}_{1,2}} \tilde{P}_1 \xrightarrow{\hat{e}_{1,1}} \tilde{P}_1 \xrightarrow{\hat{e}_{2,1}} \tilde{P}_2 \to \ldots \to \tilde{P}_{p-2} \xrightarrow{\hat{e}_{p-1,p-2}} \tilde{P}_{p-1} \\ \xrightarrow{\hat{e}_{p-1,p-1}} \tilde{P}_{p-1} \xrightarrow{\hat{e}_{p-2,p-1}} \tilde{P}_{p-2} \to \ldots \to \tilde{P}_2 \xrightarrow{\hat{e}_{1,2}} \tilde{P}_1 \xrightarrow{\hat{\varepsilon}} \mathbb{Z}_{(p)} \to 0 \to \cdots , \end{aligned}$$

which is an exact sequence.

We have proven the

Theorem 14. *Recall that $p \geq 3$ is a prime.*
The sequence (7) is a projective resolution of $\mathbb{Z}_{(p)}$, with augmentation $\tilde{\mathrm{Pr}}_0 = \tilde{P}_1 \xrightarrow{\hat{\varepsilon}} \mathbb{Z}_{(p)}$.

Lemma 15. *Recall that $p \geq 3$ is a prime. We have*

$$\begin{array}{lcll} \hat{e}_{1,1} + \hat{e}_{1,2} \circ \hat{e}_{2,1} & = & p\hat{e}_1 & \\ \hat{e}_{k,k-1} \circ \hat{e}_{k-1,k} + \hat{e}_{k,k+1} \circ \hat{e}_{k+1,k} & = & p\hat{e}_k & \text{for } k \in [2, p-2] \\ \hat{e}_{p-1,p-2} \circ \hat{e}_{p-2,p-1} + \hat{e}_{p-1,p-1} & = & p\hat{e}_{p-1} & \\ \hat{\varepsilon} \circ \hat{e}_{1,1} & = & p\hat{\varepsilon}. & \end{array}$$

Proof. We have by Remark 11

$$\begin{aligned} T_{\tilde{e}_1,\tilde{e}_1}(\hat{e}_{1,1} + \hat{e}_{1,2} \circ \hat{e}_{2,1}) &= T_{\tilde{e}_1,\tilde{e}_1}(\hat{e}_{1,1}) + T_{\tilde{e}_1,\tilde{e}_2}(\hat{e}_{1,2}) T_{\tilde{e}_2,\tilde{e}_1}(\hat{e}_{2,1}) \\ &= p\eta_{\lambda^1,1,1} + p\eta_{\lambda^2,1,n_c^2+1}\eta_{\lambda^2,n_c^2+1,1} = p(\eta_{\lambda^1,1,1} + \eta_{\lambda^2,1,1}) = T_{\tilde{e}_1,\tilde{e}_1}(p\hat{e}_1) \\ T_{\tilde{e}_k,\tilde{e}_k}(\hat{e}_{k,k-1} \circ \hat{e}_{k-1,k} &+ \hat{e}_{k,k+1} \circ \hat{e}_{k+1,k}) \\ &= T_{\tilde{e}_k,\tilde{e}_{k-1}}(\hat{e}_{k,k-1}) T_{\tilde{e}_{k-1},\tilde{e}_k}(\hat{e}_{k-1,k}) + T_{\tilde{e}_k,\tilde{e}_{k+1}}(\hat{e}_{k,k+1}) T_{\tilde{e}_{k+1},\tilde{e}_k}(\hat{e}_{k+1,k}) \\ &= \eta_{\lambda^k,n_c^k+1,1} p\eta_{\lambda^k,1,n_c^k+1} + p\eta_{\lambda^{k+1},1,n_c^{k+1}+1}\eta_{\lambda^{k+1},n_c^{k+1}+1,1} \\ &= p(\eta_{\lambda^k,n_c^k+1,n_c^k+1} + \eta_{\lambda^{k+1},1,1}) = T_{\tilde{e}_k,\tilde{e}_k}(p\hat{e}_k) \\ T_{\tilde{e}_{p-1},\tilde{e}_{p-1}}(\hat{e}_{p-1,p-2} \circ \hat{e}_{p-2,p-1} &+ \hat{e}_{p-1,p-1}) \end{aligned}$$

$$
\begin{aligned}
&= T_{\tilde{e}_{p-1},\tilde{e}_{p-2}}(\hat{e}_{p-1,p-2})T_{\tilde{e}_{p-2},\tilde{e}_{p-1}}(\hat{e}_{p-2,p-1}) + T_{\tilde{e}_{p-1},\tilde{e}_{p-1}}(\hat{e}_{p-1,p-1}) \\
&= \eta_{\lambda^{p-1},n_c^{p-1}+1,1}p\eta_{\lambda^{p-1},1,n_c^{p-1}+1} + p\eta_{\lambda^p,1,1} \\
&= p(\eta_{\lambda^{p-1},n_c^{p-1}+1,n_c^{p-1}+1} + \eta_{\lambda^p,1,1}) = T_{\tilde{e}_{p-1},\tilde{e}_{p-1}}(p\hat{e}_{p-1}).
\end{aligned}
$$

Finally for $x \in \tilde{P}_1$, we have

$$(\hat{\varepsilon}^0 \circ \hat{e}_{1,1})(x) = \eta_{\lambda^1,1,1} \cdot p\eta_{\lambda^1,1,1} \cdot x = p\eta_{\lambda^1,1,1} \cdot x = p\hat{\varepsilon}^0(x),$$

thus $\hat{\varepsilon} \circ \hat{e}_{1,1} = \hat{\varepsilon}^1 \circ \hat{\varepsilon}^0 \circ \hat{e}_{1,1} = p\hat{\varepsilon}^1 \circ \hat{\varepsilon}^0 = p\hat{\varepsilon}$. □

1.3. A projective resolution of $\mathbb{F}_p$ over $\mathbb{F}_p\mathrm{S}_p$

We obtain the desired projective resolution by reducing the projective resolution of $\mathbb{Z}_{(p)}$ "modulo p". Technically this will be done via a tensor product functor.

Reduction modulo I

Let R be a principal ideal domain. Let (A, ρ) be an R-algebra. Let I be an ideal of R. We set $\bar{R} := R/I$.

As R is a principal ideal domain, $\rho(I)A$ is an additive subset of A. As $\rho(I)$ is a subset of the center of A, $\rho(I)A$ is an ideal of A and $A/(\rho(I)A) =: \bar{A}$ is an $\bar{R}$-algebra.

We regard a right A-module M_A as a right R-module M_R via $m \cdot r := m \cdot \rho(r)$ for $m \in M$, $r \in R$.

Lemma 16. *The functors $-\underset{A}{\otimes}\bar{A}$ and $-\underset{R}{\otimes}\bar{R}$ from* Mod-A *to* Mod-R *are naturally isomorphic. The natural isomorphism $-\underset{A}{\otimes}\bar{A} \to -\underset{R}{\otimes}\bar{R}$ is given at the module M_A by*

$$
\begin{array}{rcl}
M_A \underset{A}{\otimes} {}_A\bar{A} & \xrightarrow{\sim} & M_R \underset{R}{\otimes} {}_R\bar{R} \\
m \otimes (a + \rho(I)A) & \longmapsto & ma \otimes (1 + I) \\
m \otimes (r + \rho(I)A) & \longleftarrow & m \otimes (r + I).
\end{array}
$$

Proof. By the universal property of the tensor product, the two maps given above are well-defined and R-linear. Straightforward calculation gives that they invert each other and that we have a natural transformation. □

Lemma 17. *The functor $-\underset{A}{\otimes} {}_A\bar{A}_{\bar{A}}$ from* Mod-A *to* Mod-$\bar{A}$ *maps exact sequences of right A-modules that are free and of finite rank as R-modules to exact sequences of right $\bar{A}$-modules.*

Proof. Because $-\underset{A}{\otimes} {}_A\bar{A}_{\bar{A}}$ is an additive functor, it maps complexes to complexes. For considerations of exactness, we may compose our functor with the forgetful functor from $\mathtt{Mod}\text{-}\bar{A}$ to $\mathtt{Mod}\text{-}R$. This composite is $-\underset{A}{\otimes}{}_A\bar{A}$. By the natural isomorphism given in Lemma 16, it suffices to show that $-\underset{R}{\otimes}{}_R\bar{R}$ transforms exact sequences of right A-modules that are free and of finite rank as R-modules into exact sequences.

Let $\cdots \xrightarrow{d_{i+1}} M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$ be an exact sequence of right A-modules that are free and of finite rank as R-modules. Then $\operatorname{im} d_i$ is a submodule of the free R-module M_{i-1}. As R is a principal ideal domain, $\operatorname{im} d_i$ is free. Hence the short exact sequence $\operatorname{im} d_{i+1} \to M_i \to \operatorname{im} d_i$ splits. Now the additive functor $-\underset{R}{\otimes}{}_R\bar{R}$ maps split short exact sequences to (split) short exact sequences and the proof is complete. $\square$

Reduction modulo p

The isomorphism $\mathbb{Z}_{(p)}\mathrm{S}_p \to \Lambda$ from Proposition 5 induces an isomorphism of $\mathbb{F}_p$-algebras $\mathbb{F}_p\mathrm{S}_p = \mathbb{Z}_{(p)}\mathrm{S}_p\,/(p\mathbb{Z}_{(p)}\mathrm{S}_p) \xrightarrow{\bar{r}} \Lambda/(p\Lambda) =: \bar{\Lambda}$. For the sake of simplicity in the next step, we identify $\bar{\Lambda}$ and $\mathbb{F}_p\mathrm{S}_p$ along $\bar{r}$.

Lemma 18. *Recall that $p \geq 3$ is a prime. Applying the functor $-\underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}}$, we obtain*

- *the projective modules $P_k := \tilde{P}_k \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}}$ for $k \in [1, p-1]$,*
- *$\mathbb{F}_p := \mathbb{Z}_{(p)} \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}}$ (the $\mathbb{F}_p\mathrm{S}_p$-module corresponding to the trivial representation of S_p),*
- $$\begin{array}{llll} e_k & := \hat{e}_k \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}} & \in \operatorname{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_k, P_k) & \text{for } k \in [1, p-1], \\ e_{1,1} & := \hat{e}_{1,1} \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}} & \in \operatorname{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1, P_1), & \\ e_{p-1,p-1} & := \hat{e}_{p-1,p-1} \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}} & \in \operatorname{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_{p-1}, P_{p-1}), & \\ e_{k+1,k} & := \hat{e}_{k+1,k} \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}} & \in \operatorname{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_k, P_{k+1}) & \text{for } k \in [1, p-2], \\ e_{k,k+1} & := \hat{e}_{k,k+1} \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}} & \in \operatorname{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_{k+1}, P_k) & \text{for } k \in [1, p-2], \end{array}$$
  cf. Definition 12, and
- *$\varepsilon := \hat{\varepsilon} \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}} \in \operatorname{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1, \mathbb{F}_p)$, which is surjective as $\hat{\varepsilon}$ is surjective.*

So we obtain

$$\operatorname{PRes}\mathbb{F}_p := (\operatorname{PRes}\mathbb{Z}_{(p)}) \underset{\Lambda}{\otimes}{}_\Lambda\bar{\Lambda}_{\bar{\Lambda}} = (\cdots \xrightarrow{d_3} \mathrm{Pr}_2 \xrightarrow{d_2} \mathrm{Pr}_1 \xrightarrow{d_1} \mathrm{Pr}_0 \xrightarrow{0=d_0} 0 \to \cdots), \tag{8}$$

$$\mathrm{Pr}_i := \begin{cases} P_{\omega(i)} & i \geq 0 \\ 0 & i < 0 \end{cases} \qquad d_i := \begin{cases} e_{\omega(i-1),\omega(i)} : P_{\omega(i)} \to P_{\omega(i-1)} & i \geq 1 \\ 0 & i \leq 0, \end{cases}$$

which is by Lemma 17 a projective resolution of $\mathbb{F}_p$, with augmentation $\varepsilon : P_1 \to \mathbb{F}_p$. More explicitly, $\mathrm{PRes}\,\mathbb{F}_p$ *is*

$$\begin{aligned} \ldots \to \underbrace{P_2}_{l+1} \xrightarrow{e_{1,2}} \underbrace{P_1}_{l=2(p-1)} \xrightarrow{e_{1,1}} \underbrace{P_1}_{(p-2)+p-1} \xrightarrow{e_{2,1}} \underbrace{P_2}_{(p-2)+p-2} \to \ldots \to \underbrace{P_{p-2}}_{p=(p-2)+2} \xrightarrow{e_{p-1,p-2}} \underbrace{P_{p-1}}_{(p-2)+1} \\ \xrightarrow{e_{p-1,p-1}} \underbrace{P_{p-1}}_{p-2} \xrightarrow{e_{p-2,p-1}} \underbrace{P_{p-2}}_{p-3} \to \ldots \to \underbrace{P_2}_{1} \xrightarrow{e_{1,2}} \underbrace{P_1}_{0} \to 0, \end{aligned}$$

and the corresponding extended projective resolution is

$$\begin{aligned} \ldots \to P_2 \xrightarrow{e_{1,2}} P_1 \xrightarrow{e_{1,1}} P_1 \xrightarrow{e_{2,1}} P_2 \to \ldots \to P_{p-2} \xrightarrow{e_{p-1,p-2}} P_{p-1} \\ \xrightarrow{e_{p-1,p-1}} P_{p-1} \xrightarrow{e_{p-2,p-1}} P_{p-2} \to \ldots \to P_2 \xrightarrow{e_{1,2}} P_1 \xrightarrow{\varepsilon} \mathbb{F}_p \to 0. \end{aligned}$$

Lemma 19. *Recall that $p \geq 3$ is a prime.*

(a) *We have the relations*

$$\begin{array}{lcll} e_{1,1} + e_{1,2} \circ e_{2,1} & = & 0 & \\ e_{k,k-1} \circ e_{k-1,k} + e_{k,k+1} \circ e_{k+1,k} & = & 0 & \textit{for } k \in [2, p-2] \\ e_{p-1,p-2} \circ e_{p-2,p-1} + e_{p-1,p-1} & = & 0 & \\ \varepsilon \circ e_{1,1} & = & 0 & \end{array}$$

and e_k is the identity on P_k for $k \in [1, p-1]$.

(b) *Given $k \in [2, p-1]$, we have* $\mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_k, \mathbb{F}_p) = \{0\}$.

(c) *Given $k, k' \in [1, p-1]$ such that $|k - k'| > 1$, we have* $\mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_k, P_{k'}) = \{0\}$.

(d) *The set $\{\varepsilon\}$ is an $\mathbb{F}_p$-basis of* $\mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1, \mathbb{F}_p)$.

Proof. For $k \in [1, p-1]$, we denote the idempotent $\tilde{e}_k + p\Lambda \in \bar{\Lambda} = \Lambda/p\Lambda = \mathbb{F}_p\mathrm{S}_p$ by $\dot{e}_k$ and identify P_k with $\dot{e}_k\mathbb{F}_p\mathrm{S}_p$.

Ad (a). This results immediately from Lemma 15 and the fact that $\hat{e}_k$ is the identity on $\tilde{P}_k$.

Ad (b). For $y \in \mathbb{Z}_{(p)}$, we have $y \cdot \tilde{e}_k = 0$ as $\tilde{e}_k^{\lambda^1} = 0$. Thus for $x \in \mathbb{F}_p$, we have $x \cdot \dot{e}_k = 0$. Now for $g \in \mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_k, \mathbb{F}_p)$, we have $g(\dot{e}_k) = g(\dot{e}_k \cdot \dot{e}_k) = g(\dot{e}_k)\dot{e}_k = 0$. As P_k is generated by $\dot{e}_k$, we have $g = 0$.

Ad (c). The sets $\{\lambda^k, \lambda^{k+1}\}$ and $\{\lambda^{k'}, \lambda^{k'+1}\}$ are disjoint. Thus for all $y \in \tilde{P}_{k'}$, we have $y \cdot \tilde{e}_k = 0$, which implies $x \cdot \dot{e}_k = 0$ for all $x \in P_{k'} = \dot{e}_{k'}\mathbb{F}_p\mathrm{S}_p$. Now for $g \in \mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_k, P_{k'})$, we have $g(\dot{e}_k) = g(\dot{e}_k \cdot \dot{e}_k) = g(\dot{e}_k)\dot{e}_k = 0$. As P_k is generated by $\dot{e}_k$, we have $g = 0$.

Ad (d). As P_1 is $\mathbb{F}_p\,\mathrm{S}_p$-generated by $\dot{e}_1$, an element $f \in \mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1, \mathbb{F}_p)$ is determined uniquely by $f(\dot{e}_1)$. Furthermore $\mathbb{F}_p$ has $\mathbb{F}_p$-dimension 1, thus $\{f\}$ is a basis of $\mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1, \mathbb{F}_p)$ for any $f \in \mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1, \mathbb{F}_p)$ with $f(\dot{e}_1) \neq 0$. As $\varepsilon(\dot{e}_1)$ determines ε, and as ε maps surjectively onto $\mathbb{F}_p$, we have $\varepsilon(\dot{e}_1) \neq 0$. So $\{\varepsilon\}$ is an $\mathbb{F}_p$-basis of $\mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1, \mathbb{F}_p)$. $\square$

2. A_∞-algebras

2.1. General theory

In this subsection, we review results presented in [12].

Let R be a commutative ring. We understand linear maps between R-modules to be R-linear. Tensor products are tensor products over R.

Definition 20. A *graded R-module V* is a R-module of the form $V = \oplus_{q\in\mathbb{Z}} V^q$. An element $v_q \in V^q$, $q \in \mathbb{Z}$ is said to be of degree q. An element $v \in V$ is called *homogeneous* if there is an integer $q \in \mathbb{Z}$ such that $v \in V^q$. For homogeneous elements v resp. graded maps g (see below), we denote their degrees by $|v|$ resp. $|g|$.

Definition 21. Let $A = \oplus_{q\in\mathbb{Z}} A^q$, $B = \oplus_{q\in\mathbb{Z}} B^q$ be two graded R-modules. A *graded map of degree $z \in \mathbb{Z}$* is a linear map $g : A \to B$ such that $\operatorname{im} g\big|_{A^q} \subseteq B^{q+z}$ for $q \in \mathbb{Z}$.

Definition 22. Let $A = \oplus_{q\in\mathbb{Z}} A^q$, $B = \oplus_{q\in\mathbb{Z}} B^q$ be two graded R-modules. We have

$$A \otimes B = \bigoplus_{z_1,z_2\in\mathbb{Z}} A^{z_1} \otimes B^{z_2} = \bigoplus_{q\in\mathbb{Z}} \left(\bigoplus_{z_1+z_2=q} A^{z_1} \otimes B^{z_2} \right).$$

As we understand the direct sums to be internal direct sums in $A \otimes B$ and understand $A^{z_1} \otimes B^{z_2}$ to be the linear span of the set $\{a \otimes b \in A \otimes B \mid a \in A^{z_1}, b \in A^{z_2}\}$, we have equations in the above, not just isomorphisms.

We then set $A \otimes B$ to be graded by $A \otimes B = \bigoplus_{q\in\mathbb{Z}} (A \otimes B)^q$, where $(A \otimes B)^q := \bigoplus_{z_1+z_2=q} A^{z_1} \otimes B^{z_2}$.

Moreover, we grade the direct sum

$$A \oplus B = \bigoplus_{q\in\mathbb{Z}} (A^q \oplus B^q)$$

by $(A \oplus B)^q := A^q \oplus B^q$.

Definition 23. In the definition of the tensor product of graded maps, we implement the *Koszul sign rule*: Let A_1, A_2, B_1, B_2 be graded R-modules and $g : A_1 \to B_1$, $h : A_2 \to B_2$ graded maps. Then we set

$$(g \otimes h)(x \otimes y) := (-1)^{|h|\cdot|x|} g(x) \otimes h(y), \tag{9}$$

where $x \in A_1, y \in A_2$ are homogeneous elements. Note that $g \otimes h$ has degree $|g \otimes h| = |g| + |h|$.

Remark 24. It is known that for graded R-modules A, B, C, the map

$$\begin{array}{rccc} \Theta : & (A \otimes B) \otimes C & \longrightarrow & A \otimes (B \otimes C) \\ & (a \otimes b) \otimes c & \longmapsto & a \otimes (b \otimes c) \end{array} \tag{10}$$

is an isomorphism of R-modules. Because of the following, Θ is homogeneous of degree 0.

$$\begin{aligned}
((A \otimes B) \otimes C)^q &= \bigoplus_{y+z_3=q} (A \otimes B)^y \otimes C^{z_3} = \bigoplus_{y+z_3=q} \bigoplus_{z_1+z_2=y} (A^{z_1} \otimes B^{z_2}) \otimes C^{z_3} \\
&= \bigoplus_{z_1+z_2+z_3=q} (A^{z_1} \otimes B^{z_2}) \otimes C^{z_3} \\
(A \otimes (B \otimes C))^q &= \bigoplus_{z_1+y=q} A^{z_1} \otimes (B \otimes C)^y = \bigoplus_{z_1+y=q} \bigoplus_{z_2+z_3=y} A^{z_1} \otimes (B^{z_2} \otimes C^{z_3}) \\
&= \bigoplus_{z_1+z_2+z_3=q} A^{z_1} \otimes (B^{z_2} \otimes C^{z_3})
\end{aligned}$$

Let $A_1, A_2, B_1, B_2, C_1, C_2$ be graded R-modules, $f : A_1 \to A_2$, $g : B_1 \to B_2$, $h : C_1 \to C_2$ graded maps. For homogeneous elements $x \in A_1$, $y \in B_1$, $z \in C_1$, we have

$$\begin{aligned}
((f \otimes g) \otimes h)((x \otimes y) \otimes z) &= (-1)^{|x \otimes y| \cdot |h|} ((f \otimes g)(x \otimes y)) \otimes h(z) \\
&= (-1)^{(|x|+|y|)|h| + |x| \cdot |g|} (f(x) \otimes g(y)) \otimes h(z) \\
(f \otimes (g \otimes h))(x \otimes (y \otimes z)) &= (-1)^{|x| \cdot |g \otimes h|} f(x) \otimes ((g \otimes h)(y \otimes z)) \\
&= (-1)^{|x|(|g|+|h|) + |y| \cdot |h|} f(x) \otimes (g(y) \otimes h(z)) \\
&= (-1)^{(|x|+|y|)|h| + |x| \cdot |g|} f(x) \otimes (g(y) \otimes h(z)).
\end{aligned}$$

Thus we have the following commutative diagram (Θ_1 and Θ_2 are derived from (10))

$$\begin{tikzcd}
(A_1 \otimes B_1) \otimes C_1 \arrow[r, "\Theta_1"] \arrow[d, "(f \otimes g) \otimes h"] & A_1 \otimes (B_1 \otimes C_1) \arrow[d, "f \otimes (g \otimes h)"] \\
(A_2 \otimes B_2) \otimes C_2 \arrow[r, "\Theta_2"] & A_2 \otimes (B_2 \otimes C_2)
\end{tikzcd}$$

It is therefore valid to use Θ as an identification and to omit the brackets for the tensorization of graded R-modules and the tensorization of graded maps.

Concerning the signs in the definition of A$_\infty$-algebras and A$_\infty$-morphisms, we follow the variant given e.g. in [16].

Definition 25. Let $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

(i) Let A be a graded R-module. A *pre-*A$_n$*-structure on* A is a family of graded maps $(m_k : A^{\otimes k} \to A)_{k \in [1,n]}$ with $|m_k| = 2 - k$ for $k \in [1, n]$. The tuple $(A, (m_k)_{k \in [1,n]})$ is called a pre-A$_n$-algebra.

(ii) Let A, A' be graded R-modules. A *pre-*A$_n$*-morphism from* A' *to* A is a family of graded maps $(f_k : A'^{\otimes k} \to A)_{k \in [1,n]}$ with $|f_k| = 1 - k$ for $k \in [1, n]$.

Definition 26. Let $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

(i) An A_n-*algebra* is a pre-A_n-algebra $(A,(m_k)_{k\in[1,n]})$ such that for $k \in [1,n]$

$$\sum_{\substack{k=r+s+t,\\ r,t\geq 0, s\geq 1}} (-1)^{rs+t} m_{r+1+t} \circ (1^{\otimes r} \otimes m_s \otimes 1^{\otimes t}) = 0. \tag{11)[k}$$

In abuse of notation, we sometimes abbreviate $A = (A,(m_k)_{k\geq 1})$ for A_∞-algebras.

(ii) Let $(A',(m'_k)_{k\in[1,n]})$ and $(A,(m_k)_{k\in[1,n]})$ be A_n-algebras. An A_n-*morphism* or *morphism of* A_n-*algebras* from $(A',(m'_k)_{k\in[1,n]})$ to $(A,(m_k)_{k\in[1,n]})$ is a pre-A_n-morphism $(f_k)_{k\in[1,n]}$ such that for $k \in [1,n]$, we have

$$\sum_{\substack{k=r+s+t\\ r,t\geq 0,s\geq 1}} (-1)^{rs+t} f_{r+1+t} \circ (1^{\otimes r} \otimes m'_s \otimes 1^{\otimes t}) = \sum_{\substack{1\leq r\leq k\\ i_1+\ldots+i_r=k\\ i_s\geq 1}} (-1)^v m_r \circ (f_{i_1} \otimes f_{i_2} \otimes \ldots \otimes f_{i_r}), \tag{12)[k}$$

where

$$v := \sum_{1\leq t<s\leq r} (1-i_s)i_t.$$

Example 27 (dg-algebras)**.** Let $(A,(m_k)_{k\geq 1})$ be an A_∞-algebra. If $m_n = 0$ for $n \geq 3$ then A is called a *differential graded algebra* or *dg-algebra*. In this case the equations (11)[n] for $n \geq 4$ become trivial: We have $(r+1+t)+s = n+1 \Rightarrow (r+1+t)+s \geq 5$ $\Rightarrow m_{r+1+t} = 0$ or $m_s = 0$. So all summands in (11)[n] are zero for $n \geq 4$. Here are the equations for $n \in \{1,2,3\}$:

$$\begin{aligned}
&(11)[1]: && 0 = m_1 \circ m_1\\
&(11)[2]: && 0 = m_1 \circ m_2 - m_2 \circ (m_1 \otimes 1 + 1 \otimes m_1)\\
&(11)[3]: && 0 = m_1 \circ m_3 + m_2 \circ (1 \otimes m_2 - m_2 \otimes 1)\\
& && \quad + m_3 \circ (m_1 \otimes 1^{\otimes 2} + 1 \otimes m_1 \otimes 1 + 1^{\otimes 2} \otimes m_1)\\
& && \overset{m_3=0}{=} m_2 \circ (1 \otimes m_2 - m_2 \otimes 1)
\end{aligned}$$

So (11)[1] ensures that m_1 is a differential. Moreover, (11)[3] states that m_2 is an associative binary operation, since for homogeneous $x,y,z \in A$ we have $0 = m_2 \circ (1 \otimes m_2 - m_2 \otimes 1)(x \otimes y \otimes z) = m_2(x \otimes m_2(y \otimes z) - m_2(x \otimes y) \otimes z)$, where because of $|m_2| = 0$ there are no additional signs caused by the Koszul sign rule. Equation (11)[2] is the Leibniz rule which can be motivated by the product rule in the algebra of differential forms on a smooth manifold: We set $m_1 f := \partial f$ and $m_2(f \otimes g) := f \wedge g$ and we have for homogeneous differential forms f, g

$$\partial(f \wedge g) = (\partial f) \wedge g + (-1)^{|f|} f \wedge (\partial g).$$

The signs on the right side also motivate the Koszul sign rule.

Example 28 (A_n-morphisms induce complex morphisms)**.**
Let $n \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$. Let $(A', (m'_k)_{k\in[1,n]})$ and $(A, (m_k)_{k\in[1,n]})$ be two A_n-algebras and let $(f_k)_{k\in[1,n]} : (A', (m'_k)_{k\in[1,n]}) \to (A, (m_k)_{k\in[1,n]})$ be an A_n-morphism.

By (11)[1], (A', m'_1) and (A, m_1) are complexes. Equation (12)[1] is

$$f_1 \circ m'_1 = m_1 \circ f_1.$$

Thus $f_1 : (A', m'_1) \to (A, m_1)$ is a complex morphism.

For $n \geq 2$, we have also (12)[2]:

$$f_1 \circ m'_2 - f_2 \circ (m'_1 \otimes 1 + 1 \otimes m'_1) = m_1 \circ f_2 + m_2 \circ (f_1 \otimes f_1) \tag{13}$$

Recall the conventions concerning $\mathrm{Hom}^k_B(C, C')$.

Lemma 29. *Let B be an (ordinary) R-algebra and $M = ((M_i)_{i\in\mathbb{Z}}, (d_i)_{i\in\mathbb{Z}})$ a complex of B-modules, that is a sequence $(M_i)_{i\in\mathbb{Z}}$ of B-modules and B-linear maps $d_i : M_i \to M_{i-1}$ such that $d_{i-1} \circ d_i = 0$ for all $i \in \mathbb{Z}$. Let*

$$\begin{aligned}\mathrm{Hom}^i_B(M, M) &:= \prod_{z\in\mathbb{Z}} \mathrm{Hom}_B(M_{z+i}, M_z) \\ &= \{g = (g_z)_{z\in\mathbb{Z}} \mid g_z \in \mathrm{Hom}_B(M_{z+i}, M_z) \text{ for } z \in \mathbb{Z}\}.\end{aligned}$$

Then

$$A = \mathrm{Hom}^*_B(M, M) := \bigoplus_{i\in\mathbb{Z}} \mathrm{Hom}^i_B(M, M)$$

is a graded R-module. We have $d := (d_{z+1})_{z\in\mathbb{Z}} = \sum_{i\in\mathbb{Z}} \lfloor d_{i+1} \rfloor^i_{i+1} \in \mathrm{Hom}^1_B(M, M)$. We define $m_1 := d_{\mathrm{Hom}^*(M,M)} : A \to A$, that is for homogeneous $g \in A$ we have

$$m_1(g) = d \circ g - (-1)^{|g|} g \circ d.$$

We define $m_2 : A^{\otimes 2} \to A$ for homogeneous $g, h \in A$ to be composition, i.e.

$$m_2(g \otimes h) := g \circ h.$$

For $n \geq 3$ we set $m_n : A^{\otimes n} \to A$, $m_n = 0$. Then $(m_n)_{n\geq 1}$ is an A_∞-algebra structure on $A = \mathrm{Hom}^*_B(M, M)$. More precisely, $(A, (m_n)_{n\geq 1})$ is a dg-algebra.

Proof. Because of $|d| = 1$ we have $|m_1| = 1 = 2 - 1$. The graded map m_2 has degree $0 = 2 - 2$. The other maps m_n are zero and have therefore automatically correct degree. As discussed in Example 27 we only need to check (11)[n] for $n = 1, 2, 3$. Equation (11)[1] holds because for homogeneous $g \in A$ we have

$$m_1(m_1(g)) = m_1[d \circ g - (-1)^{|g|} g \circ d]$$

$$
\begin{aligned}
&= d \circ [d \circ g - (-1)^{|g|} g \circ d] - (-1)^{|g|+1} [d \circ g - (-1)^{|g|} g \circ d] \circ d \\
&\overset{d^2=0}{=} -(-1)^{|g|} d \circ g \circ d - (-1)^{|g|+1} d \circ g \circ d = 0.
\end{aligned}
$$

Concerning (11)[2], we have for homogeneous $g, h \in A$

$$
\begin{aligned}
(m_2 \circ (m_1 \otimes 1 + 1 \otimes m_1))(g \otimes h) &= m_2(m_1(g) \otimes h + (-1)^{|g|} g \otimes m_1(h)) \\
&= (d \circ g - (-1)^{|g|} g \circ d) \circ h + (-1)^{|g|} g \circ (d \circ h - (-1)^{|h|} h \circ d) \\
&= d \circ g \circ h - (-1)^{|g|+|h|} g \circ h \circ d \\
&= (m_1 \circ m_2)(g \otimes h).
\end{aligned}
$$

The map m_2 is induced by the composition of morphisms which is associative. As discussed in Example 27, equation (11)[3] holds. $\square$

Remark 30. In $\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_p, \mathrm{PRes}\,\mathbb{F}_p)$ we have (cf. (8))

$$
d = \sum_{i \geq 0} \lfloor e_{\omega(i),\omega(i+1)} \rfloor_{i+1}^{i} .
$$

Definition 31 (Homology of A_∞-algebras, quasi-isomorphisms, minimality, minimal models)**.** As $m_1^2 = 0$ (cf. (11)[1]) and $|m_1| = 1$, we have the complex

$$
\cdots \to A^{i-1} \xrightarrow{m_1|_{A^{i-1}}} A^i \xrightarrow{m_1|_{A^i}} A^{i+1} \to \cdots .
$$

We define $\mathrm{H}^k A := \ker(m_1|_{A^k}) / \operatorname{im}(m_1|_{A^{k-1}})$ and $\mathrm{H}^* A := \bigoplus_{k \in \mathbb{Z}} \mathrm{H}^k A$, which gives the homology of A the structure of a graded R-module.

A morphism of A_∞-algebras $(f_k)_{k \geq 1} : (A', (m'_k)_{k \geq 1}) \to (A, (m_k)_{k \geq 1})$ is called a *quasi-isomorphism* if the morphism of complexes $f_1 : (A', m'_1) \to (A, m_1)$ (cf. Example 28) is a quasi-isomorphism.

An A_∞-algebra is called *minimal*, if $m_1 = 0$. If A is an A_∞-algebra and A' is a minimal A_∞-algebra quasi-isomorphic to A, then A' is called a *minimal model of A*.

The existence of minimal models is assured by the following theorem.

Theorem 32. *(minimality theorem, cf. [13] (history), [9], [8], [20], [5], [7], [18], ...) Let $(A, (m_k)_{k \geq 1})$ be an A_∞-algebra such that the homology $\mathrm{H}^* A$ is a projective R-module. Then there exists an A_∞-algebra structure $(m'_k)_{k \geq 1}$ on $\mathrm{H}^* A$ and a quasi-isomorphism of A_∞-algebras $(f_k)_{k \geq 1} : (\mathrm{H}^* A, (m'_k)_{k \geq 1}) \to (A, (m_k)_{k \geq 1})$, such that*

- *$m'_1 = 0$ and*
- *the complex morphism $f_1 : (\mathrm{H}^* A, m'_1) \to (A, m_1)$ induces the identity in homology. I.e. each element $x \in \mathrm{H}^* A$, which is a homology class of (A, m_1), is mapped by f_1 to a representing cycle.*

We give a proof of Theorem 32 in appendix A.4, cf. Theorem 67.

There is a general statement concerning the computation of minimal models of dg-algebras:

Lemma 33 (cf. [24, Theorem 5])**.** *Let R be a commutative ring and $(A,(m_n)_{n\geq 1})$ be a dg-algebra (over R). Suppose given a graded R-module B and graded maps $f_n : B^{\otimes n} \to A$, $m'_n : B^{\otimes n} \to B$ for $n \geq 1$. Suppose given $k \geq 1$ such that*

$$\begin{aligned} f_i &= 0 && \text{for } i \geq k \\ m'_i &= 0 && \text{for } i \geq k+1, \end{aligned}$$

and such that (12)[n] is satisfied for $1 \leq n \leq 2k-2$. Then (12)[n] is satisfied for all $n \geq 1$.

Proof. We need to check (12)[n] for $n \geq 2k-1$:
The left side of (12)[n] is zero: For $f_{r+1+t} \circ (1^{\otimes r} \otimes m'_s \otimes 1^{\otimes t})$ to be non-zero it is necessary that $r+1+t \leq k-1$ and $s \leq k$, so $n+1 = r+s+t+1 \leq 2k-1$, which is not the case. Thus all summands on the left side of (12)[n] are zero.
The right side of (12)[n] is zero: As A is a dg-algebra, we have $m_n = 0$ for $n \geq 3$. So all non-zero summands on the right side have $r \leq 2$. For a non-zero summand we also have $i_y \leq k-1$ for all $y \in [1,r]$. So for those we have

$$n = \sum_{y=1}^{r} i_y \overset{r\leq 2}{\leq} 2(k-1) = 2k-2.$$

But $n \geq 2k-1$, so all summands on the right side of (12)[n] are zero. □

2.2. The homology of $\mathrm{Hom}^*_{\mathbb{F}_p \mathrm{S}_p}(\mathrm{PRes}\,\mathbb{F}_p, \mathrm{PRes}\,\mathbb{F}_p)$

We need a well-known result of homological algebra in a particular formulation:

Lemma 34. *Let F be a field. Let B be an F-algebra. Let M be a B-module. Let $Q = (\cdots \to Q_2 \xrightarrow{d_2} Q_1 \xrightarrow{d_1} Q_0 \to 0 \to \cdots)$ be a projective resolution of M with augmentation $\varepsilon : Q_0 \to M$, i.e. the sequence $\cdots \to Q_2 \xrightarrow{d_2} Q_1 \xrightarrow{d_1} Q_0 \xrightarrow{\varepsilon} M \to 0$ is exact. Then we have maps for $k \in \mathbb{Z}$*

$$\begin{aligned} \Psi_k : \mathrm{Hom}^k_B(Q,Q) &\to \mathrm{Hom}^k_B(Q,M) := \mathrm{Hom}_B(Q_k, M) \\ (g_i : Q_{i+k} \to Q_i)_{i\in\mathbb{Z}} &\mapsto \varepsilon \circ g_0 \end{aligned}$$

The right side is equipped with the differentials (dualization of d_k)

$$\begin{aligned} (d_k)^* : \mathrm{Hom}_B(Q_k, M) &\to \mathrm{Hom}_B(Q_{k+1}, M) \\ g &\mapsto (-1)^k g \circ d_k \end{aligned}$$

and the left side is equipped with the differential m_1 *of its dg-algebra structure, cf. Lemma 29.*

Then $(\Psi_k)_{k\in\mathbb{Z}}$ *becomes a complex morphism from the complex* $\mathrm{Hom}^*_B(Q,Q)$ *to the complex* $\mathrm{Hom}^*_B(Q,M)$ *that induces isomorphisms* $\bar{\Psi}_k$ *of* F*-vector spaces on the homology*

$$\bar{\Psi}_k : \mathrm{H}^k\,\mathrm{Hom}^*_B(Q,Q) \xrightarrow{\simeq} \mathrm{H}^k\,\mathrm{Hom}^*_B(Q,M)$$
$$\overline{(g_i : Q_{i+k} \to Q_i)_{i\in\mathbb{Z}}} \mapsto \overline{\varepsilon \circ g_0}$$

Lemma 34 is a special case of [3, §5 Proposition 4]: The complex morphism

$$\begin{tikzcd}
Q \arrow[d, "\psi"] & = & (\cdots \arrow[r] & Q_2 \arrow[r, "d_2"] \arrow[d] & Q_1 \arrow[r, "d_1"] \arrow[d] & Q_0 \arrow[r] \arrow[d, "\varepsilon"] & 0 \arrow[r] \arrow[d] & \cdots) \\
\mathrm{Conc}(M) & := & (\cdots \arrow[r] & 0 \arrow[r] & 0 \arrow[r] & M \arrow[r] & 0 \arrow[r] & \cdots)
\end{tikzcd}$$

is a quasi-isomorphism since Q is a projective resolution of M. Application of [3, §5 Proposition 4] now gives that the induced homomorphism $\Psi : \mathrm{Hom}^*_B(Q,Q) \to \mathrm{Hom}^*_B(Q,\mathrm{Conc}(M))$ is a quasi-isomorphism. By removing zero components of the elements of $\mathrm{Hom}^*_B(Q,\mathrm{Conc}(M))$, we readily obtain an isomorphism of complexes from $\mathrm{Hom}^*_B(Q,\mathrm{Conc}(M))$ to $\mathrm{Hom}^*_B(Q,M)$. Now composition of these two quasi-isomorphisms gives the quasi-isomorphism described in Lemma 34.

Proposition 35. *Recall that* $p \geq 3$ *is a prime and* $l = 2(p-1)$.
Write $A := \mathrm{Hom}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathrm{PRes}\,\mathbb{F}_p, \mathrm{PRes}\,\mathbb{F}_p)$. *Let*

$$\begin{aligned}
\iota &:= \sum_{i\geq 0} \lfloor e_{\omega(i)} \rfloor^{i}_{i+l} = \sum_{i\geq 0}\sum_{k=0}^{l-1} \lfloor e_{\omega(k)} \rfloor^{il+k}_{(i+1)l+k} \in A^l \\
\chi &:= \sum_{i\geq 0}\left(\lfloor e_1 \rfloor^{il}_{il+l-1} + \left(\sum_{k=1}^{p-2} \lfloor e_{k+1,k} \rfloor^{il+k}_{il+l-1+k} \right)\right. \\
&\qquad \left. + \lfloor e_{p-1} \rfloor^{il+(p-1)}_{il+l-1+(p-1)} + \left(\sum_{k=1}^{p-2} \lfloor e_{p-k-1,p-k} \rfloor^{il+(p-1)+k}_{il+l-1+(p-1)+k} \right)\right) \in A^{l-1}.
\end{aligned}$$

(a) *For* $j \geq 0$, *we have*

$$\iota^j = \sum_{i\geq 0} \lfloor e_{\omega(i)} \rfloor^{i}_{i+jl} = \sum_{i\geq 0}\sum_{k=0}^{l-1} \lfloor e_{\omega(k)} \rfloor^{il+k}_{(i+j)l+k}\,. \tag{14}$$

(b) *Suppose given* $y \geq 0$. *Let* $h \in A^y$ *be* l*-periodic, that is*

$$h = \sum_{i\geq 0}\sum_{k=0}^{l-1} \lfloor h_k \rfloor^{il+k}_{il+k+y}\,.$$

Then for $j \geq 0$, we have

$$h \circ \iota^j = \iota^j \circ h = \sum_{i \geq 0} \sum_{k=0}^{l-1} \lfloor h_k \rfloor_{(i+j)l+k+y}^{il+k} \in A^{y+jl}.$$

(c) *Suppose given $y \in \mathbb{Z}$. For $h \in A^y$ and $j \geq 0$, we have $m_1(h \circ \iota^j) = m_1(h) \circ \iota^j$.*

(d) *For $j \geq 0$, we have $m_1(\iota^j) = 0$. Thus ι^j is a cycle.*

(e) *For $j \geq 0$, we have*

$$\begin{aligned} \chi\iota^j &:= \chi \circ \iota^j = \iota^j \circ \chi \\ &= \sum_{i \geq 0} \Bigg(\lfloor e_1 \rfloor_{(i+j+1)l-1}^{il} + \left(\sum_{k=1}^{p-2} \lfloor e_{k+1,k} \rfloor_{(i+j+1)l-1+k}^{il+k} \right) \\ &\quad + \lfloor e_{p-1} \rfloor_{(i+j+1)l-1+(p-1)}^{il+(p-1)} + \left(\sum_{k=1}^{p-2} \lfloor e_{p-k-1,p-k} \rfloor_{(i+j+1)l-1+(p-1)+k}^{il+(p-1)+k} \right) \Bigg) \in A^{jl+l-1}. \end{aligned}$$

For convenience, we also define $\chi^0\iota^j := \iota^j$ and $\chi^1\iota^j := \chi\iota^j = \chi \circ \iota^j$ for $j \geq 0$.

(f) *For $j \geq 0$, we have $m_1(\chi\iota^j) = 0$. Thus $\chi\iota^j$ is a cycle.*

(g) *Suppose given $k \in \mathbb{Z}$. A $\mathbb{F}_p$-basis of $\mathrm{H}^k A$ is given by*

$$\begin{aligned} &\{\overline{\iota^j}\} \text{ if } k = jl \text{ for some } j \geq 0 \\ &\{\overline{\chi\iota^j}\} \text{ if } k = jl + l - 1 \text{ for some } j \geq 0 \\ &\emptyset \text{ else.} \end{aligned}$$

Thus the set $\mathfrak{B} := \{\overline{\iota^j} \mid j \geq 0\} \sqcup \{\overline{\chi\iota^j} \mid j \geq 0\}$ is an $\mathbb{F}_p$-basis of $\mathrm{H}^* A = \bigoplus_{z \in \mathbb{Z}} \mathrm{H}^z A$.

Before we proceed we display ι and χ for the case $p = 5$ as an example:
The period is of length $l = 2p - 2 = 2 \cdot 5 - 2 = 8$. The terms inside circles denote the degrees.

$$\mathrm{PRes}(\mathbb{F}_5)[8] \xrightarrow{\iota} \mathrm{PRes}(\mathbb{F}_5)$$

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] \\
8 & P_1 \arrow[r, "e_1"] \arrow[d, "e_{1,1}"'] & P_1 \arrow[d, "e_{1,1}"] \\
7 & P_1 \arrow[r, "e_1"] \arrow[d, "e_{2,1}"'] & P_1 \arrow[d, "e_{2,1}"] \\
6 & P_2 \arrow[r, "e_2"] \arrow[d, "e_{3,2}"'] & P_2 \arrow[d, "e_{3,2}"] \\
5 & P_3 \arrow[r, "e_3"] \arrow[d, "e_{4,3}"'] & P_3 \arrow[d, "e_{4,3}"] \\
4 & P_4 \arrow[r, "e_4"] \arrow[d, "e_{4,4}"'] & P_4 \arrow[d, "e_{4,4}"] \\
3 & P_4 \arrow[r, "e_4"] \arrow[d, "e_{3,4}"'] & P_4 \arrow[d, "e_{3,4}"] \\
2 & P_3 \arrow[r, "e_3"] \arrow[d, "e_{2,3}"'] & P_3 \arrow[d, "e_{2,3}"] \\
1 & P_2 \arrow[r, "e_2"] \arrow[d, "e_{1,2}"'] & P_2 \arrow[d, "e_{1,2}"] \\
0 & P_1 \arrow[r, "e_1"] \arrow[d, "e_{1,1}"'] & P_1 \arrow[d] \\
-1 & P_1 \arrow[r] \arrow[d, "e_{2,1}"'] & 0 \arrow[d] \\
-2 & P_2 \arrow[r] \arrow[d, "e_{3,2}"'] & 0 \arrow[d] \\
-3 & P_3 \arrow[r] \arrow[d, "e_{4,3}"'] & 0 \arrow[d] \\
-4 & P_4 \arrow[r] \arrow[d, "e_{4,4}"'] & 0 \arrow[d] \\
-5 & P_4 \arrow[r] \arrow[d, "e_{3,4}"'] & 0 \arrow[d] \\
-6 & P_3 \arrow[r] \arrow[d, "e_{2,3}"'] & 0 \arrow[d] \\
-7 & P_2 \arrow[r] \arrow[d, "e_{1,2}"'] & 0 \arrow[d] \\
-8 & P_1 \arrow[r] \arrow[d] & 0 \arrow[d] \\
-9 & 0 \arrow[r] \arrow[d] & 0 \arrow[d] \\
 & \vdots & \vdots
\end{tikzcd}$$

$$\mathrm{PRes}(\mathbb{F}_5)[8-1] \xrightarrow{\chi} \mathrm{PRes}(\mathbb{F}_5)$$

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] \\
9 & P_1 \arrow[r, "e_{2,1}"] \arrow[d, "-e_{1,1}"'] & P_2 \arrow[d, "e_{1,2}"] \\
8 & P_1 \arrow[r, "e_1"] \arrow[d, "-e_{2,1}"'] & P_1 \arrow[d, "e_{1,1}"] \\
7 & P_2 \arrow[r, "e_{1,2}"] \arrow[d, "-e_{3,2}"'] & P_1 \arrow[d, "e_{2,1}"] \\
6 & P_3 \arrow[r, "e_{2,3}"] \arrow[d, "-e_{4,3}"'] & P_2 \arrow[d, "e_{3,2}"] \\
5 & P_4 \arrow[r, "e_{3,4}"] \arrow[d, "-e_{4,4}"'] & P_3 \arrow[d, "e_{4,3}"] \\
4 & P_4 \arrow[r, "e_4"] \arrow[d, "-e_{3,4}"'] & P_4 \arrow[d, "e_{4,4}"] \\
3 & P_3 \arrow[r, "e_{4,3}"] \arrow[d, "-e_{2,3}"'] & P_4 \arrow[d, "e_{3,4}"] \\
2 & P_2 \arrow[r, "e_{3,2}"] \arrow[d, "-e_{1,2}"'] & P_3 \arrow[d, "e_{2,3}"] \\
1 & P_1 \arrow[r, "e_{2,1}"] \arrow[d, "-e_{1,1}"'] & P_2 \arrow[d, "e_{1,2}"] \\
0 & P_1 \arrow[r, "e_1"] \arrow[d, "-e_{2,1}"'] & P_1 \arrow[d] \\
-1 & P_2 \arrow[r] \arrow[d, "-e_{3,2}"'] & 0 \arrow[d] \\
-2 & P_3 \arrow[r] \arrow[d, "-e_{4,3}"'] & 0 \arrow[d] \\
-3 & P_4 \arrow[r] \arrow[d, "-e_{4,4}"'] & 0 \arrow[d] \\
-4 & P_4 \arrow[r] \arrow[d, "-e_{3,4}"'] & 0 \arrow[d] \\
-5 & P_3 \arrow[r] \arrow[d, "-e_{2,3}"'] & 0 \arrow[d] \\
-6 & P_2 \arrow[r] \arrow[d, "-e_{1,2}"'] & 0 \arrow[d] \\
-7 & P_1 \arrow[r] \arrow[d] & 0 \arrow[d] \\
-8 & 0 \arrow[r] \arrow[d] & 0 \arrow[d] \\
 & \vdots & \vdots
\end{tikzcd}$$

Proof of Proposition 35. The element ι is well-defined since $\omega(y) = \omega(l+y)$ for $y \geq 0$. In the definition of χ we need to check that the "$\lfloor * \rfloor_*^*$" are well defined. This is easily proven by calculating the $\omega(y)$ where y is the lower respective upper index of "$\lfloor * \rfloor_*^*$".

(a): As $\mathrm{Pr}_i = \{0\}$ for $i < 0$, the identity element of A is given by $\iota^0 = \sum_{i \geq 0} \lfloor e_{\omega(i)} \rfloor_i^i$, which agrees with (14) in case $j = 0$. So we have proven the induction basis for induction on j. So now assume that for some $j \geq 0$ the equation (14) holds. Then

$$\begin{aligned}\iota^{j+1} = \iota \circ \iota^j &= \left(\sum_{i \geq 0} \lfloor e_{\omega(i)} \rfloor_{i+l}^i \right) \circ \left(\sum_{i' \geq 0} \lfloor e_{\omega(i')} \rfloor_{i'+jl}^{i'} \right) \\ &= \sum_{i \geq 0} \lfloor e_{\omega(i)} \circ e_{\omega(i+l)} \rfloor_{i+l+jl}^i = \sum_{i \geq 0} \lfloor e_{\omega(i)} \rfloor_{i+(j+1)l}^i .\end{aligned}$$

Thus the proof by induction is complete.

(b): We have

$$\begin{aligned}\iota^j \circ h &= \left(\sum_{i \geq 0} \sum_{k=0}^{l-1} \lfloor e_{\omega(il+k)} \rfloor_{(i+j)l+k}^{il+k} \right) \circ \left(\sum_{i' \geq 0} \sum_{k'=0}^{l-1} \lfloor h_{k'} \rfloor_{i'l+k'+y}^{i'l+k'} \right) \overset{\substack{i' \rightsquigarrow i+j \\ k' \rightsquigarrow k}}{=} \sum_{i \geq 0} \sum_{k=0}^{l-1} \lfloor h_k \rfloor_{(i+j)l+k+y}^{il+k} \\ h \circ \iota^j &= \left(\sum_{i \geq 0} \sum_{k=0}^{l-1} \lfloor h_k \rfloor_{il+k+y}^{il+k} \right) \circ \left(\sum_{i' \geq 0} \lfloor e_{\omega(i')} \rfloor_{i'+jl}^{i'} \right) = \sum_{i \geq 0} \sum_{k=0}^{l-1} \lfloor h_k \rfloor_{(i+j)l+k+y}^{il+k} .\end{aligned}$$

So we have proven (b).

(c): The differential d of $\mathrm{PRes}\,\mathbb{F}_p$ is l-periodic (cf. Remark 30) and thus

$$\begin{aligned} m_1(h) \circ \iota^j &= (d \circ h - (-1)^y h \circ d) \circ \iota^j \\ &\overset{(b), |\iota^j| \equiv_2 0}{=} d \circ h \circ \iota^j - (-1)^{y + |\iota^j|} h \circ \iota^j \circ d = m_1(h \circ \iota^j).\end{aligned}$$

(d): We have

$$m_1(\iota^j) \overset{(c)}{=} m_1(\iota^0) \circ \iota^j = (d \circ \iota^0 - (-1)^0 \iota^0 d) \circ \iota^j = (d - d) \circ \iota^j = 0.$$

(e) is implied by (b) using the fact that χ is l-periodic.

(f): Because of (c) we have $m_1(\chi \iota^j) = m_1(\chi) \circ \iota^j$. Because $|\chi| = l - 1$ is odd we have

$$\begin{aligned} m_1(\chi) &= d \circ \chi - (-1) \chi \circ d = \chi \circ d + d \circ \chi \\ &\overset{\text{R.30}}{=} \left(\sum_{i \geq 0} \left(\lfloor e_1 \rfloor_{il+l-1}^{il} + \left[\sum_{k=1}^{p-2} \lfloor e_{k+1,k} \rfloor_{il+l-1+k}^{il+k} \right] + \lfloor e_{p-1} \rfloor_{il+l-1+(p-1)}^{il+(p-1)} \right.\right. \\ &\quad \left.\left. + \left[\sum_{k=1}^{p-2} \lfloor e_{p-k-1,p-k} \rfloor_{il+l-1+(p-1)+k}^{il+(p-1)+k} \right] \right) \right) \circ \left(\sum_{y \geq 0} \lfloor e_{\omega(y), \omega(y+1)} \rfloor_{y+1}^y \right)\end{aligned}$$

$$
\begin{aligned}
&+\left(\sum_{y\geq 0}\lfloor e_{\omega(y),\omega(y+1)}\rfloor^{y}_{y+1}\right)\circ\left(\sum_{i\geq 0}\left(\lfloor e_1\rfloor^{il}_{il+l-1}+\left[\sum_{k=1}^{p-2}\lfloor e_{k+1,k}\rfloor^{il+k}_{il+l-1+k}\right]\right.\right.\\
&\left.\left.+\lfloor e_{p-1}\rfloor^{il+(p-1)}_{il+l-1+(p-1)}+\left[\sum_{k=1}^{p-2}\lfloor e_{p-k-1,p-k}\rfloor^{il+(p-1)+k}_{il+l-1+(p-1)+k}\right]\right)\right)\\
&=\sum_{i\geq 0}\left(\lfloor e_1\circ e_{1,1}\rfloor^{il}_{il+l}+\left[\sum_{k=1}^{p-2}\lfloor e_{k+1,k}\circ e_{k,k+1}\rfloor^{il+k}_{il+l+k}\right]\right.\\
&\left.+\lfloor e_{p-1}\circ e_{p-1,p-1}\rfloor^{il+(p-1)}_{il+l+(p-1)}+\left[\sum_{k=1}^{p-2}\lfloor e_{p-k-1,p-k}\circ e_{p-k,p-k-1}\rfloor^{il+(p-1)+k}_{il+l+(p-1)+k}\right]\right)\\
&+\sum_{i\geq 1}\lfloor e_{1,1}\circ e_1\rfloor^{il-1}_{il+l-1}+\sum_{i\geq 0}\left(\left[\sum_{k=1}^{p-2}\lfloor e_{k,k+1}\circ e_{k+1,k}\rfloor^{il+k-1}_{il+l+k-1}\right]\right.\\
&\left.+\lfloor e_{p-1,p-1}\circ e_{p-1}\rfloor^{il-1+(p-1)}_{il+l-1+(p-1)}+\left[\sum_{k=1}^{p-2}\lfloor e_{p-k,p-k-1}\circ e_{p-k-1,p-k}\rfloor^{il-1+(p-1)+k}_{il+l-1+(p-1)+k}\right]\right)\\
&\overset{*}{=}\sum_{i\geq 0}\left(\lfloor e_{1,1}+e_{1,2}\circ e_{2,1}\rfloor^{il}_{il+l}+\left[\sum_{k=1}^{p-3}\lfloor e_{k+1,k}\circ e_{k,k+1}+e_{k+1,k+2}\circ e_{k+2,k+1}\rfloor^{il+k}_{il+l+k}\right]\right.\\
&+\lfloor e_{p-1,p-2}\circ e_{p-2,p-1}+e_{p-1,p-1}\rfloor^{il+p-2}_{il+l+p-2}+\lfloor e_{p-1,p-1}+e_{p-1,p-2}\circ e_{p-2,p-1}\rfloor^{il+p-1}_{il+l+p-1}\\
&+\left[\sum_{k=1}^{p-3}\lfloor e_{p-k-1,p-k}\circ e_{p-k,p-k-1}+e_{p-k-1,p-k-2}\circ e_{p-k-2,p-k-1}\rfloor^{il+p-1+k}_{il+l+p-1+k}\right]\\
&\left.+\lfloor e_{1,2}\circ e_{2,1}+e_{1,1}\rfloor^{(i+1)l-1}_{(i+1)l+l-1}\right)\overset{\mathrm{L.19}(a)}{=}0
\end{aligned}
$$

In the step marked by "$*$" we sort the summands by their targets. Note that when splitting sums of the form $\sum_{k=1}^{p-2}(\ldots)_k$ into $(\ldots)_1+\sum_{k=2}^{p-2}(\ldots)_k$ or into $(\ldots)_{p-2}+\sum_{k=1}^{p-3}(\ldots)_k$, the existence of the summand that is split off is ensured by $p\geq 3$.

(g): We first show that the differentials of the complex $\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_p,\mathbb{F}_p)$ (cf. Lemma 34) are all zero: By Lemma 19, $\{\varepsilon\}$ is an $\mathbb{F}_p$-basis of $\mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_1,\mathbb{F}_p)$, and for $k\in[2,p-1]$ we have $\mathrm{Hom}_{\mathbb{F}_p\mathrm{S}_p}(P_k,\mathbb{F}_p)=0$. So the only non-trivial $(d_k)^*$ are those where $\mathrm{Pr}_k=\mathrm{Pr}_{k+1}=P_1$. This is the case only when $k=lj+l-1$ for some $j\geq 0$. Then $d_k=e_{1,1}$. For $\varepsilon\in\mathrm{Hom}(P_1,\mathbb{F}_p)$, we have $(d_k)^*(\varepsilon)=(-1)^k\varepsilon\circ e_{1,1}\overset{\mathrm{L.19}(a)}{=}0$. As $\mathrm{Hom}(P_1,\mathbb{F}_p)=\langle\varepsilon\rangle_{\mathbb{F}_p}$, we have $(d_k)^*=0$.

So $\mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_p,\mathbb{F}_p)=\mathrm{Hom}^k(\mathrm{PRes}\,\mathbb{F}_p,\mathbb{F}_p)$. We use Lemma 34.

For $k=jl$, $j\geq 0$, we have $\bar{\Psi}^k(\overline{\iota^j})\overset{(a)}{=}\varepsilon$, and $\{\varepsilon\}$ is a basis of $\mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_p,\mathbb{F}_p)$.

For $k=jl+l-1$, $j\geq 0$, we have $\bar{\Psi}^k(\overline{\chi\iota^j})\overset{(e)}{=}\varepsilon$, and $\{\varepsilon\}$ is a basis of $\mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_p,\mathbb{F}_p)$. Finally, for $k=jl+r$ for some $j\geq 0$ and some $r\in[1,l-2]$ and for $k<0$, we have $\mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_p,\mathbb{F}_p)=\{0\}$. □

2.3. An A_∞-structure on $\operatorname{Ext}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathbb{F}_p, \mathbb{F}_p)$ as a minimal model of $\operatorname{Hom}^*_{\mathbb{F}_p\mathrm{S}_p}(\operatorname{PRes}\mathbb{F}_p, \operatorname{PRes}\mathbb{F}_p)$

Recall that $p \geq 3$ is a prime. Write $A := \operatorname{Hom}^*_{\mathbb{F}_p\mathrm{S}_p}(\operatorname{PRes}\mathbb{F}_p, \operatorname{PRes}\mathbb{F}_p)$, which becomes an A_∞-algebra $(A, (m_n)_{n\geq 1})$ over $R = \mathbb{F}_p$ via Lemma 29. We implement $\operatorname{Ext}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathbb{F}_p, \mathbb{F}_p)$ as $\operatorname{Ext}^*_{\mathbb{F}_p\mathrm{S}_p}(\mathbb{F}_p, \mathbb{F}_p) := \mathrm{H}^*A$.

Our goal in this section is to construct an A_∞-structure $(m'_n)_{n\geq 1}$ on H^*A and a morphism of A_∞-algebras $f = (f_n)_{n\geq 1} : (\mathrm{H}^*A, (m'_n)_{n\geq 1}) \to (A, (m_n)_{n\geq 1})$ which satisfy the statements of Theorem 32. I.e. we will construct a minimal model of A. In preparation of the definitions of the f_n and m'_n, we name and examine certain elements of A:

Lemma 36. *Suppose given $k \in [2, p-1]$. We set*

$$\gamma_k := \sum_{i\geq 0} \left(\lfloor e_k \rfloor^{k-1+li}_{k(l-1)+li} + \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{k(l-1)+(p-1)+li} \right) \in A^{k(l-2)+1}.$$

For $j \geq 0$, we have

$$\gamma_k \iota^j := \gamma_k \circ \iota^j = \iota^j \circ \gamma_k = \sum_{i\geq 0} \left(\lfloor e_k \rfloor^{k-1+li}_{k(l-1)+l(i+j)} + \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{k(l-1)+(p-1)+l(i+j)} \right) \in A^{k(l-2)+1+jl}$$

and

$$\begin{aligned} m_1(\gamma_k\iota^j) = \sum_{i\geq 0} \Big(& \lfloor e_{k-1,k} \rfloor^{k-2+li}_{k(l-1)+l(i+j)} + \lfloor e_{p-k+1,p-k} \rfloor^{k-2+(p-1)+li}_{k(l-1)+(p-1)+l(i+j)} \\ & + \lfloor e_{k,k-1} \rfloor^{k-1+li}_{k(l-1)+1+l(i+j)} + \lfloor e_{p-k,p-(k-1)} \rfloor^{k-1+(p-1)+li}_{k(l-1)+p+l(i+j)} \Big). \end{aligned}$$

Proof. We need to prove that γ_k is well-defined. Let $i \geq 0$.
We consider the first term. The complex $\operatorname{PRes}\mathbb{F}_p$ (cf. (8), (6)) has entry P_k at position $k(l-1)+li$ and at position $k-1+li$: We have $k(l-1)+li = (k-1+i)l + l - k$. So $\omega(k(l-1)+li) = l-(l-k) = k$ since $p-1 \leq l-k \leq l-1$. We have $\omega(k-1+li) = (k-1)+1 = k$ since $0 \leq k-1 \leq p-2$. As $k(l-1)+li, k-1+li \geq 0$, we have $\operatorname{Pr}_{k(l-1)+li} = P_{\omega(k(l-1)+li)} = P_k$ and $\operatorname{Pr}_{k-1+li} = P_{\omega(k-1+li)} = P_k$. So the first term is well-defined.
Now consider the second term. The complex $\operatorname{PRes}\mathbb{F}_p$ has entry P_{p-k} at position $k(l-1)+(p-1)+li$ and at position $k-1+(p-1)+li$: We have $k(l-1)+(p-1)+li = (i+k)l+(p-1)-k$, so $\omega(k(l-1)+(p-1)+li) = (p-1)-k+1 = p-k$ since $0 \leq (p-1)-k \leq p-2$. We have $\omega(k-1+(p-1)+li) = 2(p-1)-(k-1)-(p-1) = p-k$ since $p-1 \leq k-1+(p-1) \leq 2(p-1)-1$. As $k(l-1)+(p-1)+li, k-1+(p-1)+li \geq 0$, we have $\operatorname{Pr}_{k(l-1)+(p-1)+li} = P_{\omega(k(l-1)+(p-1)+li)} = P_{p-k}$ and $\operatorname{Pr}_{k-1+(p-1)+li} = P_{\omega(k-1+(p-1)+li)} = P_{p-k}$. So the second term is well-defined.

The degree of the tuple of maps is computed to be $(k(l-1)+li) - (k-1+li) = k(l-2)+1 = (k(l-1)+(p-1)+li) - (k-1+(p-1)+li)$.

The explicit formula for $\gamma_k\iota^j$ is an application of Proposition 35(b).

The degree $|\gamma_k\iota^j| = k(l-2)+1$ is odd, so

$$\begin{aligned}
m_1(\gamma_k\iota^j) &\overset{\text{L.29}}{=} d\circ\gamma_k\iota^j + \gamma_k\iota^j\circ d \\
&\overset{\text{R.30}}{=} \sum_{i\geq 0}\lfloor e_{\omega(k-2),\omega(k-1)}\rfloor^{k-2+li}_{k-1+li}\circ\sum_{i\geq 0}\lfloor e_k\rfloor^{k-1+li}_{k(l-1)+l(i+j)} \\
&\quad + \sum_{i\geq 0}\lfloor e_{\omega(p-1+k-2),\omega(p-1+k-1)}\rfloor^{k-2+(p-1)+li}_{k-1+(p-1)+li}\circ\sum_{i\geq 0}\lfloor e_{p-k}\rfloor^{k-1+(p-1)+li}_{k(l-1)+(p-1)+l(i+j)} \\
&\quad + \sum_{i\geq 0}\lfloor e_k\rfloor^{k-1+li}_{k(l-1)+l(i+j)}\circ\sum_{i\geq 0}\lfloor e_{\omega(l-k),\omega(l-k+1)}\rfloor^{k(l-1)+l(i+j)}_{k(l-1)+1+l(i+j)} \\
&\quad + \sum_{i\geq 0}\lfloor e_{p-k}\rfloor^{k-1+(p-1)+li}_{k(l-1)+(p-1)+l(i+j)}\circ\sum_{i\geq 0}\lfloor e_{\omega(p-1-k),\omega(p-k)}\rfloor^{k(l-1)+(p-1)+l(i+j)}_{k(l-1)+p+l(i+j)} \\
&= \sum_{i\geq 0}\lfloor e_{k-1,k}\rfloor^{k-2+li}_{k(l-1)+l(i+j)} + \sum_{i\geq 0}\lfloor e_{p-k+1,p-k}\rfloor^{k-2+(p-1)+li}_{k(l-1)+(p-1)+l(i+j)} \\
&\quad + \sum_{i\geq 0}\lfloor e_{k,k-1}\rfloor^{k-1+li}_{k(l-1)+1+l(i+j)} + \sum_{i\geq 0}\lfloor e_{p-k,p-(k-1)}\rfloor^{k-1+(p-1)+li}_{k(l-1)+p+l(i+j)}
\end{aligned}$$

Note that in the second line $k-2+li\geq 0$ as $i\geq 0$ and $k\geq 2$. $\square$

Lemma 37. *For* $j,j'\geq 0$, *we have*

$$\chi\iota^j\circ\chi\iota^{j'} = m_1(\gamma_2\iota^{j+j'}).$$

Proof. It suffices to prove that $\chi\circ\chi = m_1(\gamma_2)$ since then $\chi\iota^j\circ\chi\iota^{j'} \overset{\text{P.35}(e)}{=} \chi\circ\chi\circ\iota^{j+j'} = m_1(\gamma_2)\circ\iota^{j+j'} \overset{\text{P.35}(c)}{=} m_1(\gamma_2\iota^{j+j'})$.
To determine when a composite is zero, we will need the following. For $0\leq k,k'<l$, we examine the condition

$$il+l-1+k = i'l+k'. \tag{15}$$

If $k=0$ then (15) holds iff $i=i'$ and $k'=l-1$.
If $k\geq 1$ then (15) holds iff $i+1=i'$ and $k'=k-1$.
So

$$\begin{aligned}
\chi\circ\chi \overset{p\geq 3}{=} &\left(\sum_{i\geq 0}\left(\lfloor e_1\rfloor^{il}_{il+l-1} + \lfloor e_{2,1}\rfloor^{il+1}_{il+l} + \left(\sum_{k=2}^{p-2}\lfloor e_{k+1,k}\rfloor^{il+k}_{il+l-1+k}\right)\right.\right. \\
&\left.\left. + \lfloor e_{p-1}\rfloor^{il+(p-1)}_{il+l-1+(p-1)} + \lfloor e_{p-2,p-1}\rfloor^{il+p}_{il+l+p-1} + \left(\sum_{k=2}^{p-2}\lfloor e_{p-k-1,p-k}\rfloor^{il+(p-1)+k}_{il+l-1+(p-1)+k}\right)\right)\right) \\
&\circ\left(\sum_{i'\geq 0}\left(\lfloor e_1\rfloor^{i'l}_{i'l+l-1} + \left(\sum_{k'=1}^{p-3}\lfloor e_{k'+1,k'}\rfloor^{i'l+k'}_{i'l+l-1+k'}\right) + \lfloor e_{p-1,p-2}\rfloor^{i'l+p-2}_{i'l+l+p-3}\right.\right.
\end{aligned}$$

$$+ \lfloor e_{p-1}\rceil_{i'l+l-1+(p-1)}^{i'l+(p-1)} + \left(\sum_{k'=1}^{p-3} \lfloor e_{p-k'-1,p-k'}\rceil_{i'l+l-1+(p-1)+k'}^{i'l+(p-1)+k'} \right) + \lfloor e_{1,2}\rceil_{i'l+l+2(p-2)}^{i'l+l-1} \Bigg)\Bigg)$$

$$= \sum_{i\geq 0} \Bigg(\lfloor e_1 \circ e_{1,2}\rceil_{il+l+2(p-2)}^{il} + \lfloor e_{2,1} \circ e_1\rceil_{il+2l-1}^{il+1} + \left(\sum_{k=2}^{p-2} \underbrace{\lfloor e_{k+1,k} \circ e_{k,k-1}\rceil_{il+2l-1+k-1}^{il+k}}_{=0 \text{ by L.19(c)}} \right)$$

$$+ \lfloor e_{p-1} \circ e_{p-1,p-2}\rceil_{il+2l+p-3}^{il+(p-1)} + \lfloor e_{p-2,p-1} \circ e_{p-1}\rceil_{il+2l+p-2}^{il+p}$$

$$+ \left(\sum_{k=2}^{p-2} \underbrace{\lfloor e_{p-k-1,p-k} \circ e_{p-k,p-k+1}\rceil_{il+2l-1+p-1+k-1}^{il+(p-1)+k}}_{=0 \text{ by L.19(c)}} \right) \Bigg)$$

$$= \sum_{i\geq 0} \left(\lfloor e_{1,2}\rceil_{(i+2)l-2}^{il} + \lfloor e_{2,1}\rceil_{(i+2)l-1}^{il+1} + \lfloor e_{p-1,p-2}\rceil_{(i+2)l+p-3}^{il+p-1} + \lfloor e_{p-2,p-1}\rceil_{(i+2)l+p-2}^{il+p} \right)$$

$$\overset{\text{L.36}}{=} m_1(\gamma_2)$$

□

Below are the definitions which will give a minimal A_∞-algebra structure on H^*A and a quasi-isomorphism of A_∞-algebras $\mathrm{H}^*A \to A$.

Definition 38. Recall from Proposition 35 that $\mathfrak{B} = \{\overline{\iota^j} \mid j \geq 0\} \sqcup \{\overline{\chi\iota^j} \mid j \geq 0\} = \{\overline{\chi^a\iota^j} \mid j \geq 0, a \in \{0,1\}\}$ is a basis of H^*A. For $n \in \mathbb{Z}_{\geq 1}$, we set

$$\mathfrak{B}^{\otimes n} := \{\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}} \in (\mathrm{H}^*A)^{\otimes n} \mid a_i \in \{0,1\} \text{ and } j_i \in \mathbb{Z}_{\geq 0} \text{ for all } i \in [1,n]\},$$

which is a basis of $(\mathrm{H}^*A)^{\otimes n}$ consisting of homogeneous elements.

For $n \geq 1$, we define the $\mathbb{F}_p$-linear map $f_n : (\mathrm{H}^*A)^{\otimes n} \to A$ as follows:

Case $n = 1$**:** f_1 is given on $\mathfrak{B}$ by $f_1(\overline{\iota^j}) := \iota^j$ and $f_1(\overline{\chi\iota^j}) := \chi\iota^j$.

Case $n \in [2, p-1]$**:** f_n is given on elements of $\mathfrak{B}^{\otimes n}$ by

$$f_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) := \begin{cases} 0 & \text{if } \exists i \in [1,n] : a_i = 0 \\ (-1)^{n-1}\gamma_n\iota^{j_1+\ldots+j_n} & \text{if } 1 = a_1 = a_2 = \ldots = a_n \end{cases}$$

Case $n \geq p$**:** We set $f_n := 0$.

For $n \geq 1$, we define the $\mathbb{F}_p$-linear map $m'_n : (\mathrm{H}^*A)^{\otimes n} \to \mathrm{H}^*A$ by defining it on elements $\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}} \in \mathfrak{B}^{\otimes n}$:

Case $\exists i \in [1,n] : a_i = 0$**:**
$m'_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) := 0$ for $n \neq 2$ and
$m'_2(\overline{\chi^{a_1}\iota^{j_1}} \otimes \overline{\chi^{a_2}\iota^{j_2}}) := \overline{\chi^{a_1+a_2}\iota^{j_1+j_2}}$ (Note that $a_1 + a_2 \in \{0,1\}$).

Case $a_1 = a_2 = \ldots = a_n = 1$**:**
$m'_n(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) := 0$ for $n \neq p$ and
$m'_p(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_p}}) := (-1)^p\overline{\iota^{p-1+j_1+\ldots+j_p}} = -\overline{\iota^{p-1+j_1+\ldots+j_p}}$.

Note that since $p \geq 3$, we have $m_2'(\overline{\chi\iota^{j_1}} \otimes \overline{\chi\iota^{j_2}}) = 0$ for $j_1, j_2 \geq 0$.

Theorem 39. *The pair* $(\mathrm{H}^*A, (m_n')_{n\geq 1})$ *is a minimal* A_∞*-algebra. The tuple* $(f_n)_{n\geq 1}$ *is an quasi-isomorphism of* A_∞*-algebras from* $(\mathrm{H}^*A, (m_n')_{n\geq 1})$ *to* $(A, (m_n)_{n\geq 1})$*. More precisely,* $f_1 : (\mathrm{H}^*A, m_1') \to (A, m_1)$ *induces the identity in homology.*

The proof of Theorem 39 will take the remainder of section 2.3. We will use Lemma 64.

Lemma 40. *The maps* f_n *and* m_n' *have degree* $|f_n| = 1-n$ *and* $|m_n'| = 2-n$*. I.e.* $(f_n)_{n\geq 1}$ *is a pre-*A_∞*-morphism from* H^*A *to* A*, and* $(\mathrm{H}^*A, (m_n')_{n\geq 1})$ *is a pre-*A_∞*-algebra.*

Proof. We have $|f_1| = 0$ as $|\overline{\iota^j}| = |\iota^j|$ and $|\overline{\chi\iota^j}| = |\chi\iota^j|$. For $n \geq p$ the map f_n is of degree $1-n$ as $f_n = 0$. For $n \in [2, p-1]$ the statement $|f_n| = 1-n$ is proven by checking the degrees for the elements of the basis $\mathfrak{B}^{\otimes n}$ whose image under f_n is non-zero:

$$\begin{aligned}|f_n(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}})| &= |(-1)^{n-1}\gamma_n\iota^{j_1+\ldots+j_n}| \overset{\text{L.36}}{=} (j_1+\ldots+j_n)l + n(l-1) + 1 - n \\ &= 1 - n + \sum_{x=1}^{n} |\overline{\chi\iota^{j_x}}| = 1 - n + |\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}|\end{aligned}$$

Thus $|f_n| = 1-n$ for all n and we have proven the first statement.

Now we show $|m_n'| = 2-n$. As before, we only need check the degrees for basis elements whose image is non-zero: For $\overline{\chi^{a_1}\iota^{j_1}} \otimes \overline{\chi^{a_2}\iota^{j_2}}$, $j_1, j_2 \geq 0$, $a_1, a_2 \in \{0,1\}$, $0 \in \{a_1, a_2\}$, we have

$$\begin{aligned}|m_2'(\overline{\chi^{a_1}\iota^{j_1}} \otimes \overline{\chi^{a_2}\iota^{j_2}})| &= |\overline{\chi^{a_1+a_2}\iota^{j_1+j_2}}| = (a_1+a_2)(l-1) + l(j_1+j_2) \\ &= a_1(l-1) + j_1 l + a_2(l-1) + j_2 l = |\overline{\chi^{a_1}\iota^{j_1}} \otimes \overline{\chi^{a_2}\iota^{j_2}}| + (2-2).\end{aligned}$$

For $\overline{\chi\iota^{j_1}} \otimes \cdots \otimes \overline{\chi\iota^{j_p}}$, $j_x \geq 0$ for $x \in [1,p]$, we have

$$\begin{aligned}|m_p'(\overline{\chi\iota^{j_1}} \otimes \cdots \otimes \overline{\chi\iota^{j_p}})| &= |\overline{\iota^{p-1+j_1+\ldots+j_p}}| = l(p-1+j_1+\ldots+j_p) \\ &= lp - l + l(j_1+\ldots+j_p) = lp - 2p + 2 + l(j_1+\ldots+j_p) \\ &= p(l-1) + l(j_1+\ldots+j_p) + 2 - p = |\overline{\chi\iota^{j_1}} \otimes \cdots \otimes \overline{\chi\iota^{j_p}}| + 2 - p\end{aligned}$$

□

Lemma 41. *We have* $m_1' = 0$*. The equation* (12)[1] *holds. The complex morphism* $f_1 : (A', m_1') \to (A, m_1)$ *is a quasi-isomorphism inducing the identity in homology.*

Proof. The equality $m_1' = 0$ follows immediately from the definition. Thus $m_1 \circ f_1 = 0 = f_1 \circ m_1'$. Moreover f_1 is a quasi-isomorphism inducing the identity in homology by construction, cf. Proposition 35(g). □

Lemma 42. *The map* f_1 *is injective.*

Proof. The set $X := \{\chi^a\iota^j \mid a \in \{0,1\}, j \in \mathbb{Z}_{\geq 1}\} \subseteq A$ is linearly independent, since it consists of nonzero elements of different summands of the direct sum $A = \bigoplus_{k\in\mathbb{Z}} \mathrm{Hom}^k(\mathrm{PRes}\,\mathbb{F}_p, \mathrm{PRes}\,\mathbb{F}_p)$. The set $\mathfrak{B}$, which is a basis of H^*A, is mapped bijectively to X by f_1, so f_1 is injective. □

Lemma 43. *The equation* (12)[2] *holds.*

Proof. As $m'_1 = 0$, equation (12)[2] is equivalent to (cf. (13))

$$f_1 \circ m'_2 = m_1 \circ f_2 + m_2 \circ (f_1 \otimes f_1).$$

We check this equation on $\mathfrak{B}^{\otimes 2}$: Recall Proposition 35 and Definition 38.

$$\begin{aligned}
f_1 m'_2(\overline{\iota^j} \otimes \overline{\iota^{j'}}) &= \iota^{j+j'} = m_2(f_1 \otimes f_1)(\overline{\iota^j} \otimes \overline{\iota^{j'}}) = (m_1 \circ f_2 + m_2 \circ (f_1 \otimes f_1))(\overline{\iota^j} \otimes \overline{\iota^{j'}})\\
f_1 m'_2(\overline{\iota^j} \otimes \overline{\chi\iota^{j'}}) &= \chi\iota^{j+j'} = m_2(f_1 \otimes f_1)(\overline{\iota^j} \otimes \overline{\chi\iota^{j'}})\\
&= (m_1 \circ f_2 + m_2 \circ (f_1 \otimes f_1))(\overline{\iota^j} \otimes \overline{\chi\iota^{j'}})\\
f_1 m'_2(\overline{\chi\iota^j} \otimes \overline{\iota^{j'}}) &= \chi\iota^{j+j'} = m_2(f_1 \otimes f_1)(\overline{\chi\iota^j} \otimes \overline{\iota^{j'}})\\
&= (m_1 \circ f_2 + m_2 \circ (f_1 \otimes f_1))(\overline{\chi\iota^j} \otimes \overline{\iota^{j'}})\\
f_1 m'_2(\overline{\chi\iota^j} \otimes \overline{\chi\iota^{j'}}) &= 0 \overset{\text{L.37}}{=} -m_1(\gamma_2\iota^{j+j'}) + m_2(f_1 \otimes f_1)(\overline{\chi\iota^j} \otimes \overline{\chi\iota^{j'}})\\
&= (m_1 \circ f_2 + m_2 \circ (f_1 \otimes f_1))(\overline{\chi\iota^j} \otimes \overline{\chi\iota^{j'}})
\end{aligned}$$

Note that there are no additional signs due to the Koszul sign rule since $|f_1| = 0$. □

The following results directly from Definition 38.

Corollary 44. *For $n \geq 2$ and $a_1, \ldots, a_n \in \{0,1\}$, $j_1, \ldots, j_n \geq 0$, we have*

$$f_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = f_n(\overline{\chi^{a_1}} \otimes \ldots \otimes \overline{\chi^{a_n}}) \circ \iota^{j_1+\ldots+j_n}.$$

If there is additionally an $x \in [1,n]$ with $a_x = 0$ then

$$f_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0.$$

Equation (12)[n] can be reformulated as

$$\begin{aligned}
&\underbrace{f_1 \circ m'_n + \sum_{\substack{n=r+s+t\\ r,t\geq 0, s\geq 1\\ s\leq n-1}} (-1)^{rs+t} f_{r+1+t} \circ (1^{\otimes r} \otimes m'_s \otimes 1^{\otimes t})}_{=:\Phi_n}\\
&= m_1 \circ f_n + \underbrace{\sum_{\substack{2\leq r\leq n\\ i_1+\ldots+i_r=n\\ i_s\geq 1}} (-1)^v m_r \circ (f_{i_1} \otimes f_{i_2} \otimes \ldots \otimes f_{i_r})}_{=:\Xi_n},
\end{aligned}$$

where $v = \sum_{1\leq t<s\leq r}(1-i_s)i_t$.

A term of the form $f_{r+1+t}\circ(1^{\otimes r}\otimes m'_s\otimes 1^{\otimes t})$, $s\geq 3$, $r+t\geq 1$, is zero because of Corollary 44 and the definition of m'_p. Also recall $m'_1 = 0$. Thus

$$\Phi_n = \sum_{\substack{n=r+2+t\\ r,t\geq 0}}(-1)^{2r+t}f_{n-1}\circ(1^{\otimes r}\otimes m'_2\otimes 1^{\otimes t}) = \sum_{r=0}^{n-2}(-1)^{n-r}f_{n-1}\circ(1^{\otimes r}\otimes m'_2\otimes 1^{\otimes n-r-2}). \tag{16}$$

Because of $m_k = 0$ for $k\geq 3$, we have

$$\Xi_n = \sum_{\substack{i_1+i_2=n\\ i_1,i_2\geq 1}}(-1)^{(1-i_2)i_1}m_2\circ(f_{i_1}\otimes f_{i_2}) = \sum_{i=1}^{n-1}(-1)^{ni}m_2\circ(f_i\otimes f_{n-i}). \tag{17}$$

We have proven:

Lemma 45. *For $n\geq 1$, condition (12)[n] is equivalent to $f_1\circ m'_n + \Phi_n = m_1\circ f_n + \Xi_n$ where Φ_n and Ξ_n are as in (16) and (17).*

Lemma 46. *Condition (12)[n] holds for $n\geq 3$ and arguments $\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}\in\mathfrak{B}^{\otimes n} = \{\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}\in(\mathrm{H}^*A)^{\otimes n}\mid a_i\in\{0,1\}$ and $j_i\in\mathbb{Z}_{\geq 0}$ for all $i\in[1,n]\}$ where $0\in\{a_1,\ldots,a_n\}$.*

Proof. Because of Lemma 45 and Definition 38 it is sufficient to show that

$$\Phi_n(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = \Xi_n(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}})$$

if at least one a_x equals 0.

Case 1 At least two a_x equal 0:

To show $\Phi_n(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = 0$, we show $f_{n-1}(1^{\otimes r}\otimes m'_2\otimes 1^{\otimes n-r-2})(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = 0$ for $r\in[0,n-2]$: In case both components of the argument of m'_2 are of the form $\overline{\chi^0\iota^j}$, the result of m'_2 is of the form $\overline{\iota^{j'}}$ (see Definition 38). Since $2\leq n-1$, Corollary 44 implies the result of f_{n-1} is zero. Otherwise at least one of the components of the argument of f_{n-1} must be of the form $\overline{\iota^j}$ and the result of f_{n-1} is zero as well. So $\Phi_n(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = 0$.
To show $\Xi_n(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = 0$, we show $m_2(f_i\otimes f_{n-i})(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = 0$ for $i\in[1,n-1]$:

- Suppose given $i\in[2,n-2]$: The statements $a_1=\ldots=a_i=1$ and $a_{i+1}=\ldots=a_n=1$ cannot be true at the same time, so $f_i(\ldots)=0$ or $f_{n-i}(\ldots)=0$ and we have $m_2(f_i\otimes f_{n-i})(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = 0$.
- Suppose that $i=1$. Because at least two a_x equal 0 the statement $a_2=\ldots=a_n=1$ cannot be true. Since $n-1\geq 2$, we have $f_{n-1}(\ldots)=0$ and $m_2(f_1\otimes f_{n-1})(\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_n}\iota^{j_n}}) = 0$.

- The case $i = n-1$ is analogous to the case $i = 1$.

So we have $\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0 = \Xi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}})$.

Case 2a Exactly one a_x equals 0, where $x \in [2, n-1]$.
We have $\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0$: In case $n \geq p+1$, it follows from $f_{n-1} = 0$. Let us check the case $n \in [3, p]$: Because of Definition 38, we have $f_{n-1}(1^{\otimes r} \otimes m_2' \otimes 1^{\otimes n-r-2})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0$ unless $r \in \{x-2, x-1\}$. So

$$\begin{aligned}
&\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) \\
&\qquad = (-1)^{n-x+2} f_{n-1}(1^{\otimes x-2} \otimes m_2' \otimes 1^{\otimes n-x} - 1^{\otimes x-1} \otimes m_2' \otimes 1^{n-x-1}) \\
&\qquad\quad (\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) \\
&\qquad = (-1)^{n-x} f_{n-1}(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_{x-2}}} \otimes m_2'(\overline{\chi\iota^{j_{x-1}}} \otimes \overline{\iota^{j_x}}) \otimes \overline{\chi\iota^{j_{x+1}}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}} \\
&\qquad\quad - \overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_{x-1}}} \otimes m_2'(\overline{\iota^{j_x}} \otimes \overline{\chi\iota^{j_{x+1}}}) \otimes \overline{\chi\iota^{j_{x+2}}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&\qquad = (-1)^{n-x} f_{n-1}(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_{x-2}}} \otimes \overline{\chi\iota^{j_{x-1}+j_x}} \otimes \overline{\chi\iota^{j_{x+1}}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}} \\
&\qquad\quad - \overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_{x-1}}} \otimes \overline{\chi\iota^{j_x+j_{x+1}}} \otimes \overline{\chi\iota^{j_{x+2}}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&\qquad = (-1)^{n-x}((-1)^{n-2}\gamma_{n-1}\iota^{j_1+\ldots+j_n} - (-1)^{n-2}\gamma_{n-1}\iota^{j_1+\ldots+j_n}) = 0
\end{aligned}$$

To show $\Xi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0$, we show $m_2(f_i \otimes f_{n-i})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0$ for $i \in [1, n-1]$: The element $\chi^{a_x}\iota^{j_x}$ is a tensor factor of the argument of f_i or of f_{n-i}. We write $y = i$ or $y = n-i$ accordingly. Then $y \geq 2$ since $x \notin \{1, n\}$, so $f_y(\ldots) = 0$ and thus $m_2(f_i \otimes f_{n-i})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0$.
So $\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0 = \Xi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}})$.

Case 2b Only $a_1 = 0$, all other a_x equal 1.
We have $f_{n-1}(1^{\otimes r} \otimes m_2' \otimes 1^{\otimes n-r-2})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0$ unless $r = 0$. So

$$\begin{aligned}
\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) &= (-1)^n f_{n-1}(1^{\otimes 0} \otimes m_2' \otimes 1^{\otimes n-2})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) \\
&= (-1)^n f_{n-1}(m_2'(\overline{\iota^{j_1}} \otimes \overline{\chi\iota^{j_2}}) \otimes \overline{\chi\iota^{j_3}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&= (-1)^n f_{n-1}(\overline{\chi\iota^{j_1+j_2}} \otimes \overline{\chi\iota^{j_3}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&= \begin{cases} \gamma_{n-1}\iota^{j_1+\ldots+j_n} & 3 \leq n \leq p \\ 0 & n \geq p+1 \end{cases}
\end{aligned}$$

We have $(f_i \otimes f_{n-1})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = 0$ if $i \geq 2$. So

$$\begin{aligned}
\Xi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) &= (-1)^{1 \cdot n} m_2(f_1 \otimes f_{n-1})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) \\
&\overset{(9)}{=} (-1)^n m_2\left((-1)^{n \cdot |\iota^{j_1}|} f_1(\overline{\iota^{j_1}}) \otimes f_{n-1}(\overline{\chi\iota^{j_2}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}})\right) \\
&= (-1)^n m_2\left(\iota^{j_1} \otimes f_{n-1}(\overline{\chi\iota^{j_2}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}})\right) \\
&= \begin{cases} (-1)^n m_2(\iota^{j_1} \otimes (-1)^{n-2}\gamma_{n-1}\iota^{j_2+\ldots+j_n}) & 3 \leq n \leq p \\ 0 & n \geq p+1 \end{cases}
\end{aligned}$$

$$= \begin{cases} \gamma_{n-1}\iota^{j_1+\ldots+j_n} & 3 \le n \le p \\ 0 & n \ge p+1 \end{cases}$$

So $\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = \Xi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}})$.

Case 2c Only $a_n = 0$, all other a_x equal 1.
Argumentation analogous to case 2b gives

$$\begin{aligned}\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) &= (-1)^2 f_{n-1}(1^{\otimes n-2} \otimes m_2' \otimes 1^{\otimes 0})(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) \\ &\overset{|m_2'|=0}{=} f_{n-1}(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_{n-2}}} \otimes m_2'(\overline{\chi\iota^{j_{n-1}}} \otimes \overline{\iota^{j_n}})) \\ &= \begin{cases} (-1)^{n-2}\gamma_{n-1}\iota^{j_1+\ldots+j_n} & 3 \le n \le p \\ 0 & n \ge p+1 \end{cases}\end{aligned}$$

and

$$\begin{aligned}\Xi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) &= (-1)^{n(n-1)} m_2(f_{n-1} \otimes f_1)(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) \\ &\overset{|f_1|=0}{=} m_2\left(f_{n-1}(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_{n-1}}}) \otimes f_1(\overline{\iota^{j_n}})\right) \\ &= \begin{cases} (-1)^{n-2}\gamma_{n-1}\iota^{j_1+\ldots+j_n} & 3 \le n \le p \\ 0 & n \ge p+1 \end{cases}\end{aligned}$$

So $\Phi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}}) = \Xi_n(\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}})$.

$\square$

Now we examine the cases where $a_1 = \ldots = a_n = 1$:

Lemma 47. *For $n \ge 3$, we have $\Phi_n(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) = 0$ for $\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}} \in \mathfrak{B}^{\otimes n} = \{\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}} \in (\mathrm{H}^*A)^{\otimes n} \mid a_i \in \{0,1\}$ and $j_i \in \mathbb{Z}_{\ge 0}$ for all $i \in [1,n]\}$.*

Proof. We have $\Phi_n(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) = 0$ since $\Phi_n = \sum_{r=0}^{n-2}(-1)^{n-r} f_{n-1}(1^{\otimes r} \otimes m_2' \otimes 1^{\otimes n-r-2})$ and the argument of m_2' is always of the form $\overline{\chi\iota^x} \otimes \overline{\chi\iota^y}$, whence its result is zero. $\square$

Lemma 48. *Condition (12)[n] holds for $n \in [3, p-1]$ and arguments $\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}} \in \mathfrak{B}^{\otimes n} = \{\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}} \in (\mathrm{H}^*A)^{\otimes n} \mid a_i \in \{0,1\}$ and $j_i \in \mathbb{Z}_{\ge 0}$ for all $i \in [1,n]\}$.*

Proof. For computing Ξ_n, we first show that $m_2(f_k \otimes f_{n-k})(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) = 0$ for $k \in [2, n-2]$. We will need the following congruence.

$$\begin{aligned}\underbrace{(k(l-1) + l(i+x))}_{\equiv_{p-1} k(l-1)+(p-1)+l(i+x)} - \underbrace{(n-k-1+li')}_{\equiv_{p-1} n-k-1+(p-1)+li'} &\equiv_{p-1} -k + k - n + 1 = -(n-1) \\ &\not\equiv_{p-1} 0 \end{aligned} \tag{18}$$

The last statement results from $2 \leq n \leq p-1$. We set "±" as a symbol for the (a posteriori irrelevant) signs in the following calculation. For $k \in [2, n-2]$, we have

$$
\begin{aligned}
& m_2(f_k \otimes f_{n-k})(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&= \pm\, m_2((-1)^{k-1}\gamma_k\iota^{j_1+\ldots+j_k} \otimes (-1)^{n-k-1}\gamma_{n-k}\iota^{j_{k+1}+\ldots+j_n}) \\
&\overset{\substack{j_1+\ldots+j_k=:x,\\ j_{k+1}+\ldots+j_n=:y}}{=} \pm\, \gamma_k\iota^x \circ \gamma_{n-k}\iota^y \\
&= \pm \left(\sum_{i\geq 0} \lfloor e_k \rfloor^{k-1+li}_{k(l-1)+l(i+x)} + \sum_{i\geq 0} \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{k(l-1)+(p-1)+l(i+x)} \right) \\
&\quad \circ \left(\sum_{i'\geq 0} \lfloor e_{n-k} \rfloor^{n-k-1+li'}_{(n-k)(l-1)+l(i'+y)} + \sum_{i'\geq 0} \lfloor e_{p-n+k} \rfloor^{n-k-1+(p-1)+li'}_{(n-k)(l-1)+(p-1)+l(i'+y)} \right) \overset{(18)}{=} 0.
\end{aligned}
$$

So

$$
\begin{aligned}
& \Xi_n(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&\qquad = m_2((-1)^n f_1 \otimes f_{n-1} + (-1)^{n(n-1)} f_{n-1} \otimes f_1)(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&\qquad = m_2((-1)^{n+n|\overline{\chi\iota^{j_1}}|} f_1(\overline{\chi\iota^{j_1}}) \otimes f_{n-1}(\overline{\chi\iota^{j_2}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \\
&\qquad\quad + f_{n-1}(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_{n-1}}}) \otimes f_1(\overline{\chi\iota^{j_n}})) \\
&\qquad = m_2(\chi\iota^{j_1} \otimes (-1)^{n-2}\gamma_{n-1}\iota^{j_2+\ldots+j_n} + (-1)^{n-2}\gamma_{n-1}\iota^{j_1+\ldots+j_{n-1}} \otimes \chi\iota^{j_n}) \\
&\qquad = (-1)^n(\chi\iota^{j_1} \circ \gamma_{n-1}\iota^{j_2+\ldots+j_n} + \gamma_{n-1}\iota^{j_1+\ldots+j_{n-1}} \circ \chi\iota^{j_n}) \\
&\qquad \overset{\text{P.35}(e),\text{L.36}}{=} (-1)^n(\chi \circ \gamma_{n-1} + \gamma_{n-1} \circ \chi) \circ \iota^{j_1+\ldots+j_n}
\end{aligned}
$$

$$
\begin{aligned}
\chi \circ \gamma_{n-1} &= \left(\sum_{i\geq 0} \left(\lfloor e_1 \rfloor^{il}_{(i+1)l-1} + \left(\sum_{k=1}^{p-2} \lfloor e_{k+1,k} \rfloor^{il+k}_{(i+1)l-1+k} \right) \right.\right. \\
&\qquad \left.\left. + \lfloor e_{p-1} \rfloor^{il+(p-1)}_{(i+1)l-1+(p-1)} + \left(\sum_{k=1}^{p-2} \lfloor e_{p-k-1,p-k} \rfloor^{il+(p-1)+k}_{(i+1)l-1+(p-1)+k} \right) \right) \right) \\
&\qquad \circ \left(\sum_{i'\geq 0} \lfloor e_{n-1} \rfloor^{n-2+li'}_{(n-1)(l-1)+li'} + \sum_{i'\geq 0} \lfloor e_{p-n+1} \rfloor^{n-2+(p-1)+li'}_{(n-1)(l-1)+(p-1)+li'} \right) \\
&\overset{\substack{3\leq n\leq p-1\\ k\rightsquigarrow n-1\\ i'\rightsquigarrow i+1}}{=} \sum_{i\geq 0} \lfloor e_{n,n-1} \circ e_{n-1} \rfloor^{il+n-1}_{(n-1)(l-1)+l(i+1)} \\
&\qquad + \sum_{i\geq 0} \lfloor e_{p-n,p-n+1} \circ e_{p-n+1} \rfloor^{il+p-1+n-1}_{(n-1)(l-1)+(p-1)+l(i+1)} \\
&= \sum_{i\geq 0} \left(\lfloor e_{n,n-1} \rfloor^{il+n-1}_{n(l-1)+1+li} + \lfloor e_{p-n,p-n+1} \rfloor^{il+p-1+n-1}_{n(l-1)+p+li} \right) \\
\gamma_{n-1} \circ \chi &= \left(\sum_{i'\geq 0} \lfloor e_{n-1} \rfloor^{n-2+li'}_{(n-1+i'-1)l+2(p-1)-(n-1)} + \sum_{i'\geq 0} \lfloor e_{p-n+1} \rfloor^{n-2+(p-1)+li'}_{(n-1+i')l-n+p} \right)
\end{aligned}
$$

$$\begin{aligned}
&\circ\left(\sum_{i\geq 0}\left(\lfloor e_1\rfloor^{il}_{(i+1)l-1}+\left(\sum_{k=1}^{p-2}\lfloor e_{k+1,k}\rfloor^{il+k}_{(i+1)l-1+k}\right)\right.\right.\\
&\left.\left.+\lfloor e_{p-1}\rfloor^{il+(p-1)}_{(i+1)l-1+(p-1)}+\left(\sum_{k=1}^{p-2}\lfloor e_{p-k-1,p-k}\rfloor^{il+(p-1)+k}_{(i+1)l-1+(p-1)+k}\right)\right)\right)\\
\overset{k\rightsquigarrow p-n}{=}&\sum_{i'\geq 0}\lfloor e_{n-1}\circ e_{n-1,n}\rfloor^{n-2+li'}_{(n-1+i')l-1+(p-1)+(p-n)}\\
&+\sum_{i'\geq 0}\lfloor e_{p-n+1}\circ e_{p-n+1,p-n}\rfloor^{n-2+(p-1)+li'}_{(n+i')l-1+p-n}\\
=&\sum_{i'\geq 0}\lfloor e_{n-1,n}\rfloor^{n-2+li'}_{n(l-1)+i'l}+\sum_{i'\geq 0}\lfloor e_{p-n+1,p-n}\rfloor^{n-2+(p-1)+li'}_{n(l-1)+(p-1)+i'l}
\end{aligned}$$

So $\chi\circ\gamma_{n-1}+\gamma_{n-1}\circ\chi=m_1(\gamma_n)$ by Lemma 36. Therefore

$$\begin{aligned}
\Xi_n(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_n}})&=(-1)^n m_1(\gamma_n)\circ\iota^{j_1+\ldots+j_n}\overset{\text{P.35(c)}}{=}(-1)^n m_1(\gamma_n\iota^{j_1+\ldots+j_n})\\
&=-m_1((-1)^{n-1}\gamma_n\iota^{j_1+\ldots+j_n})\\
&=-m_1\circ f_n(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_n}}).
\end{aligned}$$

We conclude using Lemma 45 by

$$(f_1\circ m'_n+\Phi_n)(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_n}})\overset{\text{L.47,D.38}}{=}0=(m_1\circ f_n+\Xi_n)(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_n}}).$$

□

Lemma 49. *Condition* (12)[p] *holds for arguments* $\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_p}}\in\mathfrak{B}^{\otimes p}=\{\overline{\chi^{a_1}\iota^{j_1}}\otimes\ldots\otimes\overline{\chi^{a_p}\iota^{j_p}}\in(\mathrm{H}^*A)^{\otimes p}\mid a_i\in\{0,1\}$ *and* $j_i\in\mathbb{Z}_{\geq 0}$ *for all* $i\in[1,p]\}$.

Proof. Recall that $|\iota|=l=2(p-1)$ is even, $|\chi|=l-1$ is odd and $|f_i|=1-i$ by Lemma 40. We have

$$\begin{aligned}
\Xi_p(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_p}})&=\sum_{i=1}^{p-1}(-1)^{pi}m_2(f_i\otimes f_{p-i})(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_p}})\\
&=\sum_{i=1}^{p-1}(-1)^{pi+i(1-(p-i))}m_2(f_i(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_i}})\otimes f_{p-i}(\overline{\chi\iota^{j_{i+1}}}\otimes\ldots\otimes\overline{\chi\iota^{j_p}}))\\
&=\sum_{i=1}^{p-1}f_i(\overline{\chi\iota^{j_1}}\otimes\ldots\otimes\overline{\chi\iota^{j_i}})\circ f_{p-i}(\overline{\chi\iota^{j_{i+1}}}\otimes\ldots\otimes\overline{\chi\iota^{j_p}})\\
&\overset{p\geq 3}{=}\chi\iota^{j_1}\circ(-1)^{p-2}\gamma_{p-1}\iota^{j_2+\ldots+j_p}+(-1)^{p-2}\gamma_{p-1}\iota^{j_1+\ldots+j_{p-1}}\circ\chi\iota^{j_p}\\
&\quad+\sum_{i=2}^{p-2}(-1)^{i-1}\gamma_i\iota^{j_1+\ldots+j_i}\circ(-1)^{p-i-1}\gamma_{p-i}\iota^{j_{i+1}+\ldots+j_p}
\end{aligned}$$

$$\overset{\text{P.35}(b)}{=} (-1)^p \left(\chi \circ \gamma_{p-1} + \gamma_{p-1} \circ \chi + \sum_{k=2}^{p-2} \gamma_k \circ \gamma_{p-k} \right) \circ \iota^{j_1+\ldots+j_p}$$

$$\begin{aligned}
\chi \circ \gamma_{p-1} = &\left(\sum_{i\geq 0} \left(\lfloor e_1 \rfloor^{il}_{(i+1)l-1} + \left(\sum_{k=1}^{p-2} \lfloor e_{k+1,k} \rfloor^{il+k}_{(i+1)l-1+k} \right) \right.\right.\\
&\left.\left. + \lfloor e_{p-1} \rfloor^{il+(p-1)}_{(i+1)l-1+(p-1)} + \left(\sum_{k=1}^{p-2} \lfloor e_{p-k-1,p-k} \rfloor^{il+(p-1)+k}_{(i+1)l-1+(p-1)+k} \right) \right) \right)\\
&\circ \left(\sum_{i'\geq 0} \lfloor e_{p-1} \rfloor^{(p-1)-1+li'}_{(p-1)(l-1)+li'} + \sum_{i'\geq 0} \lfloor e_1 \rfloor^{-1+2(p-1)+li'}_{(p-1)(l-1)+(p-1)+li'} \right)\\
= &\sum_{i\geq 0} \lfloor e_{p-1} \rfloor^{il+(p-1)}_{(p-1)(l-1)+l(i+1)} + \sum_{i\geq 0} \lfloor e_1 \rfloor^{il}_{(p-1)(l-1)+(p-1)+li}\\
= &\sum_{i\geq 0} \lfloor e_{p-1} \rfloor^{il+(p-1)}_{(p+i-1)l+(p-1)} + \sum_{i\geq 0} \lfloor e_1 \rfloor^{il}_{(p+i-1)l}
\end{aligned}$$

$$\begin{aligned}
\gamma_{p-1} \circ \chi = &\left(\sum_{i'\geq 0} \lfloor e_{p-1} \rfloor^{(p-1)-1+li'}_{(p+i'-2)l+(p-1)} + \sum_{i'\geq 0} \lfloor e_1 \rfloor^{-1+2(p-1)+li'}_{(p+i'-1)l} \right)\\
&\circ \left(\sum_{i\geq 0} \left(\lfloor e_1 \rfloor^{il}_{(i+1)l-1} + \left(\sum_{k=1}^{p-2} \lfloor e_{k+1,k} \rfloor^{il+k}_{(i+1)l-1+k} \right) \right.\right.\\
&\left.\left. + \lfloor e_{p-1} \rfloor^{il+(p-1)}_{(i+1)l-1+(p-1)} + \left(\sum_{k=1}^{p-2} \lfloor e_{p-k-1,p-k} \rfloor^{il+(p-1)+k}_{(i+1)l-1+(p-1)+k} \right) \right) \right)\\
= &\sum_{i'\geq 0} \lfloor e_{p-1} \rfloor^{(p-1)-1+li'}_{(p+i'-1)l-1+(p-1)} + \sum_{i'\geq 0} \lfloor e_1 \rfloor^{-1+2(p-1)+li'}_{(p+i')l-1}\\
= &\sum_{i'\geq 0} \lfloor e_{p-1} \rfloor^{p-2+i'l}_{(p+i'-1)l+p-2} + \sum_{i'\geq 0} \lfloor e_1 \rfloor^{i'l+l-1}_{(p+i'-1)l+l-1}
\end{aligned}$$

$$\begin{aligned}
\gamma_k \circ \gamma_{p-k} = &\left(\sum_{i\geq 0} \lfloor e_k \rfloor^{k-1+li}_{(i+k-1)l+l-k} + \sum_{i\geq 0} \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{(i+k)l+(p-1)-k} \right)\\
&\circ \left(\sum_{i'\geq 0} \lfloor e_{p-k} \rfloor^{p-k-1+li'}_{(p-k)(l-1)+li'} + \sum_{i'\geq 0} \lfloor e_k \rfloor^{-k+2(p-1)+li'}_{(p-k)(l-1)+(p-1)+li'} \right)\\
= &\sum_{i\geq 0} \lfloor e_k \rfloor^{k-1+li}_{(p-k)(l-1)+(p-1)+l(i+k-1)} + \sum_{i\geq 0} \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{(p-k)(l-1)+l(i+k)}\\
= &\sum_{i\geq 0} \lfloor e_k \rfloor^{k-1+li}_{(p-k+i+k-1)l-(p-k)+(p-1)} + \sum_{i\geq 0} \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{(p-k+i+k)l-(p-k)}
\end{aligned}$$

$$= \sum_{i\geq 0} \lfloor e_k \rfloor^{k-1+li}_{(p+i-1)l+k-1} + \sum_{i\geq 0} \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{(p+i-1)l+k-1+(p-1)} .$$

Thus

$$\begin{aligned}
\chi \circ \gamma_{p-1} + \gamma_{p-1} \circ \chi + \sum_{k=2}^{p-2} \gamma_k \circ \gamma_{p-k} \\
&= \sum_{i\geq 0}\sum_{k=0}^{p-2} \left(\lfloor e_{k+1} \rfloor^{k+li}_{(p+i-1)l+k} + \lfloor e_{p-k-1} \rfloor^{k+(p-1)+li}_{(p+i-1)l+k+(p-1)} \right) \\
&= \sum_{i\geq 0}\sum_{k'=0}^{l-1} \lfloor e_{\omega(k')} \rfloor^{k'+li}_{(p-1+i)l+k'} \overset{\mathrm{P.35}(a)}{=} \iota^{p-1}
\end{aligned}$$

and

$$\Xi_p(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_p}}) = (-1)^p \iota^{p-1+j_1+\ldots+j_p} .$$

So we conclude using Lemma 45 by

$$\begin{aligned}
(f_1 \circ m'_p + \Phi_p)(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_p}}) &\overset{\mathrm{L.47,D.38}}{=} (-1)^p \iota^{p-1+j_1+\ldots+j_p} \\
&\overset{\mathrm{D.38}}{=} (m_1 \circ f_p + \Xi_p)(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_p}}).
\end{aligned}$$

□

Lemma 50. *Condition* (12)[n] *holds for* $n \in [p+1, 2(p-1)]$ *and arguments* $\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}} \in \mathfrak{B}^{\otimes n} = \{\overline{\chi^{a_1}\iota^{j_1}} \otimes \ldots \otimes \overline{\chi^{a_n}\iota^{j_n}} \in (\mathrm{H}^*A)^{\otimes n} \mid a_i \in \{0,1\}$ *and* $j_i \in \mathbb{Z}_{\geq 0}$ *for all* $i \in [1,n]\}$.

Proof. As $f_k = 0$ for $k \geq p$, we have

$$\Xi_n(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) = \sum_{k=n-p+1}^{p-1} (-1)^{nk} m_2(f_k \otimes f_{n-k})(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}})$$

The right side is a linear combination of terms of the form $\gamma_k \circ \gamma_{n-k}$ for $k \in [n-p-1, p-1]$. We have

$$\begin{aligned}
\gamma_k \circ \gamma_{n-k} = &\left(\sum_{i\geq 0} \lfloor e_k \rfloor^{k-1+li}_{k(l-1)+li} + \sum_{i\geq 0} \lfloor e_{p-k} \rfloor^{k-1+(p-1)+li}_{k(l-1)+(p-1)+li} \right) \\
&\circ \left(\sum_{i'\geq 0} \lfloor e_{n-k} \rfloor^{n-k-1+li'}_{(n-k)(l-1)+li'} + \sum_{i'\geq 0} \lfloor e_{p-n+k} \rfloor^{n-k-1+(p-1)+li'}_{(n-k)(l-1)+(p-1)+li'} \right)
\end{aligned}$$

A necessary condition for that term to be non-zero is $k(l-1) \equiv_{p-1} n-k-1$ as $l = 2(p-1)$. We have

$$k(l-1) - (n-k-1) \equiv_{p-1} -k - n + k + 1 = 1 - n \not\equiv_{p-1} 0,$$

since $p \leq n-1 \leq 2(p-1)-1$. So $\gamma_k \circ \gamma_{n-k} = 0$ and $\Xi_n(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) = 0$. We conclude using Lemma 45 by

$$(f_1 \circ m'_n + \Phi_n)(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}) \overset{\text{L.47,D.38}}{=} 0 \overset{\text{D.38}}{=} (m_1 \circ f_n + \Xi_n)(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}}).$$

□

One could formulate a lemma similar to Lemma 50 for the case $n > 2(p-1)$ as then the sum $\sum_{k=n-p+1}^{p-1}(-1)^{nk} m_2(f_k \otimes f_{n-k})(\overline{\chi\iota^{j_1}} \otimes \ldots \otimes \overline{\chi\iota^{j_n}})$ is in fact empty. Instead we use Lemma 33 to prove (12)[n] for $n > 2p-2$:

Proof of Theorem 39. Lemmas 41, 43, 46 and 48 to 50 ensure that (12)[n] holds for $n \in [1, 2p-2]$. Then Lemma 33 with $k = p$ proves that (12)[n] holds for all $n \in [1, \infty]$, cf. also Definition 38. By Lemma 42, f_1 is injective. By Lemma 40, the degrees are as required in Lemma 64. Lemma 64 proves that $(\mathrm{H}^* A, (m'_n)_{n\geq 1})$ is an A_∞-algebra and $(f_n)_{n\geq 1}$ is an A_∞-morphism from $(\mathrm{H}^* A, (m'_n)_{n\geq 1})$ to $(A, (m_n)_{n\geq 1})$. By Lemma 41, we have $m'_1 = 0$. Thus $(\mathrm{H}^* A, (m'_n)_{n\geq 1})$ is a minimal A_∞-algebra. By Lemma 41, the complex morphism $f_1 : (\mathrm{H}^* A, m'_1) \to (A, m_1)$ is a quasi-isomorphism which induces the identity in homology. So the A_∞-morphism $(f_n)_{n\geq 1} : (\mathrm{H}^* A, (m'_n)_{n\geq 1}) \to (A, (m_n)_{n\geq 1})$ is a quasi-isomorphism and the proof of Theorem 39 is complete. □

2.4. At the prime 2

We examine the case at the prime 2. We use a direct approach. Note that S_2 is a cyclic group so the theory of cyclic groups applies as well.

We have $\mathbb{F}_2\,\mathrm{S}_2 = \{0, (\mathrm{id}), (1,2), (\mathrm{id}) + (1,2)\}$. We have maps given by

$$\begin{array}{rrcl} \varepsilon : & \mathbb{F}_2\,\mathrm{S}_2 & \longrightarrow & \mathbb{F}_2 \\ & a(\mathrm{id}) + b(1,2) & \longmapsto & a+b \\ D : & \mathbb{F}_2\,\mathrm{S}_2 & \longrightarrow & \mathbb{F}_2\,\mathrm{S}_2 \\ & a(\mathrm{id}) + b(1,2) & \longmapsto & (a+b)\left((\mathrm{id}) + (1,2)\right). \end{array}$$

We see that ε is surjective and $\ker \varepsilon = \ker D = \operatorname{im} D = \{0, (\mathrm{id}) + (1,2)\}$. The maps ε and D are $\mathbb{F}_2\,\mathrm{S}_2$-linear, where $\mathbb{F}_2$ is the $\mathbb{F}_2\,\mathrm{S}_2$-module that corresponds to the trivial representation of S_2. So we have a projective resolution of $\mathbb{F}_2$ by

$$\operatorname{PRes} \mathbb{F}_2 := (\cdots \xrightarrow{D} \underbrace{\mathbb{F}_2\,\mathrm{S}_2}_{1} \xrightarrow{D} \underbrace{\mathbb{F}_2\,\mathrm{S}_2}_{0} \to \underbrace{0}_{-1} \to \cdots),$$

where the degrees are written below. We have the corresponding extended projective resolution

$$\cdots \xrightarrow{D} \mathbb{F}_2\,\mathrm{S}_2 \xrightarrow{D} \mathbb{F}_2\,\mathrm{S}_2 \xrightarrow{\varepsilon} \mathbb{F}_2 \to 0 \to \cdots$$

We set e_1 to be the identity on $\mathbb{F}_2\,\mathrm{S}_2$.

Let $A := \mathrm{Hom}^*_{\mathbb{F}_2\,\mathrm{S}_2}(\mathrm{PRes}\,\mathbb{F}_2, \mathrm{PRes}\,\mathbb{F}_2)$ and let the A_∞-structure on A be $(m_n)_{n\geq 1}$ (cf. Lemma 29). Recall the conventions concerning $\mathrm{Hom}^k_B(C, C')$ for complexes C, C' and $k \in \mathbb{Z}$.

Lemma 51. *An $\mathbb{F}_2$-basis of H^*A is given by $\{\overline{\xi^j} \mid j \geq 0\}$ where*

$$\xi := \sum_{i\geq 0} \lfloor e_1 \rfloor^i_{i+1} \in A.$$

Proof. Straightforward induction yields, for $j \geq 0$,

$$\xi^j = \sum_{i\geq 0} \lfloor e_1 \rfloor^i_{i+j}\,.$$

We have

$$\begin{aligned} m_1(\xi^j) &= d \circ \xi^j - (-1)^j \xi^j \circ d = d \circ \xi^j + \xi^j \circ d \\ &= \left(\sum_{i\geq 0} \lfloor D \rfloor^i_{i+1}\right) \circ \left(\sum_{i\geq 0} \lfloor e_1 \rfloor^i_{i+j}\right) + \left(\sum_{i\geq 0} \lfloor e_1 \rfloor^i_{i+j}\right) \circ \left(\sum_{i\geq 0} \lfloor D \rfloor^i_{i+1}\right) \\ &= \sum_{i\geq 0} \lfloor D \rfloor^i_{i+j+1} + \sum_{i\geq 0} \lfloor D \rfloor^i_{i+j+1} = 0, \end{aligned}$$

so ξ^j is a cycle. As $\mathrm{Hom}_{\mathbb{F}_2\,\mathrm{S}_2}(\mathbb{F}_2\,\mathrm{S}_2, \mathbb{F}_2) = \{0, \varepsilon\}$ and $\varepsilon \circ D = 0$, the differentials of $\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_2, \mathbb{F}_2)$ (cf. Lemma 34) are all zero. So $\{\varepsilon\}$ is an $\mathbb{F}_2$-basis of $\mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_2, \mathbb{F}_2)$ for $k \geq 0$. Since in the notion of Lemma 34, $\bar{\Psi}_k(\overline{\xi^k}) = \varepsilon$, the set $\{\overline{\xi^k}\}$ is an $\mathbb{F}_2$-basis of $\mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_2, \mathrm{PRes}\,\mathbb{F}_2)$ for $k \geq 0$. For $k < 0$ we have $\mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_2, \mathrm{PRes}\,\mathbb{F}_2) \cong \mathrm{H}^k\,\mathrm{Hom}^*(\mathrm{PRes}\,\mathbb{F}_2, \mathbb{F}_2) = 0$. So $\{\overline{\xi^j} \mid j \geq 0\}$ is an $\mathbb{F}_2$-basis of H^*A. $\square$

We define families of maps $(f_n : (\mathrm{H}^*A)^{\otimes n} \to A)_{n\geq 1}$ and $(m'_n : (\mathrm{H}^*A)^{\otimes n} \to \mathrm{H}^*A)_{n\geq 1}$ as follows. f_1 and m'_2 are given on a basis by

$$\begin{aligned} f_1(\overline{\xi^j}) &:= \xi^j && \text{for } j \geq 0 \\ m'_2(\overline{\xi^j} \otimes \overline{\xi^k}) &:= \overline{\xi^{j+k}} && \text{for } j, k \geq 0. \end{aligned}$$

All other maps are set to zero.

It is straightforward to check that $(\mathrm{H}^*A, (m'_n)_{n\geq 1})$ is a pre-A_∞-algebra and $(f_n)_{n\geq 1}$ is a pre-A_∞-morphism from H^*A to A. As m'_2 is associative, $(\mathrm{H}^*A, (m'_n)_{n\geq 1})$ is a dg-algebra, so in particular an A_∞-algebra. As $f_k = 0$ for $k \neq 1$, (12)[n] simplifies to

$$f_1 \circ m'_n = m_n \circ (\underbrace{f_1 \otimes \cdots \otimes f_1}_{n \text{ factors}}).$$

As $m'_n = 0$ and $m_n = 0$ for $n \geq 3$, (12)[n] is satisfied for all $n \geq 3$. For $n \in \{1, 2\}$, we have

$$\begin{aligned} f_1 \circ m'_1 &= m_1 \circ f_1 \\ f_1 \circ m'_2 &= m_2(f_1 \otimes f_1). \end{aligned}$$

The second equation follows immediately from the definition of m'_2 and f_1. The first equation holds as $m'_1 = 0$ and the images of f_1 are all cycles. So (12)[n] holds for all n and $(f_n)_{n\geq 1}$ is an A_∞-morphism from $(\mathrm{H}^*A, (m'_n)_{n\geq 1})$ to $(A, (m_n)_{n\geq 1})$. By the construction of f_1, it induces the identity on homology. Thus $(\mathrm{H}^*A, (m'_n)_{n\geq 1})$ is a minimal model of $(A, (m_n)_{n\geq 1})$.

Remark 52 (Comparison with primes $p \geq 3$)**.** At a prime $p \geq 3$, we have constructed a projective resolution with period length $l = 2(p-1)$ in (7). If one constructs a projective resolution of $\mathbb{Z}_{(2)}$ analogous to the case $p \geq 3$, we have a sequence of the form

$$\cdots \to \mathbb{Z}_{(2)}\,\mathrm{S}_2 \xrightarrow{\hat{e}^*_{2,2}} \mathbb{Z}_{(2)}\,\mathrm{S}_2 \xrightarrow{\hat{e}_{2,2}} \mathbb{Z}_{(2)}\,\mathrm{S}_2 \xrightarrow{\hat{e}^*_{2,2}} \mathbb{Z}_{(2)}\,\mathrm{S}_2 \xrightarrow{\hat{e}_{2,2}} \mathbb{Z}_{(2)}\,\mathrm{S}_2 \to 0 \to \cdots$$

with a period length of 2, where

$$\begin{aligned} \hat{e}_{2,2}\colon \ (\mathrm{id}) &\longmapsto (\mathrm{id}) - (1,2) \\ \hat{e}^*_{2,2}\colon \ (\mathrm{id}) &\longmapsto (\mathrm{id}) + (1,2). \end{aligned}$$

However, modulo 2 the differentials $\hat{e}_{2,2}$ and $\hat{e}^*_{2,2}$ reduce to the same map $D : \mathbb{F}_2\,\mathrm{S}_2 \to \mathbb{F}_2\,\mathrm{S}_2$, so we obtain a period length of 1.

The maps ι resp. χ from Proposition 35 may be identified with ξ^2 resp. ξ. This way, the definition of m'_2 at the prime 2 is readily compatible with Definition 38.

A. On the bar construction

We reuse the conventions given at the beginning of section 2.1.

A.1. The Koszul sign rule for the composition of graded maps

Lemma 53. *Let A_i, B_i, $i \in \{1,2,3\}$ be graded R-modules and $f : A_1 \to A_2$, $g : B_1 \to B_2$, $h : A_2 \to A_3$, $i : B_2 \to B_3$ graded maps. Then*

$$(h \otimes i) \circ (f \otimes g) = (-1)^{|f| \cdot |i|} (h \circ f) \otimes (i \circ g) \tag{19}$$

Proof. Let $a \in A_1$, $b \in B_1$ be homogeneous elements. Then

$$\begin{aligned}
((h \otimes i) \circ (f \otimes g))(a \otimes b) &= (-1)^{|a| \cdot |g|} (h \otimes i)(f(a) \otimes g(b)) \\
&= (-1)^{|a| \cdot |g| + |f(a)| \cdot |i|} (h \circ f)(a) \otimes (i \circ g)(b) \\
&= (-1)^{|a|(|g| + |i|) + |f| \cdot |i|} (h \circ f)(a) \otimes (i \circ g)(b) \\
&= (-1)^{|f| \cdot |i|} ((h \circ f) \otimes (i \circ g))(a \otimes b).
\end{aligned}$$

□

Multiple application of Lemma 53 yields the following

Corollary 54. *Let $n \geq 1$. Given graded R-modules V_i, W_i, U_i and graded maps $f_i : V_i \to W_i$, $g_i : W_i \to U_i$ for $i \in [1, n]$, we have*

$$(g_1 \otimes \cdots \otimes g_n) \circ (f_1 \otimes \cdots \otimes f_n) = (-1)^s (g_1 \circ f_1) \otimes \cdots \otimes (g_n \circ f_n),$$

where $s = \sum_{2 \leq i \leq n} |g_i| \cdot \left(\sum_{1 \leq j < i} |f_j| \right) = \sum_{1 \leq j < i \leq n} |g_i| \cdot |f_j|$.

A.2. Coalgebras and differential coalgebras

Definition 55.

(i) A *R-coalgebra* (B, Δ) is an R-module B equipped with a linear and coassociative *comultiplication* $\Delta : B \to B \otimes B$. *Coassociativity* means that $(1 \otimes \Delta) \circ \Delta = (\Delta \otimes 1) \circ \Delta$. We will denote R-coalgebras simply as "coalgebras".

(ii) A *coderivation of a coalgebra* (B, Δ) is a linear map $b : B \to B$ such that $\Delta \circ b = (b \otimes 1 + 1 \otimes b) \circ \Delta$.

(iii) A *codifferential of a coalgebra* (B, Δ) is a coderivation $b : B \to B$ satisfying $b^2 = 0$.

(iv) A *coalgebra morphism* $F : (B', \Delta') \to (B, \Delta)$ between coalgebras (B', Δ'), (B, Δ) is a linear map $F : B' \to B$ such that $\Delta \circ F = (F \otimes F) \circ \Delta'$.

(v) A *differential coalgebra* (B, Δ, b) is a coalgebra (B, Δ) with a codifferential b on (B, Δ).

(vi) A *morphism of differential coalgebras* $F : (B', \Delta', b') \to (B, \Delta, b)$ is a coalgebra morphism $F : (B', \Delta') \to (B, \Delta)$ that commutes with the differentials, i.e. $b \circ F = F \circ b'$.

Lemma 56.

(a) *A morphism of coalgebras is an isomorphism if and only if it is bijective.*

(b) *A morphism of differential coalgebras is an isomorphism if and only if it is bijective.*

Proof. Each isomorphism of (differential) coalgebras is bijective as it is also an isomorphism in the category of sets.

Now let $F : (B', \Delta') \to (B, \Delta)$ be a bijective morphism of coalgebras. Then we have an R-linear inverse F'. We have

$$\Delta' \circ F' = (F' \otimes F') \circ (F \otimes F) \circ \Delta' \circ F' = (F' \otimes F') \circ \Delta \circ F \circ F' = (F' \otimes F') \circ \Delta$$

so F' is a morphism of coalgebras and F an isomorphism of coalgebras.

For a bijective morphism of differential coalgebras $F : (B', \Delta', b') \to (B, \Delta, b)$, we need to check that its inverse coalgebra morphism F' commutes with the differentials. In fact,

$$F' \circ b = F' \circ b \circ F \circ F' = F' \circ F \circ b \circ F' = b \circ F'.$$

So F is an isomorphism of differential coalgebras. □

A.3. The bar construction

The following may be found e.g. in [16, 1.2.2].

Definition/Remark 57. Let V be a graded R-module. We shall define the structure of a (graded) coalgebra on the graded module $TV := \bigoplus_{k \geq 1} V^{\otimes k}$ which then will be called the *tensor coalgebra of* V. The grading on TV is given by the grading of tensor products and sums of graded R-modules, i.e. $|v_1 \otimes \cdots \otimes v_k| = \sum_{i \in [1,k]} |v_i|$ for homogeneous elements $v_1, \ldots, v_k$. The coalgebra structure is given by the comultiplication $\Delta : TV \to TV \otimes TV$ defined for elements $v_1 \otimes \cdots \otimes v_k \in V^{\otimes k}$ by

$$\begin{aligned} \Delta(v_1 \otimes \cdots \otimes v_k) &:= \sum_{1 \leq i \leq k-1} (v_1 \otimes \cdots \otimes v_i) \bigotimes (v_{i+1} \otimes \cdots \otimes v_k) \\ &= \sum_{\substack{i_1 + i_2 = k \\ i_1, i_2 \geq 1}} (v_1 \otimes \cdots \otimes v_{i_1}) \bigotimes (v_{i_1+1} \otimes \cdots \otimes v_{i_1+i_2}) \end{aligned}$$

Δ is coassociative, as for $v_1 \otimes \cdots \otimes v_k \in V^{\otimes k}$ we have

$$((\Delta \otimes 1) \circ \Delta)(v_1 \otimes \cdots \otimes v_k)$$

$$
\begin{aligned}
&= \sum_{\substack{i_1+i_2+i_3=k \\ i_1,i_2,i_3\geq 1}} (v_1 \otimes \cdots \otimes v_{i_1}) \bigotimes (v_{i_1+1} \otimes \cdots \otimes v_{i_1+i_2}) \bigotimes (v_{i_1+i_2+1} \otimes \cdots \otimes v_k) \\
&= ((1 \otimes \Delta) \circ \Delta)(v_1 \otimes \cdots \otimes v_k)
\end{aligned}
$$

So (TV, Δ) is indeed a coalgebra. The map Δ is graded of degree 0.

We have the canonical inclusions and projections for $k \geq 1$:

$$
\begin{array}{rcl}
\iota_k : V^{\otimes k} & \longrightarrow & TV \\
\pi_k : TV & \longrightarrow & V^{\otimes k}
\end{array}
$$

If we have several graded R-modules V, V', we will usually distinguish the comultiplications, inclusions and projections on TV resp. TV' by Δ resp. Δ', ι_k resp. ι'_k and π_k resp. π'_k.

We will prove $\Delta x = 0 \Leftrightarrow x \in V$ for $x \in TV$, i.e.

$$\ker \Delta = V \tag{20}$$

We have readily $V \subseteq \ker \Delta$. To prove equality we first compose Δ with the projection $\pi_1 \otimes \mathrm{id} : TV \otimes TV \to V \otimes TV$ which maps $TV \otimes TV = \bigoplus_{k\geq 1}(V^{\otimes k} \otimes TV)$ onto its first component. Secondly we compose with the multiplication $\mu : V \otimes TV \to TV, v_1 \bigotimes (v_2 \otimes \cdots \otimes v_k) \mapsto v_1 \otimes v_2 \otimes \cdots \otimes v_k$. Application to $v_1 \otimes \cdots \otimes v_k \in V^{\otimes k}$, $k \geq 2$, gives

$$
\begin{array}{ccc}
TV & \xrightarrow{\Delta} & TV \otimes TV \\
v_1 \otimes \cdots \otimes v_k & \mapsto & \displaystyle\sum_{\substack{i_1+i_2=k \\ i_1,i_2\geq 1}} (v_1 \otimes \cdots \otimes v_{i_1}) \bigotimes (v_{i_1+1} \otimes \cdots \otimes v_{i_1+i_2}) \\
 & \xrightarrow{\pi_1 \otimes \mathrm{id}} & V \otimes TV & \xrightarrow{\mu} & TV \\
 & \longmapsto & v_1 \bigotimes (v_2 \otimes \cdots \otimes v_k) & \mapsto & v_1 \otimes v_2 \otimes \cdots \otimes v_k
\end{array}
$$

So Δ is injective on $\bigoplus_{k\geq 2} V^{\otimes k}$ and zero on V, which proves (20).

For $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$, we set

$$TV_{\leq n} := \bigoplus_{k \in [1,n]} V^{\otimes k} \subseteq TV.$$

In particular $TV_{\leq \infty} = TV$.

Note that for $k \in \mathbb{Z}_{\geq 1}$

$$\operatorname{im}\left(\Delta\big|_{V^{\otimes k}}\right) \subseteq TV_{\leq k-1} \otimes TV_{\leq k-1} \subseteq TV_{\leq k} \otimes TV_{\leq k} \tag{21}$$

so $\left(TV_{\leq n}, \Delta\big|_{TV_{\leq n}}\right)$ is a subcoalgebra of (TV, Δ).

Lemma 58 (Lifting to coderivations)**.** *Let V be a graded R-module. Let $n\in\mathbb{Z}_{\geq 1}\cup\{\infty\}$. Then the map from the set of graded coderivations of $TV_{\leq n}$ of degree 1 to the set of families of graded maps $(b_k : V^{\otimes k} \to V)_{k\in[1,n]}$ with $|b_k| = 1$ for $k \in [1, n]$ that is given by*

$$b \longmapsto (\pi_1 \circ b\big|_{V^{\otimes k}})_{k\in[1,n]}$$

is bijective. Its inverse is given by $(b_k)_{k\in[1,n]} \mapsto b$, where b is defined by

$$b\big|_{V^{\otimes k}} := \sum_{\substack{r+s+t=k \\ r,t\geq 0,\ s\geq 1}} 1^{\otimes r} \otimes b_s \otimes 1^{\otimes t} \tag{22}$$

Proof. To show that $b \mapsto (b_k)_{k\in[1,n]}$ is surjective, let $(b_k : V^{\otimes k} \to V)_{k\in[1,n]}$ be a family of graded maps with $|b_k| = 1$ and construct b as given in (22). The properties $|b| = 1$, $\operatorname{im} b \subseteq TV_{\leq n}$ and $\pi_1 \circ b\big|_{V^{\otimes k}} = b_k$ follow immediately. We show that b is a coderivation:

$$\begin{aligned}
\Delta \circ b|_{V^{\otimes k}} &= \Delta \circ \sum_{\substack{r+s+t=k \\ r,t\geq 0, s\geq 1}} 1^{\otimes r} \otimes b_s \otimes 1^{\otimes t} \\
&= \sum_{\substack{r_1+r_2+s+t=k \\ r_2,t\geq 0 \\ r_1,s\geq 1}} 1^{\otimes r_1} \otimes (1^{\otimes r_2} \otimes b_s \otimes 1^{\otimes t}) + \sum_{\substack{r+s+t_1+t_2=k \\ r,t_1\geq 0 \\ t_2,s\geq 1}} (1^{\otimes r} \otimes b_s \otimes 1^{\otimes t_1}) \otimes 1^{\otimes t_2} \\
&= \sum_{\substack{r_1+t_2=k \\ r_1,t_2\geq 1}} \left(\sum_{\substack{r_2+s+t=t_2 \\ r_2,t\geq 0,s\geq 1}} 1^{\otimes r_1} \otimes (1^{\otimes r_2} \otimes b_s \otimes 1^{\otimes t}) + \sum_{\substack{r+s+t_1=r_1 \\ r,t_1\geq 0,s\geq 1}} (1^{\otimes r} \otimes b_s \otimes 1^{\otimes t_1}) \otimes 1^{\otimes t_2} \right) \\
&= (1 \otimes b + b \otimes 1) \circ \Delta
\end{aligned}$$

So $b \mapsto (b_k)_{k\in[1,n]}$ is surjective and we find a preimage as indicated by (22). For injectivity, we use the fact that set of graded coderivations of degree 1 is closed under addition, i.e. it is a R-module. So we only need to check that the kernel of $b \mapsto (b_k)_{k\in[1,n]}$ is zero:
Let $b : TV_{\leq n} \to TV_{\leq n}$ be a graded coderivation of degree 1 such that $\pi_1 \circ b\big|_{V^{\otimes k}} = 0$ for all $k \in [1, n]$. We prove by induction on $k \geq 0$ that $b\big|_{TV_{\leq k}} = 0$ thus $b = 0$: For $k = 0$ there is nothing to prove. So suppose for the induction step that $b\big|_{TV_{\leq k}} = 0$ and $k + 1 \in [1, n]$. Then $\Delta \circ b \circ \iota_{k+1} = (1 \otimes b + b \otimes 1) \circ \Delta \circ \iota_{k+1} \overset{(21),\text{ind.hyp.}}{=} 0$. So by (20), we have $b \circ \iota_{k+1} = \iota_1 \circ (\pi_1 \circ b \circ \iota_{k+1}) = 0$ and we have proven $b\big|_{TV_{\leq k+1}} = 0$.
Thus the map $b \mapsto (b_k)_{k\in[1,n]}$ is bijective and its inverse images are given by (22). $\square$

Lemma 59 (Lifting to coalgebra maps)**.**
Let V, V' be graded R-modules. Let $n \in \mathbb{Z}_{\geq 1} \cup \{\infty\}$.
The map from the set of graded coalgebra morphisms $F : TV'_{\leq n} \to TV_{\leq n}$ of degree 0 to the set of families of graded maps $(F_k : V'^{\otimes k} \to V)_{k\in[1,n]}$ with $|F_k| = 0$ for $k \in [1, n]$ given by

$$F \mapsto (\pi_1 \circ F\big|_{V'^{\otimes k}})_{k\in[1,n]}$$

is bijective. Its inverse is given by $(F_k)_{k\in[1,n]} \mapsto F$*, where* F *is defined by*

$$F\Big|_{V'^{\otimes k}} := \sum_{\substack{i_1+\ldots+i_s=k \\ i_j\geq 1}} F_{i_1}\otimes\cdots\otimes F_{i_s} \tag{23}$$

Proof. To show that $F \mapsto (F_k)_{k\in[1,n]}$ is surjective, let $(F_k : V'^{\otimes k} \to V)_{k\in[1,n]}$ be a family of graded maps with $|F_k| = 0$ for all $k \in [1,n]$ and construct F be as in (23). The properties $\pi_1 \circ F|_{V'^{\otimes k}} = F_k$, $\operatorname{im} F \subseteq TV_{\leq n}$ and $|F| = 0$ follow immediately. We show that F is a coalgebra morphism:

$$\begin{aligned}
\Delta\circ F|_{V'^{\otimes k}} &= \sum_{\substack{i_1+\ldots+i_{s+s'}=k \\ s,s',i_j\geq 1}} (F_{i_1}\otimes\cdots\otimes F_{i_s}) \otimes (F_{i_{s+1}}\otimes\cdots\otimes F_{i_{s+s'}}) \\
&= \sum_{\substack{y_1+y_2=k \\ y_1,y_2\geq 1}} \sum_{\substack{i_1+\ldots+i_s=y_1 \\ i_{s+1}+\ldots+i_{s+s'}=y_2 \\ i_j\geq 1}} (F_{i_1}\otimes\cdots\otimes F_{i_s}) \otimes (F_{i_{s+1}}\otimes\cdots\otimes F_{i_{s+s'}}) \\
&= (F\otimes F)\circ\Delta'
\end{aligned}$$

So $F \mapsto (F_k)_{k\in[1,n]}$ is surjective and we obtain a preimage as indicated by (23). To prove that $F \mapsto (F_k)_{k\in[1,n]}$ is injective, let $(F_k)_{k\in[1,n]}$ be as before and let $F, F' : TV'_{\leq n} \to TV_{\leq n}$ be coalgebra maps of degree 1 satisfying $\pi_1 \circ F\big|_{V'^{\otimes k}} = \pi_1 \circ F'\big|_{V'^{\otimes k}} = F_k$ for all $k \in [1,n]$. We prove by induction on $k \geq 0$ that $F\big|_{TV'_{\leq k}} = F'\big|_{TV'_{\leq k}}$ so $F = F'$. For $k = 0$ there is nothing to prove. So suppose $F\big|_{TV'_{\leq k}} = F'\big|_{TV'_{\leq k}}$ and $k+1 \in [1,n]$ for the induction step. We have

$$\begin{aligned}
\Delta\circ(F-F')\big|_{V'^{\otimes k+1}} &= (F\otimes F - F'\otimes F')\circ\Delta'\big|_{V'^{\otimes k+1}} \\
&= (F\otimes(F-F') - (F'-F)\otimes F')\circ\Delta'\big|_{V'^{\otimes k+1}} = 0
\end{aligned}$$

as $\operatorname{im}\left(\Delta'\big|_{V'^{\otimes k+1}}\right) \subseteq TV'_{\leq k}\otimes TV'_{\leq k}$. As $\ker\Delta = V$, we have

$$(F-F')\big|_{V'^{\otimes k+1}} = \iota_1\circ\pi_1\circ(F-F')\big|_{V'^{\otimes k+1}} = \iota_1\circ(F_{k+1}-F_{k+1}) = 0.$$

Thus we have $F\big|_{TV'_{\leq k+1}} = F'\big|_{TV'_{\leq k+1}}$ and the induction is complete. We have $F = F'$ so $F \mapsto (F_k)_{k\in[1,n]}$ is bijective and its inverse images are given by (23). □

Lemma 60. *Let* $n \in \mathbb{Z}_{\geq 1}\cup\{\infty\}$*. Let* $k \in [0,n]$ *such that* $k+1 \in [1,n]$*.*

(i) Let V *be a graded* R*-module and* $b\colon TV_{\leq n} \to TV_{\leq n}$ *be a graded coderivation with* $|b| = 1$*. Then* $b^2\big|_{TV_{\leq k}} = 0$ *implies* $\operatorname{im}(b^2\circ\iota_{k+1}) \subseteq V$*.*

(ii) Let V*,* V' *be graded* R*-modules and* $b\colon TV_{\leq n}\to TV_{\leq n}$*,* $b'\colon TV'_{\leq n}\to TV'_{\leq n}$ *be graded coderivations. Let* $F : TV'_{\leq n} \to TV_{\leq n}$ *be a graded coalgebra map with* $|F| = 0$*. Then* $(b\circ F - F\circ b')\big|_{TV'_{\leq k}} = 0$ *implies* $\operatorname{im}\left((b\circ F - F\circ b')\circ\iota'_{k+1}\right) \subseteq V$*.*

Proof. At the steps marked by "$*$" in the following, we use (21), and $b^2\big|_{TV_{\leq k}} = 0$ respectively $(F \circ b' - b \circ F)\big|_{TV'_{\leq k}} = 0$.

$$\begin{aligned}\Delta \circ b^2 \circ \iota_{k+1} &= (1 \otimes b + b \otimes 1) \circ (1 \otimes b + b \otimes 1) \circ \Delta \circ \iota_{k+1} \\ &\overset{(19),|b|=1}{=} [1 \otimes b^2 - b \otimes b + b \otimes b + b^2 \otimes 1] \circ \Delta \circ \iota_{k+1} \\ &= [1 \otimes b^2 + b^2 \otimes 1] \circ \Delta \circ \iota_{k+1} \overset{*}{=} 0\end{aligned}$$

$$\begin{aligned}\Delta \circ (F \circ b' - b \circ F) \circ \iota'_{k+1} &= [(F \otimes F) \circ \Delta' \circ b' - (1 \otimes b + b \otimes 1) \circ \Delta \circ F] \circ \iota'_{k+1} \\ &= [(F \otimes F) \circ (1 \otimes b' + b' \otimes 1) - (1 \otimes b + b \otimes 1) \circ (F \otimes F)] \circ \Delta' \circ \iota'_{k+1} \\ &\overset{(19),|F|=0}{=} [F \otimes (F \circ b' - b \circ F) + (F \circ b' - b \circ F) \otimes F] \circ \Delta' \circ \iota'_{k+1} \overset{*}{=} 0\end{aligned}$$

The lemma now follows from $\ker \Delta = V$. □

Definition/Remark 61. For a graded R-module A, we define the R-module SA with shifted grading by $SA = A$ and $(SA)^q := A^{q+1}$. We have the graded map $\omega : SA \to A$, $\omega(x) = x$ with $|\omega| = 1$. We write $SA^{\otimes k} := (SA)^{\otimes k}$ for $k \geq 1$.

Let $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$. A *corresponding pre-*$\mathrm{A}_n$*-triple on* A is defined as a triple $((m_k)_{k\in[1,n]}, (b_k)_{k\in[1,n]}, b)$ consisting of

(i) a pre-A_n-structure $(m_k)_{k\in[1,n]}$ on A,

(ii) a family of graded maps $(b_k : SA^{\otimes k} \to SA)_{k\in[1,n]}$ satisfying $|b_k| = 1$ and

(iii) a graded coalgebra map $b : TSA_{\leq n} \to TSA_{\leq n}$ of degree 1

such that $b_k = \omega^{-1} \circ m_k \circ \omega^{\otimes k}$ for $k \in [1, n]$ and $\pi_1 \circ b\big|_{SA^{\otimes k}} = b_k$ for $k \in [1, n]$.
Given a pre-A_n-structure $(m_k)_{k\in[1,n]}$ on A, a family of graded maps $(b_k : SA^{\otimes k} \to SA)_{k\in[1,n]}$ satisfying $|b_k| = 1$ or a graded coalgebra map $b : TSA_{\leq n} \to TSA_{\leq n}$ of degree 1, i.e. a datum of type (i), (ii) or (iii), it can be uniquely extended to a corresponding pre-A_n-triple on A: The condition $b_k = \omega^{-1} \circ m_k \circ \omega^{\otimes k}$ for $k \in [1, n]$ induces a bijection between data of type (i) and of type (ii). Similarly, Lemma 58 gives a bijection between data of types (ii) and (iii).

Let $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$. Let A, A' be graded R-modules. A *corresponding pre-*A_n*-morphism triple from* A' *to* A is defined as a triple $((f_k)_{k\in[1,n]}, (F_k)_{k\in[1,n]}, F)$ consisting of

(i) a pre-A_n-morphism $(f_k)_{k\in[1,n]}$ from A' to A,

(ii) a family of graded maps $(F_k : SA'^{\otimes k} \to SA)_{k\in[1,n]}$, $|F_k| = 0$ for $k \in [1, n]$ and

(iii) a graded coalgebra morphism $F : TSA'_{\leq n} \to TSA_{\leq n}$ with $|F| = 0$

such that $F_k = \omega^{-1} \circ f_k \circ \omega'^{\otimes k}$ for $k \in [1, n]$ and $\pi_1 \circ F\big|_{SA'^{\otimes k}} = F_k$ for $k \in [1, n]$. Analogous to corresponding pre-A_n-triples, given a datum of type (i), (ii) or (iii), it can be uniquely extended to a corresponding pre-A_n-morphism triple via Lemma 59 and the bijection induced by $F_k = \omega^{-1} \circ f_k \circ \omega'^{\otimes k}$.

Theorem 62 (Stasheff [21]). *Let A be a graded R-module. Let $\tilde{n} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$. Let $((m_k)_{k\in[1,\tilde{n}]}, (b_k)_{k\in[1,\tilde{n}]}, b)$ be a corresponding pre-$\mathrm{A}_{\tilde{n}}$-triple on A.*
Let $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$, $n \leq \tilde{n}$. The following are equivalent:

(a) *Equation (11)[k] holds for $k \in [1,n]$, i.e. $(m_k)_{k\in[1,n]}$ is an A_n-structure on A.*

(b) *For all $k \in [1,n]$, we have*

$$\sum_{\substack{k=r+s+t,\\ r,t\geq 0,\ s\geq 1}} b_{r+1+t} \circ (1^{\otimes r} \otimes b_s \otimes 1^{\otimes t}) = 0. \tag{24)[k}$$

(c) *$b^2\big|_{TSA_{\leq n}} = 0$, i.e. $b\big|_{TSA_{\leq n}}$ is a coalgebra differential on $TSA_{\leq n}$.*

Proof. We prove (a) $\Leftrightarrow$ (b): We have

$$\begin{aligned}
&\sum_{\substack{k=r+s+t,\\ r,t\geq 0,\ s\geq 1}} b_{r+1+t} \circ (1^{\otimes r} \otimes b_s \otimes 1^{\otimes t}) \\
=&\sum_{\substack{k=r+s+t,\\ r,t\geq 0,\ s\geq 1}} \omega^{-1} \circ m_{r+1+t} \circ (\omega^{\otimes r} \otimes \omega \otimes \omega^{\otimes t}) \circ (1^{\otimes r} \otimes b_s \otimes 1^{\otimes t}) \\
\overset{\text{C.54}}{=}&\,\omega^{-1} \circ \sum_{\substack{k=r+s+t,\\ r,t\geq 0,\ s\geq 1}} (-1)^{|\omega^{\otimes t}|\cdot|b_s|} m_{r+1+t} \circ (\omega^{\otimes r} \otimes (\omega \circ b_s) \otimes \omega^{\otimes t}) \\
=&\,\omega^{-1} \circ \sum_{\substack{k=r+s+t,\\ r,t\geq 0,\ s\geq 1}} (-1)^{t} m_{r+1+t} \circ (\omega^{\otimes r} \otimes (m_s \circ \omega^{\otimes s}) \otimes \omega^{\otimes t}) \\
\overset{\text{C.54}}{=}&\,\omega^{-1} \circ \sum_{\substack{k=r+s+t,\\ r,t\geq 0,\ s\geq 1}} (-1)^{t}(-1)^{r(2-s)} m_{r+1+t} \circ (1^{\otimes r} \otimes m_s \otimes 1^{\otimes t}) \circ (\omega^{\otimes r} \otimes \omega^{\otimes s} \otimes \omega^{\otimes t}) \\
=&\,\omega^{-1} \circ \sum_{\substack{k=r+s+t,\\ r,t\geq 0,\ s\geq 1}} (-1)^{rs+t} m_{r+1+t} \circ (1^{\otimes r} \otimes m_s \otimes 1^{\otimes t}) \circ \omega^{\otimes k}.
\end{aligned}$$

So (11)[k] $\Leftrightarrow$ (24)[k], whence (a) $\Leftrightarrow$ (b).

We prove (b) $\Leftrightarrow$ (c): We first prove for finite n that ((24)[k] for $k \in [1,n]$) $\Leftrightarrow b^2|_{TSA_{\leq n}} = 0$. We proceed by induction on $n \geq 0$.
For $n = 0$ we have $[1,n] = \emptyset$ and $TSA_{\leq n} = \{0\}$, so there is nothing to prove. So now assume for induction that $b^2|_{TSA_{\leq n}} = 0 \Leftrightarrow$ (24)[k] for $k \in [1,n]$. We have to show that $b^2|_{TSA_{\leq n+1}} = 0 \Leftrightarrow$ (24)[k] for $k \in [1, n+1]$. It is sufficient to prove under the assumption $b^2|_{TSA_{\leq n}} = 0$ the equivalence $b^2|_{SA^{\otimes n+1}} = 0 \Leftrightarrow$ (24)[$n+1$]. So we assume $b^2|_{TSA_{\leq n}} = 0$. By Lemma 60(i), we have

$$b^2|_{SA^{\otimes n+1}} = \iota_1 \circ \pi_1 \circ b^2|_{SA^{\otimes n+1}} \overset{(22)}{=} \sum_{\substack{n+1=r+s+t,\\ r,t\geq 0,\ s\geq 1}} b_{r+1+t} \circ (1^{\otimes r} \otimes b_s \otimes 1^{\otimes t}).$$

So $b^2|_{SA^{\otimes n+1}} = 0 \Leftrightarrow$ (24)[$n+1$] and the induction step is complete.

The case $n = \infty$ follows by

$$\begin{aligned} & \forall k \in \mathbb{Z}_{\geq 1} : (24)[k] && \Leftrightarrow \quad \forall k \in \mathbb{Z}_{\geq 0}\, \forall k' \in [1,k] : (24)[k'] \\ \Leftrightarrow \quad & \forall k \in \mathbb{Z}_{\geq 0} : b^2|_{TSA_{\leq k}} = 0 && \Leftrightarrow \quad b^2 = 0. \end{aligned}$$

□

Lemma 63. *Let A, A' be graded R-modules. Let $\tilde{n} \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.*
Let $((m_k)_{k\in[1,\tilde{n}]}, (b_k)_{k\in[1,\tilde{n}]}, b)$ resp. $((m'_k)_{k\in[1,\tilde{n}]}, (b'_k)_{k\in[1,\tilde{n}]}, b')$ be corresponding pre-$\mathrm{A}_{\tilde{n}}$-triples on A resp. A'. Let $((f_k)_{k\in[1,\tilde{n}]}, (F_k)_{k\in[1,\tilde{n}]}, F)$ be a corresponding pre-$\mathrm{A}_{\tilde{n}}$-morphism triple from A' to A.
Let $n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ be such that $n \leq \tilde{n}$. The following are equivalent:

(a) *Assertion (12)[k] holds for $k \in [1, n]$.*

(b) *For $k \in [1, n]$, we have*

$$\sum_{\substack{k=r+s+t \\ r,t\geq 0,\ s\geq 1}} F_{r+1+t} \circ (1^{\otimes r} \otimes b'_s \otimes 1^{\otimes t}) = \sum_{\substack{1\leq r\leq k \\ i_1+\ldots+i_r=k \\ i_s\geq 1}} b_r \circ (F_{i_1} \otimes F_{i_2} \otimes \cdots \otimes F_{i_r}). \qquad (25)[k]$$

(c) $F \circ b'\big|_{TSA'_{\leq n}} = b \circ F\big|_{TSA'_{\leq n}}$

Note that we only require conditions on the grading of $(m_n)_{n\geq 1}$ and $(m'_n)_{n\geq 1}$. We do not require them to be A_n- resp. A_∞-algebra structures on A and A'.

Proof. We prove (a) ⇔ (b): Analogously to the proof of (a) ⇔ (b) of Theorem 62 we obtain for the left side of (25)[k]

$$\sum_{\substack{k=r+s+t \\ r,t\geq 0,\ s\geq 1}} F_{r+1+t} \circ (1^{\otimes r} \otimes b'_s \otimes 1^{\otimes t}) = \omega^{-1} \circ \sum_{\substack{k=r+s+t \\ r,t\geq 0,\ s\geq 1}} (-1)^{rs+t} f_{r+1+t} \circ (1^{\otimes r} \otimes m'_s \otimes 1^{\otimes t}) \circ \omega'^{\otimes k}.$$

It remains to examine the right side:

$$\begin{aligned} \sum_{\substack{1\leq r\leq k \\ i_1+\ldots+i_r=k \\ i_s\geq 1}} b_r \circ (F_{i_1} \otimes \cdots \otimes F_{i_r}) &= \sum_{\substack{1\leq r\leq k \\ i_1+\ldots+i_r=k \\ i_s\geq 1}} \omega^{-1} \circ m_r \circ \omega^{\otimes r} \circ (F_{i_1} \otimes \cdots \otimes F_{i_r}) \\ &\overset{\text{C.54}}{=} \omega^{-1} \circ \sum_{\substack{1\leq r\leq k \\ i_1+\ldots+i_r=k \\ i_s\geq 1}} (-1)^0 m_r \circ ((\omega \circ F_{i_1}) \otimes \cdots \otimes (\omega \circ F_{i_r})) \\ &= \omega^{-1} \circ \sum_{\substack{1\leq r\leq k \\ i_1+\ldots+i_r=k \\ i_s\geq 1}} m_r \circ ((f_{i_1} \circ \omega'^{\otimes i_1}) \otimes \cdots \otimes (f_{i_r} \circ \omega'^{\otimes i_r})) \\ &= \omega^{-1} \circ \sum_{\substack{1\leq r\leq k \\ i_1+\ldots+i_r=k \\ i_s\geq 1}} (-1)^v m_r \circ (f_{i_1} \otimes \cdots \otimes f_{i_r}) \circ \omega'^{\otimes k} \end{aligned}$$

In the last step, Corollary 54 gives the exponent

$$v = \sum_{s=2}^{r} \left(|f_{i_s}| \sum_{1 \le t < s} |\omega'^{\otimes i_t}| \right) = \sum_{2 \le s \le r} \left((1 - i_s) \sum_{1 \le t < s} i_t \right) = \sum_{1 \le t < s \le r} (1 - i_s) i_t$$

So we have (12)$[k]$ $\Leftrightarrow$ (25)$[k]$, whence (a) $\Leftrightarrow$ (b).

We prove (b) $\Leftrightarrow$ (c).
We first prove (b) $\Leftrightarrow$ (c) for finite n. We proceed by induction on $n \in [0, \tilde{n}]$: For $n = 0$ we have $[1, n] = \emptyset$ and $TSA'_{\le n} = \{0\}$, so there is nothing to prove. Now suppose given n. As induction hypothesis, suppose the equivalence $F \circ b'\big|_{TSA'_{\le n}} = b \circ F\big|_{TSA'_{\le n}} \Leftrightarrow$ ((25)$[k]$ for $k \in [1, n]$) holds. For the induction step we need to prove that $F \circ b'\big|_{TSA'_{\le n+1}} = b \circ F\big|_{TSA'_{\le n+1}} \Leftrightarrow$ ((25)$[k]$ for $k \in [1, n+1]$). Suppose that $F \circ b'\big|_{TSA'_{\le n}} = b \circ F\big|_{TSA'_{\le n}}$. It suffices to show the equivalence $F \circ b'\big|_{SA'^{\otimes n+1}} = b \circ F\big|_{SA'^{\otimes n+1}} \Leftrightarrow$ (25)$[n+1]$.
By Lemma 60(ii), we have $(F \circ b' - b \circ F) \circ \iota'_{n+1} = \iota_1 \circ [\pi_1 \circ (F \circ b' - b \circ F) \circ \iota'_{n+1}]$. Now $\pi_1 \circ (F \circ b' - b \circ F) \circ \iota'_{n+1}$ is exactly the difference of the sides of (25)$[n+1]$, cf. (22),(23). So $F \circ b'\big|_{SA'^{\otimes n+1}} = b \circ F\big|_{SA'^{\otimes n+1}} \Leftrightarrow$ (25)$[n+1]$ and the induction step is complete.

The case $n = \infty$ follows by

$$\begin{array}{rlcl} & \forall k \in \mathbb{Z}_{\ge 1} : (25)[k] & \Leftrightarrow & \forall k \in \mathbb{Z}_{\ge 0}\, \forall k' \in [1, k] : (25)[k'] \\ \Leftrightarrow & \forall k \in \mathbb{Z}_{\ge 0} : F \circ b'\big|_{TSA'_{\le k}} = b \circ F\big|_{TSA'_{\le k}} & \Leftrightarrow & F \circ b' = b \circ F. \end{array}$$

□

A.4. Applications. Kadeishvili's algorithm and the minimality theorem.

In this subsection we will discuss the construction of minimal models of A_∞-algebras. Firstly, Lemma 64 states that certain pre-A_n-structures and pre-A_n-morphisms that arise in the construction of minimal models are actually A_n-structures and A_n-morphisms. Secondly, we give a proof of Theorem 32. We will review KADEISHVILI's original proof of [9] as it gives a an algorithm for constructing minimal models which can be used for the direct calculation of examples. Note that LEFÈVRE-HASEGAWA has given a generalization of the minimality theorem, see [16, Théorème 1.4.1.1], which we will not cover.

Lemma 64. *Let $n \in \mathbb{Z}_{\ge 1} \cup \{\infty\}$. Let $(A', (m'_k)_{k \in [1,n]})$ be a pre-A_n-algebra. Let $(A, (m_k)_{k \in [1,n]})$ be an A_n-algebra. Let $(f_k)_{k \in [1,n]}$ be a pre-A_n-morphism from A' to A such that* (12)$[k]$ *holds for $k \in [1, n]$. Suppose f_1 to be injective.*
Then $(A', (m'_k)_{k \in [1,n]})$ is an A_n-algebra and $(f_k)_{k \in [1,n]}$ is a morphism of A_n-algebras from $(A', (m'_k)_{k \in [1,n]})$ to $(A, (m_k)_{k \in [1,n]})$.

Proof. We have the corresponding pre-A_n-triple $((m'_k)_{k\in[1,n]}, (b'_k)_{k\in[1,n]}, b')$, the corresponding pre-$\mathrm{A}_n$-triple $((m_k)_{k\in[1,n]}, (b_k)_{k\in[1,n]}, b)$ and the corresponding pre-A_n-morphism triple $((f_k)_{k\in[1,n]}, (F_k)_{k\in[1,n]}, F)$. It suffices to prove by induction on $k \in [0,n]$ that $(b')^2\big|_{TSA'_{\leq k}} = 0$, cf. Theorem 62.

For $k = 0$, there is nothing to prove. For the induction step, suppose that $b'^{\,2}\big|_{TSA'_{\leq k}} = 0$. Then by Lemma 60(i), we have $\mathrm{im}(b'^{\,2} \circ \iota'_{k+1}) \subseteq SA$. Thus $0 = b^2 \circ F \circ \iota'_{k+1} \overset{\text{L.63}}{=} F \circ b'^{\,2} \circ \iota'_{k+1} = F_1 \circ b'^{\,2} \circ \iota'_{k+1}$. As the injectivity of f_1 implies the injectivity of F_1, we have $b'^{\,2} \circ \iota'_{k+1} = 0$ and thus $b'^{\,2}\big|_{TSA'_{\leq k+1}} = 0$. □

The following two lemmas give the incremental step in Kadeishvili's algorithm. By a quasi-monomorphism of complexes we will denote a complex morphism that induces monomorphisms on homology.

Lemma 65. *Let $n \in \mathbb{Z}_{\geq 1}$. Let A, A' be graded R-modules.*
Let $((m'_k)_{k\in[1,n+1]}, (b'_k)_{k\in[1,n+1]}, b')$ be a corresponding pre-A_{n+1}-triple on A'.
Let $((m_k)_{k\geq 1}, (b_k)_{k\geq 1}, b)$ be a corresponding pre-A_∞-triple on A.
Let $((f_k)_{k\in[1,n+1]}, (F_k)_{k\in[1,n+1]}, F)$ be a corresponding pre-A_{n+1}-morphism triple from A' to A.
Suppose that the following hold.

(i) *We have $b'^{\,2}\big|_{TSA'_{\leq n}} = 0$, $b^2 = 0$ and $F \circ b'\big|_{TSA'_{\leq n}} = b \circ F\big|_{TSA'_{\leq n}}$.*

(ii) *We have $b'_1 = 0$ and F_1 is a quasi-monomorphism from the complex (SA', b'_1) to the complex (SA, b_1).*

We set $h : SA'^{\otimes n+1} \to SA$,

$$h := \sum_{\substack{n+1=r+s+t\\ r,t\geq 0,\, s\in[2,n]}} F_{r+1+t} \circ (1^{\otimes r} \otimes b'_s \otimes 1^{\otimes t}) \quad - \sum_{\substack{r\in[2,n+1]\\ i_1+\ldots+i_r=n+1\\ i_s\geq 1}} b_r \circ (F_{i_1} \otimes F_{i_2} \otimes \cdots \otimes F_{i_r}).$$

Then

(a) $b'^{\,2} = 0$, i.e. $(A', (m'_k)_{k\in[1,n+1]})$ is an A_{n+1}-algebra[1].

(b) $b_1 \circ h = 0$.

(c) $F \circ b' = b \circ F \Leftrightarrow F_1 \circ b'_{n+1} - b_1 \circ F_{n+1} + h = 0$.

Proof. By Lemma 63, we have $F \circ b' = b \circ F \Leftrightarrow (25)[n+1]$. The difference of the sides of $(25)[n+1]$ is given by

$$\pi_1 \circ (F \circ b' - b \circ F) \circ \iota'_{n+1}$$

[1]Note that $(11)[n+1]$ does not depend on m'_{n+1} or f_{n+1}, as $m'_1 = \omega' \circ b'_1 \circ (\omega')^{-1} = 0$.

$$\overset{(22),(23)}{=} \sum_{\substack{n+1=r+s+t\\ r,t\geq 0, s\geq 1}} F_{r+1+t}\circ(1^{\otimes r}\otimes b'_s\otimes 1^{\otimes t}) \quad - \sum_{\substack{1\leq r\leq n+1\\ i_1+\ldots+i_r=n+1\\ i_s\geq 1}} b_r\circ(F_{i_1}\otimes F_{i_2}\otimes\cdots\otimes F_{i_r})$$

$$\overset{b'_1=0}{=} F_1\circ b'_{n+1} - b_1\circ F_{n+1} + h$$

Thus we have proven (c). We have

$$\begin{aligned}
b_1\circ h &= b_1\circ\pi_1\circ(F\circ b' - b\circ F)\circ\iota'_{n+1} - b_1\circ F_1\circ b'_{n+1} + (b_1)^2\circ F_{n+1}\\
&\overset{(i)}{=} b_1\circ\pi_1\circ(F\circ b' - b\circ F)\circ\iota'_{n+1} - F_1\circ b'_1\circ b'_{n+1}\\
&= b_1\circ\pi_1\circ(F\circ b' - b\circ F)\circ\iota'_{n+1}\\
&\overset{(22)}{=} b\circ\iota_1\circ\pi_1\circ(F\circ b' - b\circ F)\circ\iota'_{n+1}\\
&\overset{\mathrm{L.60}(ii)}{=} b\circ(F\circ b' - b\circ F)\circ\iota'_{n+1}\\
&\overset{(i)}{=} b\circ F\circ b'\circ\iota'_{n+1}
\end{aligned}$$

As $b'_1=0$, we obtain $\mathrm{im}(b'\circ\iota'_{n+1})\subseteq TSA'_{\leq n}$, cf. (22). By $b\circ F\big|_{TSA'_{\leq n}} = F\circ b'\big|_{TSA'_{\leq n}}$, we conclude

$$b_1\circ h = F\circ b'^{\,2}\circ\iota'_{n+1} \overset{\mathrm{L.60}(i)}{=} F\circ\iota_1\circ\pi_1\circ b'^{\,2}\circ\iota'_{n+1} = F_1\circ\pi_1\circ b'^{\,2}\circ\iota'_{n+1}$$

For $x\in SA'^{\otimes n+1}$, $(b'^{\,2}\circ\iota'_{n+1})(x) \overset{\mathrm{L.60}(i)}{=} (\pi_1\circ b'^{\,2}\circ\iota'_{n+1})(x)$ is a cycle as $b'_1=0$. Now $(F_1\circ\pi_1\circ b'^{\,2}\circ\iota'_{n+1})(x) = (b_1\circ h)(x)$ is a boundary. As F_1 is a quasi-monomorphism, $(b'^{\,2}\circ\iota'_{n+1})(x)$ is a boundary. As $b'_1=0$, this implies

$$(b'^{\,2}\circ\iota'_{n+1})(x) = 0 \tag{26}$$

So $b'^{\,2}=0$, whence $(m'_k)_{k\in[1,n+1]}$ is an A_{n+1}-structure on A' as claimed in (a). Thus, $b_1\circ h = F_1\circ\pi_1\circ b'^{\,2}\circ\iota'_{n+1} = 0$ as claimed in (b). □

Lemma 66. *Let $n\in\mathbb{Z}_{\geq 1}$. Let $(A,(m_k)_{k\geq 1})$ be an A_∞-algebra. Let $(A',(m'_k)_{k\in[1,n]})$ be an A_n-algebra. Let $(f_k)_{k\in[1,n]}$ be an A_n-morphism from $(A',(m'_k)_{k\in[1,n]})$ to $(A,(m_k)_{k\in[1,n]})$. Suppose the following hold.*

(i) We have $m'_1=0$ and f_1 is a quasi-isomorphism from the complex (A',m'_1) to the complex (A,m_1).

(ii) A' is a projective R-module.

Then there exist f_{n+1} and m'_{n+1} such that $(A',(m'_k)_{k\in[1,n+1]})$ is an A_{n+1}-algebra and $(f_k)_{k\in[1,n+1]}$ is an A_{n+1}-morphism from $(A',(m'_k)_{k\in[1,n+1]})$ to $(A,(m_k)_{k\in[1,n+1]})$.

Note that $(A')^k\cong H^k(A,m_1)$ for $k\in\mathbb{Z}$.

Proof. We have the corresponding triples $((m_k)_{k\geq 1},(b_k)_{k\geq 1},b)$, $((m'_k)_{k\in[1,n]},(b'_k)_{k\in[1,n]},b')$ and $((f_k)_{k\in[1,n]},(F_k)_{k\in[1,n]},F)$. Note that the term h of Lemma 65 does not depend on

b'_{n+1} or F_{n+1}, so h can be unambiguously defined even when m'_{n+1} and F_{n+1} are not yet defined and we have $b_1 \circ h = 0$. Motivated by Lemma 65(c), we seek (properly graded) morphisms $b'_{n+1} : SA'^{\otimes n+1} \to SA'$ and $F_{n+1} : SA'^{\otimes n+1} \to SA$ such that the following holds.

$$h = b_1 \circ F_{n+1} - F_1 \circ b'_{n+1} \tag{27}$$

We will construct b'_{n+1} and F_{n+1} on each $(SA'^{\otimes n+1})^q$, $q \in \mathbb{Z}$ individually. As $SA' \cong A$ as R-modules, SA' is projective. As a tensor product of projective modules, $SA'^{\otimes n+1}$ is projective. $(SA'^{\otimes n+1})^q$ is projective as a direct summand of $SA'^{\otimes n+1}$. There exists a free R-module G together with a surjective morphism $g : G \to (SA'^{\otimes n+1})^q$ (e.g. set G to be the free R-module over the set $(SA'^{\otimes n+1})^q$). By the universal property of the projective module $(SA'^{\otimes n+1})^q$, there exists a morphism $g^* : (SA'^{\otimes n+1})^q \to G$ such that $g \circ g^* = \mathrm{id}_{(SA'^{\otimes n+1})^q}$. Let $\mathscr{B}$ be a basis of G. We will define $\tilde{b}'_{n+1} : G \to (SA')^{q+1}$ and $\tilde{F}_{n+1} : G \to (SA)^q$ such that

$$h \circ g = b_1 \circ \tilde{F}_{n+1} - F_1 \circ \tilde{b}'_{n+1}. \tag{28}$$

We define $\tilde{b}'_{n+1}$ and $\tilde{F}_{n+1}$ by giving them on basis elements $v \in \mathscr{B}$: As $b_1 \circ h = 0$, $h(g(v))$ is a cycle. As by (i), F_1 is a quasi-isomorphism from (SA', b'_1) to (SA, b_1) and $b'_1 = 0$, F_1 is in fact a quasi-isomorphism from the homology of SA to SA, i.e. each homology class of SA contains exactly one element of $\operatorname{im} F_1$. Thus there is an unique element $y \in SA'$ such that $h(g(v))$ and $F_1(y)$ are in the same homology class. As $|h| = 1$ and $|F_1| = 0$, we have $|y| = |g(v)| + 1 = q + 1$. Thus $h(g(v)) - F_1(y)$ is a boundary and homogeneous of degree $q + 1$. Thus as $|b_1| = 1$, we can select an element $z \in SA$, $|z| = q$ such that $h(g(v)) - F_1(y) = b_1(z)$. Now set $\tilde{b}'_{n+1}(v) := -y$ and $F_{n+1}(v) := z$. By the grading of y and z, we obtain morphisms $\tilde{b}'_{n+1} : G \to (SA')^{q+1}$ and $\tilde{F}_{n+1} : G \to (SA)^q$. These maps satisfy by construction (28). We set $b'_{n+1}\big|_{(SA'^{\otimes n+1})^q} = \tilde{b}'_{n+1} \circ g^*$ and $F_{n+1}\big|_{(SA'^{\otimes n+1})^q} = \tilde{F}_{n+1} \circ g^*$. Then

$$\begin{aligned} h\big|_{(SA'^{\otimes n+1})^q} &= h \circ g \circ g^* \overset{(28)}{=} (b_1 \circ \tilde{F}_{n+1} - F_1 \circ \tilde{b}'_{n+1}) \circ g^* \\ &= b_1 \circ F_{n+1}\big|_{(SA'^{\otimes n+1})^q} - F_1 \circ b'_{n+1}\big|_{(SA'^{\otimes n+1})^q} \end{aligned}$$

Thus we obtain morphisms b'_{n+1} and F_{n+1} such that (27) holds. As $\operatorname{im}\left(b'_{n+1}\big|_{(SA'^{\otimes n+1})^q}\right) \subseteq (SA')^{q+1}$ and $\operatorname{im}\left(F_{n+1}\big|_{(SA'^{\otimes n+1})^q}\right) \subseteq (SA)^q$, we have $|b'_{n+1}| = 1$ and $|F_{n+1}| = 0$. Using b'_{n+1} and F_{n+1}, we extend the corresponding triples $((m'_k)_{k\in[1,n]}, (b'_k)_{k\in[1,n]}, b')$ and $((f_k)_{k\in[1,n]}, (F_k)_{k\in[1,n]}, F)$ to corresponding triples $((m'_k)_{k\in[1,n+1]}, (b'_k)_{k\in[1,n+1]}, \hat{b}')$ and $((f_k)_{k\in[1,n+1]}, (F_k)_{k\in[1,n+1]}, \hat{F})$. Recall Theorem 62 and Lemma 63. Via Lemma 65, $(A', (m'_k)_{k\in[1,n+1]})$ is an A_{n+1}-algebra and $\hat{F} \circ \hat{b}' = b \circ \hat{F}$. So we have proven that $(f_k)_{k\in[1,n+1]} : (A', (m'_k)_{k\in[1,n+1]}) \to (A, (m_k)_{k\in[1,n+1]})$ is a morphism of A_{n+1}-algebras. $\square$

Concerning Lemma 66, we may now also construct m'_{m+1} and f_{m+1} directly: We construct (properly graded) maps m'_{m+1} and f_{m+1} such that (12)$[m+1]$ holds. Such m'_{m+1} and f_{m+1} exist by Lemma 66. Then Lemma 64 ensures that all other requirements are met.

Theorem 67 (Kadeishvili's algorithm for the minimality theorem)**.** *Let $(A,(m_k)_{k\geq 1})$ be an A_∞-algebra. Let H^*A be its homology. Suppose H^*A is a projective R-module. Then we construct a minimal model as follows:*

For $q \in \mathbb{Z}$, $\mathrm{H}^qA = \ker(m_1\big|_{A^q})/\operatorname{im}(m_1\big|_{A^{q-1}})$ is projective as a direct summand of H^*A. The residue class map $P_q : \ker(m_1\big|_{A^q}) \to \mathrm{H}^qA$ is surjective. By the universal property of the projective module H^qA, there exists $P_q^* : \mathrm{H}^qA \to \ker(m_1\big|_{A^q})$ such that $P_q \circ P_q^* = id_{\mathrm{H}^qA}$. Thus P_q^* maps each homology class $\bar{x}$ in H^qA to a representing cycle x with $|x| = q = |\bar{x}|$. Then $f_1 : \mathrm{H}^*A \to A$ defined by $f_1\big|_{\mathrm{H}^qA} = P_q^*$ maps each homology class to a representing cycle and $|f_1| = 0$.

We set $m_1' : \mathrm{H}^*A \to \mathrm{H}^*A$, $m_1' = 0$. We have $f_1 \circ m_1' \overset{m_1'=0}{=} 0 \overset{\operatorname{im} f_1 \subseteq \ker m_1}{=} m_1 \circ f_1$, so $f_1 : (\mathrm{H}^*A, m_1') \to (A, m_1)$ is a quasi-isomorphism and also a morphism of A_1-algebras. By construction, $f_1 : (\mathrm{H}^*A, m_1') \to (A, m_1)$ induces the identity in homology.

We then use Lemma 66 to inductively construct an A_∞-structure $(m_k')_{k\geq 1}$ on H^*A and a quasi-isomorphism $(f_k)_{k\geq 1}$ of A_∞-algebras from $(\mathrm{H}^*A, (m_k')_{k\geq 1})$ to $(A, (m_k)_{k\geq 1})$.

References

[1] Benson, D.J. *Representations and cohomology I: Basic representation theory of finite groups and associative algebras*, Cambridge Univ. Press, 1998

[2] Bourbaki, N. *Éléments de mathématique. - Fasc. 27 : Algèbre commutative*, 1961

[3] Bourbaki, N. *Éléments de mathématique - Algèbre - Chapitre 10: Algèbre homologique*, 1980

[4] Green, J.A. *Walking around the Brauer tree*, Journal of the Australian Mathematical Society, Volume 17, Issue 2, p. 197-213, 1974

[5] Gugenheim, V.K.A.M., Lambe, L.A., and Stasheff, J.D., *Perturbation theory in differential homological algebra II*, Illinois J. Math. 35, p. 357-373, 1991

[6] James, G.D., *The Representation Theory of the Symmetric Groups*, Lecture Notes in Mathematics 682, Springer-Verlag, 1978

[7] Johansson, L., and Lambe, L.*Transferring Algebra Structures Up to Homology Equivalence*, Math. Scand. 89, p. 181-200, 2001

[8] Kadeishvili, T.V., *On the homology theory of fiber spaces*, Russian Math. Surveys, 35:3, p. 231-238, 1980

[9] Kadeishvili, T.V., *Algebraic Structure in the Homologies of an* $A(\infty)$*-Algebra (Russian)*, Bulletin of the Academy of Sciences of the Georgian SSR 108 No 2, p. 249-252, 1982

[10] Kadeishvili, T.V., *The functor D for a category of A(∞)-algebras (Russian)*, Bulletin of the Academy of Sciences of the Georgian SSR 125, p. 273-276, 1987

[11] Keller, B., *A-infinity algebras in representation theory*, Contribution to the Proceedings of ICRA IX, Beijing, 2000

[12] Keller, B., *Introduction to A-infinity algebras and modules*, Homology, Homotopy and Applications vol. 3(1), 2001

[13] Keller, B., *Addendum to 'Introduction to A-infinity algebras and modules'*, 2002

[14] Klamt, A., A_∞*-structures on the algebra of extension of Verma modules in the parabolic category* $\mathcal{O}$, Diplomarbeit, 2010

[15] Künzer, M., *Ties for the integral group ring of the symmetric group*, Thesis, 1999

[16] Lefèvre-Hasegawa, K., *Sur les* A_∞*-catégories*, Thesis, 2003

[17] Madsen, D.,*Homological aspects in representation theory*, Thesis, 2002

[18] Merkulov, S.A., *Strong homotopy algebras of a Kähler manifold*, Int. Math. Res. Notices, Vol. 1999, p. 153-164, 1999

[19] Peel, M.H., *Hook representations of the symmetric groups*, Glasgow Mathematical Journal, 1971

[20] Prouté, A., *Algèbres différentielles fortement homotopiquement associatives*, Thèse d'Etat, Université Paris VII, 1984

[21] Stasheff, J.D., *Homotopy associativity of H-spaces II*, Trans. Amer. Math. Soc. 108, p. 293-312, 1963

[22] Vejdemo-Johansson, M., *Computation of* A_∞*-algebras in group cohomology*, Thesis, 2008

[23] Vejdemo-Johansson, M., *A partial* A_∞*-structure on the cohomology of* $C_m \times C_n$, Journal of Homotopy and Related Structures, vol. 3(1), p. 1-11, 2008

[24] Vejdemo-Johansson, M., *Blackbox computation of* A_∞*-algebras*, Georgian Mathematical Journal Volume 17 Issue 2, p. 391-404, 2010