Encoding Cohomology, Classifying Extensions, and Explicit Galois Gerbs

Nir Elber

July 11, 2022

Abstract

We use group cohomology to provide some general theory to classify all group extensions of a G-module A in the case of an abelian group G. The main idea is to use a group presentation of G provide a group presentation of the extension using specially chosen elements of A. It turns out that this "encoding" of the extension into elements of A enjoys a number of homological niceties, which are of separate interest. This machinery is then used to provide explicit group presentations for the various Kottwitz gerbs [Kot14], in special cases.

Contents

1 Introduction

Given a Galois extension of fields of L/K with Galois group G and an algebraic torus $\mathbb{T}$, a Galois gerb $\mathcal{E}$ of L/K bound by $\mathbb{T}$ is a group extension

$$0 \to \mathbb{T}(L) \to \mathcal{E} \to G \to 0.$$

Roughly speaking, the goal of the paper is to be able to describe such Galois gerbs—and group extensions in general—explicitly by giving $\mathcal{E}$ a group presentation.

More specifically, let L/K be a finite Galois extension of global fields with Galois group G. In [Kot14], Kottwitz defined three global gerbs $\mathcal{E}_1$, $\mathcal{E}_2$, and $\mathcal{E}_3$. The overall goal of this paper is to be able to provide a somewhat explicit description of the group law for $\mathcal{E}_3$ in the toy case of $L = \mathbb{Q}(\zeta_q)$ and $K = \mathbb{Q}$ for q a prime-power. Along the way, we will develop various tools which suggest that the methods can be feasibly extended beyond this toy case.

To describe the approach, we quickly recall the definitions of $\mathcal{E}_1$, $\mathcal{E}_2$, and $\mathcal{E}_3$. Let V_F denote the set of places of a global field F. We begin with the following short exact sequences.

$$0 \to \mathbb{Z}[V_L]_0 \to \mathbb{Z}[V_L] \to \mathbb{Z} \to 0 \tag{X}$$
$$0 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{A}_L^\times / L^\times \to 0 \tag{A}$$

Selecting the global fundamental class $\alpha_1(L/K) = u_{L/K} \in \widehat{H}^2(G, \mathbb{A}_L^\times/L^\times)$, we may construct the Galois gerb

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{A}_L^\times/L^\times) \to \mathcal{E}_1 \to G \to 0.$$

By gluing together local fundamental classes, we may construct a class $\alpha_2(L/K) \in \widehat{H}^2(G, \mathbb{A}_L^\times)$ defining the Galois gerb

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], \mathbb{A}_L^\times) \to \mathcal{E}_2 \to G \to 0.$$

Constructing $\mathcal{E}_3$ is more difficult. Denote the set of morphisms of short exact sequences from (X) to (A) by $\mathrm{Hom}(X, A)$. It turns out that

$$\begin{array}{ccc} H^2(G, \mathrm{Hom}(X, A)) & \longrightarrow & H^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], \mathbb{A}_L^\times)) \\ \downarrow & & \downarrow \\ H^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{A}_L^\times/L^\times)) & \longrightarrow & H^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], \mathbb{A}_L^\times/L^\times)) \end{array} \tag{1.1}$$

is a pull-back square, so we can check that we can construct a unique element $\alpha(L/K) \in H^2(G, \mathrm{Hom}(X, A))$ by $\alpha_1(L/K)$ and $\alpha_2(L/K)$. Projecting $\alpha(L/K)$ to $H^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L]_0, L^\times))$ yields α_3 and hence the Galois gerb

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L]_0, L^\times) \to \mathcal{E}_3 \to G \to 0.$$

Most of this definition can be turned directly into a computation. For example, a 2-cocycle representing $\alpha_1(L/K) = u_{L/K}$ is not too hard to construct, especially in our toy case of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$. Continuing, finding a representative for $\alpha_2(L/K)$ is simply a matter of constructing local fundamental classes and then gluing them together appropriately. However, it is harder to make the pull-back square of (1.1). In short, this requires choosing a representative for α_2 in such a way to appropriately cohere with our choice of representative for α_1. This is by far the hardest part of this approach.

The layout of the paper is as follows. To write down the group law of a group extension of a group G by a G-module A requires being able to easily carry around 2-cocycles in $Z^2(G, A)$. As such, section 3 is interested in studying how one can, in general, encode cocycles. This section is rather pure homological algebra and is largely of separate interest.

The rest of the paper is interested in abelian groups G. In section 4, we describe a natural way to give a group extension of G by a G-module A a group law and use this to provide a classification of group extensions. In section 5, we recast this theory in the abstract more machinery established in section 3.

Having established enough algebra, we turn to executing the above computation. In section 6, we use the framework provided by section 4 to write down local fundamental classes of abelian extensions. Lastly, section 7 finishes the computation by gluing the local fundamental classes together appropriately to represent $\alpha_2(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and so also $\alpha_3(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, in our toy case.

2 Background

In this section, we familiarize ourselves with various tools used throughout the paper.

2.1 Group Cohomology

Fix G to be a group. There is a unique sequence of functors $H^i(G, -)\colon \mathrm{Mod}_G \to \mathrm{Ab}$ for $i \in \mathbb{N}$ satisfying the following set of properties.

- $H^0(G, -) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -) = (-)^G$.

- $H^i(G, I) = 0$ for all $i > 1$ and injective modules I.
- There is a functor taking short exact sequences

$$0 \to A \to B \to C \to 0$$

of G-modules to long exact sequences

$$0 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \cdots.$$

The functors $H^i(G, -)$ are the cohomology functors. Analogously, there is a unique sequence of functors $H_i(G, -) \colon \mathrm{Mod}_G \to \mathrm{Ab}$ for $i \in \mathbb{N}$ satisfying the following set of properties.

- $H_0(G, -) = \mathbb{Z} \otimes_{\mathbb{Z}[G]} -$.
- $H_i(G, P) = 0$ for all $i > 1$ and projective modules P.
- There is a functor taking short exact sequences

$$0 \to A \to B \to C \to 0$$

of G-modules to long exact sequences

$$\cdots \to H_2(G, C) \to H_1(G, A) \to H_1(G, B) \to H_1(G, C) \to H_0(G, A) \to H_0(G, B) \to H_0(G, C) \to 0.$$

Finish? It turns out that we can tie these together by defining Tate cohomology:

2.2 Group Extensions

We continue with G as a group and A as a G-module. We have the following definition.

Definition 1. Let G be a group and A a G-module. A *group extension $\mathcal{E}$ of G by A* is a short exact sequence

$$0 \to A \xrightarrow{\iota} \mathcal{E} \xrightarrow{\pi} G \to 0$$

such that any $a \in A$ and $w \in \mathcal{E}$ have

$$\pi(w) \cdot \iota(a) = \iota\left(waw^{-1}\right).$$

For example, Galois gerbs are group extensions.

An isomorphism of group extensions $\mathcal{E}_1 \to \mathcal{E}_2$ is a morphism of the corresponding short exact sequences, as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathcal{E}_1 & \longrightarrow & G & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & \mathcal{E}_2 & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

By the Five lemma, all such morphisms must be isomorphisms of short exact sequences, which justify why these are isomorphisms of group extensions.

We have the following classification result.

Theorem 2 ([Bro82, Theorem IV.3.12])**.** Let G be a group and A a G-module. Then isomorphism classes of group extensions $\mathcal{E}$ of G by A are in bijection with cohomology classes in $H^2(G, A)$.

Sketch. We will describe the maps from 2-cocycles to group extensions and vice versa; that the maps are well-defined and provided the needed isomorphism are a matter of computation. In one direction, fix a group extension

$$0 \to A \xrightarrow{\iota} \mathcal{E} \xrightarrow{\pi} G \to 0.$$

Now, choose a set-theoretic lift $s\colon G \to \mathcal{E}$ of π, and it turns out that the function $c\colon G^2 \to A$ given by

$$c(g,h) \coloneqq s(g)s(h)s(gh)^{-1}$$

defines a 2-cocycle $c \in Z^2(G,A)$.

In the other direction, fix a 2-cocycle $c \in Z^2(G,A)$. Then we build the extension

$$0 \to A \xrightarrow{\iota} \mathcal{E}_c \xrightarrow{\pi} G \to 0$$

as follows. As a set, $\mathcal{E}_c = A \times G$, with group law defined by

$$(a,g)(a',g') \coloneqq \big(a + g \cdot a' + c(g,g'), gg'\big).$$

The identity is $(-c(1,1),1)$. To finish, we define $\pi\colon \mathcal{E}_c \to G$ by projection and $\iota\colon A \to \mathcal{E}_c$ by $a \mapsto (a - c(1,1),1)$. ■

The isomorphism of Theorem 2 also behaves well with the functoriality of our cohomology groups. For example, a group homomorphism $\varphi\colon G \to H$ and G-module A induces a map $H^2(H,A) \to H^2(G,A)$. On the side of group extensions, given a class $u \in H^2(H,A)$ corresponding to the group extension $\mathcal{E}$, we can construct $\mathcal{E}'$ corresponding to $\varphi(u)$ by pulling back as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathcal{E} & \longrightarrow & H & \longrightarrow & 0 \\ & & \| & & \uparrow & & \uparrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & A & \longrightarrow & \mathcal{E}' & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

Similarly, a G-module homomorphism $f\colon A \to B$ induces a map $H^2(G,A) \to H^2(G,B)$. On the side of group extensions, given a class $u \in H^2(G,A)$ corresponding to the group extension $\mathcal{E}$, we can construct $\mathcal{E}'$ corresponding to $f(u)$ by pushing out as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathcal{E} & \longrightarrow & G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & B & \longrightarrow & \mathcal{E}' & \longrightarrow & G & \longrightarrow & 0 \end{array}$$

2.3 Class Field Theory

For our purposes, class field theory will be used to be able to describe certain cohomology groups associated to local and global fields.

2.3.1 Local Class Field Theory

We begin with the local story. Let L/K be a finite Galois extension of degree n and Galois group $G \coloneqq \mathrm{Gal}(L/K)$. Because we are interested in extensions, we begin with what $H^2\left(G, L^\times\right)$ looks like.

Theorem 3 ([Mil20, Lemma III.2.2]). Let L/K be a Galois extension of local fields of degree n and Galois group $G \coloneqq \mathrm{Gal}(L/K)$. Then there is a canonical isomorphism

$$\mathrm{inv}\colon H^2\left(G, L^\times\right) \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

The element of $H^2(G,L^\times)$ corresponding to $\frac{1}{n}$ deserves a name.

Definition 4. Let L/K be a Galois extension of local fields of degree n and Galois group $G \coloneqq \mathrm{Gal}(L/K)$. Then the *local fundamental class* $u_{L/K}$ is the class in $H^2(G, L^\times)$ with

$$\mathrm{inv}\, u_{L/K} = 1/n.$$

The local fundamental class satisfies a number of good functoriality properties.

Proposition 5 ([Mil20, Lemma III.2.7])**.** Let $M/L/K$ be a tower of finite local field extensions where M/K is Galois. Then

$$\mathrm{Res}\, u_{M/K} = u_{M/L}.$$

If L/K is also Galois, then

$$\mathrm{Inf}\, u_{L/K} = [M : L] u_{M/K}.$$

With the machinery in place, we might as well mention the local Artin reciprocity map.

Theorem 6 ([Mil20, Theorem III.3.1])**.** Let L/K be a finite Galois extension of local fields with Galois group G. Then the map

$$(u_{L/K} \cup -) \colon \widehat{H}^i(G, \mathbb{Z}) \to \widehat{H}^{i+2}\left(G, L^\times\right)$$

is an isomorphism for all $i \in \mathbb{Z}$.

Remark 7. More generally, if T is an algebraic K-torus which splits over L, then the map

$$(u_{L/K} \cup -) \colon \widehat{H}^i(G, X_*(T)) \to \widehat{H}^{i+2}\left(G, L^\times\right)$$

is an isomorphism for all $i \in \mathbb{Z}$; see [PR94, Theorem 6.2].

2.3.2 Global Class Field Theory

We now turn to the global story. Given a global field K, we let V_K denote its set of places.

Let L/K be a finite Galois extension of global fields of degree n and Galois group $G \coloneqq \mathrm{Gal}(L/K)$. To be able to make class field theory, we need to fix the correct objects.

Definition 8. Given a global field K, we define the *ring of adelés* to be the restricted direct product

$$\mathbb{A}_K \coloneqq \prod_{v \in V_K} (K_v, \mathcal{O}_v).$$

Namely, we are considering infinite tuples $(a_v)_{v \in V_K}$, where $a_v \in K_v$ for each $v \in V_K$ but $v \in \mathcal{O}_v$ for all but finitely many $v \in V_K$.

Observe that there is a natural embedding $K \hookrightarrow \mathbb{A}_K$ by

$$a \mapsto (a)_{v \in V_K}.$$

This embedding descends to an embedding $K^\times \hookrightarrow \mathbb{A}_K^\times / K^\times$, which lets us consider the quotient $\mathbb{A}_K^\times / K^\times$.

It turns out that $\mathbb{A}_K^\times$ and $\mathbb{A}_K^\times / K^\times$ are the right objects to study. For example, we have the following result.

Theorem 9 ([Mil20, Proposition 2.5])**.** Let L/K be a finite Galois extension of global fields with Galois group $G \coloneqq \mathrm{Gal}(L/K)$. Then the various restrictions define an isomorphism

$$\widehat{H}^i(G, \mathbb{A}_L^\times) \simeq \bigoplus_{u \in V_K} \widehat{H}^i(G, L_v^\times),$$

for $i \geq 0$, where the $v \in V_L$ is a chosen prime over each $u \in V_K$.

We also have a global invariant map.

Theorem 10 ([Tat10, p. 194])**.** Let L/K be a finite Galois extension of global fields of degree n with Galois group $G \coloneqq \mathrm{Gal}(L/K)$. Then there is a canonical map

$$\mathrm{inv} = \sum_{v \in V_L} \mathrm{inv}_v \colon H^2(G, \mathbb{A}_L^\times) \to \mathbb{Q}/\mathbb{Z}$$

induced by the local invariant maps and Theorem 9. This map induces an isomorphism

$$\mathrm{inv} \colon H^2(G, \mathbb{A}_L^\times / L^\times) \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

As before, the canonical generator we chose will be of special interest.

Definition 11. Let L/K be a Galois extension of global fields of degree n with Galois group G. Then the *global fundamental class* $u_{L/K}$ is the class in $H^2\left(G, \mathbb{A}_L^\times / L^\times\right)$ with

$$\mathrm{inv}\, u_{L/K} = 1/n.$$

And, for fun, here is our global Artin reciprocity map.

Theorem 12 ([Tat10, p. 197])**.** Let L/K be a Galois extension of global fields of degree n with Galois group G. Then the map

$$(u_{L/K} \cup -) \colon \widehat{H}^i(G, \mathbb{Z}) \to \widehat{H}^{i+2}\left(G, \mathbb{A}_L^\times / L^\times\right)$$

is an isomorphism for all $i \in \mathbb{Z}$.

3 Generalized Periodic Cohomology

The goal of this section is to separate out what we can, a priori, expect from "encoding" modules from what is a special property of the specific encoding module we study in the rest of the paper. As such, we should begin by motivating encoding modules.

Throughout this section, let G be a finite group. When $G = \langle \sigma \rangle$ is a cyclic group of order n, it is an amazing feature that there is some $\chi \in \widehat{H}^2(G, \mathbb{Z})$ granting isomorphisms

$$(\chi \cup -) \colon \widehat{H}^0(G, M) \to \widehat{H}^2(G, M) \tag{3.1}$$

for any G-module M. In fact, it is not too hard to write down χ as being represented by the "carrying" 2-cocycle

$$\left(\sigma^i, \sigma^j\right) \mapsto \left\lfloor \frac{i+j}{n} \right\rfloor,$$

so (3.1) is telling us that we can represent each cohomology class of $\widehat{H}^2(G, M)$ by a 2-cocycle of the form

$$\left(\sigma^i, \sigma^j\right) \mapsto \left\lfloor \frac{i+j}{n} \right\rfloor \alpha$$

for some $\alpha \in M^G$. This "classification" of 2-cocycles in $\widehat{H}^2(G, M)$ is incredibly useful and makes cyclic groups very easy to work with computationally.

From one perspective, this classification of 2-cocycles for cyclic groups says that we can retrieve all 2-cocycles by keeping track of the single element $\alpha \in M^G = H^0(G, M)$, modulo some equivalence relation coming from Tate cohomology. The algebraic way to choose a single element of M^G is by elements in

$$\mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, M^G\right) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

As such, one can phrase (3.1) as providing a natural isomorphism

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)) \Rightarrow \widehat{H}^2(G, -).$$

Here, the choice of G-module $\mathbb{Z}$ in some sense "encodes" 2-cocycles from $\widehat{H}^2(G, M)$ into a single morphism from $\mathbb{Z}$ to M, modulo some equivalence relations.

More generally, permit G to be non-cyclic, and suppose we have a G-module $\mathbb{Z}[G]^m/I$ for some $m \geq 0$ and G-submodule I with isomorphisms

$$\widehat{H}^0\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^m/I, M)\right) \to \widehat{H}^2(G, M),$$

for any G-module M. In this case, we see we are still encoding 2-cocycles into morphisms, where these morphisms look like

$$\widehat{H}^0\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^m/I, M)\right) = \frac{\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathbb{Z}[G]^m/I, M\right)}{N_G \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^m/I, M)}.$$

To see the encoding here, view the numerator as choosing out an m-tuple of elements of M in the same way that we would choose morphisms $\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathbb{Z}[G]^m, M\right)$, but we can't just choose any m elements because they must saitsfy some relations dictated by I. Then the denominator provides an equivalence relation of the m-tuples which determines if two tuples live in the same "class."

The above discussion is intended to motivate the following definition.

Definition 13. Let G be a finite group and $r \in \mathbb{Z}$ be an index. Then a G-module X is an *r-encoding G-module* if and only if there is a natural isomorphism

$$\Phi_\bullet \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{i+r}(G, -)$$

for some $i \in \mathbb{Z}$.

We will abbreviate the G from "r-encoding G-module" whenever confusion is unlikely to arise.

It will turn out that the index $i \in \mathbb{Z}$ is more or less irrelevant. Indeed, we will be able to show the following equivalences.

Theorem 14. Let G be a finite group. Given a G-module X and index $r \in \mathbb{Z}$, the following are equivalent.

(a) X is an r-encoding module.

(b) If $r \geq 0$, then X is cohomologically equivalent to $I_G^{\otimes r}$; if $r < 0$, then X is cohomologically equivalent to $\mathrm{Hom}_{\mathbb{Z}}(I_G^{\otimes r}, \mathbb{Z})$.

(c) There is $x \in \widehat{H}^r(G, X)$ granting a natural isomorphism

$$(x \cup -)\colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{i+r}(G, -)$$

for any $i \in \mathbb{Z}$.

(d) There are $x \in \widehat{H}^r(G, X)$ and $x^\vee \in \widehat{H}^{-r}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}))$ such that

$$x \cup x^\vee = [1] \in \widehat{H}^0(G, \mathbb{Z}) \qquad \text{and} \qquad x^\vee \cup x = [\mathrm{id}_X] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)).$$

(e) We can find $x \in \widehat{H}^r(G, X)$ yielding natural isomorphisms

$$(- \cup x)\colon \widehat{H}^i(G, -) \Rightarrow \widehat{H}^{i+r}(G, - \otimes_{\mathbb{Z}} X)$$

for all $i \in \mathbb{Z}$.

If X is also $\mathbb{Z}$-free, these are equivalent to

(f) $\widehat{H}^r(G, X) \cong \mathbb{Z}/\#G\mathbb{Z}$ and $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X))$ is cyclic.

Proof. The equivalence of (a) and (b) follow from combining Proposition 47 with Example 48 and Example 80. The equivalence of (c) follows from Corollary 51. Continuing, the equivalence of (d) follows from Proposition 60. The equivalence of (e) follows from Theorem 66 and the discussion in Remark 67. Lastly, the equivalence of (f) follows from Proposition 71. ∎

When we may take $X = \mathbb{Z}$ (e.g., when G is cyclic), we are essentially studying groups with periodic cohomology, so many results in this section will mimic these results. However, periodic cohomology requires somewhat stringent conditions on the group itself, and allowing this "free parameter" X will permit general groups at the cost of a perhaps more complex X. For example, when $r \geq 0$, we can take $X = I_G^{\otimes r}$ for any finite group G, though this G-module is quite rough to handle.

In general, it can be an interesting question what specified abelian groups X can be turned into encoding modules or dually what the encoding modules for a given group G look like. Many of the results in this section are motivated by a desire to provide partial answers or intuition towards answers to these questions.

3.1 Shiftable Functors

The main point of this section is to set up some theory around what we call shiftable functors, whose main application will be in the proofs of Corollary 26 and Corollary 27.

Definition 15. Let G be a finite group. Then a functor $F\colon \mathrm{Mod}_G \to \mathrm{Mod}_G$ is a *shiftable functor* if and only if F is both additive and sends induced modules to induced modules.

The main point to shiftable functors F is that the dimension-shifting short exact sequences

$$\begin{aligned} 0 &\to I_G \otimes_{\mathbb{Z}} A \to \quad \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \quad \to \quad A \quad \to 0 \\ 0 &\to \quad A \quad \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \to \mathrm{Hom}_{\mathbb{Z}}(I_G, A) \to 0 \end{aligned}$$

will remain exact upon applying F (because F is additive, and these short exact sequences are $\mathbb{Z}$-split), and the middle term will remain induced.

Here are our key examples of shiftable functors.

Lemma 16. Let G be a finite group and X a G-module. Then $\mathrm{Hom}_{\mathbb{Z}}(-, X)$ is a (contravariant) shiftable functor.

Proof. We already know that $\mathrm{Hom}_{\mathbb{Z}}(-, X)$ is additive, so the main check is that we send induced modules to induced modules. Well, without loss of generality, let $M \coloneqq \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ be our induced module. Then the tensor–hom adjunction gives

$$\mathrm{Hom}_{\mathbb{Z}}(M, X) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G] \otimes_{\mathbb{Z}} A, X) \simeq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathrm{Hom}_{\mathbb{Z}}(A, X)),$$

which is also a G-module isomorphism. This finishes. ■

Lemma 17. Let G be a finite group and X a G-module. Then $\mathrm{Hom}_{\mathbb{Z}}(X, -)$ is a shiftable functor.

Proof. It is known that $\mathrm{Hom}_{\mathbb{Z}}(X, -)$ is an additive functor, so we just need to check that it sends induced modules to induced modules. Well, pick up some induced module $M \coloneqq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ for some G-module A. Then we see

$$\mathrm{Hom}_{\mathbb{Z}}(X, M) = \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)) \simeq \mathrm{Hom}_{\mathbb{Z}}(X \otimes_{\mathbb{Z}} \mathbb{Z}[G], A),$$

which is induced by noting $X \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ is induced and using Lemma 16. ■

Lemma 18. Let G be a finite group and X a G-module. Then $X \otimes_{\mathbb{Z}} -$ is a shiftable functor.

Proof. Again, $X \otimes_{\mathbb{Z}} -$ is additive, so we just need to check that it sends induced modules to induced modules. Well, suppose $M \coloneqq \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ is an induced module. Then we note the isomorphisms

$$X \otimes_{\mathbb{Z}} M = X \otimes_{\mathbb{Z}} \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} (X \otimes_{\mathbb{Z}} A)$$

are all also isomorphisms of G-modules. Because $\mathbb{Z}[G] \otimes_{\mathbb{Z}} (X \otimes_{\mathbb{Z}} A)$ is induced, we are done. ■

Of course, we can create some crazier examples of shiftable functors by melding them together.

Lemma 19. Let G be a finite group. If F and F' are shiftable functors, then $F \circ F'$ is a shiftable functor.

Proof. This follows directly from the definition. ■

Example 20. The functor

$$A \mapsto \mathrm{Hom}_{\mathbb{Z}}\left(A \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, I_G \otimes_{\mathbb{Z}} A), I_G\right)$$

is a shiftable functor.

3.2 Shifting by Cup Products

A key property of shiftable functors is how we will be able to relate them to each other via cup products. With this in mind, we have the following definition.

Definition 21. Let G be a finite group. Then we define a *shifting pair* (F, F', X, η) to be a pair of shiftable functors F and F' equipped with a natural transformation

$$\eta_\bullet \colon X \otimes_{\mathbb{Z}} F \Rightarrow F'.$$

The following will be our key example.

Example 22. Given G-modules X and X', there is a canonical composition map

$$\begin{array}{ccccc} \eta_\bullet : \mathrm{Hom}_{\mathbb{Z}}(X', X) \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, -) & \Rightarrow & \mathrm{Hom}_{\mathbb{Z}}(X', -) \\ \varphi \otimes \quad f & \mapsto & f \circ \varphi \end{array}$$

so $(\mathrm{Hom}_{\mathbb{Z}}(X, -), \mathrm{Hom}_{\mathbb{Z}}(X', -), \mathrm{Hom}_{\mathbb{Z}}(X', X), \eta_\bullet)$ is a shifting pair.

In particular, cup products assemble into natural transformations.

Lemma 23. Let G be a finite group, and let (F, F', X, η) be a shifting pair. Then, given indices $r, s \in \mathbb{Z}$ and $c \in \widehat{H}^r(G, X)$, the cup-product maps

$$(c \cup -) \colon \widehat{H}^s(G, F-) \Rightarrow \widehat{H}^{r+s}(G, F'-)$$

make a natural transformation of cohomology functors.

Proof. Given a G-module A, we note that our cup-product map is defined by

$$\widehat{H}^s(G, FA) \xrightarrow{c \cup -} \widehat{H}^{r+s}(G, X \otimes_{\mathbb{Z}} FA) \xrightarrow{\eta_A} \widehat{H}^{r+s}(G, F'A).$$

So, to check naturality, we pick up a G-module homomorphism $\varphi \colon A \to B$ and draw the following diagram.

$$\begin{array}{ccccc} \widehat{H}^s(G, FA) & \xrightarrow{c \cup -} & \widehat{H}^{r+s}(G, X \otimes_{\mathbb{Z}} FA) & \xrightarrow{\eta_A} & \widehat{H}^{r+s}(G, F'A) \\ {\scriptstyle f}\downarrow & & {\scriptstyle f}\downarrow & & {\scriptstyle f}\downarrow \\ \widehat{H}^s(G, FB) & \xrightarrow{c \cup -} & \widehat{H}^{r+s}(G, X \otimes_{\mathbb{Z}} FB) & \xrightarrow{\eta_B} & \widehat{H}^{r+s}(G, F'B) \end{array}$$

The left square commutes by functoriality of cup products (see [Neu13], Proposition I.5.3), and the right square commutes by the naturality of η and functoriality of $\widehat{H}^{r+s}(G, -)$. ∎

It will turn out occasionally that we have multiple evaluation maps flying around, so we pick up the following lemma for reassurance.

Lemma 24. Let G be a finite group, and let A, B, C be G-modules equipped with maps

$$\begin{aligned} \varphi_{AB} &\colon A \otimes_{\mathbb{Z}} B \to X \\ \varphi_{XC} &\colon X \otimes_{\mathbb{Z}} C \to Z \\ \varphi_{BC} &\colon B \otimes_{\mathbb{Z}} C \to Y \\ \varphi_{AY} &\colon A \otimes_{\mathbb{Z}} Y \to Z \end{aligned}$$

making the diagram

$$\begin{array}{ccc} A \otimes_{\mathbb{Z}} B \otimes_{\mathbb{Z}} C & \xrightarrow{\varphi_{AB}} & X \otimes_{\mathbb{Z}} C \\ {\scriptstyle \varphi_{BC}}\downarrow & & \downarrow{\scriptstyle \varphi_{XC}} \\ A \otimes_{\mathbb{Z}} Y & \xrightarrow{\varphi_{AY}} & Z \end{array}$$

commute. Then, for any $a \in \widehat{H}^r(G, A)$ and $b \in \widehat{H}^s(G, B)$ and $c \in \widehat{H}^t(G, C)$, we have

$$(a \cup b) \cup c = a \cup (b \cup c) \in \widehat{H}^{r+s+t}(G, Z).$$

Proof. The point is to track $b \in \widehat{H}^s(G, B)$ through the following very large commutative diagram.

$$\begin{array}{ccccc}
\widehat{H}^s(G,B) & \xrightarrow{a\cup -} & \widehat{H}^{r+s}(G, A\otimes_{\mathbb{Z}} B) & \xrightarrow{\varphi_{AB}} & \widehat{H}^{r+s}(G,X) \\
\downarrow{\scriptstyle c\cup -} & (1) & \downarrow{\scriptstyle c\cup -} & (2) & \downarrow{\scriptstyle c\cup -} \\
\widehat{H}^{s+t}(G, B\otimes_{\mathbb{Z}} C) & \xrightarrow{a\cup -} & \widehat{H}^{r+s+t}(G, A\otimes_{\mathbb{Z}} B\otimes_{\mathbb{Z}} C) & \xrightarrow{\varphi_{AB}} & \widehat{H}^{r+s+t}(G, X\otimes_{\mathbb{Z}} C) \\
\downarrow{\scriptstyle \varphi_{BC}} & (3) & \downarrow{\scriptstyle \varphi_{BC}} & (4) & \downarrow{\scriptstyle \varphi_{XC}} \\
\widehat{H}^{s+t}(G,Y) & \xrightarrow{a\cup -} & \widehat{H}^{r+s+t}(G, A\otimes_{\mathbb{Z}} Y) & \xrightarrow{\varphi_{AY}} & \widehat{H}^{r+s+t}(G,Z)
\end{array}$$

Namely, $(a \cup b) \cup c$ corresponds to following the top and then right legs of the diagram, and $a \cup (b \cup c)$ corresponds to following the left and then bottom legs of the diagram.

Thus, it suffices to show that the entire diagram square commutes. Well, (1) commutes by associativity of the cup product, (2) and (3) commute by naturality of the cup product, and (4) commutes by the hypothesized square and functoriality of $\widehat{H}^{r+s+t}(G, -)$. This finishes. ■

Let's start with a key result on shiftable functors, which gives a taste for why our hypotheses are so specially chosen.

Proposition 25. Let G be a finite group, and let (F, F', X, η) be a shifting pair. If we have indices $r, s \in \mathbb{Z}$ and $c \in H^r(G, X)$ such that the cup-product map

$$(c \cup -)\colon \widehat{H}^s(G, F-) \Rightarrow \widehat{H}^{r+s}(G, F'-)$$

is a natural isomorphism, then the cup-product map

$$(c \cup -)\colon \widehat{H}^j(G, F-) \Rightarrow \widehat{H}^{r+j}(G, F'-)$$

is a natural isomorphism for all indices $j \in \mathbb{Z}$.

Proof. This proof is by dimension-shifting on j. Note that it suffices by Lemma 23 to only worry about the component morphisms being isomorphisms.

To shift downwards, we suppose that the cup-product map is always an isomorphism for j, and we show that it is always an isomorphism $j-1$. Namely, fix a G-module A, and we are interested in showing that the cup-product map

$$(c \cup -)\colon \widehat{H}^{j-1}(G, FA) \to \widehat{H}^{r+j-1}(G, F'A)$$

is an isomorphism. To do so, we note the short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \tag{3.2}$$

which splits over $\mathbb{Z}$ and thus gives us the short exact sequences

$$0 \longrightarrow F(I_G \otimes_{\mathbb{Z}} A) \longrightarrow F(\mathbb{Z}[G] \otimes_{\mathbb{Z}} A) \longrightarrow FA \longrightarrow 0$$

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X\otimes_{\mathbb{Z}} F(I_G\otimes_{\mathbb{Z}} A) & \longrightarrow & X\otimes_{\mathbb{Z}} F(\mathbb{Z}[G]\otimes_{\mathbb{Z}} A) & \longrightarrow & X\otimes_{\mathbb{Z}} FA & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \eta_{I_G}} & & \downarrow{\scriptstyle \eta_{\mathbb{Z}[G]}} & & \downarrow{\scriptstyle \eta_A} & & \\
0 & \longrightarrow & F'(I_G\otimes_{\mathbb{Z}} A) & \longrightarrow & F'(\mathbb{Z}[G]\otimes_{\mathbb{Z}} A) & \longrightarrow & F'A & \longrightarrow & 0
\end{array}$$

where the bottom two rows commute by definition of η and thus give a morphism of short exact sequences. These short exact sequences give us boundary morphisms

$$\begin{aligned}
\delta\colon &\quad \widehat{H}^{r+j-1}(G, F'A) &&\to \quad \widehat{H}^{r+j}(G, F'(I_G\otimes_{\mathbb{Z}} A)) \\
\delta_h\colon &\quad \widehat{H}^{j-1}(G, FA) &&\to \quad \widehat{H}^{j}(G, F(I_G\otimes_{\mathbb{Z}} A)) \\
\delta_t\colon &\ \widehat{H}^{r+j-1}(G, X\otimes_{\mathbb{Z}} FA) \to \widehat{H}^{r+j}(G, X\otimes_{\mathbb{Z}} F(I_G\otimes_{\mathbb{Z}} A)).
\end{aligned}$$

Notably, all these δ morphisms because their short exact sequences have induced middle terms: all of F and $X \otimes_{\mathbb{Z}} F$ and F' are shiftable functors.

Now, the key to this dimension-shifting is claiming that the diagram

$$\begin{array}{ccc} \widehat{H}^{j-1}(G, FA) & \xrightarrow{c\cup -} & \widehat{H}^{r+j-1}(G, F'A) \\ \downarrow{\scriptstyle \delta_h} & & \downarrow{\scriptstyle (-1)^r\delta} \\ \widehat{H}^{j}(G, F(I_G \otimes_{\mathbb{Z}} A)) & \xrightarrow{c\cup -} & \widehat{H}^{r+j}(G, F'(I_G \otimes_{\mathbb{Z}} A)) \end{array}$$

commutes. Indeed, this will be enough because the bottom row is an isomorphism by the inductive hypothesis, and the left and morphisms are isomorphisms as discussed above, which makes the top row into an isomorphism. Well, to see that the diagram commutes, we expand the diagram as follows.

$$\begin{array}{ccccc} \widehat{H}^{j-1}(G, FA) & \xrightarrow{c\cup -} & \widehat{H}^{r+j-1}(G, X \otimes_{\mathbb{Z}} FA) & \xrightarrow{\eta_A} & \widehat{H}^{r+j-1}(G, F'A) \\ \downarrow{\scriptstyle \delta_h} & & \downarrow{\scriptstyle (-1)^r\delta_t} & & \downarrow{\scriptstyle (-1)^r\delta} \\ \widehat{H}^{j}(G, F(I_G \otimes_{\mathbb{Z}} A)) & \xrightarrow{c\cup -} & \widehat{H}^{r+j}(G, X \otimes_{\mathbb{Z}} F(I_G \otimes_{\mathbb{Z}} A)) & \xrightarrow{\eta_{I_G}} & \widehat{H}^{r+j}(G, F'(I_G \otimes_{\mathbb{Z}} A)) \end{array}$$

The left square commutes because cup products commute with boundary morphisms; the right square commutes by functoriality of boundary morphisms.

Shifting upwards is similar. Suppose that the cup-product in question is always an isomorphism for j, and we show that it is always an isomorphism for $j+1$. Namely, fix a G-module A, and we are interested in showing that the cup-product map

$$(c \cup -) \colon \widehat{H}^{j+1}(G, FA) \to \widehat{H}^{r+j+1}(G, F'A)$$

is an isomorphism. As before, we use (3.2) to induce the short exact sequences

$$0 \longrightarrow FA \longrightarrow F(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)) \longrightarrow F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \longrightarrow 0$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X \otimes_{\mathbb{Z}} FA & \longrightarrow & X \otimes_{\mathbb{Z}} F(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)) & \longrightarrow & X \otimes_{\mathbb{Z}} F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A)) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \eta_A} & & \downarrow{\scriptstyle \eta_{\mathbb{Z}[G]}} & & \downarrow{\scriptstyle \eta_{I_G}} & & \\ 0 & \longrightarrow & F'A & \longrightarrow & F'(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)) & \longrightarrow & F'(\mathrm{Hom}_{\mathbb{Z}}(I_G, A)) & \longrightarrow & 0 \end{array}$$

where again the bottom rows commute by definition of η. As before, we have the boundary morphisms

$$\begin{aligned} \delta \colon \quad & \widehat{H}^{r+j}(G, F'(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) \quad \to \quad \widehat{H}^{r+j+1}(G, F'A) \\ \delta_h \colon \quad & \widehat{H}^{j}(G, F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) \quad \to \quad \widehat{H}^{j+1}(G, FA) \\ \delta_t \colon \quad & \widehat{H}^{r+j}(G, X \otimes_{\mathbb{Z}} F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) \to \widehat{H}^{r+j+1}(G, X \otimes_{\mathbb{Z}} FA). \end{aligned}$$

We again note that all δ are isomorphisms because the middle terms of our short exact sequences are induced: all of F and $X \otimes_{\mathbb{Z}} F$ and F' are shiftable functors.

Once more, the key to the dimension-shifting will be the claim that the diagram

$$\begin{array}{ccc} \widehat{H}^{j}(G, F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) & \xrightarrow{c\cup -} & \widehat{H}^{r+j}(G, F'(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) \\ \downarrow{\scriptstyle \delta_h} & & \downarrow{\scriptstyle (-1)^r\delta} \\ \widehat{H}^{j+1}(G, FA) & \xrightarrow{c\cup -} & \widehat{H}^{r+j+1}(G, F'A) \end{array}$$

commutes. This will be enough because the top arrow is an isomorphism by the inductive hypothesis, and the left and right arrows are isomorphisms as discussed above, thus making the bottom arrow also an iso-

morphism. Now, to see that the diagram commutes, we expand out our cup products as follows.

$$\begin{array}{ccccc} \widehat{H}^j(G, F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) & \xrightarrow{c\cup -} & \widehat{H}^{r+j}(G, X \otimes_{\mathbb{Z}} F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) & \xrightarrow{\eta_{I_G}} & \widehat{H}^{r+j}(G, F'(\mathrm{Hom}_{\mathbb{Z}}(I_G, A))) \\ \downarrow{\scriptstyle \delta_h} & & \downarrow{\scriptstyle (-1)^r\delta_t} & & \downarrow{\scriptstyle (-1)^r\delta} \\ \widehat{H}^{j+1}(G, FA) & \xrightarrow{c\cup -} & \widehat{H}^{r+j+1}(G, X \otimes_{\mathbb{Z}} FA) & \xrightarrow{\eta_A} & \widehat{H}^{r+j+1}(G, F'A) \end{array}$$

The left square commutes because cup products commute with boundary morphisms, and the right square commutes by functoriality of boundary morphisms. This finishes. ■

Here are some applications.

Corollary 26. Let G be a finite group. There exists $c \in \widehat{H}^1(G, I_G)$ such that, for any G-module X,

$$(c \cup -)\colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{i+1}(G, \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} -))$$

is a natural isomorphism for any $i \in \mathbb{Z}$.

Proof. Here, we are using the shifting pair $(\mathrm{Hom}_{\mathbb{Z}}(X, -), \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} -), I_G, \eta)$, where

$$\eta_A\colon I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A) \to \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} A)$$

is the canonical map sending $z \otimes f$ to $x \mapsto z \otimes f(x)$.

Now, in light of Proposition 25, we merely have to find $c \in \widehat{H}^1(G, I_G)$ and show that we have a natural isomorphism at $i = 0$. Because we already have a natural transformation by Lemma 23, we are only worried about making the component morphisms

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \to \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} A))$$

isomorphisms for all G-modules A. Well, we note that we have the $\mathbb{Z}$-split short exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} A) \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A) \to \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} A) \to 0$$

which will induce a δ morphism between the correct modules. In fact, because $\mathrm{Hom}_{\mathbb{Z}}(X, -)$ is a shiftable functor, the middle term here is induced, so the δ morphism

$$\delta\colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \to \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} A))$$

is an isomorphism.

To finish, we claim that this δ morphism arises as a cup product. We simply show this by hand by tracking through the δ morphism. Given $[f] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$ where $f\colon X \to A$ is a G-module homomorphism, we can pull this back to the 0-chain $\widetilde{f}\colon X \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ defined by

$$\widetilde{f}\colon x \mapsto 1 \otimes f(x).$$

Applying the differential, we get the 1-cocycle $d\widetilde{f} \in B^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}[G] \otimes_{\mathbb{Z}} A))$ defined by

$$\begin{aligned} (d\widetilde{f})(g)(x) &= (g\widetilde{f})(x) - \widetilde{f}(x) \\ &= g \cdot \widetilde{f}\left(g^{-1}x\right) - \widetilde{f}(x) \\ &= g\left(1 \otimes f(g^{-1}x)\right) - (1 \otimes f(x)) \\ &= (g-1) \otimes f(x), \end{aligned}$$

which we know must be a 1-cocycle representing $\delta([f]) \in H^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} A))$.

Thus, we see that we should set $c \in \widehat{H}^1(G, I_G)$ to be represented by $g \mapsto (g-1)$. This will work as long as $g \mapsto (g-1)$ is actually 1-cocycle in $\widehat{H}^1(G, I_G)$. Well, take $X = A = \mathbb{Z}$ and $f = \mathrm{id}_{\mathbb{Z}}$ in the above argument so that $\delta(f)$ is exactly $g \mapsto (x \mapsto (g-1) \otimes x)$, which is $g \mapsto (g-1)$ after applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, I_G) \simeq I_G$. ■

Corollary 27. Let G be a finite group. There exists $c \in \widehat{H}^1(G, I_G)$ such that, for any G-module X,

$$(c \cup -)\colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, -))) \Rightarrow \widehat{H}^{i+1}(G, \mathrm{Hom}_{\mathbb{Z}}(X, -))$$

is a natural isomorphism for any $i \in \mathbb{Z}$.

Proof. Similar to before, we are using the shifting pair $(\mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, -)), \mathrm{Hom}_{\mathbb{Z}}(X, -), I_G, \eta)$, where

$$\eta_A\colon I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \Rightarrow \mathrm{Hom}_{\mathbb{Z}}(X, -)$$

is the canonical map sending $z \otimes f$ to $x \mapsto f(x)(z)$.

Using Proposition 25 and Lemma 23 again, it will suffice to find $c \in \widehat{H}^1(G, I_G)$ such that we have isomorphisms

$$(c \cup -)\colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, A))) \to \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$$

for all G-modules A. This time around we use the $\mathbb{Z}$-split short exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X, A) \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)) \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \to 0$$

which will induce a boundary morphism

$$\delta\colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, A))) \to \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)).$$

In fact, δ is an isomorphism because our middle term $\mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A))$ is induced.

We now show that δ is a cup product by hand. Pick up some $[f] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)))$ where $f\colon X \to \mathrm{Hom}_{\mathbb{Z}}(I_G, A)$ is a G-module homomorphism. This pulls back to the 0-cochain

$$\widetilde{f}\colon x \mapsto \big(z \mapsto f(x)(z - \varepsilon(z))\big).$$

Applying the differential, we compute

$$\begin{aligned}
(d\widetilde{f})(g)(x)(z) &= (g\widetilde{f} - \widetilde{f})(x)(z) \\
&= (g\widetilde{f})(x)(z) - \widetilde{f}(x)(z) \\
&= \left(g \cdot \widetilde{f}\left(g^{-1}x\right)\right)(z) - \widetilde{f}(x)(z) \\
&= g \cdot \widetilde{f}\left(g^{-1}x\right)\left(g^{-1}z\right) - \widetilde{f}(x)(z) \\
&= g \cdot f\left(g^{-1}x\right)\left(g^{-1}z - \varepsilon(z)\right) - f(x)(z - \varepsilon(z)) \\
&= g \cdot \left(g^{-1}f\left(x\right)\right)\left(g^{-1}z - \varepsilon(z)\right) - f(x)(z - \varepsilon(z)) \\
&= f(x)\left(z - g\varepsilon(z)\right) - f(x)(z - \varepsilon(z)) \\
&= \varepsilon(z)f(x)\left(1 - g\right).
\end{aligned}$$

Thus, this pulls back to the 1-cocycle $g \mapsto (x \mapsto f(x)(1-g))$ in $\widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$.

In particular, we see that we should take c represented by $g \mapsto (1-g)$, which will work as soon as we know that $g \mapsto (1-g)$ is a 1-cocycle. Well, this is the negation of the 1-cocycle $g \mapsto (g-1)$ found in Corollary 26. We close by remarking that we can actually take c represented by $g \mapsto (g-1)$ because negating c does not change the fact that the cup product gives an isomorphism. ∎

Remark 28. Essentially the same proofs for Corollary 26 and Corollary 27 will work when $\mathrm{Hom}_{\mathbb{Z}}(X, -)$ is replaced by $X \otimes_{\mathbb{Z}} -$, or any composite of these. There isn't an analogue for arbitrary shiftable functors because, for example, there is no way obvious way to construct η in general. Regardless, we will not need to work in these levels of generality.

The point of Corollary 26 and Corollary 27 is that have a somewhat general version of dimension-shifting granted by cup products. In fact, we see that we can use the same $c \in \widehat{H}^1(G, I_G)$ represented by $g \mapsto (g-1)$ for both shifting isomorphisms.

3.3 Shifting Natural Transformations

Observe that a natural transformation $F \Rightarrow F'$ of shiftable functors will induce natural transformations in cohomology

$$\widehat{H}^i(G, F-) \Rightarrow \widehat{H}^i(G, F'-)$$

It will turn out that, when $F = \mathrm{Hom}_{\mathbb{Z}}(X, -)$ and $F' = \mathrm{Hom}_{\mathbb{Z}}(X', -)$, we will be able to force all natural transformations in cohomology will come from natural transformations $F \Rightarrow F'$.

To begin, we show this result for $i = 0$.

Lemma 29. Let G be a finite group, and let X and X' be G-modules. Suppose that, for given index $r \in \mathbb{Z}$, there is a natural transformation

$$\Phi_\bullet \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(X', -)).$$

Then there exists $[x] \in \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(X', X))$ such that $\Phi_\bullet = ([x] \cup -)$, where the cup product is induced by the shifting pair of Example 22.

Proof. This is essentially the Yoneda lemma. As such, set $[x] := \Phi_X([\mathrm{id}_X])$. The point is to fix some G-module A and $[\overline{f}] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$ in order to track through the commutativity of the following diagram.

$$\begin{array}{ccc} \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) & \xrightarrow{\Phi_X} & \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(X', X)) \\ \Big\downarrow{\scriptstyle \overline{f}} & & \Big\downarrow{\scriptstyle \overline{f}} \\ \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) & \xrightarrow{\Phi_A} & \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(X', A)) \end{array} \tag{3.3}$$

Because we will need to deal with the cup products with negative indices, we will use the standard resolution of [AW10]. For example, we interpret $f \in [\overline{f}] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$ as a constant function $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], \mathrm{Hom}_{\mathbb{Z}}(X, A))$ outputting $\overline{f} \in \mathrm{Hom}_{\mathbb{Z}[G]}(X, A)$, which means that $f(z)$ is the same G-module homomorphism for each $z \in \mathbb{Z}[G]$.

As such, we can track the left arrow of (3.3) as

$$\begin{array}{rcl} \overline{f} \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) & \to & \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \\ [z \mapsto \mathrm{id}_X] & \mapsto & [z \mapsto f(z) \circ \mathrm{id}_X] = [\overline{f}]. \end{array}$$

So, along the bottom of (3.3), we are evaluating $\Phi_A([\overline{f}])$.

Along the top of (3.3), we immediately send $[z \mapsto \mathrm{id}_X]$ to $\Phi_X([z \mapsto \mathrm{id}_X]) = [x]$, so to finish the proof, we need to show that

$$\overline{f}([x]) \stackrel{?}{=} [x] \cup [\overline{f}],$$

which will be enough by the commutativity of (3.3). We have two similar cases to appropriately deal with the cup product.

- Suppose that $r \geq 0$ so that we can interpret x as an element of $\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathbb{Z}[G^{r+1}], X\right)$, using the standard resolution. As such, we compute

  $$(x \cup f)(g_0, \ldots, g_p) = x(g_0, \ldots, g_p) \otimes f(g_r),$$

  where our output is in $\mathrm{Hom}_{\mathbb{Z}}(X', X) \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A)$. Applying evaluation, the cup product is outputting

  $$(g_0, \ldots, g_r) \mapsto \overline{f} \circ x(g_0, \ldots, g_r)$$

  as our element of $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{r+1}], \mathrm{Hom}_{\mathbb{Z}}(X', A))$. Indeed, this morphism represents $\overline{f}([x])$.

- Analogously, suppose that $r < 0$ so that we interpret x as an element of $\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^r, \mathbb{Z}), X\right)$. To decrease headaches, we let $g^* \colon \mathbb{Z}[G] \to \mathbb{Z}$ denote the G-module homomorphism sending $g \mapsto 1$ and other group elements to 0. Then r-tuples $(g_1^*, \dots, g_r^*)$ form a $\mathbb{Z}$-basis of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^r, \mathbb{Z})$, so it's enough to specify
$$(x \cup f)(g_1^*, \dots, g_r^*) = x(g_1^*, \dots, g_r^*) \otimes f(g_r),$$
where the output is in $\mathrm{Hom}_{\mathbb{Z}}(X', X) \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A)$. Applying evaluation, the cup product is outputting
$$(g_1^*, \dots, g_r^*) \mapsto \overline{f} \circ x(g_1^*, \dots, g_r^*)$$
as an element of $\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^r, \mathbb{Z}), \mathrm{Hom}_{\mathbb{Z}}(X', A)\right)$. Indeed, this represents $\overline{f}([x])$.

The above cases finish tracking through (3.3) and hence finish the proof. ∎

The case of $r = 0$ will be particularly interesting to us, so we note that we have the following more concrete description.

Lemma 30. Let G be a finite group, and let X and X' be G-modules. Then, given a G-module morphism $\varphi \colon X' \to X$, the maps $(- \circ \varphi)$ and $([\varphi] \cup -)$ on
$$\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X', -))$$
assemble into the same natural transformation for any $i \in \mathbb{Z}$.

Proof. This follows from unpacking the definitions.

We already know that $([\varphi] \cup -)$ is a natural transformation by Lemma 23, so it suffices to show that the two maps agree on components. (Namely, naturality of $(- \circ \varphi)$ will immediately follow.) To see this, we fix a G-module A to evaluate the morphism
$$\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \to \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X', A)),$$
for which we use the standard resolution of [AW10]. For this, we represent $[\varphi]$ by the morphism $\widetilde{\varphi} \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G], \mathrm{Hom}_{\mathbb{Z}}(X, A))$ which constantly outputs φ.

Now, pick up $[x] \in \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$. We have two cases.

- If $i \geq 0$, we can interpret x as an element of $\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathbb{Z}[G]^{i+1}, \mathrm{Hom}_{\mathbb{Z}}(X, A)\right)$. Then our cup product is
$$(\widetilde{\varphi} \cup x)(g_0, \dots, g_i) = \widetilde{\varphi}(x_0) \otimes x(g_0, \dots, g_i),$$
which evaluates to
$$(g_0, \dots, g_i) \mapsto x(g_0, \dots, g_i) \circ \varphi,$$
which represents the desired class $(- \circ \varphi)([x])$.
- If $i < 0$, we can interpret x as an element of $\mathrm{Hom}_{\mathbb{Z}[G]}\left(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^i, \mathbb{Z}), \mathrm{Hom}_{\mathbb{Z}}(X, A)\right)$. Our cup product is
$$(\widetilde{\varphi} \cup x)(g_1^*, \dots, g_i^*) = \widetilde{\varphi}(g_1) \otimes x(g_1^*, \dots, g_i^*),$$
which evaluates to
$$(g_1^*, \dots, g_i^*) \mapsto x(g_1^*, \dots, g_i^*) \circ \varphi,$$
which represents the desired class $(- \circ \varphi)([x])$.

The above cases finish the proof. ∎

We now get the main result by dimension-shifting.

Proposition 31. Let G be a finite group, and let X and X' be G-modules. Then, given indices $r, s \in \mathbb{Z}$, any natural transformation

$$\Phi_\bullet^{(s)} \colon \widehat{H}^s(G, \mathrm{Hom}_\mathbb{Z}(X, -)) \Rightarrow \widehat{H}^{r+s}(G, \mathrm{Hom}_\mathbb{Z}(X', -)),$$

is $\Phi_\bullet^{(s)} = (x \cup -)$ for some $x \in \widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X', X))$.

Proof. This argument is by dimension-shifting the s upwards and downwards. Namely, we show the conclusion of the statement by induction on s; for $s = 0$, this is Lemma 29. We will show how to induct upwards to $s \geq 0$ in detail, and inducting downwards is similar. For brevity, we set $F := \mathrm{Hom}_\mathbb{Z}(X, -)$ and $F' := \mathrm{Hom}_\mathbb{Z}(X', -)$.

To induct upwards, suppose the statement is true for $s = i$, and we show $s = i + 1$, so fix a natural transformation

$$\Phi_\bullet^{(i+1)} \colon \widehat{H}^{i+1}(G, F-) \Rightarrow \widehat{H}^{p+i+1}(G, F'-),$$

which we would like to know arises as $(x \cup -)$ for some $x \in \widehat{H}^p(G, \mathrm{Hom}_\mathbb{Z}(X', X))$. The main idea is to use $\Phi_\bullet^{(i+1)}$ in order to construct $\Phi_\bullet^{(i)}$. Well, using Corollary 26, we have some $c \in \widehat{H}^1(G, I_G)$ given by $g \mapsto (g - 1)$ yielding the following isomorphisms for any G-module A.

$$\begin{aligned} (c \cup -)_d &\colon \widehat{H}^i(G, FA) \to \widehat{H}^{i+1}(G, F(I_G \otimes_\mathbb{Z} A)) \\ (c \cup -)'_d &\colon \widehat{H}^{r+i}(G, F'A) \to \widehat{H}^{r+i+1}(G, F'(I_G \otimes_\mathbb{Z} A)) \end{aligned}$$

As such, we have the diagram

$$\begin{array}{ccc} \widehat{H}^i(G, FA) & \xrightarrow{(c\cup-)_d} & \widehat{H}^{i+1}(G, F(I_G \otimes_\mathbb{Z} A)) \\ \vdots & & \downarrow \Phi^{(i+1)}_{I_G \otimes_\mathbb{Z} A} \\ \widehat{H}^{r+i}(G, F'A) & \xrightarrow{(c\cup-)'_d} & \widehat{H}^{r+i+1}(G, F'(I_G \otimes_\mathbb{Z} A)) \end{array}$$

where the horizontal arrows are isomorphisms. Thus, we induce a morphism

$$\Phi_A^{(i)} := ((c \cup -)'_d)^{-1} \circ \Phi^{(i+1)}_{I_G \otimes_\mathbb{Z} A} \circ (c \cup -)_d.$$

Note that $\Phi_\bullet^{(i)}$ is the composition of natural transformations (the cup product is a natural transformation by construction) and therefore is a natural transformation.

Thus, the inductive hypothesis now tells us that $\Phi_\bullet^{(i)} = (x \cup -)$ for some $x \in \widehat{H}^p(G, \mathrm{Hom}_\mathbb{Z}(X', X))$. We now need to turn this around on $\Phi_\bullet^{(i+1)}$, which essentially means we need to shift back in the other direction. As such, we use Corollary 27 to give the following isomorphisms for any G-module A.

$$\begin{aligned} (c \cup -)_u &\colon \widehat{H}^i(G, F(\mathrm{Hom}_\mathbb{Z}(I_G, A))) \to \widehat{H}^{i+1}(G, FA) \\ (c \cup -)'_u &\colon \widehat{H}^{r+i}(G, F(\mathrm{Hom}_\mathbb{Z}(I_G, A))) \to \widehat{H}^{r+i+1}(G, FA) \end{aligned}$$

Now, to deal with $\Phi_\bullet^{(i+1)}$, we claim that associativity and commutativity of cup products implies $\big((-1)^i x \cup -\big)$ can be used to make the right arrow in the diagram

$$\begin{array}{ccc} \widehat{H}^i(G, F(\mathrm{Hom}_\mathbb{Z}(I_G, A))) & \xrightarrow{(c\cup-)_u} & \widehat{H}^{i+1}(G, FA) \\ \downarrow{\scriptstyle x\cup-} & & \vdots \\ \widehat{H}^{r+i}(G, F'(\mathrm{Hom}_\mathbb{Z}(I_G, A))) & \xrightarrow{(c\cup-)'_u} & \widehat{H}^{r+i+1}(G, F'A) \end{array} \tag{3.4}$$

commute. Indeed, applying Lemma 24 to the square

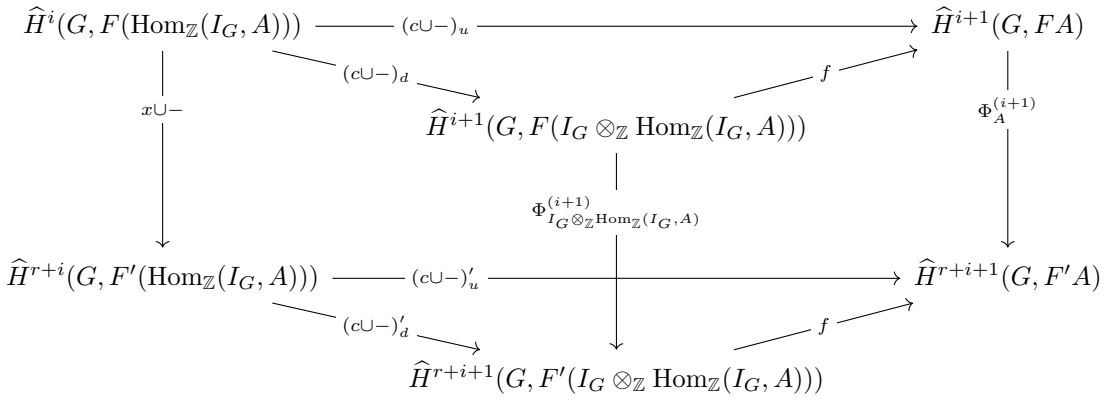
$$\begin{array}{ccc} I_G \otimes_\mathbb{Z} \mathrm{Hom}_\mathbb{Z}(X, \mathrm{Hom}_\mathbb{Z}(I_G, A)) \otimes_\mathbb{Z} \mathrm{Hom}_\mathbb{Z}(X', X) & \longrightarrow & \mathrm{Hom}_\mathbb{Z}(X, A) \otimes_\mathbb{Z} \mathrm{Hom}_\mathbb{Z}(X', X) \\ \downarrow & & \downarrow \\ I_G \otimes_\mathbb{Z} \mathrm{Hom}_\mathbb{Z}(X', \mathrm{Hom}_\mathbb{Z}(I_G, A)) & \longrightarrow & \mathrm{Hom}_\mathbb{Z}(X', A) \end{array}$$

shows that any $a \in \widehat{H}^i(G, F(\mathrm{Hom}_{\mathbb{Z}}(I_G, A)))$ has

$$c \cup (x \cup a) = (-1)^{ir} c \cup (a \cup x) = (-1)^{ir}(c \cup a) \cup x = (-1)^{ir+i(r+1)} x \cup (c \cup a) = (-1)^i x \cup (c \cup a),$$

which is what we wanted.

Now, this right arrow of (3.4) is unique because the horizontal arrows are isomorphisms, so we will be done if we can show that we can place $\Phi_A^{(i+1)}$ in the right arrow to also make the diagram commute as well. For this, we draw the following very large diagram.

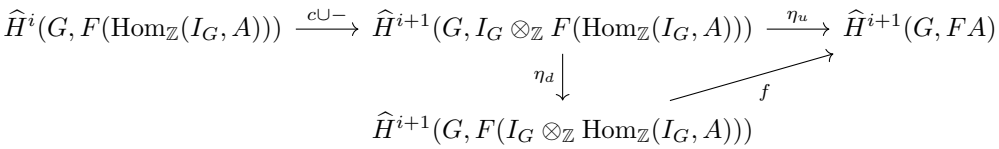


Here, the f maps are induced by the evaluation map

$$f \colon I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, A) \to A.$$

We want the outer rectangle to commute, for which it suffices to show that each parallelogram and the small top and bottom triangles to commute.

- The left parallelogram commutes by definition of $\Phi_A^{(i)}$.
- The right parallelogram commutes by naturality of $\Phi_\bullet^{(i+1)}$.
- Showing that the bottom triangle commutes will be analogous to showing that the top triangle commutes, so we will only show the top. Unwinding Corollary 26 and Corollary 27, we see that this triangle is actually induced by the following diagram.



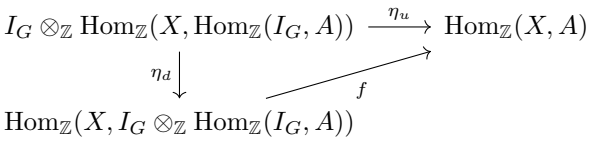
Here, $\eta_u \colon I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \to \mathrm{Hom}_{\mathbb{Z}}(X, A)$ behaves as

$$\eta_u \colon z \otimes f \mapsto \big(x \mapsto f(x)(z)\big),$$

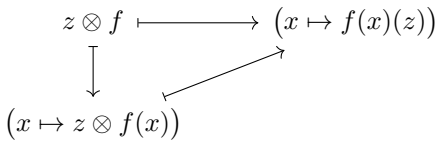
and $\eta_d \colon I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \to \mathrm{Hom}_{\mathbb{Z}}(X, I_G \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(I_G, A))$ behaves as

$$\eta_d \colon z \otimes f \mapsto \big(x \mapsto z \otimes f(x)\big).$$

Now, to check our commutativity, it suffices to show that the triangle



commutes. Well, we can simply track through the diagram as follows.



The above commutativity checks finish the induction upwards.

We will not give detail for the induction downwards from $i-1$ to i, except to say that we reverse the applications of Corollary 26 and Corollary 27. The rest of the approach essentially goes through verbatim, constructing $\Phi_\bullet^{(i)}$ from a given $\Phi_\bullet^{(i-1)}$, applying the inducting hypothesis to $\Phi_\bullet^{(i)}$, and then finishing by shifting back to $\Phi_\bullet^{(i-1)}$. ■

Remark 32. Essentially the same proof can show that, for any pair of shiftable functors $F, F' \colon \mathrm{Mod}_G \to \mathrm{Mod}_G$, a natural transformation (respectively, isomorphism)

$$\Phi_\bullet^{(i)} \colon \widehat{H}^i(G, F-) \Rightarrow \widehat{H}^i(G, F'-),$$

at $i = r$ induces natural transformations (respectively, isomorphisms) at all $i \in \mathbb{Z}$. Instead of using Corollary 26 and Corollary 27, we must instead dimension-shifting using the usual short exact sequences.

Corollary 33. Let G be a finite group, and let X and X' be G-modules. Then, given indices $s \in \mathbb{Z}$, any natural transformation

$$\Phi_\bullet^{(s)} \colon \widehat{H}^q(G, \mathrm{Hom}_\mathbb{Z}(X, -)) \Rightarrow \widehat{H}^s(G, \mathrm{Hom}_\mathbb{Z}(X', -)),$$

is $\Phi_\bullet^{(s)} = (- \circ \varphi)$ for some G-module morphism $\varphi \colon X' \to X$.

Proof. Proposition 31 tells us that the natural transformation takes the form $([\varphi] \cup -)$ for some G-module morphism $\varphi \colon X' \to X$. Then $([\varphi] \cup -)$ is simply $(- \circ \varphi)$ by Lemma 30. ■

3.4 Cohomological Equivalence

It might be the case that "many" different shiftable functors give the same cohomology groups. Because we are mostly interested in the case of $\mathrm{Hom}_\mathbb{Z}(X, -)$, we now have the tools to talk fairly concretely about what this means. We have the following definition.

Definition 34. Let G be a finite group. We say that two G-modules X, X' are *cohomologically equivalent* if and only if there exist morphisms $[\varphi] \in \widehat{H}^0(G, \mathrm{Hom}_\mathbb{Z}(X', X))$ and $[\varphi'] \in \widehat{H}^0(G, \mathrm{Hom}_\mathbb{Z}(X, X'))$ such that

$$[\varphi \circ \varphi'] = [\mathrm{id}_X] \in \widehat{H}^0(G, \mathrm{Hom}_\mathbb{Z}(X, X)) \qquad \text{and} \qquad [\varphi' \circ \varphi] = [\mathrm{id}_{X'}] \in \widehat{H}^0(G, \mathrm{Hom}_\mathbb{Z}(X', X')).$$

Example 35. All induced modules X are cohomologically equivalent to 0. To see this, we set $\varphi \colon 0 \to X$ and $\varphi' \colon X \to 0$ equal to the zero maps (which are our only options). Then note that $\mathrm{Hom}_\mathbb{Z}(X, X)$ is induced by Lemma 17 and $\mathrm{Hom}_\mathbb{Z}(0, 0) = 0$, so

$$\widehat{H}^0(G, \mathrm{Hom}_\mathbb{Z}(X, X)) = \widehat{H}^0(G, \mathrm{Hom}_\mathbb{Z}(X', X')) = 0,$$

making the checks on φ and φ' both trivial.

More concretely, X and X' are cohomologically equivalent if and only if we have two G-module morphisms $\varphi\colon X' \to X$ and $\varphi'\colon X \to X'$ and two $\mathbb{Z}$-module morphisms $f\colon X \to X$ and $f'\colon X' \to X'$ such that

$$\varphi \circ \varphi' = \mathrm{id}_X + N_G f \qquad \text{and} \qquad \varphi' \circ \varphi = \mathrm{id}_{X'} + N_G f'.$$

As a quick sanity check that this is a reasonable notion of equivalence of modules, we have the following.

Lemma 36. Let G be a finite group. If the G-modules X and X' are equivalent and Y and Y' are equivalent, then $X \oplus Y$ is equivalent to $X' \oplus Y'$.

Proof. We are promised the morphisms

- $\varphi\colon X' \to X$ and $\varphi'\colon X \to X'$ (as morphisms of G-modules),
- $f\colon X \to X$ and $f'\colon X' \to X'$ (as morphisms of $\mathbb{Z}$-modules),
- $\psi\colon Y' \to Y$ and $\psi'\colon Y \to Y'$ (as morphisms of G-modules),
- $g\colon Y \to Y$ and $g'\colon Y' \to Y'$ (as morphisms of $\mathbb{Z}$-modules),

which are required to satisfy

$$\begin{aligned} \varphi \circ \varphi' &= \mathrm{id}_X + N_G f \qquad \text{and} \qquad \varphi' \circ \varphi = \mathrm{id}_{X'} + N_G f', \\ \psi \circ \psi' &= \mathrm{id}_Y + N_G g \qquad \text{and} \qquad \psi' \circ \psi = \mathrm{id}_{Y'} + N_G g'. \end{aligned}$$

Summing everywhere, we get the G-module homomorphisms $\varphi \oplus \psi\colon X \oplus Y \to X' \oplus Y'$ and $\varphi' \oplus \psi'\colon X' \oplus Y' \to X \oplus Y$ satisfying

$$\begin{aligned} (\varphi \oplus \psi) \circ (\varphi' \oplus \psi') &= (\varphi \circ \varphi') \oplus (\psi \circ \psi') \\ &= (\mathrm{id}_X + N_G f) \oplus (\mathrm{id}_Y + N_G g) \\ &= \mathrm{id}_X \oplus \mathrm{id}_Y + N_G(f \oplus g). \end{aligned}$$

The other check is analogous, switching primed and unprimed variables. ∎

We now show that this notion of equivalence correctly translates to shiftable functors.

Proposition 37. Let G be a finite group, and let X and X' be G-modules. Then X and X' are cohomologically equivalent if and only if there is a natural isomorphism

$$\Phi_\bullet\colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', -)).$$

Proof. In the forward direction, suppose X and X' are cohomologically equivalent so that we have $[\varphi] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', X))$ and $[\varphi'] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X'))$ such that

$$[\varphi] \cup [\varphi'] = [\varphi \circ \varphi'] = [\mathrm{id}_X] \qquad \text{and} \qquad [\varphi'] \cup [\varphi] = [\varphi' \circ \varphi] = [\mathrm{id}_{X'}],$$

where we are using the canonical evaluation maps for the cup products. Now, we note that, for any G-module A, we have inverse morphisms

$$\begin{array}{ccc} \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) & \simeq & \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \\ [f] & \mapsto & [f \circ \varphi] \\ [f' \circ \varphi'] & \leftarrow\!\shortmid & [f']. \end{array} \tag{3.5}$$

Indeed, these are mutually inverse because

$$[f \circ \varphi \circ \varphi'] = [f] \cup [\varphi \circ \varphi'] = [f] \circ [\mathrm{id}_X] = [f]$$

and similar on the other side. To finish, we note that the isomorphisms (3.5) assemble into a natural isomorphism by Lemma 23 and Lemma 30.

We now show the backwards direction. Suppose we have a natural isomorphism $\Phi_\bullet$. Then applying Lemma 29 in both directions, we get $[\varphi] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', X))$ and $[\varphi'] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X'))$ such that the morphisms

$$\begin{array}{rccc} \Phi_\bullet \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) & \simeq & \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \\ [f] & \mapsto & [f \circ \varphi] \\ [f' \circ \varphi'] & \leftarrow\!\shortmid & [f'] \end{array}$$

are mutually inverse. In particular, we see that

$$[\mathrm{id}_X] = [\mathrm{id}_X \circ \varphi \circ \varphi'] = [\varphi \circ \varphi'],$$

so $[\varphi \circ \varphi'] = [\mathrm{id}_X]$. Swapping primed and unprimed variables, we see $[\varphi' \circ \varphi] = [\mathrm{id}_{X'}]$ as well. ■

Remark 38. The above result makes it fairly clear that cohomological equivalence actually makes an equivalence relation. In particular, we can invert and compose natural isomorphisms, which gives symmetry and transitivity of cohomological equivalence respectively.

One use of this machinery is that we have pretty good tools to tell what is cohomologically equivalent to 0.

Corollary 39. Let G be a finite group, and let X be a G-module. Then X is cohomologically equivalent to 0 if and only if $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) = 0$.

Proof. On one hand, if X is cohomologically equivalent to 0, then Proposition 37 promises a natural isomorphism

$$\Phi_\bullet \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(0, -)) = 0,$$

so it follows $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) = 0$ by plugging in X.

On the other hand, if $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) = 0$, then the G-module homomorphism $\mathrm{id}_X \colon X \to X$ must be equivalent to 0 in this group. So let $\varphi \colon 0 \to X$ and $\varphi' \colon X \to 0$ be the canonical zero morphisms so that

$$[\varphi \circ \varphi'] = [0] = [\mathrm{id}_X] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X))$$

and

$$[\varphi' \circ \varphi] = [0] = [\mathrm{id}_0] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(0, 0)),$$

which finishes. ■

Example 40. It is not in general true that two G-modules X and X' are cohomologically equivalent if and only if $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) \cong \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', X'))$. Indeed, let $G = \langle \sigma \rangle \cong \mathbb{Z}/2\mathbb{Z}$ act on $X = \mathbb{Z}$ trivially and on $X' = \mathbb{Z}i$ by $\sigma \colon i \mapsto -i$. Then

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z} \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}i, \mathbb{Z}i)$$

as G-modules (!), but these modules are not cohomologically equivalent because

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})) \cong \mathbb{Z}/2\mathbb{Z} \ncong 0 \cong \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}i)).$$

Namely, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}i) = 0$ as G-modules.

Corollary 41. Let G be a finite group, and let A and B be G-modules. Then, if $A \oplus B$ is cohomologically equivalent to 0, then both A and B are cohomologically equivalent to 0.

Proof. This is not too hard to see directly, but it falls immediately out of using Corollary 39 and writing

$$\begin{aligned} 0 &= \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A \oplus B, A \oplus B)) \\ &\simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A)) \oplus \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, B)) \oplus \\ &\quad \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, A)) \oplus \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, B)), \end{aligned}$$

from which $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A)) = \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, B)) = 0$ is forced. ∎

Example 42. By Example 35, free $\mathbb{Z}[G]$-modules $\mathbb{Z}[G]^S \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}^S$ for sets S are cohomologically equivalent to 0. It follows that all projective $\mathbb{Z}[G]$-modules are cohomologically equivalent to 0 from Corollary 41.

Here is a quick partial converse to Example 42.

Proposition 43. Let G be a finite group. If X is $\mathbb{Z}$-projective and cohomologically equivalent to 0, then X is $\mathbb{Z}[G]$-projective.

Proof. It suffices to show that $\mathrm{Hom}_{\mathbb{Z}[G]}(X, -)$ is exact. Well, given a short exact sequence

$$0 \to A \to B \to C \to 0$$

of G-modules, the $\mathbb{Z}$-projectivity of X implies that

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X, A) \to \mathrm{Hom}_{\mathbb{Z}}(X, B) \to \mathrm{Hom}_{\mathbb{Z}}(X, C) \to 0$$

is also exact. Taking cohomology, we have the exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(X, A) \to \mathrm{Hom}_{\mathbb{Z}[G]}(X, B) \to \mathrm{Hom}_{\mathbb{Z}[G]}(X, C) \to H^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)),$$

and $H^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) = 0$ by Proposition 37. So indeed, $\mathrm{Hom}_{\mathbb{Z}[G]}(X, -)$ is exact. ∎

Remark 44. Overall, it seems like an interesting question to pin down exactly which G-modules are cohomologically equivalent to 0. It is possible to show that all such X must be acyclic, but it seems currently out of reach to show that being acyclic is also sufficient.

Anyway, the alternate definition for cohomological equivalence from Proposition 37 also provides us with a way to multiply.

Corollary 45. Let G be a finite group. If X and X' are cohomologically equivalent and Y and Y' are cohomologically equivalent, then $X \otimes_{\mathbb{Z}} X'$ is cohomologically equivalent to $Y \otimes_{\mathbb{Z}} Y'$.

Proof. We are granted natural isomorphisms as follows.

$$\begin{aligned} \Phi_\bullet &: \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', -)) \\ \Psi_\bullet &: \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(Y, -)) \Rightarrow \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(Y', -)) \end{aligned}$$

Now, repeatedly using the hom–tensor adjunction, we can chain together natural isomorphisms

$$\begin{aligned}
\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X \otimes_{\mathbb{Z}} Y, -)) &\simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathrm{Hom}_{\mathbb{Z}}(Y, -))) \\
&\overset{\Phi \mathrm{Hom}(Y,-)}{\simeq} \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', \mathrm{Hom}_{\mathbb{Z}}(Y, -))) \\
&\simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X' \otimes_{\mathbb{Z}} Y, -)) \\
&\simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(Y \otimes_{\mathbb{Z}} X', -)) \\
&\simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(Y, \mathrm{Hom}_{\mathbb{Z}}(X', -))) \\
&\overset{\Psi \mathrm{Hom}_{\mathbb{Z}}(X',-)}{\simeq} \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(Y', \mathrm{Hom}_{\mathbb{Z}}(X', -))) \\
&\simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(Y' \otimes_{\mathbb{Z}} X', -)) \\
&\simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X' \otimes_{\mathbb{Z}} Y', -)),
\end{aligned}$$

which is what we wanted. ■

One might hope that we can get more information by using indices away from 0, but in fact we cannot.

Proposition 46. Let G be a finite group, and let X and X' be G-modules. Then the following are equivalent.

(a) X and X' are cohomologically equivalent.

(b) For some $r \in \mathbb{Z}$, there is a natural isomorphism

$$\Phi_\bullet^{(r)} \colon \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(X', -)).$$

(c) There is a G-module homomorphism $\varphi \colon X' \to X$ such that the induced maps

$$(- \circ \varphi) \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X', -))$$

are natural isomorphisms for all $i \in \mathbb{Z}$.

Proof. Note that (a) implies (b) by taking $r = 0$ and applying Proposition 37. Also, (c) implies (a) by taking $i = 0$ and again applying Proposition 37. Lastly, to show (b) implies (c), we note that Proposition 31 promises us $\varphi \colon X' \to X$ such that

$$\Phi_\bullet^{(r)} = (- \circ \varphi).$$

We would like to use Proposition 25. Let our shifting pair be $(\mathrm{Hom}_{\mathbb{Z}}(X, -), \mathrm{Hom}_{\mathbb{Z}}(X', -), \mathrm{Hom}_{\mathbb{Z}}(X', X), \eta)$, where $\eta_\bullet$ is the canonical pre-composition map

$$\eta_\bullet \colon \mathrm{Hom}_{\mathbb{Z}}(X', X) \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, -) \to \mathrm{Hom}_{\mathbb{Z}}(X', -).$$

Then we take $r = r$ and $s = 0$ and $c = [\varphi]$ as above so that the cup-product natural transformation

$$([\varphi] \cup -) \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X', -))$$

is simply induced by $(- \circ \varphi)$ for any $i \in \mathbb{Z}$ by Lemma 30. So we are given that this is a natural isomorphism at $i = r$, so Proposition 25 gives us this isomorphism at all $i \in \mathbb{Z}$, which proves (c). ■

3.5 Encoding Modules

Lastly, we arrive at the application we care about: encoding cohomology. Cohomological equivalence is exactly what we need to talk about uniqueness.

Proposition 47. Let G be a finite group, and let $r, s \in \mathbb{Z}$ be indices. Then, if nonempty, the set of G-module X with a natural isomorphism

$$\Phi_\bullet \colon \widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X, -)) \Rightarrow \widehat{H}^{r+s}(G, -)$$

make up exactly one cohomological equivalence class.

Proof. Fix some G-module X with such a natural isomorphism

$$\Psi_\bullet \colon \widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X, -)) \Rightarrow \widehat{H}^{r+s}(G, -).$$

We would like to show that a G-module X' has a natural isomorphism $\Phi_\bullet$ between the analogous functors if and only if X and X' are cohomologically equivalent.

If X and X' are cohomologically equivalent, then we can compose the promised natural isomorphism of Proposition 46 (c) with $\Psi_\bullet$, giving a natural isomorphism

$$\widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X', -)) \Rightarrow \widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X, -)) \overset{\Psi_\bullet}{\Rightarrow} \widehat{H}^{r+s}(G, -).$$

In the other direction, if we have a natural isomorphism

$$\Phi_\bullet \colon \widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X', -)) \Rightarrow \widehat{H}^{r+s}(G, -),$$

then we can compose with $\Psi_\bullet^{-1}$ to build a natural isomorphism

$$\widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X', -)) \overset{\Phi_\bullet}{\Rightarrow} \widehat{H}^{r+s}(G, -) \overset{\Psi_\bullet^{-1}}{\Rightarrow} \widehat{H}^r(G, \mathrm{Hom}_\mathbb{Z}(X, -)),$$

from which it follows that X and X' are cohomologically equivalent by Proposition 37 (b). ∎

Example 48. Take $s \geq 0$. Dimension-shifting iteratively with the short exact sequence

$$0 \to I_G \otimes_\mathbb{Z} A \to \mathbb{Z}[G] \otimes_\mathbb{Z} A \to A \to 0$$

shows that

$$\widehat{H}^{r+s}(G, A) \simeq \widehat{H}^r\left(G, \mathrm{Hom}_\mathbb{Z}(I_G^{\otimes s}, A)\right),$$

and in fact these isomorphisms are natural by the functoriality of boundary morphisms. So the equivalence class of Proposition 47 is represented by $I_G^{\otimes s}$.

Remark 49. We will show in Example 80 that all of these equivalence classes are nonempty.

Example 50. Not all r-encoding modules are $\mathbb{Z}$-torsion-free. For example, if M is an r-encoding module, and A is induced, then $M \oplus A$ is cohomologically equivalent to M, so $M \oplus A$ is an r-encoding module. However, not all induced modules A are $\mathbb{Z}$-torsion-free.

In fact, akin to the classification of natural transformations from Proposition 31, we can show that these encoding maps must be cup products.

Corollary 51. Let G be a finite group, and let $r \in \mathbb{Z}$ be an index. Suppose we have a G-module X and index $i \in \mathbb{Z}$ with a natural transformation

$$\Phi_\bullet \colon \widehat{H}^i(G, \mathrm{Hom}_\mathbb{Z}(X, -)) \Rightarrow \widehat{H}^{i+r}(G, -).$$

Then there exists $[x] \in \widehat{H}^r(G, X)$ such that $\Phi_\bullet$ is the cup-product map $([x] \cup -)$.

Proof. The point is to set $X' = \mathbb{Z}$ in Proposition 31. For technical reasons, we note that we have a natural isomorphism

$$([1] \cup -) \colon \widehat{H}^{i+r}(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)) \Rightarrow \widehat{H}^{i+r}(G, -)$$

by checking at index 0 and then using Proposition 25. Thus, $\Phi_\bullet$ will induce a natural transformation

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \overset{\Phi_\bullet}{\Rightarrow} \widehat{H}^{i+r}(G, -) \overset{([1]\cup -)^{-1}}{\Rightarrow} \widehat{H}^{i+r}(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, -)).$$

By Proposition 31, we are promised $[x] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, X))$ such that this composite is $([x] \cup -)$. It follows that $\Phi_\bullet$ is

$$[1] \cup \big([x] \cup -\big) \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{i+r}(G, -).$$

Associating, this natural isomorphism is the same as $\big(([1] \cup [x]) \cup -\big)$; indeed, fixing a G-module A to plug in, we get the result by noting the commutativity of

$$\begin{array}{ccc} \mathbb{Z} \otimes_{\mathbb{Z}} X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A) & \longrightarrow & \mathbb{Z} \otimes_{\mathbb{Z}} A \\ \downarrow & & \downarrow \\ X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A) & \longrightarrow & A \end{array} \qquad \begin{array}{ccc} z \otimes y \otimes f & \longmapsto & z \otimes f(y) \\ \downarrow & & \downarrow \\ zy \otimes f & \longmapsto & f(zy) \end{array}$$

and passing through Lemma 24. ∎

Example 52. For $r \geq 0$, we can continue Example 48 to note that standard dimension-shifting arguments give natural isomorphisms

$$\widehat{H}^0\left(G, \mathrm{Hom}_{\mathbb{Z}}(I_G^{\otimes r}, -)\right) \Rightarrow \widehat{H}^r(G, -),$$

so Corollary 51 implies that these isomorphisms are cup products with an element of $\widehat{H}^r(G, I_G^{\otimes r})$. For example, when $r = 0$, we have $[1] \in \widehat{H}^0(G, \mathbb{Z})$; and when $r = 1$, we have $g \mapsto (1 - g)$ in $\widehat{H}^1(G, I_G)$. Observe that we could also see this by inductively dimension-shifting with Corollary 27.

Because cup products are better-behaved than just general natural transformations, we get the following nice statement.

Corollary 53. Let G be a finite group, and let $r \in \mathbb{Z}$ an index. Then an r-encoding module X has $x \in \widehat{H}^r(G, X)$ such that

$$(x \cup -) \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{i+r}(G, -)$$

is a natural isomorphism for all $i \in \mathbb{Z}$.

Proof. By definition of X, we know that there is some $i \in \mathbb{Z}$ such that we have a natural isomorphism

$$\Phi_\bullet \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{i+r}(G, -).$$

Then Corollary 51 tells us that this natural isomorphism arises as $(x \cup -)$ for some $x \in \widehat{H}^r(G, X)$.

To finish, we extend $(x \cup -)$ being a natural isomorphism from a single i to all $i \in \mathbb{Z}$ by using Proposition 25. Indeed, take $F = \mathrm{Hom}_{\mathbb{Z}}(X, -)$ and $F' = \mathrm{id}$ and $X = X$ and $\eta \colon X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, -) \Rightarrow \mathrm{id}$ to be the canonical evaluation maps. This finishes. ∎

Remark 54. Taking $X = \mathbb{Z}$ above, we are asserting that, if G is a group such that all G-modules admit period-r cohomology which is natural in some sense at a single index i, then this periodicity extends to all indices and arises from a cup product with an element of $\widehat{H}^r(G, \mathbb{Z})$.

Observe that the naturality in the isomorphisms is important: letting $G \coloneqq \mathbb{Z}/p\mathbb{Z}$ act on $A \coloneqq \mathbb{Z}/p\mathbb{Z}$ trivially,

$$\widehat{H}^{-1}(G, A) = \frac{\mathbb{Z}/p\mathbb{Z}}{0} \simeq \widehat{H}^0(G, A),$$

but this does not extend to all G-modules. For example,

$$\widehat{H}^{-1}(G, \mathbb{Z}) = 0 \ncong \frac{\mathbb{Z}}{p\mathbb{Z}} = \widehat{H}^0(G, \mathbb{Z}).$$

The element defined in Corollary 53 is so special that we will give it a name.

Definition 55. Let G be a finite group and X an r-encoding module. An element $x \in \widehat{H}^r(G, X)$ as constructed in Corollary 53 is the *encoding element*.

It will turn out that encoding elements are unique, though they will be almost unique.

3.6 Encoding Is Unique

Fix an r-encoding module X. As a brief intermission, we will show that there is essentially one way to do the encoding

$$\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{i+r}(G, -).$$

Namely, we know from Corollary 51, that this natural isomorphism must come from a cup-product with an element $x \in \widehat{H}^r(G, X)$, so we might wonder how unique this element x is. The answer to this, roughly speaking, will be that $\widehat{H}^r(G, X)$ is cyclic of order $\#G$ generated by x. In the process, we will be able to compute all the cohomology groups $\widehat{H}^i(G, X)$.

Anyway, the main idea will be to use the following duality result.

Proposition 56 ([CE56, Corollary XII.6.5])**.** Let G be a finite group and A be any G-module. Then the cup-product pairing induces an isomorphism

$$\widehat{H}^{i-1}(G, \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Q}/\mathbb{Z})) \to \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-i}(G, A), \widehat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z})\right)$$

for all $i \in \mathbb{Z}$. Indeed, this is a duality upon embedding $\widehat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z})$ into $\mathbb{Q}/\mathbb{Z}$.

And here is our computation.

Corollary 57. Let G be a finite group and X an r-encoding module. Picking up an encoding element $x \in \widehat{H}^r(G, X)$, $\widehat{H}^r(G, X)$ is cyclic of order $\#G$ generated by x.

Proof. For brevity, set $n \coloneqq \#G$. By Corollary 53, we have the isomorphism

$$x \cup -\colon \widehat{H}^{-p-1}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z})) \to \widehat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) = \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

In particular, $\widehat{H}^{-p-1}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) \simeq \mathbb{Z}/n\mathbb{Z}$, generated by some element $x^\vee$ such that $x \cup x^\vee = [1/n]$.

Now, we apply Proposition 56 to say that the cup-product pairing induces an isomorphism

$$\tfrac{1}{n}\mathbb{Z}/n\mathbb{Z} \simeq \widehat{H}^{-p-1}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z})) \to \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^p(G, X), \widehat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z})\right) \simeq \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^p(G, X), \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}\right).$$

Because $\widehat{H}^p(G,X)$ is n-torsion, homomorphisms $\widehat{H}^2(G,X) \to \mathbb{Q}/\mathbb{Z}$ must have image in $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, so in fact the rightmost group is the dual of $\widehat{H}^p(G,X)$. Because an abelian group is isomorphic to its dual, we see that $\widehat{H}^p(G,X)$ is in fact cyclic of order n.

It remains to show that x is a generator; for this, we show that x has order at least n, which will be enough because $H^2(G,X)$ is cyclic of order n. Well, if we have $k \in \mathbb{Z}$ such that $kx = 0$, then

$$[k/n] = k\big(x \cup x^\vee\big) = kx \cup x^\vee = [0] \cup x^\vee = [0]$$

in $\widehat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z}) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, so $n \mid k$. This finishes. ■

Remark 58. Conversely, if $x \in \widehat{H}^r(G,X)$ is any generator, then

$$(x \cup -)\colon \widehat{H}^i(G, \operatorname{Hom}_{\mathbb{Z}}(X,-)) \Rightarrow \widehat{H}^{i+r}(G,-)$$

is a natural isomorphism. Indeed, certainly some generator $x_0 \in \widehat{H}^p(G,X)$ conjured from Corollary 53 suffices, but then $x = kx_0$ for some $k \in (\mathbb{Z}/\#G\mathbb{Z})^\times$, so we have the equality

$$(x \cup -) = \big((kx_0) \cup -\big) = k(x_0 \cup -)$$

of natural transformations. But multiplication by k is a natural isomorphism $\widehat{H}^\bullet(G,-) \Rightarrow \widehat{H}^\bullet(G,-)$ because these cohomology groups are $\#G$-torsion, so we conclude $(x \cup -) = k(x_0 \cup -)$ is a natural isomorphism.

And here is our uniqueness result.

Corollary 59. Let G be a finite group, and let X be a finitely generated r-encoding module. Then, given $i \in \mathbb{Z}$ and two natural isomorphisms

$$\Phi_\bullet, \Phi'_\bullet\colon \widehat{H}^i(G, \operatorname{Hom}_{\mathbb{Z}}(X,-)) \Rightarrow \widehat{H}^{i+r}(G,-),$$

there exists a unique $k \in (\mathbb{Z}/\#G\mathbb{Z})^\times$ such that $\Phi'_\bullet = k\Phi_\bullet$.

Proof. Note that we are allowed to interpret $k \pmod n$ because these cohomology groups are $\#G$-torsion, so $\#G \cdot \Phi_\bullet = 0$.

Anyway, by Corollary 51, we know that there are $x, x' \in \widehat{H}^r(G,X)$ such that

$$\Phi_\bullet = (x \cup -) \qquad \text{and} \qquad \Phi'_\bullet = (x' \cup -).$$

However, by Corollary 57, we see that $\widehat{H}^r(G,X)$ is cyclic generated by x of order $\#G$, so we can write $x' = kx$ for a unique $k \in \mathbb{Z}/\#G\mathbb{Z}$.

It remains to show that $\Phi'_\bullet = k\Phi_\bullet$. Well, for any G-module A and $c \in \widehat{H}^i(G, \operatorname{Hom}_{\mathbb{Z}}(X,A))$, we write

$$\Phi'_A(c) = x' \cup c = kx \cup c = k(x \cup c) = k\Phi_A(c).$$

It follows that $\Phi'_\bullet = k\Phi_\bullet$. ■

3.7 The Dual Element

In the theory of periodic cohomology (e.g., see [CE56, Section XII.11]), it is helpful to phrase the theory in terms of having some elements $x \in \widehat{H}^r(G,\mathbb{Z})$ and $y \in \widehat{H}^{-r}(G,\mathbb{Z})$ such that

$$x \cup y = [1] \in \widehat{H}^0(G,\mathbb{Z}).$$

In contrast, given an r-encoding module X, we cannot hope to have $x \in \widehat{H}^r(G,X)$ and $y \in \widehat{H}^{-r}(G,X)$ with $x \cup y \in \widehat{H}^0(G,\mathbb{Z})$ because there is no obvious map $X \otimes_{\mathbb{Z}} X \to \mathbb{Z}$. To remedy this, we observe that this is a canonical map

$$X \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}) \to \mathbb{Z}.$$

This idea gives the following result.

Proposition 60. Let G be a finite group, and let X be a G-module and $r \in \mathbb{Z}$ be an index. The following are equivalent.

(a) X is an r-encoding module.

(b) There are $x \in \widehat{H}^r(G,X)$ and $x^\vee \in \widehat{H}^{-r}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}))$ such that

$$x \cup x^\vee = [1] \in \widehat{H}^0(G,\mathbb{Z}) \qquad \text{and} \qquad x^\vee \cup x = [\mathrm{id}_X] \in \widehat{H}^0(G,\operatorname{Hom}_{\mathbb{Z}}(X,X)).$$

Proof. For brevity, set $n \coloneqq \#G$.

We start by showing (a) implies (b). By Corollary 53, we can find an encoding element $x \in \widehat{H}^r(G,X)$ yielding the isomorphism

$$(x \cup -)\colon \widehat{H}^{-r}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})) \to \widehat{H}^0(G,\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

As such, we can find a unique $x^\vee \in \widehat{H}^{-r}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}))$ such that $x \cup x^\vee = [1]$. It remains to show that $x^\vee \cup x = [\mathrm{id}_X]$.

Note that $(x \cup -)$ and $(x^\vee \cup -)$ induce morphisms

$$\begin{aligned} (x \cup -)\colon \widehat{H}^0(G,\operatorname{Hom}_{\mathbb{Z}}(X,X)) &\to \widehat{H}^r(G,X) \\ (x^\vee \cup -)\colon \widehat{H}^r(G,X) &\to \widehat{H}^0(G,\operatorname{Hom}_{\mathbb{Z}}(X,X)) \end{aligned}$$

We claim that these are inverse. Because $(x \cup -)$ is already an isomorphism, it suffices to show that we have an inverse on one side. Well, $\widehat{H}^r(G,X)$ is cyclic generated by x by Corollary 57, so it suffices to note that any $kx \in \widehat{H}^r(G,X)$ has

$$\big((x \cup -) \circ (x^\vee \cup -)\big)(kx) = x \cup (x^\vee \cup kx) \overset{*}{=} (x \cup x^\vee) \cup kx = [1] \cup kx = kx.$$

Notably, $\overset{*}{=}$ has used Lemma 24, noting that the square

$$\begin{array}{ccc} X \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}) \otimes_{\mathbb{Z}} X & \longrightarrow & X \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}}(X,X) \\ \downarrow & & \downarrow \\ \mathbb{Z} \otimes_{\mathbb{Z}} X & \longrightarrow & X \end{array} \qquad \begin{array}{ccc} x_1 \otimes f \otimes x_2 & \longmapsto & x_1 \otimes (y \mapsto f(y)x_2) \\ \downarrow & & \downarrow \\ f(x_1) \otimes x_2 & \longmapsto & f(x_1)x_2 \end{array}$$

commutes. Anyway, we now see that we have inverse morphisms, so

$$x \cup [\mathrm{id}_X] = \mathrm{id}_X(x) = x$$

implies that $x^\vee \cup x = [\mathrm{id}_X]$, finishing.

We now show (b) implies (a). Let $i \in \mathbb{Z}$ be any index. The main point is that

$$\begin{aligned} (x \cup -)\colon \widehat{H}^i(G,\operatorname{Hom}_{\mathbb{Z}}(X,-)) &\Rightarrow \widehat{H}^{i+r}(G,-) \\ (x^\vee \cup -)\colon \widehat{H}^{i+r}(G,-) &\Rightarrow \widehat{H}^i(G,\operatorname{Hom}_{\mathbb{Z}}(X,-)) \end{aligned}$$

ought to be inverse natural transformations. More formally, we want to show $(x \cup -)$ is a natural isomorphism, for which we note naturality follows from Lemma 23.

Thus, given a G-module A, it remains to show that its component morphisms

$$(x \cup -) \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \to \widehat{H}^{i+r}(G, A).$$

In fact, we claim that the corresponding map

$$(x^\vee \cup -) \colon \widehat{H}^{i+r}(G, A) \to \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$$

is the inverse morphism. We have two checks.

- In one direction, we note that any $a \in \widehat{H}^{i+r}(G, A)$ has

$$\big((x \cup -) \circ (x^\vee \cup -)\big)(a) = x \cup (x^\vee \cup a) \overset{*}{=} (x \cup x^\vee) \cup a = [1] \cup a = a$$

  where $\overset{*}{=}$ holds by using Lemma 24 on the following commuting square.

$$\begin{array}{ccc} X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} A & \longrightarrow & X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A) \\ \downarrow & & \downarrow \\ \mathbb{Z} \otimes_{\mathbb{Z}} A & \longrightarrow & A \end{array} \qquad \begin{array}{ccc} y \otimes f \otimes b & \longmapsto & y \otimes (y_0 \mapsto f(y_0)b) \\ \downarrow & & \downarrow \\ f(y) \otimes b & \longmapsto & f(y)b \end{array}$$

- In the other direction, we note that $a^\vee \in \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$ will have

$$\big((x^\vee \cup -) \circ (x \cup -)\big)(a^\vee) = x^\vee \cup (x \cup a) \overset{*}{=} (x^\vee \cup x) \cup a = [\mathrm{id}_X] \cup a = \mathrm{id}_X(a) = a,$$

  where $\overset{*}{=}$ holds by using Lemma 24 on the following commuting square.

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A) & \to & \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} A \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbb{Z}}(X, X) \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X, A) \end{array} \qquad \begin{array}{ccc} f \otimes y \otimes g & \longrightarrow & f \otimes g(y) \\ \downarrow & & \downarrow \\ (y_0 \mapsto f(y_0)y) \otimes g & \to & \big(y_0 \mapsto f(y_0)g(y)\big) \end{array}$$

This finishes the proof. ■

We quickly note that the proof of Proposition 60 actually managed to conjure the inverse natural transformation to $(x \cup -)$.

Corollary 61. Let G be a finite group, and let X be an r-encoding module. Constructing $x \in \widehat{H}^r(G, X)$ and $x^\vee \in \widehat{H}^{-r}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}))$ from Proposition 60, the natural transformations

$$\begin{array}{rcl} (x \cup -) \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) & \to & \widehat{H}^{i+r}(G, -) \\ (x^\vee \cup -) \colon \widehat{H}^{i+r}(G, -) & \to & \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \end{array}$$

are inverse for each $i \in \mathbb{Z}$.

Proof. In the proof, we showed that, given a G-module A, the morphisms

$$(x^\vee \cup -) \colon \widehat{H}^{i+r}(G, A) \to \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$$

provide the inverses for $(x \cup -)$. This is what we wanted. ■

As such, we will give the element $x^\vee$ a name.

Definition 62. Let G be a finite group and X an r-encoding module. Element $x^\vee \in \widehat{H}^{-r}(G, \mathrm{Hom}_\mathbb{Z}(X, \mathbb{Z}))$ as constructed in Proposition 60 are *dual elements*.

Here is another amusing corollary we get from this.

Corollary 63. Let G be a finite group, and let X be an r-encoding module with encoding element $x \in \widehat{H}^r(G, X)$. Then, for any subgroup $H \subseteq G$, X is an r-encoding H-module so that any index $i \in \mathbb{Z}$ has the natural isomorphism

$$(\mathrm{Res}\, x \cup -)\colon \widehat{H}^i(H, \mathrm{Hom}_\mathbb{Z}(X, -)) \Rightarrow \widehat{H}^{i+r}(H, -).$$

Proof. The point is that restriction commutes with cup products, so we may use Proposition 60. Indeed, we are given $x \in \widehat{H}^r(G, X)$ and $x^\vee \in \widehat{H}^{-r}(G, \mathrm{Hom}_\mathbb{Z}(X, X))$ such that

$$x \cup x^\vee = [1] \in \widehat{H}^0(G, \mathbb{Z}) \qquad \text{and} \qquad x^\vee \cup x = [\mathrm{id}_X] \in \widehat{H}^0(G, \mathrm{Hom}_\mathbb{Z}(X, X)).$$

Applying restriction to H everywhere, we see

$$\begin{aligned} \mathrm{Res}\, x \cup \mathrm{Res}\, x^\vee &= \mathrm{Res}(x \cup x^\vee) \\ &= \mathrm{Res}([1]) \\ &= [1] \in \widehat{H}^0(H, \mathbb{Z}), \end{aligned}$$

and

$$\begin{aligned} \mathrm{Res}\, x^\vee \cup \mathrm{Res}\, x &= \mathrm{Res}(x^\vee \cup x) \\ &= \mathrm{Res}([\mathrm{id}_X]) \\ &= [\mathrm{id}_X] \in \widehat{H}^0(H, \mathrm{Hom}_\mathbb{Z}(X, X)), \end{aligned}$$

which is enough by Proposition 60 to show that X is an r-encoding H-module. The remarks from Corollary 61 explain why the needed isomorphism is given by $(\mathrm{Res}\, x \cup -)$. ∎

Remark 64. Essentially the same proof should hold for inflation.

Example 65. It is not true that, if X is an r-encoding G_p-module for all Sylow p-subgroups $G_p \subseteq G$, then X is an r-encoding G-module. Indeed, take $X = \mathbb{Z}$ and $G = S_3$: all Sylow p-subgroups of S_3 are cyclic, so $\mathbb{Z}$ is a 2-encoding module for all these subgroups. However, S_3 is not cyclic, so

$$\widehat{H}^{-2}(G, \mathrm{Hom}_\mathbb{Z}(X, \mathbb{Z})) \simeq \widehat{H}^{-2}(G, \mathbb{Z}) \simeq S_3/[S_3, S_3] \ncong \mathbb{Z}/6\mathbb{Z} = \widehat{H}^0(G, \mathbb{Z}).$$

3.8 Encoding by Tensoring

It turns out that we can also encode "on the other side," in the following sense.

Theorem 66. Let G be a finite group, and let X be an r-encoding module with encoding element $x \in \widehat{H}^r(G, X)$. Then the cup products

$$(- \cup x)\colon \widehat{H}^i(G, -) \Rightarrow \widehat{H}^{i+r}(G, - \otimes_\mathbb{Z} X)$$

assemble into a natural isomorphism for any $i \in \mathbb{Z}$.

Proof. That we have a natural transformation follows from the naturality of cup products. Thus, it suffices to pick up a G-module A and show that the component morphisms

$$(-\cup x)\colon \widehat{H}^i(G,A) \to \widehat{H}^{i+r}(G, A\otimes_{\mathbb{Z}} X)$$

is an isomorphism. For this, we pick up a dual element $x^\vee \in \widehat{H}^{i+r}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}))$ so that

$$x\cup x^\vee = [1]\in \widehat{H}^0(G,\mathbb{Z}) \qquad \text{and} \qquad x^\vee \cup x = [\mathrm{id}_X]\in \widehat{H}^0(G,\operatorname{Hom}_{\mathbb{Z}}(X,X)).$$

As such, we claim that the morphisms

$$\begin{aligned}(-\cup x)\colon &\quad \widehat{H}^i(G,A) &&\to \widehat{H}^{i+r}(G,A\otimes_{\mathbb{Z}} X)\\ (-\cup x^\vee)\colon \widehat{H}^{i+r}(G,A\otimes_{\mathbb{Z}} X) &\to \quad \widehat{H}^i(G,A)\end{aligned}$$

are inverse, which will finish; here $(-\cup x^\vee)$ is using the following evaluation map.

$$\begin{aligned}(A\otimes_{\mathbb{Z}} X)\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}) &\to A\\ b\otimes y\otimes f &\mapsto f(y)b\end{aligned}$$

We have now checks for our morphisms to be inverse.

- On one hand, pick up $a\in\widehat{H}^i(G,A)$. Then we can use Lemma 24 on the commuting square

$$\begin{array}{ccc} A\otimes_{\mathbb{Z}} X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}) & \longrightarrow & A\otimes_{\mathbb{Z}}\mathbb{Z}\\ \| & & \downarrow\\ A\otimes_{\mathbb{Z}} X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}) & \longrightarrow & A\end{array} \qquad \begin{array}{ccc} b\otimes y\otimes f & \longmapsto & b\otimes f(y)\\ \| & & \downarrow\\ b\otimes y\otimes f & \longmapsto & f(y)b\end{array}$$

  to evaluate

$$\big((-\cup x^\vee)\circ(-\cup x)\big)(a) = (a\cup x)\cup x^\vee = a\cup(x\cup x^\vee) = a\cup[1] = a.$$

- On the other hand, pick up $a^\vee\in\widehat{H}^{i+r}(G,A\otimes_{\mathbb{Z}} X)$. Then we can use Lemma 24 on the commuting square

$$\begin{array}{ccc} (A\otimes_{\mathbb{Z}} X)\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\otimes_{\mathbb{Z}} X & \longrightarrow & A\otimes_{\mathbb{Z}} X\\ \downarrow & & \|\\ (A\otimes_{\mathbb{Z}} X)\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,X) & \longrightarrow & A\otimes_{\mathbb{Z}} X\end{array} \qquad \begin{array}{ccc} b\otimes y\otimes f\otimes y' & \longmapsto & f(y)b\otimes y'\\ \downarrow & & \|\\ b\otimes y\otimes(y_0\mapsto f(y_0)y') & \longmapsto & b\otimes f(y)y'\end{array}$$

  to evaluate

$$\big((-\cup x)\circ(-\cup x^\vee)\big)(a) = (a\cup x^\vee)\cup x = a^\vee\cup(x^\vee\cup x) = a^\vee\cup[\mathrm{id}_X] = a^\vee.$$

The above checks complete the proof. ∎

Remark 67. One could rebuild the theory we have in the previous sections, in particular showing that all natural isomorphisms of the form

$$\widehat{H}^i(G,-\otimes_{\mathbb{Z}} A)\Rightarrow\widehat{H}^{i+r}(G,-\otimes_{\mathbb{Z}} B)$$

are cup products from an element of $\widehat{H}^r(G,\operatorname{Hom}_{\mathbb{Z}}(A,B))$. Thus, for some G-module X, natural isomorphisms

$$\widehat{H}^i(G,-)\Rightarrow\widehat{H}^{i+r}(G,-\otimes_{\mathbb{Z}} X)$$

promise $x\in\widehat{H}^r(G,X)$ (from using $A=\mathbb{Z}$ and $B=X$ with $i=0$) and $x^\vee\in\widehat{H}^{-r}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}))$ (from using $A=X$ and $B=\mathbb{Z}$ with $i=-r$) which we can evaluate to have

$$x\cup x^\vee = [1]\in\widehat{H}^0(G,\mathbb{Z}) \qquad \text{and} \qquad x^\vee\cup x = [\mathrm{id}_X]\in\widehat{H}^0(G,\operatorname{Hom}_{\mathbb{Z}}(X,X)).$$

Namely, X is an r-encoding module!

Corollary 68. Let G be a finite group, and let X be an r-encoding module with encoding element $x \in \widehat{H}^r(G, X)$. Then the cup products

$$(- \cup x) \colon \widehat{H}^i(G, \mathbb{Z}) \to \widehat{H}^{i+r}(G, X)$$

are isomorphisms for all $i \in \mathbb{Z}$.

Proof. Plug in $\mathbb{Z}$ into Theorem 66. ∎

3.9 Torsion-Free Encoding

In the theory of periodic cohomology, one can show that it is enough to check the single cohomology group

$$\widehat{H}^r(G, \mathbb{Z}) \cong \mathbb{Z}/\#G\mathbb{Z}$$

for some index $r \in \mathbb{Z}$ to get r-periodic cohomology. We might hope that something similar is true for our r-encoding modules. To this end, we pick up the following "integral" duality statement.

Proposition 69. Let G be a finite group, and let X be a $\mathbb{Z}$-free G-module. Then the cup-product pairing induces an isomorphism

$$\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) \to \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-i}(G, X), \widehat{H}^0(G, \mathbb{Z})\right)$$

for all $i \in \mathbb{Z}$. Indeed, this is a duality upon identifying $\widehat{H}^0(G, \mathbb{Z})$ with $\frac{1}{\#G}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$.

Proof. This proof is analogous to [CE56, Theorem XII.6.6]. The key to the proof is the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0. \tag{3.6}$$

The main point is that X being $\mathbb{Z}$-free implies that X is projective (as an abelian group), so we can apply $\mathrm{Hom}_{\mathbb{Z}}(X, -)$ to get out the short exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}) \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z}) \to 0. \tag{3.7}$$

Now, note that the multiplication-by-n endomorphism on $\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q})$ is an isomorphism (namely, $\mathbb{Q}$ is a divisible abelian group), so the same will be true of $\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}))$ for any $i \in \mathbb{Z}$. However, these cohomology groups must be $\#G$-torsion, so in fact $\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q})) = 0$ for all $i \in \mathbb{Z}$.

Similarly, we note that we can hit (3.7) with the functor $- \otimes_{\mathbb{Z}} X$ to get another short exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} X \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}) \otimes_{\mathbb{Z}} X \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} X \to 0. \tag{3.8}$$

Notably, this is exact because X is $\mathbb{Z}$-free and hence flat as a $\mathbb{Z}$-module. Now, $\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}) \otimes_{\mathbb{Z}} X$ is still a divisible abelian group, so again $\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q})) = 0$ for all $i \in \mathbb{Z}$.

The rest of the proof is tracking boundary morphisms around. Fix some $i \in \mathbb{Z}$. Note (3.6) and (3.7) and (3.8) induce boundary isomorphisms

$$\begin{aligned}
\delta &\colon \widehat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \to \widehat{H}^0(G, \mathbb{Z}) \\
\delta_h &\colon \widehat{H}^{i-1}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z})) \to \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) \\
\delta_t &\colon \widehat{H}^{-1}(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} X) \to \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} X).
\end{aligned}$$

We also note that we have a morphism of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} X & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}) \otimes_{\mathbb{Z}} X & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z}) \otimes_{\mathbb{Z}} X & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \eta_{\mathbb{Z}}} & & \downarrow{\scriptstyle \eta_{\mathbb{Q}}} & & \downarrow{\scriptstyle \eta_{\mathbb{Q}/\mathbb{Z}}} & & \\
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0
\end{array}$$

where the $\eta_\bullet$ are evaluation maps. Now, Proposition 56 tells us that

$$\begin{array}{ccc} \widehat{H}^{i-1}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z})) & \to & \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-i}(G, X), \widehat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z})\right) \\ a & \mapsto & (b \mapsto \eta_{\mathbb{Q}/\mathbb{Z}}(a \cup b)) \end{array}$$

is an isomorphism. Composing this with various other isomorphisms, we can build the isomorphism

$$\begin{array}{ccccccc} \widehat{H}^{i}(G, X^\vee) & \to & \widehat{H}^{i-1}(G, X^*) & \to & \mathrm{Hom}\left(\widehat{H}^{-i}(G, X), \widehat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z})\right) & \to & \mathrm{Hom}\left(\widehat{H}^{-i}(G, X), \widehat{H}^{0}(G, \mathbb{Q}/\mathbb{Z})\right) \\ a & \mapsto & \delta_h^{-1} a & \mapsto & \left(b \mapsto \eta_{\mathbb{Q}/\mathbb{Z}}(\delta_h^{-1} a \cup b)\right) & \mapsto & \left(b \mapsto \delta\eta_{\mathbb{Q}/\mathbb{Z}}(\delta_h^{-1} a \cup b)\right) \end{array}$$

where $X^\vee := \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})$ and $X^* := \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Q}/\mathbb{Z})$, for brevity. This gives an isomorphism between the desired objects, but to prove the result we need to show that the above map is $a \mapsto (b \mapsto \eta_{\mathbb{Z}}(a \cup b))$. Well, given $a \in \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}))$ and $b \in \widehat{H}^{-i}(G, X)$, properties of the boundary morphisms tells us

$$\begin{aligned} \delta\eta_{\mathbb{Q}/\mathbb{Z}}\left(\delta_h^{-1} a \cup b\right) &= \eta_{\mathbb{Z}}\delta_t\left(\delta_h^{-1} a \cup b\right) \\ &= \eta_{\mathbb{Z}}\left(\delta_h \delta_h^{-1} a \cup b\right) \\ &= \eta_{\mathbb{Z}}(a \cup b), \end{aligned}$$

which is what we wanted. ∎

Remark 70. The hypothesis that X be $\mathbb{Z}$-free is necessary: the statement is false for $X = \mathbb{Z}/\#G\mathbb{Z}$ and $i = 0$, for example.

And here is our result.

Proposition 71. Let G be a finite group, and let X be a $\mathbb{Z}$-free G-module. The following are equivalent.

(a) X is an r-encoding module.

(b) $\widehat{H}^r(G, X) \cong \mathbb{Z}/\#G\mathbb{Z}$ and $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) \cong \mathbb{Z}/\#G\mathbb{Z}$.

(c) $\widehat{H}^r(G, X) \cong \mathbb{Z}/\#G\mathbb{Z}$ and $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X))$ is cyclic.

Proof. For brevity, set $n := \#G$. That (a) implies (b) is not hard: Corollary 57 tells us that $\widehat{H}^r(G, X) \cong \mathbb{Z}/n\mathbb{Z}$, and then being an r-encoding module promises an isomorphism

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) \simeq \widehat{H}^r(G, X) \cong \mathbb{Z}/n\mathbb{Z}.$$

Continuing, we see that (b) implies (c) easily. Thus, the interesting direction is showing that (c) implies (a).

For this, we use Proposition 69 and Proposition 60. We are given $x \in \widehat{H}^r(G, X)$ of order n, so we note that there is a morphism

$$\widehat{H}^r(G, X) \simeq \mathbb{Z}/n\mathbb{Z} = \widehat{H}^0(G, \mathbb{Z})$$

sending x to $[1]$. Thus, Proposition 69 grants $x^\vee \in \widehat{H}^{-r}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}))$ such that

$$x \cup x^\vee = [1] \in \widehat{H}^0(G, \mathbb{Z}).$$

It remains to check that $x^\vee \cup x = [\mathrm{id}_X] \in \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X))$. This is more difficult.

For this, we will show that

$$(x \cup -) \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, X)) \to \widehat{H}^r(G, X) \tag{3.9}$$

is injective while showing that $x^\vee \cup x$ and id_X have the same image under $(x \cup -)$.

Indeed, on one hand, let A be a G-module (which we will set to be X shortly), and we claim that the composite

$$\widehat{H}^r(G,A) \xrightarrow{x^\vee \cup -} \widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,A)) \xrightarrow{x \cup -} \widehat{H}^r(G,A)$$

is the identity. Then the commutativity of the diagram

$$\begin{array}{ccc} X \otimes_\mathbb{Z} \mathrm{Hom}_\mathbb{Z}(X,\mathbb{Z}) \otimes_\mathbb{Z} A & \longrightarrow & X \otimes_\mathbb{Z} \mathrm{Hom}_\mathbb{Z}(X,A) \\ \downarrow & & \downarrow \\ \mathbb{Z} \otimes_\mathbb{Z} A & \longrightarrow & A \end{array} \qquad \begin{array}{ccc} x_0 \otimes f \otimes a_0 & \longmapsto & x_0 \otimes \big(y \mapsto f(y)a_0\big) \\ \downarrow & & \downarrow \\ f(x_0) \otimes a_0 & \longmapsto & f(x_0)a_0 \end{array}$$

allows us to compute, for any $a \in \widehat{H}^p(G,A)$,

$$x \cup x^\vee \cup a = [1] \cup a = a, \tag{3.10}$$

as desired.

Now, taking $A = X$, we note

$$x \cup [\mathrm{id}_X] = x \in \widehat{H}^r(G,X). \tag{3.11}$$

So we will be done once we show that (3.9)is injective. Well, note $[\mathrm{id}_X] \in \widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X))$ has order n: if $k[\mathrm{id}_X] = 0$, then $0 = k(x \cup [\mathrm{id}_X]) = kx$, so $n \mid k$. Because $\widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X))$ is cyclic (by hypothesis!) and n-torsion, we conclude that in fact $\widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X))$ is cyclic of order n generated by $[\mathrm{id}_X]$. Thus, we note that there is a unique isomorphism

$$\widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X)) \cong \mathbb{Z}/n\mathbb{Z} \cong \widehat{H}^r(G,X)$$

sending $[\mathrm{id}_X]$ to 1 to x, so this isomorphism must be $(x \cup -)$ by (3.11); in particular, $(x \cup -)$ is injective.

Finishing up, comparing the injectivity of $(x \cup -)$ with (3.10) and (3.11) forces us to conclude that $x^\vee \cup x = [\mathrm{id}_X]$. This finishes. ∎

Example 72. The $\mathbb{Z}$-free condition is necessary. As in Remark 54, let $G := \mathbb{Z}/p\mathbb{Z}$ act on $X := \mathbb{Z}/p\mathbb{Z}$ trivially. Then

$$\widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X)) \simeq \widehat{H}^0(G,X) \cong \widehat{H}^{-1}(G,X) = \mathbb{Z}/p\mathbb{Z}.$$

However, X is not a (-1)-encoding module because

$$\widehat{H}^1(G,\mathrm{Hom}_\mathbb{Z}(X,\mathbb{Z})) \simeq \widehat{H}^1(G,0) = 0 \ncong \mathbb{Z}/p\mathbb{Z} = \widehat{H}^0(G,\mathbb{Z}).$$

Remark 73. As we will discuss later in Remark 82, the requirement that X be $\mathbb{Z}$-free is not too serious.

Example 74. To see that $\widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X))$ being cyclic is necessary, we use the example from Example 40. Let $G = \langle\sigma\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ act on $X := \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$ by conjugation. Then

$$\widehat{H}^0(G,X) \simeq \widehat{H}^0(G,\mathbb{Z}) \oplus \widehat{H}^0(G,\mathbb{Z}i) \simeq \mathbb{Z}/2\mathbb{Z},$$

but

$$\begin{aligned} \widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X)) \simeq{}& \widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(\mathbb{Z},\mathbb{Z})) \oplus \widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(\mathbb{Z},\mathbb{Z}i)) \\ &\oplus \widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(\mathbb{Z}i,\mathbb{Z})) \oplus \widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(\mathbb{Z}i,\mathbb{Z}i)) \end{aligned}$$

comes out to $\mathbb{Z}/2\mathbb{Z} \oplus 0 \oplus 0 \oplus \mathbb{Z}/2\mathbb{Z}$. Thus,

$$\widehat{H}^0(G,\mathrm{Hom}_\mathbb{Z}(X,X)) \ncong \widehat{H}^0(G,X),$$

so X is not a 0-encoding module even though X is $\mathbb{Z}$-free and $\widehat{H}^0(G,X) \cong \mathbb{Z}/\#G\mathbb{Z}$.

In some sense, the issue with the above example is that we could decompose our G-module into $A \oplus B$ when in fact there is no reason to talk about these sorts of G-modules as encoding modules.

Corollary 75. Let G be a finite p-group. If $A \oplus B$ is a finitely generated $\mathbb{Z}$-free r-encoding module, then one of A or B is an r-encoding module and the other is cohomologically equivalent to 0.

Proof. This follows quickly from the check in Proposition 71. On one hand,

$$\begin{aligned}\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A \oplus B, A \oplus B)) \simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A)) \oplus \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, B)) \\ \oplus \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, A)) \oplus \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, B))\end{aligned}$$

tells us that both $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A))$ and $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, B))$ are both cyclic because $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A \oplus B, A \oplus B))$ is.

On the other hand, we note

$$\widehat{H}^r(G, A) \oplus \widehat{H}^r(G, B) \simeq \widehat{H}^r(G, A \oplus B) \cong \mathbb{Z}/\#G\mathbb{Z},$$

so we are forced to have $\widehat{H}^r(G, A) \cong \mathbb{Z}/\#G\mathbb{Z}$ or $\widehat{H}^r(G, B) \cong \mathbb{Z}/\#G\mathbb{Z}$ because G is a finite p-group.

Thus, one of A or B is an r-encoding module; without loss of generality, say that A is. It remains to show that B is cohomologically equivalent to 0. Well, we have

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A)) \cong \widehat{H}^r(G, A) = \mathbb{Z}/\#G\mathbb{Z}$$

because A is an r-encoding module, so the embedding

$$\underbrace{\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, A))}_{\mathbb{Z}/\#G\mathbb{Z}} \oplus \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, B)) \subseteq \underbrace{\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A \oplus B, A \oplus B))}_{\mathbb{Z}/\#G\mathbb{Z}}$$

forces $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(B, B)) = 0$. As such, Corollary 39 finishes. ∎

Remark 76. It is conceivable that Corollary 75 is true without requiring $A \oplus B$ to be $\mathbb{Z}$-free nor G to be a p-group.

3.10 New Encoding Modules From Old

The goal of this section is to build encoding modules up from smaller ones.

Proposition 77. Let G be a finite group. Given an r-encoding module A and an s-encoding module B, the G-module $A \otimes_{\mathbb{Z}} B$ is an $(r+s)$-encoding module.

Proof. By Corollary 53, we have natural isomorphisms

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A, -)) \simeq \widehat{H}^r(G, -) \qquad \text{and} \qquad \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(B, -)) \simeq \widehat{H}^{r+s}(G, -).$$

Whiskering, we have a natural isomorphism

$$\begin{aligned}\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(A \otimes_{\mathbb{Z}} B, -)) &\simeq \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(A, \mathrm{Hom}_{\mathbb{Z}}(B, -))) \\ &\simeq \widehat{H}^r(G, \mathrm{Hom}_{\mathbb{Z}}(B, -)) \\ &\simeq \widehat{H}^{r+s}(G, -),\end{aligned}$$

which is what we wanted. ∎

Remark 78. With some care, it is possible to use Corollary 45 to show this result. The difficulty in realizing this approach lies in the fact that r and s need not both be nonnegative.

Proposition 79. Let G be a finite group, and let X be an r-encoding module. Then $\mathrm{Hom}_{\mathbb{Z}}(X,\mathbb{Z})$ is a $(-r)$-encoding module.

Proof. We use Proposition 60. For brevity, we set $X^\vee \coloneqq \mathrm{Hom}_{\mathbb{Z}}(X,\mathbb{Z})$ and $X^{\vee\vee} \coloneqq \mathrm{Hom}_{\mathbb{Z}}(X^\vee,\mathbb{Z})$. Observe that there is a (canonical) map $\varphi\colon X \to X^{\vee\vee}$ by

$$\varphi\colon f \mapsto f\circ\varphi.$$

By Proposition 60, we may find $x \in \widehat{H}^r(G,X)$ and $x^\vee \in \widehat{H}^{-r}(G,X^\vee)$ such that

$$x\cup x^\vee = [1] \in \widehat{H}^0(G,\mathbb{Z}) \qquad \text{and} \qquad x^\vee \cup x = [\mathrm{id}_X] \in \widehat{H}^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,X)).$$

As such, we set $y \coloneqq x^\vee$ and $y^\vee \coloneqq (-1)^r\varphi(x)$. The commutative diagram

$$\begin{array}{ccc} X\otimes_{\mathbb{Z}} X^\vee & \longrightarrow & \mathbb{Z} \\ {\scriptstyle \varphi\otimes\mathrm{id}}\downarrow & & \| \\ X^{\vee\vee}\otimes_{\mathbb{Z}} X^\vee & \longrightarrow & \mathbb{Z} \end{array} \qquad\qquad \begin{array}{ccc} x\otimes f & \longmapsto & f(x) \\ \downarrow & & \| \\ (g\mapsto g(x))\otimes f & \longmapsto & f(x) \end{array}$$

tells us that we may evaluate

$$\varphi(x)\cup x^\vee = x\cup x^\vee = [1] \in \widehat{H}^0(G,\mathbb{Z}),$$

so $y\cup y^\vee = [1] \in \widehat{H}^0(G,\mathbb{Z})$ after being careful with signs.

On the other hand, we set $A = B = X$ for clarity and define $\psi\colon \mathrm{Hom}_{\mathbb{Z}}(A,B) \to \mathrm{Hom}_{\mathbb{Z}}(B^*,A^*)$ by

$$\psi(f)\colon g \mapsto (g\circ f),$$

yielding the commutative diagram

$$\begin{array}{ccc} A^\vee\otimes_{\mathbb{Z}} B & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(A,B) \\ {\scriptstyle \mathrm{id}\otimes\varphi}\downarrow & & \downarrow{\scriptstyle \psi} \\ A^\vee\otimes_{\mathbb{Z}}\mathrm{Hom}_{\mathbb{Z}}(B^\vee,\mathbb{Z}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(B^\vee,A^\vee) \end{array} \qquad\qquad \begin{array}{ccc} f\otimes b & \longmapsto & \big(a\mapsto f(a)b\big) \\ \downarrow & & \downarrow \\ f\otimes\big(g\mapsto g(b)\big) & \longmapsto & \big(g\mapsto g(b)f\big) \end{array}$$

which tells us that we may evaluate

$$x^\vee\cup\varphi(x) = \psi(x^\vee\cup x) = \psi([\mathrm{id}_X]) = [\mathrm{id}_{X^\vee}] \in \widehat{H}^0(G,\mathrm{Hom}_{\mathbb{Z}}(X^\vee,X^\vee)),$$

so $y^\vee\cup y = [\mathrm{id}_{X^\vee}]$ after being careful with signs. This completes the proof. ∎

Example 80. Example 48 established that $I_G^{\otimes r}$ is an r-encoding module for $r\geq 0$. As such, $\mathrm{Hom}_{\mathbb{Z}}\left(I_G^{\otimes r},\mathbb{Z}\right)$ is a $(-r)$-encoding module for $-r\leq 0$. Thus, we have established existence for r-encoding modules for all $r\in\mathbb{Z}$.

Corollary 81. Let G be a finite group, and let X be a finitely generated r-encoding module. Letting X_t denote the $\mathbb{Z}$-torsion subgroup of X, we have that X_t is a G-submodule of X, and X/X_t is an r-encoding module.

Proof. To see that X_t is a G-submodule, we note that any $x \in X_t$ has some $k \in \mathbb{Z}$ such that $kx = 0$, so any $g \in G$ will have

$$k \cdot gx = g(kx) = g \cdot 0 = 0.$$

Thus, $X_t \subseteq X$ is preserved by G.

It remains to show that $X_f := X/X_t$ is an r-encoding module. To begin, we claim that

$$\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}), \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X_f, \mathbb{Z}), \mathbb{Z}) \tag{3.12}$$

as G-modules; by Proposition 79, this will imply that $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X_f, \mathbb{Z}), \mathbb{Z})$ is an r-encoding module. To see this, we note that the short exact sequence

$$0 \to X_t \to X \to X_f \to 0$$

becomes the left exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X_f, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(X_t, \mathbb{Z}).$$

However, $\mathrm{Hom}_{\mathbb{Z}}(X_t, \mathbb{Z}) = 0$ because X_t is $\mathbb{Z}$-torsion, so the above left exact sequence witnesses the isomorphism $\mathrm{Hom}_{\mathbb{Z}}(X_f, \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})$. Applying $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ again yields (3.12).

To finish, we note that

$$\varphi \colon X_f \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X_f, \mathbb{Z}), \mathbb{Z})$$

by $x \mapsto (f \mapsto f(x))$ is a G-module morphism and isomorphism of abelian groups because X_f is torsion-free and finitely generated. Thus, φ is an isomorphism of G-modules, implying that X_f is an r-encoding module. ∎

Remark 82. Even though Example 50 asserts that not all p-encoding modules X are $\mathbb{Z}$-torsion-free, Corollary 81 explains that we can canonically obtain a $\mathbb{Z}$-torsion-free p-encoding module from X in the form of $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}), \mathbb{Z}) \cong X/X_t$.

Proposition 83. Let G be a finite group, and let

$$0 \to X' \to M \to X \to 0$$

be a $\mathbb{Z}$-split short exact sequence such that M is an induced G-module. Then X is an r-encoding module if and only if X' is an $(r+1)$-encoding module.

Proof. Given a G-module A, we recall that $\mathrm{Hom}_{\mathbb{Z}}(-, A)$ is a shiftable functor by Lemma 16, so $\mathrm{Hom}_{\mathbb{Z}}(M, A)$ is induced. Now, because the short exact sequence is $\mathbb{Z}$-split, we have the short exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(X, A) \to \mathrm{Hom}_{\mathbb{Z}}(M, A) \to \mathrm{Hom}_{\mathbb{Z}}(X', A) \to 0$$

which gives the isomorphism

$$\delta_A \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', A)) \to \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$$

because $\mathrm{Hom}_{\mathbb{Z}}(M, A)$ is induced. In fact, the δ_A make a natural isomorphism $\delta_\bullet \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', -)) \Rightarrow \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, -))$: given a G-module morphism $f \colon A \to B$, the morphism of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(M, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X', A) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} & & \\
0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X, B) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(M, B) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(X', B) & \longrightarrow & 0
\end{array}$$

induces the desired commuting square, as follows.

$$\begin{array}{ccc} \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', A)) & \xrightarrow{\delta_A} & \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', B)) & \xrightarrow{\delta_B} & \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, B)) \end{array}$$

We now proceed with the proof. In one direction, if X is an r-encoding module, then Corollary 53 promises us a natural isomorphism

$$\Phi_\bullet \colon \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{r+1}(G, -),$$

so the composite

$$\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X', -)) \overset{\delta_\bullet}{\Rightarrow} \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \overset{\Phi_\bullet}{\Rightarrow} \widehat{H}^{r+1}(G, -)$$

shows that X' is a $(r+1)$-encoding module. The other direction is analogous, concatenating with $\delta_\bullet^{-1}$. ■

Example 84. Fix a finite group G generated by $S \coloneqq \langle \sigma_1, \dots, \sigma_n \rangle$, and let $M \coloneqq \mathbb{Z}[G]^{\#S}$ have basis $\{e_i\}_{i=1}^m$. Then there is a projection $\pi \colon \mathbb{Z}[G]^{\#G} \twoheadrightarrow I_G$ by sending $e_i \mapsto (\sigma_i - 1)$, giving the short exact sequence

$$0 \to \ker \pi \to \mathbb{Z}[G]^{\#S} \to I_G \to 0.$$

This short exact sequence is $\mathbb{Z}$-split because I_G is $\mathbb{Z}$-free. Because $\mathbb{Z}[G]^{\#S} \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}^{\#S}$ is induced and I_G is a 1-encoding module, we conclude that $\ker \pi$ is a 2-encoding module by Proposition 83.

By this point, we have a wide array of ways of making p-encoding modules, so we call it quits here.

3.11 A Perfect Pairing

We close this section with a hint of Artin reciprocity. The main goal of this subsection is to prove the following result.

Theorem 85. Let G be a finite group, and let X and A be G-modules and $r \in \mathbb{Z}$ be an index. Then, if there exists an element $c \in H^r(G, X)$ such that the cup-product maps

$$\begin{aligned} (c \cup -) \colon \widehat{H}^{-r}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) &\to \widehat{H}^0(G, \mathbb{Z}) \\ (c \cup -) \colon \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) &\to \widehat{H}^r(G, A) \end{aligned}$$

are isomorphisms, then the cup-product pairing induces an isomorphism

$$\widehat{H}^r(G, A) \to \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-r}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})), \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))\right).$$

Proof. Applying Lemma 24 to the commutative square

$$\begin{array}{ccc} X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} A & \longrightarrow & X \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(X, A) \\ \downarrow & & \downarrow \\ \mathbb{Z} \otimes_{\mathbb{Z}} A & \longrightarrow & A \end{array} \qquad \begin{array}{ccc} x \otimes f \otimes a & \longmapsto & x \otimes (y \mapsto f(y)a) \\ \downarrow & & \downarrow \\ f(x) \otimes a & \longmapsto & f(x)a \end{array}$$

we are able to conclude that any $u \in H^p(G, A)$ makes the diagram

$$\begin{array}{ccc} \widehat{H}^{-r}(G, \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) & \xrightarrow{-\cup u} & \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \\ {\scriptstyle c\cup -}\downarrow & & \downarrow{\scriptstyle c\cup -} \\ \widehat{H}^0(G, \mathbb{Z}) & \xrightarrow[-\cup u]{} & \widehat{H}^r(G, A) \end{array}$$

commute. Now, by hypothesis, the left and right arrows are isomorphisms, so the commutativity means that showing

$$\begin{array}{ccc} \widehat{H}^r(G,A) & \to & \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-r}(G,\mathrm{Hom}_{\mathbb{Z}}(X,\mathbb{Z})),\widehat{H}^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,A))\right) \\ u & \mapsto & (a\mapsto(a\cup u)) \end{array}$$

is an isomorphism is the same as showing that

$$\begin{array}{ccc} \widehat{H}^r(G,A) & \to & \mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^0(G,\mathbb{Z}),\widehat{H}^r(G,A)\right) \\ u & \mapsto & (k\mapsto(k\cup u)) \end{array}$$

is an isomorphism.

Setting $n \coloneqq \#G$, we see $\widehat{H}^0(G,\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$, and the cup product we are looking at sends $k \in \mathbb{Z}/n\mathbb{Z}$ and $u \in \widehat{H}^2(G,A)$ to $k\cup u = ku$ by how the isomorphism $\mathbb{Z}\otimes_{\mathbb{Z}} A \simeq A$ behaves. Thus, we are showing that

$$\begin{array}{ccc} \widehat{H}^p(G,A) & \to & \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z},\widehat{H}^r(G,A)\right) \\ u & \mapsto & (k\mapsto ku) \end{array}$$

is an isomorphism.

However, $\widehat{H}^r(G,A)$ is n-torsion, so in fact maps $\mathbb{Z}\to\widehat{H}^p(G,A)$ automatically have $n\mathbb{Z}$ in their kernel and hence reduce to maps $\mathbb{Z}/n\mathbb{Z}\to\widehat{H}^r(G,A)$. Conversely, any map $\mathbb{Z}/n\mathbb{Z}\to\widehat{H}^p(G,A)$ can be extended by $\mathbb{Z}\twoheadrightarrow\mathbb{Z}/n\mathbb{Z}$ to a map $\mathbb{Z}\to\widehat{H}^r(G,A)$, so we have a natural isomorphism

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z},\widehat{H}^r(G,A)\right) & \simeq & \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z},\widehat{H}^r(G,A)\right) \\ f & \mapsto & (k\mapsto f([k])) \\ ([k]\mapsto f(k)) & \mapsfrom & f. \end{array}$$

In particular, it suffices to show that

$$\begin{array}{ccc} \widehat{H}^r(G,A) & \to & \mathrm{Hom}_{\mathbb{Z}}\left(\mathbb{Z},\widehat{H}^r(G,A)\right) \\ u & \mapsto & (k\mapsto ku) \end{array}$$

is an isomorphism. But this is a standard fact about the functor $\mathrm{Hom}_{\mathbb{Z}}$, so we are done. ■

We now synthesize this with the theory we have been building.

Corollary 86. Let G be a finite group, and let X be an r-encoding module. Then, given a G-module A, the cup-product pairing induces an isomorphism

$$\widehat{H}^r(G,A)\to\mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-r}(G,\mathrm{Hom}_{\mathbb{Z}}(X,\mathbb{Z})),\widehat{H}^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,A))\right).$$

Proof. We apply Theorem 85 to our case; we take c to be the x of Corollary 51. The cup-product maps in question are isomorphisms by Corollary 53. Thus, Theorem 85 kicks in, completing the proof. ■

Remark 87. The other side of the pairing

$$\widehat{H}^{-r}(G,\mathrm{Hom}_{\mathbb{Z}}(X,\mathbb{Z}))\to\mathrm{Hom}_{\mathbb{Z}}\left(\widehat{H}^r(G,A),\widehat{H}^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,A))\right)$$

need not be an isomorphism; for example, take $A=0$.

Remark 88. When X is a $\mathbb{Z}$-free 2-encoding module, we can think about $\mathrm{Hom}_{\mathbb{Z}}(X, -)$ as a torus T. For example, if L/K is an extension of local fields, and the torus T splits over L, then the above statement says that the Artin reciprocity map

$$\widehat{H}^{-2}(L/K, X_*(T)) \to \widehat{H}^0(L/K, TL)$$

uniquely determines $u_{L/K} \in \widehat{H}^2(L/K, L^\times)$. It is conceivable that a sufficiently concrete description of this reciprocity map might then be able to describe $u_{L/K}$.

4 Group Laws of Group Extensions

Having established some background of what we expect from our encoding modules, we will spend the next few sections building a particularly nice example of a 2-encoding module with ties to classifying group extensions.

Much of the theory in this section will be similar to that built in [AS78] and [Tig81]. In particular, providing a group law for the extensions built from our G-module A is essentially the same problem as being able to write down a group law for abelian crossed products. Regardless, we will build the theory from the ground.

4.1 Motivating Results

Throughout this section, G will be a finite group and A will be a G-module; we will write the group operation of A and the group action of G on A multiplicatively. To sketch the idea here, begin with an extension

$$1 \to A \to \mathcal{E} \xrightarrow{\pi} G \to 1.$$

We know that we can abstractly represent $\mathcal{E}$ as the set $A \times G$ with some group law dictated by a 2-cocycle in $Z^2(G, A)$, so we expect that $\mathcal{E}$ can be presented by A and a choice of lifts from G, with some specially chosen relations.

Here are some basic observations realizing this idea. We start by lifting a single element of G.

Lemma 89. Let A be a G-module, and let

$$1 \to A \to \mathcal{E} \xrightarrow{\pi} G \to 1$$

denote a group extension. Further, fix some $\sigma \in G$ of order n_σ, and find $F \in \mathcal{E}$ such that $\sigma \coloneqq \pi(F)$. Then

$$\alpha \coloneqq F^{n_\sigma}$$

has $\alpha \in A^{\langle\sigma\rangle}$.

Proof. A priori, we only know that $\alpha \in \mathcal{E}$, so we compute

$$\pi(\alpha) = \pi\left(F^{n_\sigma}\right) = \sigma^{n_\sigma} = 1,$$

so $\alpha \in \ker \pi = A$. Thus, we may say that

$$\sigma(\alpha) = F\alpha F^{-1} = F^{n_\sigma} = \alpha,$$

so $\alpha \in A^{\langle\sigma\rangle}$, as desired. ∎

We can make the above proof more explicit by specifying the group law of $\mathcal{E}$.

Lemma 90. Let A be a G-module. Picking up some 2-cocycle $c \in Z^2(G, A)$, let

$$1 \to A \to \mathcal{E}_c \xrightarrow{\pi} G \to 1$$

be the corresponding extension. Fixing $\sigma \in G$ of order n_σ, let $F \coloneqq (m, \sigma) \in \mathcal{E}_c$ be a lift. Supposing $c(1, \sigma) = 1$, then

$$\alpha \coloneqq F^{n_\sigma} = N_\sigma(m) \prod_{i=0}^{n_\sigma - 1} c\left(\sigma^i, \sigma\right),$$

where $N_\sigma \coloneqq \sum_{i=0}^{n_\sigma - 1} \sigma^i$.

Proof. This is a direct computation. By induction, we can show that

$$F^k = \left(\prod_{i=0}^{k-1} \sigma^i(m) c\left(\sigma^i, \sigma\right), \sigma^k \right)$$

for $k \in \mathbb{N}$. Indeed, there is nothing to say for $k = 0$, and the inductive step merely expands out $F^k \cdot F$.

It follows that

$$\alpha = F^{n_\sigma} = \left(\prod_{i=0}^{n_\sigma - 1} \sigma^i(m) \cdot \prod_{i=0}^{n_\sigma - 1} c\left(\sigma^i, \sigma\right), 1 \right),$$

which is what we wanted. ∎

Having this explicit formula lets us say how α changes as we vary the lift.

Proposition 91. Let A be a G-module. Fixing a cohomology class $u \in H^2(G, A)$, let

$$1 \to A \to \mathcal{E} \xrightarrow{\pi} G \to 1$$

be a group extension whose isomorphism class corresponds to u. Further, fix some $\sigma \in G$ of order n_σ, and let $A_\sigma \coloneqq A^{\langle \sigma \rangle}$ be the fixed submodule. Then the set

$$S_{\mathcal{E},\sigma} \coloneqq \{F^{n_\sigma} : \pi(F) = \sigma\}$$

is an equivalence class in $A_\sigma / N_\sigma(A)$, independent of the choice of $\mathcal{E}$, where $N_\sigma \coloneqq \sum_{i=1}^{n_\sigma - 1} \sigma^i$.

Proof. Note that $S_{\mathcal{E},\sigma} \subseteq A_\sigma$ already from Lemma 89.

The point is to use Lemma 90. Note the extension $\mathcal{E}$ corresponds to the equivalence class $u \in H^2(G, A)$, so let $c \in Z^2(G, A)$ be a representative. Letting $\mathcal{E}_c$ be the extension constructed from c, we are promised an isomorphism $\varphi \colon \mathcal{E} \cong \mathcal{E}_c$ making the following diagram commute.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A & \longrightarrow & \mathcal{E} & \xrightarrow{\pi} & G & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle \varphi} & & \| & & \\
1 & \longrightarrow & A & \longrightarrow & \mathcal{E}_c & \xrightarrow{\pi_c} & G & \longrightarrow & 1
\end{array}$$

We start by claiming that $S_{\mathcal{E},\sigma} = S_{\mathcal{E}_c,\sigma}$, which will show that $S_{\mathcal{E},\sigma}$ is independent of the choice of representative $\mathcal{E}$. To show $S_{\mathcal{E},\sigma} \subseteq S_{\mathcal{E}_c,\sigma}$, note that $\alpha \in S_{\mathcal{E},\sigma}$ has $F \in \mathcal{E}$ with $\pi(F) = \sigma$ and $\alpha = F^{n_\sigma}$. Pushing this through φ, we see $\varphi(F) \in \mathcal{E}_c$ has

$$\pi_c(\varphi(F)) = \varphi(\pi(F)) = \sigma \qquad \text{and} \qquad \varphi(F)^{n_\sigma} = \varphi(F^{n_\sigma}) = \alpha,$$

so $\alpha \in S_{\mathcal{E}_c,\sigma}$ follows. An analogous argument with φ^{-1} shows the other needed inclusion.

It thus suffices to show that $S_{\mathcal{E}_c,\sigma}$ is an equivalence class in $A_\sigma / N_\sigma(A)$. However, this is exactly what Lemma 90 says as we let the possible lifts $F = (m, \sigma) \in \mathcal{E}_c$ of σ vary over $m \in A$. ∎

The fact that we are taking elements of G to equivalence classes in $A_\sigma/N_\sigma(A)$ is reminiscent of the (inverse) Artin reciprocity map, and indeed that is exactly what is going on.

Corollary 92. Work in the context of Proposition 91. Then

$$S_\sigma \coloneqq S_{\mathcal{E},\sigma} = [\sigma] \cup [\operatorname{Res} c],$$

where $\cup\colon \widehat{H}^{-2}(\langle\sigma\rangle, \mathbb{Z}) \times \widehat{H}^2(\langle\sigma\rangle, A) \to \widehat{H}^0(\langle\sigma\rangle, A)$ is the cup product in Tate cohomology.

Proof. Note that $S_\sigma \in A_\sigma/N_\sigma(A) = \widehat{H}^0(\langle\sigma\rangle, A)$, so the conclusion at least makes sense.

Now, using notation as in the proof of Proposition 91, we recall that $S_\sigma = S_{\mathcal{E}_c,\sigma}$, so it suffices to prove the result for $\mathcal{E}_c$. Well, by Lemma 90, S_σ is represented by

$$\prod_{i=0}^{n_\sigma - 1} c\left(\sigma^i, \sigma\right),$$

which is exactly the cup product $[\sigma] \cup [c]$. ∎

Corollary 93. Let L/K be a finite Galois extension of local fields with Galois group $G \coloneqq \operatorname{Gal}(L/K)$. Further, let

$$1 \to L^\times \to \mathcal{E} \xrightarrow{\pi} G \to 1$$

be an L/K-gerb bound by $\mathbb{G}_m$ whose isomorphism class corresponds to the fundamental class $u_{L/K} \in H^2(G, L^\times)$. Further, fix some $\sigma \in G$ of order n_σ, and let $L_\sigma \coloneqq L^{\langle\sigma\rangle}$ be the fixed field. Then

$$\theta^{-1}_{L/L_\sigma}(\sigma) = \left\{F^{n_\sigma} : \pi(F) = \sigma\right\}.$$

Proof. Recalling θ^{-1}_{L/L_σ} is a cup product map, note that $\theta^{-1}_{L/L_\sigma}(\sigma)$ is given by $[\sigma] \cup u_{L/K}$. So we are done by Corollary 92. ∎

The above results are all interested in lifting single elements of G and studying how they behave on their own. In the discussion that follows, we will need to study how the lifts interact with each other, but for now, we will justify why lifts are adequate to study as follows.

Proposition 94. Let A be a G-module. Further, let

$$1 \to A \to \mathcal{E} \xrightarrow{\pi} G \to 1$$

be a group extension. Given elements Σ which generate G, then $\mathcal{E}$ is generated by A and a set of lifts $\{F_\sigma\}_{\sigma\in\Sigma}$ with $\pi(F_\sigma) = \sigma$ for each $\sigma \in \Sigma$.

Proof. Fix some element $w \in \mathcal{E}$, which we need to exhibit as a product of elements in A and F_σs. Well, because the $\sigma \in \Sigma$ generate G, we know that $\pi(w) \in G$ can be written as

$$\pi(w) = \prod_{\sigma\in\Sigma}^{m} \sigma^{a_\sigma}$$

for some sequence of integers $\{a_\sigma\}_{\sigma\in\Sigma} \in \mathbb{N}^{\oplus\Sigma}$. It follows that

$$\pi\left(\frac{w}{\prod_{\sigma\in\Sigma} F_\sigma^{a_\sigma}}\right) = 1,$$

so $w/\prod_{\sigma\in\Sigma} F_\sigma^{a_\sigma} = \ker\pi = A$. Thus, we can find some $a \in A$ such that

$$w = a \cdot \prod_{\sigma\in\Sigma} F_\sigma^{a_\sigma},$$

which is what we wanted. ∎

4.2 Tuple Data

The results from subsection 4.1 are very focused on single elements, which are only enough when our group G is cyclic. Our goal will be to be able to cover all abelian groups, so if we want to keep track of the fact our group is abelian, we should extract the elements of A which can do so.

Lemma 95 ([AS78, Lemma 1.2])**.** Let A be a G-module, and let

$$1 \to A \to \mathcal{E} \xrightarrow{\pi} G \to 1$$

be a group extension. Further, fix some $F_1, F_2 \in \mathcal{E}$ and define $\sigma_i \coloneqq \pi(F_i)$ for $i \in \{1,2\}$, and let $\sigma_i \in G$ have order n_i. Then, setting

$$\alpha_i \coloneqq F_i^{n_i} \qquad \text{and} \qquad \beta \coloneqq F_1F_2F_1^{-1}F_2^{-1},$$

we have the following.

(a) $\alpha_i \in A^{\langle\sigma_i\rangle}$ for $i \in \{1,2\}$ and $\beta \in A$.

(b) $N_1(\beta) = \alpha_1/\sigma_2(\alpha_1)$ and $N_2(\beta^{-1}) = \alpha_2/\sigma_1(\alpha_2)$, where $N_i \coloneqq \sum_{p=0}^{n_i-1}\sigma_i^p$.

Proof. These checks are a matter of force. For brevity, we set $A_i \coloneqq A^{\langle\sigma_i\rangle}$ for $i \in \{1,2\}$.

(a) That $\alpha_i \in A_i$ follows from Lemma 89. Lastly, $\beta \in A$ follows from noting

$$\pi(\beta) = \pi(F_1)\pi(F_2)\pi(F_1)^{-1}\pi(F_2)^{-1} = 1,$$

so $\beta \in \ker\pi = A$.

(b) We will check that $\mathrm{N}_{L/L_1}(\beta) = \alpha_1/\sigma_2(\alpha_1)$; the other equality follows symmetrically after switching 1s and 2s because $\beta^{-1} = F_2F_1F_2^{-1}F_1^{-1}$. Well, we compute

$$\begin{aligned}
N_1(\beta) &= \sigma_1^{-1}(\beta)\cdot\sigma_1^{-2}(\beta)\cdot\sigma^{-3}\cdot\ldots\cdot\sigma^{-n_1}(\beta)\\
&= F_1^{-1}\left(F_1F_2F_1^{-1}F_2^{-1}\right)F_1\\
&\quad\cdot F_1^{-2}\left(F_1F_2F_1^{-1}F_2^{-1}\right)F_1^2\\
&\quad\cdot F_1^{-3}\left(F_1F_2F_1^{-1}F_2^{-1}\right)F_1^3\cdot\ldots\\
&\quad\cdot F_1^{-n_1}(F_1F_2F_1^{-1}F_2^{-1})F_1^{n_1}\\
&= F_2F_1^{-1}\\
&\quad\cdot F_1^{-1}\\
&\quad\cdot F_1^{-1}\cdot\ldots\\
&\quad\cdot F_1^{-1}F_2^{-1}F_1^{n_1}\\
&= F_2F_1^{-n_1}F_2^{-1}F_1^{n_1}\\
&= \alpha_1/\sigma_2(\alpha_1).
\end{aligned}$$

The above computations finish the proof. ∎

The proof of (b) above might appear magical, but in fact it comes from a more general idea.

Lemma 96 ([AS78, Lemma 1.1(b)])**.** Fix everything as in Lemma 95. Then, for $x, y \geq 0$, we have

$$F_1^x F_2^y = \prod_{k=0}^{x-1} \prod_{\ell=0}^{y-1} \sigma_1^k \sigma_2^\ell(\beta) F_2^y F_1^x.$$

Proof. We induct. We take a moment to write out the case of $x = 1$, for which we induct on y. To be explicit, we will prove

$$F_1 F_2^y = \prod_{\ell=0}^{y-1} \sigma_2^\ell(\beta) F_2^y F_1.$$

For $y = 0$, there is nothing to say. So suppose the statement for y (and $x = 1$), and we show $y+1$ (and $x = 1$). Well, we compute

$$\begin{aligned}
F_1 F_2^{y+1} &= F_1 F_2^y \cdot F_2 \\
&= \prod_{\ell=0}^{y-1} \sigma_2^\ell(\beta) F_2^y F_1 \cdot F_2 \\
&= \prod_{\ell=0}^{y-1} \sigma_2^\ell(\beta) F_2^y \beta F_2 F_1 \\
&= \prod_{\ell=0}^{y-1} \sigma_2^\ell(\beta) \cdot \sigma_2^y(\beta) F_2^y \cdot F_2 F_1 \\
&= \prod_{\ell=0}^{(y+1)-1} \sigma_2^\ell(\beta) \cdot F_2^{y+1} F_1,
\end{aligned}$$

which is what we wanted.

We now move on to the general case. We will induct on y. Note that $y = 0$ makes the product empty, leaving us with $F_1^x = F_1^x$, for any x. So suppose that the statement is true for some $y \geq 0$, and we will show $y + 1$. For this, we now turn to inducting on x. For $x = 0$, we note that the product is once again empty, so we are left with showing $F_2^{y+1} = F_2^{y+1}$, which is true.

To finish, we suppose the statement for x and show the statement for $x + 1$. Well, we compute

$$\begin{aligned}
F_1^{x+1} F_2^{y+1} &= F_1 \cdot F_1^x F_2^{y+1} \\
&= F_1 \cdot \prod_{k=0}^{x-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k \sigma_2^\ell(\beta) \cdot F_2^{y+1} F_1^x \\
&= \sigma_1 \left(\prod_{k=0}^{x-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k \sigma_2^\ell(\beta) \right) \cdot F_1 F_2^{y+1} F_1^x \\
&= \prod_{k=1}^{(x+1)-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k \sigma_2^\ell(\beta) \cdot F_1 F_2^{y+1} F_1^x \\
&= \prod_{k=1}^{(x+1)-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k \sigma_2^\ell(\beta) \cdot \prod_{\ell=0}^{(y+1)-1} \sigma_2^\ell(\beta) \cdot \sigma_2^y(\beta) \cdot F_2^{y+1} F_1 \cdot F_1^x \\
&= \prod_{k=0}^{(x+1)-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k \sigma_2^\ell(\beta) F_2^{y+1} F_1^{x+1},
\end{aligned}$$

which is what we wanted. ∎

Remark 97. Setting $x = n_1$ and $y = 1$ recovers $\mathrm{N}_{L/L^{\langle\sigma_1\rangle}}(\beta) = \alpha_1/\sigma_2(\alpha_1)$.

In particular, Remark 97 tells us that coherence of the group law in $\mathcal{E}$ should give rise to relations between our elements of A. Here is a more complex example.

Lemma 98 ([AS78, Lemma 1.2])**.** Let A be a G-module, and let

$$1 \to A \to \mathcal{E} \xrightarrow{\pi} G \to 1$$

be a group extension. Further, fix some $F_1, F_2, F_3 \in \mathcal{E}$ and define $\sigma_i \coloneqq \pi(F_i)$ for $i \in \{1, 2, 3\}$, and let $\sigma_i \in G$ have order n_i. Then, setting

$$\beta_{ij} \coloneqq F_i F_j F_i^{-1} F_j^{-1}$$

for each pair of indices (i, j) with $i > j$. Then

$$\frac{\sigma_2(\beta_{31})}{\beta_{31}} = \frac{\sigma_1(\beta_{32})}{\beta_{32}} \cdot \frac{\sigma_3(\beta_{21})}{\beta_{21}}.$$

Proof. The point is to turn $F_3F_2F_1$ into $F_1F_2F_3$ in two different ways. On one hand,

$$\begin{aligned}(F_3F_2)F_1 &= \beta_{32}F_2F_3F_1\\ &= \beta_{32}F_2\beta_{31}F_1F_3\\ &= \beta_{32}\sigma_2(\beta_{31})(F_2F_1)F_3\\ &= \beta_{32}\sigma_2(\beta_{31})\beta_{21}F_1F_2F_3.\end{aligned}$$

On the other hand,

$$\begin{aligned}F_3(F_2F_1) &= F_3\beta_{21}F_1F_2\\ &= \sigma_3(\beta_{21})(F_3F_1)F_2\\ &= \sigma_3(\beta_{21})\beta_{31}F_1(F_3F_2)\\ &= \sigma_3(\beta_{21})\beta_{31}F_1\beta_{32}F_2F_3\\ &= \sigma_3(\beta_{21})\beta_{31}\sigma_1(\beta_{32})F_1F_2F_3.\end{aligned}$$

Thus,

$$\beta_{32}\sigma_2(\beta_{31})\beta_{21} = \sigma_3(\beta_{21})\beta_{31}\sigma_1(\beta_{32}),$$

which rearranges into the desired equation. ∎

Remark 99. The relation from Lemma 98 may look asymmetric in the β_{ij}, but this is because the definitions of the β_{ij}s themselves are asymmetric in F_i.

Remark 100. So far we have mostly been able to recover the results from subsection 4.1 beyond working with just a single $\sigma \in G$ and αs to be able to work with lots of group elements in G and some βs. We have not built an analogue for Corollary 92, though we will explain that it is possible to do so much later in Remark 147.

4.3 Tuples to Cocycles

4.3.1 The Set-Up

The proceeding lemmas Lemma 95 and Lemma 98 is intended to give intuition that the element β is helping to specify the group law on $\mathcal{E}$.

More concretely, we will take the following set-up for the following results: fix a G-module A, and let

$$1 \to A \to \mathcal{E} \to G \to 1$$

be a group extension. Once we choose elements $\{\sigma_i\}_{i=1}^m$ generating G, we know by Proposition 94 that we can generate $\mathcal{E}$ by A and some arbitrarily chosen lifts $\{F_i\}_{i=1}^m$ of the $\{\sigma_i\}_{i=1}^m$. Then, letting n_i be the order of σ_i, we set

$$\alpha_i \coloneqq F_i^{n_i}$$

for each index i and

$$\beta_{ij} \coloneqq F_i F_j F_i^{-1} F_j^{-1}$$

for each index $1 \leq j, i \leq m$. Notably, it suffices to only work with $j < i$: indeed, $\beta_{ii} = 1$ and $\beta_{ij} = \beta_{ji}^{-1}$ for any i and j. Setting $A_i \coloneqq A^{\langle \sigma_i \rangle}$ and $N_i \coloneqq \sum_{p=0}^{n_i - 1} \sigma_i^p$, the story so far is that

$$\alpha_i \in A_i \text{ for each } i \qquad \text{and} \qquad \beta_{ij} \in A \text{ for each } i > j \tag{4.1}$$

and

$$N_i(\beta_{ij}) = \alpha_i / \sigma_j(\alpha_i) \qquad \text{and} \qquad N_j(\beta_{ij}^{-1}) = \alpha_j / \sigma_i(\alpha_j) \qquad \text{for each } i > j \tag{4.2}$$

by Lemma 95, and

$$\frac{\sigma_j(\beta_{ik})}{\beta_{ik}} = \frac{\sigma_k(\beta_{ij})}{\beta_{ij}} \cdot \frac{\sigma_i(\beta_{jk})}{\beta_{jk}} \qquad \text{for each } i > j > k \tag{4.3}$$

by Lemma 98. This data is so important that we will give it a name.

Definition 101. In the above set-up, the data of $(\{\alpha_i\}, \{\beta_{ij}\})$ satisfying (4.1) and (4.2) and (4.3) will be called a $\{\sigma_i\}_{i=1}^m$-*tuple*. When understood, the $\{\sigma_i\}_{i=1}^m$ will be abbreviated. Once G and A are fixed, we will denote the set of $\{\sigma_i\}_{i=1}^m$-tuples by $\mathcal{T}(G, A)$.

Note that this definition is independent of $\mathcal{E}$, but a choice of extension $\mathcal{E}$ and lifts F_i give a $\{\sigma_i\}_{i=1}^m$-tuple as described above.

Remark 102. The $\mathcal{T}(G, A)$ form a group under multiplication in A. Indeed, the conditions (4.1) and (4.2) and (4.3) are closed under multiplication and inversion.

We also know from Lemma 96 that

$$F_i^x F_j^y = \prod_{k=0}^{x-1} \prod_{\ell=0}^{y-1} \sigma_i^k \sigma_j^\ell(\beta_{ij}) F_j^y F_i^x$$

for $i > j$ and $x, y \geq 0$. It will be helpful to have some notation for the residue term in A, so we define

$$\sigma^{(x)} \coloneqq \sum_{i=0}^{x-1} \sigma^i$$

so that we can write

$$\sigma_i^{(x)} \sigma_j^{(y)} \beta_{ij} = \prod_{k=0}^{x-1} \prod_{\ell=0}^{y-1} \sigma_i^k \sigma_j^\ell(\beta_{ij}).$$

Now, combined with the fact that $F_i x = \sigma_i(x) F_i$ for each F_i and $x \in A$, we have been approximately told how the group operation works in $\mathcal{E}$. Namely, we could conceivably write any element of $\mathcal{E}$ in the form

$$x F_1^{a_1} \cdots F_m^{a_m}$$

for $x \in A$ and $a_i \in \mathbb{Z}/n_i\mathbb{Z}$ because we know how to make these elements commute and generate $\mathcal{E}$. Further, we can multiply out two terms of the form

$$x F_1^{a_1} \cdots F_m^{a_m} \cdot y F_1^{b_1} \cdots F_m^{b_m}$$

into a term of the form $z F_1^{c_1} \cdots F_m^{c_m}$. In fact, it will be helpful for us to see how to do this.

Proposition 103. Fix everything as in the set-up, except drop the assumption that $\{\sigma_i\}_{i=1}^m$ generate G. Then, choosing $a_i, b_i \in \mathbb{N}$ for each i, we have

$$\left(\prod_{i=1}^m F_i^{a_i}\right)\left(\prod_{i=1}^m F_i^{b_i}\right) = \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left(\prod_{i=1}^m F_i^{a_i+b_i}\right).$$

Proof. The reason that we dropped the assumption on $\{\sigma_i\}_{i=1}^m$ is so that we may induct directly on m. We start by showing that

$$\left(\prod_{i=1}^m F_i^{a_i}\right)F_1^{b_1} = \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_1^{(b_1)}\beta_{i1}\right]F_1^{a_1+b_1}\prod_{i=2}^m F_i^{a_i}.$$

We do this by induction on m. When $m = 0$ and even for $m = 1$, there is nothing to say. For the inductive step, we assume

$$\left(\prod_{i=1}^m F_i^{a_i}\right)F_1^{b_1} = \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_1^{(b_1)}\beta_{i1}\right]F_1^{a_1+b_1}\prod_{i=2}^m F_i^{a_i}$$

and compute

$$\begin{aligned}
\left(\prod_{i=1}^{m+1} F_i^{a_i}\right)F_1^{b_1} &= \left(\prod_{i=1}^m F_i^{a_i}\right)F_{m+1}^{a_{m+1}}F_1^{b_1}\\
&= \left(\prod_{i=1}^m F_i^{a_i}\right)\sigma_{m+1}^{(a_{m+1})}\sigma_1^{(b_1)}\beta_{m+1,1}F_1^{b_1}F_{m+1}^{a_{m+1}}\\
&= \left[\left(\prod_{k=1}^m \sigma_k^{a_k}\right)\sigma_{m+1}^{(a_{m+1})}\sigma_1^{(b_1)}\beta_{m+1,1}\right]\left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_1^{(b_1)}\beta_{i1}\right]\cdot\\
&\quad F_1^{a_1+b_1}\left(\prod_{i=2}^m F_i^{a_i}\right)F_{m+1}^{a_{m+1}}\\
&= \left[\prod_{1<i\le m+1}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_1^{(b_1)}\beta_{i1}\right]F_1^{a_1+b_1}\left(\prod_{i=2}^{m+1} F_i^{a_i}\right),
\end{aligned}$$

which completes our inductive step.

We now attack the statement of the proposition directly, again inducting on m. For $m = 0$ and even for $m = 1$, there is again nothing to say. For the inductive step, take $m > 1$, and we get to assume that

$$\left(\prod_{i=2}^m F_i^{a_i}\right)\left(\prod_{i=2}^m F_i^{b_i}\right) = \left[\prod_{2\le j<i\le m}\left(\prod_{2\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left(\prod_{i=2}^m F_i^{a_i+b_i}\right).$$

From here, we can compute

$$\begin{aligned}
\left(\prod_{i=1}^m F_i^{a_i}\right)\left(\prod_{i=1}^m F_i^{b_i}\right) &= \left(\prod_{i=1}^m F_i^{a_i}\right) F_1^{b_1} \left(\prod_{i=2}^m F_i^{b_i}\right) \\
&= \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_1^{(b_1)}\beta_{i1}\right] F_1^{a_1+b_1}\left(\prod_{i=2}^m F_i^{a_i}\right)\left(\prod_{i=2}^m F_i^{b_i}\right) \\
&= \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_1^{(b_1)}\beta_{i1}\right] F_1^{a_1+b_1}\cdot \\
&\qquad \left[\prod_{2\le j<i\le m}\left(\prod_{2\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left(\prod_{i=2}^m F_i^{a_i+b_i}\right) \\
&= \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_1^{(b_1)}\beta_{i1}\right]\cdot \\
&\qquad \sigma_1^{a_1+b_1}\left[\prod_{2\le j<i\le m}\left(\prod_{2\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left(\prod_{i=2}^m F_i^{a_i+b_i}\right).
\end{aligned}$$

From here, a little rearrangement finishes the inductive step. ∎

The reason we exerted this pain upon ourselves is for the following result.

Proposition 104. Fix everything as in the set-up. Then, if well-defined, we can represent the cohomology class corresponding to $\mathcal{E}$ by the cocycle

$$c(g,h) \coloneqq \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left[\prod_{i=1}^m\left(\prod_{1\le k<i}\sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right],$$

where $g=\prod_i \sigma_i^{a_i}$ and $h=\prod_i \sigma_i^{b_i}$.

Observe that Proposition 104 has a fairly strong hypothesis that c is well-defined; we will return to this later.

Proof. Very quickly, we use the division algorithm to define

$$a_i+b_i = n_iq_i+r_i$$

where $q_i\in\{0,1\}$ and $0\le r_i<n_i$. In particular,

$$gh=\prod_{i=1}^m F_i^{r_i}.$$

Now, because the elements σ_i generate G, we see that the lifts $\sigma_i\mapsto F_i$ defines a section $s\colon G\to\mathcal{E}$. As such, we can compute a representing cocycle for our cohomology class as

$$\begin{aligned}
c(g,h) &= s(g)s(h)s(gh)^{-1} \\
&= \left(\prod_{i=1}^m F_i^{a_i}\right)\left(\prod_{i=1}^m F_i^{b_i}\right)\left(\prod_{i=1}^m F_i^{r_i}\right)^{-1} \\
&= \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left(\prod_{i=1}^m F_i^{a_i+b_i}\right)\left(\prod_{i=1}^m F_{m-i+1}^{-r_{m-i+1}}\right).
\end{aligned}$$

It remains to deal with the last products; we claim that it is equal to

$$\left(\prod_{i=1}^{m} F_i^{a_i+b_i}\right)\left(\prod_{i=1}^{m} F_{m-i+1}^{-r_{m-i+1}}\right) = \prod_{i=1}^{m}\left(\prod_{1\le k<i} \sigma_k^{a_k+b_k}\right)\alpha_i^{q_i},$$

which will finish the proof. We induct on m; for $m = 0$ and $m = 1$, there is nothing to say. For the inductive step, we assume that

$$\left(\prod_{i=2}^{m} F_i^{a_i+b_i}\right)\left(\prod_{i=1}^{m-1} F_{m-i+1}^{-r_{m-i+1}}\right) = \prod_{i=2}^{m}\left(\prod_{2\le k<i} \sigma_k^{a_k+b_k}\right)\alpha_i^{q_i}$$

and compute

$$\begin{aligned}
\left(\prod_{i=1}^{m} F_i^{a_i+b_i}\right)\left(\prod_{i=1}^{m} F_{m-i+1}^{-r_{m-i+1}}\right) &= F_1^{a_1+b_1}\left(\prod_{i=2}^{m} F_i^{a_i+b_i}\right)\left(\prod_{i=1}^{m-1} F_{m-i+1}^{-r_{m-i+1}}\right) F_1^{-a_1-b_1} F_1^{a_1+b_1-r_1} \\
&= F_1^{a_1+b_1}\left(\prod_{i=2}^{m}\left(\prod_{2\le k<i} \sigma_k^{a_k+b_k}\right)\alpha_i^{q_i}\right) F_1^{-a_1-b_1}\alpha_1^{q_1} \\
&= \left(\prod_{i=2}^{m}\left(\prod_{1\le k<i} \sigma_k^{a_k+b_k}\right)\alpha_i^{q_i}\right)\alpha_1^{q_1} \\
&= \prod_{i=1}^{m}\left(\prod_{1\le k<i} \sigma_k^{a_k+b_k}\right)\alpha_i^{q_i},
\end{aligned}$$

finishing. ■

4.3.2 The Modified Set-Up

A priori we have no reason to expect that the c constructed in Proposition 104 is actually a cocycle, especially if the σ_i have nontrivial relations.

To account for this, we modify our set-up slightly. By the classification of finitely generated abelian groups, we may write

$$G \simeq \bigoplus_{k=1}^{m} G_k,$$

where $G_k \subseteq G$ with $G_k \cong \mathbb{Z}/n_k\mathbb{Z}$ and $n_k > 1$ for each n_k. As such, we let σ_k be a generating element of G_k so that we still know that the σ_k generate G. In this case, we have the following result.

Theorem 105 ([AS78, Theorem 1.3])**.** Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Then a $\{\sigma_i\}_{i=1}^m$-tuple of $\{\alpha_i\}_{i=1}^m$ and $\{\beta_{ij}\}_{i>j}$ makes

$$c(g,h) \coloneqq \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j} \sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i} \sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left[\prod_{i=1}^{m}\left(\prod_{1\le k<i} \sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor \frac{a_i+b_i}{n_i}\right\rfloor}\right],$$

where $g \coloneqq \prod_i \sigma_i^{a_i}$ with $h \coloneqq \prod_i \sigma_j^{a_j}$ and $0 \le a_i, b_i < n_i$, into a cocycle in $Z^2(G, A)$.

Proof. Note that c is now surely well-defined because the elements g and h have unique representations as described. Anyway, we relegate the direct cocycle check to Appendix A because it is long, annoying, and unenlightening. We will also present an alternative proof in Theorem 129, using more abstract theory. ■

Observe that the above construction has now completely forgotten about $\mathcal{E}$! Namely, we have managed to go from tuples straight to cocycles; this is theoretically good because it will allow us to go fully in reverse: we will be able to start with a tuple, build the corresponding cocycle, from which the extension arises. However, equivalence classes of cocycles give the "same" extension, so we will also need to give equivalence classes for tuples as well.

4.4 Building Tuples

We continue in the modified set-up of the previous section. There is already an established way to get from a cocycle to an extension, which means that it should be possible to go straight from the cocycle to a $\{\sigma_i\}_{i=1}^m$-tuple. Again, it will be beneficial to write this out.

Lemma 106. Fix everything as in the modified set-up, but suppose that $\mathcal{E} = \mathcal{E}_c$ is the extension generated from a cocycle $c \in Z^2(G, A)$. Then, if $F_i = (x_i, \sigma_i)$ are our lifts, we have

$$\alpha_i = N_i(x_i) \cdot \prod_{k=0}^{n_i-1} c\left(\sigma_i^k, \sigma_i\right) \qquad \text{and} \qquad \beta_{ij} = \frac{x_i}{\sigma_j(x_i)} \cdot \frac{\sigma_i(x_j)}{x_j} \cdot \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)}$$

for each α_i and β_{ij}.

Proof. The equality for the α_i follow from Lemma 90. For the equality about β_{ij}, we simply compute by brute force, writing

$$\begin{aligned} F_iF_j &= (x_i \cdot \sigma_i x_j \cdot c(\sigma_i, \sigma_j), \sigma_i\sigma_j) \\ F_jF_i &= (x_j \cdot \sigma_j x_i \cdot c(\sigma_j, \sigma_i), \sigma_j\sigma_i) \\ (F_jF_i)^{-1} &= \left((\sigma_j\sigma_i)^{-1}(x_j \cdot \sigma_j x_i \cdot c(\sigma_j, \sigma_i))^{-1}, \sigma_i^{-1}\sigma_j^{-1}\right), \end{aligned}$$

which gives

$$\begin{aligned} \beta_{ij} &= (F_iF_j)(F_jF_i)^{-1} \\ &= \left(\frac{x_i}{\sigma_j x_i} \cdot \frac{\sigma_i x_j}{x_j} \cdot \frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)}, 1\right), \end{aligned}$$

finishing. ∎

Here is a nice sanity check that we are doing things in the right setting: not only can we build tuples from extensions, but we can find an extension corresponding to any tuple.

Corollary 107. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Given any $\{\sigma_i\}_{i=1}^m$-tuple of $\{\alpha_i\}_{i=1}^m$ and $\{\beta_{ij}\}_{i>j}$, there exists an extension $\mathcal{E}$ and lifts F_i of the σ_i so that

$$\alpha_i = F_i^{n_i} \qquad \text{and} \qquad \beta_{ij} = F_iF_jF_i^{-1}F_j^{-1}.$$

Proof. From Theorem 105, we may build the cocycle $c \in Z^2(G, A)$ defined by

$$c(g,h) \coloneqq \left[\prod_{1\le j<i\le m} \left(\prod_{1\le k<j} \sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i} \sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left[\prod_{i=1}^m \left(\prod_{1\le k<i} \sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor \frac{a_i+b_i}{n_i}\right\rfloor}\right], \tag{4.4}$$

where $g \coloneqq \prod_i F_i^{a_i}$ and $h \coloneqq \prod_i F_j^{a_j}$ and $0 \le a_i, b_i < n_i$. As such, we use $\mathcal{E} \coloneqq \mathcal{E}_c$ to be the corresponding extension and $F_i \coloneqq (1, \sigma_i)$ as our lifts. We have the following checks.

- To show $\alpha_i = F_i^{n_i}$, we use Lemma 106 to compute $F_i^{n_i}$, which means we want to compute

$$\prod_{k=0}^{n_i-1} c\left(\sigma_i^k, \sigma_i\right).$$

  Well, plugging $c\left(\sigma_i^k, \sigma_i\right)$ into (4.4), we note that all $\beta_{k\ell}^{(a_k b_\ell)}$ terms vanish (either $a_k = 0$ or $b_\ell = 0$ for each $k \neq \ell$), so the big left product completely vanishes.

  As for the right product, the only term we have to worry about is

$$\left(\prod_{1\leq k<i} \sigma_k^{0+0}\right)\alpha_i^{\left\lfloor \frac{k+1}{n_i}\right\rfloor},$$

  which is equal to 1 when $k \leq n_i - 1$ and α_i when $k = n_i - 1$. As such, we do indeed have $\alpha_i = F_i^{n_i}$.

- To show $\beta_{ij} = F_i F_j F_i^{-1} F_j^{-1}$ for $i > j$, we again use Lemma 106 to compute $F_i F_j F_i^{-1} F_j^{-1}$, which means we want to compute

$$\frac{c(\sigma_i, \sigma_j)}{c(\sigma_j, \sigma_i)}.$$

  Plugging into (4.4) once more, there is no way to make $\lfloor (a_k + b_k)/n_k \rfloor$ nonzero (recall we set $n_k > 1$ for each k) in either $c(\sigma_i, \sigma_j)$ or $c(\sigma_j, \sigma_i)$. As such, the right-hand product term disappears.

  As for the left product, we note that it still vanishes for $c(\sigma_j, \sigma_i)$ because $i > j$ implies that either $a_k = 0$ or $b_\ell = 0$ for each $k > \ell$. However, for $c(\sigma_i, \sigma_j)$, we do have $a_i = 1$ and $b_j = 1$ only, so we have to deal with exactly the term

$$\left(\prod_{1\leq k<j} \sigma_k^{a_k+b_k}\right)\left(\prod_{j\leq k<i} \sigma_k^{a_k}\right)\beta_{ij}.$$

  With $i > j$ and $a_k = b_k = 0$ for $k \notin \{i, j\}$, we see that the product of all the σ_ks will disappear, indeed only leaving us with β_{ij}.

The above computations complete the proof. ■

And here is our first taste of (partial) classification.

Corollary 108. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Then the formula of Theorem 105 and the formulae of Lemma 106 (setting $x_i = 1$ for each i) are homomorphisms of abelian groups between tuples in $\mathcal{T}(G, A)$ and cocycles in $Z^2(G, A)$. In fact, the formula of Theorem 105 is a section of the formulae of Lemma 106.

Proof. The formulae in Theorem 105 and Lemma 106 are both large products in their inputs, so they are multiplicative (i.e., homomorphisms). It remains to check that we have a section. Well, starting with a $\{\sigma_i\}_{i=1}^m$-tuple and building the corresponding cocycle c by Theorem 105, the proof of Corollary 107 shows that the formulae of Lemma 106 recovers the correct $\{\sigma_i\}_{i=1}^m$-tuple. ■

4.5 Equivalence Classes of Tuples

We continue in the modified set-up. We would like to make Corollary 108 into a proper isomorphism of abelian groups, but this is not feasible; for example, the cocycle c generated by Theorem 105 will always have $c(\sigma_j, \sigma_i) = 1$ for $i > j$, which is not true of all cocycles in $Z^2(G, A)$.

However, we did have a notion that the data of a $\{\sigma_i\}_{i=1}^m$ should be enough to specify the group law of the extension that the tuple comes from, so we do expect to be able to define all extensions—and hence achieve all cohomology classes—from a specially chosen $\{\sigma_i\}_{i=1}^m$-tuple.

To make this precise, we want to define an equivalence relation on tuples which go to the same cohomology class and then show that the map Theorem 105 is surjective on these equivalence classes. The correct equivalence relation is taken from Lemma 106.

Definition 109. Fix everything as in the modified set-up. We say that two $\{\sigma_i\}_{i=1}^m$-tuples $(\{\alpha_i\},\{\beta_{ij}\})$ and $(\{\alpha_i'\},\{\beta_{ij}'\})$ are *equivalent* if and only if there exist elements $x_1,\dots,x_m \in A$ such that

$$\alpha_i = N_i(x_i)\cdot\alpha_i' \qquad \text{and} \qquad \beta_{ij} = \frac{x_i}{\sigma_j(x_i)}\cdot\frac{\sigma_i(x_j)}{x_j}\cdot\beta_{ij}'$$

for each α_i and β_{ij}. We may notate this by $(\{\alpha_i\},\{\beta_{ij}\}) \sim (\{\alpha_i'\},\{\beta_{ij}'\})$.

Remark 110. It is not too hard to see directly from the definition that this is in fact an equivalence relation. In fact, the set of tuples equivalent to the "trivial" tuple of all 1s is closed under multiplication (and inversion) and hence forms a subgroup of $\mathcal{T}(G,A)$. As such, the set of equivalence classes forms a quotient group of $\mathcal{T}(G,A)$. We will denote this quotient group by $\overline{\mathcal{T}}(G,A)$.

This notion of equivalence can be seen to be the correct one in the sense that it correctly generalizes Proposition 91.

Proposition 111 ([AS78, Theorem 1.4])**.** Fix everything as in the modified set-up with an extension $\mathcal{E}$. As the lifts F_i change, the corresponding values of

$$\alpha_i \coloneqq F_i^{n_i} \qquad \text{and} \qquad \beta_{ij} \coloneqq F_iF_jF_i^{-1}F_j^{-1}$$

go through a full equivalence class of $\{\sigma_i\}_{i=1}^m$-tuples.

Proof. We proceed as in Proposition 91. Given an extension $\mathcal{E}'$, let $S_{\mathcal{E}'}$ be the set of $\{\sigma_i\}_{i=1}^m$-tuples generated as the lifts F_i change. We start by showing that an isomorphism $\varphi\colon \mathcal{E}\cong\mathcal{E}'$ of extensions implies that $S_{\mathcal{E}} = S_{\mathcal{E}'}$; by symmetry, it will be enough for $S_{\mathcal{E}} \subseteq S_{\mathcal{E}'}$. The isomorphism induces the following diagram.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \mathcal{E} & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle\varphi} & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & \mathcal{E}' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

To show that $S_{\mathcal{E}} \subseteq S_{\mathcal{E}'}$, pick up some $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\},\{\beta_{ij}\})$ generated from lifts $F_i \in \mathcal{E}$ (i.e., $\pi(F_i)=\sigma_i$), where

$$\alpha_i \coloneqq F_i^{n_i} \qquad \text{and} \qquad \beta_{ij} \coloneqq F_iF_jF_i^{-1}F_j^{-1}.$$

Now, we note that $F_i' \coloneqq \varphi(F_i)$ will have

$$\pi(F_i') = \pi(\varphi(F_i)) = \varphi(\pi(F_i)) = \sigma_i$$

by the commutativity of the diagram, so the F_i' are lifts of the σ_i. Further, we see that

$$(F_i')^{n_i} = \varphi(F_i)^{n_i} = \varphi\left(F_i^{n_i}\right) = \varphi(\alpha_i) = \alpha_i$$

for each i, and

$$F_i'F_j'(F_i')^{-1}(F_j')^{-1} = \varphi\left(F_iF_jF_i^{-1}F_j^{-1}\right) = \varphi(\beta_{ij}) = \beta_{ij}$$

for each $i>j$. Thus, $(\{\alpha_i\},\{\beta_{ij}\})$ is a $\{\sigma_i\}_{i=1}^m$-tuple generated by lifts from $\mathcal{E}'$, implying that $(\{\alpha_i\},\{\beta_{ij}\}) \in S_{\mathcal{E}'}$.

It now suffices to show the statement in the proposition for a specific extension isomorphic to $\mathcal{E}$. Well, the isomorphism class of $\mathcal{E}$ corresponds to some cohomology class in $H^2(G,A)$, for which we let c be a representative; then $\mathcal{E}\simeq\mathcal{E}_c$, so we may show the statement for $\mathcal{E}\coloneqq\mathcal{E}_c$. Indeed, as the lifts $F_i=(x_i,\sigma_i)$ change, we know by Lemma 106 that

$$\alpha_i = N_i(x_i)\cdot\prod_{k=0}^{n_i-1} c\left(\sigma_i^k,\sigma_i\right) \qquad \text{and} \qquad \beta_{ij} = \frac{x_i}{\sigma_j(x_i)}\cdot\frac{\sigma_i(x_j)}{x_j}\cdot\frac{c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)}$$

for each α_i and β_{ij}. All of these live in the same equivalence class by definition of the equivalence, and as the x_i are allowed to vary over all of A, they will fill up that equivalence class fully. This finishes. ■

We are now ready to upgrade our section.

Corollary 112. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Fixing a cohomology class $[c] \in H^2(G, A)$, the set of $\{\sigma_i\}_{i=1}^m$-tuples which correspond to $[c]$ (via Theorem 105) forms exactly one equivalence class.

Proof. We show that two tuples are equivalent if and only if their corresponding cocycles (via Theorem 105) to the same cohomology class, which will be enough.

In one direction, suppose $(\{\alpha_i\}, \{\beta_{ij}\}) \sim (\{\alpha_i'\}, \{\beta_{ij}'\})$. By Corollary 107, we can find an extension $\mathcal{E}$ which gives $(\{\alpha_i\}, \{\beta_{ij}\})$ by choosing an appropriate set of lifts. By Proposition 111, we see that $(\{\alpha_i'\}, \{\beta_{ij}'\})$ must also come from choosing an appropriate set of lifts in $\mathcal{E}$. However, the cocycles in $Z^2(G, A)$ generated by Theorem 105 from our two tuples now both represent the isomorphism class of $\mathcal{E}$ by Proposition 104, so these cocycles belong to the same cohomology class.

In the other direction, name the cocycles corresponding to $(\{\alpha_i\}, \{\beta_{ij}\})$ and $(\{\alpha_i'\}, \{\beta_{ij}'\})$ by c and c' respectively, and suppose $[c] = [c']$. Then $\mathcal{E}_c \cong \mathcal{E}_{c'}$ as extensions, but we know by the proof of Corollary 107 that $(\{\alpha_i\}, \{\beta_{ij}\})$ comes from choosing lifts of $\mathcal{E}_c$ and similar for $(\{\alpha_i'\}, \{\beta_{ij}'\})$. In particular, because $\mathcal{E}_c \cong \mathcal{E}_{c'}$, we know that $(\{\alpha_i'\}, \{\beta_{ij}'\})$ will also come from choosing some lifts in $\mathcal{E}_c$ (recall the proof of Proposition 111), so $(\{\alpha_i\}, \{\beta_{ij}\}) \sim (\{\alpha_i'\}, \{\beta_{ij}'\})$ follows. ■

Theorem 113. The maps described in Corollary 108 descend to an isomorphism of abelian groups between the equivalence classes in $\overline{\mathcal{T}}(G, A)$ and cohomology classes in $H^2(G, A)$.

Proof. The fact that the maps are well-defined (in both directions) and hence injective is Corollary 112. The fact that we had a section from tuples to cocycles implies that the map from cocycles to tuples was also surjective. Thus, we have a bona fide isomorphism. ■

4.6 Classification of Extensions

We remark that we are now able to classify all extensions up to isomorphism, in some sense. At a high level, an isomorphism class of extensions corresponds to a particular cohomology class in $H^2(G, A)$, so choosing a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$ corresponding to this class, we can write out a representative of this cocycle by Theorem 105, properly corresponding to the original extension by Proposition 104.

In fact, the cocycle in Proposition 104 is generated by the description of the group law in Proposition 103, and the entire computation only needed to use the following relations, for the appropriate choice of lifts F_i.

(a) $F_i x = \sigma_i(x) F_i$ for each i and $x \in A$.

(b) $F_i^{n_i} = \alpha_i$ for each i.

(c) $F_i F_j F_i^{-1} F_j^{-1} = \beta_{ij}$ for each $i > j$; i.e., $F_i F_j = \beta_{ij} F_j F_i$.

As such, the above relations fully describe the extension because they also specify the cocycle, and we know that this cocycle is well-defined. We summarize this discussion into the following theorem.

Theorem 114. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Further, fix a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\},\{\beta_{ij}\})$, and define the group $\mathcal{E}(\{\alpha_i\},\{\beta_{ij}\})$ as being generated by A and elements $\{F_i\}_{i=1}^n$ having the following relations.

(a) $F_i x = \sigma_i(x) F_i$ for each i and $x \in A$.

(b) $F_i^{n_i} = \alpha_i$ for each i.

(c) $F_i F_j = \beta_{ij} F_j F_i$ for each $i > j$.

Then the natural embedding $A \hookrightarrow \mathcal{E}(\{\alpha_i\},\{\beta_{ij}\})$ and projection $\pi\colon \mathcal{E}(\{\alpha_i\},\{\beta_{ij}\}) \twoheadrightarrow G$ by $F_i \mapsto \sigma_i$ makes $\mathcal{E}(\{\alpha_i\},\{\beta_{ij}\})$ into an extension. In fact, all extensions are isomorphic to some $\mathcal{E}(\{\alpha_i\},\{\beta_{ij}\})$.

Proof. This follows from the preceding discussion, though we will provide a few more words in this proof. The exactness of

$$1 \to A \to \mathcal{E}(\{\alpha_i\},\{\beta_{ij}\}) \xrightarrow{\pi} G \to 1$$

follows quickly. Further, the action of conjugation of $\mathcal{E}$ on A corresponds correctly to the G-action by (a). So we do indeed have an extension.

It remains to show that all extensions are isomorphic to one of this type. Well, note that Proposition 103 and Proposition 104 use only the above relations to write down a cocycle representing the isomorphism class of $\mathcal{E}(\{\alpha_i\},\{\beta_{ij}\})$, and it is the cocycle corresponding to the $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\},\{\beta_{ij}\})$ itself as described in Theorem 105.

However, we know that as the equivalence class of $(\{\alpha_i\},\{\beta_{ij}\})$ changes, we will hit all cohomology classes in $H^2(G,A)$ by Theorem 113. Thus, because every extension is represented by some cohomology class, every extension will be isomorphic to some $\mathcal{E}(\{\alpha_i\},\{\beta_{ij}\})$. This completes the proof. ∎

4.7 Change of Group

We continue in the modified set-up, but we will no longer need access to an extension $\mathcal{E}$. In this subsection, we are interested in what happens to tuples when the cocycle operations of $\mathrm{Inf}\colon H^2\left(G/H, A^H\right) \to H^2(G,A)$ and $\mathrm{Res}\colon H^2(G,A) \to H^2(H,A)$ are applied, where $H \subseteq G$ is some subgroup.

In general, this is difficult because the structure of a subgroup $H \subseteq G$ might not be particularly amenable to forming a tuple from a tuple in G. More concretely, H might have generators which look very different from those of G. However, it will be enough for our purposes to restrict our attention to the subgroups of the form

$$H = \langle \sigma_1^{d_1}, \dots, \sigma_m^{d_m} \rangle,$$

where the $\{d_i\}_{i=1}^m$ are some positive integers with $d_i \mid n_i$ for each i. With that said, here are our computations. We begin with inflation.

Lemma 115. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Further, let $H \coloneqq \langle \sigma_1^{d_1}, \dots, \sigma_m^{d_m} \rangle$ be a subgroup with $d_\bullet \mid n_\bullet$, and let $\overline{\sigma}_i$ be the image of σ_i in G/H. Consider the inflation map $\mathrm{Inf}\colon H^2\left(G/H, A^H\right) \to H^2(G,A)$.

If the cocycle $\overline{c} \in Z^2\left(G/H, A^H\right)$ gives the $\{\overline{\sigma}_i\}_{i=1}^m$-tuple $(\{\overline{\alpha}_i\},\{\overline{\beta}_{ij}\})$ (by Corollary 108), then the cocycle $\mathrm{Inf}\,\overline{c} \in Z^2(G,A)$ gives the $\{\sigma_i\}_{i=1}^m$-tuple

$$\mathrm{Inf}(\{\overline{\alpha}_i\},\{\overline{\beta}_{ij}\}) \coloneqq (\{\alpha_i\},\{\beta_{ij}\}) = \left(\left\{\overline{\alpha}_i^{n_i/d_i}\right\}, \{\overline{\beta}_{ij}\}\right).$$

Proof. The point is to use the explicit formulae for the α_i and β_{ij} of Lemma 106.

More explicitly, the map of Corollary 108 tells us that we can compute the tuple for $\operatorname{Inf}\overline{c}$ by using our explicit formulae for α_i and β_{ij} on the 2-cocycle $\operatorname{Inf}\overline{c} \in Z^2(G,A)$. For some α_i, the computation is

$$\begin{aligned}\alpha_i &= \prod_{k=0}^{n_i-1} (\operatorname{Inf}\overline{c})\left(\sigma_i^k, \sigma_i\right) \\ &= \prod_{k=0}^{n_i-1} \overline{c}\left(\overline{\sigma}_i^k, \overline{\sigma}_i\right) \\ &= \left(\prod_{k=0}^{d_i-1} \overline{c}\left(\overline{\sigma}_i^k, \overline{\sigma}_i\right)\right)^{n_i/d_i}\end{aligned}$$

where the last equality is because $\overline{\sigma}_i^{d_i} = 1$ in G/H. In fact, d_i is the order of $\overline{\sigma}_i$, so the product is just $\overline{\alpha}_i$ by Lemma 106 and how we defined $\overline{\alpha}_i$. It follows

$$\alpha_i = \overline{\alpha}_i^{n_i/d_i}.$$

Continuing, for some β_{ij}, we have

$$\begin{aligned}\beta_{ij} &= \frac{(\operatorname{Inf}\overline{c})(\sigma_i,\sigma_j)}{(\operatorname{Inf}\overline{c})(\sigma_j,\sigma_i)} \\ &= \frac{\overline{c}(\overline{\sigma}_i,\overline{\sigma}_j)}{\overline{c}(\overline{\sigma}_j,\overline{\sigma}_i)} \\ &= \overline{\beta}_{ij},\end{aligned}$$

where the last equality is by how we defined $\overline{\beta}_{ij}$. These computations complete the proof. ■

Remark 116. We can also the statement of Lemma 115 as asserting that the diagram

$$\begin{array}{ccc} Z^2\left(G/H, A^H\right) & \xrightarrow{\operatorname{Inf}} & Z^2(G,A) \\ \downarrow & & \downarrow \\ \mathcal{T}\left(G/H, A^H\right) & \xrightarrow{\operatorname{Inf}} & \mathcal{T}(G,A) \end{array}$$

commutes, where the vertical morphisms are from Corollary 108.

Remark 117. In light of the fact that the cohomology class of some $\operatorname{Inf}\overline{c} \in Z^2(G,A)$ is only defined up to the cohomology class of $\overline{c} \in Z^2\left(G/H, A^H\right)$, changing an input tuple $(\{\overline{\alpha}_i\},\{\overline{\beta}_{ij}\}) \in \mathcal{T}\left(G/H, A^H\right)$ up to equivalence will not change the cohomology class of the associated cocycle in $\overline{c} \in Z^2\left(G/H, A^H\right)$ and hence will not change the cohomology class of $\operatorname{Inf}\overline{c}$ nor the equivalence class of $\operatorname{Inf}(\{\overline{\alpha}_i\},\{\overline{\beta}_{ij}\}) \in \mathcal{T}(G,A)$. All this is to say that we have a well-defined map

$$\operatorname{Inf}\colon \overline{\mathcal{T}}\left(G/H, A^H\right) \to \overline{\mathcal{T}}(G,A)$$

and commutative diagram

$$\begin{array}{ccc} \overline{\mathcal{T}}\left(G/H, A^H\right) & \xrightarrow{\operatorname{Inf}} & \overline{\mathcal{T}}(G,A) \\ \downarrow & & \downarrow \\ H^2\left(G/H, A^H\right) & \xrightarrow{\operatorname{Inf}} & H^2(G,A) \end{array}$$

induced by modding out from Remark 116.

Restriction is similar.

Lemma 118. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Further, let $H \coloneqq \langle \sigma_1^{d_1}, \dots, \sigma_m^{d_m} \rangle$ be a subgroup with $d_\bullet \mid n_\bullet$. Consider the restriction map $\mathrm{Res}\colon H^2(G,A) \to H^2(H,A)$.

If the cohomology class $[c] \in H^2(G,A)$ is represented by the $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$, then the cohomology class $[\mathrm{Res}\, \overline{c}]$ is represented by the $\{\sigma_i^{d_i}\}_{i=1}^m$-tuple

$$(\{\overline{\alpha}_i\}, \{\overline{\beta}_{ij}\}) = \left(\left\{ \alpha_i^{1_{d_i = n_i}} \right\}, \left\{ \sigma_i^{(d_i 1_{n_i = d_i})} \sigma_j^{(d_j 1_{n_j = d_j})} \beta_{ij} \right\} \right).$$

Proof. As in the previous proof, we will simply define c by Theorem 105, and we will use the formulae of Lemma 106 to retrieve the $\{\sigma_i^{d_i}\}$-tuple for $\mathrm{Res}\, c$. Indeed, we compute

$$\begin{aligned}
\overline{\alpha}_i &= \prod_{k=0}^{n_i/d_i - 1} (\mathrm{Res}\, c)\left(\sigma_i^{d_i k}, \sigma_i^{d_i}\right) \\
&= \prod_{k=0}^{n_i/d_i - 1} c\left(\sigma_i^{d_i k}, \sigma_i^{d_i}\right) \\
&= \prod_{k=0}^{n_i/d_i - 1} \alpha_i^{\lfloor d_i (k+1)/n_i \rfloor},
\end{aligned}$$

where in the last equality we have used the construction of c. Now, if $n_i = d_i$, and the product is empty, and we get 1; otherwise, the last term of the product $k = n_i/d_i - 1$ is the only term which does not return 1, and it returns α_i. So this matches the claimed $\alpha_i^{1_{n_i = d_i}}$.

Continuing, we compute

$$\begin{aligned}
\overline{\beta}_{ij} &= \frac{(\mathrm{Res}\, c)\left(\sigma_i^{d_i}, \sigma_j^{d_j}\right)}{(\mathrm{Res}\, c)\left(\sigma_j^{d_j}, \sigma_i^{d_i}\right)} \\
&= \frac{c\left(\sigma_i^{d_i}, \sigma_j^{d_j}\right)}{c\left(\sigma_j^{d_j}, \sigma_i^{d_i}\right)} \\
&= c\left(\sigma_i^{d_i}, \sigma_j^{d_j}\right),
\end{aligned}$$

where in the last step we have used the construction of c. Now, if $n_i = d_i$ or $n_i = d_j$, then we are computing $c\left(1, \sigma_j^{d_j}\right)$ or $c\left(\sigma_i^{d_i}, 1\right)$, which are both 1, as needed. Otherwise, $d_i < n_i$ and $d_j < n_j$, so

$$\overline{\beta}_{ij} = \beta_{ij}^{(d_i d_j)},$$

which again is as claimed. ∎

Thankfully, we will really only care about inflation in the following discussion, but we will say that there are analogues of Remark 116 and Remark 117.

4.8 Profinite Groups

In this subsection, we will use our results on change of group to extend our results a little to allow profinite groups. As such, we will want to slightly modify our set-up; we will call the following set-up the "profinite set-up."

Let $\mathcal{I}$ be a poset category such that any pair of elements has an upper bound (i.e., a directed set), and let the functor $G_\bullet\colon \mathcal{I}^{\mathrm{op}} \to \mathrm{FinAbGrp}$ be an inverse system of finite abelian groups. These will create a profinite group

$$G \coloneqq \varprojlim_{i \in \mathcal{I}} G_i.$$

In order to be able to apply our theory, we will assume that G is a finite direct sum of procyclic groups as

$$G \simeq \bigoplus_{k=1}^{m} \overline{\langle \sigma_k \rangle}$$

for some elements $\{\sigma_k\}_{k=1}^m \subseteq G$. Further, we will require that the kernel N_i of the map $G \twoheadrightarrow G_i$ to take the form

$$N_i \coloneqq \overline{\left\langle \sigma_1^{d_{i,1}}, \dots, \sigma_m^{d_{i,m}} \right\rangle}$$

in such a way that $\langle \sigma_k N_i \rangle$ has order $d_{i,k}$. In short, our restriction on the N_i will allow our inflation maps to be computable in the sense of Lemma 115. We quickly remark that, because the topology on G is the coarsest one making the projections $G \twoheadrightarrow G_i$ continuous, the subsets $\{N_i\}_{i \in \mathcal{I}}$ give a fundamental system of open neighborhoods around the identity.

Remark 119. Of course, one could also start with G being a finite direct sum of procyclic groups and then define the N_i and G_i accordingly. We have chosen the above approach because in application one might only have access to select G_is, and it is not obvious how to choose these from such a "top-down" approach.

Example 120. To show that we are still allowing interesting groups, we can set

$$G_{m,\nu} \coloneqq \operatorname{Gal}\left(\mathbb{Q}_p(\zeta_{p^m-1})\mathbb{Q}_p(\zeta_{p^\nu})/\mathbb{Q}_p\right) \simeq \operatorname{Gal}\left(\mathbb{Q}_p(\zeta_{p^m-1})/\mathbb{Q}_p\right) \oplus \operatorname{Gal}\left(\mathbb{Q}_p(\zeta_{p^\nu})/\mathbb{Q}_p\right),$$

which becomes $G = \operatorname{Gal}\left(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p\right) \simeq \widehat{\mathbb{Z}} \oplus \mathbb{Z}_p^\times$ upon taking the inverse limit. It is not very hard to check that the kernels are generated correctly; for example, when p is odd, we have $\mathbb{Z}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p$, and under our isomorphisms, we will have

$$\operatorname{Gal}\left(\mathbb{Q}(\zeta_{p^\nu})/\mathbb{Q}_p\right) \simeq \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p/p^{\nu-1}\mathbb{Z}_p,$$

so the kernel of $G \twoheadrightarrow G_{m,\nu}$ is $m\widehat{\mathbb{Z}} \oplus (\mathbb{Z}/(p-1)\mathbb{Z})^{1_{\nu=0}} \oplus p^{\nu-1}\mathbb{Z}_p$.

Remark 121. I'm not sure if such an explicit construction can be extended to other local fields K (say, via Lubin–Tate theory). Because $K^\times$ is not topologically finitely generated when K is in positive characteristic (see for example [Neu99, Proposition II.5.7]) such a construction must do something subtle.

Let A be a discrete G-module. The main goal of this subsection is to be able to provide a notion of a "compatible system" of tuples from each individual $H^2(G_i, A)$ to be able to exactly describe an element of $H^2(G, A)$. To effect this, we have the following somewhat annoying checks.

Lemma 122. Suppose that $\mathcal{P}$ is a directed set, and let $\mathcal{P}' \subseteq \mathcal{P}$ be a subcategory such that any $x \in \mathcal{P}$ has some $x' \in \mathcal{P}'$ such that $x \leq x'$. Then, given a functor $F \colon \mathcal{P} \to \mathcal{C}$, we have

$$\varinjlim_{\mathcal{P}} F \simeq \varinjlim_{\mathcal{P}'} F,$$

provided that both colimits exist.

Proof. For concreteness, if $x \leq y$ in $\mathcal{P}$, we will let $f_{yx} \colon x \to y$ be the corresponding morphism; in particular, $x \leq y \leq z$ has $f_{zx} = f_{zy} f_{yx}$. Now, for brevity, set

$$X \coloneqq \varinjlim_{\mathcal{P}} F \qquad \text{and} \qquad X' \coloneqq \varinjlim_{\mathcal{P}'} F.$$

By the Yoneda lemma, it suffices to fix some object $Y \in \mathcal{C}$ and show that $\mathrm{Mor}_{\mathcal{C}}(X, Y) \simeq \mathrm{Mor}_{\mathcal{C}}(X', Y)$. Well, morphsims $X \to Y$ are in (natural) bijection with cones under F with nadir Y, and morphisms $X' \to Y$ are in (natural) bijection with cones under $F' \coloneqq F|_{\mathcal{P}'}$ with nadir Y.

Thus, it suffices to give a natural bijection between cones under F with nadir Y and cones under F' with nadir Y. Well, given a cone under F with nadir Y, we can simply restrict it to $\mathcal{P}'$ to get a cone under F'. In the other direction, given a cone under F' with nadir Y, we can build a cone under F with nadir Y as follows; let $\varphi_{x'} \colon F(x') \to Y$ for $x' \in \mathcal{P}'$ be the corresponding morphisms in our cone.

For any $x \in \mathcal{P}$, find $x' \in \mathcal{P}'$ such that $x \le x'$. Then set

$$\varphi_x \coloneqq \varphi_{x'} \circ f_{x'x}$$

Note that φ_x is in fact independent of our choice of x': if $x \le x'_1$ and $x \le x'_2$, then because $\mathcal{P}$ is a directed set, we can find $y \in \mathcal{P}$ such that $x'_1, x'_2 \le y$ and then $y' \in \mathcal{P}'$ with $y \le y'$. Then

$$\begin{aligned} \varphi_{x'_\bullet} \circ f_{x'_\bullet x} &= \varphi_{y'} \circ f_{y'x'_\bullet} \circ f_{x'_\bullet x} \\ &= \varphi_{y'} \circ f_{y'x} \end{aligned}$$

for $x'_\bullet \in \{x'_1, x'_2\}$. Anyway, we can check that the morphisms φ do assemble to a cone under F': if $x \le y$ in $\mathcal{P}$, then find $y' \in \mathcal{P}$ with $x \le y \le y'$, and we compute

$$\begin{aligned} \varphi_y \circ f_{yx} &= \varphi_{y'} \circ f_{y'y} \circ f_{yx} \\ &= \varphi_{y'} \circ f_{y'x} \\ &= \varphi_x. \end{aligned}$$

Thus, we do have a natural, well-defined map sending cones under F' with nadir Y to cones under F with nadir Y. It is not too hard to see that these maps are inverse to each other (for example, the cone under F', extended to F, does indeed restrict back to F' properly), which completes the proof. ∎

Remark 123. One can remove the hypothesis that the colimits exist and use essentially the same proof.

Proposition 124. Fix everything as in the profinite set-up. Then, given a discrete G-module A,

$$H^2(G, A) \simeq \varinjlim_{i \in \mathcal{I}} H^2\left(G_i, A^{N_i}\right).$$

Here, the morphisms between the collection of $H^2\left(G_i, A^{N_i}\right)$ are induced by inflation: if $i \to j$ in $\mathcal{I}$, then $G_j \to G_i$ in $\mathrm{FinAbGrp}$, giving an inflation map $\mathrm{Inf} \colon H^2\left(G_i, A^{N_i}\right) \to H^2\left(G_j, A^{N_j}\right)$.

Proof. Let $\mathcal{N}$ be the poset category of open normal subgroups of G, reverse ordered under inclusion; i.e., $N_1 \subseteq N_2$ in G induces a map $N_2 \to N_1$. Then it is already known that

$$H^2(G, A) \simeq \varinjlim_{N \in \mathcal{N}} H^2\left(G/N, A^N\right).$$

On the other hand, observe that $i \le j$ in $\mathcal{I}$ induces $G_j \to G_i$, so $N_j \subseteq N_i$. In other words, $i \mapsto N_i$ will define a functor $\mathcal{I} \to \mathcal{N}$; functoriality follows because $\mathcal{I}$ and $\mathcal{N}$ are poset categories. Letting $\mathcal{N}'$ denote the image of $\mathcal{I}$ in $\mathcal{N}$, we see

$$\varinjlim_{i \in \mathcal{I}} H^2\left(G_i, A^{N_i}\right) \simeq \varinjlim_{N \in \mathcal{N}'} H^2\left(G/N, A^N\right).$$

Notably, the inflation maps $\mathrm{Inf} \colon H^2\left(G_i, A^{N_i}\right) \to H^2\left(G_j, A^{N_j}\right)$ when $i \le j$ become the inflation maps $\mathrm{Inf} \colon H^2\left(G/N, A^N\right) \to H^2\left(G/N', A^{N'}\right)$ when $N' \subseteq N$. So if we let $F \colon \mathcal{N} \to \mathrm{AbGrp}$ be the functor taking N to $H^2\left(G/N, A^N\right)$ (and $N \subseteq N'$ to the inflation map), we are trying to show

$$\varinjlim_{\mathcal{N}} F = \varinjlim_{\mathcal{N}'} F.$$

For this, we use Lemma 122. Indeed, for a given open normal subgroup $N \in \mathcal{N}$, we need to find some $N' \in \mathcal{N}'$ such that $N \leq N'$, which means $N' \subseteq N$.

However, the elements of $\mathcal{N}'$ are the collection $\{N_i\}_{i\in\mathcal{I}}$, which form a fundamental system of open neighborhoods around the identity. Thus, the fact that N is an open set containing the identity implies there is some $N_i \in \mathcal{N}'$ such that $N_i \subseteq N$. This finishes the proof. ■

Observe that the above proofs did not use the extra hypotheses on G nor N_i to be products of procyclic groups. We use these hypotheses now. To work more concretely, we note that any $i \in \mathcal{I}$ has

$$G_i \simeq \frac{G}{N_i} \simeq \bigoplus_{p=1}^{m} \overline{\langle\sigma_p\rangle}/\overline{\langle\sigma_p^{d_{i,p}}\rangle} \simeq \bigoplus_{p=1}^{m} \langle\sigma_p\rangle/\langle\sigma_p^{d_{i,p}}\rangle \subseteq \bigoplus_{p=1}^{m} \mathbb{Z}/d_{i,p}\mathbb{Z}$$

is a finite abelian group generated by the elements $\sigma_p N_i$. By choosing the $d_{i,p}$ appropriately, recall that we also forced the order of $\sigma_p N_i$ to be $d_{i,p}$.

Regardless, the main point is that, given a discrete G-module A, we can consider the $\{\sigma_p N_i\}_{p=1}^m$-tuples $\mathcal{T}\left(G_i, A^{N_i}\right)$. Now, as discussed above, $i \leq j$ in $\mathcal{I}$ induces a quotient map $G_j \simeq G/N_j \twoheadrightarrow G/N_i \simeq G_i$. From this, we have the following coherence check.

Lemma 125. Fix everything as in the profinite set-up, and let A be a discrete G-module. Then, given $i \leq j \leq k$ in $\mathcal{I}$, the diagram

$$\begin{array}{ccc} \mathcal{T}\left(G_i, A^{N_i}\right) & \xrightarrow{\text{Inf}} & \mathcal{T}\left(G_j, A^{N_j}\right) \\ & \searrow^{\text{Inf}} & \downarrow{\scriptstyle \text{Inf}} \\ & & \mathcal{T}\left(G_k, A^{N_k}\right) \end{array}$$

commutes. Here, the Inf maps are defined as in Lemma 115.

Proof. For each $i \in \mathcal{I}$, we let $n_{i,p}$ denote the order of $\sigma_p N_i \in G_i$. Using the definition of Inf from Lemma 115, we just pick up some $\{\sigma_p N_p\}_{p=1}^m$-tuple $(\{\alpha_p\}, \{\beta_{pq}\})$-tuple in $\mathcal{T}\left(G_i, A^{N_i}\right)$ and track through the diagram as follows.

$$\begin{array}{ccc} (\{\alpha_p\}, \{\beta_{pq}\}) & \xrightarrow{\qquad\text{Inf}\qquad} & \left(\{\alpha_p^{d_{j,p}/d_{i,p}}\}, \{\beta_{pq}\}\right) \\ {\scriptstyle \text{Inf}}\downarrow & & \downarrow{\scriptstyle \text{Inf}} \\ \left(\{\alpha_p^{1_{d_{k,p}=d_{i,p}} d_{k,p}/d_{i,p}}\}, \{\beta_{pq}\}\right) & = & \left(\{\alpha_p^{(1_{d_{j,p}=d_{i,p}} d_{j,p}/d_{i,p})(1_{d_{k,p}=d_{j,p}} d_{k,p}/d_{j,p})}\}, \{\beta_{pq}\}\right) \end{array}$$

Notably, $d_{k,p} = d_{i,p}$ implies that these are both equal to $d_{j,p}$ because $i \leq j \leq k$ upon tracking the order of σ_p through our morphisms $G_k \to G_j \to G_i$. This completes the proof. ■

And here is the result.

Theorem 126. Fix everything as in the profinite set-up, and let A be a discrete G-module. Then the isomorphisms of Theorem 113 upgrade into an isomorphism

$$H^2(G, A) \simeq \varinjlim_{i\in\mathcal{I}} \overline{\mathcal{T}}\left(G_i, A^{N_i}\right).$$

Here the morphisms between the $\overline{\mathcal{T}}\left(G_i, A^{N_i}\right)$ are inflation maps of Lemma 115.

Proof. Note that the objects $\overline{\mathcal{T}}\left(G_i, A^{N_i}\right)$ do make a directed system over $\mathcal{I}$ because of the commutativity of Lemma 125. Namely, the lemma checks that $\mathcal{I} \to \mathrm{AbGrp}$ by $i \mapsto \overline{\mathcal{T}}\left(G_i, A^{N_i}\right)$ is actually functorial;

technically we must also check that the maps $\overline{\mathcal{T}}\left(G_i, A^{N_i}\right) \to \overline{\mathcal{T}}\left(G_i, A^{N_i}\right)$ are the identity, but this follows from the definition.

Now, by Proposition 124, we have

$$H^2(G, A) \simeq \varinjlim_{i \in \mathcal{I}} H^2\left(G_i, A^{N_i}\right),$$

but now the natural isomorphism induced by Remark 117 induces an isomorphism of direct limits

$$\varinjlim_{i \in \mathcal{I}} H^2\left(G_i, A^{N_i}\right) \simeq \varinjlim_{i \in \mathcal{I}} \overline{\mathcal{T}}\left(G_i, A^{N_i}\right)$$

given by the isomorphism of Theorem 113 acting pointwise. This completes the proof. ■

Because there are reasonably explicit descriptions of direct limits of abelian groups, and we already have an explicit description of each $\overline{\mathcal{T}}\left(G_i, A^{N_i}\right)$ term in addition to a description of the inflation maps between them, we will be content with our sufficiently explicit description of $H^2(G, A)$. So we call it done here.

5 Tuples as Encoding Modules

The story from section 4 was able to encode a cohomology class in $H^2(G, A)$ into a (somewhat complex) tuple of elements in A. This mirrors the introductory comments from section 3, so we will spend this section connecting the two stories.

5.1 Set-Up and Overview

The approach here will be to attempt to abstract our data away from the G-module A as much as possible. To set up our discussion, we continue with

$$G \simeq \bigoplus_{i=1}^{m} G_i,$$

where $G_i = \langle \sigma_i \rangle \subseteq G$ and σ_i has order n_i. These variables allow us to define

$$T_i \coloneqq (\sigma_i - 1) \qquad \text{and} \qquad N_i \coloneqq \sum_{p=0}^{n_i - 1} \sigma_i^p$$

for each index i. In fact, it will be helpful to continue to use the notation

$$\sigma^{(a)} \coloneqq \sum_{p=0}^{a-1} \sigma^p$$

for any $\sigma \in G$ and nonnegative integer $a \geq 0$; in particular, $\sigma^{(0)} = 0$ and $\sigma_i^{(n_i)} = N_i$. The main benefits to this notation will be the facts that

$$\sigma^{(a+b)} = \sigma^{(a)} + \sigma^a \sigma^{(b)} \qquad \text{and} \qquad \sigma_i^a = T_i \sigma_i^{(a)} + 1,$$

which can be seen by direct expansion. Given $g \in \prod_{p=1}^{n} \sigma_p^{a_p}$, we will also define the notation

$$g_{(i)} \coloneqq \prod_{p=1}^{i-1} \sigma_p^{a_p}$$

for $i \geq 0$. In particular $g_{(0)} = g_{(1)} = 1$ and $g_{(m+1)} = g$.[1]

[1] We are using a subscript here because we are more or less taking a subsequence of g.

The key to our discussion will be the magical map $\mathcal{F}\colon \mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}} \to \mathbb{Z}[G]^m$ defined by

$$\mathcal{F}\colon \left((x_i)_{i=1}^m, (y_{ij})_{i>j}\right) \mapsto \left(x_i N_i - \sum_{j=1}^{i-1} y_{ij} T_j + \sum_{j=i+1}^{m} y_{ji} T_j\right)_{i=1}^m.$$

This is of course a G-module homomorphism. We will go ahead and state the main results we will prove. Roughly speaking, $\mathcal{F}$ is manufactured to make the following result true.

Proposition 127. Fix everything as in the set-up. Then the function

$$\overline{c}(g) \coloneqq \left(g_{(i)} \sigma_i^{(a_i)}\right)_{i=1}^m,$$

where $g \coloneqq \prod_{i=1}^m \sigma_i^{a_i}$ with $0 \le a_i < n_i$ for each i, is a 1-cocycle in $Z^1(G, \operatorname{coker} \mathcal{F})$.

The reason we care about this cocycle is that we can pass it through a boundary morphism induced by the short exact sequence

$$0 \to \underbrace{\frac{\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}}{\ker \mathcal{F}}}_{X \coloneqq} \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0,$$

so we have a 2-cocycle $\delta(\overline{c}) \in Z^2(G, X)$; in fact, we will be able to explicitly compute $\delta(\overline{c})$ as a result of the proof of Proposition 127.

Only now will we bring in tuples. The first result provides an alternate description of tuples.

Proposition 128. Fix everything as in the set-up, and now let A be a G-module. Then $\{\sigma_i\}_{i=1}^m$-tuples are canonically isomorphic to $\operatorname{Hom}_{\mathbb{Z}[G]}(X, A) = H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))$.

The second result brings in the last ingredient, the cup product.

Theorem 129. Fix everything as in the set-up. Also, fix a G-module A and a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$. Observe there is a natural cup product map

$$\cup\colon H^2(G, X) \times H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \to H^2(G, A).$$

Then, using the isomorphism of Proposition 128, the cocycle defined in Theorem 105 is simply the output of $\delta(\overline{c}) \cup (\{\alpha_i\}, \{\beta_{ij}\})$ on cocycles.

Because we know that the cup product sends cocycles to cocycles, this will show that the cocycle of Theorem 105 is in fact well-defined. More importantly, X will be a 2-encoding module.

5.2 Preliminary Work

We continue in the set-up of the previous subsection. Before jumping into any hard logic, we define some (more) notation which will be useful later on as well. First, in $\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}$, we define

$$\kappa_p \coloneqq \left((1_{i=p})_i, (0)_{i>j}\right) \qquad \text{and} \qquad \lambda_{pq} \coloneqq \left((0)_i, (1_{(i,j)=(p,q)})_{i>j}\right)$$

for all relevant indices p and q so that the κ_p and λ_{pq} are a basis for $\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}$ as a $\mathbb{Z}[G]$-module. Secondly, we define

$$\varepsilon_p \coloneqq (1_{i=p})_{i=1}^m \in \mathbb{Z}[G]^m$$

for all indices p, again giving a basis for $\mathbb{Z}[G]^m$ as a $\mathbb{Z}[G]$-module. For example, this notation lets us write

$$\mathcal{F}\left(\sum_{i=1}^m x_i \kappa_i + \sum_{i>j} y_{ij} \lambda_{ij}\right) = \sum_{i=1}^m x_i N_i \varepsilon_i + \sum_{i>j} y_{ij} (T_i \varepsilon_j - T_j \varepsilon_i), \tag{5.1}$$

and

$$\overline{c}(g) = \sum_{i=1}^{m} g_i \sigma_i^{(a_i)} \varepsilon_i$$

where $g \coloneqq \prod_{i=1}^{m} \sigma_i^{a_i}$.

Additionally, so that we do not need to interrupt our discussion later, we establish a few lemmas which will aide our proof of Proposition 127.

Lemma 130. Fix everything as in the set-up. For any set of distinct indices $\{i_1, \dots, i_k\} \subseteq \{1, \dots, m\}$, we have

$$\bigcap_{p=1}^{k} \operatorname{im} N_{i_p} = \operatorname{im} \prod_{p=1}^{k} N_{i_p},$$

where we are identifying $x \in \mathbb{Z}[G]$ with its associated multiplication map $x \colon \mathbb{Z}[G] \to \mathbb{Z}[G]$.

Proof. The point is that the elements of $\bigcap_{p=1}^{k} \operatorname{im} N_{i_p}$ and $\operatorname{im} \prod_{p=1}^{k} N_{i_p}$ are both simply the elements whose expansion in the form $\sum_g c_g g \in \mathbb{Z}[G]$ have c_g "constant in σ_p and σ_q." More explicitly, of course, $\prod_{p=1}^{k} N_{i_p} \in \bigcap_{p=1}^{k} \operatorname{im} N_{i_p}$, so

$$\operatorname{im} \prod_{p=1}^{k} N_{i_p} \subseteq \bigcap_{p=1}^{k} \operatorname{im} N_{i_p}.$$

In the other direction, suppose that we have some element

$$z \coloneqq \sum_{\{a_i\}_i} c_{\{a_i\}_i} \sigma_1^{a_1} \cdots \sigma_m^{a_m} \in \bigcap_{p=1}^{k} \operatorname{im} N_{i_p},$$

the sum is over sequences $\{a_i\}_{i=1}^{m}$ such that $0 \leq a_i < n_i$ for each index i. We will show $z \in \operatorname{im} \prod_{p=1}^{k} N_{i_p}$.

Now, $z \in \operatorname{im} N_r$ for given r is equivalent to $z \in \ker T_r$, but upon multiplying by $(\sigma_r - 1)$ we see that we are asking for

$$\sum_{\{a_i\}_i} c_{\{a_i\}_i} \sigma_1^{a_1} \cdots \sigma_{r-1}^{a_{r-1}} \sigma_r^{a_r} \sigma_{r+1}^{a_{r+1}} \cdots \sigma_n^{a_n} = \sum_{\{a_i\}_i} c_{\{a_i\}_i} \sigma_1^{a_1} \cdots \sigma_{r-1}^{a_{r-1}} \sigma_r^{a_r+1} \sigma_{r+1}^{a_{r+1}} \cdots \sigma_n^{a_n}.$$

In other words, this is asking for $c_{(a_i)_i} = c_{(a_i)_i + (1_{i=r})_i}$, or more succinctly just that c is constant in the $i = r$ coordinate.

Thus, c is constant in all the $i = i_p$ coordinates for each index i_p. Thus, we let $d_{\{a_i\}_{i \notin \{i_p\}}}$ be the restricted function equal to $c_{(a_i)_i}$ but forgetting the information input from any of the a_{i_p}. This allows us to write

$$\begin{aligned} z &= \sum_{\{a_i\}_i} c_{\{a_i\}_i} \sigma_1^{a_1} \cdots \sigma_m^{a_m} \\ &= \sum_{\{a_i\}_{i \notin \{i_p\}}} \sum_{a_{i_1}=0}^{n_{i_1}-1} \cdots \sum_{a_{i_k}=0}^{n_{i_k}-1} d_{\{a_i\}_{i \notin \{i_p\}}} \sigma_1^{a_1} \cdots \sigma_m^{a_m} \\ &= \left(\sum_{\{a_i\}_{i \notin \{i_p\}}} d_{\{a_i\}_{i \notin \{i_p\}}} \prod_{\substack{i=0 \\ i \notin \{i_p\}}}^{m} \sigma_i^{a_i} \right) \left(\sum_{a_{i_1}=0}^{n_{i_1}-1} \sigma_{i_1}^{a_{i_1}} \right) \cdots \left(\sum_{a_{i_k}=0}^{n_{i_k}-1} \sigma_{i_k}^{a_{i_k}} \right), \end{aligned}$$

which is now manifestly in $\operatorname{im} \prod_{p=1}^{k} N_{i_p}$. ∎

Lemma 131. Fix everything as in the set-up. Then, given $g \coloneqq \prod_{i=1}^{m} \sigma_i^{a_i}$, we have

$$g_{(i)} = 1 + \sum_{p=1}^{i-1} g_{(p)} \sigma_p^{(a_p)} T_p$$

for $i \geq 1$.

Proof. This is by induction. For $i = 1$, there is nothing to say. For the inductive step, we take $i > 1$ where we may assume the statement for $i - 1$. Via some relabeling, we may make our inductive hypothesis assert

$$\prod_{p=2}^{i-1} \sigma_p^{a_p} = 1 + \sum_{p=2}^{i-1} \left(\prod_{q=2}^{p-1} \sigma_q^{a_q} \right) \sigma_p^{(a_p)} T_p.$$

In particular, multiplying through by $\sigma_1^{a_1}$ yields

$$\begin{aligned} g_{(i)} &= \sigma_1^{a_1} \cdot \prod_{p=2}^{i-1} \sigma_p^{a_p} \\ &= \sigma_1^{a_1} + \sigma_1^{a_1} \sum_{p=2}^{i-1} \left(\prod_{q=2}^{p-1} \sigma_q^{a_q} \right) \sigma_p^{(a_p)} T_p \\ &= \sigma_1^{a_1} + \sum_{p=2}^{i-1} g_{(p)} \sigma_p^{(a_p)} T_p \\ &= 1 + \sigma_1^{(a_1)} T_1 + \sum_{p=2}^{i-1} g_{(p)} \sigma_p^{(a_p)} T_p, \end{aligned}$$

which is exactly what we wanted, after a little more rearrangement. ∎

And mostly because we can, we show that our main short exact sequence splits.

Lemma 132. Fix everything as in the set-up. Then consider $\mathbb{Z}$-module map $\rho \colon \mathbb{Z}[G]^m \to \mathbb{Z}[G]^m$ defined by

$$\rho(g\varepsilon_i) \coloneqq g_{(i)} \left(\sigma_i^{a_i} - N_i 1_{a_i = n_i - 1} \right) \varepsilon_i + \sum_{j=i+1}^{m} g_{(j)} \sigma_j^{(a_j)} T_i \varepsilon_j,$$

where $g \coloneqq \prod_{i=1}^{m} \sigma_i^{a_i}$ with $0 \leq a_i < n_i$. Then ρ descends to a map $\overline{\rho} \colon \operatorname{coker} \mathcal{F} \to \mathbb{Z}[G]^m$ witnessing the $\mathbb{Z}$-splitting of the short exact sequence

$$0 \to X \to \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0.$$

Proof. Observe that we have a well-defined map $\rho \colon \mathbb{Z}[G]^m \to \mathbb{Z}[G]^m$ because $\mathbb{Z}[G]^m$ is a free abelian group generated by $g\varepsilon_i$ for $g \in G$ and indices i. It remains to show that $\operatorname{im} \mathcal{F} \subseteq \ker \rho$ to get a map $\overline{\rho} \colon \operatorname{coker} \mathcal{F} \to \mathbb{Z}[G]^m$ and then to show that $\rho(z) \equiv z \pmod{\operatorname{im} \mathcal{F}}$ to get the splitting. We show these individually.

To show that $\operatorname{im} \mathcal{F} \subseteq \ker \rho$, we note from (5.1) that $\operatorname{im} \mathcal{F}$ is generated over $\mathbb{Z}[G]$ by the elements $N_i \varepsilon_i$ and $T_i \varepsilon_j - T_j \varepsilon_i$ for $g \in G$ and relevant indices i and j. Thus, $\operatorname{im} \mathcal{F}$ is generated over $\mathbb{Z}$ by the elements $g N_i \varepsilon_i$ and $g T_i \varepsilon_j - g T_j \varepsilon_i$ for relevant indices i and j. Thus, we fix any $g \coloneqq \prod_{i=1}^{n} \sigma_i^{a_i}$ with $0 \leq a_i < n_i$ and show that $g N_i \varepsilon_i \in \ker \rho$ and $g T_i \varepsilon_j - g T_j \varepsilon_i \in \ker \rho$ for relevant indices i and j.

- We show $g N_i \varepsilon_i \in \ker \rho$ for any i. Because $g N_i = g \sigma_i N_i$, we may as well as assume that $a_i = 0$. Then

$$\rho\left(g \sigma_i^a \varepsilon_i\right) = g_{(i)} \left(\sigma_i^a - N_i 1_{a = n_i - 1} \right) \varepsilon_i + \sum_{j=i+1}^{m} g_{(j)} \sigma_i^a \sigma_j^{(a_j)} T_i \varepsilon_j.$$

As a varies from 0 to $n_i - 1$, we note that the term $g_{(i)}\left(\sigma_i^a - N_i 1_{a=n_i-1}\right)\varepsilon_i$ will only get the $-N_i$ contribution exactly once at $a = n_i - 1$. Summing, we thus see that

$$\rho(gN_i\varepsilon_i) = g_{(i)}\left(-N_i + \sum_{a=0}^{n_i-1}\sigma_i^a\right)\varepsilon_i + \sum_{a=0}^{n_i-1}\sum_{j=i+1}^{m} g_{(j)}\sigma_i^a\sigma_j^{(a_j)}T_i\varepsilon_j.$$

The left term vanishes because $N_i = \sum_{a=0}^{n_i-1}\sigma_i^a$. Additionally, the right term vanishes because we can factor out $T_i\sum_{a=0}^{n_i-1}\sigma_i^a = T_iN_i = 0$. So $gN_i\varepsilon_i \in \ker\rho$.

- We show $gT_p\varepsilon_q - gT_q\varepsilon_p \in \ker\rho$ for any $p > q$. Equivalently, we will show that $\rho(g\sigma_p\varepsilon_q) - \rho(g\varepsilon_q) = \rho(g\sigma_q\varepsilon_p) - \rho(g\varepsilon_p)$. On one hand, note

$$\begin{aligned}\rho(g\sigma_p\varepsilon_q) = g_{(q)}\left(\sigma_q^{a_q} - N_i 1_{a_q=n_q-1}\right)\varepsilon_q \\ + \sum_{j=q+1}^{p-1} g_{(j)}\sigma_j^{(a_j)}T_q\varepsilon_j \\ + g_{(p)}\left(\sigma_p^{(a_p+1)} - N_p 1_{a_p=n_p-1}\right)T_q\varepsilon_p \\ + \sum_{j=p+1}^{m}\sigma_p g_{(j)}\sigma_j^{(a_j)}T_q\varepsilon_j\end{aligned}$$

because $g_{(j)}$ doesn't "see" the extra σ_p term until $j > p$. (For the $j = p$ term, we would like to write $\sigma_p^{(a_p+1)}$ above, but when $a_p = n_p - 1$, we actually end up with $\sigma_p^{(0)} = 0$ and hence have to subtract out $\sigma_p^{(n_p)} = N_p$.) Thus,

$$\rho(g\sigma_p\varepsilon_q) - \rho(g\varepsilon_q) = g_{(p)}\left(\sigma_p^{a_p} - N_p 1_{a_p=n_p-1}\right)T_q\varepsilon_p + \sum_{j=p+1}^{m} g_{(j)}\sigma_j^{(a_j)}T_pT_q\varepsilon_j.$$

On the other hand, we have

$$\rho(g\sigma_q\varepsilon_p) = \sigma_q g_{(p)}\left(\sigma_p^{a_p} - N_p 1_{a_p=n_p-1}\right)\varepsilon_p + \sum_{j=p+1}^{m}\sigma_q g_{(j)}\sigma_j^{(a_j)}T_p\varepsilon_j$$

where this time all $j > p$ also have $j > q$ and so $(\sigma_q g)_{(j)} = \sigma_q g_{(j)}$. Thus,

$$\rho(g\sigma_q\varepsilon_p) - \rho(g\varepsilon_p) = g_{(p)}\left(\sigma_p^{a_p} - N_p 1_{a_p=n_p-1}\right)T_q\varepsilon_p + \sum_{j=p+1}^{m} g_{(j)}\sigma_j^{(a_j)}T_pT_q\varepsilon_j,$$

as desired.

We now check the splitting. For this, we simply need to check that $\rho(g\varepsilon_i) \equiv g\varepsilon_i \pmod{\operatorname{im}\mathcal{F}}$, and we will get the result for all elements of $\mathbb{Z}[G]^m$ by additivity of ρ. Well, using Lemma 131, we write

$$\begin{aligned}g\varepsilon_i &= g_{(i)}\sigma_i^{a_i}\left(\prod_{j=i+1}^{m}\sigma_j^{a_j}\right)\varepsilon_i \\ &= g_{(i)}\sigma_i^{a_i}\left(1 + \sum_{j=i+1}^{m}\left(\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)\sigma_j^{(a_j)}T_j\right)\varepsilon_i \\ &= g_{(i)}\sigma_i^{a_i}\varepsilon_i + \sum_{j=i+1}^{m} g_{(i)}\sigma_i^{a_i}\left(\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)\sigma_j^{(a_j)}T_j\varepsilon_i \\ &\equiv g_{(i)}\sigma_i^{a_i}\varepsilon_i + \sum_{j=i+1}^{m} g_{(j)}\sigma_j^{(a_j)}T_i\varepsilon_j \pmod{\operatorname{im}\mathcal{F}},\end{aligned}$$

where in the last step we have used the fact that $T_j\varepsilon_i \equiv T_j\varepsilon_i \pmod{\operatorname{im}\mathcal{F}}$. Lastly, we note that $hN_i\varepsilon_i \equiv h\varepsilon_i \pmod{\operatorname{im}\mathcal{F}}$ for any $h \in G$, so in fact

$$g\varepsilon_i \equiv g_{(i)}\left(\sigma_i^{a_i} - N_i 1_{a_i=n_i-1}\right)\varepsilon_i + \sum_{j=i+1}^{m} g_{(j)}\sigma_j^{(a_j)}T_i\varepsilon_j,$$

and now the right-hand side is $\rho(g\varepsilon_i)$. ∎

5.3 Verification of 1-Cocycles

Here we prove Proposition 127. Namely, we show that the 1-cochain $\overline{c} \in C^1(G, \operatorname{coker}\mathcal{F})$ defined by

$$\overline{c}(g) = \sum_{i=1}^{m} g_{(i)}\sigma_i^{(a_i)}\varepsilon_i$$

where $g \coloneqq \prod_{i=1}^m \sigma_i^{a_i}$ with $0 \le a_i < n_i$ is actually a 1-cocycle. It will be beneficial for us to do this by hand, which is a matter of brute force. Set $c \in C^1\left(G, \mathbb{Z}[G]^m\right)$ defined by

$$c(g) \coloneqq \sum_{i=1}^{m} g_{(i)}\sigma_i^{(a_i)}\varepsilon_i,$$

where $g \coloneqq \prod_{i=1}^m \sigma_i^{a_i}$ with $0 \le a_i < n_i$. We will show that $\operatorname{im} dc \subseteq \operatorname{im}\mathcal{F}$, which we will mean that $\operatorname{im}\overline{dc} = \operatorname{im} d\overline{c} = 0$, where $f \mapsto \overline{f}$ is the map $C^\bullet\left(G, \mathbb{Z}[G]^m\right) \twoheadrightarrow C^\bullet\left(G, \operatorname{coker}\mathcal{F}\right)$ induced by modding out.

As such, we set $g \coloneqq \prod_{i=1}^m \sigma_i^{a_i}$ and $h \coloneqq \prod_{i=1}^m \sigma_i^{b_i}$ with $0 \le a_i, b_i < n_i$ for each i. Then, using the division algorithm, write

$$a_i + b_i = n_i q_i + r_i$$

where $q_i \in \{0, 1\}$ and $0 \le r_i < n_i$ for each i. Now, we want to show $dc(g,h) \in \operatorname{im}\mathcal{F}$, so we begin by writing

$$\begin{aligned} dc(g,h) &= gc(h) - c(gh) + c(g) \\ &= \sum_{i=1}^{m}\left(gh_{(i)}\sigma_i^{(b_i)}\varepsilon_i - \prod_{p=0}^{i-1}\sigma_p^{r_p}\sigma_i^{(r_i)}\varepsilon_i + g_{(i)}\sigma_i^{(a_i)}\varepsilon_i\right) \\ &= \sum_{i=1}^{m}\left(gh_{(i)}\sigma_i^{(b_i)}\varepsilon_i - g_{(i)}h_{(i)}\sigma_i^{(r_i)}\varepsilon_i + g_{(i)}\sigma_i^{(a_i)}\varepsilon_i\right). \end{aligned} \tag{5.2}$$

We now go term-by-term in (5.2). The easiest is the middle term of (5.2), for which we write

$$\begin{aligned} g_{(i)}h_{(i)}\sigma_i^{(r_i)} &= g_{(i)}h_{(i)}\sigma_i^{(a_i+b_i)} - g_{(i)}h_{(i)}\sigma_i^{r_i}\sigma_i^{(n_iq_i)} \\ &= g_{(i)}h_{(i)}\sigma_i^{(a_i+b_i)} - g_{(i)}h_{(i)}\sigma_i^{a_i+b_i}\cdot q_iN_i \\ &= g_{(i)}h_{(i)}\sigma_i^{(a_i+b_i)} - g_{(i)}h_{(i)}\cdot q_iN_i, \end{aligned}$$

where the last equality is because $\sigma_iN_i = N_i$. Thus,

$$\begin{aligned} -\sum_{i=1}^{m} g_{(i)}h_{(i)}\sigma_i^{(r_i)}\varepsilon_i &= -\sum_{i=1}^{m} g_{(i)}h_{(i)}\sigma_i^{(a_i+b_i)}\varepsilon_i + \sum_{i=1}^{m} g_{(i)}h_{(i)}\cdot q_iN_i\varepsilon_i \\ &= -\sum_{i=1}^{m} g_{(i)}h_{(i)}\sigma_i^{(a_i+b_i)}\varepsilon_i + \sum_{i=1}^{m}\mathcal{F}\left(g_{(i)}h_{(i)}q_i\kappa_i\right). \end{aligned}$$

Now, using Lemma 131, the ith coordinate of the left term of (5.2) is

$$\begin{aligned} gh_{(i)}\sigma_i^{(b_i)} &= g_{(i)}\sigma_i^{a_i}\left(\prod_{j=i+1}^{m}\sigma_j^{a_j}\right)h_i\sigma_i^{(b_i)} \\ &= g_{(i)}\left(1+\sum_{j=i+1}^{m}\left(\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)\sigma_j^{(a_j)}T_j\right)h_{(i)}\sigma_i^{a_i}\sigma_i^{(b_i)} \\ &= g_{(i)}h_{(i)}\sigma_i^{a_i}\sigma_i^{(b_i)} + \sum_{j=i+1}^{m}\left(g_{(i)}\sigma_i^{a_i}\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)h_{(i)}\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j \\ &= g_{(i)}h_{(i)}\sigma_i^{a_i}\sigma_i^{(b_i)} + \sum_{j=i+1}^{m} g_{(j)}h_{(i)}\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j. \end{aligned}$$

And lastly, for the right term of (5.2), the ith coordinate is

$$\begin{aligned} g_{(i)}\sigma_i^{(a_i)} &= g_{(i)}\left(h_{(i)} - \sum_{j=1}^{i-1}h_{(j)}\sigma_j^{(b_j)}T_j\right)\sigma_i^{(a_i)} \\ &= g_{(i)}h_{(i)}\sigma_i^{(a_i)} - \sum_{j=1}^{i-1} g_{(i)}h_{(j)}\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j. \end{aligned}$$

So to finish, we continue from (5.2), which gives

$$\begin{aligned} dc(g,h) - \sum_{i=1}^{m}\mathcal{F}\big(g_{(i)}h_{(i)}q_i\kappa_i\big) &= \sum_{i=1}^{m}\left(g_{(i)}h_{(i)}\sigma_i^{a_i}\sigma_i^{(b_i)}\varepsilon_i - g_{(i)}h_{(i)}\sigma_i^{(a_i+b_i)}\varepsilon_i + g_{(i)}h_{(i)}\sigma_i^{(a_i)}\varepsilon_i\right) \\ &\qquad + \sum_{i=1}^{m}\left(\sum_{j=i+1}^{m} g_{(j)}h_{(i)}\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j - \sum_{j=1}^{i-1} g_{(i)}h_{(j)}\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j\right)\varepsilon_i \\ &= \sum_{i=1}^{m}\left(-\sum_{j=1}^{i-1} g_{(i)}h_{(j)}\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j + \sum_{j=i+1}^{m} g_{(j)}h_{(i)}\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j\right)\varepsilon_i \\ &= \sum_{i>j}\mathcal{F}\left(g_{(i)}h_{(j)}\sigma_i^{(a_i)}\sigma_j^{(b_j)}\lambda_{ij}\right). \end{aligned}$$

Thus,

$$dc(g,h) = \mathcal{F}\left(\sum_{i=1}^{m} g_{(i)}h_{(i)}\kappa_i + \sum_{i>j} g_{(i)}h_{(j)}\sigma_i^{(a_i)}\sigma_j^{(b_j)}\lambda_{ij}\right) \in \operatorname{im}\mathcal{F}. \tag{5.3}$$

This completes the proof of Proposition 127.

In fact, the above proof has found an explicit element z so that $\mathcal{F}(z) = dc(g,h)$ for each $g,h\in G$. As such, we recall that we set

$$X \coloneqq \frac{\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}}{\ker\mathcal{F}}$$

to give the short exact sequence

$$0 \to X \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \operatorname{coker}\mathcal{F} \to 0.$$

In particular, we can track $\overline{c}\in Z^1(G,\operatorname{coker}\mathcal{F})$ through a boundary morphism: we already have a chosen lift $c\in Z^1(G,\mathbb{Z}[G]^m)$ for $\overline{c}$, and we have also computed $\mathcal{F}^{-1}\circ dc$ from the above work. This gives the following result.

Corollary 133. Fix everything as in the set-up. Then the $\overline{c}$ of Proposition 127 has

$$\delta(c)(g,h) \coloneqq \sum_{i=1}^{m} g_{(i)} h_{(i)} \kappa_i + \sum_{i>j} g_{(i)} h_{(j)} \sigma_i^{(a_i)} \sigma_j^{(b_j)} \lambda_{ij}$$

where δ is induced by

$$0 \to X \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0.$$

Proof. This follows from tracking how δ behaves, using (5.3). ∎

Remark 134. In some sense, this $\delta(c)$ is exactly the cocycle of Theorem 105, where we have abstracted away everything about A. We will rigorize this notion in our proof of Theorem 129.

5.4 Tuples via Cohomology

We continue in the set-up of the previous subsection. The goal of this subsection is to prove Proposition 128. The main idea is that we will be able to finitely generate $\ker \mathcal{F}$ essentially using the relations of a $\{\sigma_i\}_{i=1}^m$-tuple.

We start with the following basic result.

Lemma 135. Fix everything as in the set-up. Then $\ker \mathcal{F}$ contains the following elements.

(a) $T_p \kappa_p$ for any index p.

(b) $N_p N_q \lambda_{pq}$ for any pair of indices (p,q) with $p > q$.

(c) $T_q \kappa_p + N_p \lambda_{pq}$ for any pair of indices (p,q) with $p > q$.

(d) $T_p \kappa_q - N_q \lambda_{pq}$ for any pair of indices (p,q) with $p > q$.

(e) $T_q \lambda_{pr} - T_r \lambda_{pq} - T_p \lambda_{qr}$ for any triplet of indices (p,q,r) with $p > q > r$.

Proof. We start by showing that all the listed elements are in fact in $\ker \mathcal{F}$.

(a) Note that $\mathcal{F}$ only ever takes the x_i term to $x_i N_i$, so if $x_i = T_i$, then the effect of x_i vanishes.

(b) Similarly, note that $\mathcal{F}$ only ever takes the y_{ij} term to $y_{ij} T_i$ or $y_{ij} T_j$. As such, if $y_{ij} = N_i N_j$, then the effect of y_{ij} vanishes again.

(c) The only relevant terms are at indices p and q. Here, $i = p$ has $\mathcal{F}$ output

$$T_q N_p - N_p T_q + 0 = 0.$$

For $i = q$, we have no x_q term, so we are left with $N_p T_p = 0$.

(d) Again, the only relevant terms are at indices p and q. This time the interesting term is at $i = q$, where we have

$$T_p N_q - 0 + (-N_q) T_p = 0.$$

Then at $i = p$, we simply have $0 N_p - (-N_q) T_q + 0 = 0$.

(e) The relevant terms, as usual, are for $i \in \{p,q,r\}$.

- At $i = p$, we have $0 - (T_q T_r + (-T_r) T_q) + 0 = 0$.

- At $i = q$, we have $0 - (-(T_p)T_r) + ((-T_r)T_p) = 0$.
- At $i = r$, we have $0 - 0 + (T_qT_p + (-T_p)T_q) = 0$.

The above checks complete this part of the proof. ■

Remark 136. The above elements are intended to encode the relations to be a $\{\sigma_i\}_{i=1}^n$-tuple. We will see this made rigorous in the proof of Proposition 128.

In fact, the following is true.

Lemma 137. Fix everything as in the set-up. Then the elements (a)–(e) of Lemma 135, with (b) removed, generate $\ker \mathcal{F}$.

Proof. We remark that we callously removed (b) because it is implied: $T_q\kappa_p + N_p\lambda_{pq} \in \ker \mathcal{F}$ implies that

$$N_q \cdot (T_q\kappa_p + N_p\lambda_{pq}) = N_pN_q\lambda_{pq}$$

is also in $\ker \mathcal{F}$. Anyway, this proof is long and annoying and hence relegated to Appendix B. ■

Here is the payoff for the hard work in Lemma 137.

Proposition 128. Fix everything as in the set-up, and now let A be a G-module. Then $\{\sigma_i\}_{i=1}^m$-tuples are canonically isomorphic to $\operatorname{Hom}_{\mathbb{Z}[G]}(X, A) = H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))$.

Proof. Let $\mathcal{T}$ denote the set of $\{\sigma_i\}_{i=1}^m$-tuples. We now define the map $\varphi\colon \operatorname{Hom}_{\mathbb{Z}[G]}(X, A) \to \mathcal{T}$ by

$$\varphi\colon f \mapsto \Big(\big(f(\kappa_i)\big)_i, \big(f(\lambda_{ij})\big)_{i>j} \Big).$$

In other words, we simply read off the values of f from indicators on the coordinates of X. It's not hard to see that φ is in fact a G-module homomorphism, but we will have to check that φ is well-defined, for which we have to check the conditions on being a $\{\sigma_i\}_{i=1}^m$-tuple.

Lemma 138. Fix everything as in the set-up, and let A be a G-module. Then, given $f\colon \mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}$, we have $\ker \mathcal{F} \subseteq \ker f$ if and only if

$$\Big(\big(f(\kappa_i)\big)_i, \big(f(\lambda_{ij})\big)_{i>j} \Big)$$

is a $\{\sigma_i\}_{i=1}^m$-tuple.

Proof. By Lemma 137, we see $\ker \mathcal{F} \subseteq \ker f$ if and only if f vanishes on the elements given in Lemma 135. As such, we now run the following checks.

1. We discuss (4.1). For one, note that $f(\lambda_{ij}) \in A$ essentially for free. Now, we note

$$\begin{aligned} f(\kappa_i) \in A^{\langle \sigma_i \rangle} &\iff T_i f(\kappa_i) = 0 \\ &\iff f(T_i\kappa_i) = 0 \\ &\iff T_i\kappa_i \in \ker f. \end{aligned}$$

2. We discuss (4.2). On one hand, note that $i > j$ has

$$\begin{aligned} N_i f(\lambda_{ij}) = -T_j f(\lambda_i) &\iff f(N_i\lambda_{ij} + T_j\lambda_i) \\ &\iff N_i\lambda_{ij} + T_j\lambda_i \in \ker f. \end{aligned}$$

On the other hand,

$$\begin{aligned} -N_j f(\lambda_{ij}) = -T_i f(\lambda_j) &\iff f(N_j\lambda_{ij} + T_i\lambda_j) = 0 \\ &\iff N_j\lambda_{ij} + T_i\lambda_j \in \ker f. \end{aligned}$$

3. We discuss (4.3). Simply note indices $i > j > k$ have

$$\begin{aligned} T_j f(\lambda_{ik}) = T_k f(\lambda_{ij}) + T_i f(\lambda_{jk}) &\iff f(T_j\lambda_{ik} - T_k\lambda_{ij} - T_i\lambda_{jk}) = 0 \\ &\iff T_j\lambda_{ik} - T_k\lambda_{ij} - T_i\lambda_{jk} \in \ker f. \end{aligned}$$

In total, we see that satisfying the relations to be a $\{\sigma_i\}_{i=1}^m$-tuple exactly encodes the data of having the generators of $\ker \mathcal{F}$ live in $\ker f$. ■

So indeed, given $f\colon X \to A$, the above lemma applied to the composite

$$\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}} \twoheadrightarrow X \xrightarrow{f} A$$

shows that $\varphi(f) \in \mathcal{T}$.

To show that φ is an isomorphism, we exhibit its inverse; fix some $(\{\alpha_i\}, \{\beta_{ij}\}_{i>j}) \in \mathcal{T}$. Well, $\mathbb{Z}[G] \times \mathbb{Z}[G]^{\binom{m}{2}}$ has as a basis the κ_i and λ_{ij}, so we can uniquely define a G-module homomorphism $f\colon X \to A$ by

$$f(\kappa_i) \coloneqq \alpha_i \qquad \text{and} \qquad f(\lambda_{ij}) \coloneqq \beta_{ij}$$

for all relevant indices i, j, and in fact the map $\mathcal{T} \to \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}, A\right)$ we can see to be a G-module homomorphism. However, because these outputs are a $\{\sigma_i\}_{i=1}^m$-tuple, we can read Lemma 138 backward to say that f has kernel containing $\ker \mathcal{F}$, so in fact we induce a map $\overline{f}\colon X \to A$.

So in total, we get a G-module homomorphism $\psi\colon \mathcal{T} \to \operatorname{Hom}_{\mathbb{Z}[G]}(X, A)$ by

$$\psi\colon (\{\alpha_i\}, \{\beta_{ij}\}_{i>j}) \mapsto \overline{f},$$

where $\overline{f}$ is defined on the basis elements above. Further, ψ is the inverse of φ essentially because the $\{\kappa_i\}_i \cup \{\lambda_{ij}\}_{i>j}$ form a basis of $\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}$. This completes the proof. ■

And now because it is so easy, we might as well prove Theorem 129.

Theorem 129. Fix everything as in the set-up. Also, fix a G-module A and a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$. Observe there is a natural cup product map

$$\cup\colon H^2(G, X) \times H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \to H^2(G, A).$$

Then, using the isomorphism of Proposition 128, the cocycle defined in Theorem 105 is simply the output of $\delta(\overline{c}) \cup (\{\alpha_i\}, \{\beta_{ij}\})$ on cocycles.

Proof. The main point is that we have a computation of $\delta(\overline{c})$ from Corollary 133, which we merely need to track through. In particular, fix a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}_i, \{\beta_{ij}\}_{i>j})$, and let $f \in H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))$ be the corresponding morphism. As such, we may compute our cup product out as

$$\big(\delta(\overline{c}) \cup f\big)(g, h) = \delta(\overline{c})(g, h) \otimes_{\mathbb{Z}} gh \cdot f = \delta(\overline{c})(g, h) \otimes_{\mathbb{Z}} f.$$

To pass through evaluation, we set $g \coloneqq \prod_i \sigma_i^{a_i}$ and $h \coloneqq \prod_i \sigma_i^{b_i}$ with $0 \leq a_i, b_i < n_i$, from which we get

$$\begin{aligned} f\big(\delta(\overline{c})(g,h)\big) &= f\left(\sum_{i=1}^{m} g_{(i)}h_{(i)}q_i\kappa_i + \sum_{i>j} g_{(i)}h_{(j)}\sigma_i^{(a_i)}\sigma_j^{(b_j)}\lambda_{ij}\right) \\ &= \sum_{i=1}^{m} g_{(i)}h_{(i)}\left\lfloor \frac{a_i+b_i}{n_i}\right\rfloor \cdot \alpha_i + \sum_{\substack{i,j=1\\ i>j}}^{m} g_{(i)}h_{(j)}\sigma_i^{(a_i)}\sigma_j^{(b_j)} \cdot \beta_{ij} \\ &= \sum_{\substack{i,j=1\\ i>j}}^{m} \left(\prod_{p<i}\sigma_p^{a_p}\right)\left(\prod_{q<j}\sigma_q^{b_q}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij} + \sum_{i=1}^{m} g_{(i)}h_{(i)}\alpha_i^{\left\lfloor \frac{a_i+b_i}{n_i}\right\rfloor}. \end{aligned}$$

Doing a little more rearrangement and writing this multiplicatively exactly recovers the cocycle of Theorem 105. This completes the proof. ■

Though we have successfully provided an alternate proof of Theorem 105, there is more to discuss with our alternate description of tuples. Namely, we now begin showing that X is a 2-encoding module.

Proposition 139. Fix everything as in the set-up, and let A be a G-module. Then the isomorphism of Proposition 128 descends to an isomorphism between equivalence classes of $\{\sigma_i\}_{i=1}^m$-tuples are canonically isomorphic to $\widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$.

Proof. Recall that the short exact sequence

$$0 \to X \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \mathrm{coker}\,\mathcal{F} \to 0$$

of G-modules splits as $\mathbb{Z}$-modules by Lemma 132, so we have a short exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{coker}\,\mathcal{F}, A) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^m, A) \xrightarrow{-\circ\mathcal{F}} \mathrm{Hom}_{\mathbb{Z}}(X, A) \to 0.$$

Now, the key trick will be to compare regular group cohomology with Tate cohomology. To begin, we note that our cohomology theories give the following commutative diagram with exact rows.

$$\begin{array}{ccccc} H^0(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^m, A)) & \xrightarrow{-\circ\mathcal{F}} & H^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) & \longrightarrow & H^1(G, \mathrm{Hom}_{\mathbb{Z}}(\mathrm{coker}\,\mathcal{F}, A)) \\ & & \downarrow & & \| \\ 0 & \longrightarrow & \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) & \longrightarrow & \widehat{H}^1(G, \mathrm{Hom}_{\mathbb{Z}}(\mathrm{coker}\,\mathcal{F}, A)) \end{array} \tag{5.4}$$

Here, the middle vertical map is reduction modulo $\mathrm{im}\, N_G$. The rows are exact from the long exact sequences, and the square commutes by construction of Tate cohomology. Now, the point is that the diagram induces the isomorphism

$$\frac{H^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))}{\mathrm{im}(-\circ\mathcal{F})} \simeq \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)), \tag{5.5}$$

which simply sends $[f] \mapsto [f]$.

Thus, the main content here will be to track through the image of $-\circ\mathcal{F}$ in (5.4). Let $\mathcal{T}$ denote the set of $\{\sigma_i\}_{i=1}^m$-triples of A, and let $\mathcal{T}_0$ denote the set (in fact, equivalence class) of triples corresponding to $[0] \in H^2(G, A)$. Letting $\varphi\colon H^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \to \mathcal{T}$ be defined by

$$\varphi\colon f \mapsto \Big(\big(f(\kappa_i)\big)_i, \big(f(\lambda_{ij})\big)_{i>j}\Big)$$

be the isomorphism of Proposition 128, we claim that the image of $-\circ\mathcal{F}$ in $H^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, A))$ corresponds under φ to exactly $\mathcal{T}_0$.

Indeed, we take a G-module homomorphism $f\colon \mathbb{Z}[G]^m \to A$ to the G-module homomorphism $(f \circ \mathcal{F})\colon X \to A$. Then we compute

$$\begin{aligned}(f\circ\mathcal{F})(\kappa_i) &= f(N_i\varepsilon_i)\\ &= N_i f(\varepsilon_i)\\ (f\circ\mathcal{F})(\lambda_{ij}) &= f(T_i\varepsilon_j - T_j\varepsilon_i)\\ &= T_i f(\varepsilon_j) - T_j f(\varepsilon_i)\end{aligned}$$

for all relevant indices i and j. Thus,

$$\varphi(f\circ\mathcal{F}) = \left(\left(N_i f(\varepsilon_i)\right)_i, \left(T_i f(\varepsilon_j) - T_j f(\varepsilon_i)\right)_{i>j}\right),$$

which we can see lives in $\mathcal{T}_0$ by definition of our equivalence relation (upon using multiplicative notation). In fact, as f varies, we see that the values of $f(\varepsilon_i)$ may vary over all A, so the image of $f \mapsto \varphi(f\circ\mathcal{F})$ is exactly all of $\mathcal{T}_0$. Thus, φ induces an isomorphism

$$\overline{\varphi}\colon \frac{H^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,A))}{\mathrm{im}(-\circ\mathcal{F})} \simeq \frac{\mathcal{T}}{\mathcal{T}_0}.$$

Composing this with the "identity" map (5.5) finishes the proof. ∎

Remark 140. This proof feels more motivated coming from the perspective that X "should" be a 2-encoding module (for example, $\mathrm{coker}\,\mathcal{F}$ "should" be a 1-encoding module, allowing us to use Proposition 83). Namely, we should think of the equivalence relation on the tuples from Definition 109 as being unmotivated before and instead is best motivated now as coming out of the quotient

$$H^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,-)) \Rightarrow \widehat{H}^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,-)).$$

Indeed, the equivalence relations had better match up anyway.

5.5 Algebraic Corollaries

We continue in the set-up of the previous subsection. Observe that Proposition 139 combined with Theorem 113 tells us that we have isomorphisms

$$[\delta(\overline{c})]\cup -\colon \widehat{H}^0(G,\mathrm{Hom}_{\mathbb{Z}}(X,A)) \to \widehat{H}^2(G,A).$$

In fact, Lemma 23 tells us that these isomorphisms assemble into a natural isomorphism, so we have the following result.

Theorem 141. Fix everything as in the set-up. Then X is a 2-encoding module.

Proof. This follows from the above discussion. ∎

Remark 142. It is perhaps useful to note that we can show that X is a 2-encoding module, without the need to digress to tuples as done in Proposition 139. Indeed, we recall that

$$0 \to X \to \mathbb{Z}[G]^m \to \mathrm{coker}\,\mathcal{F} \to 0$$

splits by Lemma 132, so because $\mathbb{Z}[G]^m \cong \mathbb{Z}[G]\otimes_{\mathbb{Z}}\mathbb{Z}^m$ is induced, it suffices to show that $\mathrm{coker}\,\mathcal{F}$ is a 1-encoding module by Proposition 83.

For this, we can use Proposition 60 and manually give x and $x^\vee$; here, $x = [\overline{c}]$ will work, and one can solve for $x^\vee$. Alternatively, one could check the cohomology groups from Proposition 71. One could even solve for $[\delta(\overline{c})]^\vee$ explicitly, though this is harder.

Now that we have a 2-encoding module, we can apply all the theory we built in section 3. For example, it might have felt like magic that the isomorphism sending a tuple to its cohomology class was induced by a cup product, but in fact this must have been true all along by Corollary 51.

Here are some other results.

Corollary 143. Fix everything as in the set-up. Then X is cohomologically equivalent to $I_G \otimes_{\mathbb{Z}} I_G$.

Proof. We know that $I_G \otimes_{\mathbb{Z}} I_G$ is a 2-encoding module by Example 48, so Proposition 47 finishes. ■

Corollary 144. Fix everything as in the set-up. Then, for any $i \in \mathbb{Z}$ and subgroup $H \subseteq G$, we have natural isomorphisms

$$\mathrm{Res}[\delta(\overline{c})] \cup -\colon \widehat{H}^i(H, \mathrm{Hom}_{\mathbb{Z}}(X, A)) \to \widehat{H}^{i+2}(H, A).$$

Proof. Follow the proof of Corollary 53 to see that we can set $x = [\delta(\overline{c})]$ there. This gives the result for $H = G$, and we get general subgroups by appealing to Corollary 63. ■

Remark 145. Even though we have some notion of restriction from Lemma 118, writing a "tuple" in $\widehat{H}^0(H, \mathrm{Hom}_{\mathbb{Z}}(X, A))$ seems somewhat difficult in general. For example, it is not clear how to (in general) write X as $\mathbb{Z}[H]^m/M$ for an H-module M. In simple cases, we have worked this out in Lemma 118.

Corollary 146. Fix everything as in the set-up. Then $\widehat{H}^2(G, X)$ is cyclic of order $\#G$ generated by $[\delta(\overline{c})]$.

Proof. This follows from Corollary 57. ■

Remark 147. Fix notation as in subsection 5.1, and take $m = 2$. Then there are natural transformations

$$\widehat{H}^2(G, -) \overset{[\delta(\overline{c})]^\vee \cup -}{\Rightarrow} \widehat{H}^0(G, \mathrm{Hom}_{\mathbb{Z}}(X, -)) \Rightarrow \widehat{H}^{-1}(G, -)$$

sending a 2-cocycle to its $\{\sigma_i\}_{i=1}^m$-tuple and then to the (class of) β_{10}. (It turns out that, because G is bicyclic, the equivalence relation on β_{10} is exactly what we need to form a class of $\widehat{H}^{-1}$.) Now, applying Corollary 51, we see that the right natural transformation must be a cup-product map, so by associativity of the cup product, the entire natural transformation is a cup-product map.

Thus, analogously to what Corollary 92 says for αs, we can describe the projection from 2-cocycles to βs purely via (restricted) cup products.

Remark 148. Noting that $\mathcal{F}\colon X \hookrightarrow \mathbb{Z}[G]^m$ implies that X is $\mathbb{Z}$-free, there is a torus $T := \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{G}_m)$. It is conceivable that one could realize the approach of Remark 88 for our torus T.

6 Local Gerbs

In the following two sections, we will use the results of (largely) section 4 in order to provide explicit group laws for some of the Kottwitz gerbs [Kot14]. In this section, we will focus on abelian extensions of local fields. The approch here is similar to the approach for global fundamental classes in [Buc13], though we work in more generality than multiquadratic extensions.

6.1 Set-Up

Fix a finite abelian extension of local fields L/K which is not unramified.

Remark 149. Assuming that L/K is not unramified is a purely technical requirement; indeed, most of the arguments go through in this case. Regardless, when unramified, there already exist descriptions of the local fundamental class.

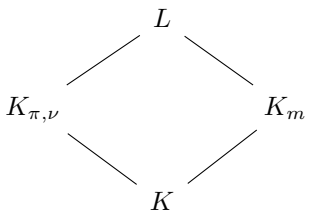
Then let K_m be the largest unramified subextension, which we will give degree m; let $\overline{\sigma}_K \in \mathrm{Gal}(L/K)$ denote the Frobenius automorphism, which lets us set

$$K_{\pi,\nu} \coloneqq L^{\langle \overline{\sigma}_K \rangle}.$$

In particular, $K_{\pi,\nu}/K$ is totally ramified because, for example, the residue fields of $K_{\pi,\nu}$ and K have the same order.

Example 150. For $K = \mathbb{Q}_p$, we can take $K_m = \mathbb{Q}_p\left(\zeta_{p^m-1}\right)$ and $K_{\pi,\nu} = \mathbb{Q}_p\left(\zeta_{p^\nu}\right)$.

This gives us the following tower of fields.



Quickly, we note that $L/K_{\pi,\nu}$ has Galois group generated by the Frobenius $\overline{\sigma}_K$ and therefore has degree m, so we have that $K_{\pi,\nu}$ and K_m are linearly disjoint over K and

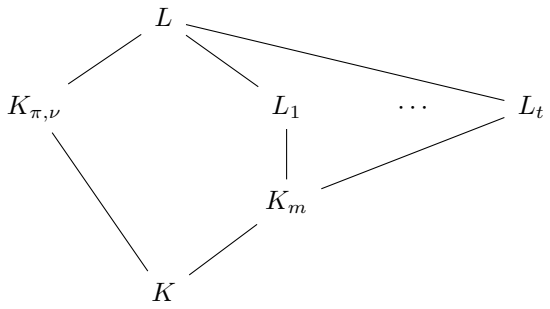
$$[L:K] = [L:K_{\pi,\nu}] \cdot [K_{\pi,\nu}:K] = [K_m:K] \cdot [K_{\pi,\nu}:K],$$

which implies that $L = K_{\pi,\nu}K_m$ as well.

We provide some quick commentary on these extensions.

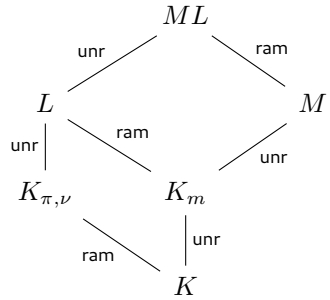
- The extension K_m/K is unramified of degree $f \coloneqq m$; note we are assuming $L \neq K_m$ and hence $f < n$. Its Galois group is thus generated by the Frobenius element defined by $\overline{\sigma}_K$.
- The extension $K_{\pi,\nu}/K$ is totally ramified of degree $[K_{\pi,\nu} : K]$. Because we are assuming this Galois group is abelian, we may write
$$\mathrm{Gal}(K_{\pi,\nu}/K) \simeq \Gamma_1 \times \cdots \times \Gamma_t$$
where $\Gamma_i = \langle \tau_i \rangle \subseteq \mathrm{Gal}(K_{\pi,\nu}/K)$ is a cyclic group of order n_i.
- Because $K_{\pi,\nu}/K$ is totally ramified and K_m/K is unramified, we have that the fields $K_{\pi,\nu}$ and K_m are linearly disjoint over K. As such, $L = K_{\pi,\nu}K_m$ has
$$\begin{aligned}
\mathrm{Gal}(L/K_{\pi,\nu}) &\simeq \mathrm{Gal}(K_m/K) = \langle \overline{\sigma}_K \rangle \\
\mathrm{Gal}(L/K_m) &\simeq \mathrm{Gal}(K_{\pi,\nu}/K) = \Gamma_1 \times \cdots \times \Gamma_t \\
\mathrm{Gal}(L/K) &\simeq \mathrm{Gal}(K_m/K) \times \mathrm{Gal}(K_{\pi,\nu}/K) = \langle \overline{\sigma}_K \rangle \times \Gamma_1 \times \cdots \times \Gamma_t.
\end{aligned}$$
In light of these isomorphisms, we will upgrade $\overline{\sigma}_K$ to the automorphism of L/K which restricts properly on K_m/K and fixing $K_{\pi,\nu}$; we do analogously for the τ_i. We also acknowledge that our degree is
$$n \coloneqq [L:K] = [K_m:K] \cdot [K_{\pi,\nu}:K] = f \cdot [K_{\pi,\nu}:K].$$

For brevity, we will also set $L_i \coloneqq L^{\langle \tau_i \rangle}$ for each i, which makes the fields under L look like the following.



In particular, $\mathrm{Gal}(L/L_i) = \langle \tau_i \rangle$ is cyclic for each i.

Now, the main idea in the computation is to use an unramified extension $M \coloneqq K_n$ of the same degree n as L/K. This modifies our diagram of fields as follows.



We have labeled the unramified extensions by "unr" and the totally ramified extensions by "ram."

As before, we provide some comments on the field extensions.

- The extension M/K is unramified of degree n. As before, its Galois group is cyclic, generated by the Frobenius element $\sigma_K \in \mathrm{Gal}(M/K)$. Observe that σ_K restricted to K_m is $\overline{\sigma}_K$, explaining our notation. In particular, σ_K has order n, but $\overline{\sigma}_K$ has order $f < n$.
- As before, note that $K_{\pi,\nu}$ and M are linearly disjoint over K because $K_{\pi,\nu}/K$ is totally ramified while M/K is unramified. As such, we may say that

$$\begin{aligned} \mathrm{Gal}(ML/M) &\simeq \mathrm{Gal}(K_{\pi,\nu}/K) = \Gamma_1 \times \cdots \times \Gamma_t \\ \mathrm{Gal}(ML/K_{\pi,\nu}) &\simeq \mathrm{Gal}(M/K) = \langle \sigma_K \rangle \\ \mathrm{Gal}(ML/K) &\simeq \mathrm{Gal}(M/K) \times \mathrm{Gal}(K_{\pi,\nu}/K) = \langle \sigma_K \rangle \times \Gamma_1 \times \cdots \times \Gamma_t. \end{aligned}$$

  Again, we will upgrade σ_K and the τ_i to their corresponding automorphisms on any subfield of ML.

- We take a moment to compute

$$\mathrm{Gal}(ML/L) \simeq \left\{ \sigma_K^a \tau \in \mathrm{Gal}(ML/K) : \sigma_K^a \tau|_L = \mathrm{id}_L \right\}.$$

  Because L is $K_{\pi,\nu}K_m$, it suffices to fix each of these fields individually. Well, to fix $K_{\pi,\nu}$, we need τ to vanish, so we might as well force $\tau = 1$. But to fix K_m, we need $\sigma_K^a|_{K_m} = \overline{\sigma}_K^a$ to be the identity, so we are actually requiring that $f \mid a$ here. As such,

$$\mathrm{Gal}(ML/L) = \langle \sigma_K^f \rangle.$$

These comments complete the Galois-theoretic portion of the analysis.

6.2 Idea

We will begin by briefly describe the outline for the computation. For a finite extension of local fields L/K, let $u_{L/K} \in H^2(L/K)$ denote the fundamental class.

Now, take variables as in our set-up in subsection 6.1. The main idea is to translate what we know about the unramified extension M/K over to the general extension L/K. In particular, we are able to compute the fundamental class $u_{M/K} \in H^2(M/K)$, so we observe that, by Proposition 5,

$$\mathrm{Inf}_{M/K}^{ML/K} u_{M/K} = [ML : M]u_{M/K} = n \cdot u_{ML/K} = [ML : L]u_{ML/L} = \mathrm{Inf}_{L/K}^{ML/K} u_{L/K}.$$

As such, we will be able to compute $u_{L/K}$ as long as we are able to invert the inflation map $\mathrm{Inf}\colon H^2(L/K) \to H^2(ML/K)$. This is not actually very easy to do in general, but we are in luck because this inflation map here comes from the Inflation–Restriction exact sequence

$$0 \to H^2(L/K) \overset{\mathrm{Inf}}{\to} H^2(ML/K) \overset{\mathrm{Res}}{\to} H^2(ML/L).$$

The argument for the Inflation–Restriction exact sequence is an explicit computation on cocycles (involving some dimension shifting), but it can be tracked backwards to give the desired cocycle.

6.3 Computation

In this section we record the details of the computation.

6.3.1 Explicit Inflation–Restriction

The results and commentary here mirror [Buc13, Section 2]. Throughout this section, G will be a group (usually finite) and $H \subseteq G$ will be a subgroup (usually normal).

We begin by recalling the statement of the Inflation–Restriction exact sequence; we will provide the proof for completeness because we will use the proof for our computation.

Theorem 151 ([AW10, Proposition 5])**.** Let G be a finite group with normal subgroup $H \subseteq G$. Given a G-module A, suppose that the $H^i(H, A) = 0$ for $1 \leq i < q$ for some index $q \geq 1$. Then the sequence

$$0 \to H^q\left(G/H, A^H\right) \overset{\mathrm{Inf}}{\to} H^q(G, A) \overset{\mathrm{Res}}{\to} H^q(H, A)$$

is exact.

Proof. The proof is by induction on q, via dimension shifting. For $q = 1$, we can just directly check this on 1-cocycles. The main point is the exactness at $H^q(G, A)$: if $c \in Z^1(G, A)$ has $\mathrm{Res}(c) \in B^1(H, A)$, then find $a \in A$ with

$$\mathrm{Res}(c)(a) \coloneqq h \cdot a - a.$$

As such, we define $f_a \in B^1(G, A)$ by $f_a(g) \coloneqq g \cdot a - a$, which implies that $c - f_a$ vanishes on H. It is then possible to stare at the 1-cocycle condition

$$(c - f_a)(gg') = (c - f_a)(g) + g \cdot (c - f_a)(g')$$

to check that $c - f_a$ only depends on the cosets of H (e.g., by taking $g' \in H$) and that $\mathrm{im}(c - f_a) \subseteq A^H$ (e.g., by taking $g \in H$).

For $q > 1$, we use dimension shifting via the following lemma. Indeed, suppose the statement is true for q. Then the short exact sequence

$$0 \to A \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \to \mathrm{Hom}_{\mathbb{Z}}(I_G, A) \to 0$$

induces vertical isomorphisms in the following commutative diagram.

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^q\left(G/H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H\right) & \longrightarrow & H^q(G, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) & \longrightarrow & H^q(H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \\
 & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\
0 & \longrightarrow & H^{q+1}\left(G/H, A^H\right) & \longrightarrow & H^{q+1}(G, A) & \longrightarrow & H^{q+1}(H, A)
\end{array}$$

The top row is exact by the inductive hypothesis, so the bottom row is therefore also exact. ■

Our goal is to make the above proof explicit in the case of $q = 2$, which is the only reason we sketched the above proofs at all. We begin by making the dimension shifting explicit.

Lemma 152 ([Buc13, Lemma 2.1])**.** Let G be a group with subgroup $H \subseteq G$, and let $\{g_\alpha\}_{\alpha\in\lambda}$ be coset representatives for $H\backslash G$. Now, given a G-module A, the maps

$$\begin{aligned}
\delta_H \colon Z^1(H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) &\to Z^2(H, A) \\
c &\mapsto \left[(h, h') \mapsto h \cdot c(h')(h^{-1} - 1)\right] \\
\left[h \mapsto \left((h' g_\bullet - 1) \mapsto h' \cdot u((h')^{-1}, h)\right)\right] &\hookleftarrow u
\end{aligned}$$

are group homomorphisms descending to the isomorphism $\overline{\delta} \colon H^1(H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \simeq H^2(H, A)$. The map δ_H above is surjective, and the reverse map is a section; when $H = G$, these are isomorphisms.

Proof. To show that δ_H descends to an isomorphism properly, we could track through dimension-shifting by hand, or we can use the machinery we've built. Namely, setting $X = \mathbb{Z}$ in Corollary 27 told us that the 1-cocycle $\chi \in Z^1(G, I_G)$ defined by

$$\chi(\sigma) \coloneqq (1 - \sigma)$$

provides an isomorphism

$$(\chi \cup -) \colon \widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)) \to \widehat{H}^{i+1}(G, A).$$

Computing our cup product, we have

$$\begin{aligned}
(\chi \cup c)(h, h') &= \big(hc(h')\big)\big(\chi(h)\big) \\
&= h \cdot c(h')\big(h^{-1}(1 - h)\big) \\
&= h \cdot c(h')\big(h^{-1} - 1\big).
\end{aligned}$$

So we see that $\delta_H = (\chi \cup -)$ on cocycles and therefore descends to the needed isomorphism. Additionally, it is a homomorphism by properties of the cup product.

It remains to prove the last sentence. We run the following checks; given $u \in Z^2(H, A)$, define $c_u \in C^1(H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A))$ by

$$c_u(h)(h' g_\bullet - 1) = h' \cdot u\left((h')^{-1}, h\right).$$

Note that this is enough data to define $c_u(h) \colon I_G \to A$ because I_G is a free $\mathbb{Z}$-module generated by $\{g - 1 : g \in G\}$.

- We verify that c_u is a 1-cocycle. This is a matter of force. Pick up $h, h' \in H$ and $g_\bullet h'' \in G$ and write

$$\begin{aligned}
&(hc_u(h'))(h'' g_\bullet - 1) + c_u(hh')(h'' g_\bullet - 1) + c_u(h)(h'' g_\bullet - 1) \\
&= h \cdot c_u(h')\left(h^{-1} h'' g_\bullet - h^{-1}\right) + c_u(hh')(h'' g_\bullet - 1) + c_u(h)(h'' g_\bullet - 1) \\
&= h \cdot \left(h^{-1} h'' u\left((h'')^{-1} h, h'\right) - h^{-1} u(h, h')\right) + h'' u\left((h'')^{-1}, hh'\right) + h'' u\left((h'')^{-1}, h\right) \\
&= h'' u\left((h'')^{-1} h, h'\right) - u(h, h') + h'' u\left((h'')^{-1}, hh'\right) + h'' u\left((h'')^{-1}, h\right).
\end{aligned}$$

  This is just the 2-cocycle condition for u upon dividing out by h'', so we are done.

- For $u \in Z^2(H, A)$, we verify that $\delta_H(c_u) = u$. Indeed, given $h, h' \in H$, we check

$$\begin{aligned}\delta_H(c_u)(h, h') &= h \cdot c_u(h') \left(h^{-1} - 1\right) \\ &= h \cdot h^{-1} \cdot u(h, h') \\ &= u(h, h').\end{aligned}$$

So far we have verified that δ has section $u \mapsto c_u$ and hence must be surjective. Lastly, we take $H = G$ and show that $c_{\delta c} = c$ to finish. Indeed, for $g, g' \in G = H$, we write

$$\begin{aligned}c_{\delta_H c}(g)(g' - 1) &= g' \cdot (\delta_H c)\left((g')^{-1}, g\right) \\ &= g'(g')^{-1} \cdot c(g)(g' - 1) \\ &= c(g)(g' - 1),\end{aligned}$$

which is what we wanted. ■

We also have used dimension shifting to show that $H^1\left(G/H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H\right) \to H^2\left(G/H, A^H\right)$ is an isomorphism, but this requires a little more trickery. To begin, we discuss how to lift from $\mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H$ to $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)^H$.

Lemma 153. Let G be a group with subgroup $H \subseteq G$. Fix a G-module A with $H^1(H, A) = 0$. Then, for any $\psi \in \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H$, the function $h \mapsto h\psi\left(h^{-1} - 1\right)$ is a cocycle in $Z^1(H, A) = B^1(H, A)$, so we can define a function $\eta_\bullet \colon \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H \to A$ such that

$$\psi(h - 1) = h \cdot \eta_\varphi - \eta_\varphi$$

for all $h \in H$. In fact, given $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H$, we can construct $\widetilde{\varphi} \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)^H$ by

$$\widetilde{\varphi}(z) \coloneqq \varphi(z - \varepsilon(z)) + \varepsilon(z)\eta_\varphi$$

so that $\widetilde{\varphi}|_{I_G} = \varphi$.

Proof. We will just run the checks directly.

- We start by checking $\psi \in \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H$ give 1-cocycles $c(h) \coloneqq \varphi\left(h - 1\right)$ in $Z^1(A, H)$. To begin, we note that $\psi \in \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H$ simply means that any $z - \varepsilon(z) \in I_G$ has

$$\psi(z - \varepsilon(z)) = (h\psi)(z - \varepsilon(z)) = h\psi\left(h^{-1}z - h^{-1}\varepsilon(z)\right)$$

  for all $h \in H$. In particular, replacing h with h^{-1} tells us that

$$h\psi(z - \varepsilon(z)) = \psi(hz - h\varepsilon(z)).$$

  Now, we can just compute

$$\begin{aligned}(dc)(h, h') &= hc(h') - c(hh') + c(h) \\ &= hc\left(h' - 1\right) - c\left(hh' - 1\right) + c\left(h - 1\right) \\ &= c\left(hh' - h\right) - c\left(hh' - 1\right) + c\left(h - 1\right),\end{aligned}$$

  where in the last equality we used the fact that $\psi \in \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H$. Now, $(dc)(h, h')$ manifestly vanishes, so we are done.

- Note that $\widetilde{\varphi} \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ because it is a linear combination of (compositions of) homomorphisms.

- Note that any $z \in I_G$ has $\varepsilon(z) = 0$, so

$$\widetilde{\varphi}(z) = \varphi(z - 0) + 0 \cdot \eta_\varphi = \varphi(z),$$

  so $\widetilde{\varphi}|_{I_G} = \varphi$.

- It remains to check that $\widetilde{\varphi}$ is fixed by H. This requires a little more effort. Recall that $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H$ means that any $z - \varepsilon(z) \in I_G$ has
$$h\varphi(z - \varepsilon(z)) = \varphi\left(hz - h\varepsilon(z)\right)$$
for any $h \in H$. Now, we just compute
$$\begin{aligned}(h\widetilde{\varphi})(z) &= h\widetilde{\varphi}\left(h^{-1}z\right)\\ &= h\left(\varphi\left(h^{-1}z - \varepsilon(h^{-1}z)\right) + \varepsilon(h^{-1}z)\eta_\varphi\right)\\ &= \varphi\left(z - h\varepsilon(z)\right) + \varepsilon(z)\cdot h\eta_\varphi\\ &= \varphi\left(z - h\varepsilon(z)\right) + \varepsilon(z)\varphi(h-1) + \varepsilon(z)\eta_\varphi\\ &= \varphi(z - \varepsilon(z)) + \varepsilon(z)\eta_\varphi\\ &= \widetilde{\varphi}(z).\end{aligned}$$

The above checks complete the proof. ∎

And now we can now make our dimension shifting explicit.

Lemma 154. Work in the context of Lemma 153 and assume that $H \subseteq G$ is normal. We track through the isomorphism
$$\delta\colon H^1\left(G/H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H\right) \simeq H^2\left(G/H, A^H\right)$$
given by the exact sequence
$$0 \to A^H \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)^H \to \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H \to 0.$$

Proof. We begin with some $c \in H^1\left(G/H, \mathrm{Hom}_{\mathbb{Z}}(I_G, A)^H\right)$. To track through the δ, we define
$$\widetilde{c}(gH) \coloneqq c(gH)(z - \varepsilon(z)) + \eta_{c(gH)}\varepsilon(z)$$
to be the lift given in Lemma 153. Now, we are given that $dc = 0$, which here means that any $z \in \mathbb{Z}[G]$ and $gH, g'H \in G/H$ will have
$$\begin{aligned}0 &= (dc)(gH, g'H)(z - \varepsilon(z))\\ 0 &= (gH\cdot c(g'H) - c(gg'H) + c(gH))(z - \varepsilon(z))\\ 0 &= g\cdot c(g'H)\left(g^{-1}z - g^{-1}\varepsilon(z)\right) - c(gg'H)(z - \varepsilon(z)) + c(gH)(z - \varepsilon(z))\\ g\cdot c(g'H)\left(g^{-1} - 1\right)\varepsilon(z) &= g\cdot c(g'H)\left(g^{-1}z - \varepsilon(z)\right) - c(gg'H)(z - \varepsilon(z)) + c(gH)(z - \varepsilon(z))\\ g\cdot c(g'H)\left(g^{-1} - 1\right)\varepsilon(z) &= g\cdot c(g'H)\left(g^{-1}z - \varepsilon(g^{-1}z)\right) - c(gg'H)(z - \varepsilon(z)) + c(gH)(z - \varepsilon(z)).\end{aligned}$$

We now directly compute that
$$\begin{aligned}(d\widetilde{c})(gH, g'H)(z) &= (gH\cdot c(g'H) - c(gg'H) + c(gH))(z)\\ &= g\cdot c(g'H)\left(g^{-1}z - \varepsilon(g^{-1}z)\right) + g\eta_{c(g'H)}\varepsilon(z)\\ &\quad - c(gg'H)(z - \varepsilon(z)) - \eta_{c(gg'H)}\varepsilon(z)\\ &\quad + c(gH)(z - \varepsilon(z)) + \eta_{c(gH)}\varepsilon(z)\\ &= \left(g\cdot c(g'H)\left(g^{-1} - 1\right) + g\cdot\eta_{c(g'H)} - \eta_{c(gg'H)} + \eta_{c(gH)}\right)\varepsilon(z)\end{aligned}$$

As such, we have pulled ourselves back to the 2-cocycle given by
$$\boxed{u(gH, g'H) \coloneqq g\cdot c(g'H)\left(g^{-1} - 1\right) + g\cdot\eta_{c(g'H)} - \eta_{c(gg'H)} + \eta_{c(gH)}}.$$

We quickly note that this is in fact independent of our choice of representative $g \in gH$: changing representative of g to gh for $h \in H$ will only affect the terms
$$h\cdot c(g'H)\left(h^{-1}g^{-1} - 1\right) + h\eta_{c(g'H)} = c(g'H)\left(g^{-1} - h\right) + c(g'H)(h-1) + \eta_{c(g'H)} = c(g'H)\left(g^{-1} - 1\right) + \eta_{c(g'H)},$$
so we are indeed safe. This completes the proof. ∎

We now make Theorem 151 explicit in the case of $q = 2$.

Lemma 155 ([Buc13, Lemma 2.3])**.** Let G be a group with normal subgroup $H \subseteq G$. Fix a G-module A with $H^1(H, A) = 0$, and define the function $\eta_\bullet : \operatorname{Hom}_{\mathbb{Z}}(I_G, A)^H \to A$ of Lemma 153. Given $c \in Z^2(G, A)$ such that $\operatorname{Res}^G_H c \in B^2(H, A)$; in particular, suppose we have $b \in \operatorname{Hom}_{\mathbb{Z}}(I_G, A)$ such that all $h \in H$ have

$$\operatorname{Res}^G_H(\delta^{-1}c)(h) = (db)(h) = h \cdot b - h,$$

where δ^{-1} is the inverse isomorphism of Lemma 152. Then we find $u \in Z^2\left(G/H, A^H\right)$ such that

$$[\operatorname{Inf} u] = [c]$$

in $H^2(G, A)$.

Proof. The main point is that boundary morphisms δ commute with Res and Inf. By construction, we have that $\left(\operatorname{Res}^G_H \delta^{-1}c\right) - db = 0$ in $Z^1(H, \operatorname{Hom}_{\mathbb{Z}}(I_G, A))$. Pulling back to $Z^1(G, \operatorname{Hom}_{\mathbb{Z}}(I_G, A))$, we note that

$$c' \coloneqq \left(\delta^{-1}c - db\right) \in Z^1(G, \operatorname{Hom}_{\mathbb{Z}}(I_G, A))$$

vanishes on H by hypothesis. Because $\delta^{-1}c - db$ is a 1-cocycle, we are able to write

$$c'(gg') = c'(g) + gc'(g').$$

Letting g' vary over H, we see that $\delta^{-1}c - db$ is well-defined on G/H. On the other hand, for any $h \in H$ and $g \in G$, we note that $g^{-1}hg \in H$, so

$$c'(g) = c'\left(g \cdot g^{-1}hg\right) = c'\left(hg\right) = c'\left(h\right) + hc(g),$$

implying that $c'(g) \in \operatorname{Hom}_{\mathbb{Z}}(I_G, A)^H$.

We are now ready to apply Lemma 154, which we use on c', thus defining $u \coloneqq \delta(c')$. Explicitly, we have

$$\boxed{u(gH, g'H) = g \cdot c'(g'H)\left(g^{-1} - 1\right) + g \cdot \eta_{c'(g'H)} - \eta_{c'(gg'H)} + \eta_{c'(gH)}}.$$

This is explicit enough for our purposes. Observe that $[\operatorname{Inf} u] = [c]$ because $[\operatorname{Inf} c'] = [\delta^{-1}c]$, and δ commutes with Inf. ∎

6.3.2 Computing the Cocycle

Given a finite Galois extension E/F of local fields, we will let $c_{E/F}$ denote a representative of the fundamental class in $H^2(\operatorname{Gal}(E/F), E^\times)$.

We now return to the set-up in subsection 6.1 and track through Lemma 155 in our case. For reference, the following is the diagram that we will be chasing around; here $G \coloneqq \operatorname{Gal}(ML/K)$ and $H \coloneqq \operatorname{Gal}(ML/L)$.

$$\begin{array}{ccccccc}
 & & & & H^2(\operatorname{Gal}(M/K), M^\times) & & \\
 & & & & \downarrow{\scriptstyle \operatorname{Inf}} & & \\
0 & \longrightarrow & H^2(\operatorname{Gal}(L/K), L^\times) & \xrightarrow{\operatorname{Inf}} & H^2(G, ML^\times) & \xrightarrow{\operatorname{Res}} & H^2(\operatorname{Gal}(ML/L), ML^\times) \\
 & & \uparrow{\scriptstyle \delta} & & \uparrow{\scriptstyle \delta} & & \uparrow{\scriptstyle \delta} \\
0 & \longrightarrow & H^1(G/H, \operatorname{Hom}_{\mathbb{Z}}(I_G, ML^\times)^H) & \xrightarrow{\operatorname{Inf}} & H^1(G, \operatorname{Hom}_{\mathbb{Z}}(I_G, ML^\times)) & \xrightarrow{\operatorname{Res}} & H^1(H, \operatorname{Hom}_{\mathbb{Z}}(I_G, ML^\times))
\end{array}$$

To begin, we know that we can write

$$c_{M/K}\left(\sigma_K^i, \sigma_K^j\right) \coloneqq \pi^{\left\lfloor \frac{i+j}{n} \right\rfloor} = \begin{cases} 1 & i + j < n, \\ \pi & i + j \geq n, \end{cases}$$

where π is a uniformizer of K. Inflating this down to $H^2(G, ML^\times)$ gives

$$(\operatorname{Inf} c_{M/K})\left(\sigma_K^{a_1}\tau, \sigma_K^{b_1}\tau'\right) = \pi^{\left\lfloor \frac{a_1+b_1}{n}\right\rfloor}.$$

Now, we use Lemma 152 to move down to $H^1(G, \operatorname{Hom}_{\mathbb{Z}}(I_G, ML^\times))$ as

$$\delta^{-1}(\operatorname{Inf} c_{M/K})\left(\sigma_K^{a_1}\tau\right)\left(\sigma_K^{b_1}\tau' - 1\right) = \sigma_K^{b_1}\tau' \cdot (\operatorname{Inf} u_{M/K})\left(\sigma_K^{[-b_1]}(\tau')^{-1}, \sigma_K^{a_1}\tau\right) = \pi^{\left\lfloor \frac{a_1+[-b_1]}{n}\right\rfloor},$$

where $[k]$ denote the integer $0 \le [k] < n$ such that $k \equiv [k] \pmod n$.

It will be helpful to see explicitly that the restriction to $H = \langle \sigma_k^f \rangle$ is a coboundary. That is, we need to find $b \in \operatorname{Hom}_{\mathbb{Z}}(I_G, ML^\times)$ such that

$$\delta^{-1}(\operatorname{Inf} u_{M/K})\left(\sigma_K^{fa_1}\right) = \frac{\sigma_K^{fa_1} \cdot b}{b}.$$

Because I_G is freely generated by elements of the form $g - 1$ for $g \in G$, it suffices to plug in some arbitrary $\sigma_K^{b_1}\tau' - 1$, which we see requires

$$\begin{aligned}\pi^{\left\lfloor \frac{fa_1+[-b_1]}{n}\right\rfloor} &= \frac{\left(\sigma_K^{fa_1} \cdot b\right)\left(\sigma_K^{b_1}\tau' - 1\right)}{b\left(\sigma_K^{b_1}\tau' - 1\right)} \\ &= \frac{\sigma_K^{fa_1} b\left(\sigma_K^{b_1 - fa_1}\tau' - 1\right)}{\sigma_K^{fa_1} b\left(\sigma_K^{-fa_1} - 1\right) b\left(\sigma_K^{b_1}\tau' - 1\right)}.\end{aligned}$$

We can see that b should not depend on τ', so we define $\hat{b}\left(\sigma_K^a\right) = b\left(\sigma_K^a\tau' - 1\right)$; the above is then equivalent to

$$\begin{aligned}\pi^{\left\lfloor \frac{fa_1+[-b_1]}{n}\right\rfloor} &= \frac{\sigma_K^{fa_1}\hat{b}\left(\sigma_K^{b_1 - fa_1}\right)}{\sigma_K^{fa_1}\hat{b}\left(\sigma_K^{-fa_1}\right)\hat{b}\left(\sigma_K^{b_1}\right)} \\ \pi^{\left\lfloor \frac{fa_1+b_1}{n}\right\rfloor} &= \frac{\hat{b}\left(\sigma_K^{-b_1 - fa_1}\right)}{\hat{b}\left(\sigma_K^{-fa_1}\right)\sigma_K^{-fa_1}\hat{b}\left(\sigma_K^{-b_1}\right)},\end{aligned}$$

where we have negated b_1 in the last step. At this point, the right-hand side will look a lot more natural if we set $\tau_K \coloneqq \sigma_K^{-1}$, which turns this into

$$\frac{\hat{b}\left(\tau_K^{fa_1}\right)\tau_K^{fa_1}\hat{b}\left(\tau_K^{b_1}\right)}{\hat{b}\left(\tau_K^{b_1 fa_1}\right)} = (1/\pi)^{\left\lfloor \frac{fa_1+b_1}{n}\right\rfloor}$$

after taking reciprocals. Thus, we see that $\hat{b}$ should be counting carries of τ_Ks. With this in mind, we let ϖ be a uniformizer of $K_{\pi,\nu}$ and note that ϖ is also a uniformizer of L because $L/K_{\pi,\nu}$ is an unramified extension. It follows that

$$\varpi^{[ML:L]} \in \mathrm{N}_{ML/L}\left(ML^\times\right).$$

Further, $\varpi^{[ML:L]}$ has the same absolute value as π because $K_{\pi,\nu}/K$ is a totally ramified extension of degree $[K_{\pi,\nu} : K] = [ML : M] = [ML : L]$. Thus, $\pi/\varpi^{[ML:L]}$ and therefore π is a norm in $\mathrm{N}_{ML/L}(ML^\times)$ because ML/L is unramified and so $\mathcal{O}_L^\times \subseteq \mathrm{N}_{ML/L}(ML^\times)$. Thus, we find $\gamma \in ML^\times$ such that

$$\mathrm{N}_{ML/L}(\gamma) = \pi.$$

The point of doing all of this is so that we can codify our carrying by writing

$$\hat{b}\left(\tau_K^a\right) \coloneqq \prod_{i=0}^{\lfloor a/f\rfloor - 1} \tau_K^{if}(\gamma)^{-1}.$$

Tracking out $\hat{b}$ backwards to b, our desired $b \in \mathrm{Hom}_{\mathbb{Z}}(I_G, ML^\times)$ is given by

$$\boxed{b\left(\sigma_K^a \tau - 1\right) = \prod_{i=0}^{\lfloor [-a]/f \rfloor - 1} \sigma_K^{-if}(\gamma)^{-1}}.$$

We take a moment to write out $c \coloneqq \delta^{-1}(\mathrm{Inf}\, c_{M/K})/db$, which looks like

$$\begin{aligned}
c\left(\sigma_K^{a_1}\tau\right)\left(\sigma_K^{b_1}\tau' - 1\right) &= \frac{\delta^{-1}(\mathrm{Inf}\, c_{M/K})}{db}\left(\sigma_K^{a_1}\tau\right)\left(\sigma_K^{b_1}\tau' - 1\right) \\
&= \frac{\delta^{-1}(\mathrm{Inf}\, c_{M/K})\left(\sigma_K^{a_1}\tau\right)\left(\sigma_K^{b_1}\tau' - 1\right)}{\left(\sigma_K^{a_1}\tau \cdot b\right)\left(\sigma_K^{b_1}\tau' - 1\right)/b\left(\sigma_K^{b_1}\tau' - 1\right)} \\
&= \frac{\pi^{\lfloor (a_1 + [-b_1])/n \rfloor}}{\sigma_K^{a_1}\tau \cdot b\left(\sigma_K^{b_1 - a_1}\tau'\tau^{-1} - \sigma_K^{-a_1}\tau^{-1}\right)/b\left(\sigma_K^{b_1}\tau' - 1\right)} \\
&= \pi^{\lfloor (a_1 + [-b_1])/n \rfloor} \cdot \hat{b}\left(\sigma_K^{b_1}\right) \cdot \sigma_K^{a_1}\tau\left(\frac{\hat{b}\left(\sigma_K^{-a_1}\right)}{\hat{b}\left(\sigma_K^{b_1 - a_1}\right)}\right).
\end{aligned}$$

Before proceeding, we discuss a few special cases.

- Taking $\sigma_K^{a_1}\tau = \tau_i$ for some τ_i, we get

$$\begin{aligned}
c\left(\tau_i\right)\left(\sigma_K^{b_1}\tau' - 1\right) &= \pi^{\lfloor (0 + [-b_1])/n \rfloor} \cdot \hat{b}\left(\sigma_K^{b_1}\right) \cdot \tau_i\left(\frac{1}{\hat{b}\left(\sigma_K^{b_1}\right)}\right) \\
&= \hat{b}\left(\sigma_K^{b_1}\right)/\tau_i \hat{b}\left(\sigma_K^{b_1}\right).
\end{aligned}$$

  In particular, $c\left(\tau_i\right)\left(\sigma_K^{-1} - 1\right) = 1$, provided that $f > 1$. Additionally, $c(\tau_i)\left(\tau' - 1\right) = 1$.

  Our general theory says that $h \mapsto c(\tau_i)(h-1)$ is a 1-cocycle in $Z^1(H, ML^\times)$ (though we could also check this directly), so Hilbert's Theorem 90 promises us a magical element $\eta_i \in ML^\times$ such that

$$\frac{\sigma_K^{fb_1}\eta_i}{\eta_i} = \frac{\hat{b}\left(\sigma_K^{fb_1}\right)}{\tau_i \hat{b}\left(\sigma_K^{fb_1}\right)}$$

  for all $\sigma_K^{fb_1} \in H$. This condition will be a little clearer if we write everything in terms of $\tau_K \coloneqq \sigma_K^{-1}$, which transforms this into

$$\frac{\tau_K^{fb_1}\eta_i}{\eta_i} = \frac{\hat{b}\left(\tau_K^{-fb_1}\right)}{\tau_i \hat{b}\left(\tau_K^{-fb_1}\right)} = \prod_{i=0}^{b_1 - 1} \frac{\tau_K^{if}(\gamma^{-1})}{\tau_i \tau_K^{if}(\gamma^{-1})} = \prod_{i=0}^{b_1 - 1} \frac{\tau_i \tau_K^{if}(\gamma)}{\tau_K^{if}(\gamma)}.$$

  Because we are dealing with a cyclic group H, it is not too hard to see that it suffices merely for $b_1 = 1$ to hold, so our magical element η_i merely requires

$$\boxed{\frac{\sigma_K^{-f}(\eta_i)}{\eta_i} = \frac{\tau_i(\gamma)}{\gamma}}$$

  after inverting τ_K back to σ_K.

- Taking $\sigma_K^{a_1}\tau = \sigma_K$, we get

$$c(\sigma_K)\left(\sigma_K^{b_1}\tau' - 1\right) = \pi^{\lfloor (1+[-b_1])/n \rfloor} \cdot \hat{b}\left(\sigma_K^{b_1}\right) \cdot \sigma_K\left(\frac{\hat{b}\left(\sigma_K^{-1}\right)}{\hat{b}\left(\sigma_K^{b_1-1}\right)}\right).$$

In particular, $\sigma_K^{b_1}\tau' = \tau_i^{-1}$ will give $c(\sigma_K)\left(\tau_i^{-1} - 1\right) = 1$. We will also want $c(\sigma_K)\left(\sigma_K^{-b_1} - 1\right)$ for $0 \leq b_1 < f$. We now have two cases.

  - Suppose that L/K is not totally ramified so that $f > 1$. Using the fact that $f < n$ and $f > 1$, it is not too hard to see that everything will cancel down to 1 except in the case where $b_1 = f - 1$, where we get

$$c(\sigma_K)\left(\sigma_K^{-(f-1)} - 1\right) = \sigma_K\left(\frac{1}{\hat{b}\left(\sigma_K^{-f}\right)}\right) = \sigma_K(\gamma).$$

  - Otherwise, our extension is totally ramified so that $f = 1$. Here, $b_1 = 0$ is forced, so we are computing $c(\sigma_K)(\tau' - 1) = 1$. (Our extension being unramified promises $n > 1$.)

Continuing as before, our general theory says that $h \mapsto c(\sigma_K)(h-1)$ is a 1-cocycle in $Z^1(H, ML^\times)$, though again we could just check this directly. It follows that Hilbert's Theorem 90 promises us a magical element $\eta_K \in ML^\times$ such that

$$\frac{\sigma_K^{fb_1}\eta_K}{\eta_K} = \pi^{\lfloor (1+[-fb_1])/n \rfloor} \cdot \hat{b}\left(\sigma_K^{fb_1}\right) \cdot \sigma_K\left(\frac{\hat{b}\left(\sigma_K^{-1}\right)}{\hat{b}\left(\sigma_K^{fb_1-1}\right)}\right)$$

for all $\sigma_K^{fb_1} \in H$. To simplify this condition, we once again split into two cases.

  - Suppose that L/K is not totally ramified so that $f > 1$. Using $f > 1$, this collapses down to

$$\frac{\sigma_K^{fb_1}\eta_K}{\eta_K} = \frac{\hat{b}\left(\sigma_K^{fb_1}\right)}{\sigma_K\hat{b}\left(\sigma_K^{fb_1-1}\right)}.$$

    As before, this condition will be a little clearer if we set $\tau_K \coloneqq \sigma_K^{-1}$, which turns the condition into

$$\frac{\tau_K^{fb_1}\eta_K}{\eta_K} = \frac{\hat{b}\left(\tau_K^{fb_1}\right)}{\sigma_K\hat{b}\left(\tau_K^{fb_1+1}\right)} = \prod_{i=0}^{b_1-1} \frac{\tau_K^{if}(\gamma^{-1})}{\sigma_K\tau_K^{if}(\gamma^{-1})} = \prod_{i=0}^{b_1-1} \frac{\sigma_K\tau_K^{if}(\gamma)}{\tau_K^{if}(\gamma)}.$$

    (Notably, $\hat{b}\left(\tau_K^{fb_1}\right) = \hat{b}\left(\tau_K^{fb_1+1}\right)$ because $f > 1$.) Again, because H is cyclic generated by τ_K^f, an induction shows that it suffices to check this condition for $b_1 = 1$, which means that our magical element $\eta_K \in ML^\times$ is constructed so that

$$\boxed{\frac{\sigma_K^{-f}(\eta_K)}{\eta_K} = \frac{\sigma_K(\gamma)}{\gamma}}$$

    where we have again inverted back from τ_K to σ_K.

  - Suppose that L/K is totally ramified so that $f = 1$. Switching over to τ_K as usual, we can evaluate

$$\frac{\tau_K^{b_1}\eta_K}{\eta_K} = \pi^{\lfloor (1+b_1)/n \rfloor} \cdot \hat{b}\left(\tau_K^{b_1}\right) \cdot \tau_K^{-1}\left(\frac{\hat{b}\left(\tau_K\right)}{\hat{b}\left(\tau_K^{b_1+1}\right)}\right) = \pi^{\lfloor (1+b_1)/n \rfloor} \cdot \tau_K^{-1}\left(\frac{\tau_K\hat{b}\left(\tau_K^{b_1}\right) \cdot \hat{b}(\tau_K)}{\hat{b}\left(\tau_K^{b_1+1}\right)}\right).$$

When $b_1 < n-1$, everything will cancel out. When $b_1 = n-1$, then $\hat{b}(\tau_K^{b_1+1}) = 1$ while $\tau_K \hat{b}(\tau_K^{b_1}) \cdot \hat{b}(\tau_K)$ collects to $\prod_{i=0}^{n-1} \tau_K(\gamma)^{-1} = \pi^{-1}$, so everything will still cancel out. So we want

$$\frac{\tau_K^{b_1} \eta_K}{\eta_K} = 1,$$

for which $\eta_K = 1$ suffices. As usual, it suffices to just look at $b_1 = 1$ by an induction, so we are asking for $\tau_K \eta_K / \eta_K = 1$.

- We will not actually need a more concrete description of this, but we remark that we can run the same story for any $g \in G$ through to get an element $\eta_g \in ML^\times$ such that

$$\frac{\sigma_K^{fb_1} \eta_g}{\eta_g} = \frac{1}{c(g)(\sigma_K^{fb_1} - 1)}$$

for any $\sigma_K^{fb_1} \in H$. As usual, this follows from our general theory.

We are now ready to describe the local fundamental class. Piecing what we have so far, we know from Lemma 155 that we can write

$$c_{L/K}(g, g') \coloneqq g \cdot c(g') \left(g^{-1} - 1\right) \cdot \frac{g\eta_{g'} \cdot \eta_g}{\eta_{gg'}}.$$

This will be explicit enough for us.

6.3.3 Computing the Tuple

We now use our computation of $c_{L/K}$ representing $u_{L/K}$ from the previous subsection to compute the tuple corresponding to $c_{L/K}$. Here are the values that we care about for our specific computation; for consistency, we set $\tau_0 \coloneqq \sigma_K$ and $n_0 \coloneqq f$ to be the order of τ_0.

- We write

$$\begin{aligned} c_{L/K}(\sigma_K, \tau_i) &= \sigma_K c(\tau_i) \left(\sigma_K^{-1} - 1\right) \cdot \frac{\sigma_K \eta_i \cdot \eta_K}{\eta_{\sigma_K \tau_i}} \\ &= \frac{\sigma_K \eta_i \cdot \eta_K}{\eta_{\sigma_K \sigma_x}}. \end{aligned}$$

- We write

$$\begin{aligned} c_{L/K}(\tau_i, \sigma_K) &= \tau_i c(\sigma_K) \left(\tau_i^{-1} - 1\right) \cdot \frac{\tau_i \eta_K \cdot \eta_i}{\eta_{\sigma_x \sigma_K}} \\ &= \frac{\tau_i \eta_K \cdot \eta_i}{\eta_{\sigma_x \sigma_K}}. \end{aligned}$$

- In particular, we know that we can set β_{i0} to

$$\begin{aligned} \beta_{i0} &\coloneqq \frac{c_{L/K}(\tau_i, \sigma_K)}{c_{L/K}(\sigma_K, \tau_i)} \\ &= \frac{\tau_i \eta_K \cdot \eta_i / \eta_{\sigma_x \sigma_K}}{\sigma_K \eta_i \cdot \eta_K / \eta_{\sigma_K \sigma_x}} \\ \boxed{\beta_{i0} &= \frac{\eta_i}{\sigma_K(\eta_i)} \cdot \frac{\tau_i(\eta_K)}{\eta_K}}. \end{aligned}$$

- We write

$$\begin{aligned} c_{L/K}(\tau_i, \tau_j) &= \tau_i c(\tau_j) \left(\tau_j^{-1} - 1\right) \cdot \frac{\tau_i \eta_j \cdot \eta_i}{\eta_{\tau_i \tau_j}} \\ &= \frac{\tau_i \eta_j \cdot \eta_i}{\eta_{\tau_i \tau_j}}. \end{aligned}$$

- Thus, for $i > j > 0$, we can set β_{ij} to

$$\begin{aligned}\beta_{ij} &\coloneqq \frac{c_{L/K}(\tau_i, \tau_j)}{c_{L/K}(\tau_j, \tau_i)} \\ &= \frac{\tau_i \eta_j \cdot \eta_i / \eta_{\tau_i \tau_j}}{\tau_j \eta_i \cdot \eta_j / \eta_{\tau_i \tau_j}} \\ \boxed{\beta_{ij} &= \frac{\eta_i}{\tau_j \eta_i} \cdot \frac{\tau_i \eta_j}{\eta_j}}.\end{aligned}$$

- For α_0, our element is given by

$$\begin{aligned}\alpha_0 &\coloneqq \prod_{i=0}^{f-1} c_{L/K}\left(\sigma_K^i, \sigma_K\right) \\ &= \prod_{i=0}^{f-1} \left(\sigma_K^i c\left(\sigma_K\right)\left(\sigma_K^{-i} - 1\right) \cdot \frac{\sigma_K^i \eta_K \cdot \eta_{\sigma_K^i}}{\eta_{\sigma_K^{i+1}}} \right).\end{aligned}$$

  Recall from our general theory that η_g only depends on the coset of g in G/H, so we see that the product of the quotients $\eta_{\sigma_K^i} / \eta_{\sigma_K^{i+1}}$ will cancel out.

  To finish the computation, we have two cases.

  - If L/K is not totally ramified, we know from our computation that this is 1 until $i = f - 1$, which gives $\sigma_K(\gamma)$. As such, we collapse down to

$$\alpha_0 = \sigma_K^f(\gamma) \cdot \prod_{i=0}^{f-1} \sigma_K^i\left(\eta_K\right) = \boxed{\sigma_K^f(\gamma) \cdot \sigma_K^{(f)}(\eta_K)}.$$

  - If L/K is totally ramified so that $f = 1$, then we computed $c(\sigma_K)(\sigma_K^{-i} - 1) = 0$ always—note we only have an $i = 0$ term—so we are left with just $\boxed{\eta_K = \sigma_K^{(f)} \eta_K}$.

- For α_i with $i > 0$, our element is given by

$$\begin{aligned}\alpha_i &\coloneqq \prod_{p=0}^{n_i - 1} c_{L/K}\left(\tau_i^p, \tau_i\right) \\ &= \prod_{p=0}^{n_i - 1} \tau_i^p c(\tau_i)\left(\tau_i^{-p} - 1\right) \cdot \frac{\tau_i^p \eta_i \cdot \eta_{\tau_i^p}}{\eta_{\tau_i^{p+1}}}.\end{aligned}$$

  Recalling that τ_i has order n_i, our quotient term $\eta_{\tau_i^i} / \eta_{\tau_i^{i+1}}$ will again cancel out. Additionally, the cocycle c always spits out 1 on these inputs, so we are left with

$$\alpha_i = \prod_{p=0}^{n_i - 1} \tau_i^p\left(\eta_i\right) = \boxed{\tau_i^{(n_i)}(\eta_i)}.$$

We summarize the results above in the following theorem.

Theorem 156. Fix everything as in the set-up. Then there exists some $\gamma \in ML^\times$ such that $\mathrm{N}_{ML/L}(\gamma) = \pi$ and elements in $\eta_K, \eta_i \in ML^\times$ for $1 \le i \le t$ such that

$$\frac{\sigma_K^{-f}(\eta_K)}{\eta_K} = \begin{cases} \sigma_K(\gamma)/\gamma & L/K \text{ not totally ramified,} \\ 1 & L/K \text{ totally ramified,} \end{cases} \quad \text{and} \quad \frac{\sigma_K^{-f}(\eta_i)}{\eta_i} = \frac{\tau_i(\gamma)}{\gamma}.$$

Then the tuple given by

$$\alpha_i := \begin{cases} \sigma_K^f(\gamma) \cdot \sigma_K^{(f)}(\eta_K) & i = 0,\ L/K \text{ not totally ramified,} \\ \tau_i^{(n_i)}(\eta_i) & \text{else,} \end{cases} \quad \text{and} \quad \beta_{ij} := \frac{\eta_i}{\tau_j \eta_i} \cdot \frac{\tau_i \eta_j}{\eta_j},$$

where $n_0 = f$ and $\tau_0 = \sigma_K$, corresponds to the fundamental class $u_{L/K} \in H^2(\mathrm{Gal}(L/K), L^\times)$.

We remark that we can replace $\sigma_K^f(\gamma)$ with merely γ (which still has norm p) while keeping all other variables the same; this gives us the following slightly prettier presentation. Note that we have multiplied the equations for $\eta_\bullet$ by σ_K^f on both sides.

Corollary 157. Fix everything as in the set-up. Then there exists some $\gamma \in ML^\times$ such that $\mathrm{N}_{ML/L}(\gamma) = \pi$ and elements in $\eta_K, \eta_i \in ML^\times$ (for $1 \le i \le t$) such that

$$\frac{\eta_K}{\sigma_K^f(\eta_K)} = \begin{cases} \sigma_K(\gamma)/\gamma & L/K \text{ not totally ramified,} \\ 1 & L/K \text{ totally ramified,} \end{cases} \quad \text{and} \quad \frac{\eta_i}{\sigma_K^f(\eta_i)} = \frac{\tau_i(\gamma)}{\gamma}.$$

Then the tuple given by

$$\alpha_i := \begin{cases} \gamma \cdot \sigma_K^{(f)}(\eta_K) & i = 0,\ L/K \text{ not totally ramified,} \\ \tau_i^{(n_i)}(\eta_i) & \text{else,} \end{cases} \quad \text{and} \quad \beta_{ij} := \frac{\eta_i}{\tau_j \eta_i} \cdot \frac{\tau_i \eta_j}{\eta_j},$$

where $n_0 = f$ and $\tau_0 = \sigma_K$, corresponds to the fundamental class $u_{L/K} \in H^2(\mathrm{Gal}(L/K), L^\times)$.

For brevity later on, we will give a name to these conditions.

Definition 158. Fix an extension L/K. The $\{\sigma_i\}_{i=1}^m$-tuples constructed in Corollary 157 will be called *fundamental tuples*.

We will show shortly that fundamental tuples actually give the entire equivalence class of $\{\sigma_i\}_{i=1}$-tuples associated to the fundamental class.

Remark 159. This result is essentially a stronger version of Dwork's theorem [Ser91, Theorem XIII.2]. Namely, Dwork and Serre are interested in computing the reciprocity map, which roughly means we only want access to the αs, but above we are interested in computing the full fundamental class.

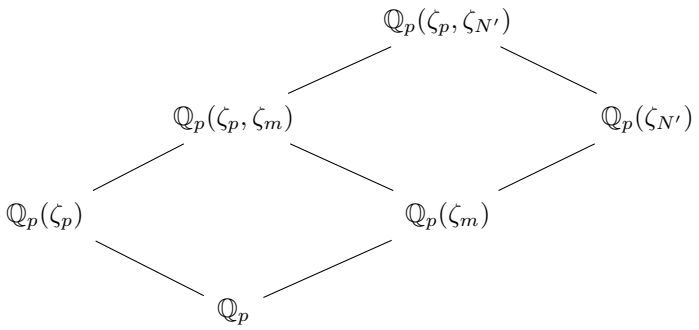
Remark 160. The $\eta_\bullet$s have a degree of freedom in that these elements are unique only up to multiplication by a nonzero element of $ML^{\langle \sigma_K^f \rangle} = L$. As the $\eta_\bullet$s vary (with γ fixed), it is not too hard to see directly from the formulae that we will encounter a full equivalence class of tuples. We will not write this out.

Remark 161. Even when L/K is unramified, which we technically disallowed for our computation, we can see that $M = L$ and then $\gamma = \pi$ so that $\eta_K = 1$ are all forced, giving $\alpha_0 = \pi$. So indeed, the above formulation does work for all abelian extensions L/K.

6.4 Tame Ramification

In this section, we work through Corollary 157 very explicitly in a basic case. Let p be an odd prime because the following discussion has no content in the case of $p = 2$. Set $K \coloneqq \mathbb{Q}_p$ and $K_m \coloneqq \mathbb{Q}_p(\zeta_m)$ with $f \coloneqq [\mathbb{Q}_p(\zeta_m) : \mathbb{Q}_p]$.

The main simplification we will make which allows explicit computation is that we will set $K_{\pi,\nu} \coloneqq \mathbb{Q}_p(\zeta_p)$. Continuing with the set-up, we see $L = \mathbb{Q}_p(\zeta_p, \zeta_m)$ with $n \coloneqq (p-1) \cdot f$; as such, set $N' \coloneqq p^n - 1$ so that $M = \mathbb{Q}_p(\zeta_{N'})$. Here is the diagram of our fields.



So that we are able to isolate our set-up, we note that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$$

is cyclic, so we choose some $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ to generate, which corresponds to the automorphism $\sigma_x \colon \zeta_p \mapsto \zeta_p^x$. Namely, we may set $\tau_1 \coloneqq \sigma_x$.

Now, the reason we set $K_{\pi,\nu} = \mathbb{Q}_p(\zeta_p)$ is that we will be able to set

$$\gamma \coloneqq (-p)^{1/(p-1)} \in \mathbb{Q}_p(\zeta_p).$$

Indeed, we sneakily set $\pi = -p$ to be our uniformizer of $\mathbb{Q}_p$ so that $\mathrm{N}_{ML/L}(\gamma) = \gamma^{p-1} = -p$. Because it will be helpful for us shortly, we will actually give a construction of $(-p)^{1/(p-1)}$, for completeness.

Lemma 162. Let p be a prime. Then we can find some $\gamma \coloneqq (-p)^{1/(p-1)}$ in $\mathbb{Q}_p(\zeta_p)$. In fact, we can take $\gamma \equiv c\varpi \pmod{\varpi^2}$ for any $c \in \mathbb{F}_p^\times$, where $\varpi \coloneqq \zeta_p - 1$ is a uniformizer.

Proof. That a root γ exists is well-known. The factorization

$$x^{p-1} - 1 \equiv \prod_{c \in \mathbb{F}_p^\times} (x - c) \pmod{p}$$

lifts to a factorization in $\mathbb{Z}_p$ by [Neu99, Lemma II.4.6]. As such, as soon as we have one root γ of $x^{p-1} + p$, observe that $|\gamma| = p^{1/(p-1)} = |\varpi|$, so γ is a uniformizer as well, meaning that the c in

$$\zeta_{p-1}\gamma \equiv c\varpi \pmod{\varpi^2}$$

is nonzero and will vary across all representatives in $\mathbb{F}_p^\times$ as we exchange the root γ with $\zeta_{p-1}\gamma$ for various ζ_{p-1}. ∎

In light of Lemma 162, we will just take γ to have $\gamma^{p-1} = -p$ with $\gamma \equiv c\pi \pmod{\pi^2}$ for any particular $c \in \mathbb{F}_p^\times$. This satisfies $\mathrm{N}_{ML/L}(\gamma) = -p$ as discussed above.

We will now compute the tuple. We start with the unramified side because it is easier. Namely, $\gamma \in \mathbb{Q}_p(\zeta_p)$ is fixed by the Frobenius automorphism σ_K, so we may set $\eta_K \coloneqq 1$ to have

$$\frac{\eta_K}{\sigma_K^f(\eta_K)} = 1 = \frac{\sigma_K(\gamma)}{\gamma}.$$

The corresponding α_0 is thus

$$\boxed{\alpha_0 = \gamma}.$$

We now deal with ramification. We begin with a computational lemma, tying in what we have with Teichmüller lifts.

Lemma 163. Fix everything as above. Then $\zeta_{p-1} \coloneqq \sigma_x(\gamma)/\gamma$ is a primitive $(p-1)$st root of unity and in particular lies in $\mathbb{Q}_p$. In fact, $\zeta_{p-1} \equiv x \pmod{p}$.

Note that we are defining ζ_{p-1} above, which is okay: in the worst case, we might have to adjust the definitions of $\zeta_{N'}$ and ζ_m to correspond with this particular ζ_{p-1}, but otherwise ζ_{p-1} may be any fixed primitive $(p-1)$st root of unity.

Proof. To see that ζ_{p-1} is a $(p-1)$st root of unity, we note that $\sigma_x(\gamma) = \zeta_{p-1} \cdot \gamma$, so an induction shows that

$$\sigma_x^k(\gamma) = \zeta_{p-1}^k \cdot \gamma.$$

Setting $k = p-1$ shows that $\zeta_{p-1}^{p-1} = 1$, so ζ_{p-1} is a $(p-1)$st root of unity.

We next show $\zeta_{p-1} \equiv x \pmod{p}$; this will automatically imply that ζ_{p-1} is primitive because it will force ζ_{p-1} to have at least the order of $x \pmod{p}$, which is $p-1$. Let $\varpi \coloneqq \zeta_p - 1$ be a uniformizer of $\mathbb{Q}_p(\zeta_p)$. Because $\zeta_{p-1}, x \in \mathbb{Q}_p$, it is enough for $v_{\mathbb{Q}_p}(\zeta_{p-1} - x) > 0$; as such, we will show that

$$\zeta_{p-1} \overset{?}{\equiv} x \pmod{\varpi}.$$

To see this, recall $\gamma \equiv c\varpi \pmod{\varpi^2}$, so

$$\zeta_{p-1} = \frac{\sigma_x(\gamma)}{\gamma} \equiv \frac{c \cdot \sigma_x(\varpi)}{c \cdot \varpi} \equiv \frac{\sigma_x(\varpi)}{\varpi} \pmod{\varpi}.$$

However, $\sigma_x(\varpi) = \zeta_p^x - 1$, so

$$\frac{\sigma_x(\varpi)}{\varpi} = \frac{\zeta_p^x - 1}{\zeta_p - 1} \equiv 1 + \zeta_p + \cdots + \zeta_p^{x-1} \equiv \underbrace{1 + \cdots + 1}_{x} \equiv x \pmod{\varpi},$$

finishing. ∎

We are almost able to compute $\eta_x \coloneqq \eta_1$. To do this, we pick up a quick lemma.

Lemma 164. Let p and f be integers. Then

$$\frac{p^{f(p-1)} - 1}{(p-1)\,(p^f - 1)} \in \mathbb{Z}.$$

Proof. Observe

$$\frac{p^{f(p-1)} - 1}{p^f - 1} = \sum_{k=0}^{p-1} p^{fk} \equiv \sum_{k=0}^{p-1} 1 = p - 1 \equiv 0 \pmod{p-1}.$$

This finishes. ∎

In light of the above lemma, we define

$$z \coloneqq -\frac{p^{f(p-1)} - 1}{(p-1)\,(p^f - 1)}.$$

Note the sign here: it is very important! It follows that $\eta_x \coloneqq \zeta_{N'}^z$ will have

$$\frac{\eta_x}{\sigma_K^f(\eta_x)} = \frac{\zeta_{N'}^z}{\zeta_{N'}^{zp^f}} = \zeta_{N'}^{-z\left(p^f-1\right)} = \zeta_{N'}^{N'/(p-1)} = \zeta_{p-1},$$

which is indeed $\sigma_x(\gamma)/\gamma$. Thus, the corresponding α_1 is

$$\begin{aligned}\alpha_1 &= \prod_{i=0}^{p-1} \sigma_x^i(\eta_i) \\ &= \eta_i^{p-1} \\ &= \zeta_{N'}^{z(p-1)} \\ &= \zeta_{N'}^{-N'/\left(p^f-1\right)} \\ \boxed{\alpha_1 &= \zeta_{p^f-1}^{-1}}.\end{aligned}$$

Lastly, we compute our β_{10} as

$$\begin{aligned}\beta_{10} &= \frac{\eta_K}{\sigma_x \eta_K} \cdot \frac{\sigma_K \eta_x}{\eta_x} \\ &= \zeta_{N'}^{z(p-1)} \\ \boxed{\beta_{10} &= \zeta_{p^f-1}^{-1}}.\end{aligned}$$

In total, we get the following nice result.

Theorem 165. Let p be an odd prime, and fix $K \coloneqq \mathbb{Q}_p$ and $L \coloneqq \mathbb{Q}_p(\zeta_p, \zeta_m)$, where $p \nmid m$. Further, set $L_0 \coloneqq \mathbb{Q}_p(\zeta_p)$ and $L_1 \coloneqq \mathbb{Q}_p(\zeta_m)$ so that $L = L_0 L_1$ and $L_0 \cap L_1 = K$. Now, pick up the following data.

- Suppose the order of p modulo m is f.
- Let $\sigma_x \colon \zeta_p \mapsto \zeta_p^x$ be a generator of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$.
- Find $\gamma \in \mathbb{Q}_p(\zeta_p)$ such that $\gamma^{p-1} + p = 0$ and $\sigma_x(\gamma)/\gamma = \zeta_{p-1}$. (Equivalently, set $\zeta_{p-1} \coloneqq \sigma_x(\gamma)/\gamma$.)

Then the fundamental class $u_{L/K} \in H^2(\mathrm{Gal}(L/K), L^\times)$ is represented by the triple

$$(\alpha_0, \alpha_1, \beta_{10}) = \left(\gamma, \zeta_{p^f-1}^{-1}, \zeta_{p^f-1}^{-1}\right).$$

Remark 166. We verify Artin reciprocity for $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$. Let $c \in Z^2(\mathrm{Gal}(L/K), L^\times)$ represent the fundamental class. The explicit formula for α_1 tells us that

$$\alpha_1 = \prod_{i=0}^{p-1} c\left(\sigma_x^i, \sigma_x\right) = [\sigma_x] \cup \operatorname{Res} u_{L/\mathbb{Q}_p} = [\sigma_x] \cup u_{L/\mathbb{Q}_p(\zeta_m)} = \theta_{L/\mathbb{Q}_p(\zeta_m)}^{-1}(\sigma_x).$$

Taking norms down to $K^\times$, we see on one hand that

$$\mathrm{N}_{\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p}(\alpha_1) = \prod_{i=0}^{f-1} \zeta_{p^f-1}^{-p^i} = \zeta_{p^f-1}^{-\left(1+p+\cdots+p^{f-1}\right)} = \zeta_{p^f-1}^{-\left(p^f-1\right)/(p-1)} = \zeta_{p-1}^{-1} \equiv x^{-1} \pmod p.$$

On the other hand,

$$\mathrm{N}_{\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p}\, \theta_{L/\mathbb{Q}_p(\zeta_m)}^{-1}(\sigma_x) = \theta_{L/\mathbb{Q}_p}^{-1}(\sigma_x) = \theta_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}^{-1}(\sigma_x).$$

So $\theta_{\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p}^{-1}$ sends $\sigma_x \colon \zeta_p \mapsto \zeta_p^x$ to $x^{-1} \pmod p$, as predicted by Lubin–Tate theory.

6.5 Towers

In this section, we will use the notions but not the exact notation as in the set-up. Instead, we will build a "tower set-up" below. Our goal is to be able to force some compatibility among the data in the tuples of Corollary 157 in towers. This is particularly simple in the case where we fix some unramified extension and allow our ramification to ascend in a tower.

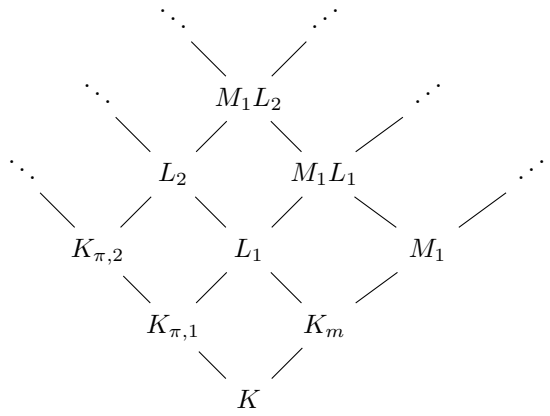
As such, fix a base field K and unramified extension K_m, and we also fix a tower of totally ramified extensions

$$K \coloneqq K_{\pi,0} \subseteq K_{\pi,1} \subseteq K_{\pi,2} \subseteq \cdots.$$

For example, we might choose Lubin–Tate extensions for this purpose. For brevity, we set

$$K_\pi \coloneqq \bigcup_{i \geq 0} K_{\pi,i}$$

to be the (very large) composite totally ramified extension. Now, for each $i \geq 0$, we define $L_i \coloneqq K_m K_{\pi,i}$ for each and M_i to be the unramified extension of degree $[L_i : K]$ over K; notably, $[K_m : K] \mid [L_i : K]$, so $K_m \subseteq M_i$ for each $i \geq 0$. Here is our diagram.



Arrows going up and to the left are unramified; arrows going up and to the right are (totally) ramified. Now, we are interested in constructing a "compatible" system of tuples representing fundamental classes for the ascending chain of extensions L_1/K, L_2/K, L_3/K, etc.

For coherence reasons, we will also place a few assumptions on our Galois groups. Namely, we will assume that

$$\mathrm{Gal}(K_\pi/K) = \bigoplus_{i=1}^{m} \overline{\langle \tau_i \rangle}$$

is a direct sum of finitely many procyclic groups. For example, if we are using Lubin–Tate extensions, and we are in characteristic 0, then this is automatic. Additionally, we will assume that our quotients are

$$\mathrm{Gal}(K_{\pi,i}/K) = \bigoplus_{i=1}^{m} \langle \tau_i|_{K_i} \rangle$$

for each $i \geq 0$. This requirement, though strong, is essentially the only way we could hope for compatibility among our tuples—namely, it tells us that each L_i/K has Galois group generated by the same elements (up to restriction) and hence have more or less the same requirements to yield a fundamental tuple. As an example, this requirement is satisfied when $K = \mathbb{Q}_p$ and $K_i = \mathbb{Q}_p(\zeta_{p^i})$; in fact, $m \in \{1, 2\}$ in this case.

The main focus of the construction is to construct compatible γ elements, but the notion of compatibility will in fact extend. As such, we will codify this into the following definition.

Definition 167. Fix everything as above. Then a sequence $\{x_i\}_{i=0}^{\infty}$ of elements $x_i \in M_iL_i$ is *compatible in towers* if and only if

$$\mathrm{N}_{M_{i+1}L_{i+1}/M_iL_{i+1}}(x_{i+1}) = x_i.$$

This definition is written down sequentially so that verifying its existence is easy.

Lemma 168. Fix a uniformizer $\pi_K \in K$. There is a sequence $\{\gamma_i\}_{i=0}^{\infty}$ of elements compatible in towers such that $\gamma_0 \in M_0L_0 = K_m$ is $\gamma_0 = \pi_K$.

Proof. This comes down to a norm argument and an induction. Extend a valuation $v_K \colon K \to \mathbb{Z}$ to all fields above. Suppose we have constructed γ_i such that γ_i is a uniformizer of M_iL_i. We claim that we can construct γ_{i+1} to also be a uniformizer of $M_{i+1}L_{i+1}$ and with

$$\mathrm{N}_{M_{i+1}L_{i+1}/M_iL_{i+1}}(\gamma_{i+1}) = \gamma_i.$$

This claim will finish the proof inductively.

Now, observe that the extension M_iL_{i+1}/M_iL_i is a totally ramified extension, so if we let ϖ denote a uniformizer of M_iL_{i+1}, we have

$$v\left(\varpi^{[M_iL_{i+1}:M_iL_i]}\right) = v(\gamma_i). \tag{6.1}$$

Continuing, $M_{i+1}L_{i+1}/M_iL_{i+1}$ is an unramified extension, so in fact ϖ continues to be a uniformizer up in $M_{i+1}L_{i+1}$. As such, we see that it suffices to construct $u \in M_{i+1}L_{i+1}$ such that

$$\mathrm{N}_{M_{i+1}L_{i+1}/M_iL_{i+1}}(u) = \frac{\gamma_i}{\mathrm{N}_{M_{i+1}L_{i+1}/M_iL_{i+1}}(\varpi)}.$$

But the right-hand side is a unit because it has valuation 0 from (6.1), so we can construct a unit u for the left-hand side as well because the norm map surjects from units to units in unramified extensions. In total, $\gamma_{i+1} \coloneqq u\varpi$ is the element we are looking for. ∎

However, the definition of compatibility does not actually tell us that each of these γ_i will behave the way that we need them to as required by Corollary 157. The compatibility is also a little unnatural because it only moves one step at a time. To fix both of these issues, we have the following.

Lemma 169. Suppose that the sequence $\{x_i\}_{i=0}^{\infty}$ is compatible in towers. Then for any nonnegative integers $p \geq q$, we have

$$\mathrm{N}_{M_pL_p/M_qL_p}(x_p) = x_q.$$

Proof. This will require us to actually describe the Galois groups involved. Set $\sigma_K \in \mathrm{Gal}(K^{\mathrm{unr}}/K)$ to the Frobenius automorphism on K, but extend σ_K to all K^{ab} by acting trivially on totally ramified extensions. Additionally, for brevity we set

$$f \coloneqq [K_m : K] \qquad \text{and} \qquad e_i \coloneqq [K_{\pi,i} : K]$$

for each $i \geq 0$. Now, the extension M_pL_p/M_qL_p is unramified and hence has Galois group generated by its Frobenius element. The Frobenius element of M_qL_p is equal to the Frobenius element of M_q because the extension M_jL_i/M_j is totally ramified, and because M_q/K is unramified, we may compute the Frobenius element of M_q as

$$\sigma_K^{[M_q:K]},$$

where $[M_q : K] = [L_q : K] = [L_q : K_{\pi,q}] \cdot [K_{\pi,q} : K] = [K_m : K] \cdot [K_{\pi,q} : K] = fe_q$. As for the order of $\mathrm{Gal}(M_pL_p/M_qL_p)$, we first compute, for any $i \geq 0$,

$$[M_iL_i : L_i] = \frac{[M_iL_i : K]}{[L_i : K]} = \frac{[M_iL_i : M_i] \cdot [M_i : K]}{[L_i : K]} = [M_iL_i : M_i] = [K_{\pi,i} : K] = e_i,$$

so the degree we want is e_p/e_q. Thus,

$$\mathrm{N}_{M_pL_p/M_qL_p}(x_p) = \prod_{i=0}^{e_p/e_q-1} \sigma_K^{fe_qi}(x_p).$$

Now, we show that this equals x_q by induction on p. When $p = q$, there is nothing to say. Then, supposing we have the equality at p, we write

$$\begin{aligned}
\mathrm{N}_{M_{p+1}L_{p+1}/M_qL_{p+1}}(x_{p+1}) &= \prod_{i=0}^{e_{p+1}/e_q-1} \sigma_K^{fe_qi}(x_{p+1}) \\
&= \prod_{b=0}^{e_p/e_q-1} \prod_{a=0}^{e_{p+1}/e_p-1} \sigma_K^{fe_q(a(e_p/e_q)+b)}(x_{p+1}) \\
&= \prod_{b=0}^{e_p/e_q-1} \sigma_K^{fe_qb}\left(\prod_{a=0}^{e_{p+1}/e_p-1} \sigma_K^{fe_pa}(x_{p+1}) \right) \\
&= \prod_{b=0}^{e_p/e_q-1} \sigma_K^{fe_qb}\left(\prod_{a=0}^{e_{p+1}/e_p-1} \sigma_K^{fe_pa}(x_{p+1}) \right).
\end{aligned}$$

Doing the same Galois theory, we see $\mathrm{Gal}(M_{p+1}L_{p+1}/M_pL_{p+1})$ is cyclic generated by $\sigma_K^{fe_p}$ of order e_{p+1}/e_p, so the inner term is $\mathrm{N}_{M_{p+1}L_{p+1}/M_pL_{p+1}}(x_{p+1})$, which we know to be x_p. Now, $x_p \in M_pL_p$, so in fact the entire product collapses to

$$\mathrm{N}_{M_{p+1}L_{p+1}/M_qL_{p+1}}(x_{p+1}) = \mathrm{N}_{M_pL_p/M_qL_p}(x_p) = x_q,$$

which is what we wanted. This completes the proof. ∎

In particular, our sequence $\{\gamma_i\}_{i=0}^{\infty}$ compatible in towers with $\gamma_0 = 0$ will have

$$\mathrm{N}_{M_iL_i/L_i}(\gamma_i) = \mathrm{N}_{M_iL_i/M_0L_i}(\gamma_i) = \gamma_0 = \pi_K$$

for each $i \geq 0$, so these $\gamma_i \in M_iL_i$ do in fact satisfy the needed requirement of Corollary 157.

Thus, we have described how to construct our γ terms in the tower, from which the rest of the fundamental tuple follows. However, we do remark that it is possible to choose the η terms to be compatible in towers as well.

Lemma 170. Fix everything as above. Further, fix some $\sigma \in \mathrm{Gal}\left(\bigcup_{i\geq 0} L_i/K\right)$. Then there exists a sequence $\{\eta_i\}_{i=0}^{\infty}$ compatible in towers such that

$$\frac{\eta_i}{\sigma_K^f(\eta_i)} = \frac{\sigma(\gamma_i)}{\gamma_i} \tag{6.2}$$

for each $i \geq 0$.

Proof. Well, to begin we have $\gamma_0 = \pi_K$, which is fixed by σ, so the right-hand side is 1, meaning that we might as well take $\eta_0 = 1$. We now claim that, given η_i satisfying (6.2) which is a unit, we can construct η_{i+1} with

$$\mathrm{N}_{M_{i+1}L_{i+1}/M_iL_{i+1}}(\eta_{i+1}) = \eta_i$$

also satisfying (6.2) (for $i+1$) which is a unit. For brevity, set $\mathrm{N} \coloneqq \mathrm{N}_{M_{i+1}L_{i+1}/M_iL_{i+1}}$. To begin, we note that η_i is a unit in M_iL_{i+1} as well, so because $M_{i+1}L_{i+1}/M_iL_{i+1}$ is unramified, we may simply guess any $\eta \in M_{i+1}L_{i+1}$ such that

$$\mathrm{N}(\eta) = \eta_i.$$

We now need to correct for (6.2). Well, we start by noting we're pretty close because

$$\begin{aligned}\mathrm{N}\left(\frac{\eta}{\sigma_K^f(\eta)}\Big/\frac{\sigma(\gamma_{i+1})}{\gamma_{i+1}}\right) &= \frac{\mathrm{N}\,\eta}{\sigma_K^f(\mathrm{N}\,\eta)}\Big/\frac{\sigma(\mathrm{N}\,\gamma_{i+1})}{\mathrm{N}\,\gamma_{i+1}}\\ &= \frac{\eta_i}{\sigma_K^f(\eta_i)}\Big/\frac{\sigma(\gamma_i)}{\gamma_i}\\ &= 1.\end{aligned}$$

Now, $M_{i+1}L_{i+1}/M_iL_{i+1}$ is unramified and hence cyclic, and we know that its Galois group is generated by $\sigma_K^{fe_i}$ as computed earlier, so Hilbert's theorem 90 allows us to find some $u \in M_{i+1}L_{i+1}$ such that

$$\frac{\eta}{\sigma_K^f(\eta)}\Big/\frac{\sigma(\gamma_{i+1})}{\gamma_{i+1}} = \frac{u}{\sigma_K^{fe_i}u}.$$

Quickly, note that we may multiply u by any element in M_iL_{i+1} without adjusting the equality. Thus, taking ϖ to be a uniformizer of M_iL_{i+1}, we note that we can divide out u by some number of ϖs to force u to be a unit because the extension $M_{i+1}L_{i+1}/M_iL_{i+1}$ is unramified, making ϖ also a uniformizer of $M_{i+1}L_{i+1}$. This is all to say that we may assume that u is a unit.

Now, we note that

$$\frac{u}{\sigma_K^{fe_i}u} = \prod_{k=0}^{e_i-1}\frac{\sigma_K^{fk}u}{\sigma_K^{f(k+1)}u} = \underbrace{\left(\prod_{k=0}^{e_i-1}\sigma_K^{fk}u\right)}_{v:=}\Big/\sigma_K^f\left(\prod_{k=0}^{e_i-1}\sigma_K^{fk}u\right) = \frac{v}{\sigma_K^f v}.$$

Because u is a unit, v is as well. In total, we see that

$$\frac{\eta}{\sigma_K^f(\eta)}\Big/\frac{\sigma(\gamma_{i+1})}{\gamma_{i+1}} = \frac{u}{\sigma_K^{fe_i}u} = \frac{v}{\sigma_K^f v}$$

now implies that

$$\frac{\eta/v}{\sigma_K^f(\eta/v)} = \frac{\sigma(\gamma_{i+1})}{\gamma_{i+1}}.$$

Thus, we set $\eta_{i+1} \coloneqq \eta/v$, which we know to be a unit because both η and v are. This completes the inductive step and hence the proof. ■

As such, we define $\{\eta_{\sigma,i}\}_{i=0}^{\infty}$ for each $\sigma \in \mathrm{Gal}\left(\bigcup_{i\geq 0} L_i/K\right)$ as constructed above, and we know these to be compatible in towers.

To finish our discussion, we note that because the expressions for the α_i and β_{ij} are multiplicative and because norms commute with automorphisms in abelian extensions, choosing the γs and ηs to be compatible in towers will imply that the entire fundamental tuples will be (pointwise) compatible in towers.

As an example, we write this compatibility out for α_0; the rest of the terms are similar. We define

$$\alpha_{0,i} \coloneqq \gamma_i \cdot \prod_{k=0}^{f-1}\sigma_K^k(\eta_{\sigma_K,i})$$

in accordance with Corollary 157. To check that this is compatible in towers, we set $\mathrm{N} \coloneqq \mathrm{N}_{M_{i+1}L_{i+1}/M_iL_{i+1}}$

for some index i and compute

$$\begin{aligned}\mathrm{N}(\alpha_{0,i+1}) &= \mathrm{N}\left(\gamma_{i+1}\cdot\prod_{k=0}^{f-1}\sigma_K^k(\eta_{\sigma_K,i+1})\right)\\ &= \mathrm{N}\,\gamma_{i+1}\cdot\prod_{k=0}^{f-1}\sigma_K^k(\mathrm{N}\,\eta_{\sigma_K,i+1})\\ &= \gamma_i\cdot\prod_{k=0}^{f-1}\sigma_K^k(\eta_{\sigma_K,i})\\ &= \alpha_{0,i},\end{aligned}$$

which is what we wanted.

7 Global Gerbs

In this section we provide a concrete description of the Kottwitz gerbs $\mathcal{E}_2$ and $\mathcal{E}_3$ from [Kot14] associated to the global extension $\mathbb{Q}(\zeta_{p^m})/\mathbb{Q}$ when p is a prime.

7.1 Set-Up

We quickly recall the construction of $\mathcal{E}_2$. Given a global field K, let V_K denote the set of places of K. We follow [Kot14] and [Tat66].

Fix an extension of global fields L/K with Galois group $G \coloneqq \mathrm{Gal}(L/K)$. For later use, we will also let $G_v \subseteq G$ denote the decomposition group of a place $v \in V_L$. Now, we have the two short exact sequences. To begin, we note that the augmentation map $\mathbb{Z}[V_K] \twoheadrightarrow \mathbb{Z}$ induces the short exact sequence

$$0 \to \mathbb{Z}[V_L]_0 \to \mathbb{Z}[V_L] \to \mathbb{Z} \to 0 \tag{X}$$

where $\mathbb{Z}[V_L]$ is the kernel of $\mathbb{Z}[V_L] \twoheadrightarrow \mathbb{Z}$. We also have the short exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{A}_L^\times/L^\times \to 1 \tag{A}$$

where the inclusion $L^\times \hookrightarrow \mathbb{A}_L^\times$ is diagonal.

Let $\mathbb{D}_2 \coloneqq \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], -)$ denote the protorus with character group $\mathbb{Z}[V_L]$. Then $\mathcal{E}_2(L/K)$ is the Galois gerb associated to a particular class $\alpha_2 \in H^2(G, \mathbb{D}(\mathbb{A}_L))$. To construct this class, we need the following lemma.

Lemma 171 ([Tat66, p. 714])**.** Let L/K be an extension of global fields with Galois group G, and let V_L and V_K denote the set of places of L and K respectively. Given a place $v \in V_L$, let $G_v \subseteq G$ denote its decomposition group. Then, for any $i \in \mathbb{Z}$,

$$\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], M)) \simeq \prod_{u\in V_K}\widehat{H}^i(G_{v(u)}, M),$$

where the product is over places $u \in V_K$ taking a fixed place $v(u) \in V_L$ above u.

Proof. We give the proof for later use. This is essentially a matter of separating our places and then applying Shapiro's lemma. For each $u \in V_K$, let $V_u \subseteq V_L$ denote the set of places in L above u. Then we see

$$\mathbb{Z}[V_L] \simeq \bigoplus_{u\in V_K}\mathbb{Z}[V_u]$$

as G-modules because the G-orbit of a place $v \in V_L$ lying over a place $u \in V_K$ is exactly V_u. Thus, we have the isomorphisms

$$\begin{aligned}\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], M)) &\simeq \widehat{H}^i\left(G, \mathrm{Hom}_{\mathbb{Z}}\left(\bigoplus_{u \in V_L} \mathbb{Z}[V_u], M\right)\right) \\ &\simeq \widehat{H}^i\left(G, \prod_{u \in V_K} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], M)\right) \\ &\simeq \prod_{u \in V_K} \widehat{H}^i\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], M)\right).\end{aligned}$$

It remains to show that

$$\widehat{H}^i\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], M)\right) \overset{?}{\simeq} \widehat{H}^i(G_{v(u)}, M).$$

Well, for each place $u \in V_K$, find a place $v(u) \in V_L$ above it. As discussed above, V_u is a transitive G-set, and the stabilizer of $v(u)$ is $G_{v(u)}$. Thus, $V_u \simeq G_{v(u)} \backslash G$ as G-sets (note the distinction between left and right G-sets is somewhat irrelevant because $gG_v = G_v g$ for each $g \in G_v$), so $\mathbb{Z}[V_u] \simeq \mathbb{Z}[G_{v(u)} \backslash G]$ as G-modules. Thus, we may write

$$\begin{aligned}\widehat{H}^i\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], M)\right) &\simeq \widehat{H}^i\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_{v(u)} \backslash G], M)\right) \\ &\simeq \widehat{H}^i\left(G, \mathrm{Mor}_{\mathrm{Set}}(G_{v(u)} \backslash G, M)\right) \\ &\simeq \widehat{H}^i\big(G, \mathrm{CoInd}_{G_{v(u)}}^G(M)\big),\end{aligned}$$

where the last isomorphism is because $\mathrm{Mor}_{\mathrm{Set}}(G_{v(u)} \backslash G, M) \simeq \mathrm{CoInd}_H^G(M)$ by taking $f \colon G_{v(u)} \backslash G \to M$ to the function $g \mapsto gf\left(G_v g^{-1}\right)$. Now, this last cohomology group is isomorphic to $\widehat{H}^i(G_{v(u)}, M)$ by Shapiro's lemma, thus finishing. ■

Remark 172. Tracking through the application of Shapiro's lemma above, we can see that the isomorphism behaves as

$$\widehat{H}^i(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], M)) \overset{\mathrm{Res}}{\to} \widehat{H}^i(G_v, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], M)) \overset{\mathrm{eval}_v}{\to} \widehat{H}^i(G_v, M)$$

on components; here eval_v is induced by the evaluation-at-v map $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], M) \to M$.

Thus, to specify $\alpha_2 \in \widehat{H}^2(G, \mathbb{D}_2(\mathbb{A}_L))$, it is enough to specify a set of classes

$$\alpha_2(u) \in \widehat{H}^2\left(G_{v(u)}, \mathbb{A}_L^\times\right)$$

for each $u \in V_K$. To do so, we note that $G_{v(u)} = \mathrm{Gal}(L_{v(u)}/K_u)$, so we use the natural embedding $i_v \colon L_v \hookrightarrow \mathbb{A}_L^\times$ (for $u \in V_L$) to set

$$\alpha_2(u) \coloneqq i_{v(u)}\big(\alpha(L_{v(u)}/K_u)\big),$$

where $\alpha(L_{v(u)}/K_u) \in \widehat{H}^2\left(G_{v(u)}, L_{v(u)}^\times\right)$ is the local fundamental class.

7.2 An Explicit Cocycle

We continue in the context of subsection 7.1, in the case of $K \coloneqq \mathbb{Q}$ and $L \coloneqq \mathbb{Q}(\zeta_{p^\nu})$; for brevity, set $\zeta \coloneqq \zeta_{p^\nu}$. The goal of the computation is to fully reverse Lemma 171 to be able to write down a 2-cocycle in $Z^2(G, \mathbb{D}_2(\mathbb{A}_L))$ representing α_2, which will then specify a gerb in the correct equivalence class of $\mathcal{E}_2$. As such, for each $u \in V_K$, we choose some $v(u) \in V_L$ above u.

7.2.1 Extracting Elements

We are going to choose our local fundamental class representatives to be compatible with a choice of global fundamental class for L/K. However, this will require extracting certain magical elements of $L^\times$, so we will go ahead and extract these before getting into the computation.

To begin, we need to write down $G \coloneqq \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ in some concrete way, so we pick a generator $x \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times$ (recall that p is odd) so that $\sigma\colon \zeta \mapsto \zeta^x$ is a generator of G of order $n \coloneqq \varphi(p^\nu) = (p-1)p^{\nu-1}$. To be able to properly localize, for each prime $q \neq p$, we define $k_q \geq 0$ to have

$$x^{k_q} \equiv q \pmod{p}$$

so that $\sigma^{k_q}\colon \zeta \mapsto \zeta^q$. We also set $d_q \coloneqq \gcd(k_q, n)$ so that $\langle \sigma^{k_q}\rangle = \langle \sigma^{d_q}\rangle$ with order $n_q \coloneqq n/d_q$.

Additionally, we let $\mathfrak{P}$ denote the prime of L above (p) of K; notably, L/K is totally ramified at (p), so there is in fact one prime $\mathfrak{P}$ here. In particular, we can check that

$$c_p(\sigma^i, \sigma^j) = x^{-\left\lfloor \frac{i+j}{n}\right\rfloor}$$

is a 2-cocycle in $Z^2(G, L_{\mathfrak{P}}/K_{(p)})$ representing the local fundamental class in $\widehat{H}^2(G, L_{\mathfrak{P}}^\times)$. Passing $c_{\mathfrak{P}}$ through $L_{\mathfrak{P}}^\times \hookrightarrow \mathbb{A}_L^\times \twoheadrightarrow \mathbb{A}_L^\times/L^\times$, we see that

$$i_{\mathfrak{P}} c_p(\sigma^i, \sigma^j) = i_{\mathfrak{P}} x^{-\left\lfloor \frac{i+j}{n}\right\rfloor}$$

has cohomology class of global invariant $1/n$ and therefore represents the global fundamental class $u_{L/K} \in \widehat{H}^2(G, \mathbb{A}_L^\times/L^\times)$.

We now start choosing elements of $L^\times$. The following conjures the element that we need for infinite places. Set $\tau \coloneqq \sigma^{n/2}$ to be the "conjugation" action on L.

Lemma 173. Let $v \coloneqq v(\infty)$ be our chosen infinite place, and set $G_v = \{1, \tau\}$. Then there exists $\xi_\infty \in L^{\langle\tau\rangle}$ such that

$$\xi_\infty \equiv i_v(-1) \cdot i_{\mathfrak{P}} x \pmod{N_{\langle\tau\rangle}\mathbb{A}_L^\times}.$$

Proof. It is a fact that we can represent the local fundamental class of L_v/K_∞ by

$$c_v(\tau^i, \tau^j) = (-1)^{\left\lfloor \frac{i+j}{2}\right\rfloor}.$$

Again, embedding this into $\mathbb{A}_L^\times/L^\times$, we see that

$$i_v c_v(\tau^i, \tau^j) = i_v(-1)^{\left\lfloor \frac{i+j}{2}\right\rfloor}$$

has global invariant $1/2$ and therefore should live in the same cohomology class as $\mathrm{Res}_{G_v} i_{\mathfrak{P}} c_{\mathfrak{P}}$. In particular, we place $[\tau] \in \widehat{H}^{-2}(G_v, \mathbb{Z})$ and note that

$$[i_v c_v] \cup [\tau] = [n/2 \cdot i_{\mathfrak{P}} c_p] \cup [\tau]$$

as elements in $\widehat{H}^0(G_v, \mathbb{A}_L^\times/L^\times)$. Rearranging, this implies that

$$[1] = [i_v(-1) \cdot i_{\mathfrak{P}} x]$$

as elements in $\widehat{H}^0(G_v, \mathbb{A}_L^\times/L^\times)$. Now, this group is $\mathbb{A}_L^\times/L^\times$ modded out by $N_{G_v}\mathbb{A}_L^\times$, so we can unwind this as promising some $\xi_\infty \in L^\times$ such that

$$\xi_\infty \equiv i_v(-1) \cdot i_{\mathfrak{P}} x \pmod{N_{G_v}\mathbb{A}_L^\times}.$$

It remains to show that $\xi_\infty \in L^{\langle\tau\rangle}$. Well, the above turns into

$$\xi_\infty = i_v(-1) \cdot i_{\mathfrak{P}} x \cdot a \cdot \tau a$$

for some $a \in \mathbb{A}_L^\times$, and this equality has each factor on the right-hand side fixed by τ. ∎

Remark 174. For certain primes, one can choose ξ_∞ from the circulant units of $\mathbb{Q}(\zeta_p)$, making ξ_∞ effectively computable. However, in general this does not work; this fails first for $\mathbb{Q}(\zeta_{29})$.

Continuing, we note that, because G_v is preserved by conjugation, we have

$$g\xi_\infty \equiv i_{gv}(-1) \cdot i_{\mathfrak{P}} x \pmod{N_{G_{gv}} \mathbb{A}_L^\times}$$

as well, so we set $\xi_{gv} \coloneqq g\xi_\infty$. Because ξ_∞ is preserved by τ, the choice of $g \in G$ yielding gv is irrelevant.

We are going to want to "inflate" ξ_v to be helpful with larger subgroups, for which we establish the following lemma.

Lemma 175. Fix everything as above. Picking any infinite place $v \mid \infty$ and subgroup $H \subseteq G$ containing τ, the element

$$\xi_{v,H} \coloneqq \prod_{g\langle\tau\rangle \in H/\langle\tau\rangle} g\xi_v$$

has

$$\xi_{v,H} \in L^H \qquad \text{and} \qquad \xi_{v,H} \equiv i_{\mathfrak{P}} x^{\#H/2} \cdot \prod_{w \in Hv} i_w(-1) \pmod{N_H \mathbb{A}_L^\times}.$$

Technically, we must choose some coset representatives for $H/\langle\tau\rangle$ to define $\xi_{v,H}$, but because ξ_v is fixed by τ, they all yield the same element of L^H.

Proof. By construction,

$$\xi_v = i_{\mathfrak{P}} x \cdot i_v(-1) \cdot N_{\langle\tau\rangle} a$$

for some $a \in \mathbb{A}_L^\times$. Now, we choose coset representatives $\{g_1, \dots, g_m\}$ for $H/\langle\tau\rangle$ so that

$$\begin{aligned}
\xi_{v,H} &= \prod_{k=1}^m g_k \xi_v \\
&= \left(\prod_{k=1}^m g_k i_{\mathfrak{P}} x\right)\left(\prod_{k=1}^m g_k i_v(-1)\right)\left(\prod_{k=1}^m g_k(a \cdot \tau a)\right) \\
&= \left(\prod_{k=1}^m i_{g_k \mathfrak{P}}(g_k x)\right)\left(\prod_{k=1}^m i_{g_k v} g_k(-1)\right)\left(\prod_{k=1}^m g_k a \cdot g_k \tau a\right) \\
&= i_{\mathfrak{P}} x^{\#H/2}\left(\prod_{k=1}^m i_{g_k v}(-1)\right) N_H a.
\end{aligned}$$

Quickly, we show that the (multi)set of $g_k v$ is the same as Hv. Well, $gv = v$ if and only if $g \in \langle\tau\rangle$, so the stabilizer of v in the H-set in Hv is $\langle\tau\rangle$. It follows that there is an isomorphism $H/\langle\tau\rangle \cong Hv$ of H-sets, which is what we wanted.

Thus,

$$\xi_{v,H} = i_{\mathfrak{P}} x^{\#H/2}\left(\prod_{w \in Hv} i_w(-1)\right) N_H a.$$

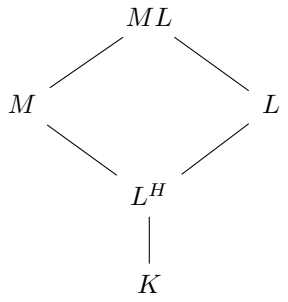
To show $\xi_{v,H} \in L^H$, we observe that the above factors are each fixed by H, finishing. ∎

Next we turn to our finite unramified places. The following is the key idea.

Lemma 176. Fix everything as above. For each subgroup $H \subseteq G$ and ideal class $c \in \operatorname{Cl} L^H$, there exists a prime L^H-ideal $\mathfrak{r}_{H,c}$ satisfying the following constraints.

- $\mathfrak{r}_{H,c}$ has ideal class c.
- $\mathfrak{r}_{H,c}$ splits completely in L.

Proof. This is an application of the Chebotarev density theorem. Let M be the Hilbert class field of L^H, yielding the following tower of fields.



The main claim is that $M \cap L = L^H$. Certainly $M \cap L$ contains L^H, so we make the following two observations.

- Because $M \cap L$ is a subextension of the unramified extension $L^H \subseteq M$, the extension $L^H \subseteq M \cap L$ is also unramified.
- Because the extension $L^H \subseteq L$ is totally ramified, the only way for a sub-extension to be unramified is for the subextension to be L^H.

Combining the above two observations forces $M \cap L = L^H$.

It follows that M and L are linearly disjoint over L^H, so

$$\mathrm{Gal}(ML/L^H) \simeq \mathrm{Gal}\left(M/L^H\right) \times \mathrm{Gal}\left(L/L^H\right) \simeq \mathrm{Cl}\, L^H \times H.$$

Thus, choose $g \in \mathrm{Gal}(M/L^H)$ corresponding to $c \in \mathrm{Cl}\, L^H$ and then use the Chebotarev density theorem to find a prime L^H-ideal $\mathfrak{r}$ such that $\mathrm{Frob}_{\mathfrak{r}} = (g, 1)$. We claim that $\mathfrak{r}_{H,c} \coloneqq \mathfrak{r}$ will do the trick.

For concreteness, let $\mathfrak{R}$ be a prime of ML above $\mathfrak{r}$, and set $\mathfrak{R}_M \coloneqq \mathfrak{R} \cap M$ and $\mathfrak{R}_L \coloneqq \mathfrak{R} \cap L$. Then

$$\mathrm{Frob}_{\mathfrak{R}_M/\mathfrak{r}} = \mathrm{Res}_M \mathrm{Frob}_{\mathfrak{R}/\mathfrak{r}} = g,$$

so $\mathfrak{r}$ has the correct ideal class. Similarly,

$$\mathrm{Frob}_{\mathfrak{R}_L/\mathfrak{r}} = \mathrm{Res}_L \mathrm{Frob}_{\mathfrak{R}/\mathfrak{r}} = 1,$$

so $\mathfrak{r}$ splits completely up in L. ∎

Now, let $(q) \neq (p)$ be a finite prime of K, and choose some place $v \coloneqq v(u) \in V_L$ above (q) corresponding to the prime $\mathfrak{Q}$. Intersecting down, set $\mathfrak{q} \coloneqq \mathfrak{Q} \cap L^{G_v}$.

We will want to choose a well-behaved uniformizer of $\mathfrak{q}$ to represent our local fundamental class. Choosing $q \in \mathfrak{q}$ turns out to cause difficulties when $\mathfrak{q}$ is not inert in L. Instead, we use Lemma 176 to find the constructed L^{G_v}-prime $\mathfrak{r}_u$ such that $\mathfrak{r}_u$ splits completely in L and $\mathfrak{q}\mathfrak{r}_u$ is principal. As such, we find $\varpi_u \in L^{G_v}$ such that

$$\mathfrak{q}\mathfrak{r}_u = (\varpi_u).$$

Observe that if we work with $gv(u)$ instead of $v(u)$ for some $g \in G$, we can analogously write

$$(g\mathfrak{q})(g\mathfrak{r}_u) = (g\varpi_u),$$

so we set $\varpi_{gv(u)} \coloneqq g\varpi_u$ for $g \in G$. Observe that this is well-defined: $gv(u) = g'v(u)$ implies that $g^{-1}g' \in G_v$, so $g^{-1}g\varpi_u = \varpi_u$, so $g\varpi_u = g'\varpi_u$.

7.2.2 Choosing Local Fundamental Cocycles

To work up Lemma 171, we must find explicit 2-cocycles to represent the various $i_{v(u)}\alpha(L_{v(u)}/K_u)$s. Some of these will be easy. For example, for $v = v((p)) = \mathfrak{P}$, we can set

$$c_p(\sigma^i, \sigma^j) = x^{-\left\lfloor \frac{i+j}{n} \right\rfloor}$$

to represent $u_{L_{\mathfrak{P}}/K_{(p)}} \in \widehat{H}^2(G, L_{\mathfrak{P}}^\times)$, so we set $\widetilde{c}_p \coloneqq i_{\mathfrak{P}} c_p$.

Additionally, for $v = v(\infty)$, we set

$$c_\infty(\tau^i, \tau^j) = (-1)^{\left\lfloor \frac{i+j}{2} \right\rfloor}$$

to represent $u_{L_v/K_\infty} \in \widehat{H}^2(G, L_v^\times)$. However, we won't want to use $i_v c_\infty$ for our 2-cocycle. Instead, we recall that

$$[i_v c_\infty] \cup [\tau] = [i_v(-1)] = [\xi_\infty / i_{\mathfrak{P}} x]$$

as elements of $\widehat{H}^0(G_v, \mathbb{A}_L^\times)$. Thus, $[i_v c_\infty]$ is also represented by

$$\widetilde{c}_\infty(\tau^i, \tau^j) \coloneqq (\xi_\infty / i_{\mathfrak{P}} x)^{\left\lfloor \frac{i+j}{2} \right\rfloor}$$

by cupping with $(\tau^i, \tau^j) \mapsto \left\lfloor \frac{i+j}{2} \right\rfloor$, which represents the generator of $\widehat{H}^2(G_v, \mathbb{Z})$.

Lastly, we let $u = (q) \neq (p)$ denote a finite (unramified) place of V_K, and we set $v \coloneqq v(u)$ associated to the finite prime $\mathfrak{Q}$. For brevity, set $H \coloneqq G_v$, and note $H = \langle \sigma^{k_q} \rangle$ because $\sigma^{k_q} \colon \zeta \mapsto \zeta^{k_q}$. Now, because our chosen ϖ_u is a uniformizer of $\mathfrak{Q} \cap L^{G_v}$, we can set

$$\left(\sigma^{k_q i}, \sigma^{k_q j}\right) \mapsto \varpi_u^{\left\lfloor \frac{i+j}{n_q} \right\rfloor}$$

to represent $u_{L_v/K_u} \in \widehat{H}^2(H, L_v^\times)$. It will be helpful to be able to change between generators, so we pick up the following lemma.

Lemma 177. Let $G = \langle \sigma \rangle$ be a finite cyclic group of order n. Further, suppose $k \in \mathbb{Z}$ has $\gcd(k, n) = 1$. Then define $\chi, \chi_d \in Z^2(G, \mathbb{Z})$ by

$$\chi\left(\sigma^i, \sigma^j\right) \coloneqq \left\lfloor \frac{i+j}{n} \right\rfloor \qquad \text{and} \qquad \chi_k\left(\sigma^{ki}, \sigma^{kj}\right) \coloneqq \left\lfloor \frac{i+j}{n} \right\rfloor,$$

where $0 \leq i, j < n$. Then $[\chi] = k[\chi_k]$ in $H^2(G, \mathbb{Z})$.

Proof. It is well-known that

$$(- \cup [\chi_k]) \colon \widehat{H}^0(G, \mathbb{Z}) \to \widehat{H}^2(G, \mathbb{Z}) \tag{7.1}$$

is an isomorphism. Now, for $m \in \mathbb{Z}$, we see that $[m] \cup [\chi_k] = [m\chi_k]$, so we see that we can actually invert the above isomorphism explicitly because

$$\sum_{g \in G} (m\chi_k)\left(g, \sigma^k\right) = m \sum_{\ell k = 0}^{n-1} \chi_k\left(\sigma^{\ell k}, \sigma^k\right) = m,$$

so $[c] \mapsto [c] \cup \left[\sigma^k\right] = \left[\sum_{g \in G} c(g, \sigma^k)\right]$ describes the inverse of (7.1). As such, we pick up χ and compute

$$\sum_{g \in G} \chi\left(g, \sigma^k\right) = \sum_{\ell=0}^{n-1} \chi\left(\sigma^\ell, \sigma^k\right) = k.$$

Thus, $[k] \cup [\chi_k] = [\chi]$, which is what we wanted. ∎

As such, we set $\chi_{d_q} \in Z^2(G,\mathbb{Z})$ by $\chi_{d_q}\colon \left(\sigma^{d_q i}, \sigma^{d_q j}\right) \mapsto \left\lfloor \frac{i+j}{n} \right\rfloor$. Then Lemma 177 tells us that

$$[\chi_{d_q}] = (k_q/d_q)[\chi_{k_q}].$$

Thus, we find $y_q \in \mathbb{Z}$ with $y_q \cdot k_q/d_q \equiv 1 \pmod{n_q}$ so that we can represent $\alpha(L_v/K_u)$ by

$$([\varpi_u] \cup y_q \chi_{d_q})\colon \left(\sigma^{d_q i}, \sigma^{d_q j}\right) \mapsto \varpi_u^{y_q \left\lfloor \frac{i+j}{n} \right\rfloor}.$$

For brevity, let this 2-cocycle be $c_q \in Z^2\left(H, L_v^\times\right)$.

Again, we won't want to represent $i_v u_{L_v/K_u} \in \widehat{H}^2(H, \mathbb{A}_L^\times)$ by $i_v c_q$. To find the desired representative, we begin by embedding $\varpi_u \in L^\times$ to $\mathbb{A}_L^\times$, yielding

$$\varpi_u = \prod_{w \in V_L} i_w \varpi_u.$$

We claim that if $v' \in V_L$ is a finite place not lying over (p), $\mathfrak{q}$, nor $\mathfrak{r}$, then

$$\prod_{w \in Hv'} i_w \varpi_u \tag{7.2}$$

is a norm in $N_H \mathbb{A}_L^\times$. Indeed, all places in Hv' are unramified (they don't lie over (p)), and the fact that v' avoids both $\mathfrak{q}$ and $\mathfrak{r}$ implies that $\varpi_u \in \mathcal{O}_w^\times$ for each $w \in Hv'$. In particular, there is some $a_{v'} \in L_{v'}$ such that $\varpi_u = N_{H_{v'}} a$, so

$$N_H(i_{v'} a_{v'}) = \prod_{h \in H} i_{hv'} h a_{v'} = \prod_{[h_0] \in H/H_{v'}} i_{h_0 v'} \left(h_0 \prod_{h \in H_{v'}} h a_{v'} \right) = \prod_{w \in Hv'} i_w \varpi_u,$$

where the last equality used the fact that ϖ_u is fixed by $h_0 \in H$. Now, multiplying elements of the form (7.2) together, we conclude that

$$\varpi_u \equiv i_v \varpi_u \cdot i_{\mathfrak{p}} \varpi_u \cdot \prod_{w \mid \mathfrak{r}} i_w \varpi_u \cdot \prod_{w \mid \infty} i_w \varpi_u \pmod{N_H \mathbb{A}_L^\times}. \tag{7.3}$$

We deal with the remaining terms one at a time, in sequence.

Lemma 178. Fix everything as above, with finite place u not above (p) chosen. Then there exists $\xi_u \in L^\times$ and $e_u \in \mathbb{Z}$ such that

$$\xi_u \varpi_u \equiv i_v \varpi_u \cdot i_{\mathfrak{p}} x^{e_u} \pmod{N_H \mathbb{A}_L^\times}.$$

Proof. Looking at (7.3), we have to deal with places about $\mathfrak{r}$ and places above ∞. We deal with these separately.

Let's begin with the places above $\mathfrak{r}$. Fix some v' above $\mathfrak{r}$. Because $\mathfrak{r}$ is totally split in L, we have $H_{v'} = \{1\}$, so

$$N_H(i_{v'} \varpi_u) = \prod_{h \in H} i_{hv'} \varpi_u = \prod_{w \mid \infty} i_w \varpi_u.$$

So the places over $\mathfrak{r}$ actually dissolve into a norm, implying

$$\varpi_u \equiv i_v \varpi_u \cdot i_{\mathfrak{p}} \varpi_u \cdot \prod_{w \mid \infty} i_w \varpi_u \pmod{N_H \mathbb{A}_L^\times}.$$

Next we turn to the infinite places. We begin by fixing some infinite place $v' \mid \infty$. We have two cases.

- If $\tau \notin H$, then we see that
$$N_H i_{v'} \varpi_u = \prod_{h \in H} i_{hv'} h \varpi_u = \prod_{w \in Hv'} i_w \varpi_u,$$
where the last step is because $hv' = h'v'$ for $h, h' \in H$ implies $h = h'$. Thus, these are all norms.

- Otherwise, $\tau \in H$. For concreteness, associate v' to the embedding $\sigma\colon L \to \mathbb{C}$; note hv is associated to the embedding $L \xrightarrow{h} L \to \mathbb{C}$. In fact, $\sigma(L^H) \subseteq \mathbb{R}$ because L^H is fixed by $\tau \in H$, so we'll consider

$$i_{v'}\sqrt{\sigma(\varepsilon_{u,v'}\varpi_u)} \in \mathbb{A}_L^\times,$$

where the sign $\varepsilon_{u,v'} \in \{\pm 1\}$ is chosen to ensure $\sigma(\varepsilon_{u,v'}\varpi_u) > 0$. Thinking concretely, $\sqrt{\varepsilon_{u,v'}\sigma\varpi_u}$ is a Cauchy sequence of elements of L^H under the metric induced by $\sigma\colon L^H \to \mathbb{R}$, whose square approaches $\varepsilon_{u,v'}\sigma\varpi_u > 0$. Notably, we may choose a Cauchy sequence for our square root from L^H because $\sigma(\varepsilon_{u,v'}\varpi_u) > 0$.

Applying $h\colon L_{v'} \to L_{hv'}$ to this Cauchy sequence, we get another Cauchy sequence, but this time the Cauchy sequence is under the metric induced by $\sigma h^{-1}\colon L^H \to \mathbb{R}$ and approaches $\varepsilon_{u,v'}\sigma h\varpi_u$. However, these metric are the same, and $h\varpi_u = \varpi_u$, meaning that applying h here merely produced another $\sqrt{\varepsilon_{u,v'}\sigma\varpi_u} \in L_{hv'}$. The whole point of this is to be able to write

$$\begin{aligned} N_H i_{v'}\sqrt{\sigma(\varepsilon_{u,v'}\varpi_u)} &= \prod_{h\in H} h i_{v'}\sqrt{\sigma(\varepsilon_{u,v'}\varpi_u)} \\ &= \prod_{h\langle\tau\rangle\in H/\langle\tau\rangle} i_{hv'}\left(\sqrt{\sigma(\varepsilon_{u,v'}\varpi_u)}\cdot\tau\sqrt{\sigma(\varepsilon_{u,v'}\varpi_u)}\right) \\ &= \prod_{w\in Hv'} i_w(\varepsilon_{u,v'}\varpi_u). \end{aligned}$$

In total, we see that

$$\prod_{w\in Hv'} i_w\varpi_u \equiv \prod_{w\in Hv'} i_w(\varepsilon_{u,v'}) \equiv \left(\xi_{v',H}\cdot i_{\mathfrak{P}}x^{-\#H/2}\right)^{(1-\varepsilon_{u,v'})/2}$$

by Lemma 178.

We now synthesize. If $\tau \in H$, then we take $\xi_u = 1$ and $e_u = 0$ so that (7.3) gives

$$\varpi_u \equiv i_v\varpi_u \cdot i_{\mathfrak{P}}\varpi_u \pmod{N_H\mathbb{A}_L^\times}.$$

When $\tau \in H$, this is a little more complicated. For notational reasons, we will let V_∞ denote the set of infinite places in V_L, letting us write

$$\begin{aligned} \prod_{w\in V_\infty} i_w\varpi_u &= \prod_{[v']\in V_\infty/H}\prod_{w\in Hv'} i_{hw}\varpi_u \\ &\equiv \prod_{[v']\in V_\infty/H}\left(\xi_{v',H}\cdot i_{\mathfrak{P}}x^{-\#H/2}\right)^{(1-\varepsilon_{u,v'})/2} \\ &\equiv \prod_{[v']\in V_\infty/H}\xi_{v',H}^{(1-\varepsilon_{u,v'})/2}\cdot\prod_{[v']\in V_\infty/H} i_{\mathfrak{P}}x^{-\#H/2\cdot(1-\varepsilon_{u,v'})/2} \pmod{N_H\mathbb{A}_L^\times}. \end{aligned}$$

So we can collapse this product down to $\xi_u^{-1}\cdot i_{\mathfrak{P}}x^{e_u}$ as above. Plugging into (7.3) gets the result. ∎

Lastly, we fix the $i_{\mathfrak{P}}$ term. For this, we use the following lemma.

Lemma 179. Fix everything as above. Suppose that we have a subgroup $H \subseteq G$ and power $e \in \mathbb{Z}$ such that

$$[i_{\mathfrak{P}}x^e] = [1]$$

as elements of $\widehat{H}^0(H, \mathbb{A}_L^\times/L^\times)$. Then

$$i_{\mathfrak{P}}x^e \equiv 1 \pmod{N_H\mathbb{A}_L^\times}.$$

Proof. The point is to show that $\#H \mid e$. Let $H = \langle \sigma^d \rangle$ for a fixed $d \mid n$. We have already established that

$$(\sigma^i, \sigma^j) \mapsto i_{\mathfrak{P}} x^{-\left\lfloor \frac{i+j}{n} \right\rfloor}$$

represents the fundamental class of $\widehat{H}^2(G, \mathbb{A}_L^\times / L^\times)$, so restricting implies that

$$(\sigma^{di}, \sigma^{dj}) \mapsto i_{\mathfrak{P}} x^{-\left\lfloor \frac{i+j}{n/d} \right\rfloor}$$

represents the fundamental class of $\widehat{H}^2(H, \mathbb{A}_L^\times / L^\times) \simeq \mathbb{Z}/\#H\mathbb{Z}$. Cupping with $[\sigma^d] \in \widehat{H}^{-2}(H, \mathbb{Z})$ reveals that $i_{\mathfrak{P}} x^{-1}$ is a generator of $\widehat{H}^0(H, \mathbb{A}_L^\times / L^\times)$ of order $\#H$.

Thus,

$$[i_{\mathfrak{P}} x]^e = [1]$$

as elements of $\widehat{H}^0(H, \mathbb{A}_L^\times / L^\times)$ implies that $\#H \mid e$. In particular, we conclude that $\#H \mid e$. To finish, we see that

$$N_H i_{\mathfrak{P}} x^{e/\#H} = i_{\mathfrak{P}} x^e,$$

finishing. ∎

Remark 180. The above lemma has the amusing corollary that all totally positive units of $\mathbb{Q}(\zeta_{p^m})$ must be equivalent to $1 \pmod{\mathfrak{P}}$, where $\mathfrak{P} = (1 - \zeta_{p^m})$ is the (unique) prime lying above (p).

Currently, we have some ξ_u and e_u such that

$$\xi_u \varpi_u \equiv i_v \varpi_u \cdot i_{\mathfrak{P}} x^{e_u} \pmod{N_H \mathbb{A}_L^\times}.$$

However, we know abstractly that the 2-cocycles $i_v c_q$ and $\operatorname{Res} \widetilde{c}_p$ both represent the fundamental class of $\widehat{H}^2(H, \mathbb{A}_L^\times / L^\times)$, which means that they need to have the same cup product with $\left[\sigma^{d_q}\right]$, giving the equality

$$[i_v \varpi_u^{y_q}] = \left[i_{\mathfrak{P}} x^{-1}\right]$$

as elements of $\widehat{H}^0(H, \mathbb{A}_L^\times / L^\times)$. Combining,

$$[1] = [i_v \varpi_u^{y_q} \cdot i_{\mathfrak{P}} x^{y_q e_u}] = [i_{\mathfrak{P}} x^{y_q e_u - 1}] = [i_{\mathfrak{P}} x]^{y_q e_u - 1}$$

as elements of $\widehat{H}^0(H, \mathbb{A}_L^\times / L^\times)$. Thus, Lemma 179 lets us conclude that

$$i_{\mathfrak{P}} x^{y_q e_u} \equiv i_{\mathfrak{P}} x \pmod{N_H \mathbb{A}_L^\times}.$$

Thus,

$$(\xi_u \varpi_u)^{y_q} \equiv i_v \varpi_u^{y_q} \cdot i_{\mathfrak{P}} x \pmod{N_H \mathbb{A}_L^\times}.$$

In total, we can choose

$$\widetilde{c}_q\left(\sigma^i, \sigma^j\right) \coloneqq \left(\xi_u^{y_q} \varpi_u^{y_q} / i_{\mathfrak{P}} x\right)^{\left\lfloor \frac{i+j}{n_q} \right\rfloor}$$

to represent $i_v u_{L_v/K_u} \in \widehat{H}^2(H, \mathbb{A}_L^\times)$.

To synthesize all places, we set

$$\omega_u \coloneqq \begin{cases} 1 & u = (p), \\ \xi_\infty & u = \infty, \\ \xi_u^{y_q} \varpi_u^{y_q} & u \notin \{(p), \infty\}, \end{cases} \quad \text{and} \quad d_u \coloneqq \begin{cases} d_q & u = q \neq p \text{ is finite}, \\ 1 & u = p, \\ n/2 & u = \infty, \end{cases} \tag{7.4}$$

so that

$$\widetilde{c}_u\left(\sigma^{d_u i}, \sigma^{d_u j}\right) = \left(\omega_u / i_{\mathfrak{P}} x\right)^{\left\lfloor \frac{i+j}{n/d_u} \right\rfloor}$$

in all cases.

7.2.3 Inverting Shapiro's Lemma

The next step in reversing Lemma 171 is to invert the Shapiro's lemma isomorphism

$$\widehat{H}^2\left(G_{v(u)}, \mathbb{A}_L^\times\right) \simeq \widehat{H}^2\big(G, \mathrm{CoInd}_{G_{v(u)}}^G(\mathbb{A}_L^\times)\big)$$

for each place $u \in V_K$. Until the end of this section, we will fix the place $u \in V_K$ and set $v := v(u) \in V_L$ and $H := G_v = G_{v(u)}$ for brevity. It is known that (e.g., see [Kal18]) this inverse morphism can be constructed as the composite

$$\widehat{H}^2\left(H, \mathbb{A}_L^\times\right) \xrightarrow{\iota} \widehat{H}^2\big(H, \mathrm{CoInd}_H^G \mathbb{A}_L^\times\big) \xrightarrow{\mathrm{cor}} \widehat{H}^2\big(G, \mathrm{CoInd}_H^G \mathbb{A}_L^\times\big),$$

where $\iota\colon \mathbb{A}_L^\times \to \mathrm{CoInd}_H^G \mathbb{A}_L^\times$ takes a to $\iota(a)\colon g \mapsto \big(g 1_{g\in H}\big)a$.

Thus, we have two maps to track on the level of our 2-cocycles. For the time being, we will ignore that we have chosen a specific 2-cocycle $c_u \in Z^2(H, \mathbb{A}_L^\times)$ and track everything through abstractly. To track ι, we start by computing

$$(\iota c_u)\,(h, h') : g \mapsto (g c_u(h, h'))^{1_{g\in H}}.$$

Next we must track through cor. This is more difficult; we follow [NSW08]. To begin, we choose representatives for cosets in $H\backslash G$, letting $\overline{Hg}$ denote the representative of $H\backslash G$; for coherence reasons, we require $\overline{He} = e$, where $e \in G$ is the identity. With this notation, we may compute

$$(\mathrm{cor}\,\iota c_u)\,(g_1, g_2) = \sum_{Hg\in H\backslash G} (\overline{Hg})^{-1} \cdot (\iota c_u)\left(\overline{Hg}g_1\overline{Hgg_1}^{-1}, \overline{Hgg_1}g_2\overline{Hgg_1g_2}^{-1}\right).$$

Now, the G-action on $\mathrm{CoInd}_H^G \mathbb{A}_L^\times$ takes $f\colon G \to \mathbb{A}_L^\times$ to $(gf)\colon x \mapsto f(xg)$. So when we plug in $g_0 \in G$, we get

$$\begin{aligned}(\mathrm{cor}\,\iota c_u)\,(g_1, g_2)\,(g_0) &= \prod_{Hg\in H\backslash G} (\iota c_u)\left(\overline{Hg}g_1\overline{Hgg_1}^{-1}, \overline{Hgg_1}g_2\overline{Hgg_1g_2}^{-1}\right)\left(g_0\overline{Hg}^{-1}\right)\\ &= \prod_{Hg\in H\backslash G} \left(g_0\overline{Hg}^{-1} c_u\left(\overline{Hg}g_1\overline{Hgg_1}^{-1}, \overline{Hgg_1}g_2\overline{Hgg_1g_2}^{-1}\right)\right)^{1_{g_0\overline{Hg}^{-1}\in H}}.\end{aligned}$$

The only opportunity for a factor in the product to not output 1 is when $g_0\overline{Hg}^{-1} \in H$, which is equivalent to $Hg_0 = Hg$, yielding

$$(\mathrm{cor}\,\iota c_u)\,(g_1, g_2)\,(g_0) = g_0\overline{Hg_0}^{-1} c_u\left(\overline{Hg_0}g_1\overline{Hg_0g_1}^{-1}, \overline{Hg_0g_1}g_2\overline{Hg_0g_1g_2}^{-1}\right).$$

This will be explicit enough for our purposes.

Continuing, we go from $Z^2\big(G, \mathrm{CoInd}_{G_v}^G \mathbb{A}_L^\times\big)$ up to $Z^2\big(G, \mathrm{Mor}_{\mathrm{Set}}(H\backslash G, \mathbb{A}_L^\times)\big)$, for which we note that $f \in \mathrm{CoInd}_{G_v}^G \mathbb{A}_L^\times$ should be sent to $Hg \mapsto gf\left(g^{-1}\right)$. (This is well-defined because $f(hg) = hf(g)$ for $h \in H$ here.) This gives the 2-cocycle

$$(g_1, g_2) \mapsto Hg_0 \mapsto \overline{Hg_0^{-1}}^{-1} c_u\left(\overline{Hg_0^{-1}}g_1\overline{Hg_0^{-1}g_1}^{-1}, \overline{Hg_0^{-1}g_1}g_2\overline{Hg_0^{-1}g_1g_2}^{-1}\right).$$

The above immediately extends to a 2-cocycle in $Z^2\big(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G_v\backslash G], \mathbb{A}_L^\times)\big)$, which then turns into the 2-cocycle

$$(g_1, g_2) \mapsto g_0 v \mapsto \overline{Hg_0^{-1}}^{-1} c_u\left(\overline{Hg_0^{-1}}g_1\overline{Hg_0^{-1}g_1}^{-1}, \overline{Hg_0^{-1}g_1}g_2\overline{Hg_0^{-1}g_1g_2}^{-1}\right)$$

in $c_2 \in Z^2\big(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], \mathbb{A}_L^\times)\big)$.

Should this by g0 inverse v?

Only now do we let the place $u \in V_K$ vary, extending c_2 accordingly to

$$c_2(g_1, g_2)\colon g_0 v(u) \mapsto \overline{G_{v(u)}g_0^{-1}}^{-1} c_u\left(\overline{G_{v(u)}g_0^{-1}}g_1\overline{G_{v(u)}g_0^{-1}g_1}^{-1}, \overline{G_{v(u)}g_0^{-1}g_1}g_2\overline{G_{v(u)}g_0^{-1}g_1g_2}^{-1}\right) \tag{7.5}$$

in $c_2 \in Z^2(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], \mathbb{A}_L^\times))$; this is the representative of α_2 we are looking for.

Example 181. If $g_1, g_2 \in H$ and $g_0 = e$, then

$$c_2(g_1, g_2) \colon v(u) \mapsto c_u(g_1, g_2),$$

as needed; notably, we used the requirement that $\overline{He} = e$.

7.2.4 Finishing Up

We will now be more concrete to our example. Because G is cyclic, and $G_{v(u)}$ is cyclic generated by σ^{d_u}, we can set

$$\overline{G_{v(u)}\sigma^i} = \sigma^i$$

for each $0 \le i < d_u$. This gives the 2-cocycle

$$c_2\left(\sigma^i, \sigma^j\right) : \sigma^c v(u) \mapsto \sigma^c(\omega_u / i_{\mathfrak{P}} x)^{\left\lfloor \frac{\left[\left\lfloor \frac{i+[-c]_{d_u}}{d_u} \right\rfloor\right]_{n_u} + \left[\left\lfloor \frac{i+j+[-c]_{d_u}}{d_u} \right\rfloor - \left\lfloor \frac{i+[-c]_{d_u}}{d_u} \right\rfloor\right]_{n_u}}{n_u} \right\rfloor}$$

in $c_2 \in Z^2\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], \mathbb{A}_L^\times)\right)$ after tracking through (7.5).

As a last addendum, we go ahead and compute the α associated to c_2. Namely, we want to compute

$$\begin{aligned}
\alpha\left(\sigma^c v(u)\right) &= \prod_{i=0}^{n-1} c\left(\sigma^i, \sigma\right)\left(\sigma^c v(u)\right) \\
&= \sigma^c(\omega_u / i_{\mathfrak{P}} x)^{\sum_{i=0}^{n-1} \left\lfloor \frac{\left[\left\lfloor \frac{i+[-c]_{d_u}}{d_u} \right\rfloor\right]_{n_u} + \left[\left\lfloor \frac{i+1+[-c]_{d_u}}{d_u} \right\rfloor - \left\lfloor \frac{i+[-c]_{d_u}}{d_u} \right\rfloor\right]_{n_u}}{n_u} \right\rfloor}.
\end{aligned}$$

It turns out that the giant sum is just 1, which we outsource to the following lemma.

Lemma 182. Let $n, d > 0$ be positive integers. Then, for any $c \in [0, d)$, we have

$$\sum_{i=0}^{nd-1} \left\lfloor \frac{\left[\left\lfloor \frac{i+c}{d} \right\rfloor\right]_n + \left[\left\lfloor \frac{i+1+c}{d} \right\rfloor - \left\lfloor \frac{i+c}{d} \right\rfloor\right]_n}{n} \right\rfloor = 1.$$

Proof. Note that each term in the sum is either 0 or 1 because the terms take the form $\left\lfloor \frac{a+b}{n} \right\rfloor$ where $0 \le a, b < n$. As such, we are counting the number of nonzero terms in the sum.

Well, we claim that the term is nonzero if and only if $i = nd - c - 1$. Note that $n, d > 0$ and $c < d$ implies that $nd - c - 1$ is a valid input in $[0, nd - 1)$. Anyway, we start by showing that, if the term

$$\left\lfloor \frac{\left[\left\lfloor \frac{i+c}{d} \right\rfloor\right]_n + \left[\left\lfloor \frac{i+1+c}{d} \right\rfloor - \left\lfloor \frac{i+c}{d} \right\rfloor\right]_n}{n} \right\rfloor$$

is nonzero, then $i = nd - c - 1$. Note that $\left\lfloor \frac{i+1+c}{d} \right\rfloor - \left\lfloor \frac{i+c}{d} \right\rfloor$ must be positive for this to be possible, or else the entire numerator is less than n. However, for this to be positive, we need $i + 1 + c$ to be a multiple of d, which means

$$i \equiv -c - 1 \pmod{d}.$$

Even still, we don't get much from this, only that $\left\lfloor \frac{i+1+c}{d} \right\rfloor - \left\lfloor \frac{i+c}{d} \right\rfloor = 1$. As such, we're going to need

$$\left[\left\lfloor \frac{i+c}{d} \right\rfloor\right]_n = n - 1$$

for our term to be nonzero. Of course, $i < nd$ and $c < d$, so $\frac{i+c}{d} < n$, so we don't even have to worry about modding out by n here. As such, we really just need $\frac{i+c}{d} \geq n-1$, which translates into

$$i \geq nd - c - d.$$

Combining this with the fact that $i < nd$ and $i \equiv -c-1 \pmod{d}$, we see that we are forced to have $i = nd - c - 1$.

We finish by remarking that $i = nd - c - 1$ will give

$$\left\lfloor \frac{\left[\left\lfloor \frac{i+c}{d} \right\rfloor\right]_n + \left[\left\lfloor \frac{i+1+c}{d} \right\rfloor - \left\lfloor \frac{i+c}{d} \right\rfloor\right]_n}{n} \right\rfloor = \left\lfloor \frac{n-1+1}{n} \right\rfloor = 1$$

as discussed above. This completes the proof. ∎

In total, our value of α comes out to be

$$\alpha^{(2)} \colon \sigma^c v(u) \mapsto \sigma^c \omega_u / i_{\mathfrak{P}} x.$$

For brevity, we set $\omega_{\omega^c v(u)} \coloneqq \sigma^c \omega_u$. By construction, $\omega_u \in L^{G_v}$, so ω_v does not depend on the exact choice of σ^c among coset representatives in G/G_v. So we can write more succinctly that

$$\boxed{\alpha^{(2)} \colon v \mapsto \omega_v / i_{\mathfrak{P}} x}.$$

This completes the computation.

7.3 Localizing

Note that there is a (unique) map $\lambda_v \colon \mathbb{Z} \to \mathbb{Z}[V_L]$ by $1 \mapsto v$, which induces a map of protori $\lambda_v \colon \mathbb{D} \to \mathbb{G}_m$. With respect to α_2, we are interested in this map as moving

$$(- \circ \lambda_v) \colon \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], \mathbb{A}_L^\times) \to \mathbb{A}_L^\times,$$

which we can track as the evaluation-at-v map eval_v. In particular, we defined α_2 by Lemma 171 to be the unique cohomology class in $\widehat{H}^2(G, \mathbb{D}(\mathbb{A}_L))$ such that

$$\operatorname{eval}_{v(u)} \operatorname{Res}_{G_{v(u)}} \alpha_2 = \alpha(L_v/K_u)$$

for each place $u \in V_K$ (see Remark 172), which we now see is equivalent to

$$\lambda_{v(u)} \operatorname{Res}_{G_{v(u)}} \alpha_2 = \alpha(L_v/K_u).$$

On the level of gerbs, we are asking for α_2 to be the unique cohomology class making the following diagram commute for all $u \in V_K$; here $v \coloneqq v(u)$.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{D}(\mathbb{A}_L) & \longrightarrow & \mathcal{E}_2(L/K) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\
 & & \| & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & \mathbb{D}(\mathbb{A}_L) & \longrightarrow & \mathcal{E}_2''(L/K) & \longrightarrow & \mathrm{Gal}(L_v/K_u) & \longrightarrow & 1 \\
 & & {\scriptstyle \lambda_v}\downarrow & & {\scriptstyle \widetilde{\lambda}_v}\downarrow & & \| & & \\
1 & \longrightarrow & \mathbb{G}_m(\mathbb{A}_L) & \longrightarrow & \mathcal{E}_2'(L/K) & \longrightarrow & \mathrm{Gal}(L_v/K_u) & \longrightarrow & 1 \\
 & & {\scriptstyle i_v}\uparrow & & {\scriptstyle \widetilde{i}_v}\uparrow & & \| & & \\
1 & \longrightarrow & \mathbb{G}_m(L_v) & \longrightarrow & \mathcal{E}(L_v/K_u) & \longrightarrow & \mathrm{Gal}(L_v/K_u) & \longrightarrow & 1
\end{array}$$

Here, the morphisms $\widetilde{\lambda}_v$ and $\widetilde{i}_v$ are induced by the rest of the diagram.

7.3.1 Choosing Lifts

We now work in a little more generality, taking L/K to be the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$, where N is odd.

Remark 183. We will take N to be odd entirely for psychological reasons. The arguments below in fact extend to allow N to satisfy any of the following conditions:

- N is not divisible by 8,
- N is not divisible by 3, or
- N divisible by 9.

Taking a prime factorization of N, we write

$$N = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m}$$

and so choose generators $x_i \in (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^\times$ so that

$$\sigma_i \colon \zeta_{p_i^{a_i}} \mapsto \zeta_{p_i^{a_i}}^{x_i}$$

extends to an automorphism $\sigma_i \in \mathrm{Gal}(L/K)$ (namely, acting as the identity on the other ζ_{p^a}s) so that

$$\mathrm{Gal}(L/K) \simeq \bigoplus_{i=1}^{m} \langle \sigma_i \rangle.$$

Now, when we localize to some place $v \in V_L$ lying over a finite place $q = u \in V_K$, the unramified part of the decomposition group G_v will be generated by the Frobenius automorphism

$$\sigma_q \colon \zeta \mapsto \zeta^q,$$

where $\zeta = \zeta_{N/q^a}$ with $\gcd(N/q^a, q) = 1$.

Our goal for this subsection is to choose lifts $f_i \in \mathcal{E}_2(L/K)$ so that the $\widetilde{\lambda}_v f_i$ commute as much as possible in $\mathcal{E}_2'(L/K)$. In particular, when $v \coloneqq v(u) \in V_L$ lies over $u \in V_K$, we claim that we can arrange things so that

$$(\widetilde{\lambda}_v f_i)(\widetilde{\lambda}_v f_j) = (\widetilde{\lambda}_v f_j)(\widetilde{\lambda}_v f_i)$$

as long as neither p_i nor p_j are primes corresponding to the place u. To begin, we note that

$$\widehat{H}^2\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_L], \mathbb{A}_L^\times)\right) \simeq \prod_{u \in V_K} \widehat{H}^2\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], \mathbb{A}_L^\times)\right)$$

is an isomorphism at the level of 2-cocycles simply by gluing all the local α_2s together. Namely, we may choose whatever 2-cocycles we want from $Z^2\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], \mathbb{A}_L^\times)\right)$ (as long as they cohere correctly via Shapiro's lemma according to Remark 172), and we know that they will combine into a coherent 2-cocycle for α_2.

This is all to say that we may set all the $\widetilde{\lambda}_v f_i \in \mathbb{A}_L^\times$ independently and not worry about coherence issues. As such, we now fix $u \in V_K$ and $v \coloneqq v(u) \in V_L$. So, for the time being, we set c_u to represent $\alpha(L_v/K_u)$ by some triple and extend c_u up to

$$c_{2u} \coloneqq \mathrm{cor}\, \iota i_v c_u \in Z^2\left(G, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[V_u], \mathbb{A}_L^\times)\right)$$

as in (7.5). We will simply set

$$\widetilde{\lambda}_v f_i \coloneqq (1, \sigma_i)$$

and see how far it gets us. In particular, we can compute

$$(\widetilde{\lambda}_v f_i)(\widetilde{\lambda}_v f_j)(\widetilde{\lambda}_v f_i)^{-1}(\widetilde{\lambda}_v f_j)^{-1} = \frac{c_{2u}(\sigma_i, \sigma_j)(v)}{c_{2u}(\sigma_j, \sigma_i)(v)},$$

so we want to force $c_{2u}(\sigma_i, \sigma_j) = c_{2u}(\sigma_j, \sigma_i)$ as much as possible. Thus, we expand

$$c_{2u}(\sigma_i, \sigma_j) \colon v \mapsto i_v c_u \left(g_1 \overline{G_v g_1}^{-1}, \overline{G_v g_1} g_2 \overline{G_v g_1 g_2}^{-1} \right).$$

Now, by definition of c_u, we note that

$$c_u(1, g) = c_u(g, 1) = 1$$

for each $g \in G_v$, so we have at least have a chance of forcing things to work out.

Let S be the image of $G_v \backslash G \to G$ given by $G_v g \mapsto \overline{G_v g}$, which essentially makes our degrees of freedom in defining c_{2u}. It will not matter very much if v is ramified or unramified, so we will just assume (roughly without loss of generality) that $u = p_m$ so that we are interested in showing the $\widetilde{\lambda}_v f_i$ for $i < m$; in the unramified cases, we should just skip this step of the construction and replace m with $m-1$ going forward.

Finish this.

Now, to begin, we claim that we can pack S to contain all but at most one of the σ_i.

7.4 Computing $\mathcal{E}_3$

In this section we continue the computation with $L \coloneqq \mathbb{Q}(\zeta_{p^m})$ and $K \coloneqq \mathbb{Q}$ from subsection 7.2. Namely, at the end we computed that

$$\widetilde{c}_2 \left(\sigma^i, \sigma^j \right) : v \mapsto (\omega_v / i_{\mathfrak{P}} x)^{\left\lfloor \frac{i+j}{n} \right\rfloor}$$

represents $\alpha_2 \in \widehat{H}^2(G, \mathbb{A}_L^\times)$. We now recall that

$$c_1(\sigma^i, \sigma^j) \coloneqq i_{\mathfrak{P}} x^{-\left\lfloor \frac{i+j}{n} \right\rfloor}$$

represents the global fundamental class $\alpha_1 \in \widehat{H}^2(G, \mathbb{A}_L^\times / L^\times)$. However, our careful choice of c_2 and c_1 implies that the following diagram commutes for all $g, g' \in G$.

$$\begin{array}{ccc} \mathbb{Z}[V_L] & \longrightarrow & \mathbb{Z} \\ {\scriptstyle c_2(g,g')}\downarrow & & \downarrow{\scriptstyle c_1(g,g')} \\ \mathbb{A}_L^\times & \longrightarrow & \mathbb{A}_L^\times / L^\times \end{array}$$

These two morphisms induce a unique morphism $c_1(g, g') \colon \mathbb{Z}[V_L]_0 \to L^\times$ as follows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}[V_L]_0 & \longrightarrow & \mathbb{Z}[V_L] & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & {\scriptstyle c_3(g,g')}\downarrow & & \downarrow{\scriptstyle c_2(g,g')} & & \downarrow{\scriptstyle c_1(g,g')} & & \\ 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{A}_L^\times & \longrightarrow & \mathbb{A}_L^\times / L^\times & \longrightarrow & 0 \end{array}$$

In fact, because we have

$$\frac{g c_i(g', g'') \cdot c_i(g, g' g'')}{c_i(g, g') \cdot c_i(g g', g'')} = 1$$

for all $g, g', g'' \in G$ and $i \in \{1, 2\}$, the uniqueness of the induced arrow c_3 implies that the same relation must hold for $i = 3$ above. In particular, c_3 is a 2-cocycle, and by construction c_3 represents α_3.

We can even write down c_3 explicitly. Indeed, given $v - v' \in \mathbb{Z}[V_L]_0$, we have

$$c_2(\sigma^i, \sigma^j)(v - v') = (\omega_v / \omega_{v'})^{\left\lfloor \frac{i+j}{n} \right\rfloor} \in L^\times,$$

so we have

$$c_3(\sigma^i, \sigma^j)(v - v') = (\omega_v / \omega_{v'})^{\left\lfloor \frac{i+j}{n} \right\rfloor}.$$

In particular, our value of α comes out to be

$$\boxed{\alpha^{(3)} \colon (v - v') \mapsto \omega_v / \omega_{v'}}.$$

We quickly recall that $\omega_{\sigma^c v(u)} \coloneqq \sigma^c \omega_u$, where ω_u was defined in (7.4).

References

[CE56] Henri Cartan and Samuel Eilenberg. *Homological Algebra*. Princeton mathematical series. Princeton: Princeton University Press, 1956.

[Tat66] John Tate. "The cohomology groups of tori in finite Galois extensions of number fields". In: *Nagoya Mathematical Journal* 27.P2 (1966), pp. 709–719.

[AS78] Shimshon A. Amitsur and David J. Saltman. "Generic abelian crossed products and p-algebras". In: *Journal of Algebra* 51 (1978), pp. 76–87.

[Tig81] Jean-Pierre Tignol. "Produits croisés abéliens". In: *Journal of Algebra* 70.2 (1981), pp. 420–436. ISSN: 0021-8693. DOI: https://doi.org/10.1016/0021-8693(81)90227-1. URL: https://www.sciencedirect.com/science/article/pii/0021869381902271.

[Bro82] Kenneth S. Brown. *Cohomology of Groups*. 1st ed. Graduate Texts in Mathematics. Springer New York, 1982.

[Ser91] Jean-Pierre Serre. *Local Fields*. 1st ed. Graduate Texts in Mathematics. Springer New York, 1991.

[PR94] Vladimir Platonov and Andrei Rapinchuk. *Algebraic Groups and Number Theory*. Vol. 139. Pure and Applied Mathematics. Elsevier, 1994, pp. 583–608. DOI: https://doi.org/10.1016/S0079-8169(08)62077-2. URL: https://www.sciencedirect.com/science/article/pii/S0079816908620772.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin, Heidelberg, 1999.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of Number Fields*. 2nd ed. Grundlehren der mathematischen Wissenschaften. Springer Berlin, Heidelberg, 2008.

[AW10] M. F. Atiyah and C. T. C. Wall. "Cohomology of Groups". In: *Algebraic Number Theory: Proceedings of an Instructional Conference*. Ed. by J. W. S. Cassels and A. Fröhlich. 2nd ed. London Mathematical Society, 2010.

[Tat10] J. T. Tate. "Global Class Field Theory". In: *Algebraic Number Theory: Proceedings of an Instructional Conference*. Ed. by J. W. S. Cassels and A. Fröhlich. 2nd ed. London Mathematical Society, 2010.

[Buc13] Paul R. Buckingham. "Local and global fundamental classes for multiquadratic extensions". In: *Journal of Number Theory* 133.2 (2013), pp. 620–638. ISSN: 0022-314X. DOI: https://doi.org/10.1016/j.jnt.2012.08.014. URL: https://www.sciencedirect.com/science/article/pii/S0022314X12002600.

[Neu13] Jürgen Neukirch. *Class Field Theory: The Bonn Lectures*. Ed. by Alexander Schmidt. Springer Berlin, Heidelberg, 2013.

[Kot14] Robert Kottwitz. "B(G) for all local and global fields". In: (Jan. 2014).

[Kal18] Tasho Kaletha. "Global rigid inner forms and multiplicities of discrete automorphic representations". In: *Inventiones mathematicae* 213.1 (July 2018), pp. 271–369. ISSN: 1432-1297. DOI: 10.1007/s00222-018-0791-3. URL: https://doi.org/10.1007/s00222-018-0791-3.

[Mil20] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

A Verification of the Cocycle

In this section, we verify Theorem 105. As such, in this section, we will work under the modified set-up, forgetting about the extension $\mathcal{E}$ but letting $(\{\alpha_i\}, \{\beta_{ij}\})$ be some $\{\sigma_i\}_{i=1}^m$-tuple.

Here the formula looks like

$$c(g,g') \coloneqq \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij}\right]\left[\prod_{i=1}^m\left(\prod_{1\le k<i}\sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right],$$

where $g=\prod_i\sigma_i^{a_i}$ and $g'=\prod_i\sigma_i^{b_i}$ with $0\le a_i,b_i<n_i$ and $q_i\coloneqq\lfloor(a_i+b_i)/n_i\rfloor$. To make this more digestible, we define

$$g_i\coloneqq\prod_{1\le k<i}\sigma_k^{a_k}$$

for any $g=\prod_i\sigma_i^{a_i}\in G$. Also, for extra brevity, we will define

$$\beta_{ij}^{(a_ib_j)}\coloneqq\sigma_i^{(a_i)}\sigma_j^{(b_j)}\beta_{ij},$$

so we can write down our formula as

$$c(g,g')\coloneqq\left[\prod_{1\le j<i\le m}g_ig_j'\beta_{ij}^{(a_ib_j)}\right]\left[\prod_{i=1}^m g_ig_i'\alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right].$$

Now, given $g,g',g''\in G$, we would like to check

$$gc(g',g'')\cdot c(g,g'g'')\overset{?}{=}c(gg',g'')\cdot c(g,g'),$$

where $g=\prod_i\sigma_i^{a_i}$ and $g'=\prod_i\sigma_i^{b_i}$ and $g''=\prod_i\sigma_i^{c_i}$ with $0\le a_i,b_i,c_i<n_i$.

A.1 Carries

We will begin our verification by dealing with carries; we start with the following lemma, intended to beef up our relation (4.2).

Lemma 184. Given indices $i>j$ with $a_i,a_j,q_i,q_j\ge 0$, we have

$$\beta_{ij}^{(a_ia_j)}=\beta_{ij}^{(a_i+q_in_i,a_j)}\left(\frac{\sigma_j^{a_j}(\alpha_i)}{\alpha_i}\right)^{q_i}\qquad\text{and}\qquad\beta_{ij}^{(a_ia_j)}=\beta_{ij}^{(a_i,a_j+q_jn_j)}\left(\frac{\alpha_j}{\sigma_i^{a_i}(\alpha_j)}\right)^{q_j}.$$

Proof. This is a matter of force. For one, we compute

$$\begin{aligned}\beta_{ij}^{(a_i+n_iq_i,a_j)}&=\prod_{p=0}^{a_i+n_iq_i-1}\prod_{q=0}^{a_j-1}\sigma_i^p\sigma_j^q\beta_{ij}\\&=\left(\prod_{p=0}^{a_i-1}\prod_{q=0}^{a_j-1}\sigma_i^p\sigma_j^q\beta_{ij}\right)\left(\prod_{q=0}^{a_j-1}\prod_{p=a_i}^{a_i+n_iq_i-1}\sigma_i^p\sigma_j^q\beta_{ij}\right)\\&=\beta_{ij}^{(a_ia_j)}\left(\prod_{q=0}^{a_j-1}\sigma_j^q\,\mathrm{N}_{L/L_i}(\beta_{ij})\right)^{q_i}.\end{aligned}$$

Now, using the relation $\mathrm{N}_{L/L_i}(\beta_{ij}) = \alpha_i/\sigma_j(\alpha_i)$ from (4.2), this becomes

$$\begin{aligned}\beta_{ij}^{(a_i+n_iq_i,a_j)} &= \beta_{ij}^{(a_ia_j)}\left(\prod_{q=0}^{a_j-1}\frac{\sigma_j^q\alpha_i}{\sigma^{j+1}\alpha_i}\right)^{q_i}\\ &= \beta_{ij}^{(a_ia_j)}\left(\frac{\alpha_i}{\sigma^{a_j}\alpha_i}\right)^{q_i},\end{aligned}$$

which rearranges into what we wanted.

For the other, we again just compute

$$\begin{aligned}\beta_{ij}^{(a_i,a_j+n_jq_j)} &= \prod_{p=0}^{a_i-1}\prod_{q=0}^{a_j+n_jq_j-1}\sigma_i^p\sigma_j^q\beta_{ij}\\ &= \left(\prod_{p=0}^{a_i-1}\prod_{q=0}^{a_j-1}\sigma_i^p\sigma_j^q\beta_{ij}\right)\left(\prod_{p=0}^{a_i-1}\prod_{q=q_j}^{a_j+n_jq_j-1}\sigma_i^p\sigma_j^q\beta_{ij}\right)\\ &= \beta_{ij}^{(a_ia_j)}\left(\prod_{p=0}^{a_i-1}\sigma_i^p\,\mathrm{N}_{L/L_q}(\beta_{ij})\right)^{q_i}.\end{aligned}$$

This time, we use the relation $\mathrm{N}_{L/L_j}(\beta_{ij}) = \sigma_i(\alpha_j)/\alpha_j$, which gives

$$\begin{aligned}\beta_{ij}^{(a_i,a_j+n_jq_j)} &= \beta_{ij}^{(a_ia_j)}\left(\prod_{p=0}^{a_i-1}\frac{\sigma_i^{p+1}(\alpha_j)}{\sigma_i^p(\alpha_j)}\right)^{q_i}\\ &= \beta_{ij}^{(a_ia_j)}\left(\frac{\sigma_i^{a_j}(\alpha_j)}{\alpha_j}\right)^{q_i},\end{aligned}$$

which again rearranges into the desired. ■

We are now ready to begin the computation, dealing with carries to start. Use the division algorithm to write

$$a_i + b_i = n_iu_i + x_i \qquad \text{and} \qquad b_i + c_i = n_iv_i + y_i,$$

where $u_i, v_i \in \{0,1\}$ and $0 \le x_i, y_i < n_i$ for each i. We start by collecting remainder terms on the side of $gc(g',g'')\cdot c(g,g'g'')$.

1. Note

$$gc(g',g'') = g\left[\prod_{1\le j<i\le m} g_i'g_j''\beta_{ij}^{(b_ic_j)}\right]\cdot g\left[\prod_{i=1}^m g_i'g_i''\alpha_i^{v_i}\right],$$

so we set

$$R_1 \coloneqq \prod_{i=1}^m gg_i'g_i''\alpha_i^{v_i}$$

to be our remainder term.

2. Note

$$\begin{aligned}c(g,g'g'') &= \left[\prod_{1\le j<i\le m} g_ig_j'g_j''\beta_{ij}^{(a_iy_j)}\right]\left[\prod_{i=1}^m g_ig_i'g_i''\alpha_i^{\left\lfloor\frac{a_i+y_i}{n_i}\right\rfloor}\right]\\ &= \left[\prod_{1\le j<i\le m} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)}\cdot g_ig_j'g_j''\left(\frac{\alpha_j}{\sigma_i^{a_i}\alpha_j}\right)^{v_i}\right]\left[\prod_{i=1}^m g_ig_i'g_i''\alpha_i^{\left\lfloor\frac{a_i+y_i}{n_i}\right\rfloor}\right]\\ &= \left[\prod_{1\le j<i\le m} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)}\right]\left[\prod_{1\le j<i\le m} g_ig_j'g_j''\left(\frac{\alpha_j}{\sigma_i^{a_i}\alpha_j}\right)^{v_i}\right]\left[\prod_{i=1}^m g_ig_i'g_i''\alpha_i^{\left\lfloor\frac{a_i+y_i}{n_i}\right\rfloor}\right],\end{aligned}$$

so we set

$$R_2 \coloneqq \left[\prod_{1\le j<i\le m} g_i g_j' g_j'' \left(\frac{\alpha_j}{\sigma_i^{a_i}\alpha_j}\right)^{v_i}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor}\right]$$

to be our remainder term.

3. Lastly, we collect our remainders. Observe

$$\begin{aligned}
R_2 &= \left[\prod_{j=1}^m g_j' g_j'' \left(\prod_{i=j+1}^m g_i \cdot \frac{\alpha_j}{\sigma_i^{a_i}\alpha_j}\right)^{v_i}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{j=1}^m g_j' g_j'' \left(\prod_{i=j+1}^m \frac{(\sigma_1^{a_1}\cdots\sigma_{i-1}^{a_{i-1}})\alpha_j}{(\sigma_1^{a_1}\cdots\sigma_{i-1}^{a_{i-1}})\sigma_i^{a_i}\alpha_j}\right)^{v_i}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{j=1}^m g_j' g_j'' \left(\prod_{i=j+1}^m \frac{g_i\alpha_j}{g_{i+1}\alpha_j}\right)^{v_i}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{j=1}^m g_j' g_j'' \cdot \frac{g_{j+1}\alpha_j^{v_j}}{g\alpha_j^{v_j}}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor}\right].
\end{aligned}$$

We now note that $g_{j+1}\alpha_j = g_j\alpha_j$ because α_j is fixed by σ_j. As such,

$$\begin{aligned}
R_1R_2 &= \left[\prod_{i=1}^m g g_i' g_i'' \alpha_i^{v_i}\right]\left[\prod_{i=1}^m g_i' g_i'' \cdot \frac{g_i\alpha_i^{v_i}}{g\alpha_i^{v_i}}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor}\right] \\
&= \prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{v_i+\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor},
\end{aligned}$$

which is nice enough for us now.

Now, we collect remainder terms from $c(gg', g'') \cdot c(g, g')$.

1. Note

$$\begin{aligned}
c(gg', g'') &= \left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \beta_{ij}^{(x_i c_j)}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)} \cdot g_i g_i' g_j'' \left(\frac{\sigma_j^{c_j}\alpha_i}{\alpha_i}\right)^{u_i}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)}\right]\left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \left(\frac{\sigma_j^{c_j}\alpha_i}{\alpha_i}\right)^{u_i}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right],
\end{aligned}$$

so we set

$$R_3 \coloneqq \left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \left(\frac{\sigma_j^{c_j}\alpha_i}{\alpha_i}\right)^{u_i}\right]\left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right].$$

2. Note

$$c(g, g') = \left[\prod_{1\le j<i\le m} g_i g_j' \beta_{ij}^{(a_i b_j)}\right]\left[\prod_{i=1}^m g_i g_i' \alpha_i^{u_i}\right],$$

so we set

$$R_4 \coloneqq \left[\prod_{i=1}^m g_i g_i' \alpha_i^{u_i}\right].$$

3. Lastly, we collect our remainder terms. Observe

$$\begin{aligned}
R_3 &= \left[\prod_{i=1}^{m} g_i g_i' \left(\prod_{j=1}^{i-1} g_j'' \cdot \frac{\sigma_j^{c_j}\alpha_i}{\alpha_i}\right)^{u_i}\right]\left[\prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{i=1}^{m} g_i g_i' \left(\prod_{j=1}^{i-1} \frac{(\sigma_1^{c_1}\cdots\sigma_{j-1}^{c_{j-1}})\sigma_j^{c_j}\alpha_i}{(\sigma_1^{c_1}\cdots\sigma_{j-1}^{c_{j-1}})\alpha_i}\right)^{u_i}\right]\left[\prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{i=1}^{m} g_i g_i' \left(\prod_{j=1}^{i-1} \frac{g_{j+1}''\alpha_i}{g_j''\alpha_i}\right)^{u_i}\right]\left[\prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\
&= \left[\prod_{i=1}^{m} g_i g_i' \cdot \frac{g_i''\alpha_i^{u_i}}{\alpha_i^{u_i}}\right]\left[\prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right].
\end{aligned}$$

Thus,

$$\begin{aligned}
R_3R_4 &= \left[\prod_{i=1}^{m} g_i g_i' \cdot \frac{g_i''\alpha_i^{u_i}}{\alpha_i^{u_i}}\right]\left[\prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right]\left[\prod_{i=1}^{m} g_i g_i' \alpha_i^{u_i}\right] \\
&= \prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{u_i+\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor},
\end{aligned}$$

which is again simple enough for our purposes.

We now note that, for each i,

$$u_i + \left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor = \left\lfloor \frac{a_i+b_i+c_i}{n_i}\right\rfloor = v_i + \left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor$$

by how carried addition behaves. It follows that

$$R_1R_2 = \prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{v_i+\left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor} = \prod_{i=1}^{m} g_i g_i' g_i'' \alpha_i^{u_i+\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor} = R_3R_4.$$

Thus, it suffices to show that

$$\frac{gc(g',g'')}{R_1}\cdot\frac{c(g,g'')}{R_2} \stackrel{?}{=} \frac{c(gg',g'')}{R_3}\cdot\frac{c(g,g')}{R_4},$$

which is equivalent to

$$g\left[\prod_{1\le j<i\le m} g_i' g_j'' \beta_{ij}^{(b_i c_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_i g_j' g_j'' \beta_{ij}^{(a_i, b_j+c_j)}\right] \stackrel{?}{=} \left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_i g_j' \beta_{ij}^{(a_i b_j)}\right]$$

by the work above.

A.2 Finishing

We need to verify that

$$g\left[\prod_{1\le j<i\le m} g_i' g_j'' \beta_{ij}^{(b_i c_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_i g_j' g_j'' \beta_{ij}^{(a_i, b_j+c_j)}\right] \stackrel{?}{=} \left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_i g_j' \beta_{ij}^{(a_i b_j)}\right]$$

as discussed in the previous subsection.

Before beginning the check, we recall the relations on the βs from (4.3) can be written as

$$\frac{\sigma_2(\beta_{31})}{\beta_{31}} = \frac{\sigma_1(\beta_{32})}{\beta_{32}} \cdot \frac{\sigma_3(\beta_{21})}{\beta_{21}},$$

because we only have one triple (i,j,k) of indices with $i > j > k$. This is somewhat difficult to deal with directly, so we quickly show a more general version.

Lemma 185. Fix indices with $i > j > k$, and let $a_i, a_j, a_k \geq 0$. Then

$$\frac{\sigma_j^{a_j}\beta_{ik}^{(a_i a_k)}}{\beta_{ik}^{(a_i a_k)}} = \frac{\sigma_k^{a_k}\beta_{ij}^{(a_i a_j)}}{\beta_{ij}^{(a_i a_j)}} \cdot \frac{\sigma_i^{a_i}\beta_{jk}^{(a_j a_k)}}{\beta_{jk}^{(a_j a_k)}}.$$

Proof. We simply compute

$$\begin{aligned}
\frac{\sigma_i^{a_i}\beta_{jk}^{(a_j a_k)}}{\beta_{jk}^{(a_j a_k)}} \cdot \frac{\sigma_k^{a_k}\beta_{ij}^{(a_i a_j)}}{\beta_{ij}^{(a_i a_j)}} &= \prod_{r=0}^{a_i-1} \frac{\sigma_i^{r+1}\beta_{jk}^{(a_j a_k)}}{\sigma_i^{r}\beta_{jk}^{(a_j a_k)}} \cdot \prod_{p=0}^{a_k-1} \frac{\sigma_k^{p+1}\beta_{ij}^{(a_i a_j)}}{\sigma_k^{p}\beta_{ij}^{(a_i a_j)}} \\
&= \prod_{p=0}^{a_k-1}\prod_{q=0}^{a_j-1}\prod_{r=0}^{a_i-1} \left(\frac{\sigma_k^p\sigma_j^q\sigma_i^{r+1}\beta_{jk}}{\sigma_k^p\sigma_j^q\sigma_i^r\beta_{jk}} \cdot \frac{\sigma_k^{p+1}\sigma_j^q\sigma_i^r\beta_{ij}}{\sigma_k^p\sigma_j^q\sigma_i^r\beta_{ij}} \right) \\
&= \prod_{p=0}^{a_k-1}\prod_{q=0}^{a_j-1}\prod_{r=0}^{a_i-1} \sigma_k^p\sigma_j^q\sigma_i^r \left(\frac{\sigma_i\beta_{jk}}{\beta_{jk}} \cdot \frac{\sigma_k\beta_{ij}}{\beta_{ij}} \right) \\
&= \prod_{p=0}^{a_k-1}\prod_{q=0}^{a_j-1}\prod_{r=0}^{a_i-1} \sigma_k^p\sigma_j^q\sigma_i^r \left(\frac{\sigma_j\beta_{ik}}{\beta_{ik}} \right),
\end{aligned}$$

where in the last equality we have use the relation on the βs. Continuing,

$$\begin{aligned}
\frac{\sigma_i^{a_i}\beta_{jk}^{(a_j a_k)}}{\beta_{jk}^{(a_j a_k)}} \cdot \frac{\sigma_k^{a_k}\beta_{ij}^{(a_i a_j)}}{\beta_{ij}^{(a_i a_j)}} &= \prod_{q=0}^{a_j-1} \left(\prod_{p=0}^{a_k-1}\prod_{r=0}^{a_i-1} \frac{\sigma_j^{q+1}\sigma_k^p\sigma_i^r\beta_{ik}}{\sigma_j^q\sigma_k^p\sigma_i^r\beta_{ik}} \right) \\
&= \prod_{q=0}^{a_j-1} \frac{\sigma_j^{q+1}\beta_{ik}^{(a_i a_k)}}{\sigma_j^{q}\beta_{ik}^{(a_i a_k)}} \\
&= \frac{\sigma_j^{a_j}\beta_{ik}^{(a_i a_k)}}{\beta_{ik}^{(a_i a_k)}},
\end{aligned}$$

which is what we wanted. ∎

We now proceed with the check, by induction. More precisely, we claim that any $m' \leq m$ gives

$$g_{m'+1}\left[\prod_{j<i\leq m'} g_i' g_j'' \beta_{ij}^{(b_i c_j)}\right]\left[\prod_{j<i\leq m'} g_i g_j' g_j'' \beta_{ij}^{(a_i, b_j+c_j)}\right] \stackrel{?}{=} \left[\prod_{j<i\leq m'} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)}\right]\left[\prod_{j<i\leq m'} g_i g_j' \beta_{ij}^{(a_i b_j)}\right]$$

which we will show by induction on m'. For $m' = 1$, there is nothing to say because there are no indices $i > j$.

So now suppose we have equality for $m' < m$, and we give equality for $m'' := m' + 1$. That is, we want to show that

$$g_{m'+2}\prod_{j<i\leq m'+1} g_i' g_j'' \beta_{ij}^{(b_i c_j)} \cdot \prod_{j<i\leq m'+1} g_i g_j' g_j'' \beta_{ij}^{(a_i, b_j+c_j)} \stackrel{?}{=} \prod_{j<i\leq m'+1} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)} \cdot \prod_{j<i\leq m'+1} g_i g_j' \beta_{ij}^{(a_i b_j)}$$

but by the inductive hypothesis it suffices for

$$\frac{g_{m''+1}\displaystyle\prod_{j<i\le m'+1} g_i' g_j'' \beta_{ij}^{(b_i c_j)}}{g_{m'+1}\displaystyle\prod_{j<i\le m'} g_i' g_j'' \beta_{ij}^{(b_i c_j)}} \cdot \frac{\displaystyle\prod_{j<i\le m'+1} g_i g_j' g_j'' \beta_{ij}^{(a_i, b_j+c_j)}}{\displaystyle\prod_{j<i\le m'} g_i g_j' g_j'' \beta_{ij}^{(a_i, b_j+c_j)}} \stackrel{?}{=} \frac{\displaystyle\prod_{j<i\le m'+1} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)}}{\displaystyle\prod_{j<i\le m'} g_i g_i' g_j'' \beta_{ij}^{(a_i+b_i, c_j)}} \cdot \frac{\displaystyle\prod_{j<i\le m'+1} g_i g_j' \beta_{ij}^{(a_i b_j)}}{\displaystyle\prod_{j<i\le m'} g_i g_j' \beta_{ij}^{(a_i b_j)}}$$

which is collapses to

$$\frac{g_{m''+1}\displaystyle\prod_{j<i\le m'+1} g_i' g_j'' \beta_{ij}^{(b_i c_j)}}{g_{m'+1}\displaystyle\prod_{j<i\le m'} g_i' g_j'' \beta_{ij}^{(b_i c_j)}} \cdot \prod_{j\le m'} g_{m''} g_j' g_j'' \beta_{m'' j}^{(a_{m''}, b_j+c_j)} \stackrel{?}{=} \prod_{j\le m'} g_{m''} g_{m''}' g_j'' \beta_{m'' j}^{(a_{m''}+b_{m''}, c_j)} \cdot \prod_{j\le m'} g_{m''} g_j' \beta_{ij}^{(a_{m''} b_j)}$$

because the terms with $i < m'' = m' + 1$ got cancelled in the rightmost three products. Rearranging, this is the same as

$$\frac{g_{m''+1}\displaystyle\prod_{j<i\le m'+1} g_i' g_j'' \beta_{ij}^{(b_i c_j)}}{g_{m'+1}\displaystyle\prod_{j<i\le m'} g_i' g_j'' \beta_{ij}^{(b_i c_j)}} \stackrel{?}{=} \frac{\displaystyle\prod_{j<m''} g_{m''} g_{m''}' g_j'' \beta_{m'' j}^{(a_{m''}+b_{m''}, c_j)} \cdot \prod_{j<m''} g_{m''} g_j' \beta_{m'' j}^{(a_{m''} b_j)}}{\displaystyle\prod_{j<m''} g_{m''} g_j' g_j'' \beta_{m'' j}^{(a_{m''}, b_j+c_j)}}.$$

Peeling off the $i = m'' = m' + 1$ terms from the left-hand side numerator, we're showing

$$\frac{g_{m''+1}\displaystyle\prod_{j<i\le m'} g_i' g_j'' \beta_{ij}^{(b_i c_j)}}{g_{m'+1}\displaystyle\prod_{j<i\le m'} g_i' g_j'' \beta_{ij}^{(b_i c_j)}} \stackrel{?}{=} \frac{\displaystyle\prod_{j<m''} g_{m''} g_{m''}' g_j'' \beta_{m'' j}^{(a_{m''}+b_{m''}, c_j)} \cdot \prod_{j<m''} g_{m''} g_j' \beta_{m'' j}^{(a_{m''} b_j)}}{\displaystyle\prod_{j<m''} g_{m''+1} g_{m''}' g_j'' \beta_{m'' j}^{(b_{m''} c_j)} \cdot \prod_{j<m''} g_{m''} g_j' g_j'' \beta_{m'' j}^{(a_{m''}, b_j+c_j)}}.$$

We take a moment to simplify the left-hand side with Lemma 185 by writing

$$\begin{aligned}
g_{m'+1}\prod_{j<i\le m'} g_i' g_j''\left(\frac{\sigma_{m''}^{a_{m''}}\beta_{ij}^{(b_i c_j)}}{\beta_{ij}^{(b_i c_j)}}\right) &= g_{m''}\prod_{j<i\le m'} g_i' g_j''\left(\frac{\sigma_i^{b_i}\beta_{m'' j}^{(a_{m''} c_j)}}{\beta_{m'' j}^{(a_{m''} c_j)}}\cdot\frac{\beta_{m'' i}^{(a_{m''} b_i)}}{\sigma_j^{c_j}\beta_{m'' i}^{(a_{m''} b_i)}}\right) \\
&= g_{m''}\left[\prod_{j=1}^{m'} g_j''\prod_{i=j+1}^{m'} g_i'\left(\frac{\sigma_i^{b_i}\beta_{m'' j}^{(a_{m''} c_j)}}{\beta_{m'' j}^{(a_{m''} c_j)}}\right)\cdot\prod_{i=1}^{m'} g_i'\prod_{j=1}^{i-1} g_j''\left(\frac{\beta_{m'' i}^{(a_{m''} b_i)}}{\sigma_j^{c_j}\beta_{m'' i}^{(a_{m''} b_i)}}\right)\right] \\
&= g_{m''}\left[\prod_{j=1}^{m'}\frac{g_{m'+1}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}}{g_{j+1}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}}\cdot\prod_{i=1}^{m'}\frac{g_i'\beta_{m'' i}^{(a_{m''} b_i)}}{g_i' g_i''\beta_{m'' i}^{(a_{m''} b_i)}}\right] \\
&= g_{m''}\left[\prod_{j<m''}\frac{g_{m''}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}}{g_{j+1}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}}\cdot\prod_{j<m''}\frac{g_j'\beta_{m'' j}^{(a_{m''} b_j)}}{g_j' g_j''\beta_{m'' j}^{(a_{m''} b_j)}}\right]
\end{aligned}$$

after doing a lot of telescoping. Now, we can remove $g_{m''}$ everywhere to give

$$\prod_{j<m''}\frac{g_{m''}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}}{g_{j+1}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}}\cdot\prod_{j<m''}\frac{g_j'\beta_{m'' j}^{(a_{m''} b_j)}}{g_j' g_j''\beta_{m'' j}^{(a_{m''} b_j)}} \stackrel{?}{=} \frac{\displaystyle\prod_{j<m''} g_{m''}' g_j''\beta_{m'' j}^{(a_{m''}+b_{m''}, c_j)}\cdot\prod_{j<m''} g_j'\beta_{m'' j}^{(a_{m''} b_j)}}{\displaystyle\prod_{j<m''} g_{m''+1}' g_j''\beta_{m'' j}^{(b_{m''} c_j)}\cdot\prod_{j<m''} g_j' g_j''\beta_{m'' j}^{(a_{m''}, b_j+c_j)}},$$

or

$$\prod_{j<m''}\frac{g_{m''}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}}{g_{j+1}' g_j''\beta_{m'' j}^{(a_{m''} c_j)}} \stackrel{?}{=} \frac{\displaystyle\prod_{j<m''} g_{m''}' g_j''\beta_{m'' j}^{(a_{m''}+b_{m''}, c_j)}\cdot\prod_{j<m''} g_j' g_j''\beta_{m'' j}^{(a_{m''} b_j)}}{\displaystyle\prod_{j<m''} g_{m''+1}' g_j''\beta_{m'' j}^{(b_{m''} c_j)}\cdot\prod_{j<m''} g_j' g_j''\beta_{m'' j}^{(a_{m''}, b_j+c_j)}}.$$

Rearranging, we want

$$\prod_{j<m''} \frac{g_j' g_j'' \beta_{m''j}^{(a_{m''}, b_j + c_j)}}{g_j' g_j'' \beta_{m''j}^{(a_{m''} b_j)} \cdot g_{j+1}' g_j'' \beta_{m''j}^{(a_{m''} c_j)}} \stackrel{?}{=} \prod_{j<m''} \frac{g_{m''}' g_j'' \beta_{m''j}^{(a_{m''} + b_{m''}, c_j)}}{g_{m''}' g_j'' \beta_{m''j}^{(a_{m''} c_j)} \cdot g_{m''+1}' g_j'' \beta_{m''j}^{(b_{m''} c_j)}},$$

which is

$$\prod_{j<m''} g_j' g_j'' \left(\frac{\beta_{m''j}^{(a_{m''}, b_j + c_j)}}{\beta_{m''j}^{(a_{m''} b_j)} \cdot \sigma_j^{b_j} \beta_{m''j}^{(a_{m''} c_j)}} \right) \stackrel{?}{=} \prod_{j<m''} g_{m''}' g_j'' \left(\frac{\beta_{m''j}^{(a_{m''} + b_{m''}, c_j)}}{\beta_{m''j}^{(a_{m''} c_j)} \cdot \sigma_{m''}^{a_{m''}} \beta_{m''j}^{(b_{m''} c_j)}} \right).$$

However, by definition of the $\beta_{ij}^{(xy)}$, we see that

$$\frac{\beta_{m''j}^{(a_{m''}, b_j + c_j)}}{\beta_{m''j}^{(a_{m''} b_j)} \cdot \sigma_j^{b_j} \beta_{m''j}^{(a_{m''} c_j)}} = \frac{\beta_{m''j}^{(a_{m''} + b_{m''}, c_j)}}{\beta_{m''j}^{(a_{m''} c_j)} \cdot \sigma_{m''}^{a_{m''}} \beta_{m''j}^{(b_{m''} c_j)}} = 1,$$

so everything does indeed cancel out properly. This completes the check.

B Computation of $\ker \mathcal{F}$

In this section we give a proof of Lemma 137. As such, we will use all the context from the statement and proceed directly with the proof; as mentioned earlier, we may add (b) back to our list of generators because it is induced by (c). Pick up some $z := ((x_i)_i, (y_{ij})_{i>j}) \in \ker \mathcal{F}$, which is equivalent to saying

$$x_i N_i - \sum_{j=1}^{i-1} y_{ij} T_j + \sum_{j=i+1}^{m} y_{ji} T_j = 0$$

for each index i. We want to write z as a $\mathbb{Z}[G]$-linear combination of the elements from (a)–(e). The main idea will be to slowly subtract out $\mathbb{Z}[G]$-linear combinations of the above elements (which does not affect $z \in \ker \mathcal{F}$) until we can prove that we have 0 left over. We start with the x_i terms, which we do in two steps.

1. We begin by dealing with the x_i terms. Fix some index p, and we will subtract out a suitable $\mathbb{Z}[G]$-linear combination of the above generators to set $x_p = 0$ while not changing the other x_i terms. Well, using the element
$$\kappa_p T_p, \tag{a}$$
we may assume that x_p has no σ_p terms because $\sigma_p \equiv 1 \pmod{T_p}$. Then for each $q < p$, we can subtract out a suitable multiple of
$$T_q \kappa_p + N_p \lambda_{pq} \tag{c}$$
to make it so that we may assume x_p has no σ_q terms because $\sigma_q \equiv 1 \pmod{T_q}$. Similarly, for each $q > p$, we can subtract out a suitable multiple of
$$T_q \kappa_p - N_p \lambda_{pq} \tag{d}$$
to make it so that we may assume x_p has no σ_q terms because $\sigma_q \equiv 1 \pmod{T_q}$.

2. Thus, the above process allows us to assume that $x_p \in \mathbb{Z}$, and the above linear combinations have not affected any x_i for $i \neq p$. We now use the fact that $z \in \ker \mathcal{F}$. Indeed, we know that
$$x_p N_p - \sum_{j=1}^{p-1} y_{pj} T_j + \sum_{j=p+1}^{m} y_{jp} T_j = 0.$$
Applying the augmentation map $\varepsilon \colon \mathbb{Z}[G] \to \mathbb{Z}$, sending $\varepsilon \colon \sigma_i \mapsto 1$ for each index i, we see that $x_p \in \mathbb{Z}$ implying that x_p remains fixed. On the other hand $\varepsilon \colon T_j \mapsto 0$ for each index j and $\varepsilon \colon N_p \mapsto n_p$, so we are left with
$$n_p x_p = 0.$$
Because $n_p \neq 0$ (it's the order of σ_p), we conclude that $x_p = 0$. Applying this argument to the other x_i terms, we conclude that we may assume $x_i = 0$ for each i.

It remains to deal with the y_{ij} terms, which is a little more involved. For reference, we are showing that

$$-\sum_{j=1}^{i-1} y_{ij}T_j + \sum_{j=i+1}^{m} y_{ji}T_j = 0$$

for each index i implies that $z = ((0)_i, (y_{ij})_{i>j})$ is a $\mathbb{Z}[G]$-linear combination of the terms from (b) and (e).

We will now more or less proceed with the y_{ij} by induction on m, allowing the group G (in its number of generators m) to be changed in the process. For $m = 1$, there is nothing to say because there is no y_{ij} term at all. For a taste of how we will use Lemma 130, we also work out $m = 2$: our equations read

$$\underbrace{-y_{21}T_1 = 0}_{i=1} \qquad \text{and} \qquad \underbrace{y_{21}T_2 = 0}_{i=2}.$$

Thus, $y_{21} \in (\ker T_1) \cap (\ker T_2) = (\operatorname{im} N_1) \cap (\operatorname{im} N_2)$, which is $\operatorname{im} N_1N_2$ by Lemma 130.

We now proceed with the general case; take $m > 2$. Let $G' := \langle \sigma_2, \dots, \sigma_m \rangle$, which has $m-1$ generators. By the inductive hypothesis, we may assume the statement for G'. Explicitly, we will assume that, if $(y'_{ij})_{i>j\geq 2} \in \mathbb{Z}[G']^{\binom{m-1}{2}}$ are variables satisfying

$$-\sum_{j=2}^{i-1} y'_{ij}T_j + \sum_{j=i+1}^{m} y'_{ji}T_j = 0$$

for each index $i \geq 2$, then y'_{ij} are a linear combination of terms from the elements from (b) and (e) above, only using indices at least 2.

We will again proceed in steps, for clarity.

1. To apply the inductive hypothesis, we need to force $y_{pq} \in \mathbb{Z}[G']$ for each pair of indices (p, q) with $p > q \geq 2$. Well, we use the relation (e) so that we can subtract multiples of

   $$T_q\lambda_{p1} - T_1\lambda_{pq} - T_p\lambda_{q1}.$$

   In particular, this element will subtract out T_1 from y_{pq} while only introducing chaos to the elements y_{p1} and y_{q1} in the process. Thus, subtracting a suitable multiple allows us to assume that y_{pq} has no σ_1 terms while not affecting any other y_{ij} with $i > j \geq 2$.

   Applying this process to all y_{ij} with $i > j \geq 2$, we do indeed get $y_{ij} \in \mathbb{Z}[G']$ for each $i > j \geq 2$.

2. We are now ready to apply the inductive hypothesis. For each index $i \geq 2$, we have the equation

   $$-y_{i1}T_1 - \sum_{j=2}^{i-1} y_{ij}T_j + \sum_{j=i+1}^{m} y_{ji}T_j = 0.$$

   Because each y_{pq} term with $p > q \geq 2$ features no σ_1, applying the transformation $\sigma_1 \mapsto 1$ will affect no term in the sums while causing $y_{i1}T_1$ to vanish. Thus, we have the equations

   $$-\sum_{j=2}^{i-1} y_{ij}T_j + \sum_{j=i+1}^{m} y_{ji}T_j = 0$$

   for each index $i \geq 2$. Because $y_{ij} \in \mathbb{Z}[G']$ for $i > j \geq 2$ already, we see that we may apply the inductive hypothesis to assert that the y_{ij} are $\mathbb{Z}[G']$-linear combinations of terms from (b) and (e) (only using indices at least 2).

   Subtracting these linear combinations out, we may assume $y_{ij} = 0$ for each $i > j \geq 2$.

3. To take stock, our equations for $i \geq 2$ now read

   $$-y_{i1}T_1 = 0,$$

which simply tells us that $y_{i1} \in \operatorname{im} N_1$ for each $i \geq 2$. As such, we pick up $w_i \in \mathbb{Z}[G]$ so that $y_{i1} = w_i N_1$ for each $i \geq 2$; because $\sigma_1 N_1 = N_1$, we may assume that $w_i \in \mathbb{Z}[G']$ for each $i \geq 2$.

Now the equation for $i = 1$ reads

$$\sum_{j=2}^{m} y_{j1} T_j = 0,$$

or

$$\sum_{i=2}^{m} w_i N_1 T_i = 0.$$

Sending $\sigma_1 \mapsto 1$, we see that w_i and T_i are both fixed because they feature no σ_1s, so we merely have

$$n_1 \sum_{i=2}^{m} w_i T_i = 0.$$

Dividing out by n_1, we are left with

$$\sum_{i=2}^{m} w_i T_i = 0.$$

4. At this point, we may appear stuck, but we have one final trick: taking indices $p > q \geq 2$, subtracting out multiples of

$$\left(T_q \lambda_{p1} - T_1 \lambda_{pq} - T_p \lambda_{q1}\right) \cdot N_1$$

will not affect the y_{pq} term because $T_1 N_1$. Indeed, subtracting this term out looks like

$$T_q N_1 \lambda_{p1} - T_p N_1 \lambda_{q1},$$

which after factoring out N_1 takes $w_p \mapsto w_p - T_q$ and $w_q \mapsto w_q + T_p$.

In particular, fixing any $q \geq 2$ and then applying this trick for all $p > q$, we may assume that w_q does not feature any σ_p terms for $p > q$. Thus, looking at our equation

$$\sum_{i=2}^{m} w_i T_i = 0,$$

we are now able to show that $w_i \in \ker T_i = \operatorname{im} N_i$ for each $i \geq 2$, which will finish because it shows $y_{i1} \in N_i N_1$. Indeed, starting with $i = 2$, we see that w_2 features no σ_p for $p > 2$, so we may take $\sigma_p \mapsto 1$ for each $p > 2$ safely, giving the equation

$$w_2 T_2 = 0,$$

finishing for w_2. Thus, we are left with the equation

$$\sum_{i=3}^{m} w_i T_i = 0,$$

from which we see we can induct downwards (this has fewer variables) to finish.

The above steps complete the proof, as advertised.