Classifying Extensions of Abelian Groups

Nir Elber

June 9, 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 provide a group presentation of the extension using specially chosen elements of A.

Contents

1 General Group Extensions

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

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

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 $H^2(G, A)$, 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 1. 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 $\sigma := \pi(F)$. Then

$$\alpha := F^{n_\sigma}$$

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

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

be the corresponding extension. Fixing $\sigma \in G$ of order n_σ, let $F := (m, \sigma) \in \mathcal{E}$ be a lift. Then

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

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

Proof. This is a direct computation. By induction, we have 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 3. 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 $A_\sigma := A^{\langle\sigma\rangle}$ be the fixed submodule. Then the set

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

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

Proof. Note that $S_{\mathcal{E},\sigma} \subseteq A_\sigma$ already from Lemma 1.

The point is to use Lemma 2. 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 $\varphi\colon \mathcal{E} \simeq \mathcal{E}_c$ making the following diagram commute.

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, equal] & \mathcal{E} \arrow[r, "\pi"] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & A \arrow[r] & \mathcal{E}_c \arrow[r, "\pi_c"] & G \arrow[r] & 1
\end{tikzcd}$$

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 2 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 $A_\sigma^\times/N_\sigma(A)$ is reminiscent of the (inverse) Artin reciprocity map, and indeed that is exactly what is going on.

Corollary 4. Work in the context of Proposition 3. Then

$$S_\sigma := S_{\mathcal{E},\sigma} = [\sigma] \cup [c],$$

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

Proof. Using notation as in the proof of Proposition 3, we recall that $S_\sigma = S_{\mathcal{E}_c,\sigma}$, so it suffices to prove the result for $\mathcal{E}_c$. Well, by Lemma 2, S_σ is represented by

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

However, this product is exactly the cup product $[\sigma] \cup [c]$. ■

Corollary 5. Let L/K be a finite Galois extension of local fields with Galois group $G := \operatorname{Gal}(L/K)$. 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 $L_\sigma := L^{\langle\sigma\rangle}$ be the fixed field. Then

$$\theta_{L/L_\sigma}^{-1}(\sigma) = \{F^{n_\sigma} : \pi(F) = \sigma\}.$$

Proof. Recalling θ_{L/L_σ}^{-1} is a cup product map, note that $\theta_{L/L_\sigma}^{-1}(\sigma)$ is given by $[\sigma] \cup u_{L/K}$. So we are done by Corollary 4. ∎

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 6. 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 $\{\sigma_i\}_{i=1}^m$ which generate G, then $\mathcal{E}$ is generated by A and a set of lifts $\{F_i\}_{i=1}^m$ with $\pi(F_i) = \sigma_i$ for each i.

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

$$\pi(e) = \prod_{i=1}^m \sigma_i^{a_i}$$

for some sequence of integers $\{a_i\}_{i=1}^m$. It follows that

$$\pi\left(\frac{e}{\prod_{i=1}^m F_i^{a_i}}\right) = 1,$$

so $\frac{e}{\prod_{i=1}^m F_i^{a_i}} = \ker \pi = A$. Thus, we can find some $x \in A$ such that

$$e = x \cdot \prod_{i=1}^m F_i^{a_i},$$

which is what we wanted. ∎

2 Abelian Group Extensions

2.1 Extensions to Tuples

The above proofs technically don't even require that the group G is abelian. 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 7. 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 $\sigma_i := \pi(F_i)$ for $i \in \{1,2\}$, and let $\sigma_i \in G$ have order n_i. Then, setting

$$\alpha_i := F_i^{n_i} \qquad \text{and} \qquad \beta := F_1 F_2 F_1^{-1} F_2^{-1},$$

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 $N_i := \sum_{p=0}^{n_i-1} \sigma_i^p$.

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

(a) That $\alpha_i \in A_i$ follows from Lemma 1. 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 $\beta^{-1} = F_2 F_1 F_2^{-1} F_1^{-1}$. Well, we compute

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

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 8. Fix everything as in Lemma 7. 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

$$\begin{aligned}
F_1F_2^{y+1} &= F_1F_2^y \cdot F_2 \\
&= \prod_{\ell=0}^{y-1} \sigma_2^\ell(\beta) F_2^y F_1 \cdot F_2 \\
&= \prod_{\ell=0}^{y-1} \sigma_2^\ell(\beta) F_2^y \beta F_2 F_1 \\
&= \prod_{\ell=0}^{y-1} \sigma_2^\ell(\beta) \cdot \sigma_2^y(\beta) F_2^y \cdot F_2F_1 \\
&= \prod_{\ell=0}^{(y+1)-1} \sigma_2^\ell(\beta) \cdot F_2^{y+1}F_1,
\end{aligned}$$

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

$$\begin{aligned}
F_1^{x+1}F_2^{y+1} &= F_1 \cdot F_1^x F_2^{y+1} \\
&= F_1 \cdot \prod_{k=0}^{x-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k\sigma_2^\ell(\beta) \cdot F_2^{y+1}F_1^x \\
&= \sigma_1\left(\prod_{k=0}^{x-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k\sigma_2^\ell(\beta)\right) \cdot F_1F_2^{y+1}F_1^x \\
&= \prod_{k=1}^{(x+1)-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k\sigma_2^\ell(\beta) \cdot F_1F_2^{y+1}F_1^x \\
&= \prod_{k=1}^{(x+1)-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k\sigma_2^\ell(\beta) \cdot \prod_{\ell=0}^{(y+1)-1} \sigma_2^\ell(\beta) \cdot \sigma_2^y(\beta) \cdot F_2^{y+1}F_1 \cdot F_1^x \\
&= \prod_{k=0}^{(x+1)-1} \prod_{\ell=0}^{(y+1)-1} \sigma_1^k\sigma_2^\ell(\beta) F_2^{y+1}F_1^{x+1},
\end{aligned}$$

which is what we wanted. ■

Remark 9. 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 9 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 10. 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 $\sigma_i := \pi(F_i)$ for $i \in \{1, 2, 3\}$, and let $\sigma_i \in G$ have order n_i. Then, setting

$$\beta_{ij} := F_i F_j F_i^{-1} F_j^{-1}$$

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 11. The relation from Lemma 10 may look asymmetric in the β_{ij}, but this is because the definitions of the β_{ij}s themselves are asymmetric in F_i.

2.2 Tuples to Cocycles

2.2.1 The Set-Up

The proceeding lemma 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 6 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

$$\alpha_i := F_i^{n_i}$$

for each index i and

$$\beta_{ij} := F_i F_j F_i^{-1} F_j^{-1}$$

for each index $1 \leq j < i \leq m$. Notably, we will not need more βs: indeed, $\beta_{ii} = 1$ and $\beta_{ij} = \beta_{ji}^{-1}$ for any i and j. Setting $A_i := A^{\langle \sigma_i \rangle}$ and $N_i := \sum_{p=0}^{n_i-1} \sigma_i^p$, the story so far is that

$$\alpha_i \in A_i \text{ for each } i \qquad \text{and} \qquad \beta_{ij} \in A \text{ for each } i > j \tag{2.1}$$

and

$$N_i(\beta_{ij}) = \alpha_i/\sigma_j(\alpha_i) \qquad \text{and} \qquad N_j(\beta_{ij}^{-1}) = \alpha_j/\sigma_i(\alpha_j) \qquad \text{for each } i > j \tag{2.2}$$

by Lemma 7, and

$$\frac{\sigma_j(\beta_{ik})}{\beta_{ik}} = \frac{\sigma_k(\beta_{ij})}{\beta_{ij}} \cdot \frac{\sigma_i(\beta_{jk})}{\beta_{jk}} \qquad \text{for each } i > j > k \tag{2.3}$$

by Lemma 10. This data is so important that we will give it a name.

Definition 12. In the above set-up, the data of $(\{\alpha_i\}, \{\beta_{ij}\})$ satisfying (2.1) and (2.2) and (2.3) will be called a $\{\sigma_i\}_{i=1}^m$*-tuple*. When understood, the $\{\sigma_i\}_{i=1}^m$ will be abbreviated.

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 13. The set of $\{\sigma_i\}_{i=1}^m$-tuples form a group under multiplication in A. Indeed, the conditions (2.1) and (2.2) and (2.3) are closed under multiplication and inversion.

We also know from Lemma 8 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

$$\beta_{ij}^{(k\ell)} := \prod_{k=0}^{x-1} \prod_{\ell=0}^{y-1} \sigma_i^k \sigma_j^\ell(\beta_{ij}).$$

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 14. 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

$$\left(\prod_{i=1}^m F_i^{a_i}\right)\left(\prod_{i=1}^m F_i^{b_i}\right) = \left[\prod_{1 \leq j < i \leq m} \left(\prod_{1 \leq k < j} \sigma_k^{a_k + b_k}\right)\left(\prod_{j \leq k < i} \sigma_k^{a_k}\right) \beta_{ij}^{(a_i b_j)}\right]\left(\prod_{i=1}^m F_i^{a_i + b_i}\right).$$

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

$$\left(\prod_{i=1}^m F_i^{a_i}\right) F_1^{b_1} = \left[\prod_{1 < i \leq m} \left(\prod_{1 \leq k < i} \sigma_k^{a_k}\right) \beta_{i1}^{(a_i b_1)}\right] F_1^{a_1 + b_1} \prod_{i=2}^m F_i^{a_i}.$$

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

$$\left(\prod_{i=1}^{m} F_i^{a_i}\right) F_1^{b_1} = \left[\prod_{1<i\le m} \left(\prod_{1\le k<i} \sigma_k^{a_k}\right) \beta_{i1}^{(a_i b_1)}\right] F_1^{a_1+b_1} \prod_{i=2}^{m} F_i^{a_i}$$

and compute

$$\begin{aligned}
\left(\prod_{i=1}^{m+1} F_i^{a_i}\right) F_1^{b_1} &= \left(\prod_{i=1}^{m} F_i^{a_i}\right) F_{m+1}^{a_{m+1}} F_1^{b_1} \\
&= \left(\prod_{i=1}^{m} F_i^{a_i}\right) \beta_{m+1,1}^{(a_{m+1}b_1)} F_1^{b_1} F_{m+1}^{a_{m+1}} \\
&= \left[\left(\prod_{k=1}^{m} \sigma_k^{a_k}\right) \beta_{m+1,1}^{(a_{m+1}b_1)}\right] \left[\prod_{1<i\le m} \left(\prod_{1\le k<i} \sigma_k^{a_k}\right) \beta_{i1}^{(a_i b_1)}\right] F_1^{a_1+b_1} \left(\prod_{i=2}^{m} F_i^{a_i}\right) F_{m+1}^{a_{m+1}} \\
&= \left[\prod_{1<i\le m+1} \left(\prod_{1\le k<i} \sigma_k^{a_k}\right) \beta_{i1}^{(a_i b_1)}\right] F_1^{a_1+b_1} \left(\prod_{i=2}^{m+1} F_i^{a_i}\right),
\end{aligned}$$

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

$$\left(\prod_{i=2}^{m} F_i^{a_i}\right) \left(\prod_{i=2}^{m} F_i^{b_i}\right) = \left[\prod_{2\le j<i\le m} \left(\prod_{2\le k<j} \sigma_k^{a_k+b_k}\right) \left(\prod_{j\le k<i} \sigma_k^{a_k}\right) \beta_{ij}^{(a_i b_j)}\right] \left(\prod_{i=2}^{m} F_i^{a_i+b_i}\right).$$

From here, we can compute

$$\begin{aligned}
\left(\prod_{i=1}^{m} F_i^{a_i}\right) \left(\prod_{i=1}^{m} F_i^{b_i}\right) &= \left(\prod_{i=1}^{m} F_i^{a_i}\right) F_1^{b_1} \left(\prod_{i=2}^{m} F_i^{b_i}\right) \\
&= \left[\prod_{1<i\le m} \left(\prod_{1\le k<i} \sigma_k^{a_k}\right) \beta_{i1}^{(a_i b_1)}\right] F_1^{a_1+b_1} \left(\prod_{i=2}^{m} F_i^{a_i}\right) \left(\prod_{i=2}^{m} F_i^{b_i}\right) \\
&= \left[\prod_{1<i\le m} \left(\prod_{1\le k<i} \sigma_k^{a_k}\right) \beta_{i1}^{(a_i b_1)}\right] F_1^{a_1+b_1} \cdot \\
&\qquad \left[\prod_{2\le j<i\le m} \left(\prod_{2\le k<j} \sigma_k^{a_k+b_k}\right) \left(\prod_{j\le k<i} \sigma_k^{a_k}\right) \beta_{ij}^{(a_i b_j)}\right] \left(\prod_{i=2}^{m} F_i^{a_i+b_i}\right) \\
&= \left[\prod_{1<i\le m} \left(\prod_{1\le k<i} \sigma_k^{a_k}\right) \beta_{i1}^{(a_i b_1)}\right] \cdot \\
&\qquad \sigma_1^{a_1+b_1} \left[\prod_{2\le j<i\le m} \left(\prod_{2\le k<j} \sigma_k^{a_k+b_k}\right) \left(\prod_{j\le k<i} \sigma_k^{a_k}\right) \beta_{ij}^{(a_i b_j)}\right] \left(\prod_{i=2}^{m} F_i^{a_i+b_i}\right).
\end{aligned}$$

From here, a little rearrangement finishes the inductive step. ■

The reason we exerted this pain upon ourselves is for the following result.

Proposition 15. Fix everything as in the set-up. Then, if well-defined, we can represent the cohomology class corresponding to $\mathcal{E}$ by the cocycle

$$c(g,h) := \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}^{(a_ib_j)}\right]\left[\prod_{i=1}^m\left(\prod_{1\le k<i}\sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right],$$

where $g = \prod_i \sigma_i^{a_i}$ and $h = \prod_i \sigma_i^{b_i}$.

Observe that Proposition 15 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 $q_\in \{0,1\}$ 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

$$\begin{aligned}
c(g,h) &= s(g)s(h)s(gh)^{-1} \\
&= \left(\prod_{i=1}^m F_i^{a_i}\right)\left(\prod_{i=1}^m F_i^{b_i}\right)\left(\prod_{i=1}^m F_i^{r_i}\right)^{-1} \\
&= \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}^{(a_ib_j)}\right]\left(\prod_{i=1}^m F_i^{a_i+b_i}\right)\left(\prod_{i=1}^m F_{m-i+1}^{-r_{m-i+1}}\right).
\end{aligned}$$

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. ■

2.2.2 The Modified Set-Up

A priori we have no reason to expect that the c constructed in Proposition 15 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 16. 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

$$c(g,h) := \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}^{(a_ib_j)}\right]\left[\prod_{i=1}^{m}\left(\prod_{1\le k<i}\sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right],$$

where $g := \prod_i \sigma_i^{a_i}$ with $h := \prod_i \sigma_j^{a_j}$ 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 section 3, 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.

2.3 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 17. 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 2. For the equality about β_{ij}, we simply compute by brute force, writing

$$\begin{aligned} F_iF_j &= (x_i\cdot\sigma_ix_j\cdot c(\sigma_i,\sigma_j),\sigma_i\sigma_j) \\ F_jF_i &= (x_j\cdot\sigma_jx_i\cdot c(\sigma_j,\sigma_i),\sigma_j\sigma_i) \\ (F_jF_i)^{-1} &= \left((\sigma_j\sigma_i)^{-1}(x_j\cdot\sigma_jx_i\cdot c(\sigma_j,\sigma_i))^{-1},\sigma_i^{-1}\sigma_j^{-1}\right), \end{aligned}$$

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 18. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. For 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 16, we may build the cocycle $c \in Z^2(G, A)$ defined by

$$c(g,h) := \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}^{(a_ib_j)}\right]\left[\prod_{i=1}^{m}\left(\prod_{1\le k<i}\sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right], \tag{2.4}$$

where $g := \prod_i F_i^{a_i}$ and $h := \prod_i F_j^{a_j}$ and $0 \le a_i, b_i < n_i$. As such, we use $\mathcal{E} := \mathcal{E}_c$ to be the corresponding extension and $F_i := (1, \sigma_i)$ as our lifts. We have the following checks.

- To show $\alpha_i = F_i^{n_i}$, we use Lemma 17 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 (2.4), we note that all $\beta_{k\ell}^{(a_kb_\ell)}$ terms vanish (either $a_k = 0$ or $b_\ell = 0$ for each $k \ne \ell$), so the big left product completely vanishes.

  As for the right product, the only term we have to worry about is

  $$\left(\prod_{1\le k<i}\sigma_k^{0+0}\right)\alpha_i^{\left\lfloor\frac{k+1}{n_i}\right\rfloor},$$

  which is equal to 1 when $k \le n_i - 1$ and α_i when $k = n_i - 1$. As such, we do indeed have $\alpha_i = F_i^{n_i}$.
- To show $\beta_{ij} = F_iF_jF_i^{-1}F_j^{-1}$ for $i > j$, we again use Lemma 17 to compute $F_iF_jF_i^{-1}F_j^{-1}$, which means we want to compute

  $$\frac{c(\sigma_i,\sigma_j)}{c(\sigma_j,\sigma_i)}.$$

  Plugging into (2.4) 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

  $$\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}.$$

  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 19. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Then the formula of Theorem 16 and the formulae of Lemma 17 (setting $x_i = 1$ for each i) are homomorphisms of abelian groups between the set of $\{\sigma_i\}_{i=1}^m$-tuples and cocycles in $Z^2(G, A)$. In fact, the formula of Theorem 16 is a section of the formulae of Lemma 17.

Proof. The formulae in Theorem 16 and Lemma 17 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 16, the proof of Corollary 18 shows that the formulae of Lemma 17 recovers the correct $\{\sigma_i\}_{i=1}^m$-tuple. ■

2.4 Equivalence Classes of Tuples

We continue in the modified set-up. We would like to make Corollary 19 into a proper isomorphism of abelian groups, but this is not feasible; for example, the cocycle c generated by Theorem 16 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 16 is surjective on these equivalence classes. The correct equivalence relation is taken from Lemma 17.

Definition 20. 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 $x_1, \ldots, x_m \in A$ such 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}. We may notate this by $(\{\alpha_i\}, \{\beta_{ij}\}) \sim (\{\alpha_i'\}, \{\beta_{ij}'\})$.

This notion of equivalence can be seen to be the correct one in the sense that it correctly generalizes Proposition 3.

Proposition 21. Fix everything as in the modified set-up with an extension $\mathcal{E}$. As the lifts F_i change, the corresponding values of

$$\alpha_i := F_i^{n_i} \qquad \text{and} \qquad \beta_{ij} := F_i F_j F_i^{-1} F_j^{-1}$$

go through a full equivalence class of $\{\sigma_i\}_{i=1}^m$-tuples.

Proof. We proceed as in Proposition 3. 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 $\varphi\colon \mathcal{E} \simeq \mathcal{E}'$ 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.

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, equal] & \mathcal{E} \arrow[r, "\pi"] \arrow[d, "\varphi"] & G \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & A \arrow[r] & \mathcal{E}' \arrow[r, "\pi'"] & G \arrow[r] & 1
\end{tikzcd}$$

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

$$\alpha_i := F_i^{n_i} \qquad \text{and} \qquad \beta_{ij} := F_i F_j F_i^{-1} F_j^{-1}.$$

Now, we note that $F_i' := \varphi(F_i)$ 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 $\mathcal{E} := \mathcal{E}_c$. Indeed, as the lifts $F_i = (x_i, \sigma_i)$ change, we know by Lemma 17 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 22. 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 $\{\sigma_i\}_{i=1}^m$ which correspond to $[c]$ (via Theorem 16) forms exactly one equivalence class.

Proof. We show that two tuples are equivalent if and only if their corresponding cocycles (via Theorem 16) to the same cohomology class, which will be enough.

In one direction, suppose $(\{\alpha_i\}, \{\beta_{ij}\}) \sim (\{\alpha_i'\}, \{\beta_{ij}'\})$. By Corollary 18, we can find an extension $\mathcal{E}$ which gives $(\{\alpha_i\}, \{\beta_{ij}\})$ by choosing an appropriate set of lifts. By Proposition 21, 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 16 from our two tuples now both represent the isomorphism class of $\mathcal{E}$ by Proposition 15, 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 $\mathcal{E}_c \simeq \mathcal{E}_{c'}$ as extensions, but we know by the proof of Corollary 18 that $(\{\alpha_i\}, \{\beta_{ij}\})$ comes from choosing lifts of $\mathcal{E}_c$ and similar for $(\{\alpha_i'\}, \{\beta_{ij}'\})$. In particular, because $\mathcal{E}_c \simeq \mathcal{E}_{c'}$, we know that $(\{\alpha_i'\}, \{\beta_{ij}'\})$ will also come from choosing some lifts in $\mathcal{E}_c$ (recall the proof of Proposition 21), so $(\{\alpha_i\}, \{\beta_{ij}\}) \sim (\{\alpha_i'\}, \{\beta_{ij}'\})$ follows. ■

Theorem 23. The maps described in Corollary 19 descend to an isomorphism of abelian groups between the equivalence classes of $\{\sigma_i\}_{i=1}^m$-tuples 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 22. 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. ■

2.5 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 16, properly corresponding to the original extension by Proposition 15.

In fact, the cocycle in Proposition 15 is generated by the description of the group law in Proposition 14, 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 24. Fix everything as in the modified set-up, forgetting about the extension $\mathcal{E}$. Given a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$, 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 14 and Proposition 15 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 16.

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 23. 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. ■

3 Studying Tuples

The story so far has been able to generalize the one-variable results from section 1 to results using all generators of an abelian group in section 2. It remains to prove Theorem 16, which is the main goal of this section.

3.1 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_k. These variables allow us to define

$$T_i := (\sigma_i - 1) \qquad \text{and} \qquad N_i := \sum_{p=0}^{n_i - 1} \sigma_i^p$$

for each index i. In fact, it will be helpful to also have notation

$$\sigma^{(a)} := \sum_{p=0}^{a-1} \sigma^p$$

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

$$g_i := \prod_{p=1}^{i-1} \sigma_p^{a_p}$$

for $i \geq 0$. In particular $g_0 = g_1 = 1$ and $g_{n+1} = g$.

Now, our tool in the proof of Theorem 16 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 25. Fix everything as in the set-up. Then the function

$$\overline{c}(g) := \left(g_i \sigma_i^{(a_i)} \right)_{i=1}^m ,$$

where $g := \prod_{i=1}^m \sigma_i^{a_i}$, 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

$$0 \to \underbrace{\frac{\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}}{\ker \mathcal{F}}}_{X :=} \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0,$$

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 25.

Only now will we bring in tuples. The first result provides an alternate description of tuples.

Proposition 26. 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 27. Fix everything as in the set-up. Further, fix a G-module A and a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$. Then observe there is a natural cup product map

$$\cup\colon H^2(G, X) \times H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \to H^2(G, A)$$

by using the evaluation map $X \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}}(X, A) \to A$. Then, using the isomorphism of Proposition 26, the cocycle defined in Theorem 16 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 16 is in fact well-defined.

3.2 Classification of 1-Cocycles

We continue in the set-up of the previous subsection. The goal of this subsection is to prove Proposition 25. In fact, we will show the following stronger result.

Proposition 28. Fix everything as in the set-up. Then $H^1(G, \operatorname{coker} \mathcal{F})$ is cyclic generated by the class $[\overline{c}]$ represented by $\overline{c}$, where

$$\overline{c}(g) := \left(g_i \sigma_i^{(a_i)}\right)_{i=1}^m,$$

with $g := \prod_{i=1}^m \sigma_i^{a_i}$

Before jumping into the proof, 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

$$\kappa_p := \big((1_{i=p})_i, (0)_{i>j}\big) \in X \qquad \text{and} \qquad \lambda_{pq} := \big((0)_i, (1_{(i,j)=(p,q)})_{i>j}\big)$$

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

$$\varepsilon_p := (1_{i=p})_{i=1}^m$$

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

$$\mathcal{F}\left(\sum_{i=1}^m x_i \kappa_i + \sum_{i>j} y_{ij} \lambda_{ij}\right) = \sum_{i=1}^m x_i N_i \varepsilon_i + \sum_{i>j} y_{ij}(T_i \varepsilon_j - T_j \varepsilon_i), \tag{3.1}$$

and

$$\overline{c}(g) = \sum_{i=1}^m g_i \sigma_i^{(a_i)} \varepsilon_i$$

where $g := \prod_{i=1}^m \sigma_i^{a_i}$.

Additionally, so that we do not need to interrupt our discussion later, we establish a few lemmas which will aide our proof of Proposition 28.

Lemma 29. Fix everything as in the set-up. Then, for any set of distinct indices $(i_1, \ldots, i_k)$, 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_j "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

$$z := \sum_{(a_i)_i} c_{(a_i)_i}\sigma_1^{a_1}\cdots\sigma_m^{a_m} \in \bigcap_{p=1}^k \operatorname{im} N_{i_p},$$

the sum is over sequences $(a_i)_{i=1}^m$ such that $0 \le a_i < n_i$ 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 $r \in \{p,q\}$ 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 30. Fix everything as in the set-up. Then, given $g := \prod_{i=1}^m \sigma_i^{a_i}$, we have

$$g_i = 1 + \sum_{p=1}^{i-1} g_p\sigma_p^{(a_p)}T_p$$

for $i \ge 1$.

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. ■

Lemma 31. 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

$$\rho(g\varepsilon_i) := g_i\big(\sigma_i^{a_i} - N_i 1_{a_i = n_i - 1}\big)\varepsilon_i + \sum_{j=i+1}^{m} g_j \sigma_j^{(a_j)} T_i \varepsilon_j,$$

where $g := \prod_{i=1}^m \sigma_i^{a_i}$ with $0 \le a_i < n_i$. Then ρ descends to a map $\overline{\rho}\colon \operatorname{coker} \mathcal{F} \to \mathbb{Z}[G]^m$ witnessing the splitting of the short exact sequence

$$0 \to X \to \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0$$

over $\mathbb{Z}$.

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 (3.1) 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 relevant indices i and j. Thus, $\operatorname{im} \mathcal{F}$ is generated over $\mathbb{Z}$ by the elements $gN_i\varepsilon_i$ and $gT_i\varepsilon_j - gT_j\varepsilon_i$ for relevant indices i and j. Thus, we fix any $g := \prod_{i=1}^n \sigma_i^{a_i}$ and show that $gN_i\varepsilon_i \in \ker \rho$ and $gT_i\varepsilon_j - gT_j\varepsilon_i \in \ker \rho$ for relevant indices i and j.

- We show $gN_i\varepsilon_i \in \ker \rho$ for any i. Because $gN_i = g\sigma_i N_i$, we may as well as assume that $a_i = 0$. Then

  $$\rho\left(g\sigma_i^a \varepsilon_i\right) = g_i\big(\sigma_i^a - N_i 1_{a = n_i - 1}\big)\varepsilon_i + \sum_{j=i+1}^{m} g_j \sigma_i^a \sigma_j^{(a_j)} T_i \varepsilon_j.$$

  As a varies from 0 to $n_i - 1$, we note that the term $g_i\big(\sigma_i^a - N_i 1_{a=n_i-1}\big)\varepsilon_i$ 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 $T_i \sum_{a=0}^{n_i-1} \sigma_i^a = T_i N_i = 0$. 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

$$\begin{aligned}\rho(g\sigma_p\varepsilon_q) = g_q\big(&\sigma_q^{a_q} - N_i 1_{a_q=n_q-1}\big)\varepsilon_q \\ &+ \sum_{j=q+1}^{p-1} g_j\sigma_j^{(a_j)}T_q\varepsilon_j \\ &+ g_p\left(\sigma_p^{(a_p+1)} - N_p 1_{a_p=n_p-1}\right)T_q\varepsilon_p \\ &+ \sum_{j=p+1}^{m} \sigma_p g_j\sigma_j^{(a_j)}T_q\varepsilon_j\end{aligned}$$

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

$$\rho(g\sigma_q\varepsilon_p) = \sigma_q g_p\big(\sigma_p^{a_p} - N_p 1_{a_p=n_p-1}\big)\varepsilon_p + \sum_{j=p+1}^{m} \sigma_q g_j\sigma_j^{(a_j)}T_p\varepsilon_j$$

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 30, we write

$$\begin{aligned}g\varepsilon_i &= g_i\sigma_i^{a_i}\left(\prod_{j=i+1}^{m}\sigma_j^{a_j}\right)\varepsilon_i \\ &= g_i\sigma_i^{a_i}\left(1 + \sum_{j=i+1}^{m}\left(\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)\sigma_j^{(a_j)}T_j\right)\varepsilon_i \\ &= g_i\sigma_i^{a_i}\varepsilon_i + \sum_{j=i+1}^{m} g_i\sigma_i^{a_i}\left(\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)\sigma_j^{(a_j)}T_j\varepsilon_i \\ &\equiv g_i\sigma_i^{a_i}\varepsilon_i + \sum_{j=i+1}^{m} g_j\sigma_j^{(a_j)}T_i\varepsilon_j,\end{aligned}$$

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 $\rho(g\varepsilon_i)$. ∎

Remark 32. The purpose of Lemma 31 is to give an injective map from $\operatorname{coker}\mathcal{F}$ to a more controlled setting. In particular, it is somewhat annoying to check if an element $z \in \mathbb{Z}[G]^m$ lives in $\operatorname{im}\mathcal{F}$, but it is easier to check the equivalent condition $\overline{\rho}(z) = 0$.

We are now ready to more directly attack the proof of Proposition 28. We begin by reducing the amount of data we have to carry around in a cocycle.

Lemma 33. Fix everything as in the set-up, and let A be a G-module. Then, if $f \in Z^1(G, A)$ is a cocycle, then

$$f(g) = \sum_{i=1}^m g_i \sigma_i^{(a_i)} f(\sigma_i),$$

where $g := \prod_{i=1}^m \sigma_i^{a_i}$ with $a_i \geq 0$.

Proof. Unsurprisingly, this is by induction. To begin, we claim that

$$f\left(\sigma^a\right) = \sigma^{(a)} f(\sigma)$$

by induction on a. When $a = 0$, we are showing that $f(1) = 0$, for which we note that the 1-cocycle condition implies $f(1) = f(1) + f(1)$ and so $f(1) = 0$. Then for the inductive step, we assume $f(\sigma^a) = \sigma^{(a)} f(\sigma)$ and note

$$f\left(\sigma^{a+1}\right) = \sigma f\left(\sigma^a\right) + f(\sigma) = \left(1 + \sigma\sigma^{(a)}\right) f(\sigma) = \sigma^{(a+1)} f(\sigma),$$

finishing.

We now show the original statement by an induction on m. For $m = 0$, this is asserting $f(1) = 0$, which is true. Then for the inductive step, we assume for $m - 1$ and note that $m > 1$ has

$$f\left(g_m \sigma_m^{a_m}\right) = f(g_m) + g_m f\left(\sigma_m^{a_m}\right) = \sum_{i=1}^{m-1} g_i \sigma_i^{(a_i)} f(\sigma_i) + g_m \sigma_m^{(a_m)} f(\sigma_m),$$

which is what we wanted. ■

Thus, to build a 1-cocycle, we only have to specify $f(\sigma_i)$ for indices i and then check the 1-cocycle condition to make sure we are okay.

As such, we now run through what the 1-cocycle check requires.

Lemma 34. Fix everything as in the set-up. Further, fix some $z \in \mathbb{Z}[G]^m$. Then $N_i z \in \operatorname{im}\mathcal{F}$ if and only if $[z] \in \operatorname{coker}\mathcal{F}$ has a representative of the form $a_i \varepsilon_i \in \mathbb{Z}[G]^m$ where $a_i \in \mathbb{Z}[G]$.

Proof. In one direction, if $z \equiv a_i \varepsilon_i \pmod{\operatorname{im}\mathcal{F}}$, then

$$N_i z \equiv a_i \cdot N_i \varepsilon_i \equiv a_i \cdot 0 \equiv 0 \pmod{\operatorname{im}\mathcal{F}}$$

because $N_i \varepsilon_i \in \operatorname{im}\mathcal{F}$.

In the other direction, we pass through $\overline{\rho}$ of Lemma 31. By possibly rearranging our σs, we may set $i = 1$. As such, suppose $N_1 z \in \operatorname{im}\mathcal{F}$, and write

$$z := \sum_{i=1}^m z_i \varepsilon_i$$

where $z_i \in \mathbb{Z}[G]$. By using the fact that $T_i \varepsilon_1 \equiv T_1 \varepsilon_i \pmod{\operatorname{im}\mathcal{F}}$ for any index i, we can find a representative for z in $\mathbb{Z}[G]^m$ such that z_i has no σ_1 powers for each $i > 1$; without loss of generality, replace z with this representative.

We thus claim that $w := z - z_1\varepsilon_1 \in \operatorname{im}\mathcal{F}$, which means that z is represented by $z_1\varepsilon_1$; to show this, we already know that $N_1 w = N_1(z - z_1\varepsilon_1) \in \operatorname{im}\mathcal{F}$, so we pass through $\overline{\rho}$. In other words, it suffices to show that $\rho(w) = 0$ from $\rho(N_1 w) = 0$ and the fact that w features no σ_1 nor ε_1 terms.

Well, because w features no σ_1 nor ε_1 terms, the only terms we care about have $g\varepsilon_i$ where g has no σ_1 and $i > 1$; in this case,

$$\rho\left(g\sigma_1^a\varepsilon_i\right) := \sigma_1^a g_i\left(\sigma_i^{a_i} - N_i 1_{a_i = n_i - 1}\right)\varepsilon_i + \sum_{j=i+1}^{m} \sigma_1^a g_j \sigma_j^{(a_j)} T_i \varepsilon_j = \sigma_1^a \rho(g\varepsilon_i),$$

where $g := \prod_{i=2}^m \sigma_i^{a_i}$ with $0 \le a_i < n_i$. Looping over all possible g and ε_i, we see $\rho(\sigma_1^a w) = \sigma_1^a \rho(w)$, so

$$N_1\rho(w) = \rho(N_1 w) = 0.$$

Thus, $\rho(w) \in \operatorname{im} T_1$, so say $\rho(w) = (\sigma_1 - 1)w'$. However, because w has no ε_1 terms nor any term with a σ_1, we can see from the expansion of $\rho(w)$ that $\rho(w)$ will have no σ_1 terms. It follows that $\rho(w) \in \mathbb{Z}[G]^m$ is preserved upon applying $\sigma_1 \mapsto 1$, but then $(\sigma_1 - 1)w'$ gets sent to 0, so it follows $\rho(w) = 0$. This finishes. ■

Lemma 35. Fix everything as in the set-up. Suppose we have $\{z_i\}_{i=1}^m \subseteq \mathbb{Z}[G]$ such that

$$T_i z_j \varepsilon_j = T_j z_i \varepsilon_i$$

in $\operatorname{coker}\mathcal{F}$, for any pair of indices (i, j). Then there exists $z \in \mathbb{Z}[G]$ such that $z\varepsilon_i = z\varepsilon_i$ (in $\operatorname{coker}\mathcal{F}$) for each index i.

Proof. We proceed by induction on m. For $m = 1$, we simply set $z := z_1$. For the inductive step, take $m > 1$, and we are given elements $\{z_i\}_{i=1}^m \subseteq \mathbb{Z}[G]$ such that

$$T_i z_j \varepsilon_j = T_j z_i \varepsilon_i$$

for any pair of indices (i, j). By the inductive hypothesis, we may use the equations with indices less than m to conjure some $z \in \mathbb{Z}[G]$ such that

$$z\varepsilon_i \equiv z_i\varepsilon_i \pmod{\operatorname{im}\mathcal{F}}$$

for each $i < m$. It remains to deal with the equations which have m as an index; namely, for each $i < m$, we have an equation

$$T_i z_m \varepsilon_m \equiv T_m z_i \varepsilon_i \equiv T_m z \varepsilon_i \pmod{\operatorname{im}\mathcal{F}}.$$

Now, $T_m\varepsilon_i \equiv T_i\varepsilon_m \pmod{\operatorname{im}\mathcal{F}}$, so this is equivalent to asserting

$$T_i(z_m - z)\varepsilon_m \equiv 0 \pmod{\operatorname{im}\mathcal{F}}$$

for each index $i < m$. Thus, $T_i(z_m - z)\varepsilon_m \in \operatorname{im}\mathcal{F}$ for each i, which we will use by passing through the ρ of Lemma 31: this is equivalent to $\rho(T_i(z_m - z)\varepsilon_m) = 0$ for each $i < m$. Now, we note that any $g = \prod_{j=1}^m \sigma_j^{a_j}\sigma \in G$ and $i < m$ will have

$$\rho(\sigma_i g\varepsilon_m) = \sigma_i g_m\left(\sigma_m^{a_m} - N_i 1_{a_m = n_m - 1}\right)\varepsilon_m = \sigma_i \rho(g\varepsilon_m),$$

where in particular the sum in ρ vanished because m is the largest index. (Also, we note $(\sigma_i g)_m = \sigma_i g_m$ because $i < m$.) Extending this linearly over all $g \in G$, we see that

$$0 = \rho(T_i(z_m - z)\varepsilon_m) = T_i\rho((z_m - z)\varepsilon_m)$$

for each $i < m$. In particular, letting $\rho((z_m - z)\varepsilon_m) = r\varepsilon_m$, we see$r \in \operatorname{im} N_i$ for each $i < m$, so it follows from Lemma 29 that $r \in \operatorname{im} N_1 \cdots N_{m-1}$, so we can find $w \in \mathbb{Z}[G]$ such that

$$\rho((z_m - z)\varepsilon_m) = N_1 \cdots N_{m-1} w\varepsilon_m.$$

Now, for technical reasons we note that any $g = \prod_{j=1}^m \sigma_j^{a_j}$ gives

$$\rho(g\varepsilon_m) = g_m\big(\sigma_m^{a_m} - N_i 1_{a_m = n_m - 1}\big)\varepsilon_m,$$

which can have no $\sigma_m^{n_m-1}$ term in it because this would have to come from $\big(\sigma_m^{a_m} - N_i 1_{a_m=n_m-1}\big)$, which manually kills all such terms. As such, $N_1 \cdots N_{m-1} w$ should have no $\sigma_m^{n_m-1}$ terms, which means w itself should have no such terms.

With this in mind, we set $z' := z + N_1 \cdots N_{m-1} w$. To check that we haven't broken anything, we note that any $i < m$ has

$$z'\varepsilon_i = z\varepsilon_i + N_1 \cdots N_{m-1} w\varepsilon_i \equiv z\varepsilon_i \equiv z_i\varepsilon_i \pmod{\operatorname{im}\mathcal{F}}$$

where we note that $N_i\varepsilon_i \equiv 0 \pmod{\operatorname{im}\mathcal{F}}$. It remains to deal with $i = m$. Because w features no $\sigma_m^{a_m-1}$ terms, we can check that any $g = \prod_{j=1}^m \sigma_j^{a_j}$ with $a_m < n_m - 1$ has

$$\rho(g\varepsilon_m) = g_m\big(\sigma_m^{a_m} - N_i 1_{a_m=n_m-1}\big)\varepsilon_m = g_m\sigma_m^{a_m}\varepsilon_m = g\varepsilon_m,$$

so ρ will just act as the identity on w! Extending this linearly, we see that

$$\begin{aligned}\rho((z_m - z')\varepsilon_m) &= \rho((z_m - z)\varepsilon_m) - \rho(N_1 \cdots N_{m-1} w\varepsilon_m) \\ &= N_1 \cdots N_{m-1} w\varepsilon_m - N_1 \cdots N_{m-1} w\varepsilon_m \\ &= 0.\end{aligned}$$

Thus, $(z_m - z')\varepsilon_m \in \operatorname{im}\mathcal{F}$, so $z_m\varepsilon_m \equiv z\varepsilon_m \pmod{\operatorname{im}\mathcal{F}}$ as well. ■

We are now ready to classify our 1-cocycles.

Proposition 36. Fix everything as in the set-up. If $f \in Z^1(G, \operatorname{coker}\mathcal{F})$ is a 1-cocycle, then there exists $z \in \mathbb{Z}[G]$ such that $f(\sigma_i) = z\varepsilon_i$ for each index i. Combined with the formula in Lemma 33, this fully determines f.

Proof. We start by noting that each index i has

$$0 = f(1) = f\left(\sigma_i^{n_i}\right) = \sigma_i^{(n_i)} f(\sigma_i) = N_i(f(\sigma_i))$$

by plugging in $\sigma_i^{n_i}$ into Lemma 33. Thus, Lemma 34 grants us some $z_i \in \mathbb{Z}[G]$ such that $f(\sigma_i) = z_i\varepsilon_i$ for each index i.

Continuing, we note that each pair of indices (i, j) has

$$\sigma_i f(\sigma_j) + f(\sigma_i) = f(\sigma_i\sigma_j) = f(\sigma_j\sigma_i) = \sigma_j f(\sigma_i) + f(\sigma_j),$$

so

$$T_i z_j \varepsilon_j = T_i f(\sigma_j) = T_j f(\sigma_i) = T_j z_i \varepsilon_i.$$

Thus, we know from Lemma 35 that there exists $z \in \mathbb{Z}[G]$ such that $f(\sigma_i) = z_i\varepsilon_i = z\varepsilon_i$ for each index i. This completes the proof. ■

Note that Proposition 36 does not say that all the conjured 1-cocycles are actually 1-cocycles. It will be beneficial for us to show this by hand, so we postpone it to the next subsection.

3.3 Verification of 1-Cocycles

The point of this subsection is to verify that all the 1-cocycles of Proposition 36 are indeed 1-cocycles. The main step is in showing 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 $g \coloneqq \prod_{i=1}^m \sigma_i^{a_i}$ 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

$$c(g) \coloneqq \left(g_i \sigma_i^{(a_i)}\right)_{i=1}^m,$$

where $g \coloneqq \prod_{i=1}^m \sigma_i^{a_i}$. 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

$$\begin{aligned} dc(g,h) &= gc(h) - c(gh) + c(g) \\ &= g\left(h_i \sigma_i^{(b_i)}\right)_{i=1}^m - \left(\prod_{p=0}^{i-1} \sigma_p^{r_p} \cdot \sigma_i^{(r_i)}\right)_{i=1}^m + \left(g_i \sigma_i^{(a_i)}\right)_{i=1}^m \\ &= \left(g h_i \sigma_i^{(b_i)}\right)_{i=1}^m - \left(g_i h_i \sigma_i^{(r_i)}\right)_{i=1}^m + \left(g_i \sigma_i^{(a_i)}\right)_{i=1}^m. \end{aligned} \tag{3.2}$$

We now go term-by-term in (3.2). The easiest is the middle term of (3.2), for which we write

$$\begin{aligned} g_i h_i \sigma_i^{(r_i)} &= g_i h_i \sigma_i^{(a_i+b_i)} - g_i h_i \sigma_i^{r_i} \sigma_i^{(n_i q_i)} \\ &= g_i h_i \sigma_i^{(a_i+b_i)} - g_i h_i \sigma_i^{a_i+b_i} \cdot q_i N_i \\ &= g_i h_i \sigma_i^{(a_i+b_i)} - g_i h_i \cdot q_i N_i, \end{aligned}$$

where the last equality is because $\sigma_i N_i = N_i$. Thus,

$$\begin{aligned} -\left(g_i h_i \sigma_i^{(r_i)}\right)_{i=1}^m &= -\left(g_i h_i \sigma_i^{(a_i+b_i)}\right)_{i=1}^m + \left(g_i h_i \cdot q_i N_i\right)_{i=1}^m \\ &= -\left(g_i h_i \sigma_i^{(a_i+b_i)}\right)_{i=1}^m + \mathcal{F}\big((g_i h_i q_i)_i, (0)_{i>j}\big). \end{aligned}$$

Now, using Lemma 30, the ith coordinate of the left term of (3.2) is

$$\begin{aligned} g h_i \sigma_i^{(b_i)} &= g_i \sigma_i^{a_i} \left(\prod_{j=i+1}^m \sigma_j^{a_j}\right) h_i \sigma_i^{(b_i)} \\ &= g_i \left(1 + \sum_{j=i+1}^m \left(\prod_{q=i+1}^{j-1} \sigma_q^{a_q}\right) \sigma_j^{(a_j)} T_j\right) h_i \sigma_i^{a_i} \sigma_i^{(b_i)} \\ &= g_i h_i \sigma_i^{a_i} \sigma_i^{(b_i)} + \sum_{j=i+1}^m \left(g_i \sigma_i^{a_i} \prod_{q=i+1}^{j-1} \sigma_q^{a_q}\right) h_i \sigma_j^{(a_j)} \sigma_i^{(b_i)} T_j \\ &= g_i h_i \sigma_i^{a_i} \sigma_i^{(b_i)} + \sum_{j=i+1}^m g_j h_i \sigma_j^{(a_j)} \sigma_i^{(b_i)} T_j. \end{aligned}$$

And lastly, for the right term of (3.2), 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 (3.2), which gives

$$\begin{aligned}dc(g,h)-\mathcal{F}\big((g_ih_iq_i)_i,(0)_{i>j}\big)&=\left(g_ih_i\sigma_i^{a_i}\sigma_i^{(b_i)}\right)_{i=1}^m-\left(g_ih_i\sigma_i^{(a_i+b_i)}\right)_{i=1}^m+\left(g_ih_i\sigma_i^{(a_i)}\right)_{i=1}^m\\&\quad+\left(\sum_{j=i+1}^m g_jh_i\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j-\sum_{j=1}^{i-1}g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j\right)_{i=1}^m\\&=\left(-\sum_{j=1}^{i-1}g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j+\sum_{j=i+1}^m g_jh_i\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j\right)_{i=1}^m\\&=\mathcal{F}\left((0)_i,\left(g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}\right)_{i>j}\right).\end{aligned}$$

Thus,

$$dc(g,h)=\mathcal{F}\left((g_ih_iq_i)_i,\left(g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}\right)_{i>j}\right)\in\operatorname{im}\mathcal{F}. \tag{3.3}$$

This completes the proof of Proposition 25.

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

$$X:=\frac{\mathbb{Z}[G]^m\times\mathbb{Z}[G]^{\binom{m}{2}}}{\ker\mathcal{F}}$$

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 37. Fix everything as in the set-up. Then the $\overline{c}$ of Proposition 25 has

$$\delta(c)(g,h):=\left((g_ih_iq_i)_i,\left(g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}\right)_{i>j}\right)\in Z^2(G,X)$$

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 (3.3). ■

Remark 38. In some sense, this $\delta(c)$ is exactly the cocycle of Theorem 16, where we have abstracted away everything about A. We will rigorize this notion in our proof of Theorem 27.

We are now ready to complete the proof of Proposition 28. In fact, we show the following stronger result.

Proposition 39. Fix everything as in the set-up. Further, let $\varepsilon\colon\mathbb{Z}[G]\to\mathbb{Z}$ be the augmentation map sending $\sigma_i\mapsto 1$ for each i. Then the following are true.

(a) Given any $z\in\mathbb{Z}[G]$, the formula

$$f(g)=\sum_{i=1}^m g_i\sigma_i^{(a_i)}\cdot z\varepsilon_i=(z\cdot\overline{c})(g)$$

for $g:=\prod_{i=1}^m\sigma_i^{a_i}$ defines a 1-cocycle in $Z^1(G,\operatorname{coker}\mathcal{F})$. These are all the 1-cocycles.

(b) If $f\in Z^1(G,\operatorname{coker}\mathcal{F})$ is a 1-cocycle, then $[f]=[\varepsilon(z)\cdot\overline{c}]$ in $H^1(G,\operatorname{coker}\mathcal{F})$, for the $z\in\mathbb{Z}[G]$ of Proposition 36. In particular, $H^1(G,\operatorname{coker}\mathcal{F})$ is a cyclic abelian group generated by $[\overline{c}]$.

Proof. We proceed one at a time.

(a) Given $z \in \mathbb{Z}[G]$, to see that f is a 1-cocycle, note that $f = z \cdot \overline{c}$. Thus, for the 1-cocycle check, we just note that any $g, h \in G$ have

$$\begin{aligned} f(gh) &= z \cdot \overline{c}(gh) \\ &= z \cdot (g\overline{c}(h) + \overline{c}(g)) \\ &= gf(h) + f(g) \end{aligned}$$

because we already know that $\overline{c} \in Z^1(G, \operatorname{coker} \mathcal{F})$.

To see that these are all the 1-cocycles, let $f \in Z^1(G, \operatorname{coker} \mathcal{F})$ be any 1-cocycle. Then Proposition 36 promises $z \in \mathbb{Z}[G]$ such that $f(\sigma_i) = z\varepsilon_i$ for each index i, for which Lemma 33 tells us that

$$f(g) = \sum_{i=1}^{m} g_i \sigma_i^{(a_i)} f(\sigma_i) = \sum_{i=1}^{m} g_i \sigma_i^{(a_i)} \cdot z\varepsilon_i$$

for $g \coloneqq \prod_{i=1}^{m} \sigma_i^{a_i}$. So f does have the desired form.

(b) Fix $f \in Z^1(G, \operatorname{coker} \mathcal{F})$, and conjure the corresponding $z \in \mathbb{Z}[G]$ of Proposition 36. We note in part (a) that $f = z \cdot \overline{c}$, so it remains to show that $[z \cdot \overline{c}] = [\varepsilon(z) \cdot \overline{c}]$ in $H^1(G, \operatorname{coker} \mathcal{F})$.

By linearity of $\mathbb{Z}[G]$, it suffices to show that $[g \cdot \overline{c}] = [\overline{c}]$ for each $g \in G$. By induction on the number of generators σ_i appearing in $g \in G$, it suffices to show that $[\sigma_i \cdot \overline{c}] = [\overline{c}]$ for each index i. Lastly, by rearranging the σ_i, it suffices to show that $[\sigma_1 \cdot \overline{c}] = [\overline{c}]$.

Well, for any σ_i, we note that

$$(\sigma_1 \overline{c} - \overline{c})(\sigma_i) = \sigma_1 \varepsilon_i - \varepsilon_i = T_1 \varepsilon_i = T_i \varepsilon_1,$$

where in the last equality we have used that we're living in $\operatorname{coker} \mathcal{F}$. Letting $d \colon C^0(G, \operatorname{coker} \mathcal{F}) \to B^1(G, \operatorname{coker} \mathcal{F})$ denote the corresponding differential, we see

$$(\sigma_1 \overline{c} - \overline{c} - d\varepsilon_1)(\sigma_i) = T_i \varepsilon_1 - (\sigma_i - 1)\varepsilon_1 = 0$$

for each index i. Thus, $\sigma_1 \overline{c} - \overline{c} - d\varepsilon_1) \in Z^1(G, \operatorname{coker} \mathcal{F})$ vanishes on all σ_i, so Lemma 33 tells us that it vanishes on all $g \in G$. It follows $[\sigma_1 \overline{c} - \overline{c}] = [0]$, which finishes.

The above parts complete the proof. ■

Corollary 40. Fix everything as in the set-up. Then $H^2(G, X)$ is a cyclic abelian group generated by $[\delta(\overline{c})]$, where δ is induced by

$$0 \to X \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0.$$

Proof. From the long exact sequence of cohomology, we see that

$$\delta \colon H^1(G, \operatorname{coker} \mathcal{F}) \to H^2(G, X)$$

is an isomorphism because $\mathbb{Z}[G]^m$ is projective and hence acyclic. Thus, this follows from (b) of Proposition 39. ■

3.4 Tuples via Cohomology

We continue in the set-up of the previous subsection. The goal of this subsection is to prove Proposition 26. 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 41. 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) $N_pN_q\lambda_{pq}$ 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_iN_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 $y_{ij} = N_iN_j$, 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

$$T_qN_p - N_pT_q + 0 = 0.$$

For $i=q$, we have no x_q term, so we are left with $N_pT_p = 0$.

(d) Again, the only relevant terms are at indices p and q. This time the interesting term is at $i=q$, where we have

$$T_pN_q - 0 + (-N_q)T_p = 0.$$

Then at $i=p$, we simply have $0N_p - (-N_q)T_q + 0 = 0$.

(e) The relevant terms, as usual, are for $i \in \{p,q,r\}$.

- At $i=p$, we have $0 - (T_qT_r + (-T_r)T_q) + 0 = 0$.
- 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 42. 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 26.

In fact, the following is true.

Lemma 43. Fix everything as in the set-up. Then the elements (a)–(e) of Lemma 41, with (b) removed, generate $\ker \mathcal{F}$.

Proof. We remark that we callously removed (b) because it is implied (c): $T_q\kappa_p + N_p\lambda_{pq} \in \ker \mathcal{F}$ 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 43.

Proposition 26. 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

$$\varphi\colon f \mapsto \left(\left(f(\kappa_i)\right)_i, \left(f(\lambda_{ij})\right)_{i>j} \right).$$

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 44. 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

$$\left(\left(f(\kappa_i)\right)_i, \left(f(\lambda_{ij})\right)_{i>j} \right)$$

is a $\{\sigma_i\}_{i=1}^m$-tuple.

Proof. By Lemma 43, we see $\ker \mathcal{F} \subseteq \ker f$ if and only if f vanishes on the elements given in Lemma 41. As such, we now run the following checks.

1. We discuss (2.1). 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 (2.2). 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 (2.3). 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

$$f(\kappa_i) := \alpha_i \qquad \text{and} \qquad f(\lambda_{ij}) := \beta_{ij}$$

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 44 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 27.

Theorem 27. Fix everything as in the set-up. Further, fix a G-module A and a $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$. Then observe there is a natural cup product map

$$\cup \colon H^2(G, X) \times H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \to H^2(G, A)$$

by using the evaluation map $X \otimes_{\mathbb{Z}} \operatorname{Hom}_{\mathbb{Z}}(X, A) \to A$. Then, using the isomorphism of Proposition 26, the cocycle defined in Theorem 16 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 37, 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

$$\delta(\overline{c}) \cup f \colon (g, h) \mapsto \delta(\overline{c})(g, h) \otimes_{\mathbb{Z}} gh \cdot f = \delta(\overline{c})(g, h) \otimes_{\mathbb{Z}} f.$$

To pass through evaluation, we set $g := \prod_i \sigma_i^{a_i}$ and $h := \prod_i \sigma_i^{b_i}$, from which we get

$$\begin{aligned} f(\delta(\overline{c})(g, h)) &= f\left((g_i h_i q_i)_i, \left(g_i h_j \sigma_i^{(a_i)} \sigma_j^{(b_j)}\right)_{i>j}\right) \\ &= \sum_{i=1}^m g_i h_i \left\lfloor \frac{a_i + b_i}{n_i} \right\rfloor \cdot \alpha_i + \sum_{\substack{i,j=1 \\ i>j}}^m g_i h_j \sigma_i^{(a_i)} \sigma_j^{(b_j)} \cdot \beta_{ij} \\ &= \sum_{\substack{i,j=1 \\ i>j}}^m \left(\prod_{p<i} \sigma_p^{a_p}\right)\left(\prod_{q<j} \sigma_q^{b_q}\right) \sigma_i^{(a_i)} \sigma_j^{(b_j)} \beta_{ij} + \sum_{i=1}^m g_i h_i \alpha_i^{\left\lfloor \frac{a_i+b_i}{n_i} \right\rfloor}. \end{aligned}$$

Doing a little more rearrangement and writing this multiplicatively exactly recovers the cocycle of Theorem 16. This completes the proof. ■

3.5 Some Loose Ends

We continue in the set-up and notation of the previous subsection. Though we have proven everything we set out to do in subsection 3.1, there is more to discuss with our alternate description of tuples. The main goal of this subsection is to prove the following extension of Proposition 26.

Proposition 45. Fix everything as in the set-up, and let A be a G-module. Then the isomorphism of Proposition 26 descends to an isomorphism between equivalence classes of $\{\sigma_i\}_{i=1}^m$-tuples are canonically isomorphic to $\widehat{H}^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))$.

Proof. Recall that the short exact sequence

$$0 \to X \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0$$

of G-modules splits as $\mathbb{Z}$-modules by Lemma 31, so we have a short exact sequence

$$0 \to \operatorname{Hom}_{\mathbb{Z}}(\operatorname{coker}\mathcal{F}, A) \to \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^m, A) \xrightarrow{-\circ\mathcal{F}} \operatorname{Hom}_{\mathbb{Z}}(X, A) \to 0.$$

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.

$$\begin{tikzcd} H^0(G, \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^m, A)) \arrow[r, "-\circ\mathcal{F}"] & H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \arrow[r] \arrow[d, two heads] & H^1(G, \operatorname{Hom}_{\mathbb{Z}}(\operatorname{coker}\mathcal{F}, A)) \arrow[d, equal] \\ 0 \arrow[r] & \widehat{H}^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \arrow[r] & \widehat{H}^1(G, \operatorname{Hom}_{\mathbb{Z}}(\operatorname{coker}\mathcal{F}, A)) \end{tikzcd} \tag{3.4}$$

Here, the middle vertical map is reduction modulo $\operatorname{im} N_G$. 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

$$\frac{H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))}{\operatorname{im}(-\circ\mathcal{F})} \simeq \widehat{H}^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)), \tag{3.5}$$

which simply sends $[f] \mapsto [f]$.

Thus, the main content here will be to track through the image of $-\circ\mathcal{F}$ in (3.4). 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 $\varphi\colon H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \to \mathcal{T}$ be defined by

$$\varphi\colon f \mapsto \left(\big(f(\kappa_i)\big)_i, \big(f(\lambda_{ij})\big)_{i>j}\right)$$

be the isomorphism of Proposition 26, we claim that the image of $-\circ\mathcal{F}$ in $H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))$ 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,

$$\varphi(f\circ\mathcal{F}) = \left(\big(N_i f(\varepsilon_i)\big)_i, \big(T_i f(\varepsilon_j) - T_j f(\varepsilon_i)\big)_{i>j}\right),$$

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

$$\overline{\varphi}\colon \frac{H^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))}{\operatorname{im}(-\circ\mathcal{F})} \simeq \frac{\mathcal{T}}{\mathcal{T}_0}.$$

Composing this with the "identity" map (3.5) finishes the proof. ■

Another loose end we have to tie up is that we showed $H^2(G, X)$ is cyclic generated by $[\delta(\overline{c})]$, but we do not actually know the order. Tracking through Tate–Nakayama duality in the proof will tell us that the order is $\#G$, but this requires G to be a Galois group. Thankfully, we are able to work this out for general G using the rest of the theory that we have built.

Lemma 46. Fix everything as in the set-up. If $z \in \mathbb{Z}[G]$ has $z\varepsilon_i = 0$ in $\operatorname{coker} \mathcal{F}$, then $z \in \operatorname{im} N_i$.

Proof. The point is to pass through ρ of Lemma 31. By possibly rearranging the σ_i, we may assume that $i = m$. Then, for any $g := \prod_{i=1}^m \sigma_i^{a_i}$, we see

$$\rho(g\varepsilon_m) = g_m\left(\sigma_m^{a_m} - N_m 1_{a_m = n_m - 1}\right)\varepsilon_m = g\varepsilon_m - g_m 1_{a_m = n_m - 1} \cdot N_m \varepsilon_m.$$

Namely, $\rho(g\varepsilon_m) - g\varepsilon_m = N_m z_g \varepsilon_m$ for some $z_g \in \mathbb{Z}[G]$.

Extending this linearly, we see that

$$\rho(z\varepsilon_m) - z\varepsilon_m = w \cdot N_m \varepsilon_m$$

for some $w \in \mathbb{Z}[G]$, but $z\varepsilon_m = 0$ in $\operatorname{coker} \mathcal{F}$ makes this say $z\varepsilon_m = -w \cdot N_m \varepsilon_m$. Because this is now an equality in $\mathbb{Z}[G]^m$, we conclude $z = -w \cdot N_m \in N_m$. ■

Lemma 47. Fix everything as in the set-up. Then $z \cdot \overline{c} = 0$ in $Z^1(G, \operatorname{coker} \mathcal{F})$ if and only if $z \in \operatorname{im} N_G$, where $N_G = \sum_{g \in G} g$.

Proof. In one direction, if $z = N_G w$, then

$$z\varepsilon_i = N_G w \varepsilon_i \equiv 0 \pmod{\operatorname{im} \mathcal{F}}$$

for each index i, so it follows that $(z \cdot \overline{c})(\sigma_i) = z\varepsilon_i = 0$ for each σ_i. Thus, using Lemma 33, we conclude that $z \cdot \overline{c} = 0$.

The other direction is more difficult. Suppose that $z \cdot \overline{c} = 0$. In particular, it follows that $(z \cdot \overline{c})(\sigma_i) = z\varepsilon_i$ must equal 0 for each index i. In particular, by Lemma 46, we conclude that $z \in \operatorname{im} N_i$ for each index i, which by Lemma 29 tells us that

$$z \in \operatorname{im} N_1 \cdots N_m = \operatorname{im} N_G.$$

This completes the proof. ■

Proposition 48. Fix everything as in the set-up. Then $H^1(G, \operatorname{coker} \mathcal{F})$ is cyclic of order $\#G$, generated by $[\overline{c}]$.

Proof. To help us use Proposition 39, let $\varepsilon \colon \mathbb{Z}[G] \to \mathbb{Z}$ denote the augmentation map.

Note that we already know $H^1(G, \operatorname{coker} \mathcal{F})$ is cyclic generated by $[\overline{c}]$ by Proposition 39, so it only remains to compute the order of $[\overline{c}]$. On one hand, we have an upper bound on the order of $[\overline{c}]$ because $H^1(G, \operatorname{coker} \mathcal{F})$ is $\#G$-torsion, but we can also see this directly: note that Lemma 47 tells us that

$$[0] = [N_G \cdot \overline{c}].$$

However, $[N_G \cdot \overline{c}] = [\varepsilon(N_G) \cdot \overline{c}] = [\#G \cdot \overline{c}]$ by Proposition 39, so we do see that $\#G \cdot \overline{c} = 0$.

It remains to show that $[\overline{c}]$ has order at least $\#G$. As such, it suffices to show that if n has $[n \cdot \overline{c}] = [0]$, then $\#G \mid n$. In particular, $n \cdot \overline{c}$ is a coboundary, so letting $d \colon C^0(G, \operatorname{coker} \mathcal{F}) \to B^1(G, \operatorname{coker} \mathcal{F})$ denote the corresponding differential, we have

$$n \cdot \overline{c} = d\left(\sum_{i=1}^m b_i \varepsilon_i\right) = \sum_{i=1}^m b_i (d\varepsilon_i)$$

for some $\{b_i\}_{i=1}^m \subseteq \mathbb{Z}[G]$. Now, $(d\varepsilon_i)(\sigma_j) = T_j \varepsilon_i = T_i \varepsilon_j$ for any pair of indices (i, j), so by the uniqueness of the extension in Lemma 33, we conclude $d\varepsilon_i = T_i \overline{c}$. Thus, we set

$$z := n - \sum_{i=1}^m b_i T_i$$

so that $\varepsilon(z) = n$ and $z \cdot \overline{c} = 0$.

To finish, we note Lemma 47 now tells us that $z \in \operatorname{im} N_G$, so letting $z = N_G w$, we see that

$$n = \varepsilon(z) = \varepsilon(N_G)\varepsilon(w) = \#G \cdot \varepsilon(w),$$

so $\#G \mid n$. This completes the proof. ■

Corollary 49. Fix everything as in the set-up. Then $H^1(G, \operatorname{coker} \mathcal{F})$ is cyclic of order $\#G$, generated by $[\delta(\overline{c})]$, where δ is induced by

$$0 \to X \xrightarrow{\mathcal{F}} \mathbb{Z}[G]^m \to \operatorname{coker} \mathcal{F} \to 0.$$

Proof. As in the proof of Corollary 40, we note $\delta \colon H^1(G, \operatorname{coker} \mathcal{F}) \to H^2(G, X)$ is an isomorphism, so this follows from Proposition 48. ■

3.6 Preliminaries on the Cup Product

We take a brief intermission to establish a little theory on cup products. In this section, we let G denote a generic finite group (not necessarily assumed to be abelian) and A a G-module.

Lemma 50 ([Neu13], Proposition I.5.3)**.** Let G be a finite group. Given any G-modules A, B, C with a G-module homomorphism $\varphi \colon B \to C$, the following diagram commutes for any $p, q \in \mathbb{Z}$ and $[a] \in \widehat{H}^p(G, A)$.

$$\begin{tikzcd}
\widehat{H}^q(G,B) \arrow[r, "\varphi"] \arrow[d, "{[a]\cup -}"'] & \widehat{H}^q(G,C) \arrow[d, "{[a]\cup -}"] \\
\widehat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} B) \arrow[r, "\mathrm{id}_A \otimes \varphi"] & \widehat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} C)
\end{tikzcd}$$

Proof. When $p, q \geq 0$, we can argue directly. Indeed, we claim that the diagram commutes on the level of homogeneous cochains: let $[a] \in \widehat{H}^p(G, A)$ and $[b] \in \widehat{H}^q(G, B)$ be cohomology classes represented by the homogeneous cochains $a \in [a]$ and $b \in [b]$. Tracking along the top of the diagram, we see

$$\begin{aligned}
(a \cup \varphi(b))(g_0, \ldots, g_{p+q}) &= a(g_0, \ldots, g_p) \otimes \varphi(b)(g_p, \ldots, g_{p+1}) \\
&= a(g_0, \ldots, g_p) \otimes \varphi(b(g_p, \ldots, g_{p+1})).
\end{aligned}$$

Tracking along the bottom of the diagram, we see

$$\begin{aligned}
(\mathrm{id}_A \otimes \varphi)(a \cup b)(g_0, \ldots, g_{p+q}) &= (\mathrm{id}_A \otimes \varphi)(a(g_0, \ldots, g_p) \otimes b(g_p, \ldots, g_{p+q})) \\
&= a(g_0, \ldots, g_p) \otimes \varphi(b(g_p, \ldots, g_{p+q})),
\end{aligned}$$

which is equal. This completes the proof in the case of $p, q \geq 0$.

We will only need the case of $p, q \geq 0$ in the application, but we will go ahead and do the general case now; we dimension-shift p and q downwards. For example, to shift p downwards, we note that the (split) short exact sequence

$$0 \to A \otimes_{\mathbb{Z}} I_G \to A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \to A \to 0 \tag{3.6}$$

induces the isomorphism $\delta \colon \widehat{H}^{p-1}(G, A) \to \widehat{H}^p(G, I_G \otimes_{\mathbb{Z}} A)$. As such, given $a \in \widehat{H}^{p-1}(G, A)$, the inductive hypothesis reassures that the following diagram commutes.

$$\begin{tikzcd}
\widehat{H}^q(G,B) \arrow[r, "\varphi"] \arrow[d, "\delta(a)\cup -"'] & \widehat{H}^q(G,C) \arrow[d, "\delta(a)\cup -"] \\
\widehat{H}^{p+q}(G, I_G \otimes_{\mathbb{Z}} A \otimes_{\mathbb{Z}} B) \arrow[r, "\varphi"] & \widehat{H}^{p+q}(G, I_G \otimes_{\mathbb{Z}} A \otimes_{\mathbb{Z}} C)
\end{tikzcd}$$

In other words, all $b \in \widehat{H}^q(G,B)$ have $\varphi(\delta(a) \cup b) = \delta(a) \cup \varphi(b)$.

Now, because (3.6) is split, we can hit it with $- \otimes_{\mathbb{Z}} B$ and $- \otimes_{\mathbb{Z}} C$ to induce the following commutative diagram with exact rows.

$$\begin{tikzcd} 0 \arrow[r] & A \otimes_{\mathbb{Z}} I_G \otimes_{\mathbb{Z}} B \arrow[r] \arrow[d, "\varphi"'] & A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \otimes_{\mathbb{Z}} B \arrow[r] \arrow[d, "\varphi"'] & A \otimes_{\mathbb{Z}} B \arrow[r] \arrow[d, "\varphi"'] & 0 \\ 0 \arrow[r] & A \otimes_{\mathbb{Z}} I_G \otimes_{\mathbb{Z}} C \arrow[r] & A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \otimes_{\mathbb{Z}} C \arrow[r] & A \otimes_{\mathbb{Z}} C \arrow[r] & 0 \end{tikzcd}$$

Letting $\delta_B \colon \widehat{H}^{p-1}(A \otimes_{\mathbb{Z}} B) \to \widehat{H}^p(I_G \otimes_{\mathbb{Z}} A \otimes_{\mathbb{Z}} B)$ and $\delta_C \colon \widehat{H}^{p-1}(A \otimes_{\mathbb{Z}} B) \to \widehat{H}^p(I_G \otimes_{\mathbb{Z}} A \otimes_{\mathbb{Z}} B)$ denote the corresponding isomorphisms (note that the middle terms are induced and hence acyclic), we note that the functoriality of boundary morphisms tells us that $\varphi\delta_B = \delta_C\varphi$. In total, it follows that $b \in \widehat{H}^q(G,B)$ will have

$$\delta_C(\varphi(a \cup b)) = \varphi(\delta_B(a \cup b)) = \varphi(\delta(a) \cup b) \stackrel{*}{=} \delta(a) \cup \varphi(b) = \delta_C(a \cup \varphi(b)),$$

where we have used the inductive hypothesis at $\stackrel{*}{=}$. Because δ_C is an isomorphism, this completes the step to shift p downwards to $p-1$.

Shifting q downwards is similar. This time we start with the following commutative diagram whose rows are (split) short exact sequences.

$$\begin{tikzcd} 0 \arrow[r] & I_G \otimes_{\mathbb{Z}} B \arrow[r] \arrow[d, "\varphi"'] & \mathbb{Z}[G] \otimes_{\mathbb{Z}} B \arrow[r] \arrow[d, "\varphi"'] & B \arrow[r] \arrow[d, "\varphi"'] & 0 \\ 0 \arrow[r] & I_G \otimes_{\mathbb{Z}} C \arrow[r] & \mathbb{Z}[G] \otimes_{\mathbb{Z}} C \arrow[r] & C \arrow[r] & 0 \end{tikzcd}$$

In particular, we let $\delta'_B \colon \widehat{H}^{q-1}(G,B) \to \widehat{H}^q(G, I_G \otimes_{\mathbb{Z}} B)$ and $\delta'_C \colon \widehat{H}^{q-1}(G,B) \to \widehat{H}^q(G, I_G \otimes_{\mathbb{Z}} C)$ denote the induced isomorphisms, and again functoriality of the boundary morphisms tells us that $\varphi\delta_B = \delta_C\varphi$. Now, the inductive hypothesis tells us that the following diagram commutes for any $a \in \widehat{H}^p(G,A)$.

$$\begin{tikzcd} \widehat{H}^q(G, I_G \otimes_{\mathbb{Z}} B) \arrow[r, "\varphi"] \arrow[d, "a\cup-"'] & \widehat{H}^q(G, I_G \otimes_{\mathbb{Z}} C) \arrow[d, "a\cup-"] \\ \widehat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} I_G \otimes_{\mathbb{Z}} B) \arrow[r, "\varphi"] & \widehat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} I_G \otimes_{\mathbb{Z}} C) \end{tikzcd}$$

Namely, any $b \in \widehat{H}^{p-1}(G,B)$ has

$$\delta'_C(a \cup \varphi(b)) = a \cup \delta'_C(\varphi(b)) = a \cup \varphi(\delta'_B(b)) \stackrel{*}{=} \varphi(a \cup \delta'_B(b)) = \varphi(\delta'_B(a \cup b)) = \delta'_C(\varphi(a \cup b)),$$

where we've applied the inductive hypothesis at $\stackrel{*}{=}$. Because δ'_C is an isomorphism, this completes shifting q downwards to $q-1$. ■

Remark 51. An analogous argument shows that a G-module homomorphism $\psi \colon A \to B$ induces the following commutative diagram, for any $p, q \in \mathbb{Z}$ and $c \in \widehat{H}^q(G,C)$.

$$\begin{tikzcd} \widehat{H}^p(G,A) \arrow[r, "\psi"] \arrow[d, "-\cup c"'] & \widehat{H}^p(G,B) \arrow[d, "-\cup c"'] \\ \widehat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} C) \arrow[r, "\psi"] & \widehat{H}^{p+q}(G, B \otimes_{\mathbb{Z}} C) \end{tikzcd}$$

In a different direction, we will want a duality result. To begin, we recall the following.

Proposition 52 ([Car56], Corollary XII.6.5)**.** Let G be a finite group and A be any G-module. Then the cup-product pairing induces an isomorphism

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

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

We will use this to prove the following.

Proposition 53. Let G be a finite group, and let X be a finitely generated $\mathbb{Z}$-free G-module. Then the cup-product pairing induces an isomorphism

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

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 [Car56], Theorem XII.6.6. The key to the proof is the short exact sequence

$$0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to0. \tag{3.7}$$

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

$$0\to\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\to\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Q})\to\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Q}/\mathbb{Z})\to0. \tag{3.8}$$

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

Similarly, we note that we can hit (3.8) with the functor $-\otimes_{\mathbb{Z}}X$ to get another short exact sequence

$$0\to\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\otimes_{\mathbb{Z}}X\to\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Q})\otimes_{\mathbb{Z}}X\to\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Q}/\mathbb{Z})\otimes_{\mathbb{Z}}X\to0. \tag{3.9}$$

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

The rest of the proof is tracking boundary morphisms around. Fix some $i\in\mathbb{Z}$. Note (3.7) and (3.8) and (3.9) induce boundary isomorphisms

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

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

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\otimes_{\mathbb{Z}}X \arrow[r] \arrow[d, "\eta_{\mathbb{Z}}"'] & \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Q})\otimes_{\mathbb{Z}}X \arrow[r] \arrow[d, "\eta_{\mathbb{Q}}"'] & \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Q}/\mathbb{Z})\otimes_{\mathbb{Z}}X \arrow[r] \arrow[d, "\eta_{\mathbb{Q}/\mathbb{Z}}"'] & 0 \\ 0 \arrow[r] & \mathbb{Z} \arrow[r] & \mathbb{Q} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

where the $\eta_\bullet$ are evaluation maps. Now, Proposition 52 tells us that

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

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

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

where $X_* := \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})$ and $X^* := \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Q}/\mathbb{Z})$, 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 $a\in \widehat{H}^i(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z}))$ 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 54. 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.

3.7 A Reciprocity

The main goal of this subsection is to prove the following result.

Theorem 55. Let G be a finite group, and let X and A be G-modules. Then, if there exists an element $c\in H^2(G,X)$ such that the cup-product maps

$$\begin{aligned} c\cup -\colon \widehat{H}^{-2}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})) &\to \widehat{H}^0(G,\mathbb{Z}) \\ c\cup -\colon \widehat{H}^{0}(G,\operatorname{Hom}_{\mathbb{Z}}(X,A)) &\to \widehat{H}^2(G,A) \end{aligned}$$

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

$$\widehat{H}^2(G,A)\to \operatorname{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-2}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})),\widehat{H}^0(G,\operatorname{Hom}_{\mathbb{Z}}(X,A))\right).$$

The main step in the proof is the following lemma.

Lemma 56. Let G be a finite group, and let X and A be G-modules. Pick up another G-module A. Then, given any $i\in\mathbb{Z}$ and $c\in\widehat{H}^2(G,X)$ and $u\in\widehat{H}^2(G,A)$, the following diagram commutes, where all arrows are cup-product maps.

$$\begin{tikzcd} \widehat{H}^{i-2}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})) \arrow[r, "-\cup u"] \arrow[d, "c\cup -"'] & \widehat{H}^{i}(G,\operatorname{Hom}_{\mathbb{Z}}(X,A)) \arrow[d, "c\cup -"] \\ \widehat{H}^i(G,\mathbb{Z}) \arrow[r, "-\cup u"'] & \widehat{H}^{i+2}(G,A) \end{tikzcd}$$

Proof. Formally, our cup-product maps are induced by the following "evaluation morphisms."

- For the left arrow, we have $\eta_L\colon X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\to\mathbb{Z}$ by evaluation.
- For the top arrow, we have $\eta_T\colon \operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\otimes_{\mathbb{Z}}A\to\operatorname{Hom}_{\mathbb{Z}}(X,A)$ by $f\otimes a\mapsto (x\mapsto f(x)a)$.
- For the bottom arrow, we have $\eta_B\colon \mathbb{Z}\otimes_{\mathbb{Z}}A\to A$ by $k\otimes a\mapsto ka$.

- For the right arrow, we have $\eta_R\colon X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,A)\to A$ by evaluation.

In particular, these maps are defined so that the following diagram commutes.

$$\begin{tikzcd} X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\otimes_{\mathbb{Z}}A \arrow[r, "\eta_T"] \arrow[d, "\eta_L"'] & X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,A) \arrow[d, "\eta_R"] \\ \mathbb{Z}\otimes_{\mathbb{Z}}A \arrow[r, "\eta_B"'] & A \end{tikzcd} \tag{3.10}$$

Indeed, we can just compute along the following diagram.

$$\begin{tikzcd} x\otimes f\otimes a \arrow[r, maps to, "\eta_T"] \arrow[d, maps to, "\eta_L"'] & x\otimes(x'\mapsto f(x')a) \arrow[d, maps to, "\eta_R"] \\ f(x)\otimes a \arrow[r, maps to, "\eta_B"'] & f(x)a \end{tikzcd}$$

Now, the core of the proof is in drawing the following very large diagram.

$$\begin{tikzcd} \widehat{H}^{i-2}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})) \arrow[r, "-\cup u"] \arrow[d, "c\cup-"'] \arrow[dr, phantom, "(1)"] & \widehat{H}^{i}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\otimes_{\mathbb{Z}}A) \arrow[r, "\eta_T"] \arrow[d, "c\cup-"'] \arrow[dr, phantom, "(2)"] & \widehat{H}^{i}(G,\operatorname{Hom}_{\mathbb{Z}}(X,A)) \arrow[d, "c\cup-"'] \\ \widehat{H}^{i}(G,X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})) \arrow[r, "-\cup u"] \arrow[d, "\eta_L"'] \arrow[dr, phantom, "(3)"] & \widehat{H}^{i+2}(G,X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})\otimes_{\mathbb{Z}}A) \arrow[r, "\eta_T"] \arrow[d, "\eta_L"'] \arrow[dr, phantom, "(4)"] & \widehat{H}^{i+2}(G,X\otimes_{\mathbb{Z}}\operatorname{Hom}_{\mathbb{Z}}(X,A)) \arrow[d, "\eta_R"'] \\ \widehat{H}^{i}(G,\mathbb{Z}) \arrow[r, "-\cup u"] & \widehat{H}^{2}(G,X\otimes_{\mathbb{Z}}A) \arrow[r, "\eta_B"] & \widehat{H}^{i+2}(G,A) \end{tikzcd}$$

We are being asked to show that the outer square commutes; we will show that each inner square commutes, which will be enough.

(1) This square commutes by the associativity of the cup product.

(2) This square commutes by Lemma 50.

(3) This square commutes by Lemma 50.

(4) This square commutes by functoriality of $\widehat{H}^2(G,-)$ applied to (3.10).

The above checks complete the proof. ■

We may now proceed directly with Theorem 55.

Proof of Theorem 55. We use the lemma to assert that, for any $u\in H^2(G,A)$, the diagram

$$\begin{tikzcd} \widehat{H}^{-2}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})) \arrow[r, "-\cup u"] \arrow[d, "c\cup-"'] & \widehat{H}^{0}(G,\operatorname{Hom}_{\mathbb{Z}}(X,A)) \arrow[d, "c\cup-"] \\ \widehat{H}^{0}(G,\mathbb{Z}) \arrow[r, "-\cup u"'] & \widehat{H}^{2}(G,A) \end{tikzcd}$$

commutes. By hypothesis, the left and right arrows are isomorphisms, so the commutativity means that showing

$$\begin{array}{ccc} \widehat{H}^2(G,A) & \to & \operatorname{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-2}(G,\operatorname{Hom}_{\mathbb{Z}}(X,\mathbb{Z})),\widehat{H}^0(G,\operatorname{Hom}_{\mathbb{Z}}(X,A))\right) \\ u & \mapsto & (a\mapsto(a\cup u)) \end{array}$$

is an isomorphism is the same as showing that

$$\begin{array}{ccc} \widehat{H}^2(G,A) & \to & \operatorname{Hom}_{\mathbb{Z}}\left(\widehat{H}^{0}(G,\mathbb{Z}),\widehat{H}^2(G,A)\right) \\ u & \mapsto & (k\mapsto(k\cup u)) \end{array}$$

is an isomorphism. Setting $n := \#G$, 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 "evaluation" map $\mathbb{Z} \otimes_{\mathbb{Z}} A \simeq A$ behaves. Thus, we are showing that

$$\begin{array}{ccc} \widehat{H}^2(G, A) & \to & \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \widehat{H}^2(G, A)\right) \\ u & \mapsto & (k \mapsto ku) \end{array}$$

is an isomorphism.

However, $\widehat{H}^2(G, A)$ is n-torsion, so in fact maps $\mathbb{Z} \to \widehat{H}^2(G, A)$ automatically have $n\mathbb{Z}$ in their kernel and hence reduce to maps $\mathbb{Z}/n\mathbb{Z} \to \widehat{H}^2(G, A)$. Conversely, any map $\mathbb{Z}/n\mathbb{Z} \to \widehat{H}^2(G, A)$ can be extended by $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ to a map $\mathbb{Z} \to \widehat{H}^2(G, A)$, so we have a natural isomorphism

$$\begin{array}{ccc} \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}/n\mathbb{Z}, \widehat{H}^2(G, A)\right) & \simeq & \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, \widehat{H}^2(G, A)\right) \\ f & \mapsto & (k \mapsto f([k])) \\ ([k] \mapsto f(k)) & \leftarrow\!\shortmid & f. \end{array}$$

In particular, it suffices to show that

$$\begin{array}{ccc} \widehat{H}^2(G, A) & \to & \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}, \widehat{H}^2(G, A)\right) \\ u & \mapsto & (k \mapsto ku) \end{array}$$

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

We now synthesize the theory we have been building.

Corollary 57. Fix notation as in subsection 3.1. Then, given a G-module A, the cup-product pairing induces an isomorphism

$$\widehat{H}^2(G, A) \to \operatorname{Hom}_{\mathbb{Z}}\left(\widehat{H}^{-2}(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)), \widehat{H}^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A))\right).$$

Proof. We apply Theorem 55 to our case; here X is defined as in subsection 3.1, and we take c to be $[\delta(\overline{c})]$. We have the following two checks on $[\delta(\overline{c})]$.

- The easier check is that $[\delta(\overline{c})] \cup - \colon \widehat{H}^0(G, \operatorname{Hom}_{\mathbb{Z}}(X, A)) \to \widehat{H}^2(G, A)$ is an isomorphism, which follows from applying Proposition 45 and Theorem 27.
- Seeing that $[\delta(\overline{c})] \cup - \colon \widehat{H}^{-2}(G, \operatorname{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) \to \widehat{H}^0(G, \mathbb{Z})$ is an isomorphism requires a little more thought. Let $n := \#G$.

  The idea is to use Proposition 53 upon recalling from Corollary 40 that $\widehat{H}^2(G, X) = \langle [\delta(\overline{c})] \rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Indeed, $\widehat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ as well, so Proposition 53 at least tells us that we have an isomorphism

  $$\widehat{H}^{-2}(G, \operatorname{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) \simeq \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}. \tag{3.11}$$

  More precisely, there is a morphism $\widehat{H}^2(G, X) \to \widehat{H}^0(G, \mathbb{Z})$ sending $[\delta(\overline{c})]$ to $[1]$, so in fact Proposition 53 tells us that there is some $x \in \widehat{H}^{-2}(G, \operatorname{Hom}_{\mathbb{Z}}(X, \mathbb{Z}))$ such that

  $$[\delta(\overline{c})] \cup x = [1].$$

  In particular,

  $$[\delta(\overline{c})] \cup - \colon \widehat{H}^{-2}(G, \operatorname{Hom}_{\mathbb{Z}}(X, \mathbb{Z})) \to \widehat{H}^0(G, \mathbb{Z})$$

  sends the element $x \in \widehat{H}^{-2}(G, \operatorname{Hom}_{\mathbb{Z}}(X, \mathbb{Z}))$ to the generator $[1] \in \widehat{H}^0(G, \mathbb{Z})$. In particular, $[\delta(\overline{c})] \cup -$ is surjective, but because (3.11) tells us that these groups already have the same size, we see $[\delta(\overline{c})] \cup -$ is an isomorphism.

The above checks tell us that Theorem 55 kicks in, completing the proof. ■

References

[Car56] Henri Cartan. *Homological Algebra*. Princeton mathematical series. Princeton: Princeton University Press, 1956.

[Neu13] Jürgen Neukirch. *Class Field Theory: The Bonn Lectures*. Springer Berlin, Heidelberg, 2013.

A Verification of the Cocycle

In this section, we verify Theorem 16. 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

$$c(g, g') := \left[\prod_{1\le j<i\le m}\left(\prod_{1\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}^{(a_ib_j)}\right]\left[\prod_{i=1}^m\left(\prod_{1\le k<i}\sigma_k^{a_k+b_k}\right)\alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right],$$

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 $q_i := \lfloor (a_i + b_i)/n_i \rfloor$. To make this more digestible, we define

$$g_i := \prod_{1\le k<i}\sigma_k^{a_k}$$

for any $g = \prod_i \sigma_i^{a_i} \in G$, so we can write down our formula as

$$c(g, g') := \left[\prod_{1\le j<i\le m} g_i g'_j \beta_{ij}^{(a_ib_j)}\right]\left[\prod_{i=1}^m g_i g'_i \alpha_i^{\left\lfloor\frac{a_i+b_i}{n_i}\right\rfloor}\right].$$

Now, given $g, g', g'' \in G$, we would like to check

$$gc(g', g'') \cdot c(g, g'g'') \stackrel{?}{=} c(gg', g'') \cdot c(g, g'),$$

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 (2.2).

Lemma 58. 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 (2.2), 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

$$R_2 \coloneqq \left[\prod_{1\le j<i\le m} g_ig_j'g_j''\left(\frac{\alpha_j}{\sigma_i^{a_i}\alpha_j}\right)^{v_i}\right]\left[\prod_{i=1}^m g_ig_i'g_i''\alpha_i^{\left\lfloor\frac{a_i+y_i}{n_i}\right\rfloor}\right]$$

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

$$R_3 := \left[\prod_{1\le j<i\le m} g_i g_i' g_j'' \left(\frac{\sigma_j^{c_j}\alpha_i}{\alpha_i}\right)^{u_i}\right] \left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i} \right\rfloor}\right].$$

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

$$R_4 := \left[\prod_{i=1}^m g_i g_i' \alpha_i^{u_i}\right].$$

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

$$g\left[\prod_{1\le j<i\le m} g_i'g_j''\beta_{ij}^{(b_ic_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)}\right] \stackrel{?}{=} \left[\prod_{1\le j<i\le m} g_ig_i'g_j''\beta_{ij}^{(a_i+b_i,c_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_ig_j'\beta_{ij}^{(a_ib_j)}\right]$$

by the work above.

A.2 Finishing

We need to verify that

$$g\left[\prod_{1\le j<i\le m} g_i'g_j''\beta_{ij}^{(b_ic_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)}\right] \stackrel{?}{=} \left[\prod_{1\le j<i\le m} g_ig_i'g_j''\beta_{ij}^{(a_i+b_i,c_j)}\right]\cdot\left[\prod_{1\le j<i\le m} g_ig_j'\beta_{ij}^{(a_ib_j)}\right]$$

as discussed in the previous subsection.

Before beginning the check, we recall the relations on the βs from (2.3) 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 59. Fix indices with $i > j > k$, and let $a_i, a_j, a_k \geq 0$. Then

$$\frac{\sigma_j^{a_j}\beta_{ik}^{(a_ia_k)}}{\beta_{ik}^{(a_ia_k)}} = \frac{\sigma_k^{a_k}\beta_{ij}^{(a_ia_j)}}{\beta_{ij}^{(a_ia_j)}} \cdot \frac{\sigma_i^{a_i}\beta_{jk}^{(a_ja_k)}}{\beta_{jk}^{(a_ja_k)}}.$$

Proof. We simply compute

$$\begin{aligned}
\frac{\sigma_i^{a_i}\beta_{jk}^{(a_ja_k)}}{\beta_{jk}^{(a_ja_k)}} \cdot \frac{\sigma_k^{a_k}\beta_{ij}^{(a_ia_j)}}{\beta_{ij}^{(a_ia_j)}} &= \prod_{r=0}^{a_i-1} \frac{\sigma_i^{r+1}\beta_{jk}^{(a_ja_k)}}{\sigma_i^r\beta_{jk}^{(a_ja_k)}} \cdot \prod_{p=0}^{a_k-1} \frac{\sigma_k^{p+1}\beta_{ij}^{(a_ia_j)}}{\sigma_k^p\beta_{ij}^{(a_ia_j)}} \\
&= \prod_{p=0}^{a_k-1}\prod_{q=0}^{a_j-1}\prod_{r=0}^{a_i-1} \left(\frac{\sigma_k^p\sigma_j^q\sigma_i^{r+1}\beta_{jk}}{\sigma_k^p\sigma_j^q\sigma_i^r\beta_{jk}} \cdot \frac{\sigma_k^{p+1}\sigma_j^q\sigma_i^r\beta_{ij}}{\sigma_k^p\sigma_j^q\sigma_i^r\beta_{ij}} \right) \\
&= \prod_{p=0}^{a_k-1}\prod_{q=0}^{a_j-1}\prod_{r=0}^{a_i-1} \sigma_k^p\sigma_j^q\sigma_i^r \left(\frac{\sigma_i\beta_{jk}}{\beta_{jk}} \cdot \frac{\sigma_k\beta_{ij}}{\beta_{ij}} \right) \\
&= \prod_{p=0}^{a_k-1}\prod_{q=0}^{a_j-1}\prod_{r=0}^{a_i-1} \sigma_k^p\sigma_j^q\sigma_i^r \left(\frac{\sigma_j\beta_{ik}}{\beta_{ik}} \right),
\end{aligned}$$

where in the last equality we have use the relation on the βs. Continuing,

$$\begin{aligned}
\frac{\sigma_i^{a_i}\beta_{jk}^{(a_ja_k)}}{\beta_{jk}^{(a_ja_k)}} \cdot \frac{\sigma_k^{a_k}\beta_{ij}^{(a_ia_j)}}{\beta_{ij}^{(a_ia_j)}} &= \prod_{q=0}^{a_j-1} \left(\prod_{p=0}^{a_k-1}\prod_{r=0}^{a_i-1} \frac{\sigma_j^{q+1}\sigma_k^p\sigma_i^r\beta_{ik}}{\sigma_j^q\sigma_k^p\sigma_i^r\beta_{ik}} \right) \\
&= \prod_{q=0}^{a_j-1} \frac{\sigma_j^{q+1}\beta_{ik}^{(a_ia_k)}}{\sigma_j^q\beta_{ik}^{(a_ia_k)}} \\
&= \frac{\sigma_j^{a_j}\beta_{ik}^{(a_ia_k)}}{\beta_{ik}^{(a_ia_k)}},
\end{aligned}$$

which is what we wanted. ■

We now proceed with the check, by induction. More precisely, we claim that any $m' \leq m$ gives

$$g_{m'+1}\left[\prod_{j<i\leq m'} g_i'g_j''\beta_{ij}^{(b_ic_j)}\right]\left[\prod_{j<i\leq m'} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)}\right] \stackrel{?}{=} \left[\prod_{j<i\leq m'} g_ig_i'g_j''\beta_{ij}^{(a_i+b_i,c_j)}\right]\left[\prod_{j<i\leq m'} g_ig_j'\beta_{ij}^{(a_ib_j)}\right]$$

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

$$g_{m'+2}\prod_{j<i\leq m'+1} g_i'g_j''\beta_{ij}^{(b_ic_j)} \cdot \prod_{j<i\leq m'+1} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)} \stackrel{?}{=} \prod_{j<i\leq m'+1} g_ig_i'g_j''\beta_{ij}^{(a_i+b_i,c_j)} \cdot \prod_{j<i\leq m'+1} g_ig_j'\beta_{ij}^{(a_ib_j)}$$

but by the inductive hypothesis it suffices for

$$\frac{g_{m''+1}\prod\limits_{j<i\le m'+1} g_i'g_j''\beta_{ij}^{(b_ic_j)}}{g_{m'+1}\prod\limits_{j<i\le m'} g_i'g_j''\beta_{ij}^{(b_ic_j)}}\cdot\frac{\prod\limits_{j<i\le m'+1} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)}}{\prod\limits_{j<i\le m'} g_ig_j'g_j''\beta_{ij}^{(a_i,b_j+c_j)}}\stackrel{?}{=}\frac{\prod\limits_{j<i\le m'+1} g_ig_i'g_j''\beta_{ij}^{(a_i+b_i,c_j)}}{\prod\limits_{j<i\le m'} g_ig_i'g_j''\beta_{ij}^{(a_i+b_i,c_j)}}\cdot\frac{\prod\limits_{j<i\le m'+1} g_ig_j'\beta_{ij}^{(a_ib_j)}}{\prod\limits_{j<i\le m'} g_ig_j'\beta_{ij}^{(a_ib_j)}}$$

which is collapses to

$$\frac{g_{m''+1}\prod\limits_{j<i\le m'+1} g_i'g_j''\beta_{ij}^{(b_ic_j)}}{g_{m'+1}\prod\limits_{j<i\le m'} g_i'g_j''\beta_{ij}^{(b_ic_j)}}\cdot\prod_{j\le m'} g_{m''}g_j'g_j''\beta_{m''j}^{(a_{m''},b_j+c_j)}\stackrel{?}{=}\prod_{j\le m'} g_{m''}g_{m''}'g_j''\beta_{m''j}^{(a_{m''}+b_{m''},c_j)}\cdot\prod_{j\le m'} g_{m''}g_j'\beta_{ij}^{(a_{m''}b_j)}$$

because the terms with $i<m''=m'+1$ got cancelled in the rightmost three products. Rearranging, this is the same as

$$\frac{g_{m''+1}\prod\limits_{j<i\le m'+1} g_i'g_j''\beta_{ij}^{(b_ic_j)}}{g_{m'+1}\prod\limits_{j<i\le m'} g_i'g_j''\beta_{ij}^{(b_ic_j)}}\stackrel{?}{=}\frac{\prod\limits_{j<m''} g_{m''}g_{m''}'g_j''\beta_{m''j}^{(a_{m''}+b_{m''},c_j)}\cdot\prod\limits_{j<m''} g_{m''}g_j'\beta_{m''j}^{(a_{m''}b_j)}}{\prod\limits_{j<m''} g_{m''}g_j'g_j''\beta_{m''j}^{(a_{m''},b_j+c_j)}}.$$

Peeling off the $i=m''=m'+1$ terms from the left-hand side numerator, we're showing

$$\frac{g_{m''+1}\prod\limits_{j<i\le m'} g_i'g_j''\beta_{ij}^{(b_ic_j)}}{g_{m'+1}\prod\limits_{j<i\le m'} g_i'g_j''\beta_{ij}^{(b_ic_j)}}\stackrel{?}{=}\frac{\prod\limits_{j<m''} g_{m''}g_{m''}'g_j''\beta_{m''j}^{(a_{m''}+b_{m''},c_j)}\cdot\prod\limits_{j<m''} g_{m''}g_j'\beta_{m''j}^{(a_{m''}b_j)}}{\prod\limits_{j<m''} g_{m''+1}g_{m''}'g_j''\beta_{m''j}^{(b_{m''}c_j)}\cdot\prod\limits_{j<m''} g_{m''}g_j'g_j''\beta_{m''j}^{(a_{m''},b_j+c_j)}}.$$

We take a moment to simplify the left-hand side with Lemma 59 by writing

$$\begin{aligned}
g_{m'+1}\prod_{j<i\le m'} g_i'g_j''\left(\frac{\sigma_{m''}^{a_{m''}}\beta_{ij}^{(b_ic_j)}}{\beta_{ij}^{(b_ic_j)}}\right) &= g_{m''}\prod_{j<i\le m'} g_i'g_j''\left(\frac{\sigma_i^{b_i}\beta_{m''j}^{(a_{m''}c_j)}}{\beta_{m''j}^{(a_{m''}c_j)}}\cdot\frac{\beta_{m''i}^{(a_{m''}b_i)}}{\sigma_j^{c_j}\beta_{m''i}^{(a_{m''}b_i)}}\right)\\
&= g_{m''}\left[\prod_{j=1}^{m'} g_j''\prod_{i=j+1}^{m'} g_i'\left(\frac{\sigma_i^{b_i}\beta_{m''j}^{(a_{m''}c_j)}}{\beta_{m''j}^{(a_{m''}c_j)}}\right)\cdot\prod_{i=1}^{m'} g_i'\prod_{j=1}^{i-1} g_j''\left(\frac{\beta_{m''i}^{(a_{m''}b_i)}}{\sigma_j^{c_j}\beta_{m''i}^{(a_{m''}b_i)}}\right)\right]\\
&= g_{m''}\left[\prod_{j=1}^{m'}\frac{g_{m'+1}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}{g_{j+1}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}\cdot\prod_{i=1}^{m'}\frac{g_i'\beta_{m''i}^{(a_{m''}b_i)}}{g_i'g_i''\beta_{m''i}^{(a_{m''}b_i)}}\right]\\
&= g_{m''}\left[\prod_{j<m''}\frac{g_{m''}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}{g_{j+1}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}\cdot\prod_{j<m''}\frac{g_j'\beta_{m''j}^{(a_{m''}b_j)}}{g_j'g_j''\beta_{m''j}^{(a_{m''}b_j)}}\right]
\end{aligned}$$

after doing a lot of telescoping. Now, we can remove $g_{m''}$ everywhere to give

$$\prod_{j<m''}\frac{g_{m''}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}{g_{j+1}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}\cdot\prod_{j<m''}\frac{g_j'\beta_{m''j}^{(a_{m''}b_j)}}{g_j'g_j''\beta_{m''j}^{(a_{m''}b_j)}}\stackrel{?}{=}\frac{\prod\limits_{j<m''} g_{m''}'g_j''\beta_{m''j}^{(a_{m''}+b_{m''},c_j)}\cdot\prod\limits_{j<m''} g_j'\beta_{m''j}^{(a_{m''}b_j)}}{\prod\limits_{j<m''} g_{m''+1}'g_j''\beta_{m''j}^{(b_{m''}c_j)}\cdot\prod\limits_{j<m''} g_j'g_j''\beta_{m''j}^{(a_{m''},b_j+c_j)}},$$

or

$$\prod_{j<m''}\frac{g_{m''}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}{g_{j+1}'g_j''\beta_{m''j}^{(a_{m''}c_j)}}\stackrel{?}{=}\frac{\prod\limits_{j<m''} g_{m''}'g_j''\beta_{m''j}^{(a_{m''}+b_{m''},c_j)}\cdot\prod\limits_{j<m''} g_j'g_j''\beta_{m''j}^{(a_{m''}b_j)}}{\prod\limits_{j<m''} g_{m''+1}'g_j''\beta_{m''j}^{(b_{m''}c_j)}\cdot\prod\limits_{j<m''} g_j'g_j''\beta_{m''j}^{(a_{m''},b_j+c_j)}}.$$

Rearranging, we want

$$\prod_{j<m''}\frac{g'_jg''_j\beta^{(a_{m''},b_j+c_j)}_{m''j}}{g'_jg''_j\beta^{(a_{m''}b_j)}_{m''j}\cdot g'_{j+1}g''_j\beta^{(a_{m''}c_j)}_{m''j}}\stackrel{?}{=}\prod_{j<m''}\frac{g'_{m''}g''_j\beta^{(a_{m''}+b_{m''},c_j)}_{m''j}}{g'_{m''}g''_j\beta^{(a_{m''}c_j)}_{m''j}\cdot g'_{m''+1}g''_j\beta^{(b_{m''}c_j)}_{m''j}},$$

which is

$$\prod_{j<m''}g'_jg''_j\left(\frac{\beta^{(a_{m''},b_j+c_j)}_{m''j}}{\beta^{(a_{m''}b_j)}_{m''j}\cdot\sigma_j^{b_j}\beta^{(a_{m''}c_j)}_{m''j}}\right)\stackrel{?}{=}\prod_{j<m''}g'_{m''}g''_j\left(\frac{\beta^{(a_{m''}+b_{m''},c_j)}_{m''j}}{\beta^{(a_{m''}c_j)}_{m''j}\cdot\sigma_{m''}^{a_{m''}}\beta^{(b_{m''}c_j)}_{m''j}}\right).$$

However, by definition of the $\beta^{(xy)}_{ij}$, we see that

$$\frac{\beta^{(a_{m''},b_j+c_j)}_{m''j}}{\beta^{(a_{m''}b_j)}_{m''j}\cdot\sigma_j^{b_j}\beta^{(a_{m''}c_j)}_{m''j}}=\frac{\beta^{(a_{m''}+b_{m''},c_j)}_{m''j}}{\beta^{(a_{m''}c_j)}_{m''j}\cdot\sigma_{m''}^{a_{m''}}\beta^{(b_{m''}c_j)}_{m''j}}=1,$$

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 43. 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

$$x_iN_i-\sum_{j=1}^{i-1}y_{ij}T_j+\sum_{j=i+1}^{m}y_{ji}T_j=0$$

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
$$\kappa_pT_p, \tag{a}$$
we may assume that x_p has no σ_p terms because $\sigma_p\equiv1\pmod{T_p}$. 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 $\sigma_q\equiv1\pmod{T_q}$. 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 $\sigma_q\equiv1\pmod{T_q}$.

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
$$x_pN_p-\sum_{j=1}^{p-1}y_{pj}T_j+\sum_{j=p+1}^{m}y_{jp}T_j=0.$$
Applying the augmentation map $\varepsilon\colon\mathbb{Z}[G]\to\mathbb{Z}$, sending $\varepsilon\colon\sigma_i\mapsto1$ for each index i, we see that $x_p\in\mathbb{Z}$ implying that x_p remains fixed. On the other hand $\varepsilon\colon T_j\mapsto0$ for each index j and $\varepsilon\colon N_p\mapsto n_p$, so we are left with
$$n_px_p=0.$$
Because $n_p\neq0$ (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 29, 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 29.

We now proceed with the general case; take $m > 2$. Let $G' := \langle \sigma_2, \ldots, \sigma_m \rangle$, 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

$$\big(T_q \lambda_{p1} - T_1 \lambda_{pq} - T_p \lambda_{q1}\big) \cdot N_1$$

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.