Classifying Extensions of Abelian Groups

Nir Elber

June 4, 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

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

We know that we can abstractly represent $\mathcal{E}$ as the set $A \times G$ with some group law dictated by a 2-cocycle in $H^2(G, A)$, 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

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

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 $G \coloneqq \operatorname{Gal}(L/K)$. Further, let

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

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

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

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 $\beta^{-1} = F_2F_1F_2^{-1}F_1^{-1}$. Well, we compute

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

The above computations finish the proof. ■

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

Lemma 8. Fix everything as in Lemma 7. Then, for $x, y \geq 0$, we have

$$F_1^xF_2^y = \prod_{k=0}^{x-1}\prod_{\ell=0}^{y-1}\sigma_1^k\sigma_2^\ell(\beta)F_2^yF_1^x.$$

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

$$F_1F_2^y = \prod_{\ell=0}^{y-1}\sigma_2^\ell(\beta)F_2^yF_1.$$

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

$$\begin{aligned} F_1F_2^{y+1} &= F_1F_2^y\cdot F_2 \\ &= \prod_{\ell=0}^{y-1}\sigma_2^\ell(\beta)F_2^yF_1\cdot F_2 \\ &= \prod_{\ell=0}^{y-1}\sigma_2^\ell(\beta)F_2^y\beta F_2F_1 \\ &= \prod_{\ell=0}^{y-1}\sigma_2^\ell(\beta)\cdot\sigma_2^y(\beta)F_2^y\cdot F_2F_1 \\ &= \prod_{\ell=0}^{(y+1)-1}\sigma_2^\ell(\beta)\cdot F_2^{y+1}F_1, \end{aligned}$$

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

$$\begin{aligned}
F_1^{x+1}F_2^{y+1} &= F_1\cdot F_1^xF_2^{y+1}\\
&= F_1\cdot\prod_{k=0}^{x-1}\prod_{\ell=0}^{(y+1)-1}\sigma_1^k\sigma_2^\ell(\beta)\cdot F_2^{y+1}F_1^x\\
&= \sigma_1\left(\prod_{k=0}^{x-1}\prod_{\ell=0}^{(y+1)-1}\sigma_1^k\sigma_2^\ell(\beta)\right)\cdot F_1F_2^{y+1}F_1^x\\
&= \prod_{k=1}^{(x+1)-1}\prod_{\ell=0}^{(y+1)-1}\sigma_1^k\sigma_2^\ell(\beta)\cdot F_1F_2^{y+1}F_1^x\\
&= \prod_{k=1}^{(x+1)-1}\prod_{\ell=0}^{(y+1)-1}\sigma_1^k\sigma_2^\ell(\beta)\cdot\prod_{\ell=0}^{(y+1)-1}\sigma_2^\ell(\beta)\cdot\sigma_2^y(\beta)\cdot F_2^{y+1}F_1\cdot F_1^x\\
&= \prod_{k=0}^{(x+1)-1}\prod_{\ell=0}^{(y+1)-1}\sigma_1^k\sigma_2^\ell(\beta)F_2^{y+1}F_1^{x+1},
\end{aligned}$$

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

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

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

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

for each index $1 \le j < i \le m$. 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

$$xF_1^{a_1} \cdots F_m^{a_m}$$

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

$$xF_1^{a_1} \cdots F_m^{a_m} \cdot yF_1^{b_1} \cdots F_m^{b_m}$$

into a term of the form $zF_1^{c_1} \cdots F_m^{c_m}$. 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

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

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

$$\left(\prod_{i=1}^m F_i^{a_i}\right) F_1^{b_1} = \left[\prod_{1<i\leq m}\left(\prod_{1\leq k<i}\sigma_k^{a_k}\right)\beta_{i1}^{(a_ib_1)}\right] F_1^{a_1+b_1}\prod_{i=2}^m F_i^{a_i}.$$

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

$$\left(\prod_{i=1}^m F_i^{a_i}\right) F_1^{b_1} = \left[\prod_{1<i\leq m}\left(\prod_{1\leq k<i}\sigma_k^{a_k}\right)\beta_{i1}^{(a_ib_1)}\right] F_1^{a_1+b_1}\prod_{i=2}^m F_i^{a_i}$$

and compute

$$\begin{aligned}
\left(\prod_{i=1}^{m+1} F_i^{a_i}\right) F_1^{b_1} &= \left(\prod_{i=1}^m F_i^{a_i}\right) F_{m+1}^{a_{m+1}} F_1^{b_1} \\
&= \left(\prod_{i=1}^m F_i^{a_i}\right) \beta_{m+1,1}^{(a_{m+1}b_1)} F_1^{b_1} F_{m+1}^{a_{m+1}} \\
&= \left[\left(\prod_{k=1}^m \sigma_k^{a_k}\right)\beta_{m+1,1}^{(a_{m+1}b_1)}\right]\left[\prod_{1<i\leq m}\left(\prod_{1\leq k<i}\sigma_k^{a_k}\right)\beta_{i1}^{(a_ib_1)}\right] F_1^{a_1+b_1}\left(\prod_{i=2}^m F_i^{a_i}\right) F_{m+1}^{a_{m+1}} \\
&= \left[\prod_{1<i\leq m+1}\left(\prod_{1\leq k<i}\sigma_k^{a_k}\right)\beta_{i1}^{(a_ib_1)}\right] F_1^{a_1+b_1}\left(\prod_{i=2}^{m+1} F_i^{a_i}\right),
\end{aligned}$$

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

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

From here, we can compute

$$\begin{aligned}
\left(\prod_{i=1}^m F_i^{a_i}\right)\left(\prod_{i=1}^m F_i^{b_i}\right) &= \left(\prod_{i=1}^m F_i^{a_i}\right)F_1^{b_1}\left(\prod_{i=2}^m F_i^{b_i}\right) \\
&= \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\beta_{i1}^{(a_ib_1)}\right]F_1^{a_1+b_1}\left(\prod_{i=2}^m F_i^{a_i}\right)\left(\prod_{i=2}^m F_i^{b_i}\right) \\
&= \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\beta_{i1}^{(a_ib_1)}\right]F_1^{a_1+b_1}\cdot \\
&\qquad \left[\prod_{2\le j<i\le m}\left(\prod_{2\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}^{(a_ib_j)}\right]\left(\prod_{i=2}^m F_i^{a_i+b_i}\right) \\
&= \left[\prod_{1<i\le m}\left(\prod_{1\le k<i}\sigma_k^{a_k}\right)\beta_{i1}^{(a_ib_1)}\right]\cdot \\
&\qquad \sigma_1^{a_1+b_1}\left[\prod_{2\le j<i\le m}\left(\prod_{2\le k<j}\sigma_k^{a_k+b_k}\right)\left(\prod_{j\le k<i}\sigma_k^{a_k}\right)\beta_{ij}^{(a_ib_j)}\right]\left(\prod_{i=2}^m F_i^{a_i+b_i}\right).
\end{aligned}$$

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

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

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.

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

To show that $S_{\mathcal{E}} \subseteq S_{\mathcal{E}'}$, pick up some $\{\sigma_i\}_{i=1}^m$-tuple $(\{\alpha_i\}, \{\beta_{ij}\})$ generated from lifts $F_i \in \mathcal{E}$ (i.e., $\pi(F_i) = \sigma_i$), where

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

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

$$F_i' F_j' (F_i')^{-1} (F_j')^{-1} = \varphi\left(F_i F_j F_i^{-1} F_j^{-1}\right) = \varphi(\beta_{ij}) = \beta_{ij}$$

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 as 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 A Cocycle

We continue in the set-up of the previous subsection. The goal of this subsection is to prove Proposition 25. This is a matter of brute force. Set $c \in C^1(G, \mathbb{Z}[G]^m)$ defined by

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

where $g := \prod_{i=1}^m \sigma_i^{a_i}$. 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 $C^\bullet(G, \mathbb{Z}[G]^m) \twoheadrightarrow C^\bullet(G, \operatorname{coker} \mathcal{F})$ induced by modding out.

As such, we set $g := \prod_{i=1}^m \sigma_i^{a_i}$ and $h := \prod_{i=1}^m \sigma_i^{b_i}$ 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

$$\begin{aligned} dc(g,h) &= gc(h) - c(gh) + c(g) \\ &= g\left(h_i\sigma_i^{(b_i)}\right)_{i=1}^m - \left(\prod_{p=0}^{i-1} \sigma_p^{r_p} \cdot \sigma_i^{(r_i)}\right)_{i=1}^m + \left(g_i\sigma_i^{(a_i)}\right)_{i=1}^m \\ &= \left(gh_i\sigma_i^{(b_i)}\right)_{i=1}^m - \left(g_ih_i\sigma_i^{(r_i)}\right)_{i=1}^m + \left(g_i\sigma_i^{(a_i)}\right)_{i=1}^m. \end{aligned} \tag{3.1}$$

We now go term-by-term in (3.1). The easiest is the middle term of (3.1), for which we write

$$\begin{aligned} g_ih_i\sigma_i^{(r_i)} &= g_ih_i\sigma_i^{(a_i+b_i)} - g_ih_i\sigma_i^{r_i}\sigma_i^{(n_iq_i)} \\ &= g_ih_i\sigma_i^{(a_i+b_i)} - g_ih_i\sigma_i^{a_i+b_i} \cdot q_iN_i \\ &= g_ih_i\sigma_i^{(a_i+b_i)} - g_ih_i \cdot q_iN_i, \end{aligned}$$

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

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

Now, for the left and right terms of (3.1), we will need the following lemma.

Lemma 28. 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. ■

Thus, for the left term of (3.1), the ith coordinate is

$$\begin{aligned} gh_i\sigma_i^{(b_i)} &= g_i\sigma_i^{a_i}\left(\prod_{j=i+1}^{n_2}\sigma_j^{a_j}\right)h_i\sigma_i^{(b_i)} \\ &= g_i\left(1+\sum_{j=i+1}^{n_2}\left(\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)\sigma_j^{(a_j)}T_j\right)h_i\sigma_i^{a_i}\sigma_i^{(b_i)} \\ &= g_ih_i\sigma_i^{a_i}\sigma_i^{(b_i)}+\sum_{j=i+1}^{n_2}\left(g_i\sigma_i^{a_i}\prod_{q=i+1}^{j-1}\sigma_q^{a_q}\right)h_i\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j \\ &= g_ih_i\sigma_i^{a_i}\sigma_i^{(b_i)}+\sum_{j=i+1}^{n_2}g_jh_i\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j. \end{aligned}$$

And lastly, for the right term of (3.1), the ith coordinate is

$$\begin{aligned} g_i\sigma_i^{(a_i)} &= g_i\left(h_i-\sum_{j=1}^{i-1}h_j\sigma_j^{(b_j)}T_j\right)\sigma_i^{(a_i)} \\ &= g_ih_i\sigma_i^{(a_i)}-\sum_{j=1}^{i-1}g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j. \end{aligned}$$

So to finish, we continue from (3.1), which gives

$$\begin{aligned} dc(g,h)-\mathcal{F}\big((g_ih_iq_i)_i,(0)_{i>j}\big) &= \left(g_ih_i\sigma_i^{a_i}\sigma_i^{(b_i)}\right)_{i=1}^m-\left(g_ih_i\sigma_i^{(a_i+b_i)}\right)_{i=1}^m+\left(g_ih_i\sigma_i^{(a_i)}\right)_{i=1}^m \\ &\quad+\left(\sum_{j=i+1}^{n_2}g_jh_i\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j-\sum_{j=1}^{i-1}g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j\right)_{i=1}^m \\ &= \left(-\sum_{j=1}^{i-1}g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}T_j+\sum_{j=i+1}^{n_2}g_jh_i\sigma_j^{(a_j)}\sigma_i^{(b_i)}T_j\right)_{i=1}^m \\ &= \mathcal{F}\left((0)_i,\big(g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}\big)_{i>j}\right). \end{aligned}$$

Thus,

$$dc(g,h)=\mathcal{F}\left((g_ih_iq_i)_i,\big(g_ih_j\sigma_i^{(a_i)}\sigma_j^{(b_j)}\big)_{i>j}\right)\in\operatorname{im}\mathcal{F}. \tag{3.2}$$

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

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

to give the short exact sequence

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

In particular, we can track $\overline{c}\in Z^1(G,\operatorname{coker}\mathcal{F})$ through a boundary morphism: we already have a chosen lift $c\in Z^1(G,\mathbb{Z}[G]^m)$ for $\overline{c}$, and we have also computed $\mathcal{F}^{-1}\circ dc$ from the above work. This gives the following result.

Corollary 29. 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 (3.2). ■

Remark 30. 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.

3.3 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.

To set us up, we define the notation

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

for all relevant indices p and q. We now start with the following basic result.

Lemma 31. 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 $0 - (T_q T_r + (-T_r)T_q) + 0 = 0$.
- At $i = q$, we have $0 - (-(T_p)T_r) + ((-T_r)T_p) = 0$.
- At $i = r$, we have $0 - 0 + (T_q T_p + (-T_p)T_q) = 0$.

The above checks complete this part of the proof. ■

Remark 32. 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 33. Fix everything as in the set-up. Then the elements (a)–(e) of Lemma 31, 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

$$N_q \cdot (T_q\kappa_p + N_p\lambda_{pq}) = N_p N_q \lambda_{pq}$$

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 33.

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

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

In other words, we simply read off the values of f from indicators on the coordinates of X. It's not hard to see that φ is in fact a G-module homomorphism, but we will have to check that φ is well-defined, for which we have to check the conditions on being a $\{\sigma_i\}_{i=1}^m$-tuple.

Lemma 34. Fix everything as in the set-up, and let A be a G-module. Then, given $f\colon \mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}$, we have $\ker \mathcal{F} \subseteq \ker f$ if and only if

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

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

Proof. By Lemma 33, we see $\ker \mathcal{F} \subseteq \ker f$ if and only if f vanishes on the elements given in Lemma 31. 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

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

for all relevant indices i, j, and in fact the map $\mathcal{T} \to \operatorname{Hom}_{\mathbb{Z}}\left(\mathbb{Z}[G]^m \times \mathbb{Z}[G]^{\binom{m}{2}}, A\right)$ we can see to be a G-module homomorphism. However, because these outputs are a $\{\sigma_i\}_{i=1}^m$-tuple, we can read Lemma 34 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 29, 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 $g \coloneqq \prod_i \sigma_i^{a_i}$ and $h \coloneqq \prod_i \sigma_i^{b_i}$, from which we get

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

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

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

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

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

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

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 35. 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

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

2. Note

$$c(g, g') = \left[\prod_{1\le j<i\le m} g_i g_j' \beta_{ij}^{(a_i b_j)}\right]\left[\prod_{i=1}^m g_i g_i' \alpha_i^{u_i}\right],$$

so we set

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

3. Lastly, we collect our remainder terms. Observe

$$\begin{aligned} R_3 &= \left[\prod_{i=1}^m g_i g_i' \left(\prod_{j=1}^{i-1} g_j'' \cdot \frac{\sigma_j^{c_j}\alpha_i}{\alpha_i}\right)^{u_i}\right] \left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\ &= \left[\prod_{i=1}^m g_i g_i' \left(\prod_{j=1}^{i-1} \frac{(\sigma_1^{c_1}\cdots\sigma_{j-1}^{c_{j-1}})\sigma_j^{c_j}\alpha_i}{(\sigma_1^{c_1}\cdots\sigma_{j-1}^{c_{j-1}})\alpha_i}\right)^{u_i}\right] \left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\ &= \left[\prod_{i=1}^m g_i g_i' \left(\prod_{j=1}^{i-1} \frac{g_{j+1}''\alpha_i}{g_j''\alpha_i}\right)^{u_i}\right] \left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \\ &= \left[\prod_{i=1}^m g_i g_i' \cdot \frac{g_i''\alpha_i^{u_i}}{\alpha_i^{u_i}}\right] \left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right]. \end{aligned}$$

Thus,

$$\begin{aligned} R_3 R_4 &= \left[\prod_{i=1}^m g_i g_i' \cdot \frac{g_i''\alpha_i^{u_i}}{\alpha_i^{u_i}}\right] \left[\prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{\left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}\right] \left[\prod_{i=1}^m g_i g_i' \alpha_i^{u_i}\right] \\ &= \prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{u_i + \left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor}, \end{aligned}$$

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

$$R_1 R_2 = \prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{v_i + \left\lfloor \frac{a_i+y_i}{n_i}\right\rfloor} = \prod_{i=1}^m g_i g_i' g_i'' \alpha_i^{u_i + \left\lfloor \frac{x_i+c_i}{n_i}\right\rfloor} = R_3 R_4.$$

Thus, it suffices to show that

$$\frac{gc(g',g'')}{R_1} \cdot \frac{c(g,g'')}{R_2} \stackrel{?}{=} \frac{c(gg',g'')}{R_3} \cdot \frac{c(g,g')}{R_4},$$

which is equivalent to

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

by the work above.

A.2 Finishing

We need to verify that

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

as discussed in the previous subsection.

Before beginning the check, we recall the relations on the βs from (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 36. Fix indices with $i > j > k$, and let $a_i, a_j, a_k \geq 0$. Then

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

Proof. We simply compute

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

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

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

which is what we wanted. ■

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

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

which we will show by induction on m'. For $m' = 1$, there is nothing to say because there are no indices $i > j$.

So now suppose we have equality for $m' < m$, and we give equality for $m'' := m' + 1$. That is, we want to show that

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

but by the inductive hypothesis it suffices for

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

which is collapses to

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

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

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

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

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

We take a moment to simplify the left-hand side with Lemma 36 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

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

or

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

Rearranging, we want

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

which is

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

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

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

so everything does indeed cancel out properly. This completes the check.

B Computation of $\ker \mathcal{F}$

In this section we give a proof of Lemma 33. As such, we will use all the context from the statement and proceed directly with the proof; as mentioned earlier, we may add (b) back to our list of generators because it is induced by (c). Pick up some $z := ((x_i)_i, (y_{ij})_{i>j}) \in \ker \mathcal{F}$, which is equivalent to saying

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

for each index i. We want to write z as a $\mathbb{Z}[G]$-linear combination of the elements from (a)–(e). The main idea will be to slowly subtract out $\mathbb{Z}[G]$-linear combinations of the above elements (which does not affect $z \in \ker \mathcal{F}$) until we can prove that we have 0 left over. We start with the x_i terms, which we do in two steps.

1. We begin by dealing with the x_i terms. Fix some index p, and we will subtract out a suitable $\mathbb{Z}[G]$-linear combination of the above generators to set $x_p = 0$ while not changing the other x_i terms. Well, using the element
$$\kappa_p T_p, \tag{a}$$
we may assume that x_p has no σ_p terms because $\sigma_p \equiv 1 \pmod{T_p}$. Then for each $q < p$, we can subtract out a suitable multiple of
$$T_q \kappa_p + N_p \lambda_{pq} \tag{c}$$
to make it so that we may assume x_p has no σ_q terms because $\sigma_q \equiv 1 \pmod{T_q}$. Similarly, for each $q > p$, we can subtract out a suitable multiple of
$$T_q \kappa_p - N_p \lambda_{pq} \tag{d}$$
to make it so that we may assume x_p has no σ_q terms because $\sigma_q \equiv 1 \pmod{T_q}$.

2. Thus, the above process allows us to assume that $x_p \in \mathbb{Z}$, and the above linear combinations have not affected any x_i for $i \neq p$. We now use the fact that $z \in \ker \mathcal{F}$. Indeed, we know that
$$x_p N_p - \sum_{j=1}^{p-1} y_{pj} T_j + \sum_{j=p+1}^{m} y_{jp} T_j = 0.$$
Applying the augmentation map $\varepsilon \colon \mathbb{Z}[G] \to \mathbb{Z}$, sending $\varepsilon \colon \sigma_i \mapsto 1$ for each index i, we see that $x_p \in \mathbb{Z}$ implying that x_p remains fixed. On the other hand $\varepsilon \colon T_j \mapsto 0$ for each index j and $\varepsilon \colon N_p \mapsto n_p$, so we are left with
$$n_p x_p = 0.$$
Because $n_p \neq 0$ (it's the order of σ_p), we conclude that $x_p = 0$. Applying this argument to the other x_i terms, we conclude that we may assume $x_i = 0$ for each i.

It remains to deal with the y_{ij} terms, which is a little more involved. For reference, we are showing that

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

for each index i implies that $z = ((0)_i, (y_{ij})_{i>j})$ is a $\mathbb{Z}[G]$-linear combination of the terms from (b) and (e). Before continuing, we acknowledge that we will want the following lemma.

Lemma 37. Fix everything as in the set-up. Then, for any pair of distinct indices (p, q), we have $(\operatorname{im} N_p) \cap (\operatorname{im} N_q) = \operatorname{im} N_pN_q$, 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 $(\operatorname{im} N_p) \cap (\operatorname{im} N_q)$ and $\operatorname{im} N_pN_q$ 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, $N_pN_q \in (\operatorname{im} N_p) \cap (\operatorname{im} N_j q)$, so $\operatorname{im} N_pN_q \subseteq (\operatorname{im} N_p) \cap (\operatorname{im} N_q)$. In the other direction, suppose that we have some element

$$z := \sum_{(a_i)_i} c_{(a_i)_i} \sigma_1^{a_1} \cdots \sigma_m^{a_m} \in (\operatorname{im} N_i) \cap (\operatorname{im} N_j),$$

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 $z \in \operatorname{im} N_iN_j$.

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 both the $i = p$ and $i = q$ coordinates. Thus, we let $d_{(a_i)_{i\ne p,q}}$ be the restricted function equal to $c_{(a_i)_i}$ but forgetting the information input from a_p and a_q. This allows us to write

$$\begin{aligned}
z &= \sum_{(a_i)_i} c_{(a_i)_i} \sigma_1^{a_1} \cdots \sigma_m^{a_m} \\
&= \sum_{(a_i)_{i\ne p,q}} \sum_{a_p=0}^{n_p-1} \sum_{a_q=0}^{n_q-1} d_{(a_i)_{i\ne p,q}} \sigma_1^{a_1} \cdots \sigma_m^{a_m} \\
&= \left(\sum_{(a_i)_{i\ne p,q}} d_{(a_i)_{i\ne p,q}} \prod_{i=0, i\ne p,q}^{m} \sigma_i^{a_i} \right) \left(\sum_{a_p=0}^{n_p-1} \sigma_p^{a_p} \right) \left(\sum_{a_q=0}^{n_q-1} \sigma_q^{a_q} \right),
\end{aligned}$$

which is now manifestly in $\operatorname{im} N_pN_q$. ■

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 37, 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 37.

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 $(y'_{ij})_{i>j\ge 2} \in \mathbb{Z}[G']^{\binom{m-1}{2}}$ 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 $y_{i1} = w_iN_1$ for each $i \geq 2$; because $\sigma_1N_1 = N_1$, 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
$$\sum_{i=2}^{m} w_iN_1T_i = 0.$$
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
$$n_1\sum_{i=2}^{m} w_iT_i = 0.$$
Dividing out by n_1, we are left with
$$\sum_{i=2}^{m} w_iT_i = 0.$$

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_1N_1. Indeed, subtracting this term out looks like
$$T_qN_1\lambda_{p1} - T_pN_1\lambda_{q1},$$
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
$$\sum_{i=2}^{m} w_iT_i = 0,$$
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 $y_{i1} \in N_iN_1$. 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
$$w_2T_2 = 0,$$
finishing for w_2. Thus, we are left with the equation
$$\sum_{i=3}^{m} w_iT_i = 0,$$
from which we see we can induct downwards (this has fewer variables) to finish.

The above steps complete the proof, as advertised.