MATH 2410 Final Project - Computational Homology

Mattie Ji

December 20th, 2022

Introduction:

The ability to compute homology based on a simplicial or delta complex is a common theme that arises in the field of Topological Data Analysis. In class, we have worked with plenty of examples of finite simplicial and Δ-complex and computed their homologies.

However, the limit of human computation soon proves to not be enough. For example, say there's a $100,000,000$-dimensional smooth manifold M, we certainly know M is triangulizable, so we can turn M into a simplicial complex, but then the question is - how would a computer handle these kind of information and compute its homology?

A problem with topology in general is that often it is really difficult for a computer to interpret what exactly is a continuous map is. Fortunately, the language of commutative algebra, on the other hand, is a lot easier for a computer to handle. Many standard computer algebra systems such as `Sage`, `Maple`, and `Magma` are well-equipped to solve these issues.

It turns out that there's a very remarkable way to translate the problem of compute homologies over the ring $\mathbb{Z}$ into a question about doing "Linear Algebra" with integer matrices, using what are called "Smith Normal Forms". We will approach the topic of "Smith Normal Forms" in the broader context of module theory.

In Section 1, we will first introduce the basics about modules over an arbitary ring R. In Section 2, we will introduce the notion of "free modules", which turns out to have many surprising connections with Linear Algebra. In Section 3, we will discuss Smith Normal Forms and one notable application of Smith Normal Forms - the Structure Theorem of Finitely Generated Modules over a PID.

In Section 4, we will discuss how Smith Normal Forms apply in the computation of simplicial homology. Finally, in Section 5, we will examine the simplicial homology of 3-dimensional Lens Spaces using the method proposed in Section 4.

This project assumes a first undergraduate course in Abstract Algebra and some familiarity with Simplicial Homologies. For a reference on suitable background Abstract Algebra, please see Chapter 1 to 7 of Silverman [Sil22].

Table of Content

1 Introduction to Modules

This section serves as a basic introduction to the theory of modules. If the reader is already familiar with its content, please feel free to skip ahead. Throughout this entire document, when we say the word "ring", we are always consider commutative rings with unity.

Definition 1.1. Let R be a ring. A R-module is the tuple $(M, +, \cdot)$ such that:

- $+ : M \times M \to M$ defines an abelian group structure on M
- $\bullet : R \times M \to M$ defines a "ring action" of R on M such that for all $a, b \in R$ and $x, y \in M$
  - $1_R \cdot x = x$
  - $a \cdot (x + y) = a \cdot x + a \cdot y$
  - $(a + b) \cdot x = a \cdot x + b \cdot x$
  - $(ab) \cdot x = a \cdot (b \cdot x)$

For simplicity, we will often shorten $(M, +, \cdot)$ as M instead.

For morphisms, let M, N be R-modules, a *R-module homomorphism* $f : M \to N$ is a function satisfying:

- $f(x + y) = f(x) + f(y)$ for all $x, y \in M$
- $f(r \cdot x) = r \cdot f(x)$ for all $x \in M, r \in R$

We say that f is an *isomorphism* if it is also bijective.

Remark 1.2. The two definitions aboves forms a category of R-modules, denoted $\texttt{MOD}_R$ in the sense that:

- The objects of $\texttt{MOD}_R$ are exactly the collection of all R-modules.
- For any R-modules M, N, $\text{Hom}_{\texttt{MOD}_R}(M, N)$ are the collection of R-module morphisms between M and N.

Remark 1.3. The idea of modules over an arbitrary ring immediately generalizes many concepts we are familiar with already:

1. Let k be a field, a k-module M is exactly a k-vector space.
2. A $\mathbb{Z}$-module is exactly an abelian group (for all $n \in \mathbb{Z}$, define $n \cdot x = \text{sgn}(n) \cdot \sum_{i=0}^{|n|} x$).
3. A $k[x]$-module M is exactly a k-vector space equipped with a linear transformation $L : M \to M$, by defining where x is sent to.
4. R itself is a R-module. Let I be an ideal of R, then both I and R/I are also R-modules over R.

As seen in Remark 1.3(1), there are a lot of parallels between Linear Algebra and Module Theory. This motivates us to identify these similarities and talk about them in the broader context of Module Theory.

Definition 1.4. Let $(M, +, \bullet)$ be a R-module,

- We say a subset $N \subseteq M$ is a **submodule** of M if the restriction of $+$ to $N \times N$ and $\bullet$ to $R \times N$ turns N into a R-module.
- Let $N \subseteq M$ be a submodule of M. Recall that both M and N are abelian groups, then we can turn the **quotient** group M/N into a R-module by defining the action of R on M/N as follows:

$$r \cdot (x + N) = (r \cdot x) + N, \ r \in R, x + N \in M/N$$

- Let $S \subseteq M$, the spanning set of S is defined as

$$\text{Span}(S) := \{r_1 x_1 + ... + r_n x_n \mid r_1, ..., r_n \in R, x_1, ..., x_n \in S\}$$

  We say that M is **finitely genrated** if $M = \text{Span}(S)$ and S is finite.

- Let $S \subseteq M$, we say this S is **linearly independent** if for all $r_1, ..., r_n \in R$ and distinct $x_1, ..., x_n \in M$,

$$r_1x_1 + ... + r_nx_n = 0_M \implies r_1 = ... = r_n = 0_R$$

- Let $S \subseteq M$, we say S is a **basis** of M if $M = \text{Span}(S)$ and S is linearly independent.

Note that the list above are exactly the analogues of "subspaces", "quotient spaces", "spanning sets", "linear independence", and "basis" in the theory of Linear Algebra.

Definition 1.5. Let $f : M \to N$ be an R-module homomorphism, there are a few associated R-modules to f that are of our interests:

- We define the *kernel* of f as $Ker(f) := \{x \in M \mid f(x) = 0\}$
- We define the *image* of f as $Im(f) := \{y \in N \mid y = f(x) \text{ for some } x \in M\}$
- We define the *cokernel* of f as $Coker(f) := \frac{N}{Im(f)}$

It is certainly tempting to just view Vector Spaces and Modules interchangeably, but they are very different objects! In particular, when transitioning into modules, we lose a lot of our favorite properties in Linear Algebra.

In fact, we will now make a list of properties we have cherished in Linear Algebra and show why they fail to be true in Modules:

1. If V is a finitely generated vector space, then any minimal spanning set of V is linearly independent.
2. If V is a finitely generated vector space, then any maximal linearly independent set of V spans the entire vector space.
3. Every vector space has a basis.
4. If V is a vector space with subspace W, there exists another subspace U of V such that $V = W \oplus U$
5. Let V be a finite dimensional vector space and $f : V \to W$ be a linear transformation, then $V \cong ker(f) \oplus \frac{V}{ker(f)} \cong ker(f) \oplus im(f)$. This is sometimes called the "rank-nullity theorem"
6. Let $f : V \to W$ be a linear transformation between finitely generated vector spaces, then f is injective if and only if f is surjective.

Example 1.6 (A Plethora of Counter-Examples)**.** The idea on why (1) to (3) works is that, in a vector space, one can "divide" non-zero scalars as we are working with fields. But for Modules in general, this need not be true:

- **For (1),** consider $\mathbb{Z}$ as a $\mathbb{Z}$-module. The set $\{3, 4\}$ spans the entire ring since $1 \in \text{Span}(3, 4)$ and is minimal since neither $\{3\}$ nor $\{4\}$ spans $\mathbb{Z}$. However, this is not linearly independent as $-4 \cdot 3 + 3 \cdot 4 = -12 + 12 = 0$.
- **For (2),** consider $\mathbb{Z}/6\mathbb{Z}$ when viewed as a $\mathbb{Z}$-module. Then, for any non-empty set $S \subseteq \mathbb{Z}/6\mathbb{Z}$, S cannot be linearly independent because for any $x \in S$, $6 \cdot x = 0$. But the empty set clearly does not span $\mathbb{Z}/6\mathbb{Z}$.
- **For (3),** the same setup in (2) also shows why the $\mathbb{Z}$-modules $\mathbb{Z}/6\mathbb{Z}$ does not have a basis.

For (4)**,** it turns out that this property comes from the fact that fields have no non-zero nilpotent elements and satisfies what's called a "descending chain condition" on ideals (ie. fields are **Artinian** and **reduced**). It suffices for us to then find a non-Artinian ring:

- Consider $\mathbb{Z}/4\mathbb{Z}$ as a module over itself, then $\mathbb{Z}/4\mathbb{Z}$ has exactly 3 submodules - $0, \{0, 2\}, \mathbb{Z}/4\mathbb{Z}$. If we try to find a complementary submodule of $\{0, 2\}$ then it has to be the case that

$$\mathbb{Z}/4\mathbb{Z} \cong \{0, 2\} \oplus \{0, 2\}$$

But they are clearly not isomorphic as every element on the RHS becomes 0 when one multiplies it by 2, but $2 \cdot \mathbb{Z}/4\mathbb{Z} \neq 0$.

For (5)**,** this property really comes from the fact that this short exact sequence splits for fields:

$$0 \to ker(f) \to V \to im(f) \to 0$$

This sequence need not split in general though.

For (6), consider the map $f : \mathbb{Z} \to \mathbb{Z}$ given by $x \mapsto 2x$. This is certainly injective but clearly not surjective.

Thus, a lot of properties from Linear Algebra breaks down when we get into Modules. There is however still a canonical notion of First Isomorphism Theorem for (5):

Theorem 1.7 (First Isomorphism Theorem for Modules)**.** Let $f : M \to N$ be an R-module homomorphism, then

$$\frac{M}{ker(f)} \cong im(f)$$

Proof. Define a map $F : \frac{M}{ker(f)} \to im(f)$ given by sending each coset $x+ker(f)$ to $f(x)$. This satisfies the definition of a module homomorphism, and it is well defined since if $x + ker(f) = y + ker(f)$,

$$F(x + ker(f)) - F(y + ker(f)) = F((x - y) + ker(f)) = 0$$

as $x-y \in ker(f)$. Furthermore, F is clearly surjective on $im(f)$, and the injectivity follows from the fact that $ker(f)$ has been modded out. ■

2 Free Modules and Matrices

Fortunately, there's a certain class of modules that do share many familiar properties from Linear Algebra, which we call "free modules". In this section, we will discuss how we can recover some properties we love from Linear Algebra on free modules, especially concerning matrices.

Definition 2.1. Let M be a R-module, we say M is a **free module** if M has a basis S.

Example 2.2. Let n be a natural number, $\bigoplus_{i=1}^n R$ is a free R-module with basis

$$(1,0,...,0),(0,1,...,0),...,(0,0,...,1)$$

as the usual "standard normal basis".

It turns out that free modules M has extremely simple structure - they are actually just the (possibly infinite) direct sum of copies of R! We will show this with the following theorem:

Theorem 2.3 (Universal Property of Free Modules)**.** Let M be a free R-module with basis S, and let M' be any arbitrary R-module, then let $i : S \to M$ be the inclusion map between sets and $f : S \to M'$ be a set function, then there exists an unique R-module homomorphism $F : M \to M'$ such that this diagram:

$$\begin{tikzcd}
M \arrow[r, "\exists ! F"] & M' \\
S \arrow[u, "i"] \arrow[ur, "f"'] &
\end{tikzcd}$$

commutes.

Proof. We first define F on the basis S such that for any $s \in S$,

$$F(s) := f(s)$$

Then we can extend F to a module homomorphism on M as follows - for any $x \in M$, there exists a unique linear combination of elements in the basis such that

$$x = r_1 s_1 + ... + r_n s_n,\ r_1,...,r_n \in R, s_1,...,s_n \in S$$

Then we define

$$F(x) :== r_1 F(s_1) + ... + r_n F(s_n)$$

This is well-defined exactly because S is a basis, and it is a module homomorphism by construction. We claim that this is unique, indeed, suppose $G : M \to M'$ is another module homomorphism satisfying the commutative diagram as before, then we know that

$$F(s) = G(s),\ \forall s \in S$$

But then for all $x \in M$,

$$\begin{aligned}
G(x) &= G(r_1 s_1 + ... + r_n s_n) \\
&= r_1 G(s_1) + ... + r_n G(s_n) \\
&= r_1 F(s_1) + ... + r_n F(s_n) && G \text{ agrees with } F \text{ on basis} \\
&= F(x)
\end{aligned}$$

Thus, G and F are the same module homomorphism. ■

Corollary 2.4. Let M be a free R-module with basis S, then define $R^{\oplus S}$ as:

$$R^{\oplus S} := \{f : S \to R \text{ (set function)} \mid f(s) = 0 \text{ for all but finitely many } s \in S\}$$

Note that $R^{\oplus S}$ itself is a free R-module with its basis being the collection of functions:

$$j_s : S \to R \text{ and } j_s(x) = \begin{cases} 1, & x = s \\ 0, & x \neq s \end{cases} \quad \mid s \in S$$

In other words, j_s is the indicator function on $s \in S$ and the basis of $R^{\oplus S}$ is the collection of these indicator functions.

We then claim that $M \cong R^{\oplus S}$ as R-modules.

Proof. We will invoke the universal property as in Theorem 2.3. Define $f : S \to R^{\oplus S}$ for all $s \in S$ as follows

$$f(s) = j_s$$

Since both M and $R^{\oplus S}$ are free, we obtain the following two commutative diagrams:

$$\begin{tikzcd}
M \arrow[r, "\exists! F"] & R^{\oplus S} \\
S \arrow[u, "i"] \arrow[ur, "f"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
R^{\oplus S} \arrow[r, "\exists! G"] & M \\
S \arrow[u, "f"] \arrow[ur, "i"'] &
\end{tikzcd}$$

Chaining the two diagrams gives us

$$\begin{tikzcd}
R^{\oplus S} \arrow[r, "\exists! G"] & M \arrow[r, "\exists! F"] & R^{\oplus S} \\
S \arrow[u, "f"] \arrow[ur, "i"] \arrow[urr, "f"] & &
\end{tikzcd}$$

So in other words $F \circ G : R^{\oplus S} \to R^{\oplus S}$ is a morphism. But we also know from the universal property that:

$$\begin{tikzcd}
R^{\oplus S} \arrow[r, "\exists! H"] & R^{\oplus S} \\
S \arrow[u, "f"] \arrow[ur, "f"'] &
\end{tikzcd}$$

Since H is unique, H has to be the identity morphism. Hence, combining these two diagram shows that $F \circ G = H = id_{R^{\oplus S}}$. We can similarly show that $G \circ F = id_M$. Thus, F is in fact an isomorphism. ■

Thus, we have reduced the idea of free modules to just direct sums of copies of R. This matches with our intuitive sense of vector spaces. Now recall for vector spaces, there's a well-defined notion of "dimension", we similarly want to define this for free modules.

Definition 2.5. Let M be a free R-modules with basis S. If S is finite, we define the rank of M to be $|S|$. If S is infinite, we define the rank of M to be ∞. We write this as rank(M).

It's not immediately obvious why the rank should be well-defined. We claim that it is, and in fact it is invariant up to isomorphism.

Before we prove this theorem, we will need to introduce some machinery that will help us in this journey.

Lemma 2.6 (Nakayama's Lemma)**.** Let M be a finitely generated R-module and I be an ideal of R, we define

$$IM := \{a_1x_1 + ... + a_nx_n \mid a_i \in I, x_i \in M, n \in \mathbb{Z}_{\geq 0}\}$$

as the "product" of I and M. If $M = IM$, then there exists some element $a \in I$ such that for all $x \in M$,

$$x = a \cdot x$$

Proof. We omit the proof here, please see Corollary 2.5 of Atiyah and MacDonald [AM69] if you are interested. ■

Theorem 2.7. Let M be a finitely generated R-module and $f : M \to M$ be a surjective R-module homomorphism, then f is an isomorphism.

Proof. The proof is due to Vasconcelos originally in [Vas69]. Similar to how we can realize any $k[x]$-module as a vector space equipped with a linear endomorphism, we can realize M as a $R[x]$-module by identifying

$$x \cdot m = f(m), \forall m \in M$$

Let (x) be the ideal generated by $x \in R[x]$, since f is a surjecitve R-module homomorphism, we have that $(x)M = M$. Then Nakayama's Lemma tells us that there exists some $g(x) \in (x)$ such that

$$g(x) \cdot m = m, \ \forall m \in M$$

But since $g(x) \in (x)$, we know we can factor $g(x) = xh(x)$, hence

$$x \cdot (h(x) \cdot m) = h(x) \cdot (x \cdot m)$$

Hence the module homomorphism given by $h(x)$ is the inverse of the module homomorphism given by x, hence f is invertible and hence an isomorphism. ■

Now we are ready to prove that the rank of a free module is well-defined:

Theorem 2.8. If R is not the zero ring, then the rank of a free R-module is well-defined.

Proof. It suffices for us to prove that if $R^{\oplus S} \cong R^{\oplus T}$, then rank$(S)$ = rank(T).

Now suppose both S and T are finite, write $|S| = n$, $|T| = m$, then it suffices for us to prove that $R^n \cong R^m \implies n = m$.

Suppose instead that $m \neq n$, without loss of generality we say that $m > n$, then we can identify R^n as a submodule of R^m. Let p be the standard projection map $R^m \to R^n$ that forgets the last $m - n$ coordinates, then we obtain the following sequence:

$$R^m \xrightarrow{p} R^n \xrightarrow{\cong} R^m$$

Chaining the maps together gives a surjective homomorphism from R^m to itself. So Theorem 2.7 tells us that this is an isomorphism and in particular an injective map. However, this would mean that p is injective, and so we have a contradiction. Hence $m = n$.

If S is infinite and T is infinite, then there's nothing for us to show.

Finally, suppose without loss that S is finite but T is infinite. Then we will write $R^{\oplus S}$ again as R^n.

In particular, we have the following chain of maps:

$$R^{n+1} \to R^n \cong R^{\oplus T} \to R^{n+1}$$

where the maps from R^{n+1} to R^n and $R^{\oplus T}$ to R^{n+1} are all standard projections. This is surjective, hence Theorem 2.7 tells us that this is an isomorphism and in particular all the projection maps are injective maps, which is clearly a contradiction. ■

Thus, we have proven that the rank of free modules are well-defined. Now we will stop for a moment to appreciate the thematic parallels between free modules and vector spaces:

- Every k-vector space is isomorphic to some direct sum $k^{\oplus S}$ with a basis, and every basis has the same dimension.
- Every free R-module is isomorphic to some direct sum $R^{\oplus S}$ with a basis, and every basis has the same rank.

In Linear Algebra, we could construct matrices of well-defined dimensions with respect to basis. In the world of finitely generated free modules, we can do the exact same thing!

Definition 2.9. The **standard basis vectors** of R^n, denoted $e_1, ..., e_n$, are exactly

$$e_1 = (1, 0, ..., 0), e_2 = (0, 1, ..., 0), ..., e_n = (0, 0, ..., 1)$$

We observe that if M is a free R-module of rank m, then $M \cong R^m$. In particular, any isomorphism $f : M \to R^m$ is equivalent to a choice of basis of M where the basis vectors $v_1, ..., v_m$ are

$$v_1 = f^{-1}(e_1), ..., v_m = f^{-1}(e_m)$$

Thus, for free R-modules M, N of rank m and n respectively, we can identify the collection of R-linear maps between M, N as $Hom_R(R^m, R^n)$ instead.

Just like how we can identify matrices from k^m to k^n in Linear Algebra, we can also identify elements of $Hom_R(R^m, R^n)$ in the same way!

Definition 2.10. We define $\mathcal{M}_{n,m}(R)$ as the collection of matrices of dimension $n \times m$, where every component of the matrix is an element of R.

We can identify $\mathcal{M}_{n,m}(R)$ with $Hom_R(R^m, R^n)$ as follows:

- For any matrix $M \in \mathcal{M}_{n,m}(R)$, we identify the i-th column vector of M, say v_i, as

  $$e_i \to v_i$$

  The map of the basis $e_1, ..., e_m$ to $v_1, ..., v_m$ extends to an unique R-module homomorphism.
- For any R-module homomorphism $f : R^m \to R^n$, we can create a matrix whose column vectors are the image of the standard basis vectors $e_1, ..., e_m$ of R^m.

Corollary 2.11. As R-modules, we have the following isomorphism given by the identification as above:

$$\mathcal{M}_{n,m}(R) \cong Hom_R(R^m, R^n)$$

Furthermore, matrix multiplication corresponds exactly to compositions of R-module homomorphisms.

Many of our favorite definitions on matrices carries over similarly. In particular, we will focus our attention on invertibility of these matrices.

Definition 2.12 (Invertible Matrix)**.** Let $M \in \mathcal{M}_{n,n}(R)$, we say M is invertible if there exists some matrix $N \in \mathcal{M}_{n,n}(R)$ such that

$$M \cdot N = NM = I$$

where I is the diagonal matrix whose entries are all 1_R.

In Linear Algebra, we know that a matrix is invertible if and only if its determinant is 0. We have a very similar notion of determinants for free modules:

Definition 2.13. The determinant map det : $End_R(R^n) \to R$ is defined as follows, for any $\alpha \in End_R(R^n)$, we identify α with a matrix $A = (a_{ij}) \in \mathcal{M}_{n,n}(R)$ then,

$$det(\alpha) := \sum_{\pi \in S_n} \text{sgn}(\pi) a_{1,\pi(1)} ... a_{n,\pi(n)}$$

Proposition 2.14. Let $\alpha, \beta \in End_R(R^n)$, then det$(\alpha \circ \beta) = det(\alpha)det(\beta)$.

Proof. The standard proof in Linear Algebra transitions seamlessly here. See 10.40 of Axler [Axl15] for a proof in the case of Linear Algebra, the generalization to modules is left as an exercise to the reader. ■

Theorem 2.15. Let F be a free R-module of rank n and let $\alpha \in End_R(F)$, then α is invertible if and only if $det(\alpha)$ is invertible.

Proof. **Suppose that α is invertible**, then there exists some $\beta \in End_R(F)$, such that $\alpha \circ \beta = i$ and $\beta \circ \alpha = i$ where $i \in End_R(F)$ is the identity R-endomorphism.

Then we know that $det(i) = det(\alpha \circ \beta) = det(\alpha)det(\beta)$.

Recall that the determinant map is a valid homomorphism, meaning that would be mapped to the multiplicative identity of R, so $det(i) = 1_R$. But this means that $1_R = det(\alpha)det(\beta)$.

SImilarly, since $i = \beta \circ \alpha$, this also means that $1_R = det(\beta)det(\alpha)$. So this means that $det(\beta)$ is the multiplicative inverse of $det(\alpha)$. Therefore, $det(\alpha)$ is invertible.

Suppose that $det(\alpha)$ is invertible, then let A be the matrix representation of α, now consider the adjugate matrix of A, adj(A), which is defined to be the transpose of A's cofactor matrix.

Then we know from linear algebra that the product of adj(A) and A yields diagonal matrix whose entries are the determinants of A. In particular:

$$adj(A)A = Aadj(A) = det(A)I$$

Since the determinant of A is invertible, this means that:

$$(det(A)^{-1}adj(A))A = A(det(A)^{-1}adj(A)) = I$$

Now let β be the R-endomorphism correspondent to the determinant $det(A)^{-1}adj(A)$. Since $(det(A)^{-1}adj(A))A = A(det(A)^{-1}adj(A)) = I$, their correspondent linear transformations also holds the relationship:

$$\beta \circ \alpha = \alpha \circ \beta = i$$

where i is the identity R-endomorphism. Thus, α has a valid multiplicative inverse, so α is invertible. ■

Remark 2.16. Thus, we see that the fact that matrices in vector spaces are invertible if and only if they have non-zero determinant is really just due to the fact that every non-zero element of a field is invertible.

In fact, we can recover another amazing property of linear algebra using this.

Proposition 2.17. Let F be a free R-module of rank n and $\alpha \in End_R(F)$, then α is a surjective if and only if det(α) is a unit.

Proof. **Suppose that $det(\alpha)$ is a unit**, then it is inveritble, and we know that means that α is invertible. We know that α is invertible if and only if it's bijective. Thus, α is surjective.

For the backward direction, **suppose $det(\alpha)$ is not a unit**, then we know that it is not invertible, so it's not bijective. Therefore, α is either not surjective or not injective.

If α is not surjective, then we are done. If α is not injective but is surjective, we know from Theorem 2.7 that α is actually an isomorphism, so we have a contradiction. ■

3 Smith Normal Forms and the Structure Theorm

In this section we will talk about the Smith Normal Forms of a finitely generated free modules over a principal ideal domain R. This will prove to be really helpful when computing homologies over $\mathbb{Z}$ down the line.

Since our main goal is to apply this on $\mathbb{Z}$, which is an Euclidean Domain, we will focus our discussion only on **Euclidean Domains**. The reader will have some fun trying to generalize this to a PID. To be frank, the examples of PIDs that are not Euclidean Domains are few and far between, and most PIDs we care about are all Euclidean Domains.

Definition 3.1. Let R be a principal ideal domain and $A \in \mathcal{M}_{m,n}(R)$ be a matrix. Then if there exists invertible matrices $S \in \mathcal{M}_{m,m}(R)$ and $T \in \mathcal{M}_{n,n}(R)$ such that

$$SAT = \begin{bmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{bmatrix}$$

where r is the rank of the matrix, $d_1, ..., d_r$ are unique up to a multiplication of unit, and for all i

$$d_i \mid d_{i+1}$$

Then, the d_i's are called the **elementary divisors of** A, and the matrix SAT is called the **Smith Normal Form** of A. Note that SAT is still a $m \times n$ matrix here, the diagram above may have been misleading.

It's not obvious that such Smith Normal Form need to exist at all. It is our goal in this section to prove its existence and provide an algorithm to compute it explicitly. The proof we are outlining here is done referencing Silverman in [Sil22].

Definition 3.2. Let R be a ring, and $A \in \mathcal{M}_{n,m}(R)$, we definie the **elementary matrix operations** on A as the following valid moves:

- Swap two rows (resp. columns) of A
- Let $r \in R$, we can add the row (resp. column) vector multiplied by r to any other row (resp. column).

We recall that there are exactly the standard techniques we have used in the process of Gaussian Elimination, which produces two companion invertible square matrices during the process.

Proposition 3.3. Every matrix over a field has a Smith Normal Form by using a series of elementary matrix operations.

Proof. Apply the methods of Gaussian Elimination to reduce the matrix such that it only has non-zero entries on the diagonal and order them appropriately. Since we are in a field, every non-zero element divides one another, hence we have obtained our desired Smith Normal Form. ■

The process of reducing a matrix over an Euclidean Domain into a Smith Normal Form is similar.

Theorem 3.4 (Existence)**.** Let R be an Euclidean domain with size function $\sigma : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$, and $A \in \mathcal{M}_{m,n}(R)$, then A has a Smith normal form.

Proof. This proof is due to Silverman in [Sil22]. If A is the zero matrix, then we are done. Otherwise, suppose A is non-zero, then consider the function

$$\mu : \mathcal{M}_{m,n}(R) \to \mathbb{Z}_{\geq 0} : \mu(M) = \min\{\sigma(M_{ij}) \mid M_{ij} \neq 0_R\}$$

Then we present an algorithm as follows:

1. First we perform a series of row swaps and column swaps on A such that the upper left corner entry $\sigma(A_{11})$ is $\mu(A)$.
2. If any element of A is not divisible by A_{11}, we can perform a series of elementary operations to create a new matrix A' such that
$$\mu(A') < \mu(A)$$
We can do this because a Euclidean Domain gives us the ability to create non-zero remainder r if there's some A_{ij} such that A_{11} does not divide A_{ij} (in the sense that $A_{ij} = A_{ii} \cdot q + r$. Then by definition we would have that $\sigma(r) < \sigma(A_{ii})$, and we can reduce the A_{ij} to its remainder via a series of elementary matrix operations. This new matrix A' will be less than A under μ because $\sigma(r) < \sigma(A_{ii})$.

We note that this process terminates eventually, this is because if it does not, then we have a chain of matrices $A, A', A'', ...$ such that
$$\mu(A) > \mu(A') > \mu(A'') > ...$$
But since μ is a non-negative valued integer function, the Well Ordering Principle tells us that this chain cannot exist. Hence eventually, we will transform A into some matrix B such that every entry of B is divisble by B_{11}.

If B is the zero matrix, then we are done. Otherwise, since B_{11} is non-zero and divides every element of the matrix, then we can reduce the matrix so that the first row and the first column of B all become 0 except for the component B_{11}. We then obtain the following matrix:

$$\tilde{B} = \left(\begin{array}{c|c} B_{11} & 0 \\ \hline 0 & B_{11} \cdot C \end{array}\right)$$

If C is the zero matrix, we are done. Otherwise, we can repeat this process on C (via induction on smaller dimension) to eventually decompose C down to the following matrix:

$$\tilde{B} = \left(\begin{array}{cc|c} B_{11} & 0 & \\ 0 & B_{11}B_{22} & 0 \\ \hline \multicolumn{2}{c|}{0} & B_{11}B_{22} \cdot C' \end{array}\right)$$

Note that any elementary matrix operation done on C does not affect the other entries of $\tilde{B}$ when viewed as a submatrix. We repeat this process repeatedly until we are done.

This series of column and row reductions will create the assoicated two matrices S and T respectively.

■

We will post pone the proof of uniqueness until Theorem 3.11. First, we will make the following observation:

Lemma 3.5. Let A, B, C be modules over a ring R and R-module homomorphisms $f : A \to B$ and $g : B \to C$, if furthermore that g is injective, then there is an exact sequence

$$0 \to Coker(f) \to_{\phi} Coker(g \circ f) \to_{\psi} Coker(g) \to 0$$

where the map $\phi : Coker(f) \to Coker(g \circ f)$, where from $B/im(f)$ to $C/im(g \circ f)$, we send

$$x + im(f) \mapsto g(x) + im(g \circ f)$$

The map from $Coker(g \circ f) \to Coker(g)$ is given by the projection $C/im(g \circ f)$ to $C/im(g)$ as $im(g \circ f) \subseteq im(g)$:

$$x + im(g \circ f) \mapsto x + im(g)$$

Proof. It suffices for us to check that ϕ is injective, ψ is surjective, and $im(\phi) = ker(\psi)$.

For injectivity of ϕ, suppose $\phi(x + im(f)) = 0 + im(g)$, then this implies that $g(x) \in im(g \circ f)$. Since g is injective, this can only happen if $x \in im(f)$, hence $x + im(f) = 0 + im(f)$, so the kernel of ϕ is trivial.

For surjectivity of ψ, for any $y + im(g) \in C/im(g)$, clearly $\psi(y + im(g \circ f)) = y + im(g)$.

Finally, to show that $im(\phi) = ker(\psi)$. We first note that for all $x + im(f) \in Coker(f)$,

$$\psi(\phi(x + im(f)) = \psi(g(x) + im(g \circ f)) = g(x) + im(g)$$

Clearly $g(x) \in im(g)$, so the term is 0, hence $im(\phi) \subseteq ker(\psi)$.

Conversely, suppose $y + im(g \circ f) \in ker(\psi)$, then

$$\psi(y + im(g \circ f)) = y + im(g) = 0 + im(g) \implies y \in im(g)$$

Thus, there exists some element $x \in B$ such that $g(x) = y$, but this means that

$$\phi(x + im(f)) = g(x) + im(g \circ f) = y + im(g \circ f)$$

Thus, we have that $ker(\psi) \subseteq im(\phi)$. ■

Definition 3.6. Let $A \in \mathcal{M}_{m,n}(R)$, we say the **cokernel** of A is the cokernel of the associated R-module homomorphism of A.

The reason why we are interested in cokernels is because Smith Normal Forms are actually invariant under them!

Proposition 3.7 (Invariance of Cokernel under SNF)**.** Given a matrix $A \in \mathcal{M}_{m,n}(R)$, and let SAT be its smith normal form, then

$$Coker(A) \cong Coker(SAT)$$

Proof. Let f, α, g be its associated linear transformation of S, A, T respectively, we note that α and $g \circ \alpha \circ f$ are all linear transformations from R^n to R^m.

Note that since g and f are bijective (as they are invertible), we have that

$$coker(g) \cong 0, coker(f) \cong 0$$

By Lemma 3.5, we have the following exact sequences

$$0 \to coker(\alpha \circ f) \to coker(g \circ (\alpha \circ f)) \to coker(g) \to 0$$

Since $coker(g) = 0$, we obtain the following exact sequence

$$0 \to coker(\alpha \circ f) \to coker(g \circ (\alpha \circ f)) \to 0$$

It then follows that

$$coker(\alpha \circ f) \cong coker(g \circ (\alpha \circ f))$$

Finally, since f is bijective, we know that

$$im(\alpha \circ f) = im(\alpha)$$

Hence, we have that

$$coker(g \circ \alpha \circ f) \cong= coker(\alpha \circ f) = coker(\alpha)$$

■

Lemma 3.8. Let R be a PID and M be a finitely generated module over R, then every submodule of M is also finitely generated.

Proof. We will first show that every principal ideal domain R satisfies an ascending chain condition in the sense that, suppose there's a chain of ideals

$$(a_1) \subseteq (a_2) ... \subseteq (a_n) \subset ...$$

Then there exists some $N \in \mathbb{N}$ such that

$$(a_N) = (a_{N+1}) = ...$$

In other words, every PID is Noetherian. Indeed, consider the set S defined to be the union

$$S := \bigcup_{i=1} (a_i)$$

Then S is in fact an ideal of R. Since R is a PID, there exist some element a such that $S = (a)$. Then we note that a has to lie in some (a_N). Hence all ideals after (a_N) are the same.

It is a general commutative algebra fact that a finitely generated module M over a Noetherian ring is also Noetherian, ie. M satisfies the ascending chain condition on its submodules. It is another general commutative algebra fact that every submodule of a Noetherian module is finitely generated.

The reader may refer to Chapter 6 of Atiyah and MacDonald [AM69] if they wish to learn more about the details. ■

Corollary 3.9 (Structure Theorem of Finitely Generated Modules over an Euclidean Domain)**.** Let R be an Euclidean Domain and M be a finitely generated module over R, then M is isomorphic to the cokernel of some matrix $A \in \mathcal{M}_{m,n}(R)$. Furthermore, writing out the Smith Normal Form of A with elementary divisors $d_1, ..., d_r$,

$$M \cong coker(A) \cong coker(SAT) = R^{m-r} \oplus \frac{R}{(d_1)} \oplus ... \oplus \frac{R}{(d_r)}$$

Proof. Let $x_1, ..., x_m$ be the generators of M, then consider the R-module homomorphism determined by

$$f : R^m \to M, f(e_1) = x_1, ..., f(e_m) = x_m$$

Since R is an Euclidean Domain, it is a PID, so every submodule of R^m is finitely generated by Lemma 3.8. In particular, this means that $ker(f)$ is finitely generated with say $y_1, ..., y_n$.

hen consider the matrix $A \in \mathcal{M}_{m,n}(R)$ whose column vectors are given by $y_1, ..., y_n$. Let α be the linear transformation associated with A, then we claim we have the following exact sequence:

$$R^n \to_\alpha R^m \to_f M \to 0$$

Clearly f is surjective, so it remains for us to check that $ker(f) = im(\alpha)$, but this follows immediately from the construction of A, so we are done.

Now since the sequence above splits, we have that

$$M \cong \frac{R^m}{im(\alpha)} = coker(A)$$

The explicit form of M follows directly from Propostion 3.7 and the understanding that SAT represents a R-module homomorphism that sends the standard basis vectors $e_1, ..., e_m$ to

$$e_1 \mapsto (d_1, 0, ..., 0), e_2 \mapsto (0, d_2, 0, ..., 0), ..., e_r \mapsto (0, ..., 0, d_r, 0, ..., 0), e_{r+1} \mapsto 0, ..., e_m \mapsto 0$$

■

Note that the usual version of the structure theorem above also has a uniqueness statement, but we note that this uniqueness statement follows exactly from the uniqueness of Smith Normal Forms.

We just need one last definition:

Definition 3.10. Let M be a module over R, we define the submodule $Tor(M) \subseteq M$ as

$$Tor(M) \coloneqq \{x \in M \mid r \cdot x = 0 \text{ for some non-zero } r \in R\}$$

We define the annihilator ideal $Ann(M) \subseteq R$ as

$$Ann(M) \coloneqq \{r \in R \mid r \cdot x = 0 \forall x \in M\}$$

We will now only use the existence part of our structure theorem to prove the uniqueness of Smith Normal Forms:

Theorem 3.11 (Uniqueness of SNF)**.** Let R be an Euclidean domain and $A \in \mathcal{M}_{m,n}(R)$, then the Smith normal form of A is unique up to units.

Proof. Let $d_1, ..., d_r$ and $e_1, ..., e_t$ be the elementary divisors of two possible Smith Normal Forms of A.

From Proposition 3.7, we know that the cokernel induced by any two possible Smith Normal Forms must be isomorphic. From Corollary 3.9, we know exactly what the isomorphism would look like:

$$coker(A) \cong R^{k_1} \oplus \frac{R}{(d_1)} \oplus ... \oplus \frac{R}{(d_r)} \cong R^{k_2} \oplus \frac{R}{(e_1)} \oplus ... \oplus \frac{R}{(e_t)}$$

We note that if $M \cong N$, then $M/Tor(M) \cong N/Tor(N)$. Thus, we note that $Tor(R^{k_1} \oplus \frac{R}{(d_1)} \oplus ... \oplus \frac{R}{(d_r)}) = \frac{R}{(d_1)} \oplus ... \oplus \frac{R}{(d_r)}$ and $Tor(R^{k_2} \oplus \frac{R}{(e_1)} \oplus ... \oplus \frac{R}{(e_t)}) = \frac{R}{(e_1)} \oplus ... \oplus \frac{R}{(e_t)}$. From this we obtain an isomorphism

$$R^{k_1} \cong R^{k_2}$$

Then Theorem 2.8, we know that $k_1 = k_2$ because rank is well-defined.

As for the elementary divisors, we wish to show that $r = t$, and that up to some reordering, d_i and e_i differ by a unit. Now we have the following isomorphism by removing R^{k_1} and R^{k_2} on both sides:

$$\frac{R}{(d_1)} \oplus ... \oplus \frac{R}{(d_r)} \cong \frac{R}{(e_1)} \oplus ... \oplus \frac{R}{(e_t)}$$

Since we know that $d_1|...|d_r$ and $e_1|...|e_t$, so the annhilator of the module on the left hand side must be (d_r) and the annhilator of the module on the right hand side must be (e_t). The annihilator is the same (even set wise) across isomorphisms, so we have that $(d_r) = (e_t)$.

This means that $\frac{R}{(d_r)} \cong \frac{R}{(e_t)}$, so we are left with the isomorphism:

$$\frac{R}{(d_1)} \oplus ... \oplus \frac{R}{(d_{r-1})} \cong \frac{R}{(e_1)} \oplus ... \oplus \frac{R}{(e_{t-1})}$$

If $r \neq t$, we can keep repeating this argument and remove terms of the direct sum on both sides until we obtain an isomorphism between the zero module and a non-zero module, which is a contradiction, hence $r = t$.

Then we have that

$$\frac{R}{(d_1)} \oplus ... \oplus \frac{R}{(d_r)} \cong \frac{R}{(e_1)} \oplus ... \oplus \frac{R}{(e_r)}$$

And again comparing the annihilator ideal tells us that $(d_r) = (e_r)$, so d_r and e_r differ by a unit. Then we can remove both terms and repeat on d_{r-1} and e_{r-1}, and so on.

This concludes the proof of uniqueness. ■

4 Computing Simplicial Homologies

We will discuss an algorithm to compute the simplicial homology of a given finite Δ-complex using Smith Normal Forms. We especially thank [Cam] for references in this section.

Let X be a finite Δ-complex, then we have the following sequence

$$C_{n+1}(X) \xrightarrow{\partial_{n+1}} C_n(X) \xrightarrow{\partial_n} C_{n-1}(X)$$

where $\partial_n \circ \partial_{n+1} = 0$. We defined in class that the n-th homology group of X is exactly

$$H_n(X) := \frac{ker(\partial_n)}{im(\partial_{n+1})}$$

But we note that each chain group is by definition the free abelian group on the number of simplexes of its respective dimension. So in other words, $C_k(X) \cong \mathbb{Z}^{a_k}$ for some $a_k \in \mathbb{Z}_{\geq 0}$ for all $k \geq 0$.

In other words, really our boundary maps are just $\mathbb{Z}$-module homomorphisms between free $\mathbb{Z}$-modules:

$$\mathbb{Z}^{a_{n+1}} \xrightarrow{\partial_{n+1}} \mathbb{Z}^{a_n} \xrightarrow{\partial_n} \mathbb{Z}^{a_{n-1}}$$

In particular, we can represent the boundary maps as integer matrices! Indeed, let B be the matrix for ∂_n and A be the matrix for ∂_{n+1}. Then we note that

$$H_n(X) \subseteq \frac{\mathbb{Z}^{a_n}}{im(\partial_{n+1})} = coker(A)$$

From Section 3, we know exactly what the cokernel should be:

$$coker(A) \cong \mathbb{Z}^{a_n - \text{rank}(A)} \oplus \frac{\mathbb{Z}}{(d_1)} \oplus ... \oplus \frac{\mathbb{Z}}{(d_r)}$$

where $d_1|...|d_r$ are the elementary divisors of A.

The question is then, how close are we to finding what $\frac{ker(\partial_n)}{im(\partial_{n+1})}$ is? Well it turns out we are not far away at all:

$$H_n(X) \cong \mathbb{Z}^{a_n - \text{rank}(A) - \text{rank}(B)} \oplus \frac{\mathbb{Z}}{(d_1)} \oplus ... \oplus \frac{\mathbb{Z}}{(d_r)}$$

In the remainder of this section, we will prove that the equation above is indeed true. Then, we will discuss in practice how this algorithm would be implemented.

Lemma 4.1. Let A, B, C be R-modules and suppose the following sequence is exact:

$$0 \to A \to_i B \to_f C \to 0$$

Then if C is free, then the sequence splits.

Proof. Indeed, consider the map $g : C \to B$ as follows. Consider the basis $\{e_i\}$ of C, then since f is surjective, there exist $\{x_i\}$ such that $f(x_i) = e_i$. We will fix that list, then we construct g by

$$g(e_i) = x_i$$

Then we note that $f \circ g = id_C$. Now consider the map

$$h : A \oplus C \to B, h(a, c) = i(a) + g(c)$$

We claim that h is in fact an isomorphism. Indeed, suppose $h(a, c) = 0$, then $i(a) + g(c) = 0$, so in particular $0 = f(0) = f(i(a)+g(c)) = f(i(a))+f(g(c)) = 0+f(g(c)) = c$, hence $c = 0$. So we have that $h(a, c) = i(a) = 0$.

Since i is injective, $a = 0$. Thus $(a, c) = (0, 0)$.

Now for surjectivity, for any $b \in B$, we want to find $a \in A, c \in C$ such that $b = i(a) + g(c)$, then $i(a) = b - g(f(b))$ and $g(c) = g(f(b))$ will do. It remains for us to show that i is actually surjective on $b - g(f(b))$. We know that $im(i) = ker(f)$, so it suffices for us to check if f sends this to 0.

Indeed, we have that

$$f(b - g(f(b))) = f(b) - f(g(f(b)) = f(b) - f(b) = 0$$

Thus, h is a valid isomorphism!

One can then show that $h^{-1} : B \to A \oplus C$ is exactly the isomorphism that will make the diagram required by a split exact sequence to commute. For the purposes of our document, we only really need the isomorphism between B and $A \oplus C$, so we will leave the details here to the reader. ■

Theorem 4.2. Any submodule of $\mathbb{Z}^n$ is free.

Proof. We will first prove that any submodule of $\mathbb{Z}^n$ is free, We will do this by induction. When $n = 0$, we are done. When $n = 1$, all non-zero submodules of $\mathbb{Z}$ are exactly the ideals of $\mathbb{Z}$, which are all single-generated. Indeed, let $I = (a)$ be an ideal of $\mathbb{Z}$, then the map

$$f : \mathbb{Z} \to I, x \mapsto a \cdot x$$

is a $\mathbb{Z}$-module isomorphism. Thus, every non-zero submodle of $\mathbb{Z}$ is free of rank 1.

Now suppose by our inductive hypothesis that this holds up to $n = k$. Then let N be a submodule of $\mathbb{Z}^{k+1}$ with basis $e_1, ..., e_k, e_{k+1}$. Let M be the submodule generated by $e_1, ..., e_k$ instead and consider $M \cap N \subseteq M$. By induction on $n = k$, we know that $M \cap N$ is a free $\mathbb{Z}$-module.

Now recall that $\mathbb{Z}$-modules are just abelian groups, then the Second Isomorphism Theorem tells us that

$$\frac{N}{N \cap M} \cong \frac{M + N}{M} \subset \frac{\mathbb{Z}^{k+1}}{M} \cong \mathbb{Z}$$

So in other words, $\frac{N}{N \cap M}$ is a submodule of $\mathbb{Z}$ and is hence free by our inductive hypothesis. So we obtain the following exact sequence:

$$0 \to N \cap M \to_i N \to_\pi \frac{N}{N \cap M} \to 0$$

In particular since $\frac{N}{N \cap M}$ is free, Lemma 4.1 tells us that the sequence splits, so $N \cong (N \cap M) \oplus \frac{N}{N \cap M}$ is isomorphic to a direct sum of free modules. Hence N is also free. ■

Remark 4.3. Note that there is a Second Isomorphism Theorem for Modules, and a very similar argument shows the same theorem for finitely generated free modules over a PID.

Corollary 4.4. For any homomorphism $f : \mathbb{Z}^n \to \mathbb{Z}^m$ gives a **split exact sequence**:

$$0 \to ker(f) \to \mathbb{Z}^n \to im(f) \to 0$$

Hence $\mathbb{Z}^n \cong ker(f) \oplus im(f)$.

Proof. By Theorem 4.2, we know that $im(f)$ is free, so this is a straight forward application of Lemma 4.1. ■

Now we are ready to prove our main result!

Theorem 4.5. Let $p, q, r \in \mathbb{Z}_{\geq 0}$ and $\alpha : \mathbb{Z}^p \to \mathbb{Z}^q$ and $\beta : \mathbb{Z}^q \to \mathbb{Z}^r$ be $\mathbb{Z}$-module homomorphisms such that $\beta \circ \alpha = 0$. Let A, B the matrix representation of α and β respectively, then

$$\frac{ker(\beta)}{im(\alpha)} \cong \mathbb{Z}^{q - \text{rank}(A) - \text{rank}(B)} \oplus \frac{\mathbb{Z}}{(d_1)} \oplus ... \oplus \frac{\mathbb{Z}}{(d_r)}$$

where $d_1 | ... | d_r$ are the elementary divisors of A given by the Smith Normal Form.

Proof. We wish to construct a homomorphism $\phi : coker(\alpha) \to \mathbb{Z}^r$ such that the following diagram commutes

$$\begin{tikzcd}
\mathbb{Z}^q \arrow[r, "\beta"'] \arrow[d, "\pi"'] & \mathbb{Z}^r \\
coker(\alpha) \arrow[ur, "\exists \phi"] &
\end{tikzcd}$$

Indeed, the most obvious choice is to define

$$\phi(x + im(\alpha)) = \beta(x)$$

This is clearly a module homomorphism, so it remains for us to show this is well-defined. Indeed, for any $x+im(\alpha) = y + im(\alpha)$, this happens when $x - y \in im(\alpha)$, then since $im(\alpha) \subset ker(\beta)$, $\beta(x - y) = 0$, hence

$$\phi(x + im(\alpha)) - \phi(y + im(\alpha)) = \phi((x - y) + im(\alpha)) = \beta(x - y) = 0$$

Thus, we have construct a well-defined module homomorphism $\phi : coker(\alpha) \to \mathbb{Z}^r$. Clearly, $ker(\phi)$ is isomorphic to $\frac{ker(\beta)}{im(\alpha)}$ by identifying $\frac{ker(\beta)}{im(\alpha)}$ as $\{x + im(\alpha) \mid x \in ker(\beta)\} \subseteq coker(\alpha)$.

From Corollary 3.9, we know that the cokernel of α is exactly isomorphic to

$$coker(\alpha) = \frac{B}{im(\alpha)} \cong \mathbb{Z}^{q-\text{rank}(A)} \oplus \frac{\mathbb{Z}}{(d_1)} \oplus ... \oplus \frac{\mathbb{Z}}{(d_r)}$$

Now since

$$Tor(coker(\alpha)) = \frac{\mathbb{Z}}{(d_1)} \oplus ... \oplus \frac{\mathbb{Z}}{(d_r)}$$
$$Tor(\mathbb{Z}^r) = 0$$

We note that $Tor(coker(\alpha)) \subseteq \phi$, hence let ψ be the restriction of ϕ onto $\mathbb{Z}^{q-\text{rank}(A)}$, then

$$ker(\phi) = ker(\psi) \oplus \frac{\mathbb{Z}}{(d_1)} \oplus ... \oplus \frac{\mathbb{Z}}{(d_r)}$$

Now, $\psi : \mathbb{Z}^{q-rank(A)} \to \mathbb{Z}^r$ is a homomorphism between free $\mathbb{Z}$-modules, so Corollary 4.4 tells us that

$$\mathbb{Z}^{q-rank(A)} \cong ker(\psi) \oplus im(\psi) = ker(\psi) \oplus im(\beta)$$

In particular, since all the modules are free, we have

$$\text{rank}(ker(\psi)) = \text{rank}(\mathbb{Z}^{q-rank(A)}) - \text{rank}(\text{im}(\beta)) = q - rank(A) - rank(B)$$

Thus, we have that $ker(\psi) \cong \mathbb{Z}^{q-rank(A)-rank(B)}$. Thus, we conclude that

$$\frac{ker(\beta)}{im(\alpha)} \cong \mathbb{Z}^{q-\text{rank}(A)-\text{rank}(B)} \oplus \frac{\mathbb{Z}}{(d_1)} \oplus ... \oplus \frac{\mathbb{Z}}{(d_r)}$$

■

Question 4.6. Now that we have proven what the homology group $H_n(X)$ is. How would one in practice implement an algorithm to compute this?

We have implemented this program at `https://github.com/maroon-scorch/Computational-Homology`. We will explain the main idea and construction behind our algorithm here. There are several difficulties to implementing this:

1. How does one represent a Δ-complex in code?

2. How does one represent the homology group in code?
3. How does one find the integer matrix associated with each boundary map ∂_i?

Our first decision was to represent the finite Δ-complex X and the homology group $H_n(X)$ with the following data structures:

Definition 4.7. Let X be a finite Δ-complex with dimension n with f-vector $(f_0, ..., f_n)$ recording the number of simplex in each definition. Then we represent X as a list of entries which we will call L:

- L has length $n + 1$ in total.
- Each entry of L is also a list.
- The zero-th entry of L is a list of length f_0 where each entry is just the empty list. This list represents the list of vertices of X
- For all $0 < i \leq n$, the i-th entry is a list of length f_i. This list represents the list of i-dimensional simplices of X. For each simplex on line i, it should be represented by a list of indices, where the j-th index v of the simplex represents the j-th face of the simplex. The index value v means this face is the v-th simplex of line $i - 1$.

Note, the data structure behind this finite Δ-complex is exactly one of the ways on how they are implemented in `Sage` (see [Pal] for more details).

Example 4.8. The following 2-dimensional Δ-complex X given by the list

- $0 : []$
- $1 : [0, 0], [0, 0], [0, 0]$
- $2 : [0, 1, 2], [2, 1, 0]$

Pictorially, this structure only has 1 vertex, so all of its 3 edges start and end at the same point. Its two faces go in opposite orientations, hence their edges go in opposite directions. This is exactly the Δ-complex of a 2-torus.

Definition 4.9. Let X be a finite Δ-complex of dimension n, then for all $k > n$, $H_k(X) = 0$, so we don't need to address them. Now for any $0 \leq k \leq n$, Theorem 4.5 tells us that we can write

$$H_k(X) \cong \mathbb{Z}^{a_k} \oplus \frac{\mathbb{Z}}{d_1} \oplus ... \oplus \frac{\mathbb{Z}}{d_r}$$

Then we simply represent $H_k(X)$ as a tuple $(a_k, [d_1, ..., d_r])$. This is all the information we need to represent the homology group.

Now we want to find a way to find the integer matrix represented by the boundary maps explicitly:

Construction. Let f be the f-vector on X, let $\partial_k : C_k(X) \to C_{k-1}(X)$, write $C_k(X) \cong \mathbb{Z}^{f_k}$ and $C_{k-1}(X) \cong \mathbb{Z}^{f_k}$. We identify the ordered f_k simplex of dimension k with the standard basis vectors $e_1, ..., e_{f_k}$ of $C_k(X)$. We also identify similarly the ordered f_{k-1} simplex of dimension k with the standard basis vectors $g_1, ..., g_{f_{k-1}}$ of $C_{k-1}(X)$.

We will construct the matrix $f_{k-1} \times f_k$ dimensional integer $M(\partial_k)$ as follows:

- Let v_j be the j-th column vector of $M(\partial_k)$. Let F_j be the j-th k-dimensional simplex of X with faces of index $i_1, ..., i_{k+1}$ ordered as how it was given originally, then

$$v_j := \sum_{p=0}^{k} (-1)^p \cdot g_{i_1}$$

- In other words, the column factors are the alternating sums of the respective faces under the boundary map, when identified with the standard basis vectors.

The matrix formed $M(\partial_k)$ is indeed the matrix associated to ∂_i. ■

Putting it all together, our algorithm is as follow:

```
Data: A finite $\Delta$-complex of dimension $n$
Result: The homology groups $H_0(X), ..., H_n(X)$
1. Compute the $f$-vector of $X$;
2. For each $\partial_k : C_k(X) \to C_{k-1}(X)$, construct its boundary map $M(\partial_k)$ as described above;
3. Find the Smith Normal Form and rank of each $M(\partial_k)$;
4. Compute the homology groups $H_k(X)$ as in Theorem 4.5
```

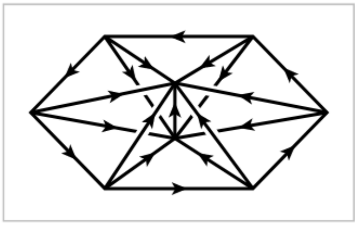
Algorithm 1: Computing Simplicial Homologies

5 Application: Construction of Lens Space

A particularly interesting example we will focus on are the construction of 3-dimensional Lens spaces. This is given as an example in Exercise 2.1.8 of Hathcer [Hat02]:

Example 5.1 (Hatcher Exercise 2.1.8)**.** We can construct the Δ-complex X of a 3-dimensional Lens space as follows:

1. Consider n tetrahedrons $T_1, ..., T_n$
2. Arrange the Tetrahedron as in the following figure (given in Hatcher):



3. Each T_i shares a common vertical face with its two neighbors T_{i-1} and T_{i+1} modulo n
4. The bottom face of each T_i is identified with the top face T_{i+1}

The claim is then that the simplicial homology groups of L_n are

$$H_0(L_n) = \mathbb{Z},\ H_1(L_n) = \mathbb{Z}/n\mathbb{Z},\ H_2(L_n) = 0,\ H_3(L_n) = \mathbb{Z}$$

and $H_k(L_n) = 0$ for all $k > 3$.

Here's how we algorithmically construct the Δ-Complex in our repository:

Construction. We will construct the entries from dimension 0 all the way to dimension 3.

In dimension 0, there are only 2 points in X up to identification, we label:

- 0 - the point at the center
- 1 - the point out at the polygon boundary

In dimension 1, there's a total of $n+2$ edges, n edges from the boundary connecting to the center, 1 edge connecting the bottom of the center to the top of the center, and 1 edge on the boundary. We will make the list of edges in that order:

- The first n edges should be labeled $[1, 0]$
- Then the next one should be labeled $[0, 0]$
- The last edge should be labeled $[1, 1]$

In dimension 2, the number of faces should be $2n$, where there are n faces on the top of the complex (ordered 0, 1, 1 vertex counter-clock wise), and n faces squeedzed between the neighbors of the Tetrahedron (ordered 0, 0, 1 vertex counter-clock wise). We will make the list of faces in that order:

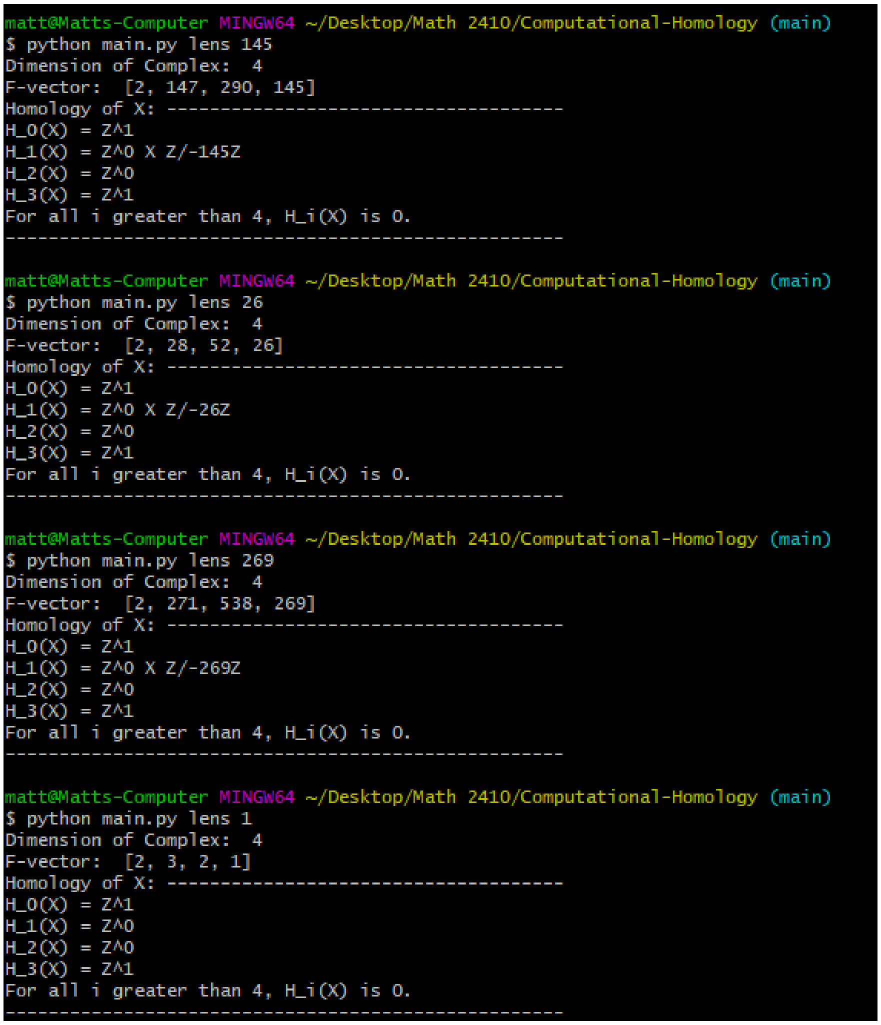
- The i-th item of first n faces should be labeled $[n+1, i+1 \mod n, i]$
- The i-th item of the second batch of n faces should be labeled $[i+1 \mod n, i, n]$

Finally, we have a list of n tetrahedrons (vertex ordered 0, 0, 1, 1) organized as follows:

- For T_i, let k be $i+1 \mod n$, then T_i should be labeled as $[k, i, n+k, n+i]$

This finished the construction of our Δ-complex. ■

Performing the algorithm on several inputs have worked:



```
matt@Matts-Computer MINGW64 ~/Desktop/Math 2410/Computational-Homology (main)
$ python main.py lens 145
Dimension of Complex:  4
F-vector:  [2, 147, 290, 145]
Homology of X: -------------------------------------
H_0(X) = Z^1
H_1(X) = Z^0 X Z/-145Z
H_2(X) = Z^0
H_3(X) = Z^1
For all i greater than 4, H_i(X) is 0.
----------------------------------------------------

matt@Matts-Computer MINGW64 ~/Desktop/Math 2410/Computational-Homology (main)
$ python main.py lens 26
Dimension of Complex:  4
F-vector:  [2, 28, 52, 26]
Homology of X: -------------------------------------
H_0(X) = Z^1
H_1(X) = Z^0 X Z/-26Z
H_2(X) = Z^0
H_3(X) = Z^1
For all i greater than 4, H_i(X) is 0.
----------------------------------------------------

matt@Matts-Computer MINGW64 ~/Desktop/Math 2410/Computational-Homology (main)
$ python main.py lens 269
Dimension of Complex:  4
F-vector:  [2, 271, 538, 269]
Homology of X: -------------------------------------
H_0(X) = Z^1
H_1(X) = Z^0 X Z/-269Z
H_2(X) = Z^0
H_3(X) = Z^1
For all i greater than 4, H_i(X) is 0.
----------------------------------------------------

matt@Matts-Computer MINGW64 ~/Desktop/Math 2410/Computational-Homology (main)
$ python main.py lens 1
Dimension of Complex:  4
F-vector:  [2, 3, 2, 1]
Homology of X: -------------------------------------
H_0(X) = Z^1
H_1(X) = Z^0
H_2(X) = Z^0
H_3(X) = Z^1
For all i greater than 4, H_i(X) is 0.
----------------------------------------------------
```

References

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to commutative algebra*. Westview Press, 1969.

[Axl15] Sheldon Jay Axler. *Linear algebra done right*. Springer, 2015.

[Cam] Omar Antolín Camarena. Using the smith normal form to compute homology.

[Hat02] Allen Hatcher. *Algebraic topology*. Cambridge University Press, 2002.

[Pal] John H Palmieri. Finite delta-complexes.

[Sil22] Joseph H. Silverman. *Abstract algebra: An integrated approach*. American Mathematical Society, 2022.

[Vas69] Wolmer V. Vasconcelos. On finitely generated flat modules. *Transactions of the American Mathematical Society*, 138:505–512, 1969.