Free Resolutions

1 Introduction

We want to "understand" mathematical objects using limited technology. For example, given a group G, we obtain a lot of information about G by just knowing its order |G|. For instance, if p is a prime such that p divides |G|, then the Sylow theorems tells us that there exists a p-Sylow subgroup of G. Another thing we get from knowing the order of a group is whether or not it is isomorphic to another group: if G and G are two groups such that $|G| \neq |H|$, then $G \ncong H$ (or in contrapositive form: if $G \cong H$ then |G| = |H|). This means that the order of a group is an invariant. Even though the order of a group is a nice invariant to have, it is not strong enough to determine the group completely: if |G| = |H|, then usually it's very difficult to determine whether $G \cong H$ or not.

There are similar tools for understanding rings and modules. -SSW

1.1 Focus of this class

1.1.1 Part I

In part I one of the class, we will focus on understanding the contents of the Hilbert Syzygy Theorem as well as giving a (partial) proof of it. Let us state the Hilbert Syzygy Theorem.

Theorem 1.1. (The Hilbert Syzygy Theorem) Let $R = k[X_1, ..., X_d]$ be the polynomial ring in d indeterminates over a field k and let I be the ideal in R generated by $f_1, ..., f_{\beta_1}$. Then there exists an exact sequence of the form

$$0 \longrightarrow R^{\beta_d} \longrightarrow \cdots \longrightarrow R^{\beta_i} \xrightarrow{\partial_i} R^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow R^{\beta_1} \xrightarrow{\partial_1} R \longrightarrow R/I \longrightarrow 0$$
 (1

The exact sequence (8) is called an **augmented free resolution of** R/I **over** R. If we remove R/I from (8), then we get a **free resolution of** R/I **over** R. We view the term R^{β_i} in (8) as sitting in **homological degree** i. The maps ∂_i in (8) are called **differentials**. We often simplify notation by writing (8) as (F, ∂) , where we think of F as a graded R-module whose homogeneous component in degree i is R^{β_i} and we think of R as a graded R-homomorphism R: R: R: R: R: R: R:

1.1.2 Part II

In part II, we will go over a bunch of examples. Here are two to consider now:

Example 1.1. Consider the case where R = k[X,Y] and $I = \langle X^2, XY \rangle$. Then we have the following short exact sequence of R-complexes

$$0 \longrightarrow R \xrightarrow{\begin{pmatrix} -Y \\ X \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} X^2 & XY \end{pmatrix}} R \longrightarrow R/I$$

Example 1.2. (Twisted Cubic) Consider the case where R = k[X, Y, Z, W] and $I = \langle XZ - Y^2, YW - Z^2, XW - YZ \rangle$. A free resolution of R/I is given by

$$0 \longrightarrow R^2 \xrightarrow{\begin{pmatrix} W & Z \\ Y & X \\ -Z & -Y \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} XZ-Y^2 & YW-Z^2 & WX-YZ \end{pmatrix}} R \longrightarrow R/I$$

Another very important example that we will consider is when $R = k[X_1, ..., X_d]$ and $I = \langle X_{i_1}, ..., X_{i_{\beta_1}} \rangle$. In this case, we can build a resolution explicitly, called the **Koszul complex of** R/I **over** R, named after Jean Louis Koszul. For example, consider $I = \langle X_1, X_2, X_3 \rangle$. Then the Koszul complex of R/I over R looks like

$$R \xrightarrow{\begin{pmatrix} X_1 \\ -X_2 \\ X_3 \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} 0 & -X_3 & -X_2 \\ -X_3 & 0 & X_1 \\ X_2 & X_1 & 0 \end{pmatrix}} R^3 \xrightarrow{\begin{pmatrix} (X_1 & X_2 & X_3) \\ -X_3 & 0 & X_1 \\ X_2 & X_1 & 0 \end{pmatrix}} R$$

$$e_{1,2,3} \longmapsto X_1 e_{2,3} - X_2 e_{1,3} + X_3 e_{1,2}$$

$$e_{2,3} \longmapsto X_2 e_3 - X_3 e_2$$

$$e_{1,3} \longmapsto X_1 e_3 - X_3 e_1$$

$$e_{1,2} \longmapsto X_1 e_2 - X_2 e_1$$

$$e_1 \longmapsto X_1 e_2 \longmapsto X_2 e_3 \longmapsto X_3 e_2$$

$$e_{3} \longmapsto X_3 e_3 \longmapsto X_3 e_3$$

1.1.3 Part III

If all f_j 's in Theorem (1.1) are homogeneous, then the resolution (8) can be built minimally and the β_i 's are independent of the choice of minimal free resolution. In this case, we call the $\beta_i = \beta_i^R(R/I)$ the ith **Betti number of** R/I **over** R, named after the Italian mathematician Enrico Betti. If J is another homogeneous ideal of R, and $\beta_i^R(R/I) \neq \beta_i^R(R/J)$ for some i, then $R/I \ncong R/J$. Thus the Betti numbers give us an invariant of R/I. However, just like in the case of orders in group theory, this invariant is not sufficiently strong enough to determine R/I: if $\beta_i^R(R/I) = \beta_i^R(R/J)$ for all i, then R/I may not be isomorphic to R/J.

In part III of the class, we will try to find finer technology. For instance, it turns out that the Koszul complex is a graded commutative *R*-algebra with the multiplication rule given by

$$e_A e_B = \begin{cases} 0 & \text{if } A \cap B = \emptyset \\ e_{A \cup B} & \text{else} \end{cases}$$

subject to the rule

$$e_A e_B = (-1)^{|A||B|} e_B e_A$$

where $A, B \subseteq \{1, ..., m\}$. Moreover, we have the Leibniz rule

$$\partial(e_A e_B) = \partial(e_A)e_B + (-1)^{|A|}e_A\partial(e_B).$$

This shows that the Koszul complex is a differential graded algebra (DGA) resolution.

2 Preliminary Material and Notation

Throughout these notes, let R be a commutative ring with identity. We also let $\mathbb{N} = \{0, 1, 2, \dots\}$ be the set of a natural numbers together with 0 (SSW: "My class, my rules").

2.1 Linear Algebra

2.1.1 Free Modules

Definition 2.1. Let *M* be an *R*-module.

- 1. A sequence $e_1, \ldots, e_n \in M$ is a **(finite) basis** for M if it generates M as an R-module and it is linearly independent over R, i.e. for every $m \in M$ there exists $r_1, \ldots, r_n \in R$ such that $m = \sum_{i=1}^n r_i e_i$, and if $a_1, \ldots, a_n \in R$ such that $\sum_{i=1}^n a_i e_i = 0$, then $a_i = 0$ for all i.
- 2. We say *M* is a **finite rank free** *R***-module** if it has a basis.

Example 2.1. R^n is the **standard free** R**-module of rank** n. It has as basis the **standard basis elements** e_i where e_i is the vector with 1 in the ith entry and 0 everywhere else.

Example 2.2. If I is a nonzero ideal in R, then R/I is not a free R-module. Indeed, if r is a nonzero element in I, then for all $s \in R$, we have $r\overline{s} = \overline{rs} = 0$ in R/I. In other words, "**torsion**" makes linear independence fail for elements of R/I when taking coefficients from R.

2.1.2 Universal Mapping Property of Free R-Modules

The universal mapping property of free R-modules can be stated as follows: Let F be a free R-module with basis $e_1, \ldots, e_n \in F$. For all R-modules M and for all $m_1, \ldots, m_n \in M$ there exists a unique R-module homomorphism $\varphi \colon F \to M$ such that $\varphi(e_i) = m_i$ for all $i = 1, \ldots, n$. In terms of diagrams, this is pictured as follows:

$$\{e_1,\ldots,e_n\} \hookrightarrow F$$

$$\downarrow_{\exists!\varphi}$$

$$M$$

Using the universal mapping property of free *R*-modules, let us prove the following theorem:

Theorem 2.1. If F and G are finite rank free R-modules with basis e_1, \ldots, e_n and f_1, \ldots, f_n respectively, then $F \cong G$.

Proof. By the universal mapping property of free *R*-modules there exists a unique *R*-module homomorphism $\varphi \colon F \to G$ such that $\varphi(e_i) = f_i$ for all $i = 1, \ldots, n$. Similarly, there exists a unique *R*-module homomorphism $\psi \colon G \to F$ such that $\psi(f_i) = e_i$ for all $i = 1, \ldots, n$. In particular, we see that $\psi \circ \varphi \colon F \to F$ satisfies $(\psi \circ \varphi)(e_i) = e_i$. But we also have $1(e_i) = e_i$ for all $i = 1, \ldots, n$, where $1 \colon F \to F$ is the identity map. Therefore by uniqueness of the map in the universal mapping property of free *R*-modules, we must have $\psi \circ \varphi = 1$. A similar argument shows that $\varphi \circ \psi = 1$.

Corollary. Let F be a free R-module with basis $e_1, \ldots, e_n \in F$. Then $F \cong R^n$.

Remark. Note that you can prove Theorem (2.1) without the universal mapping property of free *R*-modules, but the point is that you'd have to show well-definedness, linearity, etc... of the maps constructed. The point is that all of this is built into the universal mapping property of free *R*-modules.

2.1.3 Representing *R*-module Homomorphisms By Matrices

Let $\varphi: R^n \to R^m$ be an R-module homomorphism and let e_1, \ldots, e_n denote the **canonical basis** of R^n , i.e. $e_i = (0 \ldots, 1, \ldots 0)^{\top}$ where 1 is at the ith entry and 0 is in all other entries. Any $x \in R^n$ has a unique linear combination as $x = x_1 e_1 + \cdots + x_n e_n$ where $x_i \in R$. In particular, $\varphi(e_i)$ has a unique representation as

$$\varphi(e_j) = \sum_{i=1}^n a_{ij} e_i.$$

Writing x as a column vector [x] and using linearity of φ , we see that

$$\varphi(x) = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = [\varphi][x],$$

where $[\varphi] = (a_{ij})$ is an $m \times n$ matrix with entries in R. We call $[\varphi]$ the **matrix representation of** φ . Addition, scalar multiplication, and composition of R-module homomorphisms correspond to addition, scalar multiplication, and multiplication of matrices.

2.2 Noetherian Rings and Modules

Definition 2.2. An R-module M is said to be **finitely generated** if there exists a surjective R-module homomorphism from R^n to M for some $n \in \mathbb{N}$.

Theorem 2.2. The following conditions are equivalent:

- 1. Every ideal of R is finitely generated.
- 2. Ascending chain condition (acc) of ideals in R: given a chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots$$

of ideals in R, there exists $N \in \mathbb{N} = \{0, 1, 2, ...\}$ such that

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

- 3. Maximum condition for ideals in R: every non-empty set of ideals of R contains an element maximal with respect to containment.
- 4. For every $n \in \mathbb{N}$ every submodule of \mathbb{R}^n is finitely generated.
- 5. For every $n \in \mathbb{N}$, \mathbb{R}^n satisfies maximum condition on submodules.
- 6. Acc of on submodules of \mathbb{R}^n for every $n \in \mathbb{N}$.

Definition 2.3. *R* is said to be **Noetherian** if it satisfies any of the equivalent conditions of Theorem (2.2).

Theorem 2.3. (Hilbert Basis Theorem) If R is Noetherian then R[X] is also Noetherian.

Remark. More generally, if I is an ideal of $R[X_1, ..., X_n]$, then $R[X_1, ..., X_n]/I$ is Noetherian. In particular, $k[X_1, ..., X_n]/I$ is Noetherian since k is Noetherian.

2.3 Exact Sequences

Definition 2.4. A sequence of *R*-module homomorpisms

$$A \xrightarrow{\varphi} B \xrightarrow{\psi} C$$

is said to be **exact at** *B* if $Ker(\psi) = Im(\varphi)$. A sequence of *R*-module homomorphisms

$$\cdots \longrightarrow A_{i+1} \xrightarrow{\varphi_{i+1}} A_i \xrightarrow{\varphi_i} A_{i-1} \longrightarrow \cdots$$

is said to be **exact** if it is exact at every A_i . A **short exact sequence** is an exact sequence of the form

$$0 \longrightarrow A \stackrel{\varphi}{\longrightarrow} B \stackrel{\psi}{\longrightarrow} C \longrightarrow 0$$

2.3.1 Free Resolutions

Theorem 2.4. Assume that R is Noetherian and let M be a finitely generated R-module. Then there exists an exact sequence of the form

$$\cdots \longrightarrow R^{\beta_i} \xrightarrow{\partial_i} R^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow R^{\beta_1} \xrightarrow{\partial_1} R^{\beta_0} \longrightarrow M \longrightarrow 0$$
 (2)

Proof. First note that since M is finitely generated, there exists a surjective R-module homomorphism $\tau_0 \colon R^{\beta_0} \to M$. Denote $M_1 := \operatorname{Ker}(\tau_0)$ the kernel of τ_0 and denote $\iota_1 \colon M_1 \hookrightarrow R^{\beta_0}$ the inclusion map. Since R is Noetherian and M_1 is a submodule of R^{β_0} , we see that M_1 is finitely generated (by Theorem (2.2)). Therefore there exists a surjective homomorphism $\tau_1 \colon R^{\beta_1} \to M_1$. Let $\iota_1 \colon \operatorname{Ker}(\tau_0) \to R^{\beta_0}$ denote the inclusion map and let $\phi_1 := \iota_0 \circ \tau_1$. Continuing in this way, for each $i \in \mathbb{N}$, we construct short exact sequences of the form

$$0 \longrightarrow M_{i+1} \xrightarrow{\iota_{i+1}} R^{\beta_i} \xrightarrow{\tau_i} M_i \longrightarrow 0$$

where we denote $M_0 := M$. A standard argument in homological algebra says that we can connect these short exact sequences together to form the long exact sequence (2) where $\partial_{i+1} := \iota_i \circ \tau_{i+1}$.

Definition 2.5. The exact sequence (2) is called an **augmented free resolution of** *M*.

In general, free resolutions are hard to compute. However here are two examples to consider.

Example 2.3. Recall that the fundamental theorem of finitely generated abelian groups says that if G is an abelian group, then there exists $r \in \mathbb{Z}_{\geq 0}$ and $d_1, \ldots, d_n \in \mathbb{Z}_{> 1}$ such that

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_n$$
.

This boils down to the fact that there exists a free resolution of the form

$$0 \longrightarrow \mathbb{Z}^n \stackrel{\varphi}{\longrightarrow} \mathbb{Z}^{r+n} \longrightarrow G \longrightarrow 0$$

where the $(n + r) \times n$ matrix representation of φ has the form

$$[\varphi] = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & d_n \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Example 2.4. If *R* is an integral domain and *r* is a nonzero unit in *R*. Then we have the short exact sequence

$$0 \longrightarrow R \stackrel{\cdot r}{\longrightarrow} R \longrightarrow R/r \longrightarrow 0$$

If *R* is a PID, then these are all the resolutions.

Example 2.5. Let $R = k[X,Y]/\langle XY \rangle$ and let $M = R/\langle \overline{X} \rangle$. Then we have

$$\cdots \longrightarrow R \xrightarrow{\cdot \overline{X}} R \xrightarrow{\cdot \overline{Y}} R \xrightarrow{\cdot \overline{X}} R \longrightarrow R/r \longrightarrow 0$$

In fact, we can prove that this resolution does not stop. The idea is that straying away from polynomial rings makes this construction go bad.

2.3.2 Hilbert Syzygy Theorem

Theorem 2.5. (Hilbert Syzygy Theorem) Let $R = k[X_1, ..., X_d]$ with k a field and let M be a finitely generated R-module. Then there exists a free resolution

$$0 \longrightarrow R^{\beta_d} \longrightarrow \cdots \longrightarrow R^{\beta_i} \xrightarrow{\partial_i} R^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow R^{\beta_1} \xrightarrow{\partial_1} R^{\beta_0} \longrightarrow M \longrightarrow 0$$
 (3) with $\beta_i \geq 0$ for all i .

Remark. If d = 0, then R is just the field k and M is a k-vector space. If d = 1, then R is a PID. Since every submodule of a free R-module is free (when R is a PID), we see that the free resolution terminates at R^{β_1} . More variables require more work.

3 Graded Resolutions

Tracking finer information about certain resolutions. In this section, we assume that k is a field, R is a polynomial ring $R = k[X_1, ..., X_d]$.

Definition 3.1. Let *I* be an ideal in *R*. We say *I* is a **homogeneous** (or **graded**) ideal in *R* if it can be generated by homogeneous polynomials (not necessarily of the same degree).

Example 3.1. Consider the ring R = k[X,Y] and $I = \langle X^2 - XY^2, XY^2 \rangle$. Even though $X^2 - XY^2$ is not a homogeneous polynomial, the ideal I is still a homogeneous ideal. This is because $I = \langle X^2, XY^2 \rangle$.

Theorem 3.1. (Graded Hilbert Basis Theorem) If $I = \langle f_1, \dots, f_{\beta_1} \rangle$ where each f_i is homogeneous. Then there exists a free resolution

$$0 \longrightarrow R^{\beta_d} \longrightarrow \cdots \longrightarrow R^{\beta_i} \xrightarrow{\partial_i} R^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow R^{\beta_1} \xrightarrow{\partial_1} R \longrightarrow R/I \longrightarrow 0$$
 (4)

such that each differential ∂_i is represented by a matrix of homogeneous polynomials.

3.1 Examples of Graded Resolutions

Example 3.2. Consider the case where R = k[X, Y] and $I = \langle X^a, Y^b \rangle$ where $a, b \ge 1$. Then we have the following short exact sequence of R-complexes

$$0 \longrightarrow R \xrightarrow{\begin{pmatrix} -Y^a \\ X^b \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} X^a & Y^b \end{pmatrix}} R \longrightarrow R/I$$

This uses unique factorization of the indeterminates.

Example 3.3. Consider the case where R = k[X, Y] and $I = \langle X^a, XY, Y^b \rangle$ where $a, b \geq 2$. We claim that

$$0 \longrightarrow R^{2} \xrightarrow{\begin{pmatrix} -Y & 0 \\ X^{a-1} & Y^{b-1} \\ 0 & X \end{pmatrix}} R^{3} \xrightarrow{\begin{pmatrix} X^{a} & XY & Y^{b} \end{pmatrix}} R \longrightarrow R/I$$

is a free resolution of R/I. To see this, we first show $Ker(\partial_1) = Im(\partial_2)$. Let $(f, g, h)^{\top} \in Ker(\partial_1)$, so we have

$$X^a f + XYg + Y^b h = 0. (5)$$

Then (5) implies $Y|X^af$ which implies Y|f, and so $f=Yf_1$ for some $f_1 \in R$. Similarly, (5) implies $X|Y^bh$ which implies X|h, and so $h=Xh_1$ for some $h_1 \in R$. Thus we have

$$0 = X^a f + XYg + Y^b h$$

= $X^a Y f_1 + XYg + Y^b X h$
= $XY(X^{a-1} f_1 + g + Y^{b-1} h_1),$

and this further implies $X^{a-1}f_1 + g + Y^{b-1}h_1 = 0$. Solving for g, we find that $g = -X^{a-1}f_1 - Y^{b-1}h_1$. Therefore we see that

$$\begin{pmatrix} f \\ g \\ h \end{pmatrix} = \begin{pmatrix} Yf_1 \\ -X^{a-1}f_1 - Y^{b-1}h_1 \\ Xh_1 \end{pmatrix}$$
$$= f_1 \begin{pmatrix} Y \\ -X^{a-1} \\ 0 \end{pmatrix} + h_1 \begin{pmatrix} 0 \\ Y^{b-1} \\ X \end{pmatrix}$$
$$\in \operatorname{Im}(\partial_2).$$

In particular, we have $\operatorname{Im}(\partial_2) \supseteq \operatorname{Ker}(\partial_1)$ (and hence $\operatorname{Im}(\partial_2) = \operatorname{Ker}(\partial_1)$ since the reverse inclusion is already known). Finally, since R is an integral domain and since $(-Y, X^{a-1}, 0)^{\top}$ and $(0, Y^{b-1}, X)$ are linearly independent, we see that ∂_2 is injective.

3.2 Relation on the β_i

Note that the β_i in each of the previous examples satisfy the relations

$$\beta_0 - \beta_1 + \beta_2 = 0.$$

This actually happens in general:

Lemma 3.2. Let

$$0 \longrightarrow k^{\beta_d} \longrightarrow \cdots \longrightarrow k^{\beta_i} \xrightarrow{\partial_i} k^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow k^{\beta_1} \xrightarrow{\partial_1} k^{\beta_0} \longrightarrow 0$$
 (6)

be an exact sequence of k-vector spaces. Then

$$\sum_{i=0}^d (-1)^i \beta_i = 0.$$

Proof. Let $K_i := \text{Ker}(\partial_i)$ for all $0 \le i \le d$ and let $K_{-1} = 0$. Then for each $0 \le i \le d$, exactness at k^{β_i} in (6) implies exactness of

$$0 \longrightarrow K_i \hookrightarrow k^{\beta_i} \xrightarrow{\partial_i} K_{i-1} \longrightarrow 0.$$

Since the dimension function is additive on short exact sequences, we have $\beta_i = \dim(K_i) + \dim(K_{i-1})$. Therefore we have a telescoping series

$$\sum_{i=0}^{d} (-1)^{i} \beta_{i} = \sum_{i=0}^{d} (-1)^{i} (\dim(K_{i}) + \dim(K_{i-1}))$$
$$= (-1)^{d} \dim(K_{d}) + \dim(K_{-1})$$
$$= 0.$$

Theorem 3.3. Let I be a nonzero ideal in R and let

$$0 \longrightarrow R^{\beta_d} \longrightarrow \cdots \longrightarrow R^{\beta_i} \xrightarrow{\partial_i} R^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow R^{\beta_1} \xrightarrow{\partial_1} R^{\beta_0} \xrightarrow{\partial_0} R/I \longrightarrow 0$$
 (7)

be a free resolutions of R/I over R. Then

$$\sum_{i=0}^{d} (-1)^i \beta_i = 0.$$

Proof. Localizing R at $\langle 0 \rangle$ gives us a field $R_{\langle 0 \rangle} = k(X_1, \dots, X_d)$ since R is an integral domain. Since $I \neq 0$, there exists $s \in I \setminus \{0\}$ that is nonzero. We claim then that $(R/I)_{\langle 0 \rangle} = 0$. Indeed an element in $(R/I)_{\langle 0 \rangle}$ looks like \bar{r}/t where $r \in R$ and $t \in R \setminus 0$. Then

$$\frac{\overline{r}}{t} = \frac{\overline{sr}}{st} = \frac{\overline{0}}{st} = 0.$$

Therefore localizing our resolution at $\langle 0 \rangle$ (which is exact) gives us an exact sequence of vector spaces over the field $R_{\langle 0 \rangle}$:

$$0 \longrightarrow R_{\mathfrak{p}}^{\beta_d} \longrightarrow \cdots \longrightarrow R_{\mathfrak{p}}^{\beta_i} \xrightarrow{\partial_i} R_{\mathfrak{p}}^{\beta_{i-1}} \longrightarrow \cdots \longrightarrow R_{\mathfrak{p}}^{\beta_1} \xrightarrow{\partial_1} R_{\mathfrak{p}}^{\beta_0} \longrightarrow 0 \tag{8}$$

Now we apply Lemma (3.2) to obtain our desired result.