Syzygies of the apolar ideals of the determinant and permanent

Rowan Rowlands

October 2016

A thesis submitted for the degree of Bachelor of Philosophy (Honours)
at the Australian National University

Australian
National
University

Acknowledgments

There are a few books that heavily influenced the ideas of this thesis: in particular, *The Geometry of Syzygies* by David Eisenbud [4], *Commutative Algebra: with a View Toward Algebraic Geometry* also by Eisenbud [3], and *An introduction to homological algebra* by Charles A. Weibel [14].

I would like to thank my cellmates in the MSI Honours dungeon for their friendship and encouragement. Thanks also to the staff at the ANU Mathematical Sciences Institute who showed me the beauty of mathematics over the past four years. In particular, Dr Jarod Alper, Dr Vigleik Angeltveit, Dr James Borger, Dr Jack Hall, Dr Joan Licata, Assoc. Prof. Scott Morrison, Prof. Amnon Neeman and Dr David Smyth all taught me algebra that appears in this thesis.

Special thanks go to Scott Morrison for help with the Macaulay2 computations, and for the use of his super-powered desktop computer (which thought for twice as long before giving error messages!)

Finally, and most importantly, I would like to thank my supervisor, Dr Jarod Alper. Without his advice and support, I could not have even begun this thesis.

Declaration

All work in this thesis is my own, prepared under the supervision of Dr Jarod Alper, unless otherwise indicated.

Rowan Rowlands

Contents

Introduction

The determinant is one of the central functions of linear algebra. It encompasses the multiplicative properties of a matrix, and tells us if a matrix is invertible. It is fundamental to the definitions of Lie groups such as GL_n and SL_n, it is closely related to the eigenvalues of a matrix, and it plays an important role in differential equations in the form of the Wronskian.

Naïvely, it is difficult to compute the determinant for large matrices. For an $n \times n$ matrix, the determinant is a polynomial whose terms are indexed by the group of permutations on n letters, and the size of this group is $n!$, which grows quite quickly. However, there are easier ways to compute the determinant, exploiting its symmetry — for example, with row reduction.

The determinant has a close friend in the form of the permanent, which is just the determinant with its minus signs replaced by plus signs. Unsurprisingly given their similarity, the permanent and determinant share several properties — for example, they are invariant (up to sign) under permutations of the rows and columns. However, while there are quick algorithms for computing the determinant of an arbitrary matrix, no quick algorithms are known for computing the permanent [13].

Research into this paradox has focussed on trying to turn the permanent into a determinant by various manipulations. Any polynomial can be expressed as the determinant of a matrix whose entries are affine linear polynomials — the size of the smallest matrix where this is possible is called the *determinantal complexity* of the polynomial. It has been shown by Grenet [6] that the determinantal complexity of the permanent of an $n \times n$ matrix is bounded above by $2^n - 1$. The eventual aim of this field of research is motivated by the work of Valiant [13], who showed that the question of whether a polynomial upper bound exists is equivalent to an algebraic version of the P vs. NP problem.

The aim of this thesis is to use an algebraic construction called the polar pairing to compare the determinant and permanent. In particular, with the polar pairing we can associate each polynomial to its "apolar ideal", without losing any information about the polynomial. We will compute these ideals

for the determinant and permanent, and then use some homological algebra to examine their free resolutions and compute some Betti numbers. The major result of this thesis is a description of the linear second syzygies.

This thesis is divided into two parts. The first covers some necessary background material, and the second gives some new results.

Chapter 1 introduces some basic properties of the determinant and permanent, relating the determinant to exterior algebras, which will also be useful in Chapter 3. This chapter also introduces some basic properties of bilinear forms, used in Chapter 4, and gives a new proof of a theorem about magic squares, which is needed for Chapter 6.

Chapter 2 defines a dualising functor and examines some properties of these functors, inspiring the definition of a Gorenstein ring.

In Chapter 3, we discuss the concept of a graded ring, and define a free resolution of an arbitrary or graded ring. We prove some important facts about free resolutions by way of Koszul complexes — in particular, we show that any finitely generated graded R-module has a *minimal* free resolution, which gives some important invariants of the module, namely the Betti numbers.

Chapter 4 introduces Macaulay's polar pairing, an algebraic binary operation on polynomials that echoes how they interact under differentiation. This operation gives rise to the definition of an apolar ideal associated to a polynomial. We discuss some properties of this apolar ideal, and give a theorem by Macaulay that there is a one-to-one correspondence between homogeneous polynomials (up to scaling) and ideals of this form, so we lose no information about the polynomial by examining this ideal instead.

Moving into Part II, in Chapter 5 we apply the ideas of the polar pairing and the apolar ideal to the determinant and permanent functions. The central results of this chapter are Theorems 5.6 and 5.7, which re-prove a result by Shafiei [12] that the apolar ideals of the determinant and permanent are generated by degree 2 polynomials.

In Chapter 6, we build on Shafiei's result to look further down the free resolutions for the determinant and permanent apolar ideals. The major result of this thesis is a calculation of the next Betti number, $\beta_{2,3}$, in Equations (6.13) and (6.14), and a complete description of the linear second syzygies of the determinant apolar ideal, in Theorem 6.11. We conjecture that these generate all second syzygies, linear or otherwise, in the resolution of the determinant, and examine what this means for the next Betti number, $\beta_{3,4}$, in Equation (6.44).

Notation

- "Ring" means "commutative ring with unity". Usually, A will be an arbitrary ring, and R and S will be the polynomial rings $R = k[x_1, \ldots, x_n]$ and $S = k[X_1, \ldots, X_n]$ in n variables, or $R = k[x_{1,1}, \ldots, x_{n,n}]$ and $S = k[X_{1,1}, \ldots, X_{n,n}]$ in n^2 variables.
- k denotes an arbitrary field. We make no assumptions about its characteristic or whether it is algebraically closed, unless mentioned specifically.
- $\mathbb{Z}$ is the set (or group or ring...) of integers.
- Bold symbols denote matrices. In particular, the matrices

$$\mathbf{x} = \begin{bmatrix} x_{1,1} & \ldots & x_{1,n} \\ \vdots & & \vdots \\ x_{n,1} & \ldots & x_{n,n} \end{bmatrix} \qquad \text{and} \qquad \mathbf{X} = \begin{bmatrix} X_{1,1} & \ldots & X_{1,n} \\ \vdots & & \vdots \\ X_{n,1} & \ldots & X_{n,n} \end{bmatrix}$$

  will be used often.
- If $\mathbf{A}$ is a matrix, $\mathbf{A}(i;j)$ is the submatrix obtained by deleting the ith row and jth column. More generally, $\mathbf{A}(i_1, \ldots, i_a; j_1, \ldots, j_b)$ is the submatrix obtained by deleting rows $i_1, \ldots, i_a$ and columns $j_1, \ldots, j_b$.
- S_n is the symmetric group, the group of permutations on the set $\{1, \ldots, n\}$. It is written in upright font, to distinguish it from the ring S with a subscript. Its elements are written in parenthesis notation: for example, (1 3 4) denotes the permutation that sends 1 to 3, 3 to 4 and 4 to 1, fixing everything else.

Part I

Background

Chapter 1

Some linear algebra

The focus of this thesis is the determinant and the permanent, so in this chapter, we will define them and state some properties. The determinant is closely connected with the exterior algebra, so we will devote a section to discussing this too, alongside the symmetric and tensor algebras.

Later in the chapter, we give some elementary properties of bilinear forms that will be useful in Chapter 4. We also state a version of Birkhoff's theorem about semi-magic matrices, and give a new proof with relaxed assumptions.

1.1 The determinant and permanent

Definition. Define the matrix

$$\mathbf{x} = \begin{bmatrix} x_{1,1} & \dots & x_{1,n} \\ \vdots & & \vdots \\ x_{n,1} & \dots & x_{n,n} \end{bmatrix}.$$

The $n \times n$ *determinant* of $\mathbf{x}$ is

$$\det_n \mathbf{x} = \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} x_{i,\sigma i}$$

where S_n is the symmetric group on n letters, and $\operatorname{sgn}(\sigma)$ is the sign of the permutation σ, which is 1 if σ can be expressed as an even number of transpositions, and -1 otherwise.

The $n \times n$ *permanent* of $\mathbf{x}$ is

$$\operatorname{perm}_n \mathbf{x} = \sum_{\sigma \in \mathrm{S}_n} \prod_{i=1}^{n} x_{i,\sigma i}$$

that is, the same formula as the determinant but with the $\operatorname{sgn}(\sigma)$ removed.

We will view $\det_n \mathbf{x}$ and $\operatorname{perm}_n \mathbf{x}$ as elements of the polynomial ring $k[x_{1,1}, x_{1,2}, \ldots, x_{1,n}, \ldots, x_{n,n}]$ with n^2 variables.

The determinant and permanent have some important symmetries, which we will elaborate throughout Sections 1.1 and 1.2. The first of these is the following result:

Lemma 1.1. $\det_n \mathbf{x}^\top = \det_n \mathbf{x}$, *where* $\mathbf{x}^\top$ *denotes the transpose of* $\mathbf{x}$. *Similarly,* $\operatorname{perm}_n \mathbf{x}^\top = \operatorname{perm}_n \mathbf{x}$.

Proof. The functions

$$\begin{array}{c} \mathrm{S}_n \to \mathrm{S}_n \\ \sigma \mapsto \sigma^{-1} \end{array} \qquad \text{and} \qquad \begin{array}{c} \{1, \ldots, n\} \to \{1, \ldots, n\} \\ x \mapsto \sigma x \end{array}$$

are both bijections, and $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$. Therefore

$$\begin{aligned} \det_n \mathbf{x}^\top &= \sum_{\sigma \in \mathrm{S}_n} \operatorname{sgn}(\sigma) \prod_{i \in \{1,\ldots,n\}} x_{\sigma i, i} \\ &= \sum_{\sigma^{-1} \in \mathrm{S}_n} \operatorname{sgn}(\sigma^{-1}) \prod_{i \in \{1,\ldots,n\}} x_{\sigma^{-1} i, i} \\ &= \sum_{\sigma^{-1} \in \mathrm{S}_n} \operatorname{sgn}(\sigma^{-1}) \prod_{\sigma i \in \{1,\ldots,n\}} x_{\sigma^{-1}\sigma i, \sigma i} \\ &= \det_n \mathbf{x}. \end{aligned}$$

The proof for perm_n is similar, with $\operatorname{sgn}(\sigma)$ removed. □

Given a matrix $\mathbf{A}$, a submatrix $\mathbf{B}$ of $\mathbf{A}$ is a matrix obtained by deleting some rows and columns of $\mathbf{A}$. The following result will be important in Chapter 5:

Lemma 1.2. *The set of determinants of* $m \times m$ *submatrices of* $\mathbf{x}$ *is linearly independent in the vector space* $k[x_{1,1}, \ldots, x_{n,n}]$, *for any* $m = 1, \ldots, n$. *The same is true for the* $m \times m$ *permanents.*

Proof. Let $\mathbf{y}$ be an $m \times m$ submatrix of $\mathbf{x}$. Each term of $\det \mathbf{y}$ contains exactly one variable from each row and column of $\mathbf{y}$. If $\mathbf{y}'$ is a different $m \times m$ submatrix, by the pigeonhole principle there must be some row or some column that appears in $\mathbf{y}$ but not $\mathbf{y}'$. Hence every term of $\det \mathbf{y}$ contains a variable that does not appear in any term of $\det \mathbf{y}'$, so the terms must be entirely different.

Since there are no terms shared between any of the determinants of $m \times m$ submatrices, there can be no possible cancelling in a linear combination of them, so they must be linearly independent.

The same proof holds with determinants replaced by permanents. □

1.2 Exterior and symmetric algebras

To examine the symmetries of the determinant further, it will help to define it in terms of exterior algebras. Exterior algebras, and the closely related symmetric and tensor algebras, will reappear throughout this thesis, particularly in Chapter 3.

Definition. Given a ring A and an A-module M, the *tensor algebra* $T(M)$ is the non-commutative algebra composed of finite sums of products of the form

$$m_1 \otimes \cdots \otimes m_d$$

with $m_i \in M$, and $d = 0, 1, \ldots$.

The *symmetric algebra* $\mathrm{Sym}(M)$ of M is the quotient of the tensor algebra with the relation $x \otimes y = y \otimes x$ for all $x, y \in M$. We usually write $x \cdot y$ or simply xy to denote the image of $x \otimes y$ in $\mathrm{Sym}(M)$.

The *exterior algebra* $\wedge(M)$ of M is the quotient of the tensor algebra with the relation $x \otimes x = 0$ for all $x \in M$. We usually write $x \wedge y$ for the image of $x \otimes y$ in $\wedge(M)$.

This wedge relation implies that

$$\begin{aligned} 0 &= (x+y) \wedge (x+y) \\ &= x \wedge x + x \wedge y + y \wedge x + y \wedge y \\ &= x \wedge y + y \wedge x, \end{aligned}$$

so $\wedge$ is anti-commutative.[1]

There is a natural decomposition of these algebras: for instance, if we define $\wedge^d(M)$ to be the module generated by elements of the form

$$\overbrace{m_1 \wedge m_2 \wedge \cdots \wedge m_d}^{d \text{ things}}$$

then

$$\wedge(M) = \bigoplus_{d=0}^{\infty} \wedge^d(M).$$

Similarly,

$$\mathrm{Sym}(M) = \bigoplus_{d=0}^{\infty} \mathrm{Sym}^d(M) \qquad \text{and} \qquad T(M) = \bigoplus_{d=0}^{\infty} T^d(M).$$

[1] Anticommutativity is an equivalent condition to $x \wedge x = 0$ if 2 is a non-zero-divisor in A, since anticommutativity implies $0 = x \wedge x + x \wedge x = 2(x \wedge x)$.

Lemma 1.3. $\wedge$, $\wedge^d$, Sym *and* Sym^d, T *and* T^d *are functors from the category of* A*-modules to itself.*

Proof. For instance, $\wedge$ takes a map $f : M \to N$ to a map $\wedge f : \wedge M \to \wedge M$ that sends $m_1 \wedge \cdots \wedge m_d$ to $f(m_1) \wedge \cdots \wedge f(m_d)$. This clearly respects composition and identity maps, and the situation is similar for the other operations. □

From now on, we will take $A = k$ to be a field, and $M = V$ a finite-dimensional vector space. Given a basis $x_1, \ldots, x_n$ of V, we can give descriptions for the bases of the exterior and symmetric algebras:

Lemma 1.4. *The* d*th exterior power* $\wedge^d(V)$ *is the vector space with a basis of products*

$$x_{i_1} \wedge \cdots \wedge x_{i_d}$$

with $i_1 < \cdots < i_d$.

The d*th symmetric power* $\mathrm{Sym}^d(V)$ *is the vector space with a basis of products*

$$x_{i_1} \cdot \cdots \cdot x_{i_d}$$

with $i_1 \leq \cdots \leq i_d$.

The d*th tensor power* $T^d(V)$ *is the vector space with a basis of products*

$$x_{i_1} \otimes \cdots \otimes x_{i_d}$$

with no restriction on $i_1, \ldots, i_d$.

Proof. Any vector in V can be expressed as a linear combination of the basis vectors. By the bilinearity of $\otimes$, any product of vectors can thus be expressed as a linear combination of products of the basis vectors.

Suppose

$$x_{i_1} \otimes \cdots \otimes x_{i_d}$$

is a product of some basis vectors. In the tensor algebra, the set of products of this form is linearly independent.

In the symmetric algebra (so replace $\otimes$ with $\cdot$), however, swapping two adjacent x_{i_a} and x_{i_b} gives the same element of the algebra, so we may reorder the x_{i_a}s so that the i_as are in weakly increasing order. The set of such products then gives a maximal linearly independent set.

In the exterior algebra (so replace $\otimes$ by $\wedge$), swapping adjacent x_{i_a}s is still allowed, although it reverses the sign, which does not affect whether a set is linearly independent. However, we have the extra condition that if two i_a and i_b are equal, then a wedge product containing x_{i_a} and x_{i_b} is zero, so

the product cannot form part of a linearly independent set. Thus a basis of the dth exterior power is given by products of x_{i_a} with the i_as strictly increasing. □

Remark. From this description, it is clear that $\operatorname{Sym} V$ is isomorphic to the polynomial ring $k[x_1, \ldots, x_n]$, with the basis element $x_{i_1} \cdot \cdots \cdot x_{i_d}$ corresponding to the monomial $x_{i_1} \cdots x_{i_d}$.

Corollary 1.5. *If V is an n-dimensional vector space, then:*

- $\wedge^1(V) \cong \operatorname{Sym}^1 V \cong T^1(V) \cong V$.
- $\wedge^0(V) \cong \wedge^n(V) \cong k$. *(We set the modules $\wedge^0(V) = \operatorname{Sym}^0(V) = T^0(V)$ to equal k by definition.)*
- $\wedge^d(V) \cong 0$ *for $d > n$.*

Moreover, $\dim \wedge^d(V) = \binom{n}{d}$, $\dim \operatorname{Sym}^d(V) = \binom{n+d-1}{d}$, *and* $\dim T^d(V) = n^d$.

Proof. All these statements follow once we know the dimensions. It is clear from Lemma 1.4 that $\dim \wedge^d(V) = \binom{n}{d}$ and $\dim T^d(V) = n^d$, and the formula $\dim \operatorname{Sym}^d(V) = \binom{n+d-1}{d}$ follows from the combinatoric fact that the number of ways of choosing d things from a set of n, with repetition allowed, is $\binom{n+d-1}{d}$. □

Remark. The above results about exterior, symmetric and tensor algebras of a vector space also apply for free A-modules, with only minor modifications to the proofs.

We are now ready to show the connection between the determinant and exterior algebras. Note that any k-linear map $k \to k$ is multiplication by a constant.

Lemma 1.6 ([3, p. 579])**.** *If $\mathbf{A}$ is the matrix of a linear transformation $V \to V$ with respect to the basis $x_1, \ldots, x_n$, then under the isomorphism $\wedge^n V \cong k$ (Corollary 1.5) where $x_1 \wedge \cdots \wedge x_n$ corresponds to* 1*,*

$$\wedge^n V \xrightarrow{\wedge^n \mathbf{A}} \wedge^n V$$

is multiplication by a constant equal to $\det_n \mathbf{A}$.

Proof. To compute $\wedge^n \mathbf{A}$, we need only see what it does to the basis element $x_1 \wedge \cdots \wedge x_n$ of $\wedge^n V$.

$$(\wedge^n \mathbf{A})(x_1 \wedge \cdots \wedge x_n) = \mathbf{A}x_1 \wedge \cdots \wedge \mathbf{A}x_n$$

Each $\mathbf{A}x_i$ is a vector corresponding to the ith column of $\mathbf{A}$, so we can decompose it as

$$\mathbf{A}x_i = \sum_{j=1}^{n} A_{i,j}x_j$$

Taking these coefficients out of the wedge product, we get

$$\mathbf{A}x_1 \wedge \cdots \wedge \mathbf{A}x_n = \sum_{j_1=1}^{n} \cdots \sum_{j_n=1}^{n} (A_{1,j_1} \cdots A_{n,j_n})(x_{j_1} \wedge \cdots \wedge x_{j_n})$$

Because of the anti-commutativity of the exterior algebra, any term of this sum with $j_a = j_b$ for some a and b will include the product $x_{j_a} \wedge x_{j_a} = 0$, so it vanishes. Thus we may instead take the sum over permutations of $\{1, \ldots, n\}$:

$$\mathbf{A}x_1 \wedge \cdots \wedge \mathbf{A}x_n = \sum_{\sigma \in \mathrm{S}_n} (A_{1,\sigma(1)} \cdots A_{n,\sigma(n)})(x_{\sigma(1)} \wedge \cdots \wedge x_{\sigma(n)})$$

where S_n is the set of permutations on n letters.

But $x_{\sigma(1)} \wedge \cdots \wedge x_{\sigma(n)}$ may be turned into $x_1 \wedge \cdots \wedge x_n$ by swapping the terms. Each swap reverses the sign, so $x_{\sigma(1)} \wedge \cdots \wedge x_{\sigma(n)} = \mathrm{sgn}(\sigma)(x_1 \wedge \cdots \wedge x_n)$.

In summary,

$$\begin{aligned}(\wedge^n \mathbf{A})(x_1 \wedge \cdots \wedge x_n) &= \Big(\sum_{\sigma \in \mathrm{S}_n} \mathrm{sgn}(\sigma) A_{1,\sigma(1)} \cdots A_{n,\sigma(n)} \Big)(x_1 \wedge \cdots \wedge x_n) \\ &= (\det_n \mathbf{A})(x_1 \wedge \cdots \wedge x_n)\end{aligned}$$

so $\wedge^n \mathbf{A}$ is multiplication by $\det_n \mathbf{A}$. □

Corollary 1.7. $\det_n(\mathbf{AB}) = (\det_n \mathbf{A})(\det_n \mathbf{B})$.

Proof. Since $\wedge^i$ is a functor (Lemma 1.3), $\wedge^n(\mathbf{AB}) = (\wedge^n \mathbf{A})(\wedge^n \mathbf{B})$. □

Remark. The multiplicativity of the determinant is one of the properties that sets it apart from the permanent. It is not in general true that $\mathrm{perm}_n(\mathbf{AB}) = (\mathrm{perm}_n \mathbf{A})(\mathrm{perm}_n \mathbf{B})$: for example,

$$\begin{aligned}\left(\mathrm{perm}_n \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right)\left(\mathrm{perm}_n \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\right) &= 1 \cdot 1 \\ &= 1,\end{aligned}$$

but

$$\begin{aligned}\mathrm{perm}_n \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \right) &= \mathrm{perm}_n \left(\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \right) \\ &= 3.\end{aligned}$$

We will finally quote some results about the symmetries of the determinant and permanent, without proof.

Theorem 1.8 (Frobenius [5])**.** *If T is a linear transformation on the vector space of $n \times n$ matrices such that $\det_n T(\mathbf{x}) = \lambda \det_n \mathbf{x}$ for some $\lambda \in k$ non-zero, then T is either $T : \mathbf{x} \mapsto \mathbf{PxQ}$ or $T : \mathbf{x} \mapsto \mathbf{Px}^\top\mathbf{Q}$ for some non-singular matrices $\mathbf{P}$ and $\mathbf{Q}$.*

(These transformations certainly do preserve the determinant, by Lemma 1.1 and Corollary 1.7; the significant fact here is that these are *all* the symmetries.)

This group of symmetries contains some relevant subgroups. Firstly, we may take $\mathbf{P}$ and $\mathbf{Q}$ to be permutation matrices $\boldsymbol{\phi}$ and $\boldsymbol{\psi}$ (that is, matrices that are zero except for precisely one 1 in each row and column, giving a permutation on the set of basis vectors). The effect of these matrices is to permute the rows of $\mathbf{x}$ by the permutation ϕ and the columns by ψ. Secondly, $\mathbf{P}$ and $\mathbf{Q}$ could be diagonal matrices with diagonal elements $p_1, \ldots, p_n$ and $q_1, \ldots, q_n$ respectively, such that $(p_1 \cdots p_n)(q_1 \cdots q_n) = 1$. The effect of these is to scale the ith row of $\mathbf{x}$ by p_i, and the jth column by q_j. Finally, there there is the group isomorphic to $\mathbb{Z}/2$ generated by transposing $\mathbf{x}$.

There are more symmetries of the determinant than these — for example, adding one row of $\mathbf{x}$ to another. These symmetries also preserve the permanent; however, they are in fact the only ones that do.

Theorem 1.9 (Marcus and May [9])**.** *If T is a linear transformation on the vector space of $n \times n$ matrices such that $\operatorname{perm}_n T(\mathbf{x}) = \operatorname{perm}_n \mathbf{x}$, then T is either $T : \mathbf{x} \mapsto \mathbf{PxQ}$ or $T : \mathbf{x} \mapsto \mathbf{Px}^\top\mathbf{Q}$, where $\mathbf{P}$ and $\mathbf{Q}$ are products of permutation matrices and diagonal matrices, with $\operatorname{perm}_n \mathbf{P} \operatorname{perm}_n \mathbf{Q} = 1$.*

We will not refer to these theorems, but the symmetries of transposing a matrix and permuting its rows and columns will be very important in Chapter 6.

1.3 Bilinear forms

We will come across a particular bilinear form, the polar pairing, in Chapter 4, so it will help to have the following general results about bilinear forms.

Definition. If V is a vector space over a field k, a *bilinear form* is a map $V \times V \to k$ which is linear in each term. Bilinear forms are often written $\langle \cdot, \cdot \rangle$.

Example. The canonical example of a bilinear form is the dot product, taking vectors $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in k^n to the number $\langle a, b\rangle = a_1b_1 + \cdots + a_nb_n$.

Proposition 1.10 ([1, p. 230])**.** *If $x_1, \ldots, x_n$ is a basis for V, then any bilinear form $\langle \cdot, \cdot \rangle$ on V is determined as*

$$\langle v, w\rangle = v^\top \mathbf{A} w$$

for all v, w, where $\mathbf{A}$ is the matrix defined by $A_{i,j} = \langle x_i, x_j\rangle$.

The matrix $\mathbf{A}$ is called the *matrix of the form* with respect to the basis.

Proof. Write $v = \sum_i v_i x_i$ and $w = \sum_i w_i x_i$. Then

$$\begin{aligned}
\langle v, w\rangle &= \Big\langle \sum_i v_i x_i, \sum_j w_j x_j \Big\rangle \\
&= \sum_{i,j} v_i \langle x_i, x_j\rangle w_j \\
&= \sum_{i,j} v_i A_{i,j} w_j \\
&= v^\top \mathbf{A} w
\end{aligned}$$

□

Example. The matrix of the form of the dot product is the identity matrix.

Definition. A bilinear form is *symmetric* if $\langle v, w\rangle = \langle w, v\rangle$ for all $v, w \in V$.

A bilinear form is *non-degenerate* if for every non-zero vector v there is a vector w such that $\langle w, v\rangle \neq 0$.

Proposition 1.11 ([1, pp. 230, 236])**.** *A bilinear form is symmetric (resp. non-degenerate) if and only if the matrix of the form (with respect to an arbitrary basis) is a symmetric (resp. invertible) matrix.*

Proof. Let $x_1, \ldots, x_n$ be a basis for V, and let $\mathbf{A}$ be the matrix of the form with respect to this basis.

Suppose the form is symmetric; then $\langle x_i, x_j\rangle = \langle x_j, x_i\rangle$ for all basis vectors x_i, x_j; but this means that in the matrix of the form, $A_{i,j} = A_{j,i}$ for all i, j, so $\mathbf{A}$ is symmetric.

Conversely, suppose $\mathbf{A}$ is symmetric. Viewing $v^\top \mathbf{A} w$ as a 1×1 matrix, we have

$$\begin{aligned}
v^\top \mathbf{A} w &= \left(v^\top \mathbf{A} w\right)^\top \\
&= w^\top \mathbf{A}^\top \left(v^\top\right)^\top \\
&= w^\top \mathbf{A} v
\end{aligned}$$

so the form is symmetric.

Suppose the bilinear form is non-degenerate. Then for every non-zero v there is a w such that $w^\top \mathbf{A} v \neq 0$. Therefore $\mathbf{A}v$ must be non-zero for all v, which implies that the null space of A is trivial, hence $\mathbf{A}$ is invertible.

Conversely, if the bilinear form is *not* non-degenerate, there is some non-zero vector v such that $w^\top \mathbf{A} v = 0$ for all w. We must then have $\mathbf{A}v = 0$, so the null space of $\mathbf{A}$ is not trivial, thus $\mathbf{A}$ is not invertible. □

1.4 Birkhoff's theorem

In this section, we give a new proof of a generalisation of Birkhoff's theorem to an arbitrary ring. This result will be used in Chapter 6.

Definition. A square matrix is *semi-magic* with *magic constant* μ if the sums of the entries in any row and any column are μ.

Example. The following matrices are semi-magic:

$$\begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 2 & 2 & 2 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} \text{ in } \mathbb{Z}/3.$$

Their magic constants are 15, 1, 0 and 0 respectively.

We allow the entries of a semi-magic matrix to come from an arbitrary ring. This is a departure from the traditional definition, which requires the entries of the matrix to be non-negative real numbers or even non-negative integers. A more famous concept is a *magic square*, which is a semi-magic matrix whose diagonals also sum to μ, but we won't need to use this concept.

Theorem 1.12 (Birkhoff's theorem)**.** *Any semi-magic square is a linear combination of permutation matrices.*

This is a variation of a result due to Birkhoff, but the standard proofs of Birkhoff's theorem (see e.g. [7]) rely on the entries of the matrix being non-negative. We present an alternative proof that doesn't assume this.[2]

[2] A semi-magic matrix of non-negative real numbers with magic constant 1 is also called a *doubly stochastic* matrix, because of its role in probability theory. Some versions of Birkhoff's theorem say more in this case: Birkhoff's theorem states that the set of doubly stochastic matrices is not only generated by the permutation matrices, it is in fact the convex hull of the permutation matrices. If we relax the assumption of non-negativity and realness, we lose this result.

Figure 1.1: Matrices at various stages in the proof of Theorem 1.12, for $(n+1) = 4$. Stars denote unknown numbers.

(a) Start

$$\mathbf{M} = \begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}$$

(b) Step 1

$$\mathbf{M}' = \begin{bmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

(c) Step 2

$$\mathbf{M}'' = \begin{bmatrix} * & * & * & 0 \\ * & * & * & 0 \\ * & * & * & 0 \\ * & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} * & * & * & 0 \\ * & * & * & 0 \\ * & * & * & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

(d) Step 3

$$\tilde{\mathbf{m}} = \begin{bmatrix} * & * & * & 0 \\ * & * & * & 0 \\ * & * & * & 0 \\ 0 & 0 & 0 & * \end{bmatrix} = \mathbf{M}''$$

Proof. We proceed by induction on the size of the matrix.

For a 1×1 matrix, the statement is trivial, so assume it is true for all $n \times n$ matrices, and let

$$\mathbf{M} = \begin{bmatrix} M_{1,1} & \dots & M_{1,n+1} \\ \vdots & & \vdots \\ M_{n+1,1} & \dots & M_{n+1,n+1} \end{bmatrix}$$

be an $(n+1) \times (n+1)$ semi-magic matrix. We will decompose $\mathbf{M}$ into a linear combination of permutation matrices in three steps.

Step 1: First, observe two facts:

- If $\mathbf{A}$ and $\mathbf{B}$ are semi-magic matrices with magic constants α and β respectively, then $\mathbf{A}+\mathbf{B}$ is also semi-magic, with magic constant $(\alpha+\beta)$. The matrix $\lambda\mathbf{A}$, with λ a constant, is semi-magic with magic constant $\lambda\alpha$.

  (In other words, the semi-magic matrices form a vector space, and taking the magic constant is a linear map.)
- Every permutation matrix is semi-magic, with magic constant 1.

Therefore if $\boldsymbol{\sigma}$ is any permutation matrix with a 1 in position $(n+1, j)$, we can subtract $M_{n+1,j}\boldsymbol{\sigma}$ from $\mathbf{M}$ to get a semi-magic matrix with a 0 in

position $(n+1, j)$. Note that this does not affect any other entry from the $(n+1)$th row of $\mathbf{M}$.

Repeat this operation for every entry in the $(n+1)$th row of $\mathbf{M}$. The result is a semi-magic matrix $\mathbf{M}'$ whose $(n+1)$th row is entirely 0, and the difference between $\mathbf{M}$ and $\mathbf{M}'$ is a linear combination of permutation matrices. (See Figure 1.1b.)

Step 2: Now, let $\boldsymbol{\sigma}$ be any permutation matrix with 1s in positions $(n+1, 1)$ and $(i, n+1)$ for $1 \leq i \leq n$. If we subtract $M'_{i,n+1}\boldsymbol{\sigma}$ from $\mathbf{M}'$, the result has a 0 in position $(i, n+1)$ and some value in position $(n+1, 1)$, but no other entries in the $(n+1)$th row and column are changed.

Repeat this operation for all $M'_{1,n+1}, \ldots, M'_{n,n+1}$. This gives us a semi-magic matrix $\mathbf{M}''$ where the $(n+1)$th column and $(n+1)$th row are all zero except perhaps position $(n+1, 1)$, and $\mathbf{M}'' - \mathbf{M}$ is a linear combination of permutation matrices.

Since $\mathbf{M}''$ is semi-magic, in particular the $(n+1)$th row and column must both sum to the same number. But the sum along the $(n+1)$th column is zero, and the sum of the $(n+1)$th row is $M''_{n+1,1}$, so we must have $M''_{n+1,1} = 0$. (See Figure 1.1c.)

Step 3: Now we have an $(n+1) \times (n+1)$ semi-magic matrix $\mathbf{M}''$ whose only non-zero entries occur in the submatrix $\mathbf{m}$ made up of the first n rows and columns. By the induction hypothesis, there is some linear combination of $n \times n$ permutation matrices that equals $\mathbf{m}$:

$$\mathbf{m} = a_1\boldsymbol{\sigma}_1 + \cdots + a_l\boldsymbol{\sigma}_l$$

For every $n \times n$ permutation matrix $\boldsymbol{\sigma}$, there is a corresponding $(n+1) \times (n+1)$ permutation matrix $\hat{\boldsymbol{\sigma}}$ (shown in Figure 1.2) in which the $n \times n$ submatrix made of the first n rows and columns is exactly $\boldsymbol{\sigma}$, and there is a 1 in position $(n+1, n+1)$. (This is the permutation matrix corresponding to the canonical inclusion of S_n into S_{n+1}.)

Consider the $(n+1) \times (n+1)$ matrix

$$\hat{\mathbf{m}} = a_1\hat{\boldsymbol{\sigma}}_1 + \cdots + a_l\hat{\boldsymbol{\sigma}}_l.$$

This is a linear combination of semi-magic matrices, so it is itself semi-magic, and it clearly agrees with $\mathbf{M}''$ everywhere except perhaps position $(n+1, n+1)$. Each $\hat{\boldsymbol{\sigma}}_i$ contributes 1 to this position, so the entry is equal to $a_1 + \cdots + a_l$. But this is exactly the magic constant of $\mathbf{m}$, which is the magic constant of $\mathbf{M}''$, that is, 0. Therefore $\hat{\mathbf{m}} = \mathbf{M}''$. (See Figure 1.1d.)

Figure 1.2: The permutation matrix $\hat{\boldsymbol{\sigma}}$

$$\hat{\boldsymbol{\sigma}} = \begin{bmatrix} \boxed{\boldsymbol{\sigma}} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ \begin{matrix} 0 & \cdots & 0 \end{matrix} & 1 \end{bmatrix}$$

But $\hat{\mathbf{m}}$ is a linear combination of permutation matrices, thus $\mathbf{M}''$ is too, and so is $\mathbf{M}$. Therefore, by induction, all semi-magic matrices are linear combinations of permutation matrices. □

Chapter 2

Gorenstein rings

The aim of this chapter is to define a zero-dimensional Gorenstein ring, and give some results that we will use in Chapter 4. It is natural to give this definition in terms of dualising functors, so we will begin by defining these and examining some of their properties. This chapter closely follows the ideas of Sections 21.1 and 21.2 of [3].

Throughout this chapter, we will assume that A is a local, zero-dimensional ring. "Local" means there is only one maximal ideal, and "dimension" is the maximum length of a chain of prime ideals, so a local, zero-dimensional ring is one with a unique prime ideal, which is necessarily maximal.

2.1 Dualising functors

Definition. A contravariant, A-linear functor

$$D : \mathbf{Fin}\text{-}A \to \mathbf{Fin}\text{-}A$$

from the category of finitely generated A-modules to itself is a *dualising functor* if it is exact and $D^2 \cong 1$.

Remark. If A is a field k, so **Fin**-A is the category of finite-dimensional k-vector-spaces, we already know a dualising functor: the functor $V \mapsto V^\vee$ that sends a vector space V to its dual $V^\vee = \mathrm{Hom}_k(V, k)$.

This approach does not work in general: if A is an arbitrary local, zero-dimensional ring, the functor $D = \mathrm{Hom}_A(-, A)$ does not generally satisfy either exactness or $D^2 \cong 1$. The functor $\mathrm{Hom}_A(-, I)$ is exact iff I is an injective module [14, p. 40], but A is not in general injective as an A-module (for example $A = \mathbb{Z}$); and if $A = \mathbb{Z}$, we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/2, \mathbb{Z}) \cong 0$ so applying the functor again will not return $\mathbb{Z}/2$.

Before we construct a dualising functor on modules of arbitrary (local, zero-dimensional) rings, let us consider some properties that a dualising functor must satisfy. But first, we need some definitions.

Definition. A *composition series* of an A-module M is a chain of inclusions $0 \subset M_1 \subset \cdots \subset M_n = M$ such that each quotient M_{i+1}/M_i is a simple module (i.e., it has no non-trivial proper submodules).

It is a theorem that all composition series of a module have the same length [2, p. 77]. We therefore call this the *length* of the module.

Definition. If M is a module over a local, zero-dimensional ring A with maximal ideal $\mathfrak{m}$, the *top* of M is $M/\mathfrak{m}M$. The *socle* of M is the annihilator of $\mathfrak{m}$ in M, that is, the set of $m \in M$ such that $am = 0$ for all $a \in \mathfrak{m}$.

Proposition 2.1 ([3, pp. 525–526])**.** *If D is a dualising functor, then:*

(a) $D(A/\mathfrak{m}) \cong A/\mathfrak{m}$*;*

(b) D preseves lengths;

(c) D preserves annihilators, that is, $\operatorname{Ann}(M) = \operatorname{Ann}(D(M))$*;*

(d) $\operatorname{Hom}_A(M, N) \cong \operatorname{Hom}_A(D(N), D(M))$*, so in particular D preserves endomorphism rings;*

(e) D sends injective modules to projective modules, and vice versa; and

(f) D sends the top of a module to the socle, and vice versa.

Proof. (a): First, we claim that $A/\mathfrak{m}$ is the unique simple module of A. It is a field, so it must be simple.

Now suppose M is an arbitrary simple module. It is non-trivial, so we can take a non-zero element m. The submodule $Am \subseteq M$ generated by m must not be a proper submodule, since M is simple, so $Am = M$. Therefore we have the following exact sequence:

$$0 \longrightarrow \ker m \longrightarrow A \xrightarrow{m} M \longrightarrow 0$$

The kernel of $A \xrightarrow{m} M$ is an ideal, and the condition that M has no non-trivial submodules means that this ideal is maximal. Therefore the kernel is $\mathfrak{m}$, and by the first isomorphism theorem of groups, $M \cong A/\mathfrak{m}$.

Now, note that $D(A/\mathfrak{m})$ must be a simple module: if it has a proper submodule M, then we have the exact sequence

$$0 \longrightarrow M \longrightarrow D(A/\mathfrak{m})$$

which gives the exact sequence

$$D^2(A/\mathfrak{m}) \longrightarrow D(M) \longrightarrow 0$$

after applying D. Hence $D(M)$ is a proper quotient of $D^2(A/\mathfrak{m}) = A/\mathfrak{m}$. Since $A/\mathfrak{m}$ has no proper submodules, this is impossible. Hence $D(A/\mathfrak{m})$ must be simple, so, since $A/\mathfrak{m}$ is the only simple A-module, we must have $D(A/\mathfrak{m}) = A/\mathfrak{m}$.

(b): If $0 \hookrightarrow M_1 \hookrightarrow \cdots \hookrightarrow M_n = M$ is a composition series, so the cokernels are simple, then applying D gives $D(M) = D(M_n) \twoheadrightarrow \cdots \twoheadrightarrow D(M_1) \twoheadrightarrow D(0) = 0$, with the kernels of these maps being simple modules. Therefore these modules also form a composition series with the same length as the original, so the length of M is equal to the length of $D(M)$.

(c): If $a \in A$ annihilates M, that is, $aM = 0$, then by the A-linearity of D, $aD(M) = D(aM) = D(0) = 0$, so a annihilates $D(M)$. Therefore $\mathrm{Ann}(M) \subseteq \mathrm{Ann}(D(M))$; similarly, $\mathrm{Ann}(D(M)) \subseteq \mathrm{Ann}(D^2(M)) = \mathrm{Ann}(M)$, so $\mathrm{Ann}(M) = \mathrm{Ann}(D(M))$.

(d): Since D is a contravariant functor, we get the following sequence of maps:

$$\mathrm{Hom}_A(M,N) \xrightarrow{D} \mathrm{Hom}_A(D(N),D(M)) \xrightarrow{D} \mathrm{Hom}_A(M,N) \xrightarrow{D} \mathrm{Hom}_A(D(N),D(M))$$

Since the composition of any two of these maps is a bijection, each individual map must be bijective, so $\mathrm{Hom}_A(M,N) \cong \mathrm{Hom}_A(D(N),D(M))$. Taking $N = M$, we see that $\mathrm{Hom}_A(M,M) \cong \mathrm{Hom}_A(D(M),D(M))$, so D preserves endomorphism rings.

(e): We know that D reverses arrows in diagrams and preserves exact sequences, so the fact that D sends projective modules to injective ones and vice versa is immediate from the observation that the diagrams defining projective and injective objects are identical but with reversed arrows.

(f): If we apply D to the top of M, we get $D(M/\mathfrak{m}M)$, which we can view as a submodule of $D(M)$. This is clearly the set of elements of $D(M)$ which annihilate $\mathfrak{m}$, that is, the socle of $D(M)$. The fact that D sends socles to tops follows by applying D again. □

We now turn to finding a dualising functor for modules of an arbitrary (local, zero-dimensional) ring A.

Proposition 2.2 ([3, p. 527])**.** *If D is a dualising functor, then $D(-) \cong \mathrm{Hom}_A(-, D(A))$.*

Proof. To show this isomorphism of functors, we need to show that $D(M)$ is naturally isomorphic to $\mathrm{Hom}_A(M, D(A))$ for arbitrary modules M.

Any A-module homomorphism from A to the module $D(M)$ is determined uniquely by the image of 1, which can be any element of $D(M)$; thus the module $\mathrm{Hom}_A(A, D(M))$ is isomorphic to $D(M)$. By Proposition 2.1(d),

$$\mathrm{Hom}_A(A, D(M)) \cong \mathrm{Hom}_A(D^2(M), D(A)).$$

But by the definition of a dualising functor, $D^2(M) \cong M$. Therefore $D(M) \cong \mathrm{Hom}_A(M, D(A))$. □

Remark. This proposition implies that D is uniquely determined by how it acts on A.

Now let us consider $D(A)$. First, we need a definition:

Definition. A submodule N of an A-module M is *essential* if every submodule N' of M meets N non-trivially. We also say that M is an *essential envelope* of N.

It is a theorem [3, pp. 628–629] that any submodule has a unique injective essential envelope (up to isomorphism). We call this essential envelope the *injective hull*.

Proposition 2.3 ([3, p. 527])**.** *If D is a dualising functor, $D(A)$ is isomorphic to the injective hull of $A/\mathfrak{m}$.*

Proof. Since A is projective as an A-module (it is, in fact, free), $D(A)$ must be injective. (We can also see this by noting that $\mathrm{Hom}_A(-, I)$ is exact iff I is injective.)

The top of A is, by definition, the simple module $A/\mathfrak{m}$, so the socle of $D(A)$ is also simple, and therefore isomorphic to $A/\mathfrak{m}$.

Any finitely generated module of A is isomorphic to $A^n/\mathfrak{a}$ for some ideal $\mathfrak{a}$, so every finitely generated module has a simple submodule. If N is a simple module, N is isomorphic to $A/\mathfrak{m}$, so every element annihilates $\mathfrak{m}$; in other words, every simple submodule of a module M is contained in the socle of M. Putting these two facts together, we see that the socle of a module is an essential submodule.

But this means that $D(A)$ is the unique injective essential envelope of its socle $A/\mathfrak{m}$, that is, $D(A)$ is the injective hull of $A/\mathfrak{m}$. □

Based on this theorem, we define ω_A to be the injective envelope of $A/\mathfrak{m}$ for any local, zero-dimensional ring A, and call ω_A the *canonical module* of A. Propositions 2.2 and 2.3 combined tell us that if a dualising functor exists, it is uniquely specified as $D(-) = \mathrm{Hom}_A(-, \omega_A)$. We can say more than that:

Proposition 2.4 ([3, p. 528])**.** *The functor* $D(-) = \mathrm{Hom}_A(-, \omega_A)$ *is always a dualising functor.*

Proof. The functor $\mathrm{Hom}_A(-, X)$ is always contravariant and A-linear, and it is exact precisely when X is injective, so we need only show that $D^2 \cong 1$. This is clearly a natural transformation, so we must show that it is an isomorphism on every M. We do this by induction on the length of M.

To begin, let M be a module of length 1, so $M \cong A/\mathfrak{m}$. Consider $\mathrm{Hom}_A(A/\mathfrak{m}, \omega_A)$: any element ψ of this must be A-linear, so it must send elements of $A/\mathfrak{m}$ to the annihilator of $\mathfrak{m}$ inside ω_A; but this is precisely $A/\mathfrak{m}$. Therefore $\mathrm{Hom}_A(A/\mathfrak{m}, \omega_A) \cong A/\mathfrak{m}$; hence $D^2(A/\mathfrak{m}) \cong A/\mathfrak{m}$, and we are done.

Now suppose M has length greater than 1. It therefore has a proper submodule N, and the lengths of N and M/N are strictly lower than the length of M. Therefore we have the following diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\cong} & & \downarrow & & \downarrow{\scriptstyle\cong} & & \\ 0 & \longrightarrow & D^2(N) & \longrightarrow & D^2(M) & \longrightarrow & D^2(M/N) & \longrightarrow & 0 \end{array}$$

where all the vertical arrows but the middle one are isomorphisms, by the inductive hypothesis. Now a simple application of the 5-lemma [10, p. 15] shows that the middle arrow is an isomorphism too. □

2.2 Gorenstein rings

We are now, finally, ready to define Gorenstein rings (in this local, zero-dimensional case):

Definition. A local, zero-dimensional ring A is *Gorenstein* if $\omega_A \cong A$.

There are quite a few equivalent conditions:

Proposition 2.5 ([3, p. 530])**.** *The following are equivalent:*

(a) A is Gorenstein.

(b) A is itself an injective A-module.

(c) The socle of A is simple.

(d) ω_A is principally generated.

Proof. (a $\implies$ b) By definition ω_A is injective, and if A is Gorenstein, $A \cong \omega_A$.

(b $\implies$ c) Since A is injective, it must be the injective hull of its socle. The injective hull of a sum is the sum of the injective hulls of the summands; but since A is local, it is indecomposable as a direct sum of A-modules. Therefore the socle is indecomposable too, so the socle must be simple.

(c $\implies$ d) The socle of A is isomorphic to the top of the dual of A, namely $\omega_A/\mathfrak{m}\omega_A$. We now quote a lemma, without proof:

Lemma 2.6 (Nakayama [2, p. 22])**.** *If M is a finitely generated A-module and the images of $m_1, \ldots, m_i \in M$ generate the quotient $M/\mathfrak{m}M$, then $m_1, \ldots, m_i$ generate M.*

If $\omega_A/\mathfrak{m}\omega_A$ is simple, Nakayama's lemma says that ω_A is principally generated.

(d $\implies$ a) A principally generated A-module is isomorphic to $A/\mathfrak{a}$ for some ideal $\mathfrak{a}$. But Proposition 2.1 (b) tells us that A and ω_A have the same length, so $\mathfrak{a}$ must be the zero ideal, and $\omega_A \cong A$. □

Chapter 3

Syzygies

In this chapter we examine free resolutions, of modules and graded modules. We will state some properties of graded rings and modules, and examine the particular case of the graded ring $R = k[x_1, \ldots, x_n]$, whose residue field $k = R/(x_1, \ldots, x_n)$ has a particular free resolution called the Koszul complex. We find some important properties of free resolutions of R-modules: the key result is that graded R-modules have a unique, minimal free resolution. The dimensions of the components of this, called Betti numbers, give an invariant of the module, which will be the focus of Chapter 6 in a specific application.

3.1 Free resolutions

Definition. Let A be a ring. An A-module F is *free* if it is isomorphic to $\bigoplus_{i \in I} A_i$ with $A_i \cong A$ for some set I.

A *free resolution* of a module M is a chain complex of free modules

$$\cdots \to F_2 \to F_1 \to F_0$$

and a map $F_0 \to M$ such that

$$\cdots \to F_2 \to F_1 \to F_0 \to M \to 0$$

is an exact sequence.

We will sometimes abuse notation, and simply say that

$$\cdots \to F_2 \to F_1 \to F_0$$

is the free resolution.

We call the elements of F_i the *ith syzygies* of M. The 0th syzygies correspond to generators of M; the 1st syzygies correspond to relations between those generators; the 2nd syzygies correspond to relations between the relations, and so on. In Chapters 5 and 6 we will focus on the case where M is the quotient of R by an ideal; in this case, we have a free resolution where F_0 is simply R, hence the 1st syzygies correspond to generators of the ideal, the 2nd syzygies correspond to relations, and so on.

Example. The following exact sequence is a free resolution of the $\mathbb{Z}$-module $\mathbb{Z}/m$:

$$\cdots \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}/m \longrightarrow 0$$

Example. If $R = k[x, y]$, the R-module $k = R/(x, y)$ has a free resolution

$$\cdots \longrightarrow 0 \longrightarrow R \xrightarrow{\left[\begin{smallmatrix} y \\ -x \end{smallmatrix}\right]} R^2 \xrightarrow{[x\ y]} R \longrightarrow k \longrightarrow 0$$

This is an example of a Koszul resolution, which we will discuss in detail in Section 3.3.

Lemma 3.1. *For any A-module M, there exists a free module F that surjects onto M.*

Proof. For example, let F be the direct sum $\bigoplus_{m \in M} A_m$ with $A_m \cong A$, that is, the sum of one copy of A for each element of M. If 1_m is the element corresponding to 1 in A_m, define the map $F \to M$ by $1_m \mapsto m$, and extend linearly. This gives a ring module homomorphism, and it is clearly surjective. □

Remark. Taking a direct sum over all elements of M was colossal overkill: we could also have taken any set of generators of M. Very often M is infinite but has a finite set of generators — if this is the case, we say M is *finitely generated*.

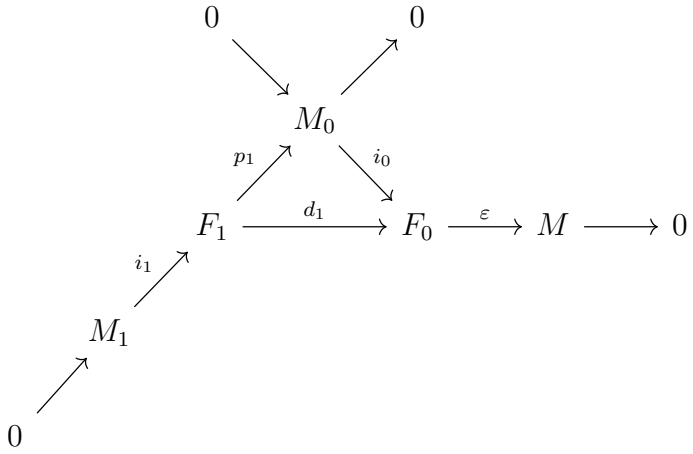
Proposition 3.2 ([14, p. 34])**.** *Any module M has a free resolution.*

Proof. We will construct a free resolution inductively.

First, by Lemma 3.1, there is some free module F_0 that surjects onto M. Let M_0 be the kernel of this surjection. We therefore have a short exact sequence (drawn crookedly for reasons that will become clear):

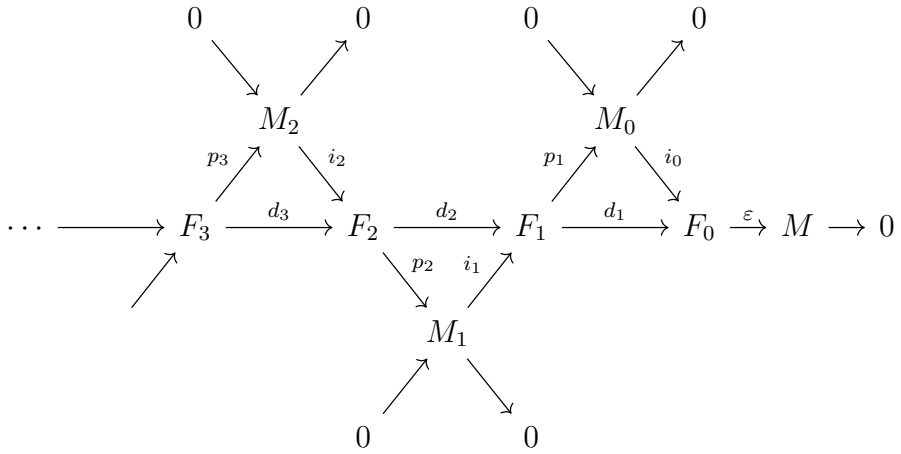
$$\begin{array}{ccccccc} 0 & & & & & & \\ & \searrow & & & & & \\ & & M_0 & & & & \\ & & & \searrow^{i} & & & \\ & & & & F_0 & \xrightarrow{\varepsilon} & M \longrightarrow 0 \end{array}$$

Since M_0 is also an A-module, we can apply Lemma 3.1 again to conclude that there is a free module F_1 that surjects onto M_0. If the kernel of this map is M_1, we can extend the diagram with the second short exact sequence $0 \to M_1 \to F_0 \to M_0 \to 0$ and the map $d_1 = i_0 \circ p_1$:



where the diagonals are exact. We claim that the horizontal line is also exact. It is exact at M by definition, and at F_0, the image of d_1 is the image of $i_0 \circ p_1$, which is the image of i_0 since p_1 is surjective. But since $0 \to M_0 \to F_0 \to M \to 0$ is exact, this is precisely the kernel of ε.

Continuing inductively, for a module M_i there is a free module F_i that surjects onto it, and taking the kernel gives us a new module M_{i+1}. We get the following commutative diagram with exact diagonals:



We must check exactness of the horizontal sequence at each F_n, $n > 0$. The image of $d_{n+1} = i_n \circ p_{n+1}$ is the image of i_n since p_{n+1} is surjective, and the kernel of $d_n = i_{n-1} \circ p_n$ is the kernel of p_n since i_{n-1} is injective, but the kernel of p_n is equal to the image of i_n since the diagonals are exact.

Therefore

$$\cdots \longrightarrow F_3 \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0$$

is a free resolution of M. □

Remark. If we add the assumption that A is noetherian, then we can augment this proof to show that any finitely generated A-module M has a free resolution with each F_i finitely generated. The only additional argument we need is that the modules $M_n = \ker(p_n : F_n \to M_{n-1})$ are finitely generated, which is true if A is noetherian.

3.2 Graded rings and the Hilbert function

Definition. A *graded ring* is a ring A with a decomposition $A = \bigoplus_{n\in\mathbb{Z}} A_n$ of abelian groups, where the product of any elements in A_n and A_m is an element of A_{n+m} for all $m, n \in \mathbb{Z}$.

If A is a graded ring, then a *graded A-module* is an A-module $M = \bigoplus_{n\in\mathbb{Z}} M_n$ such that if $a_i \in A_i$ and $m_j \in M_j$, then $a_i m_j \in M_{i+j}$.

An element of A or M is *homogeneous* if it comes from a single A_d or M_d, and we then say that d is its *degree*. Every element of a graded ring or module can be written uniquely as a finite sum of homogeneous elements with distinct degrees.

The polynomial ring $R = k[x_1, \ldots, x_n]$ is an example of a graded ring. We say that a monomial $x_1^{d_1} \cdots x_n^{d_n}$ has *degree* $d = d_1 + \cdots + d_n$, and a polynomial f is *homogeneous* of degree d if all of its terms have degree d. If R_d is the set of degree d homogeneous polynomials, then $R = \bigoplus_{d=0}^{\infty} R_d$ is a decomposition that makes R into a graded ring. (Note that under the identification between $k[x_1, \ldots, x_n]$ with $\operatorname{Sym} k^n$, this decomposition is exactly the decomposition of $\operatorname{Sym} k^n$ into $\bigoplus_d \operatorname{Sym}^d k^n$.)

An example of a graded module is a homogeneous ideal:

Definition. An ideal in a graded ring is called *homogeneous* if it can be generated by a set of homogeneous elements (not necessarily all of the same degree).

Lemma 3.3. *An ideal I in a graded ring A is homogeneous iff for every element $f \in I$, the homogeneous components of f are also all in I.*

Proof. Suppose I is homogeneous. Then it has a set of homogeneous generators, $\{g_j\}$ over some index set $j \in J$. If we take an arbitrary element

f of I, we can therefore write $f = \sum_j h_j g_j$ for some polynomials $h_j \in A$ with finitely many h_j non-zero. Write each h_j as a sum of homogeneous components: $h_j = \sum_i h_{j,i}$. Then $f = \sum_{i,j} h_{j,i} g_j$. But each $h_{j,i} g_j$ is a product of homogeneous elements, so it is itself homogeneous. Therefore, if we collect the summands with the same degree, each homogeneous component of f is a sum of some subset of the $h_{j,i} g_j$. But this is clearly in I, so every homogeneous component of f is in I.

Now suppose that if f is in I, then the homogeneous components of f are in I, for any f. Take any set of generators $\{g_j\}$ for I. Decompose each g_j into homogeneous components: $g_j = \sum_i g_{j,i}$. By assumption, each $g_{j,i}$ is also in I.

We claim that the $g_{j,i}$ also generate I. Let $\mathfrak{g}$ be the ideal generated by the $g_{j,i}$. Then $\mathfrak{g}$ is certainly contained in I since each $g_{j,i}$ is. But $\mathfrak{g}$ must contain every g_j, so it also contains I. Therefore $I = \mathfrak{g}$. Since $\mathfrak{g}$ was generated by homogeneous elements, I is a homogeneous ideal. □

Remark. A quotient of a graded ring by a homogeneous ideal is also a graded ring.

We now return to free resolutions. We need to reconsider our definition of a free resolution in the context of graded rings.

Definition. If A is a graded ring, the ring $A(-r)$ is the graded ring whose degree d component is the degree $d - r$ component of A.

We now allow a free graded A-module to be one of the form $\bigoplus_i A(-r_i)^{b_i}$ for some r_i and b_i, and we require the maps in a graded free resolution to preserve degrees. All above statements about free resolutions still hold, with only minor amendments to the proofs.

There is even more structure in $R = k[x_1, \ldots, x_n]$ than the graded decomposition into abelian groups: each R_d is not only a group, it is in fact a vector space over k. Graded R-modules also inherit this structure. We therefore have a useful measurement of the size of graded R-modules:

Definition. If M is a graded R-module, then the *Hilbert function* of M is the function

$$H_M(d) = \dim_k M_d$$

for non-negative integers d.

Lemma 3.4. *The Hilbert function of $R = k[x_1, \ldots, x_n]$ as an R-module is*

$$H_R(d) = \binom{n+d-1}{d}. \tag{3.1}$$

Proof. The ring R is isomorphic to $\operatorname{Sym} k^n$, and the dimension of the degree d component of this is $\binom{n+d-1}{d}$ by Corollary 1.5. □

There is a helpful relation between the Hilbert function of an R-module and the Hilbert functions of its free resolution. First, we need a lemma:

Lemma 3.5. *If*

$$\cdots \to 0 \xrightarrow{\phi_{r+1}} V_r \xrightarrow{\phi_r} V_{r-1} \xrightarrow{\phi_{r-1}} \cdots \xrightarrow{\phi_{s+1}} V_s \xrightarrow{\phi_s} 0 \to \cdots$$

is a bounded exact sequence of finite-dimensional vector spaces, then

$$\sum_{i=s}^{r} (-1)^i \dim V_i = 0. \tag{3.2}$$

Proof. The rank–nullity theorem tells us that

$$\dim V_i = \dim \operatorname{im} \phi_i + \dim \ker \phi_i. \tag{3.3}$$

Therefore

$$\begin{aligned}
\sum_{i=s}^{r} (-1)^i \dim V_i &= \sum_{i=s}^{r} (-1)^i \dim \operatorname{im} \phi_i + \sum_{i=s}^{r} (-1)^i \dim \ker \phi_i \\
&= \sum_{i=s}^{r} (-1)^i \dim \operatorname{im} \phi_i + \sum_{i=s}^{r} (-1)^i \dim \operatorname{im} \phi_{i+1} \\
&= \sum_{i=s}^{r} (-1)^i \dim \operatorname{im} \phi_i - \sum_{i=s+1}^{r+1} (-1)^i \dim \operatorname{im} \phi_i \\
&= (-1)^s \dim \operatorname{im} \phi_s - (-1)^{r+1} \dim \operatorname{im} \phi_{r+1} \\
&= 0 - 0 = 0
\end{aligned}$$

□

Corollary 3.6 ([4, p. 3])**.** *If*

$$\cdots \to 0 \to F_r \to \ldots \to F_1 \to F_0 \to M \to 0$$

is a bounded, graded free resolution of a graded R-module M with every F_i finitely generated, then

$$H_M(d) = \sum_i (-1)^i H_{F_i}(d). \tag{3.4}$$

Proof. Since this is a graded free resolution of R-modules, the degree d part forms an exact sequence of vector spaces. This formula follows immediately from applying Lemma 3.5. □

3.3 The Koszul complex

There is one free resolution in particular that will be important later: the Koszul complex.

The proofs in this section, and indeed in the rest of this chapter, require some more advanced homology techniques than those used so far (e.g. long exact sequence of homology, Tor). For definitions and properties of these, see e.g. [14].

Definition. If $R = k[x_1, \ldots, x_n]$, the *Koszul complex* $K(x_1, \ldots, x_n)$ is the complex of graded free R-modules whose degree m part is

$$K(x_1, \ldots, x_n)_m = \wedge^m R^n$$

and the differential is the map

$$\begin{aligned} d : \wedge^m R^n &\to \wedge^{m-1} R^n \\ v_1 \wedge \cdots \wedge v_m &\mapsto \sum_{j=1}^{m} (-1)^{j+1} x_{i_j} (v_1 \wedge \cdots \wedge \widehat{v_j} \wedge \cdots \wedge v_m) \end{aligned}$$

for $v_1, \ldots, v_n \in R^n$, where a hat means the term is omitted.

There is an alternative description of the Koszul complex that will make some proofs easier. To give this description, we need to define the tensor product of chain complexes:

Definition. If $F_\bullet$ and $G_\bullet$ are chain complexes of A-modules, then the tensor product $F_\bullet \otimes_A G_\bullet$ is defined to be the chain complex whose degree m component is

$$(F_\bullet \otimes_A G_\bullet)_m = \bigoplus_{a+b=m} F_a \otimes_A G_b$$

and if f_a and g_b are in F_a and G_b respectively, the differential sends

$$d : f_a \otimes g_b \mapsto \left(d^F(f_a) \otimes g_b\right) + (-1)^a \left(f_a \otimes d^G(g_b)\right)$$

with d^F and d^G being the differentials on $F_\bullet$ and $G_\bullet$ respectively.

It is straightforward to check that this is a complex.

We can now describe the Koszul complex using tensor products:

$$K(x_1, \ldots, x_n) \cong K(x_1) \otimes \cdots \otimes K(x_n) \tag{3.5}$$

where $K(x_i)$ is the complex (with degrees labelled above)

$$\begin{array}{ccccccccccc} & & 2 & & 1 & & 0 & & -1 & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & R & \xrightarrow{x_i} & R & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

where the map $R \xrightarrow{x_i} R$ means multiplication by x_i.

It can be shown by direct computation that Equation (3.5) is an isomorphism. The degree d component of $K(x_1) \otimes \cdots \otimes K(x_n)$ is the sum

$$\bigoplus_{\substack{D \subseteq \{1,\ldots,n\} \\ |D|=d}} \Big(\bigotimes_{i \in D} K(x_i)_1 \otimes \bigotimes_{i \notin D} K(x_i)_0 \Big) \tag{3.6}$$

with all tensor products over R. Every summand is $R \otimes \cdots \otimes R \cong R$, so this sum is the free R-module with $\binom{n}{d}$ summands, which is exactly $\wedge^d R$ by Corollary 1.5. (The differential maps are more fiddly to compute, although direct computation shows that they agree too; however, we won't need an explicit description of these.)

Analogously, we can define $K(x_{i_1}, \ldots, x_{i_m}) = K(x_{i_1}) \otimes \cdots \otimes K(x_{i_m})$ for any $i_1, \ldots, i_m$.

The importance of the Koszul complex for our purposes is the following result:

Proposition 3.7 ([3, pp. 431–432], [11])**.** *The Koszul complex $K(x_1, \ldots, x_n)$ is a free resolution of $R/(x_1, \ldots, x_n) = k$.*

Proof. We will show that $K(x_1, \ldots, x_i)$ is a free resolution of $R/(x_1, \ldots, x_i)$ by induction on i. The case $i = 1$ is trivial, so assume this is true for arbitrary i; we need to show that $K(x_1, \ldots, x_{i+1})$ is a resolution of $R/(x_1, \ldots, x_{i+1})$.

Consider the following diagram, with degrees labelled:

$$\begin{array}{ccccccccccc} & & 2 & & 1 & & 0 & & -1 & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & R & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & R & \xrightarrow{x_{i+1}} & R & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & R & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \end{array} \tag{3.7}$$

It is clearly commutative as all compositions are zero, and the columns are short exact sequences. We therefore have the short exact sequence of chain complexes

$$0 \longrightarrow R \longrightarrow K(x_{i+1}) \longrightarrow R[-1] \longrightarrow 0 \tag{3.8}$$

where the chain complex R consists of the ring R in degree 0, and the zero module elsewhere; and $R[-1]$ means the chain complex R has been shifted in degree by -1 to the right (that is, by 1 to the left) and the differentials multiplied by $(-1)^{-1}$ (although this makes no difference in this case).

For notational brevity, let $K = K(x_1, \ldots, x_i)$ and $K' = K(x_1, \ldots, x_{i+1})$. We can tensor this short exact sequence (3.8) with the complex K to get the sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K \otimes R & \longrightarrow & K \otimes K(x_{i+1}) & \longrightarrow & K \otimes R[-1] & \longrightarrow & 0 \\ & & \wr\!\downarrow & & \wr\!\downarrow & & \wr\!\downarrow & & \\ & & K & & K' & & K[-1] & & \end{array} \tag{3.9}$$

which is exact since all objects in K are free R-modules.

From a short exact sequence of chain complexes, we get a long exact sequence of homology. This long exact sequence is

$$\begin{aligned} \cdots \longrightarrow H_j(K) \longrightarrow H_j(K') \longrightarrow H_j(K[-1]) \longrightarrow \cdots \\ \cdots \longrightarrow H_1(K) \longrightarrow H_1(K') \longrightarrow H_1(K[-1]) \xrightarrow{\partial} \\ H_0(K) \longrightarrow H_0(K') \longrightarrow H_0(K[-1]) \end{aligned}$$

Note that $H_j(K[-1]) = H_{j-1}(K)$, by definition: therefore,

$$\begin{aligned} \cdots \longrightarrow H_j(K) \longrightarrow H_j(K') \longrightarrow H_{j-1}(K) \longrightarrow \cdots \\ \cdots \longrightarrow H_1(K) \longrightarrow H_1(K') \longrightarrow H_0(K) \xrightarrow{\partial} \\ H_0(K) \longrightarrow H_0(K') \longrightarrow H_{-1}(K) \end{aligned}$$

By the inductive hypothesis, K is a free resolution of $R/(x_1, \ldots, x_i)$. This means precisely that $H_j(K) = 0$ for $j \neq 0$, and $H_0(K) = R/(x_1, \ldots, x_i)$. Therefore our exact sequence is

$$\begin{aligned} \cdots \longrightarrow 0 \longrightarrow H_j(K') \longrightarrow 0 \longrightarrow \cdots \\ \cdots \longrightarrow 0 \longrightarrow H_1(K') \longrightarrow R/(x_1, \ldots, x_i) \xrightarrow{\partial} \\ R/(x_1, \ldots, x_i) \longrightarrow H_0(K') \longrightarrow 0 \end{aligned}$$

We immediately observe that $H_j(K')$ must be 0 for $j \geq 2$. To compute this homology for $j = 0$ and $j = 1$, we need to know the connecting map ∂. This

is a map from the homology of the diagram

$$\begin{array}{ccc} 0 & \longrightarrow & R \\ \downarrow & & \downarrow{\scriptstyle \mathrm{id}} \\ R & \xrightarrow{x_{i+1}} & R \\ \downarrow{\scriptstyle \mathrm{id}} & & \downarrow \\ R & \longrightarrow & 0 \end{array}$$

at the bottom left to the homology at the top right, once it is tensored with K. But this map is simply multiplication by x_{i+1}; hence the relevant section of our exact sequence is

$$0 \longrightarrow H_1(K') \longrightarrow R/(x_1, \ldots, x_i) \xrightarrow{x_{i+1}} R/(x_1, \ldots, x_i) \longrightarrow H_0(K') \longrightarrow 0$$

Thus $H_1(K')$ is the kernel of multiplication by x_{i+1}, which is zero, and $H_0(K')$ is the cokernel of this multiplication, which is $R/(x_1, \ldots, x_{i+1})$.

Therefore $K' = K(x_1, \ldots, x_{i+1})$ is a free resolution of $R/(x_1, \ldots, x_{i+1})$. By induction, $K(x_1, \ldots, x_i)$ is a free resolution of $R/(x_1, \ldots, x_i)$ for all i, so in particular, $K(x_1, \ldots, x_n)$ is a free resolution of $R/(x_1, \ldots, x_n) = k$. □

Remark. The only facts about $x_1, \ldots, x_n$ we used in this proof were that multiplication by x_{i+1} is injective in the ring $R/(x_1, \ldots, x_i)$. Equivalently, x_{i+1} is a non-zero-divisor in this quotient ring. Thus the same proof holds with $x_1, \ldots, x_n$ being any *regular sequence* in an arbitrary ring R — a regular sequence is one where each x_{i+1} is a non-zero-divisor in R modulo $x_1, \ldots, x_i$, and $(x_1, \ldots, x_n)R \neq R$ ([3, p. 423]).

3.4 Hilbert's syzygy theorem

Bounded free resolutions are much more useful than unbounded ones — for example, Corollary 3.6 lets us compute Hilbert functions from a bounded resolution — but from the construction in Proposition 3.2, it is not at all clear that bounded resolutions exist for an arbitrary module, where $R = k[x_1, \ldots, x_n]$. Surprisingly, there is always a bounded resolution for any finitely generated graded R-module. We can say much more than this: if R is a polynomial ring with n variables, then any finitely generated graded module has a resolution with length at most n.

To deduce this, we will introduce the concept of a "minimal" resolution. Naïvely, a "minimal" resolution is one where each free module is generated by the least number of elements possible to map onto the next module correctly.

It turns out that this is equivalent to an algebraically simpler condition, which we will take as the definition.

Definition. Let $\mathfrak{m}$ be the maximal ideal $(x_1, \ldots, x_n) \subset R$. A free resolution

$$\cdots \to F_n \xrightarrow{d_n} \cdots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0$$

of an R-module M is *minimal* if the image of each d_i lies in $\mathfrak{m}F_{i-1}$. That is, the differentials can be written as matrices with entries in $\mathfrak{m}$. Equivalently, the maps in the complex $F \otimes_R k = F \otimes_R R/\mathfrak{m}$ are zero.

A free resolution is *finite* if $F_{N+1} = 0$ for some N, and $F_i \neq 0$ for all $i \leq N$. We call N the *length* of the resolution (not to be confused with the length of a module defined in Chapter 2). The length of a resolution that is not finite is defined to be ∞.

Note that if

$$\cdots \to F_{N+2} \to 0 \to F_N \to \cdots \to F_0$$

is a resolution, with $F_{N+1} = 0$ and F_i arbitrary for $i > N + 1$, then it is finite with length N by this definition. The length of a finite resolution is the length of the first consecutive run of non-zero objects. The complex

$$\cdots \to 0 \to 0 \to F_N \to \cdots \to F_0$$

is also a resolution, so any finite resolution gives us a bounded one with the same length.

Corollary 3.8 ([4, p. 6])**.** *A resolution*

$$\cdots \to F_n \xrightarrow{d_n} \cdots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0$$

of an R-module M is minimal if and only if each d_i takes a basis of F_i to a minimal set of generators for $\operatorname{im} d_i$.

Proof. We have the right-exact sequence

$$F_{i+1} \to F_i \to \operatorname{im} d_i \to 0 \tag{3.10}$$

so tensoring with $R/\mathfrak{m}$ gives the exact sequence

$$F_{i+1}/\mathfrak{m}F_{i+1} \to F_i/\mathfrak{m}F_i \to (\operatorname{im} d_i)/(\mathfrak{m} \operatorname{im} d_i) \to 0. \tag{3.11}$$

The condition that the resolution above is minimal precisely means that the map $F_{i+1}/\mathfrak{m}F_{i+1} \to F_i/\mathfrak{m}F_i$ is zero, which happens if and only if the map $F_i/\mathfrak{m}F_i \to \operatorname{im} d_i/\mathfrak{m} \operatorname{im} d_i$ is an isomorphism. Hence any set of generators for $F_i/\mathfrak{m}F_i$ is sent to a set of generators for $\operatorname{im} d_i/\mathfrak{m} \operatorname{im} d_i$.

Nakayama's lemma (Lemma 2.6) has an analogue for graded rings:

Lemma 3.9 (Nakayama's lemma, graded version [4, p. 5]). *If M is a finitely generated graded R-module and the images of $m_1, \ldots, m_i \in M$ generate the quotient $M/\mathfrak{m}M$, then $m_1, \ldots, m_i$ generate M.*

By this lemma, the resolution is minimal if and only if a basis of F_i is mapped to a minimal set of generators of $\operatorname{im} d_i$. □

Remark. With this description, it is straightforward to construct a free resolution sending a basis of F_i to a minimal set of generators of $\operatorname{im} d_i = \ker d_{i-1}$, so we can conclude that every module M has a minimal resolution.

Definition. The *projective dimension* $\operatorname{pd} M$ of a graded R-module M is the minimum length of a finite free resolution of M. If M has no finite free resolutions, then $\operatorname{pd} M = \infty$.

Proposition 3.10 ([3, p. 477]). *If M is a non-zero, finitely generated graded R-module, then every minimal graded free resolution of M has length $\operatorname{pd} M$. Furthermore, $\operatorname{pd} M$ is the smallest integer i such that $\operatorname{Tor}_{i+1}^R(k, M) = 0$.*

Proof. Let I be the smallest integer i with $\operatorname{Tor}_{i+1}^R(k, M) = 0$, or ∞ if this never occurs.

First, note that since $\operatorname{Tor}_{i+1}^R(k, M)$ can be computed using any free resolution, it can be computed for a bounded free resolution of shortest length. In this case, $\operatorname{Tor}_{i+1}^R(k, M)$ is certainly 0 for all $i \geq \operatorname{pd} M$, so $I \leq \operatorname{pd} M$.

Let

$$\cdots \to F_i \to \cdots \to F_1 \to F_0$$

be a minimal free resolution of M with length L. Immediately, we must have $\operatorname{pd} M \leq L$. We can compute $\operatorname{Tor}_{i+1}^R(k, M)$ as the homology of

$$\cdots \to k \otimes_R F_i \to \cdots \to k \otimes_R F_1 \to k \otimes_R F_0 \to 0$$

But since the resolution was minimal, the differentials of this are zero, so $\operatorname{Tor}_{i+1}^R(k, M) = k \otimes_R F_{i+1}$. This is zero if and only if F_{i+1} is zero.

Hence I must equal L, so $\operatorname{pd} M \leq I$. But this means that $\operatorname{pd} M = I = L$. Thus any minimal resolution is also a resolution of shortest length, and $\operatorname{pd} M$ is the least integer i with $\operatorname{Tor}_{i+1}^R(k, M) = 0$. □

Corollary 3.11 (Hilbert Syzygy Theorem). *If $R = k[x_1, \ldots, x_n]$, every finitely generated graded R-module has a graded free resolution of length at most n.*

Proof. We can also use the symmetry of Tor ([14, p. 58]) to compute $\operatorname{Tor}_{i+1}^R(k, M)$ using a free resolution of k, instead of a resolution of M. The Koszul complex $K(x_1, \ldots, x_n)$ is a free resolution of k, so $\operatorname{Tor}_{i+1}^R(k, M)$ is the homology of

$$\cdots \to K(x_1, \ldots, x_n)_i \otimes_R M \to \cdots$$
$$\cdots \to K(x_1, \ldots, x_n)_1 \otimes_R M \to K(x_1, \ldots, x_n)_0 \otimes_R M$$

The degree i component of this is $\wedge^i R^n \otimes_R M$, so when $i > n$, it is zero. Hence the homology of this is certainly 0 for $i > n$, so $\operatorname{pd} M \leq n$. Thus M has a free resolution of length at most n. □

We know from Proposition 3.10 that all minimal resolutions of a module M have the same length. There is an even stronger result, which we will state without proof:

Theorem 3.12. *Minimal free resolutions of a finitely generated graded R-module are unique up to isomorphism.*

For a proof, see Theorem 20.2, [3, p. 495]. The proof is not difficult, but requires several more lemmas.

3.5 Betti numbers

Now that we know that minimal free resolutions exist and are unique for all finitely generated graded R-modules, we can talk about *the* minimal graded free resolution of a graded module.

Graded free resolutions of graded R-modules take the form

$$\cdots \longrightarrow F_i \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M$$
$$\wr \qquad\qquad \wr \qquad\qquad \wr$$
$$\bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{i,j}} \qquad \bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{1,j}} \qquad \bigoplus_{j\in\mathbb{Z}} R(-j)^{\beta_{0,j}}$$

The exponents $\beta_{i,j}$ of the minimal free resolution, called *Betti numbers*, completely determine the objects in the resolution up to isomorphism, and they are an important invariant of a module. The Betti number $\beta_{i,j}$ tells us that the ith object in the minimal free resolution has $\beta_{i,j}$ generators of degree j.

We often display the Betti numbers in a *Betti table*:

	0	1	...	i	...
0	$\beta_{0,0}$	$\beta_{1,1}$	...	$\beta_{i,i}$	...
1	$\beta_{0,1}$	$\beta_{1,2}$	...	$\beta_{i,i+1}$	...
$\vdots$	$\vdots$	$\vdots$		$\vdots$	
j	$\beta_{0,j}$	$\beta_{1,j+1}$	...	$\beta_{i,i+j}$	...
$\vdots$	$\vdots$	$\vdots$		$\vdots$	

Note that the entry in the ith column, jth row is $\beta_{i,i+j}$, not $\beta_{i,j}$. One reason for this is the following property:

Proposition 3.13. *If $\beta_{i,j} = 0$ for all $j < d$ and some fixed i, then $\beta_{i+1,j+1} = 0$ for all $j < d$.*

Remark. In terms of the Betti table, this means that if one column is entirely 0 above some row, then the next column to the right (and, by induction, all columns to the right) are also entirely 0 above that same row.

Proof. The minimality condition of the free resolution means that a summand $R(-j)$ of F_i must be mapped into $\mathfrak{m}F_{i-1}$. The map preserves degrees, and $\mathfrak{m}$ is precisely the subset of R generated by polynomials with positive degree. Therefore the image of a generator of $R(-j)$ must have degree at most $-j-1$, so since the maps of a minimal resolution take generators to generators bijectively, no $\beta_{i+1,j+1}$ can be non-zero for $j < d$. □

The ideas in the proof of Proposition 3.10 give us a way of computing the Betti numbers from an arbitrary free resolution:

Proposition 3.14. $\beta_{i,j} = \dim_k \operatorname{Tor}_i^R(k, M)_j$

Proof. If F is the minimal free resolution of M, then $\operatorname{Tor}_i^R(k, M)$ is the ith homology of $F \otimes k$. Since F was minimal, the maps in $F \otimes k$ are all zero by the definition of a minimal resolution, so the ith homology of $F \otimes k$ is simply $F_i \otimes k$. The dimension of the degree j component of this is exactly the number of degree j generators of F_i, which is $\beta_{i,j}$. □

Chapter 4

Apolarity

The polar pairing is a bilinear operation that lets us treat polynomials as "inverses". We can associate a polynomial f with the set of inverse polynomials that annihilate it in this system, which we call the *apolar ideal* — this set has some important properties. In particular, there is a bijection between homogeneous polynomials (up to scaling) and these sets, which implies that we lose no information about the polynomial by looking at its apolar ideal instead.

4.1 The polar pairing

Definition. Let $R = k[x_1, \ldots, x_n]$ and $S = k[x_1^{-1}, \ldots, x_n^{-1}]$ be subrings of the fraction field $K = k[x_1, x_1^{-1}, \ldots, x_n, x_n^{-1}]$ of R.

Suppose $f \in R$ and $g \in S$ are monomials. Define the binary operation $* : S \times R \to R$ in the following way:

$$g * f = \begin{cases} gf & \text{if this is an element of } R, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

Extend linearly to all polynomials. This gives R the structure of an S-module — in particular, we have the useful fact that $f * (g * h) = (fg) * h$ for all $f, g \in S$ and $h \in R$.

We will often write capital letters instead of inverses: so $x_i^{-1} = X_i$, and $S = k[X_1, \ldots, X_n]$.

Example. If $R = k[x_1, x_2, x_3]$ and $S = k[X_1, X_2, X_3]$,

$$X_1 * x_1^3 = x_1^{-1}x_1^3 = x_1^2$$
$$X_2 * x_1x_2 = x_1$$
$$X_1 * x_2x_3 = 0$$
$$(X_1 + X_2) * (x_1x_3^2 + x_2^2x_3) = x_3^2 + x_2x_3$$
$$(X_2 + X_3) * (x_2 - x_3) = 1 - 1 = 0$$

Remark. Observe that X_i acts like the partial differential operator $\frac{\partial}{\partial x_i}$ on polynomials, except that it doesn't change coefficients. That is,

$$X_i * x_i^n = x_i^{n-1},$$

whereas

$$\frac{\partial}{\partial x_i}x_i^n = nx_i^{n-1}.$$

We will sometimes abuse notation and write X_i as $\frac{\partial}{\partial x_i}$, treating this as "differentiation without coefficients", where this won't cause confusion. In particular, if f is a polynomial where no variable has exponent greater than 1, differentiation without coefficients agrees with the usual differentiation.[1]

Remark. Give S the analogous grading to R, so that a monomial $X_1^{d_1} \cdots X_n^{d_n}$ has degree $d = d_1 + \cdots + d_n$. If $f \in R$ and $g \in S$ are homogeneous polynomials with degrees d and d' respectively, then $g * f$ is clearly homogeneous with degree $d - d'$, since $g * f$ is made up of monomials that either have degree $d - d'$, or are zero.

An immediate consequence of this observation is that if $d < d'$, we must have $g * f = 0$, since there are no non-zero polynomials in R with negative degree. Also, if $d = d'$, then $g * f$ has degree 0, so it is a constant, that is, an element of k. This suggests the following definition:

Definition. The *polar pairing* is the map $\langle \cdot, \cdot \rangle : S_d \times R_d \to k$ where $\langle g, f \rangle = g * f$.

[1]The lack of coefficients is not an irrelevant detail — the systems with and without coefficients are truly different algebras. For example, with coefficients,

$$\left(\frac{\partial^2}{\partial x^2} - \frac{\partial}{\partial y}\frac{\partial}{\partial z}\right)(x^2 + yz) = 2 - 1 = 1,$$

but without coefficients,

$$(X^2 - YZ) * (x^2 + yz) = 1 - 1 = 0.$$

Recall that we defined a bilinear form in Section 1.3.

Proposition 4.1. *The pairing $\langle \cdot, \cdot \rangle$ is a non-degenerate, symmetric bilinear form, under the identification of S with R that associates X_i with x_i.*

Proof. The bilinearity follows immediately from the definition.

Since this is a bilinear form, by Proposition 1.10 we can compute the matrix of the form, with respect to the standard basis for R of monomials.

Observe that if f and g are both monomials of degree d with coefficient 1, if $f \neq g$, by the pigeonhole principle there must be a variable that has a higher exponent in g than in f, so $g * f = 0$; otherwise, if $f = g$, then $g * f = 1$. Therefore the matrix of the form with respect to the basis of monomials is the identity matrix.

The identity matrix is definitely symmetric and invertible, so by Proposition 1.11, the form is symmetric and non-degenerate. □

Remark. This pairing gives an injection $R_d \to S_d^\vee$, where $S_d^\vee$ is the vector space dual $S_d^\vee = \mathrm{Hom}_k(S_d, k)$, given by $f \mapsto \langle \cdot, f \rangle$, which is the map $g \mapsto g * f$. There is an injection in the other direction, so it follows that this map is an isomorphism between R_d and $S_d^\vee$.

4.2 The apolar ideal

Definition. Given a polynomial $f \in R$, the *apolar ideal* $f^\perp$ is the set of polynomials $g \in S$ such that $g * f = 0$.

Proposition 4.2. *For any $f \in R$, the apolar ideal $f^\perp$ is an ideal. If $f \in R_d$ is a homogeneous polynomial of degree d, $f^\perp$ is a homogeneous ideal.*

Proof. We will first check that $f^\perp$ is an ideal. If g_1 and g_2 are in $f^\perp$, by bilinearity, $(g_1 + g_2) * f = g_1 * f + g_2 * f = 0$. If $g \in f^\perp$ and h is any other polynomial, then $(hg) * f = h * (g * f) = h * 0 = 0$.

Now, we must show that the ideal is homogeneous. Suppose g is in $f^\perp$. We can write g as a sum of homogeneous components: $g = \sum_i g_i$, where g_i has degree i, and all but finitely many g_i are zero. Then

$$g * f = \sum_i (g_i * f).$$

But each $g_i * f$ has degree $d - i$, so all $g_i * f$ have different degrees. Therefore since the sum equals zero, each summand must equal zero, so every g_i is in $f^\perp$. Therefore $f^\perp$ is homogeneous by Lemma 3.3. □

Example. If f is the polynomial $f = x_1x_2^2 + x_3^3$, then $f^\perp$ is the ideal

$$f^\perp = (X_1^2,\ X_1X_3,\ X_2X_3,\ X_2^3,\ X_1X_2^2 - X_3^3,\ X_3^4).$$

These generators are homogeneous, so this is indeed a homogeneous ideal.

If f is not a homogeneous polynomial, e.g. $f = x_1x_2 + x_3$, then $f^\perp$ is not homogeneous: in this case, $f^\perp$ is

$$f^\perp = (X_1^2,\ X_2^2,\ X_3^2,\ X_1X_3,\ X_2X_3,\ X_1X_2 - X_3),$$

so $X_1X_2 - X_3$ is in the ideal while X_1X_2 and $-X_3$ are not.

Lemma 4.3. *If f is a homogeneous polynomial of degree d, there is a bilinear map*

$$\psi : (S/f^\perp)_r \times (S/f^\perp)_{d-r} \to k$$

given by $(g, h) \mapsto (gh) * f$. This map is non-degenerate, meaning that there is no $h \in (S/f^\perp)_{d-r}$ such that the map $\psi(-, h)$ is the zero map.

Proof. Observe that if $g \in (S/f^\perp)_r$ has degree r and $h \in (S/f^\perp)_{d-r}$ has degree $d-r$, then gh has degree $r + (d-r) = d$, so $(gh) * f$ has degree 0 and the map is thus well defined.

Now, fix some $h \in (S/f^\perp)$. We know that $(gh) * f = g * (h * f)$; but $h * f$ is a degree r polynomial, so since the polar pairing is non-degenerate as proved in Proposition 4.1, there is always some polynomial g of degree r with $g * (h * f) \neq 0$. Therefore $\psi(-, h)$ is not the zero map, so ψ is non-degenerate. □

Recall that for a graded R-module M, we defined the Hilbert function $H_M(r)$ in Section 3.2. The same definition works with R replaced by S.

Corollary 4.4. *If $f \in R_d$ is homogeneous of degree d, the Hilbert function of $S/f^\perp$ is symmetric:*

$$H_{S/f^\perp}(r) = H_{S/f^\perp}(d - r). \tag{4.1}$$

Proof. The map ψ in Lemma 4.3 gives us a map from $(S/f^\perp)_{d-r}$ to the dual $(S/f^\perp)_r^\vee = \mathrm{Hom}((S/f^\perp)_r, k)$:

$$\begin{aligned} \phi : (S/f^\perp)_{d-r} &\to (S/f^\perp)_r^\vee \\ h &\mapsto \psi(-, h) \end{aligned}$$

and since ψ is non-degenerate, ϕ is injective. But $(S/f^\perp)_r^\vee$ is isomorphic to $(S/f^\perp)_r$ as a vector space over k, so this injection implies that $\dim_k(S/f^\perp)_{d-r} \leq \dim_k(S/f^\perp)_r$.

Now, if we replace r with $d - r$ throughout, we also get an injection $(S/f^\perp)_r \to (S/f^\perp)^\vee_{d-r}$, so $\dim_k(S/f^\perp)_r \leq \dim_k(S/f^\perp)_{d-r}$. But this means that the two dimensions are equal; hence

$$H_{S/f^\perp}(r) = H_{S/f^\perp}(d - r). \qquad \square$$

Remark. It follows that the map $(S/f^\perp)_{d-r} \to (S/f^\perp)^\vee_r$ is in fact an isomorphism.

4.3 Macaulay's theorem

Macaulay discovered that there is a one-to-one correspondence between homogeneous polynomials (up to scaling) and apolar ideals. This theorem finally brings together the polar pairing and the ideas of Chapter 2.

Proposition 4.5. *If $f \in R_d$, that is, f is homogeneous of degree d, then $S/f^\perp$ is a Gorenstein ring.*

Proof. Recall that the socle of a local, zero-dimensional ring is the annihilator of the maximal ideal. It is clear that $S/f^\perp$ is local and zero-dimensional: its maximal ideal $\mathfrak{m}$ is the image of $(x_1, \ldots, x_n)$ in the quotient. Note that $\mathfrak{m}$ is made up of the polynomials of positive degree (and sums of such polynomials).

We claim that the socle of $S/f^\perp$ is the image of S_d in the quotient. Since $f^\perp$ is homogeneous by Proposition 4.2, the socle of $S/f^\perp$ is also homogeneous, so it suffices to prove this for homogeneous polynomials. Note that every polynomial with degree greater than d is in $f^\perp$, so the only non-zero graded components of $S/f^\perp$ have degree r with $0 \leq r \leq d$.

Suppose we have some homogeneous polynomial $g \in S$, representing a polynomial $\tilde{g}$ in the quotient $S/f^\perp$. First, suppose g has degree d. Then for any homogeneous h in $\mathfrak{m}$, $h\tilde{g}$ has degree strictly greater than d, so $h\tilde{g} = 0$ in $S/f^\perp$ and thus $\tilde{g}$ is in the annihilator of $\mathfrak{m}$ in $S/f^\perp$.

Conversely, suppose the degree of g is i with $i < d$, and $g \notin f^\perp$. Then $g * f$ is a non-zero homogeneous polynomial with degree $d - i$, so, since $*$ is non-degenerate by Proposition 4.1, there is some polynomial h with positive degree such that $h * (g * f) \neq 0$. But $h * (g * f) = (hg) * f$, so $h\tilde{g}$ is non-zero in the quotient $S/f^\perp$, hence $\tilde{g}$ is not in the annihilator of $\mathfrak{m}$.

Therefore the socle of $S/f^\perp$, that is, the annihilator of $\mathfrak{m}$, is precisely the degree d piece. By Corollary 4.4, the degree d piece has the same dimension as the degree 0 piece: this dimension is 1. Thus $(S/f^\perp)_d \cong k$, so it is simple. Therefore $S/f^\perp$ is Gorenstein, by Proposition 2.5. $\square$

Theorem 4.6 (Macaulay [8])**.** *The map $\phi : f \mapsto f^\perp$ gives a bijection between the set of homogeneous polynomials in R of degree d, up to non-zero scalar multiplication, and the set of homogeneous ideals $I \subseteq S$ such that S/I is a graded, local, zero-dimensional, Gorenstein ring with socle in degree d.*

Proof. To show the bijection, we must give an inverse map. Suppose I is a homogeneous ideal such that S/I is a local, zero-dimensional, Gorenstein ring with socle in degree d. Then we have a surjection

$$S_d \twoheadrightarrow (S/I)_d$$

where $(S/I)_d$ is isomorphic to k by the Gorenstein property. Taking the dual of this map (as a map of vector spaces) gives us an injection:

$$(S/I)_d^\vee \hookrightarrow S_d^\vee$$

Note that $S_d^\vee \cong R_d$. Take the isomorphism $(S/I)_d^\vee \cong k^\vee \cong k$ (note that this is not a canonical isomorphism) and consider the image of 1 in this isomorphism: call this image $f \in R_d$. Then define $\psi(I) = f$ (which is well defined up to scaling, since the isomorphism $(S/I)_d^\vee \cong k$ was not canonical). We claim that ψ is the inverse of ϕ.

First, consider $\psi \circ \phi(f)$, where $f \in R_d$. We have $\psi \circ \phi(f) = \psi(f^\perp)$. There is an exact sequence

$$0 \longrightarrow f_d^\perp \longrightarrow S_d \longrightarrow (S/f^\perp)_d \longrightarrow 0$$

where $(S/f^\perp)_d$ is isomorphic to k as shown in Proposition 4.5. But we also have an exact sequence

$$0 \longrightarrow \ker \varepsilon \longrightarrow S_d \xrightarrow{\varepsilon} k \longrightarrow 0.$$

$$g \longmapsto g * f$$

The kernel of ε is precisely the degree d component of $f^\perp$. Since the linear maps $S_d \to k$ in these two exact sequences have the same kernel, they must be the same map (up to scaling).

When we take the dual of this map $S_d \to k$, we get the map

$$k^\vee \to S_d^\vee.$$

In the isomorphism $k^\vee \cong k$, the element 1 corresponds to the identity map, so the image of 1 is the composition of the identity map with the map $g \mapsto g * f$.

But under the isomorphism $S_d^\vee \cong R_d$, the map $(g \mapsto g*f)$ exactly corresponds to f; therefore $\psi \circ \phi(f) = f$.

Now, let us compute $\phi \circ \psi(I)$ for a homogeneous ideal I such that S/I is a local, zero-dimensional, Gorenstein ring with socle in degree d. To compute $\psi(I)$, observe that $(S/I)_d$ is isomorphic to k by the Gorenstein property, so the dual of

$$S_d \to (S/I)_d$$

is a map

$$k^\vee \cong k \to S_d^\vee \cong R_d.$$

The image of 1 under this map is some polynomial $f \in R_d$, which corresponds to the map $g \mapsto g * f$ under the isomorphism $R_d \cong S_d^\vee$. Therefore the map $S_d \to (S/I)_d$ must have been the map $g \mapsto g * f$, which means that I_d is the kernel of this map, which is $f_d^\perp$.

Similarly to Lemma 4.3, the Gorenstein property implies that we have a non-degenerate bilinear map

$$\alpha : (S/I)_r \times (S/I)_{d-r} \to (S/I)_d \cong k$$

for any r, so we have the formula

$$\begin{aligned} I_r &= \{g \in S_r : \alpha(g, -) \text{ is the zero map}\} \\ &= \{g \in S_r : gh \in I_d \text{ for all } h \in S_{d-r}\} \\ &= \{g \in S_r : gh \in f_d^\perp \text{ for all } h \in S_{d-r}\} \\ &= f_r^\perp. \end{aligned}$$

So I and $f^\perp$ agree in every degree, so they are the same ideal. Therefore $\phi \circ \psi(I) = f^\perp = I$.

So ψ and ϕ are indeed bijections. □

Remark. Instead of studying homogeneous polynomials on their own, with this theorem we are justified in instead considering their apolar ideals. Since homogeneous polynomials and ideals of this form are in one-to-one correspondence, we lose no information about the polynomial by studying its apolar ideal.

We will take this idea to heart in the remainder of this thesis, in which we compare the determinant and permanent through their apolar ideals.

Part II

The resolutions of $S/\det_n^{\perp}$ and $S/\operatorname{perm}_n^{\perp}$

Chapter 5

The perpendicular ideals $\det_n^\perp$ and $\operatorname{perm}_n^\perp$

In Chapter 4 we defined the apolar ideal of a polynomial, and found in Theorem 4.6 that we can reconstruct a homogeneous polynomial from its apolar ideal, so we lose nothing by considering the apolar ideal in place of the polynomial. In Chapter 3 we discovered an important set of invariants of a graded R-module, the Betti numbers. In the next two chapters, we will put these ideas together and apply them to the determinant and permanent. The goal of this chapter is to re-prove a result by Shafiei [12], giving a description of the generators of the apolar ideals of the determinant and permanent.

5.1 Properties of the determinant and permanent in the polar pairing

First, let us examine how the determinant and permanent fit into the polar pairing. Recall from Chapter 1 that $\mathbf{x}$ denotes the matrix

$$\mathbf{x} = \begin{bmatrix} x_{1,1} & \dots & x_{1,n} \\ \vdots & & \vdots \\ x_{n,1} & \dots & x_{n,n} \end{bmatrix},$$

and recall that $X_{i,j} = \frac{\partial}{\partial x_{i,j}}$ means differentiation without coefficients, as explained in Chapter 4 (although in this chapter, we will never apply $X_{i,j}$ to polynomials with exponents higher than 1, so it is in fact identical to the usual differentiation *with* coefficients).

If $\mathbf{A}$ is a matrix, let $\mathbf{A}(i;j)$ denote the submatrix obtained by deleting the ith row and the jth column of $\mathbf{A}$. More generally, let $\mathbf{A}(i_1,\dots,i_a;j_1,\dots,j_b)$

be the submatrix obtained by deleting rows $i_1, \ldots, i_a$ and columns $j_1, \ldots, j_b$.

Lemma 5.1. *The $x_{i,j}$th derivative of the $n \times n$ determinant is $(-1)^{i+j}$ times the $(n-1) \times (n-1)$ determinant of the (i,j)th submatrix. That is,*

$$\frac{\partial}{\partial x_{i,j}} \det_n \mathbf{x} = (-1)^{i+j} \det_{n-1} \mathbf{x}(i;j). \tag{5.1}$$

The derivative of the permanent is the same without the change in sign:

$$\frac{\partial}{\partial x_{i,j}} \operatorname{perm}_n \mathbf{x} = \operatorname{perm}_{n-1} \mathbf{x}(i;j). \tag{5.2}$$

Proof. Recall that the $n \times n$ determinant can be expressed as

$$\det_n \mathbf{x} = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{k=1}^{n} x_{k,\sigma k}$$

Most of these terms vanish when taking the $x_{i,j}$th derivative: the only ones remaining are the ones where $\sigma(i) = j$, and in those terms, the $x_{i,j}$ variable is omitted. By inspection, this is the same as the determinant of

$$\begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ \vdots & & \vdots \\ x_{i-1,1} & \cdots & x_{i-1,n} \\ 0 & \ldots\ 0\ 1\ 0\ \ldots & 0 \\ x_{i+1,1} & \cdots & x_{i+1,n} \\ \vdots & & \vdots \\ x_{n,1} & \cdots & x_{n,n} \end{bmatrix}, \tag{5.3}$$

that is, the matrix $\mathbf{x}$ with $x_{i,j}$ replaced with 1 and the rest of the ith row set to 0. By cofactor expansion along the ith row, the determinant of this matrix is $(-1)^{i+j}$ times the determinant of the (i,j)th submatrix.

By the same argument, the derivative of the permanent is the permanent of the same matrix as in Equation (5.3), which is the permanent of the i,jth submatrix of $\mathbf{x}$. □

Remark. We need to take a little care when computing multiple derivatives of the determinant. Suppose we want to compute

$$\frac{\partial}{\partial x_{i',j'}} \frac{\partial}{\partial x_{i,j}} \det_n \mathbf{x}.$$

Figure 5.1: The sign change of the second derivative of the determinant. The quadrant that (i', j') lies in relative to (i, j) gives the change in sign of the determinant, $(-1)^\delta$.

$$\left[\begin{array}{c|c} + & - \\ \hline - & + \end{array}\right] \quad \text{with } (i,j) \text{ at the center}$$

By Lemma 5.1, this is equal to

$$(-1)^{i+j} \frac{\partial}{\partial x_{i',j'}} \det_{n-1} \mathbf{x}(i;j).$$

If $i = i'$ or $j = j'$, this is zero, since $x_{i',j'}$ will not appear in $\det_{n-1} \mathbf{x}(i;j)$, so we need only consider when $i \neq i'$ and $j \neq j'$.

When taking the (i,j)th submatrix, the rows after the ith row are shifted up by one place, and the columns after the jth are shifted left. Thus if $i' > i$ or if $j' > j$, but not both, we get an extra factor of (-1) when using Lemma 5.1 to compute this second derivative. If neither $i' > i$ nor $j' > j$, then this problem does not occur, and if both $i' > i$ and $j' > j$ we get two factors of (-1), which cancel. Therefore

$$\frac{\partial}{\partial x_{i',j'}} \frac{\partial}{\partial x_{i,j}} \det_n \mathbf{x} = (-1)^{i+j}(-1)^{i'+j'}(-1)^{\delta'} \det_{n-2} \mathbf{x}(i,i';j,j') \tag{5.4}$$

where δ' is how many of the statements $(i' > i)$ and $(j' > j)$ are true. This is summarised in Figure 5.1.

For higher derivatives, the pattern continues: if we take a further derivative by $X_{i'',j''}$, we get an extra factor of $(-1)^{\delta''}$ where δ'' is the number of i, i' that i'' is greater than plus the number of j, j' that j'' is greater than.

The exact sign of third and higher derivatives will not be important for the rest of this thesis, although we will use the fact that the derivative of the determinant by $X_{i_1,j_1}, \ldots, X_{i_m,j_m}$ is plus or minus the determinant of $\mathbf{x}(i_1, \ldots, i_m; j_1, \ldots, j_m)$.

When we take multiple derivatives of the permanent, we do not get any extra sign changes, so

$$\frac{\partial}{\partial x_{i',j'}} \frac{\partial}{\partial x_{i,j}} \operatorname{perm}_n \mathbf{x} = \operatorname{perm}_{n-2} \mathbf{x}(i,i';j,j') \tag{5.5}$$

and similarly for higher derivatives.

Recall the definition of the Hilbert function, from Chapter 3.

Proposition 5.2. *The Hilbert functions of* $S/\det_n^\perp$ *and* $S/\operatorname{perm}_n^\perp$ *are*

$$H_{S/\det_n^\perp}(d) = H_{S/\operatorname{perm}_n^\perp}(d) = \binom{n}{d}^2.$$

Proof. Consider the maps

$$\begin{aligned} \psi : S_d &\to R_{n-d} \\ g &\mapsto g * \det_n \end{aligned} \tag{5.6}$$

and

$$\begin{aligned} \psi' : S_d &\to R_{n-d} \\ g &\mapsto g * \operatorname{perm}_n \end{aligned} \tag{5.7}$$

These are linear maps, by the definition of $*$.

The kernel of ψ is the set of degree d polynomials that make $\det_n$ vanish under the polar pairing, so it is precisely $(\det_n^\perp)_d$. Similarly, the kernel of ψ' is $(\operatorname{perm}_n^\perp)_d$. The image of ψ is the space generated by determinants of $(n-d)\times(n-d)$ submatrices of $\mathbf{x}$ by Lemma 5.1, and similarly, the image of ψ' is the space generated by permanents of $(n-d)\times(n-d)$ submatrices. Denote these spaces by D_{n-d} and P_{n-d} respectively.

Therefore,

$$(S/\det_n^\perp)_d = (S_d)/(\det_n^\perp)_d \cong D_{n-d}$$

and

$$(S/\operatorname{perm}_n^\perp)_d = (S_d)/(\operatorname{perm}_n^\perp)_d \cong P_{n-d}.$$

Hence the dimensions of $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ in degree d are equal to the dimensions of D_{n-d} and P_{n-d}.

By Lemma 1.2, the set of determinants and the set of permanents of $(n-d)\times(n-d)$ submatrices of $\mathbf{x}$ are each linearly independent, so the dimension of each of these spaces is equal to the number of $(n-d)\times(n-d)$ submatrices of $\mathbf{x}$.

To choose such a submatrix, we must independently choose d rows and d columns to remove from $\mathbf{x}$, out of n rows and n columns. There are $\binom{n}{d}$ ways of choosing these rows or columns, so the number of submatrices, and hence the dimension of $(R/\det_n^\perp)_d$ or $(R/\operatorname{perm}_n^\perp)_d$, is

$$\binom{n}{d}^2. \qquad \square$$

5.2 A description of the ideals $\det_n^\perp$ and $\mathrm{perm}_n^\perp$

In this section we will give sets of generators for the perpendicular ideals of the determinant and permanent.

Proposition 5.3. *The ideal* $\det_n^\perp$ *contains the polynomials* $X_{i,j}X_{i',j'}+X_{i,j'}X_{i',j}$ *for* $i, i', j, j' \in \{1, \ldots, n\}$.

Our eventual goal is to show that these polynomials generate the entire ideal when $\operatorname{char} k \neq 2$, but for now, we will satisfy ourselves with showing that these are in the ideal.

Remark. Note that if $i' = i$, this polynomial is $2X_{i,j}X_{i,j'}$, so if $\operatorname{char} k \neq 2$ (hence 2 is invertible), we may consider $X_{i,j}X_{i,j'}$ instead. Similarly, if $j' = j$, the polynomial can be simplified to $X_{i,j}X_{i',j}$, and if both $i' = i$ and $j' = j$, the polynomial is $X_{i,j}^2$.

This description is perhaps more useful. It gives a more complete description in characteristic 2, and also allows us to describe $\mathrm{perm}_n^\perp$. We will thus restate Proposition 5.3 in this form:

Proposition 5.4. *The ideal* $\det_n^\perp$ *contains the polynomials*

- $X_{i,j}^2$,
- $X_{i,j}X_{i,j'}$ *for* $j \neq j'$,
- $X_{i,j}X_{i',j}$ *for* $i \neq i'$, *and*
- $X_{i,j}X_{i',j'} + X_{i,j'}X_{i',j}$ *for* $i \neq i'$ *and* $j \neq j'$

where $i, i', j, j' \in \{1, \ldots, n\}$. *The set of these polynomials is linearly independent.*

And the result for $\mathrm{perm}_n^\perp$:

Proposition 5.5. *The ideal* $\mathrm{perm}_n^\perp$ *contains the polynomials*

- $X_{i,j}^2$,
- $X_{i,j}X_{i,j'}$ *for* $j \neq j'$,
- $X_{i,j}X_{i',j}$ *for* $i \neq i'$, *and*
- $X_{i,j}X_{i',j'} - X_{i,j'}X_{i',j}$ *for* $i \neq i'$ *and* $j \neq j'$ *(note the added minus sign)*

where $i, i', j, j' \in \{1, \ldots, n\}$. *The set of these polynomials is linearly independent.*

Proof of Proposition 5.4. The linear independence is obvious, since every monomial appears in only one of the polynomials.

We know from Lemma 5.1 that

$$\frac{\partial}{\partial x_{i,j}} \det_n \mathbf{x} = \pm \det_{n-1} \mathbf{x}(i;j).$$

The matrix $\mathbf{x}(i;j)$ does not contain the variables $x_{i,j}$, $x_{i,j'}$ or $x_{i',j}$, so they do not appear in its determinant. Hence the derivatives $\frac{\partial}{\partial x_{i,j}}$, $\frac{\partial}{\partial x_{i,j'}}$ and $\frac{\partial}{\partial x_{i',j}}$ all send $\det_{n-1} \mathbf{x}(i;j)$ to 0. Therefore the first three polynomials are in the determinant.

The fourth polynomial is slightly trickier. Without loss of generality, we may swap the variables in each term to make $i < i'$, and still without loss of generality, we may then swap the first and second term to ensure $j < j'$.

By the discussion following Lemma 5.1, it is clear that both

$$\frac{\partial}{\partial x_{i,j}} \frac{\partial}{\partial x_{i',j'}} \det_n \mathbf{x} \tag{5.8}$$

and

$$\frac{\partial}{\partial x_{i,j'}} \frac{\partial}{\partial x_{i',j}} \det_n \mathbf{x} \tag{5.9}$$

are equal to $\pm \det_{n-2} \mathbf{x}(i,i';j,j')$, since $\mathbf{x}(i,i';j,j') = \mathbf{x}(i,i';j',j)$, as illustrated in Figure 5.2.

We must now take care with the signs. Since we assumed $i < i'$ and $j < j'$, we know that the sign of $\pm \det_{n-2} \mathbf{x}(i,i';j,j')$ given by Equation (5.8) is the expected sign, $(-1)^{i+j}(-1)^{i'+j'}$. But since $j' \not< j$, the sign given by Equation (5.9) is the reverse of the expected sign. Therefore, adding together Equations (5.8) and (5.9) gives 0, so $X_{i,j}X_{i',j'} + X_{i,j'}X_{i',j}$ is also in the perpendicular ideal. □

The proof of Proposition 5.5 is similar, except that

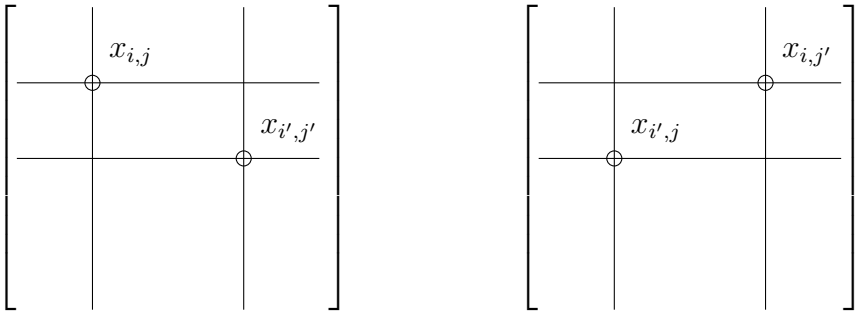
$$\frac{\partial}{\partial x_{i,j}} \frac{\partial}{\partial x_{i',j'}} \mathrm{perm}_n \mathbf{x} = \frac{\partial}{\partial x_{i,j'}} \frac{\partial}{\partial x_{i',j}} \mathrm{perm}_n \mathbf{x} = \mathrm{perm}_{n-2} \mathbf{x}(i,i';j,j')$$

with no confusion around signs.

We now come to the major result of this chapter: that the polynomials in Propositions 5.4 and 5.5 generate the entire ideals. The result was first proved by Shafiei in [12].

We will borrow some of Shafiei's terminology: we will call a monomial in $k[X_{1,1}, \ldots, X_{n,n}]$ *acceptable* if it contains no two variables from the same row or column of $\mathbf{X}$, and no variable has exponent greater than 1; and call a monomial *unacceptable* otherwise. Thus a monomial is unacceptable if and only if it is divisible by $X_{i,j}^2$, $X_{i,j}X_{i,j'}$ or $X_{i,j}X_{i',j}$ for some i, j, i', j'.

Figure 5.2: The derivatives $X_{i,j}X_{i',j'}$ and $X_{i,j'}X_{i',j}$ of the determinant give the same submatrix. Lines denote deleted rows and columns.



Theorem 5.6 (Shafiei [12, p. 10])**.** *The polynomials listed in Proposition 5.4 generate the ideal* $\det_n^\perp$*. In particular,* $\det_n^\perp$ *is generated by degree 2 polynomials.*

Proof. Let I denote the ideal generated by these polynomials. Proposition 5.4 tells us that $\det_n^\perp$ contains I, so we only need to prove the reverse inclusion.

Since the determinant is a homogeneous polynomial, Proposition 4.2 tells us that $\det_n^\perp$ is a homogeneous ideal, so it suffices to show that there are no more homogeneous elements in $\det_n^\perp$.

Suppose $f \in \det_n^\perp$ is homogeneous of degree d. Firstly, every term in f is either acceptable or unacceptable, so we can write

$$f = f_{\text{unacc.}} + f_{\text{acc.}} \tag{5.10}$$

where $f_{\text{unacc.}}$ has only unacceptable terms and $f_{\text{acc.}}$ has only acceptable terms.

Note that any unacceptable monomial is divisible by $X_{i,j}^2$, $X_{i,j}X_{i,j'}$ or $X_{i,j}X_{i',j}$, so $f_{\text{unacc.}}$ is in I. Also note that if $d > n$, by the pigeonhole principle every term in f must be unacceptable, and we are done. Hence assume $d \leq n$.

Now, suppose $\alpha X_{i_1,j_1} \cdots X_{i_d,j_d}$ is a term of $f_{\text{acc.}}$, with $\alpha \in k$. Without loss of generality, we can assume $i_1 < \cdots < i_d$. Suppose $1 \leq a < b \leq d$; then we can write

$$\alpha X_{i_1,j_1} \cdots X_{i_d,j_d} = \alpha \left(X_{i_a,j_a}X_{i_b,j_b}\right) \left(X_{i_1,j_1} \cdots \widehat{X_{i_a,j_a}} \cdots \widehat{X_{i_b,j_b}} \cdots X_{i_d,j_d}\right)$$

where a hat means the variable is omitted from the list.

Let $g(\mathbf{X}) = \left(X_{i_1,j_1} \cdots \widehat{X_{i_a,j_a}} \cdots \widehat{X_{i_b,j_b}} \cdots X_{i_d,j_d}\right)$ to simplify notation. Then

$$\begin{aligned}
&\alpha X_{i_1,j_1} \cdots X_{i_d,j_d} - \alpha \left(X_{i_a,j_a}X_{i_b,j_b} + X_{i_a,j_b}X_{i_b,j_a}\right) g(\mathbf{X}) \\
&= \alpha \left(X_{i_a,j_a}X_{i_b,j_b}\right) g(\mathbf{X}) - \alpha \left(X_{i_a,j_a}X_{i_b,j_b} + X_{i_a,j_b}X_{i_b,j_a}\right) g(\mathbf{X}) \\
&= -\alpha \left(X_{i_a,j_b}X_{i_b,j_a}\right) g(\mathbf{X}) \\
&= -\alpha \left(X_{i_1,j_1} \cdots X_{i_a,j_b} \cdots X_{i_b,j_a} \cdots X_{i_d,j_d}\right)
\end{aligned}$$

In effect, by subtracting a multiple of $(X_{i_a,j_a}X_{i_b,j_b} + X_{i_a,j_b}X_{i_b,j_a})$ from the term, we have transposed j_a and j_b (and reversed the sign).

Note that a and b were arbitrary. We now recall two facts about permutations:

- For any list $j_1, \ldots, j_d$ there is a permutation that puts them in increasing order, and
- Any permutation can be written as a sequence of transpositions.

We can conclude that by adding and subtracting multiples of the polynomial $(X_{i_a,j_a}X_{i_b,j_b} + X_{i_a,j_b}X_{i_b,j_a})$ for suitably chosen a and b, we can turn $f_{\text{acc.}}$ into a polynomial $f_{\text{ord.}}$ whose terms $X_{i_1,j_1}\cdots X_{i_d,j_d}$ have $i_1 < \cdots < i_d$ and $j_1 < \cdots < j_d$. Therefore, we can amend Equation (5.10) to say

$$f = f_{\text{unacc.}} + f_{\text{transp.}} + f_{\text{ord.}}$$

where $f_{\text{transp.}}$ is a polynomial in the ideal generated by $X_{i_a,j_a}X_{i_b,j_b}+X_{i_a,j_b}X_{i_b,j_a}$ described above, and $f_{\text{ord.}}$ is a polynomial whose terms are in order.

Now, by definition, f is an element of $\det_n^\perp$, so $f * \det_n = 0$. But by construction, all terms of $f_{\text{unacc.}}$ are unacceptable, so they are multiples of $X_{i,j}^2$, $X_{i,j}X_{i,j'}$ and $X_{i,j}X_{i',j}$ for some i, j, i', j', and thus elements of I. Similarly, all terms of $f_{\text{transp.}}$ are multiples of $X_{i,j}X_{i',j'} + X_{i,j'}X_{i',j}$ for some i, j, i', j', so $f_{\text{transp.}}$ is also an element of I. Therefore

$$\begin{aligned} 0 &= f * \det_n \\ &= (f_{\text{unacc.}} * \det_n) + (f_{\text{transp.}} * \det_n) + (f_{\text{ord.}} * \det_n) \\ &= 0 + 0 + (f_{\text{ord.}} * \det_n) \end{aligned}$$

But

$$f_{\text{ord}} = \sum_{\substack{1\le i_1<\cdots<i_d\le n \\ 1\le j_1<\cdots<j_d\le n}} \alpha_{I,J} X_{i_1,j_1}\cdots X_{i_d,j_d}$$

where $\alpha_{I,J}$ are coefficients depending on $i_1, \ldots, i_d$ and $j_1, \ldots, j_d$, so

$$f_{\text{ord.}} * \det_n = \sum_{\substack{1\le i_1<\cdots<i_d\le n \\ 1\le j_1<\cdots<j_d\le n}} \pm\alpha_{I,J} \det_{n-d} \mathbf{x}(i_1, \ldots, i_d; j_1, \ldots, j_d)$$

But this is a linear combination of determinants of distinct $(n-d)\times(n-d)$ submatrices of $\mathbf{x}$. Therefore, since the determinants of $m \times m$ submatrices

of $\mathbf{x}$ are linearly independent by Lemma 1.2, every $\alpha_{I,J}$ must be 0. Thus $f_{\text{ord.}} = 0$, and

$$f = f_{\text{unacc.}} + f_{\text{transp.}}$$

is an element of I.

Thus $\det_n^\perp \subseteq I$, so $\det_n^\perp = I$. □

And the same result holds for the permanent:

Theorem 5.7 (Shafiei [12, p. 10])**.** *The polynomials listed in Proposition 5.5 generate the ideal* $\mathrm{perm}_n^\perp$*. In particular,* $\mathrm{perm}_n^\perp$ *is generated by degree 2 polynomials.*

The proof is identical to the proof of Theorem 5.6, except that we subtract multiples of $(X_{i_a,j_a}X_{i_b,j_b} - X_{i_a,j_b}X_{i_b,j_a})$ to transpose j_a and j_b, and thus no reversal of sign occurs.

Chapter 6

Betti numbers

Now that we have completely described the S-modules $\det_n^\perp$ and $\operatorname{perm}_n^\perp$, our next goal is to consider their free resolutions. In this chapter, we will give some Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ for small n; we will use abstract results about Hilbert functions (specifically Corollary 3.6) to compute one of the Betti numbers; and finally we will give a set of relations that generates the entire space of second syzygies in degree 1. We conjecture that these relations in fact generate all second syzygies of the determinant, and compute the next Betti number if this is true.

6.1 Computational results

The Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ can be calculated by computer for small n. Tables 6.1 to 6.7, on pages 52 to 54, were computed using the Macaulay2 software. The code used is presented in Appendix A. Blank entries indicate 0. Due to memory limitations, some of these tables could only be partially computed: where this is the case, there may be more columns, but each column shown has no more non-zero values.

There are some interesting observations to make about these tables:

- The ring S is a polynomial ring with n^2 variables, so Corollary 3.11 tells us that the minimal free resolution of an S-module has length at most n^2. For the complete Betti tables, when $n \leq 4$, the minimal free resolutions of $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ have length exactly n^2, so these resolutions are as long as possible.

- When the complete Betti tables could be computed (so $n \leq 4$), the tables are rotationally symmetric. This is a consequence of the Gorenstein property and the symmetry of the Koszul resolution.

Table 6.1: Complete Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ where $n = 2$. Also see Appendix B for the full resolution.

(a) $S/\det_2^\perp$

	0	1	2	3	4
0	1				
1		9	16	9	
2					1

(b) $S/\operatorname{perm}_2^\perp$

	0	1	2	3	4
0	1				
1		9	16	9	
2					1

Table 6.2: Complete Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ where $n = 3$

(a) $S/\det_3^\perp$

	0	1	2	3	4	5	6	7	8	9
0	1									
1		36	160	315	288	100				
2					100	288	315	160	36	
3										1

(b) $S/\operatorname{perm}_3^\perp$

	0	1	2	3	4	5	6	7	8	9
0	1									
1		36	160	315	288	116				
2					116	288	315	160	36	
3										1

Table 6.3: Complete Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ where $n = 4$

(a) $S/\det_4^\perp$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1		100	800	3075	6496	7700	4800	1225									
2					2500	16800	51275	93600	113256	93600	51275	16800	2500				
3										1225	4800	7700	6496	3075	800	100	
4																	1

(b) $S/\operatorname{perm}_4^\perp$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1																
1		100	800	3087	6688	8400	4320	794									
2			12	192	3200	16320	50844	93600	113256	93600	50844	16320	3200	192	12		
3										794	4320	8400	6688	3087	800	100	
4																	1

Table 6.4: Partial Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ where $n = 5$

(a) $S/\det_5)^\perp$

	0	1	2	3	⋯
0	1				
1		225	2800	17325	
⋮					

(b) $S/\operatorname{perm}_5)^\perp$

	0	1	2	3	⋯
0	1				
1		225	2800	17425	
2			100	2400	
⋮					

Table 6.5: Partial Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ where $n = 6$

(a) $S/\det_6^\perp$

	0	1	2	⋯
0	1			
1		441	7840	
⋮				

(b) $S/\operatorname{perm}_6^\perp$

	0	1	2	⋯
0	1			
1		441	7840	
2			450	
⋮				

Table 6.6: Partial Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ where $n = 7$

(a) $S/\det_7^\perp$

	0	1	2	⋯
0	1			
1		784	18816	
⋮				

(b) $S/\operatorname{perm}_7^\perp$

	0	1	2	⋯
0	1			
1		784	18816	
2			1470	
⋮				

Table 6.7: Partial Betti tables for $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$ where $n = 8$

(a) $S/\det_8^\perp$

	0	1	⋯
0	1		
1		1296	
⋮			

(b) $S/\operatorname{perm}_8^\perp$

	0	1	⋯
0	1		
1		1296	
⋮			

- When $n \geq 3$, the Betti tables of $S/\operatorname{perm}_n^\perp$ and $S/\det_n^\perp$ are different. For example, when $n = 3$, the numbers in column 4, row 2 and column 5, row 1 are different between the two tables.

- When $n \geq 4$, $S/\operatorname{perm}_n^\perp$ has non-zero Betti numbers in column 2, row 2 and column 3, row 2, while $S/\det_n^\perp$ has 0 in these positions — this means that the permanent has additional second and third syzygies with degree 2 that don't appear for the determinant.

- These tables were computed over the field $k = \mathbb{Z}/7$. The tables are the same for most fields considered, but in $\mathbb{Z}/2$ and $\mathbb{Z}/3$, some numbers change — in particular, over $\mathbb{Z}/2$ the determinant and permanent are equal, and the Betti tables for $S/\det_n^\perp = S/\operatorname{perm}_n^\perp$ are closest to the tables for the permanent shown here.

Appendix B contains the full details of the resolution of $S/\det_n^\perp$ when $n = 2$.

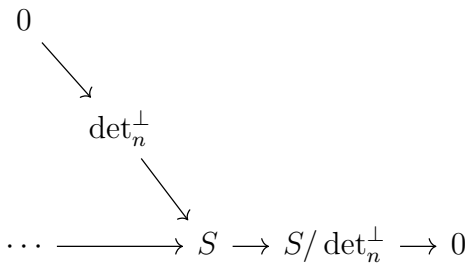
6.2 Betti numbers $\beta_{1,2}$ and $\beta_{2,3}$

6.2.1 Betti number $\beta_{1,2}$

Now that we have a description of $\det_n^\perp$, we can begin computing the minimal free resolution of $S/\det_n^\perp$. We have the exact sequence

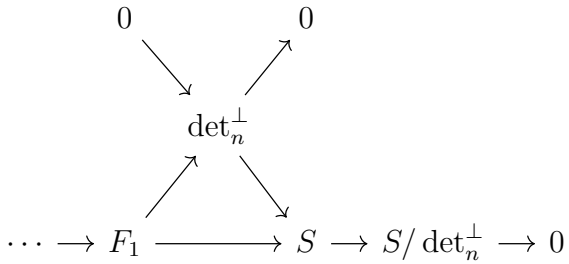
$$0 \to \det_n^\perp \to S \to S/\det_n^\perp \to 0$$

so the minimal resolution begins



To find the next component of the minimal resolution, we we need to know a minimal set of generators of $\det_n^\perp$. But we found exactly that in Chapter 5: Theorem 5.6 describes a set of generators, and Proposition 5.4

asserts that they are linearly independent, and hence minimal. Therefore we can extend the resolution:



Since the generators of $\det_n^\perp$ are all degree 2, F_1 must be a direct sum of copies of $S(-2)$, that is,

$$F_1 = S(-2)^{\beta_{1,2}} \tag{6.1}$$

where $\beta_{1,2}$ is the number of generators of $\det_n^\perp$.

We can compute the number $\beta_{1,2}$ using the description of the generators given in Proposition 5.3. This lets us specify a generator by first picking i and i' from $\{1, \ldots, n\}$, where the order doesn't matter but repetitions are allowed, and then independently picking j and j' with the same rules. Thus the number of generators is[1]

$$\beta_{1,2} = \binom{n+1}{2}^2 \tag{6.2}$$

$$= \frac{1}{4}n^2(n+1)^2. \tag{6.3}$$

[1]We could also use the description from Proposition 5.4 to compute this value.

The first type of generator, $X_{i,j}^2$, is specified by choosing i and j independently out of $\{1, \ldots, n\}$, so there are n^2 of this type of generator.

The second type is specified by choosing one row out of n (choosing i), and then picking a subset of 2 elements of that row (choosing j and j'); hence there are $n\binom{n}{2}$ of these generators. Similarly, there are $n\binom{n}{2}$ of the third type of generator.

The fourth type of generator is specified by choosing i and i' as distinct elements of $\{1, \ldots, n\}$, and then choosing j and j' independently, so there are $\binom{n}{2}^2$ of these generators.

Therefore the total number is

$$n^2 + 2n\binom{n}{2} + \binom{n}{2}^2 = \left(n + \binom{n}{2}\right)^2$$
$$= \binom{n+1}{2}^2$$

which agrees with Equation (6.2).

For small values of n, this evaluates to be

n	1	2	3	4	5	6	7	8
$\beta_{1,2}$	1	9	36	100	225	441	784	1296

which agrees with the values computed with Macaulay2.

6.2.2 Betti number $\beta_{2,3}$

The minimal free resolution of $S/\det_n^\perp$ thus far is

$$\cdots \longrightarrow F_2 \longrightarrow S(-2)^{\beta_{1,2}} \longrightarrow S \longrightarrow S/\det_n^\perp \longrightarrow 0$$

with $F_2 = S(-3)^{\beta_{2,3}} \oplus S(-4)^{\beta_{2,4}} \oplus \cdots$: we know that the least a with $R(-a)$ appearing in this sum is 3, by Proposition 3.13.

We have enough information to compute the next Betti number, $\beta_{2,3}$, the number of linear relations among the generators of $\det_n^\perp$. As above, we will use the formula for $H_M(d)$ in terms of the Hilbert functions of its free resolution, given in Corollary 3.6.

To illustrate this idea, we will first use it to verify our calculation of $\beta_{1,2}$. By Corollary 3.6, we have the expression

$$H_{S/\det_n^\perp}(2) = \sum_i (-1)^i H_{F_i}(2).$$

Due to Proposition 3.13, the only components of the resolution that are non-zero in degree 2 are $F_0 = S$ and $F_1 = S(-2)^{\beta_{1,2}}$. Therefore

$$\begin{aligned} H_{S/\det_n^\perp}(2) &= H_{F_0}(2) - H_{F_1}(2) \\ &= H_S(2) - H_{S(-2)^{\beta_{1,2}}}(2). \end{aligned} \tag{6.4}$$

Also, the degree 2 part of $S(-2)^{\beta_{1,2}}$ is the degree 0 part of $S^{\beta_{1,2}}$, which is simply $k^{\beta_{1,2}}$ as a vector space, hence

$$H_{S(-2)^{\beta_{1,2}}}(2) = \beta_{1,2}. \tag{6.5}$$

We also know $H_{S/\det_n^\perp}(2)$: by Proposition 5.2, it is

$$H_{S/\det_n^\perp}(2) = \binom{n}{2}^2. \tag{6.6}$$

And $H_S(2)$ is given by Lemma 3.4, noting that S is a polynomial ring with n^2 variables:

$$H_S(2) = \binom{n^2+1}{2}. \tag{6.7}$$

Therefore, putting Equations (6.4) to (6.7) together,

$$\begin{aligned}\beta_{1,2} &= H_S(2) - H_{S/\det_n^\perp}(2) \\ &= \binom{n^2+1}{2} - \binom{n}{2}^2 \\ &= \frac{1}{4}n^2(n+1)^2\end{aligned}$$

which agrees with the value in Equation (6.3).

Now, let us apply this method to compute $\beta_{2,3}$ by examining $H_{S/\det_n^\perp}(3)$. As before, none of the components of the minimal resolution beyond F_2 have a non-zero part in degree 3, so Corollary 3.6 gives us

$$H_{S/\det_n^\perp}(3) = H_S(3) - H_{S(-2)^{\beta_{1,2}}}(3) + H_{F_2}(3). \tag{6.8}$$

The degree 3 part of F_2 is $k^{\beta_{2,3}}$, as above, so

$$H_{F_2}(3) = \beta_{2,3}. \tag{6.9}$$

By Proposition 5.2,

$$H_{S/\det_n^\perp} = \binom{n}{3}^2. \tag{6.10}$$

And by Lemma 3.4,

$$H_S(3) = \binom{n^2+2}{3}. \tag{6.11}$$

The degree 3 part of $S(-2)^{\beta_{1,2}}$ is $\beta_{1,2}$ times the degree 3 part of $S(-2)$, which is the degree 1 part of S. Thus

$$\begin{aligned}H_{S(-2)^{\beta_{1,2}}}(3) &= \beta_{1,2}\binom{n^2}{1} \\ &= \binom{n+1}{2}^2 n^2.\end{aligned} \tag{6.12}$$

So when we combine Equations (6.8) to (6.12), we find

$$\begin{aligned}\beta_{2,3} &= H_{S/\det_n^\perp}(3) - H_S(3) + H_{S(-2)_{1,2}^\beta}(3)\\ &= \binom{n}{3}^2 - \binom{n^2+2}{3} + \binom{n+1}{2}^2 n^2\\ &= \frac{1}{9}n^2(n+1)^2(n-1)(n+2) \qquad (6.13)\\ &= 4\binom{n+1}{3}\binom{n+2}{3}. \qquad (6.14)\end{aligned}$$

For small values of n, this equates to

n	1	2	3	4	5	6	7	8
$\beta_{2,3}$	0	16	160	800	2800	7840	18816	40320

which is the same as the values computed by Macaulay2 in Tables 6.1 to 6.6.

6.3 A description of the linear second syzygies of $S/\det_n^\perp$

In this section we will give a list of relations among the generators of $\det_n^\perp$ that give a basis for F_2 in degree 1. This list will not be as simple as the list of generators for $\det_n^\perp$ found in Chapter 5, but fortunately this time we already know how many relations to expect: this number is $\beta_{2,3}$. Therefore, to give a complete description of the linear second syzygies, we need only find enough linearly independent relations.

It will help to have a general description of the dimension of some spaces of relations. To do this, we will exploit the symmetry of the determinant under permutations of the rows and columns, discussed after Theorem 1.8.

A relation ρ is a linear combination of the generators of $\det_n^\perp$, with coefficients in S. When we say a relation "involves" some variables, we mean that these variables appear in either the generators or the coefficients. Define the matrix

$$\mathbf{X} = \begin{bmatrix} X_{1,1} & \dots & X_{1,n} \\ \vdots & & \vdots \\ X_{n,1} & \dots & X_{n,n} \end{bmatrix}.$$

analogously to $\mathbf{x}$.

Lemma 6.1. *Suppose ρ is a degree d relation involving variables from some $p \times q$ submatrix $\mathbf{m}_\rho$ of $\mathbf{X}$, and that this is the smallest submatrix containing all*

variables in ρ. Then the orbit of ρ under $\mathrm{S}_n \times \mathrm{S}_n$, where S_n is the symmetric group and $(\sigma, \mu) \cdot X_{i,j} = X_{\sigma i, \mu j}$, generates a subspace of $(F_2)_d$. The dimension of this subspace is

$$\Omega(\rho)\binom{n}{p}\binom{n}{q} \tag{6.15}$$

where $\Omega(\rho)$ is the dimension of the orbit of ρ under the action $\mathrm{S}_p \times \mathrm{S}_q$ on the $p \times q$ submatrix.

Proof. Denote the orbit of ρ under a group G by $G \cdot \rho$.

We know from Theorem 1.8 that $\det_n \mathbf{x}$ is symmetric under permutations of the rows and columns by $\mathrm{S}_n \times \mathrm{S}_n$. It follows that $\det_n^\perp$ is also symmetric under this action, so it has a symmetric set of generators. We note that the set of generators we described in Chapter 5 is indeed symmetric under $\mathrm{S}_n \times \mathrm{S}_n$.

Therefore the module of relations among these generators must be symmetric too, hence the action of $\mathrm{S}_n \times \mathrm{S}_n$ sends relations to relations. Therefore the orbit of ρ stays within the set of relations, so the vector space generated by the orbit is a subspace of the space of degree d relations.

Let $P = \{i_1, \ldots, i_p\}$ and $Q = \{j_1, \ldots, j_q\}$ be subsets of $\{1, \ldots, n\}$, where $i_1, \ldots, i_p$ are the rows appearing in the submatrix $\mathbf{m}$, and $j_1, \ldots, j_q$ are the columns. Consider the set $G_P \subseteq \mathrm{S}_n$ of permutations that fix P, setwise (so G_P is the set of permutations σ such that $\sigma(i) \in P$ iff $i \in P$). It is clear that G_P is a subgroup of S_n, although it is not in general a normal subgroup.

If a permutation fixes P, then it must also fix $P^c = \{1, \ldots, n\} \setminus P$, so elements of G_P can be written uniquely as a composition $\phi \circ \psi$ of a permutation ϕ on P and a permutation ψ on P^c. Therefore the number of elements of G_P is $p!(n-p)!$, and the number of cosets, denoted $[\mathrm{S}_n : G_P]$, is

$$\begin{aligned}[\mathrm{S}_n : G_P] &= \frac{n!}{p!(n-p)!} \\ &= \binom{n}{p}\end{aligned} \tag{6.16}$$

Similarly, $[\mathrm{S}_n : G_Q] = \binom{n}{q}$.

Define the group $G_{P\times Q} = G_P \times G_Q \subseteq \mathrm{S}_n \times \mathrm{S}_n$. The index of this is

$$[\mathrm{S}_n \times \mathrm{S}_n : G_{P\times Q}] = \binom{n}{p}\binom{n}{q}$$

The left cosets of $G_{P\times Q}$ partition $\mathrm{S}_n \times \mathrm{S}_n$. If $H = (\sigma, \mu)G_{P\times Q}$ is a coset of $G_{P\times Q}$, let $k\{H \cdot \rho\}$ be the vector space generated by the orbit of ρ under H.

We claim that the vector spaces $k\{H \cdot \rho\}$ are independent. By construction, $H \cdot \rho$ is a set of relation with variables in the submatrix whose rows are $\sigma(P)$ and whose columns are $\mu(Q)$. Since p and q are minimal, every row and every column of this matrix must contain a variable appearing in $(\sigma, \mu) \cdot \rho$, so no term of $(\sigma, \mu) \cdot \rho$ can appear in any other $p \times q$ submatrix. Therefore there can be no cancellation in a linear combination of vectors from different spaces $k\{H \cdot \rho\}$, so the spaces are independent.

Therefore, we have

$$\begin{aligned}\dim(\mathrm{S}_n \times \mathrm{S}_n \cdot \rho) &= \dim\Big(\sum_{\text{cosets } H} k\{H \cdot \rho\}\Big) \\ &= \sum_{\text{cosets } H} \dim(k\{H \cdot \rho\})\end{aligned}$$

Since every coset has the same number of elements and the set of relations is symmetric, every space $k\{H \cdot \rho\}$ has the same dimension. In particular, $G_{P\times Q}$ is a coset of itself, so

$$\dim(\mathrm{S}_n \times \mathrm{S}_n \cdot \rho) = [\mathrm{S}_n \times \mathrm{S}_n : G_{P\times Q}] \dim(k\{G_{P\times Q} \cdot \rho\})$$

But $[\mathrm{S}_n \times \mathrm{S}_n : G_{P\times Q}] = \binom{n}{p}\binom{n}{q}$, and we defined $\Omega(\rho) = \dim(k\{G_{P\times Q} \cdot \rho\})$. Therefore

$$\dim(\mathrm{S}_n \times \mathrm{S}_n \cdot \rho) = \Omega(\rho)\binom{n}{p}\binom{n}{q}. \tag{6.17}$$

□

There is one other symmetry which will be useful:

Lemma 6.2. *Define the transposition action $-^\top : S \to S$ that sends $X_{i,j} \mapsto X_{j,i}$. Then if ρ is a relation, then $\rho^\top$ is a relation.*

Proof. We know that $\det_n$ is symmetric under transposition, so $\det_n^\perp$ has a symmetric set of generators. We note that the set described in Chapter 5 is such a set, so the relations are also symmetric. □

We now have a way of using a single relation to construct a large set of relations, by permutating and transposing, and we have a systematic way of computing the dimension of the resulting space of relations, based on a small submatrix of $\mathbf{X}$.

We now list some relations explicitly. Eventually, we aim to prove that these relations, and their orbits under $\mathrm{S}_n \times \mathrm{S}_n$ and transposing, generate all linear relations.

Proposition 6.3. *The following are relations between the generators of* $\det_n^\perp$*, when* n *is large enough for all the variables to be defined (so* $n \geq 2$ *or* $n \geq 3$*):*

$$\rho_1 = X_{1,1}(X_{1,2}^2) - X_{1,2}(X_{1,1}X_{1,2}) \tag{6.18}$$

$$\rho_2 = X_{1,1}(X_{1,2}X_{1,3}) - X_{1,2}(X_{1,1}X_{1,3}) \tag{6.19}$$

$$\rho_3 = X_{1,2}(X_{1,1}X_{2,1}) - X_{2,1}(X_{1,1}X_{1,2}) \tag{6.20}$$

$$\rho_4 = X_{1,1}(X_{1,1}X_{2,2} + X_{1,2}X_{2,1}) - X_{2,2}(X_{1,1}^2) - X_{1,2}(X_{1,1}X_{2,1}) \tag{6.21}$$

$$\rho_5 = X_{1,3}(X_{1,1}X_{2,2} + X_{1,2}X_{2,1}) - X_{2,2}(X_{1,1}X_{1,3}) - X_{2,1}(X_{1,2}X_{1,3}) \tag{6.22}$$

$$\begin{aligned}\rho_6 = {} & X_{1,2}(X_{2,1}X_{3,3} + X_{2,3}X_{3,1}) + X_{1,3}(X_{2,1}X_{3,2} + X_{2,2}X_{3,1}) \\ & - X_{2,1}(X_{1,2}X_{3,3} + X_{1,3}X_{3,2}) - X_{3,1}(X_{1,2}X_{2,3} + X_{1,3}X_{2,2})\end{aligned} \tag{6.23}$$

Proof. Expand the brackets. □

This notation makes it clear that these are in fact relations, but the symmetries are hard to see. We will introduce some pictorial notation to help.

Each term of these relations is shown in the minimal $p \times q$ submatrix $\mathbf{m}_\rho$ containing the variables involved in the resolution, from Lemma 6.1. Denote the coefficient by a black dot, and denote the generator of $\det_n^\perp$ by a rectangle with corners at the positions of the generator's variables: the generator $X_{i,j}X_{i',j'} + X_{1,j'}X_{i',j}$ is a rectangle between the i,jth, i,j'th, i',jth and i',j'th positions of the matrix, the generator $X_{i,j}X_{i,j'}$ is a rectangle along the ith row between the jth and j'th positions, and the generator $X_{i,j}^2$ is a square in the i,jth position. For example,

$$X_{1,2}(X_{1,1}X_{2,1}) = \left[\begin{array}{cc} \square & \bullet \\ \square & \end{array}\right].$$

In this notation,

$$\rho_1 = \left[\bullet \;\; \square\right] - \left[\square\!\!\bullet\right] \tag{6.24}$$

$$\rho_2 = \left[\bullet \;\; \square\!\square\right] - \left[\square\!\bullet\!\square\right] \tag{6.25}$$

$$\rho_3 = \left[\begin{array}{cc} \square & \bullet \\ \square & \end{array}\right] - \left[\begin{array}{cc} \square\!\square & \\ \bullet & \end{array}\right] \tag{6.26}$$

$$\rho_4 = \left[\begin{array}{cc} \bullet & \\ \square & \end{array}\right] - \left[\begin{array}{cc} \square & \\ & \bullet \end{array}\right] - \left[\begin{array}{cc} \square & \bullet \\ \square & \end{array}\right] \tag{6.27}$$

$$\rho_5 = \left[\begin{array}{|c|c|}\hline & \bullet \\ \hline \end{array}\right] - \left[\begin{array}{|c|}\hline \\ \hline \bullet \\ \cline{1-1}\end{array}\right] - \left[\begin{array}{c|c|}\multicolumn{1}{c}{\bullet} & \cline{2-2} \\ \cline{2-2}\end{array}\right] \tag{6.28}$$

$$\rho_6 = \left[\begin{array}{|c|}\hline \bullet \\ \hline \\ \hline\end{array}\right] + \left[\begin{array}{|c|c|}\hline & \bullet \\ \hline \end{array}\right] - \left[\begin{array}{c|c|}\multicolumn{1}{c}{\bullet} & \cline{2-2} \\ \cline{2-2}\end{array}\right] - \left[\begin{array}{c|c|}\multicolumn{1}{c}{} & \cline{2-2} \\ \cline{2-2}\multicolumn{1}{c}{\bullet} & \end{array}\right] \tag{6.29}$$

Let us compute the dimensions of the orbits of these relations. Note that although some of these relations only make sense when $n \geq 2$ or $n \geq 3$, we can still use the formula from Equation (6.15) in Lemma 6.1 to compute the dimensions of the spaces their orbits generate when n is too small, since $\binom{n}{p} = 0$ if $n < p$.

Proposition 6.4. *The space of relations generated by permutations of ρ_1 on $\mathbf{m}_{\rho_1}$ is*

$$\Omega(\rho_1) = 2. \tag{6.30}$$

Proof. Since ρ_1 is a relation on a 1×2 matrix, the permutation group is $\mathrm{S}_1 \times \mathrm{S}_2 \cong \mathrm{S}_2$, so the orbit of ρ_1 consists of

$$(1) \cdot \rho_1 = \left[\bullet \;\; \square\right] - \left[\square\!\bullet\right] \text{ and}$$
$$(1\ 2) \cdot \rho_1 = \left[\square \;\; \bullet\right] - \left[\bullet\!\square\right].$$

Neither term of $(1\ 2) \cdot \rho_1$ appears in $(1) \cdot \rho_1$ or vice versa, so they are linearly independent. Therefore the dimension of the subspace of $(F_2)_1$ that they generate has dimension 2. □

Proposition 6.5. *The space of relations generated by permutations of ρ_2 on $\mathbf{m}_{\rho_2}$ is*

$$\Omega(\rho_2) = 2. \tag{6.31}$$

Proof. The relation ρ_2 is on a 1×3 matrix, so the permutation group is $\mathrm{S}_1 \times \mathrm{S}_3 \cong \mathrm{S}_3$. We note that $(1\ 2)$ turns the first term into the second and vice versa, so $(1\ 2) \cdot \rho_2$ is just $-\rho_2$, which is not a linearly independent relation. We thus only need to consider cosets of $\{(1), (1\ 2)\}$, so the orbit is

$$(1) \cdot \rho_2 = -(1\ 2) \cdot \rho_2 = \left[\bullet \;\; \square\right] - \left[\square\!\bullet\right],$$
$$(1\ 2\ 3) \cdot \rho_2 = -(1\ 3) \cdot \rho_2 = \left[\square\!\bullet\right] - \left[\square \;\; \bullet\right], \text{ and}$$
$$(1\ 3\ 2) \cdot \rho_2 = -(2\ 3) \cdot \rho_2 = \left[\square \;\; \bullet\right] - \left[\bullet \;\; \square\right]$$

The first two of these relations are clearly linearly independent, but we observe that

$$(1) \cdot \rho_2 + (1\ 2\ 3) \cdot \rho_2 + (1\ 3\ 2) \cdot \rho_2 = 0.$$

Therefore the maximal linearly independent set has two elements, and the dimension of the vector space generated by these relations is 2. □

Proposition 6.6. *The space of relations generated by permutations of ρ_3 on $\mathbf{m}_{\rho_3}$ is*

$$\Omega(\rho_3) = 4. \tag{6.32}$$

Proof. The permutation group of ρ_3 is $\mathrm{S}_2 \times \mathrm{S}_2$, and the orbit is

$$\begin{aligned}
\big((1),(1)\big) \cdot \rho_3 &= \left[\begin{array}{|c|c|}\hline & \bullet \\ \hline \end{array}\right] - \left[\begin{array}{|c|}\hline \\ \hline \bullet \\ \hline \end{array}\right], \\
\big((1),(1\ 2)\big) \cdot \rho_3 &= \left[\begin{array}{|c|c|}\hline \bullet & \\ \hline \end{array}\right] - \left[\begin{array}{|c|}\hline \\ \hline \bullet \\ \hline \end{array}\right], \\
\big((1\ 2),(1)\big) \cdot \rho_3 &= \left[\begin{array}{|c|c|}\hline & \bullet \\ \hline \end{array}\right] - \left[\begin{array}{|c|}\hline \bullet \\ \hline \\ \hline \end{array}\right], \text{ and} \\
\big((1\ 2),(1\ 2)\big) \cdot \rho_3 &= \left[\begin{array}{|c|c|}\hline \bullet & \\ \hline \end{array}\right] - \left[\begin{array}{|c|}\hline \bullet \\ \hline \\ \hline \end{array}\right].
\end{aligned}$$

The terms of these are entirely distinct, so they are clearly linearly independent, and the dimension of the space they generate is 4. □

Proposition 6.7. *The space of relations generated by permutations of ρ_4 on $\mathbf{m}_{\rho_4}$ is*

$$\Omega(\rho_4) = 4. \tag{6.33}$$

Proof. Recall that

$$\rho_4 = \left[\begin{array}{|c|c|}\hline \bullet & \\ \hline & \\ \hline \end{array}\right] - \left[\begin{array}{|c|c|}\hline & \\ \hline & \bullet \\ \hline \end{array}\right] - \left[\begin{array}{|c|c|}\hline & \bullet \\ \hline & \\ \hline \end{array}\right]. \tag{6.27}$$

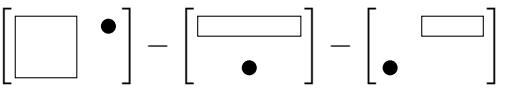
We already observed in Proposition 6.6 that the orbit of $\left[\begin{array}{|c|c|}\hline & \bullet \\ \hline \end{array}\right]$ under $\mathrm{S}_2 \times \mathrm{S}_2$ is a linearly independent set. No other element of this orbit appears in ρ_4, so the orbit of ρ_4 must be linearly independent. Therefore the dimension of the space it generates is $|\mathrm{S}_2 \times \mathrm{S}_2| = 4$. □

Remark. Note that we could have made the same argument with the orbits of $\left[\begin{array}{|c|c|}\hline \bullet & \\ \hline & \\ \hline \end{array}\right]$ or $\left[\begin{array}{|c|c|}\hline & \\ \hline & \bullet \\ \hline \end{array}\right]$ instead.

Proposition 6.8. *The space of relations generated by permutations of ρ_5 on $\mathbf{m}_{\rho_5}$ is*

$$\Omega(\rho_5) = 6. \tag{6.34}$$

Proof. Recall that

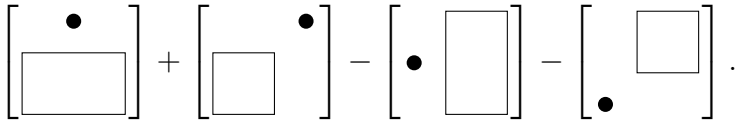
$\rho_5 =$  (6.28)

The action of $\big((1),(1\ 2)\big)$ on ρ_5, that is, swapping the first and second columns, interchanges the second and third terms of ρ_5, so overall it has no effect. However, every other permutation alters the first term, so the total number of linearly independent relations in the orbit of ρ_5 under $\mathrm{S}_2 \times \mathrm{S}_3$ is the number of cosets of the subgroup generated by $\big((1),(1\ 2)\big)$, which is $2!3!/2 = 6$. □

Proposition 6.9. *The space of relations generated by permutations of ρ_6 on $\mathbf{m}_{\rho_6}$ is*

$$\Omega(\rho_6) = 4. \tag{6.35}$$

Proof. Recall that

$\rho_6 =$  (6.29)

Notice that in each of the terms, the variables in the generator (i.e. the corners of the rectangle) are exactly the positions in the matrix that are not in the same row or column as the coefficient (i.e. the dot). Thus with this information, we need only specify the position of the coefficient to specify the term. We therefore introduce a more concise notation: on a 3×3 matrix, mark the positions where a coefficient appears, with a plus if that term is added and a minus if the term is subtracted; thus:

$$\rho_6 = \begin{bmatrix} & + & + \\ - & & \\ - & & \end{bmatrix}$$

In this notation, a pattern appears: we can create ρ_6 by putting a plus sign in all positions in the first row, and a minus sign everywhere in the first column, and cancelling the plus and the minus in position $(1,1)$.

In this new notation it is obvious that the permutations $\big((1),(2\ 3)\big)$ and $\big((2\ 3),(1)\big)$ have no effect on ρ_6. (We can see this in the dots-and-rectangles notation too: for example, $\big((1),(2\ 3)\big)$ swaps the first two terms and leaves the second two unchanged.) Therefore we only need to consider cosets of the subgroup generated by these two permutations: this subgroup is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, so there are $(3!)^2/4 = 9$ cosets.

Give ρ_6 the new name $R_{1,1}$, and generalise this notation to its permutations so that that $R_{i,j}$ has plusses in the ith row and minuses in the jth column. Equivalently, $R_{i,j} = \big((1\ i), (1\ j)\big) \cdot \rho_6$, taking $(1\ i) = (1)$ if $i = 1$. The 9 cosets we are considering correspond to the 9 relations $R_{i,j}$ with $i, j \in \{1, 2, 3\}$.

To examine the linear dependence in these diagrams, we have the following lemma:

Lemma 6.10. *$R_{1,\sigma 1} + R_{2,\sigma 2} + R_{3,\sigma 3} = 0$ for any $\sigma \in \mathrm{S}_3$. Any linear combination of the $R_{i,j}$s that cancels to 0 is a sum of linear combinations of this form.*

Proof of lemma. To see that this equation holds, observe that each $R_{i,\sigma i}$ puts a plus sign in every position in the ith row and a minus sign everywhere in the (σi)th column, so after adding all three $R_{i,\sigma i}$, there is a plus sign in every position in every row, and a minus sign everywhere in every column. These all cancel, leaving 0.

Suppose we have some linear combination $\sum_{i,j} \alpha_{i,j} R_{i,j}$ that equals zero. Construct the matrix

$$\boldsymbol{\alpha} = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} \end{bmatrix}.$$

Since each $R_{i,j}$ contributes $+1$ everywhere in the ith row and -1 in the jth column, the condition that the linear combination equals zero is equivalent to the condition that for each i, j, the sum of the entries of the ith row of $\boldsymbol{\alpha}$ is equal to the sum of the jth column, which implies that all rows and all columns have the same sum. But then $\boldsymbol{\alpha}$ is a semi-magic matrix, so Theorem 1.12 tells us that $\boldsymbol{\alpha}$ is a linear combination of permutation matrices, and permutation matrices correspond exactly to $R_{1,\sigma 1} + R_{2,\sigma 2} + R_{3,\sigma 3}$. □

We claim that the least generating set of the $R_{i,j}$s has four elements. To do this, we must show that no set of three of the $R_{i,j}$s produces all of them, and that there is a set of four that does.

Suppose we have a set of three of the $R_{i,j}$s. By symmetry, there are only four situations to consider, shown in Figure 6.1:

- All three of the $R_{i,j}$ are in the same row or column.

  In this case, without loss of generality the three $R_{i,j}$s might as well be $R_{1,1}$, $R_{1,2}$ and $R_{1,3}$. But Lemma 6.10 tells us that no more relations can be made.

- Two of the three $R_{i,j}$ are in the same row or column, in which case:

Figure 6.1: Relations generated by some sets of $R_{i,j}$. The starting relations are highlighted in grey, and the other relations they generate are also shown.

(a) All three $R_{i,j}$ in the same row

$$\begin{bmatrix} R_{1,1} & R_{1,2} & R_{1,3} \\ & & \end{bmatrix}$$

(b) Two $R_{i,j}$ in the same row, the third in the same column as another

$$\begin{bmatrix} R_{1,1} & R_{1,2} & \\ R_{2,1} & R_{2,2} & \\ & & R_{3,3} \end{bmatrix}$$

(c) Two $R_{i,j}$ in the same row, the third not in the same column as another

$$\begin{bmatrix} R_{1,1} & R_{1,2} & \\ & & R_{2,3} \\ R_{3,1} & R_{3,2} & \end{bmatrix}$$

(d) No $R_{i,j}$ in the same row or column

$$\begin{bmatrix} R_{1,1} & & \\ & R_{2,2} & \\ & & R_{3,3} \end{bmatrix}$$

(e) A set of four $R_{i,j}$ that generate all

$$\begin{bmatrix} R_{1,1} & R_{1,2} & R_{1,3} \\ R_{2,1} & R_{2,2} & R_{2,3} \\ R_{3,1} & R_{3,2} & R_{3,3} \end{bmatrix}$$

  - The third $R_{i,j}$ is in the same column or row as another.

    Without loss of generality, we may take these to be $R_{1,1}$, $R_{1,2}$ and $R_{2,1}$. Using Lemma 6.10, we also obtain $R_{3,3} = -R_{1,2} - R_{2,1}$ and $R_{2,2} = -R_{1,1} - R_{3,3}$, but no other $R_{i,j}$.
  - The third $R_{i,j}$ is not in the same column or row as another.

    Without loss of generality, take $R_{1,1}$, $R_{1,2}$ and $R_{2,3}$. We can also create $R_{3,1} = -R_{1,2} - R_{2,3}$ and $R_{3,2} = -R_{1,1} - R_{2,3}$, but nothing else.

- None of the three $R_{i,j}$ are in the same row or column.

  We may as well take $R_{1,1}$, $R_{2,2}$ and $R_{3,3}$. Then no other $R_{i,j}$ can be produced.

Hence a set of three of the $R_{i,j}$ is not enough to generate all nine.
However, the set $R_{1,2}$, $R_{1,3}$, $R_{2,1}$ and $R_{3,1}$ is sufficient. We obtain:

- $R_{2,2} = -R_{1,3} - R_{3,1}$,
- $R_{2,3} = -R_{1,2} - R_{3,1}$,
- $R_{3,2} = -R_{1,3} - R_{2,1}$,

- $R_{3,3} = -R_{1,2} - R_{2,1}$, and
- $R_{1,1} = -R_{2,2} - R_{3,3}$.

So the least spanning set of the nine $R_{i,j}$ has four elements. Therefore the dimension of the space they span, that is, the dimension of the space generated by the permutations of ρ_6, is 4. □

Finally, we can put this information together to give a full description of the linear relations.

Theorem 6.11. *The permutations of the six relations $\rho_1, \ldots, \rho_6$ and their transposes generate the entire space of linear second syzygies.*

Proof. First, consider the transposes of these six relations. The relations ρ_1, ρ_2 and ρ_5 are on strictly rectangular matrices, so their transposes are clearly distinct relations. However, the transpose of ρ_3 is simply $-\rho_3$, the transpose of ρ_4 is $\rho_4 + \rho_3$, and the transpose of ρ_6 is $-\rho_6$, so these three transposes do not contribute any new linearly independent relations.

Note that where the orbits of ρ and its transpose are independent (i.e. for ρ_1, ρ_2 and ρ_5), by symmetry the dimension of the space generated by both ρ and its transpose is

$$\Omega(\rho)\binom{n}{p}\binom{n}{q} + \Omega(\rho^T)\binom{n}{q}\binom{n}{p} = 2\Omega(\rho)\binom{n}{p}\binom{n}{q}.$$

We claim that the spaces generate by the permutations of $\rho_1, \ldots, \rho_6$ and permutations of the transposes of ρ_1, ρ_2 and ρ_5 are independent vector spaces. This is obvious: no permutation of any term in any of these relations appears in any other, with the exception of $\begin{bmatrix} \square & \bullet \\ \square & \end{bmatrix}$ in both ρ_3 and ρ_4, whose other terms are entirely distinct. Thus there can be no cancellation in a sum of vectors from the corresponding spaces.

Therefore the dimension of the space spanned by the orbit of all these relations is the sum of the dimensions of the spaces of the individual relations' orbits. Call this space V. We can use the formula of Equation (6.15) in

Lemma 6.1 to compute this:

$$\begin{aligned}\dim V &= 2\Omega(\rho_1)\binom{n}{1}\binom{n}{2} + 2\Omega(\rho_2)\binom{n}{1}\binom{n}{3} + \Omega(\rho_3)\binom{n}{2}\binom{n}{2} \\ &\quad + \Omega(\rho_4)\binom{n}{2}\binom{n}{2} + 2\Omega(\rho_5)\binom{n}{2}\binom{n}{3} + \Omega(\rho_6)\binom{n}{3}\binom{n}{3} \\ &= 2\cdot 2\binom{n}{1}\binom{n}{2} + 2\cdot 2\binom{n}{1}\binom{n}{3} + 4\binom{n}{2}\binom{n}{2} \\ &\quad + 4\binom{n}{2}\binom{n}{2} + 2\cdot 6\binom{n}{2}\binom{n}{3} + 4\binom{n}{3}\binom{n}{3} \\ &= \frac{1}{9}n^2(n+1)^2(n-1)(n+2) \end{aligned} \tag{6.36}$$

This is exactly the formula of $\beta_{2,3}$ computed in Equation (6.13), so the vector space generated by these relations is the entire space of linear relations. □

6.4 Further conjectures

Everything we discussed in Sections 6.2 and 6.3 applies to the perpendicular ideal of the permanent as well as the determinant, up to changing some signs. In particular, the calculations of $\beta_{1,2}$ and $\beta_{2,3}$ in Section 6.2 still hold, with no changes required beyond replacing "det" with "perm"; and the linear second syzygies are generated by the relations

$$\rho'_1 = X_{1,1}(X_{1,2}^2) - X_{1,2}(X_{1,1}X_{1,2}) \tag{6.37}$$

$$\rho'_2 = X_{1,1}(X_{1,2}X_{1,3}) - X_{1,2}(X_{1,1}X_{1,3}) \tag{6.38}$$

$$\rho'_3 = X_{1,2}(X_{1,1}X_{2,1}) - X_{2,1}(X_{1,1}X_{1,2}) \tag{6.39}$$

$$\rho'_4 = X_{1,1}(X_{1,1}X_{2,2} - X_{1,2}X_{2,1}) - X_{2,2}(X_{1,1}^2) + X_{1,2}(X_{1,1}X_{2,1}) \tag{6.40}$$

$$\rho'_5 = X_{1,3}(X_{1,1}X_{2,2} - X_{1,2}X_{2,1}) - X_{2,2}(X_{1,1}X_{1,3}) + X_{2,1}(X_{1,2}X_{1,3}) \tag{6.41}$$

$$\begin{aligned}\rho'_6 = &-X_{1,2}(X_{2,1}X_{3,3} - X_{2,3}X_{3,1}) + X_{1,3}(X_{2,1}X_{3,2} - X_{2,2}X_{3,1}) \\ &+ X_{2,1}(X_{1,2}X_{3,3} - X_{1,3}X_{3,2}) - X_{3,1}(X_{1,2}X_{2,3} - X_{1,3}X_{2,2})\end{aligned} \tag{6.42}$$

with the same result in Theorem 6.11. (The proof of Proposition 6.9 needs to be modified slightly: define $R'_{a,b}$ to have $(-1)^{a+j}$ in the jth entry of the ath row, and $(-1)^{i+b+1}$ in the ith entry of the bth column. We still have the relation $R'_{1,1} + R'_{2,2} + R'_{3,3} = 0$, so the rest of the proof still holds.)

One significant difference between the syzygies of $S/\det_n^\perp$ and $S/\operatorname{perm}_n^\perp$, demonstrated in the computed Betti tables in Section 6.1 (Tables 6.1 to 6.7), is that the linear second syzygies generate *all* second syzygies of $S/\det_n^\perp$ for $n \leq 8$, but this is not true for $S/\operatorname{perm}_n^\perp$ (for $4 \leq n \leq 8$). In other words, $\beta_{2,4}$ is non-zero for $S/\operatorname{perm}_n^\perp$ for $4 \leq n \leq 8$, but $\beta_{2,j} = 0$ when $j \neq 3$ for $S/\det_n^\perp$, $n \leq 8$.

We conjecture that this pattern continues for $S/\det_n^\perp$:

Conjecture 6.12. *The relations listed in Proposition 6.3 generate* all *second syzygies of $S/\det_n^\perp$, not just the linear syzygies, when the characteristic of k is not* 2*. In other words, $\beta_{2,j} = 0$ for all $j \neq 3$.*

Remark. When k has characteristic 2, the determinant and the permanent are equal. The first few Betti numbers of $S/\det_n^\perp = S/\operatorname{perm}_n^\perp$, up to the third column of the Betti table, are the same as in the Betti tables for the permanent, Tables 6.1b to 6.7b.

If this conjecture is true, we can use the ideas of Section 6.2 to calculate the next Betti number, $\beta_{3,4}$.

Corollary 3.6 gives the formula

$$\begin{aligned} H_{S/\det_n^\perp}(4) &= \sum_i (-1)^i H_{F_i}(4) \\ &= H_S(4) - H_{S(-2)^{\beta_{1,2}}}(4) + H_{S(-3)^{\beta_{2,3}}}(4) - H_{F_3}(4) \end{aligned} \tag{6.43}$$

using Proposition 3.13 to conclude that there are no more non-zero terms.

We know $H_{S/\det_n^\perp}(4)$ from Proposition 5.2: it is

$$H_{S/\det_n^\perp}(4) = \binom{n}{4}^2.$$

Lemma 3.4 says

$$H_S(4) = \binom{n^2+3}{4}.$$

We have

$$\begin{aligned} H_{S(-2)^{\beta_{1,2}}}(4) &= \beta_{1,2} H_S(2) \\ &= \binom{n+1}{2}^2 \binom{n^2+1}{2} \end{aligned}$$

from Equation (6.2); similarly,

$$\begin{aligned} H_{S(-3)^{\beta_{2,3}}}(4) &= \beta_{2,3} H_S(1) \\ &= 4\binom{n+1}{3}\binom{n+2}{3} n^2 \end{aligned}$$

from Equation (6.14); and

$$H_{F_3}(4) = \beta_{3,4}.$$

Putting this all together,

$$\begin{aligned}\beta_{3,4} &= 4\binom{n+1}{3}\binom{n+2}{3}n^2 - \binom{n+1}{2}^2\binom{n^2+1}{2} + \binom{n^2+3}{4} - \binom{n}{4}^2 \\ &= \frac{1}{192}(n-1)n^2(n+1)^2(n+2)(5n^2+5n-18). \qquad (6.44)\end{aligned}$$

For small values of n, this equals

n	1	2	3	4	5	6	7	8
$\beta_{3,4}$	0	9	315	3075	17325	70560	231084	646380

which agrees with Tables 6.1 to 6.4, as expected.

6.5 Closing remarks

These results suggest some avenues for further investigation.

- An obvious first step would be to prove (or disprove!) Conjecture 6.12, thus confirming the calculation in Equation (6.44).
- Similarly, it would be interesting to compute $\beta_{2,4}$ for the permanent, i.e. the number of second syzygies with degree 2, or even to give a general description of generators for these syzygies, as this number measures the extent to which Conjecture 6.12 fails for the permanent.
- Another way of extending these results would be to compute higher Betti numbers, e.g. $\beta_{4,5}, \beta_{5,6}, \ldots$, and to give explicit descriptions of the syzygies. This should be done mathematically, but it would also help to resolve the memory issues with the Macaulay2 computations and compute more of the Betti tables for small n. Finding a complete description of the linear third syzygies would also help to compute $\beta_{2,4}$, using the techniques in Equation (6.44).
- More broadly, comparison of the determinant and permanent falls under the purview of algebraic complexity theory. As mentioned in the introduction, research in this area of mathematics focusses on computing the determinantal complexity of the permanent and finding bounds for this number in terms of n. It is conceivable that by considering the algebraic and homological properties of the apolar ideals, better bounds could be found.

Appendix A

Macaulay2 code for computing Betti tables

In Chapter 6, we computed some Betti tables for $S/\det_n^{\perp}$ and $S/\operatorname{perm}_n^{\perp}$ using Macaulay2 — see Tables 6.1 to 6.7. The code used to compute them is shown below.

Listing A.1: Macaulay2 code to compute Betti tables Tables 6.1 to 6.7

```
-- Set a field: the field of integers modulo 7 is small
    enough to compute with quickly, but doesn't have
    too small a characteristic that things cancel
    unexpectedly

kk      = ZZ/7

-- Set the size of the matrix: e.g. n = 2, 3, 4, ...

n       = 4

-- Define the polynomial ring

Vars    = flatten apply(n,i -> apply(n,j -> X_(i,j)))
S       = kk[Vars]

-- List the generators of the determinant apolar ideal

DetGen  = flatten flatten flatten apply(n,i -> apply(n,
   j -> apply(n,k -> apply(n,l -> X_(i,j)*X_(k,l) + X_(
   i,l)*X_(k,j)))))
```

```
-- List the generators of the permanent apolar ideal

PerGen1 = flatten flatten flatten apply(n,i -> apply(n,
   j -> apply(n,k -> apply(n,l -> X_(i,j)*X_(k,l) - X_(
   i,l)*X_(k,j)))))
PerGen2 = flatten apply(n,i -> apply(n,j -> X_(i,j)^2))
PerGen3 = flatten flatten apply(n,i -> apply(n,j ->
   apply(n,k -> X_(i,j)*X_(i,k))))
PerGen4 = flatten flatten apply(n,i -> apply(n,j ->
   apply(n,k -> X_(i,j)*X_(k,j))))

-- Define the apolar ideals in terms of the generators

Idet    = trim ideal DetGen
Iper    = trim ideal join(PerGen1, PerGen2, PerGen3,
   PerGen4)

-- Define the quotients

Mdet    = S^1/Idet
Mper    = S^1/Iper

-- Hilbert function

apply(10,i -> hilbertFunction(i,Mdet))
apply(10,i -> hilbertFunction(i,Mper))

-- Compute the resolutions: increase LengthLimit to
   compute more components of the resolution

ResDet  = resolution(Mdet, LengthLimit => 6)
ResPer  = resolution(Mper, LengthLimit => 6)

-- Compute the Betti tables

betti ResDet
betti ResPer
```

Appendix B

The minimal free resolution of $S/\det_2^\perp$

When $n = 2$, n is large enough that the minimal free resolution of $S/\det_n^\perp$ is non-trivial, but small enough that the resolution can fit on a page. We present this resolution here. The resolution of $S/\operatorname{perm}_2^\perp$ is similar but with some changes in sign.

Up to isomorphism, the minimal free resolution of $S/\det_2^\perp$ is as follows:

$$0 \longrightarrow S(-6) \xrightarrow{d_4} S(-4)^9 \xrightarrow{d_3} S(-3)^{16} \xrightarrow{d_2} S(-2)^9 \xrightarrow{d_1} S \longrightarrow S/\det_2^\perp \longrightarrow 0$$

The differentials are:

$$d_1 = \begin{bmatrix} X_{1,1}^2 & X_{1,2}^2 & X_{2,1}^2 & X_{2,2}^2 & X_{1,1}X_{1,2} & X_{2,1}X_{2,2} & X_{1,1}X_{2,1} & X_{1,2}X_{2,2} & (X_{1,1}X_{2,2} + X_{1,2}X_{2,1}) \end{bmatrix},$$

$$d_2 = \begin{bmatrix} X_{1,2} & X_{2,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -X_{2,2} & 0 & 0 & 0 \\ 0 & 0 & X_{1,1} & X_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -X_{2,1} & 0 & 0 \\ 0 & 0 & 0 & 0 & X_{1,1} & X_{2,2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -X_{1,2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & X_{1,2} & X_{2,1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -X_{1,1} \\ -X_{1,1} & 0 & -X_{1,2} & 0 & 0 & 0 & 0 & 0 & X_{2,1} & X_{2,2} & 0 & 0 & -X_{2,1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -X_{2,1} & 0 & -X_{2,2} & 0 & 0 & X_{1,1} & X_{1,2} & 0 & 0 & 0 & -X_{1,2} \\ 0 & -X_{1,1} & 0 & 0 & -X_{1,2} & 0 & 0 & 0 & -X_{1,2} & 0 & -X_{2,2} & 0 & 0 & 0 & -X_{2,2} & 0 \\ 0 & 0 & 0 & -X_{1,2} & 0 & 0 & -X_{2,2} & 0 & 0 & -X_{1,1} & 0 & -X_{2,1} & 0 & -X_{1,1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & X_{1,1} & X_{1,2} & X_{2,1} & X_{2,2} \end{bmatrix},$$

$$d_3 = \begin{bmatrix} X_{2,1} & 0 & 0 & 0 & -X_{2,2} & 0 & 0 & 0 & 0 \\ -X_{1,2} & 0 & 0 & 0 & 0 & -X_{2,2} & 0 & 0 & 0 \\ 0 & X_{2,2} & 0 & 0 & X_{2,1} & 0 & 0 & 0 & 0 \\ 0 & -X_{1,1} & 0 & 0 & 0 & 0 & -X_{2,1} & 0 & 0 \\ 0 & 0 & X_{2,2} & 0 & 0 & X_{1,2} & 0 & 0 & 0 \\ 0 & 0 & -X_{1,1} & 0 & 0 & 0 & 0 & -X_{1,2} & 0 \\ 0 & 0 & 0 & X_{2,1} & 0 & 0 & X_{1,1} & 0 & 0 \\ 0 & 0 & 0 & -X_{1,2} & 0 & 0 & 0 & X_{1,1} & 0 \\ X_{1,1} & 0 & 0 & 0 & 0 & -X_{1,2} & 0 & 0 & -X_{2,2} \\ 0 & X_{1,2} & 0 & 0 & -X_{1,1} & 0 & 0 & 0 & X_{2,1} \\ 0 & 0 & -X_{2,1} & 0 & 0 & 0 & 0 & X_{2,2} & X_{1,2} \\ 0 & 0 & 0 & -X_{2,2} & 0 & 0 & X_{1,2} & 0 & -X_{1,1} \\ 0 & 0 & 0 & 0 & -X_{1,2} & -X_{2,1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & X_{1,1} & 0 & -X_{2,2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & X_{1,1} & 0 & -X_{2,2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & X_{1,2} & X_{2,1} & 0 \end{bmatrix}, \qquad d_4 = \begin{bmatrix} X_{2,2}^2 \\ -X_{2,1}^2 \\ X_{1,2}^2 \\ -X_{1,1}^2 \\ X_{2,1}X_{2,2} \\ -X_{1,2}X_{2,2} \\ X_{1,1}X_{2,1} \\ -X_{1,1}X_{1,2} \\ X_{1,1}X_{2,2} + X_{1,2}X_{2,1} \end{bmatrix}.$$

Bibliography

[1] Michael Artin. *Algebra*. Prentice Hall, 2nd edition, 2011.

[2] Michael Atiyah and Ian G. MacDonald. *Introduction to commutative algebra*. Addison–Wesley series in mathematics. Addison–Wesley Publishing Company, Reading, Massachusetts, 1969.

[3] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*. Number 150 in Graduate texts in mathematics. Springer Science+Business Media, Inc., New York, 2004.

[4] David Eisenbud. *The geometry of syzygies: a second course in commutative algebra and algebraic geometry*. Number 229 in Graduate texts in mathematics. Springer Science+Business Media, Inc., New York, 2005.

[5] Ferdinand Georg Frobenius. Über die Darstellung der endlichen Gruppen durch lineare Substitutionen. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, pages 994–1015, 1897. Available at `http://www.e-rara.ch/doi/10.3931/e-rara-18879`.

[6] Bruno Grenet. An upper bound for the permanent versus determinant problem. 2012. Accessed at `http://www.lirmm.fr/~grenet/publis/Gre11.pdf`.

[7] David B. Leep and Gerry Myerson. Marriage, magic, and solitaire. *The American Mathematical Monthly*, 106(5):419–429, 1999. Accessed at `http://www.jstor.org/stable/2589146`.

[8] F. S. Macaulay. *The algebraic theory of modular systems*. Cambridge tracts in mathematics and mathematical physics. Stechert-Hafner Service Agency, Inc., 1964.

[9] Marvin Marcus and F. C. May. The permanent function. *Canadian Journal of Mathematics. Journal Canadien de Mathématiques*, 14:177–189, 1962.

[10] V. V. Prasolov. *Elements of homology theory*, volume 81 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI. Translated from the 2005 Russian original by Olga Sipacheva.

[11] Sean Sather-Wagstaff. *Commutative Algebra Mini-Course: Koszul Cohomology, Cohen Structure Theorems, and Intersection Multiplicities*. June 2004. Accessed at `https://www.math.utah.edu/vigre/minicourses/algebra/sather-wagstaff.pdf`.

[12] Masoumeh (Sepideh) Shafiei. Apolarity for determinants and permanents of generic matrices. *ArXiv e-prints*, 2012. Available at `http://adsabs.harvard.edu/abs/2012arXiv1212.0515S`.

[13] L. G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189 – 201, 1979. Accessed at `http://www.sciencedirect.com/science/article/pii/0304397579900446`.

[14] Charles A. Weibel. *An introduction to homological algebra*. Cambridge studies in advanced mathematics. Cambridge University Press, Cambridge, United Kingdom, 1994.