2017

On Degree Bound for Syzygies of Polynomial Invariants

Zhao Gao
The College of Wooster, zgao18@wooster.edu

On Degree Bound for Syzygies of Polynomial Invariants

Independent Study Thesis

Presented in Partial Fulfillment of the
Requirements for the Degree Bachelor of Arts in
the Department of Mathematics and Computer
Science at The College of Wooster

by
Zhao Gao

The College of Wooster
2017

Advised by:

Ondřej Zindulka

Mátyás Domokos

Abstract

Suppose G is a finite linearly reductive group. The degree bound for the syzygy ideal of the invariant ring of G is given in [2]. We develop the theory of commutative algebra and give the proof from [2] that the ideal of relations of the minimal set of generators of invariant ring of a finite linearly reductive group G is generated in degree at most $2|G|$.

Acknowledgements

I would like to take the opportunity to thank my advisors for their constant encouragement and flexibility in working around my independent study experience. I also would like to thank the entire Mathematics and Computer Science department at the College of Wooster for creating an amazing major experience by maintaining patience and friendly faces throughout my hours of questioning.

Contents

Chapter 1

Introduction

Let G be a finite group, k a field. The group G is linearly reductive if and only if $|G|$ is coprime to the characteristic of k. Suppose V is a representation of G. Then G acts on the coordinate ring $k[V]$ by linear substitution. Let $\beta_G(V)$ be the smallest integer d such that the invariant ring is generated by elements of degree $\leq d$. Noether proved that $\beta_G(V) \leq |G|$ in the case when the characteristic of the base field is 0. Fleischmann extended Noether's bound to the case when the group is linearly reductive over k. Let $\beta^1_G(V)$ be the least integer d such that the ideal of relations of a minimal set of generators of invariant ring is generated by elements of degree $\leq d$. Harm Derksen proved $\beta^1_G(V) \leq 2|G|$ in [2].

In this paper, we develop commutative algebra from scratch and give the proof of Harm Derksen that $\beta^1_G(V) \leq 2|G|$. We also give Fogarty's proof of Noether's bound in the linearly reductive case in Appendix B.

Chapter 2

Commutative Algebra

This chapter is devoted to the basic concepts of rings and modules. A reader who is familiar with rings and modules may skip this chapter.

2.1 Rings

Definition 2.1.1. A **commutative ring** is an abelian group A together with an operation $(a, b) \mapsto ab$ called multiplication and an identity 1, such that $\forall a, b, c \in A$:

$$(ab)c = a(bc)$$

$$ab = ba$$

$$a(b + c) = ab + ac$$

$$1a = a1 = a$$

We shall not discuss non-commutative rings in this article, therefore we

will use the word ring for commutative ring through out the paper. We will use $\bar{a}$ for the congruent class of a.

A will always denote a ring, k will always denote a field through out the paper.

Example 2.1.2. (i) The set of integers $\mathbb{Z}$ is a ring under usual addition and multiplication.

(ii) $\mathbb{Z}_n$, the integer modulo n, is a ring under addition $\overline{a} + \overline{b} = \overline{a+b}$ and multiplication $\overline{a}\overline{b} = \overline{ab}$.

The polynomial ring $A[X]$ is a ring by adjoining an indeterminate X to the ring A. It is the ring of polynomials with coefficients in A. i.e. , $A[X] = \{\sum_1^n a_i X^i \mid a_i \in A\}$. In general, we define the n variable polynomial ring to be $A[X_1, \ldots, X_n] = \{\sum a_{\mathbf{i}} X_1^{i_1} \ldots X_n^{i_n} \mid a_{\mathbf{i}} \in A\}$, where $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$ and the sum is finite. $A[X_1, \ldots, X_n]$ can be viewed as a ring of polynomial functions from A^n to A. That is, if $f = \sum a_{\mathbf{i}} X_1^{i_1} \ldots X_n^{i_n}$, then $f(a_1, \ldots, a_n) = \sum a_{\mathbf{i}} a_1^{i_1} \ldots a_n^{i_n}$.

If A and B are two rings, then the product of A, B, denoted $A \times B$, is the product of sets $A \times B$ together with coordinate-wise addition and multiplication.

A **subring** of a ring A is a subset $S \subset A$ that is a ring itself and contains the identity element of A.

The identity of the ring is generally not equal to the zero of the ring except the case where the ring consists of only the zero element. In this case it is called the zero ring, denoted by 0.

Definition 2.1.3. A **ring homomorphism** from a ring A to a ring B is a map

$f : A \to B$ such that $\forall a, b \in A$

$$f(a + b) = f(a) + f(b)$$
$$f(ab) = f(a)f(b)$$
$$f(1_A) = 1_B$$

In other words, ring homomorphism preserves addition, multiplication and identity.

If the homomorphism is injective (surjective, bijective), we call it a monomorphism (epimorphism, isomorphism respectively).

It is easy to see that the image of a ring homomorphism is itself a ring. It is a subring of the codomain of the homomorphism. The **kernel** of the ring homomorphism is defined to be the preimage of zero. If S is a subring of A, then the inclusion map $i : S \to A$ is a monomorphism. Composition of ring homomorphisms is a ring homomorphism.

Definition 2.1.4. A **zero-divisor** in a ring A is an nonzero element $u \in A$ such that there exists a nonzero element $v \in A$ with $uv = 0$. A nonzero element that is not a zero-divisor is called a **non-zero-divisor**. A **domain** is a ring A with no zero-divisor.

In particular, a domain is a ring where the **cancellation law** holds: suppose $a \in A$ is a non-zero-divisor and $ab = ac$. Then we have $a(b - c) = 0$. Since a is a non-zero-divisor, $b - c$ must be zero, hence $b = c$. Therefore we may cancel a from both sides of the equation $ab = ac$.

Example 2.1.5. (i) The ring of integers $\mathbb{Z}$ is a domain.

(ii) The ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a domain.

(iii) If A is a domain, then the polynomial ring $A[X]$ is also a domain.

Definition 2.1.6. A **unit** in a ring A is an element $u \in A$ such that there exists an element $v \in A$ with $uv = 1$. Such v is called the inverse of u, written u^{-1}. A **field** is a ring F such that every nonzero element of F is a unit and $1 \neq 0$.

We use $A^\times$ to denote the set of all units in A. It is easy to see that $A^\times$ is a multiplicative group and A is a field if and only if $A^\times = A \setminus 0$. If $u \in A$ is a unit, then $ua = 0 \implies u^{-1}ua = 0 \implies a = 0$, hence u is a non-zero-divisor. It follows that a field is automatically a domain.

Example 2.1.7. $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ where p is a prime are fields.

Definition 2.1.8. An **ideal** in a ring A is an additive subgroup $I \subset A$ such that for any $r \in A, s \in I$ we have $rs \in I$. If I is a proper subset of A, then I is called a proper ideal of A.

Ideal is the notion corresponding to that of a normal subgroup in group theory. It can also be described as the kernel of a certain homomorphism. Often it is not a subring by itself. By the definition of ring homomorphism, the identity is mapped to the identity. Therefore if the identity of the codomain is not 0, the kernel of the homomorphism does not contain the identity, hence not a subring. We will see later that the kernel is actually a submodule.

Let X be a subset of a ring A. The ideal generated by X is the smallest ideal in A that contains X. It is denoted by (X). It is easy to verify that $(X) = \{\sum_1^n r_i s_i \mid n \in \mathbb{N}, r_i \in A, s_i \in X, 1 \leq i \leq n\}$. If $X = \{t_1, \ldots, t_n\}$ is a finite set, then we shall write $(t_1, \ldots, t_n)$ for (X). Ideals of the form $(t_1, \ldots, t_n)$ are called

finitely generated. In particular, ideals generated by a single element are called **principal**.

An ideal $I \subset A$ is a proper ideal if and only if it does not contain a unit. If it contains a unit u, then for every $a \in A$, we have $a = au^{-1}u \in I$, hence $I = A$.

It is customary to use 0 for the zero element and the ideal consisting only the zero element.

Example 2.1.9. Every ideal of the ring of integers $\mathbb{Z}$ is of the form (m), hence principal. This follows easily from the well-ordering principle. Ring with the property that every ideal is principal is called a **principal ideal ring**. If that ring is also a domain, then it is called a **principal ideal domain**.

Let I, J be two ideals of ring A. We define

$$I + J = \{i + j \mid i \in I, j \in J\}$$
$$IJ = \{\sum_{1}^{n} i_k j_k \mid n \in \mathbb{N}, i_k \in I, j_k \in J, 1 \leq k \leq n\}$$

Definition 2.1.10. An ideal P in a ring A is called **prime** if $P \neq A$ (i.e. P is a proper ideal of A) and for any ideals $I, J \subset A$ with $IJ \subset P$ we have either $I \subset P$ or $J \subset P$.

Equivalently, P is a prime ideal if and only if $\forall i, j \in A$, $ij \in P$ implies $i \in P$ or $j \in P$. A **maximal ideal** of a ring A is a proper ideal m such that any proper ideal containing m equals m. Maximal ideals always exist by the Zorn's lemma. In fact, for any proper ideal $I \subset A$, there is a maximal ideal of A containing I: it is obtained by partially ordering the set of all proper ideals containing I by set inclusion. The union of a chain is an upper bound since the

identity 1 is not in the union, hence the union is a proper ideal.Therefore by the Zorn's lemma, there exists a maximal proper ideal containing I.

The **spectrum** of a ring A is the set of all prime ideals of A, denoted $\operatorname{Spec} A$. The **maximal spectrum** of a ring A is the set of all maximal ideals of A, denoted $\mathrm{m} \cdot \operatorname{Spec} A$. A **local ring** is a ring with only one maximal ideal. We write (A, m) to denote the local ring A with maximal ideal m. This concept will be discussed in more details in the section on localization.

Example 2.1.11. (i) If A is a domain, then the zero ideal $0 \subset A$ is prime. Indeed, if $ab = 0$, A is a domain implies one of a, b is zero, hence in the zero ideal.

(ii) If $p \in \mathbb{Z}$ is a prime number, then $(p) \subset \mathbb{Z}$ is a prime ideal. This is where the name "prime" comes from.

(iii) If K is a field, then $(X), (Y), (X, Y) \subset K[X, Y]$ are all prime ideals.

Definition 2.1.12. Let I be an ideal of a ring A. The **quotient ring** A/I is the abelian quotient group A/I together with the multiplication defined by:

$$(a + I)(b + I) = ab + I$$

If $I \subset A$ is an ideal, then there is a natural surjection $\pi : A \to A/I$ with kernel I. Moreover, there is an order-preserving 1-1 correspondence between the ideals in A/I and ideals in A that contain I given by $J \mapsto \pi^{-1}(J)$. All of the ideals in A/I are of the form K/I for some ideal $K \subset A$.

Theorem 2.1.13 (First Isomorphism Theorem)**.** *If $f : A \to B$ is a ring homomorphism, then f induces an isomorphism of rings $A/\ker f \cong \operatorname{Im} f$.*

The proof is omitted.

Example 2.1.14. (i) Consider the epimorphism $f : \mathbb{Z} \to \mathbb{Z}_n$ given by $a \mapsto a \mod n$. We have $\ker f = (n)$, therefore $\mathbb{Z}/(n) \cong \mathbb{Z}_n$.

(ii) Let K be a field, $K[X_1, \ldots, X_n]$ be the polynomial ring of n variables. Let $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$ be a vector. Then $\mathbf{a}$ induces an evaluation map $ev_{\mathbf{a}} : K[X_1, \ldots, X_n] \to K$ given by $F \mapsto F(\mathbf{a})$. It is obviously surjective, and $\ker ev_{\mathbf{a}} = (X_1 - a_1, \ldots, X_n - a_n)$. Therefore $K[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n) \cong K$.

If A is a domain, it follows immediately from the definition of prime ideal that $0 \subset A$ is prime. Conversely, if $0 \subset A$ is prime, then $a \neq 0$ and $ab = 0$ implies $b = 0$, therefore a is a non-zero-divisor and A is a domain. If $u \in A$ is a unit, then $(u) = A$ since for any $a \in A$, we have $a = au^{-1}u \in (u)$. Therefore if A is a field, then 0 is the only proper ideal of A, hence a maximal ideal. Conversely, if $0 \neq a \in A$ is not a unit, then $(a) \neq A$, and thus 0 is properly contained in (a) and is not maximal. Therefore we have the following proposition.

Proposition 2.1.15. *Let A be a ring. Then*

$$A \text{ is a domain} \iff 0 \text{ is prime.}$$
$$A \text{ is a field} \iff 0 \text{ is maximal.}$$

$I \subset A$ is a prime ideal if and only if 0 is prime in A/I. Similarly $I \subset A$ is a maximal ideal if and only if 0 is maximal in A/I. Therefore if $I \subset A$ is a maximal ideal, A/I is a field hence a domain. It follows that I is also prime. Thus a maximal ideal is automatically a prime ideal.

Lemma 2.1.16. *Let A, B be two rings. Let $f : A \to B$ be a homomorphism. If P is a prime ideal in B then $f^{-1}(P)$ is a prime ideal in A.*

Proof. Consider the composition $A \xrightarrow{f} B \xrightarrow{\pi} B/P$. The kernel of this composition is $f^{-1}(P)$. Therefore f induces an embedding $A/f^{-1}(P) \to B/P$. Since P is prime, B/P is a domain, hence $A/f^{-1}(P)$ is also a domain. It follows that $f^{-1}(P)$ is prime in A. □

An analogous statement does not hold for maximal ideals. Consider the inclusion map $\mathbb{Z} \to \mathbb{Q}$: 0 is a maximal ideal in $\mathbb{Q}$ but not a maximal ideal in $\mathbb{Z}$.

We finish this section with an elementary yet useful lemma that will be used later multiple times.

Lemma 2.1.17 (prime avoidance)**.** *Let $P_1, \ldots, P_n \subset A$ be prime ideals. If I is an ideal of A such that $I \subset \bigcup_1^n P_i$, then $I \subset P_i$ for some i.*

Proof. We prove this lemma by induction on n. If $n = 1$, the statement is trivial. Now suppose $I \subset \bigcup_1^n P_i$. If $I \subset \bigcup_{i \neq j} P_i$ for some j, then by induction I is contained in one of P_i's. Thus we may assume that $I \not\subset \bigcup_{i \neq j} P_i$ for all j's. Hence there exist $x_j \in P_j$ such that $x_j \in P_j \setminus \bigcup_{i \neq j} P_i$ for all j's. We claim that $x_1 + x_2 x_3 \cdots x_n \in I$ is not contained in $\bigcup_1^n P_i$. For if $x_1 + x_2 x_3 \cdots x_n \in P_1$, we will have $x_2 x_3 \cdots x_n \in P_1$. Since P_1 is prime, it contains one of $x_2, \ldots, x_n$. But by assumption, none of $x_2, \ldots, x_n$ is in P_1. If $x_1 + x_2 \cdots x_n \in P_i$ for some i $(2 \leq i \leq n)$, then we will have $x_1 \in P_i$. But by assumption x_1 is not in any of $P_2, \ldots, P_n$. □

2.2 Modules

Modules over a ring generalize abelian groups and vector spaces. It is a concept that is broad enough to include a great amount of algebraic objects. Recall that A denotes a ring.

Definition 2.2.1. An **A-module** (or a module over A) M is an abelian group with a map $A \times M \to M$, written $(a, m) \mapsto am$, such that $\forall r, s \in A, m, n \in M$:

$$r(sm) = (rs)m$$
$$r(m + n) = rm + rn$$
$$(r + s)m = rm + sm$$
$$1_A m = m$$

Given an A-module M, for any fixed $a \in A$, the map $\varphi_a : M \to M$ given by $m \mapsto am$ is a group endomomorphism. That is, $\varphi_a \in \mathrm{End}(M)$, the ring of endomorphisms of abelian group M. It is easy to see that M is an A-module if and only if M is an abelian group together with a ring homomorphism $A \to \mathrm{End}(M)$.

Example 2.2.2. (i) $\mathbb{Z}$-modules are nothing but abelian groups.

(ii) Let K be a field. K-modules are nothing but K-vector spaces.

(iii) Let $I \subset A$ be an ideal. Then I and A/I are both A-modules.

Let M be an A-module. A **submodule** $N \subset M$ is an abelian subgroup of M such that $AN \subset N$ (i.e., for any $a \in A, n \in N$, we have $an \in N$). The

corresponding **quotient module** M/N is the quotient group M/N together with multiplication $a(m+N) = am+N$.

Definition 2.2.3. An A**-module homomorphism** from an A-module M to an A-module N is a map $f : M \to N$ such that $\forall a \in A, m, n \in M$:

$$f(m+n) = f(m) + f(n)$$
$$f(am) = af(m)$$

An A-module homomorphism is an A-linear map.

Let M, N be A-modules. We define $\mathrm{Hom}_A(M,N)$ to be the set of all A-module homomorphisms from M to N. For any $f, g \in \mathrm{Hom}_A(M,N), m \in M, a \in A$, we define $f+g$ and af by

$$(f+g)(m) = f(m) + g(m)$$
$$(af)(m) = af(m)$$

This turns $\mathrm{Hom}_A(M,N)$ into an A-module. We write $\mathrm{Hom}(M,N)$ when A is clear from the context.

The kernel of the A-module homomorphism is defined to be the preimage of zero.

Similar to groups, we have isomorphism theorems for modules.

Theorem 2.2.4 (First Isomorphism Theorem)**.** *Let $f : M \to N$ be a homomorphism of A-modules. Then* $\mathrm{Im}\, f \cong M/\ker f$.

Theorem 2.2.5 (Second and Third Isomorphism Theorem)**.** *Let M, N, L be*

A-modules.

(i) *If* $L \subset M \subset N$, *then* $(N/L)/(M/L) \cong N/M$.

(ii) *If* $L, M \subset N$, *then* $(M + L)/L \cong M/(M \cap L)$.

If $N \subset M$ is a submodule of the A-module M, then there is a one-to-one order-preserving correspondence between the submodules containing N and submodules of M/N. (Note that the corresponding statement for ideals is just a special case of this statement.)

If M, N are A-modules, the **direct sum** of M, N is $M \oplus N = \{(m, n) \mid m \in M, n \in N\}$ with coordinatewise multiplication and addition. More generally, if $\{M_\lambda\}_{\lambda \in \Lambda}$ is a possibly infinite family of A-modules, then the **direct sum** of this family is

$$\bigoplus_{\lambda \in \Lambda} M_\lambda = \{(m_\lambda)_{\lambda \in \Lambda} \mid m_\lambda = 0 \text{ for all but finitely many } \lambda \in \Lambda\}.$$

Free A**-module** of rank n is defined to be $A^n = A \oplus \cdots \oplus A$ (n copies). $e_i = (0, \ldots, 1, \ldots, 0)$ (ith), $i = 1, \ldots, n$ form the standard basis of A^n. Let M be an A-module. The submodule generated by $m_1, \ldots, m_n \in M$ is defined by $\sum_{i=1}^n Am_i = \left\{ \sum_{i=1}^n a_i m_i \mid a_i \in A \right\}$. M is called **finitely generated** if it is generated by a finite number of elements. If $M = \sum_{i=1}^n Am_i$, then there is a unique A-module homomorphism $\pi : A^n \to M$ such that $e_i \mapsto m_i$ ($i = 1, \ldots, n$). It is given by $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i m_i$. In particular, $M \cong A^n / \ker \pi = A^n / \{(a_1, \ldots, a_n) \mid \sum a_i m_i = 0\}$. $A^n / \ker \pi$ is called the representation of M by relations. (π is a common symbol for this canonical map.)

If M, N, L are A-modules, and $f : L \to M$, $g : M \to N$ are homomorphisms,

then a pair of homomorphisms $L \xrightarrow{f} M \xrightarrow{g} N$ is called **exact** if $\ker g = \operatorname{Im} f$. In general, a sequence of homomorphisms $\cdots \to L \to M \to N \to \cdots$ is exact if each pair of consecutive homomorphisms is exact. A **short exact sequence** is an exact sequence of homomorphisms $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$. That is, f is injective and g is surjective.

If M is an A-module and $m \in M$, the **annihilator** of m is $\operatorname{ann}(m) = \{a \in A \mid am = 0\}$. It is an ideal of A since it is the kernel of the A-module homomorphism $\varphi : A \to M$ given by $a \mapsto am$. The annihilator of M is $\operatorname{ann}(M) = \{a \in A \mid \forall m \in M, am = 0\}$. It is also an ideal of A.

The Cayley-Hamilton theorem in Linear Algebra works not only in the case of a module over a field, but also in the case of a module over a ring. It has a nice and important corollary called Nakayama's Lemma.

Theorem 2.2.6 (Cayley-Hamilton)**.** *Let M be a finitely generated A-module generated by n elements, and $\varphi : M \to M$ a homomorphism of A-module such that $\varphi(M) \subset JM$, where J is an ideal of A. Then there exist $a_i \in J^i$ such that $\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0$.*

Proof. Let $m_1, \ldots, m_n$ be the generators of M. We have $\varphi(m_k) = \sum_{i=1}^n y_{ik} m_i$, $y_{ik} \in J$. Let $Y = (y_{ik}) \in A^{n\times n}$ be the $n \times n$ matrix with entries in A. Make M an $A[x]$-module as follows:

$$\left(\sum c_i x^i\right) m := \sum c_i \varphi^i(m)$$

Then we have $\sum_{i=1}^n (\delta_{ik} x - y_{ik}) m_i = 0$, for $k = 1, \ldots, n$. Define matrix Z as follows:

$$Z = (z_{ij}) = \operatorname{adj}(xI - Y) \in A[x]^{n\times n}$$

For $i = 1, \ldots, n$ we have

$$\begin{aligned}\det(xI - Y)m_i &= \sum_i \delta_{ij} \det(xI - Y)m_i \\ &= \sum_i \sum_k (\delta_{ik}x - y_{ik})z_{kj})m_i \\ &= \sum_k z_{kj} \sum_i (\delta_{ik}x - y_{ik})m_i = 0.\end{aligned}$$

Since m_i's generate M, it follows that $\det(xI - Y)m = 0$ for all $m \in M$. Therefore $\det(xI - Y) = x^n + \sum a_i x^{n-1}$ is the desired monic polynomial such that $\varphi^n + a_1\varphi^{n-1} + \cdots + a_{n-1}\varphi + a_n = 0$ with $a_i \in J^i$. □

Corollary 2.2.7. *If M is a finitely generated A-module, and $M = JM$ for some ideal J of A, then there exists an $x \in A$ such that $x \equiv 1 \mod J$ and $xM = 0$.*

Proof. Apply the previous theorem to id_M to get

$$1 + a_0 + \cdots + a_n = 0 \in \mathrm{End}(M).$$

Then $1 + a_0 + \cdots + a_n \equiv 1 \mod J$ is the desired element which annihilates M. □

Corollary 2.2.8 (Nakayama's lemma)**.** *Let (A, m) be a local ring and M a finitely generated A-module. Then $M = mM$ implies $M = 0$.*

Proof. By the previous corollary, there exists an $x \in A$ such that $x \equiv 1 \mod m$ and $xM = 0$. Since A is a local ring, any element outside of the maximal ideal m must be a unit. Therefore x is a unit. Then $M = x^{-1}xM = 0$. □

Corollary 2.2.9. *Let (A, m) be a local ring, M be an A-module, $N \subset M$ a submodule. Suppose M/N is a finitely generated A-module. Then $M = N + mM$ implies $N = M$.*

In particular, if M is a finitely generated A-module and $s_1, \ldots, s_k \in M$ are elements such that $\bar{s}_1, \ldots, \bar{s}_n \in M/mM$ generate M/mM as an A/m-module, then $s_1, \ldots, s_k$ generate M as an A-module.

Proof. For the first statement, it is enough to show that $M/N = 0$. We have $m(M/N) = (N + mM)/N = M/N$. By assumption we know A is a local ring, and M/N is finitely generated. By Nakayama's lemma, we have $M/N = 0$, hence $N = M$.

For the second statement, let $N = \sum As_i$. Since $\bar{s}_i$'s generate M/mM, we have $M = N + mM$. By the first statement we have $N = M$. □

2.3 Noetherian Rings and Modules

Proposition 2.3.1. *The following conditions are equivalent for an A-module M:*

(i) *The ascending chain condition (a.c.c.) holds for submodules of M (i.e., $\forall M_1 \subset M_2 \subset \ldots$ an increasing chain of submodules, $\exists\, l : M_l = M_{l+1} = \ldots$).*

(ii) *Any nonempty set of submodules has a maximal element.*

(iii) *Any submodule of M is finitely generated.*

Proof. (i) $\implies$ (ii), (iii) If (ii) or (iii) does not hold, then we may find an ascending chain that does not terminate.

(ii) $\implies$ (i) If there exists an increasing chain of submodules that does not terminate, then this chain has no maximal element.

(iii) $\implies$ (i) Suppose $M_1 \subset M_2 \subset \ldots$ is an increasing chain of submodules. Then $\bigcup_i M_i$ is a submodule of M. By assumption it is generated by $s_1, \ldots, s_n$.

Each s_i is contained in some M_j. Then M_j contains all s_i's for the largest such j. Hence $M_j = \bigcup_i M_i$ and $M_j = M_{j+1} = \dots$.

□

Definition 2.3.2. An A-module M is **Noetherian** if any of the above conditions holds for M. A ring A is **Noetherian** if it is Noetherian as an A-module.

Lemma 2.3.3. *Let L be a submodule of an A-module M. Then M is Noetherian if and only if L and M/L are Noetherian.*

Proof. Assume M is Noetherian. Any submodule of L is a submodule of M, therefore the submodule of L is finitely generated, hence L is Noetherian. The submodules of M/L are of the form N/L where N is a submodule of M containing L. Since N is finitely generated, N/L is also finitely generated. Thus M/L is Noetherian.

Assume L and M/L are Noetherian. Let N be a submodule of M. It is easy to see that $N \cap L$ and $N/(N \cap L)$ are finitely generated implies N is finitely generated. Since N/L is a submodule of L, it is finitely generated. Since $N/(N \cap L)$ is isomorphic to $(N + L)/L$ which is a submodule of M/L, it is also finitely generated. Hence N is finitely generated and M is Noetherian. □

Corollary 2.3.4. (i) *If M_i $(i = 1, \dots, r)$ are Noetherian, then $\bigoplus_{i=1}^{r} M_i$ is Noetherian.*

(ii) *Let A be a Noetherian ring, and M be an A-module. Then M is Noetherian if and only if M is finitely generated.*

Proof. (i) Since $M' \oplus M''/M' \cong M''$, M' and M'' are Noetherian implies $M' \oplus M''$ by the previous lemma. Then (i) follows by induction on the number of

modules.

(ii) If M is Noetherian then M is obviously finitely generated. If M is finitely generated, then $M \cong A^n/\ker\pi$, which is the representation of M by relations. By (i) we know A^n is Noetherian, therefore M is Noetherian by the previous lemma. □

Theorem 2.3.5 (Hilbert Basis Theorem)**.** *If A is a Noetherian ring, then the polynomial ring $A[X]$ is Noetherian as well.*

Proof. let I be an ideal in $A[X]$. For $n \in \mathbb{N}_0$, set
$J_n = \{a \in A \mid I \text{ contains an element of the form } ax^n + \sum_{i=1}^{n-1} a_i x^k\}$. Then J_n is an ideal of A and $J_0 \subset J_1 \subset J_2 \subset \cdots$. A is Noetherian implies there exists a terminal ideal J_l of this chain of ideals. For $r = 0, 1, \ldots, l$, take $f_1^{(r)}, \ldots, f_{n_r}^{(r)} \in I$ whose leading coefficients generate J_r. We claim that I is generated by
$J = \{f_1^{(r)}, \ldots, f_{n_r}^{(r)} \mid r = 0, 1, \ldots, l\}$. Let I' be the ideal generated by J. We do induction on the degree of $f \in I$.

If $\deg f = 0$, then $f \in J_0 \subset I'$.

If $0 < d = \deg f \leq l$, $f = ax^d + LDT$, $a \in J_d$, then there exist $c_1, \ldots, c_{n_d} \in A$ such that $c_1 f_1^{(d)} + \cdots + c_{n_d} f_{n_d}^{(d)} \in I'$ has the leading coefficient a. Therefore $f - c_1 f_1^{(d)} + \cdots + c_{n_d} f_{n_d}^{(d)} \in I$ has degree less than d. By induction we have $f - c_1 f_1^{(d)} + \cdots + c_{n_d} f_{n_d}^{(d)} \in I'$, hence $f \in I'$.

If $\deg f > l$, then the leading coefficient of f is in J_l. Thus we may apply the above induction to get $f \in I'$. □

An **A-algebra** is a commutative ring S together with a ring homomorphism $\varphi : A \to S$. For $a \in A, s \in S$, we write as in place of $\varphi(a)s$. Given an ideal $I \subset S$, we write $A \cap I$ to denote $\varphi^{-1}(I)$. An **A-algebra**

homomorphism from an A-algebra S to an A-algebra T is a ring homomorphism $f : S \to T$ such that $\forall a \in A, s \in S$: $f(as) = af(s)$. If k is a field, then a k-algebra contains k as a subfield since a ring homomorphism from a field to a nonzero ring must be injective.

Given an A-algebra B and $b_1, \ldots, b_n \in B$, we define $A[b_1, \ldots, b_n]$ to be the subring of B generated by A and $b_1, \ldots, b_n$. It is clearly an A-algebra. Such algebras are called finitely generated. Clearly there is an algebra homomorphism from $A[X_1, \ldots, X_n]$ to $A[b_1, \ldots, b_n]$ by sending X_i to b_i, hence $A[b_1, \ldots, b_n] \cong A[X_1, \ldots, X_n]/I$, where I is the ideal generated by polynomials with coefficients in A such that $f(b_1, \ldots, b_n) = 0$.

By the Hilbert basis theorem, if k is field, then $k[X_1, \ldots, X_n]$ is a Noetherian ring. If follows that finitely generated k-algebras are Noetherian as well.

2.4 Integral Ring Extension

Definition 2.4.1. Let A be a subring of a ring B.

(i) $y \in B$ is integral over A if there exists a monic $f \in A[X]$ such that $f(y) = 0$.

(ii) B is integral over A if all elements of B are integral over A.

Lemma 2.4.2. *Let $A \subset B$ be a subring, $y \in B$. The following conditions are equivalent.*

(i) *y is integral over A.*

(ii) *$A[y]$ is a finitely generated A-module.*

(iii) *There exists a subring C such that $A \subset C \subset B$. $y \in C$ and C is a finitely generated A-module.*

Proof. (i) $\implies$ (ii) Suppose y is integral over A. Then there exist $a_1, \ldots, a_n \in A$ such that $y^n + a_1 y^{n-1} + \cdots + a_n = 0$. Hence
$y^n = -(a_1 y^{n-1} + \cdots + a_n) \in A + Ay + \cdots + Ay^{n-1} = M \subset A[y]$. M is a finitely generated A-module. It is easy to see that $AM \subset M$ and $yM \subset M$, therefore M is a $A[y]$-submodule (an ideal of $A[y]$). Since $1 \in M$, we have $M = A[y]$. Thus $A[y]$ is a finitely generated A-module.

(ii) $\implies$ (iii) is trivial.

(iii) $\implies$ (i) Since C is a finitely generated A-module, we may apply Cayley-Hamilton theorem: consider the A-module homomorphism $\varphi : C \to C$ given by $a \mapsto ay$. There exist $a_1, \ldots, a_n \in A$ such that $\varphi^n + a_1 \varphi^{n-1} + \cdots + a_n = 0$. It follows that $y^n + a_1 y^{n-1} + \cdots + a_n = 0$, hence y is integral over A. □

Proposition 2.4.3. *Let $A \subset B \subset C$ be subrings.*

(i) *Suppose C is a finitely generated B-module, and that B is a finitely generated A-module. Then C is a finitely generated A-module.*

(ii) *If $y_1, \ldots, y_n \in B$ are integral over A, then $A[y_1, \ldots, y_n]$ is a finitely generated A-module.*

(iii) *If C is integral over B and B is integral over A, then C is integral over A.*

(iv) *The set $\widetilde{A} := \{y \in B \mid y \text{ is integral over } A\} \subset B$ is a subring. Moreover, $\widetilde{\widetilde{A}} = \widetilde{A}$.*

Proof. (i) If $B = Ab_1 + \cdots + Ab_n$ and $C = Bc_1 + \cdots + Bc_m$, then $C = \sum Ab_i c_j$.

(ii) Clearly $A \subset A[y_1] \subset A[y_1, y_2] \subset \cdots \subset A[y_1, \ldots, y_n]$. By the previous lemma, each of these subrings is a finitely generated module over the preceding subring. Then $A[y_1, \ldots, y_n]$ is a finitely generated A module by (i).

(iii) If $z \in C$, then there exist $b_1, \ldots, b_n \in B$ such that $z^n + b_1 z^n - 1 + \cdots + b_n = 0$. Hence z is integral over $A[b_1, \ldots, b_n]$, which is a finitely generated A-module. Thus $A[y_1, \ldots, y_n, z]$ is a finitely generated module over $A[b_1, \ldots, b_n]$. Therefore $A[y_1, \ldots, y_n, z]$ is a finitely generated A-module by (i). It follows by (iii) of lemma 2.4.2. that z is integral over A. Thus C is integral over A.

(iv) Suppose $a, b \in B$ are integral over A. Then $A[a, b]$ is integral over A. Hence $ab, a + b \in A[a, b]$ are integral over A as well. Thus $\widetilde{A}$ is a subring. The second statement follows easily from (iii). □

$\widetilde{A}$ in the previous proposition is called the **integral closure** of A in B. If $A = \widetilde{A}$, then A is called **integrally closed** in B. A domain A is called **normal** if A is integrally closed in its field of fractions.

Let A be a k-algebra (k is a field). $y_1, \ldots, y_n \in A$ are **algebraically independent** over k if for any nonzero polynomial $F \in k[X_1, \ldots, X_n]$, $F(y_1, \ldots, y_n) \neq 0$. That is, $k[y_1, \ldots, y_n] \cong k[X_1, \ldots, X_n]$ by identifying y_i with X_i.

Theorem 2.4.4 (Noether Normalization Lemma)**.** *Let A be a finitely generated k-algebra (k is a field). Then there exist $z_1, \ldots, z_m \in A$ such that*

(i) *$z_1, \ldots, z_m$ are algebraically independent over k.*

(ii) *A is a finitely generated $k[z_1, \ldots, z_m]$-module.*

That is, any finitely generated k-algebra is a finitely generated module over a subring that is a polynomial ring.

Proof. It suffices to prove the following claim:

Suppose $A = k[y_1, \ldots, y_n]$ and $F \in k[X_1, \ldots, X_n]$ is a nonzero polynomial such that $F(y_1, \ldots, y_n) = 0$. Then there exist $w_1, \ldots, w_{n-1} \in A$ such that y_n is integral over $A^* = k[w_1, \ldots, w_{n-1}]$ and $A = A^*[y_n]$.

To prove the claim, suppose

$$F = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} X_1^{i_1} \ldots X_n^{i_n}$$

where I is a finite set of those $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$ for which $a_{\mathbf{i}} \neq 0$.

Take $C \in \mathbb{N}$ greater than any component $i_1, \ldots, i_n$ of any $\mathbf{i} \in I$. Set

$$\begin{aligned} w_1 &= y_1 - y_n^{c^{n-1}} \\ w_2 &= y_2 - y_n^{c^{n-2}} \\ &\ldots \\ w_{n-1} &= y_{n-1} - y_n^{c} \end{aligned}$$

Clearly $w_1, \ldots, w_{n_1}, y_n$ generate A.

$$\begin{aligned} 0 = F(y_1, \ldots, y_n) &= \sum_{\hat{i} \in I} a_{\hat{i}} (w_1 + y_n^{c^{n-1}})^{i_1} (w_2 + y_n^{c^{n-2}})^{i_2} \ldots y_n^{i_n} \\ &= \sum_{\hat{i} \in I} a_{\hat{i}} y_n^{i_1 C^{n-1} + i_2 C^{n-2} + \cdots + i_{n-1} C + i_n} + R \end{aligned}$$

where R denotes the remaining terms, they have smaller degree in y_n. Since C

is greater than any component of any $\mathbf{i} \in I$, $i_1C^{n-1} + i_2C^{n-2} + \cdots + i_{n-1}C + i_n$ can be viewed as a base C number. And each $\mathbf{i} \in I$ corresponds to a unique number. Let $\mathbf{j} \in I$ be the lexicographically greatest element of I. Then

$$F(y_1, \ldots, y_n) = a_{\mathbf{j}} y_n^{j_1C^{n-1}+j_2C^{n-2}+\cdots+j_{n-1}C+j_n} + R'$$

where R' denotes the remaining term which has lower degree in y_n. Since $a_{\hat{j}} \in k$ is a unit, by multiplying F by $a_{\mathbf{j}}^{-1}$ we see that y_n is integral over $A^* = k[w_1, \ldots, w_{n-1}]$. Since $y_1, \ldots, y_n \in A^*[y_n]$, we have $A = A^*[y_n]$. The claim is proved.

We proceed with the proof of the theorem. Suppose $A = k[y_1, \ldots, y_n]$. We prove the theorem by induction on n. If $n = 0$, then $A = k$ and we are done.

Suppose $n > 0$. If $y_1, \ldots, y_n$ are algebraically independent, then we are done. Otherwise there exists a nonzero $F \in k[X_1, \ldots, X_n]$ such that $F[y_1, \ldots, y_n] = 0$. By the claim there exist $w_1, \ldots, w_{n-1} \in A$ such that y_n is integral over $A^* = k[w_1, \ldots, w_n]$ and $A = A^*[y_n]$. By induction hypothesis, there exist $z_1, \ldots, z_m \in A$ that are algebraically independent and A^* is a finitely generated $k[z_1, \ldots, z_m]$-module. Since $A = A^*[y_n]$ is a finitely generated A^*-module, it follows that A is a finitely generated $k[z_1, \ldots, z_m]$-module. □

Let G be a finite group of automorphisms of a k-algebra A (k is a field). Set

$$A^G := \{a \in A \mid g(a) = a, \forall g \in G\}.$$

It is easy to see that A^G forms a subring of A. A^G is called the **ring of invariants** of G in A.

In the case where A is a finitely generated k-algebra, especially if $A = k[X_1, \ldots, X_n]$, it is often the case that one can find a finite set of generators for the ring of invariants. The fundamental problem of invariant theory was the existence of such finite set of generators. Hilbert solved this problem using the power of abstraction. Here we present a classical theorem of Emmy Noether:

Theorem 2.4.5 (Emmy Noether)**.** *The ring of invariants of a finite group in a finitely generated k-algebra is finitely generated as a k-algebra.*

Proof. Let G be a finite group of k-algebra automorphisms of the k-algebra A generated by $y_1, \ldots, y_n \in A$. We shall show A^G is finitely generated.

First we find a finitely generated k-subalgebra B in A^G such that each generator y_i is integral over B. Since G is a finite group, we may assume $G = \{g_1, \ldots, g_k\}$. The action of G on A extends to an action on the polynomial ring $A[X]$. For $g \in G, \sum a_i X^i \in A[X]$,

$$g(\sum a_i X^i) = \sum g(a_i) X^i.$$

Note that $(X - g_1(y))(X - g_2(y)) \ldots (X - g_k(y))$ is a monic polynomial such that y is one of its root since G contains the identity homomorphism. Let S be the set of all coefficients of $(X - g_1(y))(X - g_2(y)) \cdots (X - g_k(y))$. Then y is integral over the finitely generated k-algebra $k[S]$. Moreover, any $g \in G$ acting on $(X - g_1(y))(X - g_2(y)) \cdots (X - g_k(y))$ is simply permuting the roots of this polynomial, therefore the coefficients are invariant under G, hence they are in A^G. Let T be the set of all coefficients of $(X - g_1(y_i))(X - g_2(y_i)) \cdots (X - g_k(y_i))$,

$i = 1, \ldots, n$. Let $B = k[T]$. Then B is the desired finitely generated k-subalgebra in A^G.

Since all the generators of A are integral over B, $A = B[y_1, \ldots, y_n]$ is a finitely generated B-module. By Hilbert basis theorem, B is Noetherian, hence A is a Noetherian B-module. Note that A^G can be viewed as a B-submodule of A. Therefore A^G is a finitely generated B-module. Say $A^G = Bz_1 + \cdots + Bz_m$. Then $A^G = B[z_1, \ldots, z_m]$ is a finitely generated k-algebra generated by generators of B and $z_1, \ldots, z_m$. □

Lemma 2.4.6. *Suppose $A \subset B$ are domians. B is integral over A. Then A is a field if and only if B is a field.*

Proof. ($\Longrightarrow$) Take $0 \neq x \in B$. Since B is integral over A, there exist $a_1, \ldots, a_n \in A$ such that $x^n + a_1 x^{n-1} + \cdots + an = 0$. We may assume $a_n \neq 0$. Then $x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) = -a_n$. Thus x is a unit.

($\Longleftarrow$) Take $0 \neq x \in A$. Then there exists $x^{-1} \in B$. $x^{-}1$ is integral over A implies there exist $a_1, \ldots, a_n \in A$ such that $\left(x^{-1}\right)^n + a_1 \left(x^{-1}\right)^{n-1} + \cdots + a_n = 0$. Multiply by x^{n-1} and rearrange the equation, we get $x^{-1} = -(a_1 + a_2 x + \cdots + an_x^{n-1}) \in A$. □

Theorem 2.4.7 (Weak Nullstellensatz)**.** *Let k be a field, F a finitely generated k-algebra, which is a field. Then F is a finite field extension of k (i.e. $\dim_k(F) < \infty$), hence F is algebraic field extension over k.*

Proof. By Noether Normalization Lemma, there exist algebraically independent $z_1, \ldots, z_m \in F$ such that F is a finitely generated $k[z_1, \ldots, z_m]$-module. By the above lemma, $k[z_1, \ldots, z_m]$ is a field. Since

$z_1, \ldots, z_m$ are algebraically independent, $k[z_1, \ldots, z_m]$ is isomorphic to a polynomial ring unless $m = 0$. Since a polynomial ring cannot be a field, we have $m = 0$. Hence F is a finitely generated k-module.

For the second statement, let $x \in F$, consider $1, x, x^2, \ldots, x^n, \ldots$. Since F is a finitely dimensional k-vector space, there exists a $j \in \mathbb{N}$ such that x^j is a linear combination of $1, x, x^2, \ldots, x^{j-1}$. That is, there exist $a_1, \ldots, a_j \in k$ such that

$$x^j + a_1 x^{j-1} + \cdots + a_j = 0$$

Therefore x is algebraic over k. □

Corollary 2.4.8 (Weak Nullstellensatz)**.** *Suppose k is algebraically closed. Then there is a one-to-one correspondence between k^n and* $\mathrm{m} \cdot \mathrm{Spec}(k[X_1, \ldots, X_n])$ *given by*

$$(a_1, \ldots, a_n) \longleftrightarrow (X_1 - a_1, \ldots, X_n - a_n).$$

Proof. Let $A = k[X_1, \ldots, X_n]$. For $a = (a_1, \ldots, a_n) \in k^n$, define k-algebra homomorphism $ev_a : A \to k$ given by $f \mapsto f(a)$. It is surjective, therefore $k = \mathrm{Im}(ev_a) \cong A/\ker(ev_a)$. So $\ker(ev_a)$ is maximal. Clearly, $(X_1 - a_1, \ldots, X_n - a_n) \subset \ker(ev_a)$. Now $(X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal since for every $f \in A$ can be written as $f = f(a) + h$ where $h \in (X_1 - a_1, \ldots, X_n - a_n)$. It follows from the identity:

$$\begin{aligned} f &= \sum b_i X_1^{i_1} \cdots X_n^{i_n} \\ &= \sum b_i (a_1 + (X_1 - a_1))^{i_1} \cdots (a_n + (X_n - a_n))^{i_n} \\ &= \sum b_i a_1^{i_1} \cdots a_n^{i_n} \mod (X_1 - a_1, \ldots, X_n - a_n) \end{aligned}$$

Conversely, let m be a maximal ideal of A. Then A/m is a finitely generated k-algebra which is a field, hence by the above theorem A/m is algebraic over k. Since k is algebraically closed, we have $A/m = k$. Set $a_i = X_i + m \in A/m = k$. Then the natural map $A \to A/m = k$ is ev_a. Therefore $m = \ker(ev_a)$. □

2.5 Varieties

When we study the polynomial ring $k[X_1, \ldots, X_n]$, it is natural to view $k[X_1, \ldots, X_n]$ as a ring of polynomial functions on k^n. k^n is called **affine n-space** in this case. We often look at a collection of polynomials (ideal) instead of a single polynomial. Similarly, we will look at the common zero locus of a collection of polynomials. An **affine variety** $X \subset k^n$ is a subset of the form $V(S) = \{a \in k^n \mid \forall f \in S, f(a) = 0\}$, where $S \subset k[X_1, \ldots, X_n]$. Note that $V(S) = V(I)$, where I is the ideal generated by S. Therefore every affine variety is the vanishing locus for some ideal of $k[X_1, \ldots, X_n]$. For $X \subset k^n$, we define the ideal of X by $I(X) = \{f \in k[X_1, \ldots, X_n] \mid \forall a \in k^n, f(a) = 0\}$. It is easy to verify the following properties:

(i) If $\{I_\alpha\}$ is a collection of ideals, then $V(\bigcup_\alpha I_\alpha) = \bigcap_\alpha V(I_\alpha)$.

(ii) $V(I) \cup V(J) = V(IJ)$.

(iii) $V(0) = k^n, V(1) = \emptyset, V(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) = \{(a_1, a_2, \ldots, a_n)\}$.

(iv) $I \subset I' \implies V(I) \supset V(I'), X \subset X' \implies I(X) \supset I(X')$.

(v) $V(I(X)) \supset X$, equality holds if and only if X is an affine variety.

If we view affine varieties as closed sets in k^n, then property (i), (ii) and (iii) show affine varieties form a topology on k^n. It is called the **Zariski topology**. For an affine variety $X \subset k^n$, the **coordinate ring** $A(X)$ is defined to be $k[X_1, \ldots, X_n]/I(X)$. Two polynomial functions agree on X if and only if their difference vanishes on X, hence they are congruent modulo $I(X)$. Therefore $A(X)$ is a "faithful" representation of polynomial functions on X.

An affine variety is **irreducible** if it is not the union of two proper subvarieties. Irreducible variety corresponds to prime ideal in the polynomial ring.

Proposition 2.5.1. *An affine variety $X \subset k^n$ is irreducible if and only if $I(X)$ is prime.*

Proof. ($\Longrightarrow$) If A, B are two ideals such that $AB \subset I(X)$, then $V(A) \cup V(B) = V(AB) \subset X$. We have $X = (X \cap V(A)) \cup (X \cap V(B))$, hence $X \subset V(A)$ or $X \subset V(B)$. Therefore $A \subset I(V(A)) \subset I(X)$ or $B \subset I(V(B)) \subset I(X)$. Thus $I(X)$ is prime.

($\Longleftarrow$) Let A, B be two ideals such that $X = V(A) \cup V(B) = V(AB)$. Then $AB \subset I(V(AB)) \subset I(X)$. Since $I(X)$ is prime, we have $A \subset I(X)$ or $B \subset I(X)$, hence $V(A) \supset X$ or $V(B) \supset X$. Thus X is irreducible. □

Theorem 2.5.2. *Any affine variety $V \subset k^n$ has a unique irreducible decomposition $V = V_1 \cup \cdots \cup V_m$ such that V_i's are irreducible and $V_i \not\subset V_j$ for all $i \neq j$.*

Proof. Since $k[X_1, \ldots, X_n]$ is noetherian, any set of ideals has a maximal element. Therefore any set of affine variety has a minimal element. Apply this to the collection of affine varieties having no finite irreducible decomposition. The uniqueness is easy to check. □

The following proposition illustrates the relation between points in an affine variety and maximal ideals in a k-algebra.

Proposition 2.5.3. *Let k be an algebraically closed field. Let $A = k[x_1, \ldots, x_n]$ be a finitely generated k-algebra. Let I denote the kernel of the k-algebra homomorphism $k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n]$ given by $X_i \mapsto x_i$, $A \cong k[X_1, \ldots, X_n]/I$. Then there is a one-to-one correspondence between $V(I)$ and* $\mathrm{m} \cdot \mathrm{Spec}(A)$.

Proof. There is a one-to-one correspondence between $\mathrm{m} \cdot \mathrm{Spec}(A)$ and $\{J \in \mathrm{m} \cdot \mathrm{Spec}(k[X_1, \ldots, X_n]) \mid I \subset J\}$. By weak Nullstellensatz, each maximal ideal J is of the form $(X_1 - a_1, \ldots, X_n - a_n)$ and one-to-one corresponds to $(a_1, \ldots, a_n) \in k^n$. Since $I \subset J$ implies $\{(a_1, \ldots, a_n)\} = V(J) \subset V(I)$, we have a one-to-one correspondence between $V(I)$ and $\mathrm{m} \cdot \mathrm{Spec}(A)$. □

Note that for any proper ideal $I \subset k[X_1, \ldots, X_n]$ (k algebraically closed), we have $V(I) \supset V(J) \neq \emptyset$ for $I \subset J \in \mathrm{m} \cdot \mathrm{Spec}(k[X_1, \ldots, X_n]$ by weak Nullstellensatz.

Let $I \subset A$ be an ideal. Define the **radical** of I by
$\sqrt{I} = \{a \in A \mid a^n \in I \text{ for some } n \in \mathbb{N}\}$.

Theorem 2.5.4 (Hilbert's Nullstellensatz)**.** *Let k be an algebraically closed field, I be an ideal in $k[X_1, \ldots, X_n]$. Then $I(V(I)) = \sqrt{I}$.*

Proof. ($\supset$) Trivial.

($\subset$) Suppose $f \in I(V(I))$. Let $I' := (I, fY - 1)$ be an ideal of $k[X_1, \ldots, X_n, Y]$. Then $V(I') \subset k^{n+1}$ is empty, hence $I' = k[X_1, \ldots, X_n, Y]$. Therefore $1 = \sum_{i=1}^{r} g_i h_i + g_0(fY - 1), h_i \in I, g_0, \ldots, g_r \in k[X_1, \ldots, X_n, Y]$. Multiply both side of this equation by a high power of f, we can get $f^d = \sum G_i(X_1, \ldots, X_n, fY)h_i + G_0(X_1, \ldots, X_n, fY)(fY - 1)$. Substitute $1/f$ for Y, we have $f^d = \sum G_i(X_1, \ldots, X_n, 1)h_i \in I$. Thus $f \in \sqrt{I}$. □

Corollary 2.5.5. *Let k be an algebraically closed field.*

(i) *V and I induces one-to-one correspondences:*

$$\{\textit{affine varieties in } k^n\} \longleftrightarrow \{\textit{radical ideals in } k[X_1, \ldots, X_n]\}$$
$$\{\textit{irreducible varieties in } k^n\} \longleftrightarrow \{\textit{prime ideals in } k[X_1, \ldots, X_n]\}$$

(ii) *Suppose $A = k[x_1, \ldots, x_n] = k[X_1, \ldots, X_n]/I$ is a finitely generated k-algebra, I is a ideal of $k[X_1, \ldots, X_n]$. Then there is a one-to-one correspondence:*

$$\operatorname{Spec} A \longleftrightarrow \{\textit{irreducible subvarieties of } V(I) \subset k^n\}$$

The spectrum of a ring A also has its own Zariski topology. The closed sets are the subsets of the form $V(I) = \{P \in \operatorname{Spec} A \mid I \subset P\}$ where I is an ideal. It is easy to verify that $V(0) = \operatorname{Spec} A$, $V(A) = \emptyset$, $\cap_\alpha V(I_\alpha) = V(\sum_\alpha I_\alpha)$, $V(I_1) \cup V(I_2) = V(I_1 I_2) = V(I_1 \cap I_2)$.

2.6 Localization

Recall that a local ring is a ring with only one maximal ideal. The technique of localization reduces many problems to the local case. This turns out to be useful in many cases.

The idea of localization comes from geometry. Given a point in an affine variety $p \in X \subset k^n$, we want to investigate the property of X near p in the Zariski topology. This is done by looking at an open neighborhood of p. An open neighborhood of p is the complement of an affine variety Y which does

not contain p. We want to make this open neighborhood as small as possible, hence Y should be large. Therefore we may assume Y is the zero locus of a single polynomial f which does not vanish at p. In this case $X - Y$ is isomorphic to a affine variety in k^{n+1}.The points of $X - Y$ are points at which f does not vanish. Therefore there exists a function $z(x)$ such that $z(x)f(x) = 1$. This is the inverse function of f. The idea is to adjoin the inverse of f to $A(X)$. If $X \subset k^n$ corresponds to the ideal $I \subset k[X_1, \ldots, X_n]$, then $X - Y$ corresponds to $J = I + (zf - 1) \subset k[X_1, \ldots, x_n, z]$. $V(J)$ is a lifting of $X - Y$. If we project $V(J)$ to the $X_1, \ldots, X_n$-plane, then it is $X - Y$. We have $A(X) = k[X_1, \ldots, X_n]/I$, then we may write $k[X_1, \ldots, X_n, z]/J = A(X)[z]/(zf - 1)$. This is adjoining an inverse of f to $A(X)$.

We want to invert many polynomials at the same time. If f, g are inverted, then fg should be inverted as well. Therefore the set of inverted elements S should be **multiplicatively close**. That is, any product of S is in S. For a ring A, a subset $S \subset A$ is called a **multiplicative set** if it is multiplicatively closed and contains 1. If f is inverted and $fg = 0$, then we should make $g = 0$.

Given a ring A and a multiplicative set $S \subset A$. We define the **localization of A at S**, written as $S^{-1}A$, to be the set of equivalence classes of $A \times S$ with the equivalence relation $(a, s) \sim (m', s')$ if $u(as' - a's) = 0$ for some $u \in S$. The equivalence class of (a, s) is denoted by a/s. $S^{-1}A$ forms a ring under addition $a/s + a'/s' = (as' + a's)/ss'$ and multiplication $(a/s)(a'/s') = aa'/ss'$.

Proposition 2.6.1. (i) *$\kappa : A \to S^{-1}A, a \mapsto a/1$ is a ring homomorphism.*

(ii) *$\kappa(s)$ is a unit in $S^{-1}A$ for all $s \in S$.*

(iii) *κ is a universal S-inverting homomorphism: that is, for any ring*

homomorphism $f : A \to B$ into some ring B such that $f(S) \subset B^\times$, there is a unique $\overline{f} : S^{-1}A \to B$ such that $f = \overline{f} \circ \kappa$.

(iv) $\ker \kappa = \{a \in A \mid \exists s \in S, sa = 0\}$.

The proof is omitted.

There are two maps between ideals of A and ideals of $S^{-1}A$. Given an ideal $I \subset A$, the extension of I is $e(I) = S^{-1}I = S^{-1}A \cdot \kappa(I) = \{i/s \mid i \in I, s \in S\}$. Given an ideal J in $S^{1-}A$, the restriction of J is $r(J) = A \cap J = \kappa^{-1}(J) = \{a \in A \mid a/1 \in J\}$.

Proposition 2.6.2. (i) *For any ideal $J \subset S^{-1}A$, we have $J = e(r(J))$. It follows that if A is Noetherian, then $S^{-1}A$ is Noetherian.*

(ii) *For any ideal $I \subset A$, we have $r(e(I)) = \{a \in A \mid \exists s \in S, sa \in I\}$. In particular, $e(I) = S^{-1}A$ if and only if $I \cap S \neq \emptyset$.*

(iii) *r induces a 1-1 correspondence between* $\operatorname{Spec}(S^{-1}A)$ *and* $\{P \in \operatorname{Spec} A \mid P \cap S = \emptyset\}$.

Proof. (i) If $a/s \in J$, then $a/1 = (a/s)(s/1) \in J$, hence $a \in r(J)$. Therefore $a/s = (a/1)(1/s) \in e(r(J))$. Thus $J \subset e(r(J))$. Since $J \supset \kappa(\kappa^{-1}(J)) = \kappa(r(J))$, we have $J \supset S^{-1}A \cdot \kappa(r(J)) = e(r(J))$. For the second statement, since every ideal J of $S^{-1}A$ is the image of some ideal I of A, the image of generators of I under κ are the generators of J. Hence if I is finitely generated, J is finitely generated as well.

(ii) $b \in r(e(I))$ if and only if $b/1 = a/s$ for some $a \in I, s \in S$ if and only if $bsu = au$ for some $u \in S$. Since $su \in S, au \in I$, we have $r(e(I)) \subset \{a \in A \mid \exists s \in S, sa \in I\}$. If $as \in I, a \in A, s \in S$, then $as/1 \in e(I)$, so $(as/1)(1/s) \in e(I)$. Hence $a \in r(e(I))$. Thus $r(e(I)) \supset \{a \in A \mid \exists s \in S, sa \in I\}$. For the

second statement, if $s \in I$ for some $s \in S$, then $e(I)$ contains a unit $s/1$, hence $e(I) = S^{-1}A$. If $e(I) = S^{-1}A$, then $r(e(A)) = A \ni 1$. By the first statement, there exists an $s \in S$ such that $1 \cdot s \in I$. Therefore $I \cap S \neq \emptyset$.

(iii) If J is a prime ideal in S^1A, then $r(J) = \kappa^{-1}(J)$ is a prime ideal in A. Moreover, $J = e(r(J))$ implies $r(J) \cap S = \emptyset$ and $r : \mathrm{Spec}(S^{-1}A) \to \{P \in \mathrm{Spec}\, A \mid P \cap S = \emptyset\}$ is injective. To show r is surjective, take $P \in \mathrm{Spec}\, A, P \cap S = \emptyset$. Then $as \in P, s \in S$ implies $a \in P$ since $s \notin P$ and P is prime. Thus $P = \{a \in A \mid \exists s \in S, as \in P\} = r(e(P))$. It remains to show that $e(P)$ is a prime ideal. Suppose $(a_1/s_1)(a_2/s_2) \in e(P)$, then $a_1a_2/s_1s_2 = b/t$ for some $b \in P, t \in S$. There exists $u \in S$ such that $a_1a_2tu = bs_1s_2u \in P$. Since $tu \in S$, we have $a_1a_2 \in P$ hence $a_1 \in P$ or $a_2 \in P$. That is, $a_1/s_1 \in e(P)$ or $a_2/s_2 \in e(P)$. Thus $e(P)$ is a prime ideal. □

If P is a prime ideal of A, then $S = A \setminus P$ is multiplicatively closed. We write A_P for $S^{-1}A$ in this case. A_p is the localization of A at P. By (iii) of the above proposition, A_P is a local ring with maximal ideal $e(P)$.

Example 2.6.3. (i) $\mathbb{Z}_{(p)} = \{a/b \mid a, b \in \mathbb{Z}, p \nmid b\}$

(ii) $k[X]_{(X-a)} = \{f/g \mid g(a) \neq 0\}$

Given an A-module M, and a multiplicative set $S \subset A$. We define the **localization of M at S**, written as $S^{-1}M$, to be the set of equivalence classes of $M \times S$ with the equivalence relation $(m, s) \sim (m', s')$ if $u(sm' - s'm) = 0$ for some $u \in S$. We write m/s for the equivalence class of (m, s). $S^{-1}M$ is an $S^{-1}A$-module with operations $m/s + n/t = (tm + sn)/st$ and $(a/s) \cdot (m/t) = am/st$, $m, n \in M, s, t \in S, a \in A$. Given an A-module homomorphism $f : M \to N$, we

define the localization of f at S to be $S^{-1}f : S^{-1}M \to S^{-1}N$ given by $m/s \mapsto f(m)/s$. This is an $S^{-1}A$-module homomorphism. Moreover, if $L \xrightarrow{f} M \xrightarrow{g} N$ are A-module homomorphisms, then $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f$ and $S^{-1}id_M = id_{S^{-1}M}$.

Lemma 2.6.4. *Suppose $L \xrightarrow{f} M \xrightarrow{g} N$ is an exact sequence of A-module homomorphisms. Then $S^{-1}L \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}N$ is an exact sequence of $S^{-1}A$-module homomorphisms.*

Proof. ($\subset$) Since $S^{-1}g \circ S^{-1}f = S^{-1}(g \circ f) = 0$, we have $\operatorname{Im} S^{-1}f \subset \ker S^{-1}g$.

($\supset$) Suppose $S^{-1}g(m/s) = g(m)/s = 0 \in S^{-1}N$, then there exists $u \in S$ such that $ug(m) = 0$. Hence $g(um) = 0$, $um \in \ker g = \operatorname{Im} f$. Therefore $um = f(l)$ for some $l \in L$. We have $m/s = um/us = f(l)/us = S^{-1}f(l/us) \in \operatorname{Im} S^{-1}f$. Thus $\operatorname{Im} S^{-1}f \supset \ker S^{-1}g$. □

The above lemma is saying that localization is exact.

A property P for an A-module M is called a local property if the following holds: M has P if and only if M_Q has P for all $Q \in \operatorname{Spec} A$. Here are some examples of local properties:

Proposition 2.6.5. *Let M be an A-module. Then the following are equivalent:*

(i) $M = 0$.

(ii) $M_P = 0$ *for all* $P \in \operatorname{Spec} A$.

(iii) $M_m = 0$ *for all* $m \in \mathrm{m} \cdot \operatorname{Spec} A$.

In short, a module being zero is a local property.

Proof. (i) $\implies$ (ii) $\implies$ (iii) Trivial.

(iii) $\implies$ (i) Let $x \in M$ be given. If $x \neq 0$, then the annihilator of M $\operatorname{ann}(x) = \{a \in A \mid ax = 0\}$ is not A. Hence $\operatorname{ann}(x)$ is contained in some maximal ideal m. Then $x/1 \in A_m$ is not 0 since $x/1 = 0$ if and only if there is a $u \notin m$ such that $ux = 0$. But that means u is in $\operatorname{ann}(x) \subset m$. Since we assume $A_m = 0$ for all $m \in \mathrm{m} \cdot \operatorname{Spec} A$. There is no such $x \neq 0$, thus $M = 0$. □

Proposition 2.6.6. *Let $f : M \to N$ be an A-module homomorphism. Then the following are equivalent:*

(i) *f is injective.*

(ii) *f_P is injective for all $P \in \operatorname{Spec} A$.*

(iii) *f_m is injective for all $m \in \mathrm{m} \cdot \operatorname{Spec} A$.*

The statement is true if we replace "injective" with "surjective".

Proof. (i) $\implies$ (ii) f being injective is equivalent of saying $0 \to M \xrightarrow{f} N$ is exact. Hence $0 \to M_P \xrightarrow{f_P} N_P$ is exact for all $P \in \operatorname{Spec} A$. Thus f_P is injective for all $P \in \operatorname{Spec} A$.

(ii) $\implies$ (iii) Trivial.

(iii) $\implies$ (i) Let $L = \ker f$, then the sequence $0 \to L \to M \xrightarrow{f} N$ is exact. Hence $0 \to L_m \to M_m \xrightarrow{f_m} N_m$ is exact for all $m \in \mathrm{m} \cdot \operatorname{Spec} A$. It follows that $L_m \cong \ker f_m = 0$ for all $m \in \mathrm{m} \cdot \operatorname{Spec} A$. Therefore by the previous proposition, $L = 0$. Thus f is injective.

For the "surjective" part, reverse the arrows and replace ker with coker. □

2.7 Associated primes and primary decomposition

Let M be an A-module, $m \in M$. Recall that the annihilator of m is $\operatorname{ann}(m) = \{a \in A \mid am = 0\}$. The **support** of M is $\operatorname{Supp} M = \{P \in \operatorname{Spec} A \mid M_P \neq 0\}$. Note that $M_P \neq 0$ if and only if there exists an $m \in M$ such that $\operatorname{ann}(m) \subset P$. Recall that $V(I) = \{P \in \operatorname{Spec} A \mid I \subset P\}$ where I is an ideal of A.

Proposition 2.7.1. (i) $\operatorname{Supp}(A/I) = V(I)$

(ii) *If L is a submodule of an A-module M, then* $\operatorname{Supp} M = \operatorname{Supp} L \cup \operatorname{Supp} M/L$.

(iii) *If $M = \sum_{i \in J} M_i$, then* $\operatorname{Supp} M = \bigcup_{i \in J} \operatorname{Supp} M_i$.

(iv) *If M is a finitely generated A-module, then* $\operatorname{Supp} M = V(\operatorname{ann}(M))$.

(v) *If $P \in \operatorname{Supp} M$, then $V(P) \subset \operatorname{Supp} M$.*

Proof. (i) A/I is generated by the element $1 + I$. Hence $(A/I)_P \neq 0$ if and only if $1 + I \neq 0$ in $(A/I)_P$. That is, $I = \operatorname{ann}(1 + I) \subset P$. This is if and only if $P \in V(I)$.

(ii) Consider the exact sequence $0 \to L_P \to M_P \to (M/L)_P \to 0$. $M_P \neq 0$ if and only if $L_P \neq 0$ or $(M/L)_P \neq 0$.

(iii) ($\supset$) Trivial.

($\subset$) $P \in \operatorname{Supp} M$ if and only if $P \supset \operatorname{ann}(m)$ for some $m \in M$, $m = m_{i_1} + \cdots + m_{i_k} \in M_{i_1} + \cdots + M_{i_k}$. Hence $P \in \operatorname{Supp} M_{i_1} + \cdots + M_{i_k}$. It is sufficient to show that if $M = N_1 + N_2$, then $\operatorname{Supp} M \subset \operatorname{Supp} N_1 \cup \operatorname{Supp} N_2$. Since $M/N_1 \cong N_2/(N_1 \cap N_2)$, by (ii) we have $\operatorname{Supp} M = \operatorname{Supp} N_1 \cup \operatorname{Supp} M/N_1 = \operatorname{Supp} N_1 \cup \operatorname{Supp} N_2/(N_1 \cap N_2) \subset \operatorname{Supp} N_1 \cup \operatorname{Supp} N_2$.

(iv) Suppose $M = Am_1 + \cdots + Am_k$, then by (ii) $\operatorname{Supp} M = \bigcup_{i=1}^k \operatorname{Supp} Am_i = \bigcup_{i=1}^k V(\operatorname{ann}(m_i)) = V(\bigcap_{i=1}^k \operatorname{ann}(m_i)) = V(\operatorname{ann}(M))$.

(v) $P \in \operatorname{Supp} M$ if and only if there is an $m \in M$ such that $\operatorname{ann}(m) \subset P$, hence for all $Q \in V(P)$, $ann(m) \subset P \subset Q$. Therefore $Q \in \operatorname{Supp} M$. □

Let M be an A-module, $P \in \operatorname{Spec} A$ is an **associated prime** of M if $P = \operatorname{ann}(m)$ for some $m \in M$. It is equivalent to say that M contains a submodule Am isomorphic to A/P. The set of associated primes of M is denoted $\operatorname{Ass} M$. It is a subset of $\operatorname{Supp} M$.

Proposition 2.7.2. (i) *If $P \in \operatorname{Spec} A$, then for all $y \notin P$, $\operatorname{ann}(y + P) = P$.*

(ii) *Any maximal element in $\{\operatorname{ann}(m) \mid 0 \neq m \in M\}$ is prime (i.e. , in $\operatorname{Ass} M$).*

(iii) *If A is Noetherian, $M \neq 0$, then $\operatorname{Ass} M \neq \emptyset$.*

(iv) *If L is a submodule of M, then $\operatorname{Ass} M \subset \operatorname{Ass} L \cup \operatorname{Ass} M/L$.*

Proof. (i) Since A/P is a domain, $y + P$ is only annihilated by P.

(ii) Suppose $\operatorname{ann}(x)$ is maximal, and $st \in \operatorname{ann}(x)$, $t \notin \operatorname{ann}(x)$. Then $tx \neq 0$, and $\operatorname{ann}(tx)$ is in $\{\operatorname{ann}(m) \mid 0 \neq m \in M\}$. Since $\operatorname{ann}(tx) \supset \operatorname{ann}(x)$ and $\operatorname{ann}(x)$ is maximal, we have $\operatorname{ann}(tx) = \operatorname{ann}(x)$. Thus $s \in \operatorname{ann}(tx) = \operatorname{ann}(x)$ and $\operatorname{ann}(x)$ is prime.

(iii) If A is Noetherian, then $\{\operatorname{ann}(m) \mid 0 \neq m \in M\}$ has a maximal element which is prime by (ii).

(iv) Let $P \in \operatorname{Ass} M$, then there is a submodule $N \subset M$, such that $N \cong A/P$.
Case 1: $L \cap N = 0$. Then M/L has a submodule $(N + L)/L \cong N/0 \cong A/P$, hence $P \in \operatorname{Ass} M/L$.
Case 2: $L \cap N \neq 0$. Then there is a $0 \neq y \in L \cap N$, by (i), $\operatorname{ann}(y) = P$, hence $P \in \operatorname{Ass} L$.

□

Theorem 2.7.3. *Let A be a Noetherian ring, M be an A-module. Then the minimal element $P \in \operatorname{Supp} M$ is in* $\operatorname{Ass} M$.

Proof. Suppose $P \in \operatorname{Supp} M$ is minimal. Then for any prime ideal Q properly contained in P, $M_Q = 0$. We know $\operatorname{Spec} A_P = \{Q_P \mid Q \subset P\}$. For $P \neq Q \in \operatorname{Spec} A_P$, $(M_P)_{Q_P} = M_Q = 0$. Therefore $\operatorname{Supp} M_P = \{P_P\}$. Since A is Noetherian, $\operatorname{Ass} M_P$ is nonempty. Therefore $\operatorname{Ass} M_P = \{P_P\}$. It follows that there exists an $m \in M$ such that $\operatorname{ann}(m/1) = P_P$ (note that $\operatorname{ann}(m/s) = \operatorname{ann}(m/1)$). For all $t \in A \setminus P$, $\kappa(\operatorname{ann}(tm)) = \operatorname{ann}(tm)A_p \subset \operatorname{ann}(tm/1) = \operatorname{ann}(m/1) = P_P$. Therefore $\operatorname{ann}(tm) \subset \kappa^{-1}(\kappa(\operatorname{ann}(tm))) \subset \kappa^{-1}(P_P) = P = (p_1, \ldots, p_k)$. Since P annihilates $m/1$, $p_i m/1 = 0$ for $i = 1, \ldots, k$. Hence there exists $t_i \in A \setminus P$ such that $t_i p_i m = 0$ for $i = 1, \ldots, k$. Set $t = t_1 \cdots t_k \in A \setminus P$. Then $p_i \in \operatorname{ann}(tm)$ for $i = 1, \ldots, k$, hence $P \subset \operatorname{ann} tm$. Thus $P = \operatorname{ann}(tm)$. □

Corollary 2.7.4. *If M is a finitely generated A-module, where A is Noetherian, then* $\operatorname{Supp} M = \bigcup_{i=1}^{n} V(P_i)$ *where P_i's are the finitely many minimal prime containing* $\operatorname{ann}(M)$, $P_i \in \operatorname{Ass} M$.

Proof. Since M is finitely generated, it follows that $\operatorname{Supp} M = V(\operatorname{ann}(M))$. This closed subset $V(\operatorname{ann}(M))$ of $\operatorname{Spec} A$ is a finite union of irreducible closed sets, which correspond to the prime ideals containing $\operatorname{ann} M$. □

Let M be an A-module, an nonzero element $a \in A$ is called a **zero-divisor** on M if $am = 0$ for some $m \in M$. Clearly the set of all zero-divisors on M is $\bigcup_{0 \neq m \in M} \operatorname{ann}(m) \setminus 0$. If A is Noetherian, then the maximal elements in $\{ann(m) \mid 0 \neq m \in M\}$ are in $\operatorname{Ass} M$. It follows that $\bigcup_{0 \neq m \in M} \operatorname{ann}(m) \setminus 0 = \bigcup_{P \in \operatorname{Ass} M} P \setminus 0$.

Definition 2.7.5. An ideal Q in A is primary if for any $f, g \in Q$, $fg \in Q$ implies $f \in Q$ or $g^n \in Q$ for some $n \in \mathbb{N}$.

Equivalently, every zero-divisor of A/Q is nilpotent.

If Q is a primary ideal, then it is easy to see $P = \sqrt{Q}$ is a prime ideal. We say that Q is a P-primary ideal.

Theorem 2.7.6. *Let Q be an ideal of a Noetherian ring A. Then Q is primary if and only if* $\mathrm{Ass}(A/Q) = \{P\}$.

Proof. ($\Longrightarrow$) Suppose Q is P-primary, and $P = \sqrt{Q}$. Then every zero-divisor on A/Q (viewed as an A-module) is in P.Take $0 \neq x \in A/Q$, we have $Q \subset \mathrm{ann}(x) \subset P$. If $ann(x)$ is prime, then $ann(x) \supset \sqrt{Q} = P$, hence $ann(x) = P$. Therefore $\mathrm{Ass}(A/Q) \subset \{P\}$. Since A is Noetherian, it follows that $\mathrm{Ass}(A/Q)$ is nonempty. Thus $\mathrm{Ass}(A/Q) = \{P\}$.

($\Longleftarrow$) Suppose $\mathrm{Ass}(A/Q) = \{P\}$. Then P is the unique maximal element in $\mathrm{ann}(m) \mid 0 \neq m \in M\}$ and the unique minimal element in $\mathrm{Supp}(A/Q)$. Therefore $P = \{$zero-divisors on $A/Q\}$ and $\mathrm{Supp}(A/Q) = V(P)$. Since $V(P) = \mathrm{Supp}(A/Q) = V(Q)$, it follows that P is the unique minimal prime ideal containing Q, hence we have $\sqrt{Q} = P$. Combine this with $P = \{$zero-divisors on $A/Q\}$, we see that every zero-divisors of A/Q is nilpotent. Thus Q is P-primary. □

Definition 2.7.7. Let I be an ideal of A. Then I is called indecomposible if I cannot be written as the intersection of two strictly bigger ideals.

Proposition 2.7.8. *In a Noetherian ring A, any ideal I is an intersection of finitely many indecomposible ideals.*

Proof. Suppose the set of all ideals that is not an intersection of finitely many indecomposible ideals is not empty, and I is the maximal element in it. Then I is not an indecomposible ideal, hence I is the intersection of two strictly bigger ideals. Since I is the maximal, these two bigger ideals are intersections of finitely many prime ideals. Hence I is an intersection of finitely many prime ideals. This is a contradiction. Thus any ideal I is an intersection of finitely many indecomposible ideals. □

Proposition 2.7.9. *Suppose A is a Noetherian ring, and I is an indecomposible ideal in A. Then I is primary.*

Proof. Note that I is indecomposible if and only if 0 is indecomposible in A/I, and I is primary if and only if 0 is primary in A/I. Thus we may assume $I = 0$ is indecomposible. Suppose $x, y \in A$, and $xy = 0$. Then $y \in \operatorname{ann}(x) \subset \operatorname{ann}(x^2) \subset \cdots$. Therefore there exists an $n \in \mathbb{N}$ such that $\operatorname{ann}(x^n) = \operatorname{ann}(x^{n+1}) = \cdots$. Take $z \in (y) \cap (x^n)$. Then we have $ya = z = x^b$ for some $a, b \in A$. Multiply the equation by x we get $0 = xya = xz = x^{n+1}b$, hence $b \in \operatorname{ann}(x^{n+1}) = \operatorname{ann}(x^n)$. This implies $z = x^n b = 0$. Thus $(y) \cap (x^n) = 0$. Since we assumed 0 is indecomposible, either $y = 0$ or $x^n = 0$. Thus $I = 0$ is primary. □

Definition 2.7.10. A primary decomposition of an ideal I in a ring A is $I = Q_1 \cap \cdots \cap Q_k$ where $Q_1, \ldots, Q_k$ are primary ideals.

This is a shortest primary decomposition if

(i) $I \not\subset \bigcap_{j \neq i} Q_j$ for $i = 1, \ldots, k$.

(ii) Let $P_i = \sqrt{Q_i}$. $P_1, \ldots, P_k$ are distinct.

Proposition 2.7.11. *Let A be a Noetherian ring. Then the intersection of two P-primary ideals is P-primary.*

Proof. Suppose Q_1, Q_2 are P-primary ideals. Consider the short exact sequence

$$0 \to Q_1/(Q_1 \cap Q_2) \to A/(Q_1 \cap Q_2) \to A/Q_1 \to 0.$$

By (iv) of proposition 2.7.2., we have
$\mathrm{Ass}(A/(Q_1 \cap Q_2) \subset \mathrm{Ass}(Q_1/(Q_1 \cap Q_2)) \cup \mathrm{Ass}(A/Q_1)$. Since $Q_1/(Q_1 \cap Q_2)$ is isomorphic to $(Q_1 + Q_2)/Q_2$ which is a submodule of A/Q_2. Hence $\mathrm{Ass}(Q_1/(Q_1 \cap Q_2)) \subset \mathrm{Ass}(A/Q_2) = \{P\}$. Since $\mathrm{Ass}(A/Q_1) = \{p\}$, it follows that $\emptyset \neq \mathrm{Ass}(A/(Q_1 \cap Q_2)) \subset \{P\}$. Thus $Q_1 \cap Q_2$ is P-primary. □

If A is a Noetherian ring, then the primary decomposition of any ideal always exists. By the above proposition, the shortest primary decomposition also exists.

Theorem 2.7.12 (Lasker-Noether)**.** *Let A be a Noetherian ring. Then:*

(i) *Every ideal $I \subset A$ has a shortest primary decomposition:*
$I = Q_1 \cap \cdots \cap Q_k, P_i = \sqrt{Q_i}$.

(ii) $\mathrm{Ass}(A/I) = \{P_1, \ldots, P_k\}$.

Moreover, if $P_i \in \{P_1, \ldots, P_k\}$ is minimal, then $Q_i = \kappa^{-1}(I_{P_i})$. In particular the primary components belonging to the minimal associated primes of A/I are unique.

Proof. (i) It follows from the above proposition.

(ii) Consider the map $\iota : A/I \to \bigoplus_{i=1}^{k} A/Q_i$ given by $a + I \mapsto (a + Q_1, \ldots, a + Q_k)$. Clearly $\ker \iota = \bigcap_i (Q_i/I) = I/I = 0$. Therefore ι is injective, hence $\mathrm{Ass}(A/I) \subset \bigcup_{i=1}^{k} \mathrm{Ass}(A/Q_i) = \{P_1, \ldots, P_k\}$.

For any P_i, let $N_i = \bigcap_{j \neq i} Q_j/I \subset A/I$. Consider the map $\eta : A/I \to A/Q_i$. Clearly $\ker \eta = Q_i/I$, then $N_i \cap \ker \eta = I/I = 0$. Hence $\eta|_{N_i} : N_i \to A/Q_i$ is injective. Therefore $\emptyset \neq \mathrm{Ass}\, N_i \subset \mathrm{Ass}\, A/Q_i = \{P_i\}$. It follows that $\{P_i\} = \mathrm{Ass}(N_i) \subset \mathrm{Ass}(A/I)$. Thus $\mathrm{Ass}(A/I) = \{P_i, \ldots, P_k\}$.

For the last statement, suppose P_i is minimal in $\{P_1, \ldots, P_k\} = \mathrm{Ass}(A/I)$. Localize I at P_i, we have $I_{P_i} = Q_{1P_i} \cap \cdots \cap Q_{kP_i}$. For $j \neq i$, since $P_1, \ldots, P_k$ are distinct, there exists $t \in P_j \setminus P_i$. Since $P_j = \sqrt{Q_j}$, there exists an n such that $t^n \in Q_j \setminus P_i$. Therefore $t^n/1 \in Q_{jP_i}$ is a unit in A_{P_i}, hence $Q_{jP_i} = A_{P_i}$. It follows that $I_{P_i} = Q_{iP_i}$. On the other hand, $\kappa^{-1}(Q_{iP_i}) = \{a \in A \mid sa \in Q_i \text{ for some } s \in A \setminus P_i\}$. Since $s \notin P_i = \sqrt{Q_i}$, by the definition of primary, we have $a \in Q_i$. Hence $Q_i = \kappa^{-1}(Q_{iP_i}) = \kappa^{-1}(I_{P_i})$. □

Chapter 3

Graded rings and Modules

3.1 Tensor Products

Definition 3.1.1. Let M and N be A-modules. The **tensor product** of M and N over A, written $M \otimes_A N$, is the A-module generated by symbols $m \otimes n$ for $m \in M$ and $n \in N$, with relations

$$rm \otimes n = m \otimes rn$$

$$(m + m') \otimes n = m \otimes n + m' \otimes n$$

$$m \otimes (n + n') = m \otimes n + m \otimes n'.$$

When the context is clear we may omit the subscript A.

Let M, N and L be A-modules. A **bilinear** map from the set $M \times N$ to L is a map that is linear in each factor. The above relations say exactly that the natural map $\varphi : M \times N \to M \otimes_A N$ taking (m, n) to $m \otimes n$ is bilinear. The tensor product can be characterized in the following universal property: for any

A-module L and a bilinear map $f : M \times N \to L$, there exists a unique homomorphism $\bar{f} : M \otimes_A N \to L$ such that $f = \bar{f} \circ \varphi$.

If $\alpha : M \to M'$ and $\beta : N \to N'$ are A-module homomorphisms, then there is an induced homomorphism $\alpha \otimes \beta : M \otimes N \to M' \otimes N'$ sending $m \otimes n$ to $\alpha(m) \otimes \beta(n)$.

Proposition 3.1.2. *If M, N, K and L are A-modules, then*

(i) $M \otimes N \cong N \otimes M$ *and* $M \otimes (N \otimes K) \cong (M \otimes N) \otimes K$.

(ii) $(M \oplus N) \otimes K \cong (M \otimes K) \oplus (N \otimes K)$.

(iii) *If* $M \to N \to K \to 0$ *is an exact sequence, then the sequence* $L \otimes M \to L \otimes N \to L \otimes K \to 0$ *is exact.*

The tensor product is ***right exact*** *in the sense of* (iii).

Proof. These properties can be easily checked by using universal property. For example, the commutativity property follows from the fact that a bilinear map from $M \times N$ to K is the same as a bilinear map from $N \times M$ to K. For the third statement, it suffices to show that $\operatorname{coker}(L \otimes M \to L \otimes N)$ has the same universal property as $L \otimes K$. Note that the maps from $\operatorname{coker}(L \otimes M \to L \otimes N)$ corresponds to bilinear maps from $L \times M$ that kills the elements in $L \times N$, and these are exactly the same as bilinear maps from $L \times K$. □

3.2 Tor Functor

A **complex** of modules over a ring A is a sequence of A-modules and homomorphisms

$$\mathcal{F} : \cdots \to F_{i+1} \xrightarrow{\varphi_{i+1}} F_i \xrightarrow{\varphi_i} F_{i-1} \to \cdots$$

such that $\varphi_i \circ \varphi_{i+1} = 0$ for every i. The **homology** of $\mathcal{F}$ at F_i is defined to be

$$H_i\mathcal{F} = \ker \varphi_i / \operatorname{Im} \varphi_{i+1}.$$

The maps φ_i are called **differentials**. We shall only consider complex with $F_i = 0$ for all $i > 0$ or all $i < 0$ and not to indicate the terms that are zero. The complex $\mathcal{F}$ is said to be **exact** at F_i if $H_i\mathcal{F} = 0$. The complex $\mathcal{F}$ is called **exact** if it is exact at every F_i.

An A-module P is called **projective** if for every epimorphism of modules $f : M \to N$ and every homomorphism $g : P \to N$, there exists a map $\bar{g} : P \to M$ such that $g = f \circ \bar{g}$. Note that free modules are projective since if P is free on the generators p_i's, then we may take q_i in M that maps to the elements $g(p_i)$, and take $\bar{g}$ to be the map sending p_i to q_i.

Definition 3.2.1. A **projective resolution** of an A-module M is a complex

$$\mathcal{F} : \cdots \to F_n \xrightarrow{\varphi_n} \to \cdots \to F_1 \xrightarrow{\varphi_1} F_0$$

of projective A-modules such that $\operatorname{coker} \varphi_1 = M$ and $H_i\mathcal{F} = 0$ for $i > 0$.

If each F_i is a free module, then $\mathcal{F}$ is called a **free resolution**. If for some $n < \infty$ we have $F_{n+1} = 0$, but $F_i \neq 0$ for $0 \leq i \leq n$, then $\mathcal{F}$ is called a finite

resolution of length n.

Every module has a free resolution. To construct one, note that every module M is an image of a free module over the generators of M. Let M_1 be the kernel of this map and repeat this procedure, then we have a free resolution of M.

We now introduce the **Tor functor** and give some properties of it without proof.

If M and N are A-modules, and $\cdots \to F_{i+1} \xrightarrow{\varphi_{i+1}} F_i \to \cdots \to F_0$ is a projective resolution of M, then $\mathrm{Tor}_i^A(M,N)$ is the homology at $F_i \otimes N$ of the complex $\cdots \to F_{i+1} \otimes N \xrightarrow{\varphi_{i+1}\otimes 1_N} F_i \otimes N \to \cdots \to F_0 \otimes N$. The $\mathrm{Tor}_i^A(M,N)$ is independent of the choice of the projection resolution of M. Since the tensor product is right exact, we have $\mathrm{Tor}_0^A(M,N) = \mathrm{coker}(F_1 \to F_0) \otimes N = M \otimes N$.

The tensor product is commutative in the sense that $M \otimes N \cong N \otimes M$. The same is true for the Tor functor: $\mathrm{Tor}_i^A(M,N) \cong \mathrm{Tor}_i^A(N,M)$. Thus we can compute $\mathrm{Tor}_i^A(M,N)$ by tensoring M with a projective resolution of N.

For any short exact sequence $0 \to M' \to M \to M'' \to 0$ of A-modules, and any A-module N, there is a **long exact sequence of Tor**:

$$\cdots \to \mathrm{Tor}_i^A(M',N) \to \mathrm{Tor}_i^A(M,N) \to \mathrm{Tor}_i^A(M'',N) \to \mathrm{Tor}_{i-1}^A(M',N) \to \cdots$$
$$\cdots \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

3.3 Graded Rings and Modules

A ring A is **graded** if its additive group can be decomposed as a direct sum $A = \bigoplus_{i=0}^{\infty} A_i$ such that $A_i A_j \subset A_{i+j}$. Note that A_0 is a subring of A. If $a \in A_i$,

then we say a is **homogeneous of degree** i. Every $a \in A$ has a unique expression $a = a_0 + a_1 + a_2 + \cdots$ where each a_i is homogeneous. The a_i's are called **homogeneous component** of a. A **homogeneous ideal** of A is an ideal I generated by homogeneous elements. The ideal $\bigoplus_{i>0} A_i$ is called the **irrelevant ideal**, denoted A_+.

An A-module M is called a **graded A-module** if M can be decomposed as $M = \bigoplus_{i=0}^{\infty} M_i$ and $A_i M j \subset M_{i+j}$.

Suppose $M \bigoplus_{i=0}^{\infty} M_i$ is a graded A-module. We define $M[d]$ to be the graded module M shifted by d degrees. That is, $M[d]_i = M_{d+1}$.

Lemma 3.3.1. *Let $A = \bigoplus_{i=0}^{\infty} A_i$ be a Noetherian graded ring, and $M = \bigoplus_{i=0}^{\infty} M_i$ be a finitely generated graded A-module. Then each M_i is a finitely generated A_0-module.*

Proof. Since A is noetherian and M is finitely generated A-module, it follows that M is a noetherian A-module. Therefore the submodule AM_i is generated by a finite number of elements $m_1, \ldots, m_r \in M_i$. Clearly $M_i = \sum_{i=1}^{r} A_0 M_i$. □

Let $A = k[x_1, \ldots, x_n]$ be a finitely generated k-algebra, where k is a field, we may assign each x_i a degree d_i. Then A becomes a graded ring with $A_0 = k$. If $M = \bigoplus_{i=0}^{\infty} M_i$ is a finitely generated graded A-module, then by the above lemma, each M_i is a finite dimensional k-vector space. Hence we may talk about the dimension of each M_i. We encode this information in the **Hilbert series** $\mathrm{H}(M, t) = \sum_{i=0}^{\infty} \dim_k(M_i) t^i$.

Theorem 3.3.2 (Hilbert-Serre)**.** *Let $A = \bigoplus_{i=0}^{\infty} A_i$ be a graded ring with $A_0 = k$, where k is a field, and finitely generated as a k-algebra by homogeneous elements $x_1, \ldots, x_r$ with degrees $d_1, \ldots, d_r$. Let $M = \bigoplus_{i=0}^{\infty} M_i$ be a finitely generated graded*

A-module. Then the Hilbert series $\mathrm{H}(M,t)$ *is of the form*

$$\frac{f(t)}{\prod_{i=1}^{r}(1-t^{d_i})}$$

where $f(t)$ *is a polynomial in integer coefficients.*

Proof. We prove by induction on r. If $r=0$, then $A=k$ and M is a finite dimensional vector space, therefore $\mathrm{H}(M,t)$ is a polynomial. Suppose $r>0$, let K and L be the kernel and cokernel of multiplication by x_r, we have an exact sequence

$$0 \to K_r \to M_i \xrightarrow{x_r} M_{i+d_r} \to L_{i+d_r} \to 0.$$

From this exact sequence we have

$$\dim_k(K_i) - \dim_k(M_i) + \dim_k(M_{i+d_r}) - \dim_k(L_{i+d_r}) = 0.$$

Therefore

$$t^{d_r}\,\mathrm{H}(K,t) - t^{d_r}\,\mathrm{H}(M,t) + \mathrm{H}(M,t) - \mathrm{H}(L,t) = 0.$$

Thus

$$\mathrm{H}(M,t) = \frac{\mathrm{H}(L,t) - t^{d_r}\,\mathrm{H}(K,t)}{1-t^{d_r}}.$$

Since K an L are annihilated by x_r, they are finitely generated graded module over $k[x_1,\ldots,x_{r-1}]$, so by induction their Hilbert series have the desired form. Thus the above formula is the desired form for $\mathrm{H}(M,t)$. □

Suppose k is a field. A grade k-algebra $A=\bigoplus_{i=0}^{\infty}A_i$ with $A_0=k$ is very similar to local rings. In fact, many theorems of local rings can be translated to

theorems of grade k-algebra $A = \bigoplus_{i=0}^{\infty} A_i$ with $A_0 = k$. Note that although A may not have a unique maximal ideal, it does have a unique maximal homogeneous ideal A_+.

For the rest of this section, we assume $A = k[X_1, \ldots, X_r]$ is a graded algebra, where k is a field.

Theorem 3.3.3 (Graded Nakayama Lemma)**.** *Let $M \bigoplus_{i=0}^{\infty} M_i$ be a graded A-module. Then a subset $G \subset M$ of homogeneous elements generates M if and only if $\{x + A_+M \mid x \in G\}$ generates M/A_+M as a k-vector space.*

Proof. ($\Longrightarrow$) Trivial.

($\Longleftarrow$) It is sufficient to show each M_i is in AG. We do induction on i. If $i = 0$, the element $m \in M_0$ is of the form $m = \sum_i c_i x_i + b$, $c_i \in k, x_i \in G, b \in A_+M$. Since the homogeneous component of element in A_+M is of degree at least 1, it follows that $b = 0$ and we are done. Suppose $i > 0$, then $m \in M_i$ is of the form $m = \sum_i c_i x_i + \sum_j d_i n_i$, where $c_i \in k$, $x_i \in G$, $d_j \in A_+$, $m_j \in M$, and d_j, m_j are homogeneous. We may assume $\deg(m) = \deg(x_i)$ since x_i's are homogeneous. Then $\deg(d_j m_j) = \deg(a)$. Since $deg(d_j) > 0$, it follows that $\deg(m_j) < \deg(a) = i$. Thus by induction $m_j \in AG$ and we are done. □

Lemma 3.3.4. *A graded A-module M is projective if and only if it is free.*

Proof. Suppose M is projective. Let M_d be the first nonzero graded piece of M, and let $\{m_j\}$ be a basis of M_d as a k-vector space. Then M is a surjective image of a free module $F \oplus \bigoplus_j Am_j$ where F is a free module generated by elements of degree at least $d + 1$. Since M is projective, this map splits. The composition

of the splitting with the projection

$$M \to F \oplus \bigoplus_j Am_j \to \bigoplus_j Am_j$$

is clearly a surjection. Since $\bigoplus_j Am_j$ is free, we have $M = \bigoplus_j Am_j \oplus M'$ where M' the first nonzero piece of M' has degree at least $d+1$. Now M' is projective, so we may repeat this procedure to obtain

$$M = \bigoplus_j Am_j \oplus \bigoplus_k Am_k \oplus \cdots$$

□

Suppose M is a finitely generated graded A-module with homogenous generators $m_1, \ldots, m_r$ with degrees $d_1, \ldots, d_r$. Then we have $A^r \to M$ a free module surjecting onto M with e_i maps to m_i. We require the degree of e_i to be the degree of m_i for all i. Then A^r becomes a graded free A-module $A[-d_1] \oplus \cdots \oplus A[-d_r]$ and the natural epimorphism $A[-d_1] \oplus \cdots \oplus A[-d_r] \to M$ preserves degree. A graded free resolution of M is a resolution of M such that each free module is graded and each map preserves degree.

Proposition 3.3.5. *If M is a graded A-module, let $F_M = A \otimes_K (M/A_+M)$, a free A-module on the graded K-vector space M/A_+M of generators of M. Then there is a surjective map $\pi + M : F_M \to M$. If $\pi : F \to M$ is another free module surjecting onto M then $F \cong F' \oplus F_M$ with $\pi \mid_{F'} = 0$ and $\pi \mid_{F_M} = \pi_M$.*

Proof. Consider the map $F_M \to M/A_+M$ induced by $A \to A/A_+ = k$. Since F_M is

free, this lifts to a map $\pi_M : F_M \to M$. Let M' be the image of this map. Then

$$(M/M')/A_+(M/M') = M/(M' + A_+M) = 0.$$

Hence $M/M' = 0$ by graded Nakayama lemma and π is surjective.

Now suppose $\pi : F \to M$ is another free module surjecting onto M. Since F is free, we can lift to a map $F \to F_M$. Now F surjects onto M/A_+M, hence onto F_M/A_+F_M and so $F \to F_M$ is surjective. Since F_M is free, we can write $F \cong F' \oplus F_M$ with $\pi \mid_{F'} = 0$ and $\pi \mid_{F_M} = \pi_M$. □

Corollary 3.3.6. *If M is a graded A-module then M has a unique minimal free resolution*

$$\mathcal{F} : \cdots \to F_1 \to F_0 \to M \to 0.$$

Every free resolution of M is a direct sum of $\mathcal{F}$ and a free resolution of a zero module.

Proof. This follows by applying the proposition and induction. □

Theorem 3.3.7. *If $A = k[X_1, \ldots, X_r]$ is a graded polynomial ring, and M is a graded A-module, then the minimal resolution takes the form*

$$0 \to F_r \to F_{r-1} \to \ldots \to F_0 \to M \to 0.$$

Proof. We prove this by using the fact that $\mathrm{Tor}_i^A(M, k)$ can be calculated in both variables. First, we calculate $\mathrm{Tor}_i^A(M, k)$ using the minimal resolution of M. We have $F_i \otimes_A k = F_i/A_+F_i$, the vector space of generators of F_i. Since the resolution

is minimal, the differential $F_i \otimes k \to F_{i-1} \otimes k$ is zero, hence

$$\mathrm{Tor}_i^A(M,k) \cong F_i \otimes k \cong F_i/A_+F_i$$

On the other hand, the Koszol complex $K(X_1,\ldots,X_r)$ is a free resolution of k (see Appendix A), therefore $\mathrm{Tor}_i^A(M,k)$ is the homology of the complex $M \otimes K(X_1,\ldots,X_r)$. For $i > r$, this complex is zero, hence $\mathrm{Tor}_i^A(M,k) = 0$. This implies that $F_i/A_+F_i = 0$, hence $F_i = 0$ by graded Nakayama lemma. □

By construction of the free resolution and the fact that $\mathrm{Tor}_i^A(M,k) \cong F_i/A_+F_i$, we see that

$$0 \to \mathrm{Tor}_r^A(M,k) \otimes_k A \to \cdots \to \mathrm{Tor}_0^A(M,k) \otimes_k A \to M \to 0$$

is the minimal free resolution of M. Since each $\mathrm{Tor}_i^A(M,k)$ is a graded vector space, this makes $\mathrm{Tor}_0^A(M,k) \otimes_k A$ into a graded A-module and the free resolution into a graded free resolution.

3.4 Cohen-Macaulay Modules

The **Krull dimension** of a ring A is the supremum of the length of chain of proper inclusion of prime ideals $P_0 \supset P_1 \supset \cdots \supset P_n$. If M is an A-module, we define the Krull dimension of M to be the Krull dimension of the ring $A/\operatorname{ann}(M)$. We write $\dim(A)$ and $\dim(M)$ to denote the Krull dimension of A and M.

Suppose $A = k[x_1,\ldots,x_r]$ is a graded algebra and M is a finitely generated

graded A-module, a sequence of homogeneous elements $x_1, \ldots, x_r \in A_+$ is a **regular sequence** for M if each x_i is a non-zero-divisor on $M/(x_1, \ldots, x_{i-1})M \neq 0$. The **depth** of M is the length of the longest regular sequence for M, denoted by $\operatorname{depth}(M)$. In fact, any maximal regular sequence has the same length, see Appendix A. An A-module M is **Cohen-Macaulay** if its depth is equal to its Krull dimension.

Proposition 3.4.1. *Suppose $A = k[x_1, \ldots, x_r]$ is a graded algebra and M is a finitely generated graded A-module. Then the depth of M is at most the Krull dimenison of M.*

Proof. We prove by induction on the depth of M. Suppose the $\operatorname{depth}(M) = 0$, we are done since $\dim(M) \geq 0$. Suppose $\operatorname{depth}(M) = n$, let $a_1, \ldots, a_n$ be a maximal regular sequence for M, then $a_2, \ldots, a_n$ is a maximal regular sequence for M/a_1M. Therefore $\operatorname{depth}(M/aM) = n - 1$, by induction we have $\dim(M/a_1M) \geq n - 1$. Hence there is a chain of proper inclusion of prime ideals $P_1 \subset \cdots \subset P_{n-1}$ in A with $\operatorname{ann}(M/a_1M) \subset P_1$. Since a_1 is a non-zero-divisor on M, it is not in any associated primes of M. But $a_1 \in \operatorname{ann}(M/a_1M) \subset P_1$, so P_1 is not an associated prime of M. Since $\operatorname{ann}(M) \subset \operatorname{ann}(M/a_1M) \subset P_1$, it follows that P_1 is in the support of M. Recall that a minimal element of the support of M is an associated prime of M, hence P_1 is not minimal. Therefore there is an associated prime P_0 of M that is a proper subset of P_1, thus $P_0 \subset P_1 \subset \cdots \subset P_{n-1}$ is a chain of proper inclusion of prime ideals with $\operatorname{ann}(M) \subset P_0$. Hence $\dim(M) \geq n$. □

Corollary 3.4.2. *Suppose $A = k[x_1, \ldots, x_r]$ is a graded algebra and M is a finitely generated graded A-module. If M is Cohen-Macauley and $a \in A$ is a non-zero-divisor on M, then M/aM is Cohen-Macauley.*

Proof. Suppose $\dim(M) = n$, then $\dim(M/aM) \leq n$. Since a is a non-zero-divisor on M, we may extend it to a regular sequence of length n. Then $\operatorname{depth}(M/aM) = n - 1$. By the above proposition, we have $\dim(M/aM) \geq n - 1$. If $\dim(M/aM) = n$, then by the proof above we have $\dim(M) \geq n + 1$. But we assumed $\dim(M) = n$. Thus $\dim(M/aM) = n - 1$ and M/aM is Cohen-Macauley. □

Lemma 3.4.3. *Any finitely generated A-module M has an ascending sequence of submodules*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

with $M_i/M_{i-1} \cong A/P_i$ for some prime ideal P_i for $i = 1, \ldots, n$.

Proof. If M=0, we are done. If $M \neq 0$, then we choose $P_1 \in \operatorname{Ass}(M)$ and let M_1 be the submodule of M isomorphic to A/P_1. If $M_1 \neq M$, we repeat this process with M/M_1. Since M is Noetherian, the process eventually terminates. □

A composition series of an A-module M is an ascending sequence of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that each M_i/M_{i-1} is a simple module. That is, M_i/M_{i-1} has no submodule other than zero and itself. Clearly, a simple module is generated by any of its nonzero element. Therefore it is isomorphic to A/I where I is an ideal. Since the module is simple, I must be maximal.

Proposition 3.4.4. *If a finitely generated A-module M has Krull dimension zero, then it has a composition series of finite length. Moreover, if M is finite generated graded A-module where A is a finitely generated graded k-algebra and* $\dim(M) = 0$*, then M is a finite dimensional k-vector space.*

Proof. Suppose M has Krull dimension zero. Consider the ascending sequence of submodules $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ in the previous lemma. Since $\text{ann}(M) \subset \text{ann}(M_i/M_{i-1})$, the Krull dimension of M_i/M_{i-1} is also zero, hence P_i must be maximal. Therefore this sequence is the composition series of M.

Suppose M is a finitely generated graded A-module where A is a finitely generated k-algebra and $\dim(M) = 0$. Consider the composition series $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$. Each Mi/M_{i-1} is isomorphic to A/m where m is a maximal ideal of A. Since A/m is a finitely generated k-algebra and also a field, it is a finite field extension of k by weak Nullstellensatz. Therefore $\dim_k(M_i/M_{i-1}) < \infty$ for all i. It follows that $\dim_k(M) = \sum_i \dim_k(M_i/M_{i-1})$ is finite. □

Chapter 4

Invariant Theory

Let G be a finite group, k a field and V a finite dimensional k-vector space. Let $\varphi : G \to \mathrm{GL}(V)$ be a representation of G (i.e., φ is a group homomorphism). We write $k[V]$ for the coordinate ring of V. The group G acts on $k[V]$ via $(gf)(v) = f(\varphi(g)^{-1}v)$. The **ring of invariants** $k[V]^G$ is the set of all fixed points of this action.

By Theorem 2.4.5., the ring of invariants $k[V]^G$ is finitely generated. Let $f_1, \ldots, f_r$ be the minimal homogeneous generators of the invariant ring $R = k[V]^G$ with degrees $d_1 \leq \cdots \leq d_r$. We define the graded polynomial ring $S = k[X_1, \ldots, X_r]$ by setting the degree of X_i to be d_i for all i. Then R is an S-module by the ring epimorphism $\pi : S \to R$ given by $\pi(X_i) = f_i$ for all i. Let $0 \to F_k \to \ldots \to F_1 \to F_0 \to R \to 0$ be the minimal graded free resolution of R as an S-module. Note that $F_0 = S$. Since S is Noetherian, $\ker(F_0 \to R)$ is finitely generated, therefore F_1 is a graded free module of finite rank. It follows that all F_i are finitely generated. We define $\beta^i_G(V)$ to be the smallest integer d such that F_i is generated by the elements of degree at most d.

The module $\mathrm{Im}(F_i \to F_{i-1})$ is called the ***i*th syzygies module** of R. The image of F_1 in F_0 is the syzygy ideal J of S defined by $J = \{h \in S \mid h(f_1, \ldots, f_r) = 0\}$. The elements of J are the relations between the generators of R. In general, the ith syzygies module describes the relation between the generators of the $(i-1)$th syzygies module.

A finite group G over a field k is **linearly reductive** if and only if the characteristic of k is coprime to G. If G is linearly reductive, then the ring of invariants $k[V]^G$ is Cohen-Macaulay as an S-module. We shall use this fact without proof.

We first discuss a general degree bound for syzygies. Suppose $S = k[X_1, \ldots, X_r]$ is a graded polynomial ring with degrees $deg(X_i) = d_i$ and $d_1 \geq d_2 \geq \cdots \geq d_r$. Let M be a finitely generated graded Cohen-Macaulay S-module. Recall that the minimal graded free resolution of M is

$$0 \to \mathrm{Tor}_r^S(M,k) \otimes_k S \to \cdots \to \mathrm{Tor}_0^S(M,k) \otimes_k S \to M \to 0.$$

Here $\mathrm{Tor}_i^S(M,k)$ is a finite dimensional graded vector space. We define the **degree** of a finite dimensional graded vector space M to be the maximal degree appearing in M if M is nonzero, and it is $-\infty$ if M is zero. We use $\deg(M)$ to denote the degree of M. For a finitely generated graded module M, we define the a-invariant of M to be the degree of $\mathrm{H}(M,t)$ viewed as a rational function. That is, the degree of the numerator minus the degree of the denominator. We write $a(M)$ for the a-invariant of M.

Theorem 4.1.1 (Harm Derksen)**.** *We have the inequality*

$$\deg(\mathrm{Tor}_i^S(M,k) \leq d_1 + d_2 + \cdots + d_{s+i} + a(M)$$

where s is the Krull dimension of M

Proof. We prove the theorem by induction on $s = \dim(M)$. Suppose $\dim(M) = 0$, then M is a finite dimensional k-vector space. In the case we prove by induction on $\dim_k(M)$. If $\dim_k(M) = 0$, then M is zero and the inequality obviously holds. Suppose M is nonzero. Since M is a finite-dimensional k-vector space, M has only finitely many nonzero homogenous component. Thus the Hilbert series of M is simply a polynomial and $a = a(M)$ is the maximum degree appearing in M. Let M_a be the part of M of degree a. Then M_a is a submodule of M. We have the exact sequence

$$0 \to M_a \to M \to M/M_a \to 0.$$

Since $\dim_k(M/M_a) < \dim(M)$ and $a(M/M_a) < a$, by induction we have

$$\deg(\mathrm{Tor}_i^S(M/M_a,k)) \leq d_1 + \cdots + d_i + a - 1$$

Recall that the Koszul complex $K(X_1,\ldots,X_r)$ is a free resolution of k. The $\mathrm{Tor}_i^S(M_a,k)$ is the ith homology of the complex $M_a \otimes K(X_1,\ldots,X_r)$. The ith term of $K(X_1,\ldots,X_r)$ is generated by elements of the form $x_{j_1} \wedge \cdots \wedge x_{j_i}$ therefore the degree is at most $d_1 + d_2 + \cdots + d_i$ since we assumed $d_1 \geq \cdots \geq d_r$. Since every

element of M_a is of degree a, we have

$$\deg(\mathrm{Tor}_i^S(M_a, k)) \leq d_1 + d_2 + \cdots + d_i + a.$$

From the exact sequence $0 \to M_a \to M \to M/M_a \to 0$ we have the long exact sequence of Tor

$$\cdots \to \mathrm{Tor}_i^S(M_a, k) \to \mathrm{Tor}_i^S(M, k) \to \mathrm{Tor}_i^S(M/M_a, k) \to \cdots.$$

Since $\deg(\mathrm{Tor}_i^S(M/M_a, k)) \leq d_1 + \cdots + d_i + a - 1$, every element of degree larger than $d_1 + \cdots + d_i + a - 1$ must be in the kernel of $\mathrm{Tor}_i^S(M, k) \to \mathrm{Tor}_i^S(M/M_a, k)$ hence is in the image of $\mathrm{Tor}_i^S(M_a, k) \to \mathrm{Tor}_i^S(M, k)$. Thus we have

$$\deg(\mathrm{Tor}_i^S(M, k)) \leq d_1 + d_2 + \cdots + d_i + a.$$

Suppose $s > 0$. Since M is Cohen-Macaulay we can find a homogeneous non-zero-divisor p of degree $e > 0$ and M/pM is again Cohen-Macaulay. Since p is a non-zero-divisor, the dimension of M_i as a k-vector space is invariant under multiplication by p. Therefore $\mathrm{H}(M/pM, t) = (1 - t^e)\,\mathrm{H}(M, t)$, so $a(M/pM) = a(M) + e$. From the short exact sequence

$$0 \to M[-e] \xrightarrow{p} M \to M/pM \to 0$$

we have a long exact sequence of Tor

$$\cdots \to \mathrm{Tor}_{i+1}^S(M/pM, k) \to \mathrm{Tor}_i^S(M, k)[-e] \to \mathrm{Tor}_i^S(M, k) \to \cdots.$$

Any element of $\mathrm{Tor}_i^S(M,k)[-e]$ of maximal degree must map to 0 in $\mathrm{Tor}_i^S(M,k)$, therefore it must come from $\mathrm{Tor}_{i+1}^S(M/pM,k)$. It follows that

$$e + \deg(\mathrm{Tor}_i^S(M,k)) = \deg(\mathrm{Tor}_i^S(M,k)[-e]) \leq \deg(\mathrm{Tor}_{i+1}^S(M/pM,k))$$
$$\leq d_1 + d_2 + \cdots + d_{(s-1)+(i+1)} + a(M/pM) = d_1 + d_2 + \cdots + d_{s+i} + a(M) + e.$$

Thus $\deg(\mathrm{Tor}_i^S(M,k)) \leq d_1 + d_2 + \cdots + d_{s+i} + a(M)$. □

Let us go back to the case where $R = k[V]^G$. The previous theorem implies that $\beta_G^i(V) = \deg(\mathrm{Tor}_i^S(M,k)) \leq d_1 + d_2 + \cdots + d_{s+i} + a(R)$. Knop proved that $a(R) \leq -s$ (see [5], Satz 4) . Therefore the inequality becomes

$$\beta_G^i(V) = \deg(\mathrm{Tor}_i^S(M,k)) \leq d_1 + d_2 + \cdots + d_{s+i} - s.$$

Suppose M is a graded module over the ring $k[V]$ with minimal free resolution

$$0 \to H_l \to H_{l-1} \to \cdots \to H_0 \to M \to 0.$$

The **Castelnuovo-Mumford regularity** $\mathrm{reg}(M)$ is the smallest integer d such that H_i is generated by the elements with degree at most $d + i$ for all i.

Let $I \subset k[V]$ be the ideal generated by every homogenous elements of positive degree in $k[V]^G$. Define $\tau_G(V)$ to be the smallest integer d such that every homogeneous elements in $k[V]$ of degree at least d lies in I. We will use the fact that $\mathrm{reg}(I) = \tau_G(V)$ without proof. If G is linearly reductive over k, Fogarty's proof of the bound of $\beta_G^0(V)$ shows that $\tau_G(V) \leq |G|$ (see Appendix B or [4]).

Proposition 4.1.2. *Suppose $R = \bigoplus_{i=0}^{\infty} R_i$ is a graded ring with $R_0 = k$ and minimally generated by homogeneous elements $f_1, \ldots, f_r$ as a k-algebra. Let $S = k[X_1, \ldots, X_r]$ be the graded polynomial ring and let $\varphi : S \to R$ be the surjective ring homomorphism given by $X_i \mapsto f_i$ for all i. Then we have an exact sequence of graded vector spaces*

$$\mathrm{Tor}_2^S(k,k) \to \mathrm{Tor}_2^R(k,k) \to \mathrm{Tor}_1^S(R,k) \to 0.$$

Proof. From Exercise A3.47 in [3], we have an exact sequence

$$\mathrm{Tor}_2^S(k,k) \to \mathrm{Tor}_2^R(k,k) \to \mathrm{Tor}_1^S(R,k) \to \mathrm{Tor}_1^S(k,k) \to \mathrm{Tor}_1^R(k,k) \to 0$$

Since $\mathrm{Tor}_1^S(k,k)$ and $\mathrm{Tor}_1^R(k,k)$ can be identified with S_+/S_+^2 and R_+/R_+^2 and they are both r-dimensional, the proposition follows. □

Theorem 4.1.3 (Harm Derksen)**.** *Let G be a linearly reductive group over a field k. Suppose $\{f_1, \ldots, f_r\}$ is a minimal set of homogeneous generators of the invariant ring $k[V]^G$ with degrees $d_1 \geq \cdots \geq d_r$ and let $J \subset k[X_1, \ldots, X_r]$ be the syzygy ideal. Then J is generated in degree at most $2\tau_G(V) \leq 2|G|$.*

Proof. Let $T = k[V]$. Consider the T-module U defined by

$$U = \{(w_1, \ldots, w_r) \in T[-d_1] \oplus \cdots \oplus T[-d_r] \mid \sum_{i=1}^{r} w_i f_i = 0\}.$$

Since $I = (f_1, \ldots, f_r)$ has Castelnuovo-Mumford regularity $\tau_G(V)$, it follows that U is generated in degree $\leq \tau_G(V) + 1$. The R-module

$$M = \{(w_1, \ldots, w_r) \in R[-d_1] \oplus \cdots \oplus R[-d_r] \mid \sum_{i=1}^{r} w_i f_i = 0\}$$

gives an exact sequence

$$0 \to M \to R[-d_1] \oplus \cdots \oplus R[-d_r] \to R \to k \to 0.$$

Note that the first three terms of this exact sequence is part of the minimal resolution of k, therefore we may identify M/R_+M with $\mathrm{Tor}_2^R(k,k)$. The module M is equal to U^G. We claim that $(IU)^G = R_+U^G = R_+M$. Suppose $x = (t_1f_1 + \cdots + t_rf_r)(w_1, \ldots, w_r)$ is an element of $(IU)^G$. Then it is invariant under G, therefore

$$\begin{aligned}
|G|x &= \sum_{g\in G} g(x) \\
&= \sum_{g\in G} (g(t_1)f_1, \ldots, g(t_r)f_r)(g(w_1), \ldots, g(w_r)) \\
&= \left(\left(\sum_{g\in G} g(t_1)\right)f_1, \ldots, \left(\sum_{g\in G} g(t_r)\right)f_r\right)\left(\sum_{g\in G} g(w_1), \ldots, \sum_{g\in G} g(w_r)\right).
\end{aligned}$$

Note that $\sum_{g\in G} g(f)$ is invariant under G for any $f \in k[V]$ and $|G|$ is coprime to the characteristic of k. It follows that $x \in R_+M$.

Therefore we have $M/R_+M = U^G/(IU)^G$. Hence we have an inclusion map $M/R_+M \to U/(IU)$. Since U is generated in degree $\leq \tau_G(V) + 1$ and every homogenous polynomial of degree $\geq \tau_G(V)$ is in I, it follows that every homogenous element of U of degree $\geq 2\tau_G(V) + 1$ must lie in IU. This shows that

$$\deg(\mathrm{Tor}_2^R(k,k)) = \deg(M/R_+M) \leq \deg(U/IU) \leq 2\tau_G(V) \leq 2|G|.$$

By the previous proposition, we have $\mathrm{Tor}_2^R(k,k) \to \mathrm{Tor}_1^S(k,k)$ a surjection. Thus

$\deg(\mathrm{Tor}_1^S(k,k)) \leq \deg(\mathrm{Tor}_2^R(k,k)) \leq 2\tau_G(V) \leq 2|G|$. The theorem follows. □

We end this chapter with a conjecture of Harm Derksen.

Conjecture 4.1.4 (Harm Derksen)**.** $\beta_G^i(V) \leq i|G|$.

The proof of $i = 2$ does not seem to extend to this general case.

Chapter 5

Conclusion

In this paper we have developed the theory of commutative algebra and proved the theorem of Harm Derksen. There are some more stuff involving that we have not covered such as the homological tool that we have used.

During the independent study I have gained the knowledge on commutative algebra and invariant theory and have become confident in my research skills. The most valuable skill I gained in the study is constructing knowledge on mathematics from different sources. This experience has deepened my interest in algebra and I am willing to learn more about algebra.

Appendix A

Koszul Complex

We shall assume all rings are Noetherian, all modules are finitely generated.

Let R be a Noetherian ring, N an R-module. The exterior algebra $\wedge N$ is defined to be the free algebra $T(N) = R \oplus N \oplus (N \otimes N) \oplus \cdots$ modulo the relations $x \otimes y = -y \otimes x$ and $x \otimes x = 0$ for all $x, y \in N$. The product of $a, b \in N$ will be written $a \wedge b$. $\wedge N$ is a graded algebra with m-th component is the image of $N \otimes N \ldots \otimes N (m$ factors), written $\wedge^m N$. It is skew-commutative in the sense that for homogenous elements $a, b \in \wedge N$, $a \wedge b = (-1)^{ab} b \wedge a$ where a, b on the power of -1 means the degree of a, b. If $f : N \to M$ is an R-module homomorphism, then $\wedge f : \wedge N \to \wedge M$ is the map of algebra taking $a \wedge b \wedge \cdots$ to $fa \wedge fb \wedge \cdots$.

We shall focus on the case when N is free with rank n, then we have $\wedge^m N \cong R^{\binom{n}{m}}$ with basis $\{x_{i_1} \wedge \cdots \wedge x_{i_m} | 1 \leq i_1 < \cdots < i_m \leq n\}$. In particular, $\wedge^m N = 0$ for $m > n$.

Let $x \in N$ be given, the Koszul complex $K(x)$ is:

$$K(x) : 0 \to R \to N \to \wedge^2 N \to \cdots \to \wedge^i N \xrightarrow{d_x} \wedge^{i+1} N \to \cdots$$

where $d_x : a \mapsto x \wedge a$. If N is a free with rank n and $x = (x_1, \ldots, x_n) \in R^n \cong N$, then we shall write $K(x_1, \ldots, x_n)$ for $K(x)$.

The Koszul complex may be built from parts. First, we introduce two ways of constructing complexes: tensor products and mapping cones. Given two complexes:

$$\mathcal{F} : \cdots \to F_i \xrightarrow{\varphi_i} F_{i+1} \to \cdots$$

and

$$\mathcal{G} : \cdots \to G_i \xrightarrow{\psi_i} G_{i+1} \to \cdots$$

The tensor product of them is

$$\mathcal{F} \otimes \mathcal{G} : \cdots \to \sum_{i+j=k} F_i \otimes G_j \xrightarrow{d_k} \sum_{i+j=k+1} F_i \otimes G_j \to \cdots$$

where the map d_k on $F_i \otimes G_j (i + j = k)$ is $\varphi_i \otimes 1$ to $F_{i+1} \otimes G_j$ and $(-1)^i 1 \otimes \psi_j$ to $F_i \otimes G_{j+1}$, zero map otherwise.

If $\mathcal{G}$ is a complex then $\mathcal{G}[n]$ is the complex where $\mathcal{G}[n]_i = \mathcal{G}_{n+i}$, with differential multiplied by $(-1)^n$. We may treat R as the complex $0 \to R \to 0$ with R in the zeroth position. Then $\mathcal{G}[n] = R[n] \otimes \mathcal{G}$.

Let $y \in R$, We have the commutative diagram

$$\begin{array}{lccccc}
R[-1]: & 0 & \longrightarrow & 0 & \longrightarrow & R & \longrightarrow & 0 \\
 & & & \downarrow & & \downarrow{\scriptstyle 1} & & \\
K(y): & 0 & \longrightarrow & R & \xrightarrow{y} & R & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle 1} & & & & \\
R[0]: & 0 & \longrightarrow & R & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

a short exact sequence of complexes

$$0 \to R[-1] \to K(y) \to R[0] \to 0.$$

If we tensor this diagram with another complex $\mathcal{G}$, then we get a short exact sequence of complexes $0 \to \mathcal{G}[-1] \to K(y) \otimes \mathcal{G} \to \mathcal{G} \to 0$. $K(y) \otimes \mathcal{G}$ is the mapping cone of the map $\mathcal{G}[-1] \to \mathcal{G}$ of complexes given by multiplication by y. We get a long exact sequence

$$\cdots \to H^{i-1}(\mathcal{G}) \xrightarrow{y} H^{i-1}(\mathcal{G}) \to H^i(K(y) \otimes \mathcal{G}) \to H^i(\mathcal{G}) \xrightarrow{y} \cdots.$$

Proposition A.1. *If $N = N' \oplus N''$, then $\wedge N = \wedge N' \otimes \wedge N''$. If $x' \in N'$, $x'' \in N''$, $x = (x', x'') \in N$, then*

$$K(x) = K(x') \otimes K(x'').$$

Proof. If $N = N' \oplus N''$, then the free algebra $T(N) = T(N') \otimes T(N'') \otimes T(N') \otimes \cdots$. This may be seen from the fact that
$(N' \oplus N'') \otimes (N' \oplus N'') = N' \otimes N' \oplus N' \otimes N'' \oplus N'' \otimes N' \oplus N'' \otimes N''$. We first apply the skew-commutativity between $T(N')$ and $T(N'')$, the result is $T(N') \otimes T(N'')$. Then apply the skew-commutativity within $T(N')$ and $T(N'')$, we get
$\wedge N' \otimes \wedge N''$.

It is left to show the differentials in $\wedge N$ and $\wedge N' \otimes \wedge N''$ agree. Let $y = y' \otimes y''$, and $x = (x', x'') = x' \otimes 1 + 1 \otimes x''$. We have

$$\begin{aligned} x \wedge y &= (x' \otimes 1 + 1 \otimes x'') \wedge (y' \otimes y'') \\ &= (x' \wedge y') \otimes y'' + (-1)^{y'} y' \otimes (x'' \wedge y'') \end{aligned}$$

□

If $x = (x', y) \in N = N' \oplus R$, then by the previous proposition we have $K(x) = K(y) \otimes K(x')$. Note that this tensor product is just the mapping cone of $K(x') \xrightarrow{y} K(x')$. By tensoring an R-module M, we get a short exact sequence of complexes

$$0 \to M \otimes K(x')[-1] \to M \otimes K(x) \to M \otimes K(x') \to 0.$$

In particular, we have a long exact sequence:

$$\cdots \to H^i(M \otimes K(x')) \xrightarrow{y} H^i(M \otimes K(x')) \to H^{i+1}(M \otimes K(x)) \to H^{i+1}(M \otimes K(x')) \xrightarrow{y} \cdots$$

Definition A.2. Let R be a ring and let M be an R-module. A sequence of elements $x_1, \ldots, x_n \in R$ is called a regular sequence on M or an M-sequence if $(x_1, \ldots, x_n)M \neq M$ and for $i = 1, \ldots, n$, x_i is a nonzerodivisor on $M/(x_1, \ldots, x_{i-1})M$.

We want to use Koszul complex to study regular sequence on an R-module M. This is done by analyzing the homology of M tensoring with a Koszul complex.

Proposition A.3. *If $y_1, \ldots, y_r \in (x_1, \ldots, x_n) \subset R$, and M is an R-module, then*

$$H^*(M \otimes K(x_1, \ldots, x_n, y_1, .., y_r)) \cong H^*(M \otimes K(x_1, \ldots, x_n)) \otimes \wedge R^r$$

as graded modules. In particular, for each i we have

$$H^i(M \otimes K(x_1, \ldots, x_n, y_1, \ldots, y_r)) \cong \sum_{i=j+k} H^k(M \otimes K(x_1, \ldots, x_n)) \otimes \wedge^j R^r.$$

Thus,

$$H^i(M \otimes K(x_1, \ldots, x_n, y_1, \ldots, y_r)) = 0$$

iff

$$H^k(M \otimes K(x_1, \ldots, x_n)) = 0 \text{ for all } k \text{ with } i - r \leq k \leq i.$$

Proof. Since $y_1, \ldots, y_n \in (x_1, \ldots, x_n)$, we have $y_i = \sum_j a_{ij} x_j$. Let A be the $r \times n$ matrix with entries a_{ij}, then the invertible matrix

$$\begin{bmatrix} I & 0 \\ A & I \end{bmatrix}$$

takes the column vector with entries $x_1, \ldots, x_n, y_1, \ldots, y_r$ to the one with entries $x_1, \ldots, x_n, 0, \ldots, 0$. Then we have

$$K(x_1, \ldots, x_n, y_1, \ldots, y_r) \cong K(x_1, \ldots, x_n, 0, \ldots, 0) \cong K(x_1, \ldots, x_n) \otimes K(0, \ldots, 0).$$

Since $K(0, \ldots, 0)$ has all differentials 0, we have the first statement of the proposition, hence the other two statements. □

Proposition A.4. *If $x_1, \ldots, x_i$ is an M-sequence, then*

$$H^i(M \otimes K(x_1, \ldots, x_n)) = ((x_1, \ldots, x_i)M : (x_1, \ldots, x_n))/(x_1, \ldots, x_i)M.$$

In particular, $H^j(M \otimes K(x_1, \dots, x_n)) = 0$ for $j < i$. If $x_1, \dots, x_i$ is a maximal M-sequence in $I = (x_1, \dots, x_n)$, and $IM \neq M$, then $H^i(M \otimes K(x_1, \dots, x_n)) \neq 0$.

Proof. We prove by induction on i, if $i = 0$ the first statement is trivial. For given i, we do induction on n, starting from $n = i$. If $n = i$, we need to prove $H^n(M \otimes K(x_1, \dots, x_n)) = M/(x_1, \dots, x_n)M$. Consider the right-end of $K(x_1, \dots, x_n)$:

$$\cdots \wedge^{n-1} R^n \to \wedge^n R^n \to \wedge^{n+1} R^n = 0.$$

Let $e_1, \dots, e_n$ be the basis for R^n. We have $e_1 \wedge \cdots \wedge e_n$ the basis of $\wedge^n R^n$ and $e_1 \wedge \cdots \wedge e_{i-1} \wedge e_{i+1} \wedge \cdots \wedge e_n$, $i = 1, \dots, n$ the basis of $\wedge^{n-1} R^n$. We have

$$\left(\sum x_i e_i\right) \wedge e_1 \wedge \cdots \wedge e_{i-1} \wedge e_{i+1} \wedge \cdots \wedge e_n = \pm x_i e_i \wedge \cdots \wedge e_n.$$

Therefore $H^n(k(x_1, \dots, x_n)) = \operatorname{coker}(\wedge^{n-1} R^n \to \wedge^n R^n) = R/(x_1, \dots, x_n)$. Then

$$\begin{aligned} H^n(M \otimes K(x_1, \dots, x_n) &= \operatorname{coker}(M \otimes \wedge^{n-1} R^n \to M \otimes \wedge^n R^n) \\ &= M \otimes \operatorname{coker}(\wedge^{n-1} R^n \to \wedge^n R^n) \\ &= M \otimes H^n(K(x_1, \dots, x_n)) \\ &= M \otimes R/(x_1, \dots, x_n) \\ &= M/(x_1, \dots, x_n)M \end{aligned}$$

Now suppose $n > i$. By induction on i we have,

$$H^{i-1}(M \otimes K(x_1, \dots, x_n)) = ((x_1, \dots, x_{i-1})M : (x_1, \dots, x_n))/(x_1, \dots, x_n)M = 0$$

since x_i is a nonzerodivisor on $M/(x_1, \ldots, x_{i-1})M$. By the long exact sequence after proposition 0.1, we have

$$\begin{aligned} H^i(M \otimes K(x_1, \ldots, x_n)) &= \ker(H^i(M \otimes K(x_1, \ldots, x_{n-1})) \xrightarrow{x_n} H^i(M \otimes K(x_1, \ldots, x_{n-1})) \\ &= \ker(((x_1, \ldots, x_i)M : (x_1, \ldots, x_{n-1})/(x_1, \ldots, x_i)M \xrightarrow{x_n} \\ &((x_1, \ldots, x_i)M : (x_1, \ldots, x_{n-1})/(x_1, \ldots, x_i)M)) \\ &= ((x_1, \ldots, x_i)M : (x_1, \ldots, x_n))/(x_1, \ldots, x_i)M. \end{aligned}$$

The second statement follows from the fact that x_j is a nonzerodivisor on $M/(x_1, \ldots, x_{j-1})M$. For the last statement, if $x_1, \ldots, x_i$ is a maximal M-sequence in I, then I is contained in the set of zero-divisors on $M/(x_1, \ldots, x_i)M$. Hence I is contained in the finite union of associated primes, thus I is in one of them by the prime avoidance. Therefore $I \subset ann(m)$ for some $0 \neq m \in M/(x_1, \ldots, x_i)M$, so

$$m \in ((x_1, \ldots, x_i)M : (x_1, \ldots, x_n))/(x_1, \ldots, x_i)M = H^i(M \otimes K(x_1, \ldots, x_n)). \qquad \square$$

Theorem A.5. *Let M be a finitely generated R-module. If r is the smallest integer such that $H^r(M \otimes K(x_1, \ldots, x_n) \neq 0$, then every maximal M-sequence in $I = (x_1, \ldots, x_n) \subset R$ has length r.*

Proof. Let $y_1, \ldots, y_s$ be a maximal M-sequence in I. If r is the smallest integer such that $H^r(M \otimes K(x_1, \ldots, x_n) \neq 0$, then by proposition A.2., r is also the smallest integer such that $H^r(M \otimes K(x_1, \ldots, x_n, y_1, \ldots, y_s) \neq 0$. Since $H^r(M \otimes K(x_1, \ldots, x_n) \neq 0$, we have $IM \neq M$, which will be proven below. Then by proposition A.3. we deduce $s = r$, as desired. $\square$

The Koszul complex has a dual constructoin. For $\varphi \in Hom(N, R) = N^*$, the dual complex is:

$$K'(\varphi) : \cdots \wedge^i N \xrightarrow{\delta_\varphi} \wedge^{i-1} N \to \cdots \to N \xrightarrow{\varphi} R \to 0$$

where

$$\delta_\varphi(m_1 \wedge \cdots \wedge m_i) = \sum_{j=1}^{i} (-1)^{j-1} \delta_\varphi(m_j) \otimes m_1 \wedge \cdots \wedge \hat{m}_j \wedge \cdots \wedge m_i$$

.

δ_φ is a derivation of $\wedge N$ to itself. That is, if $n, n' \in \wedge N$ are homogenous, then

$$\delta_\varphi(n \wedge n') = \delta_\varphi(n) \wedge n' + (-1)^n n \wedge \delta_\varphi(n')$$

.

Here is one relation between $K(x)$ and $K'(\varphi)$. Let $n \in \wedge^i N$, then

$$\begin{aligned} d_x \delta_\varphi(n) + \delta_\varphi d_x(n) &= x \wedge \delta_\varphi(n) + \delta_\varphi(x \wedge n) \\ &= x \wedge \delta_\varphi(n) + \delta_\varphi(x) \wedge n - x \wedge \delta_\varphi(n) \\ &= \delta_\varphi(x) \wedge n \\ &= \varphi(x) n. \end{aligned}$$

This means we have

$$d_x \delta_\varphi + \delta_\varphi d_x = \varphi(x) \cdot 1,$$

where 1 is the identity map on $\wedge N$. Thus δ_φ is a homotopy on $K(x)$ and d_x is a homotopy on $K'(\varphi)$, showing that multiplication by $\varphi(x)$ is homotopic to 0.

If $y = \sum a_i x_i$, then the map $\varphi : R^n \to R$ with matrix $(a_1, \ldots, a_n)$ takes $(x_1, \ldots, x_n)$ to y. Therefore multiplication by y induces the zero map on homology of $H^j(M \otimes K(x_1, \ldots, x_n))$ for all M and j.

If $(x_1, \ldots, x_n)M = M$, then by Cayley-Hamilton there exists a $y \in (x_1, \ldots, x_n)$ such that $1 - y$ annihilates M, that is, the identity map and multiplication by y induces the same map on M. Thus we have $H^j(M \otimes K(x_1, \ldots, x_n) = 0$ for all j. This finishes the proof of Theorem A.4.

If $IM \neq M$, then by Theorem A.4., the lengths of maximal M-sequences in I are all the same.

Definition A.6. If $IM \neq M$, the depth of I on M, written depth(I, M), is the length of maximal M-sequence in I. If $IM = M$, we define depth$(I, M) = \infty$. We define depth I to be the depth of I on R.

Theorem A.7. *Let (R, m) be a local ring, $M \neq 0$ a f.g. R-module. Suppose $x_1, \ldots, x_n \in m$. If for some $k < n$, $H^k(M \otimes K(x_1, \ldots, x_n)) = 0$, then $H^j(M \otimes K(x_1, \ldots, x_n)) = 0$ for all $j \leq k$. In particular, if $H^{n-1}(M \otimes K(x_1, \ldots, x_n)) = 0$, then $x_1, \ldots, x_n$ is an M-sequence.*

Proof. We prove by induction on n. If $n = 1$, we have

$$M \otimes K(x) : 0 \to M \xrightarrow{x} M \to 0$$

Then $H^1(M \otimes K(x)) = 0$ implies $M = xM$. Thus $M = 0$ by Nakayama's lemma.

If $H^k(M \otimes K(x_1, \ldots, x_n)) = 0$, then by the long exact sequence after Proposition A.1., the map

$$H^{k-1}(M \otimes K(x_1, \ldots, x_{n-1})) \xrightarrow{x_n} H^{k-1}(M \otimes K(x_1, \ldots, x_{n-1}))$$

is an epimorphism. Thus $H^{k-1}(M \otimes K(x_1, \ldots, x_{n-1})) = 0$ by Nakayama's lemma. By induction we have $H^j(M \otimes K(x_1, \ldots, x_{n-1})) = 0$ for $j \leq k-1$. Then by the long exact sequence again we see that $H^j(M \otimes K(x_1, \ldots, x_n)) = 0$ for $j \leq k$, as desired.

For the second statement, we do induction on n again. The case $n = 1$ is trivial. If $H^{n-1}(M \otimes K(x_1, \ldots, x_n)) = 0$, then $H^{n-2}(M \otimes K(x_1, \ldots, x_n)) = 0$. So by induction $x_1, \ldots, x_{n-1}$ is an M-sequence. By Proposition A.3. we have

$$0 = H^{n-1}(M \otimes K(x_1, \ldots, x_n)) = ((x_1, \ldots, x_{n-1})M : (x_1, \ldots, x_n))/(x_1, \ldots, x_{n-1})M.$$

Thus x_n is a nonzerodivisor on $M/(x_1, .., x_{n-1})M$, as desired. □

Corollary A.8. *If R is local and $(x_1, \ldots, x_n) \subset R$ is a proper ideal containing an M-sequence of length n, then $x_1, \ldots, x_n$ is an M-sequence.*

Proof. Nakayama's lemma implies $H^n(M \otimes K(x_1, \ldots, x_n)) = M/(x_1, \ldots, x_n)M \neq 0$. By Theorem 0.4, $\operatorname{depth}((x_1, \ldots, x_n), M)$ is the smallest integer r such that $H^r(M \otimes K(x_1, \ldots, x_n)) \neq 0$. It follows that $\operatorname{depth}((x_1, \ldots, x_n), M) = n$. Thus $x_1, \ldots, x_n$ is an M-sequence by Theorem A.5. □

Corollary A.9. *If $x_1, \ldots, x_r$ is an M-sequence, then $x_1^{t_1}, \ldots, x_r^{t_r}$ is an M-sequence for positive t_i's. It follows that* $\operatorname{depth}(I, M) = \operatorname{depth}(\sqrt{I}, M)$.

Proof. We do induction on r. For $r = 1$, note that a power of a nonzerodivisor is again a nonzerodivisor. For general r, by induction we have $x_1^{t_1}, \ldots, x_{r-1}^{t_{r-1}}$ an M-sequence. It suffices to show that

$$0 \to M/(x_1^{t_1}, \ldots, x_{r-1}^{t_{r-1}})M \xrightarrow{x_r} M/(x_1^{t_1}, \ldots, x_{r-1}^{t_{r-1}})M$$

is exact. We may localize at a prime P, if P does not contain $x_1, \ldots, x_r$, then either $M/(x_1^{t_1}, \ldots, x_{r-1}^{t_{r-1}})M = 0$ or x_r is a unit, then the localized sequence is exact. Thus we may assume (R, P) is local with $x_1, \ldots, x_r \in P$. We have $x_1, \ldots, x_r^{t_r}$ an M-sequence. By the previous corollary, we have $x_r^{t_r}, x_1, \ldots, x_{r-1}$ an M-sequence. Therefore by repeating the argument, we have $x_1^{t_1}, \ldots, x_r^{t_r}$ an M-sequence, as desired. The last statement follows immediately. □

Appendix B

Bound of $\beta_G^0(V)$

In this appendix we give the proof of the Noether's bound for polynomial invariants, which states that the invariant ring is generated in degree of $|G|$. This proof is given by John Fogarty in [4].

Let G be a finite group of order g, V a representation of G over a field k, where the characteristic of k is coprime to g. Let $A = k[V]$ be the graded coordinate ring over V. Let $I \subset k[V]$ be the ideal generated by all homogeneous elements of positive degree in $k[V]^G$.

We first show that $gA_+^g \subset I$. That is, if $f \in A_+^g$, then $gf \in I$. Since g invertible in k, we also have $f \in I$.

Let $\{f_\gamma\}$ be g elements of A_+ indexed by the elements of G. Then

$$\sum_{\sigma \in G} \prod_{\gamma \in G} (f_\gamma - \sigma^{-}1\gamma f_\gamma) = 0,$$

since at least one of the terms in the product is zero. Suppose S is a subset of G,

we define

$$\Psi_S = \sum_{\sigma \in G} \left(\prod_{\gamma \notin S} f_\gamma \right) \left(\sigma^{-1} \prod_{\gamma \in S} (\gamma f_\gamma) \right),$$

then by expending the product of the first equation and collecting terms by subsets of G, we get

$$\sum_{S \subset G} (-1)^{|S|} \Psi_S = 0.$$

If S is nonempty, then Ψ_S is in I. It follows that $\Psi_\emptyset = g \prod_{\gamma \in G} f_\gamma$ is also in I. Thus $g A_+^g \subset I$. Since g is invertible in k, we also have $A_+^g \subset I$. Recall that $\tau_G(V)$ is the smallest integer d such that every homogeneous elements in $k[V]$ of degree at least d lies in I. It follows that $\tau_G(V) \leq |G|$.

Note that $A_+^g \subset I$ implies that I is generated by homogeneous elements $f_1, \ldots, f_r$ of degree $\leq g$. Then there exist homogeneous invariants $u_1, \ldots, u_n$ and homogeneous elements h_{ij} such that

$$f_i = \sum_j h_{ij} u_j, h_{ij} \in k[V], 1 \leq i \leq r.$$

Clearly $u_1, \ldots, u_n$ generate J and have degree $\leq g$. Therefore every element of A_+^G is of the form $g_1 u_1 + \cdots + g_n u_n$, with $g_j \in k[V]$. If $f \in k[V]$, we set

$$\varphi(f) = g^{-1} \sum_{\gamma \in G} \gamma(f).$$

It is the average of f over G. Clearly $\varphi(f)$ is invariant and $\varphi(h) = h$ if h is invarinat. Then averaging $g_1 u_1 + \cdots + g_n u_n$ over G we may replace g_i with $\varphi(g_i)$ which is invariant. It follows that A_+^G is generated by $u_1, \ldots, u_n$ as an ideal in A_G Thus $u_1, \ldots, u_n$ generate A^G as a k-algebra and A^G is generated in degree $\leq |G|$.

Bibliography

[1] D.J. Benson. *Polynomial Invariants of Finite Groups*. Lecture note series: London Mathematical Society. Cambridge University Press, 1993.

[2] Harm Derksen. Degree bounds for syzygies of invariants. *Advances in Mathematics*, 185(2):207 – 214, 2004.

[3] David Eisenbud. Commutative algebra: with a view toward algebraic geometry, 2013.

[4] John Fogarty. On noether's bound for polynomial invariants of a finite group. *Electronic Research Announcements of the American Mathematical Society [electronic only]*, 7:5–7, 2001.

[5] Friedrich Knop. Der kanonische modul eines invariantenrings. *Journal of Algebra*, 127(1):40 – 54, 1989.