1 Noetherian Rings

Definition 1.1. A ring R satisfies the **ascending chain condition (ACC)** when every ascending chain of ideals stabilizes. That is, if $I_1 \subseteq I_2 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals in R indexed by $\mathbb{N}$, then there is some n such that $A_i = A_n$ for all $i > n$. A ring satisfying the ACC is called **Noetherian** after Emmy Noether.

Proposition 1.2. *Let R be a ring. R satisfies the ACC if and only if every ideal is finitely generated.*

The following theorem [CR: 2.18] shows a nice property of polynomial rings. Although the word "basis" is in the title, it is not referring to a basis in the sense of a vector space. It is really about ideals having finite generating sets.

Theorem 1.3 (Hilbert Basis)**.** *If R is a Noetherian ring then so is $R[y]$.*

Corollary 1.4 (CR: 2.19)**.** *$K[x_1, \dots, x_n]$ is a Noetherian ring; every ideal is finitely generated.*

This proposition is a bit of a different framing of [CR: 2.20].

Proposition 1.5. *Let R be a Noetherian ring and let $S \subseteq R$ (think of it as infinite). There exists a finite subset of S that generates $\langle S \rangle$.*

Consequently, for any variety $\mathbb{V}(F)$ (think of F as infinite), there is a finite subset $G \subseteq F$ such that $\mathbb{V}(G) = \mathbb{V}(F)$.

2 Monomial Ideals and their Quotient Rings

It will be handy to have some shorthand notation for monomials and polynomials in $K[x_1, \dots, x_n]$, which I will write as $K[\bar{x}]$. We'll write exponents using greek letters. We abbreviate a monomial $\prod_{i=1}^n x_i^{\alpha_i} = x_1^{\alpha_1} x_2^{\alpha_1} \dots x_n^{\alpha_n}$ as x^α. Here $\alpha \in \mathbb{N}_0^n$. We will usually write elements of $K[\bar{x}]$ as f, g etcetera, rather than $f(x_1, \dots, x_n)$. Using our shorthand for monomials, $f = \sum_{\alpha \in \mathbb{N}_0} f_\alpha x^\alpha$, where each $f_\alpha \in K$ and only a finite number of the f_α are nonzero.

Definition 2.1. A **monomial ideal** is an ideal that is generated by monomials.

Monomial ideals are easy to understand: Notice that x^α divides x^β if and only if $\alpha_i \leq \beta_i$ for all i.

By the Hilbert Basis theorem, any monomial ideal is finitely generated. Moreover, by the proposition [CR: 2.20], if S is a set of monomials (possibly infinite) some finite subset of S generates the same ideal as $\langle S \rangle$.

Proposition 2.2. *Let M be a monomial ideal, generated by $x^{\alpha_1}, \ldots, x^{\alpha_t}$. Then $f \in M$ if and only if each term of f is divisible by one of the generators x^{α_k}.*

Let $\Gamma_M = \left\{x^\beta : \beta_i \geq \alpha_i \text{ for all } i\right\}$. Let $\Delta_M = \mathbb{N}_0 \setminus \Gamma_M$. Then

(1) $f \in I$ if and only if $f = \sum_{\alpha \in \Gamma} f_\alpha x^\alpha$. So $\{x^\alpha : \alpha \in \Gamma\}$ is a basis for M.

(2) $\left\{x^\beta : \beta \in \Delta\right\}$ is a basis for $k[\bar{x}]/M$.

Think of this as it compares to the QR theorem. The QR theorem says:

> Given any $b(x)$ of positive degree δ, and any $f(x) \in K[x]$ there are unique $q(x)$ and $r(x)$ such that $f(x) = b(x)q(x) + r(x)$ and $\deg\big(r(x)\big) < \delta$.

Ignoring the quotient, we can reinterpret that as saying that $f(x)$ is congruent modulo $\langle b(x)\rangle$ to a unique polynomial of degree less than δ. In other words $\left\{1, x, x^2, \ldots, x^{\delta-1}\right\}$ is a basis for $K[x]/\langle b(x)\rangle$.

The previous proposition says that for a monomial ideal M we have an easily identified basis for the quotient ring $k[\bar{x}]/M$. The next section shows how to extend this to an arbitrary ideal.

3 Monomial Orderings and Groebner Bases

It turns out that we can extend our QR theorem to arbitrary ideals, but we need this:

Definition 3.1. A **monomial ordering** $<$ (also called a **term ordering**) is an ordering of $\mathbb{N}_0^n$ such that

(1) $<$ is a total ordering: for any $\alpha, \beta \in \mathbb{N}_0^n$, exactly one of the following is true: $\alpha < \beta$, or $\alpha = \beta$, or $\alpha > \beta$.

(2) $<$ respects addition: $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$.

(3) $<$ is a well ordering: any nonempty subset of $\mathbb{N}_0^n$ has a least element.

Assume that a specific term ordering is chosen. We order monomials in $k[\bar{x}]$ by applying the term ordering to the exponent vector of the monomials. For $f \in k[x_1, \ldots, x_n]$ we will write its terms in descending term order. We use $\mathrm{LT}(f)$ for the leading term, $\mathrm{LM}(f)$ for the leading monomial, $\mathrm{LC}(f)$ for the leading coefficient, and $\mathrm{LE}(f)$ for the leading exponent (the exponent of the leading term). The most common term orderings are lexicographic (lex), graded lexicographic (glex or grlex), and graded reverse lexicographic (grevlex).

Definition 3.2. For $\alpha \in \mathbb{N}_0^n$, let $|\alpha| = \sum_{i=1}^n \alpha_i$. The **lex order** is defined by $\alpha < \beta$ when the last nonzero element of $\beta - \alpha$ is positive. The **glex order** is defined by $\alpha < \beta$ when $|\alpha| < |\beta|$ or $|\alpha| = |\beta|$ and the last nonzero element of $\beta - \alpha$ is positive.

Theorem 3.3 (Robianno). *Every term ordering on $\mathbb{N}_0^n$ is determined by some sequence $u_1, u_2, \ldots, u_s \in \mathbb{R}^n$, in the following sense: $\alpha < \beta$ iff there is some $t \in \{1, 2, \ldots, s\}$ such that $\alpha \cdot u_i = \beta \cdot u_i$ for $i < t$ and $\alpha \cdot u_t < \beta \cdot u_t$.*

That is, the first nonzero entry of the product below is positive.

$$\begin{bmatrix} u_{11} & u_{12} & u_{13} & \cdots & u_{1n} \\ u_{21} & u_{22} & u_{23} & \cdots & u_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ u_{s1} & u_{s2} & u_{s3} & \cdots & u_{sn} \end{bmatrix} \begin{bmatrix} \alpha_1 - \beta_1 \\ \alpha_2 - \beta_2 \\ \alpha_3 - \beta_3 \\ \cdots \\ \alpha_n - \beta_n \end{bmatrix}$$

The theorem shows that there are many monomial orderings. HENCEFORTH, WE ASSUME A TERM ORDERING $<$ IS CHOSEN AND FIXED.

Definition 3.4. For I and ideal in $K[\bar{x}]$ define a monomial ideal (often called its ideal of leading terms) by

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LM}(f) : f \in I \rangle.$$

From the Hilbert Basis theorem, we know that I and $\langle \mathrm{LT}(I) \rangle$ are finitely generated.

Now we have our generalization of the quotient-remainder theorem.

Theorem 3.5. *Let I be an ideal in $k[x]$. Let $\langle \mathrm{LT}(I) \rangle$ be its ideal of leading terms, and let $\langle \mathrm{LT}(I) \rangle = \langle x^{\alpha_1}, \ldots, x^{\alpha_t} \rangle$. There exist polynomials $g_1, g_2, \ldots, g_t \in I$ such that $\mathrm{LM}(g_i) = x^{\alpha_i}$. Furthermore $I = \langle g_1, \ldots, g_t \rangle$.*

Definition 3.6. The set of polynomials $\{g_1, g_2, \ldots, g_t\}$ is called a **Groebner basis** for I. Note: IT DEPENDS ON THE MONOMIAL ORDER $<$. It is called a **minimal Groebner basis** when no $LM(g_i)$ divides another $\mathrm{LM}(g_j)$. It is called a **reduced Groebner basis** when no term of g_i is divisible by some $\mathrm{LM}(g_j)$ for $j \neq i$.

Corollary 3.7. *Let I be an ideal in $k[x]$. Let $\langle x^{\alpha_1}, \ldots, x^{\alpha_t} \rangle$ be its ideal of leading terms (and assume no x^{α_i} divides another x^{α_j} Let $\Gamma_M = \left\{ x^\beta : \beta_i \geq \alpha_i \text{ for all } i \right\}$. Let $\Delta_M = \mathbb{N}_0^n \setminus \Gamma_M$. Then $\left\{ x^\beta : \beta \in \Delta \right\}$ is a basis for $k[\bar{x}]/I$.*

In other words, let $G = \{g_1, \ldots, g_s\}$ be a Groebner basis for I (make it minimal). given any $f \in K[\bar{x}]$ there exist $q_1, q_2, \ldots, q_s$ and r in $K[\bar{x}]$ such that $f = r + \sum_{i=1}^s g_i q_i$ with $r = \sum_{\alpha \in \Delta} a_\alpha x^\alpha$. The quotients q_i are not uniquely determined, but r is.

4 Problems

Problems 4.1. [CR: 2.2.4, 2.2.6] Properties of Noetherian rings.

- **(a)** Show that any Noetherian ring is a factorization domain.
- **(b)** Let R be Noetherian. Prove that a surjective homomorphism $\varphi : R \longrightarrow R$ is also injective, and therefore an isomorphism.

Problems 4.2. Elements of the Hilbert Basis Theorem.

- **(a)** Let $I_1 \subseteq I_2 \subseteq I_3 \cdots$ be an infinite ascending chain of ideals. Show that the union $\bigcup_{n=1}^{\infty} I_n$ is an ideal.
- **(b)** Let I be an ideal in $R[y]$. For $n \in \mathbb{N}_0$ let $J_n = \{r : r \text{ is the LC of a degree } n \text{ polynomial in } I\}$ (1) Show that J_n is an ideal. (2) Show that $J_n \subseteq J_{n+1}$
- **(c)** Let I be an ideal in $K[x, y] = \big(K[x]\big)[y]$. Let J_n be defined as in the previous problem. Show that there are $a_n(x)$ such that $J_n = \langle a_n(x) \rangle$. What can you say about the relationship among the $a_n(x)$?

Problems 4.3. The Descending Chain Condition.

- **(a)** Show that $k[x]$ has a descending chain of ideals that does not stabilize.
- **(b)** Let P be a prime ideal in a ring R. Prove: If I and J are ideals such that $IJ \subseteq P$ then either $I \subseteq P$ or $J \subseteq P$.
- **(c)** An **Artinian ring** is a ring that satisfies the descending chain condition: Any descending chain of ideals stabilizes.
  - (1) Show that (1) Prove that an Artinian ring R has only a finite number of maximal ideals. (Suppose that R has an infinite number of maximal ideals, M_i for $i \in \mathbb{N}$. (Show that $\cap_{i=1}^{n} M_i$ is an infinitely descending chain of ideals. Use (b).)
  - (2) The converse is also true: If R has a finite number of maximal ideals then R is Artinian. The proof uses the Chinese Remainder Theorem.

Problems 4.4. Term Orderings.

Think of $x = x_1$, $y = x_2$ and $z = x_3$ in this problem.

- **(a)** For $n = 3$, find a matrix the corresponds to (lexicographic order) with $x < y < z$.
- **(b)** For $n = 3$, find a matrix the corresponds to glex (graded lexicographic order) with $x < y < z$.
- **(c)** The grevlex order works as follows: first consider the total degree, $|\alpha| = |\beta|$ then $x^\alpha < x^\beta$ provided the first nonzero term of $\alpha - \beta$ is negative. For $n = 3$, find a matrix that corresponds to the grevlex order with $x < y < z$.
- **(d)** For $n = 3$, show order that glex and grevlex are intrinsically different, not just due to permutation of variables. (List the monomials of total degree at most 2 in increasing order for grevlex and for grlex. Illustrate: for each, show a triangle with the monomials of degree 2 and the path of increasing order.)

Problems 4.5. Buchberger's Algorithm.

Let $f = x^2y - 1$ and $g = xy^2 - x$.

- **(a)** Find a Groebner basis for $\langle f, g \rangle$ with respect to the lex order with $y > x$.
- **(b)** Find a Groebner basis for $\langle f, g \rangle$ with respect to the lex order with $x > y$.