Review

- The monomial $\prod_{i=1}^{n} x_i^{\alpha_i}$ is written as x^α where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$.

- A subset $I \subseteq k[x_1, \ldots, x_n]$ is an ideal if:
  - $0 \in I$
  - If $f, g \in I$, then $f + g \in I$
  - If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$

- The ideal generated by $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ is

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \;\middle|\; h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}$$

Problems

- Ideal Description: Does every ideal have a finite generating set?

- Ideal Membership: Given an ideal $I = \langle f_1, \ldots f_s \rangle$ and polynomial f, can we determine if $f \in I$?

- Previously we saw how to solve these problems for $I \subseteq k[x]$.

- The first problem is solved completely by the Hilbert Basis Theorem.

More Problems

- Solving Polynomial Equations: Can we find all points in $\mathbf{V}(f_1, \ldots, f_s)$?

- Implicitization: Given a parametric representation of some $X \subseteq k^n$, can we find an implicit representation? That is, given

$$x_1 = g_1(\mathbf{t}), \ldots, x_n = g_n(\mathbf{t})$$

  where g_i are rational functions in t_j, find $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that $X \subseteq \mathbf{V}(f_1, \ldots, f_s)$.

- If we restrict ourselves to linear functions, both of these problems can be solved using linear algebra.

Ordering Relations

- An *ordering of terms* is used in the partial solutions we have seen so far (the division algorithm for $k[x]$ and row-reduction for linear systems).

- An ordering will be a binary relation "$>$" on $\{ x^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0} \}$ (or equivalently, just $\mathbb{Z}^n_{\geq 0}$).

- Division algorithm ordering: $\cdots > x_1^m > x_1^{m-1} > \cdots > x_1^2 > x_1 > 1$.

- Row-reduction ordering: $x_1 > x_2 > \cdots > x_n$.

Definition (§2.1). *A monomial ordering on* $k[x_1, \ldots, x_n]$ *is any relation* $>$ *on* $\mathbb{Z}^n_{\geq 0}$ *satisfying:*

(i) $>$ *is a total ordering, i.e., for every* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$*,*

$$\alpha > \beta \quad \textit{or} \quad \alpha = \beta \quad \textit{or} \quad \beta > \alpha$$

(ii) If $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$*, then* $\alpha + \gamma > \beta + \gamma$

(iii) $>$ *is a well-ordering, i.e., every nonempty subset of* $\mathbb{Z}^n_{\geq 0}$ *has a smallest element*

Lemma (§2.2). *An order relation* $>$ *on* $\mathbb{Z}^n_{\geq 0}$ *is a well-ordering if and only if every strictly decreasing sequence in* $\mathbb{Z}^n_{\geq 0}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \cdots$$

eventually terminates.

Lexicographic Order

Definition (§2.3). *Let* $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. *We say* $\alpha >_{lex} \beta$ *if in the vector difference* $\alpha - \beta \in \mathbb{Z}^n$, *the leftmost nonzero entry is positive. We will write* $x^\alpha >_{lex} x^\beta$ *if* $\alpha >_{lex} \beta$.

Proposition (§2.4). $>_{lex}$ *on* $\mathbb{Z}^n_{\geq 0}$ *is a monomial ordering.*

- This generalizes the partial orderings we've used.

- Alternative lex orderings may be defined: rearranging the ordering of n variables yields $n!$ different lex orderings.

Ordering Polynomial Terms

Definition (§2.7). *Let* $f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} a_\alpha x^\alpha$ *be a nonzero polynomial in* $k[x_1, \ldots, x_n]$. *With respect to a monomial ordering:*

- *The multidegree of* f *is*

$$\text{multideg}(f) = \max(\alpha \mid a_\alpha \neq 0)$$

- *The leading coefficient of* f *is*

$$\text{LC}(f) = a_{\text{multideg}(f)}$$

- *The leading monomial of* f *is*

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

- *The leading term of* f *is*

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f)$$

Lemma (§2.8). *Let* $f, g \in k[x_1, \ldots, x_n]$ *be nonzero polynomials. Then:*

- $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$

- *If* $f + g \neq 0$*, then*

$$\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g)).$$

  Equality occurs if either

  - $\text{multideg}(f) \neq \text{multideg}(g)$

  - $\text{multideg}(f) = \text{multideg}(g)$ *and* $\text{LC}(f) \neq -\text{LC}(g)$

Division Algorithm in $k[x_1, \ldots, x_n]$

Input: $f_1, \ldots, f_s, f \in k[x_1, \ldots, x_n]$

Output: $a_1, \ldots, a_s, r \in k[x_1, \ldots, x_n]$, where $f = a_1 f_1 + \cdots + a_s f_s + r$ and $r = 0$ or r is a linear combination of monomials, none of which is divisible by any of $\text{LT}(f_1), \ldots, \text{LT}(f_s)$

Initialization: $a_i := 0$ for $i \in \{1, \ldots, s\}$, $r := 0$, $p := f$

WHILE $p \neq 0$ DO

  FOR i FROM 1 TO s DO

    IF $\text{LT}(f_i)$ divides $\text{LT}(p)$ THEN

      $a_i := a_i + \text{LT}(p)/\text{LT}(f_i)$

      $p := p - f_i \text{LT}(p)/\text{LT}(f_i)$

      BREAK

    IF $i = s$ THEN

      $r := r + \text{LT}(p)$

      $p := p - \text{LT}(p)$

Monomial Ideals

Definition (§4.1)**.** *An ideal* $I \subseteq k[x_1, \ldots, x_n]$ *is called a monomial ideal if it can be generated by monomials, i.e.,* $I = \langle x^\alpha \mid \alpha \in A \rangle$ *where* $A \subseteq \mathbb{Z}^n_{\geq 0}$.

Lemma (§4.2)**.** *Let* $I = \langle x^\alpha \mid \alpha \in A \rangle$. *Then a monomial* $x^\beta \in I$ *if and only if there is some* $\alpha \in A$ *such that* x^α *divides* x^β.

Lemma (§4.3). *Let I be a monomial ideal, and let $f \in k[x_1, \ldots, x_n]$. Then the following are equivalent:*

(i) $f \in I$

(ii) Every term of f lies in I

(iii) f is a k-linear combination of the monomials in I

Corollary (§4.4). *Two monomial ideals are the same if and only if they contain the same monomials.*

Dickson's Lemma

Theorem (§4.5). *Let* $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq k[x_1, \ldots, x_n]$. *Then there exist* $\alpha(1), \ldots, \alpha(s) \in A$ *such that* $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$. *In particular,* I *has a finite basis.*

Corollary (§4.6). *Let* $>$ *be a relation on* $\mathbb{Z}^n_{\geq 0}$ *satisfying:*

- $>$ *is a total ordering on* $\mathbb{Z}^n_{\geq 0}$
- *If* $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$, *then* $\alpha + \gamma > \beta + \gamma$

Then $>$ *is a well-ordering if and only if* $\alpha \geq 0$ *for all* $\alpha \in \mathbb{Z}^n_{\geq 0}$.

- This gives a much easier way of verifying if an ordering is a monomial ordering.

Ideal of Leading Terms

Definition (§5.1). *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$.*

- *Define $\mathsf{LT}(I)$ to be the set of leading terms of the elements of I:*

$$\mathsf{LT}(I) = \{\, cx^\alpha \mid \textit{there exist } f \in I \textit{ with } \mathsf{LT}(f) = cx^\alpha \,\}$$

- *The ideal of leading terms is $\langle \mathsf{LT}(I) \rangle$: the ideal generated by the elements of $\mathsf{LT}(I)$*

Proposition (§5.3). *Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal.*

- *$\langle \mathsf{LT}(I) \rangle$ is a monomial ideal*

- *There are $g_1, \ldots, g_t \in I$ such that $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_t) \rangle$*

Hilbert Basis Theorem

Theorem (§5.4). *Every ideal* $I \subseteq k[x_1, \ldots, x_n]$ *has a finite generating set. That is,* $I = \langle g_1, \ldots, g_t \rangle$ *for some* $g_1, \ldots, g_t \in I$.

Groebner Bases

Definition (§5.5). *Fix a monomial order. A finite subset* $G = \{g_1, \ldots, g_t\}$ *of an ideal* I *is said to be a Groebner basis (or standard basis) if*

$$\langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_t) \rangle = \langle \mathsf{LT}(I) \rangle.$$

Corollary (§5.6). *Fix a monomial order. Then every ideal* $I \subseteq k[x_1, \ldots, x_n]$ *other than* $\{0\}$ *has a Groebner basis. Furthermore, any Groebner basis for an ideal* I *is a basis of* I*.*