11.04.2018 – SESSION 1

Introduction:

The goal of this session is to define the objects and language we will use to talk about symbolic computations with polynomials in order to solve systems of equations.

- Further treatment of these topics is given in Cox, Little, O'shea, "Ideals, varieties and algorithms.

§ 1. Polynomial Ideals

- A monomial in a collection of variables $x_1, x_2, \dots, x_n$ is a product

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \quad \text{where } \alpha_i \in \mathbb{Z}_{\geq 0}, \ 1 \leq i \leq n$$

short hand notation: x^α, $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$

- The total degree of x^α is $\alpha_1 + \alpha_2 + \cdots + \alpha_n$

$$|\alpha| = \alpha_1 + \cdots + \alpha_n$$

↳ notation for total degree.

11.04.2018

Example:

If $\alpha = (2,1,1)$ then $X^\alpha = X_1^2 X_2 X_3$

$|\alpha| = 2+1+1 = 4$

→ The total degree of X^α is four.

- A term is a monomial times an element of a field $\mathbb{K}$, $a \cdot X^\alpha$, $a \in \mathbb{K}$.

e.g. $2 \cdot X^\alpha = 2 \cdot X_1^2 X_2 X_3$

term: $2 \cdot X^\alpha$; scalar: 2; monomial: $X_1^2 X_2 X_3$

- A polynomial in $X_1, \dots, X_n$ with coeff in $\mathbb{K}$ is a finite linear combination of monomials of the form

$$f = \sum C_\alpha X^\alpha, \text{ where } C_\alpha \in \mathbb{K}.$$

Ex: $\mathbb{K} = \mathbb{Q}$, $f = 2 \cdot XYZ + y^2 + 5 \cdot Z^{10}$

- Throughout we will usually have $\mathbb{K} = \mathbb{Q}, \mathbb{C}, \mathbb{R}$.
- $\mathbb{K}[X_1, \dots, X_n]$ is the collection of all polynomials in the variables $X_1, \dots, X_n$ with coeffic. in $\mathbb{K}$.

11.04.2018

- Let $f_1, \dots, f_s \in \mathbb{K}[X_1, \dots, X_n]$

$$\langle f_1, \dots, f_s \rangle := \{ p_1 f_1 + \cdots + p_s f_s : p_i \in \mathbb{K}[X_1, \dots, X_n] \text{ for } i \in \{1, \dots, s\} \}$$

Def: Let $I \subseteq \mathbb{K}[X_1, \dots, X_n]$ be a nonempty subset. I is said to be an ideal if

(i) $f + g \in I$ whenever $f, g \in I$

(ii) $p \cdot f \in I$ for $f \in I$ and $p \in \mathbb{K}[X_1, \dots, X_n]$ arbitrary.

Fact: $\langle f_1, \dots, f_s \rangle$ is an ideal for any $f_i \in \mathbb{K}[X_1, \dots, X_n]$.

- One of the most important facts about ideals in $\mathbb{K}[X_1, \dots, X_n]$ is

Hilbert's Basis Thm: Every ideal in $\mathbb{K}[X_1, \dots, X_n]$ has a finite generating set.

i.e. Given an ideal I, there exists a finite collection of polynomials $\{f_1, \dots, f_s\} \subset \mathbb{K}[X_1, \dots, X_n]$ such that

$$I = \langle f_1, \dots, f_s \rangle.$$

- An element $p \in \mathbb{K}[X_1, \dots, X_n]$ is in the ideal $\langle f_1, \dots, f_s \rangle$ if we can find polynomials $p_1, \dots, p_s$ such that $p = p_1 f_1 + \cdots + p_s f_s$

§2. Monomial Orders & Polynomial Division

11.04.2018

Q: What should we do to determine if a given polynomial is in an ideal I?

→ (partial answer) revisit the division algorithm.

- **In $\mathbb{Z}$:** Given two positive integers m, n, we can always write

$$m = q \cdot n + r \quad \text{where} \quad 0 \leq r < n$$

e.g. $15 = 3 \cdot 4 + 2$, with 2 ↳ remainder

- **in $\mathbb{K}[x]$:** Given two polynomials of positive degree f, g, we can always write

$$f = q \cdot g + r \quad \text{where} \quad \deg(r) < \deg(g)$$

e.g. $f = x^2 + x + 1 \quad g = x + 1$

$$\underbrace{x^2 + x + 1}_{f} = \underbrace{x(x+1)}_{g} + \underbrace{1}_{\text{remainder}}$$

$\deg(1) < \deg(g)$, i.e. $0 < 1$

- We want a similar notion for polynomials in several variables. To do so we need to introduce an ordering on the set of monomials.

11.04.2018

Def: A monomial order on $\mathbb{K}[X_1, \ldots, X_n]$ is any relation $>$ on the set of monomials X^α in $\mathbb{K}[X_1, \ldots, X_n]$ that satisfies

(a) $>$ is a total ordering. → Meaning any two elements are comparable.

(b) $>$ is compatible with multiplication in $\mathbb{K}[X_1, \ldots, X_n]$ if $X^\alpha > X^\beta$ and X^γ is any monomial then

$$X^\alpha \cdot X^\gamma > X^\beta \cdot X^\gamma$$

(c) $>$ is a well ordering, i.e every nonempty collection of monomials has a smallest element under $>$.

Ex: In $\mathbb{K}[x]$ we order elements by degree

$$\ldots > X^{n+1} > X^n > \ldots > X^2 > X > 1.$$

- There are many different flavors of monomial orders that can be defined in $\mathbb{K}[X_1, \ldots, X_n]$.

11.04.2018.

Def: Let X^α, X^β be monomials in $\mathbb{K}[X_1, \dots, X_n]$.

LEX: Lexicographic order

We say $X^\alpha >_{LEX} X^\beta$ if in the difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive.

Ex: $X^3 >_{LEX} X^2Y >_{LEX} X^2Z$

$>_{LEX} XY^2 > XYZ$.

GLEX: Graded lexicogr. order

We say $X^\alpha >_{GRLEX} X^\beta$ if

- $|\alpha| > |\beta|$ or
- if $|\alpha| = |\beta|$ and $X^\alpha >_{LEX} X^\beta$

Ex: Same as with LEX but order by total degree first.

GRLEX: Graded reverse lexicographic order.

We say $X^\alpha >_{GRLEX} X^\beta$ if

- $|\alpha| > |\beta|$ or
- if $|\alpha| = |\beta|$ and in $\alpha - \beta \in \mathbb{Z}^n$, the rightmost nonzero entry is negative.

Ex: $X^3, X^2Y, XY^2, X^2Z, XYZ$.

11.04.2018

- Fix a monomial order $>$ in $\mathbb{K}[X_1, \ldots, X_n]$. For $f \in \mathbb{K}[X_1, \ldots, X_n]$

$$f = \sum_{\alpha} c_\alpha X^\alpha$$

Leading term of f = term that contains the largest monomial in f w.r.t $>$

$$LT_>(f) = c X^\alpha$$

c ↓ leading coeff.

X^α ↳ leading monomial

Ex: $f = 3x^2y^2 + x^2yz^3$, $x > y > z$

$$LT_{LEX} = 3x^2y^2$$

$$LT_{GRLEX} = x^2yz^3$$

11.04.2018

Division Algorithm in $\mathbb{K}[X_1, \ldots, X_n]$

Fix any monomial order $>$ in $\mathbb{K}[X_1, \ldots, X_n]$ and let $F = (f_1, \ldots, f_s)$ be an ordered tuple of polynomials in $\mathbb{K}[X_1, \ldots, X_n]$. Then every $f \in \mathbb{K}[X_1, \ldots, X_n]$ can be written as

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

where $a_i, r \in \mathbb{K}[X_1, \ldots, X_n]$,

- for each i either $a_i f_i = 0$ or $LT_>(f) \geq LT_>(a_i f_i)$, and
- either $r = 0$, or r is a linear combin. of monomials, none of which is divisible by any of $LT_>(f_1), \ldots, LT_>(f_s)$

→ We will call r a remainder of f on division by F.

Example: $f = x^3y^2 + 2xy^4$ $\quad x > y$

$F = (\underbrace{x^2y^2 - x}_{f_1}, \underbrace{xy^3 + y}_{f_2})$ we use LEX

$$f = xf_1 + 2yf_2 + \overbrace{x^2 - 2y^2}^{\text{remainder}}$$