

REAL ALGEBRAIC GEOMETRY

KENNETH R. DRIESSEL

BORDER BASES

References: In this section I mainly follow Kehrein, Kreuzer and Rubbiano (2005). Here are several more standard references for the topic of border bases: Mourrain(1999) and Stetter(2004).

Notation: Throughout this section, we use the following notation: K denotes a field, $R := K[X_1, \dots, X_n]$ denotes the algebra of polynomials in the variables X_1, \dots, X_n with coefficients from K , I denotes an ideal in R and $A := R/I$ denotes the quotient algebra determined by I . We assume throughout that the dimension of A is finite. We use the standard multi-index notation: if α is in $\mathbb{N}^{\times n}$ is an n -tuple of natural numbers then $X^\alpha := X_1^{\alpha_1} \dots X_n^{\alpha_n}$ denotes the corresponding monomial determined by α . We use $T := T^n := \{X^\alpha : \alpha \in \mathbb{N}^{\times n}\}$ to denote the set of all monomials in the variables X_1, \dots, X_n . (Note that T is the first letter of the word "Terms".)

We consider the following problem:

Problem: Let $G := (g_1, \dots, g_\nu)$ be a finite list of polynomials in the polynomial algebra R and let I be the ideal generated by G in R . Find a basis for the algebra $A := R/I$ (which we assume to be finite dimensional).

Recall that T denotes the set of monomials in the algebra R . Note that 1 is in T since $1 = X_i^0$. Also note that T is closed under multiplication. We can regard T as a monoid.

Definition: Let \mathcal{O} be a subset of T . Then this set of monomials is an **order ideal** if it satisfies the following conditions:

- It is nonempty.
- It is finite.
- It is closed under divisors.

We can write the last condition formally as follows:

$$(\forall t, u \in T)(u \in \mathcal{O} \wedge t|u \implies t \in \mathcal{O}).$$

Note that 1 is an element of any order ideal.

Definition: For any subset S of T we use S^+ to denote the following subset of R :

$$S^+ := S \cup X_1 S \cup \dots \cup X_n S.$$

And we use ∂S to denote the following subset of T :

$$\partial S := \{t \in S^+ : t \notin S\}.$$

The set ∂S is called the **border** of S . For natural number k we define the **k th border** $\partial^k S$ of S by induction as follows:

- $\partial^0 S := S$,
- $\partial^1 S := \partial S$,
- $\partial^{k+1} := \partial(\partial^k S)$.

Example: Here is an example of an order ideal and some of its borders. Let $R := K[X, Y]$ and let $\mathcal{O} = \partial^0 \mathcal{O} := \{1, X, X^2, X^3, X^4, Y, XY, X^2Y\}$. Then $\partial \mathcal{O} = \{Y^3, XY^2, X^2Y, X^3Y, X^4Y, X^5\}$. Here is a picture showing \mathcal{O} , $\partial \mathcal{O}$ and $\partial^2 \mathcal{O}$:

$$\begin{array}{ccccccc} & & 2 & 2 & 2 & & \\ & & 1 & 1 & 1 & 2 & 2 \\ & & 0 & 0 & 0 & 1 & 1 & 2 \\ & & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{array}$$

Proposition 1. Basic properties of borders. *Let \mathcal{O} be an order ideal. Then*

- *For every natural number k , the following union is a disjoint one:*

$$\bigcup_{i=0}^k \partial^i \mathcal{O}.$$

- *The following union is a disjoint one:*

$$T = \bigcup_{i=0}^{\infty} \partial^i \mathcal{O}.$$

- *For every monomial t in T , t is divisible by monomial in $\partial \mathcal{O}$ iff t is in the set $\{t \in T : t \notin \mathcal{O}\}$.*

Proof. I leave the easy induction proof as an exercise for the reader. □

Definition: Let \mathcal{O} be an order ideal. Let t be a monomial. Then the **index of t with respect to \mathcal{O}** , denoted $\text{ind}_{\mathcal{O}}(t)$, is the unique natural number k such that t is in $\partial^k \mathcal{O}$. Let f be a nonzero polynomial in R . Then the **index of f with respect to \mathcal{O}** , denoted $\text{ind}_{\mathcal{O}}(f)$, is the maximum of the numbers $\text{ind}(t)$ such that t is a monomial in the support of f . In other words, if $f := c_1 t_1 + \cdots + c_s t_s$ where the c_i are non-zero elements of K and the t_i are monomials, then $\text{ind}_{\mathcal{O}}(f) := \max\{\text{ind}_{\mathcal{O}}(t_1), \dots, \text{ind}_{\mathcal{O}}(t_s)\}$. I shall omit the subscript \mathcal{O} when it is clear from context.

Example: Here is another simple example. Again let $R := K[X, Y]$. Now let $\mathcal{O} := \{1\}$. Then $\partial \mathcal{O} = \{X, Y\}$. Here is a picture showing this order ideal

and some of its borders:

$$\begin{array}{cccc} & & & 3 \\ & & & 2 & 3 \\ & & & 1 & 2 & 3 \\ & & & 0 & 1 & 2 & 3 \end{array}$$

Note that here the index of a monomial is the same as its degree.

Definition: Let $\mathcal{O} = \{t_1, \dots, t_\mu\}$ be an order ideal and let $\partial\mathcal{O} = \{b_1, \dots, b_\nu\}$ be its border. Then a set of polynomials $G := \{g_1, \dots, g_\nu\}$ is an **\mathcal{O} -border pre-basis** if, for all $j = 1, \dots, \nu$, $b_j - g_j$ is in the span of \mathcal{O} . With such a pre-basis we have associated production (rewrite) rules:

$$P_j : b_j \mapsto b_j - g_j.$$

We can use these production rules to define a division algorithm. Here is the problem that such an algorithm solves:

Problem: Let \mathcal{O} be an order ideal and let I be an ideal. Given h in R find (“remainder”) r in $\text{Span}(\mathcal{O})$ such that $h - r$ is in I .

Definition: The **Border Division Algorithm** is defined as follows: Let \mathcal{O} be an order ideal with border $\partial\mathcal{O} = \{b_1, \dots, b_\nu\}$ and let $G := (g_1, \dots, g_\nu)$ be an \mathcal{O} -order pre-basis. Let I be the ideal generated by G . Let h be an element of R .

- Step 1: (This is the case when h has index 0.) If h is an element of \mathcal{O} then set $r := h$ and stop. Else go to step 2.
- Step 2: (This is the case when the index of h is greater than 0.) Select a monomial t in the support of h such that the index of t equals the index of h . Let j be the smallest natural number between 1 and ν such that b_j divides t . Apply production rule P_j to t in h to get a new h . Go to Step 1.

Proof. Proof of correctness of the border division algorithm. We want to see that this algorithm terminates. We also want to see that the output r is congruent to h modulo I .

That the algorithm terminates is clear since, in step 2, either the index of the polynomial decreases or the number of terms with with maximum index decreases.

To see that congruence is preserved we only need to note that the production rules preserve congruence. □

Note that the output of the border division algorithm is unique. In particular, note that the output does not depend on the choice of the term with maximum index. (That last assertion requires a short proof which I leave to the reader.) However, the output does depend on the order of the production rules.

Definition: Let h be a polynomial let \mathcal{O} be an order ideal and let G be an \mathcal{O} -order pre-basis. Then the output of the border division algorithm is called

the normal \mathcal{O} -remainder with respect to G . We shall use $NR_{\mathcal{O},G}(h)$ to denote this remainder.

Example: Let $R := K[X, Y]$ and let $\mathcal{O} := \{1, X\}$. Then we have $\partial\mathcal{O} = \{b_1, b_2, b_3\}$ where $b_1 := Y$, $b_2 := XY$ and $b_3 := X^2$. Here is the associated picture:

$$\begin{array}{ccc} 1 & 1 & \\ 0 & 0 & 1 \end{array}$$

We consider the polynomials $g_1 := Y - a$, $g_2 := XY - b$, and $g_3 := X^2 - c$. We have the following associated production rules:

- $P_1 : Y \mapsto a$
- $P_2 : XY \mapsto b$
- $P_3 : X^2 \mapsto c$.

The division algorithm produces the following sequence of polynomials:

$$X^2Y^2 \mapsto aX^2Y \mapsto a^2X^2 \mapsto a^2c.$$

We now consider a different order. In particular, we consider the following order: $b_1 := XY$, $b_2 := Y$, $b_3 := X^2$ and $g_1 := XY - b$, $g_2 := Y - a$, $g_3 := X^2 - c$. The associated production rules are:

- $P_1 : XY \mapsto b$,
- $P_2 : Y \mapsto a$,
- $P_3 : X^2 \mapsto c$.

Now the division algorithm produces the following sequence:

$$X^2Y^2 \mapsto bXY \mapsto b^2.$$

Note that $XY - aX$ and $XY - b$ are in the ideal I generated by the g_i . Hence $aX - b$ is in I and the elements of the order basis \mathcal{O} are not independent in the algebra $A := R/I$.

Proposition 2. *Let \mathcal{O} be an order ideal and let G be a border pre-basis for this order ideal. Then the residue classes of \mathcal{O} span the algebra $A := R/I$ where I is the ideal generated by G .*

Proof. Note that the set of residues of possible remainders $NR_{\mathcal{O},G}(h)$ where h is in R , of the border division algorithm span the algebra A . But all these remainders are in \mathcal{O} . \square

The last example shows that the remainders do not necessarily form a basis of the quotient algebra A .

Definition: Let $\mathcal{O} = \{t_1, \dots, t_\mu\}$ be an order ideal, let I be an ideal in R and let $G = \{g_1, \dots, g_\mu\}$ be a \mathcal{O} -pre-basis of I . Then G is an **\mathcal{O} -border basis** of I if the residue classes $t_i + I$ form a K vector space basis of $A := R/I$.

Proposition 3. *The following conditions are equivalent:*

- *The set of polynomials G is a \mathcal{O} -border basis of I .*
- *The intersection of I and $\text{Span}(\mathcal{O})$ is the zero subspace; in symbols, $I \cap \text{Span}(\mathcal{O}) = 0$.*

- *The polynomial algebra R is the direct sum of I and $\text{Span}(\mathcal{O})$; in symbols, $R = I \oplus \text{Span}(\mathcal{O})$.*