Computational Algebra

2. Leading Terms

Let us fix a term order $\leq$. Then every polynomial $f \in k[x_1, \ldots, x_n]$ can be written in the form

$$f = \sum_{i=1}^{s} c_i t_i \qquad (*)$$

where $c_i \in k$ and $c_i \neq 0 \ \forall i$, and $t_1 \geq t_2 \geq \ldots \geq t_s$.

Definition: for a polynomial $f \in k[x_1, \ldots, x_n]$ written as in $(*)$, we define

a. the leading term of f, denoted $LT_{\leq}(f)$, to be t_1

b. the leading coefficient of f, denoted $LC_{\leq}(f)$, to be c_1

c. the leading monomial of f, denoted $LM_{\leq}(f)$, to be $c_1 \cdot t_1$.

hence we notice that $LM_{\leq}(f) = LC_{\leq}(f) \cdot LT_{\leq}(f)$

We can extend these definitions to ideals of polynomials.

Def: let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal, we define

a. the leading term ideal $LT_{\leq}(I)$ of I as

$$LT_{\leq}(I) = (\{LT_{\leq}(f) : f \in I\}) \subseteq k[x_1, \ldots, x_n]$$

b. the leading term monomodule $LT_{\leq}\{I\}$ of I as

$$LT_{\leq}\{I\} = \langle \{LT_{\leq}(f) : f \in I\} \rangle \subseteq \mathbb{T}^n$$

Remark: notice that, in general, if $I = (f_1, \dots, f_t)$, it is not true that

$$LT_{\leq}(I) = (LT_{\leq}(f_1), \dots, LT_{\leq}(f_t))$$

in fact, consider for example the term order Lex on $\mathbb{T}(x,y)$, and the ideal $I = (x^2-1,\ xy-1)$; then

$$LT_{Lex}(x^2-1) = x^2 \quad \text{and} \quad LT_{Lex}(xy-1) = xy$$

but $\quad y\cdot(x^2-1) - x\cdot(xy-1) = x - y \in I$, as

$$LT_{Lex}(x-y) = x \in LT_{Lex}(I)$$

hence $LT_{Lex}(I)$ cannot be generated by $LT_{Lex}(x^2-1)$ and $LT_{Lex}(xy-1)$

We now first see how understanding the leading terms of the polynomials in an ideal will help with a linear algebra problem, namely: given an ideal $I \subseteq k[x_1, \dots, x_n]$, how can we find a k-basis of the quotient $k[x_1, \dots, x_n]/I$? This was the question that a PhD adiver, Wolfgang Gröbner, posed to his student Bruno Buchberger. The algorithmic solution to this problem is one of the aspects that we are going to analyze during the course. For the moment, we provide a "theoretical" answer given by Macaulay's Basis Theorem, which anyway points us to the "right" direction also the the algorithmic approach.

To prove this result, we will rely on elementary properties of leading terms, which we list hereafter and whose proof is left as an exercise.

Proposition: let $\preccurlyeq$ be a term order on $\mathbb{T}^n$ and let $f_1, f_2 \in k[x_1, \dots, x_n]$

a. $\operatorname{supp}(f_1 + f_2) \subseteq \operatorname{supp}(f_1) \cup \operatorname{supp}(f_2)$ and if moreover $f_1 + f_2 \neq 0$, then

$$LT_{\preccurlyeq}(f_1 + f_2) \leq \max_{\preccurlyeq} \{ LT_{\preccurlyeq}(f_1), LT_{\preccurlyeq}(f_2) \}$$

b. if $f_1 + f_2 \neq 0$ and $LT_{\preccurlyeq}(f_1) \neq LT_{\preccurlyeq}(f_2)$ or $LC_{\preccurlyeq}(f_1) + LC_{\preccurlyeq}(f_2) \neq 0$, then

$$LT_{\preccurlyeq}(f_1 + f_2) = \max_{\preccurlyeq} \{ LT_{\preccurlyeq}(f_1), LT_{\preccurlyeq}(f_2) \}$$

c. for $t \in \mathbb{T}^n$, $LT_{\preccurlyeq}(t \cdot f_1) = LT_{\preccurlyeq}(f_1) \cdot t$

d. if t is the term in $\operatorname{supp}(f_1)$ such that $t \cdot LT_{\preccurlyeq}(f_2)$ is maximal with respect to $\preccurlyeq$, then $LT_{\preccurlyeq}(f_1 \cdot f_2) = t \cdot LT_{\preccurlyeq}(f_2)$

e. $LT_{\preccurlyeq}(f_1 \cdot f_2) = LT_{\preccurlyeq}(f_1) \cdot LT_{\preccurlyeq}(f_2)$.

Theorem: (Macaulay's Basis Theorem)

let $I \subseteq k[x_1, \dots, x_n]$ be an ideal, let $\preccurlyeq$ be a term order; define

$$B := \mathbb{T}^n \setminus LT_{\preccurlyeq}\{I\}$$

(i.e., B is the set of all terms in $\mathbb{T}^n$ that are not multiples of any leading term in I), then the classes of the elements in B form a k-basis of the vector space $k[x_1, \dots, x_n]/I$.

Proof: we prove that $\{[b]_I : b \in B\}$ generate $k[x_1, \dots, x_n]/I$ and are linearly independent; to do so, we transfer the problem on $k[x_1, \dots, x_n]$

a. proving generation is equivalent to proving that

$$\sum_{b \in B} k \cdot b + I = k[x_1, \dots, x_n]$$

let us set $N := \sum_{b \in B} k \cdot b + I$ and suppose for a contradiction that $k[x_1, \dots, x_n] \setminus N$ is not empty; since $\leq$ is a well-order, there exists an element $f \in k[x_1, \dots, x_n] \setminus N$ whose leading term is minimal with respect to $\leq$; there are, therefore, two options:

i. $LT_{\leq}(f) \in B$; then we consider $f - LC_{\leq}(f) \cdot LT_{\leq}(f)$; this cannot belong to N (otherwise f would), but it has leading terms strictly smaller than the one of f, a contraddiction;

ii. $LT_{\leq}(f) \notin B$, then $LT_{\leq}(f) \in LT_{\leq}\{I\}$, so there exists $g \in I$ such that $LT_{\leq}(f) = LT_{\leq}(g)$, then we consider $f - \frac{LC_{\leq}(f)}{LC_{\leq}(g)} \cdot g$, which again has leading term strictly smaller than f, and at the same time cannot belong to N (otherwise f would), a contradiction

b. to prove linear independence we suppose that

$$c_1 t_1 + \dots + c_s t_s = f \quad \text{with} \quad \begin{array}{l} c_1 \dots c_s \in k \setminus \{0\} \\ t_1 \dots t_s \in B \\ f \in I \end{array}$$

then $LT_{\leq}(f) \in LT_{\leq}(I)$, and

$$LT_{\leq}(f) \in supp(f) \subseteq \{t_1, \dots, t_s\} \subseteq B$$

so we get $LT_{\leq}(f) \in LT_{\leq}(I) \cap B$, a contradiction.

How do we determine a set of the form $\mathbb{T}^n \setminus LT_{\leq}\{I\}$? First of all, although we cannot use any set of generators of I to determine $LT_{\leq}\{I\}$, we will see that Dickson's Lemma ensures that a "good" set of generators in this sense always exists. These sets of generators will be the most important players for our course.

Prop: let $I \subseteq k[x_1, \dots, x_n]$ be a monomial ideal, i.e. an ideal generated by terms, and let $\{t_1, \dots, t_s\}$ be a system of generators of I constituted of terms; then for every term $t \in I$, there exists $i \in \{1, \dots, s\}$ such that t is a multiple of t_i. (this holds also for infinite generation)

Proof: by hypothesis, $t = \sum_{i=1}^{s} f_i t_i$ where $f_i \in k[x_1, \dots, x_n]$, hence

$$t \in \mathrm{supp}(f_1 t_1) \cup \dots \cup \mathrm{supp}(f_s t_s)$$

and so the statement follows.

Prop: let $I \subseteq k[x_1, \dots, x_n]$ be an ideal, let $\leq$ be a term order

a. every term $t \in LT_{\leq}(I)$ is of the form $LT_{\leq}(f)$ for some $f \in I$

b. there exist elements $f_1, \dots, f_s \in I$ such that

$$LT_{\leq}(I) = (LT_{\leq}(f_1), \dots, LT_{\leq}(f_s))$$

Proof: a. since $LT_{\leq}(I)$ is a monomial ideal, it is finitely generated by Dickson's Lemma, so we can use the previous result and get that t is of the form $t' \cdot LT_{\leq}(f)$ for some $f \in I$, hence $t = LT_{\leq}(t \cdot f)$.

b. this immediately follows from the previous item together with Dickson's Lemma.

Unfortunately, the previous statement does not tell us how to find such special systems of generators. We now see that the property of generating the leading term ideal is quite desirable, since it implies the generation of the ideal itself.

Prop. let $I \subseteq k[x_1, \dots, x_n]$ be an ideal, and suppose that $f_1, \dots f_s \in I$ are so that $LT_{\leq}(I) = \left(LT_{\leq}(f_1), \dots, LT_{\leq}(f_s) \right)$ for some term order $\leq$; then $I = (f_1, \dots, f_s)$

Proof: suppose for a contradiction, that $(f_1, \dots, f_s) \subsetneq I$; then there exists $f \in I \setminus (f_1, \dots, f_s)$ whose leading term is minimal; then $LT_{\leq}(f) \in LT_{\leq}(I) = \left(LT_{\leq}(f_1), \dots, LT_{\leq}(f_s) \right)$, so $LT_{\leq}(f) = t \cdot LT_{\leq}(f_i)$ then there exists $c \in k \setminus \{0\}$ such that $LT_{\leq}(f - c t f_i) < LT_{\leq}(f)$, but $c \cdot t \cdot f_i \in \overset{(f_1, \dots, f_s)}{\overset{\cap\!|}{I}}$, so if $f - c \cdot t \cdot f_i \in I$ then $f \in \overset{(f_1, \dots, f_s)}{\overset{\cap\!|}{I}}$, a contradiction, but if $f - c f_i \notin (f_1, \dots, f_s)$ then this contradicts the minimality of f.

Systems of generators that generate the leading term ideal are too good not to have a name, so we give them on.

Def: let $\leq$ be a term order, let $I \subseteq k[x_1, \dots x_n]$; a finite set $f_1, \dots f_s \in I$ that generates $LT_{\leq}(I)$ is called a Gröbner basis of I w.r.t. $\leq$.

The previous results show that every ideal admits a Gröbner basis. This implies that every ideal in $k[x_1, \dots, x_n]$ has a finite set of generators (Hilbert's Basis Theorem)