Computational Algebra

1. Term orderings

Although it did not lead to a solution of the problem of computing the intersection of two ideals, we will see that the intuition of using some sort of division between polynomials is one of the key ingredients for the "automatization" of operations on polynomial ideals. Actually, one of the aspects that stepped us was the fact that we were trying to rely on univariate division when working with multivariate polynomials. So, why don't we develop multivariate division?

Going towards an algorithm for division on multivariate polynomials will make us face a series of "requests of clarification", the solution of which will provide us with a robust and reliable tool, the one of Gröbner bases. But, one step at a time.

How do we divide univariate polynomials? Let us do one example:

$$\begin{array}{l|l} 2x^2 + 3x + 2 & x - 1 \\ \cline{2-2} 2x^2 - 2x & 2x + 5 \\ \cline{1-1} 5x + 2 & \\ 5x - 5 & \\ \cline{1-1} 7 & \end{array}$$

Now, notice that, before even starting the division algorithm, we write down the polynomials. This seems quite an obvious step, which does not allow any reasonable choice other than writing the powers of the variable in a polynomial in either ascending or descending order. Here an alarm alert should ring. "Obvious" is one of the most dangerous words in mathematics. To fight this danger, let us analyze why writing polynomials in this way is helpful. There is the general reason that this provides a unique way of presenting a polynomial. This, however, is a property that is common to any rule that can be clearly applied to all univariate polynomials. Writing in, say, ascending order has more. It has the property that if we write a polynomial f in ascending order and we multiply it by a monomial, then applying the distributivity law yields another polynomial which is again in ascending order. For example:

$$\underbrace{(2+3x+2x^2)}_{\text{ascending order}} \cdot \underbrace{x^2}_{\text{monomial}} = \underbrace{2x^2+3x^3+2x^4}_{\text{ascending order}}$$

So, somehow this way of ordering the monomials in a univariate polynomial is <u>compatible</u> with <u>multiplication</u>. We will ask that this property

is stressed when we design the way of ordering monomials in a multivariate polynomial. To start, we need some language.

From now on, k will denote a field: our theory will be a theory of polynomials with coefficients in a field (with no restrictions in terms of the characteristic); there are generalizations of this theory for polynomials with coefficients in more general rings or that are non-commutative, but we will not discuss about them.

Def: a polynomial $f \in k[x_1, \dots, x_n]$ of the form $f = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ with $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ is called a *term* or a *power product*; the set of all terms in $k[x_1, \dots, x_n]$ is denoted $\mathbb{T}^n$ (or $\mathbb{T}(x_1, \dots, x_n)$); given a term $t = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n}$ we define the *degree* of t to be the natural number

$$\deg(t) := \alpha_1 + \dots + \alpha_n$$

the map $\log: \mathbb{T}^n \longrightarrow \mathbb{N}^n$ defined by

$$x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} \longmapsto (\alpha_1, \dots, \alpha_n)$$

is called the *logarithm*

Def: let $f \in k[x_1, \dots, x_n]$ and write $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$, where

$$x^\alpha = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n} \quad \text{if} \quad \alpha = (\alpha_1, \dots, \alpha_n)$$

for every $\alpha \in \mathbb{N}^n$, we say that c_α is the <u>coefficient</u> of x^α; the set $\{x^\alpha : c_\alpha \neq 0\}$ is called the <u>support</u> of f, and it is denoted by $\mathrm{supp}(f)$; if $f \neq 0$, the number

$$\deg(f) := \max\{\deg(x^\alpha) : x^\alpha \in \mathrm{supp}(f)\}$$

is called the <u>degree</u> of f.

<u>Remark</u>: the set $\mathbb{T}^n$ of terms of a polynomial ring, together with multiplication, is a <u>commutative monoid</u> whose neutral element is 1; the logarithm map is a homomorphism of monoids, which is actually an isomorphism

Now we introduce the objects that are going to provide the multivariate analogues to the ascending and descending orderings of terms in a univariate polynomial.

<u>Def</u>: a total order relation $\preccurlyeq$ on $\mathbb{T}^n$ (namely, a relation in which any two terms are comparable, and that is reflexive, antisymmetric, and transitive) is called a <u>term order</u> if:

- for all $t, t_1, t_2 \in \mathbb{T}^n$, $t_1 \succcurlyeq t_2$ implies $t \cdot t_1 \succcurlyeq t \cdot t_2$ (i.e., the relation is compatible with multiplication)
- for all $t \in \mathbb{T}^n$, $1 \preccurlyeq t$.

Let us introduce some term orders that will turn out to be useful.

Def: the lexicographic term order $\succeq_{Lex}$ is defined as follows: we say that $t_1 \succeq_{Lex} t_2$ if and only if $t_1 = t_2$ or, if $t_1 \neq t_2$, the first nonzero component of $\log(t_1) - \log(t_2)$ is positive; in other words, we say that $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \succeq_{Lex} x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}$ if and only if $\alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n$ or, if this is not the case, if $\alpha_1 > \beta_1$ or, if $\alpha_1 = \beta_1$, if $\alpha_2 > \beta_2$ and so on

Example: $x_1^3 x_2 \succeq_{Lex} x_1 x_2^2$ and $x_1 \succeq_{Lex} x_3^7$

Def: the degree-lexicographic term order is defined as follows: we say that $t_1 \succeq_{DegLex} t_2$ if and only if $deg(t_1) > deg(t_2)$ or, if the degrees are equal, if $t_1 \succeq_{Lex} t_2$

Example: $x_1^3 x_2 \succeq_{DegLex} x_1 x_2^3$ and $x_1 \preceq_{DegLex} x_3^7$

Def: the degree-reverse-lexicographic term order is defined as follows: we say that $t_1 \succeq_{DegRevLex} t_2$ if $deg(t_1) > deg(t_2)$ or, if the degrees are equal, if $t_1 = t_2$ or, if $t_1 \neq t_2$, if the last non-zero component of $\log(t_1) - \log(t_2)$ is negative

Example: $x_1^3 x_2^2 x_3 \succeq_{DegRevLex} x_1 x_2^3 x_3^2$

Exercise: prove that Lex, DegLex, and DegRevLex are term orders.

Remark. if in DegRevLex we drop the conditions on the degree, then we do not obtain a term order.

To get acquainted with the notion of term order, we are going to show that they admit a characterization as so-called "well-orderings". To do this, we will first explore the monoid "$\mathbb{T}^n$" and establish a fundamental finiteness result, known as Dickson's Lemma.

Def. a non-empty subset $\Delta \subseteq \mathbb{T}^n$ is called a <u>mono-ideal</u> if

$$\Delta \cdot \mathbb{T}^n \subseteq \Delta$$

a subset $B \subseteq \Delta$ is called a <u>system of generators</u> of Δ if $\Delta = \{ t \cdot s : t \in \mathbb{T}^n, s \in B \}$; a mono-ideal is called <u>finitely-generated</u> if it admits a finite system of generators.

Prop: the following three conditions are equivalent:

a) every mono-ideal in $\mathbb{T}^n$ is finitely generated

b) every ascending chain $\Delta_1 \subseteq \Delta_2 \subseteq \dots$ of mono-ideals is eventually stationary.

c) every non-empty set of mono-ideals in $\mathbb{T}^n$ has a maximal element with respect to inclusion

Proof: a) $\Rightarrow$ b) suppose we have a sequence $\Delta_1 \subseteq \Delta_2 \subseteq \dots$ of mono-ideals that admits a subsequence that is strictly increasing, namely there

exist $n_1 < n_2 < \dots$ such that there exist elements

$$t_i \in \Delta_{n_{i+1}} \setminus \Delta_{n_i}$$

we are going to show that the monoideal Δ generated by the set $\{t_i\}_{i \in \mathbb{N}_{\geq 1}}$ is not finitely generated; in fact, by construction

$$\Delta \subseteq \bigcup_{i \geq 1} \Delta_i$$

but Δ is not contained in any of the Δ_i; however, if Δ were generated by a finite number of terms, then these terms would have to belong to one of the Δ_i, implying $\Delta \subseteq \Delta_i$, a contradiction.

b) $\Rightarrow$ c) let S be a non-empty set of mono-ideals in T'' and let $\Delta_1 \in S$; if Δ_1 is not maximal, then there exists a monoideal Δ_2 in S such that $\Delta_1 \subsetneq \Delta_2$; if S has no maximal element, then we can construct a chain that never becomes stationary, which is a contradiction.

c) $\Rightarrow$ a) let $\Delta \subseteq T''$ be a mono-ideal; consider the set of mono-ideals contained in Δ that are finitely generated. This set is not empty, so it has a maximal element, which must be Δ.

Theorem: T'' satisfies the conditions from the previous proposition; that is why it is called Noetherian.

Proof: we prove the statement by induction on the number of variables; let hence $\Delta \subseteq T''$ be a mono-ideal;

a. if $n = 1$, then Δ is generated by powers of a single variable, $\Delta = \langle \{ x^{i_1}, \dots, x^{i_n}, \dots \} \rangle$; then we take

$$i_0 := \min \{ i_k \mid k \in \mathbb{N} \}$$

and then Δ is generated by x^{i_0}

b. suppose the statement is true for $n-1$; we now show that it is also true for n; consider a chain $\Delta_1 \subseteq \Delta_2 \subseteq \dots$ of mono-ideals in Π^n and suppose that there are indices $n_1 < n_2 < \dots$ such that there exist elements $\omega_i \in \Delta_{n_{i+1}} \setminus \Delta_{n_i}$; let v_1 be a term among the $\{\omega_i\}$ that has minimal power in the variable x_1; suppose that $v_1 = \omega_{m_1}$; now let v_2 be a term in $\{ \omega_{m_1}, \omega_{m_1+1}, \dots \}$ be a term such that the the exponent of x_1 is again minimal, and so on; in this way we have constructed a sequence $v_1, v_2, \dots$ in which the exponents of the variable x_1 are in a non-decreasing; now, for all $i \in \mathbb{N}$ define

$$v_i' := x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} \quad \text{if} \quad v_i = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n}$$

now, the chain of mono-ideals

$$\langle v_1' \rangle \subseteq \langle v_1', v_2' \rangle \subseteq \dots$$

is a chain of mono-ideals in Π^{n-1}, hence it stabilizes by the induction hypothesis; then, since the exponents of x_1 are non-increasing, also $\langle v_1 \rangle \subseteq \langle v_1, v_2 \rangle \subseteq \dots$ stabilizes; however,

we now reached a contradiction, since by construction

$$v_i = w_{m_i} \notin \langle w_1, \dots, w_{m_i - 1} \rangle \supseteq \langle v_1, \dots, v_{i-1} \rangle$$

so the chain should not have stabilized.

The previous result is known as Dickson's Lemma.

Cor: any ideal $I \subseteq k[x_1, \dots, x_n]$ generated by terms is finitely generated.

With this result at hand, we are now ready to discuss well-orderings.

Prop: let $\leq$ be a total order relation on "$\mathbb{T}$" that is compatible with multiplication (i.e., for all $t, t_1, t_2 \in$ "$\mathbb{T}$" we have $t_1 \leq t_2 \Rightarrow tt_1 \leq tt_2$)
then the following conditions are equivalent

a. every non-empty subset of "$\mathbb{T}$" has a minimal element with respect to $\leq$

b. every descending chain $t_1 \geq t_2 \geq \dots$ in "$\mathbb{T}$" is eventually stationary

Proof: a. $\Rightarrow$ b. this follows from considering the set $\{t_i\}$ of a descending chain; by hypothesis this set has a minimal element, which means that the chain must become eventually stationary.

b. $\Rightarrow$ a. if a non-empty subset that is contained in "$\mathbb{T}$" has no minimal element, then we can extract from it a descending sequence that is not eventually stationary.

Def: a total order relation that satisfies the conditions from the previous proposition is called a well-order.

Actually, this is an old friend of ours

Theorem: let $\preceq$ be a total order relation on $\mathbb{T}^n$ that is compatible with multiplication; then the following are equivalent:

a. $\preceq$ is a term order

b. $\preceq$ is a well-order

Proof. a. $\Rightarrow$ b. suppose that there is a chain

$$t_1 \succcurlyeq t_2 \succcurlyeq \dots$$

that is not eventually stationary; by Dickson's lemma, the mono-ideal $\langle t_1, t_2, \dots \rangle$ is finitely generated by some terms $t_1, \dots, t_N$; since $\preceq$ is compatible with multiplication, it follows that for each $j > N$ there exists $k \in \{1, \dots, N\}$ such that $t_j \geq t_k$, which is a contradiction, since $t_j = t \cdot t_k$ for some term $t \in \mathbb{T}^n$.

b. $\Rightarrow$ a. suppose that $\preceq$ were not a term order, namely, that $1 \succ t$ for some term t; then from the compatibility with multiplication together with the fact that in $\mathbb{T}^n$ the cancellation law holds, we get $t \succ t^2$ and so on $t^i \succ t^{i+1}$; in this way we created a descending chain that does not stabilize, which contradicts the fact that $\preceq$ is a well-order.