

Math 370 Computational Algebra - Notes

List of definitions and results

1 Rings

Definition 1.1. A *ring* is a set \mathcal{R} endowed with two binary operations $+$: $\mathcal{R} \times \mathcal{R} \rightarrow \mathcal{R}$, called *sum*, and \cdot : $\mathcal{R} \times \mathcal{R} \rightarrow \mathcal{R}$, called *product*, such that the following properties hold:

1) $(\mathcal{R}, +)$ is an *abelian group*, i.e.

- there exists a "zero" element, which we denote by 0, such that $0 + a = a \forall a \in \mathcal{R}$
- the sum is associative and commutative
- every element has an "opposite" element: $\forall a \in \mathcal{R} \exists b \in \mathcal{R}$ such that $a + b = 0$. We denote this element by $-a$

2) (\mathcal{R}, \cdot) is a *monoid*, i.e.

- the product is associative
- there exist an "identity" element, which we denote by 1, such that $1 \cdot a = a \cdot 1 \forall a \in \mathcal{R}$

3) the distributive law of sum and product holds: $r \cdot (a + b) = r \cdot a + r \cdot b$ and $(a + b) \cdot r = a \cdot r + b \cdot r$

Remark 1.2. Sometimes the existence of 1 is not really required (those taking modern algebra probably do not see this axiom as being part of the definition). We then say that, if 1 exists, \mathcal{R} is a ring with identity. A property that is not part of the definition is the commutativity of the product: we do not necessarily require that $a \cdot b = b \cdot a$ for all $a, b \in \mathcal{R}$. If this holds, we say that the ring is *commutative*. The rings we will see in this class will all be commutative (and with identity!), but keep in mind that, for example, the ring of square matrices is not commutative since in general, given two square matrices A, B , $AB \neq BA$ (see linear algebra).

Some examples of rings are: the ring of integers \mathbb{Z} , the ring of rational numbers \mathbb{Q} , the ring of real numbers \mathbb{R} , and the ring of complex numbers \mathbb{C} . In particular they are all commutative with identity. However, the ring of integers is somehow "defective" in the sense that we cannot perform division properly: if we divide 7 by 3, for example, the result is no longer in \mathbb{Z} . On the contrary, in \mathbb{Q} , \mathbb{R} and \mathbb{C} division is always possible (except for division by zero!) and in particular every element has an inverse. We give a special name to such rings:

Definition 1.3. A commutative ring with identity is called a *field* if, for every nonzero element a , there exists an element b such that $ab = 1$. Such element is usually denoted by a^{-1} .

For fields, we will use the symbol \mathbb{K} . When you see \mathbb{K} in these notes, think of \mathbb{Q} , \mathbb{R} or \mathbb{C} for example. Other fields exist, for example \mathbb{Z}_p with p a prime number, which is an example of finite a field (see abstract algebra??) or the field of square matrices with nonzero determinant (see linear algebra). However, we will just consider the three numerical fields, which we will act as the "coefficients" of our polynomials.

2 Univariate Polynomials

Definition 2.1. The ring of univariate polynomials over a field of coefficients \mathbb{K} is the set

$$\mathbb{K}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid n \in \mathbb{N}, a_i \in \mathbb{K}\}$$

together with the usual sum and product of polynomials.

We actually defined the ring of polynomials as the set of eventually null \mathbb{K} -sequences with pointwise sum and Cauchy product, but that is not strictly necessary for this class, although it should remind you that polynomials are not just "functions" of x , but rather algebraic objects, which we manipulate by taking their sums and products. Also, note that there is no need in the definition to have a *field* \mathbb{K} , but one could simply use any ring \mathcal{R} and define

$$\mathcal{R}[x] = \{\sum_{i=1}^n a_i x^i \mid n \in \mathbb{N}, a_i \in \mathcal{R}\}.$$

In particular, $\mathbb{Z}[x]$ is the ring of polynomials with integer coefficients.

Definition 2.2. Given a nonzero polynomial $f = \sum_{i=1}^n a_i x^i$, with $a_n \neq 0$, we say that x^n is the *leading term* of f , and we denote it by $LT(f)$. Moreover, we say that a_n is its *leading coefficient*, $LC(f)$, and that $a_n x^n$ is its *leading monomial*, $LM(f)$. The degree of f is n and it is denoted by $deg(f)$ or $\delta(f)$. Notice that $f = 0$ has no degree, no leading term, no leading coefficient and no leading monomial.

Definition 2.3. We say that $f \mid g$ (read " f divides g "), if g is a multiple of f , i.e. if there exist another polynomial h such that $g = f \cdot h$. Note that every polynomial divides the zero polynomial, with $h = 0$. Sometimes to avoid this, we say that f *properly divides* g if $h \neq 0$. Note however that h could be a constant, so for example $x - 1$ divides $2x - 2$ (with $h = 2$) and $3x$ divides x (with $h = 1/3$).

Even when a polynomial does not divide another polynomial, it is still possible to "divide" them using the euclidean algorithm (=long division):

Theorem 2.4 (Euclidean Division). *Let f and g be nonzero polynomials. There exist two (unique) polynomials q and r such that $f = qg + r$ and either $r = 0$ or $\delta(r) < \delta(g)$.*

Definition 2.5. Given two nonzero polynomials $f, g \in \mathbb{K}[x]$, their greatest common divisor is the only¹ polynomial $d \in \mathbb{K}[x]$ such that

- d is monic, i.e. $LC(d) = 1$
- $d \mid f$ and $d \mid g$
- if there exist another polynomial $h \in \mathbb{K}[x]$ such that $h \mid f$ and $h \mid g$, then $h \mid d$.

Recursively, we set $GCD(f_1, \dots, f_n) = GCD(f_1, GCD(f_2, \dots, f_n))$.

Remark 2.6. This definition is necessary because for polynomials we do not have a good concept of what is "greater" (see the extra credit problem of HW4). However, should you need to find the GCD of a list of polynomials, just factor them completely and then take the common factors, exactly as you would do for integers. This gives you the GCD in every *factorial* ring, i.e. a commutative ring in which every element can be written "uniquely" (up to their order and up to units) as the product of irreducible elements (a UFD, for those taking Modern Algebra).

¹you had to prove uniqueness for homework!

Algorithm 2.7 (Calculation of GCD using Euclidean division). The following list of instructions will return $GCD(f, g)$ given two nonzero polynomials $f, g \in \mathbb{K}[x]$:

- Divide f by g to obtain $f = qg + r$. If $r = 0$ then the GCD is $\frac{g}{LC(g)}$. Otherwise continue.

- **Repeat**

$f := g$ and $g := r$ and find $f = qg + r$ again with euclidean division

Until $r = 0$

- **Return** the last nonzero remainder. If it is not monic, divide it by its leading coefficient.

Definition 2.8. This definition also extends to multivariate polynomials (see Definition 3.1). Given a set of polynomials f_1, \dots, f_s , the *ideal generated* by f_1, \dots, f_s is the set of polynomials

$$\langle f_1, \dots, f_s \rangle = \{b_1 f_1 + \dots + b_s f_s \mid b_i \in \mathbb{K}[x_1, \dots, x_n]\}.$$

It is basically the set of all possible *polynomial* combinations of some given polynomials f_1, \dots, f_s , which we call generators. It is crucial to note that the b_i are in fact polynomials, not just constant numbers, so the ideal contains also elements of higher degree than just the degree of any of the f_i 's, but sometimes also elements of smaller degree, for example $x - y$ is in the ideal $\langle x^2 - 1, xy + 1 \rangle$. In particular, notice the following special cases:

- $\langle 0 \rangle = \{0\}$ is the *trivial* ideal, consisting of only the zero polynomial. It is the only finite ideal of $\mathbb{K}[x_1, \dots, x_n]$.

- $\langle 1 \rangle = \mathbb{K}[x_1, \dots, x_n]$ it is the *total* ideal, consisting of ALL polynomials. It could be also generated by any other constant polynomial different from zero. Sometimes, people do not consider this to be an ideal.

- $\langle f \rangle = \{\text{multiples of } f\} = \{b \cdot f \mid b \in \mathbb{K}[x_1, \dots, x_n]\}$, the *principal* ideal generated by f . If every ideal of a ring is of this type, then the ring is called a **Principal Ideal Domain**.

Proposition 2.9. Let I be an ideal of $\mathbb{K}[x_1, \dots, x_n]$. Then

a) $0 \in I$

b) $f, g \in I \Rightarrow f - g \in I$ and $f + g \in I$

c) $f \in I \Rightarrow b \cdot f \in I$ for every polynomial b , non necessarily in I

d) either $I = \{0\}$ or I is infinite.

Notice that if we defined the set $\langle f_1, \dots, f_s \rangle$ to only be the set of *linear* combinations of the generators, then c) would not necessarily hold, and in particular the degrees of the polynomials in the set would be bounded by the maximum degree of the generators.

→ The following theorem and corollary are specific to the ring of *univariate polynomials*. An equivalent statement in $\mathbb{K}[x_1, \dots, x_n]$ would not hold true.

Theorem 2.10. Let $I = \langle f_1, \dots, f_s \rangle$ be an ideal of $\mathbb{K}[x]$. Then $I = \langle d \rangle$ where $d = GCD(f_1, \dots, f_s)$. In other words, $\mathbb{K}[x]$ is a *principal ideal domain*.

Corollary 2.11 (Univariate membership test). A univariate polynomial h belongs to the ideal $\langle f_1, \dots, f_s \rangle$ of $\mathbb{K}[x]$ if and only if $GCD(f_1, \dots, f_s)$ divides h .

3 Multivariate Polynomials and Algebraic Varieties

In what follows, the notation $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ is used for multi-indices. The *length* of α is $|\alpha| = \sum_i \alpha_i$.

Definition 3.1. The ring of polynomials in $n > 1$ variables is defined recursively as

$$\mathbb{K}[x_1, \dots, x_n] = \mathbb{K}[x_1, \dots, x_{n-1}][x_n],$$

that is, for example, the ring of polynomials in two variables $\mathbb{K}[x, y]$ can be seen as the ring of univariate polynomials in y with coefficients in the ring $\mathbb{K}[x]$. As a consequence of this definition, every polynomial of $\mathbb{K}[x_1, \dots, x_n]$ can be written as

$$f(x_1, \dots, x_n) = \sum_{\substack{(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n \\ |\alpha| < d}} c_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \quad c_\alpha \in \mathbb{K}.$$

For example, bivariate polynomials can be written as

$$f(x, y) = c_{00} + c_{10}x + c_{01}y + c_{20}x^2 + c_{11}xy + c_{02}y^2 + c_{30}x^3 + \cdots + c_{d_1 d_2} x^{d_1} y^{d_2}.$$

The largest value of $|\alpha|$ such that $c_\alpha \neq 0$ is called the degree of f , and it is indicated as $\delta(f)$. The largest exponent of x_i is called the x_i -degree of f , and it is denoted by $\delta_{x_i}(f)$.

Definition 3.2. Given a polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$, the variety associated to f is the subset of \mathbb{K}^n given by all the zeros of f , i.e.

$$\mathcal{V}(f) = \{(p_1, \dots, p_n) \in \mathbb{K}^n \mid f(p_1, \dots, p_n) = 0\}.$$

It is basically the set of all possible solutions to the equation $f = 0$. If we have a finite set of polynomials, $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$, then we define

$$\mathcal{V}(f_1, \dots, f_s) := \{(p_1, \dots, p_n) \in \mathbb{K}^n \mid f_i(p_1, \dots, p_n) = 0 \forall i \in \{1 \dots s\}\} = \bigcap_{i=1}^s \mathcal{V}(f_i).$$

More in general, given *any* subset S of $\mathbb{K}[x_1, \dots, x_n]$, even infinite, we set

$$\mathcal{V}(S) = \bigcap_{f \in S} \mathcal{V}(f).$$

Remark 3.3. You can see S as a system of polynomial equations and $\mathcal{V}(S)$ as the set of their common solutions. If you take two polynomials from S , say f and g , then you can *add* the polynomial $af + bg$ to S , for *any* choice of $a, b \in \mathbb{K}[x_1, \dots, x_n]$, and this will not change the variety. In fact, the set of solutions to $af + bg = 0$ will still at least contain those solutions to $f = 0 = g$ (this is proposition 3.8), so when you take the intersection, the possible *extra* solutions that $af + bg$ carries will not be part of the variety $\mathcal{V}(S)$ because they are not shared by *all* polynomials of S . This is, in practice, what the following results say about varieties: they do not depend really on the elements of S , but just on the ideal generated by the elements of S .

Theorem 3.4. Let f_1, \dots, f_s be polynomials in $\mathbb{K}[x_1, \dots, x_n]$, and let $I = \langle f_1, \dots, f_n \rangle$ be the ideal they generate. Then $\mathcal{V}(f_1, \dots, f_s) = \mathcal{V}(I)$.

Corollary 3.5. Let f_1, \dots, f_s and g_1, \dots, g_t be two (possibly distinct) sets of polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Suppose that $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$. Then $\mathcal{V}(f_1, \dots, f_s) = \mathcal{V}(g_1, \dots, g_t)$.

Remark 3.6. The previous corollary is crucial when trying to solve a system of polynomial equations (which means finding the variety associated to a finite set of polynomials). Corollary 3.5 says that you can *replace* your system of equations

$$\begin{cases} f_1 = 0 \\ f_2 = 0 \\ \vdots \\ f_s = 0 \end{cases} \quad \text{with a new system} \quad \begin{cases} g_1 = 0 \\ g_2 = 0 \\ \vdots \\ g_t = 0 \end{cases}$$

as long as the two sets of polynomials generate the same ideal. In particular, you can apply this to the case where you want to add an extra equation, $t = s + 1$ and $g_1 = f_1, \dots, g_s = f_s$ and $g_{s+1} = a_1 f_1 + \dots + a_s f_s$. Corollary 3.5 says that if you *add* to your system an equation obtained as a combination of the given ones, the set of solutions to the system will not change because the ideal is unchanged. Notice that the a_i 's are *polynomials*, not necessarily constants. If in particular you choose $a_i \in \mathbb{K}$ (i.e. you choose them to be constant), then you can actually *add* the new equation to your system and *remove* one of the old equations arbitrarily. Why?

Lemma 3.7 (Varieties reverse inclusions). Let I and J be two ideals of $\mathbb{K}[x_1, \dots, x_n]$ such that $I \subseteq J$. Then $\mathcal{V}(I) \supseteq \mathcal{V}(J)$.

Applying this lemma to the case of a principal ideal $I = \langle h \rangle$, we obtain the following proposition, which sometimes we used in class to prove that a polynomial h does not belong to an ideal J . Note that the converse of this proposition does not hold, so it is just a necessary condition for ideal membership.

Proposition 3.8. Let J be an ideal of $\mathbb{K}[x_1, \dots, x_n]$ and let h be a polynomial. If $h \in J$ then $\mathcal{V}(h) \supseteq \mathcal{V}(J)$.

There are some cases in which lemma 3.7 is an "if and only if". In the notes I gave you in class, I used Taylor's formula to prove a result about the ideal of a point. The ideal of a point is the "simplest" ideal such that its variety consists only of the given point.

Definition 3.9. Let $\mathcal{P} = (p_1, \dots, p_n)$ be a point of the space \mathbb{K}^n . The ideal

$$I_{\mathcal{P}} = \langle x_1 - p_1, \dots, x_n - p_n \rangle \subset \mathbb{K}[x_1, \dots, x_n]$$

is called the *ideal of \mathcal{P}* . For example, the ideal of $(3, 4, -2) \in \mathbb{R}^3$ is $\langle x - 3, y - 4, z + 2 \rangle$.

Proposition 3.10. Consider a point $\mathcal{P} = (p_1, \dots, p_n) \in \mathbb{K}^n$ and an ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$. Then

$$\mathcal{P} \in \mathcal{V}(I) \quad \Leftrightarrow \quad I \subseteq I_{\mathcal{P}}.$$

Remark 3.11. It is technically easy to find out if a point is on a variety $\mathcal{V}(I)$: you just have to verify if its coordinates solve all the equations given by the generators of I . The previous proposition gives you an alternative to this method which does not require you to "plug in" values into the equations. What the proposition requires instead, is that you prove that each generator of I is actually contained in $I_{\mathcal{P}}$. This can be a nontrivial task, but we will learn how to attack this problem in general thanks to the introduction of Gröbner bases.

4 Term Orders

There are only two "reasonable" ways of ordering *terms* in $\mathbb{K}[x]$: either by saying that $1 > x > x^2 > x^3 > \dots$ or vice versa, $1 < x < x^2 < x^3 < \dots$ which is probably a bit more natural. These two ways correspond to the only two "reasonable" ways to write a univariate polynomial, either as

$$a_0 + a_1x + a_2x^2 + \dots + a_dx^d, \quad \text{or} \quad a_dx^d + a_{d-1}x^{d-1} + \dots + a_2x^2 + a_1x + a_0.$$

However this second one is preferable because it both matches with the fact that we may want "higher degrees" to come first, and because if you accidentally perform long division writing polynomials in the first manner, you may end up with an infinite loop. Try to divide $x^2 + 2x^4$ by $x - x^2$! But what does "reasonable" mean? And how do we order multivariate terms of the type $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$? Is y^3 "greater" than x^2 because it has higher degree, or is it the other way round because x "comes first"? This section introduces different possible ways to order terms, and to write polynomials accordingly, so that the following basic "natural" property will hold: if x^α divides x^β , then $x^\alpha < x^\beta$.

Definition 4.1. The set of terms of $\mathbb{K}[x_1, \dots, x_n]$ is the set of all possible products of powers of the indeterminates, i.e.

$$\mathbb{T}^n = \{x_1^{\alpha_1} \dots x_n^{\alpha_n} \mid \alpha \in \mathbb{N}^n\}.$$

Note that 0 is not a term, while 1 is a term. *Monomials* are defined as those polynomials containing only one term, so a monomial is an element of the type $m = c_\alpha x^\alpha$ for some $\alpha \in \mathbb{N}^n$ and $c_\alpha \in \mathbb{K}^*$. The *logarithm* is the map $\log : \mathbb{T}^n \rightarrow \mathbb{N}^n$ defined by

$$\log(x_1^{\alpha_1} \dots x_n^{\alpha_n}) = (\alpha_1, \dots, \alpha_n).$$

If you know what a monoid is, then you may notice that this map is an isomorphism of monoids. Note that $\log(1) = (0, \dots, 0)$.

Remark 4.2. Pay attention to notations: what we call a term, your book calls a *power product*, while what we call monomial is actually a *term* according to the book. This might generate some confusion, but unfortunately the literature is not consistent on this terminology. CoCoA uses the one introduced in these notes, i.e. for CoCoA (and for us), x^2y is a term and $3x^2y$ is a monomial.

A *relation* on a set S is a subset \mathcal{R} of $S \times S$, i.e. a set of ordered pairs (a, b) , $a, b \in S$. If $(a, b) \in \mathcal{R}$ we say that a is in relation to b . We want to define *order* relations, i.e. those relations which can be interpreted as "being smaller than" or "greater than". For purely formal reasons, we will just define what it means to be "greater than", i.e. we will give some axioms that a relation has to satisfy in order to be called an *order*. Instead of writing pairs of \mathcal{R} as (a, b) , we will just use the symbol \geq and write $a \geq b$. Moreover, we will just focus on $S = \mathbb{T}^n$, although the first four axioms are completely general (see Discrete Math).

Definition 4.3. A relation \geq (on $S = \mathbb{T}^n$) is an *order* if it is reflexive, antisymmetric and transitive, i.e. if the following three axioms hold:

$$A_1) x^\alpha \geq x^\alpha \quad \forall \alpha \in \mathbb{N}^n$$

$$A_2) \text{ if } x^\alpha \geq x^\beta \text{ and } x^\beta \geq x^\alpha, \text{ then } x^\alpha = x^\beta$$

$$A_3) \text{ if } x^\alpha \geq x^\beta \text{ and } x^\beta \geq x^\gamma, \text{ then } x^\alpha \geq x^\gamma.$$

Obviously, if $x^\alpha \geq x^\beta$ and $\alpha \neq \beta$ then we write $x^\alpha > x^\beta$. Moreover, we say that the order \geq is *total* if

$$A_4) \forall \alpha, \beta \in \mathbb{N}^n, \text{ either } x^\beta > x^\alpha \text{ or } x^\alpha = x^\beta \text{ or } x^\alpha > x^\beta.$$

We want our order relation to behave well with respect to multiplication, and also we would like 1 to be the least possible term, being the only term of degree zero. This is achieved with the following two axioms:

Definition 4.4. An order relation \geq on \mathbb{T}^n is a *term order* if it satisfies the following further axioms:

$$A_5) x^\alpha \geq 1 \quad \forall \alpha \in \mathbb{N}^n$$

$$A_6) x^\alpha \geq x^\beta \text{ implies } x^\alpha \cdot x^\gamma \geq x^\beta \cdot x^\gamma \quad \forall \alpha, \beta, \gamma \in \mathbb{N}^n$$

Remark 4.5. For $n = 1$, you can verify that both $1 < x < x^2 < x^3 < \dots$ and $1 > x > x^2 > x^3 > \dots$ are total orders, but the second one is not a term order because it violates axiom A_5).

Some term orders arise naturally because they have an intuitive meaning, and also because they are useful for computations. The first example of a term order is called *lexicographic*, in short **Lex**. It orders terms as if they were words in a dictionary. The second term order, called *degree lexicographic*, or **DegLex**, prefers terms of higher degree, but within the same degree, it behaves exactly like **Lex**.

Definition 4.6. We say that $x^\alpha >_{\text{Lex}} x^\beta$ if, corresponding to the first value of i such that $\alpha_i \neq \beta_i$, we have $\alpha_i > \beta_i$. This means that we compare the logarithms (=the exponents!) from the left and, in case they are different, we choose the term with the largest exponent. If they are equal, we then compare the exponents of the second variable and so on.

Definition 4.7. We say that $x^\alpha >_{\text{DegLex}} x^\beta$ if either $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and $x^\alpha >_{\text{Lex}} x^\beta$.

The following two orders are very similar to the previous ones, only they compare exponents from the right, and they pick the term with the *least* exponent to be the highest one.

Definition 4.8. We say that $x^\alpha >_{\text{RevLex}} x^\beta$ if, starting from $i = n$ and going backwards, corresponding to the first value of i such that $\alpha_i \neq \beta_i$ we have $\alpha_i < \beta_i$.

Definition 4.9. We say that $x^\alpha >_{\text{DegRevLex}} x^\beta$ if either $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and $x^\alpha >_{\text{RevLex}} x^\beta$.

Example 4.10. You can find out that the following inequalities are true by applying the definition. Assume we are working in $\mathbb{K}[x, y, z]$ and comparing terms of \mathbb{T}^3 .

$$x^4 y^2 z^4 >_{\text{Lex}} x y^{10} z, \quad \text{but} \quad x^4 y^2 z^4 <_{\text{DegLex}} x y^{10} z, \quad x^4 y^2 z^4 <_{\text{RevLex}} x y^{10} z.$$

When it comes to **DegRevLex**, remember that you first compare the degrees, and then you look at the term with the least amount of z 's. In case the exponent of z is the same, you look for the least number of y 's and so on.

$$x^3 y^2 z^4 >_{\text{DegRevLex}} x^2 y^2 z^5, \quad x^{10} z^4 <_{\text{DegRevLex}} x^3 y^{10} z, \quad \text{and} \quad x^3 y^3 z^2 >_{\text{DegRevLex}} x y^5 z^2.$$

Definition 4.11. A total order $>$ on a set S is called a *well order* if every subset of S has a minimum with respect to $>$, i.e. for every $U \subseteq S$, there exists an element $m \in U$ such that $m < s \quad \forall s \in S$.

The set of natural numbers \mathbb{N} , with its usual order, is well-ordered. This may not happen for other ordered sets. For example \mathbb{R} with the usual order of real numbers, is not well ordered: no open interval (a, b) has a minimum, since $a \notin (a, b)$. Fortunately, term orders are well orders. Here are some of the main properties of (term) orders. In particular, *e)* says that, for a multiplicative total order (= all axioms but A_5), being a term order is equivalent to being a well order.

Proposition 4.12. *Suppose we work in $\mathbb{K}[x_1, \dots, x_n]$ and we consider orders on \mathbb{T}^n . The following facts hold true:*

a) *The relations defined so far on \mathbb{T}^n are all total orders. In particular, **Lex**, **DegLex** and **DegRevLex** are all term orders, while **RevLex** is not a term order.*

b) *Let $>$ be any of the orders above. Then $x_1 > x_2 > \dots > x_n$.*

c) *Let $>$ be a term order on \mathbb{T}^n . Then $1 < x_i < x_i^2 < x_i^3 < \dots$ for all $i = 1 \dots n$.*

d) *A term order is also a well-order.*

e) *Suppose that $>$ is a total order which also satisfies axiom A_6). Then it is a well order if and only if it is a term order.*

f) *Let $s, t \in \mathbb{T}^n$ be two terms, and let $>$ be any term order. Then $s|t$ implies $s < t$. [The converse is not true, think of $s = xy$ and $t = x^3$ with respect to **Lex**.]*

Definition 4.13. Given a polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$, if we write it as $\sum_{\alpha} c_{\alpha} x^{\alpha}$, the set of terms x^{α} such that $c_{\alpha} \neq 0$ is called the *support* of f and we denote it by $\text{supp}(f)$. Given $f \in \mathbb{K}[x_1, \dots, x_n]$ and a term order $>$ on \mathbb{T}^n , we set

$$LT_{>}(f) = \max_{>}(\text{supp}(f)).$$

$LT_{>}(f)$ is called the *leading term* of f . The *leading coefficient*, $LC_{>}(f)$ is the coefficient of $LT_{>}(f)$, and the *leading monomial* is $LM_{>}(f) = LC_{>}(f) \cdot LT_{>}(f)$. If S is any subset of $\mathbb{K}[x_1, \dots, x_n]$, we define the *leading term set* of S to be

$$LT_{>}\{S\} = \{LT_{>}(f) \mid f \in S\},$$

and the *leading term ideal* of S as

$$LT_{>}\langle S \rangle = \langle LT_{>}(f) \mid f \in S \rangle = \langle LT_{>}\{S\} \rangle.$$