Hilbert's Nullstellensatz and the beginning of Algebraic Geometry *

Vishwambhar Pati
Indian Statistical Institute,
Bangalore 560 059

1 A Question on polynomials

1.1 Introduction

In this article, we discuss a theorem that could be called the cornerstone of algebraic geometry over fields. In German, "Nullstellensatz" means "Zero-Set Theorem".

The objects of study in algebraic geometry are the loci, or zero sets of polynomials. In school coordinate geometry (in 2 or 3 dimensions), one encounters things like the circle, which is the zero-set of the polynomial $f(X,Y) = X^2 + Y^2 - 1$ in $\mathbf{R}^2$, or the hyperboloid, which is the zero-set of $f(X,Y,Z) = X^2 + Y^2 - Z^2 - 1$ in $\mathbf{R}^3$. These objects are examples of "affine algebraic sets", and were discussed in the article [P-S] in an earlier issue of *Resonance*.

1.2 Affine algebraic sets

So, more formally, let $\{f_i(X_1,..,X_n)\}_{i\in S}$ be some collection of polynomials in n-variables with real coefficients, indexed by some (finite or infinite) set S. The **real affine algebraic set** $V(S)$ is defined as:

$$V(S) := \{(a_1,..,a_n) \in \mathbf{R}^n : f_i(a_1,..,a_n) = 0 \text{ for all } i \in S\}$$

That is, $V(S)$ is the *set of common zeroes* (or *zero locus*) of *all* the polynomials in S. For brevity, it is often just called a **real algebraic set**. Similarly one can define a **complex algebraic set** as the common zero-set in $\mathbf{C}^n$ of some collection S of polynomials in n variables $X_1,..,X_n$ with **complex** coefficients. (If S is a finite set, say $S = \{f_i\}_{i=1}^k$, we customarily write $V(S)$ as $V(f_1,..,f_k)$. It turns out, as will be discussed later, that all algebraic sets, real or complex, can defined by only finitely many polynomials.)

It is clear that if f is a polynomial of the form:

$$f(X_1,..,X_n) = \Sigma_{f_i\in T}\, g_i(X_1,..,X_n) f_i(X_1,..,X_n)$$

where T is any finite subset of S, and g_i *any* polynomials in $X_1,..,X_n$, then f will vanish identically on the algebraic set $V(S)$. Then one can ask the converse question: Suppose one knows that some polynomial $f(X_1,..,X_n)$ identically vanishes on $V(S)$. Can one assert that f is somehow a combination of some f_i's in S ?

A trivial example shows that this is too much to expect. To wit, consider the degree 2 polynomial $F(X) = X^2$, and the algebraic set $V(F) \subset \mathbf{R}$. Clearly $V(F)$ is just the single point 0. The polynomial X clearly vanishes on $V(F)$, but the degree 1 polynomial X can never be $g(X)F(X)$, since $F(X)$ is of degree 2. This same example also works if $\mathbf{R}$ is replaced by $\mathbf{C}$. In other words, this hitch occurs over both $\mathbf{R}$ and $\mathbf{C}$. Note, however, that X^2 is a multiple of (in fact equal to) F, so we may be tempted to make the modified

* *Resonance*, Vol 4, No. 8, Aug. 1999, pp 36-57

Conjecture 1.1 Suppose a polynomial f with real (resp. complex) coefficients, in n-variables, vanishes identically on the algebraic set $V(S) \subset \mathbf{R}^n$, (resp. $\subset \mathbf{C}^n$). Then, we claim that there is a positive integer r such that:

$$f^r = g_1 f_1 + ... g_k f_k$$

where g_i are some polynomials with real (resp. complex) coefficients, and $f_i \in S$.

Let us first examine this conjecture in the real case, by looking at an example:

Take $V(F) \subset \mathbf{R}^2$ where $F(X,Y) = X^2 + Y^2$. Clearly, $V(F)$ is just the single point $(0,0)$, the origin. The polynomial X vanishes identically on $V(F)$. However, the reader can easily check that *no power* X^r of X can ever be a multiple of F.

Suppose we break out of $\mathbf{R}$, and consider this same example over the complex numbers $\mathbf{C}$. Now, $V(F) \subset \mathbf{C}^2$ becomes a large set. In fact $V(F) = \{(a, \pm ia) : a \in \mathbf{C}\}$ (where $i = \sqrt{-1}$) is a pair of (complex) lines in $\mathbf{C}^2$. Now we are in better shape because of the following:

Exercise: Prove that if a polynomial $f(X,Y)$ with complex coefficients vanishes identically on $V(F) \subset \mathbf{C}^2$, where $F(X,Y) = X^2 + Y^2$, then f is divisible by F. In this example, one does not even need to raise f to a power. (Hint: Change to new variables: $Z = X + iY$, $W = X - iY$, and show that any complex polynomial $f(Z,W)$ vanishing identically on both Z and W axes is divisible by ZW).

So, the conjecture above is verified at least for the above example, if we do everything over $\mathbf{C}$. Is it always true over $\mathbf{C}$? What can one say in the real case, if anything? Why are the two situations different? Can one use other fields besides $\mathbf{R}$ and $\mathbf{C}$? What are "fields", anyway?

2 Some Algebra

In this section we'll introduce some algebraic constructs that will help us to get a handle on the problem 1.1. The reader may wish to look at [J], [A-M] or [Z-S] for further details. Fields were recently discussed in the article [Ja] in an earlier issue of *Resonance*. However, the account below is more or less self-contained.

The basic algebraic objects that we immediately need to get familiar with are rings, fields, and finally rings of polynomials with coefficients in a field. In the sequel, one could expend effort and censor out all mention of rings, fields, ideals and the like, and state everything in terms of polynomials, multiplication and division. But it is better to do some propaganda for the axiomatic method by showing you its effectiveness. Note that the conjecture 1.1 is a concrete question about polynomials, and we are introducing some machinery to solve this problem, and not for its own sake!

2.1 Rings and fields

A **ring** is a set A together with two operations, say "+" and "." (called addition and multiplication) which satisfy the following:

(R1) $a + b = b + a$ for all $a, b \in A$ (commutativity of +)

(R2) $a + (b + c) = (a + b) + c$; $a.(b.c) = (a.b).c$ for all $a, b, c \in A$ (associativity of + and .)

(R3) There exists an element 0 satisfying $a + 0 = a$ for all $a \in A$ (existence of additive identity).

(R4) For each $a \in A$, there exists an element $(-a)$ such that $a + (-a) = 0$ (existence of additive inverses).

(R5) $a.(b + c) = a.b + a.c$, and $(b + c).a = b.a + c.a$ for all $a, b, c \in A$ (left and right distributivity).

If in addition, we also have $a.b = b.a$ for all $a, b \in A$, we call it a **commutative ring**. If there exists an element $1 \in A$, with $1 \neq 0$ and satisfying $a.1 = a = 1.a$ for all $a \in A$, we call it a **ring with identity**. A **subring** B of a ring A is a subset of A which is also a ring with the $+$ and . operations from A. If A is a commutative ring with identity such that for each *non-zero* element $a \in A$, there exists an element a^{-1} (called the multiplicative inverse of a) satisfying $a.a^{-1} = 1$, we call A a **field**. So a field is an abelian group with respect to $(+)$, and its non-zero elements form an abelian group with respect to multiplication ".".

Fields are usually denoted by the lowercase letter k, or the bold uppercase $\mathbf{F}$. If a ring A is a vector space[1] over a field k, such that the scalar multiplication from k is compatible with the ring operations (i.e. $\lambda(a+b) = \lambda a + \lambda b$ and $\lambda(a.b) = (\lambda a).b = a.(\lambda b)$ for all $\lambda \in k$ and all $a, b \in A$) then A is called a **k-algebra**. In the particular case when A contains a field k as a subring, A clearly becomes a k-algebra, with vector addition being the ring addition $+$, and scalar multiplication coming from ring multiplication "." by elements of k.

Example 2.1 (Examples of Rings, Fields, Algebras)

(i) The **set of integers $\mathbf{Z}$** is a commutative ring with identity, with its usual addition and multiplication operations. The **rational numbers $\mathbf{Q}$**, **the real numbers $\mathbf{R}$** and **complex numbers $\mathbf{C}$** with their usual operations are fields. Clearly $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ is a chain in which each inclusion is one of a subring in a bigger ring. Thus $\mathbf{R}$ is a $\mathbf{Q}$-algebra (of infinite, in fact uncountable dimension as a $\mathbf{Q}$ vector space), and $\mathbf{C}$ is an $\mathbf{R}$-algebra of vector space dimension 2 (spanned by the basis $\{1, i\}$).

(ii) Let $m \geq 2$ be a natural number. The **set of integers modulo m**, (also called **residue classes mod m**) denoted $\mathbf{Z}_m$, is the set $\{\overline{0}, \overline{1}, .., \overline{m-1}\}$. The sum $\overline{a} + \overline{b}$ is defined as $\overline{r}$ where r is the remainder $(< m)$ upon dividing the integer $a + b$ by m. Multiplication is defined similarly. These are called **addition and multiplication modulo m**, and $\mathbf{Z}_m$ becomes a commutative ring with identity under these operations. The properties R1 through R5 for $\mathbf{Z}_m$ follow from the corresponding properties for $\mathbf{Z}$.

(iii) If $m = p$ a prime, then $\mathbf{Z}_p$ becomes a field (why?), often denoted $\mathbf{F}_p$ to emphasise its "fieldhood".

(iv) The set of **continuous complex valued functions on the closed interval** $[0, 1]$ is a commutative ring with identity under the operations of multiplying and adding continuous functions pointwise, and is denoted $C([0, 1])$. Likewise $C(\mathbf{R})$, the commutative ring of continuous complex valued functions on $\mathbf{R}$. The ring $C(\mathbf{R})$ contains the subring $C_c(\mathbf{R})$ of **continuous functions on R of compact support** (i.e. continuous functions f such that $f(x) = 0$ for $|x| \geq a$, for some a depending on f). Note $C_c(\mathbf{R})$ is a ring *without* identity, (the constant function 1 is not of compact support!). In fact $C(\mathbf{R})$, since it contains the constant functions, is a $\mathbf{C}$-algebra. $C_c(\mathbf{R})$ is also $\mathbf{C}$-algebra (because multiplying a continuous compactly supported function with $\lambda \in \mathbf{C}$ gives a continuous compactly supported function) even though it does not contain $\mathbf{C}$ as a subalgebra! Another interesting way of making $C_c(\mathbf{R})$ a ring is to retain the old addition, but make multiplication the convolution product $f * g$ defined by:

$$(f * g)(x) = \int_{-\infty}^{\infty} f(x-y)g(y)dy$$

With this new ring structure, $C_c(\mathbf{R})$ becomes a commutative ring *without* identity!

[1] Take the definition of an $\mathbf{R}$-vector space, replace $\mathbf{R}$ by k everywhere, and you have the definition of a k-vector space.

(v) The set of $n \times n$ **matrices with entries in a commutative ring** A with identity, is a ring with identity under matrix addition and multiplication. It is denoted by $M(n, A)$, and is not a commutative ring (therefore not a field) if $n \geq 2$. More generally, for those who are aware of Hilbert spaces, the set of all **bounded operators** $B(\mathcal{H})$ **on a Hilbert space** $\mathcal{H}$ is a ring with identity.

(vi) The set of polynomials in n-variables with coefficients in a field k is denoted $k[X_1, .., X_n]$, and is a commutative ring with identity (with the operations of addition and multiplication of polynomials). It contains k as the subring of degree 0 polynomials, and is therefore a k-algebra. It is called the **polynomial ring** or **polynomial algebra** over k in n-variables. (Polynomials were discussed in the article [Si] in an earlier issue of Resonance).

(vii) An important object is the **field of rational functions** $k(X_1, .., X_n)$ **in** n**-variables**. It is defined as the set:

$$\left\{ \frac{P(X_1, .., X_n)}{Q(X_1, ..., X_n)} : P, Q \in k[X_1, ..., X_n],\ Q \neq 0,\ \text{gcd} \right\}$$

(where common factors in P, Q can be cancelled without changing $\frac{P}{Q}$.) **Caution:** When we say that a polynomial:

$$f(X_1, .., X_n) = \sum_{i_1 + .. i_n \leq d} a_{i_1 i_2 .. i_n} X_1^{i_1} .. X_n^{i_n}$$

in $k[X_1, .., X_n]$ is non-zero (denoted $f \neq 0$), we mean that some coefficient $a_{i_1 i_2 .. i_n}$ of that polynomial is non-zero! Its values at *all points* of k^n may be zero. For example, the 1-variable polynomial $f(X) = X^2 + X \in \mathbf{F}_2[X]$ gives zero when evaluated at the two points $\{\overline{0}, \overline{1}\}$ of $\mathbf{F}_2$, but f is not the zero polynomial. This, of course, doesn't happen in $\mathbf{R}[X_1, .., X_n]$ or $\mathbf{C}[X_1, .., X_n]$ (Why not?).

The addition and multiplication in $k(X_1, .., X_n)$ are defined analogously to what we do for rational numbers, i.e. using a common denominator etc. Note that $k(X_1, .., X_n)$ is a field, because the inverse of a non-zero element P/Q is Q/P. Also $k(X_1, .., X_n)$ clearly contains $k[X_1, .., X_n]$ as a subring, and so k is a subfield of this field, and so it is a k-algebra in a natural way. Those who have done some complex analysis will recognise the 1-variable case $\mathbf{C}(X)$ as the ring of meromorphic functions on the complex plane having at worst a pole at ∞.

2.2 Ideals

From this point on, all rings we consider will be assumed to be commutative, unless otherwise stated. For the sake of convenience we will write ab instead of $a.b$ for the product of the elements a and b in a ring. An **ideal** I of a ring A is a subset of A such that:

(I1) $a + b \in I$ for all $a, b \in I$.

(I2) $ax \in I$ for all $a \in A,\ x \in I$.

Clearly, if I contains the identity element 1, the property (I2) of an ideal would force I to be all of A. *Thus the interesting ideals do not contain* 1. An ideal I in a ring A which is not equal to A is called a **proper ideal**. Again, from (I2), proper ideals *do not contain any invertible element.*

Lemma 2.2 The only proper ideal in a field k is the zero ideal $\{0\}$. Conversely, if a commutative ring A with 1 contains no proper ideals except $\{0\}$, then it is a field.

Proof: If an ideal I in a field k contains a non-zero element a, then $a^{-1}a = 1$ is forced to lie in the ideal I. Thus $I = A$ by the above. Conversely suppose a ring A contains no non-zero ideals besides A. Then for $x \neq 0$ in A, consider the ideal $Ax := \{ax : \ a \in A\}$. This is a non-zero ideal I in A since it contains x, and therefore must be equal to A. In particular it contains 1, so $1 = ax$ for some $a \in A$, and $a = x^{-1}$, so A is a field. □

Let us run through some examples of ideals.

Example 2.3 (Examples of Ideals)

(i) If A is any ring, and $S \subset A$ is any *subset*, define the subset $< S > \subset A$ by:

$$< S >:= \{ \sum_{x_i \in F} a_i x_i : \ F \text{ a finite subset of } S, a_i \in A\}$$

$< S >$ is easily checked to be an ideal in A, called the **ideal generated by** S. Indeed, $< S >$ is the intersection of all ideals of A that contain S (prove!), and thus the smallest ideal of A containing the subset S. If S is a singleton $\{x\}$, the ideal $< S >$ is precisely Ax introduced above, and called a **principal ideal**. If an ideal I can be written as $I =< S >$ for a finite set S, it is said to be **finitely generated**.

(ii) The only ideals in $\mathbf{Z}$ are principal ideals, viz., $\mathbf{Z}m =< m >$ for some integer m. This can be seen by taking the smallest positive integer m in the ideal $I \subset \mathbf{Z}$, and using the division algorithm to prove that if some $a \in I$ were not divisible by m, there would be a minimum strictly positive remainder $s = a - rm$ on dividing a by m, and s would (i) lie in I (since a and m lie in it), and (ii) be strictly less than m, a contradiction. Since $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields, they contain no proper ideals except $\{0\}$ by lemma 2.2 above.

(iii) By the use of the result for $\mathbf{Z}$, it easily follows that the only ideals in $A = \mathbf{Z}_m$ are principal ideals Ax for some $x \in A$.

(iv) Matrix rings $M(n, A)$ for $n \geq 2$ are not commutative, so left, right and 2-sided ideals have to be distinguished. For example the set of all matrices with vanishing first column is a left ideal. Left multiplying such a matrix with any matrix will give a matrix with vanishing first column, as will adding two such matrices. Similarly, those with vanishing first row will constitute a right ideal. If A is commutative, and I is an ideal in A, the subset $M(n, I)$ will be a 2-sided ideal. The set of all compact operators on a Hilbert space $\mathcal{H}$ is a two-sided ideal in $B(\mathcal{H})$.

(v) Let $Z \subset [0, 1]$. The set of all continuous functions in $C([0, 1])$ which identically vanish on Z will constitute an ideal in $C([0, 1])$. One can define similar ideals in $C(\mathbf{R})$, and $C_c(\mathbf{R})$. The conjecture 1.1 can be formulated for $C([0, 1])$ as well: If a closed subset $Z \subset [0, 1]$ is the set of common zeroes of an ideal $I \subset C([0, 1])$, and $f \in C([0, 1])$ vanishes identically on Z, how does f relate with I? The answer, which is the famous Gelfand-Naimark Theorem in analysis, says that f lies in the closure of the ideal I with respect to the sup-norm topology on $C([0, 1])$. The forthcoming Nullstellensatz can be thought of as the analogue of this theorem for polynomial rings.

(vi) Let Z be *any* subset of k^n, where k is a field. The ideal

$$I(Z) = \{f \in k[X_1, .., X_n] : f(a_1, .., a_n) = 0 \text{ for all } \ (a_1, .., a_n) \in Z\}$$

of all polynomials vanishing identically on Z is an ideal in the polynomial ring $k[X_1, .., X_n]$. It is called **the ideal of** Z.

For any set $S \subset k[X_1, .., X_n]$, one can define an **algebraic subset** $V(S)$ **over** k as the following subset of k^n:

$$V(S) = \{(a_1, ..., a_n) \in k^n : \ f(a_1, .., a_n) = 0 \ \text{ for all } f \in S\}$$

Note that $V(S) = V(< S >)$, so all algebraic sets are zero sets of some ideal, and we might as well only consider the algebraic sets $V(I)$ for $I \subset k[X_1, .., X_n]$ an ideal. In fact, more is true:

Proposition 2.4 (Hilbert Basis Theorem) If k is a field, and $I \subset k[X_1, .., X_n]$ an ideal, then I is finitely generated. i.e. $I =< f_1, .., f_m >$ for some polynomials $f_i, \quad 1 \leq i \leq m$.

In particular, every algebraic set is the common zero set of *finitely many polynomials*, since for any subset $S \subset k[X_1, .., X_n]$:

$$V(S) = V(< S >) = V(< f_1, .., f_m >) = V(f_1, .., f_m)$$

We will not digress to prove the proposition 2.4. The case $n = 1$ is easy, because for single variable polynomial rings $k[X]$, one can divide one polynomial f by another polynomial g of degree deg $g = d$ and get a remainder r such that either $r = 0$ or deg $r < d$. The proof given in (ii) of example 2.3 above to show that all ideals in $\mathbf{Z}$ are principal (singly generated) works also for $k[X]$, by choosing the polynomial of least degree in an ideal $I \subset k[X]$. Unfortunately, this "division algorithm" fails for $n \geq 2$. In fact, convince yourself that the ideal $< X_1, X_2 >$ in $k[X_1, X_2]$ cannot be singly generated. If you are unwilling to take the above proposition on faith, or look up the (one page) proof in any of the books listed above, be assured that you can still read on by mentally substituting "finitely generated ideal" whenever you read "ideal", and be none the worse for it. Incidentally, finding minimal sets of generators for ideals in polynomial rings is an old and still very active area of algebra.

Now we can reformulate the conjecture 1.1 for any field k. Clearly, if $Z = V(I)$, i.e. the common zero set of some ideal $I \subset k[X_1, .., X_n]$, then the ideal I is certainly contained in $I(Z)$ (defined in (vi) of example 2.3 above). The conjecture 1.1 may be rephrased as:

Conjecture 2.5 Let k be a field, and $I \subset k[X_1, .., X_n]$ be an ideal. If $f \in I(V(I))$, is it true that $f^r \in I$ for some r (depending on f)? Characterise the fields k for which it is true. (We saw in §1.2 above that it is false for $k = \mathbf{R}$).

Why did we introduce ideals? Mainly because we can construct new rings out of old, "by going modulo" an ideal I. Let $I \subset A$ be an ideal in a commutative ring A. We define an equivalence relation in A as follows: $a \sim b$ if $a - b \in I$. It is also often denoted as $a \equiv b \pmod{I}$ ("a is **congruent to** b **modulo** I"). Check that it is an equivalence relation. The set of equivalence classes $\{\overline{a} : a \in A\}$ is denoted A/I. It also becomes a ring by defining $\overline{a} + \overline{b} := \overline{a + b}$ and $\overline{a}.\overline{b} := \overline{ab}$. To check that these operations are well defined, i.e. if $\overline{a} = \overline{a_1}$, $\overline{b} = \overline{b_1}$, then by definition, $a - a_1 = x \in I$ and $b - b_1 = y \in I$. Thus $(a + b) - (a_1 + b_1) = x + y \in I$,i.e. $\overline{a + b} = \overline{a_1 + b_1}$. Similarly check that $\overline{ab} = \overline{a_1 b_1}$. It is precisely here that all the properties of an ideal are used. A/I is called the **quotient** of A by I, and as a familiar example, if we take $A = \mathbf{Z}$, $I =< m >$, then $A/I = \mathbf{Z}_m$ discussed earlier. Historically, ideals were created by Kummer to handle the breakdown of unique prime factorisation of elements in rings like

$$\mathbf{Z}[\sqrt{5}] := \{m + n\sqrt{5} \subset \mathbf{R} : \ m, n \in \mathbf{Z}\}$$

(a subring of $\mathbf{R}$) (where $2.2 = (\sqrt{5} - 1)(\sqrt{5} + 1)$ are two distinct irreducible factorisations of 4), by replacing it with factorisation of ideals.

2.3 Coordinate rings, k-algebras of finite type

We can now give a geometric meaning to some quotients of polynomial rings. Let Z be an algebraic set in k^n. If we take *any* polynomial $f(X_1, .., X_n)$, it can be regarded as a k-valued function on k^n, by evaluating it at the point $p = (a_1, .., a_n)$, viz. computing $f(a_1, .., a_n)$. We can restrict such a polynomial function f to the subset $Z \subset k^n$, and get a function on Z. But different polynomials $f, g \in k[X_1, ..X_n]$ could end up restricting to the same function on Z. This will happen if and only if $f - g$ vanishes identically on Z. That is, if and only if $f - g \in I(Z)$. That is, if and only if $\overline{f} = \overline{g}$ in $k[X_1, .., X_n]/I(Z)$. Thus $k[X_1, .., X_n]/I(Z)$ is just the ring of functions on Z which are restrictions of polynomial functions on k^n, and is called the **ring of k-regular functions** or **k-coordinate ring** of Z, and denoted $k[Z]$ (not to be confused with the polynomial ring in the variable Z!). The reformulated conjecture 2.5 asks to what extent an ideal I can be gleaned from its zero-set $Z = V(I)$. Another way of formulating it would be ask to what extent can the algebraic object $k[X_1, .., X_n]/I$ be gleaned from the geometric k-coordinate ring $k[V(I)] = k[X_1, .., X_n]/I(V(I))$.

Since we are in the business of formalising everything, we note that if $I \subset k[X_1, .., X_n]$ is a proper ideal, its intersection with the degree 0 polynomials $k \subset k[X_1, .., X_n]$ is $\{0\}$. Thus the quotient ring $k[X_1, .., X_n]/I$ also contains k as a subring, and thus becomes a k-algebra. Quotient rings of the form $B = k[X_1, .., X_n]/I$, where I is a proper ideal, are called **k-algebras of finite type**. The equivalence classes $\overline{X}_i$ in B are usually denoted x_i for convenience, and called **coordinate functions**. Clearly, $\overline{f(X_1, .., X_n)} = f(x_1, .., x_n)$ by the definition of the ring operations in B, and thus these x_i's generate B as a k-algebra, i.e. every element of B can be written as a polynomial in the x_i's with coefficients from k. Unlike the polynomial ring however, some of these polynomials in the $x_i's$ maybe zero. For, if $f(X_1, .., X_n) \in I$, then by definition, the equivalence class $\overline{f(X_1, .., X_n)} = 0$ in B, i.e. $f(x_1, .., x_n) = 0$. Conversely, if $f(x_1, .., x_n) = 0$, then $f \in I$. Thus I is precisely the set of "constraints" or "relations" that measures the departure of the ring B from the polynomial ring $k[X_1, .., X_n]$. The ring B is denoted $k[x_1, .., x_n]$, the lower case letters reminding us that, unlike in the polynomial ring $k[X_1, ..., X_n]$, there may be non-trivial relations between the x_i's in $k[x_1, .., x_n]$. For example, if we take the ideal $I =< X^2 - 2 >$ in $\mathbf{Q}[X]$, then in the ring $\mathbf{Q}[X]/I = \mathbf{Q}[x]$, we have $x^2 = 2$. This ring (which turns out to be a field, why?) is therefore also written as $\mathbf{Q}[\sqrt{2}]$, and is in fact the smallest subfield of $\mathbf{R}$ containing $\mathbf{Q}$ and $\sqrt{2}$. Similarly, in the $\mathbf{R}$-algebra of finite type $\mathbf{R}[X]/ < X^2 + 1 >$ (which is $\mathbf{R}[i] = \mathbf{C}$), we have $i^2 + 1 = 0$. On the other hand, since π is transcendental[2], i.e. does not satisfy any non-zero polynomial with rational coefficients, the ring $\mathbf{Q}[\pi]$ (defined as the smallest $\mathbf{Q}$-subalgebra of $\mathbf{R}$ containing π) is identical ("isomorphic") to the polynomial ring $\mathbf{Q}[X]$.

Here is a little lemma which comes in handy later on:

Lemma 2.6 If B is a k-algebra of finite type, then the dimension of B as a k-vector space (denoted $\dim_k B$) is countable.

Proof: By definition, $B = k[x_1, .., x_n]$ for some n. Since every element in B is a polynomial in x_i with coefficients in k, it is a (not necessarily unique) finite k-linear combination of the monomials

$$\{x_1^{i_1} x_2^{i_2} .. x_n^{i_n} : i_j \in \mathbf{Z}_+\}$$

which is a countable set S. By standard linear algebra S contains a basis, which is therefore also a countable set. □

[2] A deep theorem due to Lindemann and Weierstrass.

3 Maximal ideals, field extensions

3.1 Maximal ideals

From now on, all rings are assumed to be commutative, with 1.

An ideal I in a commutative ring A is called a **maximal ideal** if it is a proper ideal, and contained in no proper ideal other than itself.

Let us prove that every proper ideal I of a ring A is contained in some maximal ideal. For, consider the family Σ of all proper ideals which contain I, which is non-empty since $I \in \Sigma$. Partially order Σ by inclusion, and check that if $\{J_\alpha\}_{\alpha\in\Gamma}$ is any totally ordered subset of Σ, then $\cup_{\alpha\in\Gamma} J_\alpha$ is a proper ideal, and in fact an element of Σ which is an upper bound for this subset. Thus, by Zorn's Lemma, (see [SMS] for a discussion of this all-pervasive lemma that is crucial to all mathematics!) Σ contains maximal elements, which are just maximal ideals containing I. Since $\{0\}$ is a proper ideal in every ring, every ring has maximal ideals.

There is an easy way to determine if I is maximal or not by looking at the quotient ring A/I. To wit,

Lemma 3.1 A proper ideal I in a ring A is maximal iff the quotient ring A/I is a field.

Proof: Clearly if $I \subset J$ for some ideal J of A, then the set $J/I := \{\overline{a} : a \in J\}$ becomes an ideal in A/I. Further, J is a proper ideal of A iff J/I is a proper ideal of A/I. Finally, $J = I$ iff $J/I = \{0\}$. Thus I is a maximal ideal iff A/I contains no proper ideals other than the zero ideal $\{0\}$. We saw in the lemma 2.2 of the last subsection that this happens iff A/I is a field. □

Example 3.2 We have seen that if $A = \mathbf{Z}$, or the single variable polynomial ring $k[X]$, all ideals in A are principal, i.e. of the form $< a >$ for some $a \in A$. Further, such ideals will be proper iff a is not an invertible element, i.e. $a \neq \pm 1$ if $A = \mathbf{Z}$, and $a \notin k \setminus \{0\}$ if $A = k[X]$. If $< a >, < b >$ are proper ideals either of these rings, then $< a > \subset < b >$ iff a is a multiple of b. Thus $< a >$ is a maximal ideal iff a is not invertible, and divisible by nothing except itself, or 1, or other invertible elements in A. In the case of $\mathbf{Z}$, this happens iff a is $\pm$ prime and $\neq \pm 1$. (Thus the lemma 3.1 explains (iii) of example 2.1). If $A = k[X]$, this happens iff a is an irreducible polynomial[3] in $k[X]$ and not in $k \setminus 0$, i.e. irreducible of degree ≥ 1. For example, $X^2 - 2$ is irreducible in $\mathbf{Q}[X]$, and $X^2 + 1$ is irreducible in $\mathbf{R}[X]$ (and the above lemma 3.1 explains why $\mathbf{Q}[\sqrt{2}]$ and $\mathbf{R}[i] = \mathbf{C}$ are fields). What are the irreducible polynomials in $\mathbf{C}[X]$? Before we answer this, let us remark that for the purposes of ideal generation in any polynomial ring $k[X]$ with k a field, the ideal $< \alpha f > = < f >$ for $\alpha \neq 0$ in k, and $f \in k[X]$ any polynomial. Thus, when talking of non-zero ideals $< f >$, we can always assume that the leading coefficient (coefficient of the highest degree term) of f is 1. Such polynomials are called **monic polynomials**.

To see what the irreducible polynomials in $\mathbf{C}[X]$ are, we need the:

Theorem 3.3 (Fundamental Theorem of Algebra) Every polynomial of degree ≥ 1 in $\mathbf{C}[X]$ has a root in $\mathbf{C}$.

This theorem is the key to why complex numbers have such magical powers. A proof of this result can be obtained by using the Liouville theorem in complex analysis, or some elementary topology. See, for example [Ahl] or [Mil], or [Sp].

Corollary 3.4 Every polynomial of degree ≥ 1 in $\mathbf{C}[X]$ is a product of polynomials of degree 1, i.e. linear polynomials.

[3] A polynomial $f \in k[X]$ is said to be irreducible if it is not a product $f = gh$ with $g, h \in k[X]$ and $\deg g < \deg f$, $\deg h < \deg f$

Proof: If deg $f(X) = 1$, there is nothing to prove. Otherwise, note that f has a root $\alpha \in \mathbf{C}$, and is therefore divisible by $(X - \alpha)$ (prove!). Thus $f = (X - \alpha)g(X)$ where deg $g =$ deg $f - 1$. Induct on degree. □

Thus the only irreducible polynomials in $\mathbf{C}[X]$ which are of degree ≥ 1 are linear polynomials, and the above discussion of example 3.2 clearly yields:

Corollary 3.5 The only maximal ideals in $\mathbf{C}[X]$ are the ideals $< X - \alpha >$, for some $\alpha \in \mathbf{C}$. Thus maximal ideals in $\mathbf{C}[X]$ are in 1-1 correspondence with $\mathbf{C}$.

Contrast this with $\mathbf{R}[X]$, where aside from the linear polynomials, quadratic polynomials like $X^2 + 1$ are also irreducible. In fact any quadratic polynomial $x^2 + ax + b$ with real coefficients a and b satisfying $a^2 < 4b$ will be irreducible in $\mathbf{R}[X]$. These, together with the linear polynomials $(X - a)$, exhaust all the irreducible monic polynomials in $\mathbf{R}[X]$ of degree ≥ 1. (Why?)

The preceding discussion leads to the following definition-cum-lemma:

Lemma 3.6 For a field k, following conditions are equivalent:

(i) Every polynomial $f(X)$ of degree ≥ 1 in $k[X]$ has a root in k, i.e. there exists an $\alpha \in k$ such that $f(\alpha) = 0$.

(ii) Every polynomial $f(X)$ of degree ≥ 1 is a product of linear factors. Hence every root of $f(X)$ is in k.

(iii) The only irreducible polynomials of degree ≥ 1 are linear polynomials.

(iv) I is a maximal ideal in $k[X]$ iff $I =< X - \alpha >$ for some $\alpha \in k$.

A field k will be called an **algebraically closed field** iff it satisfies any of the above four equivalent conditions.

3.2 Field extensions

An inclusion $k \subset K$ of fields such that k is a subring of K is called a **field extension**. For example, $\mathbf{Q} \subset \mathbf{R}$, $\mathbf{R} \subset \mathbf{C}$, or $k \subset k(X_1, .., X_n)$ where k is any field, are all field extensions. If $k \subset K$ is a field extension, an element $\alpha \in K$ is said to be **algebraic over** k if there exists a polynomial $f(X) \in k[X], f \neq 0$ such that $f(\alpha) = 0$. Otherwise it is said to be **transcendental** over k. For example $\sqrt{2} \in \mathbf{R}$ is algebraic over $\mathbf{Q}$. However, by the theorem of Lindemann-Weierstrass cited earlier, $\pi \in \mathbf{R}$ is transcendental over $\mathbf{Q}$. Similarly $1 + \sqrt{-5} \in \mathbf{C}$ is algebraic over $\mathbf{R}$, in fact even over $\mathbf{Q}$. Clearly every element of a field k is algebraic over k. Further, Theorems 3.4, 3.5 of [Ja] are easily seen to imply that the subset of elements of K which are algebraic over k form a subfield of K. Thus, the elements of $\mathbf{C}$ which are algebraic over $\mathbf{Q}$ form the field of **algebraic numbers** denoted $\overline{\mathbf{Q}}$. If $k \subset K$ is a field extension in which every element of K is algebraic over k, we call it an **algebraic field extension**. For example $\mathbf{R} \subset \mathbf{C}$ is an algebraic extension (why?), as is $\mathbf{Q} \subset \overline{\mathbf{Q}}$, but $\mathbf{Q} \subset \mathbf{R}$ is not, since e.g. π is not algebraic over $\mathbf{Q}$.

There are many other algebraically closed fields besides $\mathbf{C}$. For example, the field $\overline{\mathbf{Q}}$ is algebraically closed! In fact, there is a result (proved using Zorn's Lemma) which says that for any field k, there is a unique "smallest" algebraically closed field $\overline{k}$ containing it, called the **algebraic closure** of k. Since we won't be needing this result, we will skip the proof. (see [A-M] for a proof). Clearly, theorem 3.3 implies $\overline{\mathbf{R}} = \mathbf{C}$. Note that no finite field k can be algebraically closed, because the polynomial $f(X) = \prod_{\alpha \in k}(X - \alpha) + 1$ (of degree equal to card $k \geq 2$) will be identically $= 1$ at all points of k, and won't have a root in k therefore. However, there is an algebraically closed field $\overline{\mathbf{F}}_p$, in which p times every element is 0 (here p is a prime). The field of rational functions $k(X_1, .., X_n)$ is not algebraically

closed. (Check that no rational function $a = P/Q$ can satisfy the polynomial $f(X) = X^2 - X_1$, for example. You just mimic the proof that $\sqrt{2}$ is irrational, and use the fact that unique factorisation into irreducibles (which are also primes[4]) holds in $k[X_1, .., X_n]$). For a more detailed discussion of algebraic extensions, see the article [Ja].

In the light of (ii) of 3.6, we clearly have the following remark:

Remark 3.7 If $k \subset K$ is an algebraic field extension, and k is algebraically closed, then $k = K$.

Now we have an innocuous looking proposition which is actually equivalent to the nullstellensatz. We prove it for fields of uncountable cardinality, though it is true for all fields k. The proof in general requires the Noether Normalisation Lemma. However, with the cardinality assumption on k, we can give a cheap proof which goes back to Krull and van der Waerden.

Proposition 3.8 Let $k \subset K$ be a field extension such that K is a k-algebra of finite type. Assume that k is an uncountable set. Then K is an algebraic extension of k.

Proof: As noted in the lemma 2.6, the vector space dimension $\dim_k K$ is countable, by the hypothesis on K. Every element of k is certainly algebraic over k, so let α be any element of $K \setminus k$. Consider the set:

$$S = \{(\alpha - a)^{-1} : \ a \in k\}$$

which makes sense since $(\alpha - a) \neq 0$ for $a \in k$. Also, all of these elements are distinct. Thus the cardinality of S is the cardinality of k, that is, S is an uncountable subset of K. Thus all elements of S cannot be k-linearly independent, otherwise it could be enlarged to a k-vector space basis of K, which would also be uncountable, and contradict that $\dim_k K$ is countable. Thus there exist some non-zero elements $\{\lambda_i\}_{i=1}^n \in k$ such that:

$$\lambda_1(\alpha - a_1)^{-1} + ...\lambda_n(\alpha - a_n)^{-1} = 0$$

Now multiply this relation by $\prod_{i=1}^n (\alpha - a_i)$ to get a polynomial relation $f(\alpha) = 0$ with coefficients in k. (Check that f is not the zero polynomial!) Thus α is algebraic over k. □

From the remark 3.7 and the proposition 3.8 above, we have the immediate:

Corollary 3.9 If $k \subset K$ is a field extension such that (i) K is a k-algebra of finite type, (ii) k is uncountable and algebraically closed, then $K = k$.

4 Hilbert's Nullstellensatz

In the sequel, let k **be an uncountable algebraically closed field**. (e.g. $k = \mathbf{C}$)

4.1 Maximal ideals in polynomial rings

As remarked before, the cardinality assumption on k can be dropped, but since we need the corollary 3.9, which we have proved only with this assumption, we retain it. Note that $\mathbf{C}$ is an uncountable algebraically closed field, whereas $\overline{\mathbf{Q}}$ and $\overline{\mathbf{F}}_p$ are not (Why? Just enumerate all polynomials of all degrees with coefficients in $k = \mathbf{Q}$ or $\mathbf{F}_p$!)

We are now ready to analyse maximal ideals in $k[X_1, .., X_n]$. We have the following proposition, which is often called the "small nullstellensatz", even though it is equivalent to the later "big nullstellensatz"

[4] An element x in a ring A is said to be prime if x divides ab implies x divides a or x divides b.

Proposition 4.1 (Hilbert's Nullstellensatz I) Let k be as above. Then an ideal $I \subset k[X_1, .., X_n]$ is maximal iff $I =< X_1 - a_1, .., X_n - a_n >$ for some $a_i \in k$. In other words, maximal ideals are in 1-1 correspondence with points of k^n.

Proof: We remark that for the single variable case of $n = 1$, we have already seen this result in (iv) of lemma 3.6.

First, let us convince ourselves that all the ideals $I =< X_1 - a_1, .., X_n - a_n >$ are indeed maximal. For this we need to show that A/I is a field (by lemma 3.1), where $A = k[X_1, .., X_n]$. If $f(X_1, .., X_n)$ is any polynomial in A, one can rewrite it as $f((X_1 - a_1) + a_1, .., (X_n - a_n) + a_n)$. Now any power $((X_i - a_i) + a_i)^{n_i}$ can be written in the form $(X_i - a_i)h_i + a_i^{n_i}$ (by binomial expansion), where h_i is a polynomial in X_i. Substituting these in f, we can "Taylor expand" f:

$$f(X_1, .., X_n) = f(a_1, .., a_n) + \Sigma_{i=1}^n g_i(X_1, .., X_n)(X_i - a_i)$$

where $g_i \in A$ are some polynomials. The second term on the right hand side is clearly in the ideal $I =< X_1 - a_1, .., X_n - a_n >$. This shows that every element in $A = k[X_1, .., X_n]$ is congruent to the element $f(a_1, .., a_n) \in k \pmod I$. Also the element $a \in k \subset A$ is clearly congruent only to itself (mod I), and no other element of k (since $I \cap k = \{0\}$). Thus A/I is just the field k, and I is maximal.

It is in the converse that the algebraic assumptions on k are required. Let $I \subset A = k[X_1, .., X_n]$ be a maximal ideal. Then by definition A/I is a k-algebra of finite type, contains k, and is a field by lemma 3.1. Denote it by K. Thus $k \subset K$ is a field extension. By the corollary 3.9, $K = k$. Denoting the equivalence classes of X_i by $\overline{X}_i \in K = A/I$, it follows that $\overline{X}_i = a_i \in k$ for all $i = 1, .., n$. Saying that $\overline{X}_i = a_i$ in K, by definition, means $X_i - a_i \in I$ for all i. Thus the ideal $< X_1 - a_1, .., X_n - a_n > \subset I$. However, in the last para we saw that the ideal $< X_1 - a_1, .., X_n - a_n >$ is maximal. Thus it must be equal to I, which is a proper ideal (being a maximal ideal!). This proves the proposition. □

Exercise 4.2 Prove that for k as above, a maximal ideal in $A = k[X_1, .., X_n]$ is precisely the ideal of all polynomials vanishing at some point $(a_1, .., a_n) \in k^n$. More generally, show that for *any* ideal $I \subset A$, the points of $V(I) \subset k^n$ are in 1-1 correspondence with all the maximal ideals in A which contain I.

Corollary 4.3 Let k be as above, and $\{f_i\}_{i=1}^m$ be some set of polynomials in $A = k[X_1, .., X_n]$. Then the algebraic set $V(f_1, .., f_m)$ is empty if and only if there exist polynomials $h_i \in A$ for $i = 1, .., m$ such that $\sum_{i=1}^m h_i f_i = 1$.

Proof: Consider the ideal $J =< f_1, .., f_m >$. Then either J is a proper ideal or $J = A$. If J were a proper ideal, by the first para of §3.1, it would follow that $J \subset I$ for some maximal ideal I. By the small nullstellensatz I above, $I =< X_1 - a_1, .., X_n - a_n >$. Thus every element of J would be of the form $\sum_{i=1}^n g_i(X_i - a_i)$, and would thus vanish at the point $(a_1, .., a_n)$. In particular $V(J) = V(f_1, .., f_m)$ would contain $(a_1, .., a_n)$, and be non-empty. Thus $V(f_1, .., f_m) = \phi \Rightarrow J = A$, and hence $1 \in J =< f_1, .., f_m >$. In other words, $1 = \sum_{i=1}^m h_i f_i$ for some $h_i \in A$. The converse is obvious (since $1 \neq 0$!) □

Note how crucial it is for k to be algebraically closed for the corollary above because, for example, $V(X^2 + 1) \subset \mathbf{R}$ is empty, but you cannot multiply $X^2 + 1$ by any polynomial $h \in \mathbf{R}[X]$ to get 1.

4.2 The big Nullstellensatz

Now, for the answer to the conjectures 1.1, 2.5 posed earlier!

Theorem 4.4 (Hilbert's Nullstellensatz II) Let k be as assumed at the outset of this section (i.e. uncountable and algebraically closed). If a polynomial $f \in A = k[X_1, .., X_n]$ vanishes identically at all points of $V(I)$ for some ideal $I \subset A$, then $f^r \in I$ for some r.

Proof: By 2.4, write $I =< f_1, .., f_m >$. If $f = 0$, there is nothing to prove, so assume $f \neq 0$. The trick is to add an extra variable, and "invert f" (called the *Rabinowitch trick*). Indeed, all the polynomials in A can be regarded as elements of the bigger ring $B = k[X_1, .., X_{n+1}]$. Consider the ideal $J \subset B$ generated by the elements $f_i(X_1, .., X_n)$ for $1 \leq i \leq m$ and the extra element $X_{n+1}f(X_1, .., X_n) - 1$. Claim that $V(J) \subset k^{n+1}$ is empty. If not, there would be a point $(a_1, .., a_{n+1}) \in V(J)$. Since all the $f_i = f_i(X_1, .., X_n)$ would have to vanish at this point, it would follow that $(a_1, .., a_n) \in V(I)$. Also since $X_{n+1}f - 1$ would have to vanish at this point, we would have $a_{n+1}f(a_1, .., a_n) = 1$. But then since f vanishes identically on $V(I)$, and $(a_1, .., a_n) \in V(I)$, we have $f(a_1, .., a_n) = 0$. Thus $a_{n+1}.0 = 1$, i.e. $0 = 1$, a contradiction. This proves the claim.

So, by the corollary 4.3 above (applied to $J \subset B$), there must be polynomials $h_i(X_1, .., X_{n+1}) \in B$ such that:

$$1 = h_{m+1}(X_1, .., X_{n+1})(X_{n+1}f(X_1, .., X_n) - 1) + \sum_{i=1}^{m} h_i(X_1, .., X_{n+1})f_i(X_1, .., X_n)$$

The above identity holds in the polynomial ring $B = k[X_1, .., X_{n+1}]$. Substituting $X_i = X_i$ for $1 \leq i \leq n$ and $X_{n+1} = 1/f$ in this identity gives us an identity in the field $k(X_1, .., X_n)$, since $f \neq 0$. This subsitution kills the first term, and we get:

$$1 = \sum_{i=1}^{m} h_i(X_1, .., X_n, \frac{1}{f})f_i(X_1, .., X_n)$$

as an identity in $k(X_1, .., X_n)$. Clearly, by using high enough power f^r as the common denominator on the right hand side, (e.g. $r =$ maximum of the X_{n+1} degrees of all the h_i), and cross-multiplying, we have:

$$f^r = \sum_{i=1}^{m} P_i(X_1, .., X_n)f_i(X_1, .., X_n)$$

where P_i are some polynomials. This last identity holds in the field $k(X_1, .., X_n)$, and both sides of the identity are in $A = k[X_1, .., X_n]$. Since A sits as a subring in $k(X_1, .., X_n)$, the identity holds in A. Thus $f^r = \sum_i P_i f_i \in I$ as asserted. □

5 Concluding remarks

5.1 Radical ideals and reduced algebras

If I is any ideal in a ring A, one can define a new ideal called the the **radical of** I, denoted $\sqrt{I}$ by:

$$\sqrt{I} = \{a \in A : \ a^r \in I \text{ for some } r\}$$

It is easy to check that this is an ideal, and it contains I by definition. An ideal I is said to be a **radical ideal** if $\sqrt{I} = I$. Again it is easy to verify that the radical of any ideal is a radical ideal. The condition for an ideal I to be radical can be reformulated in terms of the quotient ring A/I. Clearly, I is a radical ideal if A/I has no nilpotent elements other than 0 (a **nilpotent element** x in a ring is an element such that some power of it is 0). Rings which have no nilpotents other than 0 are called **reduced**. The main example of a radical ideal is $I(Z)$ where Z is an algebraic set, for clearly if f^r vanishes identically on Z for a polynomial f, then f must also do so. Thus the k-coordinate ring $k[Z]$ of an algebraic set Z is a reduced k-algebra of finite type.

Thus the nullstellensatz II (Theorem 4.4) implies:

Let k be an (uncountable) algebraically closed field, and $A = k[X_1, .., X_n]$ the n-variable polynomial ring over it:

(i) For $I \subset A$ any ideal, $I(V(I)) = \sqrt{I}$. If I is a radical ideal $I(V(I)) = I$.

(ii) The maps: $I \mapsto V(I)$, and $Z \mapsto I(Z)$ are inverses of each other from the set of **radical ideals** in A to the set of **algebraic sets in** k^n.

(iii) B is a reduced k-algebra of finite type iff it is the k-coordinate ring of some algebraic set in some k^n. (By definition, $B = k[X_1, .., X_n]/I$ for some ideal I. B reduced implies I is a radical ideal. Now use (ii))

The reader may wonder what happens if we take *some subset* $S \subset k^n$, not necessarily an algebraic one, consider the ideal $I(S)$ of all polynomials vanishing identically on S (which we have seen to be an ideal in (vi) of example 2.3), and then take the algebraic set $V(I(S))$. The answer is that one gets the smallest algebraic set containing S, called the "Zariski closure of S". The algebraic subsets of k^n define the closed sets of a topology on k^n, called the **Zariski topology**, and Zariski closure is closure in this topology. (Exercise: What is the Zariski topology on $\mathbf{C}$? How does it compare with the usual topology?)

Thus, this reformulation has established a complete back-and-forth passage between the geometric objects called algebraic sets, and the algebraic objects called k-algebras of finite type, when k is algebraically closed. This has beautiful and far reaching consequences not only for algebra and geometry, but all of mathematics!

References

[Ahl] Ahlfors, L., *Complex Analysis*, 3rd Ed., McGraw Hill.

[A-M] Atiyah, M, and MacDonald, I.G.: *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[J] Jacobson, N., *Basic Algebra*, Vol. 1, Freeman, 1974.

[Ja] Jagadeeshan, Shashidhar *Ruler and Compass Constructions* Resonance, Vol 4, No. 3, March 1999.

[Mil] Milnor, J., *Topology from a Differentiable Viewpoint*, Univ. of Virginia Press.

[P-S] Paranjape, K., Srinivas, V., *The Weil Conjectures*, Resonance, Vol. 4, No. 5, May 1999.

[Si] Singh, Balwant, *Polynomial Variables and the Jacobian Problem*, Resonance, Vol. 4, No. 4, April 1999.

[SMS] S.M.Srivastava, *Transfinite Numbers-What is Infinity?* Vol. 2, No. 3, March 1997. 58-68 :

[Sp] Spanier, E., *Algebraic Topology*, Springer Verlag.

[Z-S] Zariski, O., and Samuel, P., *Commutative Algebra*, Vol. 1, Springer-Verlag GTM 28.