WHAT IS ALGEBRAIC GEOMETRY?

LUCIA CAPORASO

Algebraic Geometry - Summer School
Gulbenkian Foundation, LISBON 14-18 JULY 2014

1. Lecture 1

1.1. Notations and algebraic set up.

$\mathbb{N} = \{1, 2, 3, ...\}$ is the set of natural numbers. There is little algebraic structure on $\mathbb{N}$: we can add but not subtract, we can multiply but not divide.
$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$ is the set of integers. We can now add and substract, hence $\mathbb{Z}$ is a *group* with respect to the sum; we can multiply but, still, we cannot divide two integers. So $\mathbb{Z}$ is a *ring* (but not a field).
$\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ are the set of, respectivey, rational, real and complex numers. Within each of these sets we can add, substract and multiply any two numbers; moreover we can divide any number by any number other than zero. So these three sets are *fields*. We have, of course

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

We now consider *polynomials* with coefficients in some of the above sets. Let us start with polynomials in the biggest one, $\mathbb{C}$. Pick $n \in \mathbb{N}$; we denote by

$$\mathbb{C}[x_1, \dots, x_n]$$

the set of polynomials in n variables, $x_1, \dots, x_n$. When $n = 1$ we simplify the notation and write just $\mathbb{C}[x]$; also, if $n = 2$ we write $\mathbb{C}[x, y]$.

Now, the sum of two polynomials is again a polynomial, and the product of two polynomials is again a polynomial. These two operations have exactly the same properties of addition and multiplications of elements in $\mathbb{Z}$. So, $\mathbb{C}[x_1, \dots, x_n]$ is also a ring, and its ring structure induces the ring structure, mentioned above, on any of its subsets $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{C}[x_1, \dots, x_n]$. On the other hand it is clear that when we divide two polynomials we may fail to get another polynomial. So $\mathbb{C}[x_1, \dots, x_n]$ is not a field.

The ring $\mathbb{C}[x_1, \dots, x_n]$ is the source of all technical tools we have to work as geometers.

We now have the tools; what objects can we fabricate with them?

1.2. **The geometric objects of algebraic geometry.**

What are the geometric objects that algebraic geometry studies?

We begin with the ambient space, which will be $\mathbb{C}^n$, the set of n-tuples of complex numbers. We have chosen $\mathbb{C}$ among all sets of numbers introduced before for reasons that we shall explain in a moment.

For a point $p \in \mathbb{C}^n$ we write $p = (a_1, \dots, a_n)$ with $a_i \in \mathbb{C}$ to indicate its coordinates.

Let now $f = f(x_1, \dots, x_n) \in \mathbb{C}[x_1, \dots, x_n]$ be a polynomial, and let $p \in \mathbb{C}^n$. The value of f at p is a well defined complex number

$$f(p) = f(a_1, \dots, a_n) \in \mathbb{C}.$$

Special case 1.1. Suppose the polynomial f is an element in $\mathbb{C}$, i.e. f is a *constant polynomial*; to fix ideas, suppose $f = 1$. Then the value of f at p does not depend on p, as we have $f(p) = 1$ for every $p \in \mathbb{C}^n$.

Conversely, if $f \in \mathbb{C}[x_1, \dots, x_n]$ is such that $f(p) = f(p')$ for every $p, p' \in \mathbb{C}^n$, then $f \in \mathbb{C}$. (Exercise).

Given a polynomial f we can associate to it the locus of $p \in \mathbb{C}^n$ such that $f(p) = 0$. This is the simplest example of our geometric objects.

Definition 1.2. Let $f \in \mathbb{C}[x_1, \dots, x_n]$; we denote

$$\mathcal{Z}(f) := \{p \in \mathbb{C}^n : f(p) = 0\}.$$

More generally, for any subset $T \subset \mathbb{C}[x_1, \dots, x_n]$ we denote

$$\mathcal{Z}(T) := \{p \in \mathbb{C}^n : f(p) = 0 \quad \forall f \in T\}.$$

Sets of the form $\mathcal{Z}(T)$ are called *affine* subsets of $\mathbb{C}^n$.

Remark 1.3. If f is not a constant polynomial, then $\mathcal{Z}(f)$ is *non empty*. This is a consequence of the fact that $\mathbb{C}$ is an *algebraically closed* field, i.e. every non constant polynomial $f \in \mathbb{C}[x]$ admits a zero in $\mathbb{C}$.

Examples 1.4. (a) $\mathbb{C}^n = \mathcal{Z}(0)$. Hence $\mathbb{C}^n$ is itself an affine subset. $\mathbb{C}^n$ is called the *affine n-space*.

(b) If $f \in \mathbb{C}$ with $f \neq 0$, then $\mathcal{Z}(f) = \emptyset$.

(c) Let $n = 1$ and let $f \in \mathbb{C}[x]$ be a non constant polynomial. Then $\mathcal{Z}(f)$ is a finite set of points whose cardinality is at most equal to the degree of f.

Conversely, let $X = \{b_1, \dots, b_r\} \subset \mathbb{C}$. Then

$$X = \mathcal{Z}((x - b_1) \cdot (x - b_r)).$$

Therefore *every finite subset of $\mathbb{C}$ is an affine subset, and conversely, every affine subset of $\mathbb{C}$ is finite.*

(d) Let now $f = c_0 + c_1x_1 + \dots c_nx_n$ be a polynomial of degree 1. Then $\mathcal{Z}(f)$ is a particular type of affine subset. Indeed, if $n = 1$ then $\mathcal{Z}(f)$ is a point, if $n = 2$ then $\mathcal{Z}(f)$ is a line, if $n = 3$ then $\mathcal{Z}(f)$ is a plane. For general n the set $\mathcal{Z}(f)$ is called a *hyperplane*. Observe that for any linear f the set $\mathcal{Z}$ is non empty.

Now let us ask ourselves whether what we said so far works if we replace $\mathbb{C}$ by $\mathbb{R}$, $\mathbb{Q}$, or even by $\mathbb{Z}$. The example (d) is clearly false if we replace $\mathbb{C}$ by $\mathbb{Z}$. For example, the linear polynomial in one variable $f = 2x$ admits no zeroes in $\mathbb{Z}$.

On the other hand, by basic algebra we have that everything works equally well if we replace $\mathbb{C}$ by $\mathbb{Q}$ or $\mathbb{R}$ (or by any field), with the exception of remark 1.3. For example, let $f = x^2 + 1$. Then f has no zeroes in $\mathbb{Q}$ or in $\mathbb{R}$.

Indeed, as we shall see again several times, in classical algebraic geometry one needs to work with $\mathbb{C}$, or with an algebraically closed field, as *base field*.

Exercise 1.5. Let $T \subset \mathbb{C}[x_1, \ldots, x_n]$ and let $I := (T) \subset \mathbb{C}[x_1, \ldots, x_n]$ be the ideal generated by T. Prove that $\mathcal{Z}(T) = \mathcal{Z}(I)$

1.3. **The Zariski topology.** Let us now fix the affine n-space $\mathbb{C}^n$ and consider the class of all of its affine subsets

$$\mathcal{C} := \{\mathcal{Z}(T) : \ \forall T \subset \mathbb{C}[x_1, \ldots, x_n]\}.$$

What properties does it have?

Proposition 1.6. *$\mathcal{C}$ has the following properties.*

(a) $\mathcal{C} = \{\mathcal{Z}(T) : \ T \subset \mathbb{C}[x_1, \ldots, x_n]$ such that T is finite$\}$;
(b) $\mathcal{C}$ is closed with respect to finite union, that is $\mathcal{Z}(T_1) \cup \mathcal{Z}(T_2) \in \mathcal{C}$ for every $T_1, T_2 \subset \mathbb{C}[x_1, \ldots, x_n]$;
(c) $\mathcal{C}$ is closed with respect to arbitrary intersection, that is, for any (possibly infinite) index set J, we have $\cap_{j \in J} \mathcal{Z}(T_j) \in \mathcal{C}$ for every $T_j \subset \mathbb{C}[x_1, \ldots, x_n]$.

Proof. We begin by proving that for any set $T \subset \mathbb{C}[x_1, \ldots, x_n]$ there exists a finite set $T' \subset \mathbb{C}[x_1, \ldots, x_n]$ such that $\mathcal{Z}(T) = \mathcal{Z}(T')$.

Let $I := (T) \subset \mathbb{C}[x_1, \ldots, x_n]$ be the ideal generated by T. Then, by Exercise 1.5 we have $\mathcal{Z}(T) = \mathcal{Z}(I)$. Now, $\mathbb{C}[x_1, \ldots, x_n]$ is a noetherian ring (by Hilbert's basis theorem), therefore I admits a finite set of generators. So, there exist $f_1, \ldots, f_m \in \mathbb{C}[x_1, \ldots, x_n]$ such that $I = (f_1, \ldots, f_m)$. Set $T' = \{f_1, \ldots, f_m\}$. Then, again by Exercise 1.5, we have

$$\mathcal{Z}(T) = \mathcal{Z}(I) = \mathcal{Z}(T').$$

The first claim is proved.

To prove that $\mathcal{C}$ contains the union of any two of its subsets, set

$$T_1 \cdot T_2 := \{f_1 \cdot f_2 : \ \forall f_1 \in T_1, \ f_2 \in T_2\}.$$

Then, since $T_1 \cdot T_2$ is also a subset of $\mathbb{C}[x_1, \ldots, x_n]$ it suffices to prove the following:

$$\mathcal{Z}(T_1) \cup \mathcal{Z}(T_2) = \mathcal{Z}(T_1 \cdot T_2). \tag{1}$$

Indeed, the inclusion $\mathcal{Z}(T_1) \cup \mathcal{Z}(T_2) \subset \mathcal{Z}(T_1 \cdot T_2)$ is obvious. For the other inclusion, let $p \in \mathcal{Z}(T_1 \cdot T_2)$; if $p \notin \mathcal{Z}(T_1)$ there is $f \in T_1$ such that $f(p) \neq 0$. Now, for every $g \in T_2$ we have

$$(f \cdot g)(p) = 0 \Rightarrow f(p) \cdot g(p) = 0 \Rightarrow g(p) = 0$$

hence $p \in \mathcal{Z}(T_2)$, and we are done.

Finally, to show that $\mathcal{C}$ contains the intersection of any set of its elements it suffices to check the following trivial identity

$$\bigcap_{j \in J} \mathcal{Z}(T_j) = \mathcal{Z}(\bigcup_{j \in J} T_j). \tag{2}$$

■

Remark 1.7. An infinite union of affine subsets may fail to be affine. For example, we know that a point in $\mathbb{C}$ is affine, but an infinite union of distinct poins is not affine; see Example 1.4 (c).

Now we recall an important general definition from topology.

Definition 1.8. Let X be a non empty set and let $\mathcal{C}$ be a set of subsets of X satisfying the following properties.

(1) $X, \emptyset \in \mathcal{C}$;
(2) $\mathcal{C}$ is closed with respect to finite union, that is $Z_1 \cup Z_2 \in \mathcal{C}$ for every $Z_1, Z_2 \in \mathcal{C}$;
(3) $\mathcal{C}$ is closed with respect to arbitrary intersection, that is, for any index set J, we have $\cap_{j \in J} Z_j \in \mathcal{C}$ for every $Z_j \in \mathcal{C}$.

Then $\mathcal{C}$ defines on X a *topology* for which the elements of $\mathcal{C}$ are called *closed* subsets, and the elements of

$$\mathcal{U} := \{X \smallsetminus Z, \ \forall Z \in \mathcal{C}\}$$

are called *open* subsets.

By the examples 1.4 and Proposition 1.6 we have that the affine subsets of $\mathbb{C}^n$ define a topology, called the *Zariski* topology, for which they are the closed subsets, and their complements the open subsets. From now on we shall consider the set $\mathbb{C}^n$ endowed with the Zariski topology, which will be denoted by $\mathbb{A}^n$, the *topological affine n-space.*

Here are some basic facts about the Zariski topology.

Proposition 1.9. *(a) The points of $\mathbb{A}^n$ are closed subsets (i.e. the Zariski topolgy is T1).*

(b) For every $f \in \mathbb{C}[x_1, \ldots, x_n]$ the map ϕ_f

$$\phi_f : \mathbb{A}^n \longrightarrow \mathbb{A}^1; \quad p \mapsto f(p)$$

is continuous (i.e. the preimage of a closed subset is closed).

(c) The Zariski topology is the coarsest topology on $\mathbb{C}^n$ for which the maps ϕ_f defined in (b) *are all continuous.*

Proof. (a) Let $p = (a_1, \dots a_n)$, then $p = \mathcal{Z}(x_1 - a_1, \dots, x_n - a_n)$.

(b) We first observe that for any $a \in \mathbb{A}^1$, the preimage of a via ϕ_f is equal to $\mathcal{Z}(f - a)$ (which is well defined since $a \in \mathbb{C}$ and hence $f - a \in \mathbb{C}[x_1, \dots, x_n]$). Let $C \subsetneq \mathbb{A}^1$ be a closed subset; by Example 1.4 (c) we know that C is a finite subset of $\mathbb{A}^1$, so we can write $C = \{a_1, \dots, a_m\}$ with $a_i \in \mathbb{C}$. Then, as we observed above

$$\phi_f^{-1}(C) = \mathcal{Z}(f - a_1) \cup \dots \cup \mathcal{Z}(f - a_m) = \mathcal{Z}(\prod_{i=1}^{m}(f - a_i)),$$

where the last equality follows from (2); since $\prod_{i=1}^{m}(f - a_i) \in \mathbb{C}[x_1, \dots, x_n]$ we are done.

(c) Let $Z = \mathcal{Z}(f_1, \dots, f_m)$ and let us prove that Z must be closed in any topology for which the maps ϕ_{f_i} are continuous for $i = 1, \dots, m$. This will prove the claim.

Since ϕ_{f_i} is continuous, the set $\mathcal{Z}(f_i) = \phi_{f_i}^{-1}(0)$ is closed, because the point 0 is closed in $\mathbb{A}^1$. On the other hand, we clearly have $\mathcal{Z}(f_1) \cap \dots \cap \mathcal{Z}(f_m) = Z$. Since the intersection of closed sets is a closed set, we get that Z is closed, and we are done. ■

Exercise 1.10. Let $n \geq 2$. True or false.

(1) For every ideal $I \subsetneq \mathbb{C}[x_1, \dots, x_n]$ the set $\mathcal{Z}(I)$ is non-empty.
(2) For every $f \in \mathbb{C}[x_1, \dots, x_n]$ with f not constant, the set $\mathcal{Z}(f)$ is infinite.

Exercise 1.11. Let T_1 e T_2 be subsets of $\mathbb{C}[x_1, \dots, x_n]$. Prove that if $T_1 \subset T_2$ then $\mathcal{Z}(T_2) \subset \mathcal{Z}(T_1)$.

Show that the opposite implication fails.

Exercise 1.12. Let $I \subsetneq \mathbb{C}[x_1, \dots, x_n]$ be a proper ideal generated by homogeneous polpolynomials (a so-called homogeneous ideal). Prove that $0 = (0, \dots, 0) \in \mathbb{A}^n$.

Exercise 1.13. Identify $\mathbb{A}^2$ with $\mathbb{A}^1 \times \mathbb{A}^1$ in the obvious way. Compare the Zariski topology on $\mathbb{A}^2$ with the product topology (on $\mathbb{A}^1 \times \mathbb{A}^1$). Show that they are different and that the Zariski topology is finer than the product topology.

2. Lecture 2

2.1. **Points in $\mathbb{A}^n$ and maximal ideals in $\mathbb{C}[x_1, \ldots, x_n]$.** Recall that a maximal ideal of a ring[1] R is a proper ideal $M \subsetneq R$ which is not contained in another proper ideal of R. A fundamental characterization of maximal ideals is given in the following.

Lemma 2.1. *Let R be a ring with $1 \in R$.*
(a) R is a field if and only if its only ideals are (0) and (1).
(b) An ideal M of R is maximal if and only if R/M is a field.

Proof. It is clear that if R is a field then its only ideals are (0) and (1). Conversely, suppose the only ideals of R are (0) and (1). Let $x \in R$ be a non-invertible element; then the ideal (x) is not equal to (1). Hence $(x) = (0)$, and therefore $x = 0$. So (a) is proved.

Now (b) is an immediate consequence of (a). ∎

We mention (for later purposes) a basic fact about maximal ideals.

Fact. *Let R be a commutative ring. Every ideal of R is contained in a maximal ideal.*

Exercise 2.2. Prove Fact 2.1 assuming that R is a noetherian ring. (For a general ring one needs to use Zorn's Lemma).

In Proposition 1.9 we saw that a point $p = (a_1, \ldots, a_n)$ of $\mathbb{C}^n$ is expressed as an affine subset in a *canonical* way, namely $p = \mathcal{Z}(x_1 - a_1, \ldots, x_n - a_n)$. This phenomenon is typical of points, i.e. it does not extend to other affine sets, so for the moment we shall concentrate on points and prove the following important result.

Theorem 2.3 (Weak Hilbert Nullstellensatz)**.** *There is a bijection between the points of $\mathbb{C}^n$ and the maximal ideals of $\mathbb{C}[x_1, \ldots, x_n]$, given by associating to the point $(a_1, \ldots, a_n)$ the ideal $(x_1 - a_1, \ldots, x_n - a_n)$.*

Proof. Proof for $n = 1$. First we show that for every $a \in \mathbb{C}$ the ideal $(x - a) \subset \mathbb{C}[x]$ is maximal (this part of the proof holds for every field). Let us define a ring morphism as follows.

$$\begin{array}{ccc} \mathbb{C}[x] & \xrightarrow{v_a} & \mathbb{C} \\ f(x) & \mapsto & f(a). \end{array} \tag{3}$$

It is a surjective morphism, since its restriction to $\mathbb{C}$ is just the identity. Hence, by the above Lemma, its kernel, $\ker v_a$, is a maximal ideal of $\mathbb{C}[x]$. We claim that

$$\ker v_a = (x - a).$$

Of course, $x - a \in \ker v_a$ hence $\ker v_a \supset (x - a)$. Recall that $\mathbb{C}[x]$ is a principal ideal domain, hence there exists a polynomial $f \in \mathbb{C}[x]$ such that $(f) = \ker v_a$. We can choose f monic, and of minimal degree among all generators. Now, we have $(x - a) = f \cdot q$ with $q \in \mathbb{C}[x]$; by

[1] We always assume that our rings are commutative

our choice of f we must have $q = 1$ e $f = x - a$. This finishes the first part of the proof.

For the second part, we must prove that every maximal ideal $M \subset \mathbb{C}[x]$ is of type $M = (x - a)$ for some $a \in \mathbb{C}$ (this part of the proof extends to every algebraically closed field). Since every ideal of $\mathbb{C}[x]$ is principal, we can write $M = (g)$ for some $g \in \mathbb{C}[x]$.

Now, as $\mathbb{C}$ is algebraically closed, g admits a zero in $\mathbb{C}$, that is there exists $a \in \mathbb{C}$ such that $g(a) = 0$. Equivalently, there exists $a \in \mathbb{C}$ such that $g = (x - a)q$ with $q \in \mathbb{C}[x]$. Therefore the ideal $(g) = M$ is contained in the ideal $(x - a)$. Since by assumption M is maximal, we must have $M = (x - a)$. ■

Proof for every n. We first prove that the ideal $(x_1 - a_1, \dots, x_n - a_n)$ is maximal in $\mathbb{C}[x_1, \dots, x_n]$ (as before, this is the easy part of the proof and holds for any field). Given $\underline{a} := (a_1, \dots, a_n) \in \mathbb{C}^n$ we define the morphism $v_{\underline{a}}$ as follows

$$\begin{array}{ccc} \mathbb{C}[x_1, \dots, x_n] & \xrightarrow{v_{\underline{a}}} & \mathbb{C} \\ f(x_1, \dots, x_n) & \mapsto & f(a_1, \dots, a_n) \end{array} \tag{4}$$

Again, $v_{\underline{a}}$ is surjective, hence $\ker v_{\underline{a}}$ is a maximal ideal of $\mathbb{C}[x_1, \dots, x_n]$. For every $i = 1, \dots, n$ the polynomial $x_i - a_i$ lies in $\ker v_{\underline{a}}$, hence

$$(x_1 - a_1, \dots, x_n - a_n) \subset \ker v_{\underline{a}}.$$

We claim that equality holds above.

Suppose first $\underline{a} = (0, \dots, 0)$. Let $f \in \ker v_{\underline{a}}$, so that $f(0, \dots, 0) = 0$; hence f has no constant term and we can write

$$f = \sum_{i=1}^{n} c_i x_i + \sum_{i \le j} c_{i,j} x_i x_j + \dots = \sum_{i=1}^{n} x_i g_i$$

where $c_* \in \mathbb{C}$ and $g_i \in \mathbb{C}[x_1, \dots, x_n]$. Therefore $f \in (x_1, \dots, x_n)$ and we are done. The case of a general $\underline{a}$ can be obtained from the one we just treated by changing variables: $x_i' = x_i - a_i$ per $i = 1, \dots, n$.

Now we prove the opposite implication, i.e. the fact that any maximal ideal $M \subset \mathbb{C}[x_1, \dots, x_n]$ is generated by n linear polynomials; this is the really interesting part. Consider the quotient morphism π

$$\mathbb{C}[x_1, \dots, x_n] \xrightarrow{\pi} \frac{\mathbb{C}[x_1, \dots, x_n]}{M} = K$$

where K is a field. Let us consider the restriction of π to the subring $\mathbb{C}[x_1] \subset \mathbb{C}[x_1, \dots, x_n]$, written π_1:

$$\mathbb{C}[x_1] \xrightarrow{\pi_1} K,$$

The key step of the proof is the following claim:
Claim: π_1 *is not injective, i.e.* $\ker \pi_1 \neq (0)$*).*

We prove the claim by contradiction: suppose π_1 injective. Hence the field K contains a copy of the ring of complex polynomials in one variable; we denote by $\mathbb{C}[t] \subset K$ this copy, so that $t = \pi(x_1)$. As K is a field, K contains the quotient field of $\mathbb{C}[t]$, denoted as usual by $\mathbb{C}(t)$. So we have an inclusion

$$\mathbb{C}(t) \subset K = \frac{\mathbb{C}[x_1, \ldots, x_n]}{M}$$

which we shall now study as an inclusion of $\mathbb{C}$ vector spaces.

The vector space $\mathbb{C}[x_1, \ldots, x_n]$ has a $\mathbb{C}$-base given by the set of all monomyals:

$$\mathcal{B} = \{x_1^{d_1} \cdot \ldots \cdot x_n^{d_n}, \quad \forall d_i \geq 0\}.$$

Now $\mathcal{B}$ is a countable set, i.e. $\mathcal{B}$ has the same cardinality of $\mathbb{N}$; we shall write $\#\mathcal{B} = \#\mathbb{N}$. Now the images in K of elements of $\mathcal{B}$ span K as a $\mathbb{C}$-vector space; hence the dimension of K as $\mathbb{C}$-vector space is at most equal to $\#\mathbb{N}$.

Let us now look at $\mathbb{C}(t)$; we claim that it contains a subset $\mathcal{G}$ of $\mathbb{C}$-linearly independent elements such that the cardinality of $\mathcal{G}$ is not countable, i.e. $\#\mathcal{G} > \#\mathbb{N}$. Indeed, let

$$\mathcal{G} := \{\frac{1}{t-a} \quad \forall a \in \mathbb{C}\}.$$

It is clear that $\#\mathcal{G} = \#\mathbb{C}$ and hence, as is well known that $\#\mathbb{C} > \#\mathbb{N}$, we get $\#\mathcal{G} > \#\mathbb{N}$. Now suppose $\mathcal{G}$ has a subset of linearly dependent elements; then we have an identity:

$$\sum_{i=1}^{m} \frac{c_i}{t - a_i} = 0$$

with $c_i \in \mathbb{C} \smallsetminus \{0\}$ and $a_i \neq a_j$.

Now focus on the rational function $\frac{c_1}{t-a_1}$; from the above identity, considering the absolute values, we get

$$\Big|\frac{c_1}{t-a_1}\Big| = \Big|\sum_{i=2}^{m} \frac{c_i}{t-a_i}\Big| \leq \sum_{i=2}^{m} \Big|\frac{c_i}{t-a_i}\Big|.$$

Of course, $\frac{c_1}{t-a_1}$ is not defined for $t = a_1$, therefore $|\frac{c_1}{t-a_1}|$, is not bounded as t varies in a neighborhood of a_1.

On the other hand the rational functions $\frac{c_i}{t-a_i}$ for $i \geq 2$ are all well defined at $t = a_1$, and hence their absolute values are bounded near a_1. Summarizing, in the last inequality near $t = a_1$ the left hand side is unbounded whereas the right hand side is bounded. This is a contradiction.

We have thus proved that $\mathcal{G}$ is a linearly independent uncountable subset in K. But this is impossible, as we observed already that the dimension of K as $\mathbb{C}$-vector space is at most countable. The claim is proved.

Therefore $\ker \pi_1$ is not zero, and hence, since $\mathbb{C}[x_1]$ is a PID, there exists a nonzero $f \in \mathbb{C}[x_1]$ such that $\ker \pi_1 = (f)$; we choose f monic of minimal degree.

As $\mathbb{C}$ is algebraically closed, there exists $a_1 \in \mathbb{C}$ such that $f = (x_1 - a_1)q$ with $q \in \mathbb{C}[x_1]$ and $\deg q < \deg f$. We have

$$0 = \pi_1(f) = \pi_1(x_1 - a_1)\pi_1(q).$$

As K is a field, at least one of the two factors on the right vanishes, i.e. lies in the kernel of π_1. By our choice of f the only possibility is $q = 1$ and $f = x_1 - a_1$.

We thus proved that $x_1 - a_1 \in \ker \pi_1 \subset \ker \pi = M$. Applying the same argument to the other variables we get that there exist $a_1, \dots, a_n$ in $\mathbb{C}$ such that the ideal $(x_1 - a_1, \dots, x_n - a_n)$ lies in M.

But we know that $(x_1 - a_1, \dots, x_n - a_n)$ is a maximal ideal, hence $(x_1 - a_1, \dots, x_n - a_n) = M$. The theorem is proved ■

Remark 2.4. The previous proof shows that $K = \mathbb{C}$ and $\pi = v_{\underline{a}}$.

3. Lecture 3

Let $X \subset \mathbb{A}^n$ be any subset. We can consider the set of polynomials that vanish at every point of X:

$$\mathcal{I}(X) := \{f \in \mathbb{C}[x_1, \dots, x_n] : \ f(p) = 0 \ \ \forall p \in X\}. \tag{5}$$

Remark 3.1. $\mathcal{I}(X)$ is an ideal of $\mathbb{C}[x_1, \dots, x_n]$ for any X.
If $X = \mathcal{Z}(T)$ then $T \subset \mathcal{I}(X)$.

If X is a point, say $X = \{(a_1, \dots, a_n)\}$, then we have

$$\mathcal{I}(X) = (x_1 - a_1, \dots, x_n - a_n)$$

and we already know that points are in bijective correspondence with maximal ideals in $\mathbb{C}[x_1, \dots, x_n]$. We now ask whether this is a special case of a more general phenomenon.

As we said, to every affine subset Z of $\mathbb{A}^n$ we can associate an ideal, $\mathcal{I}(Z)$. On the other hand an affine subset Z can be given by lots of different ideals, indeed we have for every $n \in \mathbb{N}$ and every ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$

$$\mathcal{Z}(I) = \mathcal{Z}(I^n).$$

We shall now show that $\mathcal{I}(Z)$ has an interesting poperty. namely it is a *radical ideal*.

First, for any ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ we can define its *radical* as follows

$$\sqrt{I} := \{f \in \mathbb{C}[x_1, \dots, x_n] : \ f^m \in I \text{ for some } \ m \in \mathbb{N}\}.$$

It is easy to check that $\sqrt{I}$ is an ideal and that $I \subset \sqrt{I}$. We say that I is a *radical ideal* if $\sqrt{I} = I$.

Lemma 3.2. *$\mathcal{I}(Z)$ is a radical ideal for any $Z \subset \mathbb{A}^n$.*

Proof. By what we said it is enough to show that $\sqrt{\mathcal{I}(Z)} \subset \mathcal{I}(Z)$. Let $f \in \sqrt{\mathcal{I}(Z)}$; then for some $m \in \mathbb{N}$ we have $f^m(p) = 0$ for every $p \in Z$. Hence we have, for every $p \in Z$,

$$0 = f^m(p) = f(p)^m,$$

and hence $f(p) = 0$ for every $p \in Z$. Therefore $f \in \mathcal{I}(Z)$. This shows that $\sqrt{\mathcal{I}(Z)} \subset \mathcal{I}(Z)$. ■

The following natural question comes up:

Question 1. *Let I_1 and I_2 be radical ideals in $\mathbb{C}[x_1, \ldots, x_n]$.*
If $\mathcal{Z}(I_1) = \mathcal{Z}(I_2)$ does it follow that $I_1 = I_2$?

So far we know that the answer is yes if I_1 and I_2 are maximal ideals. We shall now see that this is true in general.

Theorem 3.3 (Hilbert Nullstellensatz)**.** *Let $I \subset \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. If $f \in \mathbb{C}[x_1, \ldots, x_n]$ is such that $f(p) = 0$ for every $p \in \mathcal{Z}(I)$, then $f \in \sqrt{I}$.*
(In particular, the answer to Question 1 is yes.)

Proof. To prove the Theorem it suffices to prove the following

$$\mathcal{I}(\mathcal{Z}(I)) \subset \sqrt{I}.$$

Choose a finite set of generators for I,

$$I = (f_1 \ldots, f_r).$$

Now it suffices to show that if $g \in \mathbb{C}[x_1, \ldots, x_n]$ vanishes at every point p such that $f_1(p) = \ldots f_r(p) = 0$, then there exists $d \in N$ such that $g^d \in I$.

Consider the polynomial ring in $r+1$ variables, written $\mathbb{C}[x_1, \ldots, x_n, y]$, and the polynomial

$$\ell(x_1, \ldots, x_n, y) := g(x_1, \ldots, x_n,)y - 1 \in \mathbb{C}[x_1, \ldots, x_n, y].$$

The polynomial ℓ does not vanish whenever g vanishes, of course. Therefore in $\mathbb{C}^{n+1}$ the polynomials $f_1, \ldots, f_r, \ell$ have no common zeroes. By the following Lemma 3.4 this implies that there exist polynomials $h_1, \ldots, h_{r+1}$ in $C[x_1, \ldots, x_n, y]$ such that

$$1 = \sum_{i=1}^{r} h_1 f_1 + h_{r+1}\ell.$$

In the above identity the variable y appears in the polynomials ℓ and in h_i for $i = 1 \ldots, r+1$. Noticing that

$$\ell(x_1, \ldots, x_n, \frac{1}{g(x_1, \ldots, x_n)}) = 0$$

by substituing $y = \frac{1}{g(x_1,\ldots,x_n)}$ we get

$$1 = \sum_{i=1}^{r} h_1(x_1, \ldots, x_n, \frac{1}{g(x_1, \ldots, x_n)})f(x_1, \ldots, x_n).$$

This is an identy of rational functions in $x_1, \ldots, x_n$, whose common denominator has the form $g(x_1, \ldots, x_n)^d$ for some non-negative integer d. Multiplying both members by g^d we get

$$g^d = \sum_{1}^{r} k_i f_i$$

with $k_i \in \mathbb{C}[x_1, \ldots, x_n]$. Hence $g \in (f_1, \ldots, f_n)$; the theorem is proved. ■

For the proof we used the following Lemma, which is a simple consequence of the Weak Nullstellensatz.

Lemma 3.4. *Let* $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$.

$$\mathcal{Z}(f_1, \ldots, f_s) = \emptyset \iff \exists\, h_1, \ldots, h_s \in \mathbb{C}[x_1, \ldots, x_n] : \sum_{i=1}^{s} h_i f_i = 1$$

Proof. By the various definitions we have, for any $p \in \mathbb{C}^n$,

$$p \in \mathcal{Z}(f_1, \ldots, f_s) \iff f_i \in \mathcal{I}(p),\ \forall i = 1, \ldots, s.$$

Therefore $\mathcal{Z}(f_1, \ldots, f_s) = \emptyset$ if and only if the ideal $(f_1, \ldots, f_s)$ is not contained in any ideal of type $\mathcal{I}(p)$. By Theorem 2.3 this is equivalent to saying that $(f_1, \ldots, f_s)$ is not contained in any maximal ideal of $\mathbb{C}[x_1, \ldots, x_n]$. By Fact 2.1 this is equivalent to $(f_1, \ldots, f_s) = (1)$. The Lemma is proved. ■

Corollary 3.5. $\sqrt{I} = \mathcal{I}(Z(I))$

Proof. We must show that $\sqrt{I} \subset \mathcal{I}(Z(I))$. Of course, $I \subset \mathcal{I}(Z(I))$. As $\mathcal{I}(Z(I))$ is a radical ideal (Lemma 3.2) it contains the radical of I. ■