Systems of Algebraic Equations

MTH437 — Introduction to Schemes

Kapil Hari Paranjape

IISER Mohali

9th September 2021

Recall

Finding configurations of linear subspaces in projective space that have certain kinds of incidence corresponds to solving "systems of algebraic equations".

What are systems of algebraic equations?

To begin with let us try to understand a *single* algebraic equation.

Polynomials

We start with a collection $(x_1, \ldots, x_p)$ of *variables*.

We then form *monomials* $x_1^{k_1} \cdots x_p^{k_p}$ where $(k_1, \ldots, k_p)$ are non-negative integers.

We form *terms* $a_{k_1,\ldots,k_p} x_1^{k_1} \cdots x_p^{k_p}$ where the *coefficients* $a_{k_1,\ldots,k_p}$ lie in some field F.

We now create a *polynomial* as a sum of *finitely* many terms:

$$f(x_1, \ldots, x_p) = \sum_{(0 \leq k_i \leq d_i)_{i=1,\ldots,p}} a_{k_1,\ldots,k_p} x_1^{k_1} \ldots x_p^{k_p}$$

An algebraic equation is of the form $f(x_1, \ldots, x_p) = 0$.

The coefficients are *given* elements of the field F, even if notationally they appear similar to variables!

Semi-group ring

Applying "Occam's razor" to remove unnecessary notation, a monomial is just $(k_1, \ldots, k_p)$ which is an element of $\mathbb{W}^p$, where $\mathbb{W}$ is the collection of non-negative integers.

Note that multiplication of monomials is the same as addition in $\mathbb{W}^p$ as a semi-group.

$$(x_1^{k_1} \cdots x_p^{k_p}) \cdot (x_1^{m_1} \cdots x_p^{m_p}) = x_1^{k_1+m_1} \cdots x_p^{k_p+m_p}$$

It follows that a polynomial is a finite linear combination of elements of this semi-group with coefficients in the field F.

This is *sometimes* a useful way to understand polynomials—in computer implementations as well as in algebraic geometry!

Compact notation

In any case, it is convenient to introduce the notation $\mathbf{k} = (k_1, \ldots, k_p)$ and

$$\mathbf{x}^{\mathbf{k}} = x_1^{k_1} \cdots x_p^{k_p}$$

for a monomial.

We note that $\mathbf{x}^{\mathbf{k}} \cdot \mathbf{x}^{\mathbf{m}} = \mathbf{x}^{\mathbf{k}+\mathbf{m}}$.

We then define $|\mathbf{k}| = \sum_{i=1}^{p} k_p$ as the *total degree* of this monomial.

We now have the compact notation $f(\mathbf{x}) = \sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}}$ for a polynomial with total degree at most d.

Coefficients

The field F contains a *prime* subfield $\mathbb{F}$, which is either a finite field $\mathbb{F}_p$ of order a prime p, or the field $\mathbb{Q}$ of rational numbers.

The polynomial f uses *finitely* many elements of the field F as coefficients.

Hence, these coefficients lie in a *finitely generated* field

$$E_f = \mathbb{F}\left((a_{\mathbf{k}})_{|\mathbf{k}|\leq d}\right)$$

Claim: By introducing more variables and more equations, we can reduce to the case when the coefficients lie in the prime field $\mathbb{F}$, or even $\mathbb{Z}$, the ring of integers.

Algebraic and Transcendental elements.

Given a subfield E of a field F and an element a of F, there is a natural homomorphism $e_a : E[x] \to F$ which maps x to a; here $E[x]$ denotes the polynomial ring in one variable over E.

Since F is a domain, the kernel of e_a is a prime ideal.

Thus, there are two cases:

- Either the kernel of e_a is $\{0\}$, or
- The kernel of e_a is generated by a monic irreducible polynomial $x^d + b_1x^{d-1} + \cdots + b_d$, with $b_1, \ldots, b_d$ in the field E.

Transcendental case

In the first case, we say that a is *transcendental* over E.

In this case, the above map *extends* to a field inclusion $E(x) \to F$; here $E(x)$ denotes the field of fractions of $E[x]$ which is the field of rational functions in one variable x over E.

The image is precisely $E(a)$, the subfield of F generated by a and E.

In other words, $E(x)$ and $E(a)$ are *isomorphic*.

Algebraic Case

In the second case, we say that a is *algebraic* over E.

In this case, the image $E[a]$ of e_a is a field.

Hence, $E[a]$ is the same as the subfield $E(a)$ of F generated by a over E.

General case

Working inductively over finitely many elements $a_1, \ldots, a_d$ of F, we see that we can *re-order* them so that $E(a_1, \ldots, a_d)$ is of the form $E(b_1, \ldots, b_t)[c_1, \ldots, c_u]$ where:

- b_i is transcendental over $E(b_1, \ldots . b_{i-1})$, and
- c_j is algebraic over $E(b_1, \ldots, b_t)[c_1, \ldots, c_{j-1}]$.

Here $b_i = a_{\sigma(i)}$ and $c_j = a_{\sigma(t+j)}$ for some permutation σ of $1, \ldots, d$.

Re-writing a polynomial

We apply this to the coefficients $(a_{\mathbf{k}})_{|\mathbf{k}|\leq d}$ that occur on our polynomial

There is a re-arrangement of this into a $b_1, \ldots, b_t$ and $c_1, \ldots, c_u$.

- For each $i = 1, \ldots, t$ there is a $\mathbf{k}_i$ in $\mathbb{W}^p$ so that $b_i = a_{\mathbf{k_i}}$.
- For each $j = 1, \ldots, u$ there is a $\mathbf{m}_j$ in $\mathbb{W}$ˆp\$ so that $c_j = a_{\mathbf{m}_j}$.

This, allows us to write the original polynomial equation in the more compact form

$$f(\mathbf{x}) = \sum_{i=1}^{t} b_i \mathbf{x}^{\mathbf{k}_i} + \sum_{j=1}^{u} c_j \mathbf{x}^{\mathbf{m}_j}$$

where:

- b_i is transcendental over the field $\mathbf{F}(b_1, \ldots, b_{i-1})$.
- c_j is algebraic over the field $\mathbf{F}(b_1, \ldots, b_t)[c_1, \ldots, c_{j-1}]$.

System of equations

We now apply the above discussion to a *system* of equations.

$$\sum_{\mathbf{k} \leq d_1} a_{1,\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0$$
$$\vdots$$
$$\sum_{\mathbf{k} \leq d_q} a_{q,\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0$$

There are finitely many coefficients a's which lie in the field F.

As above we organise these coefficients to re-write the equations:

$$\sum_{i=1}^{t_1} b_i \mathbf{x}^{\mathbf{k}} + \sum_{j=1}^{u_1} c_j \mathbf{x}^{\mathbf{k}} = 0$$

$$\vdots$$

$$\sum_{i=t_{q-1}}^{t} b_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_{q-1}}^{u} c_j \mathbf{x}^{\mathbf{k}} = 0$$

where:

- b_i is transcendental over the field $\mathbf{F}(b_1, \ldots, b_{i-1})$.
- c_j is algebraic over the field $\mathbf{F}(b_1, \ldots, b_t)[c_1, \ldots, c_{j-1}]$.

Adding new variables

Since the b_i's are transcendental over the field $\mathbf{F}$ we can think of them as "variables".

So we introduce the notation y_i in place of b_i (to remind us that these are variables!) and write our equations as:

$$\sum_{i=1}^{t_1} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=1}^{u_1} c_j \mathbf{x}^{\mathbf{k}} = 0$$

$$\vdots$$

$$\sum_{i=t_{q-1}}^{t} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_{q-1}}^{u} c_j \mathbf{x}^{\mathbf{k}} = 0$$

Now c_j satisfies an equation of the form

$$x^{d_j} + g_{j,1}x^{d_j-1} + \cdots + g_{j,d_j} = 0$$

where $g_{j,s}$ are elements of the field $\mathbf{F}(y_1, \ldots, y_t)[c_1, \ldots, c_{j-1}]$.

We can introduce *additional* variables $z_1, \ldots, z_u$ in place of c_i's and *add* the equations

$$z_j^{d_j} + g_{j,1}z_j^{d_j-1} + \cdots + g_{j,d_j} = 0$$

to our system of equations!

However, $g_{j,s}$ are *rational* functions of $y_1, \ldots, y_t$.

However, there are finitely many coefficients. So we can clear denominators!

$$h_{j,0}z_j^{d_j} + h_{j,1}z_j^{d_j-1} + \cdots + h_{j,d_j} = 0$$

where $h_{j,s}$ are in the ring $\mathbb{F}[y_1, \ldots, y_t][c_1, \ldots, c_{j-1}]$.

Here we have, $g_{j,s} = h_{j,s}/h_{j,0}$. So we need need $h_{j,0}$ to be invertible.

To do so, we introduce a new variable w_j and add the equation $w_j h_{i,0} - 1 = 0$.

This gives us the combined system of equations:

$$\sum_{i=1}^{t_1} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=1}^{u_1} z_j \mathbf{x}^{\mathbf{k}} = 0$$

$$\vdots$$

$$\sum_{i=t_{q-1}}^{t} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_{q-1}}^{u} z_j \mathbf{x}^{\mathbf{k}} = 0$$

$$h_{1,0} z_1^{d_1} + h_{1,1} z_1^{d_1 - 1} + \cdots + h_{1,d_1} = 0 \text{ and } h_{1,0} w_1 - 1 = 0$$

$$\vdots$$

$$h_{t,0} z_u^{d_u} + h_{u,1} z_u^{d_u - 1} + \cdots + h_{u,d_u} = 0 \text{ and } h_{2,u} w_u - 1 = 0$$

all of which have coefficients in the prime field $\mathbb{F}$. Here w's, x's, y's and z's are variables.

Conclusion

In summary, we can reduce to a *system* of polynomial equations in the variables $x_1, \ldots, x_p$ with coefficients in the prime field $\mathbb{F}$.

$$\left(\sum_{\mathbf{k} \leq d_1} a_{1,\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0 \right)_{i=1,\ldots,q}$$

In fact, if the prime field in $\mathbb{Q}$, then we can even assume that the coefficients are in the ring of integers $\mathbb{Z}$ by clearing denominators as above.

Similarly, equations with coefficients in the field $\mathbb{F}_p$ can be seen as equations with integer coefficients, by "lifting" the elements of $\mathbb{F}_p$ to integers!

We can *add* the somewhat strange equation $p = 0$ to ensure that integers are only considered modulo p.

Affine schemes

$\mathbf{Z}$-affine scheme: A $\mathbf{Z}$-*affine scheme* is of the form $A(x_1, \ldots, x_p; f_1, \cdots, f_q)$ where $f_1, \ldots, f_q$ are polynomials in the variables $x_1, \ldots, x_p$ with coefficients in the ring of integers.

Note that the $A()$ notation is a symbol to denote that we are looking at the affine scheme associated with this system of equations.

So far this "definition" is therefore just an introduction of notation!

Observe also that there are countably many affine schemes since the x_i's are "dummy" variables.