Affine Schemes

We wish to understand the solutions of systems of algebraic equations. To do so we must look for the most *general* form of such equations that we may encounter.

Algebraic equations

What is an algebraic equation?

We have 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*

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

as a sum of *finitely* many terms. Then $f(x_1, \ldots, x_p) = 0$ is an algebraic equation. (Note: The coefficients are *given* elements of the field F, even if notationally they appear similar to variables!)

Semi-group ring

If one applies "Occam's razor" to remove inessential aspects of the notation, then one can think of a monomial as $(k_1, \ldots, k_p)$ which is an element of the semi-group $\mathbb{W}^p$, where $\mathbb{W}$ is the collection of non-negative integers.

Note that multiplication of monomials is the same as addition in this 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!

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 can loosely think of this as the $\daleth$-th (multi-)power of the "vector" $\mathbf{x} = (x_1, \ldots, x_p)$. We then define $|\mathbf{k}| = \sum_{i=1}^{p} k_p$ as the *total degree* of a monomial.

This allows us to use 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.

Field of 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

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

We need to see what such fields look like.

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, either it is $\{0\}$ or it 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.

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*.

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.

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 $1, \ldots, d$.

Application to the field of coefficients

We can apply this to the field E_f to identify it with $\mathbb{F}(b_1, \ldots, b_t)[c_1, \ldots, c_u]$ where the b_i and c_j are the coefficients $a_{\mathbf{k}}$'s of the polynomial f re-arranged in some fashion.

For $i = 1, \ldots, t$, let $\mathbf{k}_i$ be the element of $\mathbb{W}^p$ so that one term of $f(\mathbf{x})$ is $b_i\mathbf{x}^{\mathbf{k}_i}$. Similarly, for $j = 1, \ldots, u$ let $\mathbf{m}_j$ be the element of $\mathbb{W}^d$ so that one term of $f(\mathbf{x})$

is $c_j \mathbf{x}^{\mathbf{m}_j}$. 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 consider a *system* of polynomial equations in the variables $x_1, \ldots, x_p$ with coefficients in a field F.

$$\begin{gathered}
\sum_{\mathbf{k} \leq d_1} a_{1,\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0 \\
\sum_{\mathbf{k} \leq d_2} a_{2,\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0 \\
\vdots \\
\sum_{\mathbf{k} \leq d_q} a_{q,\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0
\end{gathered}$$

The collection of all coefficients is finite. Hence the field generated by them over the prime field $\mathbb{F}$ is finitely generated. We can now organise these coefficients as above to re-write the equations in the form:

$$\begin{gathered}
\sum_{i=1}^{t_1} b_i \mathbf{x}^{\mathbf{k}} + \sum_{j=1}^{u_1} c_j \mathbf{x}^{\mathbf{k}} = 0 \\
\sum_{i=t_1}^{t_2} b_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_1}^{u_2} c_j \mathbf{x}^{\mathbf{k}} = 0 \\
\vdots \\
\sum_{i=t_{q-1}}^{t} b_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_{q-1}}^{u} c_j \mathbf{x}^{\mathbf{k}} = 0
\end{gathered}$$

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:

$$
\begin{aligned}
\sum_{i=1}^{t_1} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=1}^{u_1} c_j \mathbf{x}^{\mathbf{k}} &= 0 \\
\sum_{i=t_1}^{t_2} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_1}^{u_2} c_j \mathbf{x}^{\mathbf{k}} &= 0 \\
&\vdots \\
\sum_{i=t_{q-1}}^{t} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_{q-1}}^{u} c_j \mathbf{x}^{\mathbf{k}} &= 0
\end{aligned}
$$

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 not polynomials! We now resolve that issue.

Clearing denominators

Given a polynomial equation $\sum_{|\mathbf{k}| \leq d} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0$ where the coefficients a_k are in the field F of fractions of a domain R.

It follows that $a_{\mathbf{k}} = b_{\mathbf{k}} / c_{\mathbf{k}}$ where $b_{\mathbf{k}}$ and $c_{\mathbf{k}}$ lie in R. Since there are only finitely many $\mathbf{k}$ involved, we can replace $c_{\mathbf{k}}$ by the product of all $c_{\mathbf{k}}$'s to write $a_{\mathbf{k}} = b_{\mathbf{k}} / c$ for a common denominator c in R.

By clearing denominators, we see that the above equation is the same as the equation $\sum_{|\mathbf{k}| \leq d} b_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0$.

However, we need to *ensure* that c is invertible as well. To do so, we add another variable w and add the equation $cw - 1 = 0$. The *pair* of equations

$$cw - 1 = 0 \text{ and } \sum_{|\mathbf{k}| \leq d} b_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} = 0$$

replaces the above single equation over F with a system of equations over R.

Equations with integer coefficients

We now apply this discussion to the equations:

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

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

By clearing denominators, we can replace these by pairs of equations of the form

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

where $h_{j,k}$ are elements of the *ring* $\mathbf{F}[y_1, \ldots, y_t][c_1, \ldots, c_{j-1}]$ such that $g_{j,k} = h_{j,k}/h_{j,0}$.

Note that this equation is satisfied by c_j.

For each r and s, let $f_{r,s}$ denote the polynomial obtained by replacing c_j by z_j in the polynomial $h_{r,s}$.

So we *add* the above equations with b_i replaced by new variables y_i, and c_j replaced by z_i to obtain a *combined* system:

$$\begin{aligned}
\sum_{i=1}^{t_1} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=1}^{u_1} z_j \mathbf{x}^{\mathbf{k}} &= 0 \\
\sum_{i=t_1}^{t_2} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_1}^{u_2} z_j \mathbf{x}^{\mathbf{k}} &= 0 \\
&\vdots \\
\sum_{i=t_{q-1}}^{t} y_i \mathbf{x}^{\mathbf{k}} + \sum_{j=u_{q-1}}^{u} z_j \mathbf{x}^{\mathbf{k}} &= 0 \\
f_{1,0} z_1^{d_1} + f_{1,1} z_1^{d_1 - 1} + \cdots + f_{1,d_1} &= 0 \text{ and } f_{1,0} w_1 - 1 = 0 \\
f_{2,0} z_2^{d_2} + f_{2,1} z_2^{d_2 - 1} + \cdots + f_{2,d_2} &= 0 \text{ and } f_{2,0} w_2 - 1 = 0 \\
&\vdots \\
f_{t,0} z_u^{d_u} + f_{u,1} z_u^{d_u - 1} + \cdots + f_{u,d_u} &= 0 \text{ and } f_{2,u} w_u - 1 = 0
\end{aligned}$$

where the variables are the x's, y's and z's. This entire system of equations has coefficients in the prime field $\mathbb{F}$.

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.

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. In order to ensure that we only look at "integers mod p" we can add the equation $p = 0$!

In summary, the most general system of equations that we want to solve is of the form

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

where the coefficients $a_{i,\mathbf{k}}$ are *integers*.

(Perhaps this explains why number theory plays such an important role in algebraic geometry!)

$\mathbb{Z}$-affine schemes

$\mathbb{Z}$-affine scheme: A *$\mathbb{Z}$-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 $\mathbb{Z}$ 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!

Since the variables x_i are "dummy" variables which can be eliminated by using the semi-group ring of monomials, we see that such a system of equations is *determined* by the coefficients. This is a collection of integers indexed by a finite subset of $\cup_{p\geq 0}(\mathbb{N}\times\mathbb{W}^p)$. As a consequence, there are only *countably many* $\mathbb{Z}$-affine schemes.

Note that, in the definition, we *could* have used *any* commutative ring R in place of $\mathbb{Z}$ to get a definition of R-affine schemes. (Moreover one *could* allow for infinitely many equations in that case.)

R-points

Given a polynomial $f(x_1, \ldots, x_p)$ with integer coefficients and elements $a_1, \ldots, a_p$ of a commutative ring R, we can *evaluate* $f(a_1, \ldots, a_p)$ to see whether it is 0.

Given a $\mathbb{Z}$-affine scheme $X = A(x_1, \ldots, x_p; f_1, \ldots, f_q)$ and a commutative ring R, we define

$$X(R) = \left\{ (a_1, \ldots, a_p) \;\middle|\; f_1(a_1, \ldots, a_p) = \cdots = f_q(a_1, \ldots, a_p) = 0 \right\}$$

Such a solution in R is also called an R-point of X. This means $X(R)$ is the collection of R-points of X.

Note that it *is* necessary for R to be commutative in order to make sense of $f(a_1, \ldots, a_r)$.

Evaluation map

Given a commutative ring R, and elements $a_1, \ldots, a_p$ in R, the evaluation of polynomials at $\mathbf{a} = (a_1, \ldots, a_p)$ is the *same* as a ring homomorphism:

$$e_{\mathbf{a}} : \mathbb{Z}[x_1, \ldots, x_p] \to R \text{ such that } x_i \mapsto a_i \text{ for } i = 1, \ldots, p$$

The condition $f(a_1, \ldots, a_p) = 0$ becomes $e_{\mathbf{a}}(f(x_1, \ldots, x_p)) = 0$.

It follows that $X(R)$ consists of $(a_1, \ldots, a_p)$ such that $f_i(x_1, \ldots, x_p)$ lie in the kernel of $e_{\mathbf{a}}$ for $i = 1, \ldots, q$. In other words,

$$X(R) = \left\{ (a_1, \ldots, a_p) \;\middle|\; f_i \in \ker(e_{\mathbf{a}}) \text{ for } i = 1, \ldots, q \right\}$$

Note that $\ker(e_{\mathbf{a}})$ is an *ideal* in $\mathbb{Z}[x_1, \ldots, x_p]$. If $\langle f_1, \ldots, f_q \rangle$ denotes the ideal in $\mathbb{Z}[x_1, \ldots, x_p]$ generated by $f_1, \ldots, f_q$, then we see that the above condition on $\mathbf{a}$ becomes $\langle f_1, \ldots, f_q \rangle \subset \ker(e_{\mathbf{a}})$. Now, Noether's isomorphism theorem says that

$$X(R) = \mathrm{Hom}\left(\frac{\mathbb{Z}[x_1, \ldots, x_p]}{\langle f_1, \ldots, f_q \rangle}, R \right)$$

where Hom indicates *ring* homomorphisms. It is thus natural to introduce the ring:

$$\mathcal{O}(X) = \frac{\mathbb{Z}[x_1, \ldots, x_p]}{\langle f_1, \ldots, f_q \rangle},$$

which is naturally associated with the affine scheme $X = A(x_1, \ldots, x_p; f_1, \ldots, f_q)$. We then get

$$X(R) = \mathrm{Hom}\left(\mathcal{O}(X), R \right)$$

in terms of ring homomorphisms.

Solutions in finite rings

One important example of the above is when the commutative ring is taken to be a finite field $\mathbb{F}_q$.

Now $\mathbb{F}_q$ is an r-dimensional vector space over $\mathbb{F}_p$ for the prime p such that $q = p^r$. It follows that $\mathbb{F}_q$ can be identified as a sub-ring of the matrix ring $M_r(\mathbb{F}_p)$. In particular, $\mathbf{a} = (a_1, \ldots, a_p)$ can be identified with a p-tuple of *commuting* matrices in $M_r(\mathbb{F}_p)$.

Thus, we can *generalise* this and look for p-tuples $(a_1, \ldots, a_p)$ of commuting matrices over $\mathbb{F}_p$ that satisfy the given equations. Note that it is *necessary* for the matrices to commute in order to make sense of $f(a_1, \ldots, a_p)$ for a polynomial $f(x_1, \ldots, x_p)$ in $\mathbb{Z}[x_1, \ldots, x_p]$.

Note that it is *not* necessary that a commutative subring of $M_r(\mathbb{F}_p)$ is a field. For example, we have the ring

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{F}_p \right\}$$

which contains non-zero nilpotent matrices. However, $M_r(\mathbb{F}_p)$ is a *finite* ring and so the image of $e_{\mathbf{a}}$ is a finite commutative ring.

We can therefore generalise *further* and look at the collection $X(A)$ of solutions in a finite commutative ring A.

Parametric solutions

We have the well-known parametric solution:

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

of the equation $x^2 + y^2 = 1$.

In terms of the above definitions, we see that $X = A(x, y; x^2 + y^2 - 1)$ is an affine scheme. We then consider the field $\mathbb{Q}(t)$ and observe that

$$\mathbf{a} = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \in X(\mathbb{Q}(t))$$

There is a natural inclusion of the ring $S = \mathbb{Z}[t, w]/\langle w(t^2+1) - 1\rangle$ in $\mathbb{Q}(t)$ by sending t to itself and w to $1/(t^2+1)$. Moreover, we see that $\mathbf{a}$ can be seen as $(w(1-t^2), 2wt)$ in $X(S)$.

Further observe that $S = \mathcal{O}(Y)$, where $Y = A(w, t; w(t^2+1) - 1)$.

Composite homomorphisms and solutions

We generalise from the above example to consider two affine schemes X and Y and a point $\mathbf{f}$ in $X(\mathcal{O}(Y))$. As seen above this corresponds to a ring homomorphism

$$e_{\mathbf{f}} : \mathcal{O}(X) \to \mathcal{O}(Y)$$

In particular, note that the *identity* map $\mathcal{O}(X) \to \mathcal{O}(X)$ gives a special point $i_X \in X(\mathcal{O}(X))$.

Given *any* ring R, a point $\mathbf{a}$ in $Y(R)$ corresponds to a ring homomorphism $e_{\mathbf{a}} : \mathcal{O}(Y) \to R$. We thus obtain a composite homomorphism

$$\mathcal{O}(X) \stackrel{e_{\mathbf{f}}}{\to} \mathcal{O}(Y) \stackrel{e_{\mathbf{a}}}{\to} R$$

This composite homomorphism corresponds to a point in $X(R)$. We thus have a map $Y(R) \to X(R)$ given by $\mathbf{a} \mapsto \mathbf{b}$ where we have the equality

$$e_{\mathbf{b}} = e_{\mathbf{a}} \circ e_{\mathbf{f}}$$

Let us denote this map as $\mathbf{f}(R) : Y(R) \to X(R)$ since it only depends on $\mathbf{f} \in X(\mathcal{O}(Y))$ and R.

Morphisms of affine schemes

What are the properties that we would want from a geometric map $f : X \to Y$ between affine schemes?

At the very least, given an element $\mathbf{a}$ in $X(R)$, we should be able to talk about its *image* $f(\mathbf{a})$ in $Y(R)$. In other words, there should be an *induced* map $f(R) : X(R) \to Y(R)$.

Applying this to the element i_X in $X(\mathcal{O}(X))$ we see that $f(i_X)$ is an element of $Y(\mathcal{O}(X))$.

We have seen above that an element $\mathbf{f}$ in $Y(\mathcal{O}(X))$ corresponds to a ring homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$. Given an element $\mathbf{a}$ in $X(R)$, we have seen above that this gives, by composition an element $\mathbf{b}$ in $Y(R)$.

We thus, see that it is *natural* to define geometric maps (morphisms) of affine schemes as follows.

Morphism of affine schemes: A morphism $f : X \to Y$ is an $\mathcal{O}(X)$-point f of Y. In other words, f is an element of $Y(\mathcal{O}(X))$.

Equivalently, we have

$$\mathrm{Mor}(X, Y) = \mathrm{Hom}(\mathcal{O}(Y), \mathcal{O}(X))$$

where the latter is the collection of ring homomorphisms.

Polynomial substitutions

We can also understand the above definition in more "classical" terms as follows.

Suppose $X = A(x_1, \dots, x_p; f_1, \dots, f_q)$ and $Y = A(y_1, \dots, y_u; g_1, \dots, g_v)$.

We can think of a polynomial map $h : X \to Y$ as one given by a u-tuple of polynomial functions $(h_1(\mathbf{x}), \dots, h_u(\mathbf{x}))$ such that we can *substitute* $y_j = h_j(\mathbf{x})$ for $j = 1, \dots, u$ to *automatically* satisfy $g_s(\mathbf{y}) = 0$ for $s = 1, \dots, q$, *whenever* $f_t(\mathbf{x}) = 0$ are satisfied.

We see that this means that h corresponds to a ring homomorphism

$$\mathbb{Z}[y_1, \dots, y_u] \to \mathbb{Z}[x_1, \dots, x_p] \text{ given by } y_j \mapsto h_j(\mathbf{x})$$

Note that $g_s(y_1, \dots, y_u) \mapsto g_s(h_1(\mathbf{x}), \dots, h_u(\mathbf{x}))$ under this homomorphism. The previous condition is thus that the image of the ideal $\langle g_1, \dots, g_v \rangle$ under this ring homomorphism is *contained* in the ideal $\langle f_1, \dots, f_q \rangle$.

It is not difficult to check that this is the same as a ring homomorphism $\mathcal{O}(Y) \to \mathcal{O}(X)$ as considered above.