Affine Schemes

MTH437 — Introduction to Schemes

Kapil Hari Paranjape

IISER Mohali

13th September 2021

Recall

The most general form of a system of algebraic equations is

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

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

$\mathbb{Z}$-**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.

We note that this is (at this moment) just notation or terminology. The x_i are "dummy" variables.

As a result the collection of $\mathbb{Z}$-affine schemes is countable.

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

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

A solution $\mathbf{a} = (a_1, \ldots, a_p)$ in R is also called an R-point of X. So $X(R)$ 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 $\mathbb{Z}[x_1, \ldots, x_p]$.

Let $\langle f_1, \ldots, f_q \rangle$ denote the ideal in $\mathbb{Z}[x_1, \ldots, x_p]$ generated by $f_1, \ldots, f_q$.

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.

Co-ordinate ring

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

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

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.

Example of Parametric solution

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

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

The ring $S = \mathbb{Z}[t, w]/\langle w(t^2 + 1) - 1\rangle$ can be seen as a subring of $\mathbb{Q}(t)$ by sending t to itself and w to $1/(t^2 + 1)$.

Moreover, $\mathbf{a}$ can be seen as $(w(1 - t^2), 2wt)$ in $X(S) \subset X(\mathbb{Q}(t))$.

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.

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

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

A polynomial substitution h corresponds to a ring homomorphism

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

Note that $g_s(y_1, \ldots, y_u) \mapsto g_s(h_1(\mathbf{x}), \ldots, h_u(\mathbf{x}))$ under this homomorphism.

The previous condition is thus that the image of the ideal $\langle g_1, \ldots, g_v \rangle$ under this ring homomorphism is *contained* in the ideal $\langle f_1, \ldots, f_q \rangle$.

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.