Some Notes on Algebraic Maps, Elliptic Curves and Isogenies

Simon Pohmann

November 24, 2021

Contents

1 Maps on varieties

1.1 Algebraic maps

First of all, we define the basic notions of algebraic maps, that is maps that are locally defined by polynomials. For simplicity of notation, we already introduce the projective coordinate ring before.

Definition 1.1. Let $X \subseteq \mathbb{P}^n$ be a projective variety. Then the graded ring $S(X) := k[x_0, ..., x_n]/\mathbb{I}(X)$ is its projective coordinate ring.

Note that the graded ring is not invariant under isomorphisms of projective varieties.

Definition 1.2. Let $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$ be quasi-projective varieties, i.e. open subsets of the projective varieties $\bar{X}, \bar{Y}$. Then define

- A map $X \to Y$ is called *morphism*, if it is given locally by polynomials, so for each $p \in X$ there is an open neighborhood U of p and homogeneous polynomials $f_0, ..., f_m \in S(\bar{X})$ of same degree such that

$$(f_0(a), ..., f_m(a)) \neq 0 \text{ and } f(a) = [f_0(a) : ... : f_m(a)] \text{ for all } a \in U$$

- A map $X \to k$ is called *regular* at $p \in X$, if it is given by polynomials near p, i.e. there is an open neighborhood U of p such that the restriction $U \to k$ is a morphism. Denote the regular maps on X by $\mathcal{O}_{\bar{X}}(X)$. We remark that this is a k-algebra.
- A partial map $X \dashrightarrow Y$ on an irreducible quasi-projective variety X is called *rational*, if its domain is an open subset $U \subseteq X$ and it is a morphism $U \to Y$. We identify rational maps $f, g : X \dashrightarrow Y$ defined on $U, V \subseteq X$ if $f|_{U \cap V} = g|_{U \cap V}$. In other words, regular maps are morphisms $U \to Y$ with maximal domain $U \subseteq X$ open.

In particular, morphisms, rational maps and regular maps are technically all the same thing. The definitions just differ in the domain and the codomain, not in the key property "locally defined by polynomials". However, they are usually used in a different way. One often works with morphisms between varieties of the same type (e.g. morphisms between projective varieties), and then they differ fundamentally from regular maps (we only have the above equivalence by taking $Y = k$ to be an affine variety).

1.2 The coordinate rings

We have already introduced the projective coordinate ring, which is a not totally natural object, because it is not invariant under isomorphisms. Affine varieties have a much nicer coordinate ring.

Definition 1.3. For an affine variety $X \subseteq \mathbb{A}^n$, define the affine coordinate ring $k[X] := k[x_1, ..., x_n]/\mathbb{I}(X)$.

This ring has a much tighter connection to the variety.

Theorem 1.4. *Let $\mathcal{V}$ be the category of affine varieties $\subseteq \mathbb{A}^n_k$ with affine morphisms, and $\mathcal{A}$ the category of finitely generated, reduced (commutative, unital) k-algebras. Then*

$$\Phi : \mathcal{V}^{\mathrm{op}} \to \mathcal{A}, \quad V \mapsto k[V], \ \phi \mapsto \phi^*$$

is an equivalence of categories.

Further, each affine and projective (and even quasi-projective) variety has a function field.

Definition 1.5. For an affine variety $X \subseteq \mathbb{A}^n$, define the *function field* as the field of fractions $k(X) := \mathrm{Frac}(k[X])$. For a projective variety $X \subseteq \mathbb{P}^n$, define the *function field* as

$$k(X) := \{f/g \in \mathrm{Frac}(S(X)) \mid f, g \text{ homogeneous polynomials of same degree}\}$$

Note that we can evaluate an element $\frac{f}{g} \in k(X)$ at all points $a \in X \setminus \mathbb{V}(g)$ and get a well-defined value in k. To get the function field of an arbitrary quasi-projective variety, one can define it as the function field of an affine chart. We will not pursue that path further. However, the following lemma is important.

Lemma 1.6. *Let $X \subseteq \mathbb{P}^n$ be a projective variety. Then for all embeddings $\mathbb{A}^n \subseteq \mathbb{P}^n$ get*

$$k(X \cap \mathbb{A}^n) \cong k(X) \quad via \quad \frac{f}{g} \mapsto \frac{x_0^d f(x_1/x_0, ..., x_n/x_0)}{x_0^d g(x_1/x_0, ..., x_n/x_0)},\ d = \max\{\deg f, \deg g\}$$

Further, find that $k(X)$ is invariant under isomorphisms. If the embedding $\mathbb{A}^n \subseteq \mathbb{P}^n$ is clear, we will sometimes identify both fields.

Hence, the function field is again a natural property of varieties.

1.3 The connection between them

The function field is more or less equal to all regular maps defined on *some* open subset of X. Namely

Proposition 1.7. *Let $X \subseteq \mathbb{P}^n$ be an irreducible projective variety. Have a well-defined and injective k-algebra homomorphism*

$$\mathcal{O}_X(U) \to k(X), \quad f : U \to k \text{ defined locally at } p \in U \text{ by } f = g/h \ \mapsto \ \frac{g}{h}$$

Further, this is in some sense surjective, meaning that for each $f \in k(X)$ there is some open $U \subseteq X$ such that f is contained in the image of $\mathcal{O}_X(U) \to k(X)$.

If we only consider regular maps that are defined on the whole of X, we get the following statement.

Theorem 1.8. *If $X \subseteq \mathbb{P}^n$ is a projective variety, find $\mathcal{O}_X(X) \cong k$. If $X \subseteq \mathbb{A}^n$ is an affine variety, find $\mathcal{O}_X(X) \cong k[X]$.*

Proof. Consider the map

$$k[X] \to \mathcal{O}_X(X), \quad f \mapsto (a \mapsto f(a))$$

which is clearly a well-defined, injective k-algebra homomorphism. So for the second part, it is left to show that it is surjective.

Let $f \in \mathcal{O}_X(X)$. Then for each $p \in X$ there is an open neighborhood $U_p \subseteq X$ and polynomials $g_p, h_p \in S(X)$ with $f = g_p/h_p$ on U_p with $h_p(a) \neq 0$ for all $a \in U_p$. As $X \subseteq \mathbb{A}^n$, we can assume $g_p, h_p \in k[X]$. Obviously, there is a finite subcover $U_1 := U_{p_1}, ..., U_r := U_{p_r}$ with $p_1, ..., p_r \in X$.

As the U_i are an open cover, we see that $\mathbb{V}(\langle h_1, ..., h_r \rangle) = \emptyset$ and so by Hilbert's Nullstellensatz, find

$$1 = \sum_i \alpha_i h_i$$

Thus

$$f_i := \frac{g_i}{h_i} = \frac{g_i}{h_i} \sum_j \alpha_j h_j = \alpha_i g_i + \sum_{j \neq i} \alpha_j h_j \in k[X] \subseteq k(X)$$

So on each U_i, the regular map f is given by a polynomial $f_i \in k[X]$. It is left to show that those glue together to one global polynomial (this is only trivial in the case X irreducible).

First of all, show that $f_i(a) = f_j(a)$ even for all $a \in \bar{U}_j \cap \bar{U}_j$. □

Describing morphisms is slightly more difficult, but they also allow a relatively nice definition using the function field.

Theorem 1.9. *Let $X \subseteq \mathbb{P}^n$ be an irreducible projective variety. Then there is a well-defined bijection*

$$\Phi : \{f : X \dashrightarrow \mathbb{P}^m \mid f \text{ rational map}\} \to \mathbb{P}^m_{k(X)},$$
$$f \text{ defined locally by } f_0, ..., f_m \in S(X) \mapsto \left[\frac{f_0}{x_0^d} : \frac{f_1}{x_0^d} : ... : \frac{f_n}{x_0^d}\right]$$

that is compatible with evaluation maps, i.e. for $f : X \dashrightarrow Y$ and $g : Y \dashrightarrow \mathbb{P}^r$ such that the composition $g \circ f$ is well-defined, have

$$\Phi(g \circ f) = \mathrm{ev}_{\Phi(f)}(\Phi(g))$$

In particular, the restriction

$$\Phi\big|_{\{f:X\to\mathbb{P}^m \mid f \text{ morphism}\}} : \{f : X \to \mathbb{P}^m \mid f \text{ morphism}\} \to \mathbb{P}^m_{k(X)}$$

is a well-defined injection.

We sometimes will identify those two representations of rational maps. Note that $k[X \cap \mathbb{A}^n] \subseteq k(X \cap \mathbb{A}^n) \cong k(X)$, and using this makes the notation of rational maps as $[f_0 : ... : f_m]$ even more convenient, because we do not even require fractions then.

2 Elliptic Curves