Lecture 15. Regular maps; the theorem of Ax

We have seen that, for k algebraically closed, there is an intimate relationship between finitely generated k-algebras without non-zero nilpotents (also called **reduced**), that is, k-algebras of the form $k[X_1, \dots, X_n]/\sqrt{I}$, and the affine varieties $\mathcal{V}(\sqrt{I}) \subset k^n$, which are the geometric loci cut out by polynomials. What about maps between such objects?

Definition 4.41. *A* **regular mapping** *between affine varieties $V = \mathcal{V}(I) \subset k^n$ and $W = \mathcal{V}(J) \subset k^m$ is a map $\phi : V \to W$ given by polynomials $f_1, \dots, f_m \in k[X_1, \dots, X_n]$, that is,*

$$\phi(\mathbf{v}) = (f_1(\mathbf{v}), f_2(\mathbf{v}), \dots, f_m(\mathbf{v}))$$

for all $\mathbf{v} = (v_1, \dots, v_n) \in V$; in particular, the right-hand side must lie in W. The **regular functions** *on V are the regular mappings $V \to k$. They form a k-algebra under pointwise addition and multiplication, denoted by $k[V]$ and called the* **coordinate ring** *of V.*

By definition, two polynomials $f, g \in k[X_1, \dots, X_n]$ define the same regular function on V if and only if $f - g \in \mathcal{I}(V)$. Hence the algebra of regular functions on V is

$$k[V] \simeq k[X_1, \dots, X_n]/\mathcal{I}(V).$$

Since $\mathcal{I}(V)$ is radical, $k[V]$ is a finitely generated reduced k-algebra. A regular mapping $\phi = (f_1, \dots, f_m) : V \to W$ induces a k-algebra homomorphism (a k-linear ring homomorphism) in the opposite direction, the **pullback**

$$\phi^* : k[W] \simeq k[Y_1, \dots, Y_m]/\mathcal{I}(W) \to k[X_1, \dots, X_n]/\mathcal{I}(V) \simeq k[V], \qquad g \mapsto g \circ \phi,$$

which sends $Y_i \mapsto f_i(X_1, \dots, X_n)$. It is well defined because $\phi(V) \subset W$: if $g \in \mathcal{I}(W)$, then $g \circ \phi$ vanishes on V.

For k algebraically closed, the points of V correspond to the maximal ideals of $k[V]$: these are the maximal ideals of $k[X_1, \dots, X_n]$ containing $\mathcal{I}(V)$, which by Theorem 4.29 are the ideals $(X_1 - v_1, \dots, X_n - v_n)$ with $\mathbf{v} \in \mathcal{V}(\mathcal{I}(V)) = V$. Thus the maximal ideals of $k[V]$ are the ideals $\mathfrak{m}_{\mathbf{v}}$ of regular functions vanishing at a point $\mathbf{v} \in V$, and similarly for W, with maximal ideals $\mathfrak{n}_{\mathbf{w}}$, $\mathbf{w} \in W$. In these terms, ϕ is recovered from ϕ^*: $g \circ \phi$ vanishes at $\mathbf{v}$ if and only if g vanishes at $\phi(\mathbf{v})$, that is,

$$(\phi^*)^{-1}(\mathfrak{m}_{\mathbf{v}}) = \mathfrak{n}_{\phi(\mathbf{v})}.$$

◁ Show that $\phi \mapsto \phi^*$ is a bijection between the set of regular mappings $V \to W$ and the set of k-algebra homomorphisms $k[W] \to k[V]$. (Hint: given a k-algebra homomorphism $\psi : k[W] \to k[V]$, choose polynomials $f_i \in k[X_1, \dots, X_n]$ representing $\psi(Y_i)$ and check that $\phi = (f_1, \dots, f_m)$ maps V into $W = \mathcal{V}(\mathcal{I}(W))$.)

Together with the Nullstellensatz, which says that every finitely generated reduced k-algebra is of the form $k[V]$ when k is algebraically closed, this gives an (anti)equivalence between the category

of affine varieties over k, with regular mappings as morphisms, and the category of finitely generated reduced k-algebras. We leave the details to your algebraic geometry course.

We can add the following rows to our dictionary, where an isomorphism of affine varieties means a regular mapping with a regular inverse:

Algebra	Geometry
finitely generated reduced k-algebra $k[V]$	affine variety V
element $g \in k[V]$	regular function $g : V \to k$
maximal ideal $\mathfrak{m}_{\mathbf{v}} \subset k[V]$	point $\mathbf{v} \in V$
k-algebra homomorphism $\phi^* : k[W] \to k[V]$	regular mapping $\phi : V \to W$
$(\phi^*)^{-1}(\mathfrak{m}_{\mathbf{v}}) = \mathfrak{n}_{\mathbf{w}}$	$\phi(\mathbf{v}) = \mathbf{w}$
isomorphism of k-algebras	isomorphism of affine varieties

▶ Consider the regular mapping $\phi : k \to W = \mathcal{V}(Y^2 - X^3) \subset k^2$, $\phi(t) = (t^2, t^3)$, onto the cuspidal cubic, see Figure 8. It is bijective: the inverse sends $(x, y) \neq (0, 0)$ to $t = y/x$ and $(0, 0)$ to 0. In the dictionary, isomorphisms of affine varieties correspond to isomorphisms of k-algebras, and ϕ is not an isomorphism: the pullback $\phi^* : k[X, Y]/(Y^2 - X^3) \to k[T]$ sends $X \mapsto T^2$ and $Y \mapsto T^3$, so its image is $k[T^2, T^3] \subsetneq k[T]$. Equivalently, the inverse map $t = y/x$ is not a regular function on W. So a bijective regular mapping need not be an isomorphism.

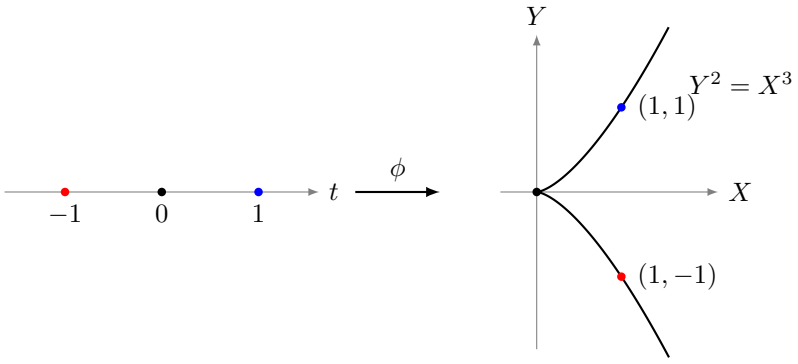


Figure 8: The bijective regular mapping $\phi(t) = (t^2, t^3)$ from the line onto the cuspidal cubic. It is not an isomorphism: ϕ^* has image $k[T^2, T^3] \subsetneq k[T]$.

5 Interlude: An application of the Nullstellensatz

We will prove the following theorem.

Theorem 5.1. *(Ax[9]) Suppose $p : \mathbb{C}^n \to \mathbb{C}^n$ is a regular mapping given by $p = (p_1, p_2, \ldots, p_n)$ with $p_i \in \mathbb{C}[X_1, \ldots, X_n]$. If p is injective, then it is also surjective.*

We will need an important consequence of Hilbert's Nullstellensatz that applies to "arithmetic" rings.

[9] J. Ax, The elementary theory of finite fields, Ann. of Math. 88 (1968), 239–271. The theorem was obtained independently by Grothendieck, EGA IV, Prop. 10.4.11, and is often called the Ax–Grothendieck theorem.

Theorem 5.2. *Let A be a finitely generated $\mathbb{Z}$-algebra, that is, $A \simeq \mathbb{Z}[X_1, \ldots, X_n]/I$, and let $\mathfrak{m} \subset A$ be a maximal ideal. Then $A/\mathfrak{m}$ is a finite field. In other words, a field which is finitely generated as a ring is finite.*

Proof. The ideal $\mathfrak{m} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ (Proposition 2.5), so it is either (p) for some prime number p or (0). First, suppose $\mathfrak{m} \cap \mathbb{Z} = (p)$. Then $A/\mathfrak{m}$ is a field which is a finitely generated algebra over $\mathbb{F}_p = \mathbb{Z}/(p)$. By Zariski's lemma (Lemma 4.30), $A/\mathfrak{m}$ is a finite extension of $\mathbb{F}_p$, hence a finite field.

Next, suppose $\mathfrak{m} \cap \mathbb{Z} = (0)$. Write $A = \mathbb{Z}[x_1, \ldots, x_d]$ with generators $x_i \in A$, and let $\bar{x}_i$ denote the image of x_i in $A/\mathfrak{m}$. The field $A/\mathfrak{m}$ contains $\mathbb{Z}$, hence $\mathbb{Q}$, and $A/\mathfrak{m} = \mathbb{Q}[\bar{x}_1, \ldots, \bar{x}_d]$ is a finitely generated $\mathbb{Q}$-algebra. By Zariski's lemma again, $A/\mathfrak{m}$ is a finite extension of $\mathbb{Q}$. So each $\bar{x}_i$ is algebraic over $\mathbb{Q}$ and, clearing denominators, satisfies a relation

$$a_i \bar{x}_i^{n_i} + \ldots = 0 \text{ with integer coefficients and } a_i \neq 0.$$

Dividing by a_i, we see that each $\bar{x}_i$ is integral over the subring $R = \mathbb{Z}[a_1^{-1}, a_2^{-1}, \ldots, a_d^{-1}] \subset \mathbb{Q}$, hence so is $A/\mathfrak{m} = R[\bar{x}_1, \ldots, \bar{x}_d]$ by Corollary 4.23(a). Since $A/\mathfrak{m}$ is a field, R is a field by Corollary 4.23(d), and as $\mathbb{Z} \subset R \subset \mathbb{Q}$ this forces $R = \mathbb{Q}$. But a prime number p not dividing $a_1 a_2 \cdots a_d$ is not invertible in R, since every element of R can be written with a denominator whose prime factors divide $a_1 \cdots a_d$. Such a prime exists by Euclid's theorem on the infinitude of primes (circa 300 BC), a contradiction. □

Proof of Theorem 5.1. The idea is to reduce to finite fields, where the statement is trivial: if k is a finite field and $p : k^n \to k^n$ is injective, then p is surjective, since an injective map from a finite set to itself is surjective. To carry out the reduction, we first use the Nullstellensatz to express injectivity and surjectivity by polynomial identities.

Injectivity: Let k be a field and $p_1, p_2, \ldots, p_n \in k[X_1, \ldots, X_n]$ polynomials such that the regular mapping $p = (p_1, \ldots, p_n) : k^n \to k^n$ is injective. Write $\mathbf{X} = (X_1, \ldots, X_n)$ and $\mathbf{Y} = (Y_1, \ldots, Y_n)$, and let $I \subset k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ be the ideal

$$I = (p_1(\mathbf{X}) - p_1(\mathbf{Y}), \ldots, p_n(\mathbf{X}) - p_n(\mathbf{Y})).$$

Its zeros are the pairs $(\mathbf{x}, \mathbf{y}) \in k^n \times k^n$ with $p(\mathbf{x}) = p(\mathbf{y})$. Since p is injective, $X_i - Y_i \in \mathcal{I}(\mathcal{V}(I))$ for all i, hence if k is algebraically closed, by the strong Nullstellensatz we can find polynomials $q_{i,j} \in k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ and $\ell_i > 0$ such that

$$\sum_{j=1}^{n} (p_j(\mathbf{X}) - p_j(\mathbf{Y}))\, q_{i,j}(\mathbf{X}, \mathbf{Y}) = (X_i - Y_i)^{\ell_i}, \quad i = 1, \ldots, n. \tag{1}$$

Conversely, if Equations (1) hold over a field k (not necessarily algebraically closed), then $p : k^n \to k^n$ is injective: if $p(\mathbf{x}) = p(\mathbf{y})$, then $(x_i - y_i)^{\ell_i} = 0$ for all i, so $\mathbf{x} = \mathbf{y}$.

Surjectivity: Let $(a_1, \ldots, a_n) \in k^n$ be such that the system $p_i(\mathbf{X}) = a_i$, $i = 1, \ldots, n$, has no solution in k^n. If k is algebraically closed, then by the weak Nullstellensatz the ideal $(p_1 -$

$a_1, \ldots, p_n - a_n)$ is not proper, so there are polynomials $h_i \in k[X_1, \ldots, X_n]$ such that

$$\sum_{i=1}^{n} (p_i(\mathbf{X}) - a_i)\, h_i(\mathbf{X}) = 1. \tag{2}$$

Conversely, if Equation (2) holds over a field k, then $(a_1, \ldots, a_n) \notin \mathrm{Im}(p)$, so $p : k^n \to k^n$ is not surjective.

Now we can complete the proof for $k = \mathbb{C}$. Suppose that $p = (p_1, \ldots, p_n) : \mathbb{C}^n \to \mathbb{C}^n$ is injective but not surjective, and let $(a_1, \ldots, a_n) \notin \mathrm{Im}(p)$. Since $\mathbb{C}$ is algebraically closed, we have polynomials $q_{i,j}$ as in Equations (1) and h_i as in Equation (2). Let $A \subset \mathbb{C}$ be the subring generated by all the coefficients of the polynomials p_i, $q_{i,j}$, h_i and by $a_1, \ldots, a_n$. It is a finitely generated $\mathbb{Z}$-algebra, the polynomials p_i have coefficients in A, and Equations (1) and (2) hold in $A[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ and $A[X_1, \ldots, X_n]$. Finally, let $\mathfrak{m}$ be a maximal ideal of A, which exists by Proposition 2.4, and reduce everything modulo $\mathfrak{m}$: the polynomials $\overline{p}_i$ with coefficients in the field $A/\mathfrak{m}$ define a mapping

$$\overline{p} : (A/\mathfrak{m})^n \to (A/\mathfrak{m})^n,$$

and Equations (1) and (2) continue to hold over $A/\mathfrak{m}$. By the two criteria, $\overline{p}$ is injective but not surjective, as $(\bar{a}_1, \ldots, \bar{a}_n)$ is not in its image. But by Theorem 5.2, $A/\mathfrak{m}$ is a finite field, contradicting the finite field version. □

► The appeal to Proposition 2.4, hence to Zorn's lemma, in the last step can be avoided, because A is countable: it is the image of $\mathbb{Z}[X_1, \ldots, X_d]$ for some d, whose elements can be listed explicitly. List the elements of A as $a_0, a_1, a_2, \ldots$, let $I_0 = (0)$, and let $I_{k+1} = I_k + (a_k)$ if this ideal is proper and $I_{k+1} = I_k$ otherwise. The union $\mathfrak{m}$ of the chain $I_0 \subset I_1 \subset \ldots$ is a proper ideal, since $1 \notin I_k$ for all k, and it is maximal: if $a_k \notin \mathfrak{m}$, then $a_k \notin I_{k+1}$, so $I_k + (a_k)$ is not proper and $1 \in I_k + (a_k) \subset \mathfrak{m} + (a_k)$. Starting instead with $I_0 = I$, the same argument gives a maximal ideal containing any proper ideal I of a countable ring. Since the Nullstellensatz was proved without choice in Theorem 4.31, the proof of Theorem 5.1 does not use the Axiom of Choice at all.

◁ Show that Nagata's polynomial mapping $p : \mathbb{C}^3 \to \mathbb{C}^3$ given by $(x, y, z) \mapsto (x - 2y(xz + y^2) - z(xz + y^2)^2, y + z(xz + y^2), z)$ is injective (hence also surjective). (Hint: $xz + y^2$ is preserved by p.)

◁ Find a polynomial mapping $p : \mathbb{Q}^n \to \mathbb{Q}^n$ (for any n) which is injective but not surjective. (Hint: consider $x \mapsto x^3$ for $x \in \mathbb{Q}$.)

◁ Prove that any polynomial mapping $p : \mathbb{R} \to \mathbb{R}$ that is injective is also surjective.

In fact, it is also true that any polynomial mapping $p : \mathbb{R}^n \to \mathbb{R}^n$ that is injective is also surjective. Our proof does not give this more difficult result.[10]

[10] A. Białynicki-Birula and M. Rosenlicht, Injective morphisms of real algebraic varieties, Proc. Amer. Math. Soc. 13 (1962), 200–203.