LECTURE 14, MONDAY APRIL 5, 2004

FRANZ LEMMERMEYER

1. Coordinate Rings

So far we have studied algebraic curves $\mathcal{C} : f(X,Y) = 0$ for some $f \in K[X,Y]$ mainly using geometric means: tangents, singular points, parametrizations, ... Now let us ask what we can do with f from an algebraic point of view. What have we got? First of all we have a polynomial ring $R = K[X,Y]$, in which the polynomial f lives. The polynomial f generates a principal ideal (f) in the ring R; in algebra we learn that if we have a ring and an ideal, then we should form the quotient. Let's do this here: the ring $K[X]/(f)$ attached to $\mathcal{C}$ is called the coordinate ring of $\mathcal{C}$ and will be denoted by $K[\mathcal{C}]$.

Although we will continue working with plane algebraic curves, let us at least make a few remarks concerning general algebraic sets. They are defined as the zero sets of polynomials $f_1, \ldots, f_n \in K[X_1, \ldots, X_m]$; for example, the algebraic set $V \subset \mathbb{A}^3K$ defined as the common zeros of $f(X,Y,Z) = X^2 + Y^2 + Z^2 - 1$ and $g(X,Y,Z) = Z$ is just the unit circle in the $X-Y$-plane. In this case, we have the ideal $I = (f_1, \ldots, f_n)$ in the ring $K[X_1, \ldots, X_m]$.

Examples. Whenever we come across some abstract construction such as $K[\mathcal{C}]$, it is important to construct lots of examples to get a feeling for these objects.

(1) The coordinate ring of lines: Consider $\ell : f(X,Y) = 0$ for $f(X,Y) = Y - mX - b$. We have $K[\ell] = K[X,Y]/(f)$. The representatives of the cosets $g + (f)$ are polynomials in $K[X,Y]$; we can replace every Y in g by $mX + b$. Thus every element of $K[\ell]$ can be written as $g(X) + (f)$ for some polynomial in X, and these elements are all pairwise distinct: $g(X) + (f) = h(X) + (f)$ means that $g(X) - h(X)$ is divisible by $f(X,Y) = Y - mX - b$, which is only possible if $g = h$. The map $K[\ell] \longrightarrow K[X]$ defined by $g(X) + (f) \longmapsto g(X)$ is a ring isomorphism, hence $K[\ell] \simeq K[X]$.

(2) The coordinate ring of the parabola $\mathcal{C} : Y - X^2 = 0$ is given by $K[\mathcal{C}] = K[X,Y]/(Y - X^2)$. Any element $g(X,Y) + (Y - X^2)$ can be represented by a polynomial in X alone since we may replace each Y by X^2 without changing the coset; in particular we have $g(X,Y) + (Y - X^2) = g(X,X^2) + (Y - X^2)$. Again, the map $g(X,Y) + (Y - X^2) \longmapsto g(X,X^2)$ is a ring isomorphism; thus $K[\mathcal{C}] \simeq K[X]$.

   The fact that $K[\mathcal{C}] \longrightarrow K[X]$ is surjective is clear, since any $h \in K[X]$ is the image of $h + (f)$, where $f(X,Y) = Y - X^2$. For showing that the map is injective, consider an element $g + (f)$ that maps to $0 + (f)$. Thus $g(X,X^2) = 0$, and we have to show that this implies that $g(X,Y)$ is a multiple of f. Consider the field $k = K(X)$; the ring $K(X)[Y]$ contains $K[X,Y]$ and is Euclidean. Write $g = qf + r$ with $q, r \in k$ and $\deg r < \deg f$

as polynomials in Y. But $\deg f = 1$, hence $r \in k$. Plugging in X^2 for Y and observin that $g(X, X^2) = f(X, X^2) = 0$ shows that $r = 0$, hence $f \mid g$.

(3) The coordinate ring of the unit circle $\mathcal{C}$: here $f(X,Y) = X^2 + Y^2 - 1$, and $K[\mathcal{C}] = K[X,Y]/(f)$. The polynomial $g(X,Y) = X^4 + X^2Y + XY^2$ has image $g + (f)$ in $K[\mathcal{C}]$; note that $g + (f) = X^4 + X^2Y + X(1 - X^2) + (f) = X^4 - X^3 + X + X^2Y + (f)$. In general, every element $g + (f)$ can be written in the form $g(X,Y) + (f) = h_1(X) + Yh_2(X) + (f)$, since we may replace every Y^2 by $1 - X^2$.

Note that $K[\mathcal{C}]$ cannot be isomorphic to $K[X]$: this is because $K[X]$ is a unique factorization domain, but $K[\mathcal{C}]$ is not; in fact, we have $Y^2 + (f) = (1 - X)(1 + X) + (f)$, and the elements $Y + (f)$, $1 + X + (f)$ and $1 - X + (f)$ are irreducible.

What can we say about the algebraic properties of the coordinate ring? Let us first observe a special property of coordinate rings, namely that they all contain fields:

Proposition 1.1. *If $\mathcal{C} : f(X,Y) = 0$ for some $f \in K[X,Y]$ with $\deg f \geq 1$, then the map $a \longmapsto a + (f)$ induces a ring monomorphism $K \hookrightarrow K[\mathcal{C}]$.*

This implies that $\mathbb{Z}$ cannot be the coordinate ring of a curve, since $\mathbb{Z}$ does not contain a field.

Proof. The map clearly is a ring homomorphism. Assume that $a + (f) = b + (f)$; then $f \mid (b - a)$, which implies that $a = b$ since $\deg(b - a) \leq 0$ and $\deg f \geq 1$. □

Proposition 1.2. *Let $f \in K[X,Y]$ be a nonconstant polynomial with coefficients from some algebraically closed field, and $\mathcal{C}_f : f(X,Y) = 0$ the corresponding affine curve. The following assertions are equivalent:*

(1) *f is irreducible in $K[X,Y]$;*
(2) *(f) is a prime ideal in $K[X,Y]$;*
(3) *the coordinate ring $K[\mathcal{C}]$ of $\mathcal{C}_f$ is a domain.*

Proof. The equivalence (2) $\iff$ (3) is clear, since by definition an ideal P is prime in some ring R if and only if R/P is a domain.

If f is irreducible, then it is prime since $K[X,Y]$ is a unique factorization domain. Conversely, if (f) is prime then f must be irreducible: for if $f = gh$ is a nontrivial factorization in $K[X,Y]$, then $[g + (f)][h + (f)] = 0 + (f)$ in $K[\mathcal{C}]$. Moreover, $g + (f) \neq 0$ since this would imply $f \mid g$, and then $f = gh$ would be a trivial factorization. □

2. Polynomial Functions

Consider the curve $\mathcal{C}_f : f(X,Y) = 0$ for some $f \in K[X,Y]$. A K-valued function $\phi : \mathcal{C}_f \longrightarrow K$ is called a *polynomial function* if there exists a polynomial $T \in K[X,Y]$ such that $f(x,y) = T(x,y)$.

Here are a few examples:

(1) The maps $(x,y) \longmapsto x$ and $(x,y) \longmapsto y$ are polynomial functions $\mathcal{C}_f \longrightarrow K$ for any curve $\mathcal{C}_f$.
(2) More generally, every polynomial $T \in K[X,Y]$ induces a polynomial function $\phi : \mathcal{C}_f \longrightarrow K$.

(3) The map $\phi : (x, y) \longmapsto \frac{x}{x^2+1}$ is not a polynomial function on the unit circle in $\mathbb{A}^2\mathbb{Q}$. Note that it is not enough to observe that $\frac{x}{x^2+1}$ is not a polynomial: we have to show that this function cannot be expressed by a polynomial. As a matter of fact, ϕ is a polynomial function on the unit circle over $\mathbb{F}_3$ since it can be expressed by $\phi(x, y) = x(x + 1)^2 + 1$.

We have already observed that any $T \in K[X, Y]$ gives a polynomial function $\phi : \mathcal{C}_f \longrightarrow K$ via $\phi(x, y) = T(x, y)$. Note, however, that different polynomials may give the same function: in fact, the polynomials T and $T + f$ induce the same function on $\mathcal{C}_f$ because f vanishes on $\mathcal{C}_f$.

In any case, the map π sending $T \in K[X, Y]$ to $T + (f) \in K[\mathcal{C}_f]$ is a ring homomorphism, and it is clearly surjective. Its kernel consists of all polynomials T with $T + (f) = 0 + (f)$, that is, we have $\ker \pi = (f)$. We can express this by saying that the sequence

$$0 \longrightarrow (f) \longrightarrow K[X, Y] \longrightarrow K[\mathcal{C}_f] \longrightarrow 0$$

is exact.

Recall that a sequence

$$0 \xrightarrow{\ o\ } A \xrightarrow{\ i\ } B \xrightarrow{\ f\ } C \xrightarrow{\ p\ } 0$$

of abelian groups (rings) is called exact if the maps i, f, p are group (ring) homomorphisms, and if $\ker i = \operatorname{im} o$, $\ker f = \operatorname{im} i$, $\ker p = \operatorname{im} f$, and $\ker p = \operatorname{im} f$. Since o is the map sending 0 to the neutral element of A, we have $\ker i = \operatorname{im} o$ if and only if i is injective; similarly p maps everything to 0, hence $\ker p = \operatorname{im} f$ if and only if f is surjective. Thus the sequence is exact if and only if i is injective, f is surjective, and $\ker f = \operatorname{im} i$.

3. Categories

Categories are all over the place in mathematics. Informally, a category consists of objects and morphisms; examples are

category	objects	morphisms
Set	sets	maps
Grp	groups	group homomorphisms
AbGrp	abelian groups	group homomorphisms
Rng	rings	ring homomorphisms
R-Mod	R-modules	R-homomorphisms
Top	topological spaces	continuous maps
K-Vec	K-vector spaces	K-linear maps

Of course categories have to satisfy certain axioms. The fact that the axioms deal with the morphisms, not with the objects, already shows that in a category, the important data are encoded into the morphisms.

A category C consists of the following data:

(1) a collection of objects;
(2) a collection of arrows (also called morphisms);
(3) for each arrow f there are unique objects $A = \operatorname{dom} f$ and $B = \operatorname{cod} f$; we write $f : A \longrightarrow B$.

(4) for each pair f, g of arrows with $\operatorname{dom} g = \operatorname{cod} f$ there is a unique arrow $g \circ f$ (the composition of f and g) with $\operatorname{dom} g \circ f = \operatorname{dom} f$ and $\operatorname{cod} g \circ f = \operatorname{cod} g$. These compositions satisfy the following associativity law: if

$$A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C \xrightarrow{\ h\ } D,$$

then $h \circ (g \circ f) = (h \circ g) \circ f$.

(5) for each object B there is a unique arrow $\mathrm{id}_A : A \longrightarrow A$ called the identity arrow; for arrows $f : A \longrightarrow B$ and $g : B \longrightarrow C$ we have $\mathrm{id}_B \circ f = f$ and $g \circ \mathrm{id}_B = g$.

If you've never seen the definition of the category, you should verify these axioms for a few categories you know. Note that there are lots of categories out there, most of them completely useless. Consider e.g. the category consisting of two objects called apple and pea, and whose morphisms are given by the two identity arrows apple $\longrightarrow$ apple, pea $\longrightarrow$ pea, as well as the arrow apple $\longrightarrow$ pea. Now check that the axioms are verified.

Similarly, the category with objects 0, 1 and 2 whose morphisms are the three identity maps as well as the arrows $0 \longrightarrow 1$ and $1 \longrightarrow 2$ is not a category.

4. Polynomial Maps

Let $\mathcal{C}_f : f(x,y) = 0$ and $\mathcal{C}_g : g(x,y) = 0$ be two affine curves defined over K. A map $F : \mathcal{C}_f \longrightarrow \mathcal{C}_g$ is a polynomial map if we have $F(P) = (F_1(P), F_2(P))$ for polynomials $F_1, F_2 \in K[X,Y]$ and $P \in \mathcal{C}_f(K)$.

Here are some examples.

(1) Consider the line $\mathcal{C}_f$ defined by $f(X,Y) = Y$ and the parabola $\mathcal{C}_g$ defined by $g(X,Y) = Y - X^2$. The map $F(X,Y) = (X, X^2)$ is a polynomial map $\mathcal{C}_f \longrightarrow \mathcal{C}_g$, where $F_1(X,Y) = X$ and $F_2(X,Y) = X^2$. Similarly, the map $G(X,Y) = (X,0)$ is a polynomial map $\mathcal{C}_g \longrightarrow \mathcal{C}_f$.

Moreover, the composition $G \circ F$ sends $(x,0) \in \mathcal{C}_f$ to $G(x,x^2) = (x,0)$, hence is the identity map on $\mathcal{C}_f$. Similarly, the composition $F \circ G$ sends (x,x^2) to $(x,0)$ and then back to (x,x^2), hence F and G are inverse maps of each other.

(2) Consider the line $\mathcal{C}_f : f(X,Y) = Y = 0$ and the singular cubic $\mathcal{C}_g : g(X,Y) = Y^2 - X^3 = 0$. The map $(x,0) \longmapsto (x^2,x^3)$ is a polynomial map $\mathcal{C}_f \longrightarrow \mathcal{C}_g$. The inverse map $(x,y) \longmapsto (\frac{y}{x}, 0)$ does not look polynomial, but it is not obvious that it cannot be written as a polynomial. For example, we have $\frac{y}{x} = \frac{y^2}{xy} = \frac{x^3}{xy} = \frac{x^2}{y}$, and it might be possible that similar manipulations can turn this into a polynomial after all.

(3) Consider $f(X,Y) = X^2 + Y^2 - 1$ and $g(X,Y) = X^2 + Y^2 - 2$. Then $F : (x,y) \longmapsto (x+y, x-y)$ is a polynomial map. The inverse map is polynomial unless the field K you are working over happens to have characteristic 2.

A polynomial map $F : \mathcal{C}_f \longrightarrow \mathcal{C}_g$ induces a ring homomorphism $F^* : K[\mathcal{C}_g] \longrightarrow K[\mathcal{C}_f]$. In fact, given an element $h + (g) \in K[\mathcal{C}_g]$, we can put $F^*(h) = h \circ F + (f)$, where $h \circ F = h(F_1(X,Y), F_2(X,Y))$. This is a well defined ring homomorphism.

Again, let us work out a few examples.

(1) Consider the line $f(X,Y) = Y$ and the parabola $g(X,Y) = Y - X^2$. The polynomial map $F(X,Y) = (X,X^2)$ induces a ring homomorphism F^* from

$K[\mathcal{C}_g] = K[X,Y]/(Y - X^2) \simeq K[X]$ to $K[\mathcal{C}_f] = k[X,Y]/(Y) \simeq K[X]$; in fact we have $F^* : h(X,Y) + (Y - X^2) \longmapsto h(X, X^2) + (Y)$.

$h(X,Y)$	X	Y	X^3	XY	$X^2 - Y$
$F^*(h)$	X	X^2	X^3	X^3	0

As you can see, the induced map $K[X] \longrightarrow K[X]$ is the identity.

(2) Consider the line $f(X,Y) = Y$ and the singular cubic $g(X,Y) = Y^2 - X^3$. The map $F : (x,y) \longmapsto (x^2, x^3)$ is a polynomial map $\mathcal{C}_f \longrightarrow \mathcal{C}_g$ which induces a ring homomorphism F^* from $K[\mathcal{C}_g] = K[X,Y]/(Y^2 - X^3)$ to $K[\mathcal{C}_f] = k[X,Y]/(Y) \simeq K[X]$. In fact, an element $h(X,Y) + (Y^2 - X^3) \in K[\mathcal{C}_g]$ gets mapped to $h(X^2, X^3) + (Y) \in K[\mathcal{C}_f]$. Again, here's a little table showing you what is going on:

$h(X,Y)$	X	Y	$Y^2 - X^3$
$F^*(h)$	X^2	X^3	0

The table shows that the image of F^* is the subring $K[X^2, X^3]$ of $K[X]$; since X cannot be written as a polynomial in X^2 and X^3, the homomorphism F^* is not surjective. As a matter of fact, the image consists of all polynomials in X without a linear term.

Observe that F is a bijective polynomial map, and that F^* is injective, but not surjective.