LECTURE 6, THURSDAY FEB. 26, 2004

FRANZ LEMMERMEYER

In the following, for a curve $\mathcal{C}_f : f(X,Y) = 0$ we denote the set $\{(x,y) \in K^2 : f(x,y) = 0\}$ of K-rational points on $\mathcal{C}_f$ by $\mathcal{C}_f(K)$.

1. Irreducible Curves

Let us now briefly explain the notion of irreducible curves. Assume that $\mathcal{C}_f : f(X,Y) = 0$ and $\mathcal{C}_g : g(X,Y) = 0$ are algebraic curves defined over some field K, i.e., with $f, g \in K[X,Y]$. Now assume that we know $g \mid f$, that is, there is an $h \in K[X,Y]$ with $f = gh$. Then clearly $\mathcal{C}_g(K) \subseteq \mathcal{C}_f(K)$ for any field K: in fact, if $g(x,y) = 0$ for $x, y \in K$, then certainly $f(x,y) = 0$, hence $(x,y) \in \mathcal{C}_f(K)$.

What about the converse? If $\mathcal{C}_g(K) \subseteq \mathcal{C}_f(K)$ for some field K, does this tell us something about the polynomials? In general, the answer is no: if, for example, $g(X,Y) = X^2 + Y^2 + 1$ and $K = \mathbb{R}$, then the set $\mathcal{C}_g(\mathbb{R})$ of points on $\mathcal{C}_g$ with coordinates in $\mathbb{R}$ is empty, hence $\mathcal{C}_g(\mathbb{R}) \subseteq \mathcal{C}_f(\mathbb{R})$ for any other curve $\mathcal{C}_f$. This question therefore only makes sense if we work over some algebraically closed field.

Lemma 1.1. *For a field K with algebraic closure $\overline{K}$, the set $C_f(\overline{K})$ is infinite.*

Proof. This is trivial if $f = 0$. If $f \neq 0$, then for any $a \in \overline{K}$ the polynomial $f(a,Y) \in \overline{K}[Y]$ has at least one zero (in fact $\deg_y f$ of them) since f splits into linear factors over the algebraic closure $\overline{K}$ of K. Since there are infinitely many $a \in \overline{K}$, this proves the claim. □

Proposition 1.2. *Let $f, g \in K[X,Y]$ be coprime polynomials. Then $C_f(L) \cap C_g(L)$ is finite for any field $L \supseteq K$.*

Proof. View f and g as elements of $R = K(X)[Y]$. Since $K(X)$ is a field, R is Euclidean and therefore a principal ideal domain. Since f and g are relatively prime, we can write 1 as a $K(X)$-linear combination of f and g, say

$$1 = \frac{p(X,Y)}{q(X)} f(X,Y) + \frac{r(X,Y)}{s(X)} g(X,Y).$$

Clearing denominators gives

$$q(X)s(X) = s(X)p(X,Y)f(X,Y) + q(X)r(X,Y)g(X,Y).$$

Now for any $(x,y) \in C_f(L) \cap C_g(L)$ we have $q(x)s(x) = 0$, which can happen only for finitely many values of x.

Repeating this argument with the roles of x and y switched we find that there are only finitely many values of y such that $(x,y) \in C_f(L) \cap C_g(L)$. This proves the claim. □

Proposition 1.3 (Study's Lemma)**.** *Let $f, g \in \overline{K}[X,Y]$ be polynomials, and assume that g is irreducible. Then $C_f(\overline{K}) \supseteq C_g(\overline{K})$ if and only if $g \mid f$.*

Proof. One direction is clear. Assume therefore that $C_f(\overline{K}) \supseteq C_g(\overline{K})$. Since $C_g(\overline{K})$ is infinite, so is $\#C_f(\overline{K}) \cap C_g(\overline{K})$. By Proposition 1.2, f and g are not coprime. Since g is irreducible, we conclude that $g \mid f$. □

Now let $\mathcal{C}_f : f(X,Y) = 0$ be an algebraic curve defined over some field K. If $f = gh$ for polynomials $g, h \in K[X,Y]$, we say that f is reducible; if $f = gh$ for polynomials $g, h \in \overline{K}[X,Y]$, we say that f is geometrically reducible. In this case, the curves $\mathcal{C}_g$ and $\mathcal{C}_h$ are called components of $\mathcal{C}_f$, or said to be contained in $\mathcal{C}_f$.

As an example, the curve $\mathcal{C} : f(X,Y) = Y^2 - 2X^2 = 0$ is irreducible over $\mathbb{Q}$, but geometrically reducible since $f = gh$ for $g(X,Y) = Y - \sqrt{2}\,X$ and $h(X,Y) = Y + \sqrt{2}\,X$.

Note that $\overline{K}[X,Y]$ is a unique factorization domain, so every polynomial $f \in \overline{K}[X,Y]$ can be factored (uniquely up to order and constant factors $\in \overline{K}^\times$) into irreducible factors.

Here's an example for an irreducible curve:

Proposition 1.4. *Let $F \in K[X]$ be a polynomial of odd degree. Then the cubic $Y^2 - F(X) = 0$ is geometrically irreducible.*

Proof. Assume not. Then the polynomial $f(X,Y) = Y^2 - F(X)$ factors nontrivially. Viewed as a polynomial in $R[Y]$, where $R = K[X]$, f has degree 2; if it factors, then $f = gh$ for linear polynomials in Y, and we have $g(X,Y) = a(X)Y + b(X)$, $h(X,Y) = c(X)Y + d(X)$. Comparing coefficients gives $a(X)c(X) = 1$, which implies that a and c are constants that may be taken to be 1. Thus $f(X,Y) = (Y + b(X))(Y + d(X))$. Comparing the coefficients of the linear term we get $d(X) = -b(X)$, hence $f(X,Y) = (Y + b(X))(Y - b(X))$. But then $F(X) = -b(X)^2$, contradicting the assumption that F have odd degree. □

2. Tangents

How do we compute the tangent at $P = (a,b)$ to a plane curve $f(x,y) = 0$? One way of doing it is to compute the Taylor expansion of f around P. Last time we have seen how to do this for polynomials in one variable.

Now assume that $f \in K[X,Y]$ is a polynomial in two variables. For finding the tangent at $P = (a,b)$, we take two "close" points (a,b) and (x,y) on the curve and put $x = a + (x-a)$ and $y = b + (y-b)$; then we develop $f(x,y)$ into a "Taylor series" and omit any term of degree 2 and higher! Letting f_1 and f_2 denote the partial derivatives at (a,b) with respect to X and Y, respectively, we find

$$\begin{aligned} 0 = f(x,y) &= f(a + (x-a), b + (y-b)) \\ &= f(a,b) + f_1(x-a) + f_2(y-b) + \text{terms of higher order.} \end{aligned}$$

Since $f(a,b) = 0$, the equation of the tangent should be

$$f_1(x-a) + f_2(y-b) = 0.$$

Let us check this for the line $rx + sy + t = 0$; the tangent at (a,b) has equation

$$0 = r(x-a) + s(y-b) = rx + sy - (ra + sb) = rx + sy + t$$

as expected.

What is the projective equation of tangents? Of course we can simply take the affine equation above and homogenizing, but the derivatives used would still be

those of the affine equation. Let us now work out the connection. The connection between the homogenization $F(X,Y,Z)$ of $f(x,y)$ and f is

$$F(X,Y,Z) = Z^{\deg f} f\Big(\frac{X}{Z}, \frac{Y}{Z}\Big). \tag{1}$$

Now we put $n = \deg f$ and compute

$$\begin{aligned} F_X &= \frac{\partial F}{\partial X} = Z^n f_1(x,y) Z^{-1} = Z^{n-1} f_1(x,y), \\ F_Y &= \frac{\partial F}{\partial Y} = Z^n f_2(x,y) Z^{-1} = Z^{n-1} f_2(x,y), \\ F_Z &= \frac{\partial F}{\partial Z} = nZ^{n-1} f(x,y) - XZ^{n-1} f_1(x,y) - YZ^{n-2} f_2(x,y). \end{aligned}$$

Evaluating these equations at $(x,y) = (a,b)$ and $[X:Y:Z] = [a:b:1]$, respectively, we get

$$\begin{aligned} F_X(P) &= f_1(a,b), \\ F_Y(P) &= f_2(a,b), \\ F_Z(P) &= -af_1(a,b) - bf_2(a,b), \end{aligned}$$

where we have put $F_X(P) = \frac{\partial F}{\partial X}([a:b:1])$ etc.

Plugging this into the affine equation for the tangent we get

$$0 = F_X(P)\Big(\frac{X}{Z} - a\Big) + F_Y(P)\Big(\frac{Y}{Z} - b\Big) \;=\; F_X(P)\frac{X}{Z} + F_Y(P)\frac{Y}{Z} + F_Z(P).$$

Multiplying through by Z now gives the projective form of the tangent equation

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0. \tag{2}$$

As an example, let us compute the tangent to the elliptic curve $E : Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$ at the point $P = [0:1:0]$ at infinity. We find $F_X(P) = -3X^2 - aZ^2|_P = 0$, $F_Y(P) = 2YZ|_P = 0$ and $F_Z(P) = Y^2 - 2aXZ - 3bZ^2|_P = 1$, hence the tangent is given by $Z = 0$, in other words: the tangent to E at its point at infinity is the line at infinity.

One more remark: it is not obvious from the form of the equation (2) that this tangent even passes through P. This is a consequence of

Proposition 2.1 (Euler's Identity)**.** *Let K be a field, and assume that $F \in K[X_1, \ldots, X_n]$ is a homogeneous polynomial of degree d. Let $F_i = \frac{\partial F}{\partial X_i}$; then*

$$d \cdot F(X_1, \ldots, X_n) = X_1F_1 + \ldots + X_nF_n.$$

Proof. Since forming derivatives is K-linear, it is sufficient to prove the claim for monomials $F = X_1^{a_1} \cdots X_n^{a_n}$. But then $X_iF_i = a_iF$, hence $X_1F_1 + \ldots + X_nF_n = (a_1 + \ldots + a_n)F = d \cdot F$. □

3. Singularities

There is one gap in the discussion of tangents above: what happens if $f_1(a,b) = f_2(a,b) = 0$ for a point $P = (a,b)$ on the affine curve? Or, equivalently, if $F_X(P) = F_Y(P) = F_Z(P) = 0$? Then the equations above collapse to $0 = 0$ and certainly do not describe lines. Points satisfying these conditions are called singular.

The computation of singular points is *always* done over algebraically closed fields. The point is that we don't want to miss any singularities just because their coordinates happen to lie in some extension field.

Let us start by giving examples for curves with a singular point:

Proposition 3.1. *The projective closure of $y^2 = g(x)$, where g has multiple roots, is singular.*

Proof. Assume that g has a double root at $x = a$; then $g(x) = (x-a)^2 h(x)$ for some polynomial h, and we claim that $P = (a, 0)$ is singular. Working projectively, the curve is given by $F(X, Y, Z) = Y^2 Z^{r-2} - G(X, Z)$, where $r = \deg g$, and the point $\iota(P) = [a : 0 : 1]$.

Clearly P lies on the curve; we find

$$\begin{aligned} F_X(P) &= -G_X(P) = -\tfrac{dG}{dX}(a, 1) = -g'(a) = 0, \\ F_Y(P) &= 2YZ^{r-2}|_P = 0, \\ F_Z(P) &= [(r-2)Y^2 Z^{r-3} - \tfrac{dG}{dZ}]|_P = 0, \end{aligned}$$

where for the last equality we have used that $G(X, Z) = (X - aZ)^2 H(X, Z)$; plugging $X = a$ and $Z = 1$ into its derivative with respect to Z gives 0. □

We also have

Proposition 3.2. *Let $\mathcal{C}_f : f(X, Y) = 0$ be a reducible curve, i.e., $f = gh$ with $\deg g, \deg h \ge 1$. If P is a point lying on both components, then P is singular.*

It will follow from Bezout's Theorem that such points P always exist (over algebraically closed fields), hence reducible curves are all singular.

Proof. We have to compute $f_1(P)$ and $f_2(P)$:

$$\begin{aligned} f_1(P) &= \frac{\partial f}{\partial x}\Big|_P = g_1(P)h(P) + h(P)h_1(P) = 0, \\ f_2(P) &= \frac{\partial f}{\partial y}\Big|_P = g_2(P)h(P) + h(P)h_2(P) = 0. \end{aligned}$$

Here we have used that P lies on both components. □