LECTURE 5, FRIDAY 20.02.04

FRANZ LEMMERMEYER

Before we start with the arithmetic of elliptic curves, let us talk a little bit about multiplicities, tangents, and singular points.

1. 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. This works fine for curves over the reals; but what should we do for arbitrary fields? Well, we'll use the fact that our curve is algebraic, that is, given by a polynomial; and the Taylor expansion of a polynomial does not require any calculus at all!

Let's start with a polynomial $f(x)$ in one variable; then

$$\begin{aligned} f(X+h) &= a_n(X+h)^n + a_{n-1}(X+h)^{n-1} + \ldots + a_1(X+h) + a_0 \\ &= a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \\ &\quad + (na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1)h \\ &\quad + \Big(\frac{n(n-1)}{2}a_nX^{n-2} + \frac{(n-1)(n-2)}{2}a_{n-1}X^{n-3} + \ldots + a_2)\Big)h^2 \\ &\quad + \text{ terms of higher degree} \\ &= f(X) + f'(X)h + \frac{f''(X)}{2!}h^2 + \ldots + \frac{f^{(n)}(X)}{n!}. \end{aligned}$$

Note that the 2! in the denominator cancels against the factor 2! present in the products $k(k-1)$; more generally, elementary number theory shows that $r!$ will divide any product $k(k-1)\cdots(k-r+1)$. In particular, $f^{(n)}(X) = n! \cdot a_n$ shows that the last term in the Taylor expansion is an integer.

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

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

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 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 $X_1F_1 + \ldots + X_nF_n = (a_1 + \ldots + a_n)F = d \cdot F$. □

2. 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.

In this section, K will always denote an algebraically closed field. 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 an example for curves with a singular point:

Proposition 2. *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. □

Thus for smooth curves of type $y^2 = g(x)$ we need polynomials g without multiple roots. Actually, this doesn't help much:

Proposition 3. *Assume that $g \in K[X]$ is a polynomial without multiple roots. Then the projective closure of $\mathcal{C} : y^2 = g(x)$ is smooth if and only if $\deg f \in \{1, 2, 3\}$.*

Proof. Homework. □

3. Multiplicity

The fundamental theorem of algebra says that any polynomial of degree $n \geq 0$ has exactly n roots in the complex numbers if we count with multiplicity. The zeros of a polynomial are just the points of intersection of the line $y = 0$ with the curve defined by $y - f(x) = 0$. Is it true that any line intersects the graph of f in n points? Obviously not, since vertical lines seem intersect the graph in just one point.

The situation improves upon introducing the projective plane because we get additional points at infinity as points of intersection. Still, we have to worry about how to count multiplicities. Defining the multiplicity of a point of intersection of two curves is difficult in general; the intersection between lines and curves is easier to understand, so let us do this now. We will do this for points of intersection in the affine plane.

Assume that $\mathcal{C} : f(x, y) = 0$ is an algebraic curve over some algebraically closed field K. The x-coordinates of the points of intersection of $\mathcal{C}$ and the line $\ell : y = mx + b$ satisfy the equation $g(x) = f(x, mx + b) = 0$. Now there are two cases: the polynomial g vanishes; this happens if and only if ℓ is a component of $\mathcal{C}$. If this is not the case, then g has finite degree, and if $P = (a, b)$ is a point on $\mathcal{C} \cap \ell$, then $g(a) = 0$. Thus we can write $g(x) = (x - a)^m h(x)$ for some polynomial h with $h(a) \neq 0$, and we say that ℓ and $\mathcal{C}$ intersect in P with multiplicity m. For lines $x = a$ we similarly define the multiplicity m by $f(a, y) = y^m h(y)$ with $h(b) \neq 0$.

Note that $\deg g \le \deg f$ since cancellation might occur; if this happens, some of the points of intersections are at infinity. Consider e.g. the hyperbola $f(x,y) = xy - 1 = 0$ and the line $y = tx$. We find $g(x) = f(x,tx) = x(tx) - 1$, which has degree 2 for $t \ne 0$ (giving two points of intersection with multiplicity 1 each) and degree 0 if $t = 0$ (implying that there is a point of intersection at infinity with multiplicity 2 – but we will deal with the projective case later).

Proposition 4. *Let T be a tangent to the curve $\mathcal{C} : f(x,y) = 0$ at $P = (a,b)$. Then T and $\mathcal{C}$ intersect with multiplicity ≥ 2 at P.*

Proof. The equation of the tangent is

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

where $f_1 = \frac{\partial f}{\partial x}(a,b)$ and $f_2 = \frac{\partial f}{\partial y}(a,b)$. Assume that $f_2 \ne 0$; then we can solve for y and get $y = -\frac{f_1}{f_2}(x-a) + b$. Plugging this into $f(x,y) = 0$ and observing that $f(x,y) = f(a,b) + f_1(x-a) + f_2(y-b) + \dots$ we get

$$\begin{aligned} g(x) &= 0 + f_1(x-a) + f_2\Big(-\frac{f_1}{f_2}(x-a)\Big) + \dots \\ &= f_1(x-a) - f_1(x-a) + \dots = 0 + \dots, \end{aligned}$$

where the dots represent terms of degree ≥ 2. This proves the claim.

Of course we also have to consider the case $f_2 = 0$ (i.e., $x = a$); I'll leave that to you. □

Let us now define multiplicity for projective curves. Let $\mathcal{C}^\# : F(X,Y,Z) = 0$ be the projective closure of the affine curve $\mathcal{C} : f(x,y) = 0$; thus F is the homogenization of f, and each term in F has degree equal to $n = \deg f$. Let $P = [r : s : t]$ be a point on $\mathcal{C}$, and consider a line $L : aX + bY + cZ = 0$ going through P. For computing the point of intersection, assume first that e.g. $b \ne 0$; then the polynomial $G \in K[X,Z]$ defined by

$$F(X,Y,Z) = F(bX,bY,bZ) = F(bX, -aX - aZ, bZ) = G(X,Z)$$

is a polynomial with the property that the points $[X : Y : Z]$ with $G(X,Z) = 0$ are the points of intersection of L and $\mathcal{C}^\#$. Note first that either $G = 0$ (in this case, the line is a component of $\mathcal{C}^\#$), or G has degree n: in fact, every term in F has the form $a_{ijk}X^iY^jZ^k$ with $i + j + k = n$, and after substituting $bY = -aX - cZ$, all the terms will have degree n. Assume that G has degree n; then we can factor G into linear factors over the algebraically closed field K and get

$$G(X,Y) = (tX - rZ)^m H(X,Z), \quad \text{where } H(r,t) \ne 0.$$

Then we say that L and $\mathcal{C}^\#$ intersect with multiplicity m at P.

If $b = 0$, then we similarly replace cZ by $-aX - bY$ or aX by $-bY - cZ$; it is an easy exercise to show that these methods yield the same result if $abc \ne 0$.

Proposition 5. *Let $\mathcal{C} : F(X,Y,Z) = 0$ be a projective algebraic curve and L a line not contained in $\mathcal{C}$. Then L and $\mathcal{C}$ have exactly $\deg F$ points of intersections, counted with multiplicity.*

Proof. Clear, since the polynomial G constructed above has degree F, hence splits into $\deg F$ linear factors over some algebraically closed field. □

4. Singular Conics and Cubics

Proposition 6. *Singular conics are degenerate.*

Proof. Let P be a singular point on the conic; let Q be any other point. Then the line PQ will intersect the conic at least twice in P and once in Q; by Proposition 5, the line PQ must be contained in $\mathcal{C}$, and this means that the conic is degenerate (it will be a pair of lines). □

Proposition 7. *An irreducible singular cubic has exactly one singular point.*

Proof. If the cubic $\mathcal{C}$ had two singular points P and Q, the line PQ would intersect $\mathcal{C}$ with multiplicity ≥ 4, hence the cubic would contain a line, and therefore be reducible. □

With a little Galois theory we can easily prove more: assume that the defining equation of the cubic has coefficients in some field K of characteristic 0; let σ be any automorphism of the algebraic closure of K. Since P^σ is also a singular point (it satisfies the same equations as P), we conclude that $P = P^\sigma$ because there is only one singularity. Thus P has coefficients in the base field K.