Chapter 4

Study's Lemma

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 $\mathcal{C}_f(K)$.

4.1 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 4.1.1. *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. □

Lemma 4.1.2. *Let $f, g \in K[X,Y]$ be coprime. Then they are also coprime as elements in the larger ring $K(X)[Y]$.*

Proof. Assume that $\gcd(f,g) = p$ for some nonunit $p \in K(X)[Y]$; the denominator of p is a polynomial in X, which in turn is a unit: this means that we may assume that p actually is a polynomial in $K[X,Y]$. Now write $f = pf_1$ and $g = pg_1$ for $f_1, g_1 \in K(X)[Y]$. Let $h(X)$ be the lcm of the denominators of f_1 and g_1; then $h(X)f = pF_1$ and $h(X)g = pG_1$ for polynomials $F_1, G_1 \in K[X,Y]$.

This implies $f/g = F_1/G_1$, hence $fF_1 = gF_1$. This is a relation in the unique factorization domain $K[X,Y]$; but $f \mid gF_1$ and $\gcd(f,g) = 1$ implies $f \mid F_1$. Thus $F_1 = fF_2$, hence $h(X)f = pF_1 = pfF_2$. This shows that $h(X) = pF_2$: but then $p \mid h(X)$, hence p is a unit in $K(X)[Y]$: contradiction. $\square$

Proposition 4.1.3. *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. $\square$

Proposition 4.1.4 (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 4.1.3, f and g are not coprime. Since g is irreducible, we conclude that $g \mid f$. $\square$

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 4.1.5. *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. $\square$

Chapter 5

Tangents

My last lecture as a bachelor. Guess it showed -)

Anyway, her goes ...

In calculus, tangents are defined by a process involving limits. Over arbitrary fields (such as finite fields) this cannot be imitated. Here are a few ways of motivating the definition of a tangent for plane algebraic curves.

5.1 Taylor Expansion for Polynomials

From calculus you know that sufficiently well behaved functions can be developed into a Taylor series. This is definitely true for polynomials, which are the functions we are interested here. One the one hand, proving the Taylor expansion for polynomials over the reals is pretty trivial, on the other hand we would like to apply this tool over arbitrary fields (and rings). Defining the derivative formally is no problem; but if we have a closer look at the Taylor expansion

$$f(x+h) = f(x) + \frac{f'(x)}{1!}h + \frac{f''(x)}{2!}h^2 + \dots$$

we notice the factorials in the denominator: these are, of course, a major problem in particular over finite fields. Luckily, for polynomials, they turn out to be not really there.

Consider e.g. the polynomial

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in R[X]$$

for some domain R. We can avoid the use of calculus for producing the Taylor

series simply by using the binomial theorem:

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

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.

5.1.1

Assume you are given a plane algebraic curve $F(X,Y) = 0$. How do you compute the tangent at (a,b) on this curve? Since the tangent goes through (a,b), it has the form $y - b = m(x-a)$, where m denotes the slope (assuming for the moment that the tangent is not vertical). Here's how: in some vicinity of (a,b) we can write $Y = f(X)$ for some differentiable function f. Now write $F(X,Y) = \sum a_{r,s}X^rY^s$; then taking the derivative of $F(X,Y)$ with respect to X shows $0 = \sum a_{r,s}rX^{r-1}Y^s + \sum a_{r,s}X^rsY^{s-1}Y' = F_X + \frac{dY}{dX}F_Y$, where F_X and F_Y denote the partial derivatives of F with respect to X and Y. Plugging in $(X,Y) = (a,b)$ we find $m = Y' = -F_X(x,b)/F_Y(a,b)$, and this leads to the equation

$$(X-a)F_X(a,b) + (Y-b)F_Y(a,b) = 0$$

for the tangent of the curve in (a,b).

5.1.2

Here's a different way of arriving at this conclusion. Let us first compute the tangent to the circle $X^2 + Y^2 = 2$ in $(1,1)$. The tangent has the equation $Y - 1 = m(X-1)$ for some slope m that we need to determine. This line will be the tangent if and only if $(1,1)$ is its only point of intersection with the circle. For computing the points of intersection, we plug the equation of the tangent into that of the circle and get

$$\begin{aligned}
0 = X^2 + Y^2 - 2 &= X^2 + (m(X-1)+1)^2 - 2 \\
&= X^2 + m^2(X-1)^2 + 2m(X-1) - 1 \\
&= (X-1)(X+1+m^2(X-1)+2m) \\
&= (X-1)(X(m^2+1) - m^2 + 2m + 1)
\end{aligned}$$

Thus we have a tangent if the second factor has $X = 1$ as a root, which happens if and only if $m^2 + 1 = m^2 - 2m - 1$, i.e., i and only if $m = -1$.

How can we generalize this to algebraic curves $F(X, Y) = 0$? Plugging the equation of the line $Y - b = m(X - a)$ we get $F(X, m(X - a) + b) = 0$. By our excursion on Taylor series for polynomials we know

$$F(X, b + m(X - a)) = F(X, b) + m(X - a)F_Y(X, b) + (X - a)^2 \cdot *,$$

where $*$ denotes some polynomial in X. If we plug in $X = a$, then we get 0 on both sides; in particular, $F(X, b)$ has a zero at $X = a$, and this means that $F(X, b)$ is divisible by $(X - a)$. Thus we get

$$\begin{aligned} F(X, b + m(X - a)) &= \frac{F(X, b)}{X - a}(X - a) + m(X - a)F_Y(X, b) + (X - a)^2 \cdot * \\ &= (X - a)\Big[\frac{F(X, b)}{X - a} + mF_Y(X, b) + (X - a) \cdot *\Big] \end{aligned}$$

Now $Y - b = m(X - a)$ will be a tangent if and only if a is also a root of the factor in square brackets. Since there is some $X - a$ in the denominator, we cannot simply plug in $X = a$. Note, however, that $F(X, b) = F(a + X - a, b) = F(a, b) + (X - a)F_X(a, b) + (X - a)^2 \cdot *$, so using $F(a, b) = 0$ we find

$$F(X, b + m(X - a)) = (X - a)[F_X(a, b) + mF_Y(X, b) + (X - a) \cdot *].$$

Thus the square bracket vanishes for $X = a$ if and only if $F_X(a, b) + mF_Y(a, b) = 0$, i.e., if and only if $m = -F_X/F_Y$. This gives the same equation for the tangent as above.

5.1.3

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_X and f_Y denote the partial derivatives at (a, b) with respect to X and Y, respectively, we find

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

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

$$f_X(x - a) + f_Y(y - b) = 0.$$

5.1.4 Example

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.

5.2 Tangents in the Projective Plane

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

$$F(X,Y,Z) = Z^{\deg f} f\Big(\frac{X}{Z}, \frac{Y}{Z}\Big). \tag{5.1}$$

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

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

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

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

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

$$F_X(P)X + F_Y(P)Y + F_Z(P)Z = 0. \tag{5.2}$$

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 (5.2) that this tangent even passes through P. This is a consequence of

Proposition 5.2.1 (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*

$$d \cdot F(X_1, \ldots, X_n) = X_1 F_1 + \ldots + X_n F_n.$$

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 $X_i F_i = a_i F$, hence $X_1F_1 + \ldots + X_nF_n = (a_1 + \ldots + a_n)F = d \cdot F$. □

5.3 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 5.3.1. *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

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

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 5.3.2. *Let $\mathcal{C}_f : f(X,Y) = 0$ be a reducible curve, i.e., $f = gh$ with $\deg g, \deg h \geq 1$. 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. □