

LECTURE 7, THURSDAY MARCH 04, 2004

FRANZ LEMMERMEYER

1. 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 $\deg g \leq \deg f$ 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 $t \neq 0$ (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 1.1. *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 $f_2 \neq 0$; 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

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

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. \square

Another example of lines intersecting curves with multiplicity ≥ 2 is given by

Proposition 1.2. *Let $P = (r, s)$ be a singular point on $\mathcal{C}_f : f(X, Y) = 0$. Then any line through P intersects \mathcal{C} with multiplicity ≥ 2 .*

Proof. Let $P = (a, b)$ be singular and $y = m(x - a) + b$ a line through P . Observe that

$$\begin{aligned} f(x, y) &= f(a, b) + f_1(x - a) + f_2(y - b) \\ &\quad + \text{terms divisible by } (x - a)^2, (x - a)(y - b), \text{ or } (y - b)^2. \end{aligned}$$

Since P is a singular on \mathcal{C} , we have $f(a, b) = f_1 = f_2 = 0$. Plugging in $f(a, b) = 0$ and $y - b = m(x - a)$ shows that $g(x)$ has only terms divisible by $(x - a)^2$, hence the line intersects \mathcal{C} with multiplicity ≥ 2 at P . \square

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. $b \neq 0$; 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

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

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 $abc \neq 0$.

Proposition 1.3. *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. \square

Let us do a few examples. First consider the elliptic curve $E : Y^2 = X^3 + X$ and the line $\ell : X = 0$. It intersects E in $P = (0, 0)$ and at the point at infinity. Let us compute the corresponding multiplicities. Plugging the line equation $X = 0$

into the one for E we end up with $Y^2 = 0$: this is an equation in Y with a double root at P .

For computing the multiplicity at $\mathcal{O} = [0 : 1 : 0]$ we have to work projectively; write $E^\# : Y^2Z - X^3 - XZ^2 = 0$ and $\ell^\# : X = 0$. Plugging this into the equation for $E^\#$ we get $Y^2Z = 0$; this polynomial has a double root at P (as before) and a single root at \mathcal{O} .

We can express the fact that $\ell^\#$ and $E^\#$ intersect twice at P and once at \mathcal{O} by writing

$$\ell^\# \cap E^\# = 2P + \mathcal{O}.$$

The object on the right hand side is called the intersection divisor of $\ell^\#$ and $E^\#$.

2. TYPES OF SINGULARITIES

Using the notion of multiplicity, we can give unified definitions of a couple of objects.

- A point P on a curve \mathcal{C} is called singular if every line through P intersects \mathcal{C} at P with multiplicity ≥ 2 .
- A singular point P is called a double point if at least one line through P intersects \mathcal{C} with exact multiplicity 2.
- More generally, P is said to be singular with multiplicity m if every line through P intersects \mathcal{C} at P with multiplicity m .
- A tangent to \mathcal{C} at a nonsingular point P is the unique (!) line that intersects \mathcal{C} at P with multiplicity 2.
- A line through a singular point P with multiplicity m is called a tangent to \mathcal{C} at P if it intersects \mathcal{C} with multiplicity $\geq m + 1$. Note that there might be more than one such tangent (think of the 5-leaved rose).
- A double point with exactly two tangents is called a node. A double point with a unique tangent is called a cusp.
- A curve \mathcal{C} has a line L as an asymptote if L is a tangent to \mathcal{C} at some nonsingular point at infinity.

As an example for asymptotes, consider the hyperbola $\mathcal{C} : XY = Z^2$. The points at infinity are $P = [0 : 1 : 0]$ and $Q = [1 : 0 : 0]$. The line $L_P : X = 0$ intersects the hyperbola at P with multiplicity 2, hence is an asymptote. Similarly for $L_Q : Y = 0$. The line $Z = 0$ at infinity, on the other hand, intersects \mathcal{C} at P and Q with multiplicity 1.

3. SINGULAR CONICS AND CUBICS

Below, we will work over algebraically closed fields.

Proposition 3.1. *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 1.3, the line PQ must be contained in \mathcal{C} , and this means that the conic is degenerate (it will be a pair of lines). \square

Proposition 3.2. *An irreducible singular cubic has exactly one singular point, and this singular point has multiplicity 2.*

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.

Assume that the singular point P has multiplicity 3; then the line PQ , for $Q \neq P$ any point on \mathcal{C} , would intersect \mathcal{C} with multiplicity ≥ 4 , showing again that \mathcal{C} would have to contain the line. \square

Now we can add something to our knowledge on curves that can be parametrized:

Proposition 3.3. *Every nondegenerate conic with a K -rational point can be parametrized over K .*

Proof. Clear. \square

Let me remind you that this parametrization gives a bijection between the K -rational points on \mathcal{C} and the projective line $\mathbb{P}^1 K$.

Proposition 3.4. *Any singular irreducible cubic can be parametrized over some algebraically closed field K .*

Proof. Let P be the singular point; given any point $Q \neq P$, the line PQ has the form $y = mx + b$ except for the finitely many points of intersection Q_1, \dots, Q_n of the line $x = x_P$ with \mathcal{C} . This line PQ will intersect the cubic at least twice in P and at least once in Q ; since \mathcal{C} has degree 3, it will actually intersect \mathcal{C} with exact multiplicity 2 at P and multiplicity 1 at Q . Thus the points Q on $\mathcal{C} \setminus \{Q_1, \dots, Q_n\}$ correspond bijectively to the elements $m \in K$.

Here's a more computational proof. By shifting the coordinate system (this does not affect the singularity of points), we may assume that the singular point has coordinates $(0, 0)$. Then the cubic must have the form $\mathcal{C} : f(x, y) = 0$ for some $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 - ex^2 - fxy - gy^2 \in K[x, y]$ (no linear terms because $(0, 0)$ is singular; moreover, we cannot have $e = f = g = 0$ since then \mathcal{C} would have a singularity of multiplicity 3). Now consider the lines $y = tx$; plugging this into the equation for \mathcal{C} gives $0 = x^3(a + bt + ct^2 + dt^3) - x^2(e + ft + gt^2) = 0$. Since $x = 0$ corresponds to the known point $(0, 0)$, the second point of intersection Q is given by

$$x = \frac{e + ft + gt^2}{a + bt + ct^2 + dt^3}, \quad y = tx.$$

Each value of t except the three values where the denominator vanishes gives a point with coordinates in K , and all points except the at most three points on the intersection of $x = 0$ and \mathcal{C} are actually hit. \square

If \mathcal{C} has an equation defined over \mathbb{Q} , then Galois theory shows that the singular point P will be rational. In this case, the parametrization will be given by rational functions with rational coefficients.