LECTURE 5, MONDAY FEB. 23, 2004

FRANZ LEMMERMEYER

1. Finite Fields

I discussed the homework and recalled the construction of finite fields as quotients R/I of polynomial rings $R = \mathbb{F}_p[X]$ by certain ideals $I = (f)$, how to compute with the classes $r + I$, and explained why $\mathbb{F}_4 \neq \mathbb{Z}/4\mathbb{Z}$.

2. Projective Closure of Lines

Using the embedding $\mathbb{A}^2K \longrightarrow \mathbb{P}^2K$ we can, of course, also embed algebraic curves. Consider the simplest example, that of a line $L : ax + by + c = 0$. Any point $P = (x, y)$ on L will get mapped to $\iota(P) = [x : y : 1] \in \mathbb{P}^1K$. This point has different presentations; we can write it as $\iota(P) = [\lambda x : \lambda y : \lambda]$ for any $\lambda \in K^\times$. These coordinates all satisfy the equation $aX + bY + cZ = 0$: in fact,

$$a(\lambda x) + b(\lambda y) + c(\lambda) = \lambda(ax + by + c) = 0.$$

We call the set of all points $[X : Y : Z]$ in the projective plane satisfying $aX + bY + cZ = 0$ the projective closure of the line L and denote it by $L^\#$. The zero set of any equation $aX + bY + cZ = 0$ with $(a, b, c) \neq (0, 0, 0)$ is called a projective line.

Let us now investigate what the points at infinity on this line $L^\#$ are; all we have to do is put $Z = 0$ in the equation of the projective line: we get $ax + by = 0$. We cannot have $a = b = 0$, since $ax + by + c = 0$ was supposed to be a line. Now $ax + by = 0$ has the general solution $(x, y) = (\lambda b, -\lambda a)$ for $\lambda \in K$. Thus the only point at infinity on $L^\#$ is the point $[b : -a : 0]$.

Proposition 2.1. *The projective closure of an affine line has exactly one point at infinity.*

The "line" $\{[x : 1 : 0]; x \in K\}$ that we were talking about before is a projective line: it is described as the set of projective solutions of $z = 0$ and is called the line at infinity. We have just seen that every affine line $L : ax + by + c = 0$ intersects the line at infinity in exactly one point $[b : -a : 0]$. Note that, if $b \neq 0$, then $m = -a/b$ is the slope of the line L, and $[1 : m : 0]$ is its point at infinity. Thus every affine line with slope m intersects the line at infinity at $[1 : m : 0]$. In particular, every pair of parallel lines has a point of intersection at infinity, and we have

Proposition 2.2. *Two distinct projective lines have exactly one point of intersection.*

This is of course the most special case of Bezout's theorem that you can imagine (Bezout's theorem states that two curves of degree m and n without common components intersect in exactly mn points, counting multiplicity).

The notion of projective closure makes sense for arbitrary affine curves $\mathcal{C}$ given by $f(x, y) = 0$ for some $f \in K[x, y]$; the image of a point $P = (x, y) \in \mathcal{C}(K)$ in the

projective plane, namely $\iota(P) = [x : y : 1]$, satisfies the equation $F(X, Y, Z) = 0$, where F is the homogenization of f defined by $F(X, Y, Z) = Z^{\deg f} f(\frac{X}{Z}, \frac{Y}{Z})$. Note that the degree of $x^a y^b$ is $a + b$.

3. Parametrization of the Unit Circle

Now let us have a second look at the parametrization of the unit circle $\mathcal{C} : x^2 + y^2 = 1$. We found that the map

$$\phi : \mathbb{A}^1\mathbb{Q} \longrightarrow \mathcal{C} \subseteq \mathbb{A}^2\mathbb{Q} : t \longmapsto \Big(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\Big)$$

gave us all rational points on the unit circle except $P = (-1, 0)$, which – intuitively – would correspond to the value $t = \infty$: but ∞ is not an element of $\mathbb{A}^1\mathbb{Q}$

On the other hand, in $\mathbb{P}^1\mathbb{Q}$ we have a point at infinity. Let us now see whether we can extend the map ϕ to a map between the projective line and the (projective) unit circle. First we clear denominators and set

$$t \longmapsto (1 - t^2 : 2t : 1 + t^2).$$

Next we write $t = \frac{m}{n}$ as a fraction and send t to $[n^2 - m^2, 2mn, n^2 + m^2]$; thus we are led to define the map

$$\phi^{\#} : \mathbb{P}^1\mathbb{Q} \longrightarrow \mathcal{C} \subseteq \mathbb{P}^2\mathbb{Q} : [m : n] \longmapsto [n^2 - m^2, 2mn, n^2 + m^2].$$

This is actually a bijection between the projective line over $\mathbb{Q}$ and the rational points on the unit circle! In fact, $P = (-1, 0)$ is, in its projective incarnation $[-1 : 0 : 1]$, the image of $[m : n] = [-1, 0]$, the point at infinity.

What you can see in this simple example is happening all over the place: results of affine geometry become much simpler if they are stated (and proved) in projective spaces.

4. Projective Closure of Conics and Cubics

Consider a curve $\mathcal{C}$ defined by the equation $f(x, y) = 0$. After embedding it via $(x, y) \longmapsto [x : y : 1]$ into the projective plane, the points $[x : y : 1]$ on $\mathcal{C}$ still satisfy the equation $f(x, y) = 0$, but this equation does not behave well with respect to rescaling: we have $[x : y : 1] = [\lambda x : \lambda y : \lambda]$ for nonzero λ, but $f(\lambda x, \lambda y) \neq 0$ in general. The solution is to homogenize f by multiplying each term in f by the power of Z that gives each term the same degree: if $f(x, y) = \sum a_{ij} x^i y^j$, put $F(X, Y, Z) = \sum a_{ij} X^i Y^j Z^k$, where $k = \deg f - i - j$. Then each term of F has degree $\deg f$, and F has the property $F(\lambda X, \lambda Y, \lambda Z) = \lambda^{\deg F} F(X, Y, Z)$. We say that

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

is the homogenization of f. The points $[x : y : 1]$ with $F(x, y, 1) = 0$ are exactly those satisfying $f(x, y) = 0$. The projective curve $\mathcal{C}^{\#} : F(X, Y, Z) = 0$ is called the projective closure of $\mathcal{C}$, and consists of the affine part $\mathcal{C}$ as well as some (possibly none) points at infinity.

Now consider the three types of conics over $K = \mathbb{R}$:

(1) the ellipse $x^2 + y^2 = 1$;
(2) the parabola $y^2 = x$;
(3) the hyperbola $x^2 - y^2 = 1$.

The projective closure of the circle is the zero set of $X^2+Y^2-Z^2=0$, its points at infinity satisfy $Z=0$ and $X^2+Y^2=0$; since $[0:0:0]$ is not part of $\mathbb{P}^2K$, the real circle does not have any points at infinity.

The points at infinity of the projective closure $\mathcal{C}^{\#}: YZ-X^2=0$ of the parabola satisfy $Z=0$ and $X=0$; there is only one such point, namely $[0:1:0]$, and this point is indeed a point at infinity on $\mathcal{C}^{\#}$.

Finally, the hyperbola has two points at infinity, namely $[1:1:0]$ and $[1:-1:0]$. Note that these points coincide with the points at infinity of the lines $y=x$ and $y=-x$: these are exactly the asymptotes of the hyperbolas, and the asymptotes intersect the hyperbola at infinity.

We can use these facts to *define* that an affine conic defined over a finite field is an ellipse, a parabola or a hyperbola according as it has no, one, or two points at infinity.

For example, if $[x:y:0]$ is a point at infinity on $\mathcal{C}: x^2+y^2=1$, then $x^2+y^2=0$; thus $\mathcal{C}$ does not have a point at infinity over $\mathbb{F}_3$ (hence is an ellipse over $\mathbb{F}_3$), but has two points at infinity over $\mathbb{F}_5$, namely $[1:2:0]$ and $[1:-2:0]$, and therefore $\mathcal{C}$ is a hyperbola over $\mathbb{F}_5$. Question: isn't $[2:1:0]$ a third point at infinity on $\mathcal{C}$?

5. Projective Closure of Weierstrass Cubics

Now consider a Weierstrass cubic

$$E: y^2+a_1y+a_3xy=x^3+a_2x^2+a_4x+a_6.$$

The homogenization of the defining equation is

$$E^{\#}: Y^2Z+a_1YZ^2+a_3XYZ=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3.$$

Putting $Z=0$ gives $X^3=0$, hence the only point at infinity on $E^{\#}$ is $[0:1:0]$. Thus every Weierstrass curve has a single point at infinity, and this point is K-rational (has coordinates in K) for any field K.

6. Calculus 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

$$f(X)=a_nX^n+a_{n-1}X^{n-1}+\dots+a_1X+a_0\in R[X]$$

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.

Summary. So far we have seen how to parametrize conics, and we have seen some examples of curves of higher degree "with a singular point" that can be parametrized. On the other hand, Mason's ABC theorem gave us a tool to show that there exist curves that cannot be parametrized. Our goal is to find out exactly which algebraic curves admit a rational parametrization; the answer will depend on a delicate invariant, the genus of curves, which in turn depends on singular points of the projective closure of the curve. We have just seen what the projective closure is; next on our agenda are singular points.