ALGEBRAIC GEOMETRY

- A Quick Guide -

Huan Q. Bui

Colby College

PHYSICS & MATHEMATICS
Statistics

Class of 2021

February 21, 2020

Preface

Greetings,

This guide is based on MA434: Algebraic Geometry, taught by Professor Fernando Q. Gouvêa. The guide consists of lecture notes and material from *Undergraduate Algebraic Geometry* by Miles Reid. A majority of the text will be reading notes. Some of the proofs won't be complete, but the idea is there for "understanding purposes."

Enjoy!

Contents

Part 1

Plane conics

Part 2

Cubics & The Group Laws

Algebraic geometry: Feb. 7

Simon Xu

Today's lecture covers essentially the first three sections in Reid's book. We will consider some of the simplest algebraic curves. The simplest of all is a line. The first question we need to address is that where should our line live? For now, we want to consider lines in the affine plane.

Definition 1. *Let k be field. Then the affine plane over k, denoted as $\mathbb{A}^2$, is the set $\{(x, y) : x, y \in k\}$.*

For our purpose today, k will always be $\mathbb{R}$. The set of $\mathbb{R}$-points in $\mathbb{A}^2$ in denoted as $\mathbb{A}^2(\mathbb{R})$, and this is merely another way of saying $\mathbb{R}^2$. A line in $\mathbb{A}^2$ is defined by an equation of the form

$$ax + by + c = 0, \qquad a, b, c \in \mathbb{R} \text{ and } a, b \text{ not both } 0.$$

How do we check that this equation actually define a line? The idea is that a line should look like an axis. So consider a parameter t and set $y = t$ (this assumes that $a \neq 0$; if $a = 0$, then instead let $x = t$). Solving for x, we get

$$x = -\frac{1}{a(bt + x)}.$$

Therefore, every points on the curve traced out by this equation can be described by the following pair:

$$(x, y) = \left(-\frac{1}{a(bt + c)}, t\right).$$

There are two ways of interpreting this pair of coordinates. The first interpretation is that this gives a mapping from the t-axis to the line. In fact, it's easy to see that it's an isomorphism with inverse given by $(a, b) \mapsto b$. Another way to look at this situation is that this line can be viewed as a point in the affine plane over the function field $\mathbb{R}(t)$.

It's also worth noticing that the equation defining a line need not to be of degree 1; we can simply take the original equation and take it to n-th power to get a new equation. But the set of zeros of the new equations has to be the same as the set of zeros of the original equation. Thus, they trace out the same line. A perhaps more interesting way is that we could multiply the original polynomial by some polynomial with no real roots. The product clearly will trace out the same line, and the degree of the new polynomial is greater than 1. This is a delicate issue that we will explore more in the future.

The next simplest curve is a circle. Consider the circle given by the equation

$$x^2 + y^2 = 1.$$

This circle has a rational point $(-1, 0)$. Now we can start to draw lines from $(-1, 0)$ that intersect the circle. They will also intersect y-axis at some point. Call the point $(0, t)$. The point this line intersect with the circle will be a function of t, so we can call it $x(t), y(t)$. To see what the coordinates actually are, we can work out the algebra: the equation of the line is $y = tx + t$, and to find $(x(t), y(t))$, we simply plug it back into the circle equation to get

$$\begin{aligned} x^2 + (tx + t)^2 &= 1 \\ x^2 + t^2x^2 + 2t^2x + t^2 - 1 &= 0 \\ (1 + t^2)x^2 + 2t^2x + t^2 - 1 &= 0. \end{aligned}$$

Thus, we need to find the roots of some quadratic polynomial. We already know one of the roots: since the line also intersects the circle at the point $(-1, 0)$, then one of the roots has to be $x = -1$. Now Vieta's formula tells us that product of two roots is given by c/a, so $-x(t) = \frac{t^2-1}{1+t^2}$. Then we have

$$(x(t), y(t)) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

Now it seems that we again have a function from the t-axis to the circle. But note that the map is

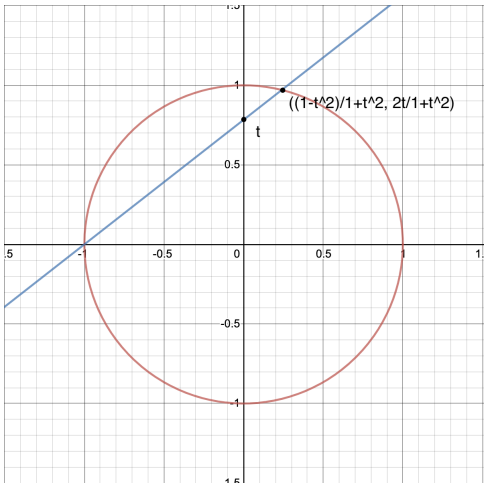


Figure 1: Parametrizing a circle.

not onto (it's one-to-one since $t = \frac{y(t)}{1+x(t)}$): the point $(-1, 0)$ is not in the image of this map. This is expected, if the line intersects at $(-1, 0)$ twice, then we would expect the line to be vertical, or in some sense, to have infinite slope. Therefore, we really want to map ∞ to $(-1, 0)$. Moreover, if we let $t \to \infty$, we get

$$\lim_{t\to\infty} (x(t), y(t)) = \lim_{t\to\infty} \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) = (-1, 0).$$

This matches well with out intuition. Another issue is that for some field (such as $\mathbb{C}$) we can have $1 + t^2 = 0$, which means that the function is not defined at some points on the t-axis. However, this parametrization says that a circle is in fact pretty close to be a line. Moreover, observe that the parametrization is defined over $\mathbb{Q}$, which means plugging any rational number t will produce a rational point on the circle. Since finding rational points on the circle is equivalent to finding Pythagorean triples, this parametrization offers us a way to find all Pythagorean triples. We will make a new definition.

Definition 2. *If a curve can be parameterized by rational functions (i.e. ratios of polynomials), we call it a rational curve.*

In particular, our circle is in fact a rational curve. Now in general, if we replace the equation with any degree 2 equation, fix a point on the curve and start to draw lines through it, we can use a similar method to parametrize this general curve. One would expect this method to work since plugging in a degree 1 equation of a line into the degree two equation will produce again a quadratic equation and everything should proceed in a similar way. So, unless the case is really strange, we expect to be able to parametrize curves traced our by degree 2 polynomials.

As an example, consider the curved traced out by

$$2x^2 + y^2 = 5.$$

It's an ellipse, and it contains the point $(0, \sqrt{5})$. Using this point, we indeed get a parametrization

$$(x(t), y(t)) = \left(\frac{10t}{5 + 2t^2}, \frac{\sqrt{5}(2t^2 - 5)}{5 + 2t^2} \right).$$

Note that this time the rational functions are no longer defined over $\mathbb{Q}$, so we cannot find rational points on this curve via the parametrization. In fact, we don't even know if there's any rational points on the curve by looking at the parametrization. The answer in fact is no, and can be gotten by doing modular arithmetic mod 5: suppose $x = a/c$ and $y = b/c$. Then we have the equation $2a^2 + b^2 = 5c^2$. We can assume that a, b, c have no common factors, but then this forces a and b to be not both divisible by 5. Then all we need to do is to check all the cases in $\mathbb{Z}/5\mathbb{Z}$, and one quickly realizes that this equation has no non-zero solution mod 5. Then it cannot have any non-trivial solution in $\mathbb{Z}$ to begin with. The interesting (and very hard) number theory question is that if we have non-trivial solutions modulo every prime, are we guaranteed to find a non-trivial solution for the original equation. But let's remind ourselves that this is a geometry class and we shall resist the temptation to go any further on this topic.

Finally, let's consider the conics. Let

$$q(x, y) = ax^2 + bxy + cy^2 + dx + ey + f.$$

What are some of the possibilities? We can get

1. A parabola (e.g. $x^2 - y = 0$);
2. a circle (e.g. $x^2 + y^2 = 1$) or an ellipse (e.g. $2x^2 + y^2 = 1$);
3. a hyperbola (e.g. $x^2 - y^2 = 1$);

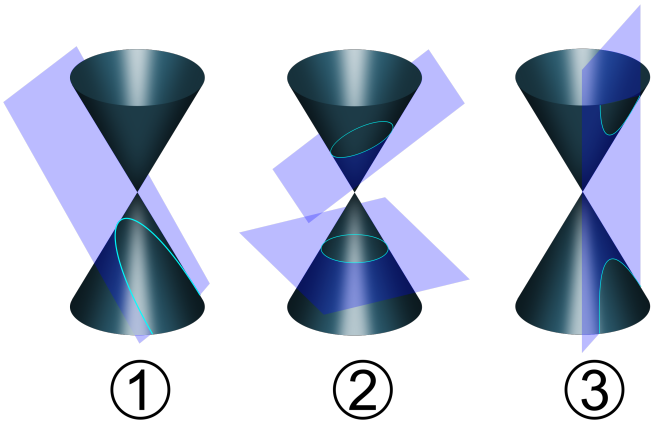


Figure 2: Non-degenerate Conics. Picture credit to Pbroks13 from Wikipedia.

Of course, there are always degenerate cases:

1. A single point (e.g. $x^2 + y^2 = 0$);

2. a single line (e.g. $(x-y)^2=0$);
3. two lines (e.g. $x^2-y^2=0$);
4. no solutions (e.g. $x^2+y^2+1=0$);
5. the entire plane (e.g. $0=0$)

The claim is that these all are the cases. There are at least two ways of proving this: the brute force method and a linear algebra method.

The brute force method. Suppose $a \neq 0$. We can first divide through by a to get

$$x^2+\frac{b}{a}xy+\frac{c}{a}y^2+\frac{d}{a}x+\frac{e}{a}y+\frac{f}{a}=0.$$

The it's just a matter of completing squares:

$$\begin{aligned} x^2+\frac{b}{a}xy+\frac{c}{a}y^2+\frac{d}{a}x+\frac{e}{a}y+\frac{f}{a}&=0\\ x^2+\frac{b}{a}xy+\frac{b^2}{4a^2}y^2+\frac{c}{a}y^2+\frac{d}{a}x+\frac{e}{a}y+\frac{f}{a}&=0\\ (x+\frac{b}{2a}y)^2+(\frac{c}{a}-\frac{b^2}{4a^2})y^2+\frac{d}{a}(x+\frac{b}{2a})+(\frac{e}{a}-\frac{db}{2a^2})y+\frac{f}{a}&=0. \end{aligned}$$

Setting $X=x+\frac{b}{2a}y$, we got a new equation of the form

$$X^2+By^2+DX+Ey+F=0.$$

Now if $B=0$, we are done: if $F\neq 0$, we get a parabola, and if $F=0$, we get some degeneracy. If $B\neq 0$, then completing the square again, we can get it into the form

$$\alpha u^2+\beta v^2+c=0.$$

From here we can get the full classification. This is quite unpleasant and not very insightful.

The linear algebra method. We first observe that

$$ax^2+bxy+cy^2=\begin{bmatrix}x & y\end{bmatrix}\begin{bmatrix}a & b/2\\ b/2 & c\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}.$$

Thus, the original equation can be written as

$$\begin{bmatrix}x & y\end{bmatrix}\begin{bmatrix}a & b/2\\ b/2 & c\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}+\begin{bmatrix}d & e\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}+f=0.$$

A theorem from linear algebra says that any symmetric matrix can be diagonalized via orthogonal matrices; in other words, $\begin{bmatrix}a & b/2\\ b/2 & c\end{bmatrix}=S^{-1}DS$, where D is a diagonal matrix of the form $\begin{bmatrix}A & 0\\ 0 & B\end{bmatrix}$ and $S^{-1}=S^T$. This change of basis amounts to a change of variable and we end up with

$$AX^2+BY^2+\text{stuff}=0,$$

where stuff is of degree 1. From here one can also complete the classification of conics. In fact, one can show that the determinant of the matrix is what determines which conic section this equation produces (as long as you are not in the degenerate case).

If we work over the projective plane, the non-degenerate conics are all the same. One could then think about all the conics, and one see that these conics can be specified by the coefficients of the equations up to some scaling. Then all the conics can be viewed as some subsets of higher dimensional spaces, and one could ask interesting questions there.

The class ends with a challenge. Consider the rational curve parametrized by $t \mapsto (t, t^2, t^3)$ in $\mathbb{A}^3$. This is called the twisted cubic. It's in fact non-planar. The challenge is to find the polynomials that cut out this curve.

The Projective Plane and Line at Infinity: Feb. 10

Christopher Toborg

Today's lecture details chapters 1.4-1.6 in Reid's book, and is all about the projective plane and what is known as the "line at infinity". It also details how the conic sections are actually all the same shape in the projective plane.

Definition (Projective Plane): Beginning with $\mathbb{R}^3$, remove the origin and setup and equivalence relation defined by $(x,y,z)\sim(\lambda x,\lambda y,\lambda z)$ for any $\lambda\neq 0$. We denote this equivalence as [x:y:z], representing the ratios between x,y, and z. This forms a projective plane, which we denote as $\mathbb{P}^2$.

There are two key advantages of working in the projective plane. The first is that it removes some exceptions of working in $\mathbb{R}^3$. Most notably, all lines in the projective plane intersect at some point. The second advantage is that the projective plane is bounded.

Definition (Line at Infinity): The set of points in the equivalence class: { [x:y:0] } is defined to be the line at infinity.

A line passing through the line at infinity has equation Ax+By=0. In $\mathbb{R}^3$, this line has equation Ax+By+C=0, so all lines of the same slope pass through the same line at infinity. As a result, lines in $\mathbb{R}^3$ that are parallel intersect at the line at infinity in $\mathbb{P}^2$.

Definition (Homogenous Polynomial): A polynomial is said to be homogenous if all of its monomials are of the same degree.

While working in $\mathbb{P}^2$, only equations of homogeneous polynomials that equal zero make sense to work with. To determine where two lines intersect, we begin with their equations in $\mathbb{R}^2$, say y=mx+b and y=mx+d. Converting these equations to coordinates in $\mathbb{P}^2$ gives $\frac{y}{z} = m\frac{x}{z} + b$ and $\frac{y}{z} = m\frac{x}{z} + d$. To convert these equations to homogenous polynomials, we multiply through by z and set them equal to zero, resulting in y-mx-bz=0 and y-mx-dz=0. If we want to determine where these lines intersect at infinity, we know that z=0 there, and since the ratio between the y and x coefficients is 1:m, the equation of the line at infinity at which these lines intersect is [1:m:0].

Definition (Projectivity): A projectivity of $\mathbb{P}^2$ is a function T(x)=Mx where M is a 3x3 invertible matrix.

We are able to use projectivities and orthonormalization to ensure that any conic section in $\mathbb{P}^2$ can be written in the form [x y z]M$[x\ y\ z]^T$ where M is a diagonal 3x3 matrix. After changing variables, any conic section in $\mathbb{P}^2$ can be written as $\boldsymbol{\alpha} x^2 + \boldsymbol{\beta} y^2 + \boldsymbol{\gamma} z^2 = 0$ where $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \{1, -1, 0\}$. When they are written like this, they have the following properties based on their coefficients:

$x^2 + y^2 + z^2 = 0$	Empty
$x^2 + y^2 - z^2 = 0$	Non degenerate conic
$x^2 + y^2 = 0$	Point
$x^2 - y^2 = 0$	Two lines
$x^2 = 0$	One line

An ellipse in $\mathbb{P}^2$ does not intersect the line at infinity. A parabola in $\mathbb{P}^2$ intersects the line at infinity once, while a hyperbola in $\mathbb{P}^2$ intersects the line at infinity twice. Topologically, all conics in $\mathbb{P}^2$ are circles since the parabola and hyperbola intersect at the line at infinity.

Algebraic Geometry: Feb. 12

Therese Surrette

To start, we thought back to the last class when we discussed what the conics might look like in projective space. Similar to $\mathbb{R}^2$, there are a limited number of conics in projective space of $\mathbb{R}$, $\mathbb{P}^2(\mathbb{R})$, which are the following:

$X^2 + Y^2 + Z^2 = 0$ which are the empty set

$X^2 + Y^2 - Z^2 = 0$ the non-degenerate conics (ellipses, hyperbola, parabolas)

$X^2 + Y^2 = 0$ the point [0:0:1]

$X^2 - Y^2 = 0$ two lines

$X^2 = 0$ one line

These are all possible conics in $\mathbb{P}^2(\mathbb{R})$ up to a change in variable. Now we will take a look more at conics in $\mathbb{P}^2(\mathbb{R})$. We want to show that the conics are rational curves in projective space, meaning that we can parameterize them by a polynomial/rational function of the line.

Conic roots are rational:

Looking at the non-degenerate conics, $X^2 + Y^2 - Z^2$ or $X^2 + Y^2 = Z^2$, we showed that in $\mathbb{R}$ we could parameterize the affine part $x^2 + y^2 = 1$ as $t \mapsto ((1-t^2)/(1+t^2), (2t)/(1+t))$.

We now want a projective parameterization by making it a triple and scaling it. A mapping which takes the variable t to projective space $t \mapsto [1 + t^2 : 2t : 1 + t^2]$ does not quite work because t is affine so it does not include the point $[-1 : 0 : 1]$. This means we want to use a mapping from the projective line for this parameterization. What we want to do is take two coordinates $[T : S]$, which should be equivalent when we scale and we get the parameterization

$$[T : S] \mapsto [S^2 - T^2 : 2TS : S^2 + T^2]$$

which will be well defined when dealing with homogeneous polynomial. This parameterization now includes the previously missing point, as [1: 0] maps to [-1; 0; 1].

Although this parameterization works, the parameterization which Miles Reid uses in his book is different and involves a change of variables. In his version we have: $X_1 = X + Z, Y_1 = -X + Z, Z_1 = Y$ and our new equation gives us $-X_1Y_1 + Z_1^2 = 0$ which we can now rewrite as $X_1Y_1 = Z_1$. Reid then wants us to swap Y_1 and Z_1 to get $XZ = Y^2$.

From this, Reid gets the parameterization

$$[U : V] \mapsto [U^2 : UV : V^2]$$

and now we have found all monomials of degree 2 in one triple. We have embedded the line into $\mathbb{P}(\mathbb{R})$ which will help us when intersecting conics.

Notice that $[U : V]$ is in $\mathbb{P}^1$ and $[U^2 : UV : V^2]$ is a non-degenerate conic in $\mathbb{P}^2$. The motivation behind this is if we want to intersect conics with curves we want to plug in equations to find U and V.

Now we want to think about the **forms of degree d in two variables**. Here, "form" means a homogeneous polynomial, i.e., something that looks like

$$F(U, V) = a_d U^d + a_{d-1} U^{d-1} V + ... + a_1 U V^{d-1} + a_0 V^d$$

where a_j are not all 0.

Going back to affine space where V=1 we get

$$f(u) = a_d u^d + ... + a_1 u + a_0$$

which may not end up being degree d depending on which a_j from the polynomial above were 0. We want to find the roots of this polynomial. We have that if $f(\alpha) = 0$ then $F(\alpha, 1) = 0$. So if $\alpha = 0$, then we can factor out to $f(u) = (u - \alpha)g(u)$ which is equivalent to $F(U, V) = (U - \alpha V)G(U, V)$. The roots still give factors, but $F(U, V)$ has an extra root where $V = 0$. Then we have that $F(1, 0) = 0$ is equivalent to $ad = 0$ which is equivalent to $F(U, V) = VG(U, V)$, so if a polynomial has enough roots and enough V here, we can completely factor out our polynomial into degree one terms.

Multiplicity of a root

Next, we want to define the multiplicity of a root. If $F(\alpha, 1) = 0$, the multiplicity of α, $m(\alpha)$ is the highest power of $(U - \alpha V)$ that we can factor out. For example, when $F(1, 0)$, $m([1 : 0])$ is the highest power of V which is equal to d- degree of $f(u)$.

This gives us the result that the number of roots of $F(U, V) = 0$ counted with multiplicity must be less than d (over an algebraically closed field, it is equal to d). Even on the projective line, with this form of equation you still get at most d roots.

We can use this to get a count of how many intersections there are between curves. A general theorem, Bezout's theorem, says that given two curves C and D where degree of C is m and degree of D is n, then the number of intersections between these two curves is mn. This theorem is too difficult to prove at this point, but a simpler result is the number of intersections of a curve and a line.

Suppose we have a curve $C = F(X, Y, Z)$ of degree n in $\mathbb{P}^2$ and a line in $\mathbb{P}^2$ given by $L : \alpha x + \beta y + \gamma z = 0 = \{[X(U, V) : Y(U, V) : Z(U, V)]\}$. Plug $X = X(U, V), Y = Y(U, V), Z + Z(U, V)$ into $F(X, Y, Z)$ to get $G(U, V) = 0$. What is the degree of G? Plugging a degree 1 equation into a monomial makes G homogeneous of degree 1. This means there are at most n roots and at most n intersections (exactly n over algebraically closed fields). This means that we can now connect the algebra and geometry of these curves. If we want to see geometrically if a curve has a certain degree we can choose any line and look at how many time it intersects a curve. In an algebraically closed field, the number of intersections will be exactly the degree of the curve.

Another question we can ask is what happens when we intersect a curve with a (non-degenerate) conic Q? When we parameterize $Q = [U^2 : UV : V^2]$ and again plug in, we get an equation $G(U, V) = 0$ of degree 2n, so there will be at most 2n intersections (exactly 2n for algebraically closed fields).

What makes Bezout's theorem so difficult is that this result is dependent on being able to parameterize lines and non-degenerate conics, but most curves cannot be parameterized. So, another question to ask is what happens when we intersect a curve with degenerate conics. The empty conic and single point conic are not interesting, but what is is the conic which is 2 lines. We can factor out this conic into $(X + Y)(X - Y) = 0$, but it is still difficult to parameterize these kinds of curves. There is also a possibility that in the degenerate case, two curves can share entire sections which is infinitely many points. This means if we want to look at the case of degenerate conics, we want to look at those cases where they do not have entire components in common.

This whole idea of being able to find an exact number of intersections over algebraically closed fields inspired mathematicians to think of $\mathbb{C}$ as the place where they should be looking at these curves. There are issues with looking at $\mathbb{C}$ though because many things don't look nice in $\mathbb{C}$ For example, the projective plane in $\mathbb{R}$ is a circle, but in $\mathbb{C}$ it is a sphere. This leads to the question which is: what would complex conics look like in projective space?

♡ Topics in Abstract Algebra: Valentines Day ♡

Lecture by Annie, Lanie, and Fernando
Notes by Joshua Schluter

Annie and Lanie's Part

Last Time (1.9):
If L is a line in $\mathbb{P}^2$ and D is a curve of degree d, then L and D intersect at most d times.
Similarly, if C is a nondegenerate conic in $\mathbb{P}^2$, then C and D intersect at most 2d times.

Corollary (1.10):
Let $\heartsuit_1, \heartsuit_2, \heartsuit_3, \heartsuit_4, \heartsuit_5 \in \mathbb{P}^2$ be distinct points such that no four points are collinear. There exists at most one conic that goes through all $\heartsuit_1, \heartsuit_2, \heartsuit_3, \heartsuit_4, \heartsuit_5$.

Proof:
For the sake of contradiction, let $C_1 \neq C_2$ be conics that contain all five points. Thus, $\{\heartsuit_1, \heartsuit_2, \heartsuit_3, \heartsuit_4, \heartsuit_5\} \subset C_1 \cap C_2$.

Case 1: Both C_1 and C_2 are nondegenerate.
Since both conics are nondegenerate, they are equivalent to $XZ = Y^2$ or $(U, V) \mapsto (U^2, UV, V^2)$ which are degree 2. Thus, by 1.9, they intersect at most $2n = 2(2) = 4$ times but C_1 and C_2 must intersect at least 5. Thus case 1 is impossible.

Case 2: One conic is degenerate and the other is nondegenerate.
WLOG: Assume C_1 is the degenerate conic. C_1 will be either a line or a line pair while C_2 is a nondegenerate conic. By 1.9, C_2 will intersect with each line of C_1 at most 2 times. Thus, C_1 and C_2 intersect at most $2+2 = 4$ times but they must intersect at least 5 times. Thus case 2 is impossible.

Case 3a: Both degenerate, don't share a line.
C_1 and C_2 will either be lines or line pairs. Each line of C_1 will intersect with each line of C_2 at most 1 time. Thus C_1 and C_2 will intersect at most $1+1+1+1 = 4$ times but they must intersect at least 5 times. Thus case 3a is impossible.

Case 3b: Both degenerate, share a line.
Since they share a line, we can write $C_1 = L_0 \cup L_1$ and $C_2 = L_0 \cup L_2$. Thus $\{\heartsuit_1, \heartsuit_2, \heartsuit_3, \heartsuit_4, \heartsuit_5\} \subset C_1 \cap C_2 = L_0 \cup (L_1 \cap L_2)$. But note that $L_1 \cap L_2$ can only contain 1 point. Thus, the other four points must lie on the line L_0 but they can't because no four points are collinear. Therefore case 3b is impossible.

Since each case is impossible, our assumption that $C_1 \neq C_2$ must have been wrong. ■

Lets define $S_2 = \{\text{Quadratic forms in } \mathbb{R}^3\} = \{3 \text{ by } 3 \text{ symmetric matrices}\} \cong \mathbb{R}^6$.

Lets fix $\heartsuit_0 = (X_0, Y_0, Z_0) \in \mathbb{P}^2(\mathbb{R})$. Now, we can define $S_2(\heartsuit_0) = \{Q \in S_2 \text{ such that } Q(\heartsuit_0) = 0\}$. For any $Q \in S_2(\heartsuit_0)$ we can write $Q(X_0, Y_0, Z_0) = aX_0^2 + bX_0Y_0 + \cdots + fZ_0^2 = 0$ which is a single linear equation with 6 variables: a,b,c,d,e,f. Thus, $\dim S_2(\heartsuit_0) = 5$.

Similarly, lets fix $\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots \heartsuit_n \in \mathbb{P}^2(\mathbb{R})$ and define $S_2(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots \heartsuit_n) = \{Q \in S_2 \text{ such that } Q(\heartsuit_i) = 0 \text{ for } i = 1, 2, 3, \cdots n\}$. Instead a single linear equation, this gives us n linear equations with 6 variables each. Thus, $\dim S_2(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots, \heartsuit_n) \geq 6 - n$.

Corollary (1.11):
If $n \leq 5$ and no 4 points are collinear then $\dim(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots, \heartsuit_n) = 6 - n$.

Proof:
We will first show that $\dim(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots, \heartsuit_n) \leq 6 - n$

Case $n = 5$:
$\dim S_2(\heartsuit_1, \heartsuit_2, \heartsuit_3, \heartsuit_4, \heartsuit_5) \leq 1 = 6 - 5 = 6 - n$. (by 1.10)

Case $n \leq 4$:
Pick 5-n points so that no 4 are collinear. This will give us a total of 5 points. Thus $1 = \dim(\heartsuit_1, \heartsuit_2, \heartsuit_3, \heartsuit_4, \heartsuit_5) \geq \dim S_2(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots, \heartsuit_5) - (5 - n)$. Adding $5 - n$ to both sides, we get $6 - n \geq \dim S_2(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots, \heartsuit_5)$.

We combine this with our previous result that $6 - n \leq \dim S_2(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots, \heartsuit_5)$ to get $6 - n = \dim S_2(\heartsuit_1, \heartsuit_2, \heartsuit_3, \cdots, \heartsuit_5)$. ■

Fernando's Part

Finding Tangent Lines in Affine and Projective Spaces

Affine Lets say we have a curve $f(x,y)=0$.
We want to find the tangent line at a point $\heartsuit=(x_0,y_0)$ on the curve.
Thankfully, $\nabla f(x_0,y_0)=(\frac{\delta f}{\delta x}(x_0,y_0),\frac{\delta f}{\delta y}(x_0,y_0))$ will always be tangent to our curve.
Thus, if (x,y) is on the targent line, then $\nabla f\cdot(x-x_0,y-y_0)=0$.
So $\frac{\delta f}{\delta x}(\heartsuit)(x-x_0)+\frac{\delta f}{\delta y}(\heartsuit)(y-y_0)=0$.
Thus our tangent line can be written as $\frac{\delta f}{\delta x}(\heartsuit)x+\frac{\delta f}{\delta y}(\heartsuit)y+(\frac{\delta f}{\delta x}(\heartsuit)x_0+\frac{\delta f}{\delta y}(\heartsuit)y_0)=0$.

Projective We can naively convert this equation as follows:
$\frac{\delta f}{\delta x}(\heartsuit)X+\frac{\delta f}{\delta y}(\heartsuit)Y+(\frac{\delta f}{\delta x}(\heartsuit)x_0+\frac{\delta f}{\delta y}(\heartsuit)y_0)Z=0$
The problem is that this equation includes $\frac{\delta f}{\delta x}$ and $\frac{\delta f}{\delta y}$ which refer to f, which isn't the projective equation.

So we let $F(X,Y,Z)=Z^d f(\frac{X}{Z},\frac{Y}{Z})$ where d is the degree of f.
Now, we calculate that $F_X=Z^d(\frac{\delta f}{\delta x}\frac{1}{Z}+\frac{\delta f}{\delta y}0)=Z^{d-1}\frac{\delta f}{\delta x}(\frac{X}{Z},\frac{Y}{Z})$
Similarly, $F_Y=Z^{d-1}\frac{\delta f}{\delta y}(\frac{X}{Z},\frac{Y}{Z})$.
Finally, we calculate that $F_Z=dZ^{d-1}f(\frac{X}{Z},\frac{Y}{Z})+Z^d(-\frac{\delta f}{\delta x}(\frac{X}{Z},\frac{Y}{Z})\frac{X}{Z^2}-\frac{\delta f}{\delta y}(\frac{X}{Z},\frac{Y}{Z})\frac{Y}{Z^2})$.

F_Z looks complicated until we plug in a point $\heartsuit=[X_0:Y_0:Z_0]$ on our curve.
Since $\heartsuit$ is on our curve, $f(X_0/Z_0,Y_0/Z_0)=0$. Thus,

$$F_X(\heartsuit)=Z_0^{d-1}\frac{\delta f}{\delta x}(\heartsuit)$$

$$F_Y(\heartsuit)=Z_0^{d-1}\frac{\delta f}{\delta y}(\heartsuit)$$

$$F_Z=Z_0^{d-1}\left(-\frac{\delta f}{\delta x}(\heartsuit)\frac{X_0}{Z_0}-\frac{\delta f}{\delta y}(\heartsuit)\frac{Y_0}{Z_0}\right)$$

Substituting these into our naive equation, we get:
$\frac{1}{Z_0^{d-1}}F_X(\heartsuit)X+\frac{1}{Z_0^{d-1}}F_Y(\heartsuit)Y+\frac{1}{Z_0^{d-1}}F_Z(\heartsuit)Z=0$.
Finally, we multiply everything by Z_0^{d-1} to get the following elegant projective tangent line equation: $F_X(\heartsuit)X+F_Y(\heartsuit)Y+F_Z(\heartsuit)Z=0$.

February 17th: The Intersection of Conics and a Pencil of Conics

Lily Santonelli

Today's lecture covers sections 1.12 to 1.14 in Miles Reid's book *Undergraduate Algebraic Geometry*. These sections focus on the intersection of conics as well as a pencil of conics. In these notes, we will investigate these topics through definitions, propositions, and examples.

Section 1.12: Intersection of Conics

Given 4 points P_1,...,P_4 in $\mathbb{P}2$, under the condition that $S2(P_1 \dots P_4)$ is a 2-dimensional vector space. Recall that S2 is the space of all conics of quadratic form on $\mathbb{R}^3$, which is essentially the set of 3x3 symmetric matrices. Then, by choosing a basis Q_1, Q_2 for $S2(P_1 \dots P_4)$, we are given two conics C_1 and C_2 such that $C_1 \cap C_2 = \{P_1 \dots P_4\}$.

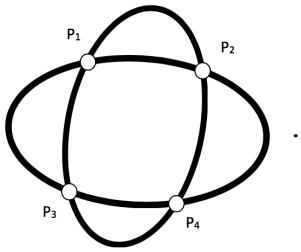
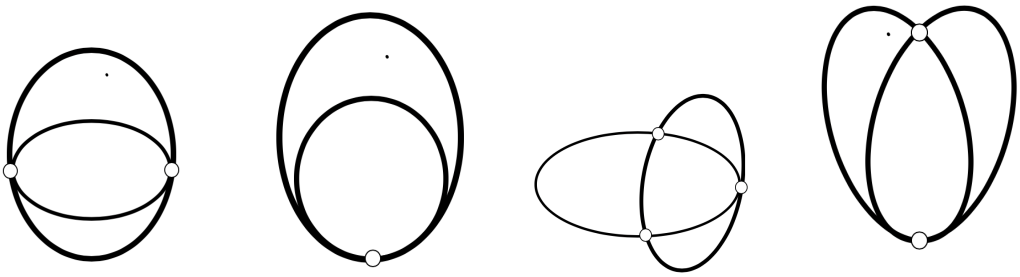


Figure 1: 4 Points of Intersection

Reid's Examples:



Section 1.13: A Pencil of Conics

In section 1.13, the main focus is degenerate conics in a pencil. Let's begin by defining a pencil of conics.

Definition: A Pencil of Conics

A family of the form $C(\lambda, \mu) = (\lambda Q_1 + \mu Q_2 = 0)$. Each element is a plane curve and the elements are parameterized by $\mathbb{P}^1$. We can think of the ratio $(\lambda : \mu)$ as a point in $\mathbb{P}^1$.

As one might expect, for special values of λ and μ the conic $C(\lambda, \mu)$ is degenerate. Let's consider detQ for the determinant of the symmetric 3x3 matrix corresponding to the quadratic form Q. When detQ = 0, the conic is degenerate. Then, it is clear that:

$$C(\lambda, \mu) \text{ is degenerate } \iff \det(\lambda Q_1 + \mu Q_2) = 0.$$

The elements Q1 and Q2 can also be written as 3x3 symmetric matrices. Below this can be expressed as:

$$F(\lambda, \mu) = det|\lambda \begin{bmatrix} a & b & d \\ b & c & e \\ d & e & f \end{bmatrix} + \mu \begin{bmatrix} a' & b' & d' \\ b' & c' & e' \\ d' & e' & f' \end{bmatrix}| = 0$$

Recall that we write $Q_1 = aX^2 + 2bXY + \ldots + fZ^2$ and Q_2 is of similar form, but uses coefficients $a', b', ..., f'$; note that these are the entries to each of the matrices. In addition, $F(\lambda, \mu)$ is a homogeneous degree 3 form in λ and μ. By applying what we learned in Section 1.8 to F, we can derive the following proposition:

Proposition:

Suppose $C(\lambda, \mu)$ is a pencil of conics in $\mathbb{P}^2(K)$, with at least one non-degenerate conic. Then the pencil has at most 3 degenerate conics. If $K = \mathbb{R}$, then the pencil has at least one degenerate conic.

Proof:

A cubic form has at least 3 roots by Section 1.8. In addition, over R, it must have at least one root.

Example 1:

Suppose that we start from the pencil of conics generated by the circle, $Q_1 : X^2+Y^2-Z^2 = 0$, and the hyperbola, $Q_2 : X^2-Y^2+Z^2 = 0$. Then, we can derive the following: $(\lambda+\mu)X^2+(\lambda-\mu)Y^2+(\mu-\lambda)Z^2 = 0$. Consider when $\lambda = 2$ and $\mu = 1$ so we have $3X^2+Y^2-Z^2 = 0$.

This can be rewritten as $3X^2 + Y^2 = 1$. No consider when $\lambda = 1$ and $\mu = 2$ so we derive the equation $3X^2 - Y^2 + Z^2 = 0$. Notice that when $\lambda = \mu$, we are given the y axis so $X^2 = 0$.

Now let's compute $F(\lambda, \mu)$. Given the equations for Q_1 and Q_2 above, $F(\lambda, \mu)$ can be written as the following:

$$\mathrm{F}(\lambda,\mu) = det|\lambda \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} + \mu \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix}| = det| \begin{bmatrix} \lambda+\mu & 0 & 0 \\ 0 & \lambda-\mu & 0 \\ 0 & 0 & \mu-\lambda \end{bmatrix}|$$

$$= (\lambda+\mu)(\lambda-\mu)(\mu-\lambda)$$

$$= -(\lambda-\mu)^2(\lambda+\mu)$$

Consider when $\lambda = 1$ and $\mu = -1$. Then, we have $(\lambda-\mu)^2(\lambda+\mu) = (1-(-1))^2(1+(-1)) = 0$.

Finally, let's investigate the procedure for finding the points of intersection. First, consider starting from the pencil of conics generated by Q_1, Q_2 in affine form such that $Q_1 = Y^2 + rY + sX + t$ and $Q_2 = Y - X^2$. We will try to find the points $P_1 \dots P_4$ of intersection. Let's plug in $Y = X^2$ into Q_1. Then, Q_1 can be rewritten as $X^4 + rX^2 + sX + t$. This equation is referred to as a "Depressed Quartic." This shows that we can convert every generic quartic into a depressed quartic following a change of variable; this allows us to recover the roots of the original quartic more easily using the depressed quartic.

In order to find the intersection points we must (1) find the 3 ratios $(\lambda : \mu)$ for which $C(\lambda : \mu)$ are degenerate conics, (2) Separate out 2 of the degenerate conics into pairs of lines and (3) the four points P_i are the points of intersection of the lines. When separating out the 2 of the degenerate conics into pairs of line, we get three values of μ/λ for which the conic $\lambda Q_1 + \mu Q_2$ breaks up as line pairs. The cubic equation whose roots are these 3 values is called the "auxiliary cubic" associated with the quartic.

Problem Day 1

Ethan Pullen

February 19 2020

1 Problem 1.6

Let k be a field with at least 4 elements, and $C : (XZ = Y^2)$ prove that if $Q(X, Y, Z)$ is a quadratic form which vanishes on C then $Q = \lambda(XZ - Y^2)$

1.1 Proof

Let $Q(X, Y, Z)$ be a quadratic such that it vanishes on $C : (XZ = Y^2)$. We can write out the equation for $Q = aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2$. We can now move the $2dXZ$ with part of cY^2 to achieve,

$$Q = 2d(XZ - Y^2) + aX^2 + 2bXY + (c - 2d)Y^2 + 2eYZ + fZ^2$$

Since $C : (XZ = Y^2)$, $Q[0 : 0 : 1] = 0 = f$, so $f = 0$. We can now rewrite Q,

$$Q = 2d(XZ - Y^2) + aX^2 + 2bXY + (c - 2d)Y^2 + 2eYZ$$

we can use the points $[1 : y : y^2] \in C$. Since Q vanishes over C, $Q[1 : y : y^2] = 0 = a + 2by + (c - 2d)y^2 + 2ey^3$. We are left with a cubic, but since k is a field with at least 4 elements, there are at least 4 zeroes of our cubic. The only way for that to happen is for all of the coefficients to be 0. We can now write,

$$Q = 2d(XZ - Y^2) + 0 * X^2 + 2bXY + 0 * Y^2 + 0 * YZ = 2d(XZ - Y^2)$$

Thus, $Q = \lambda(XZ = Y^2)$ where $\lambda = 2d$.

2 Problem 1.7

In R^3, consider the two planes $A : (Z = 1)$ and $B : (X = 1)$; a line through 0 meeting A in $(x, y, 1)$ meets B in $(1, \frac{y}{x}, \frac{1}{x})$. Consider the map $\phi : A \to B$ defined by $(x, y) \mapsto (y' = \frac{y}{x}, z' = \frac{1}{x})$; what is the image under ϕ of

2.1 the line $ax = y + b$

The line $ax = y+b$ is a pencil of parallel lines each with slope a. We will start by looking at where ϕ sends a line. Our mapping sends $(x, y) \mapsto (y' = \frac{y}{x}, z' = \frac{1}{x})$. We can solve our equation of a line for $\frac{y}{x}$ by subtracting b and dividing by x, $\frac{y}{x} = a + \frac{b}{x}$. So, $\phi : ax = y + b \mapsto (1, a - \frac{b}{x}, \frac{1}{x})$. $(1, a - \frac{b}{x}, \frac{1}{x})$ is a line with the equation $y = a - bz$. Since b can vary, our group of parallel lines in A are now a pencil of lines on the $x = 1$ plane with varying slopes that all go through $(1, a, 0)$.

2.2 circles $(x - 1)^2 + y^2 = c$ for variable c

We break this into 3 cases on c.
Case $c > 1$:
If $c > 1$, ϕ sends our circle equation to $(1, \frac{\pm\sqrt{c-(x-1)^2}}{x}, \frac{1}{x})$. We will let $\alpha = c - 1 > 0$, so we have $(1, \pm\sqrt{\frac{\alpha}{x^2} + \frac{2}{x} - 1}, \frac{1}{x})$. We can now write an equation, $y = \pm\sqrt{\alpha z^2 + 2z + 1}$, so $y^2 - \alpha z^2 - 2z + 1 = 0$. This is the equation of a hyperbola since α is positive.
Case $c = 1$:
If $c = 1$, ϕ sends our circle equation to $(1, \frac{\pm\sqrt{c-(x-1)^2}}{x}, \frac{1}{x}) = (1, \frac{\pm\sqrt{1-(x-1)^2}}{x}, \frac{1}{x}) = (1, \frac{\sqrt{2x-x^2}}{x}, \frac{1}{x}) = (1, \pm\sqrt{\frac{2}{x} - 1}, \frac{1}{x})$. So, $y = \pm\sqrt{2z - 1}$ giving us a parabola $y^2 - 2z + 1 = 0$.
Case $c < 1$:
If $c < 1$, ϕ sends our circle equation to $(1, \frac{\pm\sqrt{c-(x-1)^2}}{x}, \frac{1}{x})$. We will let $\alpha = -1 + c > 0$, so we have $(1, \pm\sqrt{-\frac{\alpha}{x^2} + \frac{2}{x} - 1}, \frac{1}{x})$. We can now write an equation, $y = \pm\sqrt{-\alpha z^2 + 2z + 1}$, so $y^2 + \alpha z^2 - 2z + 1 = 0$. This is the equation of an ellipse since α is positive.

3 Problem 1.8

3.1 Let $P_1, P_2, P_3, P_4 \in P^2$ with no 3 collinear. Prove that there is a unique coordinate system in which the 4 points are (1, 0, 0), (0, 1, 0), (0, 0, 1) and (1,1,1).

We want to define a linear transformation M such that:
$(1,0,0) \mapsto P_1$
$(0,1,0) \mapsto P_2$
$(0,0,1) \mapsto P_3$
$(1,1,1) \mapsto P_4$ Since $P_1, P_2, P_3, P_4 \in P^2$ we are allowed to scale them so that $P_1 + P_2 + P_3 = P_4$ No 3 points are collinear, so P_1, P_2, P_3 span R^3 which means there is some α, β, γ with $\alpha P_1 + \beta P_2 + \gamma P_3 = P_4$. So we want M to map each standard unit to its scaled version in P^2.
$M(1,0,0) = \alpha P_1$, $M(0,1,0) = \beta P_2$, $M(0,0,1) = \gamma P_3$
This will force $M(1,1,1) = P_4$. Thus our transformation to the coordinate system is simply M^{-1}.

3.2 Find all conics passing through $P_1 ... P_5$, where $P_5 = (x, y, z)$ is some other point

Let C be our conic, $C : aX^2 + 2bXY + cY^2 + 2dXZ + 2eYZ + fZ^2 = 0$. Since P_1, P_2, P_3 are on the curve, the points $(1,0,0), (0,1,0), (0,0,1)$ are zeroes on the conic, this means $a, c, f = 0$. Now we have $2bXY + 2dXZ + 2eYZ = 0$. P_4 is also on the curve, so $(1,1,1)$ is also a zero, thus $b + d + e = 0$. Using P_5, $bxy + dxy + eyz = 0$. We now have 2 equations for 3 variables, which means we have one solution in P^2.

3.3 Corollary 1.10

If $P_1 ... P_5 \in P^2$ are distinct points such that no 4 are collinear, then there exists at most one conic through $P_1 ... P_5$
We have shown that there is a unique way to move our coordinates to our new space and also that each time we add a fifth point, we define a single conic. Suppose there were 2 conics that go through all 5 points. This means there are 2 distinct ways to convert our coordinates, and the transformation would not be unique, thus it is impossible for 2 conics to exist.

4 Problem 1.10 and 1.11

Two forms on an algebraically closed field share a root if and only if Sylvester's Determinant is 0.

$$\begin{bmatrix}
\alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_n & 0 & 0 & \dots & 0 \\
0 & \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_n & 0 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & 0 & \dots & 0 & \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_n \\
\beta_0 & \beta_1 & \beta_2 & \dots & \beta_m & 0 & 0 & \dots & 0 \\
0 & \beta_0 & \alpha_1 & \beta_2 & \dots & \beta_m & 0 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & 0 & \dots & 0 & \beta_0 & \beta_1 & \beta_2 & \dots & \beta_m
\end{bmatrix}$$

4.1 Generalized Proof

Let A be an n degree form and B be an m degree form. We will assume A and B share a root $(\alpha : \gamma)$. There will be m variations of A (U^xV^yA with $x + y = m$) and n variations of B (U^xV^yB with $x + y = n$). Since A and B both have root $(\alpha : \gamma)$, any multiple of A and B will also have this root. Also, since all rows of Sylvester's Determinant are variations of A and B, all linear combinations will also share the root. Let $(\theta : \phi) \neq (\alpha : \gamma)$. Consider K, the $m + n$ degree form whose only root is $(\theta : \phi)$. Since this form doesn't share a root with A and B, it is not possible to create a linear combination to create K. This means the matrix form of Sylvester's Determinant does not span $m + n$ degree forms, so it is not invertible and thus, the determinant is 0. We will now assume that Sylvester's Determinant is 0 and show that A and B must share a root. We know that some non-trivial linear combination of the rows of the determinant are 0.

$$a_1U^{m-1}A + a_2U^{m-2}VA + ... + a_mV^{m-1}A - b_1U^{n-1}B - ... - b_nV^{-1}nB = 0$$

We can now do some factoring,

$$A(a_1U^{m-1} + a_2U^{m-2}V + ... + a_mV^{m-1}) - B(b_1U^{n-1} + ... + b_nV^{n)-1} = 0$$

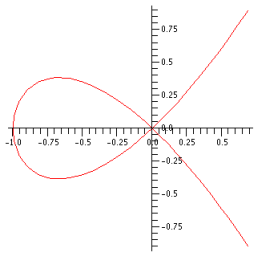
Notice that $(a_1U^{m-1} + a_2U^{m-2}V + ... + a_mV^{m-1})$ is just a form of degree $m-1$ and $(b_1U^{n-1} + ... + b_nV^{n-1})$ is a form of degree $n - 1$. We now have $A\pi = B\tau$ where π is a form of degree $m - 1$ and τ is a form of degree $n - 1$. Our forms are in $k[U, V]$, so we have unique factorization. Since $deg\pi < degB$ there is at least one root of B that is not a root of π or has a higher multiplicity in B than π. Since $A\pi = B\tau$, it must also be a root of A, thus A and B share a root.

Math 434: Class Notes February 21, 2019
Scribe: Lanie Kropp

Section 2.1[1]

Nodal Cubic

A cubic represented by $C : (y^2 = x^3 + x^2) \in \mathbb{R}^2$.



It can be parameterized in the following way:

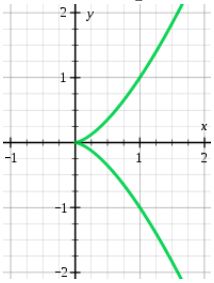
$$\rho : \mathbb{R}^1 \to \mathbb{R}^2$$

$$t \to (t^2 - 1, t^3 - t)$$

Looking at the graph, we can see that this parameterization makes sense. The x-values follow a quadratic sort of shape with an intersection at -1, hence $x = t^2 - 1$. Plugging this equation for x into the original equation, we get $y = t^3 - t$ as the parameterization of y.

Cuspidal Cubic

A cubic represented by $C : (y^2 = x^3) \in \mathbb{R}^2$.



Here, we write the parameterization:

$$t \to (t^2, t^3)$$

Again, looking at he graph we see that this parameterization makes sense.
A note from Fernando: We can derive these parameterizations starting with the fact that a line crosses a cubic three times. In the nodal cubic, it crosses at 0 twice, and we can vary t as the slope to get the other point. In the cuspidal cubic, you have to worry about how many times it intersects the cusp.

[1] Graphs of the cubics in this section found on math.purdue.edu. They are the same as what was put on the board in class, but are nicer to look at than my drawings.

Section 2.2

Claim : The curve $C : y^2 = x(x-1)(x-\lambda)$ has no rational paramterization.
Theorem : Let k be a field of characteristic not equal to 2 and $\lambda \in k$ with $\lambda \neq 0$ or 1. Let $f, g \in k(t)$ be rational functions such that

$$f^2 = g(g-1)(g-\lambda).$$

Then, $f, g \in k$ (Note: $k(t)$ is the field of fractions of the UFD $K[t]$).

Proof. We have $f, g \in k(t)$ so we can write them as fractions. Let $f = \frac{r}{s}$ and $g = \frac{p}{q}$ where $r, s, p, q \in K[t]$ (polynomials in t) with r, s are coprime and p, q are coprime. We can rewrite our equation and manipulate it:

$$(\frac{r}{s})^2 = \frac{p}{q}(\frac{p}{q} - 1)(\frac{p}{q} - \lambda)$$

$$r^2 = \frac{s^2 p}{q}(\frac{p}{1} - 1)(\frac{p}{q} - \lambda)$$

$$q^3 r^2 = s^2 p(p-q)(p-\lambda q)$$

Since r, s are coprime, we must have that s^2 divides q^2. Similarly, since p, q are coprime, q^3 must divide s^2. Thus we have $s^2 = aq$ where a is a unit in $K[t]$ (note: the units in $K[t]$ are the nonzero elements of k). We now write

$$\frac{s^2}{q^2} = aq$$

$$(\frac{s}{q})^2 = aq$$

So, aq is a square in $K[t]$. We can now rewrite our previous equation, plugging in $s^2 = aq^3$ to get:

$$q^3 r^2 = aq^3 p(p-q)(p-\lambda q)$$

The q^3's cancel, giving us

$$r^2 = ap(p-q)(p-\lambda q)$$

Because p, q are coprime, we have that $ap, p-q, p-\lambda q$ are all relatively prime. Since their product is a square, each term is itself a square. Because p, q must be constants, as will be shown in the next section, it follows that r, s must also be constants, and we are done. □

Lemma 2.3

Let k be an algebraically closed field, p, q coprime elements in $K[t]$ and assume there exists λ_i, μ_i such that $\lambda_i p + \mu_i q$ is a square in $K[t]$ for $i = 1, 2, 3, 4$. Then $p, q \in k$ (for $\lambda_i : \mu_i \in \mathbb{P}^1$).

Proof. First we will show that if we have four linear combinations that are all squares, they can be written in the form $p, p-q, p-nq, q$. Considering hitting any linear combination with an invertible $2x2$ matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} p' \\ q' \end{pmatrix}$$

where $a, b, c, d \in k$. So, four linear combinations that get hit with this matrix sill be linear combinations and maximal degree does not change. Assume we have the following:

$$ap + bq = p'$$

$$cp + dq = q'$$

and two more linear combinations. Then $p', q', \alpha p' + \beta q', \gamma p' + \delta q'$ are all squares. We can then multiply each of these by some of $\alpha, \beta, \gamma, \delta$ to get what we want:

$$\alpha\gamma p' = p$$

$$-\beta\gamma g' = q$$

$$\alpha\gamma p' + \beta\gamma q' = p - q$$

$$\alpha\gamma p' + \alpha\delta q' = p - \lambda q$$

Now that we have shown that four linear combinations can be expressed in this form, we can proceed to prove by our lemma by contradiction. Assume by contradiction that $deg(p) \neq 0$, $\deg(q) \neq 0$ and that p, q are minimal. We know that p, q are squares and we can write $p = u^2$ and $q = v^2$. We also have

$$p - q = (u + v)(u - v)$$

$$p - nq = u^2 - nv^2 = (u - \sqrt{n}v)(u + \sqrt{n}v)$$

(note: $deg(u) < deg(p)$ and $deg(v) < deg(q)$ because we assume nonzero degree by contradiction, and u, v are coprime because p, q are coprime). Now, we will show that $u - v, u + v$ are coprime and $u - \sqrt{n}v, u + \sqrt{n}v$ are coprime.

Assume that $d|(u+v)$ and $d|(u-v)$. Then $d|(u+v+u-v) = 2u$ and $d|(u+v)-(u-v) = 2v$. Since 2 is a unit, this means that d divides both u and v, but we have assumed that d, u are coprime, so $d = 1$. We can use the same argument to show that $u - \sqrt{n}v, u + \sqrt{n}v$ are coprime. Thus, we have that $u + v, u - v$ are relatively prime and their product is a square, and the same is the case for $u - \sqrt{n}v, u + \sqrt{n}v$. However, this is a contradiction because u and v have smaller degree than p and q, which we assumed to be minimal. So, $p, q \in k$.

(note: pay attention to how we used the crucial facts that we are working in an algebraically closed field and that k did not have characteristic equal to 2) □

Summary:

The main idea that we covered today is that the nodal cubic (2 distinct roots) and the cuspidal cubic (1 distinct root) can be parameterized, while $C : y^2 = x(x-1)(x-\lambda)$, which has 3 distinct routes, can not be parameterized.