Some Highlights along a Path to Elliptic Curves

Part 3: Projective Geometry and Bezout's Theorem

Steven J. Wilson, Fall 2016

Outline of the Series

1. The World of Algebraic Curves
2. Conic Sections and Rational Points
3. **Projective Geometry and Bezout's Theorem**
4. Solving a Cubic Equation
5. Exploring Cubic Curves
6. Rational Points on Elliptic Curves

Fundamental Theorem of Algebra

- Every polynomial $P(x)$ with complex coefficients and degree $n \geq 1$ has at least one complex zero.

Corollary:

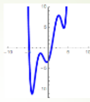
- Every polynomial $P(x)$ with complex coefficients and degree $n \geq 1$ can be factored into n linear factors.

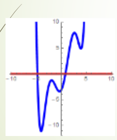
$$P(x) = a(x-c_1)(x-c_2)\cdots(x-c_n)$$

- Equivalently:
  - $P(x)=0$ has n solutions, counting multiplicities.
  - $y = P(x)$ has at most n x-intercepts.

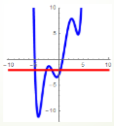
Recognizing the Degree

- What is the degree?

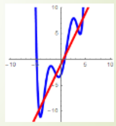




2 x-intercepts
At least 2

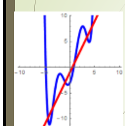


Any horizontal line
At least 4



Any non-vertical line
At least 6

Extending the Fundamental Theorem



- If $P(x)$ is a polynomial of degree $n \geq 2$, and $L(x)$ is a linear function, then the graphs of $y = P(x)$ and $y = L(x)$ intersect in at most n points.

Proof:

- Let $f(x) = P(x) - L(x)$.
- Then $f(x)$ is also a polynomial of degree n.
- By the corollary of the Fundamental Theorem of Algebra, $f(x)$ has at most n x-intercepts.
- Therefore $P(x) = L(x)$ has at most n solutions.

Extending to Algebraic Curves

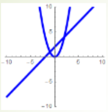
Fundamental Theorem Extended

- If $P(x)$ is a polynomial of degree $n \geq 2$,
- and $L(x)$ is a linear function,
- then the graphs of $y = P(x)$ and $y = L(x)$
- intersect in exactly n points,
- counting multiplicities,
- in the complex plane.

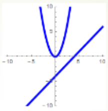
Bezout's Theorem

- If $P(x, y)$ is a polynomial of degree $n \geq 1$,
- and $Q(x, y)$ is a polynomial of degree $m \geq 1$
- with no common factors,
- then the graphs of $P(x, y) = 0$ and $Q(x, y) = 0$
- intersect in exactly mn points,
- counting multiplicities,
- in the complex plane,
- extended to include points at infinity.

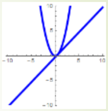
Example: Parabola and Line



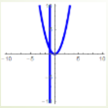
2 real solutions



2 nonreal solutions



solution with multiplicity 2

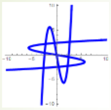


1 real, 1 infinite

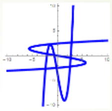
$$\begin{cases} y = x^2 \\ (1+\varepsilon)x + \varepsilon y = -1 \end{cases}$$

$$(1+\varepsilon)x + \varepsilon x^2 = -1$$
$$\varepsilon x^2 + (1+\varepsilon)x + 1 = 0$$
$$(x+1)(\varepsilon x + 1) = 0$$
$$x = -1 \text{ or } \frac{-1}{\varepsilon}$$

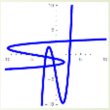
Example: Two Cubic Curves



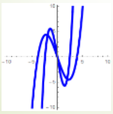
9 real solutions



7 real with mult. 1
1 real with mult. 2

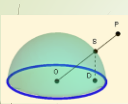


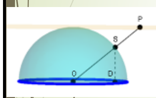
5 real
4 nonreal

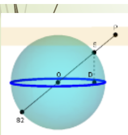


3 real
1 at infinity with mult. 6

Projecting Infinity onto a Disk







- Unit Sphere: $x^2 + y^2 + z^2 = 1$, and Plane: $z = 1$
- Points: $O(0,0,0)$ and $P(x,y,1)$
- Segments: $OP = \sqrt{x^2+y^2+1}$, and $OS = 1$
- Points: $S = \frac{OS}{OP}P = \left(\frac{x}{\sqrt{x^2+y^2+1}}, \frac{y}{\sqrt{x^2+y^2+1}}, \frac{1}{\sqrt{x^2+y^2+1}}\right)$

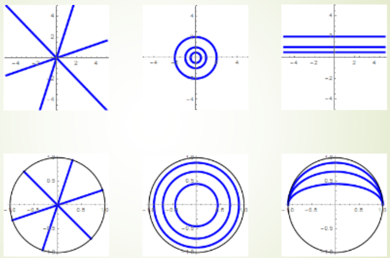
$$D = \left(\frac{x}{\sqrt{x^2+y^2+1}}, \frac{y}{\sqrt{x^2+y^2+1}}, 0\right) = (u,v,0)$$

- Inverting the formulas gives:

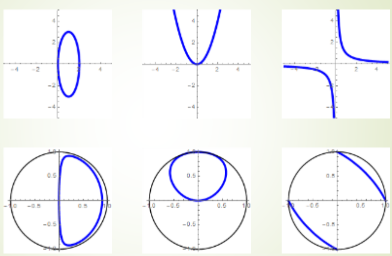
$$(x,y) = \left(\frac{u}{\sqrt{1-u^2-v^2}}, \frac{v}{\sqrt{1-u^2-v^2}}\right)$$

- This substitution projects $P(x,y) = 0$ onto the unit disk.
- Points at infinity are mapped to the disk edge.
- Antipodal points on disk edge must be considered identical.

Simple Curves on the Disk



Conics on the Unit Disk



Homogeneous Coordinates

- We can see infinity at the edge of the unit disk, but because that point is at the edge, we can't yet really understand a curve's behavior at infinity.
- The **homogeneous coordinate system** will assign three coordinates to a point in the extended real plane:
  - If $z \neq 0$, then (x, y, z) represents $\left(\frac{x}{z}, \frac{y}{z}\right)$ in the plane.
  - If $z = 0$ but $x \neq 0$, then $(x, y, 0)$ represents the point at infinity where the line through the origin with slope $\frac{y}{x}$ intersects the line at infinity.
  - If $z = x = 0$ but $y \neq 0$, then $(0, y, 0)$ represents the point at infinity where the y-axis intersects the line at infinity.
- The coordinates $(0,0,0)$ do not exist in this system.

Converting Points

From homogeneous to R^2

- $(5,-7,9)$ becomes: $\left(\frac{5}{9}, -\frac{7}{9}\right)$
- $(3,4,1)$ becomes: $(3,4)$
- $(-2,5,0)$ becomes:

  The point at infinity on the line $y=-\frac{5}{2}x$
- $(3,0,0)$ becomes:

  The point at infinity on the x-axis.

From R^2 to homogeneous

- $(5,8)$ becomes: $(5,8,1)$ or $(10,16,2)$ or ...
- Point at infinity on line $y=-2x$ is: $(1,-2,0)$ or $(2,-4,0)$ or ...
- Point at infinity on x-axis is: $(1,0,0)$ or $(2,0,0)$ or ...
- Point at infinity on y-axis is: $(0,1,0)$ or $(0,2,0)$ or ...

Homogeneous Polynomials

- A polynomial is **homogeneous** if all of its terms have the same degree.

$3x+5y$	✓	$17-2xy$	✗
$2x^2+3y+6$	✗	$8x^2+5xy+6y^3$	✗
$4x^4y^2-3xy^5$	✓	$x^{14}-3y^{14}$	✓

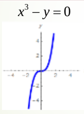
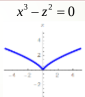
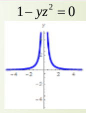
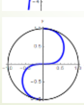
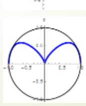
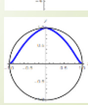
- We can **homogenize a polynomial** by introducing one more variable with an appropriate exponent.

✗	✓
$2x^2+3y+6$	$2x^2+3yz+6z^2$
$17-2xy$	$17z^2-2xy$
$8x^2+5xy+6y^3$	$8x^2z+5xyz+6y^3$

Three Ways to Dehomogenize

- Example: $x^3-y=0$, when homogenized, is $x^3-yz^2=0$.

Substitute:	z=1	y=1	x=1
Origin:	(0,0,1)	(0,1,0)	(1,0,0)
Visible Axes:	y = 0, x = 0	z = 0, x = 0	z = 0, y = 0
Axis at infinity:	z = 0	y = 0	x = 0

$x^3-y=0$	$x^3-z^2=0$	$1-yz^2=0$
		
		

- $x^3-y=0$ has a cusp at infinity. It is singular.

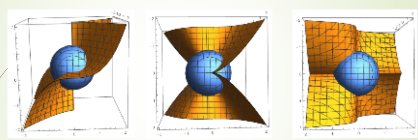
Properties

Suppose $f(x,y,z)$ is a homogeneous polynomial of degree $n \geq 1$. Then …

- The origin is a point on the graph of $f(x,y,z)=0$.
- For any $a \in R$, $f(ax,ay,az)=a^n f(x,y,z)$.
  - Proof: Factor a^n from each term of $f(ax,ay,az)$.
- If (x_0,y_0,z_0) is a point on the graph of $f(x,y,z)=0$, then so is every point on the line joining (x_0,y_0,z_0) with the origin.
- The graph of $f(x,y,z)=0$ is a double cone (but rarely circular) with its vertex at the origin.
- The shape of the cone can be easily seen where it intersects the unit sphere.

Viewing the Cone

- Example: $x^3-y=0$, when homogenized, is $x^3-yz^2=0$.

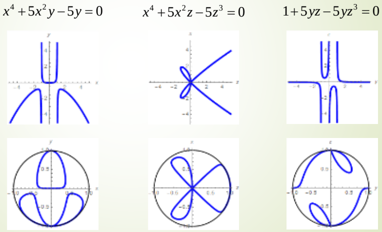


- The cone $\{(x,y,z): x^3-yz^2=0\}$ is an **algebraic variety**.
- The algebraic curve $\{(x,y,z): x^3-yz^2=0,\ z=1\}$ is a **subvariety** of the cone.
- The three dehomogenized polynomials are all subvarieties of the same algebraic variety.

A Second Example

- Consider: $x^4+5x^2y-5y=0$, same as: $y=\dfrac{-x^4}{5(x^2-1)}$
- Homogenizes as: $x^4+5x^2yz-5yz^3=0$

$x^4+5x^2y-5y=0$ $\qquad$ $x^4+5x^2z-5z^3=0$ $\qquad$ $1+5yz-5yz^3=0$

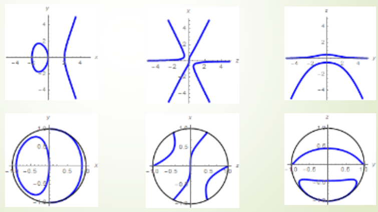


- A triple point (node) at infinity. It is singular.

An Elliptic Curve Example

- Consider: $x^3 - y^2 - 4x = 0$, same as: $y = \pm\sqrt{x^3 - 4x}$
- Homogenizes as: $x^3 - y^2 z - 4xz^2 = 0$

$x^3 - y^2 - 4x = 0$ $\quad$ $x^3 - z - 4xz^2 = 0$ $\quad$ $1 - y^2 z - 4z^2 = 0$



- The point at infinity is an ordinary point.

Intuiting Infinity: Asymptotes

Picture	Point at Infinity
	Ordinary Point
	Inflection Point (ordinary)
	Cusp (singular)
	Ramphoid Cusp (singular)

- In each case the asymptote is the line tangent to the point at infinity (assuming that the limit of the slope exists)

Intuiting Infinity: Non-Asymptotic

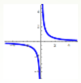
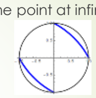
Picture	Point at Infinity
	Cusp (singular)
	Inflection Point (ordinary)
	Ordinary Point
	Ramphoid Cusp (singular)

- In each case, the line at infinity is tangent to the curve at the point at infinity (assuming that the limit of the slope exists).
- Or, the asymptote of a non-asymptotic curve might be the line at infinity.

Additional Observations

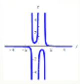
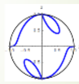
- Curves can have more than one point at infinity.

$$y = \frac{1}{x}$$
$$xy - 1 = 0$$

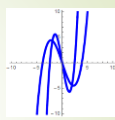
- Parallel asymptotes create a node at infinity.

$$1 + 5yz - 5yz^3 = 0$$

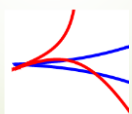



Two Cubic Functions

- When two cubic functions intersect in 9 points, 6 of them are at infinity. Why?



- Each cubic function has a cusp at infinity.
- Two cusps intersecting almost at their cuspidal point will intersect 6 times.



Challenges

1. For each type of conic, find a homogeneous polynomial, and dehomogenize it in all 3 ways. What do you find?
2. Graph the curve $y^3 = x^5 - 4x^4y + 4x^3y^2$. Can you identify the features at infinity? Then homogenize and dehomogenize it in all 3 ways. Are the features as you expected?