Math 418: HW 9 due Wednesday, April 27, 2022.

Webpage: http://dunfield.info/418

Office hours: Monday and Tuesday from 1:30–2:30pm; other times possible by appointment.

1. Consider the parabola $y = x^2$ in $\mathbb{R}^2$.

   (a) Find a polynomial $f \in \mathbb{R}[x, y, z]$ so that the variety V in $\mathbb{P}^2_{\mathbb{R}}$ defined by f has $V \cap \mathbb{R}^2$ the above parabola. Here $\mathbb{R}^2 = \{(x : y : 1)\}$.

   (b) How many points does V have in the line at infinity $\mathbb{P}^1_\infty = \{(x : y : 0)\}$?

   (c) Using a projective transformation, show that V is in fact tangent to $\mathbb{P}^1_\infty$.

   (d) Find a projective transformation so that $p_A(V) \cap \mathbb{R}^2$ is a hyperbola.

2. Let k be a field. A *line* in $\mathbb{P}^2_k$ is the variety corresponding the equation $ax + by + cz = 0$, where $a, b, c \in k$ are not all zero.

   (a) Show that, up to change of coordinates, all lines are the same. That is, given two lines L, L' there exists a matrix $A \in \mathrm{GL}_3(k)$ so that the corresponding projective transformation $p_A \colon \mathbb{P}^2_k \to \mathbb{P}^2_k$ takes L to L'.

   (b) Prove that any two distinct points $p_1, p_2 \in \mathbb{P}^2_k$ determine a unique line.

   (c) Prove that any two distinct lines intersect in exactly one point.

   Hint: What object in k^3 corresponds to a line in $\mathbb{P}^2_k$?

3. Let k be a field, and consider $\mathbb{P} = \mathbb{P}^2_k$.

   (a) Let p_1, p_2, p_3, p_4 be points in $\mathbb{P}$ so that no three are colinear, i.e. no three lie on a common line. Show there is a projective change of coordinates so that the p_i become $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$, $(1 : 1 : 1)$.

   (b) Find all conics passing through the five points

   $$(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (a : b : c)$$

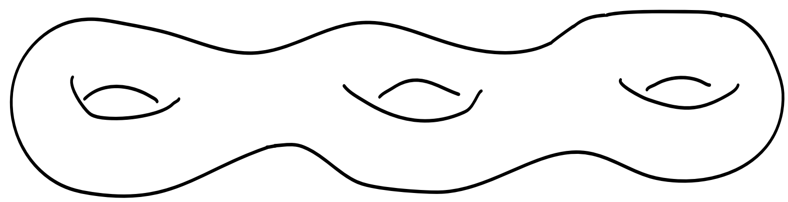
   (c) Suppose $p_1, \ldots, p_5$ are points in $\mathbb{P}$ with no *four* colinear. Use (a-b) to show there is at most one conic containing all 5 points.

   Note: This is one of many illustrations of the power of changing coordinates.

4. Consider the plane curve $X = \mathbf{V}(x^3y + y^3z + z^3x)$ in $\mathbb{P}^2_{\mathbb{C}}$.

   (a) Find $X \cap L_\infty$, where L_∞ is the line at infinity, i.e. $\mathbf{V}(z)$.

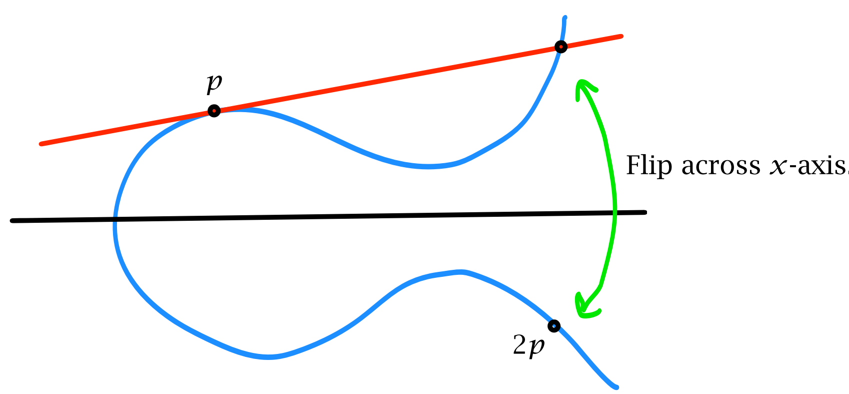
   (b) Prove that X is smooth, being sure to include those points found in (a).
   Note: Any smooth curve in $\mathbb{P}^2_{\mathbb{C}}$ is automatically irreducible, and has genus $\binom{d-1}{2}$, where d is the degree of the defining polynomial. Hence, as topological space, X is as shown below.



(c) X is very symmetric. Find a group of projective transformations of order 21 that leaves X invariant. In fact, the full group of such projective automorphisms has order 168 and is the simple group $\mathrm{PSL}_2\mathbb{F}_7$. In fact, this is the most symmetries that a genus 3 curve can have...

5. In this problem, you'll explore elliptic curves in $\mathbb{P}^2_{\mathbb{R}}$. In addition to the points in $\mathbb{R}^2$ given by a standard equation $y^2 = x(x^2 + ax + b)$, there is an additional point at infinity which is the identity element in the group law. Note: Elliptic curves are always taken to be smooth, as otherwise the group law gets confusing.

   One thing that wasn't mentioned in class is how to add a point p to itself. In this case, one takes the tangent line at p as shown:



   (a) Consider the curve E given by $y^2 = x^3 + 4x$. Show that $(2, 4)$ has order 4.

   (b) Now consider an arbitrary elliptic curve E. Explain why any point in E of the form $(x, 0)$ has order 2 in E.

   (c) Find the subgroup of E consisting of all points of order 2 (plus the identity element), and identify it as a group. Note: there are two cases here, depending on the specific curve E.