Math 418: Problem Set 9.

Due date: In class on Wednesday, April 28.
Webpage: http://dunfield.info/418
Office hours: Monday 10-11, Tuesday 3-5.

1. 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 $\mathbb{P}^2_k$?

2. 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 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.

3. Let k be an algebraically closed field. Let $V \subset k^n$ be an affine algebraic variety, and consider the ring $k[V]$ of polynomial functions on V. Here, you'll see how to extract the geometry of V from $k[V]$.

   (a) For $p \in V$, let $I_p = \{f \in k[V] \mid f(p) = 0\}$. Prove that I_p is an ideal of $k[V]$ and, moreover, is maximal.

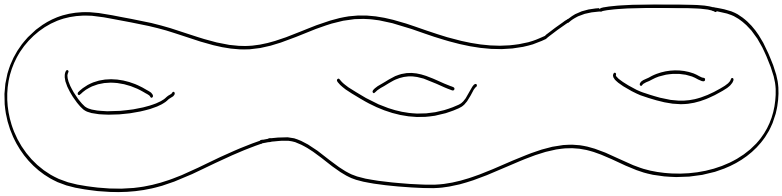
   (b) Suppose $V = k^n$, and so $k[V] = k[x_1, \ldots, x_n]$. Use Hilbert's Nullstellensatz to show that any maximal ideal I of $k[V]$ is of the form I_p for some $p \in k^n$. Hint: Argue that $\mathbf{V}(I)$ is not empty.

   (c) Now let $V \subset k^n$ again be an arbitrary affine variety. Use (b) to show that any maximal ideal of $k[V]$ is of the form I_p.

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

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

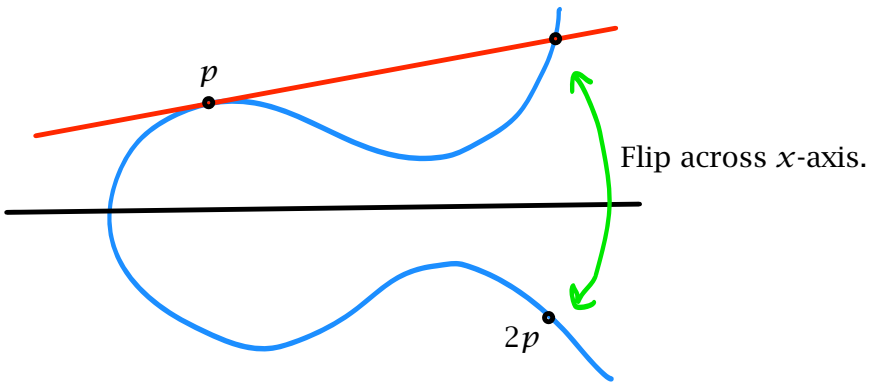
   (b) Prove that X is smooth, being sure to include those points found in (a).
   Note: Any smooth curve in $\mathbb{P}^2_{\mathbb{C}}$ is automatically irreducible, and has genus $\binom{d-1}{2}$, where d is the degree of the defining polynomial. Hence, as topological space, X is as shown below.



   (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.