The purpose of these notes is to introduce projective geometry, and to establish some basic facts about projective curves. Everything said here is contained in the long appendix of the book by Silverman and Tate, but this is a more elementary presentation. The notes also have homework problems, which are due the Tuesday after spring break.

1 The Projective Plane

1.1 Basic Definition

For any field $\boldsymbol{F}$, the projective plane $P^2(\boldsymbol{F})$ is the set of equivalence classes of nonzero points in $\boldsymbol{F}^3$, where the equivalence relation is given by

$$(x, y, z) \sim (rx, ry, rz)$$

for any nonzero $r \in \boldsymbol{F}$. Let $\boldsymbol{F}^2$ be the ordinary plane (defined relative to the field $\boldsymbol{F}$.) There is an injective map from $\boldsymbol{F}^2$ into $P^2(\boldsymbol{F})$ given by

$$(x, y) \to [(x, y, 1)],$$

the equivalence class of the point $(x, y, 1)$. In this way, we think of $\boldsymbol{F}^2$ as a subset of $P^2(\boldsymbol{F})$.

A set $S \subset \boldsymbol{F}^3$ is called a *cone* if it has the following property: For all $v \in S$ and all nonzero $r \in \boldsymbol{F}$, we have $rv \in S$. Given a cone S, we define the *projectivization* $[S] \subset P^2(\boldsymbol{F})$ to be the set of points $[v]$ such that $v \in S$.

1.2 Lines

A *line* in the projective plane is the set of equivalence classes of points in a 2-dimensional $\boldsymbol{F}$-subspace of $\boldsymbol{F}^3$. In other words, a line is the set of equivalence classes which solve the equation $ax + by + cz = 0$ for some $a, b, c \in \boldsymbol{F}$. That is, a line is the projectivization of a plane through the origin. The set of lines in $P^2(\boldsymbol{F})$ is often known as the *dual projective plane*. Think about it: Each line is specified by a triple (a, b, c), where at least one entry is nonzero, and the two triples (a, b, c) and (ra, rb, rc) give rise to the same lines.

Note that $P^2(\boldsymbol{F}) - \boldsymbol{F}^2$ is the line consisting of solutions to $z = 0$. This particular line is known as the *line at infinity* and we sometimes write it as L_∞.

Exercise 1: Prove that every two distinct lines in $P^2(\boldsymbol{F})$ intersect in a unique point. Likewise, prove that every two distinct points in $P^2(\boldsymbol{F})$ are contained in a unique line.

Exercise 2: Let $\boldsymbol{F}$ be a finite field of order $N = p^n$. How many points and lines does $P^2(\boldsymbol{F})$ have.

1.3 Projective Transformations

A linear isomorphism from $\boldsymbol{F}^3$ to itself respects equivalence classes, and therefore induces a map from $P^2(\boldsymbol{F})$ to itself. This map is called a *projective transformation*. A projective transformation is always a bijection which maps lines to lines. In case $\boldsymbol{F} = \boldsymbol{R}$ or $\boldsymbol{F} = \boldsymbol{C}$, the projective transformations are continuous. The set of projective transformations forms a group, often known as *the projective group*.

2 Homogeneous Polynomials

2.1 Basic Definition

Given a triple $I = (a_1, a_2, a_3)$, we define

$$X^I = x_1^{a_1} x_1^{a_2} x_3^{a_3}. \tag{1}$$

Here a_1, a_2, a_3 are non-negative integers. We define $|I| = a_1 + a_2 + a_3$. We say that a *homogeneous polynomial* of degree d (in 3 variables) over the field $\boldsymbol{F}$ is a polynomial of the form

$$\sum_{|I|=d} c_I X^I, \qquad c_I \in \boldsymbol{F}. \tag{2}$$

The variables here are x_1, x_2, x_3. Sometimes it is convenient to use the variables x, y, z in place of x_1, x_2, x_3.

Exercise 3: Let P be a degree d homogeneous polynomial and let T be a projective transformation. Prove that $P \circ T$ is another homogeneous polynomial of degree d.

2.2 Homogenization and Dehomogenization

A degree d polynomial in 3 variables has a *homogenization*, where we just pad the polynomial with suitable powers of the third variable to get something that is homogeneous. An example should suffice to explain this.

$$x^5 + 3x^2y^2 + x^2y - 5 \qquad \Longrightarrow \qquad x^5 + 3x^2y^2z + x^2yz^2 - 5z^5.$$

Conversely, every homogeneous polynomial of degree d in 3 variables has a *dehomogenization*, obtained by setting the third variable to 1. The operations of homogenization and dehomogenization are obviously inverses of each other.

2.3 Projective and Affine Curves

Let P be a homogeneous polynomial of degree d. If $v \in \boldsymbol{F}^3$ and $r \in \boldsymbol{F}$, we have

$$P(rv) = r^d P(v). \tag{3}$$

Therefore, when $r \neq 0$, we have $P(rv) = 0$ if and only if $P(v) = 0$. In other words, the solution $P = 0$ is a cone in $\boldsymbol{F}^3$. Because of this fact, the following definition makes sense.

$$V_P = \{[v] | \; P(v) = 0\} \subset P^2(\boldsymbol{F})\}. \tag{4}$$

This V_P is just the projectivization of the solution set $P = 0$. The set V_P is known as a *projective curve*.

A projective curve is a kind of completion of the solution set to a polynomial. Suppose that $p(x, y)$ is a degree d polynomial in 2 variables and $P(x, y, z)$ is the homogenization. Let $V_p = \{(x, y) | \; p(x, y) = 0\}$. The set V_p is known as an *affine curve*. Since $\boldsymbol{F}^2$ is naturally a subset of $P^2(\boldsymbol{F})$, in the way described above, we have the inclusion

$$V_p \subset \boldsymbol{F}^2 \subset P^2(\boldsymbol{F}). \tag{5}$$

Exercise 4: Interpreting V_p as a subset of V_P, prove that $V_p = V_P \cap \boldsymbol{F}^2$. So, the projective curve V_P is obtained from V_p by adjoining the points of $P^2(\boldsymbol{F}) - \boldsymbol{F}^2$ where P vanishes.

2.4 Nonsingular Curves

It makes sense to take the formal partial derivatives of a polynomial over any field. In particular, the *gradient*

$$\nabla P = \left(\frac{dP}{dx}, \frac{dP}{dy}, \frac{dP}{dz}\right) \tag{6}$$

makes sense. We say that a *singular point* of P is a point $v \neq 0$ such that $P(v) = 0$ and $\nabla P(v) = 0$. If $r \in \boldsymbol{F}$ is nonzero, then v is a singular point if and only if rv is a singular point. The polynomial P is called *nonsingular* if it has no singular points. The projective curve V_P is called nonsingular if P is nonsingular.

When it comes time to discuss elliptic curves, we will always work with nonsingular ones.

Exercise 5: Suppose that V is a nonsingular projective curve and T is a projective transformation. Prove that $T(V)$ is also a nonsingular projective curve.

2.5 The Tangent Line

Let P be a nonsingular projective curve and let $[v] \in P^2(\boldsymbol{F})$ be a point. The *tangent line* to P at $[v]$ is defined to be the line determined by the equation

$$\nabla P(v) \cdot (x, y, z) = 0. \tag{7}$$

In case $\boldsymbol{F} = \boldsymbol{R}$ you can think about this geometrically. In $\boldsymbol{R}^3$, the tangent plane to the level set $P(x, y, z) = 0$ at the point (x_0, y_0, z_0) is given by the equation

$$((x, y, z) - (z_0, y_0, z_0)) \cdot \nabla P = 0.$$

Here we are assuming that $P(x_0, y_0, z_0) = 0$. In case P is a homogeneous polynomial, we have

$$(z_0, y_0, z_0) \cdot \nabla P = 0.$$

Therefore, in this case, the equation of the tangent plane simplifies to

$$(x, y, z) \cdot \nabla P = 0.$$

So, in $\boldsymbol{R}^3$ the plane Π_0 given by Equation 7 is a good approximation along the line through (x_0, y_0, z_0) to the level set $P(x, y, z) = 0$. Both sets are cones, and so the projectivization of the tangent plane (the tangent line) is a good approximation of the projectivization of the polynomial level set (the projective curve).

Exercise 6: Let $f(x, y)$ be a polynomial in 2 variables, and let $P(x, y, z)$ be its homogenization. Let (x_0, y_0) be some point where $f(x_0, y_0) = 0$ and $\nabla f(x_0, y_0) \neq 0$. We think of (x_0, y_0) as a point of $P^2(\boldsymbol{R})$ by identifying it with $[x_0, y_0, 1]$, as above. Prove that the tangent line to the level set of f at (x_0, y_0) is exactly the projectivization of the plane given by Equation 7. In other words, reconcile the definition of tangent line given above with the usual definition given in a calculus class.

3 A Case of Bezout's Theorem

3.1 Homogeneous Polynomials in Two Variables

A field is $\boldsymbol{F}$ *algebraically closed* if every polynomial over $\boldsymbol{F}$ has all its roots in $\boldsymbol{F}$. The results here work for any algebraically closed field, but for convenience we'll take $\boldsymbol{F} = \boldsymbol{C}$, the field of complex numbers. The Fundamental Theorem of Algebra says that $\boldsymbol{C}$ is algebraically closed.

Exercise 7: Let $A(x, y)$ be a homogeneous polynomial of degree n in 2 variables over $\boldsymbol{C}$. Prove that $A(x, y)$ factors into linear factors

$$A(x, y) = (c_1x + d_1y)...(c_nx + d_ny).$$

Here $c_i, d_i \in \boldsymbol{C}$.

3.2 Multiplicity

Exercise 7 has implications for homogeneous polynomials in 3 variables. If $P(x, y, z)$ is such a polynomial, we can write

$$P(x, y, z) = A(x, y) + zB(x, y, z),$$

Where B has lower degree. Assuming that A is nontrivial, we can factor A as in Exercise 7. This gives

$$P(x, y, z) = (c_1x + d_1y)...(c_nx + d_ny) + zQ(x, y, z). \tag{8}$$

Let $L_\infty = P^2(\boldsymbol{C}) - \boldsymbol{C}^2$ denote the line at infinity.

Exercise 8: Prove that $V_P \cap L_\infty$ consists of the points

$$p_k = [c_k : -d_k : 0] = [-c_k : d_k : 0]. \tag{9}$$

These account for the extra points of V_P contained in in $P^2(\boldsymbol{C}) - \boldsymbol{C}^2$. See Exercise 4.

The *multiplicity* of p_k is defined to be the number of factors of $(c_k x + d_k y)$ appearing in Equation 8. With this definition, $V_P \cap L_\infty$ consists of exactly n points, counting multiplicity. Here n is the degree of P.

Exercise 9: Let T be a projective transformation such that $T(L_\infty) = L_\infty$. Let $P^* = P \circ T$. Then $T(V_{P^*}) = V_P$. Suppose that $p \in L_\infty \cap V_{P^*}$ has multiplicity m with respect to V_{P^*}. Prove that $T(p) \in V_\infty \cap V_P$ has multiplicity m with respect to V_P. (*Hint:* The map T is a projective transformation that maps L_∞ to itself. T is represented by some invertible linear transformation $\widehat{T}$. We have

$$\widehat{T}(Z) = aX + bY + cZ.$$

When $Z = 0$, we have $T(Z) = 0$ as well. This is only possible if $a = b = 0$. Hence $\widehat{T}(Z) = aZ$. We might as well divide through by a, so that $\widehat{T}(Z) = Z$. Now that you know what T looks like, do some algebra.)

Exercise 10: In the discussion in the last section, we considered the case when our homogeneous polynomial had at least one term with no z's in it. That is $A(x,y)$ is nontrivial. Suppose that P is a homogeneous polynomial such that every term of P involves the variable z. Prove that $L_\infty \subset V_P$.

3.3 Bezout's Theorem

Suppose now that L is an arbitrary line in $P^2(\boldsymbol{C})$ and that $p \in L \cap V_P$. One possibility is that $L \subset V_P$. Suppose that this doesn't happen. Then we choose a projective transformation T such that $T(L) = L_\infty$, and we define the multiplicity of p to be the multiplicity of $T_p = L_\infty \cap T(V_C)$.

Lemma 3.1 *The multiplicity of p is well-defined.*

Proof: Suppose that T_1 and T_2 are two projective transformations carrying L to L_∞. We want to see that $T_1(p)$ has the same multliplicity relative to $T_1(V_P)$ that $T_2(p)$ has relative to $T_2(V_P)$. This was the point of Exercise 9. ♠

Now that we know the multiplicity is well defined, we have a case of Bezout's Theorem.

Theorem 3.2 (Bezout) *Suppose that P is a homogeneous polynomial of degree n and V_P is the corresponding projective curve. Let L be any line that is not contained in V_P. Then $L \cap V_P$ consists of n points, counting multiplicity. In particular, if V_P contains no lines, then every line intersects V_P in n points, counting multiplicity.*

Proof: Let L be any line. To count the points of $L \cap V_P$ we move L to ∞ by a projective transformation T. Since L is not contained in V_P, the polynomial $P \circ T^{-1}$ has some nontrivial part that just involves the variables x and y. But then the analysis above shows that $T(V_P)$ intersects L_∞ in exactly n points, counting multiplicity. This means that V_P intersects L in exactly n points, counting multiplicity. ♠

The general case of Bezout's Theorem says that a projective curve of degree d_1 and a projective curve of degree d_2, having no common components, intersect in exactly $d_1 d_2$ points, when these points are counted with multiplicity. The proof of this result, as well as a good definition of multiplicity that works in any algebraically closed field, is harder.