Math 145, Final Exam.

You may assume that the ground field is $k = \mathbb{C}$.

1. (*Rational points on cubic curves.*) Consider the point $P(0,0)$ on cubic curve C with equation

$$y^2 + y = x^3 - x.$$

(i) Let $Q(a,b)$ be a point on the cubic. Show that the inverse $-Q$ has coordinates $(a, -1-b)$ for the group law with zero element the point at infinity $[0:1:0]$. Find the coordinates of the point $P+Q$.

(ii) Find the coordinates of the point nP, for $n \leq 6$, and note that nP is a rational point on C. In fact, the group of rational points $C(\mathbb{Q})$ is generated by $P(0,0)$.

2. (*Pencils of conics.*) Let Q_1 and Q_2 be two distinct *nonsingular* conics in $\mathbb{P}^2$. The family of conics

$$Q_{\lambda,\mu} = \lambda Q_1 + \mu Q_2$$

where $[\lambda : \mu] \in \mathbb{P}^1$ is called a *pencil* of conics.

(i) Recall that any conic $Q \subset \mathbb{P}^2$ determines and is determined by the symmetric matrix A of coefficients with

$$Q([x:y:z]) = [x \;\; y \;\; z] \; A \; [x \;\; y \;\; z]^T.$$

Possibly by diagonalizing A (and therefore Q), show that

$$Q \text{ is singular if and only if } \det A = 0.$$

(ii) Letting $A_{\lambda,\mu}$ be the matrix associated to the conic $Q_{\lambda,\mu}$, show that $\det Q_{\lambda,\mu}$ is a cubic polynomial in λ, μ. Prove that any pencil of conics contains (at most) 3 singular conics.

(iii) Let p_1, p_2, p_3, p_4 be points in $\mathbb{P}^2$ such that no three of them lie on a line. Show that the set of conics through p_1, p_2, p_3, p_4 is a pencil. (Feel free to change coordinates to prove this fact). What are the singular conics in this pencil?

3. (*Torsion points on cubics.*) Let C be a nonsingular cubic curve and $p_0 \in C$ an inflection point. Consider the group law on C with p_0 the zero element.

(i) Explain briefly that p is an inflection point on C if and only if p is a point of order 3 in the group law of (C, p_0). Derive that the line though any 2 inflection points intersects C in a third inflection point.

(ii) We proved in class that after a change of coordinates we may assume C can be written as

$$y^2 z = x(x-z)(x-\lambda z) \text{ and } p_0 = [0:1:0].$$

Show that a further change of coordinates $\tilde{x} = x - z \cdot \frac{\lambda+1}{3}$ brings C into the form

$$y^2 z = \tilde{x}^3 + a\tilde{x}z^2 + bz^3 \text{ and } p_0 = [0:1:0].$$

(iii) Possibly using (ii), show that C has *exactly* 9 distinct points of order 3, hence 9 inflection points.

Hint: Show that if $z = 0$, the only inflection point is $p_0 = [0:1:0]$. Next, assume $p = [\tilde{x} : y : 1]$ is a point of order 3 on the affine curve $y^2 = \tilde{x}^3 + a\tilde{x} + b$. Therefore, $2p = -p$. Find the coordinates of $2p$ and $-p$. Derive that $\tilde{x}$ satisfies a degree 4 equation, for instance

$$12\tilde{x}(\tilde{x}^3 + a\tilde{x} + b) = (3\tilde{x}^2 + a)^2.$$

Prove that there are *exactly* 4 values of $\tilde{x}$, and each value gives *exactly* 2 values of y. (You will need to show that there are no repeated roots of the quartic equation, for instance by computing the first derivative.) Count the inflection points $1 + 4 \times 2 = 9$.

(iv) From (i) and (iii), conclude that the inflection points form a subgroup of C isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

(v) Possibly using (ii), show that there are exactly 4 tangent lines to C which pass though the inflection point p_0 (the same is therefore true for any inflection point). Conclude that C has exactly 4 points of order 2, and the subgroup of points of order 2 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Remark: It can be shown that the n-torsion points form a group isomorphic to $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

4. (*Singularities of cubics*.)

(i) Show that any singular irreducible cubic in $\mathbb{P}^2$ is isomorphic to either the nodal or the cuspidal cubics:

$$y^2z = x^2(x+z) \text{ or } y^2z = x^3.$$

Hint: Assume the singularity is at $[0:0:1]$. Show that the cubic can be written as

$$(\text{quadratic polynomial in } x, y) \cdot z = Q(x, y),$$

where Q is a cubic polynomial in x, y. Change coordinates suitably and write the cubic as

$$y^2z = \widetilde{Q}(x, y) \text{ or } xyz = \widetilde{Q}(x, y).$$

Use the coordinate change $z \mapsto \lambda x + \mu y + \nu z$ to put the cubic into one of the forms

$$y^2z = (x + by)^3 \text{ or } xyz = (x + y)^3.$$

Conclude by performing one more change of coordinates.

(ii) Using (i), show that *irreducible cubics* in $\mathbb{P}^2$ can have at most 1 singular point. Exhibit a cubic in $\mathbb{P}^2$ with 3 singular points.

Remark: It can be shown that an *irreducible* degree d curve in $\mathbb{P}^2$ has at most $\binom{d-1}{2}$ singular points.

5. (*Bezout's theorem and intersection multiplicities*.) Let C and D be curves in $\mathbb{P}^2$ of degrees d and e without common irreducible components. We will define the *intersection multiplicity* $\mu_p(C, D)$ of an intersection point $p \in C \cap D$.

(i) Show that we can change coordinates such that
  (a) the point $[1:0:0]$ does not lie on C or D
  (b) $[1:0:0]$ does not lie on any line though two points of $C \cap D$.

Pick coordinates such that $(a) - (b)$ are satisfied. Note that there is a slight asymmetry in the variables, x being different than y and z. Consider $P(x:y:z), Q(x:y:z)$ the equations of C and D, and let $p = [a:b:c]$ be an arbitrary point. Let $R_{P,Q}(y, z)$ be the resultant of P and Q when P, Q are viewed as polynomials in the variable x with coefficients in $k[y, z]$. Define the multiplicity $\mu_p(C, D)$ to be the largest integer k such that

$$(bz - cy)^k \text{ divides the resultant } R_{P,Q}(y, z).$$

It turns out that this integer is independent of the choice of coordinate systems satisfying (a)-(b), but you dont have to prove it.

(ii) Explain briefly that $p \in C \cap D$ if and only if $\mu_p(C, D) \geq 1$.

(iii) Prove the strong Bezout's theorem which states that C and D intersect in exactly de points counted with multiplicity. That is,

$$\sum_{p \in C \cap D} \mu_p(C, D) = de.$$

(iv) Directly from the definition, find the intersection multiplicities for the curves

$$(x + y)^d = 0 \text{ and } x(x + z)^{e-1} = 0$$

in $\mathbb{P}^2$, and confirm Bezout's theorem. It may help to remember from the beginning of the course how the resultant of P, Q can be computed in terms of the roots of P and Q.