Problem Set Seven: Due Thursday, March 21

See the course website for policy on collaboration. All references to the textbook refer to the February 21, 2024 edition of *Foundations of Algebraic Geometry*, by Ravi Vakil.

Problem 1. This problem builds up some useful lemmas about finiteness for future use. In particular, we will eventually use it to show "projective source plus finite fibers implies finite" (so don't use that in solving this problem).

Let A be a commutative ring. Let $x_1, x_2, \ldots, x_n$ be coordinates on $\mathbb{P}^{n-1}_A$. Let U be the open set $U := \bigcup_{j=1}^{n-1} D_+(x_j)$ in $\mathbb{P}^{n-1}_A$ and let Z be the complementary closed subscheme $Z := V_+(x_1, x_1, \ldots, x_{n-1})$. Let X be a closed subscheme of $\mathbb{P}^{n-1}_A$ such that $X \cap Z = \emptyset$.

(1) Let $I \subset A[x_1, x_2, \ldots, x_n]$ be the graded ideal corresponding to X (see Exercise 15.7.J). Show that, for some integer M, the ideal I contains a homogeneous polynomial of the form
$$x_n^M + \sum_{m_1+\cdots+m_n=M,\ m_n<M} a_{m_1 m_2 \cdots m_n} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}.$$
Hint: Consider Exercise 4.5.L and the fact that $X \cap Z = \emptyset$.

(2) Let $\lambda : U \to \mathbb{P}^{n-1}_A$ be the map given in homogenous coordinates by the map $(x_1 : x_2 : \cdots : x_{n-1} : x_n) \mapsto (x_1 : x_2 : \cdots : x_{n-1})$. Show that $\lambda : X \to \mathbb{P}^{n-1}_A$ is a finite map.

(3) More generally, let U_d be the open set $U_d := \bigcup_{j=1}^{d} D_+(x_j)$ and let Z_d be the complementary closed subscheme $Z_d := V_+(x_1, x_2, \ldots, x_d)$. Let X be a closed subscheme of $\mathbb{P}^{n-1}_A$ such that $X \cap Z_d = \emptyset$ and let $\lambda_d : \mathbb{P}^{n-1}_A \to \mathbb{P}^{d-1}_A$ be the map $(x_1 : x_2 : \cdots : x_{n-1} : x_n) \mapsto (x_1 : x_2 : \cdots : x_d)$. Show that $\lambda_d : X \to \mathbb{P}^{d-1}_A$ is finite.

We'll stop the problem here because it is long enough for now; expect a sequel.

Problem 2. In this problem, we'll compute the Picard group of an elliptic curve over a field. Let k be a field where $2 \neq 0$. Let $f(x) = x^3 + ax^2 + bx + c$ be a cubic with $\mathrm{GCD}(f(x), f'(x)) = 1$. Let E be the curve in $\mathbb{P}^2_k$ with equation $Y^2 Z = X^3 + aX^2 Z + bXZ^2 + cZ^3$, and let E_0 be the affine curve $y^2 = x^3 + ax^2 + bx + c$ in $\mathbb{A}^2_k$. Let ∞ denote the point $[0 : 1 : 0]$ of E, so $E_0 = E \setminus \{\infty\}$. Finally, write R for the ring $\mathcal{O}(E_0) = k[x, y]/\langle y^2 = x^3 + ax^2 + bx + c\rangle$.

You may assume without checking that E is smooth over k, and that $v_\infty(x) = -2$ and $v_\infty(y) = -3$.

(1) Show that $\{x^j : 0 \leq j\} \sqcup \{yx^j : 0 \leq j\}$ is a k basis for R and that $\{x^j : 0 \leq j \leq d/2\} \sqcup \{yx^j : 0 \leq j \leq (d-3)/2\}$ is a k basis of $\Gamma(E, \mathcal{O}(d\infty))$. Show that $\dim \Gamma(E, \mathcal{O}(d\infty)) = d$ for $d \geq 1$.

(2) Let D be an effective divisor on E with $\deg(D) = d$. Show that $\Gamma(E, \mathcal{O}((d+1)[\infty] - D)) \neq 0$. Conclude that D is rationally equivalent to $(d+1)[\infty] - [\mathfrak{p}]$ where $\mathfrak{p}$ is a k-valued point of E.

(3) Show that every divisor on D is rationally equivalent to a divisor of the form $m[\infty] - [\mathfrak{p}_1] + [\mathfrak{p}_2]$ for some k-valued points $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of E.

Let $\mathfrak{p}$ be a k-valued point of E where $x = u$ and $y = v$. Let $\overline{\mathfrak{p}}$ be the k-valued point where $x = u$, $y = -v$.

(4) Verify that $[\mathfrak{p}] + [\overline{\mathfrak{p}}]$ is rationally equivalent to $2[\infty]$ on E, and thus $-[\mathfrak{p}] \sim [\mathfrak{p}] - 2[\infty]$.

(5) Deduce that every divisor on D is rationally equivalent to a divisor of the form $m[\infty] + [\mathfrak{p}_1] + [\mathfrak{p}_2]$ for some k-valued points $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of E. Then use one final trick to show that every divisor on D is rationally equivalent to a divisor of the form $m[\infty] + [\mathfrak{q}]$ for $\mathfrak{q}$ a single k-valued point of E.

In fact, the different k-valued points of E are not rationally equivalent to each other, so each divisor is equivalent to one of the form $m[\infty] + [\mathfrak{q}]$ for a unique $(m, \mathfrak{q})$, but we don't have the right tools to prove that yet.