E. Dummit's Math 7359 ∼ Elliptic Curves and Modular Forms, Fall 2023 ∼ Homework 2, due Fri Oct 20th.

Problems are worth points as indicated. Solve whichever problems you haven't seen before that interest you the most (suggestion: between 15 and 25 points' worth). Starred problems are especially recommended. Submit your assignments via Gradescope.

---

## 0.1 In-Lecture Exercises

- In these problems, let $V$ be a variety (assumed to be affine unless otherwise specified) defined over an algebraically closed field $k$.

### 0.1.1 Exercises from (Sep 21)

1. [2pts] Let $\mathcal{F}(V,k)$ be the ring of $k$-valued functions on $V$. We say $f \in \mathcal{F}(V,k)$ is a polynomial function if there exists $g \in k[x_1,\dots,x_n]$ such that $f(P) = g(P)$ for all $P \in V$. Show that $\Gamma(V)$ is the set of equivalence classes of polynomial functions under the relation $g_1 \sim g_2$ if $g_1(P) = g_2(P)$ for all $P \in V$.
2. [2pts*] Show that $\Gamma(V) = \cap_{P\in V}\mathcal{O}_P(V)$: in other words, that a function with no poles is a polynomial.
3. [2pts] If $P \in V$, show that the evaluation-at-$P$ map $\varphi_P : \mathcal{O}_P(V) \to k$ is a surjective ring homomorphism with kernel $m_P(V)$. Deduce that $m_P(V)$ is maximal, and show also that if $P = (a_1,\dots,a_n)$ then $m_P(V)$ is generated by the polynomials $x_i - a_i$ for $1 \le i \le n$.
4. [2pts*] Let $R$ be a commutative ring with 1 having a maximal ideal $M$. Show that $M^n/M^{n+1}$ is a vector space over the field $k = R/M$ for each positive integer $n$.
5. [1pt] Let $R$ be a local ring (a commutative ring with 1 having a unique maximal ideal $M$). Show that every element of $R$ is either a unit or an element of $M$.
6. [2pts*] Show that for any elliptic curve in reduced Weierstrass form $y^2 = x^3 + Ax + B$ and any point $P = (a,b)$ on $C$, then the corresponding maximal ideal $m_P = (x-a, y-b)$ of the local ring is principal and generated by either $y-b$ (when $y'(P) \ne 0$) or $x-a$ (when $y'(P) = 0$).
7. [1pt] Suppose $C$ is a plane curve and $f(x,y)$ is a polynomial that is not identically zero on $C$. Show that there are only finitely many $P \in C$ for which $f(P) = 0$.

### 0.1.2 Exercises from (Sep 25)

1. [3pts] Suppose $k$ is an infinite field, $P \in \mathbb{A}^{n+1}\backslash\{0\}$, and $f \in k[x_0,\dots,x_n]$. If we write $f = f_0 + f_1 + \cdots + f_d$ for homogeneous polynomials $f_i$ of degree $i$, show that $f(\lambda P) = 0$ for all $\lambda \in k^\times$ if and only if $f_i(P) = 0$ for all $i$. [Hint: Use linear algebra and the fact that Vandermonde determinants are nonvanishing.]
2. [2pts*] Identify $V(x_0)$, $V(x_0^2)$, $V(x_1 - x_0)$, $V(x_1 - x_0^2)$, $V(x_1^2 - x_0^2)$, $V(x_0,x_1)$, $V(x_0,x_1,x_2)$, and $V(x_0x_1 - x_2^2)$ in $\mathbb{P}^2(k)$.
3. [2pts] Show that an ideal $I$ of $k[x_0,\dots,x_n]$ is homogeneous (i.e., that for all $f \in I$ with homogeneous decomposition $f = f_0 + f_1 + \cdots + f_d$, it is true that each component $f_i \in I$) if and only if $I$ is generated by finitely many homogeneous polynomials.
4. [2pts] When $V$ is a nonempty projective algebraic variety with cone $C(V) = \{(x_0,x_1,\dots,x_n) : [x_0 : x_1 : \cdots : x_n] \in S\} \cup \{(0,0,\dots,0)\}$, show that $I_{\text{affine}}(C(V)) = I_{\text{projective}}(V)$, and when $I$ is a homogeneous ideal with $V_{\text{projective}}(I) \ne \emptyset$, show that $C(V_{\text{projective}}(I)) = V_{\text{affine}}(I)$.
5. [2pts] For $f,g \in k[x_1,\dots,x_n]$ and homogeneous $F,G \in k[x_0,\dots,x_n]$, show that $(FG)_* = F_*G_*$, $(fg)^* = f^*g^*$, $(f^*)_* = f$, $(F_*)^* = F/x_0^{v_{x_0}(f)}$, $(F+G)_* = F_*+G_*$, and $x_0^{\deg(f)+\deg(g)-\deg(f+g)}(f+g)^* = x_0^{\deg(g)}f^* + x_0^{\deg(f)}g^*$.

### 0.1.3 Exercises from (Sep 28)

1. [3pts*] Show that the isomorphisms $\varphi : \mathbb{A}^n \to \mathbb{A}^n$ are the invertible affine linear transformations, of the form $\varphi(x) = Ax + b$ where $A$ is an invertible $n \times n$ matrix and $b$ is any vector of constants. [Hint: First show that the degree of each coordinate in $\varphi$ and $\psi = \varphi^{-1}$ must be 1.]

### 0.1.4 Exercises from (Oct 5)

1. [3pts*] On $C = \mathbb{A}^1(\mathbb{C})$, suppose $\alpha = u\dfrac{(x-p_1)^{a_1}\cdots(x-p_l)^{a_l}}{(x-q_1)^{b_1}\cdots(x-q_m)^{b_m}}$ for $u \in k^\times$ and take distinct elements $p_1, \dots, p_l, q_1, \dots, q_m \in k$ having associated points $P_1, \dots, P_k, Q_1, \dots, Q_l$ respectively. Show that $\operatorname{div}(a) = a_1P_1 + \cdots + a_lP_l - b_1Q_1 - \cdots - b_mQ_m + [\sum_j b_j - \sum_i a_i]P_\infty$.

2. [2pts] Show that for any $C = \mathbb{A}^1(\mathbb{C})$ and any nonzero rational function $\alpha \in \mathbb{C}(C)$ we have $\deg(\operatorname{div}(\alpha)) = 0$.

3. [2pts] For any field $k$, if $f(t), g(t) \in k[t]$ are relatively prime (note $t$ is transcendental over $k$), show that $[k(t) : k(\frac{f(t)}{g(t)})] = \max(\deg f, \deg g)$. [Hint: Use Gauss's lemma to show that $q(y) = f(y) - \frac{f(t)}{g(t)}g(y) \in k(\frac{f(t)}{g(t)})[y]$ is the minimal polynomial of $t$ over $k(\frac{f(t)}{g(t)})$.]

4. [1pt] Verify that the relation on divisors given by $D_1 \sim D_2$ if $D_1 - D_2$ is principal is an equivalence relation and that the equivalence classes are the elements in the quotient group of divisors modulo principal divisors.

5. [1pt] Check that the relation $D_1 \le D_2$ when $D_2 - D_1$ is effective (i.e., when $v_P(D_2 - D_1) \ge 0$ at all $P$) is a partial ordering on divisors.

6. [3pts*] Determine $L(D)$ when $C = \mathbb{A}^1(\mathbb{C})$ for $D = P_0 - P_\infty$, $P_0 + P_\infty$, and $P_0 + P_1$.

7. [2pts] Suppose $E$ is a subfield of $k$ and $D$ is a divisor of $k$ that is defined over $E$. Show that $\dim_k[L_k(D)] = \dim_E[L_E(D)]$. [Hint: Show that a basis for $L_E$ remains a basis over $L_k$.]

## 0.2 Additional Exercises

1. [4pts*] In $\mathbb{P}^2(k)$, a <u>line</u> is the vanishing locus of a homogeneous linear polynomial $l \in k[X, Y, Z]$ such as $X + Y = 0$ or $2X - Y - Z = 0$. Show that any two distinct lines in $\mathbb{P}^2(k)$ intersect in exactly one point. (Compare to the affine statement that any two lines are either parallel or intersect in exactly one point.)

2. [5pts*] Our construction of the group law on an elliptic curve $E$ relies on describing the points $(P, Q, R)$ with $P + Q + R$ equal to the identity. The goal of this problem is to examine how much of the structure of a group is determined by this information. Let $G$ be a multiplicative group with identity $e$ and define $S = \{(g, h, k) \in G \times G \times G : ghk = e\}$ to be the set of ordered triples whose product is the identity.

   (a) Show that the set $S$ along with the knowledge of which element of $G$ is the identity fully determines the group structure of $G$ (i.e., uniquely identifies the "multiplication-table function" $\cdot : G \times G \to G$ with $(g, h) \mapsto gh$).

   (b) Show that if $G$ contains no elements of order 3, then the set $S$ by itself determines the group structure of $G$.

   (c) Find an example of a set $S$ that does not uniquely determine the group structure of $G$.