

Solve whichever problems you haven't seen before that interest you the most (suggestion: between 20 and 35 points' worth). Starred problems are especially recommended. Prepare 2-3 problems to present on the assignment due date. **Use of generative AI to solve any of the problems is expressly forbidden**; however, if after solving a problem you discover that generative AI gives an entertainingly wrong solution, you are welcome to mention that!

0.1 In-Lecture Exercises

0.1.1 Exercises from (Sep 10)

- [2pts] Show that graph of $y^2 = x^3 + Ax + B$ over $\mathbb{R}$ will have two components when the polynomial $x^3 + Ax + B$ has three distinct real roots, and will have one component otherwise.
- [1pt] Suppose E has Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on E . Show that $-P_1 = (x_0, -y_0 - a_1x_0 - a_3)$, and $P_1 + P_2$ is given by ∞ when $x_1 = x_2$ and $y_1 = -y_2 - a_1x_2 - a_3$ and by (x_3, y_3) where $x_3 = m^2 + a_1m - a_2 - x_1 - x_2$ and $y_3 = -(m + a_1)x_3 - b - a_3$ where $y = mx + b$ is the line joining P_1 and P_2 (or the tangent line when $P_1 = P_2$), which explicitly has $m = \frac{y_2 - y_1}{x_2 - x_1}$, $b = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}$ when $P_1 \neq P_2$ and has $m = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$ and $b = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$ when $P_1 = P_2$.
- [2pts*] Pick an elliptic curve in Weierstrass form (e.g., $y^2 = x^3 + 4x + 1$) and after checking whether it is nonsingular, find all of its points over $\mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}$, and $\mathbb{F}_{13}$, and identify the group structure explicitly in each case.
- [2pts*] Show that for an elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{C}$, the 2-torsion subgroup $E[2]$ is always isomorphic to the Klein 4-group $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.
- [3pts] Show that for an elliptic curve $y^2 = x^3 + Ax + B$ over $\mathbb{C}$, the 3-torsion subgroup $E[3]$ is always isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. [Hint: If $P = (x, y)$, write out the x -coordinate of $2P$.]

0.1.2 Exercises from (Sep 14)

- [2pts] Show that by rescaling variables, any rational Weierstrass form can be converted into one with A, B integers. Illustrate by finding a Weierstrass form with integer coefficients for $y^2 = x^3 + \frac{3}{2}x + \frac{2}{5}$.
- [3pts] (Tedious) Let E be an elliptic curve and $P = (x, y)$ be a point on E . Define the polynomials $\varphi_0 = 0$, $\varphi_1 = 1$, $\varphi_2 = 2y$, $\varphi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$, $\varphi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$, and in general $\varphi_{2n+1} = \varphi_{n+2} \cdot \varphi_n^3 - \varphi_{n-1}\varphi_{n+1}$ and $\varphi_{2n} = \frac{\varphi_n}{2y} \cdot (\varphi_{n+2}\varphi_{n-1}^3 - \varphi_{n-2}\varphi_{n+1}^2)$ for $n \geq 2$.
 - With $y^2 = x^3 + Ax + B$, show that φ_n can be written as a polynomial in $\mathbb{Z}[x, A, B]$ when n is odd and can be written as y times a polynomial in $\mathbb{Z}[x, A, B]$ when n is even.
 - Show that φ_n^2 is a polynomial of degree $n^2 - 1$ in x with leading coefficient n^2 while $x\varphi_n^2 - \varphi_{n-1}\varphi_{n+1}$ is a polynomial of degree n^2 in x with leading coefficient 1.
 - Show that the coordinates of $[n]P$ are (x_n, y_n) where $x_n = \frac{x\varphi_n^2 - \varphi_{n-1}\varphi_{n+1}}{\varphi_n^2}$ and $y_n = \frac{\varphi_{n+2}\varphi_{n-1}^2 - \varphi_{n-2}\varphi_{n+1}^2}{4y\varphi_n^3}$.

0.1.3 Exercises from (Sep 21)

- [2pts*] Draw $V(x)$, $V(x^2)$, $V(y - x)$, $V(y - x^2)$, $V(xy)$, $V(x, y)$, and $V(y^2 - x^3 - x)$ in $\mathbb{A}^2(\mathbb{R})$.
- [3pts] Identify $I(S)$ in $\mathbb{R}[x, y]$ for $S = \{(t, 0) : t \in \mathbb{R}\}$, $\{(t^2, t) : t \in \mathbb{R}\}$, $\{(1, 1)\}$, $\{(0, 0), (1, 1)\}$, $\{(\cos t, \sin t) : t \in \mathbb{R}\}$, and $\{(t, \sin t) : t \in \mathbb{R}\}$.
- [2pts] Prove that for any subset S of $k[x_1, \dots, x_n]$, $S \subseteq I(V(S))$ and $V(S) = V(I(V(S)))$.
- [2pts] Prove that for any subset X of $\mathbb{A}^n(k)$, $X \subseteq V(I(X))$ and $I(X) = I(V(I(X)))$.

5. [3pts*] If k is algebraically closed, show that the irreducible affine algebraic sets in $\mathbb{A}^2(k)$ are $\emptyset$, $\mathbb{A}^2(k)$, single points, and curves of the form $V(f)$ for irreducible $f \in k[x, y]$. [Hint: Show that if $f, g \in k[x, y]$ are relatively prime, then (f, g) contains a nonzero polynomial in $k[x]$ and a nonzero polynomial in $k[y]$.]
6. [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 $P \in V$.
7. [1pt] Show that $\Gamma(V) = \cap_{P \in V} \mathcal{O}_P(V)$: in other words, that a function with no poles is a polynomial. (Note that k is assumed to be algebraically closed.)
8. [2pts] Show that the evaluation-at- P map $\varphi_P : \mathcal{O}_P(V) \rightarrow k$ 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 $1 \leq i \leq n$.
9. [1pt] 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 .
10. [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 .
11. [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 $y'(P) \neq 0$) or $x - a$ (when $y'(P) = 0$).
12. [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 $f(P) = 0$.
13. [4pts] (Z.G. Memorial Exercise) Let F be a field with a discrete valuation v and valuation ring R . Also let $t \in R$ be a uniformizer (i.e., an element with $v(t) = 1$). Show that
 - (a) For any $r \in F^\times$, either r or $1/r$ is in R .
 - (b) An element $u \in R$ is a unit of R if and only if $v(u) = 0$. In particular, if $\zeta \in F$ is any root of unity, then $v(\zeta) = 0$.
 - (c) If $r \in R$ is nonzero and $v(r) = n$, then r can be written uniquely in the form $r = ut^n$ for a unit $u \in R$.
 - (d) Every nonzero ideal of R is of the form (t^n) for some $n \geq 0$.
 - (e) The ring R is a Euclidean domain (hence also a PID and a UFD) and also a local ring.
 - (f) The ring S is a DVR if and only if it is a PID and a local ring but not a field.

0.1.4 Exercises from (Sep 24)

1. [2pts] Suppose k is an infinite field, $P \in \mathbb{A}^{n+1} \setminus \{0\}$, and $f \in k[x_0, \dots, x_n]$. If we write $f = f_0 + f_1 + \dots + f_d$ 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. [3pts] Show that an ideal I of $k[x_0, \dots, x_n]$ is homogeneous if and only if I is generated by finitely many homogeneous polynomials.

0.1.5 Exercises from (Sep 28)

1. [3pts] When V is a nonempty projective variety with cone $C(V)$, show that $I_{\text{affine}}(C(V)) = I_{\text{projective}}(V)$, and when I is a homogeneous ideal with $V_{\text{projective}}(I) \neq \emptyset$, show that $C(V_{\text{projective}}(I)) = V_{\text{affine}}(I)$.
2. [1pt] Show that $(FG)_* = F_*G_*$, $(fg)^* = f^*g^*$, $(f^*)_* = f_*$, $(F^*)_* = F/x_0^{v_{x_0}(f)}$, $(F + G)_* = F_* + G_*$, and $x_0^{\deg(f) + \deg(g) - \deg(f+g)}(f + g)^* = x_0^{\deg(g)}f^* + x_0^{\deg(f)}g^*$.

- [1pt*] Show that there exists a unique projective point $[X : Y : Z]$ with $Z = 0$ on any elliptic curve with a Weierstrass equation $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$.
- [2pts] Show that the affine linear maps $\varphi : \mathbb{A}^n \rightarrow \mathbb{A}^n$ of the form $\varphi(x) = Ax + b$ where A is an invertible $n \times n$ matrix and b is any vector of constants, are isomorphisms. Find another isomorphism $\varphi : \mathbb{A}^n \rightarrow \mathbb{A}^n$ not of this form.

0.1.6 Exercises from (Oct 1)

- [2pts] Show that the map $\varphi : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ given by $\varphi[X : Y : Z] = [YZ : ZX : XY]$ is a rational map that is its own inverse, yet φ is not a morphism because it is not defined at the points $[1 : 0 : 0]$, $[0 : 1 : 0]$, and $[0 : 0 : 1]$.
- [1pt] On $C = \mathbb{A}^1(\mathbb{C})$, suppose $\alpha = u \frac{(x - p_1)^{a_1} \cdots (x - p_l)^{a_l}}{(x - q_1)^{b_1} \cdots (x - q_m)^{b_m}}$ for $u \in k^\times$ where $p_1, \dots, p_l, q_1, \dots, q_m \in k$ have associated points $P_1, \dots, P_l, Q_1, \dots, Q_m$ respectively. Show that $\text{div}(\alpha) = a_1P_1 + \cdots + a_lP_l - b_1Q_1 - \cdots - b_mQ_m + [\sum_j b_j - \sum_i a_i]\infty$.
- [2pts*] Show that for any $C = \mathbb{A}^1(\mathbb{C})$ and any nonzero rational function $\alpha \in \mathbb{C}(C)$ we have $\deg(\text{div}(\alpha)) = 0$.
- [3pts] For any field k , if $f(t), g(t) \in k[t]$ are relatively prime, 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 $k(\frac{f(t)}{g(t)})$.]
- [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.
- [1pt] Check that the relation $D_1 \leq D_2$ when $D_2 - D_1$ is effective (i.e., when $v_P(D_2 - D_1) \geq 0$ at all P) is a partial ordering on divisors.
- [2pts*] Determine $L(D)$ when $C = \mathbb{A}^1(\mathbb{C})$ for $D = P_0 - P_\infty$, $P_0 + P_\infty$, and $P_0 + P_1$.
- [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

- [4pts*] Find an elliptic curve in Weierstrass form over $\mathbb{Q}$ that has a rational point of order 4. (You may construct this curve in any manner you like, other than looking one up.)
- [5pts*] Find generators and the group structure for the group of rational torsion points on each curve. (You can check your answers with Sage, but you should use Nagell-Lutz to identify the candidate torsion points themselves first.)

(a) $y^2 = x^3 + 1$. (b) $y^2 = x^3 - 48$. (c) $y^2 = x^3 - 7x + 6$. (d) $y^2 = x^3 - 4x^2 + 16$. (e) $y^2 = x^3 - 14x^2 + 81x$.
- [5pts*] The L -Functions and Modular Forms Database (LMFDB, to its friends) contains data on many other algebraic objects of interest, including elliptic curves. Using the database, find an example of a Weierstrass form of an elliptic curve E with the given properties:

(a) $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}$. (b) $E(\mathbb{Q})$ contains a point of order 10. (c) $E(\mathbb{Q})$ is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$. (d) $E(\mathbb{Q}(i))$ is isomorphic to $\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. (e) $E(\mathbb{Q}(\sqrt{2}))$ is isomorphic to $\mathbb{Z}/11\mathbb{Z}$.
- [3pts] The algebra package Sage can, for reasonably nice elliptic curves E and number fields K , compute generators for the group $E(K)$. For each of the curves you found from the LMFDB in problem (3) above, use Sage to compute generators for the group of torsion points and the group of torsion-free points over the field requested (i.e., $\mathbb{Q}$ for (a)-(c), $\mathbb{Q}(i)$ for (d), $\mathbb{Q}(\sqrt{2})$ for (e)).
- [3pts] In $\mathbb{P}^2(k)$, a line 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.)