Problem set zero

Below you will find problems for problem set zero. This contains problems that will help us learn all the basics required before we move on to PAWS in a few weeks. We divide the problem sets into three parts - beginner, intermediate and advanced.

Feel free to go back and forth between the theory and the problems you like. There is absolutely no pressure to learn all this material at one go. Take your time and keep coming back to it as you move forward in your learning. Please be kind to yourself and your peers while learning and discussing the material. Most importantly, have fun :)

Preliminaries

Group theory

An important theorem that will give us some context for later. We will encounter these while studying the "group law" on elliptic curves.

Theorem 1. (Structure theorem) Every finitely generated abelian group is isomorphic to the group $\mathbb{Z}^n \oplus \mathbb{Z}/p_1 \oplus \cdots \oplus \mathbb{Z}/p_k$ for some positive integer n. The integer n is called the *rank* of the abelian group.

Algebraic curves

Here are some preliminary definitions. A nice reference for everything below is "Arithmetic of elliptic curves". We encourage everyone to look at examples from the book as you learn the definitions. Throughout this problem set, let K denote a field and $\bar{K}$ a fixed algebraic closure of K.

Definition 1. (Affine-n-space over K) Affine n-space (over K), denoted $\mathbb{A}^n_K$ is the set of n-tuples $(x_1, \ldots, x_n)$, $x_i \in \bar{K}$. The set of K-rational points of $\mathbb{A}^n_K$ consists of those n-tuples with coordinates in K.

Definition 2. (Affine algebraic set) To each ideal $I \subset \bar{K}[X_1, \ldots, X_n]$ we associate the set

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}$$

An (affine) algebraic set is a set of the form V_I for some I. If V is an algebraic set, the ideal of V is given by $I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in V\}$.

Definition 3. (Affine variety) An affine algebraic set V is an affine variety if $I(V)$ is prime in $\bar{K}[X]$.

Definition 4. (Affine coordinate ring) Let V be a variety defined over K. Then the affine coordinate ring of V/K is defined by $K[V] = \frac{K[X]}{I(V/K)}$ where $I(V/K) = I(V) \cap K[X]$. It is an integral domain, and its quotient field, denoted $K(V)$, is called the function field of V.

Definition 5. (Local ring of a variety) The local ring of a variety V at a point P, denoted $\bar{K}[V]_P$, is the localization of $\bar{K}[V]$ at the prime ideal $\{f \in \bar{K}[V] : f(P) = 0\}$.

Definition 6. (Dimension of a variety) The dimension of an affine variety V, denoted by $\dim(V)$ is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Definition 7. (Non-singular variety) Let V be a variety, $P \in V$, and $f_1, \ldots, f_m \in \bar{K}[X]$ a set of generators for $I(V)$. Then V is non-singular (or smooth) at P if the $m \times n$ matrix $(\partial f_i/\partial X_j(P))_{1 \leq i \leq m, 1 \leq j \leq n}$ has rank $n - \dim V$. If V is non-singular at every point, then we say that V is non-singular (or smooth). If the rank is less than $n - \dim V$, then we say the point is singular.

Definition 8. (Projective-n-space) The projective n-space (over K), denoted $\mathbb{P}^n_K$, is the set of $(n+1)$-tuples $(x_0, \ldots, x_n)$ such that at least one $x_i \in \bar{K}$ is non-zero, modulo the following equivalence relation: $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ if there exists a $\lambda \in \bar{K}^*$ with $x_i = \lambda y_i$ for all i. Note that $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$. For example, for each $0 \leq i \leq n$, there is an inclusion $\mathbb{A}^n \to \mathbb{P}^n, (y_1, \ldots, y_n) \mapsto [y_1, \ldots, y_{i-1}, 1, y_i, \ldots, y_n]$.

Definition 9. (Projective algebraic set) Let $\overline{K}[x_0, \ldots, x_n]$ denote the polynomial ring over $\bar{K}$ in $n+1$ variables. Let $I \subset \bar{K}[x_0, \ldots, x_n]$, be a homogenous ideal. We associate a subset $V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}$ to I. A projective algebraic set is any set of the form V_I.

Definition 10. (Projective variety) Let V be a projective algebraic set. The homogeneous ideal of V, denoted $I(V)$, is the ideal in $\bar{K}[x_0, \ldots, x_n]$ generated by

$$\{f \in \bar{K}[x_0, \ldots, x_n] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}$$

A projective algebraic set V is called a projective variety if its homogeneous ideal $I(V)$ is a prime ideal in $\bar{K}[x_0, \ldots, x_n]$.

Definition 11. (Dimension and function field of a projective variety) Let V be a projective variety defined over K, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ so that $V \cap \mathbb{A}^n \neq \emptyset$. The dimension of V is the dimension of $V \cap \mathbb{A}^n$. The function field of V, denoted $K(V)$, is the function field of $V \cap \mathbb{A}^n$.

Definition 12. (Non-singular projective variety) Let V be a projective variety, $P \in V$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then V is non-singular (or smooth) at P if $V \cap \mathbb{A}^n$ is non-singular at P.

Definition 13. (Rational map between varieties) Let V_1 and $V_2 \subset \mathbb{P}^n$ be projective varieties. A rational map $\varphi : V_1 \to V_2$ is a map of the form $\varphi = [f_0, \ldots, f_n]$, where $f_0, \ldots, f_n \in \bar{K}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \ldots, f_n$ are defined, $\varphi(P) = [f_0(P), \ldots, f_n(P)] \in V_2$.

Definition 14. (Regular map betwen varieties) A rational map $\varphi = [f_0, \ldots, f_n] : V_1 \to V_2$ is regular (or defined) at $P \in V_1$ if there is a function $g \in \bar{K}(V_1)$ such that

(i) each gf_i is regular at P;

(ii) for some i, $gf_i(P) \neq 0$.

Definition 15. (Curve) A curve is a projective variety of dimension one. We will generally work with smooth curves and from here on assume that all curves are smooth.

Definition 16. (Order of a meromorphic function on C) Let C be a curve and $P \in C$ a smooth point. Then $\bar{K}[C]_P$ is a discrete valuation ring. The normalized valuation on $\bar{K}[C]_P$ gives $\mathrm{ord}_P : \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}$. A uniformizer for C at P is a function $t \in \bar{K}(C)$ with $\mathrm{ord}_P(t) = 1$.

Definition 17. (Degree of a map) Let $\varphi : C_1 \to C_2$ be a non-constant map of curves defined over K. If φ is constant, we define the degree of φ to be 0; otherwise we say that φ is finite, and define its degree by $\deg \varphi = [K(C_1) : \varphi^* K(C_2)]$, where $\varphi^* : K(C_2) \to K(C_1)$ is an injection of function fields defined by $\varphi^* f = f \circ \varphi$.

Definition 18. (Ramification index of a map φ) Let $\varphi : C_1 \to C_2$ be a non-constant map of curves, and let $P \in C_1$. The ramification index of φ at P is given by $e_\varphi(P) = \mathrm{ord}_P(\varphi^* t_{\varphi(P)})$ where $t_{\varphi(P)} \in K(C_2)$ is a uniformizer at $\varphi(P)$.

Definition 19. (Divisor group of a curve)

1. The divisor group of a curve C, denoted $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum
$$D = \sum_{P \in C} n_P(P)$$
with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$.
2. The degree of D is defined by $\deg D = \sum_{P \in C} n_P$.
3. A divisor $D = \sum_{P \in C} n_P(P)$ is effective, denoted by $D \geq 0$ if $n_P \geq 0$ for every $P \in C$. Similarly, if $D_1, D_2 \in \mathrm{Div}(C)$, then we write $D_1 \geq D_2$ if $D_1 - D_2$ is effective.

Definition 20. (Divisor class group) Let $f \in \bar{K}(C)$. Associate to f the divisor
$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$$
. A divisor $D \in \mathrm{Div}(C)$ is principal if it has the form $D = \mathrm{div}(f)$ for some $f \in \bar{K}(C)^*$. The divisor class group of C is the quotient of $\mathrm{Div}(C)$ by the subgroup of principal divisors.

Definition 21. (The Riemann Roch space) Let $D \in \mathrm{Div}(C)$. We associate to D the set of functions
$$\mathscr{L}(D) = \{f \in \bar{K}(C)^* : \mathrm{div}(f) \geq -D\} \cup \{0\}$$
. It is a finite-dimensional $\bar{K}$-vector space, and we denote its dimension by $l(D)$.

Definition 22. Let C be a curve. The space of differential forms on C, denoted Ω_C, is the $\bar{K}(C)$-vector space generated by symbols of the form dx for $x \in \bar{K}(C)$, subject to the usual relations:

(i) $d(x + y) = dx + dy$ for all $x, y \in \bar{K}(C)$;

(ii) $d(xy) = xdy + ydx$ for all $x, y \in \bar{K}(C)$;

(iii) $da = 0$ for all $a \in \bar{K}$.

Definition 23. Let $\omega \in \Omega_C$. The divisor associated to ω is
$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C)$$
. Any divisor of the form $\mathrm{div}(\omega)$ is called a canonical divisor.

Theorem 2. (Riemann-Roch) Let C be a curve and K_C a canonical divisor on C. There is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in \mathrm{Div}(C)$,

$$l(D) - l(K_C - D) = \deg D - g + 1$$

.

Definition 24. (Genus) Keeping the notation above, we define the positive integer g in Theorem 2 to be the genus of the curve C.

Theorem 3. (Hurwitz) Let $\varphi : C_1 \to C_2$ be a non-constant separable map of curves. Then

$$2g(C_1) - 2 = (\deg \varphi)(2g(C_2) - 2) + \sum_{P \in C_1} (e_\varphi(P) - 1)$$

. Further, equality holds if and only if char $K = 0$, or char $K = p > 0$ and p does not divide $e_\varphi(P)$.

Magma

Magma is a software package designed for computations in algebra, number theory, algebraic geometry, and algebraic combinatorics. Here is the link for online magma calculator. For example:

Problem 1. Try the following code:

```
P<x,y,z> := ProjectiveSpace(Rationals(),2);
C := Curve(P, z*y^2 - x^3 + x*z^2);
Dimension(C);
IsNonsingular(C);
Genus(C);
p := C ! [1,0,1];
L := TangentLine(C,p);
L;
```

Here is the link for magma handbook.

Beginner Problems

Problem 2 (Counting subgroups)**.** Let p be a prime and let n, m be positive integers. Figure out the number of subgroups in

1. $\frac{\mathbb{Z}}{p} \oplus \frac{\mathbb{Z}}{p}$
2. $\frac{\mathbb{Z}}{p^n} \oplus \frac{\mathbb{Z}}{p^n}$
3. $\frac{\mathbb{Z}}{m} \oplus \frac{\mathbb{Z}}{m}$
4. $(\frac{\mathbb{Z}}{p})^{\oplus n}$
5. $(\frac{\mathbb{Z}}{p})^{\oplus n} \oplus (\frac{\mathbb{Z}}{p})^{\oplus n}$, with the additional condition that the projection of the subgroup to each $(\frac{\mathbb{Z}}{p})^{\oplus n}$ is surjective.

Problem 3 (Automorphism groups)**.** Let p be a prime and let n, m be positive integers. Figure out the automorphism groups of the following groups:

1. $(\frac{\mathbb{Z}}{p})^{\oplus n}$
2. $(\frac{\mathbb{Z}}{p^m})^{\oplus n}$
3. $(\frac{\mathbb{Z}}{m})^{\oplus n}$.

Problem 4. (Hyperelliptic curves)

1. Let $y^2 = f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ define an *affine* curve C for degree d. Let $P = (p_0, q_0)$ be a point on the curve. Write down the criteria for P to be a singular point.
2. Now suppose that the curve given in 1. is non-singular. Write down a map from C to $\mathbb{P}^1$. What is the degree of this branched cover of $\mathbb{P}^1$?
3. At what points of C is the cover $C \to \mathbb{P}^1$ ramified?
4. Using all data computed so far, find the genus of C in terms of the degree d.

Problem 5. (Silverman Example 2.9) Consider the map $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ given by:

$$\varphi([X, Y] = [X^3(X - Y)^2, Y^5]$$

Show that the map φ is unramified everywhere except the point $[0, 1]$ and $[1, 1]$. Find the ramification indices in each case as well.

Problem 6. Consider the algebraic plane curve $y^2 - x^3 - x = 0$. Show that $(0, 0)$ is a singular point of the curve.

Problem 7. Let C be a curve and denote its function field by $K(C)$. Explain the correspondence between $K(C) \cup \{\infty\}$ and morphisms $C \to \mathbb{P}^1$ defined over K.

Intermediate problems.

Problem 8. Let $\varphi : C_1 \to C_2$ be a map of curves. Prove that the map φ is either constant or surjective.

Problem 9. Let C be the smooth projective curve associated to the affine plane curve $y^3 + x^3 = 1$, and let $\varphi : C \to \mathbb{P}^1$ be the map given by the rational function x.

1. Find the ramification points of φ.
2. Compute the genus of C. Check your answer with Magma.
3. Find a map $\eta : C \to \mathbb{P}^1$ of degree 2 such that $\eta((1, 0)) = \eta((0, 1))$, and determine the ramification points of η.

Problem 10. (Arithmetic of Silverman, 2.7) Let $f(x, y, z)$ be a homogenous polynomial of degree d. Moreover, let $f = 0$ define a non-singular curve C in $\mathbb{P}^2$. Show that the genus of the curve is

$$\frac{(d-1)(d-2)}{2}.$$

(Hint: there are at least two ways of doing this. 1. Think about a map $C \to \mathbb{P}^1$. 2. Compute the canonical bundle of C in terms of the canonical bundle of $\mathbb{P}^2$ (For people familiar with the canonical bundle)).

Problem 11. For this problem refer to Theorem 2. Let C be a curve and K_C be a canonical divisor.

1. Show that $\deg(K_C) = 2g - 2$ and $l(K_C) = g$.
2. Let D be any arbitrary divisor on C. Show that if $\deg D > 2g-2$, then $l(D) = \deg D + 1 - g$.

Problem 12. Let C be a curve of genus 1 and $P, Q \in C$. Show that $(P) \sim (Q)$ if and only if $P = Q$.

Advanced problems

NOTE: For some advanced problems, you will need some knowledge of scheme theory.

Problem 13. Let E be smooth curve. Assume that the genus of E is 1 and that it has a distinguished point $\mathcal{O}$. Show that E is given by a cubic equation in the plane by following the steps given below.

1. Compute $l(nO)$ for all $n \geq 1$.
2. Use part (1) to pick bases $\{1, x\}$ and $\{1, x, y\}$ for the vector spaces $\mathscr{L}(2O)$ and $\mathscr{L}(3O)$ respectively. Conclude there must be a linear relation

$$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^3 = 0$$

   by looking at $\mathscr{L}(6O)$.

   OR (For students familiar with some scheme theory)

3. Prove that any divisor D of degree 3 on E is very ample. Then use Riemann-Roch to show $|D|$ gives an embedding into $\mathbb{P}^2$. In particular, $|3O|$ gives us an embedding of $|E|$ into $\mathbb{P}^2$.

Problem 14 (Play with tangent lines)**.** Suppose that the base field is $\mathbb{C}$. The dual projective space $\mathbb{P}^{2,*}$ is the moduli space parametrizing lines in $\mathbb{P}^2$. It is isomorphic to $\mathbb{P}^2$: a line defined by the equation $Ax + By + Cz = 0$ corresponds to the point $[A : B : C] \in \mathbb{P}^{2,*}$. Let $C \subseteq \mathbb{P}^2$ be a smooth curve of degree $d \geq 1$, then the dual curve C^* is the subset of $\mathbb{P}^{2,*}$ consisting lines tangent to C.

1. Find explicit equation for the dual of a nondegenerate conic $ax^2 + by^2 + cz^2 = 0$.
2. Show that $C^* \subseteq \mathbb{P}^{2,*}$ is a irreducible closed subvariety of dimension 1. Use an example to show that C^* may be singular. What property does C have, if C^* admits an ordinary node or an ordinary cusp?
3. The following two numbers are equal: (1) the degree of the dual curve and (2) the number of tangent lines of C that passes through a fixed general point of $\mathbb{P}^2$. Figure out this number in terms of d.
4. Let C be a smooth planar curve of degree d over $\mathbb{C}$. A point $P \in C$ is called an inflection point of order s, if the intersection multiplicity of C with the tangent line at P is greater or equal to s. For each $s \geq 3$, let $I_C(s)$ be the number of inflection points on C of order s. Show that

$$\sum_{s \geq 3} (s-2) I_C(s) = 3d(d-2)$$

   .

Problem 15 (Play with étale covers)**.** Let k be an algebraically closed field. A morphism of k-schemes is said to be étale, if it is flat and unramified. It is said to be finite étale (or an étale cover), if it is étale and finite. You can think of an étale cover as an analogue of covering spaces in algebraic geometry.

1. Show that any non-constant map between smooth (affine) curves is flat. (Hint: the local ring of a smooth curve at a point is a DVR).

2. Give an example of (1) a flat morphism which is ramified, (2) an unramified morphism which is not flat, (3) an étale morphism which is not finite, (4) a finite morphism which is not étale.

3. Show that $\mathbb{P}^1_k$ does not admit any nontrivial étale cover.

4. If char $k = 0$, show that $\mathbb{A}^1_k$ does not admit nontrivial étale cover. What happens if char $k = p$?