PAWS 2026: ALGEBRAIC GEOMETRY VIA COMPUTATION
PROBLEM SET 0

TOREN D'NELLY-WARADY, AIDAN HENNESSEY, SMITA RAJAN, JAMES RAWSON

Welcome to PAWS! Below are the exercises for Problem Set 0. The questions are divided into a theoretical and a computational section. Within each section, questions are roughly in ascending order of background. Feel free to skip around and try whichever exercises would be the most helpful for you. Try as many as you can but don't feel like you need to complete them all! Also, do not fear – the later problem sets will be much shorter.

1. Theoretical Problems

Question 0: Recall that a ring is an abelian group (called addition, and denoted $+$) along with an associative operation (called multiplication, denoted $\cdot$) with an identity, 1, that distributes over addition, i.e. $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in R$. In this course, we furthermore assume multiplication to be commutative, unless specified otherwise.

(1) Show the following are rings: $\mathbb{Z}, \mathbb{Q}$ with the usual addition and multiplication; complex polynomials $\mathbb{C}[x]$ in one variable with addition and multiplication of polynomials; and $(\mathbb{Z}/3\mathbb{Z})^2$ with coordinate wise addition, $(a,b)+(c,d) = (a+c, b+d)$, and multiplication given by $(a,b)(c,d) = (ac-bd, ad+bc)$.
(2) Let R be a ring. Show that $R \times R$ is also a ring, when addition and multiplication are defined component-wise.
(3) Let R be a ring and -1 be the additive inverse of 1 in R. Show that if $a \in R$, $-1 \times a$ is the additive inverse of a.
(4) Let R be a ring. Show 1 is the unique multiplicative identity in R, that is, if u satisfies $ua = a$ for all $a \in R$, then $u = 1$.

Question 1: Recall that a ring homomorphism $\phi : R \to S$ is a homomorphism of the additive groups such that $\phi(1) = 1$ and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$ for all $r_1, r_2 \in R$.

(1) Show that the following maps are ring homomorphisms: reduction modulo 2: $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$; evaluation at $x = 1$: $\mathbb{Q}[x] \to \mathbb{Q}$; and for any ring R the diagonal map: $\Delta : R \to R^2$, $\Delta(r) = (r, r)$.
(2) Let $\phi : R \to S$ be a ring homomorphism. Show that the image of ϕ is a ring. Give an example to show that the kernel of ϕ, $\ker(\phi) = \{r \in R : \phi(r) = 0\}$, is not necessarily a ring.
(3) Let $\phi : k \to R$ be a ring homomorphism where k is a field (a ring where every element has a multiplicative inverse). Show that ϕ is either injective or the zero map.

Question 2: Recall that an *ideal* I of a ring R is an abelian subgroup of the additive group $(R, +)$ that is closed under multiplication by elements of R. A *generating set* $\{a_j\}_{j \in J}$ is a set of elements of I such that any element of I can be written as a finite sum $r_1 a_1 + ... + r_n a_n$. We use $(a_1, a_2, ..)$ to denote the ideal $I = \{\text{finite sums } r_1 a_1 + ... + r_n a_n\}$, called "the ideal generated by $\{a_j\}$."

An ideal I is *principal* if it is generated by one element, i.e. there is some $a \in R$ such that $I = \{ab : b \in R\}$, equivalently $I = (a)$. An ideal I is *prime* if I not all of R and, whenever $i \in I$ is equal to a product $ab = i$ in R, then either $a \in I$ or $b \in I$. An ideal I is *maximal* if I is not all of R and I is not properly contained in any ideal other than R itself.

Consider the ring $\mathbb{Z}^2$.

(1) Show that the set $S = \{(a, 0) : a \in \mathbb{Z}^2\}$ is an ideal of $\mathbb{Z}^2$.

(2) Find two distinct elements which each generate this ideal. Is every element of S a generator?
(3) Show that there is a ring homomorphism $\varphi : \mathbb{Z}^2 \to \mathbb{Z}$ such that S is the kernel of φ.
(4) Is the ideal S prime?
(5) Show that S is not maximal. Can you find a maximal ideal of $\mathbb{Z}^2$ that contains S?
(6) More generally, given rings R and S, describe the set of prime ideals of $R \times S$.

Question 3: Fix a ring homomorphism $\varphi : R \to S$. The *kernel* $\ker(\varphi)$ of φ is the set of elements $\{r \in R : \varphi(r) = 0\} \subseteq R$. The *image* $\mathrm{im}(\varphi)$ of φ is the set of elements $\{\varphi(r) : r \in R\} \subseteq S$.

Furthermore, we define the *quotient ring* R/I of a ring by an ideal as follows:

- the underlying set is $\{r + I : r \in R\}$
- the addition is $(r_1 + I) + (r_2 + I) := (r_1 + r_2) + I$, where the addition on the right is the addition inherited from R
- the multiplication $(r_1 + I) * (r_2 + I) = (r_1 * r_2) + I$, where the multiplication on the right is the addition inherited from R

(1) Show that the kernel is an ideal of R. Give an example to show the image is not necessarily an ideal of R.
(2) Suppose that φ is surjective, that is, $\mathrm{im}(\varphi) = S$. Show that the quotient ring $R/\ker(\varphi) \simeq S$ (this is known as the *First Isomorphism Theorem*).

Hint: Define a map between $R/\ker(\varphi)$ and S that behaves similarly to φ. Then show that this map is a ring homomorphism and bijective.

Question 4: The *sum* $\sum_{j \in J} I_j$ of a(n arbitrary) set of ideals $\{I_j\}_{j \in J}$ is the set {finite sums $\sum_J r_j i_j$: $r_j \in R, i_j \in I_j$}. The *product* II' of ideals I and I' is the *ideal generated by* the set of products $\{ab : a \in I, b \in I'\}$.

(1) Show that the sum $I + I'$ of ideals I and I' is the smallest ideal containing both I and I'.
(2) Show that the product II' of ideals I and I' is contained in the intersection $I \cap I'$. Show by example that it is not always the largest ideal contained in this intersection. Show that the equality $II' = I \cap I'$ *does* hold under the hypothesis that $I + I' = R$.
(3) Show that the set $\{ab : a \in I, b \in I'\}$ need not be an ideal. (*Hint:* Let k be your favorite field, and consider the multivariate polynomial ring $k[x, y, z, w]$. Let $I = (x, y)$ and $J = (z, w)$. Show that $xz + yw$ cannot be written as a product of an element in I and an element in J.)

Question 5: Let R be a ring. We say R is an *integral domain* if whenever $a \cdot b = 0$, either $a = 0$ or $b = 0$. We say R is a *field* if every non-zero element a has a multiplicative inverse a^{-1}, i.e. $a \cdot a^{-1} = 1$. We call R a *principal ideal domain* (abbreviated PID) if every ideal of R is principal.

(1) Show that the zero ideal $\{0\} \subseteq R$ is prime if and only if R is an integral domain.
(2) Show that the zero ideal is maximal if and only if R is a field.
(3) Show that fields are integral domains.
(4) **Note:** This exercise is likely quite tricky if you haven't used Zorn's lemma before. Show that every proper ideal (i.e. not all of R) is contained in a maximal ideal. (*Hint:* Use Zorn's lemma.)
(5) Show that $\mathbb{Z}$ is a principal ideal domain. (*Hint:* Euclid's algorithm.)
(6) Let k be a field, and show that the polynomial ring $k[x]$ is a principal ideal domain. (*Hint:* Division with remainder.)
(7) Let k be a field. Show that $k[x, y]$ is *not* a PID. (*Hint:* Assume towards contradiction that $(x, y) = (f)$ for some $f \in k[x, y]$.)

Question 6: Let R be a ring, and $I \subseteq R$ an ideal. In this exercise you will prove the *third isomorphism theorem*, which describes the ideals of R/I.

(1) Show that there is an inclusion-preserving bijection

$$\{\text{Ideals of } R \text{ that contain } I\} \longrightarrow \{\text{ideals of } R/I\}, \qquad J \longmapsto J/I,$$

where J/I is the set of cosets

$$J/I = \{a + I : a \in J\}.$$

(2) Show that $(R/I)/(J/I) \cong R/J$.
(3) Let J be an ideal of R that contains I. Prove that J is a prime ideal of R if and only if J/I is a prime ideal of R/I. (*Hint:* Reduce to the case $I = J$, and use Question 5 (1) together with the first isomorphism theorem.)
(4) Let J be an ideal of R that contains I. Prove that J is a maximal ideal of R if and only if J/I is a maximal ideal of R/I.
(5) Show that maximal ideals are prime. (*Hint:* Question 5 (3))

Question 7: This problem surveys some main results about factorization and integrality. Some parts are fairly tough; the most important thing is that you are familiar with the definitions and statements.

Let R be an integral domain. We say an element $p \in R$ is *irreducible* if whenever $p = rs$, either r or s is a unit. We say R is a *unique factorization domain* (abbreviated UFD) if every element r admits a factorization $r = up_1 \cdots p_n$, where u is a unit, the p_i are irreducible, and the factorization is unique up to reordering and multiplying elements by units.

Given an integral domain R, we may construct a field $K = \mathrm{Frac}(R)$, called the fraction field of R, by letting

$$K = \{a/b : a, b \in R\}/\sim,$$

where $a/b \sim c/d$ if $ad = bc$. Addition and multiplication are defined as usual for fractions.

Let R be an integral domain with field of fractions K. We define the *integral closure* $\overline{R}$ of R to be the set of elements $a \in K$ expressible as a root of a monic polynomial $f \in R[x]$ with coefficients in R. If $R = \overline{R}$, we say that R is *integrally closed*.

(1) Confirm that the fraction field is indeed a field, and that $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.
(2) Show that the integral closure of a domain is a ring and is integrally closed.
(3) **(Hard)** Show that PIDs are UFDs.
(4) Let R be a UFD, and let $p \in R$ be irreducible. Show that (p) is a prime ideal.
(5) Show that UFDs are integrally closed. (*Hint/Remark:* This is grown-up restatement of the rational root theorem you likely learned in high school.)
(6) Let R be a UFD. Show that $R[x]$ is a UFD. (*Hint:* Let $K = \mathrm{Frac}(R)$. First factor over $K[x]$, then show this factorization can be made to lie over $R[x]$. For this second step, reduce to *Gauss's lemma*: if $f, g \in R[x]$ have coefficients generating the unit ideal, then fg has coefficients generating the unit ideal as well. For Gauss's lemma, proceed by contradiction, and try reducing mod the maximal ideal guaranteed by Question 5 (4).)
(7) **(Challenge)** Let k be a field, and let $f \in (x^2, xy, y^2) \subseteq k[x, y]$ be irreducible. Let $R = k[x, y]/(f)$. Show that R is not integrally closed. (*Remark:* Integral closure may seem like a strange condition. One reason to consider it is that it is closely tied to smoothness – the failure of R to be integrally closed corresponds to the failure of the graph of f to be smooth at $(0, 0)$.)

Question 8: For each of the following integral domains R, determine whether R is a PID, a UFD, and integrally closed. If R is not integrally closed, compute the integral closure. Here k is a field.

(1) $\mathbb{Z}[\sqrt{-1}]$
(2) $\mathbb{Z}[\sqrt{-5}]$
(3) $\mathbb{Z}[\sqrt{5}]$
(4) $k[x]$
(5) $k[x, y]$
(6) $k[t, t^{-1}]$
(7) $k[t^2, t^3]$

2. Computational Problems

Macaulay2 is a software package designed for symbolic computation in commutative algebra, algebraic geometry, and algebraic combinatorics. It is a great tool for computing examples and implementing algorithms in these fields. A free online version is available here. We expect the online version to be entirely sufficient for this course. Nonetheless, students may want an instance that they can run offline. For instructions on how to download Macaulay2, visit here.

Question 9: Download Macaulay2 or load up the web version. Complete as much as you can (or want to) of the introductory Macaulay2 tutorial. This will help you learn the syntax and some common commands.

Question 10: Let $R = \mathbb{Q}[x, y, z, w]/(xz - y^2, yw - z^2, xw - yz)$. Let $S = \mathbb{Q}[a^3, a^2b, ab^2, b^3]$.

(1) Construct these rings in Macaulay2.
(2) Are these rings isomorphic? Can you get Macaulay2 to tell you?
(3) Now let $A = \mathbb{Q}[t^2, ts^2, s^5, t^7]$. Express A as a quotient of a polynomial ring by an ideal. (*Hint:* Construct a map from a polynomial ring, sending a variable to each generator. Have Macaulay2 compute the kernel.)
(4) Start thinking about what the Kernel algorithm implemented in Macaulay2 might look like.

Question 11: Consider the polynomial ring $R = k[x, y]/\langle y^2 - x^2(x + 1)\rangle$.

(1) Is $\langle y^2 - x^2(x + 1)\rangle$ a prime ideal of $k[x, y]$? Use Macaulay2 to confirm.
(2) Is R an integral domain?
(3) What are the prime ideals of R? What are the maximal ideals of R? (Hint: What are the prime ideals of $k[x, y]$, and what are the prime ideals of a quotient ring R/I?)
(4) What is the integral closure of R in its field of fractions? Check your answer using the integralClosure command in Macaulay2.