PAWS 2026: ALGEBRAIC GEOMETRY VIA COMPUTATION PROBLEM SET 2

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

1. Theoretical Problems

Question 1: Ideal Membership in One Variable. Let $g \in \mathbb{K}[x]$ be nonzero and $f \in \mathbb{K}[x]$.

(a) Prove the uniqueness of the remainder in the division algorithm: if $f = qg + r = q'g + r'$ and each remainder is either zero or has degree strictly less than $\deg(g)$, show that $q = q'$ and $r = r'$.
(b) Carefully prove that $f \in \langle g \rangle$ if and only if the remainder of f divided by g is zero.
(c) Assume that an ideal of $\mathbb{K}[x]$ is presented by a generator g. Describe an algorithm that decides whether a given f lies in $\langle g \rangle$. Why does the fact that $\mathbb{K}[x]$ is a PID mean that this method applies to every ideal once a generator has been found?

Question 2: The Remainder Is Not Intrinsic: The Twisted Cubic Again. Work in $\mathbb{K}[x, y, z]$ with lex order $x > y > z$. Set $g_1 = x^2 - y$, $g_2 = xy - z$, and $I = \langle g_1, g_2 \rangle$. This is the ideal that defined the twisted cubic curve on the previous problem sheet but we have changed the signs of the displayed generators so that their leading coefficients are 1.

(a) Divide x^2y by (g_1, g_2) and show that the remainder is y^2.
(b) Divide the same polynomial by (g_2, g_1) and show that the remainder is xz.
(c) Verify the identity $yg_1 - xg_2 = xz - y^2$. Show this representation of $f = xz - y^2$ is not a standard representation (i.e. it could not come from the division algorithm).
(d) Recall that the substitution map sends $x \mapsto t$, $y \mapsto t^2$, and $z \mapsto t^3$. Check that both remainders y^2 and xz map to t^4. Explain why they represent the same polynomial function on the twisted cubic even though division has produced different representatives.
(e) Compute $\mathrm{LM}(xz - y^2)$. Divide $xz - y^2$ by either displayed list and explain why the algorithm returns the same nonzero polynomial, even though it lies in I.
(f) A zero remainder proves ideal membership. Does a nonzero remainder prove nonmembership? Use part (e) to answer, and explain why this failure is more serious than the mere nonuniqueness in parts (a) and (b).

Question 3: A Hidden Consequence of the Circle–Parabola Equations. Work in $\mathbb{K}[x, y]$ with lex order $x > y$ and set $f_1 = x^2 - y$, $f_2 = x^2 + y^2 - 1$, and $I = \langle f_1, f_2 \rangle$.

(a) Compute $\mathrm{LM}(f_1)$ and $\mathrm{LM}(f_2)$. What is the ideal generated by these two leading monomials?
(b) Consider the difference $h = f_2 - f_1 = y^2 + y - 1$. Show that $h \in I$ and compute $\mathrm{LM}(h)$.
(c) Conclude that $\langle \mathrm{LM}(f_1), \mathrm{LM}(f_2)\rangle$ is a proper subset of $\mathrm{in}_<(I)$. Which leading monomial was invisible in the original list?
(d) Divide h by the ordered list (f_1, f_2). Can either $\mathrm{LM}(f_1)$ or $\mathrm{LM}(f_2)$ be used to cancel the leading term of h at the first step? What remainder does the algorithm return, and why is this apparently uneventful calculation a decisive failure of the membership test?
(e) Geometrically, what does $h(y) = 0$ tell us about the possible y-coordinates of the intersection points? Why is it natural to call h an elimination equation?

Question 4: When Does Division Decide Membership? Let $S = \mathbb{K}[x_1, \ldots, x_n]$, let $I \subseteq S$ be an ideal, and fix a monomial order. Let $G = (g_1, \ldots, g_s)$ be a finite list of nonzero elements of I.

(a) Suppose the list is a Gröbner basis, meaning that
$$\mathrm{in}_<(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s)\rangle = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\rangle.$$
Let $f \in I$ and divide f by $(g_1, \ldots, g_s)$, obtaining remainder r. Show that $r \in I$.
(b) If $r \neq 0$, then $\mathrm{LM}(r) \in \mathrm{in}_<(I)$. Use the monomial-ideal criterion proved above to explain why the displayed equality forces some $\mathrm{LM}(g_i)$ to divide $\mathrm{LM}(r)$.
(c) On the other hand, no monomial of a remainder is divisible by any $\mathrm{LM}(g_i)$. Explain why this contradicts part (b), and conclude that $r = 0$.
(d) For this fixed ordered list G, write $\mathrm{rem}_G(f)$ for the remainder. Conclude that
$$f \in I \iff \mathrm{rem}_G(f) = 0.$$
For the reverse implication, use $\langle g_1, \ldots, g_s\rangle \subseteq I$.
(e) Since every $f \in I$ has zero remainder, use the division identity to conclude that $I = \langle g_1, \ldots, g_s\rangle$.
(f) Suppose division by G returns zero for every $f \in I$. Let $0 \neq f \in I$. Explain why,
$$\mathrm{in}_<(I) = \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\rangle.$$
Be sure to use $g_i \in I$ for the reverse containment.
(g) Suppose $I = \mathbb{I}(X)$ for an algebraic set X. Interpret this membership test geometrically as deciding whether the hypersurface $\mathbb{V}(f)$ contains X. Why must this interpretation be qualified when I is merely an ideal cutting out X, rather than the full vanishing ideal?

Question 5: Canonical Normal Forms and Quotient Bases. Suppose that $G = (g_1, \ldots, g_s)$ is a Gröbner basis for I. Let $f \in \mathbb{K}[x_1, \ldots, x_n]$. We will show that the remainder of f divided by G exists, is unique, and can be expressed in terms of the standard monomials of I.

(a) Suppose that $r, r' \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f - r \in I$ and $f - r' \in I$. Prove that $r - r' \in I$.

(b) Assume that $r-r' \neq 0$. Prove that if every monomial appearing in r or every monomial appearing in r' is a standard monomial for I then $\mathrm{LM}(r-r') \in \mathrm{in}_<(I)$.

(c) Assume that $r - r' \neq 0$. Prove that every monomial in $r - r'$ is a standard monomial. Deduce that $r = r'$.

(d) Divide f by G obtaining the following output division identity:

$$f = q_1 g_1 + \cdots q_s g_s + r$$

where no monomial appearing in r is divisible by any of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)$. Prove that every monomial in r is standard.

(e) Prove that the classes of the standard monomials in $\mathbb{K}[x_1, \ldots, x_n]/I$ form $\mathbb{K}$-basis for $\mathbb{K}[x_1, \ldots, x_n]/I$.

2. Computational Problems

Question 6: Examples of Leading Terms. Consider $f = x - y^2$ and $h = xz - y^2$ as elements of $\mathbb{K}[x, y, z]$.

(a) Compute the leading term, leading coefficient, and leading monomial of both f and h with respect to lex, graded lex, and graded reverse lexicographic order, with $x > y > z$.

(b) Run the following in a new *Macaulay2* session. After running the code, replace `Lex` first by `GLex` and then by `GRevLex`, restarting each time. Compare the three outputs with your answers to part (a).

```
restart
R = QQ[x,y,z,MonomialOrder=>Lex];
f = x-y^2;    -- the equation y^2=x in the xy-plane
h = x*z-y^2; -- the hidden twisted cubic relation

{leadMonomial f,leadCoefficient f,leadTerm f}
leadMonomial h
```

(c) In *Macaulay2*, we give a one-input function a name using the arrow notation

`name = input -> output`.

A parenthesized block may contain several statements separated by semicolons; the final expression without a semicolon is the value returned by the function. For example, the following function returns the list $\{\mathrm{LM}(p), \mathrm{LC}(p), \mathrm{LT}(p)\}$:

```
leadData = p -> (
    LMp := leadMonomial p;
    LCp := leadCoefficient p;
    LTp := leadTerm p;
    {LMp, LCp, LTp}
)
leadData f
apply({f,h},p -> leadData p)
```

Predict both outputs before running the code.

Question 7: Hidden Leading Terms in *Macaulay2*. Let us return to the circle–parabola ideal and will compute a Gröbner basis for the ideal $I = \langle x^2 - y, x^2 + y^2 - 1 \rangle$ with respect to the lex monomial order with $x > y > z$ using *Macaulay2*. It will also compute the initial ideals.

(a) Compute the leading terms of the ideal I using the given generators, and store this in a variable called `shownLeadingIdeal`. Then, use `gb` to compute a Gröbner basis for I (store it in `B`), and store the ideal generated by these leading terms in `fullLeadingIdeal`.

(b) Explain why `shownLeadingIdeal` uses only the leading terms of the displayed generators, whereas `fullLeadingIdeal` uses the basis computed from the whole ideal. Which missing leading monomial distinguishes the outputs?

(c) Compare the zero remainder `h % B` with the hand division in Exercise 3(d). Explain why the two computations use different lists of divisors.

(d) A function with two inputs is defined by placing the inputs in parentheses. Write a function named `hasZeroRemainder` which takes a polynomial p and a Gröbner basis object C and returns `true` precisely when `p % C` is zero. Use it with B and `apply` to test the three polynomials

$$h, \qquad x, \qquad x^4 + x^2 - 1$$

in a single command, predicting the three Boolean outputs before asking the computer. *Hint:* Inside `apply` use a one-input function of the form `p -> hasZeroRemainder(p,B)`. What ideal-membership principle do these outputs suggest? The next exercise will prove that this interpretation is valid.

(e) *Write the code yourself.* Start a fresh session with lex order $y > x$; remember that variables are ordered as they are declared in the ring. Compute a Gröbner basis and verify that its initial ideal is $\langle y, x^4 \rangle$, with standard monomials $1, x, x^2, x^3$. For lex $x > y$, the standard monomials were $1, x, y, xy$. Use $y \equiv x^2$ and $xy \equiv x^3$ to pass between the two lists in the quotient. Why do both orders record quotient dimension 4? Which order reveals an equation in y, and which reveals one in x?