Math 40510, Algebraic Geometry

Problem Set 1, due March 5, 2021

Note: Answers that are sloppy, either from a mathematical point of view or because they are hard to read, will result in points being deducted even if they are technically correct.

Solutions

1. In class we proved that if k is an infinite field and $f \in k[x_1, \ldots, x_n]$ then the following are equivalent:

   - f is the zero polynomial.
   - The evaluation function $f : k^n \to k$, defined by $f(P) = f(b_1, \ldots, b_n)$ for $P = (b_1, \ldots, b_n) \in k^n$, is the zero function. (I.e. f, evaluated at any point of k^n, vanishes.)

   Here we'll explore what happens when k is finite.

   a) (5 points) Let $k = \mathbb{Z}_{19}$. Give an example of a non-zero polynomial $f \in k[x]$ such that $f : k \to k$ defines the zero function.

   Solution:
   Recall Fermat's theorem: any element a of $\mathbb{Z}_{19}$ satisfies $a^{19} = a$ (in $\mathbb{Z}_{19}$). So the polynomial $f(x) = x^{19} - x$ defines the zero function, but is obviously not the zero polynomial since its coefficients are not zero. □

   b) (5 points) Let $k = \mathbb{Z}_5$. Let $f \in k[x, y]$. Give an example of a non-zero polynomial f of degree 5, **involving both variables**, for which $f : k^2 \to k$ is the zero function.

   Solution:
   Applying the same trick as in a), we can look at $f(x, y) = x^5 - x + y^5 - y$. □

   c) (5 points) Let $k = \mathbb{Z}_5$. Let $f \in k[x, y]$. Assume that f is either the zero polynomial or a polynomial of degree 4. Prove that f is the zero polynomial if and only if $f : k^2 \to k$ is the zero function. [Pay attention to the fact that f is a polynomial of two variables, not one variable!! I want a clear, well-argued proof.]

   Solution:
   We'll proceed as in class, with a tweak or two.

   If f is the zero polynomial then clearly it defines the zero function, so the interesting direction is the converse.

   Let $f(x, y)$ be a non-zero polynomial in two variables over $\mathbb{Z}_5$ that defines the zero function. We'll assume that f has degree 4, get a contradiction, and conclude that instead it must be the zero polynomial.

   Break up f according to the power of x:

   $$f(x, y) = g_0(y)x^4 + g_1(y)x^3 + g_2(y)x^2 + g_3(y)x + g_4(y) \tag{1}$$

   where $g_0(y)$ is a constant (possibly zero), $g_1(y)$ has degree at most 1 (or is the zero polynomial), $g_2(y)$ has degree at most 2 (or is the zero polynomial), etc. These bounds on the degrees of the $g_i(y)$ are because f itself has total degree 4. Our assumption that f defines the zero function means that no matter what you plug in for x and for y, the result is 0. So pick an arbitrary value $b \in \mathbb{Z}_5$ and plug it in for y. This gives a polynomial

   $$f(x, b) = g_0(b)x^4 + g_1(b)x^3 + g_2(b)x^2 + g_3(b)x + g_4(b)$$

of degree ≤ 4 in the variable x, and our assumption is that it vanishes for $x = 0, 1, 2, 3, 4$. Since a non-zero polynomial in one variable (namely x in this case) of degree ≤ 4 can't have five roots, it must be the zero polynomial. This means that the coefficients $g_i(b)$ must all be equal to 0 for $i = 0, \ldots, 4$. But b was arbitrary. This means that each $g_i(y)$ vanishes at each of $y = 0, 1, 2, 3, 4$, so by the same argument, each $g_i(y)$ is the zero polynomial. But then by equation (1), $f(x, y)$ is the zero polynomial.

d) (5 points) Parts b) and c) look somewhat contradictory at first glance. In b), a non-zero polynomial *can* define the zero function, while in c) you show that a non-zero polynomial *can't* define the zero function. Obviously the only difference is the assumption about the degree. Explain how the degree makes such a big difference here.

Solution:
In part c), at several points in the argument we had a polynomial of degree < 5 with five roots, which is impossible unless that polynomial is the zero polynomial. In part b), the polynomial of degree 5 is perfectly able to have five roots, so there is no obstacle.

2. In class we defined the twisted cubic as $C = \mathbb{V}(y - x^2, z - x^3) = \{(t, t^2, t^3) \mid t \in \mathbb{R}\} \subset \mathbb{R}^3$ (a parametrization). We say that X is a *subvariety* of Y if X is an affine variety and $X \subseteq Y$.

a) (5 points) Prove that $\{(t, t^2, t^3\} \mid t = 1, 2, 3, \ldots, 319\}$ is an affine subvariety of C. [Hint: you don't have to find explicit equations for this set!]

Solution:
This is a finite set of points. A single point in $\mathbb{R}^3$ is an affine variety: if $P = (a, b, c)$ then $P = \mathbb{V}(x - a, y - b, z - c)$. We saw in class that a finite union of affine varieties is again an affine variety.

b) (8 points) Prove that $A = \{(t, t^2, t^3) \mid t \text{ is an even integer}\}$ is not an affine subvariety of C. More precisely, suppose A were an affine variety. Then $A = \mathbb{V}(f_1, \ldots, f_r)$, where $f_i \in \mathbb{R}[x, y, z]$ for $1 \leq i \leq r$. Derive a contradiction from this. [Hint: your conclusion should *not* be that f_i is the zero polynomial in $\mathbb{R}[x, y, z]$. Carefully explain what you *can* conclude.]

Solution:
This is *not* a finite set of points, so we have to work a little harder. For each i we have that f_i vanishes at all the points of A, so $f_i(t, t^2, t^3)$ vanishes for each even integer t. This is a polynomial in t (not x, y, z because we've replaced x, y, z by expressions in t) and it vanishes for infinitely many values of t. This forces $f_i(t, t^2, t^3)$ to be the zero polynomial in $\mathbb{R}[t]$. Hence f_i (now thought of as a polynomial in x, y, z again) vanishes at every point of the form (t, t^2, t^3), i.e. it vanishes at every point of C. So there is no polynomial that vanishes on the points of A but not all the points of C. That is, the statement $A = \mathbb{V}(f_1, \ldots, f_r)$ is impossible – all you can conclude is $A \subseteq \mathbb{V}(f_1, \ldots, f_r)$. So this infinite proper subset A of the twisted cubic is not an affine variety. (Later we'll conclude that C is the *Zariski closure* of A, i.e. the smallest variety containing A.)

c) (8 points) Let Λ be any plane in $\mathbb{R}^3$. Prove that the intersection of Λ with C (i.e. $\Lambda \cap C$) consists of at most three points.

Solution:
The equation of Λ is $ax + by + cz + d = 0$ for some a, b, c, d. The intersection $\Lambda \cap C$ consists of the points of C vanishing on Λ, so we can just look at the solutions of $at + bt^2 + ct^3 + d = 0$ in the single variable t. This is a polynomial of degree 3, so there are at most three solutions, i.e. there are at most 3 points of $C \cap \Lambda$.

d) (8 points) Find a specific plane Λ with the property that $\Lambda \cap C$ consists of

(i) two points;

Solution:
We want a polynomial in t of degree 3 with only two distinct roots. For example, you could choose the polynomial

$$t^2(t-1) = t^3 - t^2 = 0t - t^2 + t^3 + 0,$$

which has only the roots $t = 0, 1$ (but there are lots of possible choices). So take $\Lambda = \mathbb{V}(0x - y + z + 0) = \mathbb{V}(z - y)$. Then

$$\Lambda \cap C = \{(0,0,0), (1,1,1)\}.$$

(ii) one point.

Solution:
Now we want a polynomial of degree 3 in t with only one distinct root. For example, you could choose

$$(t-5)^3 = t^3 - 15t^2 + 75t - 125 = 75t - 15t^2 + t^3 - 125,$$

which has only the root $t = 5$. Then take $\Lambda = \mathbb{V}(75x - 15y + z - 125)$. Then

$$\Lambda \cap C = \{(5, 25, 125)\}.$$

3. This problem is just to get your hands dirty a little bit with ideals and polynomials. Let $R = \mathbb{R}[x, y, z]$. Let

$$I = \langle y - x^2, z - x^3 \rangle \quad \text{and} \quad J = \langle z - xy, y - x^2, y^2 - xz \rangle.$$

a) (7 points) Without making any connections to the twisted cubic, prove directly that $I = J$. [You will probably want to prove the two inclusions.]

Solution:
We'll prove the two inclusions.

$\subseteq$:
It's enough to prove the each of the two generators of I is in J. Let's put the generators of I in red and the generators of J in blue. $y - x^2$ is already a generator of J, so it is clearly in J. Then

$$z - x^3 = (z - xy) + x(y - x^2) \in J$$

and we are done.

$\supseteq$:
Now we'll prove each generator of J is in I. Again, red is I and blue is J.

$$z - xy = (z - x^3) - x(y - x^2) \in I.$$

$y - x^2$ is a generator of I so it is clearly in I.

$$y^2 - xz = (y + x^2)(y - x^2) - x(z - x^3) \in I$$

and we are done.

b) (5 points) One of the given generators of J is actually redundant, meaning that if you remove it, the ideal doesn't get smaller. Prove it.

Solution:

We will show that $y^2 - xz$ is a linear combination of the other three generators of J. In fact

$$y^2 - xz = y(y - x^2) - x(z - xy).$$

This means that

$$\langle z - xy, y - x^2, y^2 - xz\rangle = \langle z - xy, y - x^2\rangle = \langle y - x^2, z - x^3\rangle.$$

4. Let I and J be ideals (in particular neither is empty) in $R = k[x_1, \ldots, x_n]$, where k is a field. For each of the following, either prove that it is again an ideal or prove that it is **not** necessarily an ideal by giving a counterexample. Either way, make sure you provide enough details. Again, you are assuming that I and J are themselves already ideals.

   a) (8 points) $I \cap J$.

   Solution:
   This is an ideal.

   - It is not empty since if $f \in I$ and $g \in J$ then $fg \in I \cap J$.
   - If f and g are in $I \cap J$ then f and g are both in I and they are both in J. Since they are both in I, and I is an ideal, then $f + g \in I$. Similarly $f + g \in J$, so $f + g \in I \cap J$, and hence $I \cap J$ is closed under addition.
   - If $f \in I \cap J$ and $h \in R$ then $hf \in I$ (since I is an ideal) and $hf \in J$ (since J is an ideal) so $hf \in I \cap J$ and so $I \cap J$ is closed under multiplication by elements of R.

   Thus $I \cap J$ is an ideal.

   b) (8 points) $I \cup J$.

   Solution:
   This is not an ideal. For example, take $I = \langle x\rangle$ and $J = \langle y\rangle$ in $k[x, y]$. Then $x \in I \cup J$ and $y \in I \cup J$ but $x + y \notin I \cup J$ since elements of $I \cup J$ have to be divisible either by x or by y, but $x + y$ isn't. So $I \cup J$ is not closed under addition.

   c) (8 points) $I \setminus J = \{f \in R \mid f \in I \text{ but } f \notin J\}$. [Hint: think before you start writing. Remember J is an ideal.]

   Solution:
   This is not an ideal since J contains 0, so if you remove 0 from I then what's left can't be an ideal.

   d) (8 points) $I : J = \{f \in R \mid f \cdot g \in I \text{ for all } g \in J\}$.

   Solution:
   This is an ideal.

   - It's not empty since $0 \in I : J$.
   - Let $f_1, f_2 \in I : J$. Then $f_1 g \in I$ for all $g \in J$ and $f_2 g \in I$ for all $g \in J$ by definition of $I : J$, so $f_1 g + f_2 g = (f_1 + f_2)g \in I$ for all $g \in J$ since I is closed under addition (it is an ideal). Thus $I : J$ is closed under addition.
   - Let $f \in I : J$ and let $h \in R$. Since $f \in I : J$, $fg \in I$ for all $g \in J$. Is $fh \in I : J$? Let $g \in J$. Then $(fh)g = f(gh) \in I$ since $gh \in J$ (remember J is an ideal) and $f \in I : J$. That is, fh knocks any $g \in J$ into I. So $fh \in I : J$.

Thus $I : J$ is an ideal.

5. (7 points) In class we proved that

- If V, W are *sets* in k^n then
$$V \subseteq W \quad \Rightarrow \quad \mathbb{I}(V) \supseteq \mathbb{I}(W)$$
where, for a set X in k^n,
$$\mathbb{I}(X) = \{f \in k[x_1, \ldots, x_n] \mid f(P) = 0 \text{ for all } P \in X\}$$
is defined exactly the same way that it is if X is a variety.
- If V is any set in k^n and W is a variety in k^n then
$$\mathbb{I}(V) \supseteq \mathbb{I}(W) \quad \Rightarrow \quad V \subseteq W.$$

(So far this is a reminder of what we proved in class, not what you have to prove in this problem.)

This problem focuses on why we need the extra assumption, in the second bullet, that W is a variety. Give an example of two sets, V and W, such that
$$\mathbb{I}(V) \supseteq \mathbb{I}(W) \quad \text{but} \quad V \text{ is not a subset of } W.$$
Be sure to justify your answer; don't just give an example without comment. [Hint: of course if W is a variety then this is impossible, thanks to the second bullet above, so focus on examples where W is not a variety. There's one in this problem set.]

Solution:

We'll use our work in problem 2. Specifically, in part b) of that problem we showed that any polynomial that vanishes on
$$A = \{(t, t^2, t^3) \mid t \text{ is an even integer}\}$$
has to vanish on the whole twisted cubic curve C. This shows $\mathbb{I}(A) \subseteq \mathbb{I}(C)$. But we also know that $A \subseteq C$, so by the first bullet we get that $\mathbb{I}(A) \supseteq \mathbb{I}(C)$. Thus $\mathbb{I}(A) = \mathbb{I}(C)$. So far this isn't what we're looking for, but it points us in the right direction.

The exact same argument can be used to show that for
$$B = \{(t, t^2, t^3) \mid t \text{ is an odd integer}\},$$
$\mathbb{I}(B) = \mathbb{I}(C)$.

Let's choose $V = A$ and $W = B$. We know that
$$\mathbb{I}(V) = \mathbb{I}(A) = \mathbb{I}(C) = \mathbb{I}(B) = \mathbb{I}(W),$$
so we have both $\mathbb{I}(V) \subseteq \mathbb{I}(W)$ and $\mathbb{I}(W) \subseteq \mathbb{I}(V)$. But not only is neither of V, W contained in the other, but in fact they are disjoint!! (This is a bit more than what the problem asked for.)