Math 40510, Algebraic Geometry

Problem Set 1 Solutions, due February 14, 2020

1. Inside the affine space $\mathbb{R}^2$ we have the subset $\mathbb{Z}^2$ consisting of all the points (a, b) where $a, b \in \mathbb{Z}$. Let $f \in \mathbb{R}[x, y]$ and assume that $f(a, b) = 0$ for all $(a, b) \in \mathbb{Z}^2$. Prove that f must be the zero polynomial. (Note that we're assuming $f(a, b) = 0$ for all $(a, b) \in \mathbb{Z}^2$, not all $(a, b) \in \mathbb{R}^2$.)

   Solution.
   Suppose f is not the zero polynomial. As in class, write f in ascending powers of y:

$$f(x, y) = g_0(x) + g_1(x) \cdot y + g_2(x)y^2 + \cdots + g_m(x)y^m \tag{1}$$

   where m is the highest power of y occurring in f. Choose any $a \in \mathbb{Z}$ and plug $x = a$ into f, and call the result $F(y)$:

$$F(y) = g_0(a) + g_1(a)y + g_2(a)y^2 + \cdots + g_m(a)y^m \in \mathbb{R}[y].$$

   Our assumption says that $F(y)$ vanishes at all integer points of $\mathbb{R}$ (of which there are infinitely many), whereas F has degree m. Thus F must be the zero polynomial. This means that $g_i(a) = 0$ for all $a \in \mathbb{Z}$, since a was chosen arbitrarily. But $g_i(x)$ is a polynomial in just one variable, x, so again, this forces g_i to be the zero polynomial, for all i, so by (1), $f(x, y)$ is the zero polynomial.

2. Informally, we often "identify" the complex plane $\mathbb{C}$ with the plane $\mathbb{R}^2$. In algebraic geometry we have to be a bit more careful.

   Consider the affine spaces, $\mathbb{C}^1$ and $\mathbb{R}^2$. Consider the unit circle C inside both of them. In $\mathbb{C}$ this is defined by $|z| = 1$, and in $\mathbb{R}^2$ it's defined by $x^2 + y^2 = 1$. Prove that as a subset of $\mathbb{C}^1$, C is *not* a variety, while in $\mathbb{R}^2$ it *is* a variety. (Note that for the former, it is not enough to just say that it's not a variety because $|z|$ is not a polynomial.)

   Solution.
   If C were a variety in $\mathbb{C}^1$, it would be of the form $C = \mathbb{V}(f_1, \dots, f_m)$ where $f_1, \dots, f_m \in \mathbb{C}[x]$. But a polynomial in one variable has a finite number of roots, so even $\mathbb{V}(f_1)$ alone must be finite, and then $\mathbb{V}(f_1, \dots, f_m) \subseteq \mathbb{V}(f_1)$ has to be finite too. But C is not finite, so we have a contradiction. This proves the first part.

   On the other hand, in $\mathbb{R}^2$ we already said $C = \mathbb{V}(x^2 + y^2 - 1)$, so it is an affine variety.

3. An ideal I is said to be *radical* if the condition $f^m \in I$ necessarily implies $f \in I$.

   a) Prove that a prime ideal is always radical.

   Solution.
   Let R be the ring in which I is an ideal. Let $f \in R$ and assume that $f^m \in I$. We will prove that $f \in I$ by induction on m. If $m = 1$ this means $f = f^1 \in I$, so we are done. Otherwise we have $f \cdot f^{m-1} \in I$. Since I is prime, this means either $f \in I$ or $f^{m-1} \in I$. In the former case we are done. In the latter case, $f \in I$ follows by induction.

   b) Is the converse true (i.e. is a radical ideal always prime?)? If so, prove it. If not, give a counterexample and justify your claim that it's a counterexample.

   Solution 1.
   No, the converse is not true. Let $R = \mathbb{C}[x, y]$ and let $I = \langle xy \rangle$. This is clearly not prime since $xy \in I$ but neither x nor y is in I. We claim that I is a radical ideal. Let $f \in R$ satisfy $f^m \in I$

for some $m \geq 1$. This means

$$f \cdot \dots \cdot f = f^m = xy \cdot g$$

for some $g \in R$. Since x is a factor on the right and R is a UFD, x is a factor on the left. Since x is irreducible, it divides f. Similarly for y. Thus $f \in \langle xy \rangle$.

Solution 2.
Let $X \subset \mathbb{R}^2$ be the set of points $\{(0,1),(0,2)\}$. We know from part (c) below that $\mathbb{I}(X)$ is a radical ideal. On the other hand, the polynomial $(y-1)(y-2)$ is clearly in $\mathbb{I}(X)$, while neither $y-1$ nor $y-2$ contains both points so neither is in $\mathbb{I}(X)$. Thus $\mathbb{I}(X)$ is not prime.

c) Prove that if S is a set in an affine space k^n then $\mathbb{I}(S)$ is a radical ideal.

Solution.
Let $f \in k[x_1, \dots, x_n] = R$ such that $f^m \in \mathbb{I}(S)$, i.e. $(f^m)(P) = 0$ for all $P \in S$. This means $f(P)^m = 0$ for all $P \in S$. But k is a field, hence also is an integral domain, so $f(P) = 0$ for all $P \in S$, and $f \in \mathbb{I}(S)$.

4. Define a function $\phi : \mathbb{C}^2 \to \mathbb{C}^3$ by $\phi(a,b) = (a^2, ab, b^2)$, where $a, b \in \mathbb{C}$.

a) Is ϕ surjective? Give a proof or disprove with a counterexample.

Solution.
No. The point $(0,1,0)$ is clearly not in the image.

b) Is ϕ injective? Give a proof or disprove with a counterexample.

Solution.
No. $\phi(1,1) = \phi(-1,-1)$.

c) Find a point of $\mathbb{C}^3$ that has exactly one preimage point, and justify your answer.

Solution.
Consider the point $(0,0,0) = \phi(0,0)$. If $(a^2, ab, b^2) = (0,0,0)$ then clearly $a = b = 0$, so $(0,0)$ is the only preimage point of $(0,0,0)$.

d) Let $R = \mathbb{C}[z_1, z_2, z_3]$. Prove that the image of ϕ is an affine variety in $\mathbb{C}^3$ by giving the defining polynomial(s) in R. Be sure to prove that the variety they define is *exactly* the image of ϕ.

Solution.
Let (a^2, ab, b^2) be any point in the image, $\phi(\mathbb{C}^2)$, of ϕ. Clearly this point satisfies the equation $z_2^2 - z_1 z_3 = 0$ since $(ab)^2 - (a^2)(b^2) = 0$. Thus $\phi(\mathbb{C}^2) \subseteq \mathbb{V}(z_2^2 - z_1 z_3)$. We claim that the reverse inclusion is true, i.e. $\mathbb{V}(z_2^2 - z_1 z_3) \subseteq \phi(\mathbb{C}^2)$. This will give us equality, so $\phi(\mathbb{C}^2)$ is an affine variety.

To see the claim, let $(d,e,f) \in \mathbb{V}(z_2^2 - z_1 z_3)$, where $d, e, f \in \mathbb{C}$. This means $e^2 = df$. We want to show that $(d,e,f) = \phi(P)$ for some $P \in \mathbb{C}^2$.

Case 1. $(d,e,f) = (0,0,0)$. We have already seen that $\phi(0,0) = (0,0,0)$.

Case 2. $e = 0$. This means $df = 0$. We have already taken care of $d = f = 0$, so assume that one of the two is not zero, say $d \neq 0$ (then we necessarily have $f = 0$ since $0 = e^2 = df$). We want to find P so that $\phi(P) = (d,0,0)$. Since d is a non-zero complex number, it has two square roots, say α and $-\alpha$. Then for example

$$\phi(\alpha, 0) = (\alpha^2, \alpha \cdot 0, 0^2) = (d, 0, 0)$$

so we can take $P = (\alpha, 0)$.

Case 3. $e \neq 0$. Then since $e^2 = df$, we also have $d, f \neq 0$. Now the complex number df has two square roots, namely e and $-e$. The complex number d has two square roots, call them α and $-\alpha$. Similarly, the complex number f has two square roots, β and $-\beta$. In particular, we have $\alpha^2 = (-\alpha)^2 = d$ and $\beta^2 = (-\beta)^2 = f$.

Note $(\alpha\beta)^2 = \alpha^2\beta^2 = df$. This means either $\alpha\beta = e$ or $\alpha\beta = -e$. If $\alpha\beta = e$ then $(d, e, f) = \phi(\alpha, \beta)$. If $\alpha\beta = -e$ then $(d, e, f) = \phi(\alpha, -\beta)$. Either way, $(d, e, f) \in \phi(\mathbb{C}^2)$, so we have proved our inclusion and we are done.

e) Let $S = \mathbb{C}[x, y]$. Let $V = \mathbb{V}(x - y)$ inside $\mathbb{C}^2$. Prove that $\phi(V)$ is a subvariety of $\mathbb{C}^3$ by giving its defining polynomial(s).

Solution.
The points of V are exactly the points $(\alpha, \alpha) \in \mathbb{C}^2$, where $\alpha \in \mathbb{C}$. Hence the points of $\phi(V)$ are exactly the points of the form $(\alpha^2, \alpha \cdot \alpha, \alpha^2) = (\alpha^2, \alpha^2, \alpha^2)$. Since every complex number has a square root, the points of the form α^2 span all of $\mathbb{C}$. Thus

$$\phi(V) = \{(\lambda, \lambda, \lambda) \mid \lambda \in \mathbb{C}\} = \mathbb{V}(z_1 - z_2, z_1 - z_3).$$

Thus we have the defining polynomials for the variety $\phi(V)$.

5. a) Explain why Problem #1 shows that $\mathbb{Z}^2$ is not an affine variety in $\mathbb{R}^2$. (This should only take a few lines.)

Solution.
If $\mathbb{Z}^2$ were an affine variety in $\mathbb{R}^2$, it would be of the form $\mathbb{Z}^2 = V(f_1, \dots, f_s)$ for some polynomials $f_1, \dots, f_s$. In particular, these polynomials have to vanish on $\mathbb{Z}^2$. By Problem #1, all of these polynomials must be the zero polynomial. But the vanishing locus of the zero polynomial is $\mathbb{R}^2$, not $\mathbb{Z}^2$. Contradiction.

b) If X is a set in $\mathbb{R}^2$ (it may or may not be an affine variety), and W is an affine variety that contains X, we'll say that "*W is the smallest variety containing X*" if there is no variety V such that

$$X \subseteq V \subsetneq W.$$

Referring again to Problem #1, what is the smallest affine variety in $\mathbb{R}^2$ that contains $\mathbb{Z}^2$? Carefully explain your answer.

Solution.
If $V = \mathbb{V}(f_1, \dots, f_s)$ is a variety containing $\mathbb{Z}^2$, in particular all the f_i have to vanish on $\mathbb{Z}^2$. Then by Problem #1, again all the f_i are the zero polynomial. Thus W must be $\mathbb{R}^2$.

c) Recall that the twisted cubic curve in $\mathbb{R}^3$ is

$$C = \{(t, t^2, t^3) \mid t \in \mathbb{R}\} = \mathbb{V}(y - x^2, z - x^3).$$

Let

$$X = \{(t, t^2, t^3) \mid t \in \mathbb{Z}\}.$$

Find the smallest affine variety in $\mathbb{R}^3$ that contains X. Carefully explain your answer.

Solution.
We'll show that the smallest affine variety W in $\mathbb{R}^2$ that contains X is $W = C$. First notice that C obviously contains X, and C is a variety since it's $\mathbb{V}(y - x^2, z - x^3)$. We'll be done once we show that any variety V that contains X also has to contain C.

So let $V = \mathbb{V}(f_1, \ldots, f_s)$ be a variety containing X, where $f_i \in \mathbb{R}[x, y, z]$. This means $f_i(t, t^2, t^3) = 0$ for all $t \in \mathbb{Z}$. But if we plug in $x = t,\ y = t^2,\ z = t^3$ into f_i, we convert f_i into a polynomial in the real variable t that vanishes at all $t \in \mathbb{Z}$. Thus this polynomial in one variable has infinitely many roots, and so it has to be the zero polynomial. This means that $f_i(t, t^2, t^3) = 0$ for all $t \in \mathbb{R}$, so f_i vanishes on all of C. This means that $C \subset \mathbb{V}(f_1, \ldots, f_s) = V$, and we are done.

d) Let
$$X = \{(t, t^2, t^3) \mid 1 \le t \le 10 \quad (t \in \mathbb{Z})\}.$$
Find the smallest affine variety in $\mathbb{R}^3$ that contains X. Carefully explain your answer.

Solution.
A single point (a, b, c) is always an affine variety, since it is $\mathbb{V}(x - a, y - b, z - c)$. We saw in class that any finite union of affine varieties is again an affine variety. Thus X is an affine variety.

Remark. The smallest variety containing a set X is usually called the *Zariski closure* of X. We'll see why when we talk about the Zariski topology for affine space.

6. Assume that $\langle f_1, \ldots, f_s\rangle = \langle g_1, \ldots, g_t\rangle$ for some polynomials $f_1, \ldots, f_s, g_1, \ldots, g_t$.

Prove that $\mathbb{V}(f_1, \ldots, f_s) = \mathbb{V}(g_1, \ldots, g_t)$. [Hint: in class we talked about what it means to say that $\langle f_1, \ldots, f_s\rangle = \langle g_1, \ldots, g_t\rangle$. You can use that.]

Solution.
The fact that $\langle f_1, \ldots, f_s\rangle = \langle g_1, \ldots, g_t\rangle$ means that each f_i is in $\langle g_1, \ldots, g_t\rangle$ and each g_j is in $\langle f_1, \ldots, f_s\rangle$. By symmetry it's enough to prove that $\mathbb{V}(f_1, \ldots, f_s) \subseteq \mathbb{V}(g_1, \ldots, g_t)$; the proof of the reverse inclusion is identical, reversing the roles of the f_i and the g_j.

So let $P \in \mathbb{V}(f_1, \ldots, f_s)$. We want to show that $P \in \mathbb{V}(g_1, \ldots, g_t)$, i.e. we want to show that $g_j(P) = 0$ for all j. But as noted, each g_j is in $\langle f_1, \ldots, f_s\rangle$, so write
$$g_j = \sum_{i=1}^{s} h_i f_i.$$
Then
$$g_j(P) = \sum_{i=1}^{s} h_i(P) \cdot f_i(P).$$
But the latter is zero since $P \in \mathbb{V}(f_1, \ldots, f_s)$, i.e. P is in the common vanishing locus of the f_i.

7. (Continuing problem #3.)

a) Let I be an ideal in $R = k[x_1, \ldots, x_n]$. (We are *not* assuming that I is a radical ideal in the language of problem #3.) Define
$$\sqrt{I} = \{f \in R \mid f^r \in I \text{ for } \textit{some} \text{ integer } r \ge 0\}.$$
Prove that $\sqrt{I}$ is again an ideal. (Note that if $f, g \in \sqrt{I}$ it means that $f^r \in I$ and $g^s \in I$ but not necessarily that $r = s$.)

Solution.
We have to prove three things to establish that $\sqrt{I}$ is an ideal.

- $0 \in \sqrt{I}$ since $0^1 = 0 \in I$ (all ideals contain 0).
- If $f, g \in \sqrt{I}$ then $f + g \in \sqrt{I}$. Indeed, suppose $f^r \in I$ and $g^s \in I$. This also means that any higher power of either f or g is also in I, by the multiplicative property of an ideal. Then consider
$$(f+g)^{r+s} = f^{r+s} + \binom{r+s}{1} f^{r+s-1}g + \cdots + g^{r+s}.$$
Each term in this expansion contains either a power of f that's larger than r or a power of g that's larger than s, since any term $Af^a g^b$ in this expansion must have $a + b = r + s$. For example,
$$(f+g)^4 = f^4 + 4f^3g + 6f^2g^2 + 4fg^3 + g^4;$$
in each term, the sum of the exponents is 4. Clearly we can't have $a < r, b < s$ but $a + b = r + s$. So each term in the expansion is in I, and hence $(f + g)^{r+s} \in I$.
- If $f \in \sqrt{I}$ and $h \in R$ then $hf \in \sqrt{I}$. Indeed, since $f \in \sqrt{I}$ we have $f^r \in I$ for some r. Then $(hf)^r = h^r f^r \in I$, so $hf \in \sqrt{I}$.

b) Prove that $\sqrt{I}$ is a radical ideal in the sense of problem #3.

Solution.
We have to show that if f is a polynomial for which $f^m \in \sqrt{I}$ for some m then f itself must be in $\sqrt{I}$. The condition that $f^m \in \sqrt{I}$ means that for some r, $(f^m)^r \in I$. That is, $f^{rm} \in I$. So we have shown that some power of f is in I. By definition, this means $f \in \sqrt{I}$.

c) Let $I = \langle x^2, y^3 \rangle \subset \mathbb{R}[x, y]$. Show that $\sqrt{I} = \langle x, y \rangle$.

Solution.
We have to show that $\sqrt{I} = \sqrt{\langle x^2, y^3 \rangle} = \langle x, y \rangle$.

First we look at the inclusion $\supseteq$. Notice that $x^2 \in \langle x^2, y^3 \rangle$, so $x \in \sqrt{\langle x^2, y^3 \rangle} = \sqrt{I}$. Similarly $y^3 \in \langle x^2, y^3 \rangle$, so $y \in \sqrt{\langle x^2, y^3 \rangle} = \sqrt{I}$. But we saw in a) that $\sqrt{\langle x^2, y^3 \rangle} = \sqrt{I}$ is an ideal, so any linear combination of x and y is also in $\sqrt{I}$, i.e. we have the desired inclusion $\supseteq$.

So now we have to show $\subseteq$.

Let $f \in \sqrt{\langle x^2, y^3 \rangle}$, so $f^r \in \langle x^2, y^3 \rangle$ for some r. We want to show that $f \in \langle x, y \rangle$. Let's make some observations.

- The statement $f \in \langle x, y \rangle$ that we want to show means exactly that if you write out f, the constant term is 0. Every other term contains either a power of x or a power of y (or both), so every other term is automatically in $\langle x, y \rangle$. But a non-zero constant is not in $\langle x, y \rangle$. **So we want to show that the constant term of f is 0**.
- The condition that $f^r \in \langle x^2, y^3 \rangle$ means that if you write out f^r as a polynomial, every term contains either x to a power ≥ 2 or y to a power ≥ 3 (or both). In particular, f^r has 0 as its constant term.
- If $f = a +$ (terms involving x and y), with a a non-zero constant, then f^r has a^r as a non-zero constant.

These bullets show that if $f^r \in \langle x^2, y^3 \rangle$ then f can't have a non-zero constant term, so $f \in \langle x, y \rangle$ as claimed.