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. Let k be a field and let $R = k[x_1, \dots, x_n]$, the polynomial ring in n variables over k.

   a) Prove that for any positive integer $n \geq 1$, $R = k[x_1, \dots, x_n]$ has the property that if $f, g \in R$ and $f \neq 0, g \neq 0$, then $fg \neq 0$. (Recall that this is the main step in showing that R is an integral domain.) [Hint: In class we showed this for $n = 1$, and you can use this fact without proving it again. Now use induction on n. Notice that we can lump together the terms according to the power of one variable, for example

$$y^2+z^3+xy^5z^4+xy^4+x^2y^3z^4+x^2yz^5+x^2z^7+x^3y^2z = x^0(y^2+z^3)+x(y^5z+y^4)+x^2(y^3z^4+yz^5+z^7)+x^3(y^2z).]$$

Solution:

We know from class that the result is true for $n = 1$, so assume $n > 1$ and use induction.

f and g are non-zero polynomials in n variables, so each of them has at least one non-zero term. Note that there is no guarantee that a non-zero term that you pick for f will have any variables in common with a non-zero term you pick for g. To simplify notation, without loss of generality let x_1 be a variable that exists in at least one term of f. For the sake of this argument, we don't care if g has any terms with x_1 in it, as long as $g \neq 0$.

As in the hint, separate f according to the powers of x_1 in the terms (lump together the terms without x_1, then the terms with exactly x_1^1, then the terms with exactly x_1^2, etc), and similarly separate g according to the powers of x_1 in the terms.

$$\begin{array}{rcl} f & = & H_0 + x_1 H_1 + x_1^2 H_2 + \cdots + x_1^m H_m \\ g & = & K_0 + x_1 K_1 + x_1^2 K_2 + \cdots + x_1^\ell K_\ell \end{array}$$

where $H_i, K_j \in k[x_2, \dots, x_n]$ for all i j (i.e. none of the H_i or the K_j involve x_1 in any way). Our assumptions give that $m \geq 1$ and $\ell \geq 0$, and $H_m \neq 0$, $K_\ell \neq 0$. (If $\ell = 0$ that just means that g has no term with an x_1 in it, but it doesn't mean $K_\ell = 0$.)

Now look at fg:

$$fg = H_0K_0 + \cdots + x_1^{i+j}(H_iK_j + H_jK_i) + \cdots + x_1^{m+\ell} H_m K_\ell.$$

The first thing to note is that no term of $x_1^{m+\ell} H_m K_\ell$ can cancel with any earlier term, by looking at powers of x_1. So it's enough to show that $x_1^{m+\ell} H_m K_\ell \neq 0$. But certainly $x_1^{m+\ell} \neq 0$, and since H_m and K_ℓ are non-zero polynomials in $< n$ variables, namely $x_2, \dots, x_n$, by induction their product is not zero so we are done. $\square$

   b) If $f, g \in R$, prove that $\deg(fg) = \deg(f) + \deg(g)$. (We know it for monomials, but you have to show that things don't get messed up when you use polynomials even though cancelation of terms can occur in a product.) [Hint: collect terms of the same degree together. For example,

$$y^2 + z^2 + xy^5z^4 + xy^4 + x^2y^3z^5 + x^2yz^2 + x^3z^7 + x^3yz$$

$$= (y^2 + z^2) + (xy^4 + x^2yz^2 + x^3yz) + (xy^5z^4 + x^2y^3z^5 + x^3z^7).]$$

Solution:

Assume $\deg(f) = m$ and $\deg(g) = p$. This time we'll decompose f and g in a different way. Let f_i be the sum of all the terms of degree i in f, $0 \le i \le m$ and let g_i be the sum of all the terms of degree i in g, $0 \le i \le p$. So

$$f = f_0 + f_1 + \cdots + f_m \quad \text{and} \quad g = g_0 + g_1 + \cdots + g_p,$$

so

$$fg = f_0g_0 + f_1g_0 + f_0g_1 + \cdots + f_mg_p.$$

Since $\deg(f) = m$ and f_m consists of all the terms of degree m, we get $f_m \neq 0$. Similarly $g_p \neq 0$. In the product, no term can have higher degree than $m + p$ (since m is the highest degree of a term in f and p is the highest degree in g). Also, the terms of degree exactly $m + p$ have to occur in f_mg_p. We just have to show that $f_mg_p \neq 0$ so fg has at least one term of degree $m + p$. But by part a), since $f_m \neq 0$ and $g_p \neq 0$ we have $f_mg_p \neq 0$ and we're done. $\square$

2. In class we proved that if k is an infinite field and $f \in k[x_1, \dots, x_n]$ then the following are equivalent:
   - f is the zero polynomial.
   - The evaluation function $f : k^n \to k$, defined by $f(P) = f(b_1, \dots, b_n)$ for $P = (b_1, \dots, b_n) \in k^n$, is the zero function. (I.e. f, evaluated at any point of k^n, vanishes.)

   Now instead we consider a finite field. Let p be a prime and consider the field $\mathbb{Z}_p$. Give an example of a polynomial $f \in \mathbb{Z}_p[x, y]$ for which $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ vanishes at **all but one** point of $\mathbb{Z}_p^2$. (Specifically, it has to fail to vanish at one and only one point of $\mathbb{Z}_p^2$.) Be sure to prove why your example works – it's not enough to just give the polynomial. [Hint: Fermat's Little Theorem.]

   Solution:

   For our purposes (there are different ways to phrase it), Fermat's theorem says that for all $a \in \mathbb{Z}_p \backslash \{0\}$, $a^{p-1} = 1$. So the roots of the polynomial $x^{p-1} - 1$ in $\mathbb{Z}_p$ are $1, 2, \dots, p - 1$.

   Now let $f(x, y) = (x^{p-1} - 1)(y^{p-1} - 1)$. For any $(a, b) \in \mathbb{Z}_p^2$ we have

   $$f(a, b) = (a^{p-1} - 1)(b^{p-1} - 1).$$

   From what we have said, this is equal to 0 in $\mathbb{Z}_p$ as long as either a or b is not 0. The only point missing is $(0, 0)$, and clearly $f(0, 0) = (0 - 1)(0 - 1) = 1 \neq 0$ so we are done. $\square$

3. If k is an infinite field, prove that the phenomenon in Problem 2 can't happen. That is, prove that if $f \in k[x, y]$ and $f(x, y) = 0$ when evaluated at every point of k^2 except one specific point (a, b) then we must also have $f(a, b) = 0$. (Make sure to indicate the relevance of the assumption that k is infinite.)

   Solution:

   $f(x, b)$ is a polynomial in one variable with infinitely many roots (namely x can be any value other than $x = a$). But the degree of f is finite, so f must be the zero polynomial and so $f(a, b) = 0$ as well. $\square$

4. Let $D \subset \mathbb{R}^3$ be the set of points

   $$D = \{(t^2, t^3, t^5) \mid t \in \mathbb{R}\}.$$

   For instance, the point $(2^2, 2^3, 2^5) = (4, 8, 32) \in \mathbb{R}^3$ is a point of D.

a) Prove that D is an affine variety. Specifically, find polynomials $f_1, \ldots, f_s$ (you get to decide what s is) so that $D = \mathbb{V}(f_1, \ldots, f_s)$. Make sure you prove both inclusions, $\subseteq$ and $\supseteq$.

Solution:

We claim $D = \mathbb{V}(x^3 - y^2, x^5 - z^2, y^5 - z^3)$. First prove $\subseteq$. If $P \in D$ then P has the form (t^2, t^3, t^5) for some t, so

$$\begin{aligned}(x^3 - y^2)(P) &= t^6 - t^6 = 0\\(x^5 - z^2)(P) &= t^{10} - t^{10} = 0\\(y^5 - z^3)(P) &= t^{15} - t^{15} = 0\end{aligned}$$

so $\subseteq$ holds.

Now prove $\supseteq$. Let $P \in \mathbb{V}(x^3 - y^2, x^5 - z^2, y^5 - z^3)$ and say $P = (a, b, c)$. If $P = (0, 0, 0)$ then clearly P is on D (take $t = 0$), so assume $a \neq 0$. If $a < 0$ then since $x^3 - y^2$ vanishes on P we get $b^2 = a^3$; but a^3 is also negative so this is impossible. So we can assume $a > 0$.

Let t be a real number satisfying

$$t^2 = a$$

(so t is either the positive or the negative square root of a). Since $(x^3 - y^2)(a, b, c) = 0$ we have

$$b^2 = a^3 = t^6 \quad \text{so} \quad b \quad \text{is either} \quad t^3 \quad \text{or} \quad -t^3.$$

Similarly, we get

$$c^2 = a^5 = t^{10} \quad \text{so} \quad c \quad \text{is either} \quad t^5 \quad \text{or} \quad -t^5.$$

So far we have shown that one of the following holds:

$$\begin{gathered}(a, b, c) = (t^2, t^3, t^5)\\(a, b, c) = (t^2, t^3, -t^5)\\(a, b, c) = (t^2, -t^3, t^5)\\(a, b, c) = (t^2, -t^3, -t^5).\end{gathered}$$

But we also know that $(y^5 - z^3)(a, b, c) = 0$ so $b^5 = c^3$. This means that b and c are either both positive or both negative. This rules out the second and third of these possibilities, so

$$(a, b, c) \quad \text{is either} \quad (t^2, t^3, t^5) \quad \text{or} \quad (t^2, -t^3, -t^5) = ((-t)^2, (-t)^3, (-t)^5).$$

Either way, $(a, b, c) \in D$ and we are done. $\square$

b) If $f \in \mathbb{R}[x, y, z]$ and $D \not\subset \mathbb{V}(f)$ (i.e. f does not vanish on all of D), show that $\mathbb{V}(f) \cap D$ consists of at most $5 \cdot \deg(f)$ points.

Solution:

D consists of all the points in $\mathbb{C}^3$ of the form (t, t^3, t^5) for some $t \in \mathbb{C}$. So $D \cap \mathbb{V}(f)$ consists of all points of the form (t, t^3, t^5) on which f vanishes, i.e. we're looking for all values of t for which $f(t, t^3, t^5) = 0$. Since f does not vanish on all of D by assumption, there are values of t for which this equation does not hold, so now thinking of t as a variable, $f(t, t^3, t^5)$ is a non-zero polynomial, and its degree is $5 \cdot \deg(f)$. But the points of $\mathbb{V}(f) \cap D$ correspond to the roots of $f(t, t^3, t^5)$, and the number of roots of a polynomial in one variable is at most the degree of the polynomial. $\square$

c) Let $\phi : \mathbb{R} \to \mathbb{R}^3$ be the function defined by $\phi(t) = (t^2, t^3, t^5)$. Prove that ϕ is one-to-one.

Solution:

Assume $\phi(s) = \phi(t)$. We want to show that necessarily $s = t$. But our assumption says that $(s^2, s^3, s^5) = (t^2, t^3, t^5)$. But in particular we have $s^3 = t^3$, and this forces $s = t$. $\square$

d) We first make the following definition:

> For any field k, if W is a set in k^n and V is a variety in k^n, we say that W is a *subvariety* of V if $W \subseteq V$ and W is itself a variety in k^n. We say that W is a *proper* subvariety of V if, in addition, $W \subsetneq V$.

In the context of the current problem, prove that a set W is a proper subvariety of D (the variety defined in a)) if and only if W consists of a finite set of points on D. You can use anything we talk about in class in your answer. (The implication $\Leftarrow$ should only take a line or two but $\Rightarrow$ will take a little more work.)

Solution:

Let's prove $\Leftarrow$ first. Assume W is a finite set of points on D. By assumption W is a subset of D, and since W is a finite set of points, we said in class that W is a variety in $\mathbb{R}^3$. So by definition, W is a subvariety of D.

Now let's prove $\Rightarrow$. Assume that W is a subvariety of D but not equal to D. This means that there exist polynomials $f_1, \ldots, f_s \in \mathbb{R}[x, y, z]$ such that $W = \mathbb{V}(f_1, \ldots, f_s)$. In particular, not all of the f_i can vanish on all of D. Let f be such a polynomial (we suppress the subscript). Then we are in the situation of part b), so $\mathbb{V}(f) \cap D$ is a finite set. But

$$W = \mathbb{V}(f_1, \ldots, f_s) \subset \mathbb{V}(f)$$

and $W \subset D$ by hypothesis, so $W \subset D \cap \mathbb{V}(f)$. Since $D \cap \mathbb{V}(f)$ is a finite set, W must be finite as well. $\square$

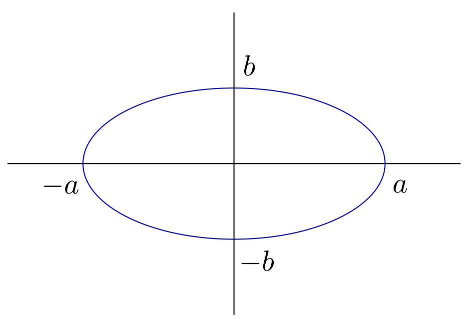
5. Let a and b be positive real numbers and let

$$V = \mathbb{V}(b^2x^2 + a^2y^2 - a^2b^2).$$

Notice that V is the solution set of the equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

so V is an ellipse. (I'm not asking you to prove this; I'm just pointing out the fact.)

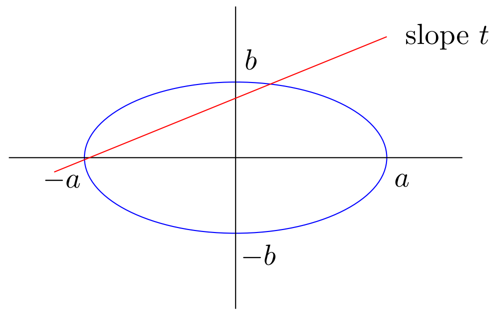


a) Mimicking what we did in class, find a rational parametrization of V. [Hint: try setting t to be the slope of a line through the point $(-a, 0)$ as we did in class.]

b) Check your answer by plugging in two specific choices of t to see if you get a point of V both times.

Solution:

a) We'll look at lines through the point $(-a, 0)$ and having slope t.



First we need to find the equation of this line, which is

$$y - 0 = t(x+a) \quad \text{or} \quad y = t(x+a).$$

This line meets the ellipse in two points, one of which is $(-a, 0)$. We have to find the second point. So we have the equations

$$\begin{aligned} b^2x^2 + a^2y^2 - a^2b^2 &= 0 \\ y &= t(x+a) \end{aligned}$$

Substituting the second into the first, we get

$$b^2x^2 + a^2t^2(x+a)^2 - a^2b^2 = 0.$$

Thus

$$b^2(x^2 - a^2) + a^2t^2(x+a)^2 = 0,$$

i.e.

$$b^2(x+a)(x-a) + a^2t^2(x+a)^2 = 0.$$

Factoring out $(x+a)$ we get

$$(x+a)\left[b^2(x-a) + a^2t^2(x+a)\right] = 0.$$

The factor on the left corresponds to the point $(-a, 0)$, so we focus on the factor on the right. Multiplying it out and setting it equal to zero we have

$$b^2x - b^2a + a^2t^2x + a^3t^2 = 0, \quad \text{or} \quad x(b^2 + a^2t^2) = b^2a - a^3t^2.$$

Thus

$$x = \frac{a(b^2 - a^2t^2)}{b^2 + a^2t^2}.$$

Then

$$y = t(x+a) = t\left[a \cdot \frac{b^2 - a^2t^2}{b^2 + a^2t^2} + a\right] = at\left[\frac{b^2 - a^2t^2}{b^2 + a^2t^2} + 1\right] = \frac{2ab^2t}{a^2t^2 + b^2}.$$

b) Let's try the slopes $t = 0$ and $t = \frac{b}{a}$. First let's see what we predict will happen. When $t = 0$, the line with slope 0 is the x-axis, and we predict that the second point will be the point $(a, 0)$, i.e. $x = a$, $y = 0$. When $t = \frac{b}{a}$ this corresponds to the line joining $(-a, 0)$ and $(0, b)$, so we predict we'll get $x = 0$, $y = b$.

Let's confirm that our predictions hold. When $t = 0$ our parametrization gives

$$x = \frac{a(b^2)}{b^2} = a \quad \text{and} \quad y = 0$$

as predicted.

When $t = \frac{b}{a}$ our parametrization gives

$$x = \frac{a(b^2 - a^2 \cdot \frac{b^2}{a^2})}{b^2 + a^2 \cdot \frac{b^2}{a^2}} = \frac{a(0)}{2b^2} = 0 \quad \text{and} \quad y = a \cdot \frac{b}{a}\left[\frac{b^2 - a^2 \cdot \frac{b^2}{a^2}}{b^2 + a^2 \cdot \frac{b^2}{a^2}} + 1\right] = b(0+1) = b$$

as predicted.