Math 176 F18: Week 1

Due: Sept. 10, 2018

Nunez, Joseph, jbnunez@hmc.edu

1. **4.1.3** Find a set of polynomials $\{P_1, \ldots, P_n\}$, all of whose coefficients are real numbers, whose common zero set is the given set.

   (a) $\{(3, y) : y \in \mathbb{R}\}$ in $\mathbb{R}^2$
   $P = \{nx - 3n : n \in \mathbb{R}\}$

   (b) $\{(1, 2)\}$ in $\mathbb{R}^2$
   $P = \{(mx - m), (ny - 2n) : m, n \in \mathbb{R}\}$

   (c) $\{(1, 2), (0, 5)\}$ in $\mathbb{R}^2$
   $P = \{(a(x-1)^2 + b(y-2)^2)(cx^2 + d(y-5)^2) : a, b, c, d \in \mathbb{R}\}$

   (d) Generalize the method from part (c) to any finite set of points in $\mathbb{R}^2$.
   For any point $(a, b) \in \mathbb{R}^2$, multiply the polynomial in the expression by $(m(x-a)^2 + n(y-b)^2)$, where $m, n \in \mathbb{R}^2$

2. **4.1.5**

   (a) Is every finite subset of $\mathbb{C}^2$ the zero set of a collection of polynomials in $\mathbb{C}[x, y]$? Prove or find a counterexample.
   Consider a point $(a + bi, c + di) \in \mathbb{C}^2$. Polynomials of the form $(mx - m(a+bi))^2 + (ny - n(c+di))^2$ where $m, n \neq 0 \in \mathbb{C}$ have this as their zero set. Note that since $\mathbb{C}$ has no zero divisors (a consequence of the property that the magnitude of a product is the product of the magnitudes), the polynomial can only be zero only at the point $(a + bi, c + di) \in \mathbb{C}^2$. Thus for any finite set of points in $\mathbb{C}^2$, we can multiply together polynomials of this form for each point in the set, and the resulting polynomial (and all others of that form up to coefficients) will have the desired finite subset as its zero set.

   (b) Is there an infinite subset of $\mathbb{C}^2$ that is the common zero set of a finite collection of polynomials in $\mathbb{C}[x, y]$?
   Yes. Simply define a polynomial with existing zeros in terms of x but which does not depend upon y, or vice versa. For example, $P = x$. This has the infinite zero set $\{(0, y) : y \in \mathbb{C}\} \subset \mathbb{C}^2$.

   (c) Find an infinite set of points in $\mathbb{C}$ that is not the common zero set of a finite collection of polynomials in $\mathbb{C}[x]$.

Consider $\mathbb{R}$. Suppose, to obtain a contradiction, that $\mathbb{R}$ is the zero set of some set of polynomials P. For this to be the case, each element of P must send all real numbers to zero and some numbers with an imaginary component to a nonzero number. However, the only way for a single polynomial to send all reals to zero is to multiply that real by zero. Therefore, all elements of P multiply x by a factor of zero. Then elements with a complex component are also in the zero set. This is a contradiction, hence $\mathbb{R}$ is not the common zero set of any finite collection of polynomials.

(d) Is there any infinite set of points in $\mathbb{C}$, besides $\mathbb{C}$ itself, that is the common zero set of a finite collection of polynomials in $\mathbb{C}[x]$?

No. With the exception of $P = 0$, there are no polynomials in $\mathbb{C}[x]$ with infinite zero sets. Polynomials are generally of the form $(x-a_1)(x-a_2)\cdots(x-a_n)$. Since $\mathbb{C}$ does not have zero divisors, such a polynomial can only be zero if $x = a_i$ for some i. Thus the number of zeroes is bounded by the degree of the polynomial, and since all polynomials have finite degree, all polynomials have finite zeros. (This argument gets reversed if we count infinite-degree polynomials, but the polynomial ring definition does not include infinite degrees.)

3. **4.1.6** Find the zero set of each polynomial in $\mathbb{A}^1(\mathbb{Z}_3)$.

(a) $x^2 + 2$

The zero set is $\{1, 2\}$ since $1^2 + 2 = 3 \equiv_3 0$ and $2^2 + 2 = 6 \equiv_3 0$, while $0^2 + 2 = 2 \equiv_3 2$.

(b) $x^2 - 2$

The zero set is $\emptyset$ since $1^2 - 2 = -1 \equiv_3 2$, $2^2 - 2 = 4 \equiv_3 1$, and $0^2 - 2 = -2 \equiv_3 1$.

4. **4.1.8**

(a) Show that if k is an infinite field, and $P \in k[x_1, \ldots, x_n]$ is a polynomial whose zero set is $\mathbb{A}^n(k)$, then $P = 0$. [Hint: Use induction on n]

Base case: $n = 1$. Since P has all of $\mathbb{A}^1(k)$ as its zero set, it must send 0 to 0, so it can have no zero order term. P must have some finite order m. Then P can have no more than m unique zeroes if $P \neq 0$. Therefore P must be zero. The base case holds.

Inductive Hypothesis: Assume that if k is an infinite field, and if $P \in k[x_1, \ldots, x_n]$ is a polynomial whose zero set is $\mathbb{A}^n(k)$, then $P = 0$ for n.

Inductive Step: Consider a polynomial $P \in k[x_1, \ldots, x_n, x_{n+1}]$. Let $P = P_1 + P_2$, where $P_1 \in k[x_{n+1}]$ and $P_2 \in k[x_1, \ldots, x_n]$. Since the first n indices must always be sent to 0, $P_2 = 0$ by the inductive hypothesis. By the same logic as in the base case, P_1 must also be 0. Thus $P = 0$

By the principle of mathematical induction, if k is an infinite field, and $P \in k[x_1, \ldots, x_n]$ is a polynomial whose zero set is $\mathbb{A}^n(k)$, then $P = 0$.

(b) Is there any finite field for which this result holds?

No, since for any finite field, say with order n, it is possible to construct an n-degree polynomial with those n elements as its zeros. For example, if the field $k = \{a_1, a_2, \ldots, a_n\}$. Then the polynomial $P = (x - a_1)(x - a_2) \cdots (x - a_n)$ has all of k as its zero set. This can be generalized for any finite field k.

5. **4.2.1** Sketch the algebraic sets

(a) $V(x^3 - 1)$ in $\mathbb{A}^1(\mathbb{C})$

(b) $V(x^3 - 1)$ in $\mathbb{A}^1(\mathbb{C})$

(c) $V((y - x^2)(y^2 - x))$ in $\mathbb{A}^2(\mathbb{R})$

(d) $V(y - x^2, y^2 - x)$ in $\mathbb{A}^2(\mathbb{R})$

(e) $V(y^2 - x^3 + x)$ in $\mathbb{A}^2(\mathbb{R})$

(f) $V(x - 2y + 3z)$ in $\mathbb{A}^3(\mathbb{R})$

(g) $V(z - 3, z - x^2 - y^2)$ in $\mathbb{A}^3(\mathbb{R})$

(h) $V(xy - z^2y) = V(y(x - z^2))$ in $\mathbb{A}^3(\mathbb{R})$

(i) $V(y - x + x^2)$ in $\mathbb{A}^2(\mathbb{Z}_3)$

6. **4.2.2** Algebraic Sets in $\mathbb{R}^n$ and $\mathbb{C}^n$:

   (a) Show that for any $a \in \mathbb{R}$ the singleton $\{a\}$ is an algebraic set.
   $\{a\}$ is the algebraic set of $P = x - a$.

   (b) Show that any finite collection of numbers in $\{a_1, \ldots, a_k\}$ in $\mathbb{R}$ is an algebraic set.
   $\{a_1, \ldots, a_k\}$ is the algebraic set of $P = (x - a_1)(x - a_2) \cdots (x - a_n)$.

   (c) Show that the set $\{(-1/\sqrt{2}, 1/\sqrt{2}), (1/\sqrt{2}, -1/\sqrt{2})\} \subset \mathbb{R}^2$ is an algebraic set.
   Consider the polynomials $P = \{x^2+y^2-1, y-x\}$. The zero set of the first polynomial is the unit circle, and the zero set of the second polynomial is the line $y = x$. These intersect at the above points.

   (d) Show that a circle in $\mathbb{R}^2$ is an algebraic set.
   Consider $P = (x-a)^2 + (y-b)^2 - r^2$. This polynomial has a zero set that is a circle with radius r centered at any point $(a, b) \in \mathbb{R}^2$.

(e) Show that any line in $\mathbb{R}^3$ is an algebraic set.

Consider an arbitrary plane in $\mathbb{R}^3$ defined by $z = ax + by + c$. This plane is then the zero set of the polynomial $P = ax + by + c - z$. Thus we can define any plane in $\mathbb{R}^3$ as a zero set. A line in R^3 may be defined by the intersection of two planes. Thus we may get a line in $\mathbb{R}^3$ as an algebraic set by choosing two polynomials which define planes that intersect at the desired line. In particular, express this as setting two planes' normal forms equal to each other, as in

$$a_1x + b_1y + c_1z - d_1 = a_2x + b_2y + c_2z - d_2,$$

then move the two all to one side to get the polynomial.

(f) Show that the positive numbers are not an algebraic set in $\mathbb{R}$. (Class)

Suppose, to obtain a contradiction, that they are an algebraic set. Then $\exists \mathcal{P}$ s.t. $V(\mathcal{P}) = \mathbb{R}^{>0}$. Every polynomial in $\mathcal{P}$ must have a root $\forall \mathbb{R} > 0$. However, for every root z in a polynomial, we can pull out a factor of $(x-z)$ from our polynomial, and we can do this infinite times, so our polynomial has infinite degree, which contradicts the definition of a polynomial.

(g) Show that the region inside the unit circle $|z| < 1$ in $\mathbb{C}$ is not an algebraic set. (Class)

Suppose, to obtain a contradiction, that they are an algebraic set. Then $\exists \mathcal{P}$ s.t. $V(\mathcal{P})$ is the unit circle. Every polynomial in $\mathcal{P}$ must have a root $\forall z \in |C|$ s.t. $|z| < 1$. However, for every root z in a polynomial, we can pull out a factor of $(x-z)$ from our polynomial, and we can do this infinite times since the unit circle contains infinite points, so our polynomial has infinite degree, which contradicts the definition of a polynomial.

(h) Give an example of a nonconstant polynomial P in $\mathbb{R}[x, y]$ such that the algebraic set $X = \{(x, y) \in \mathbb{R}^2 : P(x, y) = 0\}$ is the empty set.

Consider the polynomial $P = x^2 + y^2 + 1$. Since x^2 and y^2 are always non-negative for real numbers, the polynomial is never zero, hence its algebraic set is the empty set.

(i) Is there a nonconstant polynomial P in $\mathbb{C}[x, y]$ such that the algebraic set $X = \{(x, y) \in \mathbb{C}^2 | P(x, y) = 0\}$ is the empty set? Explain why or why not.

No. The fundamental theorem of algebra states that polynomials have existing roots, so any nonconstant polynomial must have zeros.

(j) Suppose $X_1 = \{(x, y) \in \mathbb{C}^2 | x + y = 0\}$ and $X_2 = \{(x, y) \in \mathbb{C}^2 | x - y = 0\}$. Find a polynomial $Q \in \mathbb{C}[x, y]$ such that $X_1 \cup X_2 = \{(x, y) \in \mathbb{C}^2 | Q(x, y) = 0\}$.

The algebraic set of X_1 is all points for which $x = -y$ and the algebraic set of X_2 is all points for which $x = y$. The intersection of these sets is $\{(0,0)\}$. Thus we need the algebraic set of Q to be $\{(0,0)\}$.

(k) Suppose $X_1 = \{(x_1, \ldots, x_n) \in \mathbb{C}^n | P_1(x_1, \ldots, x_n) = 0\}$ and $X_2 = \{(x_1, \ldots, x_n) \in \mathbb{C}^n | P_2(x_1, \ldots, x_n) = 0\}$. Give a single polynomial Q such that $X_1 \cup X_2 = \{(x_1, \ldots, x_n) \in \mathbb{C}^n | Q(x_1, \ldots, x_n) = 0\}$.

7. **4.2.5** Show that both the empty set and $\mathbb{A}^n(k)$ are algebraic sets in $\mathbb{A}^n(k)$.

Consider the polynomial $P = 1$, where 1 denotes the multiplicative identity in k. Then this polynomial has no zeros, so its zero set is the empty set. Therefore the empty set is an algebraic set. Consider the polynomial $P = 0$. Then this polynomial is zero everywhere, so its zero set is all of $\mathbb{A}^n(k)$. Therefore the $\mathbb{A}^n(k)$ is an algebraic set.

8. **4.2.7** Let $f(x, y), g(x, y) \in \mathbb{C}[x, y]$. Show that $V(f, g) = V(f-g, f+g)$. (Class)

   Let $(x_0, y_0) \in V(f, g)$. Then $f(x_{,0}, y_0) = 0$ and $g(x_{,0}, y_0) = 0$. Therefore $f - g = 0 - 0 = 0$ and $f + g = 0 + 0 = 0$. Therefore $V(f - g, f + g) \subseteq V(f, g)$.

   Let $(x_0, y_0) \in V(f - g, f + g)$. Then $f(x_{,0}, y_0) - g(x_{,0}, y_0) = 0$ and $f(x_{,0}, y_0) + g(x_{,0}, y_0) = 0$. Therefore $(f - g) + (f + g) = 2f = 0$, so $f = 0$, and $(f - g) - (f + g) = -2g = 0$, so $g = 0$. Therefore $V(f, g) \subseteq V(f - g, f + g)$.

   By dual containment, $V(f, g) = V(f - g, f + g)$.

9. **4.2.9** Let I be the ideal in $k[x_1, \ldots x_n]$ generated by a set $S \subset k[x_1, \ldots, x_n]$. Show that $V(S) = V(I)$. Thus every algebraic set is defined by an ideal. (Class)

   Pick $x \in V(I)$. For $P \in I$, we have $P(x) = 0$. For $P \in S$, since $S \subset I$, $P \in I$, hence $P(x) = 0$. Thus $V(I) \subseteq V(S)$

   Pick $x \in V(S)$. For $P \in S$, $P(x) = 0$. Given $Q \in I$, $Q = R_1P_1 + R_2P_2 + \cdots + R_mP_m$. Then, since all P_i are in S, they all go to zero, so all of the terms go to zero, so $Q(x) = 0$. Thus $V(S) \subseteq V(I)$.

   By dual containment, $V(S) = V(I)$.

10. **4.2.12**

    (a) Show that an arbitrary intersection of algebraic sets is an algebraic set.

    Let $\{V(S_i)\}_{i \in I} = U$ be a family of algebraic sets indexed by I. Consider $x \in V(U)$. For all $P \in U$, we have $P(x) = 0$, thus, since each $S_i \subseteq U$, $Q(x) = 0$. Therefore $x \in V(S_i)$ for each $i \in I$, which implies $x \in bigcap_{i \in I} V(S_i)$, therefore $V(U) \subseteq bigcap_{i \in I} V(S_i)$. Thus $V(\bigcup_{i \in I} S_i = \bigcap_{i \in I} V(S_i)$

    (b) Show that a finite union of algebraic sets is an algebraic set.

    Let A and B be sets of polynomials. Define $AB = \{pq : p \in A, q \in B\}$. Take $x \in V(A) \cup V(B)$, $x \in V(A) \cup V(B) \implies \forall p \in A, p(x) = 0$, $or \forall q \in B, q(x) = 0$. For all $pq \in AB$, we have $pq(x) = p(x)q(x) = 0q(x)$ or $p(x)0 = 0 \implies x \in V(AB)$, hence $V(A) \cup V(B) \subseteq V(AB)$.

Let $x \in V(AB)$. Then $\forall pq \in AB$, we have $p(x)q(x) = 0$. Then for all pq, either $p(x) = 0$ or $q(x) = 0$. If the former, then $x \in V(A)$, and if the latter, then $x \in V(B)$. Therefore, $x \in V(A) \cup V(B)$. Thus $V(AB) \subseteq V(A) \cup V(B)$.

By dual containment, $V(AB) = V(A) \cup V(B)$.

11. **4.2.14** Let X be a set of points in $\mathbb{A}^n(\mathbb{C})$. (Class)

    (a) Show that $X \subseteq V(I(X))$.

    Let $x \in X$. Take $p \in I(X)$. Then $p(x) = 0$ by construction of $I(X)$. Then $x \in V(I(X))$. Then $X \subseteq V(I(X))$.

    (b) Find a set X with $X \neq V(I(X))$.

    Omitted.

    (c) Show that if X is an algebraic set, then $X = V(I(X))$

    Since X is algebraic, $X = V(S)$ for some set of polynomials S. Let $b \in V(I(X))$. Then for all $P \in I(X)$, $P(b) = 0$. Take $q \in S$. Since $S \subseteq I(X)$, $q \in I(X)$. Then $q(b) = 0$. Thus $b \in X = V(S)$.

    Alternate proof: Since X is algebraic, there exists a set of polynomials which vanish exactly on those points. Since the ideal $I(X)$ is the smallest set of polynomials which vanish on the points of X, $I(X)$ vanishes on only X since X is the smallest algebraic set containing X.

12. **4.2.21** Let X and W be algebraic sets in $\mathbb{A}^n(k)$. Show that $X \subset W$ if and only if $I(X) \supset I(W)$. Conclude that $X = W$ if and only if $I(X) = I(W)$. (Class)

Forwards: $X \subset W$. Pick $f \in I(W), f(w) = 0 \forall w \in W$. $\forall x \in X \subset W, f(x) = 0 \implies f \in I(X) \implies I(W) \subset I(X)$.

Reverse: $I(W) \subset I(X)$. Pick $x \in X, \forall f \in I(W) \subset I(X), f(x) = 0$. $x \in V(I(W)) = W$, hence $X \subset W$