Geometry, Algebra, and Algorithms

October 24, 2016

1 Polynomials and Affine spaces

Polynomials are central to algebraic geometry, and can be defined over any field. Recall that a field is a set over which we can define some notion of addition, subtraction, multiplication, and division.
Formally, a field is an Abelian group with respect to two binary operators that obey a distributive law, and with distinct additive and multiplicative identities.
We can now define polynomials, which link algebra and geometry

(Definition) Monomial: *A* ***monomial*** *in indeterminates* $x_1, \cdots, x_n$ *is a product of the form*

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n}, \alpha_i \in \mathbb{Z}^+, 1 \leq i \leq n$$

The ***degree*** *of a monomial is the non-negative integer* $\alpha_1 + \cdots + \alpha_n$
- *Notation*: When $\alpha = (\alpha_1, \cdots, \alpha_n)$ we will write $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ and $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

(Definition) Polynomial: *A* ***polynomial*** f *over field* F *in* $x_1, \cdots, x_n$ *is a finite linear combination of monomials*:

$$f = \sum_\alpha a_\alpha x^\alpha, a_\alpha \in F$$

where the sum is over a finite number of n*-tuples.*
- The set of polynomials over F is denoted $F[x_1, \cdots, x_n]$.
- *Notation*: For small n, e.g. 2 or 3, we use x, y, z instead of x_1, x_2, x_3.
- **(Definition) Coefficient**: a_α *is the* ***coefficient*** *of the monomial* x^α.
- **(Definition) Term**: $a_\alpha x^\alpha$ *is a* ***term*** *of* f *if* $a_\alpha \neq 0$.
- **(Definition) Degree**: *The* ***degree*** *of* f *is the maximum degree of the terms of* f.

Polynomials are closely related to affine spaces, since if we view a polynomials $f \in F[x_1, \cdots, x_n]$ as a function $f : F^n \to F$ we can link geometry and algebra; such a function is given by mapping $(p_1, \cdots, p_n) \in F^n$ to

$$\sum_\alpha a_\alpha \cdot (p_1^{\alpha_1} \cdots p_n^{\alpha_n}) \in F$$

The ability to view polynomials as both functions and mathematical objects in their own right gives rise to some ambiguity. For example, it is not always the case that

$$f(p_1, \cdots, p_n) = 0, \forall (p_1, \cdots, p_n) \in F^n \iff f \text{ is the zero polynomial}$$

To see this, consider $F = \mathbb{Z}_2$. This leads to more problems, but if the field is infinite, polynomials do behave as expected.

(Theorem) Uniqueness of zero polynomial: *Let* F *be an infinite field. Then for* $f \in F[x_1, \cdots, x_n]$

$$f(p_1, \cdots, p_n) = 0, \forall (p_1, \cdots, p_n) \in F^n \text{ if and only if } f : F^n \to F \text{ is the zero function}$$

- *Proof*: One direction of the theorem is trivial; if $f : F^n \to F$ is the zero function, the by definition $f(p_1, \cdots, p_n) = 0$.

To prove the other direction, suppose that $\forall (p_1, \cdots, p_n) \in F^n : f(p_1, \cdots, p_n) = 0$. We will use proof by induction on n to show that f is the zero function.
Base case: $n = 1$. A polynomial of degree d has at most d distinct zeros; F is infinite, so f has more than d zeros. Therefore, f must be the zero function.
Now suppose, as the inductive hypothesis, that the theorem is true for the $(n-1)$-dimensional affine space F^n. If we have

$$f = \sum_\alpha a_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

then we can define

$$g_i(x_1, \cdots, x_{n-1}) := \sum_{\alpha'} a_{\alpha'} x_1^{\alpha'_1} \cdots x_{n-1}^{\alpha'_{n-1}} \text{ where } \alpha'_n = i$$

so that we have

$$f = \sum_{i=1}^{N} g_i(x_1, \cdots, x_{n-1}) x_n^i$$

We'll show that g_i must be the zero function, which forces f to be the zero function. To see this, first fix $(a_1, \cdots, a_{n-1} \in F^{n-1}$, so that $f(a_1, \cdots, a_{n-1}, x_n) \in F[x_n]$, which, by the base case, must be the zero function. The coefficients of $f(a_1, \cdots, a_{n-1}, x_n)$ are $g_i(a_1, \cdots, a_{n-1})$, which must all by zero; thus, since our choice of $(a_1, \cdots, a_{n-1}$ was arbitrary, g_i is the zero function, which proves the theorem. □ • Note that it follows as a corollary that two polynomials over an infinite field are equal precisely when they give the same function over an affine space.

2 Affine Varieties

In this section, we define the basic geometries studied in algebraic geometry.

(Definition) Affine variety: *Let F be a field and $f_1, \cdots, f_m \in F[x_1, \cdots, x_n]$. Then the **affine variety** defined by $f_1, \cdots, f_m$ is given by*

$$\mathbf{V}(f_1, \cdots, f_m) := \{(a_1, \cdots, a_n) \in F^n \text{ s.t. } f_i(a_1, \cdots, a_n) = 0, 1 \leq i \leq m\}$$

• *Motivation*: An affine variety $\mathbf{V}(f_1, \cdots, f_m) \subset F^n$ is the set of all solutions of the system of equations $f_1(x_1, \cdots, x_n) = \cdots = f_m(x_1, \cdots, x_n) = 0$. • *Examples*: Conic sections are all affine varieties. For instance circles centered at (h, k) with radius r can be seen as the affine variety of $\mathbf{V}\left((x-h)^2 + (y-k)^2 - r^2\right)$ over $\mathbb{R}$. All polynomials are trivially affine varieties, as well as rational functions.

We now discuss some basic properties of affine varieties. **(Theorem) Closure of affine varieties under union and intersection**: *If $V, W \in F^n$ are affine varieties, so are $V \cup W$ and $V \cap W$.*
• *Proof*: Let $V = \mathbf{V}(f_1, \cdots, f_s), W = \mathbf{V}(g_1, \cdots, g_t)$. We'll prove the stronger statements

$$V \cap W = \mathbf{V}(f_1, \cdots, f_s, g_1, \cdots, g_t)$$
$$V \cup W = \mathbf{V}(f_i g_j \text{ for } 1 \leq i \leq s, 1 \leq j \leq t)$$

The first equality is trivial - if V is the set of points for which f_i is zero and W is the set of points where g_j is zero, then points that are in both are points where both f_i and g_j are zero, for $1 \leq i \leq s, 1 \leq j \leq t$. The second equality follows from the fact that if f_i vanishes at a point, then so does $f_i g_j$, and since the same holds true for points at which g_j vanishes, points in V or W are in $V \cup W := \mathbf{V}(f_i g_j)$. □

3 Parameterizations of Affine Varieties

In this section we discuss how to analytically describe affine varieties. This means enumerating solutions if there are finitely many, but if there are infinitely many, describing them if more difficult. This leads us to the idea of parameterizing affine varieties, which is to say, analytically describing, usually in elementary terms, points in an affine variety.

(Definition) Rational parametric representation: *A **rational parametric representation** of an affine variety $V = \mathbf{V}(f_1, \cdots, f_s)$ is a set of rational functions $r_1, \cdots, r_n$ such that*

$$\{r_i(t_1, \cdots, t_m), 1 \leq i \leq n\} \subset V, \text{ for any } (t_1, \cdots, t_m) \in F^m$$

*Note that the parameterization doesn't have to comprehensively span all of V, but rather simply be contained in it. If all the rational functions above are polynomials, we call it a **polynomial parametric representation**.*

• Not every affine variety has any rational parametric representation (in fact, most don't), and we call those that do **unirational**. Conversely, given a rational parametric representation of an affine variety, we can always find the implicit definition of the affine variety. This can usually be done by back-substituting the variables of parameters from one rational function into another, until the parameter is completely eliminated and a set of polynomials remains. This is known as *elimination theory.*

4 Ideals

Affine varieties, and other concepts in algebraic geometry, are intimately related to ideals, a central algebraic object.

(Definition) Ideal: *A subset $I \in F[x_1, \cdots, x_n]$ is an **ideal** if it satisfies*

1. *Containment of identity*: $0 \in I$
2. *Additive closure*: $f, g \in I \to f + g \in I$
3. *Multiplicative closure*: $f \in I \to \forall h \in F[x_1, \cdots, x_n] : hf \in I$

• *Motivation*: Ring theory has a lot to say about ideals, but the basic idea is that ideals are special subsets of rings that generalize certain properties of special subsets of the integers. The defining properties of an ideal are closure and absorption property, the idea that scalar multiplication should preserve the central properties. Ideals can be used to built quotient rings, the same way normal subgroups can be used to create quotient groups. A more precise motivation comes from the idea that if we have a subset S of ring R, we might be interested in building another ring R' in which the elements of S "act" like zero (consider, for example, $R = \mathbb{Z}, S = 4x, x \in \mathbb{Z}$, which yields the familiar ring of integers modulo 4), or are in some sense negligible. The idea of behaving like zero can be formalized by the properties that if s_1, s_2 behave like zero, then clearly we must have $s_1 + s_2$ behave like zero, as well as rs_1 or $s_1 r$ for any $r \in R$. The ideal generated by S is precisely this ring of elements from R that become negligible (i.e. behave like zero) if we force elements of S to be negligible. In many ways, ideals appear as a natural generalization of modular arithmetic.
Ideals are useful in algebraic geometry because they provide a language for computation with affine varieties, for reasons that will become clear. We begin this section by defining several useful special ideals.

(Definition) Ideal generated by polynomials: *For $f_1, \cdots, f_s \in F[x_1, \cdots, x_n]$, define*

$$\langle f_1, \cdots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i f_i \text{ where } h_1, \cdots, h_s \in F[x_1, \cdots, x_n] \right\}$$

*to be the **ideal generated by** $f_1, \cdots, f_s$.*

• *Proof that $\langle f_1, \cdots, f_s \rangle$ is an ideal*: The first condition, containment of zero, of an ideal is trivially satisfied if we set every h_i to be the zero function. Next, given

$$f = \sum_{i=1}^{s} p_i f_i, g = \sum_{i=1}^{s} q_i f_i$$

it follows that

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i, hf = \sum_{i=1}^{s} (hp_i) f_i$$

which proves the second and third conditions. □

• It turns out that $\mathbf{V}(\langle f_1, \cdots, f_s \rangle)$ contains $V(f_1, \cdots f_s)$, since from the equations

$$\begin{gathered} f_1 = 0 \\ \vdots \\ f_s = 0 \end{gathered}$$

it follows that any polynomial linear combination of f_i will also be zero, i.e. $\sum_{i=1}^{s} h_i f_i = 0$ for any $h_i \in F[x_1, \cdots, x_n]$. So, $\langle f_1, \cdots, f_s \rangle$ can be interpreted as the "span" of the equation $f_1 = \cdots = f_s = 0$. We say that ideal I is **finitely generated** if such $f_1, \cdots, f_s$ exist, and that $f_1, \cdots, f_s$ form a **basis** for I. Note that a given ideal may have more than one basis. One may also draw conceptual parallels between ideals as described above and vector subspaces from linear algebra.

(Theorem) Equivalence of affine varieties: *if $f_1, \cdots, f_s$ and $g_1, \cdots, g_t$ are bases of the same ideal in $F[x_1, \cdots, x_n]$, then they describe the same affine variety. Symbolically,*

$$\langle f_1, \cdots, f_s \rangle = \langle g_1, \cdots, g_t \rangle \to \mathbf{V}(f_1, \cdots, f_s) = \mathbf{V}(g_1, \cdots, g_t)$$

• *Proof*: Suppose $x \in \mathbf{V}(f_1, \cdots, f_s)$, so that $f_1(x) = \cdots = f_s(x) = 0$. Then we have

$$f_i(x) = 0 \to h_i(x) f_i(x) = 0 \text{ for any } h_i \in F[x_1, \cdots, x_n]$$

$$\to \forall p \in \langle f_1, \cdots, f_s \rangle : p(x) = 0 \to \forall p \in \langle g_1, \cdots, g_t \rangle : p(x) = 0 \to \sum_{i=1}^{t} h_i(x) g_i(x) = 0 \text{ for any } h_i \in F[x_1, \cdots, x_n]$$

Thus, for suitable choice of h_i, it follows that $g_i(x) = 0$ for $1 \leq i \leq t$, which shows that $\mathbf{V}(f_1, \cdots, f_s) \subseteq \mathbf{V}(g_1, \cdots, g_t)$. The argument symmetrically proves the converse direction as well, and so we have $\mathbf{V}(f_1, \cdots, f_s) = \mathbf{V}(g_1, \cdots, g_t)$. □
This shows that it's possible to change the basis of an ideal generated by a set of polynomials without affecting the variety of that set of polynomials. This will later form the foundation of the idea that *ideals*, not equations, determine varieties.
The last idea we'll investigate in this section is the following - although $f_i, 1 \leq i \leq s$ vanish over all of $V := \mathbf{V}(f_i)$, and therefore by extension also any polynomial linear combination $\sum_i h_i f_i$, are there other polynomials, besides f_i, that also vanish over V? This question leads to the following definition.

(Definition) Ideal of an affine variety: *Let $V \subset F^n$ by an affine variety. The **ideal of V** is the set*

$$\mathbf{I}(V) := \{f \in F[x_1, \cdots, x_n] \text{ s.t. } \forall (a_1, \cdots, a_n) \in V : f(a_1, \cdots, a_n) = 0\}$$

That is, $\mathbf{I}(V)$ is the set of polynomials that are zero over all of V. Thus, $V \subseteq \mathbf{I}(V)$.

- *Proof that **I**(V) is an ideal:* Obviously $0 \in \mathbf{I}(V)$ since the zero polynomial vanishes over all of F^n. Next, for $f, g \in \mathbf{I}(V)$ and $h \in F[x_1, \cdots, x_n]$, we have

$$\forall (a_1, \cdots, a_n) \in V : f(a_1, \cdots, a_n) = g(a_1, \cdots, a_n) = h(a_1, \cdots, a_n) f(a_1, \cdots, a_n) = 0$$

which proves the second two conditions for $\mathbf{I}(V)$ to be an ideal. □
Although it happens fairly often, it is unfortunately not always the case that $\mathbf{I}(\mathbf{V}(f_i)) = \langle f_i \rangle$. The best we can do is that $\langle f_i \rangle \subseteq \mathbf{I}(\mathbf{V}(f_i))$, for $1 \leq i \leq s$. Although the two may not be equal, we do know that the ideal generated by a variety always contains enough information to uniquely recover the underlying affine variety.

(Theorem) Correspondence between varieties and generated ideals: *Let V, W be affine varieties. Then*

1. $V \subset W$ if and only if $\mathbf{I}(W) \subset \mathbf{I}(V)$.
2. $V = W$ if and only if $\mathbf{I}(V) = \mathbf{I}(W)$.

- *Proof*: To prove the first item, suppose that $V \subset W$. Then any polynomial vanishing over W must vanish over V, which proves that $\mathbf{I}(W) \subset \mathbf{I}(V)$. If, on the other hand, $\mathbf{I}(W) \subset \mathbf{I}(V)$, then the polynomials defining W, which are in $\mathbf{I}(W)$ must also be in $\mathbf{I}(V)$, and so they must all also vanish over V, which shows that $V \subset W$. The proof for the second item is a corollary of the first. □

5 Polynomials of One Variable

In this section, we'll focus on polynomials in one variables - $F[x]$ for field F - and revisit the polynomial division algorithm. The existence of a division algorithm has deep consequences, and is related to the general structure of ideals and the idea of a polynomial greatest common divisor. The theory developed in this section will help us solve many problems we've encountered in earlier sections, highlighting the importance of algorithms in algebraic geometry. Before diving straight into the polynomial division algorithm, we first must precisely define the notion of the leading term of a polynomial.

(Definition) Leading term: *The **leading term** of a polynomial $f \in F[x]$ given by*

$$f = a_m x^m + \cdots + a_1 x + a_0, a_m \neq 0$$

is $a_m x^m$, written $\mathrm{LT}(f) = a_m x^m$.

We can now study the division algorithm.

(Theorem) Division algorithm: *Let F be a field and $f, g \in F[x]$. Then*

$$\exists \text{ unique } q, r \in F[x] \text{ s.t. } f = qg + r, \deg(r) < \deg(g)$$

- *Proof*: We prove the theorem with the **division algorithm** below, and proving its correctness.

```
procedure DivisionAlgorithm($f, g$)
    $q \leftarrow 0, r \leftarrow f$
    while $r \neq 0$ and $\mathrm{LT}(g) | \mathrm{LT}(r)$ do
        $q \leftarrow q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}$
        $r \leftarrow r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)} g$
    end while
    return $q, r$
```

```
end procedure
```

The correctness of the above algorithm can be seen by a simple inductive proof. The initial values of q, r trivially satisfy the relation $f = qg + r$, and on each step in the WHILE loop, the relation is preserved, as can be verified from the identity

$$f = qg + r = (q + \frac{\mathrm{LT}(r))}{\mathrm{LT}(g)})g + (r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g)$$

Moreover, the loop always terminates, because $\deg(r)$ is reduced each step by an integer amount, and so much eventually become zero. The reduction can be seen by the fact that $\deg\left(r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}\right) < \deg(r)$. □

- A useful corollary of the above theorem is that f has at most $\deg(f)$ roots in F (this can be proven by induction on $m := \deg(f)$).

(Theorem) Polynomial ideals are principal: *Let F be a field. Then every ideal in $F[x]$ can be written in the form $\langle f \rangle$ for some $f \in F[x]$. Moreover, f is unique up to multiplication by a non-zero constant in F.*

- *Proof*: Let $I \subset F[x]$ be an ideal, not equal to $\{0\}$ (in this case the theorem is trivial). Then let f be a non-zero polynomial in I with minimum degree. I is an ideal, so obviously $hf \in I, \forall h \in F[x]$, and therefore $\langle f \rangle \subseteq I$. To prove that $I \subseteq \langle f \rangle$, let $g \in I$ and apply the division algorithm to find

$$g = qf + r, \deg(r) < \deg(f) \text{ or } r = 0$$

Moreover, I is an ideal $\to r = g - qf \in I \to r = 0$ since otherwise we'd have $\deg(r) < \deg(f)$, which contradicts our choice of f as a polynomial with minimum degree. Thus we have $g = qf$, for any $g \in I$, which shows $I \subseteq \langle f \rangle$ and therefore $I = \langle f \rangle$. □
An ideal generated by a single element is called a **principal ideal**. In the context of abstract algebra, the above theorem follows as immediately from the fact that $F[x]$ is a principal ideal domain.

(Definition) Greatest common divisor: *The* ***greatest common divisor*** *of $f, g \in F[x]$, denoted* $\gcd(f, g)$*, is a polynomial h such that*

1. $h|f, h|g$
2. $p|f, p|g \to p|h$

- *Proof that* $\gcd(f, g)$ *is unique up to multiplication by non-zero constant:* Suppose $h' = \gcd(f, g)$. The definition of greatest common divisor implies that h, h' divide each other, and so are constant multiples of each other.

(Theorem) Greatest common divisor generates finitely generated ideals: *Let $f, g \in F[x]$. Then* $\gcd(f, g)$ *generates $\langle f, g \rangle$.*

- *Proof*: $\langle f, g \rangle$ is a polynomial ideal in $F[x]$, and so is principal. Then there exists some $h \in F[x]$ such that $\langle f, g \rangle = \langle h \rangle$. We will show that $h = \gcd(f, g)$. Clearly, h must divide both f and g, since $f, g \in \langle h \rangle$, so it remains to show that if $p|f, p|g$ then $p|h$. Let $f = ap, g = bp$. $h \in \langle f, g \rangle \to \exists c, d$ such that $h = fc + gd = acp + bdp = (ac + bd)p \to p|h$. □

(Theorem) Euclidean algorithm for polynomials: *The Euclidean algorithm is an algorithm for dividing two integers, and can be extended to polynomials as follows*:

```
procedure PolynomialGCD($f, g$)
    $h \leftarrow f, s \leftarrow g$
    while $s \neq 0$ do
        $rem \leftarrow$ REMAINDER($h, s$)
        $h \leftarrow s, s \leftarrow rem$
    end while
    return $s$
end procedure
```

where REMAINDER$(h, s) = r$ *where* $h = qs + r$.

- *Proof of correctness:* The crux of the proof is the idea that $\gcd(f, g) = \gcd(r, g)$ where $f = qg + r$. To prove this, it suffices to prove that $\langle f, g \rangle = \langle r, g \rangle$, by the previous theorem. To prove this, first let $h \in \langle f, g \rangle$, so that $\exists h_1, h_2 \in F[x]$ s.t

$$h = h_1 f + h_2 g = h_1 (qg + r) + h_2 g = h_1 r + (h_1 q + h_2) g \to h \in \langle f, r \rangle$$

Conversely, suppose $h \in \langle r, g \rangle$ so that $\exists h_1, h_2$ s.t.

$$h = h_1 r + h_2 g = h_1 (f - qg) + h_2 g = h_1 f + (h_2 - h_1 q) g \to h \in \langle f, g \rangle$$

which shows that $\langle f, g \rangle \subseteq \langle r, g \rangle$ and $\langle r, g \rangle \subseteq \langle f, g \rangle$, and so we have $\langle f, g \rangle = \langle r, g \rangle$. □

It should be noted that all of the properties of gcd delineated above generalize to the gcd of more than two polynomials.