Ideals, Varieties, and Algorithms notes

Jasper Ty

Contents

Geometry, Algebra, and Algorithms

1 Polynomials and Affine Space

Convention 1.1. We let $\mathbf{k}$ denote an arbitrary ground field.

1.1 Monomials, polynomials

Definition 1.2. A monomial in $x_1, \ldots, x_n$ is a formal product

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

The underlying data for a monomial is just a n-tuple $\alpha = (\alpha_1, \ldots, \alpha_n)$ of nonnegative integers.

To each monomial we assign a *degree* which is computed in the obvious way.

Definition 1.3. The *degree* of a monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ is a nonnegative integer defined by

$$\deg x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} := \alpha_1 + \cdots + \alpha_n.$$

To make calculations easier, we have a common and convenient notation.

Definition 1.4. We define *multi-index notation* for monomials by

$$x^{\alpha} := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where $\alpha = (\alpha_1, \ldots, \alpha_n)$ is any n-tuple of nonnegative integers.

For example, we can compactly define the degree of a monomial by setting $\deg x^\alpha := |\alpha|$.

Definition 1.5. A *polynomial* f in $x_1, \ldots, x_n$ in $\mathbf{k}$ is a finite formal linear combination of monomials with coefficients in $\mathbf{k}$, which we write

$$f = \sum_{\alpha \text{ is a } n\text{-tuple}} c_\alpha x^\alpha, \quad c_\alpha \in \mathbf{k}.$$

That this is finite means that c_α is zero for all but finitely many α— the sum is interpreted to be exactly over all the α for which c_α is nonzero.

The number c_α is called the *coefficient* of x^α in f. The *terms* of f are the $c_\alpha x^\alpha$ for which $c_\alpha \neq 0$. If f is nonzero, the *total degree of* f is defined to be

$$\deg f := \max_{\substack{\alpha \text{is a } n\text{-tuple} \\ c_\alpha \neq 0}} \left(\deg x^\alpha\right).$$

In other words, the largest degree among all the terms of f.

Finally, the set of all polynomials in $x_1, \ldots, x_n$ in $\mathbf{k}$ is denoted $\mathbf{k}[x_1, \ldots, x_n]$.

The underlying data for a polynomial can be expressed as a function $\mathrm{coeff}_f(\alpha_1, \ldots, \alpha_n)$ giving a coefficient $c_\alpha \in \mathbf{k}$ for each monomial x^α. That the sum is finite can be interpreted as coeff_f having finite support.

Or, it can also be expressed as a large n-dimensional array with entries in $\mathbf{k}$, and the tuples α are coordinates into this array for which the coefficients of x^α are given.

This is really also a kind of *normal form* for *polynomial expressions*, an expression tree where nodes are the ring operations $(+, \times)$ and whose leaves are terms $c_\alpha x^\alpha$— we can always associate any such tree with the "correct" element of $\mathbf{k}[x_1, \ldots, x_n]$.

1.2 Polynomial rings

Now, we give polynomials their algebraic structure.

Definition 1.6. Let $f = \sum_\alpha a_\alpha x^\alpha$ and $g = \sum_\alpha b_\alpha x^\alpha$ be two polynomials; elements of $\mathbf{k}[x_1, \ldots, x_n]$. The *sum* of f and g is defined by

$$f + g := \sum_\alpha (a_\alpha + b_\alpha) x^\alpha.$$

The *product* of f and g is defined by

$$fg := \sum_\gamma \sum_{\alpha+\beta=\gamma} (a_\alpha b_\beta) x^\gamma.$$

where $\alpha + \beta$ means the coordinate-wise sum of α and β; $(\alpha+\beta)_i = (\alpha_i + \beta_i)$.

This turns $\mathbf{k}[x_1, \ldots, x_n]$ into a *ring*, and so we call it a *polynomial ring*.

Definition 1.7. The *affine space* of dimension n over $\mathbf{k}$ is the set $\mathbf{k}^n$, i.e all n-tuples of elements in $\mathbf{k}$.

In high school, we study polynomials *as functions*— we now give the formal presentation of that perspective.

Definition 1.8. Any polynomial $f = \sum_\alpha c_\alpha x^\alpha \in \mathbf{k}[x_1, \ldots, x_n]$ gives rise to a function $f : \mathbf{k}^n \to \mathbf{k}$ defined, informally, by replacing all x_i's with a_i's. More precisely,

$$f(a_1, \ldots, a_n) := \sum_\alpha c_\alpha a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n}.$$

where now the sum is carried out in $\mathbf{k}$— the terms themselves are products in $\mathbf{k}$.

Now we ask: what is the difference between "$f = 0$ as a polynomial" and "$f \equiv 0$ as a function"?

Example 1.9. Consider the polynomial $f = x^2 - x \in \mathbb{F}_2[x]$. When we evaluate this in $\mathbb{F}_2$, we find that

$$\begin{aligned} 1^2 - 1 &= 0 \\ 0^2 - 0 &= 0. \end{aligned}$$

Hence $f \equiv 0$, as a function $\mathbb{F}_2^2 \to \mathbb{F}_2$. However, f is evidently not the zero polynomial.

Proposition 1.10. If $\mathbf{k}$ is an infinite field, then in $\mathbf{k}[x_1, \ldots, x_n]$, $f = 0$ as a polynomial if and only if $f \equiv 0$ as a function.

Proof. $f = 0$ as a polynomial obviously gives us the zero function.

For the other direction, we use induction.

We start with "the easy part of the fundamental theorem of algebra"— that a nonzero univariate polynomial of degree m has at most m roots. This is proven later, using the division algorithm. With it, we have a proof of the statement when $n = 1$, the one-variable case!

Since, if we take a polynomial $f \in \mathbf{k}[x]$ and it happens to be zero as a function, it has infinitely many roots. Then we take the contrapositive of the aforementioned fact— if a polynomial has infinitely many roots, it cannot be a nonzero polynomial, hence it is the zero polynomial.

Now, assume the statement holds for n, that is, if $g : \mathbf{k}^n \to \mathbf{k}$ is the zero function, then $g \in \mathbf{k}[x_1, \ldots, x_n]$ is the zero polynomial.

Take some $f \in \mathbf{k}[x_1, \ldots, x_{n+1}]$, and assume that $f : \mathbf{k}^{n+1} \to \mathbf{k}$ is the zero function. We can "sum by rows" and group together terms by *their power of* x_{n+1}, so we write

$$f = \sum_{i=0}^{\deg f} g_i x_{n+1}^i,$$

where $g_i \in \mathbf{k}[x_1, \ldots, x_n]$. Now, we do *partial application* and evaluate f at all coordinates *except* at x_{n+1}, which we leave as a variable.

$$f(a_1, \ldots, a_n, x_{n+1}) = \sum_{i=0}^{\deg f} g_i(a_1, \ldots, a_n) x_{n+1}^i,$$

This turns all the g_i's into coefficients in $\mathbf{k}$, and so we have a polynomial in $\mathbf{k}[x_{n+1}]$. Repeating the same logic, we must have that all the $g_i(a_1, \ldots, a_n)$'s are zero, since $f(a_1, \ldots, a_n, x_{n+1})$ is the zero map.

Then, since $(a_1, \ldots, a_n)$ was arbitrary, it must be that g_i are zero as functions. But by the induction hypothesis, this means that they are zero as polynomials.

Hence, $g_i = 0$ for all i, and $f = 0$ as a polynomial, proving the case $n + 1$.

By induction, we have proven the theorem. □

Corollary 1.11. If $\mathbf{k}$ is an infinite field, then $f = g$ as polynomials if and only if $f = g$ as functions.

Proof. $f = g$ as polynomials implying $f = g$ as functions is trivial.

If $f = g$ as functions, then $f - g$ is the zero polynomial. Hence, $f - g = 0$ in $\mathbf{k}[x_1, \ldots, x_n]$, so $f = g$ as polynomials. □

We have a fairly special result for $\mathbb{C}$.

Theorem 1.12 (The fundamental theorem of algebra)**.** Every nonconstant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

Proof. Omitted. □

A field $\mathbf{k}$ which satisfies the above property, which is that every nonconstant polynomial in $\mathbf{k}[x]$ has a root in $\mathbf{k}$, is called an *algebraically closed field*.

1.3 Exercises

Exercise 1.1. Prove that $\mathbb{F}_2$ is a field.

Not doing this one.

Exercise 1.2. (a) Consider the polynomial $g(x, y) = x^2 y + y^2 x \in \mathbb{F}_2[x, y]$. Show that $g(x, y) = 0$ for every $(x, y) \in \mathbb{F}_2^2$, and explain why this does not contradict Proposition 1.10.

(b) Find a nonzero polynomial in $\mathbb{F}_2[x, y, z]$ which vanishes at every point of $\mathbb{F}_2^3$. Try to find one involving all three variables.

(c) Find a nonzero polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ which vanishes at every point of $\mathbb{F}_2^n$. Can you find one in which all of $x_1, \ldots, x_n$ appear?

$g = (xy)(x+y)$, so it is nonzero if and only if $xy \neq 0$ and $x + y \neq 0$. This means that $xy = 1$ and $x + y = 1$. The former implies that $x = y = 1$, the latter implies that $x \neq y$, a contradiction.

This does not contradict Proposition 1.10 since it does not satisfy the conditions—$\mathbb{F}_2$ is not an infinite field.

$g(x, y, z) = (xyz)(x + y)$ is a nonzero polynomial which vanishes at every point of $\mathbb{F}_2^3$ for the same reason.

For the general case, $g(x_1, \ldots, x_n) = (x_1 \cdots x_n)(x_1 + x_2)$ works.

2 Affine Varieties

2.1 Definition

Definition 2.1. Let $\mathbf{k}$ be a field, and let $f_1, \ldots, f_s$ be polynomials in $\mathbf{k}[x_1, \ldots, x_n]$. Then the *affine variety* $\mathbf{V}(f_1, \ldots, f_s)$ is defined by

$$\mathbf{V}(f_1, \ldots, f_s) := \left\{(a_1, \ldots, a_n) \in \mathbf{k}^n : f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\right\},$$

that is, the exact subset of $\mathbf{k}^n$ for which all the f_i vanish.

Morally, the affine variety is defined by *solutions* of the system of polynomial equations defined by

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ f_2(x_1, \ldots, x_n) &= 0 \\ &\cdots \\ f_s(x_1, \ldots, x_n) &= 0 \end{aligned}$$

2.2 Examples

Example 2.2. The variety $\mathbf{V}(x^2 + y^2 - 1)$ cuts out the unit circle in the plane. Moreover, all conic sections are varieties of the form

$$\mathbf{V}(ax^2 + bxy + cy^2 + dx + ey + f).$$

Example 2.3. The graph of $y = \frac{x^3-1}{x}$ is an affine variety— it is $\mathbf{V}(xy - x^3 + 1)$.

TODO: 3D affine variety examples

Definition 2.4. A *linear variety* is a variety defined by linear equations, i.e polynomials whose total degree is at most 1.

Lemma 2.5. If $V, W \subseteq \mathbf{k}^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.

Proof. Let $V = \mathbf{V}(f_1, \ldots, f_s)$ and $W = \mathbf{V}(g_1, \ldots, g_t)$. We can explicitly give $V \cup W$ and $V \cap W$: they are

$$\begin{aligned} V \cap W &= \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t) \\ V \cup W &= \mathbf{V}\Big(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t\Big). \end{aligned}$$

The first equality is obvious.

For the second equality, pick out a point in V, then all the f_i vanish at that point, so all the $f_i g_j$ vanish at that point. Similarly if it is in W, then all the g_j vanish at that point, and so do the $f_i g_j$. Then, $V \cup W \subseteq \mathbf{V}(f_i g_j)$.

For the reverse inclusion, pick out a point of $\mathbf{V}(f_i g_j)$. If all the f_i vanish at that point, it is in V and we are done. If not, then it must be that all the g_j vanish, hence it is in W. This completes the proof. $\square$

3 Parametrization of affine varieties

A *parametrization* of a variety is

Definition 3.1. Let $\mathbf{k}$ be a field. A *rational function* in $t_1, \ldots, t_m$ with coefficients in $\mathbf{k}$ is a quotient f/g of two polynomials $f, g \in \mathbf{k}[t_1, \ldots, t_m]$, where g is not the zero polynomial.

Equality of two rational functions f/g and h/k is decided by the equality $kf = hg$ in $\mathbf{k}[t_1, \ldots, t_m]$.

The set of all the aforementioned functions is denoted $\mathbf{k}(t_1, \ldots, t_m)$.

Definition 3.2. Let $V = \mathbf{V}(f_1, \ldots, f_s) \subseteq \mathbf{k}^n$ be an affine variety. A *rational parametric representation* of V is a set of rational functions $r_1, \ldots, r_n \in \mathbf{k}(t_1, \ldots, t_m)$ such that the points

$$\begin{aligned} x_1 &= r_1(t_1, \ldots, t_m) \\ x_2 &= r_2(t_1, \ldots, t_m) \\ &\vdots \\ x_n &= r_n(t_1, \ldots, t_m) \end{aligned}$$

lie in V. Moreover, V must be the *smallest* affine variety containing these points.

4 Ideals

We have the following idea from abstract algebra, the analogue of a normal subgroup of a group.

Definition 4.1. Let R be a commutative ring. A subset $I \subseteq R$ is called an *ideal* if it satisfies:

(i) $0 \in I$.

(ii) $x + y \in I$ for all $x, y \in I$.

(iii) $ax \in I$ for all $x \in I$ and $a \in R$.

Translated for our polynomial rings, an ideal is a subset $I \subseteq \mathbf{k}[x_1, \ldots, x_n]$ such that

(i) $0 \in I$.

(ii) $f + g \in I$ for all $f, g \in I$.

(iii) $hf \in I$ for all $f \in I$ and $h \in \mathbf{k}[x_1, \ldots, x_n]$.

Now, we give a way of *producing* ideals in $\mathbf{k}[x_1, \ldots, x_n]$.

Definition 4.2. Let $f_1, \ldots, f_s \in \mathbf{k}[x_1, \ldots, x_n]$. The *ideal generated by* $f_1, \ldots, f_s$, denoted $\langle f_1, \ldots, f_s \rangle$, is the set

$$\langle f_1, \ldots, f_s \rangle := \left\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in \mathbf{k}[x_1, \ldots, x_n] \right\}.$$

This can vaguely be imagined as *shrink wrapping* an ideal structure on the set $\{f_1, \ldots, f_s\}$. We're adding the extra elements which the properties of ideals allow for, and exactly only those elements.

Lemma 4.3. The ideal generated by $f_1, \ldots, f_s$ is in fact an ideal.

Proof. Set $I = \langle f_1, \ldots, f_s \rangle$. By picking $h_i = 0$ for all i, we show that $0 \in I$.

If $f, g \in I$, then let

$$f = \sum_{i=1}^{s} h_i f_i$$
$$g = \sum_{i=1}^{s} h'_i f_i,$$

where $h_i \in \mathbf{k}[x_1, \ldots, x_n]$ and $h'_i \in \mathbf{k}[x_1, \ldots, x_n]$. Then

$$f + g = \sum_{i=1}^{s} (h_i + h'_i) f_i,$$

which shows that $f + g \in I$. Finally, if we pick $h \in \mathbf{k}[x_1, \ldots, x_n]$, we have that

$$hf = \sum_{i=1}^{s} (hh_i) f_i,$$

which shows that $hf \in I$. □

Definition 4.4. Let I be an ideal. We say that I is *finitely generated* if it is equal to $\langle f_1, \ldots, f_s \rangle$ for some $f_1, \ldots, f_s \in \mathbf{k}[x_1, \ldots, x_n]$, in which case we say that $f_1, \ldots, f_s$ are a *basis* for I.

Definition 4.5. Let $V \subseteq \mathbf{k}^n$ be an affine variety. Then the *ideal of* V, $\mathbf{I}(V)$, is

$$\mathbf{I}(V) := \left\{ f \in \mathbf{k}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ for all } (a_1, \ldots, a_n) \in V \right\}.$$

Lemma 4.6. If $V \subseteq \mathbf{k}^n$ is an affine variety, then $\mathbf{I}(V)$ is in fact an ideal.

Theorem 4.7.

$$\mathbf{I}(\mathbf{V}(y - x^2, z - x^3)) = \left\langle y - x^2, z - x^3 \right\rangle.$$

5 Polynomials of One Variable

5.1 Euclidean division

Definition 5.1. Given a nonzero polynomial $f \in \mathbf{k}[x]$, let

$$f = a_0 x^m + a_1 x^{m-1} + \cdots + a_m,$$

where $a_i \in \mathbf{k}$ and $a_i \neq 0$. Then we say that $a_0 x^m$ is the *leading term* of f, denoted $\mathrm{LT}(f) = a_0 x^m$.

There is an important fact about leading terms in polynomial rings over a field:

Proposition 5.2. If $\mathbf{k}$ is a field, then for all $f, g \in \mathbf{k}[x]$,

$$\deg f \leq \deg g \iff \mathrm{LT}(f) \text{ divides } \mathrm{LT}(g).$$

This unlocks for us *the division algorithm*.

Proposition 5.3 (The division algorithm)**.** Let $\mathbf{k}$ be a field and let g be a nonzero polynomial in $\mathbf{k}[x]$. Then every $f \in \mathbf{k}[x]$ can be written as

$$f = qg + r$$

where $q, r \in \mathbf{k}[x]$ and either $r = 0$ or $\deg r < \deg g$. Furthermore, q, r are *unique*, and there is an algorithm for finding q and r.

Proof. The algorithm which finds q and r is the following:

Data: f,g
Result: q,r
begin
    $q \leftarrow 0$;
    $r \leftarrow f$;
    while $r \neq 0$ **and** $LT(g)$ *divides* $LT(r)$ **do**
        $q \leftarrow q + \mathrm{LT}(r)/\mathrm{LT}(g)$;
        $r \leftarrow r - (\mathrm{LT}(r)/\mathrm{LT}(g))g$;
    end
end

First, we prove that the result has the properties we want: that $f = qg + r$, and either $r = 0$ or $\deg r < \deg g$.

The first property, $f = qg + r$, is actually a *loop invariant* of the while block. At the first iteration, where $q = 0$ and $r = f$, clearly $f = qg + r$. Now, supposing $f = qg + r$, we have that

$$\begin{aligned} f &= qg + r \\ &= qg + r + 0 \\ &= qg + r + \left(\frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g\right) \\ &= \left(qg + \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g\right) + \left(r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g\right) \\ &= \left(q + \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}\right)g + \left(r - \frac{\mathrm{LT}(r)}{\mathrm{LT}(g)}g\right). \end{aligned}$$

Hence, if we put $q \leftarrow q + \mathrm{LT}(r)/\mathrm{LT}(g)$ and $r \leftarrow (\mathrm{LT}(r)/\mathrm{LT}(g))g$, we still have $f = qg + r$.

Next, we show that if the above terminates, it must be that the statement "$r \neq 0$ and $\mathrm{LT}(g)$ divides $\mathrm{LT}(r)$" is false, which means that either $r = 0$ or $\mathrm{LT}(g)$ does not divide $\mathrm{LT}(r)$.

For the latter part, we recall the previous proposition, Proposition 5.2, and perform *biconditional negation*. Namely, we derive from

$$\deg f \leq \deg g \iff \mathrm{LT}(f) \text{ divides } \mathrm{LT}(g)$$

the statement

$$\deg f > \deg g \iff \mathrm{LT}(f) \text{ does not divide } \mathrm{LT}(g),$$

by negating both sides of the $\iff$. Now, we can say that "$\mathrm{LT}(g)$ does not divide $\mathrm{LT}(r)$" is equivalent to "$\deg g > \deg r$". Hence, the algorithm terminates precisely when either $r = 0$ or $\deg r < \deg g$.

Finally, we have to conclude that the algorithm terminates *at all*.

□

Now, we can prove the "easy half of the fundamental theorem of algebra"

> **Corollary 5.4.** If $\mathbf{k}$ is a field and $f \in \mathbf{k}[x]$ is a nonzero polynomial, then f has at most $\deg f$ roots in $\mathbf{k}$.

Proof. We prove this by induction on the degree of f. If the degree of f is zero, □

Moreover, the division algorithm has implications for the algebraic structure of $\mathbf{k}[x]$.

> **Definition 5.5.** Let R be a ring. A ring is said to be a *principal ideal domain*, or a *PID*, if every ideal of R is of the form $\langle x \rangle$, where $x \in R$.

> **Corollary 5.6.** If $\mathbf{k}$ is a field, then $\mathbf{k}[x]$ is a PID.

Groebner Bases