

1. FIELDS

Fields and vector spaces.

Typical vector spaces: $\mathbb{R}, \mathbb{Q}, \mathbb{C}$. For infinite dimensional vector spaces, see notes by Karen Smith. Important to consider a field as a vector space over a sub-field.

Also have: algebraic closure of \mathbb{Q} . Galois fields: $GF(p^a)$.

Don't limit what field you work over.

2. POLYNOMIAL RINGS OVER A FIELD

Notation for a polynomial ring: $\mathbb{K}[x_1, \dots, x_n]$.

Monomial: $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$

Set $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$.

Write x^α for $x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$.

A *term* is a monomial multiplied by a field element: $c_\alpha x^\alpha$.

A *polynomial* is a *finite* \mathbb{K} -linear combination of monomials:

$$f = \sum_{\alpha} c_{\alpha} x^{\alpha},$$

so a polynomial is a finite sum of terms. The *support* of f are the monomials that appear (with non-zero coefficients) in the polynomial f .

If $\alpha = (\alpha_1, \dots, \alpha_n)$, put $|\alpha| = \alpha_1 + \dots + \alpha_n$.

If $f \in \mathbb{K}[x_1, \dots, x_n]$, $\deg(f) = \max\{|\alpha| : x^\alpha \text{ is in the support of } f\}$.

Example 2.1. $f = 7x^3y^2z + 11xyz^2$ $\deg(f) = \max\{6, 4\} = 6$. $7x^3y^2z$ is a *term*. x^3y^2z is a *monomial*.

Given $f \in \mathbb{K}[x_1, \dots, x_n]$, *evaluation* is the map $F_f : \mathbb{K}^n \rightarrow \mathbb{K}$ given by $(c_1, \dots, c_n) \rightarrow f(c_1, \dots, c_n)$.

When is F_f the zero map?

Example 2.2. If \mathbb{K} is a finite field, F_f can be the zero map without f being the zero polynomial. For instance take the field with two elements, $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, and consider the polynomial $f = x^2 + x = x(x+1)$. Then f is *not* zero in the ring $\mathbb{K}[x]$, however $f(c) = 0$ for all $c \in \mathbb{K}$ (there are only two to check!).

Theorem 2.3. If \mathbb{K} is an infinite field, then F_f is the zero map if and only if f is the zero polynomial.

Proof. (From Cox-Little-O'Shea) by induction.

If $n = 1$, then a non-zero $f \in \mathbb{K}[x]$ of degree d has at most d distinct roots (Euclidean algorithm). $F_f : \mathbb{K} \rightarrow \mathbb{K}$ evaluates to zero only at roots of f .

Assume this is true up to $n - 1$ variables. Consider $\mathbb{K}[x_1, \dots, x_n]$ as the polynomial ring $\mathbb{K}[x_1, \dots, x_{n-1}][x_n]$ (the polynomial ring in the variable x_n with coefficients in the polynomial ring $\mathbb{K}[x_1, \dots, x_{n-1}]$). Let $f = \sum g_i x_n^i$, where $g_i \in \mathbb{K}[x_1, \dots, x_{n-1}]$. Consider $(\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{K}^{n-1}$. Evaluate $f(\alpha_1, \dots, \alpha_{n-1}, x_n)$; this is a polynomial in a single variable, so by the base case it is zero if and only if $g_i(\alpha_1, \dots, \alpha_{n-1}) = 0$ for every coefficient. By induction, $g_i(\alpha_1, \dots, \alpha_{n-1}) = 0$ for all $(\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{K}^{n-1}$ if and only if g_i is the zero polynomial. Hence f must be the zero polynomial. \square

Corollary 2.4. Let \mathbb{K} be an infinite field. Let $f, g \in \mathbb{K}[x_1, \dots, x_n]$. Then $F_f = F_g$ if and only if $f = g$ as polynomials.

3. AFFINE VARIETIES

Definition 3.1. Let $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n]$. The *affine variety* cut out by f_1, \dots, f_r is denoted by $V(f_1, \dots, f_r)$ and is defined by

$$V(f_1, \dots, f_r) = \{c = (c_1, \dots, c_n) \in \mathbb{K}^n : f_i(c) = 0 \text{ for all } f_1, \dots, f_r\}$$

Example 3.2. $f = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$. Then $V(f)$ = unit circle. $g = x^2 + y^2 \in \mathbb{R}[x, y]$. Then $V(g)$ = point $(0, 0)$. $h = x^2 + y^2 + 1 \in \mathbb{R}[x, y]$. Then $V(h) = \emptyset$! Notice that the codimension of these affine varieties is $1, 0, -1$, respectively.

Example 3.3. Let $f_1, f_2 \in \mathbb{R}[x, y, z]$, with $f_1 = x + y + z + 7$, $f_2 = x + 3y + 2z + 11$. Then $V(f_1, f_2)$ is a line in \mathbb{R}^3 .

Example 3.4. Consider $f = x^2 + 2xy + y + 1 \in \mathbb{F}_3[x, y]$. Then $V(f)$ is a *hypersurface* in \mathbb{F}_3^2 . There are nine points in \mathbb{F}_3^2 . If $x = 0$, $f(0, y) = y + 1$, so $y = 2$. If $x = 1$, $f(1, y) = 2$, so there are no solutions. If $x = 2$, then $f(2, y) = 2 + 2y$, so $y = 2$ again. So $V(f) = \{(0, 2), (2, 2)\}$.

Remark 3.5. Given $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$, it is interesting to consider the cardinality of $V(f_1, \dots, f_r)$ when f_1, \dots, f_r are considered to be in finite fields of the form $GF(p^t)$. These cardinalities could be encoded in a power series, for instance. There are many open problems considering the relationships between the varieties $V(f_1, \dots, f_r)$ over finite fields and the varieties these polynomials define over $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.

Remark 3.6. Chebatorev's density theorem gives probabilistic information about the Galois group of a polynomial by looking at splitting types of the polynomial over different finite fields.

Example 3.7 (Chebatorev's density theorem in action). The table below lists the orders and cycle types of transitive subgroups of the symmetric group S_4 . These are the possible Galois groups of irreducible polynomials of degree four.

G	1,1,1,1	1,1,2	1,3	4	2,2	$ G $
V_4	1	0	0	0	3	4
C_4	1	0	0	2	1	4
D_4	1	2	0	2	3	8
A_4	1	0	8	0	3	12
S_4	1	6	8	6	3	24

Suppose you would like to compute the Galois group of the irreducible polynomial $f(x) = x^4 + 3x^2 - 1$. Compute its factorization modulo different primes. The factorizations have to match the cycle types.

Reducing $f(x)$ modulo first 10,000 primes. Factorization type 2,2 appears 3762 times. Factorization type 1,1,1,1 appears 1222 times. Factorization type 1,1,2 appears 2514 times. Irreducible appears 2502 times.

Chebatorev's density theorem says that, in the limit, the probability that $f(x)$ factors as a particular type is precisely the probability of picking that cycle type in the Galois group.

The statistics above match the expected cycle types of the D_4 group, which is exactly what the Galois group of $f(x)$ is.

Example 3.8 (Four-bar Linkage). Consider two fixed points with two rigid bars attached, and one more rigid bar connecting the movable endpoints of the two

movable bars. Attach a rigid triangle to the last bar. The curve traced out by the tip of the triangle is called the *coupler* curve of the mechanism.

Kempe's universality theorem says that any connected component of a real algebraic curve in the plane can be realized as the *coupler curve* of a mechanism. Some corrections and extensions of Kempe's theorem appear in Timothy Abbott's masters thesis. Here are some questions related to linkages:

- How can you construct a linkage with prescribed properties?
- Given a linkage, how do you find equations defining its motion?

Example 3.9 (Conformation space of cyclo-octane). In cyclo-octane there are eight carbon atoms linked in a cycle by edges of a fixed length and with fixed *bond angles* between the edges at each atom. To eliminate some degrees of freedom, fix the plane determined by three atoms. So consider that three (occurring in order) have coordinates $(0, 0, 0)$, $(a, 0, 0)$, and $(b, c, 0)$ (these coordinates will be completely determined by the length of the edges and the common angle). Once these are fixed, the two adjacent points on either end can each trace out a circle's worth of positions, and for each pair of choices made for the positions of these two, there are finitely many possible positions for the remaining three points. Thus the conformation space of cyclo-octane is a surface that is a finite covering of the torus $S^1 \times S^1$, and it naturally lives in \mathbb{R}^{15} (the fifteen parameters come from the coordinates of the remaining 5 points which are not fixed).

Theorem 3.10. Let $A = V(f_1, \dots, f_r), B = V(g_1, \dots, g_s)$, with $f_1, \dots, f_r, g_1, \dots, g_s \in \mathbb{K}[x_1, \dots, x_n]$. Then $A \cup B$ and $A \cap B$ are affine varieties.

Proof. Check that $A \cap B = V(f_1, \dots, f_r, g_1, \dots, g_s)$ and $A \cup B = V(\{f_i g_j : 1 \leq i \leq r, 1 \leq j \leq s\})$. \square

Some questions:

- Is $V(f_1, \dots, f_r) = \emptyset$?
- If $|V(f_1, \dots, f_r)| < \infty$, can we find them? Can we count how many there are?
- In general, can we describe $V(f_1, \dots, f_r)$?

4. PARAMETRIZATIONS OF AFFINE VARIETIES

Example 4.1. Consider the variety $V(x + y + z - 3, x + 2y + 3z - 5) \subset \mathbb{R}^3$. This is defined *implicitly* (this means the variety is given by equations). Finding a Gröbner basis is a generalization of Gaussian elimination (it's Gaussian elimination on steroids). One the augmented matrix for this linear system is put in row reduced echelon form, we obtain the system

$$\begin{array}{rcl} x & -z & = 1 \\ y & -2z & = 2 \end{array}$$

From this we obtain $x = z + 1, y = -2z + 2$. Setting $z = t$, we get the *parametrization*:

$$\begin{array}{rcl} x & = & t + 1 \\ y & = & -2t + 2 \\ z & = & t \end{array}$$

Example 4.2. Consider $V(x^2 + y^2 - 1)$ (the unit circle). A *rational parametrization* is:

$$\begin{aligned}x &= \frac{1 - t^2}{1 + t^2} \\y &= \frac{2t}{1 + t^2}\end{aligned}$$

This parametrization can be determined by considering where the line with slope t through the point $(-1, 0)$ intersects the unit circle.

Definition 4.3. A *rational function* in the variables t_1, \dots, t_n is a quotient $\frac{f}{g}$ where $f, g \in \mathbb{K}[t_1, \dots, t_n]$. Rational functions can be identified by the usual rule $\frac{f}{g} = \frac{f'}{g'}$ if and only if $fg' = f'g$. The set of all rational functions in t_1, \dots, t_n is denoted $\mathbb{K}(t_1, \dots, t_n)$.

Proposition 4.4. $\mathbb{K}(t_1, \dots, t_n)$ is a field.

Example 4.5 (Tangent surfaces of curves). The *twisted cubic* is parametrized as $x = t, y = t^2, z = t^3, -\infty < t < \infty$. Its tangent surface is the set of points that lie on any tangent line of the twisted cubic. Given a good parametrization $\mathbf{r}(t)$ of a smooth curve (tangent vectors don't vanish), a parametrization for the tangent surface is just $s(t, u) = \mathbf{r}(t) + u \cdot \mathbf{r}'(t)$. For the twisted cubic, the tangent surface is parametrized by:

$$\begin{aligned}x &= t + u \\y &= t^2 + 2tu \\z &= t^3 + 3t^2u\end{aligned}$$

Any smooth variety has an associated tangent variety which is the set of all points which lie on the variety itself or on any tangent plane.

Example 4.6. Arithmetic in rational function fields works just like it does normally. For instance, let the matrix M be defined by

$$M = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 + x & 6 \end{bmatrix}.$$

We will consider M to be a 2×3 matrix with entries in the rational function field $\mathbb{Q}(x)$ (we could also consider entries in $\mathbb{Z}(x)$, but then we would not be able to divide). We can find the reduced row echelon form of M with the usual row operations. This yields:

$$\text{rref}(M) = \begin{bmatrix} 1 & 0 & \frac{3x+3}{x-3} \\ 0 & 1 & \frac{-6}{x-3} \end{bmatrix}.$$

We can extract from $\text{rref}(M)$ all the usual information that we do in linear algebra. For instance, M has rank 2 as a matrix over the field $\mathbb{Q}(x)$. We could also derive a basis for the null space of M , etc.

Remark 4.7. The field $\mathbb{K}(t_1, \dots, t_n)$ is a special case of something called a *field of fractions*, which can be constructed for any *integral domain*. An integral domain is a commutative ring R in which there are no zero divisors (i.e. if $a, b \in R$ and

$ab = 0$ then $a = 0$ or $b = 0$). If R is an integral domain, then the field of fractions of R , denoted $\mathbf{frac}(R)$, is the field consisting of all fractions

$$\left\{ \frac{a}{b} : a, b \in R \text{ and } b \neq 0 \right\},$$

where $\frac{a}{b} = \frac{a'}{b'}$ if $ab' = a'b$.

There are several standard operations which preserve the property of being an integral domain. If R is an integral domain then so are $R[x]$ and $R[[x]]$ (power series ring in the variable x over R). Moreover, $\mathbf{frac}(R[x]) = \mathbf{frac}(R)(x)$.

If P is a *prime ideal* of R (we will define this later) then the quotient R/P is an integral domain (this is one way to define a prime ideal).

Definition 4.8. A rational parametric representation of a variety $V \subset \mathbb{K}^n$ is given by a collection of rational functions $\frac{f_1}{g_1}, \frac{f_2}{g_2}, \dots, \frac{f_n}{g_n} \in \mathbb{K}(t_1, \dots, t_n)$ such that

$$\begin{aligned} x_1 &= \frac{f_1}{g_1} \\ x_2 &= \frac{f_2}{g_2} \\ &\vdots \\ x_n &= \frac{f_n}{g_n} \end{aligned}$$

lie in V for all values of t_i and such that there is no smaller variety W for which this is true.

Definition 4.9. A variety $V \subset \mathbb{K}^n$ which has a rational representation is called *unirational*.

Remark 4.10. A variety V is said to be given *implicitly* if it is described in the form $V(f_1, \dots, f_r)$ for some polynomials f_1, \dots, f_r . An implicit representation is important for answering the question: given some point $p \in \mathbb{K}^n$, is $p \in V$? On the other hand, *parametric representations* are useful for producing lots of points on V (for instance if you would like to draw a picture).

Only very special varieties have parametric representations. There are several important questions related to this:

- (1) Given a parametric representation, can we find an implicit representation?
- (2) Given an implicit representation, can we determine if the variety has a parametric representation?
- (3) If a variety has a parametric representation, can we find one?

Example 4.11. The *twisted cubic* is the variety V in \mathbb{R}^3 defined by the parametrization $x = t, y = t^2$, and $z = t^3$. Implicitly, V is defined by the equations $x^2 - y, x^3 - z$, and $xy - z$.

5. IDEALS OF AFFINE VARIETIES

Definition 5.1. A subset $I \subset \mathbb{K}[x_1, \dots, x_n]$ is an *ideal* if it satisfies the following two properties:

- (1) If $f, g \in I$ then $f + g \in I$ and
- (2) If $f \in I, g \in \mathbb{K}[x_1, \dots, x_n]$ then $fg \in I$.

If $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n]$ then the *ideal generated by f_1, \dots, f_r* , denoted $\langle f_1, \dots, f_r \rangle$ is the smallest ideal (under containment) containing the polynomials f_1, \dots, f_r .

Proposition 5.2. *If $f_1, \dots, f_r \in \mathbb{K}[x_1, \dots, x_n]$ then $\langle f_1, \dots, f_r \rangle = \{\sum_{i=1}^r g_i f_i : g_1, \dots, g_r \in \mathbb{K}[x_1, \dots, x_n]\}$.*

Proof. Exercise. □

Definition 5.3 (Fundamental construction for ideals). An ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$ is finitely generated if there are polynomials f_1, \dots, f_r so that $I = \langle f_1, \dots, f_r \rangle$.

We will see the proof of the following fundamental result later:

Theorem 5.4 (Hilbert Basis Theorem). *Every ideal in $\mathbb{K}[x_1, \dots, x_n]$ is finitely generated.*

Definition 5.5 (Variety defined by a set of polynomials). Given any subset of polynomials (possibly infinite) $T \subset \mathbb{K}[x_1, \dots, x_n]$, the set $V(T) \subset \mathbb{K}^n$ is defined as

$$V(T) = \{(a_1, \dots, a_n) \in \mathbb{K}^n : f(a_1, \dots, a_n) = 0 \text{ for all } f \in T\}.$$

This is particularly important when T is an ideal of $\mathbb{K}[x_1, \dots, x_n]$.

Proposition 5.6. *The variety defined by f_1, \dots, f_r is the same as the variety defined by the ideal $I = \langle f_1, \dots, f_r \rangle$. In symbols, $V(f_1, \dots, f_r) = V(\langle f_1, \dots, f_r \rangle)$. More generally, the variety defined by any set T of polynomials is the same as the variety defined by the ideal $\langle T \rangle$ generated by T .*

Proof. Exercise. □

Remark 5.7. By Proposition 5.6, if T is any set of polynomials then $V(T) = V(\langle T \rangle)$. Using the Hilbert basis theorem $\langle T \rangle = \langle f_1, \dots, f_r \rangle$ for some set of polynomials f_1, \dots, f_r . Again by Proposition 5.6, $V(\langle f_1, \dots, f_r \rangle) = V(f_1, \dots, f_r)$. It follows that $V(T)$ is always an affine variety. More intuitively, this is saying that the variety defined by a possibly infinite set of polynomials can always be defined by finitely many polynomials.

Definition 5.8 (Ideal of a set). Suppose $S \subset \mathbb{K}^n$ is any subset (this is particularly important if S is an affine variety). The ideal of S is

$$I(S) = \{f \in \mathbb{K}[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in S\}.$$

Proposition 5.9. *For any $S \subset \mathbb{K}^n$, $I(S)$ is an ideal.*

Proof. Exercise. □

Definition 5.10 (Zariski Closure). Let $S \subset \mathbb{K}^n$ the Zariski closure of S is defined as $\bar{S} = V(I(S))$.

Remark 5.11. By Remark 5.7, the Zariski closure of any set $S \subset \mathbb{K}^n$ is an affine variety.

Proposition 5.12. *If $S \subset \mathbb{K}^n$, then*

- (1) $V(I(\bar{S})) = \bar{S}$
- (2) $S \subset \bar{S}$

Example 5.13. Consider $x^2 \in \mathbb{R}[x]$. Then $V(x^2) = \{a \in \mathbb{R} : a^2 = 0\} = \{0\}$. $I(V(x^2)) = \{f \in \mathbb{R}[x] : f(a) = 0\} = \{x \cdot g : g \in \mathbb{R}[x]\} = \langle x \rangle$.

Example 5.14. Consider $S = (0, 1) \subset \mathbb{R}^1$ (the open interval from 0 to 1). Then $I(S) = \{f \in \mathbb{R}[x] : f(a) = 0 \text{ for all } a \in (0, 1)\} = \{0\}$. Also $V(I(S)) = \{a \in \mathbb{R}^1 : f(a) = 0 \text{ for every } f \in I(S)\} = \mathbb{R}^1$. So $\bar{S} = \mathbb{R}$.

Proposition 5.17. *If $T \subset \mathbb{K}[x_1, \dots, x_n]$, then*

- $$\begin{aligned} (1) \quad & T \subset \bar{T} \\ (2) \quad & I(V(\bar{T})) = \bar{T}. \end{aligned}$$

By Remark 5.11, affine varieties can be thought of as precisely the possible Zariski closures of sets in \mathbb{K}^n . Algebraically, this leads us to ask what types of ideals occur as closures of subsets of $\mathbb{K}[x_1, \dots, x_n]$. We will come back to this question. Let's close with two fundamental questions.

- (1) Given an ideal $I \subset \mathbb{K}[x_1, \dots, x_n]$, can we find finitely many polynomials f_1, \dots, f_r so that $I = \langle f_1, \dots, f_r \rangle$? The answer to this question is yes by the Hilbert Basis theorem (which we will see later), but finding such polynomials can be a difficult task! Remember Example 5.15.
- (2) If $I = \langle f_1, \dots, f_r \rangle$ and $g \in \mathbb{K}[x_1, \dots, x_n]$, can we determine if $g \in I$? This is known as the *ideal membership problem*. A solution to this problem is given by Gröbner bases, which we will see soon.

We will describe the structure of ideals in the ring $\mathbb{K}[x]$. Suppose $f \in \mathbb{K}[x]$. Then $f = a_dx^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ with a_0, \dots, a_d . The *leading term* of $f(x)$ is $\text{LT}(f) = a_dx^d$ and the degree of $f(x)$ is $\deg(f) = d$, the maximum degree of a power of x appearing in $f(x)$.

Proposition 6.1. *Given $f, g \in \mathbb{K}[x]$, there are unique polynomials $Q, R \in \mathbb{K}[x]$ such that $f = gQ + R$ with either $R = 0$ or $\deg(R) < \deg(g)$.*

We will prove Proposition 6.1 via an algorithm, which we first exhibit by example.

Example 6.2. Let $f = x^3 + 3x + 2$ and $g = x + 1$. We can produce Q and R by polynomial long division.

$$\begin{array}{r} x^2 - x + 4 \\ x + 1 \overline{) } \\ \underline{-x^3 - x^2} \\ -x^2 + 3x \\ \underline{x^2 + x} \\ 4x + 2 \\ \underline{-4x - 4} \\ -2 \end{array}$$

We can read off Q and R : $Q = x^2 - x + 4$ and $R = -2$.

The LONG DIVISION ALGORITHM below generalizes the previous example.

INPUT: $R = f, Q = 0$

WHILE $\text{LT}(g) \nmid \text{LT}(R)$ **do:**

$$Q = Q + \frac{\text{LT}(R)}{\text{LT}(g)}$$

$$R = R - \frac{\text{LT}(R)}{\text{LT}(g)}g$$

OUTPUT: Q, R

Proof of Proposition 6.1. The existence of Q, R satisfying the properties is established by the LONG DIVISION ALGORITHM described above. To establish uniqueness, suppose there are two representations $f = gQ + R$ and $f = gQ' + R'$ satisfying the given properties. We see that $0 = g(Q - Q') + (R' - R)$. Since R' and R have degree strictly less than g , $Q - Q' = 0$ and hence $Q = Q'$ and $R = R'$. \square

Corollary 6.3. *A degree d polynomial in $\mathbb{K}[x]$ has at most d roots.*

Proof. Exercise. Or see the book (Corollary 3 in Section 1.5). \square

Corollary 6.4. *If I is an ideal in $\mathbb{K}[x]$ then there is an $h \in \mathbb{K}[x]$ so that $I = \langle h \rangle$.*

Proof. If I is the zero ideal this is clear ($I = \langle 0 \rangle$). Otherwise pick any $h \in I$ so that h has smallest degree (we can do this by well-ordering of the integers). Note that $\langle h \rangle \subset I$. Now let $f \in I$ and apply the division algorithm. Write $f = hQ + R$. Then $\deg(R) < \deg(h)$. But also $R = f - hQ \in I$, so if $R \neq 0$ then $\deg(R) \geq \deg(h)$ by the way that h was chosen. So $R = 0$, $f = hQ$, and hence $I = \langle h \rangle$. \square

Definition 6.5. Let $f, g \in \mathbb{K}[x]$. A greatest common divisor of f and g (GCD) is a polynomial h satisfying

- (1) $h \mid f$ and $h \mid g$ and
- (2) if $p \mid f$ and $p \mid g$ then $p \mid h$.

Remark 6.6. Any two GCD's of f and g differ by multiplication by a constant.

Proposition 6.7. *If $f, g \in \mathbb{K}[x]$ then a GCD of f and G exists.*

Proof. By Corollary 6.4, there is some $h \in \mathbb{K}[x]$ so that $\langle f, g \rangle = \langle h \rangle$. We claim that h is a GCD of f and g . Immediately, $h \mid f$ and $h \mid g$. Since $h \in \langle f, g \rangle$, there are $A, B \in \mathbb{K}[x]$ so that $h = Af + Bg$. If $p \mid f$ and $p \mid g$ then $f = pC$ and $g = pD$ for some $C, D \in \mathbb{K}[x]$. So $h = ApC + BpD = p(AC + BD)$, so $p \mid h$. \square

How do you produce a GCD of f and g ? This is produced by the EUCLIDEAN ALGORITHM, which we now describe. Start with f, g (assume $\deg(f) \geq \deg(g)$).

$$\begin{aligned} f &= gQ_1 + R_1 & \deg(g) > \deg(R_1) \text{ or } R_1 &= 0 \\ g &= R_1Q_2 + R_2 & \deg(R_1) > \deg(R_2) \text{ or } R_2 &= 0 \\ R_1 &= R_2Q_3 + R_3 & \deg(R_2) > \deg(R_3) \text{ or } R_3 &= 0 \\ &\vdots \\ R_{k-2} &= R_{k-1}Q_{k-1} + R_k \\ R_k &= 0 \end{aligned}$$

Since the degrees of the remainders R_i are decreasing, eventually we must hit a degree of zero, which shows that eventually we will terminate. Then a GCD of f and g is exactly the last non-zero remainder, namely R_{k-1} . Reversing the successive applications of the long division also allows you to write a GCD as a polynomial combination of f and g .

Definition 6.8. A GCD of the polynomials f_1, \dots, f_r is a polynomial h satisfying:

- (1) $h \mid f_1, \dots, h \mid f_r$ and
- (2) if $p \mid f_1, \dots, p \mid f_r$ then $p \mid h$.

Proposition 6.9. A GCD of f_1, \dots, f_r can be defined by $GCD(f_1, \dots, f_r) = GCD(f_1, GCD(f_2, \dots, f_r))$.

This allows a GCD of many polynomials to be computed iteratively.

At this point we can solve the ideal membership problem in one variable: to check that the polynomial $g \in \mathbb{K}[x]$ is in the ideal $\langle f_1, \dots, f_r \rangle \subset \mathbb{K}[x]$ do the following:

- (1) Find the gcd h of f_1, \dots, f_r by iterating the Euclidean algorithm in pairs as indicated in Proposition 6.9. We have seen that $\langle f_1, \dots, f_r \rangle = \langle h \rangle$.
- (2) Divide g by h using the division algorithm. $g \in \langle f_1, \dots, f_r \rangle$ if and only if the remainder of g on division by h is 0.

Example 6.10 (Euclidean algorithm in the integers). Find the gcd of 72 and 56.

$$\begin{aligned} 72 &= 56 + 16 \\ 56 &= 3 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0 \end{aligned}$$

so the gcd is 8. Notice we also get a way to write 8 as an integer linear combination of 72 and 56: $8 = 56 - 3 \cdot 16 = 56 - 3 \cdot (72 - 56) = 4 \cdot 56 - 3 \cdot 72$.

Example 6.11 (Euclidean algorithm for univariate polynomials). Find the GCD of $x^5 - 1$ and $x^3 - x$.

$$\begin{aligned} x^5 - 1 &= (x^3 - x)(x^2 + 1) + (x - 1) \\ x^3 - x &= (x - 1)(x^2 + x) + 0, \end{aligned}$$

so the GCD is $x - 1$. Notice these computations also yield that $x - 1 = (x^5 - 1) - (x^3 - x)(x^2 + 1)$, which explicitly expresses the fact that $x - 1 \in \langle x^5 - 1, x^3 - x \rangle$.

6.1. Field of fractions of an integral domain. We expand on Remark 4.7. Recall an *integral domain* is a commutative ring without any zero divisors. We have the following facts about integral domains:

- (1) Any field is an integral domain.
- (2) If R is an integral domain, then $R[x]$ is an integral domain.
- (3) If I is a prime ideal of R , then R/I is an integral domain.
- (4) Any finite integral domain is a field.
- (5) Let $f(x) \in \mathbb{K}[x]$. If f is irreducible in $\mathbb{K}[x]$, then $\langle f \rangle$ is a prime ideal so $\mathbb{K}[x]/\langle f \rangle$ is an integral domain.

Example 6.12. Consider the finite field \mathbb{F}_3 with three elements (for instance $\mathbb{Z}/3\mathbb{Z}$). The polynomial $x^3 + 2x^2 + 1$ is irreducible since it does not have any roots (just plug in $x = 0, 1, 2$ and notice the polynomial does not vanish). So $\mathbb{F}_3[x]/\langle x^3 + 2x^2 + 1 \rangle$ is an integral domain. Notice that this integral domain has 27 elements: any polynomial of degree ≥ 3 can be reduced to a polynomial of the form $ax^2 + bx + c$, and there are three choices for each of a, b, c . So $\mathbb{F}_3[x]/\langle x^3 + 2x^2 + 1 \rangle$ is a finite integral domain, and hence a field. So we can do all the operations that we are used to doing for fields.

For instance, let's find the row reduced echelon form of the matrix

$$M = \begin{bmatrix} 1 & x^2 & 1 \\ 0 & x & 2 \end{bmatrix}$$

which we consider as having entries in the field $\mathbb{F}_2[x]/\langle x^3 + 2x^2 + 1 \rangle$. Subtracting x times the second row from the first:

$$\begin{bmatrix} 1 & 0 & 1 - 2x \\ 0 & x & 2 \end{bmatrix}$$

Multiply the second row by the inverse of x , which is $2x^2 + x$:

$$\begin{bmatrix} 1 & 0 & 1 - 2x \\ 0 & 1 & x^2 + 2x \end{bmatrix}.$$

This is the row reduced echelon form of M .

7. MONOMIAL ORDERS

Monomial orders allow a generalization of the division algorithm from the last section.

Definition 7.1. A monomial order \leq on the monomials of $\mathbb{K}[x_1, \dots, x_n]$ is a

- total order (every monomial can be compared to every other monomial)
- if m_1, m_2, n are monomials and $m_1 \geq m_2$, then $m_1 n \geq m_2 n$
- if n is a monomial and $n \neq 1$, then $1 < n$ (strict inequality)

The following examples illustrate three common monomial orders. The precise definitions in terms of weight vectors is given in the section on monomial orders by vectors.

Example 7.2 (Lexicographic order or Lex order). This order prioritizes earlier variables. For example, in $\mathbb{K}[x, y, z]$, the set $\{1, x, y, z, x^2, xy, xz, yz, y^2, yz, z^2\}$ is ordered from least to greatest in Lex order by:

$$1 < z < z^2 < y < yz < y^2 < x < xz < xy < x^2$$

We may use $<_{\text{lex}}$ to clarify the use of Lex order.

Example 7.3 (Graded Lexicographic order or GLex order). This order first prioritizes degree and then compares monomials of the same degree using Lex order. The set $\{1, x, y, z, x^2, xy, xz, yz, y^2, yz, z^2\}$ is ordered from least to greatest in GLex order by:

$$1 < z < y < x < z^2 < yz < y^2 < xz < xy < x^2$$

Example 7.4 (Graded Reverse Lexicographic order or GRevLex order). This order first prioritizes degree and then compares monomials of the same degree by reversing the order of the variables and then reversing the Lex order on these (see the next section for a more user-friendly definition!). The set $\{1, x, y, z, x^2, xy, xz, yz, y^2, yz, z^2\}$ is ordered from least to greatest in GRevLex order by:

$$1 < z < y < x < z^2 < yz < xz < y^2 < xy < x^2$$

7.1. Monomial orders by vectors. Let $v_1, \dots, v_n \in \mathbb{R}_{\geq 0}^n$ be linearly independent vectors. Let x^α, x^β be monomials in $\mathbb{K}[x_1, \dots, x_n]$, where $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. Define $x^\alpha > x^\beta$ if $\alpha \cdot v_1 > \beta \cdot v_1$ or if $\alpha \cdot v_1 = \beta \cdot v_1$ and $\alpha \cdot v_2 > \beta \cdot v_2$ or if $\alpha \cdot v_2 = \beta \cdot v_2$ and $\alpha \cdot v_3 > \beta \cdot v_3$, etc. A compact representation for the monomial order is by a matrix whose columns are the vectors v_1, \dots, v_n .

Example 7.5 (Lex order by vectors). Lexicographic order in three variables is determined by

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

So $x^a y^b z^c > x^{a'} y^{b'} z^{c'}$ if and only if $a > a'$ or $a = a'$ and $b > b'$ or $a = a', b = b'$, and $c > c'$. In general Lexicographic order is encoded by the identity matrix:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Example 7.6 (Graded Lex by vectors). Graded Lexicographic order is encoded by the following matrix:

$$\begin{bmatrix} 1 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

Example 7.7 (Graded Reverse Lex order by vectors). Graded Reverse Lexicographic order is encoded by the matrix which has 1's on and above the antidiagonal:

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

Example 7.8. Consider the polynomial ring $\mathbb{K}[x, y, z]$ and the vector $v = [\pi \ e \ \ln(2)]$. The entries of v are linearly independent over \mathbb{Q} . This means that for any $\alpha, \beta \in \mathbb{Z}^3$, $v \cdot \alpha \neq v \cdot \beta$. Hence v (by itself!) gives a monomial order on $\mathbb{K}[x, y, z]$. This order cannot be determined exactly by any three vectors $v_1, v_2, v_3 \in \mathbb{Z}_{\geq 0}^3$, but it can be approximated arbitrarily well by such vectors. For instance, take good rational approximations to π, e , and $\ln(2)$ (you can obtain these by continued fractions, for instance) and clear denominators.

There is a theorem (due to Robbiano) that every monomial order can be obtained by weight vectors.

Theorem 7.9 (Robbiano). *Every monomial order can be determined from an ordered list of vectors $v_1, \dots, v_n \in \mathbb{R}_{\geq 0}^n$ and can be approximated by an ordered list of vectors v_1, \dots, v_n .*

See Exercises 10 and 11 in Section 2.5 of Cox-Little-O'Shea, as well as the discussion after these exercises, for more discussion.

Example 7.10 (Product Order). Given a monomial order $<_1$ on $\mathbb{K}[x_1, \dots, x_r]$ and a monomial order $<_2$ on $\mathbb{K}[y_1, \dots, y_s]$, you can produce a monomial order $<_{1,2}$ on $\mathbb{K}[x_1, \dots, x_r, y_1, \dots, y_s]$ as follows:

$$x^{\alpha_1} y^{\alpha_2} > x^{\beta_1} y^{\beta_2}$$

if and only if $x^{\alpha_1} > x^{\beta_1}$ or $x^{\alpha_1} = x^{\beta_1}$ and $y^{\alpha_2} > y^{\beta_2}$. This is a *product order*. If A is an $r \times r$ matrix describing $<_1$ and B is an $s \times s$ matrix describing $<_2$, then the matrix describing $<_{1,2}$ is the block matrix:

$$\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

8. MULTIVARIATE DIVISION ALGORITHM

Recall that given polynomials $f, g \in \mathbb{K}[x]$, the division algorithm produces $f = Qg + R$ where $R = 0$ or $\deg(R) < \deg(f)$. Our goal in this section is to give a generalization of this to many variables using monomial orders. Here is how we formulate the multivariate division algorithm: let f_1, \dots, f_r be an *ordered* list of polynomials, and let g be another polynomial. The multivariate division algorithm gives an expression

$$g = f_1Q_1 + f_2Q_2 + \dots + f_rQ_r + R,$$

where no term of R is divisible by a leading term of f_1, \dots, f_r . We illustrate the algorithm with some examples and then formalize it.

Example 8.1. Use Lex order on $\mathbb{K}[x, y]$. Divide $x^2y + xy^2 + y^2$ by the list $\{f_1 = xy - 1, f_2 = y^2 - 1\}$. It's crucial to keep in mind the monomial order for the leading terms!

$$\begin{array}{rcl} Q_1: & & x + y \\ Q_2: & & 1 \\ xy - 1 & & \sqrt{x^2y + xy^2 + y^2} \\ y^2 - 1 & & \\ & & \frac{-(x^2y - x)}{xy^2 + x + y^2} \\ & & \frac{-(xy^2 - y)}{x + y^2 + y} \\ & & \frac{-(y^2 - 1)}{x + y + 1} \end{array}$$

The algorithm shows that $Q_1 = x + y$, $Q_2 = 1$, and $R = x + y + 1$ so $x^2y + xy^2 + y^2 = (x + y)(xy - 1) + (1)(y^2 - 1) + x + y + 1$.

Example 8.2. Reverse the order in the last example. Specifically, use Lex order on $\mathbb{K}[x, y]$ but divide $x^2y + xy^2 + y^2$ by the list $\{f_1 = y^2 - 1, f_2 = xy - 1\}$.

$$\begin{array}{rcl}
Q_1: & & x + 1 \\
Q_2: & & x \\
y^2 - 1 & & \sqrt{x^2y + xy^2 + y^2} \\
xy - 1 & & \\
\hline
& & -(x^2y - x) \\
& & xy^2 + x + y^2 \\
\hline
& & -(xy^2 - x) \\
& & xy^2 + x + y^2 \\
\hline
& & -(xy^2 - x) \\
& & 2x + y^2 \\
\hline
& & -(y^2 - 1) \\
& & 2x + 1
\end{array}$$

The algorithm shows that $Q_1 = x + 1$, $Q_2 = x$, and $R = 2x + 1$, so $x^2y + xy^2 + y^2 = (x + 1)(y^2 + 1) + (x)(xy - 1) + 2x + 1$.

The exact steps of this algorithm are as follows: start with a polynomial f and an ordered sequence (f_1, \dots, f_r) . Initialize $Q_1 = \dots = Q_r = 0$ and $R = f$. Starting with the largest term of R (under the monomial order) see whether any term of R is divisible by any of the lead terms of f_1, \dots, f_r (proceed in order!). If a term of R is divisible by a leadterm of some f_i , update Q_i as $Q_i = \text{LT}(R)/\text{LT}(f_i) + Q_i$, update R as $R = R - \text{LT}(R)/\text{LT}(f_i) \cdot f_i$. Repeat these steps until no term of R is divisible by any of the lead terms of the f_i .

The termination of the algorithm depends on the *well-ordering property*: namely, every subset of monomials has a least element under a monomial order (the proof of this comes from Dickson's Lemma and we will see it in the next section). Notice that after every division step (under the horizontal lines), a term has been replaced by terms which are smaller in the monomial order. Since we cannot have infinite decreasing chains of monomials, the set of all terms resulting from the division algorithm must be finite (i.e. the algorithm must terminate in a finite number of steps).

9. DICKSON'S LEMMA

Definition 9.1. Let $A \subset \mathbb{Z}^n$ be a subset of \mathbb{Z}^n and let $I(A) = \langle x^\alpha : \alpha \in A \rangle$ be the ideal of $\mathbb{K}[x_1, \dots, x_n]$ generated by the monomials with exponents from A . Then $I(A)$ is called a *monomial ideal*.

Lemma 9.2 (Dickson's Lemma.). *If $I \subset \mathbb{K}[x_1, \dots, x_n]$ is a monomial ideal, then there is a finite set of monomials m_1, \dots, m_k so that $I(A) = \langle m_1, \dots, m_k \rangle$.*

Proof. By induction on the number of variables. If $n = 1$, then a monomial ideal has the form $I(A) = \langle x^n : n \in A \rangle$ where $A \subset \mathbb{Z}$. By the well-ordering property of \mathbb{Z} , A has a least element, say k . Then clearly $x^k \mid x^n$ for every $n \in A$. So $I(A) = \langle x^k \rangle$.

Now suppose $n > 1$ and write $\mathbb{K}[x_1, \dots, x_{n-1}, x_n] = \mathbb{K}[x_1, \dots, x_{n-1}, y]$. If I is a monomial ideal in $\mathbb{K}[x_1, \dots, x_{n-1}, y]$ then each monomial in I can be written in

the form $x^\alpha y^k$. Let

$$J = \langle x^\alpha \mid x^\alpha y^k \in I \text{ for some } k \rangle.$$

By the induction assumption, $J = \langle m_1, \dots, m_k \rangle$ for some monomials $m_1, \dots, m_k \in \mathbb{K}[x_1, \dots, x_{n-1}]$.

By definition of J there exist monomials in I of the form $m_1 y^{a_1}, \dots, m_k y^{a_k}$. Let $g = \max\{a_1, \dots, a_k\}$.

Let $J_i = \langle x^\alpha \mid x^\alpha y^i \in I \rangle = \langle m_{i,1}, \dots, m_{i,k_i} \rangle$ (we use the induction hypothesis again) for integers $i \geq 0$. Put $I_i = \langle y^i m_{i,1}, \dots, y^i m_{i,k_i} \rangle$.

Now we claim $I = I_0 + I_1 + \dots + I_g$. Suppose $x^\alpha y^k \in I$. If $k \leq g$ then clearly $x^\alpha y^k \in I_0 + \dots + I_g$. Suppose $k > g$. Then x^α is divisible by some $x^\beta \in J_i$ for some $i \leq g$ (by the choice of g), hence $x^\beta y^i \in I$. But $i \leq g < k$, so $x^\beta y^i \mid x^\alpha y^k$, and $x^\alpha y^k \in I_0 + \dots + I_g$. \square

Definition 9.3. A total order of a set S is a well-ordering if every subset of S has a least element.

Proposition 9.4. Let $<$ be a total order on the monomials of $\mathbb{K}[x_1, \dots, x_n]$ satisfying $m_1 < m_2 \Rightarrow nm_1 < nm_2$. Then $<$ is a well-ordering if and only if 1 is the smallest monomial of $\mathbb{K}[x_1, \dots, x_n]$ under $<$.

Proof. Suppose $<$ is a well-ordering. Then the set of all monomials has a smallest element, call it m . If $m < 1$, then $m^2 < m$, contradicting that m is the smallest monomial. So 1 is the smallest element.

Now suppose 1 is the smallest monomial. Let A be a set of monomials of $\mathbb{K}[x_1, \dots, x_n]$ and let $I(A)$ be the ideal generated by A . By Dickson's lemma, $I(A) = \langle m_1, \dots, m_k \rangle$. Re-ordering if necessary, we assume $m_1 < m_2 < \dots < m_k$. We claim that m_1 is the smallest element of A . Let m be a monomial in A . Then $m \in I(A)$, so m is divisible by m_i for some $i = 1, \dots, k$. Hence $m_i \leq m$, but $m_1 \leq m_i$. So $m_1 \leq m$. \square

Corollary 9.5. If $<$ is a monomial order then there are no infinite decreasing sequences of monomials. In particular, the division algorithm terminates in a finite number of steps.

10. GRÖBNER BASES AND THE HILBERT BASIS THEOREM

Definition 10.1. Let $<$ be a monomial order on monomials of $\mathbb{K}[x_1, \dots, x_n]$. Let $I \subset \mathbb{K}[x_1, \dots, x_n]$ be an ideal. The *leading term ideal* of I is

$$\text{LT}_{<}(I) := \{\text{LT}_{<}(f) \mid f \in I\},$$

the ideal generated by leading terms of *all* polynomials in I .

Remark 10.2. Notice that $\text{LT}_{<}(I)$ is a monomial ideal. By Dickson's Lemma, $\text{LT}_{<}(I)$ is finitely generated. Hence there are $g_1, \dots, g_k \in I$ so that $\text{LT}_{<}(I) = \langle \text{LT}_{<}(g_1), \dots, \text{LT}_{<}(g_k) \rangle$.

Theorem 10.3 (Hilbert Basis Theorem). If $I \subset \mathbb{K}[x_1, \dots, x_n]$ is an ideal, then I is finitely generated.

Proof. Pick any monomial order $<$ and write $\text{LT}_{<}(I) = \langle \text{LT}_{<}(g_1), \dots, \text{LT}_{<}(g_k) \rangle$ as in the above remark. We claim that $I = \langle g_1, \dots, g_k \rangle$. To see this, take any $f \in I$

and use the division algorithm to divide f by the ordered list (g_1, \dots, g_k) . This gives an expression

$$f = Q_1g_1 + \dots + Q_kg_k + R,$$

where *no term* of R is divisible by a leading term of any g_1, \dots, g_k . Notice also that $R \in I$ since $R = f - (Q_1g_1 + \dots + Q_kg_k)$. But if $R \neq 0$, then $\text{LT}_<(R)$ is divisible by one of $\text{LT}_<(g_1), \dots, \text{LT}_<(g_k)$, since this is how we obtained g_1, \dots, g_k . Thus $R = 0$ and $f \in I$. \square

Definition 10.4. Let $I \subset \mathbb{K}[x_1, \dots, x_n]$ be an ideal and $<$ a monomial order on $\mathbb{K}[x_1, \dots, x_n]$. A Gröbner basis for I is a finite collection of polynomials $g_1, \dots, g_k \in I$ satisfying that

$$\text{LT}_<(I) = \langle \text{LT}_<(g_1), \dots, \text{LT}_<(g_k) \rangle.$$

Remark 10.5. From the proof of the Hilbert Basis theorem, if $g_1, \dots, g_k \in I$ and $\text{LT}_<(I) = \langle \text{LT}_<(g_1), \dots, \text{LT}_<(g_k) \rangle$, then $I = \langle g_1, \dots, g_k \rangle$. So a Gröbner basis of I is a set of generators of I with the additional property that the leading terms of the g_i generate the lead term ideal of I .

Remark 10.6. By Dickson's Lemma, Gröbner bases exist with respect to any monomial order.

Remark 10.7. A Gröbner basis for I depends on the monomial order.