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: $\mathbb{K}[x_1, \ldots, x_n]$.
Monomial: $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$
Set $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$.
Write x^α for $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$.
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 $\alpha = (\alpha_1, \ldots, \alpha_n)$, put $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

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

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

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). $F_f : \mathbb{K} \to \mathbb{K}$ evaluates to zero only at roots of f.

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

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

3. Affine Varieties

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

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

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 $\mathbb{F}_3^3$. There are nine points in $\mathbb{F}_3^3$. 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 $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$, it is interesting to consider the cardinality of $V(f_1, \ldots, f_r)$ when $f_1, \ldots, f_r$ 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 $V(f_1, \ldots, f_r)$ 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	$\lvert G\rvert$
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 (occuring 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 $A \cup B = V(\{f_i g_j : 1 \le i \le r, 1 \le j \le s\})$. □

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

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

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

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

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

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

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 $t_1, \ldots, t_n$ is a quotient $\frac{f}{g}$ where $f, g \in \mathbb{K}[t_1, \ldots, t_n]$. 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 $t_1, \ldots, t_n$ is denoted $\mathbb{K}(t_1, \ldots, t_n)$.

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

Example 4.5 (Tangent surfaces of curves)**.** The *twisted cubic* is parametrized as $x = t, y = t^2, z = t^3$, $-\infty < t < \infty$. It's 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:

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

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:

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

We can extract from $\operatorname{rref}(M)$ 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 $\mathbb{K}(t_1, \ldots, t_n)$ 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

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

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 $\frac{f_1}{g_1}, \frac{f_2}{g_2}, \ldots, \frac{f_n}{g_n} \in \mathbb{K}(t_1, \ldots, t_n)$ such that

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

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 $V(f_1, \ldots, f_r)$ for some polynomials $f_1, \ldots, f_r$. 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 $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an *ideal* if it satisfies the following two properties:

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

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

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

Proof. Exercise. □

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

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

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

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

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

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

Proposition 5.6. *The variety defined by $f_1, \ldots, f_r$ is the same as the variety defined by the ideal $I = \langle f_1, \ldots, f_r \rangle$. In symbols, $V(f_1, \ldots, f_r) = V(\langle f_1, \ldots, f_r \rangle)$. 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 $\langle T \rangle = \langle f_1, \ldots, f_r \rangle$ for some set of polynomials $f_1, \ldots, f_r$. Again by Proposition 5.6, $V(\langle f_1, \ldots, f_r \rangle) = V(f_1, \ldots, f_r)$. 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

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

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 $\bar{S} = \mathbb{R}$.

Example 5.15. Consider $S = \{(1,0),(0,1),(0,0)\} \subset \mathbb{R}^2$. Then $I(S)$ has no linear polynomials (since the points are not on a line). $I(S)$ has three linearly independent quadrics. A possible basis for this space of quadrics is $xy, x(x+y-1)$, and $y(x+y-1)$. Check that these are linearly independent! In fact, $I(S)$ is generated by these three quadrics, but it might be difficult to prove this until we have more tools (try it!).

Definition 5.16. If $T \subset \mathbb{K}[x_1,\ldots,x_n]$, then define $\bar{T} = I(V(T))$.

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

(1) $T \subset \bar{T}$
(2) $I(V(\bar{T})) = \bar{T}$.

Proposition 5.18. *Suppose $V, W \subset \mathbb{K}[x_1,\ldots,x_n]$. Then $\bar{V} \subset \bar{W}$ if and only if $I(V) \supset I(W)$ and $\bar{V} = \bar{W}$ if and only if $I(V) = I(W)$.*

By Remark 5.11, affine varieties can be though 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 $\mathbb{K}[x_1,\ldots,x_n]$. We will come back to this question. Let's close with two fundamental questions.

(1) Given an ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$, can we find finitely many polynomials $f_1,\ldots,f_r$ so that $I = \langle f_1,\ldots,f_r\rangle$? 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 $I = \langle f_1,\ldots,f_r\rangle$ and $g \in \mathbb{K}[x_1,\ldots,x_n]$, 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.

6. Polynomial rings in one variable over a field

We will describe the structure of ideals in the ring $\mathbb{K}[x]$. Suppose $f \in \mathbb{K}[x]$. Then $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ with $a_0,\ldots,a_d$. The *leading term* of $f(x)$ is $\mathrm{LT}(f) = a_d x^d$ 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.

$$\begin{array}{r|l} & x^2 - x + 4 \\ \hline x+1 & x^3 \quad\quad + 3x + 2 \\ & -x^3 - x^2 \\ \hline & \quad -x^2 + 3x \\ & \quad\; x^2 + x \\ \hline & \quad\quad\; 4x + 2 \\ & \quad\quad -4x - 4 \\ \hline & \quad\quad\quad -2 \end{array}$$

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 $\mathrm{LT}(g)|\mathrm{LT}(R)$ **do:**
$Q = Q + \frac{\mathrm{LT}(R)}{\mathrm{LT}(g)}$
$R = R - \frac{\mathrm{LT}(R)}{\mathrm{LT}(g)} g$
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 $R = R'$. □

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). □

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 $I = \langle h \rangle$. □

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 $p \mid h$. □

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 $\deg(f) \geq \deg(g)$).

$$\begin{aligned}
f &= gQ_1 + R_1 && \deg(g) > \deg(R_1) \text{ or } R_1 = 0 \\
g &= R_1Q_2 + R_2 && \deg(R_1) > \deg(R_2) \text{ or } R_2 = 0 \\
R_1 &= R_2Q_2 + R_3 && \deg(R_2) > \deg(R_3) \text{ or } R_3 = 0 \\
&\vdots \\
R_{k-2} &= R_{k-1}Q_{k-1} + R_k \\
R_k &= 0
\end{aligned}$$

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 $f_1, \ldots, f_r$ is a polynomial h satisfying:

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

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

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