Algebraic Geometry

Diane Maclagan
Notes by Florian Bouyer

Contents

Books:

- Hasset: *Introduction to Algebraic Geometry*
- Cox, Little, O'shea *Ideals, Varieties and Algorithm*

1 Introduction and Basic Definitions

Algebraic geometry starts with the study of solutions to polynomial equations.
e.g.: $\{(x,y) \in \mathbb{C}^2 : y^2 = x^3 - 2x + 1\}$ (an elliptic curve)
e.g.: $\{(x,y,w,z) \in \mathbb{C}^4 : x+y+z+w = 0, x+2y+3z = 0\}$ (Subspace of $\mathbb{C}^4$)

The goals of this module is to understand solutions to polynomial equations "*varieties*". That is properties, maps between them, how to compute them and examples of them. Why would we do that? Because varieties occurs in many different parts of mathematics:
e.g.: A robot arm: any movement can be described by polynomial equations (and inequalities)
e.g.: $\{(x,y) \in (\mathbb{Q} \setminus \{0\})^2 : x^4 + y^4 = 1\} = \emptyset$ (by Fermat's Last Theorem)

Algebraic geometry seeks to understand these spaces using (commutative) algebra.

Definition 1.1. Let S be the ring of polynomial with coefficients in a field k.

Notation. $S = k[x_1, \ldots, x_n]$

Definition 1.2. The *affine space* is $\mathbb{A}^n = \{(y_!, \ldots, y_n) : y_i \in k\}$. That is k^n without the vector space structure.

Definition 1.3. Given polynomial $f_1, \ldots f_r \in S$ the *affine variety* defined by the f_i is $V(f_1, \ldots, f_r) = \{y = (y_1, \ldots, y_n) \in \mathbb{A}^n : f_i(y) = 0 \, \forall i\}$

Example. $V(x^2 + y^2 - 1) =$ circle of radius 1

Note. Two different sets of polynomials can define the same varieties.

Example. $V(x+y+z, z+2y) = V(y-z, x+2z) = \{(2a, -a, -a) : a \in k\}$

Recall: The ideal generated by $f_1, \ldots, f_r \in S$ is $I = \langle f_1, \ldots, f_r \rangle = \{\sum_{i=1}^r h_i f_i : h_i \in S\}$. It is closed under addition and multiplication by elements of S.

Lemma 1.4. *$V(f_1, \ldots, f_r) = \{y \in \mathbb{A}^n : f(y) = 0 \forall f \in \langle f_1, \ldots, f_r \rangle\}$. Thus if $\langle f_1, \ldots, f_r \rangle = \langle g_1, \ldots g_s \rangle$ then $V(f_1, \ldots, f_r) = V(g_1, \ldots, g_s)$.*

Proof. We show the inclusion both ways:
$\subseteq$: Let $y \in V(f_1, \ldots, f_r)$. Then $f_i(y) = 0 \forall i$, so let $f = \sum_{i=1}^r h_i f_i \in \langle f_1, \ldots, f_r \rangle$, then $f(y) = 0$.
$\supseteq$: Conversely if $f(y) = 0 \forall f \in \langle f_1, \ldots, f_r \rangle$ then $f_i(y) = 0 \, \forall i$. Hence $y \in V(f_1, \ldots, f_r)$. □

Notation. If $I = \langle f_1, \ldots, f_r \rangle$ we write $V(I)$ for $V(f_1, \ldots, f_r)$.

Definition. Let $X \subseteq \mathbb{A}^n$ be a set. The *ideal of function vanishing on X* is $I(X) = \{f \in S : f(y) = 0 \forall y \in X\}$

Example. $X = \{0\} \subseteq \mathbb{A}^1$. Then $I(X) = \langle x \rangle$.

Note that $I \subseteq I(V(I))$. To see this we have $f \in I \Rightarrow f(y) = 0 \, \forall y \in V(I) \Rightarrow f \in I(V(I))$. On the other hand we don't have always equality.
e.g., $I = \langle x^2 \rangle \in k[x]$, then $V(I) = \{0\} \subseteq \mathbb{A}^n$, so $I(V(I)) = \langle x \rangle \neq \langle x^2 \rangle$.
e.g., $k = \mathbb{R}$ and $I = \langle x^2 + 1 \rangle$. Then $V(I) = \emptyset$ so $I(V(I)) = \langle 1 \rangle = \mathbb{R}[x] \neq I^2$.

2 Grobner Bases

Question: Given $f_1, \dots, f_r, f \in S$, how can we decide if $f \in \langle f_1, \dots, f_r \rangle$? That is: given generators for $I(X)$ how can we decide if f vanishes on X?

Example 2.1.

- $n = 1, k = \mathbb{Q}$. Is $\langle x^2 - 3x + 2, x^2 - 4x + 4 \rangle = \langle x^3 - 6x^2 + 12x - 8, x^2 - 5x + 6 \rangle = \langle x - 2 \rangle$? Yes since we are in a PID so we can use Euler's algorithm to find the generator. This is a solved problems

- Any n and $f_1, \dots, f_r$ are linear

  - Is $y - z \in \langle x + y + z, x + 2y \rangle$? Yes.
  - Is $5x_1 + 3x_2 - 7x_4 + 8x_5 \in \langle x_1 + x_2 + x_3 + x_4 + x_5, 3x_1 - 7x_4 + 9x_5, 2x_1 + 3x_4 \rangle = \langle f_1, f_2, f_3 \rangle$? If $f \in \langle f_1, f_2, f_3 \rangle$ then $f = af_1 + bf_2 + cf_3$ for $a, b, c \in k$. So the question now becomes: is

$$(5, 3, 0, 7, 8) \in \text{row} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 3 & 0 & 0 & -7 & 9 \\ 2 & 0 & 0 & 3 & 0 \end{pmatrix}?$$

To solve this we use Gaussian elimination from Linear Algebra

As we seen from the above examples, we need a common generalization. This is the Theory of Grobner bases.

Definition 2.2. A *term order* (or *monomial order*) is a total order on the monomials (polynomial in one variable) is $S = k[x_1, \dots, x_n]$ such that:

1. $1 < x^u$ for all $u \neq 0$
2. $x^u < x^v \Rightarrow x^{u+w} < x^{v+w}$ for all $w \in \mathbb{N}^n$.

Several term orders:

Lexicographic order $X^u < X^v$ if the first non-zero element of $v - u$ is positive.

Example. $f = 3x^2 - 8xz^9 + 9y^{10}$. If $x > y > z$, then $x^2 > xz^9 > y^{10}$ (since if $v = (2, 0, 0), u = (1, 0, 9)$ then $v - u = (1, 0, -9)$.

Degreelicographic order $X^u < X^v$ if $\begin{cases} \deg(X^u) < \deg(X^v) \\ X^u <_{\text{lex}} X^v & \text{if } \deg(X^u) = \deg(X^v) \end{cases}$.

Example. $f = 3x^2 - 8xz^9 + 9y^{10}$. Then $xz^9 > y^{10} > x^2$.

Reverse lexicographic order (revlex) $X^2 < X^v$ is $\begin{cases} \deg(X^u) < \deg(X^v) \\ \text{the last non-zero entry of } v - u \text{ is negative} & \text{if } \deg(X^u) = \deg(X^v) \end{cases}$

Example. $f = 3x^2 - 8xz^9 + 9y^{10}$. Then $y^{10} > xz^9 > z^2$.

Definition 2.3. Given a polynomial $f = \sum c_u X^u \in S$ and a term order $<$, the *initial term* of f is $c_v X^v$ with $X^v > X^u$ for all u and $c_v \neq 0$. This is denoted $\text{in}_<(f)$.

Definition 2.4. The *initial ideal* of I with respect to $<$ is $\text{in}_<(I) = \langle \text{in}_<(f) : f \in I \rangle$

Warning: If $I = \langle f_1, \dots, f_r \rangle$ then $\text{in}_<(I)$ is not necessarily generated by $\langle \text{in}_<(f_1), \dots \text{in}_<(f_r) \rangle$. e.g., Let $I = \langle x + y + z, x + 2y \rangle$ and let the term ordering be $x > y > z$. Then $\text{in}_<(I) = \langle x, y \rangle$.

Definition 2.5. A set $\{g_1, \dots g_s\}$ is a *Grobner basis* for I if $\{g_1, \dots, g_s\} \subseteq I$ and $\text{in}_<(I) = \langle \text{in}_<(g_1), \dots, \text{in}_<(g_s) \rangle$.

The point of this is that long division by a Grobner basis decides the ideal membership problem, that is, is $f \in \langle f_1, \dots, f_r \rangle$?

Definition 2.6. A *monomial ideal* is an ideal $I \subseteq S$ generated by monomials X^u.

Lemma 2.7. *Let I be a monomial ideal, $I = \langle X^u : u \in A \rangle$ for some $A \subseteq \mathbb{N}^n$. Then:*

1. *$X^v \in I$ if and only if $X^u | X^v$ for some $u \in A$.*
2. *If $f = \sum c_v X^v \in I$ then each X^v with c_v non-zero is divisible by some X^u for $U \in A$, hence they lies in I.*

Proof. Note that part 1. is a special case of part 2.

Since $f \in I$ we can write $f = \sum h_u X^u$ with $u \in A$, $h_u \in S$ and all but finitely many are 0. Let us expand the RHS as a sum of monomials. Then each term is a multiple of some X^u so lies in I, hence the same is true for the terms of f. □

Theorem 2.8 (Dickson's Lemma)**.** *Let $I = \langle X^u : u \in A \rangle$ for some set $A \subseteq \mathbb{N}^n$, then there exists $a_1, \dots a_s \in A$ with $I = \langle X^{a_1}, \dots, X^{a_s} \rangle$.*

Proof. The proof is by induction on n.

$n = 1$: We have $I = \langle X^u \rangle$ for $U = \min\{U : U \in A\}$, this uses the fact that $\mathbb{N}$ is well ordered

$n > 1$: Name the variables of the polynomial ring $x_1, \dots, x_{n-1}, y$.. Let $J = \left\langle X^u : \exists j \geq 0 \text{ with } x^u y^j \in I \right\rangle \subseteq k[x_1, \dots, x_{n-1}]$. By induction hypothesis $J = \langle X^{a_{i_1}}, \dots X^{a_{i_s}} \rangle$ where $(a_{i_j}, m_j) \in A$ for some $m_j \in \mathbb{N}$. Let $m = \max(m_j)$. For $0 \leq l \leq m-1$, let $J_l = \left\langle X^u : x^u y^l \in I \right\rangle \subseteq k[x_1, \dots, x_{n-1}]$. So again by induction we have that $J_l = \left\langle x^{b_{l1}}, \dots, x^{b_{r(l)}} \right\rangle$ where $b_{ls} \in \mathbb{N}^{n-1}$ and $x^{b_{ls}} y^l \in I$. We now claim that $I = \left\langle x^{b_{ls}} y^l : 0 \leq l \leq m-1, 1 \leq s \leq r(l) \right\rangle + \langle x^{a_{ij}} y^{m_j} : 1 \leq j \leq s \rangle$. Indeed if $x^u y^j \in I$, if $j < m$ then $x^u \in J_j$ so $x^{b_{js}} | x^u$ for some b_{js} so $x^{b_{js}} y^j | x^u y^j$. If $j \geq m$ then $x^u \in J$, so there is a_i with $X^{a_i} | X^u$ so $X^{a_i} y^{m_i} | X^u y^j$. In particular, every monomial generator of I lies in $\left\langle x^{b_{ls}} y^l, x^{a_{ij}} y^{m_j} \right\rangle$ so the ideals are equal and I is finitely generated. For each of the finite number of generators we can find $a_i \in A$ with X^{a_i} dividing the generator (using the previous lemma).

□

Corollary 2.9. *A term order is well ordered (every set of monomials has a least element)*

Proof. If not, there would be an infinite chain $X^{u_1} > X^{u_2} > \dots$. Let $I = \langle X^{u_i} : i \geq 1 \rangle \subseteq k[x_1, \dots, x_n]$, then by Dickson's lemma $I = \langle X^{u_{i_1}}, \dots, X^{u_{i_s}} \rangle$ for some $i_1 < i_2 < \dots < i_s$. In particular for $j \geq i_s$ there exists l such that $X^{u_{i_l}} | X^{u_j}$. Thus $X^{u_j} = X^{u_{i_l}} X^w$, but then $X^{u_{i_l}} < X^{u_j}$ because $1 < X^W$. This is a contradiction. □

Corollary 2.10. *Let I be an ideal in $k[x_1, \dots, x_n]$ then there exists $g_1, \dots g_s \in I$ with $\mathrm{in}_<(I) = \langle \mathrm{in}_<(g_1), \dots, \mathrm{in}_<(g_s) \rangle$. Hence a Grobner basis exists.*

Proof. By definition $\mathrm{in}_<(I) = \langle \mathrm{in}_<(f) : f \in I \rangle$. By Disckson's lemma, there exists $g_1, \dots, g_s \in I$ with $\langle \mathrm{in}_<(g_1), \dots, \mathrm{in}_<(g_s) \rangle = \mathrm{in}_<(I)$. □

2.1 The Division Algorithm

Input: $f_1, \dots, f_s, f \in S$, $<$ the term order
Output: Expression of the form $\sum_{i=1}^s h_i f_i + r$ where $h_i \in S$ and $r = \sum c_u X^u$ with $\{c_u \neq 0 \Rightarrow$ X^u is not divisible by $\mathrm{in}_<(f_i) \forall i\}$, such that if $\mathrm{in}_<(f) = c_u X^u, \mathrm{in}_<(h_i f_i) = c_{v_i} X^{v_i}$ then $X^u \geq X^{v_i} \forall i$.
Step 1: Initialize $h_1 = \dots = h_s = 0, r = 0, p = f$.
Step 2: While $p \neq 0$ do:
    $i = 1$
    Divisionoccured = false
    While $i \leq s$ and Divisionoccured = false do:
        If $\mathrm{in}_<(f_i) | \mathrm{in}_<(p)$ then:
            $h_i = h_i + \frac{\mathrm{in}_<(p)}{\mathrm{in}_<(f_i)}$
            $p = p - \frac{\mathrm{in}_<(p)}{\mathrm{in}_<(f_i)} f_i$

```
                    Divisionoccured = true
                Else:
                    i = i + 1
                If Divisionoccured = false then:
                    r = r + in_<(p)
                    p = p - in_<(p)
Step 3: Output: h_1, ..., h_s, r.
```

Example 2.11.

```
Input: f_1 = x + y + z, f_2 = 3x - 2y, f = 5y + 3z, < lex (x < y < z)
Step 1: h_1 = 0, h_2 = 0, r = 0, p = 5y + 3z.
Step 2: i = 1
        Divisionoccured = false
        does in_<(f_1)|in_<(p)? Yes:
            h_1 = 0 + 3
            p = 5y + 3z) - 3 · (x + y + z) = -3x + 2y
            Divisionoccured = true
Step 2: i = 1
        Divisionoccured = false
        does in_<(f_1)|in_<(p)? No:
        i = 2
        does in_<(f_2)|in_<(p)? Yes:
            h_2 = 0 + -1
            p = -3x + 2y + (-1) · (3x - 2y) = 0
            Divisionoccured = true
Step 3: Output: h_1 = 3, h_2 = -1, r = 0
```

Note that the division algorithm depends on the ordering. (In the above example if $x > y > z$ then the output is $h_1 = h_2 = 0$ and $r = 5y + 3z$)

Proposition 2.12. *The above algorithm terminates with the correct output .*

Proof. As each stage the initial term $\mathrm{in}_<(p)$ decreases with respect to $<$. Since $<$ is a well-order, this cannot happen an infinite number of times, hence the algorithm must terminate.

At each stage we have $f = p + \sum h_i f_i + r$, where $h_i f_i$ and r satisfy the condition, so when it outputs with $p = 0$, the output has the desired correct form. □

Proposition 2.13. *If $\{g_1, \dots, g_s\}$ is a Grobner basis for I with respect to $<$, then $f \in I$ if and only if the division algorithm outputs $r = 0$.*

Proof. The division algorithm writes $f = \sum h_i g_i + r$, where no monomial in r is divisible by $\mathrm{in}_<(g_i)$. Thus $f \in I$ if and only if $r \in I$. Now if $r \neq 0$ then $\mathrm{in}_<(r) \notin \mathrm{in}_<(I) = \langle \mathrm{in}_<(g_1), \dots, \mathrm{in}_<(g_s) \rangle$, so $r \notin I$. Hence $r = 0$ if and only if $r \in I$. □

Corollary 2.14. *If $\{g_1, \dots, g_s\}$ is a Grobner basis for I then $I = \langle g_1, \dots, g_s \rangle$*

Proof. We have $\langle g_1, \dots, g_s \rangle \subseteq I$ by the definition of Grobner basis. If $f \in I$, then we divide f by $g_1, \dots, g_s$ to get $f = \sum h_i g_i + r$, but $r = 0$. So we have $f \in \langle g_1, \dots, g_s \rangle$, hence $I \subseteq \langle g_1, \dots, g_s \rangle$. □

Corollary 2.15 (Hilbert Basis Theorem)**.** *Let $I \subseteq S$ be an ideal. Then I is finitely generated.*

Proof. We know that I has a finite Grobner basis (since monomial ideals are finitely generated). By the previous corollary, this Grobner basis generates I □

Definition 2.16. A ring R is *Noetherian* if all its ideals are finitely generated.

Hence the Hilbert basis theorem says S is Noetherian. Note that there is a standard algorithm (the Buchberger algorithm) to compute Grobner bases.

Definition 2.17. A *reduced Grobner basis* for I with respect to $<$, is a Grobner basis of I which satisfies:

1. Coefficients of $\text{in}_<(g_i)$ is 1
2. No $\text{in}_<(g_i)$ divides any other-way
3. No $\text{in}_<(g_i)$ divides any other term of g_j.

Such a reduced Grobner basis exists and is unique. With this we can check whether two ideals are equal. To do this we fix a term order and compute a reduced Grobner basis for I and J.

3 Zariski Topology

Recall that a topological space is a set X and a collection $\theta = \{U\}$ of subsets of X called open sets, satisfying:

1. $\emptyset \in \theta$
2. $X \in \theta$
3. If $U, U' \in \theta$ then $U \cap U' \in \theta$
4. If $U_\alpha \in \theta$ for $\alpha \in A$, then $\cup_\alpha U_\alpha \in \theta$.

A set Z is closed if its compliment is open.

Definition 3.1. The *Zariski Topology* on $\mathbb{A}^n$ has close set $V(I)$ for $I \subseteq S$ an ideal.

Example. In $\mathbb{A}^1$, under the Zariski Topology, the closed sets are finite set, $\mathbb{A}^1$ or $\emptyset$. ($\mathbb{A}^1 = V(0)$ and $\emptyset = V(S)$)

Recall: If I, J are ideals in S then $I + J = \{i + j : i \in I, j \in J\}$, while $IJ = \langle ij : i \in I, j \in J\rangle$. In terms of generators, if $I = \langle f_1, \ldots, f_s\rangle$ and $J = \langle g_1, \ldots, g_r\rangle$ then $I + J = \langle f_1, \ldots, f_s, g_1, \ldots, g_s\rangle$ and $IJ = \langle f_i g_j : 1 \leq i \leq s, 1 \leq j \leq r\rangle$.

Proposition 3.2. *Let $X = V(I)$ and $Y = V(J)$ be two varieties in $\mathbb{A}^n$ then:*

- $X \cap Y = V(I + J)$
- $X \cup Y = V(I \cap J) = V(IJ)$

Proof.

- Let $y \in X \cap Y$. Then $f(y) = 0$ for all $f \in I$ and $g(y) = 0$ for all $g \in J$. So $(f + g)(y) = 0$ for all $f \in I$ and $g \in J$. Hence by definition $y \in V(I + J)$.
  Conversely: let $y \in V(I + J)$, then $h(y) = 0$ for all $h = f + 0$ with $f \in I$, hence $y \in V(I)$. Similarly $h(y) = 0$ for all $h = 0 + g$ with $g \in J$, hence $y \in V(J)$. So $y \in X \cap Y$.
- Let $y \in X \cup Y$. Then $y \in X$ or $y \in Y$. If $y \in X$ then $f(y) = 0 \forall f \in I$, so $f(y) = 0 \forall f \in I \cap J$, hence $y \in V(I \cap J)$. Similarly if $y \in Y$ then $g(y) = 0 \forall g \in I$, so $g(y) = 0 \forall g \in I \cap J$, hence $y \in V(I \cap J)$.
  Let $y \in V(IJ)$. Then $h(y) = 0 \forall h = fg$ with $f \in I, g \in J$. Thus $h(y) = f(y)g(y) \forall f \in I, g \in J$. Suppose $y \notin Y$, that is there exists $g \in J$ with $g(y) \neq 0$, then $f(y) = 0 \forall f \in I$, hence $y \in V(I) = X$. Thus we have $y \in X \cup Y$. So $V(IJ) \subseteq X \cup Y$.
  Note that $I \cap J \supseteq IJ$ so $V(I \cap J) \subseteq V(IJ)$ (This follows from the general fact $I \subseteq J \Rightarrow V(J) \subseteq V(J)$)
  We have shown $V(I \cap J) \subseteq V(IJ) \subseteq X \cup Y \subseteq V(I \cap J)$, thus they are all equal.

$\square$

In fact, if $\{X_\alpha : \alpha \in A\}$ is a collection of varieties in $\mathbb{A}^n$ with $X_\alpha = V(I_\alpha)$, then $\cap_\alpha X_\alpha = V(\langle \cup I_\alpha \rangle)$. Challenge question: What goes wrong with arbitrary union.

Corollary 3.3. *The Zariski topology is a topology on $\mathbb{A}^n$.*

Note: This topology is weird compare to the Euclidean topology, for example it is not Haussdorf and open sets are dense.

3.1 Morphism

Definition 3.4. A *morphism* is a map $\phi : \mathbb{A}^n \to \mathbb{A}^m$ with $\phi(y_1, \ldots, y_n) = (\phi_1(y_1, \ldots, y_n), \ldots, \phi_m(y_1, \ldots, y_n))$ where $\phi \in k[x_1, \ldots, x_n]$.

Example. $\phi : \mathbb{A}^2 \to \mathbb{A}^2$ defined by $\phi(x, y) = (x^2 - y^2, x^2 + 2xy + 3y^2)$.

Morphism plays the role of continuous functions in topology. Questions: are all continuous functions morphism? No.

Example. $f(x) = \begin{cases} x+1 & x \notin \mathbb{Q} \\ x & x \in \mathbb{Q} \end{cases}$. This is a continuous function in the Zariski topology. We don't want this, hence why we restrict to morphism.

Definition 3.5. For $f \in k[z_1, \dots, z_m]$, $\phi : \mathbb{A}^n \to \mathbb{A}^m$, the function $f \circ \phi \in k[x_1, \dots, x_n]$ is called the *pullback* if f by ϕ.

Note. $\phi^* f = f \circ \phi$.

Recall: a k-algebra is a ring R containing the field k. A k-algebra homomorphism is a ring homomorphism ϕ with $\phi(a) = a \, \forall a \in k$.

Lemma 3.6. *The map $\phi^* : k[z_1, \dots, z_m] \to k[x_1, \dots, x_n]$ is a k-algebra homomorphism*

- $\phi^*(1) = 1$
- $\phi^*(0) = 0$
- $\phi^*(a) = a \, \forall a \in k$
- $\phi^*(fg) = \phi^*(f)\phi^*(g)$
- $\phi^*(f+g) = \phi^*(f) + \phi^*(g)$

Proof. Exercise □

Note: The polynomial ring is the ring of morphism from $\mathbb{A}^n$ to $\mathbb{A}^1$.

Definition 3.7. The coordinate ring $k[X]$ of a variety $X = V(I) \subseteq \mathbb{A}^n$ is the ring of polynomial functions from X to $\mathbb{A}^1$.

Equivalently: $k[X] = \{f \in k[x_1, \dots, x_n]\}/\sim$ where $f \sim g$ if $f(y) = g(y)$ for all $y \in X$.

Note. $f(y) = g(y) \, \forall y \in X$ if and only if $(f-g)(y) = 0 \, \forall y \in X$, that is, if and only if $f - g \in I(X)$. So $k[X] = k[x_1, \dots, x_n]/I(X)$ and in particular $k[X]$ is a ring.

Example.

- $X = V(x^2 + y^2 - 1)$ then $k[X] = k[x,y]/\left\langle x^2 + y^2 - 1 \right\rangle$
- $X = V(x^3) \subseteq \mathbb{A}^1$ then $k[X] = k[x]/\langle x \rangle \cong k$.

Definition 3.8. Fix $X = V(I) \subseteq \mathbb{A}^n$. Two morphism $\phi, \psi : \mathbb{A}^n \to \mathbb{A}^m$ *are equal in* X if the induced pullback $\phi^*, \psi^* : k[z_1, \dots, z_m] \to k[Z] = k[x_1, \dots, x_n]/I(X)$ are equal.

Definition 3.9. A morphism $\phi : X \to \mathbb{A}^n$ is an equivalence class of such morphism.

Example 3.10. Let $X = V(x^2 + y^2 - 1)$, $\psi : \mathbb{A}^2 \to \mathbb{A}^1$ defined by $\psi(x,y) = x^4$ and $\phi : \mathbb{A}^2 \to \mathbb{A}^1$ defined by $\phi(x,y) = (y^2-1)^2$. We claim that $\phi = \psi$ on X since $\psi^* : k[z] \to k[x,y]$ is defined by $z \mapsto x^4$ while $\phi^* : k[z] \to k[x,y]$ is defined by $z \mapsto (y^2-1)^2$. But $k[X] = k[x,y]/(x^2+y^2-1)$, and in there $x^4 = (y^2-1)^2$, hence $\phi^* = \psi^*$.

Lemma 3.11. *If $\phi, \psi : \mathbb{A}^n \to \mathbb{A}^m$ are equal on X then $\phi(y) = \psi(y)$ for all $y \in X$.*

Proof. If $\phi(y) \neq \psi(y)$ for some $y \in X$ then they differ in some coordinate i. Then $z_i(\phi(y)) \neq z_i(\psi(y))$, so $\phi^* z_i(y) \neq \psi^* z_i(y)$. Hence $\phi^* z_i - \psi^* z_i \notin I(X)$, so the pullback homomorphism ϕ^* and ψ^* are different. □

Definition 3.12. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be varieties. A morphism $\phi : X \to Y$ is a morphism $\phi : X \to \mathbb{A}^m$ with $\phi(X) \subseteq Y$.

Example. Let $X = \mathbb{A}^1$ and $Y = V(cy - y^2) \subseteq \mathbb{A}^3$ and let $\phi : \mathbb{A}^1 \to \mathbb{A}^3$ be defined by $\phi(t) = (t, t^2, t^3)$. Then $\phi^* : k[x,y,z] \to k[t]$ is defined by $x \mapsto t$, $y \mapsto t^2$ and $z \mapsto t^3$. Since $tt^3 - (t^2)^2 = 0$, $\phi(\mathbb{A}^1) \subseteq Y$, so ϕ is a morphism from $\mathbb{A}^1 \to Y$.

Proposition. *Let $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$ be varieties. Any morphism $\phi : X \to Y$ induces a k-algebra homomorphism $\phi^* : k[Y] \to k[X]$. Conversely given a k-algebra homomorphism from $k[Y] \to k[X]$ is ϕ^* for some morphism $\phi : X \to Y$.*

Proof. Let $\phi : X \to Y$ be a morphism. Since $\phi(X) \subseteq Y$ we have $f \circ \phi(x) = 0 \, \forall x \in X$ and $f \in I(Y)$. Hence $\phi^* f \in I(X) \, \forall f \in I(Y)$, therefore the induced map $\phi^* : k[z_1, \dots, z_m] \to k[X] = k[x_1, \dots, x_n]/I(X)$ factors through $k[Y]$. So given a morphism $\phi : X \to Y$ we get $\phi^* : k[Y] \to k[X]$.

Conversely given a k-algebra homomorphism $\alpha : k[Y] \to k[X]$ it suffices to find a k-algebra homomorphism $\widetilde{\alpha}^* : k[z_1, \dots, z_m] \to k[x_1, \dots, x_n]$ for which we have a commutating diagram

$$\begin{tikzcd}
k[z_1, \dots, z_m] \arrow[r, "\widetilde{\alpha}^*"] \arrow[d, "i_Y^*"'] & k[x_1, \dots, x_n] \arrow[d, "i_X^*"] \\
k[Y] \arrow[r, "\alpha"] & k[X]
\end{tikzcd}$$

Then $\widetilde{\alpha}$ will be a morphism $\mathbb{A}^n \to \mathbb{A}^m$ with $\widetilde{\alpha}(X) \subseteq Y$. We construct such $\widetilde{\alpha}^*$ as follow. Let g_i be any polynomial in $k[x_1, \dots, x_n]$ with $i_X^*(g_i) = \alpha(i_Y^*(z_i))$. Set $\widetilde{\alpha}^* = g_i$ and extend as a k-algebra homomorphism. (g_i exists since the map i_X^* is surjective). This defines $\widetilde{\alpha}^* : k[z_1, \dots, z_m] \to k[x_1, \dots, x_n]$ and $i_X^* \circ \widetilde{\alpha}^*(z_1) = \alpha \circ i_Y^*(z_i)$ by construction, hence the diagram commutes. $\square$

Example 3.13. Let $\phi^* : k[t] \to k[x, y, z]/(x^2 - y, x^3 - z)$. Then $\phi^*(t) = x$ and $\phi^*(t) = x + x^2 - y$ is the same. This is ϕ^* for $\phi : V(x^2 - y, x^3 - z) \to \mathbb{A}^1$ defined by $\phi(x, y, z) = x$ (or $\phi(x, y, z) = x + x^2 - y$ as while they are different morphism they agree on X)

So to sum up: Morphism $\phi : X \to Y$ are the same as k-algebra homomorphism of the coordinate rings $\phi^* : k[Y] \to k[X]$. note that the homomorphism goes the other way! (contragradient).

Exercise 3.14. If $X \overset{\phi}{\to} Y \overset{\psi}{\to} Z$ with $X \overset{\alpha}{\to} Z$. Then $\alpha^* : k[Z] \to k[X]$ is $\phi^* \circ \psi^*$.

Definition 3.15. An *isomorphism* of affine varieties is a morphism $\phi : X \to Y$ for which there is a morphism $\phi^{-1} : Y \to X$ with $\phi \circ \phi^{-1} = \mathrm{id}_Y$ and $\phi^{-1} \circ \phi = \mathrm{id}_X$.

An *automorphism* of an affine variety is an isomorphism $\phi : X \to X$.

WARNING: A morphism that is a bijection needs not be an isomorphism.

3.2 Images of varieties under morphism

That is, given $\phi : \mathbb{A}^n \to \mathbb{A}^m$ what is $\phi(X)$?

Warning: $\phi(X)$ needs not to be a variety. For example $X = V(xy - 1) \subseteq \mathbb{A}^1$ and $\phi : \mathbb{A}^2 \to \mathbb{A}^1$ defined $(x, y) \to x$. Then $\phi(X) = \mathbb{A}^1 \backslash \{0\}$. (REMEMBER THIS EXAMPLE!). Notice that the closure of $\phi(X)$, is $\overline{\phi(X)} = \mathbb{A}^1$.

Another question is: Given $X \subseteq \mathbb{A}^n$ and $\phi : \mathbb{A}^n \to \mathbb{A}^m$, how do we compute $\overline{\phi(X)}$. We use the following clever trick: let $X \subseteq \mathbb{A}^n$, first we send $x \mapsto (x, \phi(x))$, then project unto the last m coordinates, i.e., $\phi(X)$ is the composition of the inclusion of X into the graph of ϕ with the projection onto the last m coordinates.

This breaks the problem into two parts:

- Describe the image of $X \mapsto \mathbb{A}^n \times \mathbb{A}^m$
- Describe $\overline{\pi(Y)}$ for $Y \subseteq \mathbb{A}^n \times \mathbb{A}^m$, where π is the projection onto the last m coordinates.

For part 1, the image of $X = V(I)$ is $V(I) \cap V(z_i - \phi_i(x)) \subseteq \mathbb{A}^n \times \mathbb{A}^m = (x_1, \dots, x_n, z_1, \dots, z_m)$

Example. Let $\phi : \mathbb{A}^2 \to \mathbb{A}^2$ defined by $\phi(x, y) = (x + y, x - y)$ and let $X = V(x^2 - y^2)$. Then the graph of X in $\mathbb{A}^2 \times \mathbb{A}^2$ is $V(x^2 - y^2, z_1 - z - y, z_2 - x + y) \subseteq (x, y, z_1, z_2)$. Then $\phi(x, y) = (z_1, z_2)$

Theorem 3.16. *Let $X \subseteq \mathbb{A}^n$ be a variety and let $\phi : \mathbb{A}^n \to \mathbb{A}^m$ be the projection onto the last m coordinates. Then $\overline{\pi(X)} = V(I(X) \cap k[x_{n-m+1}, \dots, x_n])$*

Note. We'll soon show that if $k = \overline{k}$ then we can replace $I(X)$ by I. But it is not true otherwise, for example, consider $k = \mathbb{R}$ and $X = V(x^2y^2 + 1) \subseteq \mathbb{A}^2$ and $\pi : (x, y) \mapsto y$. Then $X = \emptyset$, $\pi(X) = \emptyset$ and $I(X) = \langle 1 \rangle$. But $\langle x^2y^2 + 1 \rangle \cap k[y] = \langle 0 \rangle$

Proof. If $f \in I(X) \cap k[x_{n-m+1}, \ldots, x_m]$ then $f(y) = 0\,\forall y \in X$, so $f(y_{n-m+1}, \ldots, y_n) = 0\,\forall (y_{n-m+1}, \ldots, y_n)$ with $y \in X$, hence $f(\pi(y)) = 0\,\forall y \in X$ and thus $\pi(X) \subseteq V(I(X) \cap k[x_{n-m+1}, \ldots, x_n])$.

Conversely if $g \in I(\pi(X))$ then $g(y_{n-m+1}, \ldots, y_n) = 0\,\forall y = (y_1, \underline{\ldots, y_n}) \in X$. So $g \in I(X) \cap k[x_{n-m+1}, \ldots, x_n]$ so $I(\pi(X)) \subseteq \underline{I(X)} \cap k[x_{n-m+1}, \ldots, x_n]$. But since $\overline{\pi(X)} = V(I(\pi(X))$ this shows $V(I(X) \cap k[x_{n-m+1}, \ldots, x_n]) \subseteq \overline{\pi(X)}$. □

This leaves the question: Given $I \subseteq k[x_1, \ldots, x_n, z_1, \ldots, z_m]$ how can we compute $I \cap k[z_1, \ldots, z_m]$? The answer is to use Grobner basis.

Recall: the lexicographic term order with $x_1 > \cdots > x_n > z_1 > \cdots > z_m$ has $x^u z^v > x^{u'} z^{v'}$ if $(u - u', v - v')$ has first non-zero entry positive.

Proposition 3.17. *Let $I \subseteq k[x_1, \ldots, x_n] = S$ and let $G = \{g_!, \ldots, g_s\}$ be a lexicographic Grobner basis for I. Then a lexicographic Grobner basis for $I \cap k[x_{n-m+1}, \ldots, x_n]$ is given by $G \cap k[x_{n-m+1}, \ldots, x_n] = S'$, i.e., those elements of G that are polynomials in $x_{n-m+1}, \ldots, x_n$.*

Proof. $G \cap S'$ is a collection of polynomials in $I \cap S'$, so we just need to show that $\langle \mathrm{in}_{<\mathrm{lex}}(g) : g \in G \cap S' \rangle = \mathrm{in}_{<\mathrm{lex}}(I \cap S') \subseteq S'$. Let $f \in I \cap S'$. Then $\mathrm{in}_{<\mathrm{lex}}(f) \in \mathrm{in}_{<\mathrm{lex}}(I)$, so there is $g \in G$ with $\mathrm{in}_{<\mathrm{lex}}(g) | \mathrm{in}_{<\mathrm{lex}}(f)$. Since $f \in S'$, $\mathrm{in}_{<\mathrm{lex}}(g)$ is not divisible by $x_1, \ldots, x_{n-m}$ and thus $g \in S'$. Hence $\mathrm{in}_{<\mathrm{lex}}(f) \in \langle \mathrm{in}_{<\mathrm{lex}}(g) : g \in G \cap S' \rangle$, so $G \cap S'$ is a Grobner basis for $I \cap S'$. □

The next question is: Given $X = V(I)$, what is $I(X)$?

Hilbert's Nullstellensatz. *If $k = \overline{k}$, then $I(V(I)) = \sqrt{I}$, where $\sqrt{I}$ is the radical of I. (Denoted $r(I)$ in Commutative Algebra)*

Proof. This proof will come later in the course.

$\square$

4 Sylvester Matrix

Given $f, g \in k[x]$, how can we decide if they have a common factor?

Definition. $f = 5x^5 + 6x^4 - x^3 + 2x^2 - 1$ and $g = 7x^5 + 8x^3 - 3x^2 + 1$.

Or $f = ax + b, g = cx + d$. In this case we have that f, g has a common factor if and only if $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = 0$. Notice the analogy with $\mathbb{Z}$, that is, $n, m \in \mathbb{Z}$ have a common factor when there is no a, b such that $an + bm = 1$. This naturally leads to the next proposition.

Proposition 4.1. *Let $f = \sum_{i=0}^{l} a_i x^i$ and $g = \sum_{j=0}^{m} b_j x^j$ be two polynomials in $k[x]$. Then the following are equivalent.*

1. *f, g have a common root, i.e., there exists $\alpha \in \overline{k}$ such that $f(\alpha) = g(\alpha) = 0$*
2. *f, g have a non-constant common factor h*
3. *There does not exists $A, B \in k[x]$ with $Af + Bg = 1$*
4. *$\langle f, g \rangle \neq k[x]$*
5. *There exists $\widetilde{A}, \widetilde{B} \in k[x]$ with $\deg(\widetilde{A}) \leq m - 1, \deg(\widetilde{B}) \leq l - 1$ and $\widetilde{A}f + \widetilde{B}g = 0$.*

Proof. $1 \Rightarrow 3$: If $f(\alpha) = g(\alpha) = 0$ and $Af + Bg = 1$ then $A(\alpha)f(\alpha) + B(\alpha)g(\alpha) = 1 \Rightarrow 0 + 0 = 1$ which is a contradiction, hence no such A, B exists.

$3 \Rightarrow 4$: Suppose $\langle f, g \rangle = 1 = k[x]$, then $1 \in \langle f, g \rangle$ so there exists $A, B \in k[x]$ with $Af + Bg = 1$

$4 \Rightarrow 2$: If $\langle f, g \rangle \neq k[x]$ then, since $k[x]$ is a PID, the ideal $\langle f, g \rangle = \langle h \rangle$ for some $h \in k[x]$ non-constant. So $f, g \in \langle h \rangle$,that is, $f = \widetilde{f}h$, $g = \widetilde{g}h$ and thus f, g have a non-constant common factor.

$2 \Rightarrow 5$: We write $f = \widetilde{f}h$, $g = \widetilde{g}h$ and set $\widetilde{A} = \widetilde{g}$ and $\widetilde{B} = -\widetilde{f}$. Then $\widetilde{A}f + \widetilde{B}g = 0$ and $\widetilde{A}, \widetilde{B}$satisfy the degree bound.

$5 \Rightarrow 2$: If $\widetilde{A}f + \widetilde{B}g = 0$, then every irreducible factor of g divides $\widetilde{A}f$, since $k[x]$ is a UFD. Since $\deg(g) > \deg(\widetilde{A})$ at least one irreducible factor must divide f. Hence f and g have a common factor.

$2 \Rightarrow 1$: If f, g have a non-constant common factor h, let α be any root of h, then $f(\alpha) = g(\alpha) = 0$. So f and g have a common root.

$\square$

Part 5 is the key idea here. Given $f = \sum a_i x^i$ and $g = \sum b_j x^j$ with $0 \leq i \leq l$ and $0 \leq j \leq m$, write $\widetilde{A} = \sum_{i=0}^{m-1} c_i x^i$ and $\widetilde{B} = \sum_{j=0}^{l-1} d_j x^j$ where c_i, d_j are undeterminate coefficients.

$$\begin{aligned} 0 &= (c_{m-1}x^{m-1} + \cdots + c_0)(a_l x^l + \cdots + a_0) + (d_{l-1}x^{l-1} + \cdots + d_0)(b_m x^m + \cdots + b_0) \\ &= (c_{m-1}a_l + d_{l-1}b_m)x^{l+m-1} + (c_{m-1}a_{l-1} + c_{m-2}a_l + d_{l-1}b_{m-1} + d_{l-2}b_m)x^{l+m-2} + \cdots + (c_0 a_0 + d_0 b_0) \end{aligned}$$

Thus all the coefficients of x^j are zero. Remember that a_i and b_j are given, so we have a set of linear equations in the c and d variables. We can count that we have $l + m$ variables and linear equations.

This gives the following matrix

$$\begin{array}{c} \begin{pmatrix} a_l & 0 & \cdots & b_m & 0 & \cdots \\ a_{l-1} & a_l & \cdots & b_{m-1} & b_m & \cdots \\ a_{l-2} & a_{l-1} & \ddots & b_{m-2} & b_{m-1} & \ddots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\ & & & & & \\ & & a_0 & & & b_0 \end{pmatrix} \\ \underbrace{\hphantom{a_{l-1}\quad a_{l-1}\quad \ddots\quad}}_{m}\underbrace{\hphantom{b_{m-1}\quad b_{m-1}\quad \ddots\quad}}_{l} \end{array}$$

There exists non-zero $\widetilde{A}, \widetilde{B}$ if the correct degree with $\widetilde{A}f + \widetilde{B}g = 0$ if and only if the determinant of this matrix is zero.

Definition 4.2. Let $f = \sum_{i=0}^{l} a_i x^i$ and $g = \sum_{j=0}^{m} b_j x^j$ be polynomials in $k[x]$ with $a_l, b_m \neq 0$. The *Sylvester matrix* of f, g with respect to x is the $(l+m) \times (l+m)$ matrix

$$\mathrm{Syl}(f,g,x) = \begin{array}{c} \begin{pmatrix} a_l & 0 & \cdots & b_m & 0 & \cdots \\ a_{l-1} & a_l & \cdots & b_{m-1} & b_m & \cdots \\ a_{l-2} & a_{l-1} & \ddots & b_{m-2} & b_{m-1} & \ddots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\ & & & & & \\ & & a_0 & & & b_0 \end{pmatrix} \\ \underbrace{\hphantom{a_{l-1}\quad a_{l-1}\quad \ddots\quad}}_{m}\underbrace{\hphantom{b_{m-1}\quad b_{m-1}\quad \ddots\quad}}_{l} \end{array}$$

The determinant of $\mathrm{Syl}(f,g,x)$ is a polynomial in a_i, b_i with integer coefficients. This is called the *resultant* of f and g and is denoted $\mathrm{Res}(f,g,x)$.

Example. Let $f = x^2 + 3x + a$ and $g = x + b$. Then

$$\text{Syl (f,g,x)} = \begin{pmatrix} 1 & 1 & 0 \\ 3 & b & 1 \\ a & 0 & b \end{pmatrix}$$

so $\mathrm{Res}(f,g,x) = b^2 - (3b - a) = b^2 - 3b + a$, so f and g have a common factor if and only if $a = 3b - b^2$.

Theorem 4.3. *Fix $f, g \in k[x]$, then f, g have a common factor if and only if $Res(f,g,x) = 0$*

Proof. This is what the previous work has been about. □

Example. $f = x^2 + 2x + 1$, $g = x^2 + 3x + 2$

$$\mathrm{Syl}(f,g,x) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 1 & 3 & 1 \\ 1 & 2 & 2 & 3 \\ 0 & 1 & 0 & 2 \end{pmatrix}$$

We see that $(r_3 - r_1) - (r_2 - r_1) - r_4 = 0$, so $\mathrm{Res}(f,g,x) = 0$. (In fact the common factor is $x + 1$)
$f = ax^2 + bx + c$, $g = f' = 2ax + b$

$$\mathrm{Syl}(f,g,x) = \begin{pmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{pmatrix}$$

So $\mathrm{Res}(f,g,x) = ab^2 - 2a(b^2 - 2ac) = -ab^2 + 4a^2c = -a(b^2 - 4ac)$

Notice how in the second example we nearly ended up with the discriminant of a quadratic equations.

Definition 4.4. Let $f = \sum_{i=0}^{l} a_i x^i$. Then the *discriminant* of f, $\operatorname{disc}(f) = \frac{(-1)^{l-1}}{a_l}\operatorname{Res}(f, f', x)$

Proposition 4.5. *The polynomial disc(f) lies in $\mathbb{Z}[a_0, \dots, a_l]$. The polynomial f has a multiple root if and only if disc$(f) = 0$.*

Proof. Note that the first row of $\operatorname{Syl}(f, f', x)$ is $(a_l, 0, \dots, 0, la_l, 0, \dots, 0)$ so $a_l|\operatorname{Res}(f, f', x)$ and thus $\operatorname{disc}(f) \in \mathbb{Z}[a_0, \dots, a_l]$.

Since $\deg(f) = l$ and $a_l \neq 0$, we have $\operatorname{disc}(f) = 0$ if and only if f and f' have a common root, so we just need to check that this happens if and only if f has a multiple root. Fix a root α of f and write $f = (x - \alpha)^m \widetilde{f}$ where $\widetilde{f}(\alpha) \neq 0$. Then $f' = m(x - \alpha)^{m-1}\widetilde{f} + (x - \alpha)^m \widetilde{f}'$, so $f'(\alpha) = 0$ if $m > 1$. If $m = 1$ then $f'(\alpha) = \widetilde{f}(\alpha) \neq 0$. So α is a root of f' if and only if α is a multiple root of f. ☐

Generalizations:

1. More variables:

   Given $f, g \in k[x_1, \dots, x_n]$, write $f = \sum_{i=0}^{l} a_i x_1^i$ and $g = \sum_{j=0}^{m} b_j x_1^j$ where $a_i, b_j \in k[x_2, \dots, x_n]$ and $a_l, b_m \neq 0$. Then $\operatorname{Res}(f, g, x_1) = \det(\operatorname{Syl}(f, g, x_1)) \in k[x_2, \dots, x_n]$.

   Note. We can think about f, g as polynomials in $k(x_2, \dots, x_n)[x_1]$ (fields of rational functions). So this is a special case of the first one. In particular, either $\operatorname{Res}(f, g, x_1) = 0$ or there exists $A, B \in k(x_1, \dots, x_n)[x_1]$ with $Af + Bg = 1$.

   Example. $\widetilde{A} = A\operatorname{Res}(f, g, x_1), \widetilde{B} = B\operatorname{Res}(f, g, x_1)$ are polynomials in $k[x_1, x_2, \dots, x_n]$ so $\widetilde{A}f + \widetilde{B}g = \operatorname{Res}(f, g, x_1)$. A and B comes from solution to

   $$\operatorname{Syl}(f, g, x_1)\begin{pmatrix} c_{m-1} \\ \vdots \\ c_0 \\ d_{l-1} \\ \vdots \\ d_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \\ \vdots \\ \\ 1 \end{pmatrix}$$

   Cramer's rule states $Ax = b$, $x_i = \frac{(-1)|A_i|}{|A|}$ where A_i is A with i^{th} column replaced by b. By Cramer's rule, the c_i and d_j have the form polynomial is $x_2, \dots x_n/\operatorname{Res}(f, g, x_1)$. So $A\operatorname{Res}(f, g, x_1)$ is a polynomial in $k[x_1, \dots, x_n]$

   As a corollary to all of this we have that $\operatorname{Res}(f, g, x_1) \in \langle f, g\rangle \cap k[x_2, \dots, x_n]$. This is a cheaper way to do elimination/projection.

   Proposition 4.6. *Fix $f, g \in k[x_1, \dots, x_n]$ for degrees l, m in x_1 respectively. If Res$(f, g, x_1) \in k[x_2, \dots, x_n]$ is zero at $(c_2, \dots, c_n) \in k^{n-1}$ then either $a_l(c_2, \cdots, c_n) = 0$ or $b_m(c_2, \dots, c_n) = 0$ or $\exists c_1 \in \overline{k}$ such that $f(c_1, \dots, c_n) = g(c_1, \dots, c_n) = 0$.*

   Proof. Let $f(x_1, \underline{c}) = f(x_1, c_2, \dots, c_n) \in k[x_1]$ and similarly let $g(x_1, \underline{c}) \in k[x_1]$. If neither $a_l(\underline{c})$, $b_m(\underline{c}) = 0$ then $f(x_1, \underline{c})$ had degree l and $g(x_1, \underline{c})$ has degree m. So $\operatorname{Syl}(f(x_1, \underline{c}), g(x_1, \underline{c},), x_1)$ is $\operatorname{Syl}(f, g, x_1)$ with $c_2, \dots, c_n$ substituted for $x_2, \dots, x_n$. Thus $\operatorname{Res}(f(x_1, \underline{c}), g(x_1, \underline{c}), x_1) = 0$, so $f(x_1, \underline{c})$ and $g(x_1, \underline{c})$ have a common root $c_i \in \overline{k}$. Hence $f(c_1, c_2, \dots, c_n) = g(c_1, c_2, \dots, c_n) = 0$. ☐

2. Resultants of several polynomials.

   Given $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ we introduce new variables $u_2, \dots, u_s$ and let $g = u_2 f_2 + \dots u_s f_s$. Write $\operatorname{Res}(f_1, g, x_1) = \sum h_\alpha(x_2, \dots, x_n)u^\alpha$ with $\alpha \in \mathbb{N}^{s-1}$. We call $h_\alpha \in k[x_2, \dots, x_n]$ the generalised resultant.

Example. Let $f_1 = x^3+3x+2$, $f_2 = x+1$, $f_3 = x+5$. Then $g = u_2(x+1)+u_3(x+5)$ and

$$\mathrm{Syl}(f,g,x_1) = \begin{pmatrix} 1 & u_2+u_3 & 0 \\ 3 & u_2+5u_3 & u_2+u_3 \\ 2 & 0 & u_2+5u_3 \end{pmatrix}$$

so $\mathrm{Res}(f_1,g,x_1) = -4u_2u_3+12u_3^2$. Hence $h_{1,1} = -4$ and $h_{0,2} = 12$.

Lemma 4.7. *The polynomial h_α lies in $\langle f_1,\dots,f_s\rangle \cap k[x_2,\dots,x_n]$*

Proof. Write $\mathrm{Res}(f_1,g,x_1) = Af_1+Bg$ for $A,B \in k[u_2,\dots,u_s,x_1,\dots,x_n]$. Write $A = \sum A_\alpha u^\alpha$ and $B = \sum B_\beta u^\beta$ for $A_\alpha, B_\beta \in k[x_1,\dots,x_n]$. Then $\mathrm{Res}(f_1,g,x_1) = \sum h_\alpha u^\alpha = \sum_\alpha (A_\alpha f_1 + \sum_{i=2}^s B_{\alpha-e_i} f_i)u^\alpha$. So $h_\alpha = A_\alpha f_1 + \sum B_{\alpha-e_i} f_i \in \langle f_1,\dots,f_s\rangle$. Furthermore $h_\alpha \in k[x_2,\dots,x_n]$ by construction. □

4.1 Hilbert's Nullstellensatz

Consider $\pi: \mathbb{A}^n \to \mathbb{A}^m$ projection onto the last m coordinates. We saw $\overline{\pi(X)} = V(I(X)\cap k[x_{n-m+1},\dots,x_n])$. The question is what do we add then we take the closure? Given $y \in \overline{\pi(X)}$ is $y \in \pi(X)$?

Theorem 4.8 (Extension Theorem.). *Let $k = \overline{k}$. Let $X = V(I) \subseteq \mathbb{A}^n$ and let $\pi: \mathbb{A}^n \to \mathbb{A}^{n-1}$ be projection onto the last $n-1$ coordinates. Write $I = \langle f_1,\dots,f_s\rangle$ with $f_i = g_i(x_2,\dots,x_n)x_1^{N_i}+$*l.o.t. in *$x_i$. Let $(c_2,\dots,c_n) \in V(I\cap k[x_2,\dots,x_n])$. If $(c_2,\dots,c_n) \notin V(g_1,\dots,g_s) \subseteq \mathbb{A}^{n-1}$ then $\exists c_1 \in k$ with $(c_1,\dots,c_n) \in X$.*

Example. $X = V(xy-1)$, $f_1 = xy-1, g_1 = x$. Then the theorem say if $c_1 \in V(0) = \mathbb{A}^1$ and $c_1 \notin V(x)$ then there exists c_2 with $(c_1,c_2) \in V(xy-1)$. Note that $V(0)$ comes from $\langle xy-1\rangle \cap k[x]$.

Note. $I \subseteq I(X)$ so $I\cap k[x_2,\dots,x_n] \subseteq I(X)\cap k[x_2,\dots,x_n]$ so $V(I\cap k[x_2,\dots,x_n]) \supseteq \overline{\pi(X)}$. How useful this is depends on the choice of the generators of I. The theorem talks about I, not $I(X)$, so this brings us closer to the Nullstellensatz.

Proof. $s=1$: In this case $f = g_1(x_2,\dots,x_n)x_1^N +$ l.o.t.We have $\langle f\rangle \cap k[x_2,\dots,x_n] = \langle 0\rangle$, and $(c_2,\dots,c_n) \in V(\langle f\rangle \cap k[x_2,\dots,x_n]$

Case 1. $N \neq 0$: $g_1(c_1,\dots,c_n) \neq 0$, then $f(x_1,c_2,\dots c_n)$ is a polynomial of degree N in x_1 so has a root c_1 in k.

Case 2. $N = 0$ then $g_1 = f_1$, so if $(c_2,\dots,c_n) \in V(\langle f\rangle \cap k[x_2,\dots,x_n]) = V(f) \subseteq \mathbb{A}^{n-1}$

$s=2$: The (previous) proposition shows that if $g_1(c_1,\dots,c_n) \neq 0$ and $g_2(c_2,\dots,c_n) \neq 0$ then the desired c_1 exists. Suppose $(c_2,\dots,c_n) \notin V(g_1,g_2)$ then without loss of generality $g_1(c_2,\dots,c_n) \neq 0$. If $g_2(c_2,\dots,c_n) \neq 0$ then c_1 exists. Otherwise replace f_2 by $f_2 + x_1^N f_1$ for $N \gg 0$. This does not change the ideal $\langle f_1,f_2\rangle$ and it does not change $(c_2,\dots,c_n) \notin V(g_1,g_2) = V(g_1,g_1)$. Then the proposition implies there exists c_1 with $f_1(c_1,\dots,c_n) = f_2(c_1,\dots c_n) = 0$.

$s \geq 3$: Also assume $g_1(c_2,\dots,c_n) \neq 0$. Replace f_2 by $f_2+x_1^N f_1$ for $N \gg 0$ if necessary to guarantee $g_2(\underline{c}) \neq 0$ and $\deg_{x_1}(f_2) > \deg_{x_1}(f_i)$ for $i > 2$. Write $\mathrm{Res}(f, \sum_{i=2}^s u_i f_i, x_1) = \sum h_\alpha u^\alpha$. Since $h_\alpha \in I\cap k[x_2,\dots,x_n]$ we have $h_\alpha(c_2,\dots,c_n) = 0\,\forall\alpha$. Thus $\mathrm{Res}(f,\sum u_i f_i, x_1)(c_2,\dots,c_n,u_1,\dots,u_s)$ is the zero polynomial.
By construction the coefficients of the maximal power of x_1 in f_1 and in $\sum u_i f_i$ are g_1 and $g_1 u_1$, so are non-zero are $(c_2,\dots,c_n)$. Thus $0 = \mathrm{Res}(f,\sum u_i f_i, x_1)(c_2,\dots,c_n,u_1,\dots,u_s) = \mathrm{Res}(f_1(x_1,c_2,\dots,c_n), \sum u_i f_i(x_1,c_2,\dots,c_n), x_1)$. Thus there exists $F \in k(u_2,\dots,u_s)[x_1]$ with $\deg_{x_1} F > 0, F | f_1(x_1,c_2,\dots,c_n)$. Write $F = \widetilde{F}/g$ where $\widetilde{F} = k[u_2,\dots,u_s,x_1]$, $g \in k[u_2,\dots,u_s]$. Then $\widetilde{F}$ divides $f_1(x_1,c_2,\dots,c_n)g(u_2,\dots,u_s)$. Let F'' be an irreducible factor of $\widetilde{F}$ with positive degree in x_1. Then $F''|f_1(x_1,c_2,\dots,c_n)$. Thus it does not contain any u_i. So $F''|\sum u_i f_i(x_i,c_2,\dots,c_n)$ but $F'' \in k[x_1]$ thus $F''|f_i(x_1,c_2,\dots,c_n)$ for $2 \leq i \leq n$. Then $F''|f_i(x_1,c_2,\dots,c_n)$ for all $1 \leq i \leq s$. Then choose a root c_1 of F''. Then $F''(c_1) = 0$ so $f_i(c_1,\dots,c_n) = 0$ so $(c_1,\dots,c_n) \in X$

□

Weak Nullstellensatz. *Let $k = \overline{k}$. Suppose $I \subseteq k[x_1, \ldots, x_n]$ satisfies $V(I) = \emptyset$, then $I = \langle 1 \rangle = k[x_1, \ldots, x_n]$.*

Proof. We use an induction proof on n.

$n = 1$: $I = \langle f \rangle \subseteq k[x_1]$. If $f \notin k$ there exists $\alpha \in k$ with $f(\alpha) = 0$ so $V(I) \neq \emptyset$. Thus if $V(I) = \emptyset$, $I = \langle f \rangle = \langle 1 \rangle$.

$n > 1$: Let $I = \langle f_1, \ldots, f_s \rangle$ and suppose $V(I) = \emptyset$. We may assume $\deg(f_i) > 0$ for all i. Let the degree of f_1 be N. Consider the morphism $\phi : \mathbb{A}^n \to \mathbb{A}^n$ given by $\phi^* : k[x_1, \ldots, x_m] \to k[z_1, \ldots, z_n]$ with $\phi^*(x_i) = z_i + a_i z_1$ with $a_1 = 0$ and $a_i \in K$ for $i > 1$.
Note: ϕ^* is an isomorphism, since the matrix is

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ a_2 & 1 & 0 & \ldots & 0 \\ a_3 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & 0 & \ldots & 1 \end{pmatrix}$$

is invertible. $(\phi^*)^{-1}(z_i) = x_i - a_i x_1$. This means that $1 \in I$ if and only if $1 \in \phi^*(I)$, and $\phi^{-1}(X) = V(\phi^*(I)) = \emptyset$. (This is because $V(\phi^*(I)) = \{y : \phi^* f(y) = 0 \, \forall f \in I\} = \{y : f \circ \phi(y) = 0 \, \forall f \in I\} = \{y : \phi(y) \in V(I)\}$.)
Let $f_1 = \sum c_u x^u$. Note that $\phi^*(f_1) = c(a_2, \ldots, a_n) z_1^N + \text{l.o.t in } z_1$ where $c(a_2, \ldots, a_n)$ is the non-zero polynomial in $a_2, \ldots, a_n$, i.e., $c(a_2, \ldots, a_n) = \sum_{|u|=N} c_u \prod a_i^{u_i}$. Thus we can choose $(a_2, \ldots, a_n) \in k^{n-1}$ with $c(a_2, \ldots, a_n) \neq 0$. (Exercise: this holds because the field is infinite)
Then $g_1 \in k$, so $V(g_1, \ldots, g_s) = \emptyset$ for $\phi_1^*(f_i) = g_i z_1^{N_i} + \text{l.o.t.}$ Let $J = \phi^*(I) \cap k[z_1, \ldots, z_n]$, then by the extension theorem, if $(c_2, \ldots, c_n) \in V(J)$ then there exists $c_1 \in k$ with $(c_1, \ldots, c_n) \in V(\phi^*(I))$. Thus $V(J) = \emptyset$ and by induction $J = \langle 1 \rangle$, so $1 \in \phi^*(I)$ and so $1 \in I$.

□

Note that is $1 \in I$, we can write $1 = \sum A_i f_i$ with $A_i \in k[x_1, \ldots, x_n]$.

Nullstellensatz. *Let $k = \overline{k}$. Then $I(V(I)) = \sqrt{I}$.*

Proof. Let $f^m \in I$, then $f^m(x) = 0 \, \forall x \in V(I)$ so $f(x) = 0$ for all $x \in V(I)$. Hence $f \in I(V(I))$, thus $\sqrt{I} \subseteq I(V(I))$

For the reverse inclusion, suppose $f \in I(V(I))$ and let $I = \langle f_1, \ldots, f_s \rangle$ and $\widetilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq k[x_1, \ldots, x_n, y]$. Now that $V(\widetilde{I}) = \emptyset$ since if $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$ then $f(x_1, \ldots, x_n) = 0$ so $1 - yf(x_1, \ldots, x_n) \neq 0 \, \forall y$. So by the Weak Nullstellensatz we have that $1 \in \widetilde{I}$. So there exists $p_1, \ldots, p_s, q \in k[x_1, \ldots, x_n, y]$ with $1 = \sum p_i f_i + q(1 - yf)$. Regard this as an expression in $k(x_1, \ldots, x_n, y)$ and substitute $y = \frac{1}{f}$, then $1 = \sum p_i(x_1, \ldots, x_n \frac{1}{f}) f_i$. Choose $m > 0$ for which $p_i(x_1, \ldots, x_n \frac{1}{f}) f^m \in k[x_1, \ldots, x_n]$ then $f^m = \sum (p_i(x_1, \ldots, x_n \frac{1}{f}) f^m) f_i$, hence $f^m \in I$ and thus $f \in \sqrt{I}$.

$\square$

5 Irreducible Components

(There is some cross-over with commutative algebra here, revise both!)

Definition 5.1. A variety $X \subseteq \mathbb{A}^n$ is *reducible* if $X = X_1 \cup X_2$ with X_1, X_2 non-empty varieties in $\mathbb{A}^n$ and $X_1, X_2 \subsetneq X$

X is *irreducible* if it is not reducible.

Example.

- $X = V(x, y) \subseteq \mathbb{A}^2$ then $X = V(x) \cup V(y)$.
- $V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$ is irreducible but it is not trivial to prove. We will prove this later.
- $X \subseteq \mathbb{A}^1$ is reducible if and only if $1 < |X| < \infty$
- $X = V(f)$ is a hypersurface in $\mathbb{A}^n$. Let $f = cf_1^{\alpha_1} \dots f_r^{\alpha_r}$ where $c \in k$ and f_i are distinct irreducible polynomials. Then $V(f) = V(f_1) \cup \dots \cup V(f_r)$. Claim: If $r > 1$ then $V(f)$ is reducible. We just need too show that $V(f_i) \neq \emptyset, X$ for all i. Now $V(f_i) \neq \emptyset$ since $1 \notin \langle f_i \rangle$. If $V(f_i) = X$ then $V(f_j) \subseteq V(f_i)$ for some $j \neq i$. Hence $f_i \in I(V(f_j)) = \sqrt{f_j} = \langle f_j \rangle$ (exercise). So $f_j | f_i$ which contradicts f_i, f_j being distinct irreducible. Actually $V(f_i)$ are all irreducible, so $X = V(f_1) \cup \dots \cup V(f_r)$ is a decomposition into irreducible.

Theorem 5.2. *Let $X \subseteq \mathbb{A}^n$ be a variety. Then $X = X_1 \cup \dots \cup X_r$, where each X_r is irreducible. This representation is unique up to permutation provided it is irredundant (i.e., $X_i \nsubseteq X_j$ for any $i \neq j$)*

Proof. For this theorem, we use the fact that $k[x_1, \dots, x_n]$ is Noetherian, in particular, that there is no infinite ascending chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$ of ideals in $k[x_1, \dots, x_n]$.

Existence: If X is irreducible then we are done. Otherwise write $X = X_1 \cup X_2$ where X_1, X_2 are proper subvarieties. Again if both are irreducible then we are done. Otherwise we can write $X_1 = X_{11} \cup X_{12}$ and $X_2 = X_{21} \cup X_{22}$ where X_{ij} are proper subvarieties of X_i. Iterate this process. We claim that this process terminates with $X = \cup X_j$ (Finite union). If not we have an infinite descending chain $X \supsetneq X_1 \supsetneq X_{11} \supsetneq X_{111} \supsetneq \dots$. This gives a reverse containment $I(X) \subsetneq I(X_1) \subsetneq I(X_{11}) \subsetneq \dots$. This chain must stabilize, so $I(X_{111\dots11}) = I(X_{111\dots11111})$ but $V(I(X_{11\dots111}) = X_{11\dots11}$which contradicts the proper inclusion of varieties. Since $V(I(V(I))) = V(I)$. Hence the decomposition process must terminates.

Uniqueness: Suppose $X = X_1 \cup X_2 \cup \dots \cup X_r = X_1' \cup \dots \cup X_s'$ are two irredundant irreducible decompositions. Consider

$$
\begin{aligned}
X \cap (X_i') &= X_i' \\
&= (X_1 \cup \dots \cup X_r) \cap X_i' \\
&= (X_1 \cap (X_i')) \cup \dots \cup (X_r \cap (X_i'))
\end{aligned}
$$

Since X_i' is irreducible, there must be j with $X_j \cap (X_i') = X_i'$, so $X_i' \subseteq X_j$. The same argument shows that there is k with $X_j \subseteq X_k'$, so we have $X_i' \subseteq X_j \subseteq X_k'$. Since the decomposition is irredundant, $X_i' = X_k' = X_k$. This construct a bijection between $\{X_j\}$ and $\{X_i'\}$, hence $r = s$ and the decomposition is unique up to permutation. $\square$

Note: This was a topological proof. A topological space with no infinite descending chain of closed set is called Noetherian (note how this is the "opposite" condition to Noetherian ring). Noetherian topological spaces have irreducible decompositions.

Theorem 5.3. *Let $X \subseteq \mathbb{A}^n$ be a variety. The following are equivalent:*

1. *X is irreducible*
2. *The coordinate ring $k[X]$ is a domain*
3. *$I(X) \subseteq k[x_1, \dots, x_n]$ is prime.*

Proof. 2 $\iff$ 3: Recall $k[X] = k[x_1, \dots, x_n]/I(X)$. So if $f, g \in k[X]$ satisfy $fg = 0$ then there are lifts $\widetilde{f}, \widetilde{g} \in k[x_1, \dots, x_n]$ such that $\widetilde{f}, \widetilde{g} \notin I(X)$ and $\widetilde{f}\widetilde{g} \in I(X)$. Same argument works the other way round.

$1 \Rightarrow 3$: Suppose $I(X)$ is not prime, that is, there exists $f, g \notin I(X)$ with $fg \in I(X)$. Let $X_1 = V(f) \cap X$ and $X_2 = V(g) \cap X$. Since $f, g \notin I(X)$ then $X_1, X_2 \subsetneq X$. However $X_1 \cup X_2 = (V(f) \cap X) \cup (V(g) \cap X) = ((V(f) \cup V(g)) \cap X = V(fg) \cap X = X$ since $fg \in I(X)$. So X is reducible.

$3 \Rightarrow 1$: Suppose $X = X_1 \cup X_2$ with X_1 and X_2 proper subvarieties. Then $I(X) \subsetneq I(X_1), I(X) \subsetneq I(X_2)$ (To see this take $V(\_)$ of both side then $V(I(X_i)) = X_i$). So we may choose $f \in I(X_1) \backslash I(X)$ and $g \in I(X_2) \backslash I(X)$. Now $fg \in I(X_1) \cap I(X_2)$, so $V(I(X_1) \cap I(X_2)) \subseteq V(fg)$. But $V(I(X_1) \cap I(X_2)) = V(I(X_1)) \cup V(I(X_2)) = X_1 \cup X_2 = X$. So $fg \in I(X)$ so $I(X)$ is not prime.

□

Remark. Some text reserve the word "variety" for irreducible varieties and call what we call varieties "algebraic sets".

Warning: If $X = V(I)$ is irreducible, this does not imply that I is prime, just that $I(X)$ is. This about $I = \langle x^2, xy^2 \rangle \subseteq k[x, y]$.

Theorem 5.4. *Let $k = \overline{k}$ (this condition is unnecessary as there exists a commutative algebra proof which show this theorem holds for $k \neq \overline{k}$. See Commutative Algebra notes, this is the whole theory of Primary Decomposition). Let $I = \sqrt{I}$ (a radical ideal) in $k[x_1, \dots, x_n]$, then $I = P_1 \cap \cdots \cap P_r$ where each P_i is prime. This decomposition is unique up to order if irredundant.*

Proof. Let $X = V(I)$ and let $X = X_1 \cup \cdots \cup X_r$ be an irredundant irreducible decomposition. Let $P_i = I(X_i)$ which is prime by the previous theorem and let $P = \cap P_i$. Then $V(P) = \cup V(P_i) = \cup X_i = X$. So $\sqrt{P} = I(X) = I$. If $f^m \in P$ for some $m > 0$ then $f^m \in P_i$ for all i, so $f \in P_i$ for all i. Hence $f \in \cap P_i = P$ and thus $\sqrt{P} = P$. So $I = \cap P_i$

Uniqueness follows from the uniqueness of primary decomposition. □

The next question to come up is how can we determine the P_i, that is the prime decomposition of radical ideals.

Definition 5.5. Let I, J be ideals. Then the *colon* (or *quotient*) ideal is $(I : J) = \{f \in k[x_1, \dots, x_n] : fg = I \, \forall g \in J\} \subseteq I$.

Example. Let $I = \langle x^2, xy^2 \rangle$ and $J = \langle x \rangle$. Then $(I : J) = \{f : fg \in \langle x^2, xy^2 \rangle \; \forall g \in \langle x \rangle\} = \{f : fx \in \langle x^2, xy^2 \rangle\} = \langle x, y^2 \rangle$

Theorem 5.6. *Let $I = \sqrt{I}$ and let $I = \cap P_i$ be an irredundant primary decomposition. Then the P_i are precisely the prime ideals of the form $(I : f)$ for $f \in k[x_1, \dots, x_n]$.*

Proof. Notice: $(I : f) = (\cap P_i : f) = \cap (P_i : f)$. Now for any prime P we have $(P : f) = \begin{cases} \langle 1 \rangle & f \in P \\ P & f \notin P \end{cases}$.
So $(I : f) = \cap_{f \notin P_i} P_i$. Fix P_i, since $P_j \nsubseteq P_i$ for any $j \neq i$, we can find $f_j \in P_j \backslash P_i$. Let $f = \prod_{i \neq j} f_j$ then $f \in \cap_{j \neq i} P_j \backslash P_i$. So $(I : f) = P_i$.

Conversely if $(I : f) = P$ is prime for some f, then $P = \cap_{f \notin P_i} P_i$ (as $\cap P_i = \prod P_i$ so $P = P_i$ for some i. In more details $P \subseteq P_i$ for all i. If $P \subsetneq P_i$for all i then we can find $f_i \in P_i \backslash P$, so $f = \prod f_i \in \cap P_i \backslash P$ which is a contradiction. So $P = P_i$for some i) □

Example. Let $I = \langle xy, xz, yx \rangle$, then $V(I) =$ union of x, y, z axes $= V(x, y) \cup V(x, z) \cup V(y, z)$. So $I = \langle x, y \rangle \cap \langle x, z \rangle \cap \langle y, x \rangle$. We want to see the theorem in action, so notice that $(I : z) = \langle x, y \rangle$,$(I : y) = \langle x, z \rangle$ and $(I : x) = \langle y, z \rangle$. Warning: $(I : x + y) = \langle z, xy \rangle$ (not as obvious.)

Let $I = \langle x^3 - xy^2 - x \rangle$. Then $(I : x^2 + y^2 - 1) = \langle x \rangle$ and $(I : x) = \langle x^2 + y^2 - 1 \rangle$.

Note. If X, Y are varieties in $\mathbb{A}^n$ then $(I(X) : I(Y)) = I(X \backslash Y)$. To see this: fix $x \in X \backslash Y$, since $x \notin Y$ there is $g \in I(Y)$ with $g(x) \neq 0$. So if $f \in (I(X) : I(Y))$ then $f(x)g(x) = 0$, so $f(x) = 0$ and thus $\underline{f \in I(X\backslash Y)}$. Conversely if $f \in I(X \backslash Y)$ and $g \in I(Y)$ then $fg \in I(X)$ so $f \in (I(X) : I(Y))$. Hence $\overline{(X \backslash Y)} = V(I(X) : I(Y))$.

5.1 Rational maps

How can we decide if X is irreducible? This is hard in general! We use the following trick. If $\phi : Y \to X$ is surjective and $X = X_1 \cup X_2$ then $Y = \phi^{-1}(X_1) \cup \phi^{-1}(X_2)$. Now both sides are closed and proper if both X_1 and X_2 are. So if X is reducible then so is Y. Or if Y is irreducible then so is X.

Definition 5.7. A morphism $\phi : X \to Y$ of affine varieties is *dominant* if $\overline{\phi(X)} = Y$

Example. Take $\phi : V(xy-1) \to \mathbb{A}^1$ defined by $(x, y) \mapsto x$. This is not surjective but it is dominant.

Proposition 5.8. *A morphism $\phi : X \to Y$ is dominant if and only if $\phi^* : k[Y] \to k[X]$ is injective.*

Example. $k[x] \to k[x, y]/\langle xy-1\rangle$, $x \mapsto x$ (linked to the previous exampled) is injective.

Proof. A morphism $\phi : X \to Y$ induces a homomorphism $\phi^* : k[Y] \to k[X]$. Now $\phi(X) \subseteq Z \subsetneq Y$ (Z a variety) if and only if there exists $g \in I(X)\backslash I(Y)$ with $g(\phi(x)) = 0\,\forall x \in X$, so $\phi^*(g(x)) = 0\,\forall x \in X$. Hence $\phi^* g \in I(X)$ and thus the image of g in $k[Y]$ is non-zero but is mapped to zero by ϕ^* so ϕ^* is not injective. □

Proposition 5.9. *If $\phi : X \to Y$ is dominant and X is irreducible then so is Y.*

Proof. Since ϕ is dominant, the map $\phi^* : k[Y] \to k[X]$ is injective. Since X is irreducible, we have $k[X]$ is a domain, and thus so is $k[Y]$. Hence Y is also irreducible. □

Definition 5.10. A *rational map* $\phi : \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ is defined by $\phi(x_1, \ldots, x_n) = (\phi_1(x_1, \ldots, x_n), \ldots, \phi_m(x_1, \ldots x_n))$ with $\phi_i \in k(x_1, \ldots, x_n)$ (the field of rational functions)

Example. $\phi : \mathbb{A}^1 \dashrightarrow \mathbb{A}^1$ defined by $\phi(x) = \frac{1}{x}$.

Warning: ϕ is not necessarily a function defined on all of $\mathbb{A}^n$. Write $\phi_i = \frac{f_i}{g_i}$ for $f_i, g_i \in k[x_1, \ldots, x_n]$ and let $U = \{x \in \mathbb{A}^n : g_i(x) \neq\}$. Then $\phi : U \to \mathbb{A}^m$ is well defined. Notice that U is an open set ($U = \mathbb{A}^n \backslash V(\prod g_i)$). In the above example ϕ is defined on $U = \{x \in \mathbb{A}^1 : x \neq 0\}$.

Note. A rational map induces a k-algebra homomorphism $\phi^* : k[z_1, \ldots, z_m] \to k(x_1, \ldots, x_n)$ defined by $z_i \mapsto \phi_i$. Conversely any such k-algebra homomorphism determines a rational map.

Example. Let $\phi : \mathbb{A}^1 \to \mathbb{A}^2$ be the inverse stereographic projection, that is, defined by $\phi(t) = (\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$. It is a rational map from $\mathbb{A}^1$ to $V(x^2+y^2-1)$. It is defined on $\mathbb{A}^1 \setminus \pm i$ and the image $V(x^2+y^2-1)\backslash\{(1, 0)\}$.

Definition 5.11. Let $Y \subseteq \mathbb{A}^m$, a *rational map* $\phi : \mathbb{A} \dashrightarrow Y$ is a rational map $\phi : \mathbb{A}^n \to \mathbb{A}^m$ with $\phi^*(I(Y)) = 0$, so $\phi^* : k[Y] \to k(x_1, \ldots, x_n)$.

Example. Let $\phi : \mathbb{A}^1 \to V(x^2+y^2-1)$ be the inverse stereographic projection. Then $\phi^*(x) = \frac{t^2-1}{t^2+1}, \phi^*(y) = \frac{2t}{t^2+1}$. Hence $\phi^*(x^2+y^2-1) = (\frac{t^4-2t^2+1+4t^2}{t^4+2t^2+1} - 1) = 0$, so ϕ is indeed a rational map.

What about rational maps $\phi : X \dashrightarrow \mathbb{A}^m$? We recall that a morphism $X \to \mathbb{A}^m$ was an equivalence class of morphism $\mathbb{A}^n \to \mathbb{A}^m$. But we have some problems: consider $X = V(x) \subseteq \mathbb{A}^2$ and $\phi : \mathbb{A}^2 \dashrightarrow \mathbb{A}^3$ defined by $\phi(x, y) = (x^2, \frac{1}{xy}, y^3)$. Then ϕ is define on $U = \{(x, y) : x, y \neq 0\}$, ϕ is not defined at (x, y) for any $(x, y) \in X$. The solution to this is to allow rational maps that are defined on enough of X.

Definition 5.12. Let R be a commutative ring with identity. An element $f \in R$ is a *zero-divisor* if there exists $g \in R$ with $g \neq 0$ such that $fg = 0$.

Definition 5.13. Let $\phi : \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ be a rational map with $\phi_i = \frac{f_i}{g_i}$ where f_i and g_i have no common factors. Then ϕ is *admissible* on X if the image of each g_i in $k[X]$ is a non-zero divisor.

Example. $\phi : \mathbb{A}^2 \dashrightarrow \mathbb{A}^3$, $\phi(x, y) = (x^2, \frac{1}{xy}, y^3)$ is not admissible on $V(x)$.

Let $X = V(x^2-y^2) \subseteq \mathbb{A}^2$ and $\phi : \mathbb{A}^2 \dashrightarrow \mathbb{A}^1$ defined by $(x, y) \mapsto \frac{1}{x+y}$. Then ϕ is not admissible on X as $x+y$ is a zero divisor in $k[x, y]/(x^2-y^2)$. On the other hand $\psi : \mathbb{A}^2 \dashrightarrow \mathbb{A}^2$ defined by $\psi(x, y) = (\frac{1}{x}, \frac{1}{y})$ is.

Definition 5.14. Let U be the set of non-zero divisor on a ring R. Note $U \neq 0$ since $1 \in U$. The *total quotient ring* (ring under "obvious" multiplication and addition) is as follow

$$Q(R) = R[U^{-1}] = \frac{\{\frac{r}{s} : r \in R, s \in U\}}{\frac{r_1}{s_1} = \frac{r_2}{s_2} \text{ if } r_1 s_2 = r_2 s_1}$$

(This like the localization in Commutative Algebra)

Example. $R = \mathbb{Z}, U = \mathbb{Z} \setminus \{0\}$ then $Q(R) = \mathbb{Q}$.
$R = k[x_1, \ldots, x_n]$ then $Q(R) = k(x_1, \ldots, x_n)$.

Definition 5.15. If X is a variety, the total quotient ring of $k[X]$ is written $k(X)$ and is called the *ring of rational functions of* X.

Note. If R is a domain, $U = R \backslash \{0\}$, so $Q(R)$ is the field of fractions of R. So if X is irreducible, $k(X)$ is the field of fractions of $k[X]$.

Proposition 5.16. *Let $\phi : \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ be a rational map admissible on a affine variety $X \subseteq \mathbb{A}^n$. Then ϕ^* induces a k-algebra homomorphism $\phi^* : k[z_1, \ldots, z_n] \to k(X)$. Conversely each such homomorphism arise from a rational map.*

Proof. Write $\phi_i = f_i = g_i$ with f_i and g_i not sharing any irreducible factors. By hypothesis each g_i is a non-zero divisor on $k[X]$. So $\frac{f_i}{g_i}$ is a well defined element of $k(X)$. Thus $\phi^* : k[z_1, \ldots, z_m] \to k(X)$ given by $\phi^*(z_i) = \frac{f_i}{g_i}$ is well defined.

Conversely given $\phi^* : k[z_1, \ldots, z_m] \to k(X)$ write $\phi^*(z_i) = \frac{f_i}{g_i}$ for some $f_i, g_i \in k[x_1, \ldots, x_n]$ with g_i a non-zero divisor on $k[X]$. Then $\phi : \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ defined by $\phi_i(x) = f_i(x)/g_i(x)$ is admissible on X. □

Definition 5.17. Let $X \subseteq \mathbb{A}^n$ be an affine variety. Two rational maps $\phi, \psi : \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ admissible on X are said to be *equivalent on* X if the induced homomorphism $\phi^*, \psi^* : k[z_1, \ldots, z_m] \to k(X)$ are equal.

Example. Let $X = V(x + y) \subseteq \mathbb{A}^2$. Let $\phi : \mathbb{A}^2 \dashrightarrow \mathbb{A}^2$ be defined by $\phi(x, y) = (\frac{3x}{2y^2}, \frac{2x}{3x+5y})$. This is defined on $U_\phi = \{(x, y) : y^2 \neq 0, 3x + 5y \neq 0\}$. Let $\psi : \mathbb{A}^2 \dashrightarrow \mathbb{A}^2$ be defined by $\psi(x, y) = (\frac{3}{2x}, -1)$. This is defined on $U_\psi = \{(x, y) : x \neq 0\}$. These are clearly not the same rational maps but we will show that they are equivalent on X.

$\phi^* : k[z_1, z_2] \to k(x, y)$ is defined by $\phi^*(z_1) = \frac{3x}{2y^2}$ and $\phi^*(z_2) = \frac{2x}{3x+5y}$. And $\psi^* : k[z_1, z_2] \to k(x, y)$ is defined by $\psi^*(z_1) = \frac{3}{2x}$ and $\psi^*(z_2) = -1$. Now in $k(X) = k[x, y]/(x + y)$ we have

$$\begin{aligned} \frac{3x}{2y^2} &= \frac{3x}{2x^2} = \frac{3}{2x} \\ \frac{2x}{3x+5y} &= \frac{2x}{2y} = -1 \end{aligned}$$

So $\phi^*, \psi^* : k[z_1, z_2] \to k(X)$ are equal so ϕ, ψ are equivalent on X.
(Check $\phi = \psi$ on $U_\psi \cap U_\phi \cap X$)

Definition. Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. *A rational map* $\phi : X \dashrightarrow Y$ is an equivalence class of rational maps $\phi : \mathbb{A}^n \dashrightarrow Y$ admissible on X.

Corollary 5.18. *Let $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$ be affine varieties. Then there is a one to one correspondence between rational maps $X \dashrightarrow Y$ and k-algebra homomorphism $k[Y] \to k(X)$.*

Definition 5.19. A rational map $\phi : X \dashrightarrow Y$ is *dominant* if $\phi^* : k[Y] \to k(X)$ is injective.

Example. Let $\phi : \mathbb{A}^1 \dashrightarrow V(x^2 + y^2 - 1)$ defined by $\phi(t) = (\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$. Then ϕ is dominant.

Lemma 5.20. *If $\phi : X \dashrightarrow Y$ is dominant and X is irreducible, then so is Y*

Proof. Since ϕ is dominant we have by definition $\phi^* : k[Y] \to k(X)$ is injective. Since X is irreducible, $k[X]$ is a domain, so $k(X)$ is a field. Hence $k[Y]$ is also a domain and thus Y is irreducible. □

Corollary 5.21. *$V(x^2 + y^2 - 1)$ is irreducible.*

Definition 5.22. Let $Y \subseteq \mathbb{A}^n$ be an affine variety. A *rational parametrisation* of Y is a rational map $\phi : \mathbb{A}^n \dashrightarrow Y$ such that $Y = \overline{\operatorname{im}(\phi)}$, i.e., a dominant rational map $\phi : \mathbb{A}^n \dashrightarrow Y$. Such Y are called *unirational.*

Note. Unirational varieties are irreducible, by the lemma, and we have $k(Y) \hookrightarrow k(x_1, \ldots, x_n)$.

Definition 5.23. A variety X is *rational* if it admits a rational parametrisation $\phi : \mathbb{A}^n \dashrightarrow X$ such that the induced field extension $\phi^* : k(X) \hookrightarrow k(x_1, \ldots, x_n)$ is an isomorphism.

Corollary 5.24. *X is rational if and only if $k(X) \cong k(x_1, \ldots, x_n)$*

Proof. If X is rational then $k(X) \cong k(x_1, \ldots, x_n)$ by definition, so we just need to show the converse. Suppose we have $\phi^* : k(X) \to k(x_1, \ldots, x_n)$. Then $\phi^*|_{k[X]}$ is injective, so defines a dominant rational map $\phi : \mathbb{A}^n \dashrightarrow X$. Hence X is rational. $\square$

Definition. Let X, Y be irreducible varieties. We say X, Y are *birational* if $k(X) \cong k(Y)$ as k-algebra.

Proposition 5.25. *If X, Y are irreducible varieties and $k(X) \cong k(Y)$ then there exists dominant rational maps $X \dashrightarrow Y$ and $Y \dashrightarrow X$ that are inverses.*

Proof. If $\phi^* : k(X) \xrightarrow{\cong} k(Y)$, then $\phi^*|_{k[X]}$is injective, so the corresponding rational map $\phi : Y \dashrightarrow X$ is dominant. Similarly ϕ^{*-1} induces a dominant rational map $\phi^{-1} : X \dashrightarrow Y$. By construction $\phi^* \circ \phi^{*-1} = \operatorname{id}|_Y$.

□

6 Projective Varieties.

Definition 6.1. *Projective Space* $\mathbb{P}^n$ over a field k is $(k^{n+1}\backslash\{0\})/\sim$ where $\underline{v} \sim \lambda\underline{v}$ for $\lambda \in k^* = k\backslash\{0\}$. A point in $\mathbb{P}^n$ correspond to a line through the origin in k^{n+1}.

Notation. $[x_0 : x_1 : \cdots : x_n]$ is the equivalence class of $(x_0, x_1, \ldots, x_n) \in k^{n+1}$.

Recall: A polynomial $f = \sum c_u x^u$ is ***homogeneous*** if $|u| = d$ for all u with $c_u \neq 0$ for some d.

Definition 6.2. An ideal $I \subseteq k[x_0, x_1, \ldots, x_n]$ is homogeneous if $I = \langle f_1, \ldots, f_s\rangle$, where each f_i is homogeneous.

Example. $\left\langle 7x_0^2 + 8x_1x_2 + 9x_1^2, 3x_1^3 + x_2^3\right\rangle$ is, $\left\langle x + y^2, y^2\right\rangle = \left\langle x, y^2\right\rangle$ is.

Definition 6.3. Let $f \in k[x_0, \ldots, x_n]$. Then $f = \sum f_i$ where each f_i is a homogeneous polynomial of degree i. The f_i are called the ***homogeneous components*** of f.

Example. Let I be a homogeneous ideal and let $f \in I$. Then each homogeneous component of f is in I. Idea: we choose $g_1, \ldots, g_s$ homogeneous with $I = \langle g_1, \ldots, g_s\rangle$. Then we can write $f = \sum c_{u_i} x^{u_i} f_i$, where the $f_i$could be repeated. Then $f_i = \sum_{j:\deg(x^{u_j})+\deg(g_i)=i} c_{u_i} x^{u_i} g_i \in I$.

Definition 6.4. Let I be a homogeneous ideal in $k[x_0, x_1, \ldots, x_n]$. The *projective variety* defined by I is $\mathbb{V}(I) = \{[x] \in \mathbb{P}^n : f(x) = 0 \, \text{for all homogenous} \, f \in I\}$

Example.

- Let $I = \langle 2x_0 - x_1, 3x_0 - x_2\rangle$. Then $\mathbb{V}(I) = \{[1 : 2 : 3]\} \subseteq \mathbb{P}^3$.
- $I = \left\langle x_0x_2 - x_1^2\right\rangle$. Then $\mathbb{V}(I) = \{[1 : t : t^2] : t \in k\} \cup \{[0 : 0 : 1]\}$
- $I = \langle x_0, x_1, x_2\rangle \subseteq k[x_0, x_1, x_2]$. $\mathbb{V}(I) = \emptyset$. Note that the weak Nullstellenzatz does not apply here.
- $I = \left\langle x_0x_3 - x_1x_2, x_0x_2 - x_1^2, x_1x_3 - x_2^2\right\rangle \subseteq k[x_0, x_1, x_2, x_3]$. Then $\mathbb{V}(I) = ([1, t, t^2, t^3] : t \in k \cup \{[0 : 0 : 0 : 1]\}$. "The twisted cubic"

Note. Points in $\mathbb{V}(I)$ correspond to lines through $\underline{0}$ in $V(I) \subseteq \mathbb{A}^{n+1}$. $V(I)$ is called the affine cover over I.

Definition 6.5. *The Zariski topology* on $\mathbb{P}^n$ has closed sets $\mathbb{V}(I)$ for $I \subseteq k[x_0, \ldots, x_n]$.

6.1 Affine Charts

Definition 6.6. Let $U_i = \{[u] \in \mathbb{P}^n : x_i \neq 0\}$. We can write $x \in U_i$ uniquely as $[x_0 : \cdots : 1 : \cdots : x_n]$ (1 in i^{th} position). U_i bijection with $\mathbb{A}^n$. $\mathbb{P}^n = \cup_{i=1}^n U_i$ "affine cover of $\mathbb{P}^n$". We can think of $\mathbb{P}^n = U_0 \cup \{[x] : x_0 = 0\}$. See that U_0 is a kind of like $\mathbb{A}^n$ while the set is $\mathbb{P}^{n-1}$ sometime called "hyperplane at infinity". Fix I homogeneous in $k[x_0, \ldots, x_n]$ and let $X = \mathbb{V}(I) \subseteq \mathbb{P}^n$. Let $X \cap U_i = \{[x] \in \mathbb{P}^n : f(x) = 0 \, \forall f \in I\} = \{[x_0 : \cdots : 1 : \ldots, x_n] \in \mathbb{P}^n : f(x_0, \ldots, 1, \ldots, x_n) = 0 \, \forall f \in I\} = V(I_i) \subseteq \mathbb{A}^n$ where $I_i = \langle f(x_0, \ldots, 1, \ldots, x_n) : f \in I\rangle = 1|_{x_1=1}$.

$$X = \bigcup_{i=0}^{n} X \cap U_i.$$

Is a union of affine varieties. This is called an *affine cover*, let $X \cup U_i$ are called *affine charts*.

Example. $X = \mathbb{V}(x_0x_2 - x_1^2) \subseteq \mathbb{P}^n$. Then:

- $X \cap U_0 = V(x_2 - x_1^2) = \{(t, t^2) : t \in k\}$.
- $X \cap U_1 = V(x_0x_2 - 1) = \{(t, \frac{1}{t}) : t \in k\}$.
- $X \cap U_2 = V(x_0 - x_1^2) = \{(t^2, t) : t \in k\}$

Actually $X = (X \cap U_0) \cup (X \cap U_2)$ in this case. We can think of X as created by "gluing together" three affine varieties $X \cap U_0, X \cap U_1, X \cap U_2$. This is how abstract varieties are defined (not covered in this module).

Given an affine variety $X \subseteq \mathbb{A}^n$, we can embed it into $\mathbb{P}^n$ by identifying $\mathbb{A}^n$ with U_i for some i (normally $i = 0$).

Definition 6.7. The *projective closure* of $X \subseteq \mathbb{A}^n$ in $\mathbb{P}^n$ is the Zariski closure of $X \subseteq U_i \subseteq \mathbb{P}^n$ in $\mathbb{P}^n$ (Assume by default U_0)

Example. $X = V(x_2 - x_1^2) = \{(t, t^2) : t \in k\} \subseteq \mathbb{A}^2$. The projective closure is the Zariski closure of $\{[1 : t : t^2] : t \in k\}$. This adds $[0 : 0 : 1]$

Question: Given X how can we compute the projective closure in $\mathbb{P}^n$?

Definition 6.8. Let $f = \sum c_u x^u \in k[x_1, \dots, x_n]$. The *homogenization* of f is $\widetilde{f} = \sum_u x^u x_0^{d-|u|}$ where $d = \max |u|$

Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal. Its *homogenization* is $\widetilde{I} = \left\langle \widetilde{f} : f \in I \right\rangle$

Warning: If $I = \langle f_1, \dots, f_s \rangle$ then we do not always have $\widetilde{I} = \left\langle \widetilde{f_1}, \dots, \widetilde{f_s} \right\rangle$. For example, consider $I = \langle x_1 - 1, x_1 \rangle \subseteq k[x_1]$. We have $I = \langle 1 \rangle$, $\widetilde{I} = \langle 1 \rangle \neq \langle x_1 - x_0, x_1 \rangle = \langle x_1, x_0 \rangle$

Proposition 6.9. *Let $k = \overline{k}$, $I = \sqrt{I} \subseteq k[x_1, \dots, x_n]$. The projective closure of $V(I) \subseteq \mathbb{A}^n$ via the identification $\mathbb{A}^n = U_0$ is $\mathbb{V}(\widetilde{I}) \subseteq \mathbb{P}$*

Proof. If $x \in V(I)$, $f(x) = 0 \, \forall f \in I$ then $\widetilde{f}(I, x) = 0 \, \forall \widetilde{f} \in \widetilde{I}$. So $[1 : x] \in \mathbb{V}(\widetilde{I})$. So the projective closure of $\mathbb{V}(I)$ is contained in $\mathbb{V}(\widetilde{I})$

Conversely, suppose that $f \in k[x_0, \dots, x_n]$ is homogeneous with $f([1 : x]) = 0 \, \forall x \in V(I)$. Then $g = f(1, x) \in I(V(I)) = \sqrt{I} = I$. Then $f = x_0^k \widetilde{g}$ for some $k \geq 0$ so since $g \in I$,$f \in \widetilde{I}$ and thus $\mathbb{V}(\widetilde{I})$ is contained in the projective closure of $V(I)$. ☐

Question: How can we compute $\widetilde{I}$? Answer: Let $<$ be any term order with $\deg(X^u) > \deg(X^v) \Rightarrow X^u > X^v$ (for example we can revlex). Let $G = \{g_1, \dots, g_s\}$ be a Grobner basis for I with respect to $<$. We claim that $\widetilde{I} = \langle \widetilde{g_1}, \dots, \widetilde{g_s} \rangle$.

Proof of above claim. Extend $<$ to a term order $\widetilde{<}$ on $k[x_0, \dots, x_n]$ by setting $x_0^a x^u \widetilde{<} x_0^b x^v$ if $\begin{cases} x^u < x^v & x^u \neq x^v \\ a < b & x^u = x^v \end{cases}$.

Note that $\text{in}_{\widetilde{<}}(\widetilde{f}) = \text{in}_<(f)$. Let $F \in \widetilde{I}$ be a homogeneous polynomial in $k[x_0, \dots, x_n]$. Then $f = \sum A_i \widetilde{f_i}$ for some $f_i \in I$, $A_i \in l[x_0, \dots, x_n]$. Write $f(x_1, \dots, x_n) = F(1, x_1, \dots, x_n) \in k[x_1, \dots, x_n]$. Then $f = \sum A_i(1, x_1, \dots, x_n) f_i$ so $f \in I$. We know that $F = x_0^k \widetilde{f}$ for some $k \geq 0$ so $\text{in}_{\widetilde{<}}(\widetilde{f}) = x_0^k \text{in}_{\widetilde{<}}(\widetilde{f}) = x_0^k \, \text{in}_<(f)$. Since G is a Grobner basis for I with respect to $<$, we have that $\text{in}_<(f_j) | x_0^k \, \text{in}_<(f)$ for some g. Hence $\text{in}_{\widetilde{<}}(f) \in \langle \text{in}_{\widetilde{<}}(\widetilde{g_1}), \dots, \text{in}_{\widetilde{<}}(\widetilde{g_s}) \rangle$. So $\{\widetilde{g_1}, \dots, \widetilde{g_s}\}$ is a Grobner basis for $\widetilde{I}$, hence it generates $\widetilde{I}$. ☐

Proposition 6.10. *Let $k = \overline{k}$. $\mathbb{V}(I) = \emptyset$ if and only if $\langle x_0, \dots, x_n \rangle \subseteq \sqrt{I}$.*

Proof. Let $X = V(I) \subseteq \mathbb{A}^{n+1}$. Then $V(I) = \emptyset$, implies either $X = \emptyset$ so $1 \in I$ or $X = \{0\}$ so $\langle x_0, \dots, x_n \rangle \subseteq \sqrt{I}$.

Conversely if $\langle x_0, \dots, x_n \rangle \subseteq \sqrt{I}$ then $V(I) \subseteq \{0\}$, so $\mathbb{V}(I) = \emptyset$. ☐

Definition 6.11. The ideal $\langle x_0, \dots, x_n \rangle$ is called the *irrelevant ideal.*

Let $X \subseteq \mathbb{P}^n$. *The ideal* $I(X)$ is $I(X) = \langle \text{homogeneous} \, f \in k[x_0, \dots, x_n] : f([x]) = 0 \, \forall x \in X \rangle$

Homogeneous coordinate ring of $X \subseteq \mathbb{P}^n$ is $k[x_0, \dots, x_n]/I(X)$.

Theorem 6.12 (Projective Nullstellensatz). *Let $k = \overline{k}$. Let I be a homogeneous ideal in $[x_0, \dots, x_n]$ with $\langle x_0, \dots, x_n \rangle \nsubseteq \sqrt{I}$. Then $I(\mathbb{V}(I)) = \sqrt{I}$.*

Proof. Let $X = \mathbb{V}(I)$ and let $Y = V(I) \subseteq \mathbb{A}^{n+1}$ be affine cover of X. Then $I(\mathbb{V}(I)) = \{f \text{ homogeneous} : f([x]) = 0 \, \forall [x] \in X\} = \{f : f(x) = 0 \, \forall x \in Y\} = I(Y) = \sqrt{I}$ ☐

Definition 6.13. A projective variety X is *reducible* if $X = X_1 \cup X_2$ with $X_1, X_2 \subsetneq X$ and X_1, X_2 are subvarietes of X.

Exercise: If X is a non-empty irreducible variety then $I(X)$ is prime.

6.2 Morphisms of projective varieties.

A rational map of degree d, $\phi : \mathbb{P}^n \dashrightarrow \mathbb{P}^m$ is given by $\phi([x_0 : \cdots : x_n]) = [\phi_0(x_0, \ldots, x_n) : \cdots : \phi_m(x_0, \ldots, x_n)]$ where ϕ_i are homogeneous polynomials of degree d in $k[x_0, \ldots, x_n]$.

Example. $\phi([s : t]) = [s^2 : st : t^2]$ a rational map $\mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ of degree 2. (actually a morphism)

$\phi([s : t]) = [s^3 : s^2 : st^2]$ a rational map $\mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ of degree 3. This is not defined at $[s : t] = [0 : 1]$ (not a morphism)

A rational map $\phi : \mathbb{P}^n \dashrightarrow \mathbb{P}^m$ is a *morphism* if ϕ is defined for all $[x] \in \mathbb{P}^n$.

Note. We don't need to use rational functions as we can clear denominators. The polynomials need to be homogeneous of the same degree to make the map well defined, i.e., independent of representative of $[x] \in \mathbb{P}^n$.

ϕ is a morphism if and only if $V(\phi_0, \ldots, \phi_m) \subseteq \mathbb{P}^n$ is empty if and only if $\langle x_0, \ldots, x_n \rangle \subseteq \sqrt{\langle \phi_0, \ldots, \phi_m \rangle}$

Definition 6.14. A rational map $\phi_i : \mathbb{P}^n \dashrightarrow \mathbb{P}^m$ is *linear* if degree $\phi_i = 1\, \forall i$.

In that case ϕ is determined by a $m + 1 \times n + 1$ matrix $A = (a_{ij})$. Then ϕ is a morphism when $\text{rank} A = n + 1$ (or $\ker(A) = 0$). In the case $n = m$, then ϕ is a morphism if and only if A is invertible.

The set $\{\phi : \phi([x]) = [Ax] \, \text{for an invertible} \, (n+1) \times (n+1) \, \text{matrix} \, A\} = \text{Aut}(\mathbb{P}^n)$ forms a group under composition. Note that $A_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $A_2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ define the same morphism. If fact $\text{Aut}(\mathbb{P}^n) = \text{GL}_{n+1} / k^* =: \text{PGL}_{n+1}$ where $k^* = \{\lambda I\}$

6.2.1 Veronese Embedding

Definition 6.15. The morphism $\phi : \mathbb{P}^1 \dashrightarrow \mathbb{P}^d$ given by $\phi([x_0 : x_1]) = [x_0^d : x_0^{d-1} x_1 : \cdots : x_1^d]$ is called the d^{th} *Veronese embedding.*

$Y = \text{im}(\phi) = \mathbb{V}(y_1 y_{j+1} - y_{i+1} y_j : 0 \le i, j \le n - 1)$. Y is called the *rational normal curve of degree d.*

Example. There are $\binom{n+d}{d}$ monomials of degree d. To see this, notice that any string of d $*$ and n $|$ correspond uniquely to a monomial of degree d, for example, $***|*|**$ correspond to $x_0^3 x_1 x_2^3$ while $||**|*$ correspond to $x_2^3 x_3$. So the number of the monomials is the number of such strings.

The d^{th} *Veronese embedding* of $\mathbb{P}^n$ is $\mathbb{P}^n \dashrightarrow \mathbb{P}^{\binom{n+d}{d}-1}$ defined by $[x_0 : \cdots : x_n] \mapsto [x_0^d : x_0^{d-1} x_1 : \cdots : x_n^d]$ (all monomial of degree d). The image of ϕ is $\mathbb{V}(z_\alpha z_\beta - z_\gamma z_\delta : \alpha + \beta = \gamma + \delta)$ where z are coordinates on $k[z_\alpha : \alpha \in \mathbb{N}^{n+1}, \sum \alpha_i = d]$. This is a generalization of $y_i \leftrightarrow z_{d-i,i}$. We prove all of this in the following proposition

Proposition 6.16. $\text{im}(\phi)$ *is closed and equals* $\mathbb{V}(z_\alpha z_\beta - z_\gamma z_\delta : \alpha + \beta = \delta + \gamma)$*, where z are coordinates* $k[z_\alpha : \alpha \in \mathbb{N}^n : \sum \alpha_i = d]$.

Proof. Let $Z = \mathbb{V}(z_\alpha z_\beta - z_\gamma z_\delta : \alpha + \beta = \delta + \gamma)$. If $z = \phi(x)$ then $z_\alpha z_\beta - z_\gamma z_\delta = x^\alpha x^\beta - x^\delta x^\gamma = 0$, so if $\alpha + \beta = \gamma + \delta$ we have $\text{im}(\phi) \subseteq \mathbb{Z}$.

Conversely we want to consider $z \in Z$ and want to find $[x] \in \mathbb{P}^n$ with $\phi([x]) = [z]$. We first show there is i with $z_{de_i} \neq 0$. To see this, suppose $z_\alpha \neq 0$ for some α (there must be some such α). Without loss of generality $\alpha_0 > 0$. If $\alpha_0 < \frac{d}{2}$ we write $2\alpha = (2\alpha e_0 + \widetilde{\alpha}) + \alpha''$ where $\widetilde{\alpha}_0, \alpha''_0 = 0$ and $\sum \alpha''_i = d$ (For example if $d = 5, \alpha = (2, 2, 1)$ then $(4, 4, 2) = (4, 1, 0) + (0, 3, 2)$)

Then $z_\alpha^2 = z_{2\alpha_0 e_0 + \widetilde{\alpha}} z_{\alpha''}$ (here we have $\alpha = \beta = \alpha, \gamma = 2\alpha_0 e_0 + \widetilde{\alpha}, \delta = \alpha''$). So $z_\alpha \neq 0$ implies that $z_{2\alpha_0 e_0 + \widetilde{\alpha}} \neq 0$. So after repeated applications, we may assume $\alpha_0 > \frac{d}{2}$. Then we write $2\alpha = de_0 + (2\alpha - de_0)$, then $z_2^\alpha = z_{de_0} z_{2\alpha - de_0}$, so $z_{de_0} \neq 0$. Now set $x_i = \frac{z_{(d-1)e_0 + e_i}}{z_{de_0}}$ for $1 \le i \le n$ and $x_0 = 1$. Set $[z'] = \phi([x])$.

We now show that $[z'] = [z]$ to show this we show $z'_\alpha z_{de_0} = z_\alpha$. We do this by a proof on induction on $\sum_{i=1}^n \alpha_i$. The base case is by definition/construction. The general case follows from $z_\alpha z_{de_0} = z_{\alpha-e_i+e_0} z_{(d-1)e_0+e_i}$ for $\alpha_i > 0$. Note that this is also true for z'. Hence $z_{de_0} z'_\alpha = z_{de_0} z'_{de_0} z'_\alpha = z_{de_0} z'_{\alpha-e_1+e_0} z'_{(d-1)e_0+e_i} = z_{\alpha-e_i+e_0} z'_{(d-1)e_0+e_i} = \frac{z_{\alpha-e_1+e_0} z_{(d-1)e_0+e_p}}{z_{de_0}} = z_\alpha$. $\square$

6.2.2 Segre Embedding

The Segre embedding realizer $\mathbb{P}^n \times \mathbb{P}^m$ as a subvarieties of $\mathbb{P}^{(n+1)(m+1)-1}$. We map $([x],[y]) \in \mathbb{P}^n \times \mathbb{P}^m$ to $\phi([x],[y]) = ([x_i y_j] : 0 \le i \le n, 0 \le j \le m)$.

Proposition 6.17. $\operatorname{im}(\phi) = \mathbb{V}(z_{ij}z_{kl} - z_{il}z_{kj} : 0 \le i,k \le n, 0 \le j,l \le m)$ *where the z are coordinates on $k[z_{ij} : 0 \le i \le n, 0 \le j \le m]$. (Notice that they are the 2 by 2 minors of a generic $(n+1)\times(m+1)$ matrix (z_{ij})*

Proof. Let $Y = \mathbb{V}(z_{ij}z_{kl} - z_{il}z_{kj} : 0 \le i,k \le n, 0 \le j,l \le m)$. If $z = \phi([x],[y])$ then $z_{ij}z_{kl} - z_{il}z_{kj} = x_i y_j x_k y_l - x_i y_l x_k y_j = 0$ so $\operatorname{im}(\phi) \subseteq Y$.

Conversely, given $[z] \in Y$, without loss of generality, we may assume $z_{00} \ne 0$. Set $x_i = z_{i0}/z_{00}$ and $y_j = z_{0j}/z_{00}$, $x_0 = y_0 = 1$, and let $z' = \phi([x],[y])$. Then the equation on $z_{ij}z_{00} - z_{i0}z_{0j}$ implies that $[z'] = [z]$. $\square$

6.2.3 Grassmannian

The Grassmannian $G(d,n)$ parametrizes all d-dimensial subspace of k^n

Example. $G(1,n) = \mathbb{P}^{n-1}$ (a one dimensional subspace is a line through 0)
$G(n-1,n) = \mathbb{P}^{n-1}$

We'll describe $G(d,n)$ as a projective variety by the Pucker $G(d,n) \hookrightarrow \mathbb{P}^{\binom{n}{d}-1}$. Let $V \subseteq k^n$ be a d-dimensial subspace. Choose a basis $v_1,\dots,v_d$ for V and write $A_v = \begin{pmatrix} v_1 \\ \vdots \\ v_d \end{pmatrix}$ for the $d \times n$ matrix with rows the v_i. Map V to the vector of $d\times d$ of A_V in $\mathbb{P}^{\binom{n}{d}-1}$, for example $\phi : V \mapsto (1:3:4:-1:-2:-2)$. We name the coordinates on $\mathbb{P}^{\binom{n}{d}-1}$, x_I where $I \subseteq \{1,\dots,n\}$ and $|I| = d$. I indexes the columns of the $d \times d$ submatrix of A_v whose determinant is $\phi(V)_I$

Note.
1. $\phi(V)$ is not the zero vectors, since rank $A_V = d$, so A_v has a non-vanishing minor of size d
2. If we choose a different basis $v'_1,\dots,v'_d$ for V, then $A'_v = UA_V$ where U is a $d\times d$ invertible matrix (in fact the change of basis matrix). So the Ith minor of A'_v is $\det(U)$. So A_V, A'_V gives the same point in $\mathbb{P}^{\binom{n}{d}-1}$. This means the map $\phi : V \mapsto \phi(V) \in \mathbb{P}^{\binom{n}{d}-1}$is well defined
3. We can recover V from $\phi(V)$.

   Example. If $\phi(V) = [1:0:0:0:0:0]$ then $V = \operatorname{span}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\right)$. Since $\phi(V)_{12} = 1$ we can assume $A_V = \begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix}$.

Let I be an index with $\phi(V)_I \ne 0$ (this exists by 1). Let B be the $d\times d$ submatrix of A_V indexed by I. Then $\det(B) \ne 0$. So $A'_V = B^{-1}A_V$ has an identity matrix in the column indexed by I. But then for $j \notin I$, $(A'_V)_{ji} = \pm\phi(V)_{I\setminus\{1\}\cup\{j\}}$.

Question: What does $\operatorname{im}(\phi)$ look like?

Example. $G(2,4)$ assume that $\phi(V)_{12} \ne 0$ so that we can take $A_V = \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix}$, $\phi(V) = [1:c:d:-a:-b:ad-bc]$. Note $\phi(V) \subseteq \mathbb{V}(x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23})$. The equation $x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}$

is invariant (up to sign) under the S_4 action on the labels, where we set $x_{21} = -x_{12}$. This says that $\phi(V) \subseteq \mathbb{V}(x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23})$ any V. Alternatively, we could check the other row reduced forms.

Conversely, if $[z] \in \mathbb{V}(x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23})$ with $z_{12} \neq 0$, then $[z] = \phi(V)$ for $V = \text{row}\begin{pmatrix} 1 & 0 & -\frac{z_{23}}{z_{12}} & -\frac{z_{23}}{z_{12}} \\ 0 & 1 & \frac{z_{13}}{z12} & \frac{z_{14}}{z_{12}} \end{pmatrix}$

The formula $x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}$ is called a *Plucker relation.*

For the embedding $G(d,n) \hookrightarrow \mathbb{P}^{\binom{n}{d}-1}$ we get a Plucker relation PJ_1J_2 for all $J_1, J_2 \subseteq \{1, \dots, n\}$ with $|J_1| = d-1$, $|J_2| = d+1$.

$$PJ_1J_2 = \sum_{j \in J_2} (-1)^{\text{sgn}(j,J_1)} X_{J_1 \cup j} X_{J_2 \setminus j}$$

where $X_{J_1 \cup j} = 0$ if $j \in J_1$ and $\text{sgn}(j, J_1) = \#(i \in J_i : i > j) + \#(i \in J_2 : i < j)$

Example. $n = 4$, $d = 2$, $J_1 = \{1\}$ and $J_2 = \{2,3,4\}$. Then $PJ_1J_2 = x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}$

Definition 6.18. Let $I_{d,n} = \langle PJ_1J_2 : J_1, J_2 \subseteq \{1, \dots, n\}, |J_1| = d-1, |J_2| = d+1 \rangle \subseteq k[X_1 : |I| = d]$

Theorem 6.19. $G(d,n) = \text{im}(\phi) = \mathbb{V}(I_{d,n})$

Proof. Assignment sheet. □

Question; What are the affine charts for $G(d,n)$?

Answer: $G(d,n) \cap U_I$ is V which look like $A_V = (I_d | \widetilde{A})$ (where I_d are the columns of I and $\widetilde{A}$ the other columns, not that $\widetilde{A}$ is an arbitary $d \times (n-d)$ matrix). So $G(d,n) \cap U_I \cong \mathbb{A}^{d(n-d)}$.

Check: $G(2,4) \cap U_{1,2} = V(x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}) \subseteq \mathbb{A}^5$. This is isomorphic to $\mathbb{A}^4$ since $k[x_{13}, x_{14}, x_{23}, x_{24}, x_{34}]/(x_{12}x_{34} - x_{13}x_{24} + x_{14}x_{23}) \cong k[x_{13}, x_{14}, x_{23}, x_{24}] \cong k[\mathbb{A}^4]$

We can think of $G(d,n)$ as $\binom{n}{d}$ copies of $\mathbb{A}^{d(n-d)}$ "glue together". This worked for any field, e.g., the real Grassmannian is the manifold of dimension $d(n-d)$. Similarly for $\mathbb{C}$.

7 Dimension and Hilbert Polynomial

Definition 7.1. A ring R is *$\mathbb{Z}$-graded* if there is a decomposition (as groups) $R \cong \oplus_{i\in\mathbb{Z}} R_i$ with $R_iR_j \subseteq R_{i+j}$. The R_i are called the *graded pieces* and $f \in R_i$ is homogeneous of degree i.

A *graded* k-algebra is a k-algebra R with $cf \in R_i \,\forall f \in R_i$ (so each R_i is a k-vector space). Then $k \subseteq R_0$ (normally for our examples $R_0 = k$)

Example. $R = k[x_0, \ldots, x_n]$, R_i are polynomials of degree i.

$S = k[x_0, \ldots, x_n]$, I homegenous ideal. $R = S/I$ then $R_i = S_i/I_i$.

$X \subseteq \mathbb{P}^n$ a projective variety, $R(X) := k[x_0, \ldots, x_n]/I(X)$ is the projective coordinate ring of X.

Definition 7.2. Let R be a graded k-algbera with $\dim_k(R_i) < \infty$ for all i. The *Hilbert Function* of R is $H_R(d) = \dim_k R_d$ (note $H_R : \mathbb{Z} \to \mathbb{N}$).

Example. Let $R = k[x_0, \ldots, x_n]$. Then $H_R(d) = \binom{n+d}{d} = \binom{n+d}{n}$ since a basis for R_d is the set of monomials of degree d.

$S = k[x_0, x_1, x_2]$ and f homogeneous of degree 3. Let $R = S/\langle f\rangle$.

i	$\dim_k(S/\langle f\rangle)_i = \dim_k(S) - \dim_k \langle f\rangle_i$
<0	0
0	1
1	3
2	6
3	$\binom{2+3}{2} - 1 = 9$
4	$\binom{2+4}{2} - 3 = 12$

In general we have the following graded short exact sequence:

$$0 \longrightarrow S \longrightarrow S \longrightarrow S/\langle f\rangle \longrightarrow 0$$

$$g \longmapsto gf \quad g \longmapsto \overline{g}$$

So $\dim_k(S/\langle f\rangle)_d = \dim_k S_d - \dim_k S_{d-3}$ (assuming $d \geq 1$)

How can we compute H_R?

Proposition 7.3. *Let $I \subseteq S = k[x_1, \ldots, x_n]$ and let $<$ be a term order. The (image of the) monomials in S not in the initial ideal of I form a k-basis for S/I. Thus if I is homogeneous $H_{S/I}(d) = H_{S/\operatorname{in}_<(I)}(d)$*

Proof. Let f be polynomial in S. Then the remainder of dividing f be a Grobner basis for I with respect to $<$ is a polynomial g with $f - g \in I$ and $g = \sum c_u x^u$ where $c_u \neq 0$ implies $c^u \notin \operatorname{in}_<(I)$. So $f = g$ in S/I and $g \in \operatorname{span}\{x^U : x^U \notin \operatorname{in}_<(I)\}$, so this set spans S/I. If I is homogeneous and f has degree d, then so does g, so the set of monomials not in $\operatorname{in}_<(I)$ of degree d spans $(S/I)_d$. To see that these sets are linearly independent, note that if $f = \sum c_u x^u$ is a linear dependence, then $f \neq 0$ but $f \equiv 0$ in S/I, hence $f \in I$ and $c_u \neq 0 \Rightarrow x^u \notin \operatorname{in}_<(I)$. Then $\operatorname{in}_<(f) \notin \operatorname{in}_<(I)$ which contradicts $f \in I$. So we conclude that $\{x^u : x^u \notin \operatorname{in}_<(I)\}$ is linearly independent so is a basis for S/I. If I is homogeneous then $\{x^u : \deg(x^u) = d, x^u \notin \operatorname{in}_<(I)\}$ is a basis for $(S/I)_d$, as well as a basis for $(S/\operatorname{in}_<(I))_d$. So the Hilbert functions are equal. $\square$

This reduces the question to "how can we compute $H_{S/m}$for m a monomial ideal?" The key point is the following short exact sequence. Let I be a homogeneous ideal and f homogeneous of degree d. Then we have the following s.e.s

$$0 \to S/(I:f) \xrightarrow{\phi} S/I \xrightarrow{\psi} S/(I,f) \to 0$$

where $(I:f) = \{g \in S : fg \in I\}$ and $(I,f) = I + \langle f\rangle$. The map ϕ is defined by $g \mapsto fg$ while the map ψ is defined by $g \mapsto \overline{g}$. We check that this sequence is exact.

1. ϕ is injective: If $fg \in I$ then $g \in (I:f)$

2. $\mathrm{im}(\phi) = \ker(\psi)$:
   "$\subseteq$": $g \in S, fg \in I + \langle f \rangle$ so $\mathrm{im}(\phi) \subseteq \ker(\psi)$.
   "$\supseteq$": Suppose $g \in \ker(\psi)$ then $g = i + hf$ for $i \in I$. Hence $g - hf = i \in I$, so $g \equiv hf$ in S/I, so $g = \phi(h) \in \mathrm{im}(\phi)$.

3. ψ is surjective since $I + \langle f \rangle \supseteq I$.

This short exact sequence is graded, i.e., $0 \to (S/(I:f))_m \to (S/I)_{m+d} \to (S/(I,f))_{m+d} \to 0$. Recall: given an exact sequence $0 \to U \to V \to W \to 0$ of vector space we have $V \cong U \oplus W$. So $\dim V = \dim U + \dim W$. In our case $\dim_k(S/I)_{m+d} = \dim_k(S/(I:f))_m + \dim_k(S/(I,f))_{m+d}$. Apply this when I is a monomial ideal and f a variable. Then $(I:f),(I,f) \supseteq I$. If f is chosen carefully we have strict containment, so eventually $(I:f),(I,f)$ are monomial prime ideals, which we know the Hilbert function of.

Lemma 7.4. *Let $I = \langle x_{i_1}, \ldots, x_{i_s} \rangle \subseteq S = k[x_0, \ldots, x_n]$ be prime. Then $H_{S/I}(m) = \binom{m+n-s}{m-s} = \binom{m+n-s}{n}$*

Proof. $S/I \cong k[x_j : j \neq i_k \text{ for any } k]$. This has Hilbert function $\binom{n-s+m}{m} = \binom{n-s+m}{n-s}$. This is a polynomial in $m \geq -(n-s)$ □

Example. Let $I = \langle x_0x_3, x_0x_2, x_1x_3 \rangle \subseteq S = k[x_0, x_1, x_2, x_3]$. Let us choose $f = x_0$. Then $(I:f) = \langle x_2, x_3 \rangle$ and $(I,f) = \langle x_0, x_1x_3 \rangle$. So $H_{S/I}(d) = H_{S/\langle x_2,x_3 \rangle}(d-1) + H_{S/\langle x_0, x_1x_3 \rangle}(d)$. Take $f = x_1$. Then $(\langle x_0, x_1x_3 \rangle : x_1) = \langle x_0, x_3 \rangle$and $(\langle x_0, x_1x_3 \rangle, x_1) = \langle x_0, x_1 \rangle$. So $H_{S/I}(d) = H_{S/\langle x_1,x_3 \rangle}(d-1) + H_{S/\langle x_0,x_3 \rangle}(d-1) + H_{S/\langle x_0,x_1 \rangle}(d) = d + d + d + 1 = 3d + 1$. This is valid for $d \geq 0$.

Theorem 7.5. *Let I be a homogeneous ideal in $S = k[x_0, \ldots, x_n]$. Then there exists a polynomial $P \in \mathbb{Q}[t]$ such that $H_{S/I}(d) = P(d)$ for $d \gg 0$.*

Proof. Since $H_{S/I} = H_{S/\mathrm{in}_<(I)}$, we may assume that I is a monomial ideal. The case I is a monomial prime was the lemma. The proof is by Noetherian induction.

Given a monomial ideal I that is not prime, we may assume that the theorem is true for all monomial ideals containing I. Choose a variable x_i properly dividing a generator of I. This must exists since I is not prime. Then $(I:x_i),(I,x_i) \supsetneq I$. By induction there exists $P_1, P_2 \in \mathbb{Q}[t]$ with $H_{S/(I:x_i)}(d) = P_1(d)$ for $d \gg 0$ and $H_{S/(I,x_i)}(d) = P_2(d)$ for $d \gg 0$. Then $H_{S/I}(d) = P_1(d-1) + P_2(d)$ for $d \gg 0$ and this is a polynomial in d. □

Definition 7.6. Let $X \subseteq \mathbb{P}^n$ be a projective variety. The polynomial $P := P_x$ of the theorem for $I = I(X)$ is called the *Hilbert Polynomial.*

Let $X \subseteq \mathbb{P}^n$ be a projective variety. Then the *dimension* of X is the degree of the Hilbert Polynomial.

Example.
1. If $V \subseteq k^{n+1}$ is a subspace of $\dim(d+1)$ then $\mathbb{P}(V) \subseteq \mathbb{P}^n$ is a subsvariety of dimension d

2. $X =$ twisted cubic $=$image of $\phi : \mathbb{P}^1 \to \mathbb{P}^3$ defined by $[t_0, t_1] \mapsto [t_0^3, t_0^2t_1, t_0t_1^2, t_1^3] = \mathbb{V}(x_0x_3 - x_1x_2, x_0x_2 - x_1^2, x_1x_3 - x_2^2) = \mathbb{V}(I)$. $\mathrm{in}_<(I) = \langle x_0x_3, x_0x_2, x_1x_3 \rangle$ (where $x_0 > x_1 > x_2 > x_3$). Then from the previous work we have $H_k[x_0, \ldots, x_3]/\mathrm{in}_<(I) = 3d + 1$ for $d \geq 1$, so $\dim(X) = 1$

There are many different (equivalent) definition of dimension. Proving they are equivalent is non-trivial. For example, for $X \subseteq \mathbb{A}^n$ we can define $\dim(X)$ to be the dimension of the projective closure of X (See Eisenbud Commutative Algebra, Chapters 8-13)

7.1 Singularities

How close is a variety to a manifold?

Let $X = V(f) \subseteq \mathbb{A}^n$. Fix $\underline{a} \in X$. What is the tangent plane to X at $\underline{a}$?

Example.
- $n = 2$
  - $X = V(y - f(x))$, for example $X = V(y - x^2)$. The tangent line at a is $(y - a_2) = \frac{df}{dx}|_a(x - a_1)$

  - $X = V(f(x,y))$, for example $X = V(y^2 + x^2 - 1)$. The slope is $\frac{dy}{dx} = -\frac{\frac{df}{dx}}{\frac{df}{dy}}$. Tangent line is $y - a_2 = \frac{dy}{dx}|_a(x - a_1)$. So $\frac{df}{dy}(y - a_2) = -\frac{df}{dx}(x - a_1) \Rightarrow \frac{df}{dy}(y - a_2) + \frac{df}{dx}(x - a_1) = 0$.

- $n = 3$. $X = V(x^2 + y^2 + z^2 - 1)$, $\underline{a} = (1,0,0)$, the tangent plane to X at $\underline{a}$ is spanned by $(0,1,0), (0,0,1)$, i.e., $\{x = 1\}$. $\triangledown f(\underline{a}) = \begin{pmatrix} 2x \\ 2y \\ 2z \end{pmatrix} |_{1,0,0} = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \Rightarrow 2x - x = 0$.

The tangent space to the variety of f at $\underline{a}$ is $T_{\underline{a}}(X) = \{(y_1, \dots, y_n) : \sum \frac{df}{dx_i}|_a(y_i - a_i) = 0\}$. This is a hyperplane with normal vector $\triangledown f(a)$ unless $\triangledown f(a) = 0$

Example. $X = V(x^3 - y^2)$, $\underline{a} = (0,0)$. Then $\triangledown f(\underline{a}) = \begin{pmatrix} 3x^2 \\ -2y \end{pmatrix} |_a = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. So $T_{0,0}(X) = \{(y_1, y_2) : 0y_1 + 0y_2 = 0\} = \mathbb{A}^2$. If $a = (1,1)$ then $\triangledown f(\underline{a}) = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$. so $T_{(1,1)}(X) = \{(y_1, y_2) : 3y_1 - 2y_2 = 0\} = \{y_2 = \frac{2}{3}y_1\}$

Definition 7.7. $X = V(f)$ is *singular* at a point $\underline{a} \in X$ if the tangent space to X at $\underline{a}$ is not a hyperplane.

Let $X \subseteq \mathbb{A}^n$, fix $\underline{a} \in X$. The *tangent space* to X at $\underline{a}$ is $T_{\underline{a}}(X) = \underline{a} + \{(y_1, \dots, y_n) : \sum \frac{df}{dx_i}|_a(y_i - a_i) = 0 \, \forall f \in I(X)\}$, i.e., $T_{\underline{a}}(X) = \cap_{f : X \subseteq V(\langle f \rangle)} T_{\underline{a}}(V(f))$.

Example.

- $X = V(x^2 - y, x^3 - 2)$ and $\underline{a} = (1,1,1)$. Then $T_{\underline{a}}(X) = \{(y_1, y_2, y_3) : 2y_1 - y_2, 3y_1 - y_3 = 0\} + (1,1,1) = (1,1,1) +$ span of $(1,2,3)$

- $X = V(x^2 - y^2, xz, yz) = V(x - y, z) \cup V(x + y, z) \cup V(x, y)$.
  - $\underline{a} = (1,1,0)$ then $T_{\underline{a}} = \{(y_1, y_2, y_3) : 2y_1 - 2y_2 = 0, y_3 = 0\} + (1,1,0) = \text{span}(1,1,0)$
  - $\underline{a} = (1,-1,0)$ then $T_{\underline{a}}(X) = \{(y_1, y_2, y_3) : 2y_1 + 2y_2 = 0, y_3 = 0\} + \{1,-1,0\} = \text{span}(1,-1,0)$
  - $\underline{a} = (0,0,1)$ then $T_{\underline{a}}(X) = \text{span}(0,0,1)$
  - $\underline{a} = (0,0,0)$ then $T_{\underline{a}}(X) = \mathbb{A}^3$.