1 Geometric Representation

The “Geometric Representation” of an algebraic variety \( V \) is a special kind of triangular representation \( T = \{ f_1, \ldots, f_n \} \) where \( f_1 \in k[u_1, \ldots, u_m,x_1] \) monic in \( x_1 \) and

\[
f_i = p_i(u_1, \ldots, u_m)x_i - q_i(u_1, \ldots, u_m, x_1) \quad i = 2, \ldots, n
\]

such that \( p_i \neq 0 \) and \( q_i \) is pseudo-reduced modulo \( f_1 \). Similarly to the triangular representation computed by Wu’s method, we will require that the polynomials which pseudo-reduce to zero modulo \( T \) are the ones which vanish on \( V \) generically (see previous lecture notes). Geometric representation of higher dimensional varieties were first used by [GH91].

Not all varieties admit such a simple geometric representation. First of all, since the \( V(T) \) is always ”equidimensional”, i.e. each of its irreducible components have the same dimension, therefore \( V \) has to be equidimensional as well. \( V \) being equidimensional is almost sufficient for the geometric representation to exist. In this lecture notes we will prove that there exists a linear change of coordinates such that in the new coordinate system \( V \) admits a geometric representation. As it turns out, a random linear change of variables will work with high probability. In later lecture notes we will give methods to compute the geometric representation.

First we discuss the case when \( m = 0 \), i.e. \( V \) is zero dimensional.

1.1 Zero Dimensional Case

In the zero dimensional case the Geometric Representation is called Rational Univariate Representation (see [Rou96, Rou99]). The following theorem, called the “Shape Lemma”, is the heart of the theory behind the rational univariate representation:

**Theorem 1.1** (Shape Lemma). *Let \( k \) be algebraically closed. Let \( I \) be a zero dimensional radical ideal in \( k[x_1, \ldots, x_n] \). Assume that \( V(I) \) has \( m \) points such that their \( x_1 \)-coordinates are all distinct. Then the reduced Gröbner
basis $G$ for $I$ with respect to the lexicographic order with $x_1$ being the last variable has the following form: $G$ consists of $n$ polynomials

\[ g_1 = x_1^m + h_1(x_1) \]
\[ g_2 = x_2 + h_2(x_1) \]
\[ \vdots \]
\[ g_n = x_n + h_n(x_1) \]

where $h_1, \ldots, h_n$ are polynomials in $x_1$ of degree at most $m - 1$.

Proof. First we prove that the equivalence classes $[1], [x_1], \ldots, [x_1^{m-1}]$ form a basis for the $k$-vector space $k[x_1, \ldots, x_n]/I$. They are linearly independent over $k$, otherwise there exist $c_0, \ldots, c_{m-1} \in k$ such that

\[ g(x_1) := c_0 + c_1 x_1 + \cdots + c_{m-1} x_1^{m-1} \in I. \]

Let $\xi_{1,1}, \ldots, \xi_{m,1}$ be the $m$ distinct first coordinates of the points in $V(I)$. Since $g \in I$, we have $g(\xi_{i,1}) = 0$ for all $i = 1, \ldots, m$, which gives a homogeneous linear systems for $c_0, \ldots, c_{m-1}$ with coefficient matrix being a Vandermonde matrix. Using the fact that the Vandermonde matrix of $m$ distinct numbers is non-singular implies that all $c_i = 0$.

To prove that $[1], [x_1], \ldots, [x_1^{m-1}]$ generates $k[x_1, \ldots, x_n]/I$, it suffices to prove that

\[ \dim_k k[x_1, \ldots, x_n]/I \leq m. \]

Consider the map

\[ \phi : k[x_1, \ldots, x_n]/I \to \mathbb{C}^m; \quad [f] \mapsto (f(\xi_1), \ldots, f(\xi_m)) \quad \xi_j \in V(I). \]

If $[f_0]$ is in the kernel of $\phi$ then $f_0 \in I(V(I)) = \sqrt{I} = I$, thus $[f_0] = 0$. This proves that $[1], [x_1], \ldots, [x_1^{m-1}]$ form a basis for $k[x_1, \ldots, x_n]/I$.

Now, if we express $[x_1^m], [x_2], \ldots, [x_n]$ in this basis, we get that polynomials of the form $g_1, \ldots, g_n$ lie in the ideal $I$. Thus $V(I) \subseteq V(g_1, \ldots, g_n)$. Since $g_1, \ldots, g_n$ has at most $m$ common roots, therefore $V(g_1, \ldots, g_n) = V(I)$ which implies that

\[ I = \langle g_1, \ldots, g_n \rangle \]

since $I$ is radical. Note that $g_1, \ldots, g_n$ forms a Gröbner basis for the order described in the claim. \qed
1.2 Multivariate Case

The multivariate version of the Shape Lemma is as follows:

**Theorem 1.2** (Geometric Resolution). Let $k$ be a field of characteristic zero and $\overline{k}$ be its algebraic closure. Let $I \subset k[x_1, \ldots, x_t]$ be a radical ideal such that all irreducible components of $\mathbf{V}(I) \subset \overline{k}^t$ have dimension $m$. Then there exists a linear change of coordinates

$$y_1 = \sum_{i=1}^{t} c_{1,i} x_i,$$

$$\vdots$$

$$y_t = \sum_{i=1}^{t} c_{t,i} x_i$$

such that $y_1, \ldots, y_m$ are algebraically independent over the irreducible components of $\mathbf{V}(I)$, and if $\tilde{I} \subset k[y_1, \ldots, y_t]$ is the ideal obtained from $I$ after the change of variables, then the ideal generated by $\tilde{I}$ in $k(y_1, \ldots, y_m)[y_{m+1}, \ldots, y_t]$ is the same as

$$\langle P, L_{m+1}, \ldots, L_t \rangle \subset k(y_1, \ldots, y_m)[y_{m+1}, \ldots, y_t],$$

where $P \in k[y_1, \ldots, y_{m+1}]$ is monic in $y_{m+1}$ and

$$L_{m+2} = Q_{m+2}(y_1, \ldots, y_m) y_{m+2} + R_{m+2}(y_1, \ldots, y_{m+1}),$$

$$\vdots$$

$$L_t = Q_t(y_1, \ldots, y_m) y_t + R_t(y_1, \ldots, y_{m+1}),$$

with $Q_{m+i} \in k[y_1, \ldots, y_m]$, $R_{m+i} \in k[y_1, \ldots, y_m, y_{m+1}]$ and $\deg_{y_{m+1}}(R_{m+i}) < \deg_{y_{m+1}}(P)$ for all $i = 2, \ldots, m-t$.

We will need to prove three lemmas in order to prove the Theorem 1.2. These lemmas are important on their own right.

**Lemma 1.3.** Let $I \subset k[x_1, \ldots, x_t]$ be a radical ideal such that all irreducible components of $\mathbf{V}(I) \subset \overline{k}^t$ have dimension $m$. Then there exists coordinates $x_{i_1}, \ldots, x_{i_m}$ such that the homomorphism

$$\varphi : k[x_{i_1}, \ldots, x_{i_m}] \to k[x_1, \ldots, x_t]/I$$

is injective.
Remark 1.4. \( \varphi \) being injective is equivalent to \( x_{i_1}, \ldots, x_{i_m} \) being algebraically independent over some of the irreducible components of \( V(I) \). Moreover, if \( \overline{k} \) is algebraically closed, then \( \varphi \) is injective if and only if the projection
\[
\pi : \overline{k}^t \to \overline{k}^m; \quad (x_1, \ldots, x_t) \mapsto (x_{i_1}, \ldots, x_{i_m})
\]
restricted to \( V(I) \) is surjective.

Example 1.5. As an example, if \( I = \langle x^2 + y^2 - 1 \rangle \subset k[x, y] \) then \( m = 1 \) and we can choose either \( x \) or \( y \) to be algebraically independent over \( V(I) \). If \( I = \langle x - 3 \rangle \subset k[x, y] \) then \( m = 1 \), but \( x \) is not free over \( V(I) \).

Proof of Lemma 1.3. If \( m = 0 \) then we don’t need to prove anything. Assume that \( m \geq 1 \). For \( j = 1, \ldots, t \) we define
\[
\varphi_j : k[x_j] \to k[x_1, \ldots, x_t]/I.
\]
Then there exists \( j \) such that \( \ker(\varphi_j) = \{0\} \), otherwise, if for all \( j \) there exists \( p_j(x_j) \neq 0 \in \ker(\varphi_j) \), then we would have
\[
p_1(x_1), \ldots, p_t(x_t) \in I
\]
which would imply that \( \dim(V(I)) = 0 \). Define \( i_1 \) to be such that \( \ker(\varphi_{i_1}) = \{0\} \), which proves the \( m = 1 \) case.
If \( m \geq 2 \) then define for \( j = 1, \ldots, t, \ j \neq i_1 \)
\[
\varphi_{i_1,j} : k[x_{i_1}, x_j] \to k[x_1, \ldots, x_t]/I.
\]
Then there exists \( j \) such that \( \ker(\varphi_{i_1,j}) = \{0\} \), otherwise, similarly as above, we can prove that \( \dim(V(I)) = 1 \). Define \( i_2 \) to be such that \( \ker(\varphi_{i_1,i_2}) = \{0\} \), which proves the \( m = 2 \) case. We can use induction to define \( i_1, \ldots, i_m \) as above.

Next we define a property of the coordinate system \( \{x_1, \ldots, x_t\} \) which assures that \( x_1, \ldots, x_m \) is algebraically independent over all irreducible components of \( V \). We need two definitions first.

Definition 1.6. Given a commutative ring \( R \) and a ring extension \( S \), an element \( s \) of \( S \) is called integral over \( R \) if it is one of the roots of a monic polynomial with coefficients in \( R \). \( S \) is called an integral extension if every element of \( S \) is integral over \( R \).
Definition 1.7. The coordinate system \( \{x_1, \ldots, x_t\} \) is in normal position with respect to \( V(I) \subset \overline{k}^t \) if there exists \( m \leq t \) such that the homomorphism
\[
\varphi : k[x_1, \ldots, x_m] \to k[x_1, \ldots, x_t]/I
\]
is injective and \( k[x_1, \ldots, x_t]/I \) is integral over \( k[x_1, \ldots, x_m] \). If \( \overline{k} \) is algebraically closed, then normal position implies that the projection
\[
\pi : \overline{k}^t \to \overline{k}^m; \quad (x_1, \ldots, x_t) \mapsto (x_1, \ldots, x_m)
\]
restricted to \( V(I) \) is surjective and finite (each point has finite pre-images).

Remark 1.8. If \( \{x_1, \ldots, x_t\} \) is in normal position with respect to \( V(I) \subset \overline{k}^t \) then for all irreducible components \( V' \) of \( V(I) \) of dimension \( m \), \( x_1, \ldots, x_m \) are algebraically independent over \( V' \). We will prove this in one of the homework problems.

The second lemma is the well-known Noether Normalization Lemma, proving that a linear change of variables is sufficient to get a coordinate system in normal position.

Lemma 1.9 (Noether Normalization Lemma). Let \( k, I, V(I) \) and \( m \) as in Theorem 1.2. Then there exists a linear change of coordinates
\[
y_1 = \sum_{i=1}^t c_{1,i}x_i, \\
\vdots \\
y_t = \sum_{i=1}^t c_{t,i}x_i
\]
where \( y_1, \ldots, y_t \) are new variables, such that \( k[y_1, \ldots, y_t]/\overline{I} \) is an integral extension of \( k[y_1, \ldots, y_m] \). Here \( \overline{I} \subset k[y_1, \ldots, y_t] \) is the ideal obtained from \( I \) after the change of variables.

Proof. If \( t = m \) then \( k[x_1, \ldots, x_t]/I \) is clearly integral over \( k[x_1, \ldots, x_t] \). If \( t > m \) then the equivalence classes \( [x_1], \ldots, [x_t] \) in \( k[x_1, \ldots, x_t]/I \) are algebraically dependent over \( k \). Therefore, there exists a polynomial \( F \neq 0 \in \)
\[ k[x_1, \ldots, x_{t-1}, x_t] \text{ which vanishes modulo } I. \] 
\[ F \text{ is possibly not a monic polynomial in } x_t. \]
Let \( u_1 := x_1 - a_1 x_t, \ldots, u_{t-1} := x_{t-1} - a_{t-1} x_t \) where \( a_1, \ldots, a_{t-1} \in k \) will be specified later. Then
\[
F(x_1, \ldots, x_{t-1}, x_t) = F(u_1 + a_1 x_t, \ldots, u_{t-1} + a_{t-1} x_t, x_t) \\
= f(a_1, \ldots, a_{t-1}) x_t^{d_t} + q(u_1, \ldots, u_{t-1}, x_t)
\]
where \( f \) is some non-zero polynomial in \( t - 1 \) variables and \( \deg_{x_t}(q) < d_t \). If we choose \( a_1, \ldots, a_{t-1} \) such that \( f(a_1, \ldots, a_{t-1}) \neq 0 \), then \( F / f(a_1, \ldots, a_{t-1}) \) is a monic polynomial in \( x_t \) vanishing modulo \( \overline{I} \), where \( \overline{I} \subset k[u_1, \ldots, u_{t-1}, x_t] \) is obtained from \( I \) by substituting \( u_i + a_i x_t \) into \( x_i \). This shows that \( \{x_t\} \) is integral over \( k[u_1, \ldots, u_{t-1}] \). By induction, there is a linear change of coordinates \( y_1, \ldots, y_{t-1} \) of \( u_1, \ldots, u_{t-1} \) such that
\[ k[y_1, \ldots, y_{t-1}] / (\overline{I} \cap k[y_1, \ldots, y_{t-1}]) \]
is integral over \( k[y_1, \ldots, y_m] \). Here \( \overline{I} \) is as in the claim.

Let \( y_t := x_t \). We will prove that \( [y_t] \) satisfies a monic polynomial with coefficients in \( k[y_1, \ldots, y_m] \). To prove this, we will use the so called determinant trick. The above argument implies that there is a finite set of elements \( h_1, \ldots, h_N \in k[y_1, \ldots, y_t] \) such that the set
\[
\{[h_1], \ldots, [h_N]\} \subset k[y_1, \ldots, y_t] / \overline{I}
\]
generates \( k[y_1, \ldots, y_t] / \overline{I} \) as a \( k[y_1, \ldots, y_m] \) module. For example, \( \{[y_1^{m+1}, \ldots, y_t^i] : 0 \leq i_{m+1} < d_{m+1}, \ldots, 0 \leq i_t < d_t \} \) will work as generators, where \( d_i \) is the degree of some monic polynomials in \( \overline{I} \cap k[y_1, \ldots, y_{t-1}][y_t] \), which we proved to exist. We can assume that \( h_1 = 1 \). Therefore, there exists \( f_{ij} \in k[y_1, \ldots, y_m] \) for \( i, j = 1, \ldots, N \) such that
\[
[y_t h_i] = \sum_{j=1}^N f_{ij} [h_j]
\]
in \( k[y_1, \ldots, y_{t-1}, y_t] / \overline{I} \), or equivalently
\[
\sum_{j=1}^N (\delta_{i,j} y_t - f_{ij}) [h_j] = 0.
\]
This can be written in a matrix form as \( Ah = 0 \), where
\[
A = (\delta_{i,j} y_t - f_{ij})_{i,j=1}^N \in k[y_1, \ldots, y_m][y_t]^{N \times N} \text{ and } h = (h_j)_{j=1}^N \in k[y_1, \ldots, y_t]^N.
\]
Multiplying $A$ by its adjoint, we get that $Dh \in \bar{I}$ where $D$ is the diagonal matrix with $\det(A)$ in its diagonals. Thus, $\det(A)h_j \in \bar{I}$ for all $j = 1, \ldots, N$, and in particular $\det(A) \cdot 1 = \det(A)\bar{I}$. Now $\det(A)$ gives the desired monic polynomial with coefficients in $k[y_1, \ldots, y_m]$ vanishing on $[y_t]$. \hfill \Box

**Remark 1.10.** In the above proof we also showed that $k[y_1, \ldots, y_t]/\bar{I}$ is integral over $k[y_1, \ldots, y_m]$ if and only if it is finitely generated as a $k[y_1, \ldots, y_m]$-module. In general, a similar proof shows that a commutative ring extension $S$ of $R$ is integral over $R$ if and only if $S$ is finitely generated as an $R$-module.

This also implies that $k(y_1, \ldots, y_m)[y_{m+1}, \ldots y_t]/\langle \bar{I} \rangle$ is a finite dimensional vector space over the fraction field $k(y_1, \ldots, y_m)$. Here $\langle \bar{I} \rangle$ denotes the ideal generated by $\bar{I}$ in the ring $k(y_1, \ldots, y_m)[y_{m+1}, \ldots y_t]$.

Finally, our last lemma proves that if $\{x_1, \ldots, x_t\}$ is in normal position with respect to $V(I)$, then there exists a primitive element $[u] \in k[x_1, \ldots, x_t]/I$ such that $[u]$ generates $k[x_1, \ldots, x_t]/I$ as a $k(x_1, \ldots, x_m)$-algebra.

**Lemma 1.11** (Primitive element). Let $k$ be a field of characteristic zero. Let $I \subset k[x_1, \ldots, x_t]$ be a radical ideal as above. Assume that $\{x_1, \ldots, x_t\}$ is in normal position with respect to $V(I)$. Denote by $\langle I \rangle$ the ideal generated by $I$ in $k(x_1, \ldots, x_m)[x_{m+1}, \ldots, x_t]$. Then there exists

$$u = c_{m+1}x_{m+1} + \cdots + c tx_t \quad c_i \in k$$

such that the equivalence classes $[1], [u], \ldots, [u^d]$ generate

$$\mathcal{A} := k(x_1, \ldots, x_m)[x_{m+1}, \ldots, x_t]/\langle I \rangle$$

as a $k(x_1, \ldots, x_m)$-vector space for some $d \geq 0$.

**Outline of Proof.** We will prove that if $[u_1]$ and $[u_2]$ generate $\mathcal{A}$ as an algebra over $k(x_1, \ldots, x_m)$ for some $u_1, u_2 \in k(x_1, \ldots, x_m)[x_{m+1}, \ldots, x_t]$, then $[u] := [u_1] + \lambda[u_2]$ is a primitive element for all except a finite $\lambda \in k$. Then the general case can be proved by induction.

Since $[u_1]$ and $[u_2]$ are integral over $k[x_1, \ldots, x_m]$, there exist

$$f \in k(x_1, \ldots, x_m)[U_1] \quad \text{and} \quad g \in k(x_1, \ldots, x_m)[U_2],$$

the “minimal polynomials” of $[u_1]$ and $[u_2]$, such that $f(u_1)$ is the generator of the principal ideal $\langle I \rangle \cap k(x_1, \ldots, x_m)[u_1]$ and $g(u_2)$ is the generator of
We will prove that for all $\lambda$ radical ideal, one can prove that $f$ and $g$ are square-free over $k(x_1, \ldots, x_m)$. We will prove that for all $\lambda \in k$, $[u] := [u_1] + \lambda [u_2]$ is a primitive element, unless

$$\lambda = \frac{[u_1] - u_1'}{[u_2] - u_2'}$$

where $f(u_1') = 0$ and $g(u_2') = 0$, which excludes only finitely many choices for $\lambda$. It suffices to prove that $[u_2]$ is in the algebra generated by $[u]$ over $k(x_1, \ldots, x_m)$, since it also implies that $[u_1] = [u] - \lambda [u_2]$ is also in this algebra. Fix $\lambda$, let $U$ be a new variable and let

$$h(U_2, U) := f(U - \lambda U_2) \in k(x_1, \ldots, x_m)[U_2, U].$$

Consider the Sylvester resultant $R_0(U)$ of $h(U_2, U)$ and $g(U_2)$ in the variable $U_2$, and the first subresultant polynomial

$$R_1(U)U_2 + S_1(U) \in k(x_1, \ldots, x_m)[U_2, U].$$

By construction $R_0(U)$ and $R_1(U)U_2 + S_1(U)$ are both in $\langle h(U_2, U), g(U) \rangle$, and they have the property that $R_0(y) = R_1(y) = 0$ for some $y$ in the algebraic closure of $k(x_1, \ldots, x_m)$ if and only if $h(U_2, y)$ and $g(U_2)$ has more than one common roots, counted with multiplicity. Since $h([u_2], [u]) = 0$ and $g([u_2]) = 0$, therefore

$$R_0([u]) = 0 \quad \text{and} \quad R_1([u])[u_2] + S_1([u]) = 0.$$ 

However, $R_1([u]) \neq 0$, otherwise $h(U, [u])$ and $g(U_2)$ has at least two distinct common roots ($f$ and $g$ are square-free), so there exist $u_1'$ and $u_2'$ such that $f(u_1') = 0$ and $g(u_2') = 0$ and

$$u_1' = [u] - \lambda u_2' = [u_1'] + \lambda ([u_2] - u_2')$$

but we excluded this case for $\lambda$. We can assume that $R_0(U)$ is square-free over $k(x_1, \ldots, x_m)$, otherwise we take its square-free part. If $\gcd_U(R_0(U), R_1(U)) = d(U)$, then $d([u]) \neq 0$ and $R_0/d$ and $R_1$ are relatively prime, thus we can express

$$1 = p(U)R_0(U)/d(U) + q(U)R_1(U)$$

for some $p, q \in k(x_1, \ldots, x_m)[U]$. This implies that

$$0 = q([u]) (R_1([u])[u_2] + S_1([u])) = [u_2] + q([u])S_1([u])$$

\[8\]
which proves that \([u_2]\) is in the algebra generated by \([u]\) over \(k(x_1, \ldots, x_m)\).

Now we are ready to proof the theorem.

**Proof of Theorem 1.2.** In the Noether Normalization Lemma we proved that there exists

\[
y_1' = \sum_{i=1}^{t} c_{1,i}x_i,
\]

\[
\vdots
\]

\[
y_t' = \sum_{i=1}^{t} c_{t,i}x_i
\]

for some \(c_{i,j} \in k\) such that \(\{y_1', \ldots, y_t'\}\) is in normal position with respect to \(V(I)\). Let \(I' \subset k[y_1', \ldots, y_t']\) be the ideal obtained from \(I\) by the change of variables, and let \(\langle I' \rangle\) be the ideal generated over \(k(y_1', \ldots, y_m')\). By the primitive element theorem there exists

\[
u = c_{m+1}y_{m+1}' + \cdots + c_ty_t'
\]

such that \([u]\) is a primitive element of \(k(y_1', \ldots, y_m')[y_{m+1}', \ldots, y_t']/\langle I' \rangle\) over \(k(y_1', \ldots, y_m')\). Assume that \(c_{m+k} \neq 0\). Define \(y_i := y_i'\) for \(i = 1, \ldots, m\), \(y_{m+1} := u\), and for \(i = m + 2, \ldots, t\), \(y_i\) is defined to be one of the remaining \(y_j'\) such that \(j \neq m+k\) and \(j > m\). Let \(\tilde{I} \subset k[y_1, \ldots, y_t]\) be the ideal obtained from \(I'\) after the change of coordinates, let \(\langle \tilde{I} \rangle\) be the ideal generated by \(\tilde{I}\) over \(k(y_1, \ldots, y_m)\), and denote

\[
A := k(y_1, \ldots, y_m)[y_{m+1}, \ldots, y_t]/\langle \tilde{I} \rangle.
\]

Clearly, \(\{y_1, \ldots, y_t\}\) is also in normal position, and \([y_{m+1}]\) is a primitive element. Let \(D\) be minimal such that

\[
[1], [y_{m+1}], \ldots, [y_{m+1}^D]
\]

generates the \(k(y_1, \ldots, y_m)\)-vector space \(A\). Since \([y_{m+1}]\) is integral over \(k[y_1, \ldots, y_m]\), there exist \(P_j \in k[y_1, \ldots, y_m]\) for \(j = 0, \ldots, D\)

\[
[y_{m+1}^{D+1}] = \sum_{j=0}^{D} P_j[y_{m+1}^j].
\]
This defines the coefficients of the monic polynomial $P$ in the claim. For all $k = 2, \ldots, t - m$ and $j = 0, \ldots, D$ there exist $r_{m+k,j} \in k(y_1, \ldots, y_m)$ such that

$$[y_{m+k}] = \sum_{j=0}^{D} r_{m+k,j}[y_{m+1}] \in \mathcal{A}.$$ 

Let $Q_{m+k}$ be the least common multiple of $r_{m+k,j}$ for $j = 0, \ldots, D$, and

$$R_{m+k} := Q_{m+k} \sum_{j=0}^{D} r_{m+k,j} y_{m+1}^j \in k[y_1, \ldots, y_m, y_{m+1}].$$

Then $L_{m+k} := Q_{m+k}y_{m+k} + R_{m+k}$ is the linear polynomial in $y_{m+k}$ in the claim. We claim that

$$\langle P, L_{m+1}, \ldots, L_t \rangle = \langle \tilde{I} \rangle \subset k(y_1, \ldots, y_m)[y_{m+1}, \ldots, y_t].$$

By construction, $P, L_{m+1}, \ldots, L_t \in \langle \tilde{I} \rangle$. Also, by the minimality of $D$ we have that

$$\dim \mathcal{A} = D = \dim k(y_1, \ldots, y_m)[y_{m+1}, \ldots, y_t]/\langle P, L_{m+1}, \ldots, L_t \rangle$$

which proves that the ideals above are the same. 

**Example 1.12.** In this example we demonstrate what is the difference between the different representations of algebraic sets: Gröbner bases, Triangular Representation and Geometric Representation. Let

$$G := \{ xy^3 - y^4, x^2y^2 - z^4 \}.$$ 

Then $G$ forms a Gröbner basis for the lexicographic order with $x < y < z$. Also, $G$ is a triangular set for the variety $\mathbf{V}(G)$. However, it is not a geometric representation, since the second is not linear in $z$. Fortunately, $\{x, y, z\}$ is in normal position, since both $[y]$ and $[z]$ in $k[x, y, z]/\langle G \rangle$ are integral over $k[x]$:

$$xy^3 - y^4 \in \langle G \rangle$$

is monic in $y$ and $z^4 - x^2y^2 \in \langle G \rangle$ is monic in $z$. Therefore, the primitive element theorem asserts that $u := y - \lambda z$ is a primitive element for almost all $\lambda$. However, after substituting for example $y = u + z$ in $G$ we get that the Gröbner basis w.r.t. lex $x < u < z$ is

$$\tilde{G} := \{-4x^3u^8 + 6x^2u^9 - 4u^{10}x + u^{11}, 32x^5u^4z + \cdots \text{ etc.}\}$$

10
which shows that \( u \) is not a primitive element, since the second polynomial has a leading coefficient depending on \( u \). Other choices of \( \lambda \) are not working either.

The problem here is that \( I \) is not a radical ideal, and the “minimal polynomial” of \([y]\) is not square-free over \( k(x) \), so no primitive element exists (check where the proof of the Primitive Element Theorem breaks down). To get the geometric representation of \( V(G) \) we consider the radical ideal \( I(V(G)) \), generated by

\[
H = \{x^3y - z^4, -xy + y^2, -z^5 + x^4z, -xz + zy\}.
\]

Note that in practice we would not compute the radical of the ideal, but would instead use the square-free factorization of the minimal polynomials of the generators of the factor algebra. Notice that \( H \) already contains a subset

\[
T := \{-z^5 + x^4z, x^3y - z^4\}
\]

which is a geometric representation of \( V(H) \). Note that the ideal generated by \( T \) and by \( H \) in \( k[x, y, z] \) are not the same, hence the differing Gröbner basis. Also, \( V(H) \) and \( V(T) \) differ, since \( V(T) \) contains the superfluous component \( V(x, z) \). However, \( T \) and \( H \) generate the same ideal in \( k(x)[y, z] \). In fact, the polynomials which pseudo-reduce to 0 modulo \( T \) are the same as the ones which vanish generically on \( V(H) \).

References

