Commutative Algebra and Introduction to Invariant Theory

A thesis submitted to
Indian Institute of Science Education and Research Pune
in partial fulfilment of the requirements for the
Mathematics M.Sc Degree Program
under the supervision of
Dr. Vivek Mohan Mallick

by
Isha Garg
November, 2024

IISER PUNE

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road, Pashan, Pune India 411008

This is to certify that this thesis entitled "*Commutative Algebra and Introduction to Invariant Theory*" submitted towards the partial fulfilment of the Mathematics M.Sc Degree Program at the Indian Institute of Science Education and Research Pune represents work carried out by *Isha Garg* under the supervision of *Dr. Vivek Mohan Mallick*.

Vivek Mohan Mallick

Dr. Vivek Mohan Mallick
Master's Thesis Supervisor

Prof. Girish Ratnaparkhi
Dean (Academics)

Declaration

I hereby declare that the matter embodied in the report entitled **Commutative Algebra and Introduction to invariant theory** are the results of the work carried out by me at the Department of Mathematics, Indian Institute of Science Education and Research, Pune, under the supervision of Dr. Vivek Mohan Mallick and the same has not been submitted elsewhere for any other degree.

Isha Garg

Isha Garg

Contents

1 Polynomial Rings in several variable

Before getting ourselves introduced to division in polynomial rings in more than one variable , let's make ourselves introduced to some concepts that will unable to extend the idea of division in $R[x_1, x_2, \ldots, x_n]$
We will restrict ourselves to $R[x_1, x_2, \ldots, x_n]$ where R is Noetherian ring.

Definition 1.1. A ring is a Noetherian ring if all of its ideals are finitely generated .

Proposition 1. *R Noetherian ring if and only if for every increasing sequence of ideals $\{I_n\}_n$ terminate after some finite number of terms , that is there exists $k \in \mathbb{N}$ such that $I_k = I_s$ for all $s \geq k$*

Proof. If R is a Noetherian Ring then, $\{I_n\}_n$ is increasing sequence of ideals in R

$$\bigcup_{n=1}^{\infty} I_n \text{ is again an ideal}$$

Since each I_i is a principal ideal $I_i \subseteq T_k \ \forall \ k \geq i$
Now

$$R[f_1, f_2, \ldots, f_n] = \bigcup_{n=1}^{\infty} I_n$$

□

Theorem 1.1. *(Hilbert Basis Theorem) If R is a Noetherian Ring then $R[X]$ is also a Noetherian Ring*

Proof. Suppose R is a Noetherian Ring, Let α be ideal in $R[X]$

$$I = \{LT(f) : \quad f \in \alpha\}$$

So $LT(f) \in R \ \forall \ f \in \alpha$, Hence I is ideal in R, Let $\{a_i\}_{i \leq n}$ be generators for ideal I.

Let $LT(f) = a$ such that $a = \sum_{i=1}^{n} u_i a_i$ where $u_i \in R$ and $f = ax^m +$ (lower terms)

Now suppose $\{f_i\}_{i \leq n}$ be polynomials such that $\deg(f_i) = r_i$ and $LT(f_i) = a_i$, take $r = \max_{i \leq n}\{r_i\}$. Let $\alpha' = R[f_1, f_2, \ldots f_n] \Rightarrow \alpha' \subset \alpha$, If $\deg(f) = m > r$ then

$$f - \sum_{i=1}^{n} u_i f_i \in \alpha$$

Proceeding in this way we keep subtracting elements from α' until we get $g(x)$ with $\deg(g) < r$ then $f = g + h$ where $f \in \alpha'$ let $M = [1, x, \ldots, x^{r-1}]$ be a finitely generated ring . Then clearly $g \in M$. Now let $\alpha = \alpha \cap M + \alpha'$, Here $\alpha \cap M$ ideal of α which is finitely generated say $\{g_i\}_{k \leq i}$ where $i \leq r - 1$
Hence α is also finitely generated by $\{g_i\}_{i \leq r} \cup \{f_i\}_{i \leq n}$
If we go by induction we can even claim that $R[x_1, x_2, \ldots x_n]$ is again Noetherian Ring □

Definition 1.2. Monomial Ordering ($\geq$) It is a well ordering on set of monomial such that if $m_1 \geq m_2 \Rightarrow mm_1 \geq mm_2$ for all monomials m

Fix a monomial ordering in $R[x_1, x_2, \ldots, x_n]$
Now we will leading term , If $f(x) \in R[x_1, x_2, \ldots, x_n]$ then $LT(f)$ is define as monomial term of maximal order in f
multidegree of leading term is denoted by $\partial(f)$
Also since $R[x_1, x_2, \ldots, x_n]$ is generated by $\{x_i\}_{i \leq n}$ so we can order the polynomials by simply setting ordering on its generator set

Example 1.1. Suppose that $x > y$ in $R[x, y]$ and $f = 2x^2 + 3xy$ then $LT(f) = 2x^2$ Since $x > y$

Proposition 2. If $LT(I) = \{LT(f) : f \in I\}$ where I is ideal in $R[x_1, x_2, \ldots, x_n]$ then $LT(I)$ is ideal in R

Proof. If $f, g \in I$ then $LT(f) + LT(g) \leq \max\{LT(f), LT(g)\} = LT(f + g)$ Similarly $LT(f.g) = LT(f)LT(g)$ Hence $LT(I)$ is ideal and it is known as *monomial ideal* □

1.1 Gröbner basis

Definition 1.3. Suppose I is an ideal in $R[x_1, x_2, \ldots, x_n]$ and the finite set $\{g_1, g_2, \ldots, g_m\}$ we call Gröbner basis, if $I = \langle g_1, g_2, \ldots, g_m \rangle$ and

$$\langle LT(g_1), (g_2), \ldots, LT(g_m) \rangle = LT(I)$$

With the knowledge of monomial ordering on $R[x_1, x_2, \ldots, x_n]$ we can now do general polynomial division in the given ring.

1.2 Algorithm for general polynomial divison

Suppose $\{g_i\}_{i \leq m} \subset R[x_1, x_2, \ldots, x_n]$ such that $g_i \neq 0$ for all $1 \leq i \leq m$ and the monomial ordering of $R[x_1, x_2, \ldots, x_n]$ is $x_1 > x_2 > x_3 \cdots > x_n$ then we can divide f by $\{g_i\}_{i \leq m}$ by following steps:

Step 1 Identify $LT(f)$ and $LT(g_i)$ with respect to given monomial ordering

Step 2 *Case 1)* If $LT(g_i)$ divides $LT(f)$ then write

$$f = hf_1 + r$$

and repeat step 1 for $LT(r)$
Case 2 If $LT(f)$ will not divided by any g_i then replace f by $f - LT(f)$ and go to step 1

Remark. In $R[x_1, x_2, \ldots, x_n]$ the ordering of divisors play an important role in polynomial divison

Example 1.2. Let us check for $f = x^2 + x - y^2 + y$ and $g_1 = x + y$, $g_2 = xy + 1$. Here the ordering is $x > y$ $LT(f) = x^2,\ LT(g_1) = x,\ LT(g_2) = xy$ since $LT(g_1) \mid LT(f)$. Hence $f - xg_1 = x - y^2 + y - xy$ and $LT(f - xg_1) = -xy$ so $LT(g_1) \mid -xy$ $f - xg_1 + yg_1 = x - y$. Now $LT(f - xg_1 + yg_1) = x$ then $f - xg_1 + yg_1 - g_1 = -2y$ Hence $f = g_1(x - y + 1) - 2y$

Theorem 1.2. For a monomial ordering on $R = F[x_1, x_2, \ldots, x_n]$, suppose $\{g_i\}_{i \leq m}$ is a Gröbner basis of the non-zero ideal I in R then the following hold:

1) For every $f \in R$ can be written uniquely in the form of $f = fI + r$ where $fI \in I$ and no non zero nontrivial term for r is divisible by any of leading term g_i for all i

2) Both fI and r can be computed by general polynomial divison of f by $g_1, g_2, \ldots, g_m$ and is independent of the order of g_i

3) Also reminder r gives a unique repersentative for coset of f in $\frac{R[x_1, x_2, \ldots, x_n]}{I}$

Proof. We perform general polynomial divisor and get $f = f_I + r$ where $f_I = \sum_{i \leq m} q_i g_i$ Suppose $\{g_i\}_{i \leq m}$ is a Gröbner basis of the non zero ideal I and let $f = fI + r = f'I + r' \Rightarrow r' - r \in I$. hence $LT(r' - r)$ is divisible by any of $LT(g_i)$ $\forall\ 1 \leq g_i \leq m$ Hence $LT(r - r') = 0$ which simply means that $r' = r$ so $fI + r$ is unique decomposition on f This proves (1) (2) and (3) $\square$

Does every ideal of $R[x_1, x_2, \ldots, x_n]$ have a Gröbner basis . Let's find out

Theorem 1.3. For a fix monomial ordering in $F = R[x_1, x_2, \ldots, x_n]$ and non zero ideal I of F
1) If $\{g_i\}_{i \leq m}$ are any elements of I such that $\langle LT(g_1), LT(g_2), \ldots, LT(g_m) \rangle = LT(I)$ then $\{g_i\}_{i \leq m}$ is a Gröbner basis for I.
2) The ideal I has a Gröbner basis.

Proof. 1) We first need to check $I = \langle g_1, g_2, \ldots, g_m \rangle$ Suppose $f \in I$; $f = \sum_{i=1}^{m} q_i g_i + r$ and $r \neq 0$ this implies that $r \in I$ Hence $LT(g_i) \mid LT(r)$ for some i
Hence $\{g_i\}_{i \leq m}$ is a Gröbner basis for I
2) Since $I = \langle h_1, h_2, \ldots, h_m \rangle$ then $\langle LT(h_1), LT(h_2), \ldots, LT(h_m) \rangle \subset LT(I)$ Since $LT(I)$ is finitely generated hence we get generator set for $LT(I)$ is

$$\{LT(h_1), LT(h_2), \ldots, LT(h_m), \ldots LT(h_{m+k})\}$$

Hence I has Gröbner basis.
Now we will see how to find this Gröbner basis for any ideal I in $R[x_1, x_2, \ldots, x_n]$. For this we make use of *Buchberger's criterion.*

Lemma 1.1. Suppose $\{f_i\}_{i=1}^{m} \in R[x_1, x_2, \ldots, x_n]$ are polynimials with multidegree α and that $h = \sum_{i=1}^{m} a_i f_i$ with $a_i \in F$ such that $\deg a_i < m$ for all i then

$$h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i) \ , b_i \in F$$

where $S(f_{i-1}, f_i) = \dfrac{M f_1}{LT(f_1)} - \dfrac{M f_2}{LT(f_2)}$
Bucherberger's criterion: Let $F = R[x_1, x_2, \ldots, x_n]$ and fix monomial ordering on F. If $I = \langle g_1, g_2, \ldots, g_m \rangle$ is a non zero ideal in F then $G = \{g_1, g_2 \ldots, g_m\}$ is grobner basis for $I \iff S(g_i, g_j) = 0 \mod G \forall 1 \leq i, j \leq m$

□

1.3 Buchburger's Algorithm

Step 1 Enumerate $S(g_i, g_j) \ \forall \ 1 \leq i, j \leq m$
Case 1 if for all $S(g_i, g_j) = 0$ then G forms a Gröbner basis
Case 2 if any of $S(g_i, g_j) \equiv f \mod G$ and $f \neq 0$ then add $f = g_{m+1}$ to set G

$$G' = G \cup \{g_{m+1}\}$$

Reiterate the step till we get a set G has Gröbner basis for ideal I

Example 1.3. Let's compute the Gröbner basis for ideal Igenerated by $f_1 = x^3 y - x y^2 + 1$ and $f_2 = x^2 y^2 - y^3 - 1$ here monomial ordering is $x > y$

$$I \langle f_1, f_2 \rangle$$

$LT(f_1) = x^3y,\ LT(f_2) = x^2y^2$ Now $M = lcm(LT(f_1, f_2)) = x^3y^2$

$$S(f_1, f_2) = yf_1 - xf_2 = y + x$$

$\deg(y + x) < \deg(f_i)$ for all $i = 1, 2$ Now $G' = \langle f_1, f_2, f_3\rangle$ and $f_3 = y + x$ and $LT(f_3) = x$ then $M_{13} = x^3y$ So

$$S(f_1, f_3) = f_1 - x^2yf_3 = -xy^2 + 1 - x^2y^2 = f_4$$

Now divide $S(f_1, f_3)$ by f_1, f_2, f_3 $LT(f_4) = -x^2y^2$ $f_4 + f_2 = -xy^2 - y^3 \Rightarrow f_4 + f_2 + y^2f_3 = 0$ hence $f_4 \in \langle f_1, f_2, f_3\rangle$ $S(f_2, f_3) = S_{23}$ and $M_{23} = x^2y^2$ hence $S_{23} = -y^3 - xy^3 - 1$ Now divide $S(f_2, f_3)$ by f, f_1, f_2, f_3 suppose $f_5 = S(f_2, f_3)$ and $LT(f_5) = -xy^3$ so $f_5 + y^3f_3 = (y^4 - y^3 - 1) \mod G'$

$$G\text{''} = \{f_1, f_2, f_3, f_4\} \text{ where } f_4 = y^4 - y^3 - 1$$

Similarly if we compute

$$S(f_i, f_4) = 0\ \forall\ 1 \leq i \leq 3$$

Hence G" form Gröbner basis

$$LT(I) = \{x^3y, x^2y^2, x, y\}$$

we compute minimal Gröbner basis $LT(I) = \{x, y^4\}$

1.4 Reduced Gröbner basis

Fix a monomial ordering on $F = R[x_1, x_2, \ldots, x_n]$ thus a Gröbner basis $G = \{f_1, f_2, \ldots, f_m\}$ can be reduced if non of the monomial terms of f_i is divisible by $LT(gf_i)\ \forall\ j \neq i$

Lemma 1.2. Minimal Gröbner basis have same cardinality and have same leading terms(after a possible rearrangement of terms)

Theorem 1.4. Existence and uniqueness of reduced Gröbner basis

Proof. Suppose $G = \{g_i\}_{i=1}^m$ and $G' = \{g_i'\}_{i=1}^m$ are two reduced Gröbner bases for an ideal I then $LT(g_i) = LT(g_i')$ for some i after possible rearrengement let $h = LT(g_i) = LT(g_i')$
$g' - g \in I$ hence $h_j \mid LT(g_i - g_i')$ for some $1 \leq j \leq m$
$h_j \mid LT(g_i)$ or $h_j \mid LT(g_i')$ which leads to contradiction. Therefore, the reduced Gröbner basis of any ideal I of $R[x_1, x_2, \ldots, x_n]$ is uniquely determined. □

Corollary 1.4.1. Let I and J be two ideals of $F[x_1, x_2, \ldots, x_n]$ then $I = J \iff$ they have same reduced Gröbner basis with respect to some fixed monomials ordering.

1.5 Solving Algebraic equation

Here we will see how we can solve a system of polynomial equations via a Gröbner basis.
Suppose we want to find the $\mathcal{Z}(I)$ where ideal $I = f_1 = x^3y - xy^2 + 1$, $f_2 = x^2y^2 - y^3 - 1$ then we need to solve following system of algebraic equations $f_1 = x^3y - xy^2 + 1 = 0$ $f_2 = x^2y^2 - y^3 - 1 = 0$ We already compute the reduced Gröbner basis (denote it by G for the ideal I with respect to lexicographic monomial ordering $x \geq y$
$G = x + y, y^4 - y^3 - 1$
Now as expected we get an element of Gröbner basis in just one variable . If we solve it we get value for y and then subsequently placing y in $x + y = 0$. We get value for x as well
Hence, we can solve any system of algebraic equations .

Definition 1.4. I_i elimination ideal : If $x_1 > x_2 > x_3 \cdots > x_n$ is the lexicographic ordering on $R[x_1, x_2, \ldots, x_n]$ and if I is any ideal hen i-th elimination $I_i = R[x_{i+1}, \ldots, x_n] \cap I$.

Proposition 3. If $G = \{g_i\}$ be Gröbner basis of a non zero ideal I in $R[x_1, x_2, \ldots, x_n]$ with respect to lexicographic ordering $x_1 > x_2 > \cdots > x_m$ then $G \cap R[x_{i+1}, \ldots, x_n]$ G is Gröbner basis for the ideal I_i .

Proof. $G_i = G \cap R[x_{i+1}, \ldots, x_m]$ is Gröbner basis for ideal I $\langle LT(g_1), LT(g_2), \ldots, LT(g_m) \rangle = LT(I)$ so we need to show

$$LT(I_i) = LT(G_i)$$

$G_i \subseteq I_i \Rightarrow LT(G_i) \subseteq LT(I_i)$ to show that reverse conainment let $f \in LT(I_i)$ so is $f \in LT(i)$ then $LT(f) = \sum_{i \leq m} a_i LT(g_i)$ where $a_i \in R[x_1, x_2, \ldots, x_n]$ since $f \in I_i$ so right side of equation should be a function $x_{i+1}, \ldots, x_n$. Hence equating all sum of all polynomials in $x_1, x_2, \ldots x_n$ variable to zero so we get $LT(f) = \langle LT(G) \rangle$ Hence proof is complete $\square$

2 Polynomial rings and algebraic geometry

Definition 2.1. A ring R is a k- algebra if K is contained in the center of the ring and unity of k is same as the unity of R

Definition 2.2. A ring R is finitely generated k-algebra if it is the form $R[x_1, x_2, \ldots, x_n]$ for all $x_i \in R$

Definition 2.3. Let R and S are k- algebra . then a ring f homomorphism if $f : R \longrightarrow S$

1)
$$f(r+s) = f(r) + f(s)$$
2)
$$f(rs) = f(r)f(s)$$
3)
$$f|_k = Id$$

From this point, we will explore the connection between algebraic geometry and commutative algebra

Definition 2.4. An affine space is set of n-tuple of elements over k.
Corresponding to an affine space $\mathbb{A}^n$ over k we have a polynomial ring $K[x_1, x_2, \ldots, x_n]$ such that if $f \in K[x_1, x_2, \ldots, x_n]$ then

$$f : \mathbb{A}^n \to K \text{ defined by } (a_1, a_2, \ldots, a_n) \longrightarrow f(a_1, a_2, \ldots a_n)$$

Definition 2.5. $V \subseteq \mathbb{A}^n$ be a affine algebraic set if $V = Z(S)$ where $S \subset k[x_1, x_2, \ldots, x_n]$ and $Z(S)$ is common set of zeros of S

Now since $K[x_1, x_2, \ldots, x_n]$ is notherian ring every ideal I of $k[x_1, x_2, \ldots x_n]$ is finitley generated $S \subset \langle S \rangle$ is smallest ideal in $k[x_1, x_2, \ldots, x_n]$ containing S
$Z(\langle S \rangle) \subset Z(S)$ If $(a_1, a_2, \ldots, a_n) \in Z(S) \to f(a_1, a_2, \ldots, a_n) = 0$

$$\sum_{s \in S} k_s(x_1, x_2, x_3, \ldots, x_n) f_s(a_1, a_2, \ldots a_n) = 0 \Rightarrow (a_1, a_2, a_3, \ldots, a_n) \in Z(\langle S \rangle)$$

Hence $Z(S) = Z(\langle S \rangle)$ this implies while we deal with $S \subset k[x_1, x_2, \ldots, x_n)$ $Z(S)$ can be find out if we take finite intersection of some finite number of polynomials
Let's define an ideal $I(A) \subset R[x_1, x_2, \ldots x_n]$

$$I(A) = \{f \in R[x_1, x_2, \ldots, x_n] : \ f(a_1, a_2, a_3, \ldots a_n) = 0 \forall \ (a_1, a_2, \ldots, a_n) \in A\}$$

In fact $I(A)$ is maximal ideal of $K[x_1, x_2, \ldots x_n]$

2.1 Set theoretical properties of $\mathcal{I}$ and Z

1) Contravariant nature

$$A \subset B \Rightarrow \mathcal{I}(B) \subset \mathcal{I}(A) \, ; A, B \subset \mathbb{A}^n$$

$$X \subset Y \Rightarrow Z(Y) \subset Z(X) \, ; X, Y \in K[x_1, x_2, \ldots, x_n]$$

2)

$$\mathcal{I}(A \cup B) = \mathcal{I}(A) \cap \mathcal{I}(B)$$

$$Z(X \cup Y) = Z(X) \cap Z(Y)$$

3)

$$Z(X) \cup Z(Y) = Z(X \cup Y)$$

Relation between Z and $\mathcal{I}$ If $A \subset \mathbb{A}^n \rightarrow A \subset (Z(\mathcal{I}(A)))$ and if $I \subset K[x_1, x_2, \ldots x_n] \Rightarrow I \subset \mathcal{I}(Z(I))$
Properties
If $A = Z(I)$ then $A = Z(\mathcal{I}(A))$
If $I = \mathcal{I}(S)$ then $I = \mathcal{I}(Z(I)$
the above relation show that Z and $\mathcal{I}$ are inverse of each other when restricted to affine algebraic and ideals of type $\mathcal{I}(A)$ respectively where $A \subset \mathbb{A}^n$

Definition 2.6. $V \subseteq \mathbb{A}^n$ is an affine algebraic set then

$$K(V) = \frac{k[x_1, x_2, x_3, \ldots, x_n]}{\mathcal{I}(V)}$$

Example 2.1. If $V = Z(xy - 1)$ in $\mathbb{R}^2$ then clearly V is affine algebraic set since it is locus of hyperbola
To determine $K(V)$ we compute $\mathcal{I}(V)$

$$t \in R(x, y)$$

If we restrict ourselves to lexicographic ordering $x > y$

$$f(x, y) = t \circ (y) + g(x, y)(xy - 1)$$

if $f(x, y) \in \mathcal{I}(V)$ and if $(v_1, v_2) \in V$

$$f(v_1, v_2) = t \circ (y) + g(x, y)(v_1 v_2 - 1) = 0$$

hence $f \circ (y) = 0$

$$f(x, y) = g(x, y)(xy - 1) \; \forall \; f \in \mathcal{I}$$

Hence

$$\mathcal{I}(V) = \langle xy - 1 \rangle$$

$K(V) = \frac{R(x,y)}{\langle xy-1 \rangle} = R(\bar{x}, \bar{y})$ where

$$\bar{x} \equiv x \mod (xy - 1)$$

$$\bar{y} \equiv y \mod (xy - 1)$$

Also note that

$$\bar{x}\overline{y-1} \equiv (xy-1) \mod (xy-1) \Rightarrow \bar{x}\bar{y} \equiv 1 \mod (xy-1)$$

$$K(V) = R\left(\bar{x}, \frac{1}{\bar{x}}\right)$$

Proposition 4. $\varphi : V \longrightarrow W$ is a morphism if it is a polynomial map that is

$$\varphi(v_1, v_2, \ldots v_n) = (\varphi_1(v_1, v_2, \ldots v_n), \varphi_2(v_1, v_2, \ldots v_n), \ldots, \varphi_m(v_1, v_2, \ldots v_n))$$

each of φ_i is polynomial maps , where $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$

Definition 2.7. $\varphi : V \to W$ is a bijective morphism such that φ^{-1} is also a morphism is called an isomorphism

Theorem 2.1. $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ then there is a bijective correspodence between

$\{$Morphism from $\varphi : V \longrightarrow W\}$. $\leftrightarrow$ $\{k$- algebra morphism from $k(W) \longrightarrow K(V)\}$

Proof. Suppose $\varphi : V \to W$ is a morphism, define $\varphi' : k(W) \to k(V)$ such that $\varphi'(f) = f \circ \varphi$

$$f \equiv F \mod \mathcal{I}(W) \text{ where } F \in K[x_1, x_2, \ldots, x_n]$$

Let's check if $f \circ \varphi \in K(V)$ since $f \in K(W)$ then $f : W \to k$ then

$$\begin{tikzcd} V \arrow[rr, "\varphi"] \arrow[dr, "\varphi'"'] & & W \arrow[dl, "f"] \\ & k & \end{tikzcd}$$

$$f \circ \varphi : V \to k \text{ then } f \circ \varphi \in k(V)$$

Check if φ' is well defined

$$f(a_1, a_2, \ldots, a_m) = 0 \,\forall\, (a_1, a_2, \ldots, a_m) \in W \text{ and } \varphi(a_1, a_2, \ldots, a_m) \subset W$$

$$f \circ \varphi(a_1, a_2, \ldots, a_n) = 0 = \varphi'(f) = 0$$

Also φ' is k algebra homomorphism
Conversely if $\psi : K(W) \to k(W)$ is $k-$algebra homomorphism $\varphi(\bar{x_i}) = \bar{F_i}$

$$\bar{x_i} \equiv x_i \mod \mathcal{I}(W)$$

$$\bar{F_i} = F_i \mod \mathcal{I}(W)$$

then $\varphi = (F_1, F_2, \ldots, F_m)$ is a polynomial map $\varphi : V \to W$ next we show φ is a morphism for that it is sufficient to show

$$\varphi(v_1, v_2, \ldots, v_n) \in W$$

Proof. If $g \in \mathcal{I}(W) \subset k[x_1, x_2, \ldots, x-n]$ then

$$g(x_1 + \mathcal{I}(W), x_2 + \mathcal{I}(W), \ldots, x_m + \mathcal{I}(W)) = g(x_1, x_2, \ldots, x_m) + \mathcal{I}(W)$$

$$\mathcal{I}(W) \in k(W)$$

So

$$\Phi \circ g(x_1 + \mathcal{I}(W), x_2 + \mathcal{I}(W), \ldots, x_m + \mathcal{I}(W)) = 0 \in k(W)$$

Since Φ is k algebra homomorphism it follows that

$$g(\Phi(x_1 + \mathcal{I}(W)), \Phi(x_2 + \mathcal{I}(W), \ldots, \Phi(x_m + \mathcal{I}(W))) = 0 \in k[V]$$

$$\Phi(x_1 + \mathcal{I}(W)) \equiv F_i \mod \mathcal{I}(V)$$

so

$$g(F_1, F_2, \ldots, F_m) \in \mathcal{I}(V)$$

then if

$$g \in \mathcal{I}(W) \Rightarrow g \circ \varphi(a_1, a_2, \ldots, a_n) = 0$$

,
Now

$$\varphi(a_1, a_2, \ldots, a_n) \in \mathcal{Z}(\mathcal{I}(W)) = W$$

Since W is affine algebraic set ,so $\varphi : V \to W$ is a morphism
Since this morphism φ induces ϱ k algebra homomorphism implies $\varrho = \varphi$ □

□

2.2 Radicals and affine varieties

Definition 2.8. Let I be an ideal in a ring R then its radical rad(I) is the intersection of all prime ideals containing it

$$rad(I) = \bigcap P \in specRP$$

Its clear $rad(P) = P, P \in specR$
nilradical(R) $= rad(0) = \{x | x^n = 0 \text{ for some } n \in \mathbb{N}\}$

In this section we how radical ideals are linked to affine algebraic sets and also develop an algorithm for their computation in polynomial rings
In next theorem we see how radicals are even simpler in case of Noetherian rings

Theorem 2.2. Let R be a Noetherian ring and I be its ideal then there exists n in $\mathbb{N}$ such that $(radI)^n \in I$

2.3 Computation of Radicals

2.4 Zariski Topology

Definition 2.9. The Zariski topology on an affine space $\mathbb{A}^n$ is the one in which the closed sets are the affine algebraic subsets

Topological properties of Zariski topology
1 It is coarsest topology in which singleton sets are closed
2 It cannot be Hausdorff for any open set of this topology does not contain only some finite points
3 Non-empty Zariski open sets are dense subsets of $\mathbb{A}^n$

Definition 2.10. Zariski closure If $A \subseteq \mathbb{A}^n$ then Zariski closure of A is defined as the smallest affine algebraic set containing it .
If zariski closure of A is Y then A is zariski dense in Y
Note zariski closure of

$$A \subseteq \mathbb{A}^n = \mathcal{Z}(\mathcal{I})(V)$$

2.5 Affine Varieties

Definition 2.11. An affine algebraic set is irreducible if it cannot be written as union of proper affine algebraic sets
A irreducible affine algebraic set is called an affine variety

2.6 Primary decomposition of affine algebraic set

Every affine algebraic set V can be decomposed uniquely in the following way

$$V = V_1 \cup V_2 \cup \cdots \cup V_q$$

where V_i is irreducible and $V_i \nsubseteq V_j \forall i \neq j$

Proof. First lets show the existence part
Suppose $\mathcal{S}$ be a nonempty collection of affine algebraic sets in an affine space $\mathbb{A}^n$ which cannot be wriiten as a finite union of affine varieties then as every descending chain of affine algebraic sets has a minimal element so by Zorns lemma we are sure to get a minimal element V_0 of this set $\mathcal{S}$. then $V_0 = \mathcal{I}(I_0)$ so I_0 is the maximal element in set of ideals corresponding to these affine algebraic sets Since this $V_0 \in \mathcal{S}$ then being minimal element it cannot be irreducible so if $V_0 = V_1 \cup V_2$ then V_1 and V_2 can be written as finite union of affine varieties then consequently $V_0 \in \mathcal{S}$. This leads to contradiction

To prove uniqueness, suppose V has two decompositions into affine varieties

$$V = V_1 \cup V_2 \cdots \cup V_n = U_1 \cup U_2 \cup \cdots \cup U_s$$

Then V_1 is contained in the union of U_1.Since $V_1 \cap U_1$ is an algebraic set for each i, we obtained decomposion of V_1 into algebraic subsets:

$$V_1 = (V_1 \cap U_1) \cup (V_1 \cap U_2) \cup \cdots \cup (V_1 \cap U_s)$$

Since V_1 is irreducible , we must have $V_1 = V_1 \cap U_j$ for some j i.e $V_1 \subseteq U_j$ By the symmetric argument we have $U_j \subseteq V_{j'}$ for some j'. Thus $V_1 \subseteq V_{j'}$ so $j' = 1$ and $V_1 = U_j$. Applying a similar argument for each V_l it follows that $r = s$ and that $\{V_1, \ldots, V_n\} = \{U_1, \ldots U_s\}$. This completes the proof.

□

3 localisation in rings

Theorem 3.1. If R is a commutative ring with unity then for every multiplicative closed set S containing unity , $D^{-1}S$ becomes a ring where $D = S - 0$.Then $h : R \to D^{-1}R$ Also for every $f : R \to S$ ring homomorphism which carries unity to unity and h(d) is unit $\forall d \in D$ then $\exists$ a unique $g : D^{-1}R \Rightarrow S$ a ring homomorphism such that the following diagram commutes .

Proof. First we define a relation on $D \times S$ as $(a, b) \sim (c, d)$ if $\exists x \in D$ such that $x(ad - bc) = 0$ clearly this is an equivalence relation so we define addition and multiplication operation on $D \times S$ as
$(a \mid b) + (c \mid d) = (a + b) \mid (c + d)$
$a \mid b \times c \mid d = (ab) \mid cd$ under these operation $D^{-1}S$ becomes a ring also
$h : R \to D^{-1}R$ is a injective ring homomorphism as
$h(r) = r|1$
Now if we define $g : D^{-1}R \to S$ by
$g(r|d) = f(r)|h(d)$ the map g is well defined for if $r|d = s|e$ then $x(re - sd) = 0$ for some $x \in D$ So $g(x)(g(re) - g(sd)) = 0$
hence $g(r|d) = g(s|e)$ Clearly g is a ring homomorphism too. Lets show its uniqueness Since $x|d \in D^{-1}R$ then $x|d = x|1(r|1)^{-1}$
if $g(x|1) = gh(x|1) = f(x)$
hence g is uniquely determined □

This ring $D^{-1}R$ is called ring of fraction of R at D
When we replace this D by $R\backslash\{0\}$ and R is integral domain then this ring is known as field of fractions of R

3.1 Extension and contraction of ideals

If I is an ideal in a ring R and if $f : R \to S$ be ring homomorphism then I^e is known as extension of ideal I which is the smallest ideal in S containing I and if J is an ideal in S then J^c is the contraction of ideal J in R which is simply the inverse image of ideal J in R

Theorem 3.2. if $h : R \to D^{-1}R$ be a ring homomorphism then for any ideal J in $D^{-1}R$ and ideal I in R we have
1) $J = J^{ce}$
2) $I^{ec} = \{r \in R \text{ f } dr \in I \text{ for some } d \in D\}$
3) there is a bijective correspondence between

$\{$ prime ideals P of R such that $P \cap D = \emptyset\}$ $\overset{c}{\longleftarrow}$ $\{$prime ideals of $D^{-1}R$ $\}$ $\overset{b}{\longrightarrow}$
4) if R is noetherian (artinian) then $D^{-1}R$ is also noetherian(artinian)

Proof. 1) By definition

$$J^{ce} \subseteq J$$

to show the reverse containment
if $a|d \in D^{-1}R$ then $a|1 = d(a|d) \in J^e$ hence $a \in J^{ec}$ hence $J = (J^e)^c$
2) for the next proof we consider $I` = \{r \in R$ such that $dr = 0$ for some $d \in D\}$
then if $r \in I`$ then $\exists\, d \in D$ such that $rd \in I \implies rd = a$ for some $a \in I$
$r|1 = a|d \in I^e$ so $r \in I^{ec}$
to show reverse containment let $r \in I^{ec}$
$\implies r|1 = a|d \in I^e$
$\implies rd = a \in I^e$
$\implies r \in I`$
hence $I^{ec} \subseteq I`$

3) We need to show that $P^e(c) = P$
and $P^{ce} = P$
Let Q be a prime ideal of $D^{-1}R$ then Q^c will be prime ideal too as inverse image of every prime ideal is prime ideal and as $Q^{ce} = Q$
to show reverse containment let P be a prime ideal in R then let $Q^e = P$
first we show that Q is a prime ideal
let $(a|d_1)(b|d_2) \in Q$
then $(a|d_1)(b|d_2) = c|d \in Q$
then $x(d(ab) - c(d_1)(d_2)) = o$ for some $x \in D$
Since $c \in P$ then $xd(ab) \in P$
$ab \in P$ hence either a or $b \in P$
So $a|d_1| \in P^e$ or $b|d_2 \in P^e$
So P is a prime ideal in $D^{-1}R$

by above proposition $(P^e)^c = P$

4) Suppose R is Noetherian and let be an increasing sequence of ideals in $D^{-1}R$ then
$I_1{}^c \subseteq (I_2)^c \subseteq (I_3)^c \subseteq \dots$
terminates after some finite number of terms as $\bigcup (I_i)^c$ is an ideal in R which is Noetherian
since

$$(I_i{}^c)^e = I_i$$

this implies $D^{-1}R$ is Noetherian
Similarly one can prove the Artinian case also

□

Definition 3.1. Suppose R is a commutative ring with unity and let D be a multiplicative closed subset containing unity .So we define saturation of an ideal I in R to be $(I^e)^c$
here contraction and extension is wrt ring homomorphoism f: $R \longrightarrow D^{-1}R$
If I is saturated ideal then $(I^e)^c = I$

Proposition 5. Suppose R is a commutative ring with unity and let I be an ideal in $R[x]$ then I is a prime ideal in $R[x]$ $\iff$
1 $J = I \cap R$ and J is prime ideal in R so $S = R/J$ is an integral domain and
2 if $\bar{I}$ is the image of I in $S[x]$ then $\bar{I}F[x]$ is prime ideal in $F[x]$ such that it statisfies

$$\bar{I}F(x) \cap S[x] = \bar{I}$$

Using this proposition now we will form an algorithm for checking whether an ideal in $R[x]$ is prime ideal or not

3.2 Algorithm for determining prime ideals in $R = k[x_1, \dots x_n]$

Step 1 Firstly we will compute reduced Gröbner basis for ideal I in R wrt some lexicographic monomial ordering
Step 2 next we compute reduced Gröbner basis for $P_i = P \cap k[x_1, \dots, x_i]$
Step 3 We check if P_i is a prime ideal or not .If any P_i is not a prime ideal then P fails to be a prime ideal too
Suppose P_{i-1} is a prime ideal then let $S = k[x_1, x_2, \dots, x_{i-1}]|P_{i-1}$ and let F be the field of frations of S.
Now if P_i is a zero ideal then we are done (because $S[x_i]$ is an integral domain but if not then compute an irreducible polynomial $h(x_i)$ in P_i.This is justified for $F[x_i]$ is an euclidean domain and so that is why each of its ideal will be principle ideal. One can find this generator polynomial by applying euclidean divison algorithm to reduced Gröbner basis of this P_i

Step 3 Now P_i is a prime ideal only if

$$h(x_i)$$

is a irreducible polynomial otherwise its not. Next we check that this P_i is in-fact a saturated ideal. For this let us denote the leading coefficient of $h(x_i)$ by a. Compute the reduced Gröbner basis for the ideal

$$(P_i, 1 - at)$$

.If reduced Gröbner basis for this ideal lying in

$$k[x_1, \ldots x_i]$$

coincide with the reduced Gröbner basis for P_i then P_i is a prime ideal otherwise its not

Example 3.1. Consider an ideal $P = xz - y^2, yz - x^3, z^2 - x^2y$ in $k[x, y, z]$. We check if its prime ideal or not Set the monomial ordering $x \geq y \geq z$. Here the reduced grobner basis for P is set $G = x - yz, x^2y - z^2, xy^3 - z^3, xz - y^2, y^5 - z^4$ (by using Buchberger criterion)
here $P_1 = P \cap Q[z] = 0$. Hence P_1 is prime ideal since $Q(y, z)|P_1$ is an integral domain
Now $P_2 = P \cap Q[y, z] = (y^5 - z^4)$ Clearly its an irreducible polynomial in $Q(y, z)$ here $(y^5 - z^4) \in Q(y)(z)$ so the leading coefficient $a = 1$

$$A = ((y^5 - z^4), 1 - t)$$

There reduced grobner basis for $A = y^5 - z^4, 1 - t$ so P_2 is saturated ideal hence it is a prime ideal
lets check for P_3
In this case $S = Q(y, z)|(y^5 - z^4)$

$$S = Q(\bar{z})\bar{y} + Q(\bar{z})\bar{y}^2 + Q(\bar{z})\bar{y}^3 + Q(\bar{z})\bar{y}^4$$

Field of fraction

$$F = Q[\bar{z}]\bar{y} + Q[\bar{z}]\bar{y}^2 + Q[\bar{z}]\bar{y}^3 + Q[\bar{z}]\bar{y}^4$$

Now P is a prime in $F(x)$ hence P will be a principal ideal in $F(x)$ then $P = (f(x))$ for some $f \in Q(y, z)$
Lets find out this $f(x)$ which will be gcd of following polynomials in

$$Q[\overline{y, z}x]$$

$$f_1 = x^3 - \overline{yz}$$

$$f_2 = x^2\bar{y} - \bar{z}^2$$

$$f_3 = x\bar{y}^3 - \bar{z}^3$$

$$f_4 = x\overline{z - \bar{y}^2}$$

Using Euclidean divison algorithm in $Q[\bar{y,}z(x)]$ we get gcd of these $f_i = x\bar{z} - \bar{y}^2$
Hence f_4 is a irreducible polynomial in $Q[\bar{y,}z](x)$ hence P is a prime ideal in $F(x)$
Let A be ideal generated by $xz - y^2, yz - x^3, z^3 - x^2y, 1 - zt$
reduced grobner basis for this ideal A is $G` = ty^2 - x, tz - 1 \cup G$

$$G` \cap k(x, y, z) = G$$

hence

$$(P^e)^c = P$$

So P is a prime ideal in $Q(x, y, z)$

4 Localization of Modules

Let M be a R module and let D be a multiplicatively closed subaet of R such that D contains 1 then D^{-1}R -module D^{-1}M is called module of fractions of M with respect to D

Proposition 6. Let M be a R module and let D be a multiplicative closed subset of R such that D contains 1 then

$$D^{-1}M \cong D^{-1}R \otimes RM$$

Proof. Lets define map

$$\Phi D^{-1}R \times M \to D^{-1}M$$

$$\phi(r|d, m) = (rm)|d$$

since ϕ is well defined and R balanced so it induces a homomorphism from $D^{-1}R \times M$

□

Theorem 4.1. Let R be a noetherian ring and let

$$I = Q_1 \cap \cap \cdots \cap Q_m$$

be a minimal primary decomposition of an ideal I in ring R where Q_i is P_i primary ideal and let D be a multiplicative closed subset of R such that D contains 1. Q_i are numbered such that $D \cap P_i = \emptyset \; \forall 1 \leq i \leq t$ and $D \cap P_i \neq \emptyset \; \forall \; t+1 \geq i \leq mt$
Then

$$D^{-1}I = D^{-1}Q_1 \cap \ldots \cap D^{-1}Q_m$$

is a minimal primary decomposition of an ideal $D^{-1}I$ in ring $D^{-1}R$ where $D^{-1}Q_i$ is $D^{-1}P_i$ primary ideal Also $(D^{-1}Q_i)^c = Q_i \forall 1 \geq i \leq t$

Theorem 4.2. The primary ideals belonging to isolated primes in a minimal primary decomposition of an ideal I are uniquely determined

Proof. If P be a minimal element in the set of primes corresponding to an ideal I and lets take $D = R - P$ and $D \cap P_i = \emptyset$ for $P = P_i$. $(D^{-1}I)^c = Q_i$. Since $\cup_i P_i \forall i$ are uniquely determined by minimal primary decomposition of ideal I then isolated prime ideals are also unique.

□

Definition 4.1. A commutative ring containing unity is called local ring if it has a unique maximal ideal

Proposition 7. For any commutative ring containing unity if R_p is the localisation of R at prime ideal P and P^e denotes the extension of R to R_p .Then
1 This R_p is infact a local ring with unique maximal ideal P^e. Also $(P^e)^c = P$.
2 If R is an integral domain then R_p too an integral domain.
3 The prime ideals of R_p are in bijective correspondence with the prime ideals of R which contains P.
4 If P is a unique prime ideal of R then it is too a unique prime ideal of R_p
5 If $P = M$ is a maximal ideal and I is any M-primary ideal then $R_M | I^e \cong R|I$.

Proof. Firstly we prove the 3 We know already that prime ideals of R_p are in bijective correspondence with the prime ideals in R statisfying $P` \cap D = \emptyset$. Now its clear that $P` \cap D = \iff P \subseteq P`$. Hence this proves statement 3.
Now lets prove statement 1
Clearly P^e is a prime ideal too of R_p . Let M be a maximal ideal containing this P ($M \in$ maxpec R). So $P` \subseteq P$ This implies P^e infact a unique maximal ideal of R_p .Hence R_p is a local ring
$(P^e)^c = r \in R : \exists d \in R - P$ and $dr \in P$

if $rd \in P \implies r \in P$. hence P is a saturated ideal in R
for statement 2 if $\phi : R \longrightarrow R_P$ be an injective map such that

$$\phi(r) = r|1$$

.
hence this map induces an isomorphism

$$\bar{\phi} : R|P \longrightarrow R|P^e$$

□

Definition 4.2. Let M be a R- module and P some be its prime ideal then and $D = R \backslash P$. then R_p-module $D^{-1}M$ localisation an R-module M .
Note this localisation of R module kills all its P‘torsion elements where P‘ is some prime element such that $P‘ \nsubseteq P$

Proposition 8. If M be an R-module then the following statements are equivalent
1 $M = \{0\}$
2 $M_p = \{0\} \forall$ prime ideal P
3$M_N = \{0\} \forall$ maximal ideal N

Proof. 1 $\implies$ 2 $\implies$ 3 is obvious
we will show how 3 $\implies$ 1
Suppose $\exists m \neq 0$ such that $m \in M$ then $m|1 \in M_N$. Now since $M_N = 0$ this imply $\exists r \in R \backslash M$ such that $rm = 0$, but such $r \in$ Ann(R) $= I$ but every ideal M is a subset of some maximal ideal of R hence this leads to a contradiction and hence $m = 0$
this proves 3 $\implies$ 1 □

Proposition 9. If R is an integral domain then R is the intersection of all its localisations , $R = \cap R_P \; \forall P$

Proof. Since R is contained in each localised ring R_P then $R \subseteq \cap R_P \; \forall P$ is obvious . Now let us show the reverse containment.
Every localised ring is always a subring of field of fractions of R
Let $a \in F$ (field of fractions of R) such that $a \in R_M \; \forall M \in$ maxspec R
then set $I_a = \{d \in R \mid da \in R\}$ is an ideal of R .Now $a \in R \iff 1 \in I_a$
Suppose $I_a \neq R$ then I_a is a subset of some maximal ideal M in R.Now since $a \in R_M$ then $a = r|d \in R_M$. hence $d \in I_a$ but $d \in R_M$
This leads to a contradiction
hence $a \in R$ and the proof follows.

□

Proposition 10. If R be an integral domain then the following statements are equivalent
1 R is normal
2 R_P is normal $\forall P \in \text{spec}R$
3 R_M is normal $\forall M \in \text{maxspec}R$

Proof. Lets prove $1 \implies 2$
Suppose $y \in F$ then y satisfies a monic polynomial with coeffecients in R_P then $y` = y(d_0 \dots d_n)^n$ is integral over R
and $y = y`|(d_0 \dots d_n)$ hence $y \in F$ such that it is integral over R
So $y \in R_P$
$2 \implies 3$ is obvious
$3 \implies 1$ Let $y \in F$ such that it is integral over R We need to show $y \in R$
Now $R = \cap R_M \forall M \in$ maxpec R. Hence $y \in R_M$ for some $M \in$ maxspec R then $y \in R$. Hence proved $3 \implies 1$

□

4.1 Local rings of affine varieties

Here we will get used to by localisation of ideals in coordinate ring of some vector space V

Definition 4.3. Coordinate rings $k[V]$ and its field of fractions $k(V)$

$$k(V) = \{f|g : f \text{ and } g \in k[V] \text{ such that } g \neq 0\}$$

Definition 4.4. Regular functions $f|g$ is said to be a regular or defined at $v \in V$ if $\exists f_1$ and $g_1 \in k[V]$ and $g_1 \neq 0$ such that $f|g = f_1|g_1$
Note : Clearly if f is defined at some $v \in V$ then its also defined on zariski open neighbourhood V_a and as we know zariski open sets are dense in V so this f is defined almost everywhere in some sense.

Definition 4.5. Local rings in affine variety $(O_{v,V})$

$$c = \{f|g \in k(V)|(f|g) \text{ is regular at v }\}$$

Note : This local ring is localization of $k(V)$ at i

Since we call $O_{v,V}$ a local ring then lets talk about its unique maximal ideal $m_{v,V}$

$$m_{v,V} = \{f|g \in O_{v,V} \ |f|g = f_1|g_1 \text{ then } f_1(v) = 0 \text{ and } g_1 \neq 0\}$$

Proposition 11. Polynomial rings are precisely those regular functions which are regular on all points of V provided V is defined on an algebraically closed field

Proof. To prove this recall $R = \cap R_P \forall P \in$ spec R .so if we say f is regular on V is same as saying that $f \in k(V)_P \forall P = \mathcal{I}I(v)$ and hence $f \in k(V)$ this proves the proposition

□

4.2 Tangent Space $(T_{v,V})$

$$T_{v,V} = \mathcal{Z}\{D_v(f)(x_1, \dots, x_n) | f \in I(V)\}$$

where $D_v(f)$ are the formal partial derivatives .

5 Introduction to Invariant theory

5.1 Polynomial functions

Let $\mathbb{K}$ be an infinite field and W be a finite dimensional vector space over $\mathbb{K}$
Then $f : W \longrightarrow \mathbb{K}$ is said to be a polynomial function if it can be written in the polynomial form with coeffecients in $\mathbb{K}$ and coordinates determined wit respect to W.

5.2 Coordinate ring

In fact the set of all polynomial functions over W forms a $\mathbb{K}$-algebra $\mathbb{K}[\mathbb{W}]$. This is termed as coordinate ring of $\mathbb{W}$'
If $w_1, \dots w_n$ form basis of W and $x_1, \dots, x_n$ be the corresponding dual vectors of W^* then $K[W] = k[x_1, \dots x_n]$
In fact the coordinate functions are algebraically independent
Lets check this out
Suppose $f(a_1, \dots, a_n) = 0$ such that $f \neq 0$ then since x_i are dual basis corresponding to w_i such that $x_i(w_i) = \delta_{x_i(w_i)}$
So $f(x_1, x_2, \dots x_n)w_j = 0 \; \forall 1 \leq i \leq n$
This implies $f = 0$

5.3 Homogenous polynomial functions

Polynomial $f \in K[W]$ is said to be homogenous of degree d if $f(tw) = t^d f(w)$ $\forall t \in K$ and $w \in W$

Note $k[W] = \bigoplus K[W]_d$
So $K[W]$ is a graded k algebra for if f and $g \in K[W]_d$ and $K[W]_e$ respectively then $fg \in K[W]_{d+e}$

5.4 Invariants

A polynomial function $f \in k[W]$ is said to be G invariant if $f(gw) = f(w)\forall g \in G$ and $w \in W$
Here the action of g on W is defined as
$gw = H(g)w$ where $H : G \Longrightarrow Gl_nW$ is a representation of G on W via H
The invariants form a subalgebra denoted by $k[W]^G$
A function $f \in K[W]$ is G invariant if it is constant on all orbits of G in W

5.5 Regular representation of G on $k[W]$

With respect to this representation the action of G on $K[W]$ is defined as $gf(w) = f(g^{-1}w)\forall g \in G$ and $w \in W$
With this action of G on W , f is G invariant if $gf = f\ \forall g \in G$
$k[W]_d$ is G invariant ring as if $f \in k[W]_d$ and $g \in Ggf = f(g^{-1}w)$ has degree d.
So $k[W]^G = \bigoplus k[W]_d$
Hence $k[W]^G$ is a graded algebra
Examples of invariant rings

Example 5.1. Prove $k[x,y]^{Gl_2} = k[x,y]^{Sl_2} = k$
Since $Sl_2 \subseteq Gl_2 then$k[x,y]$^{Gl_2} \subseteq k[x,y]^{Sl_2}$
Suppose $f \in k[x,y]^{Gl_2}$
$\Rightarrow g^{-1}f = f\forall g \in G$.
$\Rightarrow f(gw) = f(w)$
When $f = x$ then

$$x \circ (gw) = x \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \right)$$

where $w = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$
let

$$x(gw) = \begin{bmatrix} aw_1 + bw_2 \\ cw_2 + dw_2 \end{bmatrix}$$

$x \circ (gw) = aw_1 + bw_2$
$x(w) = w_1$
So $b = 0$ and $a = 1$
Now let $f = y$ Then $y \circ g(w) = cw_1 + dw_2 = y(w) = w_2$

$\Rightarrow c = 0$
x will be invariant only under the action of

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}$$

So x and $y \notin k[x, y]_G$
So $k[x, y]_G = k$
$k \subseteq k[x, y]^{Gl_2} \subseteq k[x, y]^{Sl_2} = k$
$\implies k[x, y]^{Gl_2} = k$

Example 5.2. Prove that $k[x, y] = k[y]$ where $U = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} : s \in k$
such that $U \subseteq Sl2(k)$
Suppose $f \in k[x, y]^U$
$g^{-1}f(w) = f(gw)$

$$gw = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} w_1 + sw_2 \\ w_2 \end{pmatrix}$$

where $g \in U$ and

$$w = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$$

$g^{-1}x(w) = x(gw) = w_1 + sw_2$
Suppose $x \in k(x, y)^U$
$\implies x(gw) = x(w) = w_1 + w_2 = w_1$
$\implies s = 0$
So $x \notin k[x, y]^U$
Now $y \circ (gw) = w_2 = y(w)$
$k[x, y]^U = k[y]$

Example 5.3. Prove that $k[W]^{Gl_1(k)} = k[x, y]$
where

$$t \longrightarrow \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$$

Let $f \in k[W]^G l_1(k)$

$$tw = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} tw_1 \\ t^{-1}w_2 \end{pmatrix}$$

Then $t^{-1}f(w) = f(w)$

$$f(tw) = f(w)$$

Suppose $f = x$

$$x(tw) = x(w)$$

$$tw_1 = w_1$$

$$w_1(t-1) = 0$$

$\implies t = 1$
Now let $t^{-1}xy(w) = xy(tt^{-1}w) = w_1w_2$

$$k[W]^{Gl_1}(k)$$

is generated by xy
$k[W]^{Gl_1}(k) = k[xy]$

Example 5.4. Prove $k[M_n]^{Sl_n} = k[det]$
action of Sl_n on M_n is defined as

$$(g.A) \longrightarrow (gA)$$

where $g \in Sl_n$ and $A \in M_n(k)$
Proof $\det(gA) = (\det g)(\det A) = \det A$
So $\det A \in k[M_n]^{Sn}$
Let f be invariant
Define polynomial $p(t) \in k[t]$ by

$$p(t) = f\left\{\begin{pmatrix} t & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\right\}$$

Then

$$A = g\left\{\begin{pmatrix} \det(A) & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}\right\} \text{ where } g \in SL(K)$$

$$f(A) = f\left\{ g\begin{pmatrix} \det(A) & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \right\} = p(\det(A) = p(\det A))$$

so $f \in k(\det A)$

References

[Dummit and Foote(2004)] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[Kraft and Procesi(July 1996)] Hanspeter Kraft and Claudio Procesi. Invariant theory. July 1996.