Applications of Groebner Bases

Harshita Mahla

A dissertation submitted for the partial fulfillment of BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali

April 2017

Certificate of Examination

This is to certify that the dissertation titled "Applications of Groebner Bases" submitted by **Ms. Harshita Mahla** (Registration Number: **MS12111**) for the partial fulfillment of **BS-MS dual degree program** of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Varadharaj R. Srinivasan Dr. Abhik Ganguli Dr. Chetan Balwe

(Supervisor)

Dated: April 21, 2017

Declaration

The work presented in this dissertation has been carried out by me under the guidance of Dr. Chetan balwe at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of work done by me and all sources listed within have been detailed in the bibliography.

Harshita Mahla

(Candidate)

Dated: April 21, 2017

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Chetan Balwe

(Supervisor)

Acknowledgement

I take this opportunity with immense pleasure to thank all the people who have helped me in successful completion of my master's thesis. First of all I would like to express my gratitude to Dr. Chetan Balwe for providing me the opportunity to work under his guidance and for giving me timely advice to understand my goals.

I would like to express my sincere thanks to my family for being constant support and invaluable guidance. I would also like to thank my friends Parul and Adarsh at IISER Mohali for their immense support and for helping me with LaTeX. I would also like to thank the authors of all the books and research articles whose ideas and results I have presented in this work.

Harshita Mahla

Notation

k	Field
Z	Ring of integers
$R[y]$	Ring generated by y over R
$R[y_1, .., y_n]$	Ring generated by $y_1, ..., y_n$ over R.
Y	n-tuple $y_1, ..., y_n$.
$R[Y]$	Ring generated by $y_1, ..., y_n$ over R.
$\mathbb{Z}$	$\{...., -2, -1, 0, 1, 2, ...\}$.
$\mathbb{R}$	Field of Real numbers.
$\mathbb{C}$	Field of Complex numbers.

Contents

Abstract

This work consists of four chapters. In the first three chapters work is done only over field k. The initial part includes the study of division algorithm in the polynomial ring in one variable y over the field. It is shown that ideal description problem (IDP) and ideal membership problem (IMP) are solvable in $k[y]$. In division algorithm in $k[y]$ for every division one get a unique remainder. But the uniqueness of remainder fails for the division algorithm in the polynomial ring in multiple variables $y_1, ..., y_n$ over k. The division algorithm in $k[y]$ helps in solving the IMP. In $k[y]$, $r = 0$ is the only condition for solving IMP. But because uniqueness of r fails in $k[y_1, ..., y_n]$, $r = 0$ is the sufficient condition for IMP in $k[x_1, ..., x_n]$, not the necessary. So some "good" generators with special properties are needed such that when some polynomial get divided by these generates one get unique remainder and $r = 0$ mean that polynomial belongs to the ideal. These "good" generators are called "Groebner Basis". So in this work, the ideal membership problem and ideal description problem are solved using Groebner Basis in an algorithmic fashion. Groebner bases are constructed using $S-$ polynomials by Buchberger's algorithm in this thesis.(see [DO07])

In the third chapter, it is shown that how algebra is linked to geometry. Then the concept of variety is introduced. The ideal-variety correspondence is proved. Ideal and variety connect the algebra with geometry. Varieties provide a geometrical view to the algebraic understanding given by ideals. Then weak, strong and Hilbert's Nullstellensatz is given, which establishes some connection between ideals and varieties. Next, it is given that any property of varieties leads to some property for ideals in an almost opposite way and vice versa. Construction of radical of an ideal using Groebner basis is given. The decomposition of a variety into irreducibles is given and since there is a correspondence between ideals and variety, decomposition of ideals is also possible.

In the last chapter, the work is done on the commutative Noetherian ring with identity. It's given that for zero-dimensional ideals Groebner basis possesses some special properties. It is possible to recognize a zero-dimensional ideal just by looking at it's

Groebner basis. Then the ways by which one can compute Groebner bases for some basic operations on ideals are given. An algorithm is given which is helpful in checking whether a given ideal is prime or not. Then primary decomposition of zero-dimensional ideals is being presented. One is the general standard way. The second is when the coefficient ring is the field of characteristic 0, then one first makes the ideal in the general position then decompose it. Then an algorithm to primary decompose a general ideal where the ring is a polynomial ideal domain is given. It's given how one can reduce the high dimensional ideals into zero-dimensional ideals by using the localization at principal prime ideals. So first these general ideals can be turned into some zero-dimensional ideals and then the primary decomposition can be done. (see [GG])

Chapter 1

Polynomial ring in one variable over field

I will use Groebner basis in giving the solutions of the two important problems related to ideals in $K[y_1, ..., y_n]$. These problems that I want to solve are Ideal membership problem and ideal description problem. The solution will be derived in an algorithmic way.
These are the statements of the problems that are mentioned above-

1. **Ideal Description Problem (IDP)**:- Is it possible to find some finite basis for ideals in $k[y_1, ..., y_n]$?

2. **Ideal Membership Problem (IMP)** :- Given a finite generating set for an ideal $I \subset k[y_1, ..., y_n]$, is there any way to find out whether a given polynomial h belongs to ideal I or not?

In this chapter, I will prove that there is always a way to find solution for IDP and IMP in $k[y]$.

Assume that $g = b_0y^n + b_1y^{n-1} + ... + y_n$, clearly $g \in k[y]$. The conditions $b_0 \neq 0$ and every $b_i \in k$ are given. So lt(g) (lt means leading term) is equal to b_0y^n.

Given that $g, h \neq 0$, if the degree of h is greater than the degree of g then lt(g) will divide lt(h) and vice versa.

Proposition 1 ***(The division algorithm)*** *Suppose k is a field , $h \neq 0$ and in $k[y]$. Then every l in $k[y]$ has the following form*

$$l = ph + r,$$

Here p and r conditioned to be unique and they belong to $k[y]$. r is zero or the degree of r is less than the polynomial h. There exists an algorithm which helps us to find p and r.

1: Input : h, l

2: Output : p, r

3: $p := 0; r := l$

4: WHILE $r \neq 0$ AND $lt(h)$ divides $lt(r)$ DO

5: $\quad p := p + lt(r)/lt(h)$

6: $\quad r := r - (lt(r)/lt(h))h$

Proof: First, let me explain the each step of the algorithm. So here p and r are the output means the result that we want. We are changing the values of p and r every time we go through the while-do loop. This loop will go on until the value of r becomes zero or the leading term of h stop dividing leading term of r (means the degree of r becomes smaller than the degree of h). For every algorithm, there are three things to check about it -

(1) It always works which means that even after that p and r keep changing the values the form of l $l = ph + r$, should always be the same.

(2) It should terminate. Which simply means that the while-do loop must stop somewhere. As we mentioned earlier that it implies that r should become zero at some point in time or the leading term of h should stop dividing leading term of r.

(3) In the end, when it terminates, it should give the expected values of p and r means that it must give us the unique p and r.

For proving (1) let us first see that the values that we decided for p and r in the starting of the algorithm satisfy the form $l = ph + r$. So in the starting the values were

$p = 0; r = l$, when we put these values in $l = ph + r$ it becomes $l = 0.h + l = l = l$ so the argument is proved for the initial values. Now let this prove for the changing values of p and r. For that let us put $p := p + lt(r)/lt(h)$ and $r := r - (lt(r)/LT(h))h$ in $l = ph + r$. Then $l = ph + r$ becomes

$$l = (p + lt(r)/lt(h))h + (r - (lt(r)/lt(h))h) = ph + r.$$

So our argument is proved for every value of p and r.

For proving (2) let us first prove our claim that $r := r - (lt(r)/LT(h))h$ is zero or its degree is less than degree of r. For proving the claim I would like to assume some form of h and r.

$$h = a_0y^s + ... + a_s, lt(h) = a_0y^s,$$

$$r = b_0y^q + ... + b_q, lt(r) = b_0y^q,$$

Let us assume that degree of r is greater than degree of h means $q \geqslant s$. So

$$r - (lt(r)/lt(h))h = (b_0y^q + ...) - (b_0/a_0)y^{q-s}(a_0y^s + ...),$$

If we look at this we sense that $deg(r)$ has to drop. we have value q finite which clearly means that degree can't drop more than finite times. And that implies that algorithm will terminate at some finite point.

Now, this is time to prove our third point. Let us say we don't have the unique p and r, we also have p' and r' with same properties such that $l = ph + r = p'h + r'$. Here as we said the degree of r is less than the degree of h and degree of r' is less than the degree of h'. Which implies that degree of $r - r'$ is less than the degree of h.

By readjusting $l = ph + r = p'h + r'$ we get $(p - p')h = r - r'$. Since r and r' are different $(p - p')$ can' be 0. So we see that $deg(r - r')$ which we can write as $deg((p - p')h) = deg((p - p')) + deg(h)$ which is definitely greater than $deg(h)$. That is the contradiction and this makes $r = r'$, and $q = q'$. Hence we proved our third point. Here the proof ends.

□

Example 1 *Let us give an example of the division algorithm- We want to divide* $l(y) = y^5 - 3y^2 + 1$ *by* $h(y) = y^2 - 4y + 7$,

As we keep in our mind the leading term of these polynomials we write them in decreasing order of terms. $lt(l(y)) = y^5 = y^3.lt(h(y)))$,

so we will subtract $y^3.h(y)$ *from* $l(y)$ *to cancel lt(l(y)).*

So, $l(y) - y^3.h(y) = 4y^4 - 7y^3 - 3y^2 + 1$.

Now $lt(l(y) - y^3.h(y)) = 4y^2.lt(h(y))$ *,so let us do*

$(l(y) - y^3.h(y)) - 4y^2.(h(y)) = 9y^3 - 31y^2 + 1$

and we will continue with the same calculation till we get a polynomial which does not have degree more than 1.

$9y^3 = 9y.lt(h(y))$ *so,* $(9y^3 - 31y^2 + 1) - 9y.h(y) = 5y^2 - 63y + 1$

$5y^2 = 5.lt(h(y))$ *, so* $(5y^2 - 63y + 1) - 5.h(y) = -43y - 34$

So, $l(y) - y^3.h(y) - 4y^2.h(y) - 9y.h(y) - 5.h(y) = -43y - 34$

so, $l(y) = (y^3 + 4y^2 + 9y + 5).h(y) + (-43y - 34)$

here $p(y) = y^3 + 4y^2 + 9y + 5$ *and* $r(y) = -43y - 34$.

Here we have the following order on the variable y

$$.... > y^{n+1} > y^n > ..... > y^2 > y > 1.$$

The credit of the algorithm being successful goes to the the systematic way of working on leading terms of h and l.

Corollary 1 *The ideals of* $k[y]$ *have a single element as their generator.*

Proof: $k[y]$ is a Euclidean domain which makes it a PID. This completes our argument. □

So we found solution to our IDP in above corollary.

We can always compute the greatest common divisor of elements of $k[y]$. We have an algorithm named *Euclidean algorithm* for computing greatest common divisor. [DO07]

Now I will explain the method to derive solution for IMP.

Step 1- The very first thing that we are supposed to do is to find greatest common divisor

of the finite basis of our given ideal.

Step 2- Then we divide the given polynomial h by the generators of the ideal with the help of division algorithm.

Step 3 - Now we will check the value of r. If our r is zero then h belongs to the ideal otherwise, doesn't.

Chapter 2

Polynomial ring in n variables over fields

2.1 Monomial ordering and the Division Algorithm in $k[y_1, ..., y_n]$

There exists a relation between monomials in Polynomial ring of n variables and elements of $Z^n_{\geq 0}$ because the elements of $Z^n_{\geq 0}$ are of the form $\beta = (\beta_1, ..., \beta_n)$ and the monomials have the form $y^\beta = y_1^{\beta_1}...y_n^{\beta_n}$. So if we have an ordering on $Z^n_{\geq 0}$ that will directly form the ordering on monomials.

Basically monomial ordering on the polynomial ring with multiple variables is a relation $>$ on $Z^n_{\geq 0}$, such that (1) $>$ is a total order on $Z^n_{\geq 0}$ (2) If two elements β and γ are there in $Z^n_{\geq 0}$ such that $\beta > \gamma$ and we have α in $Z^n_{\geq 0}$ then then sum of $\beta + \alpha > \gamma + \alpha$. The last property is (3) Each subset of $Z^n_{\geq 0}$ should have a smallest element in it under the relation $>$.
So basically if we have $\beta > \gamma$ then it is confirmed that $y^\beta > y^\gamma$.

There exists many kinds of ordering on the elements of $Z^n_{\geq 0}$. Mostly we use these two -

Definition 1 ***(Lexicographic Order)*** *Assume that we have two elements β and γ of $Z^n_{\geq 0}$. The elements β and γ can be written as $\beta = (\beta_1, ..., \beta_n)$ and $\gamma = (\gamma_1, ..., \gamma_n)$. When we take the difference between them say $\beta - \gamma = (\beta_1 - \gamma_1, ..., \beta_n - \gamma_n)$ then if the $\beta_1 - \gamma_1$*

is positive, then it means that $\beta >_{lex} \gamma$. This implies that $y^\beta >_{lex} y^\gamma$.

Definition 2 ***(Graded Lex Order)*** *Assume that we have two elements β and γ of $Z^n_{\geq 0}$. The elements β and γ can be written as $\beta = (\beta_1, ..., \beta_n)$ and $\gamma = (\gamma_1, ..., \gamma_n)$. Let us say we have $|\beta| = \sum_{i=1}^n \beta_i$ and $|\gamma| = \sum_{i=1}^n \gamma_i$. Then (1) if $|\beta| > |\gamma|$ then $\beta >_{grlex} \gamma$. And (2) if $|\beta| = |\gamma|$ then we will check for lexicographic order and then if we have $\beta >_{lex} \gamma$, then $|\beta| >_{grlex} |\gamma|$.*

If we are going to work in say 3 variables then instead of y_1, y_2, y_3 we will use y, x, z. The lexicographic ordering will be defined like $y > x > z$.

Suppose we have a polynomial h in $k[y_1, ..., y_n]$ which is not zero. Let us say it has the form $h = \sum_\beta b_\beta y^\beta$. Assume that we are given a monomial ordering $>$. We want to define some terms- Multidegree of h is the maximum of β such that b_β is non-zero. b_β where the β is the multidegree is called leading coefficient (lc(h)). Similarly y^β where β is the multidegree is called the leading monomial (lm(h)), it should have coefficient 1. And finally, the multiplication of leading coefficient and leading monomial of h is known as the leading term (lt(h)).

Lemma 1 *Consider two elements g and h from $k[y_1, ..., y_n]$, which are nonzero. Then we can see that*
(1)Multidegree of the multiplication of g and h is equal to the sum of multidegree of g and the multidegree of h.
(2) If the sum of those two polynomials is non-zero then multidegree of the sum of g and h is less than or equal to the maximum of multidegree of g and h. If we add one more condition to it that multidegree of g and h are different then the multidegree of the sum of g and h is equal to the maximum of multidegree of g and h.

Theorem 1 *Assume that we have a monomial ordering $>$ on $Z^n_{\geq 0}$. If we have a m-tuple $H = (h_1, ..., h_m)$ which is ordered, all h_i are polynomials. Then each h of $k[x_1, ..., x_n]$ has the form*

$$h = b_1 h_1 + ... + b_m h_m + r$$

all the b_i and r belongs to $k[y_1, ..., y_n]$. Here r is conditioned to be 0 or a linear combination of monomials where none of the $lt(h_1), ..., lt(h_m)$ can divide them and the coefficient in the linear combination are from k. r is called remainder of the polynomial h when H

divides it. When the terms b_ih_is are non zero then the multidegree of h is greater than or equal to multidegree of b_ih_i.

Proof: Here we introduce some new variables like q and *divisionoccurred*. So we call q the intermediate dividend. And the *divisionoccurred* is a term by which we means that lt(q) is divided by some $lt(h_i)$. Going through the while do means that one of the following two steps is happening-

- (Division Step) Whenever $lt(q)$ is being divided by some $lt(h_i)$, then the division algorithm works like the algorithm of $k[y]$.
- (Remainder Step) If $lt(q)$ is not divisible by any $lt(h_i)$ then $lt(q)$ is added to r by the algorithm.

Input : $h_1, ..., h_m, f$
Output : $b_1, ..., b_m, r$
$b_1 := 0; ....; b_m := 0; r := 0$
$q := h$
WHILE $q \neq 0$ DO
    $i = 1$
    divisionoccurred := false
    WHILE $i \leqslant m$ AND divisionoccurred = false DO
        IF $lt(h_i)$ divides (q) THEN
            $b_i := b_i + lt(q)/lt(h_i)$
            $q := q - (lt(q)/lt(h_i))h_i$
            divisionoccurred:= true
        ELSE
            $i := i + 1$
    IF divisionoccurred = false THEN
        $r := r + lt(q)$
        $q := q - lt(q)$

Just as the case of one variable we need to check three things about this algorithm

but here we have on more thing to check, that is the multidegree of h and $b_i h_i$. So we need to check the following-

(1) It always works which means that even after that p, r and b_is keep changing the values according to the division and remainder step, the form of h,

$$h = b_1 h_1 + ... + b_m h_m + p + r \tag{2.1}$$

should always be the same.

(2) It should terminate. Which simply means that the while-do loop must stop somewhere. It implies that $lt(q)$ must be divided by some $lt(h_i)$ in the end.

(3) In the end, when it terminates, it should give the expected values of p and r mentioned in the theorem statement.

(4) In the last, we need to check that When the terms $b_i h_i$s are non-zero then the multidegree of h is greater than or equal to multidegree of $b_i h_i$.

For proving (1) let us first see that the values that we decided for $b_i, .., b_m$,p and r in the starting of the algorithm satisfy the equation (2.1). So in the starting the values were $p = h$; $b_i, .., b_m$ = 0 and $r = 0$, when we put these values in (2.1) it becomes $h = 0.h_1 + ... + 0.h_m + h + 0 = h$. The argument is true in the starting. Now let us check whether it holds on the division step or not. So in the division step $lt(q)$ is being divided by some $lt(h_i)$. so $b_i h_i + q$ becomes $(b_i + lt(q)/lt(h_i))h_i + q - (lt(q)/lt(h_i))h_i$ and by this we get $b_i h_i + q$ again. As we didn't change other variables so (2.1) holds. Now we check for the remainder step. In this step values of q and r changes and if put the new values of p and r in $q + r$ then it becomes $q - lt(q) + r - lt(q)$ which will become $q + r$ again. We didn't change any other variable so (2.1) is the same.

Now I will prove (2), We need to prove that in the end, q will be zero. So first let us look at q at the time of division step let us say $q' = q - (lt(q)/lt(h_i))h_i$

By the lemma (1), we get $lt((lt(q)/lt(h_i))h_i) = (lt(q)/lt(h_i)).lt(h_i) = lt(q)$ So basically the leading term of q will get canceled and then multidegree of q' will become less than multidegree of q. which means the multidegree of q is decreasing. Now we see that in the remainder step $q' := q - lt(q)$.Again the leading terms are getting canceled so multidegree of q is decreasing. It is decreasing with every step. So we are having a sequence of mutidegrees which is a decreasing sequence. Since the monomial order is well-ordering, this sequence infinite. So the algorithm will be ended after finite steps.

Now let us prove the point (3). When we have the value of q zero then (2.1) have the form $h = b_1h_1 + ... + b_mh_m + r$. And according the algorithm we only add those terms to r which are not divisible by $lt(h_i)$. From here we see that all b_i and r have the expected values.

In the end, I will prove the point (4). So we can see that b_i have the term $lt(q)/lt(h_i)$. In the starting, we had the value of q, h And by the time multidegree of q start to decrease. So $lt(q) < lt(h)$. By the property of monomial ordering multidegree of b_ih_i will be less than multidegree of h. So we proved the theorem. □

I would like to give an example of the uniqueness of r.

Example 2 *Let us assume that $h_1 = xy + 1, h_2 = x^2 - 1$ belongs to $k[y, x]$. We have the lex order here. Whe we divide $h = yx^2 - y$ by $H = (h_1, h_2)$ then we get*

$$yx^2 - y = x.(xy + 1) + 0.(x^2 - 1) + (-y - x).$$

But when we change the order of polynomials such $H = (h_2, h_1)$ then we get

$$yx^2 - y = y.(x^2 - 1) + 0.(xy + 1) + 0.$$

So we get two different r because of the change in the order of polynomials. Which contradicts the uniqueness of r.

Division algorithm in $k[y_1, ..., y_n]$ doesn't solve the IMP in the way Division algorithm in $k[y]$ do. As even if h belongs to the ideal which has generating elements h_1, h_2,there is a possibility that we get the value of r not equal to zero on getting divided by $H = (h_1, h_2)$.

Thus $r = 0$ is a sufficient condition for IMP. But, according to the above example, we can have the polynomial in the ideal even if the value of r is not zero.
We want our remainder r on division by the generators to be provided uniquely and the condition $r = 0$ should be same as having that the polynomial belongs to the ideal. So, we want different generators with special properties.

2.2 Groebner Bases and their properties

Definition 3 *Suppose that we have a subset H of $Z^n_{\geq 0}$. If an ideal J of $k[y_1, ..., y_n]$ contains all polynomials which are finite sums of the form $\sum_{\beta \in H} f_\beta y^\beta$, then J is said to be monomial ideal. Here f_β is an element of $k[y_1, ..., y_n]$. We denote J as the ideal generated by y^β.*

Lemma 2 *Suppose that J is a monomial ideal generated by y^β. Then we see that y^γ belongs to the ideal J iff y^β divides y^γ where γ and β belongs to the subset H of $Z^n_{\geq 0}$.*

Proof: Suppose that y^β divides y^γ which means that y^γ can be written as $b.y^\beta$ for some b in $k[y_1, ..., y_n]$. Which simply implies that y^γ belongs to the ideal J.
Now to prove the other containment let us assume that y^γ belongs to the ideal J so we can write y^γ as $\sum_{i=1}^n f_i y^{\beta(i)}$ here the f_i are polynomials in $k[y_1, ..., y_n]$ and $\beta(i)$ belongs to H. Since we every f_i can be written as a linear combination of monomials which will implies that we can divide every term of $\sum_{i=1}^n f_i y^{\beta(i)}$ by some $x^\beta(i)$.So, x^β must have the same property. □

For being two monomial ideal to be equal they must have all same monomials and vice versa.

Theorem 2 ***(Dickson's lemma)*** *Suppose that J is a monomial ideal in $k[y_1, ..., y_n]$ which is generated by y^β where β belongs to H. Then we can see that J has a finite generating set, say $y^{\beta(1)}, ..., y^{\beta(m)}$ such that $\beta(1), .., \beta(m)$ belongs to the subset H.*

Proof: We will prove the theorem by the induction on the number of the variables n. If we take n = 1 then J is generated by the monomials y_1^β , where β belongs to H. Let us assume that α is the smallest element of H. Then $\alpha \leqslant \beta$ for all β belongs to H. So now we can see that y_1^α divides all other generators y_1^β. So it follows that J is generated by y_1^α.
Now suppose that this theorem is true for $n-1$ and we need to prove it for n, where $n > 1$. Now let us write the variables as $y_1, ..., y_{n-1}, x$ such that the monomials in $k[y_1, ..., y_{n-1}, x]$ can be written as $y^\beta x^s$, where $\beta = (\beta_1, ..., \beta_{n-1})$ which belongs to $\mathbb{Z}^{n-1}_{\geqslant 0}$ and s belongs to $\mathbb{Z}_{\geqslant 0}$.
Let us assume that $J \subset k[y_1, ..., y_{n-1}, x]$ is a monomial ideal. Suppose that I is the ideal

in $k[y_1, ..., y_{n-1}]$ generated by the monomials y^β such that $y^\beta x^s$ belongs to J for some $s \geqslant 0$. Since I is a monomial ideal in $k[y_1, ..., y_{n-1}]$, our inductive hypothesis implies that finitely many of the y^β's generate I. Let us say $J = \langle y^{\beta(1)}, ..., y^{\beta(m)} \rangle$. We can see the ideal I as the projection of J into $k[y_1, ..., y_{n-1}]$. According to the way we defined I, $y^{\beta(i)} x^{s_i}$ will belong to J, for each $1 \leqslant i \leqslant m$ and some $s_i \geqslant 0$. Suppose that s is the largest of the s_i . Then, for each $0 \leqslant k \leqslant s-1$, consider the ideal $I_k \subset k[y_1, ..., y_{n-1}]$ generated by the monomials y^α such that $y^\alpha x^k$ belongs to J . We can think of I_k as the slice of J generated by monomials which contains x exactly to the kth power. By using our inductive hypothesis again, we can see that I_k has a finite generating set of monomials, say $I_k = \langle y^{\beta_k(1)}, ..., y^{\beta_k(m_k)} \rangle$.

Now we claim that J is generated by the monomials in the following list:

$$fromI : y^{\beta(1)} x^s, ..., y^{\beta(m)} x^s$$

,

$$fromI_0 : y^{\beta(1)}, ..., y^{\beta_0(m_0)},$$

$$fromI_1 : y^{\beta_1(1)} x, ..., y^{\beta_1(m_1)} x$$

,

$$..$$

$$..$$

$$fromI_{s-1} : y^{\beta_{s-1}(1)} x^{s-1}, ..., y^{\beta_{s-1}(m_{s-1})} x^{s-1},$$

We claim that we can divide every monomial in J by one on the list. To prove the claim let $y^\beta x^p$ belongs to J. If $p \geqslant s$, then by the way we constructed I we can see that some $y^{\beta(i)} x^s$ divides $y^\beta x^p$. On the other hand, if $p \leqslant s-1$, then by the construction of I_p we see that some $y^{\beta_p(j)} x^p$ divide $y^\beta x^p$. Now from lemma (2) it follows that the above monomials generate an ideal having the same monomials as J . So the ideals will be same. So our claim is proved now.

The last thing we need to show is that the finite set of generators can be chosen from a given set of generators for the ideal. If we switch back to writing the variables as $y_1, ..., y_n$, then our monomial ideal is $J = \langle y^\beta : \beta \in H \rangle \subset k[y_1, ..., y_n]$. So We need to show that J is generated by finitely many of the y^β's, where $\beta \in H$. We already know that $J = \langle y^{\alpha(1)}, ..., y^{\alpha(m)} \rangle$ for some monomials $y^{\alpha(i)}$ in J. Since $y^{\alpha(i)} \in J = \langle y^\beta : \beta \in$

$H\rangle$, we can see that each $y^{\alpha(i)}$ is divisible by $y^{\beta(i)}$ for some $\beta(i) \in H$. From here we can see that $J = \langle y^{\beta(1)}, ..., y^{\beta(m)}\rangle$. This completes the proof. □

Definition 4 *Suppose I is an ideal of $k[y_1, ..., y_n]$ and it is not the zero ideal then-*

1. *$lt(I)$ denotes the set which contains the leading terms of all elements of the ideal I. So, we have*

$$lt(I) = \{by^\beta : \exists h \in I \quad such \quad that \quad lt(h) = by^\beta\}$$

2. *The elements contained in $lt(I)$ generates the ideal $\langle lt(I)\rangle$.*

Let us say that I is generated by some finite elements $h_1, ..., h_m$. Then it is not necessary for $lt(I)$ and the ideal generated by $lt(h_1), .., lt(h_m)$ to be equal.

Proposition 2 *Suppose we have an ideal I of $k[y_1, ..., y_n]$*

1. *Then the ideal $\langle lt(I)\rangle$ is monomial ideal.*

2. *$\exists$ some elements $g_1, ..., g_m$ in I so that the ideal $\langle lt(I)\rangle$ is equal to the ideal generated by $lt(g_1), .., lt(g_m)$.*

Proof:

1. As we know we can always have an ideal generated by monomials of polynomials of I which is the monomial ideal. And we know that there is only the difference of constant between the leading monomial and the leading term of an element. So the monomial ideal will be equal to the ideal generated by leading terms of polynomials of I. Our argument is proved.

2. As we have seen before that leading monomials of elements g_i of I generates $\langle lt(I)\rangle$ so according to the Dickson's lemma only finitely many leading monomials of $g_1, .., g_m$ will generate $\langle lt(I)\rangle$. And as I mentioned earlier there is only the difference of constant between the leading monomial and the leading term of an element. So finitely many leading terms of elements $g_1, .., g_m$ of the ideal I will generate $\langle lt(I)\rangle$. Our argument is proved.

□

Theorem 3 ***(Hilbert Basis Theorem)*** *There exists a generating set $g_1, .., g_m$ for every ideal in $k[y_1, ..., y_n]$. This set is finite and elements $g_1, .., g_m$ belongs to I.*

Proof: So let us start with the zero ideal. Then zero will generate the ideal.
Now if we have some element in I then we can construct the basis $g_1, .., g_m$ for it. As we proved in the last proposition that $\exists$ some elements $g_1, ..., g_m$ in I so that the ideal $\langle lt(I)\rangle$ is equal to the ideal generated by $lt(g_1), .., lt(g_m)$. So now I want to prove that the basis for the ideal I is $g_1, .., g_m$.

As g_i's are the elements of I so the ideal generated by $g_1, .., g_m$ will also be in the I. For the other inclusion let us assume that we have a polynomial h from I. Let us use the division algorithm here, when $g_1, .., g_m$ will divide h we will have

$$h = b_1g_1 + ... + b_mg_m + r$$

Here $lt(g_i)$'s don't divide the any term of r. We want to prove that r is equal to 0. We can write

$$r = h - b_1g_1 - .... - b_mg_m$$

which will belong to I. If we have r nonzero then since my r is in I , it's leading term will be in $\langle lt(I)\rangle$. Which is equal to the ideal generated by $lt(g_1), .., lt(g_m)$. That means some $lt(g_i)$ divides $lt(r)$. Which contradicts the properties of r. So r has to be zero. So h will be $h = b_1g_1 + ... + b_mg_m$. Which simply means that h belongs to the ideal generated by $g_1, .., g_m$. So we proved the theorem. □

Definition 5 *Let us determine a monomial ordering. Groebner basis is a subset of I ,$G = \{g_1, ..., g_m\}$, which is finite and has the property -*

$$\langle lt(I)\rangle. = \langle lt(g_1), ..., lt(g_m)\rangle$$

Corollary 2 *Let us determine a monomial ordering. Groebner basis exists for each ideal in $k[y_1, ..., y_n]$.*

So by the above theorem, the ideal description problem is solved for ideals in polynomial rings in multiple variables.

Proposition 3 *Suppose that for an ideal I in $k[y_1, ..., y_n]$, $G = \{g_1, ..., g_m\}$ is a Groebner basis. We have a polynomial h from $k[y_1, ..., y_n]$. Then there exists a polynomial r, which is unique and belong to $k[y_1, ..., y_n]$,with properties given below-*

1. *None of the $lt(g_1), ..., lt(g_m)$ can divide terms of r.*

2. *We always have a f from I so that we can write h as $h = f + r$.*
   Basically, whenever h gets divided by G we have r as the remainder. When we use division algorithm listing order of elements $\{g_1, ..., g_m\}$ does not matter, we will always get the same r.

Proof: Whenever h gets divided by G we have $h = b_1g_1 + ... + b_mg_m + r$ according to division algorithm. The properties of the r from division algorithm satisfies the point (1). Now if we assume that $f = b_1g_1 + ... + b_mg_m$, then f will belong to I as well as full fill the point (2). So at least till now we proved that r exists.
The only part that is remained to prove is the uniqueness of r. So to prove that, let us say we have another f' and r' with the same properties. Then $h = f + r = f' + r'$, by rearranging the terms we get $r - r' = f' - f$ which belongs to I. Now we see that if r and r' are not equal then leading term of $r - r'$ will belong to $\langle lt(I)\rangle$. That is equivalent to have that some $lt(g_i)$ will divide $lt(r - r')$. Which is a contradiction as we know that none of the $lt(g_i)$'s can divide r and r', so they can't divide $r - r'$ also. So r and r' has to be same. □

Corollary 3 *Suppose that ideal I belongs to $k[y_1, ..., y_n]$ has $G = \{g_1, ..., g_m\}$ as a Groebner basis. Assume we have a polynomial h from $k[y_1, ..., y_n]$. Then we see h is contained in I iff when G divides h we get the value of r zero.*

Proof: If h is contained in I then we can write h as h + 0. Here 0 indicated that r is zero.
If the remainder r has value zero then we already know that h is contained in I. □

This gives us the solution of IMP.

$\overline{h}^H$ denotes the remainder which we get when the ordered m-tuple $H = (h_1, ..., h_m)$ divides h.

Next, we want to see is there any way to identify that the given basis is Groebner basis.

Basically, there is only one answer to the question- why a particular set of basis say $\{h_1, ..., h_m\}$ is not Groebner basis. The answer is that in some linear combination of these elements the leading terms get canceled. Because of which the leading term of this combination will not belong to the ideal $\langle lt(h_1), ..., lt(h_m)\rangle$ but always belong to $\langle lt(I)\rangle$.

Example 3 *Let $I = \langle h_1, h_2\rangle$, where $h_1 = y^3 - 2xy$ and $h_2 = xy^2 - 2x^2 + y$, and let us define grlex ordering in $k[y, x]$. Then we will have one linear combination of h_1 and h_2 be like*

$$y.(xy^2 - 2x^2 + y) - x.(y^3 - 2xy) = y^2$$

Here as we can see y^2 will belong to I. Thus the leading term of polynomial y^2 which is y^2 will belong to $\langle lt(I)\rangle$. But $lt(h_1)$ which is y^3, or $lt(h_2)$ which is xy^2,both does not divide y^2 which means that y^2 does not belong to $\langle lt(h_1), lt(h_2)\rangle$.

Let us present $S - polynomial.$ which will explain the cancellation that happened above-

Definition 6 *Let us assume that g, h are polynomials from $k[y_1, ..., y_n]$.*

1. *Suppose α is the multidegree of g where we have $\alpha = (\alpha_1, .., \alpha_n)$ and β is the multidegree of h such that $\beta = (\beta_1, .., \beta_n)$ then we have $\gamma = (\gamma_1, ..., \gamma_n)$ such that each γ_i is the maximum of α_i and β_i. So basically y^γ is the LCM of $lm(g)$ and $lm(h)$.*

2. *We can write $S - polynomial$ of g and h in the following way-*

$$S(g, h) = \frac{y^\gamma}{lt(g)}.g - \frac{y^\gamma}{lt(h)}.h$$

Lemma 3 *Let us say there is a sum $\sum_{i=1}^{m} b_i h_i$ such that each coefficiant b_i is in the field k and each h_i has multidegree δ which belongs to $Z^n_{\geqslant 0}$. Whenever we see that multidegree of the sum $\sum_{i=1}^{m} b_i h_i$ is less than δ then it is fixed that this sum is basically equal to the linear combination of $S - polynomials$ of h_j, h_k foe every j, k between 1 to m, and coefficients belong to k. So multidegree of each S- polynomial is less than δ.*

Theorem 4 ***(Buchberger's Criterion)*** *Suppose I is ideal in $k[y_1, ..., y_n]$. Then generating set of I, $G = \{g_1, ..., g_m\}$ is called a Groebner basis iff When G divides $S(g_i, g_j)$ for all $i \neq j$, we get zero as the remainder.*

Proof: First assume that G is Groebner basis. Since $S(g_i, g_j)$ is basically a linear combination of g_i and g_j, which is a elements of I so when when G will divide $S(g_i, g_j)$ we will get zero as the remainder.
For proving the other way, assume that h is a polynomial from I, which is not 0. Then we want to prove that that $lt(h)$ will belong to $\langle lt(g_1), ..., lt(g_m)\rangle$, if we have remainder's value 0 when G divides $S-polynomials$. There exists polynomials f_i's in $k[y_1, ..., y_n]$ so that we can write h in the form

$$h = \sum_{i=1}^{m} f_i g_i \tag{2.2}$$

According to lemma (1) we can see that

$$multideg(h) \leqslant max(multideg(f_i g_i)). \tag{2.3}$$

Suppose $m(i)$ is the multidegree of $(f_i g_i)$ and let us assume that δ is the maximum of all $m(i)$s. So from here we can see that

$$multideg(h) \leqslant \delta.$$

Since we can write f as equation (2.3) in many possible ways. And there is a possibility that for every different expression ,δ will be different. We want to have the such a way to write h so that we can have δ minimum and this is possible as monomial ordering possesses a property of well ordering.

Basically what I want to do to prove this theorem is that I want to prove that multidegree of h is actually equal to the maximum of multidegrees of $f_i g_i$s. Because If I prove so, I would be able to see that some $lt(g_i)$ divides $lt(h)$. Which proves our theorem. Now for proving that multidegree of h is actually equal to the maximum of multidegrees of $f_i g_i$s, I have to write h in terms of $S - polynomials$, which I can do because if we see that there is no equality in the equation (2.3), then it means that some leading terms are cancelling each other. As we said in the statement that when G divides $S(g_i, g_j)$ for all $i \neq j$, we get zero as the remainder. that means we can write

$S - polynomials$ in some linear combination of g_is. By which at some point in time we can get leading terms which will not cancel out each other. So, in the end, I will be able to prove that there is an equality in equation (2.3).

As I mentioned earlier I need to prove that $multideg(h)$ is equal to δ. I would like to use contradiction here.

I want to write h in such a way that I can put those terms separately which have multidegree δ .

$$h = \sum_{m_i=\delta} f_i g_i + \sum_{m_i<\delta} f_i g_i = \sum_{m_i=\delta} lt(f_i) g_i + \sum_{m_i=\delta} (f_i - lt(f_i)) g_i + \sum_{m_i<\delta} f_i g_i \qquad (2.4)$$

So for multidegree(f) being less than δ, the sum at the first place must have multidegree less than δ.

I will study the first sum separately-

Assume that $lt(f_i) = d_i y^{\beta(i)}$. First sum can be written as

$$\sum_{m_i=\delta} lt(f_i) g_i = \sum_{m_i=\delta} d_i y^{\beta(i)} g_i$$

According to lemma (3) this sum can be written as a linear combination of $S(y^{\beta(j)} g_j, y^{\beta(k)} g_k)$. From the definition of $S - polynomials$

$$S(y^{\beta(j)} g_j, y^{\beta(k)} g_k) = \frac{y^\delta}{y^{\beta(j)} lt(g_j)} y^{\beta(j)} g_j - \frac{y^\delta}{y^{\beta(k)} lt(g_k)} y^{\beta(k)} g_k = y^{\delta - \alpha_{jk}} S(g_j, g_k)$$

, Here $y^{\alpha_{jk}}$ is the least common multiple of $lm(g_j$ and $lm(g_k)$. Now we can write the first sum as

$$\sum_{m_i=\delta} lt(f_i) g_i = \sum_{j,k} d_{jk} y^{\delta - \alpha_{jk}} S(g_j, g_k) \qquad (2.5)$$

where d_{jk} are the coefficients from k.

Now we will write $S - polynomials$ as a combination of g_is for the reason that I mentioned earlier. Then

$$S(g_j, g_k) = \sum_{i=1}^{m} c_{ijk} g_i \qquad (2.6)$$

such that c_{ijk} are from $k[y_1, ..., y_n]$. Accordng to the division algorithm multidegree of $c_{ijk} g_i$ is less than equal to multidegree of $S(g_j, g_k)$ for all i, j, k. Now we do the follwing multiplication

$$y^{\delta - \alpha_{jk}} S(g_j, g_k) = \sum_{i=1}^{m} a_{ijk} g_i$$

, Here a_{ijk} denotes $y^{\delta-\alpha_{jk}}c_{ijk}$. Then by applying lemma (3) we can see that

$$multideg(a_{ijk}g_i) \leqslant multideg(y^{\delta-\alpha_{jk}}S(g_j,g_k)) < \delta. \tag{2.7}$$

Now let us put the another form of $x^{\delta-\gamma_{jk}}S(g_j,g_k)$ in equation (2.5), we will get

$$\sum_{m_i=\delta} lt(f_i)g_i = \sum_{j,k} d_{jk}(\sum_{i=1}^{m} a_{ijk}g_i) = \sum_i \overline{f_i}\ g_i$$

As given above multidegree of $(\overline{f_i}\ g_i$ is less than δ for all i. So now we need to put the new form of $\sum_{m_i=\delta} lt(f_i)g_i$ in (2.4). By doing that such a form of f can be achieved in which multidegee of every term is less than δ. This is a contradiction to the minimality of δ. Our theorem is proved.

□

With the help of S-polynomial, we can construct Groebner basis.

Theorem 5 ***(Buchberger's Algorithm:-)*** *Soppose we have an ideal I from $k[y_1,...,y_n]$ which is generated by finite elements $h_1,....,h_t$. Then in finitely many steps we can construct the Groebner basis of I with the help of algorithm-*

1: Input : $H = (h_1,...,h_t)$
2: Output : A Groebner basis $G = (g_1,...,g_m)$ for I, with $H \subset G$
3:
4: $G := H$
5: REPEAT
6: $\quad G' := G$
7: $\quad$ FOR each pair $p, q, p = q$ in G' DO
8: $\quad\quad S := \overline{S(p,q)}^{G'}$
9: $\quad\quad$ IF $S \neq 0$ THEN $G := G \cup S$
10: UNTIL $G = G'$

Proof: For every algorithm, there are three things to check about it -

(1) G should always be contained in the I.

(2) When the algorithm will be terminated we will get a G, that G should be the Groebner

basis.

(3) The algorithm must be terminated at some finite point.

So in order to prove (1) let us see that in the starting we have said that G is equal to the H. H is a basis of I so it has to be in the ideal so G will also be contained in the I. Now at some point G will be $G \cup S$, where S is the remainder that we get by dividing $S(p, q)$, for p, q in G, with G'. Now as know that G is contained in I so p, q does belong to I. By following the same argument $S - polynomial$ of p and q also belongs to I and G' also belongs to I. So basically the remainder will also be in I. So from here, we have $G \cup S$ will belong to I. There is one more thing to notice that F is always contained in G so for I G is also a basis. So we proved our argument.

Now for proving the second point we see that we get G equal to G' in the end when algorithm gets terminated. So at that time, we will have the remainder of the $S(p, q)$ by dividing with G' zero. Then according to the above theorem, G will be considered as Groebner basis.

Only things which are left to prove is that at some finite point the algorithm will end. We have to see what happens when one loop ends and we for next loop. So we see that when algorithm goes on G' and the remainder that we get when we divide $S - polynomials$ of elements of G' by G', belongs to the new G. As we know that G contains G' so we can see that $\langle lt(G)\rangle \supset \langle lt(G')\rangle$. Now I wish to prove that whenever G and G' are not equal, we see that ideal generated by leading terms of element os G' is strictly contained in ideal generated by leading terms of elements of G. For proving this let us see that new G has remainder r along with G', so leading term of this r belongs to the ideal $\langle lt(G)\rangle$, but since we get this r when G' divided $S - polynomials$ which means that no term of (r) can be divided by leading term of any element of G'. So leading term of r doesn't belongs to the $\langle lt(G')\rangle$. Which means that $\langle lt(G')\rangle$ is strictly contained in $\langle lt(G)\rangle$. Now we can see that every time we finish one loop one element get attached to G, this whole process makes a chain of $\langle lt(G')\rangle$, which is ascending. So by the ACC of ideals, this chain has to stabilize, which will happen after finite steps. So in the end we will get that $\langle lt(G)\rangle$ is equal to $\langle lt(G')\rangle$. Which implies that both G and G' are same. So basically algorithm gets terminated after some finite steps. □

Lemma 4 *Suppose we have an ideal J in $k[y_1, .., y_n]$. And we have the Groebner basis of J. Suppose that we have an element g of G such that it's leading term belongs to the ideal generated by the leading terms of the elements of $G - \{g\}$. Then $G - \{g\}$ is also considered to be the Groebner basis of J.*

Proof: As we have seen that ideal generated by $lt(G)$ is equal to the ideal generated by $lt(I)$. If we assume that $lt(g)$ belongs to the ideal generated by the leading terms of the elements of $G - \{g\}$. Then since $lt(g)$ is in $lt(I)$, so it implies that the ideal generated by the leading terms of the elements of $G - \{g\}$ has to be equal to ideal generated by $lt(G)$. So eventually it will be equal to the ideal generated by $lt(I)$. Which proves that $G - \{g\}$ is a Groebner basis. □

Definition 7 *Suppose we have a Groebner basis G of I in $k[y_1, .., y_n]$. If leading coefficient of each element of G is 1 and leading term of any element won't belong to the ideal generated by leading terms of every other element of G. Then G is said to be a* ***minimal Groebner basis****.*

Definition 8 *Suppose we have a Groebner basis G of I in $k[y_1, .., y_n]$. If leading coefficient of each element of G is 1 and no monomial of any element of G, belong to the ideal generated by leading terms of every other element of G. Then G is said to be a* ***reduced Groebner basis****.*

Example 4 *We want to construct the Groebner bases for the ideal J generated by two polynomials h_1 and h_2. h_1 is $y^3 - 2xy$ and $h_2 = y^2x - 2x^2 + y$ given in example (4). Let us use grlex ordering on monomials in $k[y, x]$. From example (4) we concluded that $H = \{h_1, h_2\}$ is not a Groebner basis for I. So we will first calculate $S - polynomial$ of h_1 and h_2-*

$$S(y^3 - 2xy, y^2x - 2x^2 + y) = -y^2$$

This belongs to J. so,

$$\overline{S(h_1, h_2)}^H = -y^2$$

, This is not zero, let us denote $-y^2$ as h_3 so have to add this to the generating set. So generating set become $H = (h_1, h_2, h_3)$. So now compute

$$S(h_1, h_2) = h_3$$

, so now since the H includes h_3 also-

$$\overline{S(h_1,h_2)}^H = 0,$$

$$S(h_1,h_3) = (y^3 - 2xy) - (-y)(-y^2) = -2xy$$

,but the remiander is-

$$\overline{S(h_1,h_3)}^H = -2xy$$

Since the remainder in not zero, hence let us take $h_4 = -2xy$. So now our generating set is $H = (h_1, h_2, h_3, h_4)$ so we have-

$$\overline{S(h_1,h_2)}^H = \overline{S(h_1,h_3)}^H = 0$$

Now calculate -

$$S(h_1,h_4) = x(y^3 - 2xy) - (-\frac{1}{2})y^2(-2xy) = -2yx^2 = xh_4,$$

since it is a multiple of h_4 , it is divisible by h_4 and will have 0 remainder-

$$\overline{S(h_1,h_4)}^H = 0$$

$$S(h_2,h_3) = (y^2x - 2x^2 + y) - (-x)(-y^2) = -2x^2 + y,$$

but

$$\overline{S(h_2,h_3)}^H = -2x^2 + y.$$

Since the remainder is not 0 we should add this to H. So till now H has become $H = \{h_1, h_2, h_3, h_4, h_5\}$, Now if we compute the S-polynomials of h_i and h_j for all i not equal to j, then we get 0 remainder. So, our Groebner basis for J will be

$$\{h_1, h_2, h_3, h_4, h_5\} = \{y^3 - 2xy, y^2x - 2x^2 + y, -y^2, -2xy, -2x^2 + y\}$$

.

Example 5 *Let $J = \langle h_1, h_2\rangle = \langle xz - x^2, y^3 - z^2\rangle \in [y, x, z]$, and we have considered the grlex ordering. Suppose we have given $h = -4y^2x^2z^2 + x^6 + 3z^5$. We wish to check if h belongs to the ideal J .*

Since S-polynomial of h_1 and h_2 belongs to the ideal J it's leading terms will also belong to the $lt(J)$. Since $S(h_1, h_2) = -y^2x^2 + z^3$ so it's leading term is $-x^2y^2$. Since the ideal $\langle lt(h_1), lt(h_2)\rangle = \langle yz, y^3\rangle$. As we can see that $-x^2y^2$ doesn't belong to the

$\langle lt(h_1), lt(h_2)\rangle$ but belong to the ideal generated by $lt(J)$. Which means the given generating set is not a Groebner basis. Now we will find the Groebner basis of J as we did in the previous example. So we get

$$G = (xz - x^2, y^3 - z^2, x^2y^2 - z^3, yx^4 - z^4, x^6 - z^5).$$

now we need to divide h by G so we have

$$h = (-4yx^2z - 4x^4)\cdot(xz - x^2) + 0.(y^3 - z^2) + 0.(x^2y^2 - z^3) + 0.(yx^4 - z^4) + (-3).(x^6 - z^5) + 0\cdot$$

As we can see we get 0 remainder, it means that h belongs to the ideal J .

Chapter 3

Affine varieties and Ideals

3.1 Introduction to Affine varieties

Definition 9 *(**Affine Space:-**) Suppose that k is a field then*

$$k^n = \{(b_1, ..., b_n) : b_1, ..., b_n \in k\}$$

is called the n-dimensional affine space over k, where n is +ve integer.

Definition 10 *(**Affine variety:-**) Suppose that k is a field. Assume that we have polynomials $h_1, ..., h_m$ from $k[y_1, ..., y_n]$. Then the affine variety defined by $h_1, ..., h_m$ is given by-*

$$V(h_1, ..., h_m) = \{(b_1, ..., b_n) \in k^n : h_i(b_1, ..., b_n) = 0 \quad for \quad all \quad 1 \leqslant i \leqslant m\}$$

Lemma 5 *Assume that we have two affine varieties,V and T which belongs to k^n, then $V \cup T$ and $V \cap T$ are also the affine varieties.*

Proof: Let us assume that V and T are defined as $V = V(h_1, ..., h_s)$ and $T = V(f_1, ..., f_t)$. Then we want to prove that

$$V \cap T = V(h_1, ..., h_s, f_1, ..., f_t),$$

$$V \cup T = V(h_i f_j : 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t).$$

We want to prove the first claim first- intersection of varieties V and T means that in this intersection all h_i's and all f_i's all zero. Which is same as having a variety of all

f_i's and g_i's.

Now we want to prove the second one- So let us say that we have an element $(b_1, ..., b_n)$ from the variety defined by $h_i f_j)$. I want to prove that it belongs to the $V \square \cup T$. So let us assume that variety defined by $h_i f_j)$ is not contained in the V then it must have some $h_{i_0}(b_1, ..., b_n)$ which is not zero. But since we have that $h_{i_0} f_j$ is zero in $V(h_i f_j)$ for all j at the point $(b_1, ..., b_n)$. That implies that f_j's are zero at $(b_1, ..., b_n)$. So $V(h_i f_j)$ should be contained in T. The same argument can be given by using T instead of V. That means variety defined by $h_i f_j)$ contained in $V \cup T$. Now let us assume that we have an element $(b_1, ..., b_n)$ of V. Since all h_i's are zero at $(b_1, ..., b_n)$, so $h_i f_j)$ will also be zero at this element. So V is contained in $V(h_i f_j)$. The same argument can be given for variety T. That proves the theorem. $\square$

Proposition 4 *If we have an affine variety named V which belongs to k^n then $I(V)$ defined as-*

$$I(V) = \{h \in k[y_1, ..., y_n] : h(b_1, ..., b_n) = 0 \quad for \quad all(b_1, ..., b_n) \in V\}.$$

is called an ideal in $k[y_1, ..., y_n]$.

Proof: Since we all know that zero polynomial is zero everywhere. It is also zero in V. which means that it belongs to $I(V)$.

Now let us assume that we have two elements of $I(V)$ say h and f. We need to prove that basis properties of being in a ideal will be satisfied. So imagine one polynomial g from $k[y_1, ..., y_n]$ and take one arbitary element $(b_1, ..., b_n)$ from V. The sum $h(b_1, ..., b_n)$ + $f(b_1, ..., b_n)$ is zero. which means that $h + f$ also belongs to $I(V)$. Now the multiplication $g(b_1, ..., b_n).f(b_1, ..., b_n)$ is equal to 0 as $f(b_1, ..., b_n)$ is zero, that means gf also belongs to $I(V)$. So $I(V)$ is proved to be an ideal. $\square$

Proposition 5 *Assume that we have two affine varieties V and T in k^n. So,*

1. $T \supset V \iff I(T) \subset I(V)$.
2. $V = T \iff I(V) = I(T)$.

Proof: Let us assume that $T \supset V$ so every polynomials which vanishes in T, has to vanish in V also. That simply means that $I(T) \subset I(V)$.
Now let us suppose that $I(T) \subset I(V)$. Let us say that polynomials $h_1, ..., h_m$ which belongs to $k[y_1, ..., y_n]$, define the variety T. Which means that all these h_i's will be in $I(T)$. Since $I(T)$ is contained in $I(V)$, all h_i's will be in $I(V)$. This implies that $h_1, ..., h_m$ will vanish in V. As we know that all the common solution of these $h_1, ..., h_m$ are in T so $T \supset V$.
We can prove $T \subset V \iff I(T) \supset I(V)$ in the same manner. And by combining these two arguments we can say that $V = T \iff I(V) = I(T)$. The theorem is proved now. □

3.2 The Elimination and Extension Theorem

We have some fine way in which variables can be eliminated from the polynomial equations system. The idea is given by the Elimination Theorem and the Extension Theorem.

Definition 11 *If we have an ideal I in $k[y_1, ..., y_n]$ generated by $h_1, ..., h_t$ $k[y_1, ..., y_n]$. Then we can define a new ideal in $k[y_{m+1}, ..., y_n]$*

$$I_m = I \cap k[y_{m+1}, ..., y_n]$$

This ideal is called ***the m-th elimination ideal*** *I_l.*

If we find some polynomials in the I_m, which are not zero, then we can see that they are in the variables $y_{m+1}, ..., y_n$, so basically we eliminated $y_1, .., y_m$.

We need a way to find polynomials in I_m, that's what the Elimination theorem is all about.

Theorem 6 ***(The Elimination Theorem:-)*** *Suppose we have I as an ideal in $k[y_1, ..., y_n]$. We decide a lex order which is $y_1 > y_2 > ... > y_n$.Assume that I has a Groebner basis say G. Then we define Groebner basis*

$$G_m = G \cap k[y_{m+1}, ..., y_n]$$

for the $m - th$ elimination ideal I_m, where $0 \leqslant m \leqslant n$

Proof: $0 \leqslant m \leqslant n$, choose some m. I want to show that G_m is Groebner basis for I_m. There are two things that I want to prove. First is that I_m contains G_m. The second thing is that the ideal generated by $lt(I_m)$'s and ideal $\langle lt(G_m)\rangle$ are equal. The first thing we can see from way we defined G_m.
Now I want to prove the second thing. So we see that $\langle lt(G_m)\rangle$ is contained in $\langle I_m\rangle$. So we should prove that $\langle I_m\rangle$ is also contained in $\langle lt(G_m)\rangle$. So if I take h from I and prove that some $lt(g_i)$ divide $lt(h)$ then automatically h will belong to $\langle lt(G_m)\rangle$.
So since h is in I_m, it is also in I.For some g_i in G, $lt(g_i)$ will divide $lt(h)$. But we know that $lt(h)$ is in the variables $y_m+1, ..., y_n$ so g_i will be in these variables only. According to the order that we defined on the variables, terms which doesn't includes $y_1, .., y_m$ are smaller than the ones which includes them. Since $lt(g_i)$ only has $y_m+1, ..., y_n$ variables hence g_i is in $k[y_m+1, ..., y_n]$. Which implies that g_i belongs to G_m. That completes the proof. □

Let use take the last example of the last section. If we apply elimination theorem on that Groebner basis then we see that Groebner basis G_1 for I_1, where I_1 is the intersection of I with $\mathbb{C}[x, z]$, is $x^3 - z^2$ so we can put that equal to zero and find the values of variables. G_2 for I_2, where I_2 is the intersection of I with $\mathbb{C}[z]$ is $\{0\}$.

We are done with the elimination step, now I would like to discuss the extension step. Let us say we have an ideal I in $k[y_1, ..., y_n]$. If I say that I want to find about all the elements of the variety of this ideal, then there is a way to do it. First I will compute the $m-th$ elimination ideal and say that we have an element $(b_{m+1}, ..., b_n)$ of the variety $V(I_m)$. This element is called the partial solution. Then we need to expend it to the element of the $V(I)$ which is $(b_1, ..., b_n)$ we refer as the complete solution. We will add one coordinate at a time. First we must add such b_m to $(b_{m+1}, ..., b_n)$ that can make it an element of $V(I_{m-1})$. For finding this b_m let us say that I_m is generated by $g_1, .., g_t$ which belongs to $k[y_m, ..., y_n]$. and consider b_m as a variable say y_m then we need to solve the following system of polynomials to find b_m-

$$g_1(y_m, b_{m+1}, ..., y_n) = ... = g_t(y_m, b_{m+1}, ..., b_n) = 0.$$

But sometimes we don't have a solution for this system. That means those particular partial solutions can't be extended.

I am presenting such an example where one partial solution can't be extended.

Example 6 *Let us have an ideal I in $k[y, x, z]$ generated by*

$$yx = 1, yz = 1 \tag{3.1}$$

First we find its Groebner basis and conclude that elimination ideal I_1 is generated by $x - z$. By putting this equal to zero I get (b, b) as a solution where b varies over field k. We can see that $y = \frac{1}{x}$ so $y = \frac{1}{b}$ will be added to the partial solution in order to get complete solution. So $(\frac{1}{b}, b, b)$ is the complete solution but as we can see that the partial solution $(0, 0)$ can't be extended to this complete solution.

Theorem 7 ***(The Extension Theorem:-)*** *Suppose that we have an ideal I in $\mathbb{C}[y_1, ..., y_n]$ which has a basis $h_1, ..., h_t$. Assume that first elimination ideal is I_1. h_i can be written as*

$$h_i = f_i(y_2, ..., y_n)y_1^{N_i} \quad + \quad \textit{terms in which} \quad y_1 \quad \textit{has degree} \quad < \quad N_i,$$

for every i between 1 and t. Here N_i is greater than zero. Here these f_i's are not zero and belong to the $\mathbb{C}[y_2, ..., y_n]$. Assume that $(b_2, ..., b_n)$ exists in $V(I_1)$ as a partial solution . Then there $\exists\, b_1$ in the field $\mathbb{C}$ which will extend to the $(b_1, b_2, ..., b_n)$ such that it belongs to $V(I)$ only if the partial solution is not an element of variety defined by $(f_1, ..., f_t)$.

We will use the statement of the Extension theorem but we don't need the proof here. (see [DO07])

This theorem can't be true on real numbers. Because sometimes when we solve polynomial system where $lc(y)$ is non-zero, we see that variable have values from complex numbers. So the partial solution which contains real number can extend, but rest can't.

When we say that partial solution $(b_2, ..., b_n)$ is not an element of variety defined by $(f_1, ..., f_t)$. Here these f_i's are basically the $lc(h_i)$'s. So basically we are saying that at these $(b_2, ..., b_n)$ the $lc(h_i)$'s should not be zero simultaneously. In the previous example at $(0, 0)$ the $lc(y)$ which are x and z be zero. So by extension theorem $(0, 0)$ doesn't extend.

We have defined our extension theorem only for the first elimination ideal. But we can generalize it to as many elimination ideals as we want. We just extend our partial solution belongs to some elimination ideal, one coordinate at a time to reach the partial

solution of the next elimination ideal. Each time at this step we check that at this partial solution leading coefficient should not be zero. If it's not zero then we extend it. And go for adding the next coordinate in this partial solution till we reach our complete solution.

Corollary 4 *Suppose that we have an ideal I in $\mathbb{C}[y_1, ..., y_n]$ which has a basis $h_1, ..., h_t$. Assume that first elimination ideal is I_1. h_i can be written as*

$$h_i = ay_1^N \quad + \quad \textit{terms in which} \quad y_1 \quad \textit{has degree} \quad < \quad N,$$

for some i between 1 and t. Here N is greater than zero. Here a's is not equal to zero and it's belong to $\mathbb{C}$ Assume that $(b_2, ..., b_n)$ exists in $V(I_1)$ as a partial solution . Then there $\exists$ b_1 in the field $\mathbb{C}$ which will extend to the $(b_1, b_2, ..., b_n)$ such that it belongs to $V(I)$.

Proof: We just have to recall the extension theorem and see that f_i from the theorem are a here which is not zero so this means that variety defined by $(f_1, ..., f_t)$ is empty. This implies that no partial solution belongs to the variety defined by $(f_1, ..., f_t)$. So there $\exists$ b_1 in the field $\mathbb{C}$ which will extend to the $(b_1, b_2, ..., b_n)$ such that it belongs to $V(I)$. □

3.3 The Ideal–Variety Correspondence and radical ideal

Whenever we have a variety in k^n we can define it's ideal. This is we have seen before. And when we have an ideal we can define its variety. So there is always a map in ideal and variety.

We can't say that this map is 1-1. Because same variety can exist for two ideals. Let us assume that we have ideals $\langle y \rangle$ and $\langle y^2 \rangle$ in $k[y]$. We can see that both have empty variety. But we solve this problem in $k[y]$ when k is an algebraically closed field. Since in $k[y]$, every ideal will be generated by a single polynomial. So the variety of ideal just have the roots of that polynomial. And we know that there $\exists$ root of a polynomial in $k[y]$ because it is algebraically closed. So if we want our variety empty we must have the generator of the ideal a constant except zero. Assume that $I = \langle h \rangle$, since h is constant which is not zero so its inverse also belong to the field. Which simply implies that 1 belongs to the ideal. Which means ideal I is the whole $k[y]$. So the only ideal which

has empty variety is the whole $k[y]$ itself. We can generalize this onto the $[y_1, .., y_n]$.

Theorem 8 ***(The Weak Nullstellensatz:-)*** *Suppose the field k is algebraically closed field. We have an ideal I in the polynomial ring $k[y_1, ..., y_n]$, which has empty variety. Then we can say that this ideal I is the whole $k[y_1, ..., y_n]$.*

Proof: To prove this theorem we need to prove that 1 is in the ideal I. We will induction here. For $n = 1$ we proved it above. Suppose that the theorem is true for $n - 1$ variables.

Let us suppose that we have ideal I in $k[y_1, ..., y_n]$ which is generated by $h_1, .., h_m$. Let us assume that h_1 is polynomial which has degree N more than 1. We would like to change the coordinates to get the special form of h_1. Consider-

$$y_1 = \overline{y_1}$$

$$y_2 = \overline{y_2} + b_2\overline{y_1}$$

..

..

$$y_n = \overline{y_n} + b_n\overline{y_1}$$

b_i are the constant that are not determined yet. So after substitution h_1 has the form

$$h_1(y_1, ..., y_n) = h(\overline{y_1}, \overline{y_2} + b_2\overline{y_1}, ..., \overline{y_n} + b_n\overline{y_1}) == c(b_2, ..., b_n)\overline{y_1}^{N}.$$

$$+terms \quad in \quad which \quad \overline{y_1} \quad has \quad degree \quad < \quad N$$

. Since we know that k is infinite as it is algebraically closed field. So we have select a combination of $b_2, ..., b_n$ so that $c(b_2, ..., b_n)$ becomes the polynomial which is not zero.By this coordinate change each h from $k[y_1, ..., y_n]$ changed into $\overline{h}$ in $k[\overline{y_1}, \overline{y_2}, ..., \overline{y_n}]$. If we make these $\overline{h}$ generators for some set $\overline{I}$, where h belongs to I, then $\overline{I}$ will definitely be ideal in $k[\overline{y_1}, \overline{y_2}, ..., \overline{y_n}]$. As we know that if these new polynomials are solvable then so are the old ones so $V(\overline{I})$ is also empty. Basically now I want to show that $(\overline{I})$ has 1, because then I will also have 1.

So let us say that $\overline{I_1} = \overline{I} \cap k[\overline{y_2}, ..., \overline{y_n}]$. We have $V(\overline{I_1}) = \pi_1(V(\overline{I}))$. (see chapter 3[DO07]). We have seen before that $V(\overline{I})$ is empty so $V(\overline{I_1})$ will also be empty.

Which means that $\overline{I}$ is the whole $k[\overline{y_2}, ..., \overline{y_n}]$. So 1 will be contained in $\overline{I_1}$, therefore it will be contained in $\overline{I}$. Which means that 1 is in I. Hence the theorem is proved. □

We have a question about the variety that is generally called **consistency problem**. Let us assume that I is ideal generated by $h_1, ..., h_m$. $h_1, ..., h_m$ are polynomials in $k[y_1, ..., y_n]$ We want to know whether $V(I)$ is empty or not. We assume that k is an algebraically closed field. From the above theorem, we can see that variety of ideal I will be empty if the ideal contains 1.

We first want to look at the reduced Groebner basis $g_1, .., gt$ for such an ideal which is generated by 1. Since 1 will belong to the $\langle lt(I)\rangle$ hence some $lt(g_i)$ will divide 1. Which makes that g_i a constant. Now we know that rest of the $lt(g_i)$'s are just the multiple of this constant. So we will remove every other g_i. Now since we know that for that particular g_i leading term was constant. So that g_i will be constant. And we can make it 1 by multiplying it by some constant. So we proved that for an ideal which is generated by 1, reduced Groebner basis are just 1. So for proving that $V(I)$ is empty, we just need to compute the reduced Groebner basis. If it's 1 then yes, $V(I)$ is empty. If it's not 1, then $V(I)$ is not empty.

Theorem 9 ***(Hilbert's Nullstellensatz)*** *Suppose that some polynomials $h, h_1, ..., h_m$ belongs to $k[y_1, ..., y_n]$, where k is algebraically closed field. We assume that h belongs to the ideal of $V(h_1, ..., h_m)$. Then we always have an integer s such that*

$$h^s \in \langle h_1, ..., h_m\rangle$$

where s is greater than or equal to 1. The converse is also true.

Proof: Basically we need to prove that there ∃ integer s which is greater than or equal to 1, and some polynomials $p_1, .., p_m$ such that h can be written as-

$$h^s = \sum_{i=1}^{m} p_i h_i$$

Assume the ideal given below-

$$\overline{I} = \langle h_1, ..., h_m, 1 - xh\rangle$$

belong to $k[y_1, ..., y_n, x]$. First I want to prove that variety of $\overline{I}$ is empty. This will lead us to the proof of the theorem.

For proving that variety of $\overline{I}$ is empty assume that $(b_1, ..., b_n, b_{n+1})$ belongs to k^{n+1}. There are only two possibilities that

1. $h_1, ..., h_m$ all vanishes at $(b_1, ..., b_n)$.

2. not all of $h_1, ..., h_m$ vanishes at $(b_1, ..., b_n)$.

Let us take the first case first. Since h belongs to the ideal of $V(h_1, ..., h_m)$ so h will also vanish at $(b_1, ..., b_n)$. Now we can write $1 - xf$ as $1 - b_{n+1}h(b_1, ..., b_n)$ which will be 1 not zero.So by this we can see that $(b_1, ..., b_n, a_{b+1})$ is not an element of $V(\overline{I}\ )$. Now take the second case. We will have at least one h_i such that $h_i(b_1, ..., b_n)$ is not zero. Assume that h_i is a function of $n+1$ variables. But h_i is independent of $n+1$. So we see that $h_i(b_1, ..., b_n, b_{n+1})$ is not zero. Which means that $(b_1, ..., b_n, b_{n+1})$ is not contained in the variety of $\overline{I}$. As we considered $(b_1, ..., b_n, b_{n+1})$ an arbitrary element of k^{n+1} ,so we proved that $V(\overline{I}\ )$ is empty.
So now from the above theorem we can see that 1 will be contained in $\overline{I}$. Which means we can write 1 as

$$1 = \sum_{i=1}^{m} f_i(y_1, ..., y_n, x)h_i + g(y_1, ..., y_n, x)(1 - xh) \tag{3.2}$$

Here f_i, g are polynomials which belongs to $k[y_1, ..., y_n, x]$. Consider $x = 1/h(y_1, ..., y_n)$ and put this in the above equation then

$$1 = \sum_{i=1}^{m} f_i(y_1, ..., y_n, 1/h)h_i \tag{3.3}$$

If we multiply the above equation with h^s then we get

$$h^s = \sum_{i=1}^{m} p_i h_i \tag{3.4}$$

where all the denominators gets canceled out because we selected s that way. The theorem is proved. □

Lemma 6 *Suppose that h^s belongs to the $I(V)$. Then h will belong to $I(V)$.*

Proof: Assume that b is an element of V. So if h^s is in $I(V)$, then we can see that $(h(b))^s$ is zero. Which simply implies that $h(b)$ is zero. As we considered b as an arbitrary element to V, it's proved that h is in $I(V)$. □

Definition 12 *I is called to be a radical ideal if whenever h^s belongs to I, h also belong to I, where s is some non negative integer.*

Definition 13 *Suppose that I is an ideal in $k[y_1, ..., y_n]$. Then the set*

$$\{h : h^s \in I \quad for \quad some \quad non \quad negative \quad integer\}.$$

is called the radical of I. We denote is as $\sqrt{I}$.

By the above lemma and definition, we can see that $I(V)$ is, in fact, a radical ideal.

Theorem 10 ***(The Strong Nullstellensatz:-)*** *Suppose that we have an ideal I which belongs to $k[y_1, ..., y_n]$, then*

$$I(V(I)) = \sqrt{I}$$

Proof: Let us consider an arbitrary element h of $I(V(I))$. Which means that h is zero in $V(I)$. And by the above theorem, we know that h^s will be in I for some nonnegative integer s. Which implies that h is contained in the $\sqrt{I}$. As we considered h an arbitrary element, $I(V(I))$ will be contained in $\sqrt{I}$.
Now let us prove the other inclusion.Suppose we have an element h in the radical of ideal I. Which means that h^s will be in I for some nonnegative integer. Which implies that h^s will be zero in the variety of I. As we have seen before which simply mean that h will also be zero in $V(I)$. So h is an element of $I(V(I))$.
□

Theorem 11 ***(The Ideal–Variety Correspondence:-)*** *Assume that k is an arbitrary field.*

1. *The map I*

$$affine \quad varieties \rightarrow ideals$$

and the map identified as V

$$ideals \rightarrow affine \quad varieties$$

are inclusion-reversing which means that if I_1 is contained in I_2 are ideals, then $V(I_2)$ will be contained in $V(I_1)$. In the same way if V_1 is contained in V_2 then $I(V_2)$ will be contained in $I(V_1)$. And also for any variety V, $V(I(V)) = V$ so that I is always one-to-one.

2. *Now suppose that k is algebraically closed and we only consider radical ideals, then the map identified as I*

$$affine \quad varieties \rightarrow radical \quad ideals$$

and the map V

$$radical \quad ideals \rightarrow affine \quad varieties$$

are inclusion-reversing bijections which are inverses of each other.

Proof:

1. We have shown this before that variety and ideals are inclusion reversing.Now we just want to show that $V(I(V)) = V$. Let us say that $V = V(h_1, ..., h_m)$ is contained in k^n. So whenever we take an element h of $I(V)$ we know that it is zero in V, which implies that variety is a subset of $V(I(V))$.
   Now since we know that $h_1, ..., h_m$ are elements of ideal fo variety. Hence the ideal generated by these $h_1, ..., h_m$ will also be in $I(V)$. As we know that variety is inclusion-reversing, so the $V(I(V))$ will be contained in $V(\langle h_1, ..., h_m\rangle)$ which is equal to the V. So we get that $V(I(V)) = V$. As map I has a left inverse it is one-one.

2. We know that $I(V)$ is radical ideal, it means that I works like a map which correspond varieties to radical ideals. We have seen above that $V(I(V)) = V$ for every variety from the first part. We just need to prove it for radical ideals $I(V(I)) = I$. In the above theorem we saw that $I(V(I)) = \sqrt{I}$. As we are talking about radical ideals I would be equal to the radical of I. Which implies that $I(V(I)) = I$. So it is proved that variety and ideal maps are inverses of each other.That completes the proof.

□

Proposition 6 ***(Radical Membership:-)*** *Suppose that we have k as an arbitrary field. Assume that we have an ideal I of $k[y_1, ..., y_n]$, which is generated by $h_1, ..., h_m$. Then h belongs to the radical of the I iff 1 is contained in the ideal from $k[y_1, ..., y_n, x]$, $\overline{I} = \langle h_1, ..., h_m, 1 - xh\rangle$.*

Proof: As we have in the proof of theorem (9), if 1 is contained in $\overline{I}$ then h^s will be contained in I for some non negative s. And that without any doubt implies that h will be in the radical of I.
Now suppose that we have an element h from the radical of I. Which implies that h^s is in I for some non negative s and as we know that I is a subset of $\overline{I}$. So h^s will also be in $\overline{I}$. Since $1 - xh$ is also a element of $\overline{I}$ so 1 can be written as-

$$1 = x^s h^s + (1 - x^s h^s)$$

which will be equivalent of having-

$$1 = x^s.h^s + (1 - xh).(1 + xh + ... + x^{s-1}h^{s-1})$$

which is contained in $\overline{I}$. That completes the proof. □

This leads to the **radical membership algorithm**. If we have a question that whether h is in the radical ideal of I or not, where I is generated by $h_1, ..., h_m$, then we first need to consider the ideal $\overline{I}$ generated by $h_1, ..., h_m, 1 - xh$ and then we will fix some ordering on the variables and compute the reduced Groebner basis for $\overline{I}$. If the reduced Groebner basis is 1 then h is in the radical of ideal I. Otherwise, it won't be contained in radical of I.

Proposition 7 *Let us suppose that h is an element of $k[y_1, ..., y_n]$ and we have an ideal I generated by h. If we can factorize h as $h = bh_1^{c_1}...h_s^{c_s}$ which is a product of distinct irreducible polynomials, then the radical of I will be generated by $h_1h_2...h_s$.*

Proof: The very first thing I want to prove is that $h_1h_2...h_s$ belong to the radical of I. Let us consider integer M which is not less than any of c_i's. So we can write -

$$(h_1h_2...h_s)^M = h_1^{M-c_1}h_2^{M-c_2}...h_s^{M-c_s}h$$

Since this is multiple of h it will belong to I, which mean that $h_1h_2...h_s$ will be in the radical of I. So the ideal generated by $h_1h_2...h_s$ will also belong to the radical of I.

Now let us assume that f is an element of $\sqrt{I}$. Then f^N will be in I for some integer N. Since I is generated by h ,so we can write f^N as $g{\cdot}h$ where g is in $k[y_1, ..., y_n]$.

Now let us factor the f in product of irreducible polynomials which are all distinct. So $f = f_1^{a_1} f_2^{a_2} ... f_t^{a_t}$. So now we also have factorization of $f^N = f_1^{a_1 N} f_2^{a_2 N} ... f_t^{a_t M}$ which is a product of irreducible polynomials which are all distinct. So, we have-

$$f^N = f_1^{a_1 N} f_2^{a_2 N} ... f_t^{a_t M} = g.h_1^{c_1} ... h_s^{c_s}$$

So now we know that we have irreducible polynomials in the right hand side as well as left hand side. We know that it is supposed to be a unique factorization. So basically each h_i is some multiple of some f_k so f is basically a multiple of $h_1 h_2 ... h_s$. From here we can see that f is in the ideal which is generated by $h_1, ..., h_s$ Now the proof is complete. □

3.4 Decomposition of a Variety into Irreducible and Primary Decomposition of Ideals

Definition 14 *An affine variety V which is contained in k^n is called **irreducible** if when we write V as $V = V_1 \cup V_2$, then either $V_1 = V$ or $V_2 = V$, where V_1 and V_2 are affine varieties.*

Proposition 8 *Suppose that V which is contained in k^n is an affine variety. Then V is irreducible $\iff$ ideal of the variety is a prime ideal.*

Proof: Let us suppose that V is an irreducible variety. Suppose that gh belongs to the ideal of the variety $I(V)$. Let us say that V_1 is the intersection of V and $V(g)$, and V_2 is the intersection of V and $V(h)$. As we know that intersection of affine varieties gives us another affine variety. which implies that we have V_1 and V_2 as affine varieties. As we assumed that gh is in $I(V)$ it means that gh vanishes on V, so it gives us that V is the union of varieties V_1 and V_2. Since we assumed that V is an irreducible variety, so it can be equal to only V_1 or $V = V_2$. Suppose that it is equal to V_2 then V will be the intersection of V and $V(h)$. That makes it clear that h is zero on V, it implies that h belongs to $I(V)$. Which proves that $I(V)$ is a prime ideal.

Now suppose that $I(V)$ is a prime ideal. Let us say that V is the union of varieties V_1 and V_2. Let us assume that V is not equal to the V_1. Now at first, I want to prove that

$I(V)$ is same as the $I(V_2)$. So for this as we know that V_2 is contained in V since V is the union of V_1 and V_2. We also know that map I is inclusion reversing so we can see that $I(V)$ will be contained in $I(V_2)$. Now I want to prove the other containment. So we can see that since V_1 is contained in V, but it's not equal to V, so it means that $I(V)$ is contained in $I(V_1)$ but it's not equal to that. Let us pick an element h such that it belong to the $I(V_1)$ but doesn't belong to $I(V)$. Let us take a polynomial f from $I(V_2)$. Then we can see that hf will be zero in V as V is the union of V_1 and V_2. Which means that hf will belong to $I(V)$. Since ideal of variety is prime ideal, only one of h or f will be in $I(V)$. We have picked f in such a way that it doesn't belong to $I(V)$ so we are left with h that h is in $I(V)$. It means that $I(V)$ is same as $I(V_2)$. As we know map I is 1-1 so it is proved that V is equal to the V_2. So V is irreducible variety. □

Corollary 5 *Let us suppose that k is an algebraically closed field then we can see that there is a 1-1 correspondence between irreducible varieties, which belong to k^n and prime ideal, which are contained in $k[y_1, ..., y_n]$, induced by maps I and V.*

Proposition 9 ***(The Descending Chain Condition:-)*** *If we have a chain*

$$V_1 \supset V_2 \supset V_3 \supset ....$$

Which is descending then there must $\exists$ some +ve integer M such that chain gets stabilized by having the property that V_M will be equal to $V_M + 1$ and so on.

Proof: As we know that the map I is inclusion reversing so we will have the following chain-

$$I(V_1) \subset I(V_2) \subset I(V_3) \subset .....$$

So from the ACC which is for ideals, we know that there $\exists$ M so that chain of ideals get stabilized by having the property that $I(V_M)$ will be equal to $I(V_M + 1)$ and so on. As we know that we have $V(I(V)) = V$ so by mapping V, V_M will be equal to V_{M+1} and so on. So the chain of varieties will be stabilized. □

Theorem 12 *Let us assume that we have a variety V which is in k^n. Then we can write V as a finite union of irreducible varieties, say*

$$V = V_1 \cup .... \cup V_s$$

Proof: We are going to prove this with contradiction so suppose that we can't write V as a finite union of irreducibles. So basically V is not irreducible so we can write V as the union of V_1 and V_2 which the property that V is not equal to V_1, as well as V, is not equal to V_2. Now, for keeping V irreducible it is important that one of V_1 and V_2 won't be a finite union of irreducibles. Let us assume that V_1 is not a finite union of irreducibles. By continuously repeating the process, we can write V_1 as a union of V_3 and V_4 with the property that V_1 is not equal to V_3 as well as it is also not equal to V_4 and we must have that V_3 is not a finite union of irreducibles. So by the process, we will have an infinite sequence

$$V \supset V_1 \supset V_3 \supset ....$$

where none of them are equal, which is a contradiction to DCC of varieties.That completes the proof. □

Definition 15 *Let us assume that we have a variety V which is in k^n. Then minimal decomposition of variety V is the decomposition of V into irreducibles*

$$V = V_1 \cup .... \cup V_s$$

where V_i's are not contained in V_j's when i and j are not same .

Theorem 13 *Let us assume that we have a variety V which is in k^n. Then V has a minimal decomposition*

$$V = V_1 \cup .... \cup V_m$$

And this minimal decomposition is unique up to the order in which $V_1, ..., V_m$ are written.

Proof: First we see that we can write V as finite union of irreducibles $V = V_1 \cup .... \cup V_s$. And whenever we see that V_i is contained in V_j for some i which is not same as j then we will remove V_i from the union. So continuing this way, in the end, we will achieve the minimal decomposition of the V.

Now we want to show the uniqueness of the minimal decomposition. So assume that we have some another minimal decomposition for V say, $V = V_1' \cup .... \cup V_t'$. Now we see that we can write each V_i belonging to the first decomposition as following

$$V_i = V_i \cap V$$

Now we will put the first minimal decomposition at the place of V

$$V_i = V_i \cap (V_1' \cup .... \cup V_t') = (V_i \cap V_1') \cup ... \cup (V_i \cap V_t').$$

AS V_i belong to the minimal decomposition it is irreducible so we will have V_i as the intersection of V_i and V_k' for some k. Which means that V_i is contained in V_k'. Now we can apply the same argument to V_k'. So we will write V_k' as an intersection of V_k' and V. Then we will put the second minimal decomposition of V in this intersection in place of V. By which in the end we will get that V_k' is contained in some V_j. So basically we have that V_i is contained in V_k' which is contained in V_j but by the minimality of decomposition V_i can't be contained in V_j as this will contradict the minimality of decomposition. So V_i will be equal to V_k.Which implies that V_i will be equal to V_k'. So we can see that every V_i will be appearing in the $V = V_1' \cup .... \cup V_t'$ which simply follows that s is smaller than t. And since every V_k' will be appearing in $V = V_1, .., V_s$ so t will be smaller than s. So basically s and t are equal. V_i and V_i' are just the permutations of each other. So it's unique. That completes the proof. □

Theorem 14 *Let us assume that k is a algebraically closed field, then we can write every radical ideal which belongs to $k[y_1, .., y_n]$ as -*

$$I = P_1 \cap .... \cap P_s$$

here s is a finite number and P's are prime ideals, this intersection is unique- such that P_i are not contained in P_j when i and j are not equal.

Definition 16 *We call an ideal I primary if when some gh belong to I then either g belong to I or h belongs to the radical of I, where I is an ideal in $k[y_1, .., y_n]$.*

Definition 17 *Let us assume that we have two ideals I and J in $k[y_1, ..., y_n]$, the ideal quotient $I : J$ is defined by-*

$$\{h \in k[y_1, ..., y_n] : fh \in I \quad for \quad all \quad f \in J\}$$

.

Theorem 15 *Let us say that we have any ideal I in the $k[y_1, ..., y_n]$. Then we can write this I in the form of an intersection of primary ideals.This intersection will be finite.*

Proof: First I want to prove that we can write every ideal as a finite intersection of irreducible ideals. We are going to prove this with contradiction so suppose that we can't write I as a finite intersection of irreducibles. So basically I is not irreducible so we can write I as the intersection of I_1 and I_2 with the property that I is not equal to I_1, as well as I, is not equal to I_2. Now, for keeping I irreducible it is important that one of I_1 and I_2 won't be the finite intersection of irreducibles. Let us assume that I_1 is not a finite intersection of irreducibles. By continuously repeating the process, we can write I_1 as a intersection of I_3 and I_4 with the property that I_1 is not equal to I_3 as well as it is also not equal to I_4 and we must have that I_3 is not a finite intersection of irreducibles. So by the process, we will have an infinite sequence

$$I \subset I_1 \subset I_3 \subset ....$$

where none of them are equal, which is a contradiction to ACC of ideals.
Now I want to prove that irreducible ideals are always the primary ideals. So if we take an element from the irreducible ideal then I want to see that definition of primary ideal work on that element. Now suppose that we consider I as an irreducible ideal. and pick an element gh from I. So for I being the primary ideal, we need to show that either g is in I or h^M where M is positive integer will belong to I. So Let us assume that g does not belong to I. So we need to show that h^m where m is positive integer will belong to I.
First, let us see some other inclusions. So we the definition of quotient ideals we can see that elements of $I : h^{m+1}$ are multiples of elements of $I : h^m$ so it means that $I : h^m$ is contained in $I : h^{m+1}$ for all nonnegative integers m. So by this, we have the following chain-

$$I : h \subset I : h^2 \subset ....$$

it's a chain of ideal because there is quotient ideal and it's ascending. So we can apply ACC here. So we can see that this chain gets stabilized with the property that for some nonnegative M, $I : h^M = I : h^{M+1}$ and so on. Now we can observe that when we take an intersection of $(I + \langle h^M \rangle)$ with $(I + \langle g \rangle)$ we will anyhow get I. And as we assumed I is irreducible and only one of the terms in the intersection can be equal to it. Since we know that g is not in the ideal because we assumed it the starting so the first term $(I + \langle h^M \rangle)$ is equal to I. So this shows that h^M is in the ideal I. That's what we wanted to prove. □

Definition 18 *If we can write I as- $I = \bigcap_{i=1}^{s} J_i$ where J_i's are primary ideals and I is an ideal in $k[y_1, .., y_n]$ then this intersection is called the* ***primary decomposition****. When no $\sqrt{J_i}$'s are the same and none of the J_i contains the intersection of all J_j's when i is not equal to j, then we will refer it as minimal decomposition .*

Whenever we have two primary ideals such that their radical are equal then we can see that their intersection is also primary.

Theorem 16 *(*(Lasker–Noether)*) There exists a minimal primary decomposition for every ideal of $k[y_1, .., y_n]$.*

Proof: As we have see in the earlier given theorem that we can write ideal I as $I = \bigcap_{i=1}^{s} J_s$. Now let us take two primary ideals J_i and J_k such that they have the same radical then as mentioned before intersection of J_i and J_k, say J_j will also be the primary ideal so we can remove the J_i and J_k from the primary decomposition and put J_j there.So by following this process in the end we will get a form of I such that radical of all J_i be different.

Now I want to show that none of the J_i will contain the intersection of all J_k's for i not equal to k. We will prove this by contradiction. So assume that we have J_i such that intersection of all J_k's for i is not equal to k, is contained in J_i. Then we can drop J_i from the intersection $I = \bigcap_{i=1}^{s} J_s$. And put the intersection of all J_k's for i is not equal to k at the place of J_i. By following this process we will get the decomposition in which none of the J_i contains the intersection of all J_j's when i is not equal to j. That completes the proof. □

Chapter 4

Primary Decomposition of Polynomial ideals

4.1 Operation on Ideals

Throughout this chapter, we will consider R as a Noetherian commutative ring with identity such that it is possible to solve linear equations in it.

When we say that it is possible to solve linear equations in R, we mean that two problems called IMP and syzygies are solvable in it. We already mentioned IMP is the first chapter. let us explain what do we mean when we say that syzygies is solvable in R. It means that suppose some elements of R are given, say $b_1, ..., b_s$ then it is possible to find a basis, which is finite, for the R- module- $\{(c_1, ..., c_s) \in R^s | \quad such \quad that \sum c_i b_i = 0\}$.

Definition 19 *Let us assume that we have a subset M of R, which is multiplicatively closed, then we can define the ring of fractions of R w.r.t M as following-*

$$M^{-1}R = \{s/t| \quad where \quad s \in R \quad and \quad t \in M\}$$

.

Definition 20 *Assume that we have an element h of R such that $M = \{h^m\}$, then localisation of R at h denoted by R_h, can be defined as $M^{-1}R$.*

Definition 21 *Assume that we have a prime ideal p of R, and a set $M = R - p$. Then we can define Rp, which is the localisation of R at p as $M^{-1}R$.*

Definition 22 *Assume that we have an ideal I of R, where R is a Noetherian ring. Then the following set-*

$$Ass(I) = \{Q \subset R | Q \quad are \quad prime \quad ideals, Q = I : \langle a \rangle for some a in R\}.$$

is called the associated primes of I.

Definition 23 *Let us assume that we have an element h and a subset G of the $R[y_1, .., y_n]$. Then h is said to be reducible modulo G only if $h \neq 0$, and leading term of h contained in the ideal generated by leading terms of elements of G.*
If h doesn't not satisfy these conditions then it is called reduced modulo G.

Proposition 10 ***(Reduction algorithm)*** *Let us assume that we have given an element h and a subset G of the $R[y_1, .., y_n]$. where $G = \{g_1.....gs\}$. Then we can always construct such an element h' of $R[y_1, .., y_n]$ which itself is reduced modulo G so that $h = h' mod(g_l, ...g_s)R[y_1, ..., y_n]$.*

Proof: Since we know that IMP is solvable in R. So by using it we can easily check if h is in the ideal generated by elements of G, if it is true then we can see that leading term of h is divisible by leading term of some element of the generating set, which implies that leading term of h is contained in the ideal generated by leading terms of G. So basically we can check if h is reducible modulo G. If f is not reducible then we can see that $h = h'$ and we are done. And if f is reducible modulo G then we can find a_i such that $lt(h) = \sum a_i lt(g_i)$. Now suppose $h_1 = h - \sum a_i g_i$. So the $lt(\sum a_i g_i)$ will cancel the $lt(h)$ by construction, so we will get that degree of h_1 is less than degree of h. Since induction is applicable on the well ordering $<$ hence by using induction here we are able to find a reduced h' with the property that $h' \equiv h_1 \text{ mod } (g_1, ..., g_s)$. But since $h \equiv h_1 \text{ mod } (g_1, ..., g_s)$ so $h \equiv h' \text{ mod } (g_1, ..., g_s)$. That completes the proof. □

The old definition that we read in the second chapter was that the basis has the property that ideal generated by leading terms of elements of the basis is equal to the ideal generated by the leading terms of elements of the ideal.
Now we will redefine Groebner Bases.

Definition 24 *Let us assume that we have an ideal I of the $R[y_1, .., y_n]$ and a subset G of this ideal then G is called to be a Groebner basis if any element of I which is not zero, is reducible modulo G.*

If we observe the following proposition, we will notice that it is basically a replacement of division algorithm for checking if an element belongs to the ideal or not.

Proposition 11 *Assume that we have G as Groebner basis for the ideal I in $R[y_1, .., y_n]$. Then an element h of $R[y_1, .., y_n]$ will belong to the ideal I if and only if when we apply reduction algorithm to h we get h' to be zero.*

Proof: Suppose $h \neq 0$,where $h \in R[y_1, .., y_n]$. Consider h' is same as in the reduction algorithm. As we it is given that G is Groebner basis of I which means that it is contained in I so we can write $h = h' mod I$ instead of $h = h' mod(g_l, ...g_s)R[y_1, ..., y_n]$.
So now suppose that h belongs to the ideal I then we know from the above that h' will also belong to the ideal I. so leading term of h' which belongs to the ideal generated by leading term of elements of ideal I, also belong to the ideal generated by leading terms of elements of G. Which happens when h' is reducible modulo G, but we assumed h' such a way that it is reduced modulo G. That's a contradiction so h' has to be zero.
Conversely, as we mentioned earlier $h = h' mod I$ so if say that h' is suppose to be zero then from this equality it is clear that h belong to the ideal I. That completes the proof. □

Corollary 6 *Assume that we have two ideals in $R[y_1, .., y_n]$ such that one ideal is contained in the other. If the ideal generated by leading term of one ideal is same as the ideal generated by the leading term of the second ideal then these two ideals are bound to be equal.*

Proof: The given property that the ideal generated by leading term of one ideal is same as the ideal generated by the leading term of second ideal forces both ideals to be each others Groebner basis. Which simply means that these ideals generate each other. But we know that ideal possess a special property that the only ideal it generates is itself. So from here, we conclude that both ideals are just the same. □

Proposition 12 *If a generating set is given for any ideal in $R[y_1, .., y_n]$. Then it is possible to compute Groebner basis of it.*

Proof: I have proved this for for the case of R being field. For general case see [Tri] .

□

Proposition 13 *Let us consider that we have an ideal I in the $R[x_1, ...x_m, y_1, ..., y_n]$. Suppose that we are provided with two monomial orders, one is $>_1$ for the monomials in y and the second one is $>_2$ which is for the monomials is x. Then we define a new order on the monomials in yx such that $y^a x^{a'} > y^b x^{b'}$ if $y^a >_1 y^b$ or if we have y^a is equal to the y^b according to the ordering $>_1$ then $x^{a'} >_2 x^{b'}$. Now suppose that we have an order $>$ and Groebner basis G for an ideal I in $R[x_1, ...x_m, y_1, ..., y_n]$. Then-*

1. *If we consider monomial ordering $>_1$ on $R([x_1, ...x_m])[y_1, ..., y_n]$, even then also I has the same Groebner basis G.*

2. *The ideal $I \cap R[x_1, ..., x_m]$ has Groebner basis $G \cap R[x_1, ..., x_m]$ w.r.t. the order $>_2$.*

Proof:

1. Basically we wish to prove that the ideal generated by leading terms of elements of G is equal to the ideal generated by leading terms of elements of I w.r.to monomial ordering $>_1$. So if we have an element h of $R[x_1, ...x_m, y_1, ..., y_n]$, then if we first choose leading term of h w.r.t. ordering $>_1$ and then apply ordering $>$ on it, we get the same leading term if we have applied directly $>$. Because in the $>$ anyhow we first work on y's. Let us denote the ideal generated by leading terms of any subset G as $LT(G)$.

   $$LT_>(LT_{>_1}(G)) = LT_>(G)$$

   From the assumption made in the statement of the theorem $LT_>(G) = LT_>(I)$, And by above $LT_>(I)$ is equal to $LT_>(LT_{>_1}(I))$. So

   $$LT_>(LT_{>_1}(G)) = LT_>(LT_{>_1}(I))$$

   Which basically implies that $LT_{>_1}(G) = LT_{>_1}(I)$ by corollary (6).

2. As we see from the monomial ordering $>$ that whenever we add any y_i to some term, it becomes greater than all other terms which are only in x_i's. Which simply implies that if we have an element such that its leading term only contains x_i's

means the leading terms belongs to $R[x_1, ...x_m]$, then since it's a leading term it must be the greatest term so no remaining terms can have any y_i's. That means that leading term of h is in $R[x_1, ...x_m]$ if and only if the element itself is in $R[x_1, ...x_m]$. So in the following equality contraction with $R[x_1, ...x_m]$ won't bother us.

$$LT_>(G \cap R[x_1, .., x_m]) = LT_>(G) \cap R[x_1, .., x_m]$$

Since from the assumption made in the statement of the theorem $LT_>(G) = LT_>(I)$, so the above equality becomes-

$$LT_>(I) \cap R[x_1, .., x_m] = LT_>(I \cap R[x_1, .., x_m])$$

. Which shows that $I \cap R[x_1, .., x_m]$ has $G \cap R[x_1, .., x_m]$ as a Groebner basis w.r.t. monomial ordering $>$. Since we are only talking about the ordering on $R[x_1, .., x_m]$ so $>$ and $>_2$ will work in the same way. So this completes the proof.

□

Corollary 7 *Assume that we have two ideals I and J in the $R[y_1, .., y_n]$ and we are given the Groebner basis for both of them, then we can compute the Groebner basis for followings-*

1. *$I \cap J$.*
2. *$I : J$, where J doesn't have zero divisors as the generating set.*
3. *The kernel of a given homomorphism $\phi : R[x_1, .., x_n] \mapsto R[y_1, .., y_n]/J$.*
4. *The ideal of polynomial relations among $h_l, ..., h_s$ which are the elements of $R[y_1, .., y_n]$.*
5. *$IR[y_1, .., y_n]_h \cap R[y_1, .., y_n]$ for any nonzero divisor h which is an element of $R[y_1, .., y_n]$.*

Proof:

1. $I \cap J$ will be given by $(tI, (t-1)J)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$, where t is the new indeterminate.
   We should prove that $I \cap J$ is equal to the $(tI, (t-1)J)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$

so first let us assume that an element h belongs to the intersection of I and J. Which means that h belongs to I as well as J. So since h is in I it means that th will be in tI. In the same way since h is in J, it implies that $(1-t)h$ will be in $(1-t)J$. Since h can be written as $h = th + (1-t)h$ which belongs to $tI + (1-t)J$. As as assumed that I and J are ideals in $R[y_1, .., y_n]$ so it means that h belongs to $(tI, (t-1)J)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$. So it is proved that intersection of I and J is contained in $(tI, (t-1)J)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$. Now it is time to prove the other containment. So suppose that h is an element of $(tI, (t-1)J)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$. Then h can be written as $h(y_1, .., y_n) = f(y_1, .., y_n, t) + g(y_1, .., y_n, t)$ such that $f(y_1, .., y_n, t)$ belongs to tI and $g(y_1, .., y_n, 1-t)$ belongs to $(1-t)J$. Let us assume that t is equal to 0 then since we know that every element of tI is a multiple of t so $f(y_1, .., y_n, t)$ will be zero when we put t zero. So in this case $h(y_1, .., y_n) = 0 + g(y_1, .., y_n, 0)$. Which implies that h belongs to J. When we put t 1 instead of 0 then since we know that every element of $(1-t)J$ is a multiple of $1-t$, so $g(y_1, .., y_n, 1)$ will be zero. So $h(y_1, .., y_n) = f(y_1, .., y_n, 1) + 0$ Which implies that h belongs to I. Now as we have see that h belongs to both I and J, it will be in their intersection. So $(tI, (t-1)J)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$ is contained in intersection of I and J. Which proves that $I \cap J$ is equal to the $(tI, (t-1)J)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$. So we will first compute the Groebner basis for $(tI, (t-1)J)R[y_1, .., y_n, t]$ and we will pick only those Groebner basis which doesn't contain t. So those will be the required Groebner basis.

2. Assume that the idea J has a generating set $(h_1, ..., h_s)$. Then from the properties of ideal quotient we can write $I : J$ as $\bigcap_i^s I : (h_i)$. So we first need to compute each $I : (h_i)$. Then we will take the intersection of all $I : (h_i)$ to get $I : J$ and compute the intersection using part (1). So for computing $I : (h_i)$ we first compute $I \cap (h_i)$ with the help of (1). Let us assume that when we compute the Greobner basis for $I \cap (h_i)$ we get $\{g_1, ..., g_t\}$, then the basis for $I : (h_i)$ will be $\{g_1/h_i, ..., g_t/h_i\}$. So we wish to prove that if the basis for $I \cap (h_i)$ is $\{g_1, ..., g_t\}$ then the basis for $I : (h_i)$ will be $\{g_1/h_i, ..., g_t/h_i\}$.

   So assume that b belongs to (h_i) so we can write b as ch_i, where c belongs to $R[y_1, .., y_n]$. So if we say that f belongs to the ideal generated by $g_1/h_i, ..., g_t/h_i$,

then we can see that bf which is equal to ch_if belongs to the ideal generated by $g_1, ..., g_t$. which is equal to $I \cap (h_i)$. It is conatined in I. So it implies that f belongs to $I : (h_i)$. Now for proving the other way round let us assume that f is an element of $I : (h_i)$. Which mean that fh_i belongs to I. As we know that fh_i also belongs to (h_i), so we can see that fh_i is in the intersection of I and (h_i). Since $I \cap (h_i)$ is generated by elements $g_1, ..., g_t$ so we can write fh_i as $\sum a_ig_i$. As we know that every g_i is an element of (h_i) so it implies that g_i/h_i is some polynomial. So f can be written as $f = \sum a_i(g_i/h_i)$. Which implies that f belongs to the ideal generated by elements $g_1/h_i, ..., g_t/h_i$. So it is proved that $I : (h_i)$ will be $\{g_1/h_i, ..., g_t/h_i\}$.

3. Let the homomorphism $\phi : R[x_1, .., x_n] \mapsto R[y_1, .., y_n]/J$ is given by $\phi(x_i) = f_i$ mod J. Then the kernal of the map ϕ is generated by $((x_i - f_i), J)R[y_1, ..., y_n, x_1, ..., x_n] \cap R[x_1, .., x_n]$. We will prove this by showing that $\phi(g_i) \in J$, where g_i is an arbitrary element from $((x_i - f_i), J)R[y_1, ..., y_n, x_1, ..., x_n] \cap R[x_1, .., x_n]$. Let us say that $g_i = \sum h_i(x_i - f_i) + j$ where $j \in J$.
So $\phi(g_i) = \phi(\sum h_i(x_i - f_i)) + \phi(j)$. Since f_i belong to $R[y_1, .., y_n]$ we can't apply ϕ to it. So we need a new mapping. First let us define an inclusion say Ψ,

$$\Psi : R[x_1, .., x_n] \mapsto R[y_1, .., y_n, x_1, ..x_n]$$

. Let us define a new mapping

$$\Pi : R[y_1, .., y_n, x_1, .., x_n] \mapsto R[y_1, .., y_n]/J$$

defined as $\Pi(y_i) = y_i mod J$ and $\Pi(x_i) = f_i mod J$. Then by the universal property we can use Π instead of Φ so

$$\Pi : R[y_1, .., y_n, x_1, .., x_n] \mapsto R[y_1, .., y_n]/J$$

such that $\Pi(g_i) = \Pi(\sum h_i(x_i - f_i)) + \Pi(j)$ which will be equal to 0. Which implies that g_i is in J. Since g_i is an arbitrary element so it is proved that kernal will be given by $((x_i - f_i), J)R[y_1, ..., y_n, x_1, ..., x_n] \cap R[x_1, .., x_n]$. So first we will compute the Groebner basis for the ideal $((x_i - f_i), J)R[y_1, ..., y_n, x_1, ..., x_n]$ and then we will pick only those elements of Groebner basis which contains only variables $x_1, .., x_n$. Those will be the required Groebner basis.

4. We just need to take $J = 0$ in the (3).

5. As we can see that $R[y_1, .., y_n]_h$ is isomorphic to $R[y_1, .., y_n, t]/(th - 1)$, where t is the new indeterminate. So it follows that $IR[y_1, .., y_n]_h \cap R[y_1, .., y_n]$ will be generated by $(I, th - 1)R[y_1, .., y_n, t] \cap R[y_1, .., y_n]$. So we will first compute the Groebner basis for the ideal $(I, th - 1)R[y_1, ..., y_n, t]$ and then contract it to $R[y_1, .., y_n]$. We are basically applying elimination theorem here. By eliminating terms which contains t, from the Groebner basis we will have Groebner basis for $IR[y_1, .., y_n]_h \cap R[y_1, .., y_n]$.

□

Proposition 14 *Suppose that we have an ideal J in $R[y_1, .., y_n]$ and we have a quotient map, given by $\Pi : R[y_1, .., y_n] \mapsto (R/J \cap R)[y_1, .., y_n]$. Suppose we have a subset G of J then -*

1. *If J has G as a Groebner basis, then $J \cap R$ will be generated by $G \cap R$, and $\Pi(J)$ will be generated by $\Pi(G)$.*

2. *J has G as minimal Groebner basis $\iff$ $J \cap R$ has $G \cap R$ as minimal basis. $\Pi(J)$ will have $\Pi(G - G \cap R)$ as minimal Groebner basis such that $\Pi(lt(g))$ is not equal to zero for any g which belongs to $G - G \cap R$.*

Proof: *First we wish to prove that $\Pi(LT(J)) = LT(\Pi(J))$. Since as we know $\Pi(lt(h))$ is either 0 or $lt(\Pi(h))$ where $lt(h) \in R[y_1, .., y_n]$. From here we have that $\Pi(LT(J))$ is a subset of $LT(\Pi(J))$. Now conversely, if $h \in J$ is given then we can see $h = h_0 + h_1$ such that $\Pi(h_0) = 0$ and $\Pi(lc(h_1))$ is not equal to 0. So from here we see that h_0 belongs to J , so h_1 will also be contained in J. So, $lt(\Pi(h)) = lt(\Pi(h_1)) = \Pi(lt(h_1)) \in \Pi(LT(J))$. So we finally get $\Pi(LT(J)) = LT(\Pi(J))$ and our claim is proved. Therefore $LT(\Pi(G)) = \Pi(LT(G)) = \Pi(LT(J)) = LT(\Pi(J))$. so it's proved that $\Pi(J)$ is generated by $\Pi(G)$. From proposition (13) it directly follows that $G \cap R$ generates $J \cap R$. The second part also follows directly from the proposition (13)(2) and the definition of minimal Groebner basis.* □

Now we want to talk about the ring of fractions of $R[y_1, .., y_n]$ w.r.t. the subsets which are multiplicatively closed. We can compute the Groebner basis for ideal in this ring also-

Proposition 15 *Let us assume that we have a subset M of R which is multiplicatively closed. Assume that we have an ideal J in $R[y_1, .., y_n]$ which has Groebner basis G. Then the Groebner basis for $M^{-1}J$ ideal in $(M^{-1}R)[y_1, .., y_n]$ will be G again.*

Proof: As we can see that $LT(M^{-1}J)$ is equal to the $M^{-1}LT(J)$. Since we know that $LT(J) = LT(I)$. so $LT(M^{-1}J) = M^{-1}LT(G)$. Which means that $LT(G)$ is the generating set of $Lt(M^{-1}J)$ in $M^{-1}R[y_1, .., y_n]$. □

Now let us have a look at the construction $M^{-1}J \cap R[y_1, .., y_n]$. which is called the saturation of an ideal J of $R[y_1, .., y_n]$ w.r.t. to the subset M of the ring R.

Lemma 7 *Suppose that we have two subsets M and N of R, which are multiplicatively closed. Assume that we have an ideal J in $R[y_1, .., y_n]$. Then if-*

$$M^{-1}LT(J) \cap R[y_1, .., y_n] = N^{-1}LT(J) \cap R[y_1, ., y_n]$$

then

$$M^{-1}J \cap R[y_1, .., y_n] = N^{-1}J \cap R[y_1, .., y_n]$$

Proof: Since we know that intersection of $LT(M^{-1}J$ with $N^{-1}R[y_1, .., y_n])$ is contained in the intersection of $LT(M^{-1}J)$ with $N^{-1}R[y_1, .., y_n]$. And Since $LT(M^{-1}J)$ is equal to the $M^{-1}LT(J)$. So we can write the intersection of $LT(M^{-1}J)$ with $N^{-1}R[y_1, .., y_n]$ as the intersection of $M^{-1}LT(J)$ with $N^{-1}R[y_1, .., y_n]$. Now since we know that N is contained in M so we can write $M^{-1}LT(J) \cap N^{-1}R[y_1, .., y_n]$ as $N^{-1}(M^{-1}LT(J) \cap R[y_1, .., y_n])$. Now from the equality that is given, we can write this as $N^{-1}(N^{-1}LT(J) \cap R[y_1, .., y_n])$ which is equal to the $N^{-1}LT(J)$. Which is same as $LT(N^{-1}J)$. So basically till here we proved that intersection of $LT(M^{-1}J$ with $N^{-1}R[y_1, .., y_n])$ is eventually contained in $LT(N^{-1}J)$. Since we can see clearly that $N^{-1}J$ is a subset of $M^{-1}J \cap N^{-1}R[y_1, .., y_n]$. so if we take ideals generated by leading terms of their elements we get that $LT(N^{-1}J$ is contained in $LT(M^{-1}J \cap N^{-1}R[y_1, .., y_n])$. The other containment is already proved above so that gives us that intersection of $LT(M^{-1}J$ with $N^{-1}R[y_1, .., y_n]$ is equal to the $LT(N^{-1}J$. Then as mentioned earlier $M^{-1}J \cap N^{-1}R[y_1, .., y_n]$ is equal to $N^{-1}J$. Now let us take the intersection of these terms with $R[y_1, .., y_n]$ so we will get $M^{-1}J \cap R[y_1, .., y_n] = N^{-1}J \cap R[y_1, .., y_n]$. That completes the proof. □

The interpretation of the above lemma is that if we say that set N only has 1 as an element then if the ideal generated by the leading terms of elements of ideal J is saturated then we see that J is also saturated w.r.t. M.

Proposition 16 *Suppose that we have a subset M of R, which is multiplicatively closed. Assume that we have an ideal J in $R[y_1, .., y_n]$. So if-*

$$M^{-1}LT(J) \cap R[y_1, .., y_n] = (LT(J)R_r[y_1, .., y_n]) \cap R[y_1, .., y_n] \tag{4.1}$$

for some $r \in M$ then

$$M^{-1}J \cap R[y_1, .., y_n] = JR_r[y_1, .., y_n] \cap R[y_1, .., y_n]$$

Proof: Basically by R_r we mean that we are localising R at r which means that we are inverting the elements r^m for some non negative integer m. So if we just say that set N from the previuos lemma has only one element which is $\{r^m\}$. Then the result will follow. □

If we find a $r \in M$ which satisfy the condition (4.1) then $M^{-1}J \cap R[y_1, .., y_n]$ can be computed. Because

$$M^{-1}J \cap R[y_1, .., y_n] = JR_r[y_1, .., y_n] \cap R[y_1, .., y_n]$$

and we have seen in corollary (7) that computation of $JR_r[y_1, .., y_n] \cap R[y_1, .., y_n]$ is possible.

Proposition 17 *Assume that R is an integral domain and we have a prime ideal (q), which is principal, in R. Now assume that Groebner basis $G = g_1, .., g_n$ for ideal J of $R[y_1, .., y_n]$ is given. Then we can find an element r which belongs to $R - (q)$ so that $JR_{(q)}[y_1, .., y_n] \cap R[y_1, .., y_n]$ is same as having $JR_r[y_1, .., y_n] \cap R[y_1, .., y_n]$.*

Proof: The most important thing that we need in this proof is the result that $\bigcap(q^j)$ is zero. So we wish to prove this first. So assume that we have an element h in the intersection of (q^j). Then we can write h as $q^j.a$. And q^j as $q^{j+1}.b$. So $q^j = q^{j+1}.b$, which implies that $q^j(1 - qb) = 0$. So from here q^j will be equal to 0. Which means that $h = q^j.a$ will be 0. So we proved that $\bigcap(q^j)$ is zero.

So basically any element s of the ring R, which is not zero, belong to some ideal (q^j),

but will not belong to (q^{j+1}). Then we can write s as rq^j where r can not contained in (q) otherwise s has to be in the (q^{j+1}), which will be contradiction. From ideal membership algorithm we can easily compute j and r.
We can write $lt(g_i) = r_i q^{j_i} y^{b_i}$ where $r_i \notin (q)$. Then $LT(J) = (r_i q^{j_i} y^{b_i})$. And $LT(J)R_q[y_1, .., y_n] \cap R[y_1, .., y_n] = (q^{j_i} y^{b_i})$. So for applying the proposition (18) we have to find an r such that every r_i is invertible in $R_r[y_1, .., y_n]$. We can see clearly that $r = \prod r_i$ satisfies the condition. □

Essentially from this proposition, we learned to construct the element r.

Corollary 8 *Suppose that R be an integral domain, K the quotient field of R. Now assume that Groebner basis $G = g_1, .., g_n$ for ideal J of $R[y_1, .., y_n]$ is given. Then we can compute the intersection of $JK[y_1, .., y_n]$ and $R[y_1, .., y_n]$.*

Proof: If we take $(q) = 0$ in the previous proposition which means that we are having every element of R is invertible so $JR_{(0)}[y_1, .., y_n]$ can be written as $JK[y_1, .., y_n]$. Here we see that the product of leading coefficient of elements of the G is the mentioned r which satisfies the condition (4.1). □

4.2 Primality Test and Zero- dimensional Ideals

We want to construct a way to check whether a given ideal is a prime ideal or not because it is very complicated to take every element of the ideal and see if it satisfies the required properties of elements of prime ideals. I am stating some useful facts which will provide the base to our algorithm- Suppose we have an ideal J in $R[y_1, ..., y_n]$. Then J is a prime ideal if and only if its contraction to R is a prime ideal of R and if we take the image of J in $(R/J \cap R)[y_1, .., y_n]$, then that is also prime ideal. (see [OZ])

Assume that R is an integral domain, K is the quotient field of R. Let us assume that we have such an ideal J in $R[y_1, ..., y_n]$ so that when we contract this ideal to R it becomes the zero ideal. Then this ideal J is a prime ideal if and only if the ideal $JK[y_1, .., y_n]$ is also a prime ideal and ideal J is equal to the ideal $JK[y_1, .., y_n] \cap R[y_1, .., y_n]$.(see [OZ]).

Here we make some assumption that we know the test to see whether an ideal is prime or not in the ring R. And also that we know the test to see whether a uni variate polynomial over quotient fields of residue rings of $R[y_1, ..., y_n]$ is irreducible or not.

Proposition 18 *Assume that we have any ideal J in $R[y_1, .., y_n]$ such that its generating set is given. Then We can check whether J is a prime ideal or not.*

Proof: We will use induction here to prove the theorem, on variables. Let us consider that we have an ideal J which belongs to $R[y_1]$. Let us say J^c is the contraction of J to R. J^c can be computed since we know the generating set of J, by proposition (13). As we assumed that we can test whether ideal in R is a prime ideal or not, since J^c is an ideal in R, so we can check it. If it is not a prime ideal then as we mentioned above the proposition, J will also not be the prime ideal. And we are done with the primality test for J.
Now if J^c is prime then we only need to check whether the image of J in $(R/J \cap R)[y_1]$ is prime ideal or not. Let us assume that R is an integral domain where the contraction of J to R is zero ideal then we can put R instead of $(R/J \cap R)$ in $(R/J \cap R)[y_1]$. So we are left with $R[y_1]$. Assume that we have the quotient field K of R. So now we check the primality of ideal by the second fact that I mentioned earlier. As can see that $JK[y_1]$ is an ideal in the field so it is a principal ideal. Since a principal ideal is a prime ideal if and only if its generator is irreducible. By the assumption that I made earlier, we can test the irreducibility of its generator. If it is not irreducible then J is not prime. Otherwise, we will compute the intersection of $JK[y_1]$ and $R[y_1]$ and see if it equal to J itself. If it is, then J is prime ideal, otherwise not. □

For variable $n = 1$ we proved it in the proof. When $n = 2$ we already know about $n = 1$. So we will consider that ideal for $n = 1$ as I mentioned in the algorithm. And check for $n = 2$ and so on. So basically if we need to check whether an ideal in $R[y_1, .., y_n]$ is prime or not then we have to go through this algorithm n times.

We want to see what special properties Groebner basis possess for zero-dimensional ideals.

Lemma 8 *Suppose we have an ideal J in $R[y_1, .., y_n]$. We have the property that contraction of J to R is zero dimensional. Then we see that J is said to be zero dimensional*

Algorithm 1 PT $(R; Y; J)$. Primality test

1: Input : Ring R; variables $Y = y_1, ..., y_n$;ideal $J \subset R[Y]$.
2: Assumptions : (none)
3: Output : TRUE if I is prime, otherwise FALSE.
4: Step 1 : If $n = 0$ then $J \subset R$ is prime the return TRUE otherwise FALSE.
5: Step 2 : Compute $I = J \cap R[y_2, ..., yn]$.
6: Step 3 : If PT $(R; y_2, ..., y_n; I)$ = FALSE then return FALSE.
7: Step 4 : Let $R' = R[y_2, ..., y_n]/I$, $J' = JR'[y_1]$, K' = quotient field of R'.
8: Step 5 : Compute $J'K'[y_1] = (h)$.
9: Step 6 : If h is not irreducible over K' then return FALSE.
10: Step 7 : Compute $J^{ec} = J'K'[y_1] \cap R'[y_1]$.
11: Step 8 : If $J^{ec} \subset J'$ then return TRUE, otherwise return FALSE.

$\iff$ *$R[y_1, .., y_n]/J$ is integral over R.*

Proposition 19 *Suppose we have an ideal J in $R[y_1, .., y_n]$. Then we see that $R[y_1, .., y_n]/J$ is integral over me $\iff$ the ideal generated by $(y_1, .., y_n)$ is contained in the radical of $LT(J)$.*

Proof: If $R[y_1, .., y_n]/J$ is integral over R then it means that each $y_i + J \in R[y_1, .., y_n]/J$ is integral over R. It means that J contains a monic polynomial $h(y_i) \in R[y_i]$ for each i. So, $lt(h(x_i)) \in LT(J)$. And as we know that $lt(h(y_i))$ is a power of y_i, so $(y_l, ..., y_n) \subset \sqrt{LT(J)}$.
Conversely let $(y_l, ..., y_n) \subset \sqrt{Lt(I)}$. We wish to prove that $R[y_1, .., y_n]/J$ is integral over R. When we say that $R[y_1, .., y_n]/J$ is integral over R then it is equivalent of having that $R[y_1, .., y_n]/J$ is finitely generated as an R- module. Let us assume that $y_i^{s_i}$ belongs to the $LT(I)$. Let us say that

$$M = \sum_{c_i < s_i} R y_1^{c_1} .... y_n^{c_n}$$

is the finitely generated R-module. Let us define a R module map Π say $\Pi : M \mapsto R[y_1, .., y_n]/J$, such that $\Pi(f) = f + J$. We wish to prove that this map is surjective. If we prove this claim, eventually we are proving that $R[y_1, .., y_n]/J$ is finitely generated as an R- module. Suppose $h \in R[y_1, .., y_n]$. Let us imagine that $h + J$ belongs to

$R[y_1, .., y_n]/J$. As we see that $0 + J$ is in the image of Π, we can imagine that h does not belong to J. By the reduction algorithm we can see that there $\exists$ an h' which belongs to $h+J$ with the property that leading term of h' does not belong to the $LT(J)$. From our assumption it means that $lt(h') \notin (y_1^{s_1}, ..., y_n^{s_n})$. Which implies that leading term of h' belongs to K.As we know that $h-h'$ belongs to J and leading term of h' is not in $LT(J)$, so we get that $lt(h - h')$ is not equal to $lt(h')$. So we can see that degree of h' is smaller than degree of h. Which implies that degree of $h' - lt(h)$ is smaller than the degree of h. Now by applying induction on the $deg(h)$ we can suppose that $(h' - lt(h')) + J$ is in the image of Π, let's assume that $\Pi(f) = (h' - lt(h')) + J$ for some element f of K. Then we can see that $\Pi(lt(h') + f)$ can be written as $\Pi(lt(h')) + \Pi(f)$ which is same as $(lt(h') + J) + (h' - lt(h') + J) = h' + J = h + J$. That shows that $h + I$ is in the image of Π. Which shows that the map Π is surjective and proves the claim. That completes the proof. □

So we can see that if $y_i \notin \sqrt{LT(J)}$ then $y_i + J$ is not integral over R.
Let us assume G is the Groebner basis for J, then let

$$G_i = \{g \in G | lt(g) = by_i^s \quad for \quad some \quad b \in R, s \quad is \quad non \quad negative\}$$

and

$$L_i = \langle lc(g_i) | g_i \in G_i \rangle$$

We will notice that $LT(G_i)$ is just the contraction of $LT(G)$ to $R[y_i]$. Which means that $y_i \in \sqrt{LT(J)} = \sqrt{LT(G)} \iff y_i \in \sqrt{LT(G_i)}$. There is only one way to make is possible which is L_i has to be (1). So we can decide if y_i belongs to the $\sqrt{LT(J)}$ just by verifying this single condition which means just by examining a Groebner basis for J.

Since we can check if y_i's belongs to the radical of $LT(J)$ or not, which means that we can directly check that $R[y_1, .., y_n]/J$ is integral over R or not. And if it is not integral then as I mentioned above we can even find the i for which $y_i + J$ is not integral over R, as we can find that i for which y_i won't belong to radical to $LT(J)$. Which implies that we can check J is a zero-dimensional ideal or not, And if not then for which i contraction of J with $R[y_i]$ fails to be zero-dimensional, just by following the steps mentioned above.

Proposition 20 *Suppose that we have an ideal J in $R[]y_1, .., y_n$. Imagine that contrac-*

tion of J to R is zero dimensional and primary ideal. Suppose that Groebner basis for J is given. Then J is said to zero dimensional ideal $\iff$ there $\exists$ an element g_i of G with the property that leading term of g_i is $b_i y_i^{s_i}$, for every i. Here b_i which belongs to R is a unit modulo the contraction of J to R.

Proof: Suppose that G_i and L_i are same as I mentioned earlier. We see that $G_i \supset G \cap R$ so $L_i \supset J \cap R$. As we assumed that $J \cap R$ is zero- dimensional primary then $\sqrt{J \cap R}$ is maximal. For J being zero-dimensional, the only condition is L_i hs to be (1). So $L_i = (1) \iff L_i \not\subset \sqrt{J \cap R}$. Which can happen if and only if there $\exists$ some $g_i \in G_i$ with the property that leading coefficient of (g_i) does not belong to the radical of $I \cap R$. And this is equivalent of having that there exists a $g_i \in G$ such that $lt(g_i) = b_i y_i^{s_i}$, $b_i \in R$ a unit modulo $J \cap R$. □

As we can see that any $f \in J$ such that $y_i^{s_i}$ divides $lt(f_i)$, is said to be reducible modulo $\{g_i\} \cup (G \cap R)$. Let us say that we have given a Groebner basis G of J, which is minimal. Assume we have an element g_i of G with the property that leading term of g_i is $b_i y_i^{s_i}$ and suppose that we have another element g_j in G_i which has degree in y_i, s where $s \geqslant s_i$. If we go modulo intersection of J and R, then all the leading coefficient of elements of G_i will be 1.So then leading term of g_j will divide leading term of g_i which is the contradiction to minimality of G. So except g_i, degree of remaining elements of G_i in y_i will be less than s_i.

So if we have given a minimal Groebner basis G for J, and we need to see that J is zero-dimensional ideal or not, then by the above discussion e if G has only one element with the largest degree and unit ideal is generated by its leading coefficient and $G \cap R$. Then it is confirmed that J is zero-dimensional. There is no need to check other element's leading coefficients.

Lemma 9 *Suppose that we have an ideal J on $R[y_1]$. Imagine that intersection of J and J is zero dimensional. Let us assume that y_1^s belong to the $LT(J)$ but y_1^{s-1} does not belong to $LT(J)$. Then we see that each element of J which has degree less than s is a zero divisor modulo intersection of J and R.*

Proof: Suppose we have $L \subset R$ defined as

$$L = \langle lc(h) | h \in J, deg(h) < s \rangle$$

We claim that if $deg(h) < s$ where $h \in J$ then $h \equiv 0 mod L$. So let us say $h = a_1 y_1^{s-1} + ... + a_s$, then we can see that $a_1 = 0$ or $a_1 = lc(h)$ which means that $a_1 \in L$. There $\exists$ a g which belongs to J such that leading term of (g) is y_1^s by our assumption. Now suppose we have $h' = y_1 h - a_1 g$. Then as we see h' belongs to J and h' can be written as $h' = a_1' y_1^{s-1} + ... + a_s'$ where $a_1' \equiv a_{i+1} mod L$. So from induction we see that a_i's are in L for every i, which proves the claim.
Now we see that if L is equal to (1) then it means that L contains a monic polynomial t such that $deg(t) < s$, which contradict the assumption that $y_1^{s-1} \notin LT(J)$. So it means that L is a proper ideal which will be contained in some maximal ideal. Since contraction of J to R is zero dimensional, its associated primes are maximal. Since $J \cap R$ are contained in L hence L is contained in some associated prime of contraction of J to R. So there $\exists$ an element b which is not in $J \cap R$ with the property that bL is contained in $J \cap R$. Then we can see that $bh \equiv 0 mod J \cap R$ whenever the degree of h is less than s. □

Lemma 10 *Suppose that we have an ideal J on $R[y_1]$, which is zero-dimensional. Imagine that intersection of J and R is zero-dimensional as well as primary ideal. Suppose that we are given a minimal Groebner basis G of J. Imagine that g_1 is an element of G with the property that leading term of g_1 is $b_1 y_1^{s_1}$. Then we can see that radical of J is same as the radical of the ideal generated by the element g_1 with $J \cap R$.*

Proof: As we mentioned above leading term of g_1 is $b_1 y_1^{s_1}$ where b_1 is a unit modulo intersection of J and R by assumption. As we can see that $y_1^{s_1}$ belongs to $LT(g_1, J \cap R)$ which is a subset of $LT(J)$. As we assumed G is a minimal Groebner basis of J so $LT(J)$ can not contain any smaller powers of y_1. Because if it has smaller powers than g_1 will be reducible which will contradict the minimality of G. Each element h of I such that $deg(h) < s_1$ is a zero divisor modulo intersection of J and R by the previous lemma. Since we know that $J \cap R$ is primary. Assume that we have an element cd which belongs to $J \cap R$. Then c will belong to $J \cap R$ or some power of d will belong to $J \cap R$. Assume that c does not belong to $J \cap R$, then some power of d will belong to $J \cap R$.

which means that d will belong to the radical of $J \cap R$. So when we go modulo $J \cap R$, the set of zero divisors clearly will be radical of $J \cap R$. So from this can see that if h is in J such that $deg(h)$ is less than s_1 then $h \equiv 0 mod \sqrt{J \cap R}$. Now suppose h is in J then from the reduction algorithm there $\exists\ h'$ with the property that h' is congruent to h mod $(g_1, J \cap R)$ and h' is reduced modulo $(g_1, J \cap R)$. As we know that $y_1^{s_1}$ belongs to $LT(g_1, J \cap R)$ and $deg(h') < s_1$ hence we can see that $h' \equiv 0 mod \sqrt{J \cap R}$.
So we see that h is contained in $(g_1, J \cap R) + \sqrt{J \cap R}$ which is equal to $(g_1, \sqrt{J \cap R})$. Which means that

$$I \subset (g_1, \sqrt{J \cap R}) \subset \sqrt{J}$$

Now by taking radicals it will be

$$\sqrt{J} = \sqrt{(g_1, J \cap R)}$$

. That completes the proof. □

Proposition 21 *Suppose that we have an ideal J on $R[y_1, .., y_n]$, which is zero dimensional. Imagine that intersection of J and R is zero dimensional as well as primary ideal. Consider the laxicographical ordering with $y_1 > .... > y_n$. Suppose that we are given a minimal Groebner basis G of J. Assume that element $g_1, ...g_n$ of G are same as mentioned in (20). Then we see that J is said to be primary ideal $\iff$ elements g_i's of G are some power of irreducibles modulo the radical of $J \cap R[y_{i+1}, ..., y_n]$ for every i. Tf this happens than every f such that it belongs to the contraction of G to $R[y_i, .., y_n]$ but it's not equal to g_i, is congruent to 0 mod radical of $J \cap R[y_{i+1}, ..., y_n]$.*

Proof: We can reduce this problem to a much simpler problem. suppose that $R' = R[y_2, ..., y_n]$ and J' is the contraction of J to R'. Then we can see that hypothesis of the this proposition is satisfied by J' and $g_2, ..., g_n$ which belongs to $G \cap R'$ as J' is also zero dimensional ideal. So now we only need to show that J is primary $\iff$ J' is. And instead of all g_i's now we just need to see for g_1 that it is some power of irreducible modulo radical of J'. Then every other element of G except g_1 is 0 modulo radical of J'.

So it is clear that if J is primary then so is J' because J' is just the contraction of J to R' . Now suppose that leading term of g_1 is $b_1 y_1^{s_1}$. Assume that f belongs to G which is not equal to g_1 then since we don't want it to be reducible by (g_1, J') so $deg(f_1) \leq s_1$. So

from (9), we can see that $f =\equiv 0 \bmod \sqrt{J'}$. As J is zero dimensional then we know that it will be primary ideal $\iff$ its $\sqrt{J}$ is prime ideal. So as we know that radical of J can be written as $\sqrt{(g_1, J')}$ which is now equal to $\sqrt{(g_1, \sqrt{J'})}$. So we see that J is primary $\iff$ $(g_1, \sqrt{J'})$ is primary, which is same as having $\langle g_i \rangle$ is primary in $(R'/\sqrt{J'})[y_1]$. That completes the proof. □

Proposition 22 *Suppose that we have an ideal J on $R[y_1, .., y_n]$, which is zero dimensional. Imagine that intersection of J and R is zero dimensional as well as prime ideal. Consider the laxicographical ordering with $y_1 > .... > y_n$. Suppose that we are given a minimal Groebner basis G of J. Assume that element $g_1, ...g_n$ of G are same as mentioned in proposition (20). Then we see that J is said to be a prime ideal $\iff$ g_i's are irreducible polynomials modulo contraction of J to $R[y_{i+1}, .., y_n]$, for every i. If this happens then G is equal to the union of $\{g_l, ..., g_n\}$ and $(G \cap R)$.*

Proof: Let us assume that J is a prime ideal. And $g_i \equiv f_i^{a_i}$ where a_i is an irreducible polynomial modulo $I \cap R[y_{i+1}, ..., y_n]$. Now as we assumed that J is a prime ideal so f_i has to be in J. We can see that if the power of f_i, which is a_i, is larger than 1 then g_i will be reducible by f_i which has degree less than g_i. It will ne contraction as G is minimal. So a_i has to be 1. And therefore we can directly see that g_i is reducible mod $J \cap R[y_{i+1}, ..., y_n]$. Conversely , let us assume that $J \cap R[x_{i+1}, ..., x_n]$ is prime and g_i is not reducible modulo $J \cap R[y_{i+1}, ..., y_n]$. Thus we can see that $(g_i, J \cap R[y_{i+1}, ..., y_n])$ which is a subset of $R[y_i, ..., y_n]$ is prime. Suppose f belongs to $G \cap R[y_i, ..., y_n]$ which is not equal to g_i then we see that $f \equiv 0 \bmod J \cap R[y_{i+1}, ..., y_n]$ by the previous proposition. So basically f is reducible modulo $G \cap R[y_{i+1}, ..., y_n]$. Since G is a minimal Groebner basis so f has to be an element of $G \cap R[y_{i+1}, ..., y_n]$ otherwise it will be contradiction due to the minimality of G . It means that except g_i every other element of $G \cap R[y_i, ..., y_n]$ basically belongs to $G \cap R[y_{i+1}, ..., y_n]$. So $G \cap R[y_i, ..., y_n] = \{g_i\} \cup (G \cap R[y_{i+1}, ..., y_n])$. And then consequently $J \cap R[y_i, ..., y_n] = (g_i, J \cap R[y_{i+1}, ..., y_n])$. Since $(g_i, J \cap R[y_{i+1}, ..., y_n])$ is prime so $J \cap R[y_i, ..., y_n]$ is prime. Now the proposition will follow by induction. □

4.3 Zero-dimensional Primary Decomposition

Suppose that a maximal ideal of the ring R is given, say Q. Then we make an assumption that polynomials in 1 variable can be factorized over algebraic extensions of R/Q, where the extensions are finitely generated. (see [Dav])

Proposition 23 *Suppose that we have an ideal J in $R[y_1, .., y_n]$, which is zero dimensional. Assume that radical of intersection of J with R is the maximal ideal Q of R. Then it is possible to construct ideals $J_1, .., J_t$ in $R[y_1, .., y_n]$ and distinct ideals $Q_1, .., Q_t$ in $R[y_n]$, where all J_i's are zero dimensional ideals and all Q_i's are maximal ideals with the property that J can be written as the intersection of all J_i's and radical of the intersection of J_i with $R[y_n]$ is simply Q_i.*

Proof: Suppose $J^c = J \cap R[y_n]$. Since $J^c \in R[y_n]$ is a zero dimensional ideal and satisfies all the conditions of lemma (10) so it is possible for us to find an element g which belongs to Groebner basis of J^c such that $\sqrt{J^c} = \sqrt{(g, Q)}$. Let g_n be the element of largest degree. Let us do the complete factorization of g modulo Q, say $g(y_n) = \prod p_i(y_n)^{s_i}$ mod Q. Which simply means the image of polynomials $p_i(y_n)$ are irreducible non-units in $(R/Q)[y_n]$ and they are also pairwise comaximal. As we see $\prod p_i^{s_i} \in (g, Q)$. Since $\sqrt{J^c} = \sqrt{(g, Q)}$ hence $(g, Q) \subset \sqrt{J^c}$. So $\prod p_i^{s_i} \in \sqrt{J^c}$ which implies $(\prod p_i^{s_i})^s \in J^c$ for some s.
Now as we know p_i and p_j are comaximal modulo Q .By assumption $J \cap R$ is Q-primary so J contains a power of Q. So all this implies that p_i and p_j are comaximal modulo J. Since p_i and p_j are irreducible thus $\bigcap_i (p_i^{s_i s}, J) = (\prod p_i^{s_i s}, J) = J$. Now let $J_i = (p_i^{s_i s}, J)$ and $Q_i = (p_i, Q)R[y_n]$. We can see clearly that Q_i's are maximal. As $J_i \cap R[y_n]$ contains a power of Q_i, so it is either a unit ideal or Q_i-primary. If we take the first possibility that $J_i = (1)$ then since we have $\prod_{j \neq i} p_j^{s_i s} J_i \subset J$ it implies that $\prod_{j \neq i} p_j \in \sqrt{J^c} = \sqrt{(g, Q)}$. If we go modulo Q then we see that $\prod_{j \neq i} p_j$ belongs to $\sqrt{(g, Q)}/Q$, where $\sqrt{(g, Q)}/Q$ is contained in $R/Q[y_n]$. We see that elements of $\sqrt{(g, Q)}/Q$ has to be of the form $(\prod_i p_i)R/Q[y_n]$. So p_j's will be some multiple of p_i's, means p_i's have to divide p_j's. But since p_j's are irreducible, p_i's have to be unit modulo Q. But we factorized g in such a way that p_i's are non-units modulo Q. So this

is a contradiction. Which implies that J_i can't be unit ideal. So it is proved that J_i is Q_i-primary. □

The above proof described the reason behind every step of the following algorithm for zero dimensional primary decomposition.

Algorithm 2 ZPD $(R; Y; M)$; Zero-dimensional primary decomposition

1: Input : Ring R; variables $Y = y_1, ..., y_n$;ideal $J \subset R[y_1, .., y_n]$;ideal Q of R.
2: Assumptions : Q is maximal , J is zero-dimensional, $\sqrt{J \cap R} = Q$.
3: Output : $\{(J_1, Q_1), ..., (J_t, Q_t)\}$, J_i,Q_i ideals in $R[y_1, .., y_n]$ where Q_i is maximal, $Q_i \neq Q_j$, $\sqrt{J_i} = Q_i$ and $J = \bigcap_i J_i$.
4: Step 1 : If $n = 0$ then return $\{(J, Q)\}$.
5: Step 2 : Compute a minimal Groebner basis G for $J \cap R[y_n]$.
6: Step 3 : pick the $g \in G$ with maximum degree.
7: Step 4 : Compute the complete factorization of g mod Q, $g = \prod p_i^{s_i}$ in $(R/Q)[y_n]$, $p_i \in R[y_n]$.
8: Step 5 : Find s such that $(\prod p_i^{s_i})^s \in J \cap R[y_n]$.
9: Step 6 : Let $J_i = (p_i^{s_i}, J)$, $Q_i = (p_i, Q)R[y_n]$.
10: Step 7 : Return $\bigcup_i ZPD(R[y_n]; y_1, ..., y_{n-1}; J_i; Q_i)$.

So basically what we saw is first we will make the case in 1 variable by taking the contraction of the ideal in $R[y_1, .., y_n]$ with $R[y_n]$ so that we can factorize its element of basis. Then the irreducible polynomials that we got from this factorization will be the whole meat of this algorithm.

4.4 Zero-dimensional Ideals over Fields of Characteristic 0

Let us consider here that K is a field of characteristic zero. For every ideal J in the $K[y_1, .., y_n]$, elements of their Greobner basis has leading coefficients 1.
Imagine that we have an ideal J in $K[y_1, .., y_n]$. Then we can have ideals J_i's in $K[y_i, .., y_n]$ such that they are the contraction of J with $K[y_i, .., y_n]$. If we consider that a prime ideal J is zero dimensional and consider lexicographical ordering on monomials, then as we have seen earlier that minimal Groebner basis for J will be like $\{g_1(y_l, ..., y_n), g_2(y_2, ..., y_n), ...g_n(y_n)\}$.

Elements of its Groebner basis are in a particular form. Each element g_i of G has leading elements in y_i with coefficient 0. Each g_i is irreducible modulo the contraction of J with $K[y_{i+1}, .., y_n]$.

Proposition 24 *Suppose that we have a prime ideal J in $K[y_1, .., y_n]$, which is zero-dimensional. It has minimal Groebner basis in the form described above. Then for almost all linear transformations of co ordinates we will get elements of new Groebner basis in the form $g_i = y_i - p_i(y_{i+1}, ..., y_n)$ where i is strictly less than n.*

Proof: Primitive element theorem (see [OZ]) tells us that suppose that K is an infinite field. $K[y_1, ..., y_n]$ is the algebraic extension of the field k the we can find elements $c_1, ..., c_n \in K$ such that by setting $\beta = c_1y_1 + c_2y_2 + ... + c_ny_n$ we get that the algebraic extension of the field K is equal to $K(\beta)$. Since we know that $K[y_1, .., y_n]/J$ is the algebraic extension of the field K then we can find $c_1, ..., c_n \in K$ such that we get

$$K[y_1, .., y_n]/J \simeq K(c_1y_1 + c_2y_2 + ... + c_ny_n)$$

This is true for almost all elements of K. Now let us do the change of coordinates. Let y_i's be x_i's where i is strictly less than n. And put x_n as $c_1y_1 + c_2y_2 + ... + c_ny_n$. So the above relation will change into-

$$K[x_1, ..., x_n]/J \simeq K(x_n)$$

. As we can see that each x_i belongs to $K[x_n]$,then because of above relation it implies that $x_i = h_i(x_n)$ also belongs to $K[x_1, ..., x_n]/J$. As we can see that $x_i - h_i(x_n)$ is equal to 0 so they are contained in the ideal J in $K[x_1, ..., x_n]/J$ where i is strictly less than n.

Now assume that we get new Groebner basis G for the ideal J after the coordinate change. Since $x_i - h_i(x_n)$ belongs to the ideal J hence it will be reducible modulo G. As we can see from the form of given Groebner basis that g_i is the single element of G which have the ability to reduce x_i because g_i's have leading terms in y_i's. Thus we have the leading term of g_i equal to z_i as we need it to be. □

Suppose that we have a prime ideal J in $K[y_1, .., y_n]$, which is zero-dimensional. Consider we have lexicographical ordering on the monomials then if the elements of

minimal Groebner basis for J satisfies all the properties given in the above proposition then J is said to be in the general position.

So if we want to check whether an ideal whose Groebner basis is given, is in general position or not, then we first check if the ideal is prime. For that we will check the form of elements of Groebner basis if they have the form given in the starting of the section then it means that ideal is prime then we check if the elements of Groebner basis are in the form mentioned in the above proposition. If the condition satisfies then ideal is in general position.

If we have an arbitrary ideal which is zero-dimensional. Then if its associated primes are in general position and their contraction to $K[y_n]$ are pairwise comaximal then the ideal is said to be in general position.

Corollary 9 *Let us assume that we have a primary ideal J in $K[y_1, .., y_n]$ which is zero-dimensional and also in the general position. Then we can say that the element g_i's of Groebner basis mentioned in proposition (20), will be the powers of linear equations modulo radical of the contraction of ideal J to $K[y_{i+1}, .., y_n]$ where i is strictly less than n.*

Proposition 25 *Suppose that we have a zero-dimensional ideal J in $K[y_1, .., y_n]$, which is in general position. Let us consider the lexicographical ordering on the monomials. Suppose that we are given the Groebner basis $G$of J. All elements of G are same as mentioned in prop (20). Let us say that we are given irreducible decomposition $g_n = \prod_{i=1}^{t} p_i^{s_i}$. Then we see that primary decomposition of J will be the intersection of $(p_i^{s_i}, J)$ over all i.*

Proof: First we will prove that $J = \bigcap_{i=1}^{t}(p_i^{s_i}, J)$. It's clear that $J \subset \bigcap_{i=1}^{t}(p_i^{s_i}, J)$. Now for the other way round imagine that $p^{(i)} := g_n/p_i^{s_i}$ for $i = 1, ..., t$. Then from the construction of these polynomials $p^{(1)}, ..., p^{(t)}$ in $K[y_n]$ will have GCD 1. So there will exist some $c_1, ..., c_t \in K[y_n]$ with $\sum_{i=1}^{t} c_i g^i = 1$. Now suppose $h \in \bigcap_{i=1}^{t}\langle J, p_i^{s_i}\rangle$. It means that for some element h_i of J and some element α_i of $K[y_1, .., y_n]$, h can be

written as $h = h_i + \alpha_i p_i^{s_i}$ for i is 1 to t. Therefore

$$h = \sum_{i=1}^{t} c_i g^i (h_i + \alpha_i p_i^{s_i}) = \sum_{i=1}^{t} (c_i g^i h_i + c_i \alpha_i g_n) \in J$$

. So it's proved that $J = \bigcap_i (p_i^{s_i}, J)$.

So now we can see that $\langle J, p_i^{s_i} \subsetneq K[y_1, .., y_n]$ and $Ass(\langle J, p_i^{s_i} \rangle) \subset Ass(J)$. We can see this in the following manner-

Let us say that 1 can be written as $1 = h + cp_i^{s_i}$ for some element h of the ideal J and c of $K[y_1, .., y_n]$, then we can clearly see that $g_n/p_i^{s_i}$ belongs to the ideal generated by h and g_n which will be contained in J which contradicts that contraction of J with $K[y_n]$ is generated by g_n. And $J \subset \langle J, p_i^{s_i} \rangle$ and from the uniqueness property of associated primes we see that some associated prime of J is bound to be contained in every associated prime of the ideal generated by J, $p_i^{s_i}$. But as know the property of zero-dimensional ideals also, that is- its associated primes will be the maximal ideals. Let us suppose that we denote associated primes of J by $Q_1, ..., Q_l$. We also assume that contraction of these primes to $K[y_n]$ is generated by f_i. So we can see that

$$\bigcap_{i=1}^{l} (Q_i \cap K[y_n]) = \bigcap_{i=1}^{l} \langle f_i \rangle$$

We can see as a result of existing assumptions that these $f_1, ..., f_l$ are pairwise coprime. That implies that

$$\bigcap_{i=1}^{l} \langle f_i \rangle = \langle \prod_{i=1}^{l} f_i \rangle$$

So basically

$$\bigcap_{i=1}^{l} (Q_i \cap K[y_n]) = \langle \prod_{i=1}^{l} f_i \rangle$$

Now let us notice that $\bigcap_{i=1}^{l} (Q_i \cap K[y_n])$ also can be written as $(\bigcap_{i=1}^{l} Q_i) \cap K[y_n]$.As we know that radical of J is equal to the intersection of these Q_i's. So

$$\bigcap_{i=1}^{l} (P_i \cap K[x_n]) = \sqrt{J} \cap K[y_n]$$

. Hence, according to the assumption $J \cap K[y_n] = \langle g_n \rangle$ we can see that g_n is divisible by $\prod_{i=1}^{l} f_i$, also some power of $\prod_{i=1}^{l} f_i$ is divisible by g_n. This gives us that l and t are equal. Basically we can consider that p_i's and f_i's are equal for i which varies from 1

to t. So from here we can state that Q_i is the the unique associated prime of J which contains $p_i^{s_i}$. Now from all this discussion that we had we can come up with the result that $Ass(\langle J, p_i^{s_i}\rangle)$ are simply the primes Q_i. Which gives us that ideal generated by J and $p_i^{s_i}$ is primary ideal. That completes the proof. (see, [GMG]) □

Algorithm 3 ZPDF $(K; Y; I)$; Zero-dimensional primary decomposition over a field

1: Input : Field K; variables $Y = y_1, ..., y_n$;ideal $J \subset K[y_1, .., y_n]$.
2: Assumptions : K is a field of characteristic 0; J is zero-dimensional.
3: Output : $\{J_1, ..., J_m\}$ such that , $I_i \subset K[y_1, .., y_n]$ is a primary ideal, $J = \bigcap_i J_i$ and $\sqrt{J_i} \neq \sqrt{J_j}$.
4: Step 1 : Select random $a_1, ..., a_{n-1} \in K$ and replace y_n by $y_n + \sum a_i y_i$.
5: Step 2 : Compute $J \cap K[y_n] = (g)$.
6: Step 3 : Compute the complete factorization of g, $g = \prod p_i^{s_i}$.
7: Step 4 : If $(p_i^{s_i}, J)$ is not a primary ideal in general position then go to step 1.
8: Step 5 : Replace y_n by $y_n - \sum a_i y_i$.
9: Step 6 : Return $\{(p_i^{s_i}, J)\}$.

So basically we can make an ideal in general position by doing the coordinate changes. So in the algorithm, we see that first, we attempt to make the ideal in general position. Since we are given the Groebner basis for the ideal, we find the Groebner basis for this new ideal we got by coordinate changing. Then we contract them to $K[y_n]$ to get the Grobner basis for contraction of ideal to $K[y_n]$. Since it is an ideal of the field, we will get a single element in the basis. Then we do the complete factorization of this element, say $g = \prod p_i^{s_i}$. Then this $\bigcap_i (p_i^{s_i})$ can be the primary decomposition for an ideal J which is in general position only if we can prove that $(p_i^{s_i}, J)$ are the primary ideals in general position. So we take $(p_i^{s_i}, J)$ and compute their Groebner basis and see if they satisfie the corollary (9). If it does then these are the primary ideals in general position. Then we again change the coordinates in the old ones. And get our primary decomposition. But if it is not then we keep changing the coordinates until we make our ideal in general position.

4.5 Primary Decomposition in Principal Ideal Domain

Lemma 11 *Let us assume that we have an ideal J in $R[y_1, .., y_n]$ and a subset M of R which is multiplicatively closed. Assume that we have an element r of M. If we have that intersection of $M^{-1}J$ with R is contained in $(J : r)$, then we can see that*

$$J = (J : r) \cap (J, r).$$

Proof: It is clear from the definition of $(J : r)$ and (J, r) that the intersection of $(J : r)$ and (J, r) contains the ideal J.

Now let h belongs to the intersection of $(J : r)$ and (J, r). We want to prove that h will also belong to the ideal J. So according to the assumption h can be written as $h = j + br$ where j is an element of J. Then as we know $j + br$ is in $(J : r)$ which implies that $jr + br^2$ is in J so that br^2 belongs to J. And the fact that br^2 is in J implies that b belongs to $M^{-1}J \cap R$ So it gives us that b belongs to $(J : r)$ that means br is in J so now it's proved that h has to be in J. Which completes the proof. □

Proposition 26 *Suppose that R is an integral domain. We assume that (q) is a prime ideal of R, which is principal. So we can find an element s of $R - (q)$ so that ideal J is equal to the intersection of (J, s) and $JR_q[y_1, .., y_n] \cap R[y_1, .., y_n]$, where J is any ideal of $R[y_1, .., y_n]$ such that its generating set is given. We denote $JR_{(q)}[y_1, .., y_n] \cap R[y_1, .., y_n]$ as J^{ec}.*

Proof: We have given a construction for such an element r of $R-(q)$ so that $JR_{(q)}[y_1, .., y_n] \cap R[y_1, .., y_n]$ will be equal to $JR_r[y_1, .., y_n] \cap R[y_1, .., y_n]$. So we will get r. We know how to compute J^{ec} by corollary (7). As mentioned in the starting of this chapter that we consider R as a Noetherian ring, so some t will $\exists$ which will make $r^t J^{ec}$ a subset of J. Once we compute the groebner basis for J^{ec}, we can easily find t. We just need to check for what values for t , $r^t G$ will be contained in J. So according to the statement of theorem $s = r^m$ is value of s that is required. □

Proposition 27 *Suppose that R is a principal ideal domain. We have an ideal J of $R[]y_1, .., y_n$. Assume that we have an ideal (q) in R such that it is a maximal ideal. If the radical of contraction of J to R is equal to the (q) then we can compute the primary decomposition of the ideal J.*

Proof: First we will check whether J is a zero-dimensional ideal or not. If it is then we know how to compute its primary decomposition. We can use any algorithm given before. Otherwise we can find an i for which contraction of ideal J to $R[y_i]$ is not zero dimensional with the help of proposition (19). Now denote $R' = R[y_i]$ and $y' = y_1, ..., y_{i-1}, y_{i+1}, ..., y_n$. So basically we have that $R[y_1, .., y_n]$ is same as $R'[y']$ and contraction of J to R' is not zero dimensional ideal. Now we can apply the previous proposition. So eventually we will find element s' of $R' - (q)R'$ so that J will be equal to intersection of (J, s') and J^{ec}. which is equal to $(J, s') \cap JR'_q[y'] \cap R'[y']$. So now we will decompose (J, s') and J^{ec} separately.
First we will try to decompose (J, s'). Since (q)-primary ideal $J \cap R$ and $s' \notin (q)R'$ both are contained in $(J, s') \cap R'$. Any ideal which is generated by both of $J \cap R$ and s' will have dimension greater than (q), since $J \cap R$ is a (q) primary ideal. If we go modulo then $R/(q)$ is an integral domain and basically we have a map from the ideal generated by both $J \cap R$ and s' to $s'(R/(q))$. As we can see that any ideal in $s'(R/(q))$ is one dimensional so its preimage ideal which is contained in the ideal generated by both $J \cap R$ and s' to $s'(R/(q))$ will be of 1 dimensional. That means the ideal generated by both $J \cap R$ and s' to $s'(R/(q))$ is zero dimensional. Which simply implies that $(J, s') \cap R'$ is zero dimensional ideal or a unit ideal. So let us suppose $(J, s') \cap R'$ is zero dimensional ideal then we can compute the primary decomposition of (J, s') by the algorithms given before. And if $(J, s') \cap R'$ is unit ideal then $J = J^{ec}$ and there is need to decompose J^{ec} only.

Now we want to decompose J^{ec} which is $JR'_{(q)}[y'] \cap R'[y']$. So for computing J^{ec} first $JR'_{(q)}[y'] = J^e$ should be decomposed and then we will do its contraction to $R'[y']$. We can see that $R'_{(q)}$ is a principal ideal domain. Since (q) is a maximal ideal in R, $(q)R'_{(q)}$ has to be maximal in $R'_{(q)}$. We first wish to prove that radical of $J^e \cap R'_{(q)}$ is same as $(q)R'_{(q)}$. So basically by proving this claim we will put $R'_{(q)}$, $(q)R'_{(q)}$, $J^e \cap R'_{(q)}$ in position of R, (q) and $J \cap R$ respectively and they will satisfy the hypothesis of the proposition. Now we will prove the claim. As we can see that radical of contraction of J to R is equal to (q) and some power of q is contained in $JR'_(q))$ because J contains a power of q. So there is only need to show that $J'R'[y'] \cap R'$ is contained in $(q)R'$. Assume that we have some associated prime of $I \cap R'$ whose dimension is not zero, say Q. Then

we see that $(q)R'$ is conatined in Q. Since R' is two dimensional, $(q)R'$ has to be one dimensional so Q must be equal to $(q)R'$. This proves the claim. And as I mentioned earlier I^e full fills our hypothesis of this proposition. So it can be decomposed by the induction on n. □

So basically we are reducing high dimensional ideals in zero-dimensional ideal by using some localization at principal primes.

Corollary 10 *Let us assume that we have a field K. Then every ideal of $K[y_1, .., y_n]$ can be primary decomposed.*

Proof: We just need to take $p = 0$ in the previous proposition and the whole proof will follow. □

Proposition 28 *Suppose that R is a principal ideal domain. Assume we have an ideal J in $R[y_1, .., y_n]$. Then primary decomposition can be computed for J.*

Proof: First we will check whether intersection of J and R is zero dimensional or not. $I \cap R$ won't be zero dimensional if it is zero or R is a field. So if it is not zero dimensional then then we use the proposition (27) by taking $p = 0$ and find a nonzero s so that we can write J as $(J, s) \cap (JR_{(0)}[y_1, .., y_n] \cap R[y_1, .., y_n])$. We can decompose $(JR_{(0)}[y_1, .., y_n] \cap R[y_1, .., y_n])$ by first decomposing $JR_{(0)}[y_1, .., y_n]$ by putting $q = 0$ in the proposition (27) and then by contracting it to $R[y_1, .., y_n]$. Now we only have to decompose (J, s). (J, s) contracts to a ideal in R which is zero dimensional. So now by this we can assume that $J \cap R$ is zero dimensional. So we can write $J \cap R = (\prod p_i^{m_i})$, where $(p_i)R$ is maximal ideal. Then we can see that $(p_i^{m_i}, J) \cap R$ is (p_i)-primary. So $(p_i^{m_i}, J)$ satisfies all the hypothesis of the proposition (27). So we can decompose $(p_i^{m_i}, J)$ by using the algorithm given in proposition (27). Since $J = \bigcap_i (p_i^{m_i}, J)$, so by getting the decomposition of $(p_i^{m_i}, J)$ we get the decomposition of J. □

Algorithm 4 PPD $(R; Y; J)$; Primary decomposition over a PID

1: Input : Ring R; variables $Y = y_1, ..., y_n$;ideal $J \subset R[y_1, .., y_n]$.
2: Assumptions : R is a PID.
3: Output : $\{Q_1, ..., Q_m\}$ such that $Q_i \subset R[y_1, .., y_n]$ is a primary ideal, $J = \bigcap_i Q_i$.
4: Step 1 : Find $s \neq 0$ such that $J = (J, s) \cap (JR_{(0)}[y_1, .., y_n] \cap R[y_1, .., y_n])$.
5: Step 2 : Let $\{Q_1, ..., Q_k\} = PPD - 0(R_{(0)}); Y; JR_{(0)}[y_1, .., y_n]; 0)$
6: Step 3 : Let $Q_i^c = Q_i \cap R[y_1, .., y_n]$.
7: Step 4 : Compute $(J, s) \cap R = (s')$.
8: Step 5 : If s is a unit, return $\{Q_1^c, ..., Q_m^c\}$.
9: Step 6 : Factor $s' = \prod p_i^{m_i}$, p_i is irreducible.
10: Step 7 : For each i let $\{Q_1^i, ..., Q_{k_i}^i\} = PPD - 0(R; Y; (J, p_i^{m_i}); p_i)$.
11: Step 8 : Return $\{Q_1^c, ..., Q_m^c\} \cup \bigcup_i \{Q_1^i, ..., Q_{k_i}^i\}$.

Algorithm 5 PPD-0 $(R; Y; J; q)$; Primary decomposition over a PID, primary contraction case

1: Input : Ring R; variables $Y = y_1, ..., y_n$;ideal $J \subset R[y_1, .., y_n]$; $q \in R$
2: Assumptions : R is a PID, $(q)R$ is maximal, $J \cap R$ is (q)- primary.
3: Output : $\{Q_1, ..., Q_m\}$ such that $Q_i \subset R[y_1, .., y_n]$ is a primary ideal, $J = \bigcap_i Q_i$.
4: Step 1 : If J is not zero-dimensional then return its decomposition using ZPD or ZPDF.
5: Step 2 : Find i such that $J \cap R[y_i]$ is not zero-dimensional.
6: Step 3 : Let $R' = R[y_i]$, $y' = y_1, ..., y_{i-1}, y_{i+1}, ..., y_n$, $J^e = JR'_{(q)}[y']$.
7: Step 4 : Find $s' \in R' - (q)R'$ such that $J = (J, s') \cap (J^e \cap R'[y'])$.
8: Step 5 : Let $\{Q_1, ..., Q_m\} = PPD - 0(R'_{(q)}; y'; J^e; q)$.
9: Step 6 : Let $Q_i^c = Q_i \cap R'[y']$.
10: Step 7 : If $(J, s') = (1)$ then return $\{Q_1^c, ..., Q_m^c\}$.
11: Step 8 : Let $\{Q'_1, ..., Q'_k\} = PPD - 0(R; Y; (J, s'); q)$.
12: Step 9 : Return $\{Q_1^c, ..., Q_m^c, Q'_1, ..., Q'_k\}$

Bibliography

[Dav] Trager B Davenport, J., *Factorization over finitely generated fields. proceedings of the 1981 symposium on symbolic and algebraic computation-snowbird, utah, pp. 200-205.*

[DO07] J.Little D.Cox and D. O'Shea, *Ideals, varieties, and algorithms*, Springer-Verlag, New York, 1997, 2007.

[G.] Zacharias G., *Generalized gröbner bases in commutative polynomial rings*.

[GG] B.Trager Gianni and G.Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*.

[GMG] Gerhard Pfister Gert-Martin Greuel, *A singular introduction to commutative algebra*, Springer-Verlag Berlin Heidelberg.

[Kap] I. Kaplansky, *Commutative rings*, Queen Mary College Math Notices, London.

[OZ] Pierre Samuel Oscar Zariski, *Commutative algebra 1*, Springer-Verlag, New York, 1975.

[Tri] W. Trinks, *Über b. buchbergers verfahren, systeme algebraischer gleichungen zu lösen. j. number theory, 10, 475-488.*