GRÖBNER BASES AND SOME APPLICATIONS

by

BİLGE ŞİPAL

A Thesis Submitted to the
Graduate School of Sciences & Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Mathematics

Koç University

June, 2007

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

BİLGE ŞİPAL

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

_____

Assistant Prof. Müfit Sezer

_____

Prof. Ali Ülger

_____

Assistant Prof. Müge Kanuni

_____

Assistant Prof. Emre Alkan

_____

Assistant Prof. Sinan Ünver

Date: _____

TABLE OF CONTENTS

0.1 General Notation and Terminology.

In this section we will present some general notation and terminology.

Numbers and Sets

$\mathbb{N} = \{0, 1, 2, \ldots\} =$ the set of natural numbers

$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$

$\mathbb{Z} =$ the set of all rational integers

$\mathbb{Q} =$ the set of all rational numbers

$\mathbb{R} =$ the set of all real numbers

$\mathbb{C} =$ the set of all complex numbers

$P =$ partially ordered set

$\leqslant$ ordering relation

$\mathbb{T}^n =$ set of terms in the indeterminates $x_1, ..., x_n$

$\mathcal{O} =$ order ideal

Orderings

Lex= Lexicographic Ordering

DegLex= Degree Lexicographic Ordering

DegRevLex= Degree Reverse Lexicographic Ordering

Rings

Unless otherwise stated R will denote throughout this thesis a commutative ring with identity element.

$$(x_1, x_2, \ldots, x_n) = \left\{ \sum_{1 \le i \le n} r_i x_i \,|\, r_1, r_2, \ldots, r_n \in R \right\} = \text{ the ideal of } R$$
$$\text{generated by } x_1, x_2, \ldots, x_n \in R$$
$$(x) = Rx = \text{ the principal ideal of } R$$
$$\text{generated by } x \in R$$
$$R[x_1, \ldots, x_n] = \text{ the polynomial ring in the indeterminates}$$
$$x_1, \ldots, x_n \text{ with coefficients from the ring } R$$
$$1 \quad \text{is the identity element of the ring } R$$
$$I_R \quad \text{is the identity map from ring } R \text{ to itself}$$
$$I \quad I \text{ is an ideal of } R$$
$$M_n(R) = \text{the ring of } n \times n \text{ matrices over a ring } R$$
$$\mathrm{Ker}(\varphi) = \text{the kernel of a morphism } \varphi$$
$$\mathrm{Im}(\varphi) = \text{the image of a morphism } \varphi$$

Modules

M is a R-module

$\mathrm{Hom}_R(M,N)$ = the set of R-morphisms from M to N

$\mathrm{End}_R(M)$ = the ring of R-endomorphisms of M

$M \oplus N$ = direct sum of modules M and N

$\prod_{\alpha\in I} M_\alpha$ = the direct product of an arbitrary family $(M_\alpha)_{\alpha\in I}$ of modules

$\bigoplus_{\alpha\in I} M_\alpha$ = the direct sum of an arbitrary family $(M_\alpha)_{\alpha\in I}$ of modules

k is a Field

Chapter 1

PRELIMINARIES

1.1 Rings

We begin with some definitions

Definition 1.1.1. *Let S be a ring. A function*

$$\varphi : R \longmapsto S$$

is ring homomorphism provided that for all $a, b \in R$:

$$\varphi(a+b) = \varphi(a) + \varphi(b),$$

$$\varphi(ab) = \varphi(a)\varphi(b).$$

The composition of ring homomorphisms is again a ring homomorphism. An *endomorphism* of a ring is a homomorphism of the ring into itself. An *isomorphism* of rings is a ring homomorphism which is one-to-one and onto. A subset S of a ring R is called a *subring* if S is closed under addition and multiplication and contains the same identity element as R. A subset I of a ring R is called a *left ideal*(resp. *right ideal*) of R if I is a subgroup of the additive group of R and if $ri \in I$ (resp. $ir \in I$) for all $r \in R, i \in I$.

Proposition 1.1.2. *Let*

$$I_0 \subseteq I_1 \subseteq ... \subseteq I_m \subseteq ...$$

be a chain of ideals of R. Then

$$I = \bigcup_{i \in \Lambda} I_i$$

is an ideal of R, where Λ is any index set.

Proof. If $x \in I$ then $\exists I_k$ in the chain such that $x \in I_k$ for some $k \in \Lambda$. I_k is an ideal of R so for any $r \in R$, $rx \in I_k$. Therefore $rx \in I$. If we take $m, n \in I$ then $\exists I_i, I_j$ in the chain such that $m \in I_i$ and $n \in I_j$ for some $i, j \in \Lambda$. These submodules are elements of the chain, we can assume $I_i \subseteq I_j$. Hence $m, n \in I_j$. I_j is an ideal of R so $m - n \in I_j$ and therefore $m - n \in I$ and I is an ideal of R.

□

Theorem 1.1.3 (*The Fundamental Theorem of Isomorphism For Rings*)**.** *Let S be rings with identity. If*

$$\varphi : R \longmapsto S$$

is a ring homomorphism then the $\mathrm{Ker}(\varphi)$ *is a two-sided ideal of R,* $\mathrm{Im}(\varphi)$ *is a subring of R and*

$$R/\,\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi).$$

Definition 1.1.4. *A non-empty set S is a multiplicative set if*

i)$\forall s_1, s_2,\ s_1 s_2 \in S$

ii) 0 *is not an element of S.*

Example 1.1.5. *If R is a commutative ring and P is a prime ideal, then $R - P$ is a multiplicative set. Assume $R - P \neq \emptyset$. Let $a, b \in R - P$ and ab is not an element of $R - P$. Thus $ab \in P$ i.e., either $a \in P$ or $b \in P$, that is either a is not in $R - P$ or b is not in $R - P$. That is a contradiction. Therefore if $ab \in R - P$ and $0 \in P$, then 0 is not in $R - P$.*

Proposition 1.1.6. *If S is a multiplicative set in R then R/S contains a prime ideal.*

Proof. Let

$$K = \{I \ \ ideals \ \ of \ \ R : I \cap S = \emptyset\}.$$

K is non-empty. $\{0\} \in K$ since $\{0\} \cap S0 = \emptyset$. If $\{I_j\}_{j \in \Delta}$ is a chain in K then $\bigcup_{j \in \Delta} I_j$ is also an ideal of R. Therefore this union is an upper bound. By *Zorn's Lemma* K

has a maximal element say P. Now let $a, b \in R$ such that $ab \in P$. If a is not in P then form $P + (a) \supseteq P$. Since P is the maximal element in K, $P + (a) \cap S$ is not empty, i.e., there exists $s_1 \in K$ such that $s_1 = p_1 + r_1 a$ for some $p_1 \in P$ and $r_1 \in R$. Similarly if b is not an element of P then there exists $s_2 \in K$ such that $s_2 = p_2 + r_2 b$ for some $p_2 \in P$ and $r_2 \in R$. Consider

$$\begin{aligned} s_1 s_2 &= (p_1 + r_1 a)(p_2 + r_2 b) \\ &= p_1 p_2 + p_1 r_2 b + p_2 r_1 a + a b r_1 r_2 \end{aligned}$$

Clearly $s_1 s_2 \in P$ but also $s_1 s_2 \in S$,i.e., $P \cap S$ is not empty. But this contradicts with $P \in K$. Therefore P is a prime ideal such that $P \in K$. □

1.2 Modules

Definition 1.2.1 (*Module homomorphism*)**.** *Let M and N be R modules. A function*

$$\varphi : M \longmapsto N$$

is a module homomorphism provided that:

$$\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2), \quad \forall m_1, m_2 \in M$$

$$\varphi(rm) = r\varphi(m), \quad \forall m \in M, r \in R.$$

Theorem 1.2.2 (*The Fundamental Theorem of Isomorphism For Modules*)**.** *Let M and N be R-modules. If a function φ:$M \longrightarrow N$ is a module morphism;*

$$M/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi).$$

Theorem 1.2.3. *Let N be a submodule of M. There is a bijection between the submodules of M which contain N and the submodules of M/N.*

Proposition 1.2.4. *Let M be a module and*

$$N_0 \subseteq N_1 \subseteq ... \subseteq N_m \subseteq ...$$

be a chain of submodules of M. Then

$$N = \bigcup_{i \in \mathbb{N}} N_i$$

is a submodule of M.

Proof. If $x \in N$ then $\exists N_k$ in the chain such that $x \in N_k$ for some $k \in \mathbb{N}$. N_k is a R-module so for any $r \in R$, $rx \in N_k$. Therefore $rx \in N$. If we take $m, n \in N$ then $\exists N_i, N_j$ in the chain such that $m \in N_i$ and $n \in N_j$ for some $i, j \in \mathbb{N}$. These submodules are elements of the chain, so without lost of generality we can assume $N_i \subseteq N_j$. Hence $m, n \in N_j$. N_j is a R-module so $m+n \in N_j$ and therefore $m+n \in N$ and N is submodule of M.

□

The R-module M is called *cyclic* if there exists $m \in M$ such that $M = Rm$. The R-module M is said to be *finitely generated* if there exists $m_1, m_2, ..., m_n \in M$ such that $M = \sum_{j=1}^{n} Rm_j$. In this case, we say $m_1, m_2, ..., m_n$ is a set of generators for M. A submodule $N \subseteq M$ is called *maximal submodule* if $N \neq M$ and for any submodule K with $N \subseteq K \subseteq M$, either $N = K$ or $K = M$.

Definition 1.2.5. *Let $(M_i)_{i \in I}$ be a collection of R-modules indexed by the set I. The direct product of the modules $(M_i)_{i \in I}$ is the* cartesian product

$$\prod_{i \in I} M_i = \left\{ (x_i)_{i \in I} : x_i \in M_i \right\}$$

with componentwise addition *and* scalar multiplication. *If $x, y \in \prod_{i \in I} M_i$, $x = (x_i)_{i \in I}$ and $y = (y_i)_{i \in I}$ with components $x_i, y_i \in M_i$ for all $i \in I$, then $x + y$ is defined to be the element with*

$$(x + y)_i = x_i + y_i, \quad \forall i \in I.$$

If $r \in R$, then rx is defined to be the element with components

$$(rx)_i = rx_i, \quad \forall i \in I.$$

The submodule of $\prod_{i\in I} M_i$ *consisting of all elements* m *such that* $m_i = 0$ *for all but finitely many components* m_i *is called* the external direct sum *of the modules* $(M_i)_{i\in I}$*, and is denoted by*

$$\bigoplus_{i\in I} M_i.$$

Definition 1.2.6. *If* $(M_i)_{i\in I}$ *is a family of submodules of a given module, we can define a new submodule of* M*, called the* sum *of the family* $(M_i)_{i\in I}$ *of submodules as follows*

$$\sum_{i\in I} M_i = \left\{ \sum_{i\in I} x_i | x_i \in M_i, \forall i \in I, x_i = 0 \, for \; almost \; all \, i \in I \right\}.$$

1.3 Determinant Trick

Definition 1.3.1 (*Kronecker Delta*)**.** *For any index set* J *and ring* R *with identity the symbol* δ_{ij} *denotes*

$$0 \in R \quad if \quad i \neq j$$

and

$$1_R \in R \quad if \quad i = j.$$

Theorem 1.3.2. *Let* M *be a finite* R*-module generated by* n *elements and*

$$\varphi : M \longrightarrow M$$

a homomorphism. Suppose that I *is an ideal of* R *such that* $\varphi(M) \subset IM$*. Then* φ *satisfies a relation of the form*

$$\varphi^n + a_1\varphi^{n-1} + ... + a_{n-1}\varphi + a_n = 0$$

where $a_i \in I^i$ *for* $i = 1, 2, ..., n$*.*

Proof. Let $m_1, m_2, ..., m_n$ be a set of generators of M. Since $\varphi(m_i) \in IM$ we can write

$$\varphi(m_i) = \sum a_{ij} m_j \quad where \quad a_{ij} \in I$$

i.e $\varphi(m_i) = a_{i1}m_1 + a_{i2}m_2 + ... + a_{in}m_n$ where $i = 1, ..., n$. This can also be written as

$$\sum((\delta_{ij}\varphi - a_{ij})m_j) = 0.$$

Now write $\Delta = (\delta_{ij}\varphi - a_{ij})m_j$, i.e.

$$\Delta = \begin{pmatrix} \varphi - a_{11} & -a_{12} & ... & -a_{1n} \\ -a_{21} & \varphi - a_{22} & ... & -a_{2n} \\ ... & ... & ... & ... \\ -a_{n1} & -a_{n2} & ... & \varphi - a_{nn} \end{pmatrix}.$$

Also if we do the calculations we will see that

$$det\Delta = \varphi^n + a_1\varphi^{n-1} + ... + a_{n-1}\varphi + a_n.$$

Let $adj\Delta$ denote the adjoint matrix of Δ. We also know that

$$adj\Delta = \begin{pmatrix} \varphi - a_{11} & -a_{21} & ... & -a_{n1} \\ -a_{21} & \varphi - a_{22} & ... & -a_{n2} \\ ... & ... & ... & ... \\ -a_{1n} & -a_{2n} & ... & \varphi - a_{nn} \end{pmatrix}.$$

Clearly

$$\Delta(adj\Delta) = (det\Delta)m_k = 0, \quad m_k \neq 0, \quad \forall k = 1, ..., n.$$

Therefore $det\Delta = \varphi^n + a_1\varphi^{n-1} + ... + a_{n-1}\varphi + a_n = 0$ □

1.4 Exact Sequences

Suppose that L, M and N are R-modules, and

$$L \overset{\alpha}{\longmapsto} M \overset{\beta}{\longrightarrow} N$$

is a sequence of homomorphisms. It is called exact at M if $\mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$, this means that the composite $\beta o \alpha = 0$, and that α maps surjectively to $\mathrm{Ker}(\beta)$. A longer sequence

$$... \longmapsto M_1 \longmapsto M_2 \longmapsto M_3 \longmapsto ...$$

is exact if it is exact at each term. An exact sequence of the form

$$0 \overset{\alpha_1}{\longmapsto} L \overset{\alpha}{\longmapsto} M \overset{\beta}{\longmapsto} N \overset{\beta_1}{\longmapsto} 0$$

is called *short exact sequence* where $\mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$ and also $\mathrm{Ker}(\alpha) = \mathrm{Im}(\alpha_1) = 0$, i.e. α is a monomorphism and $\mathrm{Ker}(\beta_1) = \mathrm{Im}(\beta) = 0$, i.e. β is an epimorphism. If we have a direct sum $L \oplus N$ then we can construct a short exact sequence in a natural way

$$0 \longmapsto L \overset{\alpha}{\longmapsto} L \oplus N \overset{\beta}{\longmapsto} N \longmapsto 0$$

here α is the inclusion map $\alpha(l) = (l, 0)$ where $l \in L$ and β is the projection $\beta((l, n)) = n$ where $m \in N$.

Chapter 2

NOETHERIAN RINGS AND NOETHERIAN MODULES

2.1 Noetherian Rings

Proposition 2.1.1. *The followings are equivalent*

1)The set of ideals of R has ACC*.*

2)Any non-empty collection of ideals have maximal element.

3)Any ideal of R is finitely generated

Proof. (1)$\Longrightarrow$ (2) Let S be a collection of ideals in R. Now assume $S \neq \emptyset$. Let $I_1 \in S$, if I_1 is maximal with respect to inclusion then I_1 is a maximal element if not then $\exists I_2 \in S$ such that $I_1 \subseteq I_2$. Again if I_2 is maximal then I_2 is a maximal element. If we proceed as such we will have $I_1 \subseteq I_2 \subseteq ....$ But R has ACC so this chain stabilizes after an ideal , say I_N, than this I_N is a maximal element in S.

(2)$\Longrightarrow$(3) Let I be an ideal of R. Consider the set of finitely generated submodules of I, say S. By our assumption S has a maximal element, say I_0. If there is $x \in I \backslash I_0$ then $I_0 + Rx$ is a larger finitely generated ideal so it is an element of S. Then $I_0 \subseteq I_0 + Rx$ but I_0 is a maximal element of S. Therefore $I = I_0$. Thus I is finitely generated.

(3)$\Longrightarrow$(1) Take an increasing chain of ideals

$$I_1 \subseteq I_2 \subseteq ... \subseteq I_m \subseteq ....$$

Let

$$I = \bigcup_{i \in \Lambda} I_i$$

be the union of all ideals in the chain and by *Proposition 1.1.2* I is an ideal of R and so I is finitely generated by our assumption,i.e. $I = (x_1, x_2, ..., x_n)$ for $n \in \mathbb{Z}^+$. And also

$\forall i, \quad i = 1, ..., n$ there is $m_i \in \Lambda$ such that $x_i \in I_{m(i)}$. Now let $m = max\{m_1, ..., m_n\}$, $I_{m(i)} \subseteq I_m \ \forall i = 1, ..., n$ so $x_1, x_2, ..., x_n \in I_m$. That is $I = (x_1, x_2, ..., x_n) \subseteq I_m$ and therefore this chain terminates.

□

Definition 2.1.2 (*Noetherian Ring*)**.** *If the conditions of* Proposition 2.1.1 *hold for a ring R, then R is called* Noetherian ring.

A ring R whose ideals satisfy the descending chain condition(DCC), that is any decreasing chain

$$I_1 \supseteq I_2 \supseteq ... \supseteq I_k \supseteq ...$$

of ideals of R eventually stops, is called *Artinian Ring.* A ring R is called local ring if and only if R has only one maximal ideal. And also A ring R is called local ring if and if all units of R form an ideal.

Proposition 2.1.3. *If M is a finite R-module and $M = IM$ then there exists an element $x \in R$ such that $x \equiv 1 \mod I$ and $xM = 0$*

Proof. Consider the identity homomorphism

$$id_M : M \longrightarrow M$$

$id_M(M) = M = IM$ then by *determinant trick* we have

$$0 = (id_M)^n + a_1(id_M)^{n-1} + ... + a_{n-1}(id_M) + a_n = id_M + a_1 id_M + ... + a_{n-1} id_M + a_n.$$

id_M is the identity element of the set of endomorphisms of M. So we have

$$id_M(1 + a_n + ... + a_1) = 0 \ \ where \ \ a_i \in I$$

Therefore

$$x = a_n + ... + a_1 \equiv 1 \mod I.$$

□

Proposition 2.1.4. *If R is a local ring with the maximal ideal I then every element of $R - I$ is a unit.*

Proof. Let $y \in R - I$ and assume y is not a unit. Clearly (y) is an ideal of R which is different from R. Therefore $I \subset I + (y) \neq R$. But that contradicts with the maximality of I. So y is a unit.

□

Lemma 2.1.5 (*Nakayama Lemma*)**.** *Let R be a local ring with the maximal ideal I and M be a finite module then $M = IM$ implies $M = 0$.*

Proof. From *proposition 2.1.3* there exists an element $x \in R$ such that $x \equiv 1 \mod I$. Also from *Proposition 2.1.4* x is a unit. So there exists y such that $xy = 1$. From *Proposition 2.1.3* $xM = 0$. Therefore

$$M = yxM = xyM = 0.$$

□

Proposition 2.1.6. *Let R be an Artinian local ring. The maximal ideal M is nilpotent.*

Proof. R is a local ring then it has a unique maximal ideal. Say M. Since R is Artinian and M is the unique max ideal, the descending chain

$$M \supseteq M^2 \supseteq ... \supseteq M^k \supseteq ...$$

will eventually stops,i.e. $\exists k \in \mathbb{Z}^+$ such that $M^k = M^{k+1}$. Now assume $M^k \neq 0$ and let $x \in M - M^k$ such that $(x)M^k \neq 0$ where (x) is the ideal generated by x. We have $(x)M^k \neq 0$ and $M^k = M^{k+1}$, so $(x)M^k = (x)M^{k+1}$. That means $(x)M^k = (x)M^kM = (x)MM^k$ and (x) can be considered as a finitely generated R-module then by Nakayama's Lemma $M^k = 0$. □

Proposition 2.1.7. *Let R be a Noetherian ring. Any surjective ring homomorphism*

$$\varphi : R \longrightarrow R$$

is also injective.

Proof. If $a \in \operatorname{Ker}\varphi$ then $\varphi(a) = 0$ and $\varphi(\varphi(a)) = 0$,i.e. $a \in \operatorname{Ker}\varphi^2$. Therefore $\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\varphi_2$. As we proceed that way we will have

$$\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\varphi^2 \subseteq ... \subseteq \operatorname{Ker}\varphi^n \subseteq ....$$

We know R is Noetherian and elements of this chain are ideals of R, so this ascending chain of ideals of R must terminate after finitely many steps. Now assume $\operatorname{Ker}\varphi \neq 0$ and take $a \in \operatorname{Ker}\varphi$. Since φ is onto, we can find $b \in R$ such that $\varphi(b) = a$ then $\varphi^2(b) = \varphi(a) = 0$, i.e. $b \in \operatorname{Ker}\varphi^2$. That means we have a strictly ascending chain $\forall n \in \mathbb{N}$

$$\operatorname{Ker}\varphi \subset \operatorname{Ker}\varphi^2 \subset ... \subset \operatorname{Ker}\varphi^n \subset ....$$

But this contradicts that R is Noetherian. So $a = 0$, i.e. $\operatorname{Ker}\varphi = 0$ □

Theorem 2.1.8 (*Cohen's Theorem*)**.** *If all prime ideals of a ring R are finitely generated then R is a Noetherian ring.*

Proof. Let

$$S = \{I \subseteq R : \ \textit{ideals which are not finitely generated}\}$$

and assume $S \neq \emptyset$. S is partially ordered by inclusion. Let

$$I_1 \subseteq I_2 \subseteq ...$$

be an ascending chain in S and

$$I = \bigcup_{i \in \Lambda} I_i$$

where Λ is any index set. I is an upper bound for S. By *Zorn's Lemma* S has a maximal element, say J. We claim that J is a prime ideal. To prove this claim, let $ab \in J$ such that a, b are not in J. Then $J \subseteq J + a$ and $J \subseteq J + b$. Therefore $J + a$ and $J + b$ are finitely generated then $(J + a)(J + b) = J + ab$ is finitely generated and that means $(J + ab) = J$ is finitely generated, that contradicts with our assumption $S \neq \varnothing$.

□

2.2 Noetherian Modules

An R module M is Noetherian (resp. Artinian) if the submodules of M have the ACC(resp. DCC), that is any increasing chain $M_1 \subset M_2 \subset ... \subset M_k \subset ...$(resp. decreasing chain $M_1 \supset M_2 \supset ... \supset M_k \supset ...$) of submodules eventually stops. Just as before, it is equivalent to say that any non empty set of submodules of M has a maximal element, or that every submodule of M is finite.

Let L, M, N be $R-$modules and

$$0 \longmapsto L \overset{\alpha}{\longmapsto} M \overset{\beta}{\longmapsto} N \longmapsto 0 \quad (*)$$

a short exact sequence of $R-$modules.

Lemma 2.2.1. *We use the above notation* $(*)$*. For submodules* $M_1 \subseteq M_2 \subseteq M$*,*

$$L \cap M_1 = L \cap M_2 \quad \textit{and} \quad \beta(M_1) = \beta(M_2) \Longrightarrow M_1 = M_2.$$

[2]

Proof. If $m \in M_2$ then $\beta(m) \in \beta(M_1) = \beta(M_2)$, so that there is an $n \in M_1$ such that $\beta(m) = \beta(n)$. Then $\beta(m - n) = 0$, so that $m - n \in M_2 \cap \mathrm{Ker}(\beta)$. Hence $m \in M_1$.

□

Proposition 2.2.2. *We use the above notation* $(*)$*. M is Noetherian if and only if L and N are.[2]*

Proof. If M is Noetherian then clearly L and N are Noetherian because ascending chain of submodules in L and N correspond one-to-one to certain ascending chains in M. Now assume L and N are Noetherian we want to show M is Noetherian. Suppose $M_1 \subset M_2 \subset ... \subset M_k \subset ...$ is an increasing chain of submodules of M, then identifying $\alpha(L)$ with L and taking intersection gives a chain

$$L \cap M_1 \subset L \cap M_2 \subset ... \subset L \cap M_k \subset ...$$

of submodules of L and applying β gives

$$\beta M_1 \subset \beta M_2 \subset ... \subset \beta(M_k) \subset ...$$

of submodules of N. Each of these chains eventually stops by the assumption on L and N. Without loss of generality assume $\beta(M_n) = \beta(M_{n+1}) = ...$ and $L \cap M_n = L \cap M_{n+1} = ...$ Therefore by *Lemma 2.2.1*$M_n = M_{n+1} = ...$ i.e., M is Noetherian.

□

Proposition 2.2.3. *If $I_1, ..., I_k$ are ideals such that R/I_i is a Noetherian ring, then $\bigoplus R/I_i$ is a Noetherian R-module. Also if $\cap I_i = 0$ then R is Noetherian.*

Proof. As we mentioned in *Section Exact Sequences* we can construct an exact sequence for $n = 2$ whereR/I_1 and R/I_2 are Noetherian as follows,

$$0 \longrightarrow R/I_1 \longrightarrow R/I_1 \oplus R/I_2 \longrightarrow R/I_2 \longrightarrow 0.$$

From the *Proposition 2.2.2* $R/I_1 \oplus R/I_2$ is Noetherian. By the same way we can construct

$$0 \longrightarrow R/I_1 \oplus R/I_2 \longrightarrow R/I_1 \oplus R/I_2 \oplus R/I_3 \longrightarrow R/I_3 \longrightarrow 0.$$

And as the previous step $R/I_1 \oplus R/I_2 \oplus R/I_3$ is Noetherian. As we proceed that way for k steps where $k \in \mathbb{Z}^+$ we will end up with an exact sequence

$$0 \longrightarrow R/I_1 \oplus ... \oplus R/I_{k-1} \longrightarrow R/I_1 \oplus ... \oplus R/I_{k-1} \oplus R/I_k \longrightarrow R/I_k \longrightarrow 0.$$

Then clearly

$$\bigoplus_{i=1}^{k} R/I_i$$

is Noetherian. Now to prove the next part of the proposition let us define the map φ such that

$$\varphi : R \longrightarrow \bigoplus_{i=1}^{k} R/I_i$$

for any $a \in R$, $\varphi(a) = (I_1 + a, I_2 + a, ..., I_k + a)$. Clearly this is a well-defined module homomorphism. Now consider

$$\text{Ker}(\varphi) = \{a : \varphi(a) = (I_1, ..., I_k)\} = \{a : a \in I_1 \cap I_2 \cap ... \cap I_k\} = 0.$$

That shows our map φ is a one-to-one map. Then there is a one-to-one correspondence with the ideals of R and ideals of $\bigoplus_{i=1}^{k} R/I_i$, since $\bigoplus_{i=1}^{k} R/I_i$ is Noetherian, R is Noetherian.

□

Proposition 2.2.4. *Let R be a Noetherian ring and M be a finite R-module. $\exists$ an exact sequence*

$$R^q \xrightarrow{\alpha} R^p \xrightarrow{\beta} M \longrightarrow 0$$

Proof. M is a finite module. Let the generator set $G_M = \{m_1, ..., m_p\}$ have p many elements where $p \in \mathbb{Z}^+$. Let us define

$$\beta : R^p \longrightarrow M$$

where $\beta((a_1, ..., a_p)) = m_1a_1 + ... + m_pa_p$. Obviously this is a well-defined onto module morphism. Let

$$K = \text{Ker}\,\beta = \{(a_1, ..., a_p) : m_1a_1 + ... + m_pa_p = 0\}.$$

This is a submodule of R^p and so it is a finite module. Assume the generator set G_K of K has q many elements where $q \in \mathbb{Z}^+$, i.e. $G_K = \{k_1, ..., k_q\}$. Define φ such that

$$f : R^q \longrightarrow K$$

such that $\beta((a_1, ..., a_q)) = k_1a_1 + ... + k_qa_q$. Clearly this is a well-defined and onto module homomorphism. So we have

$$R^q \xrightarrow{f} K \xrightarrow{i} R^p \xrightarrow{\beta} M \longrightarrow 0.$$

i is embedding so it is an injection, since K is the kernel of β. Now let $\alpha = i \circ f$,then by construction we can say $\operatorname{Im}\alpha = \operatorname{Ker}\beta$ and therefore

$$R^q \xrightarrow{\alpha} R^p \xrightarrow{\beta} M \longrightarrow 0$$

is an exact sequence.

□

2.3 Hilbert Basis Theorem

Theorem 2.3.1 (*Hilbert Basis Theorem*)**.** *If R is a Noetherian ring then so is the polynomial ring $R[x]$*

Proof. Let I be a non-zero ideal in $R[X]$ and for every positive integer d

$$A_d = \{a_d : a_d x^d + lower \;\; degree \;\; terms \in I\}$$

If for any $a_d, b_d \in A_d$ then $f(x) = a_d x^d + ..., g(x) = b_d x^d + ... \in I$ and since I is an ideal of $R[X]$ we have $f(x) - g(x) \in I$ and $\forall r \in R$, $rf(x) \in I$. Therefore $a_d - b_d \in A_d$ and $\forall r \in R \; ra_d \in A_d$. Clearly A_d is an ideal of R and

$$A_0 \subseteq A_1 \subseteq A_2 \subseteq ....$$

is chain of ideals in R. Let

$$A = \bigcup_{i=0}^{\infty}.$$

A is an ideal of R and A is finitely generated as in *proposition 2.1.1* because R is Noetherian. Assume $A =< \alpha_0, \alpha_1, ..., \alpha_k >$ where $\alpha_i \in R$. Also we know there is $m \in, \mathbb{Z}^+$ such that $\alpha_0, \alpha_1, ..., \alpha_k \in A_m$. Now let $b_{i1}, b_{i2}, ..., b_{in}$ be the generators of A_i for all $i = 1, ..., m$ and f_{ij} be the polynomial of I with leading coefficient b_{ij} and degree i. We claim that

$$I = \langle f_{ij} : i = 0, ..., m \;\; and \;\; j = 0, ..., m \rangle.$$

To prove our claim, let $g(x) \neq 0 \in I$, we will do induction on degree of $g(x)$. If $deg(g(x)) = 0$ then $g(x)$ is constant and so it is an element of A_0, therefore $g(x) \in R$.

By induction hypothesis assume the result holds for polynomials in I with degree less than degree of $g(x)$. Now let $deg(g(x)) = t$ where $t \geq 1$,

Case(1): $t \leq m$

Let

$$g(x) = c_t x^t + ...; \quad c_t \in A_t \quad so \quad c_t = \beta_1 b_{t1} + ... + \beta_{n_t} b_{tn_t}$$

where b_{ti} generators of A_t and $\beta_i \in R$. Then form

$$h(x) = \beta_1 f_{t1} + \beta_2 f_{t2} + ... + \beta_{n_t} f_{tn_t}$$

$h(x)$ and $g(x)$ have the same leading coefficients so

$$g(x) - (\beta_1 f_{t1} + \beta_2 f_{t2} + ... + \beta_{n_t} f_{tn_t})$$

has degree less than $deg(g((x))$. So by induction it belongs to the ideal generated by f_{ij}.

Case(2): $t > m, \quad t - m > 0$

Let $g(x) = c_t x^t + ...; \quad c_t \in A_t = A_m$ since $t > m$ and R is Noetherian,i.e $A_1 \subseteq A_2 \subseteq A_3 \subseteq .... \subseteq A_t = A_{t+1} = ... = A_m = ...$ so $\exists i = 1, ..., n_m$ such that

$$c_t = \beta_1 b_{m1} + ... + \beta_{n_m} b_{mn_m}.$$

Then form

$$h(x) = (\beta_1 f_{m1} + \beta_2 f_{m2} + ... + \beta_{n_m} f_{mn_m}) x^{t-m}.$$

The leading coefficient of h and g are the same so $deg(g - h) < deg(g)$. So it can be written as a linear combination of f_{ij}.

□

The trivial examples for Noetherian Rings are $, \mathbb{Z}$ and fields. As an example for rings which are not Noetherian, we can consider the ring R of polynomials in x, y such that

$$R = F[x, xy, xy^2, ...]$$

where F is a field. Clearly $I = (x, xy, xy^2, ...)$ is an ideal of R which is not finitely generated. To prove this claim assume I is finitely generated. Let $G = \{a_1, a_2, ..., a_n\}$ where $n \in \mathbb{Z}^+$ be the finite generator set of R. $\forall a_i \in G$ $a_i = xy^{\alpha i}$ for some $\alpha i \in \mathbb{Z}^+$ and also $\forall a \in R$, $a = xy^m$ for some $m \in \mathbb{Z}^+$ and $xy^m = r_1xy^{\alpha 1} + r_2xy^{\alpha 2} + r_3xy^{\alpha 3} + ... + r_nxy^{\alpha n}$ $\forall r_i \in F[x, xy, xy^2, ...]$. So $r_i's$ are of the form xy^{ki} $ki \in \mathbb{Z}^+$. Then $\forall m \in \mathbb{Z}^+$

$$r_1xy^{\alpha 1} + r_2xy^{\alpha 2} + r_3xy^{\alpha 3} + ... + r_nxy^{\alpha n} = x^2y^{\alpha 1+k1} + x^2y^{\alpha 2+k2} + x^2y^{\alpha 3+k3} + ... + x^ny^{\alpha n+kn} \neq xy^m.$$

That means G is not finite.

A subring of a Noetherian ring does not have to be Noetherian. As an example consider

$$C[x, xy, xy^2, xy^3, ...] \subseteq C[x, y].$$

$C[x, y]$ is Noetherian by *Hilbert Basis Theorem* since C is Noetherian so by *Hilbert Basis Theorem* $C[x]$ is Noetherian and again by *Hilbert Basis Theorem* $C[x, y]$ is Noetherian. But $C[x, xy, xy^2, xy^3, ...]$ is not a Noetherian ring because $(x, xy, xy^2, xy^3, ...)$ is an ideal of $C[x, xy, xy^2, xy^3, ...]$ which is not finitely generated.

Chapter 3

INTEGRAL EXTENSIONS AND HILBERT'S NULLSTELLENSATZ

3.1 Finite and Integral R-algebra

An R- algebra A is by definition a ring A with a given ring homomorphism

$$\varphi : R \longrightarrow A.$$

The point is that A is then a R-module, with the multiplication defined by

$$\varphi(a).b$$

where $a \in R, \quad b \in A$. An important case of this is when $R \subset A$, A is also called an *extension ring* of R, we can usually reduce to this case by writing

$$\varphi(R) = R' \subset A.$$

A is a finite R-algebra(or finite over R) if it is finite as a R-module. An element $a \in A$ is integral over R if there exists a monic polynomial $f(x) = x^n + r_{n-1}x^{n-1} + ... + r_0 \in R'[x]$ such that

$$(1) \quad f(a) = a^n + r_{n-1}a^{n-1} + ... + r_0 = 0.$$

The algebra A is integral over R if every $a \in A$ is integral. In terms of A viewed as a R-module, the integral dependence relation (1) is a linear relation

$$a^n + r_{n-1}a^{n-1} + ... + r_0 = 0$$

between the powers of a, with coefficients in R, and such that the highest power a^n has coefficient 1. [2]

Proposition 3.1.1. *If $\varphi : R \longrightarrow A$ and A is an R-algebra, and $a \in A$, then there are three equivalent conditions:*

(i) a is integral over R.

(ii)The subring $R'[a] \subset A$ generated by $R' = \varphi(R)$ and a is finite over A.

(iii)There exists an R-subalgebra $C \subset A$ such that $R'[a] \subset C$ and C is finite over R.[2]

Proof. $(i) \Longrightarrow (ii)$ If a is integral over R then there is a polynomial $f(x) = x^n + r_{n-1}x^{n-1} + ... + r_0$ in $R[x]$ such that

$$f(a) = a^n + r_{n-1}a^{n-1} + ... + r_0 = 0.$$

Now by induction assume proposition holds for polynomial with degree smaller than n. It can be written as a linear combination of a^i where $i = 1, ..., n$. Take a polynomial $g \in R'[x]$ with degree m. If $m < n$ by induction hypothesis this polynomial can be generated by $1, a, ..., a^n$. Now assume $m > n$, $g(x) = b_m x^m + b_{m-1}x^{m-1} + ... + b_0$. $f(x)$ is a monic polynomial multiply $f(x)$ by $b_m x^{m-n}$ then we get

$$h(x) = g(x) - b_m x^{m-n} f(x).$$

The degree of $h(x)$ is smaller than n. So $h(x)$ can be written as a linear combination a^i, where $i = 1, ..., n$, and also

$$g(a) - b_m a^{m-n} f(a) = h(a)$$

i.e $g(a) = h(a)$ so $g(x)$ can be written as a linear combination of a^i, where $i = 1, ..., n$.

$(ii) \Longrightarrow (iii)$ is clear.

$(iii) \Longrightarrow (i)$ Consider the R-module homomorphism

$$f = \mu_a : C \longrightarrow C$$

defined by multiplication by a. Then C is a finite R-module. We can apply the *Determinant Trick* to f. This gives a relation

$$f^n + r_{n-1}f^{n-1} + ... + r_0 = 0.$$

Also $f^i(1) = a.a...a.1(i \ \ times) = a^i$, which is what we wanted. □

3.2 Radicals and Affine Algebraic Sets

Definition 3.2.1. *For a positive integer n we define the affine n-space*

$$\mathbb{A}^n = \{(a_1, a_2, ..., a_n) : a_i \in k, i = 1, ..., n\}.$$

[4]

A polynomial $f \in k[x_1, ..., x_n]$ determines a function f,

$$f : \mathbb{A}^n \longrightarrow k$$

$$(a_1, ..., a_n) \longrightarrow f(a_1, ..., a_n)$$

where $(a_1, ..., a_n) \in \mathbb{A}^n$. This function is called evaluation. There are two ways, f can be viewed as a polynomial and also a k-valued function on $\mathbb{A}^n$. $f \in k[x_1, ..., x_n]$ we define $V(f)$ to be the set of solutions of the equation $f = 0$, i.e.,

$$\mathbf{V}(f) = \{(a_1, ..., a_n) \in \mathbb{A}^n : f(a_1, ..., a_n) = 0\} \subseteq \mathbb{A}^n.$$

$\mathbf{V}(f)$ is called the variety defined by f. This evaluation function gives a ring of k-valued functions on $\mathbb{A}^n$ denoted by $k[\mathbb{A}^n]$ and called the coordinate ring of $\mathbb{A}^n$. Also for any set $S \subseteq k[\mathbb{A}^n]$,

$$\mathbf{V}(S) = \{(a_1, ..., a_n) \in \mathbb{A}^n : f(a_1, ..., a_n) = 0 for all f \in S\}.$$

Obviously $\mathbf{V}(\emptyset) = \mathbb{A}^n$.

Definition 3.2.2. *A subset V of $\mathbb{A}^n$ is called an affine algebraic set, if V is the set of common zeros of some set S of polynomials, i.e., if $V = \boldsymbol{V}(S)$ for some $S \subseteq k[\mathbb{A}^n]$. $V = V(S)$ is called the locus of S in $\mathbb{A}^n$.*

The one point subsets of $\mathbb{A}^n$ for any n are algebraic since $\{(a_1, ..., a_n)\}$ is $\mathbf{V}(x_1 - a_1, ..., x_n - a_n)$. More generally any finite subset of $\mathbb{A}^n$ is an affine algebraic set.

Proposition 3.2.3. *$\boldsymbol{V}(S) = \boldsymbol{V}(I)$ where $I = (S)$ is the ideal in $k[\mathbb{A}^n]$ generated by the subset S.*

Proof. $(a_1, ..., a_n) \in \mathbf{V}(S)$ if and only if $f_i(a_1, ..., a_n) = 0$ for all $f_i \in S$ if and only if $g_i(a_1, ..., a_n) = 0$ where $g_i = \sum f_i h_i$ $g_i \in I$ and $h_i (\neq 0) \in k[k^n]$ if and only if $(a_1, ..., a_n) \in V(I)$.

□

Proposition 3.2.3 shows that, every affine algebraic set corresponding to an ideal of the coordinate ring,

$$\mathbf{V} : \{ideals \ \ of \ \ k[\mathbb{A}^n]\} \longrightarrow \{affine \ \ algebraic \ \ sets \ \ in \ \ A^n\}$$

While the ideal I where $V = \mathbf{V}(I)$ is not unique(for example, in affine 2-space over $\mathbb{R}$, y-axis is the locus of the ideal (x) of $\mathbb{R}[x, y]$ also is the locus of $(x^2), (x^3)$,...,etc.), there is a unique largest ideal that determines V, given by the set of polynomials that vanish on V. For any subset $S \subseteq s^n$

$$\mathbf{I}(S) = \{f \in k[x_1, ..., x_n] : f(a_1, ..., a_n) = 0 \ \ for \ \ all (a_1, ..., a_n) \in \mathbb{A}^n\}$$

Clearly $\mathbf{I}(S)$ is an ideal and is the unique largest ideal of functions that are identically zero on S. So there is a correspondence

$$\mathbf{I} : \{subsets \ \ in \ \ \mathbb{A}^n\} \longrightarrow \{ideals \ \ of \ \ k[\mathbb{A}^n]\}.$$

Example 3.2.4. *Define φ;*

$$\varphi : k[x_1, ..., x_n] \longrightarrow k$$

$$f_i(x_1, ..., x_n) \longrightarrow f_i(a_1, ..., a_n)$$

where $(a_1, ..., a_n) \in k^n$. Clearly φ is a well-defined surjective ring homomorphism. By The Fundamental Theorem For Isomorphism For Rings $\varphi(k[x_1, ..., x_n])/\operatorname{Ker}(\varphi) \cong k$. *Therefore* $\operatorname{Ker}(\varphi)$ *is the maximal ideal. Clearly*

$$\operatorname{Ker}(\varphi) \supseteq \boldsymbol{I}((a_1, ..., a_n)) = (x_1 - a_1, ..., x_n - a_n).$$

Now let $f \in \operatorname{Ker} \varphi$ and if f is not an element of $\boldsymbol{I}((a_1, ..., a_n))$ then we can write

$$f = h_1(x_1 - a_1) + ... + h_n(x_n - a_n) + q(x_1, ..., x_n)$$

where $q(x_1, ..., x_n), h_i \in k[x_1, ..., x_n]$ $i = 1, ..., n$ *and* q *is not divisible by* $(x_i - a_i)$ $i = 1, ..., n$. *Obviously* $q(a_1, ..., a_n) = 0$ *i.e,* $q \in \operatorname{Ker}\varphi$. *Also* $deg(q) < deg((x_i - a_i)) = 1$. *Hence* $q \in k$. *Since* $q \in \operatorname{Ker}\varphi$ *and* $q \in k$ $q = 0$.

Definition 3.2.5. *Let* I *be an ideal in a commutative ring* R.

1)The radical *of* I *denoted* $radI$, *is the ideal* $\cap P$, *where the intersection is taken over all prime ideals* P *which contains* I. *If the set of prime ideals containing* I *is empty, then* $radI$ *is defined to be* R.

2) The radical of the zero ideal is called the nilradical *of* R.

3) An ideal is called a radical ideal if $I = radI$.

Example 3.2.6. *In any integral domain the zero ideal is prime, hence* $rad0 = 0$. *In the ring* $\mathbb{Z}$, $Rad(12) = (2) \cap (3)$ *and also* $rad(4) = rad(32) = (2)$.

Proposition 3.2.7. *If* I *is an ideal in* R, *then*

$$radI = \{r \in R : r^n \in I \quad for \quad some \quad n > 0\}.$$

Proof. If $radI = R$ then $\{r \in R : r^n \in I\} \subseteq radI$. Now assume this is not the case. If $r^n \in I$ and P is any prime ideal containing I, then $r^n \in P$. Since P is a prime ideal $r \in P$. Therefore $\{r \in R : r^n \in I\} \subseteq radI$. Conversely if $t \in R$ and t^n is not an element of I for all $n > 0$, then $S = \{t^n + x : x \in I\}$ is a multiplicative set such that $S \cap I = \emptyset$. By *Proposition 1.1.6* there is a prime ideal P disjoint from S that contains I. By construction t is not in P and hence is not an element of $radI$. Thus $radI \subseteq \{r \in R : r^n \in I\}$. □

If a is in the nilradical of R then some power of a is 0, so the nilradical of R is the set of all nilpotent elements of R.

Proposition 3.2.8. *Let* I *be an ideal in* R. R/I *has no nilpotent elements if and only if* $I = radI$.

Proof. It is clear that $I \subseteq radI$. As we mentioned before nilradical of R is the set of nilpotent elements. If x is any element from the nilradical of R/I, then $x = I + r$ where $r \in R$ and $x^n = I + r^n = I$ for some $n > 0$, i.e., $r^n \in I$. Thus $r \in radI$. Therefore R/I has no nilpotent elements if and only if there exists no $r \in R - I$ such that $r^n \in I$, i.e., there exists no $r \in radI$. Thus $I = radI$. □

The elements of the ring $k[k^n]/\mathbf{I}(V)$ give k-valued functions on V and since k has no nilpotent elements, powers of non-zero functions are also non-zero functions. Therefore $k[k^n]/\mathbf{I}(V)$ has no nilpotent elements and by the *Proposition 3.2.8* $\mathbf{I}(V) = rad(\mathbf{I}(V))$.

3.3 Noether Normalisation

Definition 3.3.1. *Let A be a k-algebra. Elements $a_1, ..., a_n \in A$ are algebraically independent over k if the natural surjection $k[x_1, ..., x_n] \longrightarrow k[a_1, ..., a_n]$ is an isomorphism, where the left-hand side is the polynomial ring. This just means that there are no non-zero polynomial relations $F(a_1, ..., a_n) = 0$ with coefficients in k.[2]*

Theorem 3.3.2. *Suppose that $A = k[r_1, ..., r_m]$ is a finitely generated $k-$algebra. Then for some q, $0 \leq q \leq m$, there are algebraically independent elements $y_1, ..., y_q \in A$ such that A is integral over $k[y_1, ..., y_q]$ [4]*

Proof. We will do induction on m. If $r_1, ..., r_m$ are algebraically independent over k then take $y_i = r_i$, $i = 1, ..., m$. Otherwise, there exists $f(x_1, ..., x_m) \in k[x_1, ..., k_m]$ such that $f(r_1, ..., r_m) = 0$. The polynomial f is a sum of monomials of the form $ax_1^{e_1}...x_m^{e_m}$, where the degree of this monomial is $e_1 + ... + e_m$ and the degree, d, of f is maximum of the degrees of its monomials. Renumbering the variables if necessary, we say assume that f is a nonconstant polynomial in x_m with coefficients in the ring $k[x_1, ..., x_{m-1}]$. Now we will perform a change of variables that transforms (or normalizes) f into a monic polynomial in x_m with coefficients from a subring of A which is generated over k by $m - 1$ elements, at which point we shall be apply induction.

Define integers $\alpha_i = (1+d)^i$ and new variables $X_i = x_i - x_m^{\alpha_i}$ for $1 \leq i \leq m-1$. Let

$$g(X_1, ..., X_{m-1}, x_m) = f(X_1 x_m^{\alpha_1} +, ..., X_{m-1} + x_m^{\alpha_{m-1}}, x_m)$$

so $g \in k[X_1, ..., X_{m-1}, x_m]$. Each monomial term of f contributes a single term of the form a constant times x_m^e to g. Also the choice of α_i ensures that distinct monomials in f give different values of e. If N is the highest power of x_m that occurs, then it follows that

$$g = cx_m^N + \sum_{i=0}^{N-1} h_i(X_1, ..., X_{m-1}) x_m^i$$

for some non-zero $c \in k$. If now $s_i = r_i - r_m^{\alpha_i}$ then

$$\frac{1}{c} g(s_1, ..., s_{m-1}, r_m) = \frac{1}{c} f(r_1, ..., r_{m-1}, r_m) = 0,$$

which shows that r_m is integral over $B = k[s_1, ..., s_{m-1}]$. Each r_i for $1 \leq i \leq m-1$ is integral over $B[r_m]$ since r_i is a root of the monic polynomials $x - s_i - r_m^{\alpha_i}$, so A is integral over $B[r_m]$. By transitivity of integrality, A is integral over B. Since B is a $k-$algebra generated by $m-1$ elements, induction completes the proof.

□

Proposition 3.3.3. *If R is an integral domain and i, j are relatively prime integers then, the ideal $(x^i - y^j)$ is a prime ideal.*

Proof. Define

$$\varphi : R[x, y] \longrightarrow R[t]$$

$$x \longrightarrow t^j$$

$$y \longrightarrow t^i$$

where $i, j \in \mathbb{Z}^+$. Clearly φ is a well-defined ring homomorphism and $(x^i - y^j) \subseteq \mathrm{Ker}(\varphi)$ since $x^i - y^j \in \mathrm{Ker}(\varphi)$. Pick $g \in \mathrm{Ker}(\varphi)$, clearly $g \in R[x, y]$ so it can be

written as

$$g = f(x,y)(x^i - y^j) + h(x,y)$$

where $h(x,y) \in R[x,y]$ and $f(x,y) \in R[x,y]$. $h(x,y)$ is a polynomial of the form

$$h(x,y) = c_1 x^r y^s + ...$$

where $0 \leq s < j$. Now we want to show $h(x,y) = 0$. $g \in \mathrm{Ker}(\varphi)$ so $\varphi(g) = 0$. Clearly $\varphi(h(x,y)) = 0$. That is

$$\varphi(h(x,y)) = \varphi(c_1 x^{r_1} y^{s_1} + c_2 x^{r_2} y^{s_2} + c_3 x^{r_3} y^{s_3} + ...) = c_1 t^{r_1 j + s_1 i} + c_2 t^{r_2 j + s_2 i} + ... = 0.$$

Now without loss of generality we may assume$(r_m - r_n > 0)$. Also assume that the exponents are not distinct,i.e.

$$r_m j + s_m i = r_n j + s_n i$$

where $m, n \in \mathbb{Z}^+$. Therefore we obtain,

$$(r_m - r_n) = i(s_n - s_m)/j.$$

By our assumption we have $(i,j) = 1$, $j \mid (s_n - s_m)$ and $s_n - s_m > 0$. But we know that $s_n - s_m < j$. That shows our assumption is not correct, i.e. all the exponents are distinct. Therefore $h(x,y) = 0$. That is $g \in (x^i - y^j)$ so $\mathrm{Ker}(\varphi) = (x^i - y^j)$. Now we want to show that $(x^i - y^j)$ is a prime ideal. By the first isomorphism theorem we have

$$R[x,y]/\mathrm{Ker}(\varphi) \cong \varphi(R[x,y]) \subseteq R[t].$$

By our assumption we know that R is an integral domain so R[t] is an integral domain and also $\varphi(R[x,y])$ is a subring of $R[t]$ so it is an integral domain,too. That shows $\mathrm{Ker}(\varphi) = (x^i - y^j)$ is a prime ideal.

□

Example 3.3.4. *Consider* $R = k[x,y]/(y^3 - x^5)$, $(3,5) = 1$ *so by* Proposition 3.3.3 R *is an integral domain.*

Example 3.3.5. *Consider* $R = k[x, y]/(y^5 - x^{19})$, $(5, 19) = 1$ *so by* Proposition 3.3.3 R *is an integral domain.*

Proposition 3.3.6. *The ring* $R = k[x, y]/(y^2 - x^3)$ *is not normal and its field of fractions,* $FracR = k(t)$ *where* $t = y/x$.

Proof. $(2, 3) = 1$ so by *Proposition 3.3.3* $(y^2 - x^3)$ is a prime ideal so $k[x, y]/(y^2 - x^3)$ is an integral domain. $t = y/x$ and t is integral over R since

$$(y/x)^3 - y = 0.$$

And also for $x \in R$, $x = t^2$ so $x \in k[t]$. By the same way $y \in R$, $y = t^3$ and so $y \in k[t]$. Therefore $R \subseteq k[t]$. Since t is integral over R, $k[t]$ is integral over R. We have $R \subseteq k[t]$ and clearly $Frack[t] = k(t)$ and so $R \subseteq k(t)$. Also $y/x = t \in FracR$ and by definition of $FracR$, $k(t) = FracR$. Obviously $t \in k[t]$ but t is not in R so R is not integrally closed.

□

Proposition 3.3.7. $k[x, y]/(y^2 - x^2 - x^3)$ *is an integral domain.*

Proof. Let $t = y/x$. Define

$$\varphi : k[x, y] \longrightarrow k[t]$$

$$x \longrightarrow t^2 - 1$$

$$y \longrightarrow t(t^2 - 1)$$

Our first aim is the show that $\mathrm{Ker}(\varphi) = (y^2 - x^2 - x^3)$. If we prove that then as in the *Proposition 3.3.3* this will show $k[x, y]/(y^2 - x^2 - x^3)$ is an integral domain. Clearly $(y^2 - x^2 - x^3) \subseteq \mathrm{Ker}(\varphi)$. To show $(y^2 - x^2 - x^3) \supseteq \mathrm{Ker}(\varphi)$, pick $g \in \mathrm{Ker}(\varphi)$. Let $g = f(x, y)(y^2 - x^2 - x^3 + h(x, y)$ where $f, g \in k[x, y]$ where

$$h(x, y) = c_1 x^{r_1} y^{s_1} + c_2 x^{r_2} y^{s_2} + c_3 x^{r_3} y^{s_3} 4...$$

and $\forall i \in \mathbb{N}, s_i < 2$. Obviously $\varphi(h(x, y)) = 0$.

$$\varphi(h(x, y)) = \varphi(c_1 x^{r_1} y^{s_1} + c_2 x^{r_2} y^{s_2} + c_3 x^{r_3} y^{s_3} 4...) = 0$$

$$\varphi(h(x,y)) = c_1 t^{3s_1+2s_1r_1} + c_2 t^{3s_2+2s_2r_2} + c_3 t^{3s_3+2s_3r_3} + ... = 0$$

Now assume

$$3s_i + 2s_i r_i = 3s_j + 2s_j r_j \ \ where \ \ i \neq j \ \ and \ \ i, j \in \mathbb{N}.$$

Therefore

$$s_i - s_j/(s_j r_j - s_i r_i) = 2/3.$$

But we know that $s_i > 2$ so $s_i - s_j = 0$ *or* $s_i - s_j = 1$. Clearly $s_i - s_j \neq 0$ but $s_j r_j - s_i r_i$ is an integer and so $s_i - s_j = 1 \neq 1$. That shows our assumption is not correct. That means all the exponents are distinct. So $h(x,y) = 0$ and $g \in (y^2 - x^2 - x^3)$.

□

Proposition 3.3.8. *If $R = k[x,y]/(y^2 - x^2 - x^3)$, then normalization of R is $k(t)$ where $t = y/x$.*

Proof. From the *Proposition 3.3.7* we know that $k[x,y]/(y^2 - x^2 - x^3)$ is an integral domain. If $x \in R$ then $x = t^2 - 1$ so $x \in k[t]$ and by the same way $y \in R$ then $y = t(t^2 - 1)$ so $y \in k[t]$. Therefore $R \in k[t]$. Also t is integral over R $((y/x)^3 - (y/x) - y = 0)$ which also means $k[t]$ er is integral over R. So as in *Proposition 3.3.6* $FracR = k(t)$. □

3.4 Hilbert's Nullstellensatz

Proposition 3.4.1. *Let R be a subring of the integral domain S and S be integral over R. Then R is a field if and only if S is a field. [4]*

Proof. Assume R is a field and let s be a nonzero element of S. The element s is integral over R, so

$$s^n + a_{n-1}s^{n-1} + ... + a_1 s + a_0 = 0$$

for some $a_0, ..., a_{n-1} \in R$. We may assume $a_0 \neq 0$ since S is an integral domain. Then

$$s(s^{n-1} + a_{n-1}s^{n-2} + ... + a_1) = -a_0$$

and $-1/a_0 \in R$. Therefore we can find an inverse of $s \in S$, so S is a field. Conversely, suppose S is a field and r is a nonzero element of R. S is integral over R, thus $r^{-1} \in S$ and,

$$r^{-m} + a_{m-1}r^{1-m} + ... + a_1 r^{-1} + a_0 = 0$$

for some $a_0, ..., a_{n-1} \in R$. Then $r^{-1} = a^{m-1} + ... + a_1 r^{m-2} + a_0 r^{m-1} \in R$, so R is a field. □

Proposition 3.4.2 (*Lying Over*)**.** *Let R be a subring of S and S be integral over R. If P is a prime ideal in R then there is a prime ideal Q in S with $P = Q \cap R$. Moreover, P is maximal if and only if Q is maximal. [1]*

Proof. P is a prime ideal so by *Example 1.1.5* $R - P$ is a multiplicative subset of R and hence multiplicative subset of S. 0 is not an element of $R - P$. By *Proposition 1.1.6* there is an ideal Q of S that is maximal in the set of ideals I of S such that $I \cap (R - P) = \emptyset$ and that Q is prime in S. Thus $Q \cap (R - P) = \emptyset$, i.e., $Q \cap R \subseteq P$. If $Q \cap R \neq P$, choose $u \in P$ such that u is not in Q, then the ideal $Q + (u) \subseteq S$ and $Q \subseteq Q + (u)$. Since Q is the maximal ideal of S that satisfies $Q \cap (R - P) = \emptyset$ then $\exists c \in (Q + (u)) \cap (R - P) \neq \emptyset$, $c = q + su$ where $q \in Q$ *and* $s \in S$. S is integral over R so $\exists a_i \in R, i = 1, ..., n-1$ such that

$$s^n + a_{n-1}s^{n-1} + ... + a_1 s + a_0 = 0$$

multiplying by u^n,

$$(su)^n + a_{n-1}u(su)^{n-1} + ... + a_1 u^{n-1} su + a_0 u^n = 0$$

$su = c - q$,

$$(c-q)^n + a_{n-1}u(c-q)^{n-1} + ... + a_1 u^{n-1}(c-q) + a_0 u^n = 0$$

$$v = (c)^n + a_{n-1}u(c)^{n-1} + ... + a_1 u^{n-1} c + a_0 u^n \in Q$$

Also $v \in R$ and hence $v \in R \cap Q \subseteq P$. But $u \in P$ and $v \in P$ implies $c^n \in P$. P is prime therefore $c \in P$ but that is a contradiction so $P = Q \cap R$. For the second

part of the statement, S/Q is integral extension of R/P. By *proposition 3.4.1* S/Q is a field if and only if R/P is a field, i.e., Q is a maximal ideal if and only if P is a maximal ideal.

□

Theorem 3.4.3 (*Hilbert's Nullstellensatz-Weak Form*)**.** *Let k be an algebraically closed field. Then M is a maximal ideal in the polynomial ring $k[x_1, ..., x_n]$ if and only if $M = (x_1 - a_1, ..., x_n - a_n)$ for some $a_1, ..., a_n \in k$. Equivalently the maps $\boldsymbol{V}$ and $\boldsymbol{I}$ give bijective correspondence*

$$\{points \in \mathbb{A}^n\} \leftrightarrows \{maximal \ ideals \ in \ k[\mathbb{A}^n]\}.$$

Moreover, If I is any proper ideal in $k[x_1, ..., x_n]$, then $\boldsymbol{V}(I) \neq \emptyset$. [4]

Proof. Clearly $(x_1 - a_1, ..., x_n - a_n)$ is a maximal ideal in $k[x_1, ..., x_n]$. (see*Example 3.2.4*) For the converse, for any maximal ideal M in $k[x_1, ..., x_n]$, let $E = k[x_1, ..., x_n]/M$. Then E is a finitely generated field over k. By *Noether Normalization Lemma*, E is integral over a polynomial ring $k[z_1, ..., z_m]$. By *Proposition 3.4.1* $k[z_1, ..., z_q]$ is a field since E is a field but this can only happen when $q = 0$. Since E is integral over k, E is algebraic over k but k algebraically closed. Therefore $E = k$. Hence for i $= 1, ...,$ n there is some $a_i \in k$ such that $x_i - a_i \in M$, i.e., the maximal ideal $(x_1 - a_1, ..., x_n - a_n) \in M$. Thus $M = (x_1 - a_1, ..., x_n - a_n)$. Finally if I is any nonzero ideal in $k[x_1, ..., x_n]$ then it is contained in a maximal ideal $M = (x_1 - a_1, ..., x_n - a_n)$ and so $(a_1, ..., a_n) \in \mathbf{V}(I)$ □

Theorem 3.4.4 (*Hilbert's Nullstellensatz*)**.** *Let k be an algebraically closed field. Then is $I(V(I)) = radI$ for every ideal I in the polynomial ring $k[x_1, ..., x_n]$. Moreover the maps $\boldsymbol{V}$ and $\boldsymbol{I}$ give bijective correspondence*

$$\{affine \ \ algebraic \ \ sets\} \leftrightarrows \{radical \ \ ideals\}.$$

Moreover, If I is any proper ideal in $k[x_1, ..., x_n]$, then $\boldsymbol{V}(I) \neq \emptyset$.[4]

Proof. Clearly $radI \subseteq \mathbf{I}(\mathbf{V}(I))$(see *Example 3.2.4*). For the converse, By *Hilbert Basis Theorem* $I = (f_1, ..., f_m)$. Let $g \in \mathbf{I}(\mathbf{V}(I))$. Introduce a new variable x_{n+1} such that $k[x_1, ..., x_n, x_{n+1}]$, and consider the ideal I' generated by $f_1, ..., f_m$ and $x_{n+1}g - 1$. At any point of $\mathbb{A}^{n+1}$ where $f_1, ..., f_m$ vanish the polynomial $g \in \mathbf{I}(\mathbf{V}(I))$ also vanishes, so that $x_{n+1}g - 1$ is non zero. Hence $\mathbf{V}(I') = \emptyset$ in $\mathbb{A}^{n+1}$. By the *Weak Form of the Nullstellensatz* I' can not be a proper ideal, i.e., $1 \in I'$. Therefore, for some $a_i \in k[x_1, ..., x_n, x_{n+1}]$

$$1 = a_1 f_1 + ... + a_m f_m + a_{m+1}(x_{n+1}g - 1).$$

Let $y = 1/x_{n+1}$ and multiply the equation by y^N.

$$y^N = c_1 f_1 + ... + c_m f_m + c_{m+1}(g - y)$$

for some $c_i \in k[x_1, ..., x_n, y$. If we substitute g for y, the polynomial equation will show that $g^N \in I$ i.e., $g \in radI$. Thus $radI = \mathbf{I}(\mathbf{V}(I))$. □

if S is an integral extension of R with $1 \in R$ and if I is an ideal of R, then

$$(rad_S IS) \cap R = rad_R I$$

where IS is the ideal generated by I and S and the subscript indicates the ring in which radicals are computed. To see it, let P_i be any ideal that contains I in R. By *proposition 3.4.2* there is a prime ideal that contains I in S such that $Q_i \cap R = P_i$. if we take intersection of all prime ideals in R and S which satisfies $Q_i \cap R = P_i$ we will end up with $\cap Q_i \bigcap R = \cap P_i = rad_R I$. Clearly, $I \subseteq \cap Q_i$, hence $I \in Q_i \forall i$. Q_i are ideals of S so for any $g \in S$, $gI \in Q_i$, i.e., for every i, $IS \in Q_i$. Therefore $IS \subseteq \cap Q_i = rad_S(IS) \cap R = rad_R I$.

Proposition 3.4.5 (*Hilbert's Nullstellensatz For The Varieties*)**.** *If k is any field with algebraic closure $\bar{k}$ and I is the ideal in $k[x_1, ..., x_n]$, then $\boldsymbol{I}_k(\boldsymbol{V}_{\bar{k}}(I)) = radI$ where $\boldsymbol{V}_{\bar{k}}(I)$ is the zero set in $\bar{k}$ of the polynomials in I and $\boldsymbol{I}_k(\boldsymbol{V}_{\bar{k}}(I))$ is the ideal of polynomials $k[x_1, ..., x_n]$ vanishing at all points in $\boldsymbol{V}_{\bar{k}}(I)$. In particular, $I = (1)$ if and only if there are no common zeros in $\bar{k}^n$ of the polynomials in I.*

Proof. Let $R = k[x_1, ..., x_n]$ and $S = \bar{k}[x_1, ..., x_n]$. Clearly S is an integral extension of R and I is an ideal of R where $1 \in R$. So by previous remark we can say $rad_S(IS) \cap R = rad_R I$. Also by *Hilbert Nullstellensatz* $\mathbf{I}_{\bar{k}}(\mathbf{V}_{\bar{k}}(IS)) = rad_S(IS)$. Therefore

$$\mathbf{I}_k(\mathbf{V}_{\bar{k}}(I)) = \mathbf{I}_k(\mathbf{V}_{\bar{k}}(IS)) \cap R = rad_S(IS) \cap R = rad_R I.$$

For the second part, by *Hilbert Nullstellensatz* if $I = (1)$ then, $\mathbf{V}_{\bar{k}}(I) = \emptyset$. Now we want to show if $\mathbf{V}_{\bar{k}}(I) = \emptyset$ then, $I = (1)$. From *Hilbert Nullstellensatz* if $\mathbf{V}_{\bar{k}}(I) = \emptyset$ then, $IS = (1)$. Now assume I is not a proper ideal of R. I is contained in a prime ideal i.e., $I \subseteq P$. By *Proposition 3.4.2* there exists a proper prime ideal in S such that $IS \in Q$. But that contradicts with $1 \in IS$. Therefore $I = (1)$. □

Chapter 4

GRÖBNER BASIS

4.1 Monomials

A non-zero polynomial in $x_1, x_2, ..., x_n$ with coefficients in R is a finite sum of non-zero monomial terms i.e., a finite sum elements of the form

$$ax_1^{\alpha_1}x_2^{\alpha_1}...x_n^{\alpha_n}$$

$a \in R$ and α_i non-negative integers. A monic term $x_1^{\alpha_1}x_2^{\alpha_2}...x_n^{\alpha_n}$ is simply the monomial part of the term. The exponent α_i is called the degree in x_i of the term and the sum $\alpha = (\alpha_1 + ... + \alpha_n)$ is called the *degree* of the term. The ordered $n-$tuple $(\alpha_1, ..., \alpha_n)$ is the *multidegree* of the term.

4.1.1 Monomial Ordering

Definition 4.1.1. *A monomial ordering is a well ordering "$\leqslant$" on the set of monomials that satisfies $mm_1 \geqslant mm_2$ whenever $m_1 \geqslant m_2$ for monomials m, m_1, m_2.[4]*

There are infinitely many orderings that are "admissible" for "Gröbner Bases" theory. In this section we will give three types of monomial orderings as examples, lexicographic ordering(Lex), degree lexicographic ordering(DegLex), degree reverse lexicographic ordering (DegRevLex). And also every monomial ordering is a well ordering. Actually using *Hilbert Basis Theorem* one can show any total ordering on monomials is a well ordering (monomial ordering). Throughout this thesis unless otherwise is stated, the ordering in use is Lex ordering.

Definition 4.1.2. ***Lexicographic ordering(Lex)*** *Let* $x_1 > x_2 > ... > x_n$ *and* $\alpha = (\alpha_1, ..., \alpha_n) \quad \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}$. *We define*

$$x_\alpha < x_\beta \Longleftrightarrow \begin{cases} \textit{the first coordinates } \alpha_i \textit{ and } \beta_i \textit{ in } \alpha \\ \textit{and } \beta \textit{ from the left, which are different, satisfy } \alpha_i < \beta_i. \end{cases}$$

[3]

Example 4.1.3. *If we use Lex order* $x > y$ *on* $k[x, y]$, *then we have,*

$$1 < y < y^2 < y^3 < ... < x < xy < y^2x < ... < x^2 < ....$$

Definition 4.1.4. ***Degree Lexicographic ordering(DegLex)*** *Let* $x_1 > x_2 > ... > x_n$ *and* $\alpha = (\alpha_1, ..., \alpha_n) \quad \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}$. *We define*

$$x_\alpha < x_\beta \Longleftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ or \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \quad and \quad x_\alpha < x_\beta \\ with \text{ respect to lex with } x_1 > x_2 > ... > x_n. \end{cases}$$

[3]

Example 4.1.5. *If we use DegLex order* $x > y$ *on* $k[x, y]$, *then we have,*

$$1 < y < x < y^2 < xy < x^2 < y^3 < y^2x < yx^2 < x^3....$$

Definition 4.1.6. ***Degree Reverse Lexicographic ordering(DegRevLex)*** *Let* $x_1 > x_2 > ... > x_n$ *and* $\alpha = (\alpha_1, ..., \alpha_n) \quad \beta = (\beta_1, ..., \beta_n) \in \mathbb{N}$. *We define*

$$x_\alpha < x_\beta \Longleftrightarrow \begin{cases} \sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i \\ or \\ \sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i \quad \textit{and the first coordinates} \quad \alpha_i \quad \textit{and} \quad \beta_i \\ in \alpha \textit{ and} \quad \beta \quad \textit{from the right, which are different, satisfy} \quad \alpha_i > \beta_i. \end{cases}$$

[3]

To illustrate the difference between DegLex and DegRevLex, consider a three variable case. Since the in the two variable case Deglex and DegRevLex are the same. Following example shows,

$$x_1^2x_2x_3 > x_1x_2^3 \text{ with respect to the DegLex } x_1 > x_2 > x_3$$

but

$$x_1^2x_2x_3 < x_1x_2^3 \text{ with respect to the DegRevLex } x_1 > x_2 > x_3.$$

Definition 4.1.7. *Fix a monomial ordering on the polynomial ring $k[x_1, x_2, ..., x_n]$,*

i) The leading term of a non-zero polynomial f in $k[x_1, x_2, ..., x_n]$ denoted $LT(f)$ is the monomial term of a maximal order in f.

ii) Multi-degree of f is the multi-degree of the leading term of f and is denoted as $\partial(f)$.

4.1.2 General Polynomial Division

We will give an "Algorithm" for general polynomial division. Fix a monomial ordering on $k[x_1, ..., x_n]$ and suppose $g_1, ..., g_m$ is the set of non-zero polynomials in $k[x_1, ..., x_n]$. Let $q_1, ..., q_m$ be the set of quotients and r be the remainder(all initially zero). Then the algorithm is as follows,

- Check if $LT(f)$ is divisible by $LT(g_i)$ in that order $g_1, ..., g_m$.
- If $LT(f)$ is divisible by $LT(g_i)$, say, $LT(f) = a_iLT(g_i)$, add a_i to the quotient q_i and replace f by $f - a_ig_i$ and reiterate the process.
- If $LT(f)$ is not divisible by any of $LT(g_1), ..., LT(g_m)$, add the leading term of f to the remainder r and replace f by the dividend $f - LT(f)$ and reiterate the entire process.

Monomial ordering is a well-ordering on the set of monomials i.e., every non-empty subset of a monomial has a smallest element. Therefore every descending chain of

monomials terminates and that also means that the polynomial division process terminates,too. This process terminates when the dividend is 0 and the results is in the set of quotients $q_1, ..., q_m$ and a remainder r with

$$f = q_1 g_1 + ... + q_m g_m + r.$$

Each $a_i g_i$ has multi-degree less than or equal to multi-degree of f and r has the property that no non-zero term is divisible by any of $LT(g_1), ..., LT(g_m)$.

Example 4.1.8. *Fix Lex ordering $x > y$ on $k[x, y]$. Suppose $f = x^4 + 3x^2y^4$ and $g = xy^2$. The leading term of f, x^4 ,is not divisible by the leading term of g, so add x^4 the remainder r and replace f with $f - LT(f) = 3x^2y^4$ as in the algorithm and start over. $3x^2y^4$ is divisible by $LT(g) = xy^2$, with quotient $q_1 = 3xy^2$, add $3xy^2$ to the quotient q and replace $3x^2y^4$ by $3x^2y^4 - q_1 LT(g) = 0$ which means the process terminates. The result is*

$$f = x^4 + 3x^2y^4 = qg + r = (3xy^2)(xy^2) + x^4.$$

Definition 4.1.9. *For a fixed ordering on $R = k[x_1, ..., x_n]$ and ordered set of polynomials $G = \{g_1, ..., g_m\}$ in R we write;*

$$f \equiv r \mod G,$$

where the remainder r is obtained by general polynomial division by $g_1, ..., g_m$ in that order i.e.,

$$f = q_1 g_1 + ... + q_m g_m + r.$$

[4]

4.1.3 Monomial Ideals

Definition 4.1.10. *If I is an ideal in $k[x_1, x_2, ..., x_n]$, the ideal of leading terms denoted $LT(I)$ is the ideal generated by the leading terms of all the elements in the ideal, i.e.*

$$LT(I) = (LT(f) : f \in I).$$

[4]

One can easily see that

$$\partial(fg) = \partial(f) + \partial(g)$$

$$LT(fg) = LT(f) + LT(g).$$

LT(I) is by definition generated by monomial ideals. Such ideals are called monomial ideals. Also, if $I = (f_1, ..., f_n)$ then

$$LT(I) \supseteq (LT(f_1), LT(f_2), ..., LT(f_n)).$$

Next we will show that a polynomial is contained in a monomial ideal if and only if each of its monomial terms is a multiple of one of the generators for the ideal

Proposition 4.1.11. *Suppose I is a monomial ideal generated by monomials $m_1, ..., m_k$. A polynomial $f \in k[x_1, ..., x_n]$ is contained in a monomial ideal if and only if each of its monomial terms is a multiple of one of the $m_i's$.*

Proof. Let I be a monomial ideal generated by monomials $I = (m_1, ..., m_k)$ and $f \in k[x_1, ..., x_n]$. By General Polynomial Division we can write,

$$f = \sum_{i=1}^{k} q_i m_i + r$$

where none of the m_i divides r and $q_i \in k[x_1, ..., x_n]$ If $f \in I$ then $r = 0$. Therefore

$$f = q_1 m_1 + ... + q_k m_k$$

where m_i's are monomials and so every monomial term is multiple of at least one m_i. For the converse assume $r \neq 0$ and r is not divisible by $m_i's$. Since each of f's monomial terms is a multiple of one of the generators for I, r must be divisible one of the m_i's. That means $r = 0$ and therefore $f \in I$.

□

Definition 4.1.12. *The ideal quotient of two ideals I and J in a ring R is the ideal*

$$(I : J) = \{r \in R : rJ \in I\}.$$

[4]

Proposition 4.1.13. *Suppose R is an integral domain $f \neq 0$ and I is an ideal in R. If $\{g_1, ..., g_m\}$ are generators for the ideal $I \cap (f)$ then $\{g_1/f, ..., g_m/f\}$ are generators for the ideal quotient .*

Proof. If $g \in \frac{1}{f}(I \cap (f))$ then $gf \in I$ and hence $g \in (I : (f))$.

Conversely is $g \in I : (f)$ then $gf \in J$ and hence $g \in I \cap (f)$ so $g \in \frac{1}{f}(J \cap (f)$. □

Proposition 4.1.14. *If I is an ideal in the commutative ring R and $f_1, ..., f_m \in R$ then the ideal quotient $(I : (f_1, ..., f_m))$ is the ideal*

$$\bigcap_{i=1}^{m}(I : (f_i)).$$

Proof. Let $J = (f_1, ..., f_m)$. We want to show $(I : J) = \bigcap_{i=1}^{m}(I : (f_i) = \{g \in R : gJ \in I\}$. If $g \in I : J$ then $gJ \subseteq I$ so $gf_i \in I$ for $i = 1, .., m$. Therefore $g \in \bigcap_{i=1}^{m}(I : (f_i))$. Conversely if $g \in \bigcap_{i=1}^{m}(I : (f_i))$ then $g(f_i \subseteq I)$ for $i = 1, .., m$ so $gJ \subseteq I$ and therefore $g \in (I : J)$.

□

One can show that the intersection of two monomial ideals is a monomial ideal by showing that $M \cap N = (e_{i,j} : i \in Iandj \in J)$ where $e_{i,j}$ is the least common multiple of the generators $m_i : i \in I \ \ and \ \ n_j : j \in J$ for some index sets I and J. First we will show that $lcm(f, g) = (f) \cap (g)$ for monomials f, g. If $l = lcm(f, g)$ then $l \in (f) \cap (g)$ by definition of l. Conversely if $h \in (f) \cap (g)$ then $h = af = bg$ for some $a, b \in k[x_1, ..., x_n]$. Therefore f and g divides h. Thus l divides h. So by definition of least common multiple, $h \in (l)$. Obviously $M \cap N \supseteq \{e_{i,j} : i \in Iandj \in J\}$. We will try to show the converse by using *Proposition 4.1.11.* If $f \in M \cap N$ where M and N are monomial ideals then $f \in M$ and $f \in N$. So by *Proposition 4.1.11* every monomial term is a multiple of generators of both M and M and also from the previous result we can say every monomial term of f is a multiple of least common multiple of the generators of M and M i.e., $f \in (e_{i,j} : i \in I \ \ and \ \ j \in J)$. Therefore

$$M \cap N = (e_{i,j} : i \in I \ \ and \ \ j \in J).$$

Let M be a monomial ideal generated by monomials,$M = (m_i : i \in I)$, one can show that for any monomial n, the ideal quotient $(M : (n)) = (\frac{m_i}{d_i} : i \in I)$ where d_i is the greatest common divisor of m_i. We know that for any polynomial f and g we have

$$\gcd(f, g) = \frac{fg}{lcm(f, g)}.$$

To show our assumption we will use this, for our case, we have

$$lcm(m_i, n) = \frac{m_i n}{\gcd(m_i, n)}$$

for $i \in I$. Therefore

$$lcm(m_i, n) = \frac{m_i n}{d_i} \in M$$

and by definition of quotient ideal $\frac{m_i}{d_i} \in (M : (n))$ for every $i \in I$. For the converse, if $g \in (M : (n))$ then $g(n) \subseteq M$ that also means $gn \in M \cap N$. Therefore $gn \in lcm(m_i, n)$ i.e., $gn \in \frac{m_i n}{d_i}$ and $g \in \frac{m_i}{d_i}$.

4.2 Gröbner Basis

A Gröbner basis for an ideal I in the polynomial ring $k[x_1, x_2, ..., x_n]$ is a finite set of generators $\{g_1, g_2, ..., g_m\}$ for I whose leading terms generate the ideal of all leading terms, i.e.,

$$LT(I) = (LT(g_1), ..., LT(g_m)).$$

In general we will show that the remainder and the quotients are not unique and depend on the order with an example . Choose Lex ordering $x > y$ on $k[x, y]$. Let $f = x^2 + x - y^2 + y$ where $g_1 = xy + 1$ and $g_2 = x + y$. f can be written as

$$f = (-1)(xy + 1) + (x + 1)(x + y) + (-y^2 + 1)$$

$$= q_1 g_1 + q_2 g_2 + r$$

where $q_1 = -1$, $q_2 = x + 1$ and $r = -y^2 + 1$. We can also write

$$f = (x - y + 1)(x + y) = q_1 g_1 + q_2 g_2 + r$$

where $q_1 = x - y + 1$, $q_2 = 0$ and $r = 0$. This shows that $f \in I = (x + y, xy + 1)$ since $r = 0$ but previously we found $r = -y^2 + 1$ and we can not say f is an element of I.

If we use *Gröbner Basis* for the ideal I then these difficulties do not arise, we obtain a unique remainder, which in turn can be used to determine whether polynomial f is an element of the ideal I. And this fact makes the Gröbner Bases theory very useful.

Now fix a monomial ordering on $R = k[x_1, ..., x_n]$ and let I be a non-zero ideal in R.

Theorem 4.2.1. *Suppose $\{g_1, ..., g_m\}$ is a Gröbner Basis for I. Every polynomial $f \in R$ can be written uniquely in the form*

$$f = f_1 + r$$

where $f_1 \in I$ and no non-zero monomial term of the remainder "r" is divisible by any of the leading terms $LT(g_1), ..., LT(g_m)$.[4]

Proof. Let

$$f = q_1 g_1 + ... + q_m g_m + r$$

where $g_1, ..., g_m$ is a Gröbner basis for I and

$$f_1 = q_1 g_1 + ... + q_m g_m$$

where $f_1 \in I$. If $f = f_1 + r = f_1' + r'$ then $r - r' = f_1' - f_1 \in I$ then $LT(r - r') \in LT(I) = (LT(g_1), ..., LT(g_m))$. But r, r' can not be a multiple of $LT(g_1), ..., LT(g_m)$. Therefore $r - r' = 0$. □

Theorem 4.2.2. *Suppose $\{g_1, ..., g_m\}$ is a Gröbner basis for I. Both f_1 and r can be computed by general polynomial division by $\{g_1, ..., g_m\}$ and are independent of order in which these polynomials are used in the division.[4]*

Proof. r is independent of the order so it is uniquely determined and so is f_1. □

Proposition 4.2.3. *If $g_1, ..., g_m$ are any elements of I such that $LT(I) = (LT(g_1), ..., LT(g_m))$ then $g_1, ..., g_m$ is a Gröbner Basis.[4]*

Proof. We want to show that $I = (g_1, g_2, ..., g_m)$. Let $f \in I$ and

$$f = \sum_{i=1}^{m} q_i g_i + r$$

where r is not divisible by any of the leading terms of $\{g_1, ..., g_m\}$. Since $f \in I$, $LT(f) \in LT(I)$ and also $LT(r) \in LT(I)$. But that means r is divisible by any of $LT(g_i)$ where $i = 1, ..., m$ and $m \in \mathbb{N}$ which shows $r = 0$. Therefore f is generated by $\{g_1, ..., g_m\}$. □

Next proposition shows that Gröbner Basis exists for every ideal $I \subseteq k[x_1, x_2, ..., x_n]$.

Proposition 4.2.4. *The ideal I has a Gröbner Basis.*

Proof. As we showed before $LT(I)$ is the ideal generated by leading coefficients of all elements in the ideal I where $LT(I)$ is a monomial ideal. By *Hilbert Basis Theorem* $LT(I)$ is finitely generated i.e.,

$$LT(I) = (LT(g_1), ..., LT(g_n))$$

where n is an positive integer. Hence by *Proposition 4.2.3* $\{g_1, ..., g_n\}$ is a Gröbner Basis for I.

□

Using the tools we obtain from Gröbner Basis Theory, Hilbert Basis Theorem follows. We will now discuss S-polynomials which take a crucial part in the Gröbner Basis Theory.

If f_1, f_2 are two polynomials in $F[x_1, ..., x_n]$ and M is the monic least common multiple of the monomial terms $LT(f_1)$ *and* $LT(f_2)$ then we can cancel the leading terms by taking the difference;

$$\mathbf{S}(f_1, f_2) = \frac{M}{LT(f_1)} f_1 - \frac{M}{LT(f_2)} f_2.$$

Theorem 4.2.5 (*Buchberger's Criterion*)**.** *Let $R = F[x_1, ..., x_n]$ and fix a monomial ordering on R. If $I = (g_1, ..., g_m)$ is a non-zero ideal in R then $G = \{g_1, ..., g_m\}$ is a Gröbner Basis if and only if $\boldsymbol{S}(g_i, g_j) \equiv 0 \mod G$ for $1 \leqslant i < j \leqslant m$.[4]*

The termination of the algorithm follows from *Hilbert Basis Theorem.*

Proposition 4.2.6. *Suppose* $G = \{g_1, ..., g_n\}$ *is a generators of the non-zero ideal* I*. If* $\boldsymbol{S}(g_i, g_j)$ *is not equivalent to* $0 \mod G$ *then the ideal* $(LT(g_1), ..., LT(g_n), LT(\boldsymbol{S}(g_i, g_j)))$ *is strictly larger than the ideal* $(LT(g_1), ..., LT(g_n))$*. Thus* Buchberger Algorithm *stops after a finite number of steps.*

Proof. Let $\mathbf{S}(g_i, g_j)$ be not equivalent to $0 \mod G$. Then $\exists r \in I$ such that no term in r is divisible by $\{LT(g_1), ..., LT(g_n)\}$ where r is obtained by general polynomial division. Therefore $(LT(g_1), ..., LT(g_n), LT(\mathbf{S}(g_i, g_j)))$ is larger than $(LT(g_1), ..., LT(g_n))$. Then we can increase G by appending the polynomial $g_{n+1} = r$ where $G' = \{g_1, ..., g_n, g_{n+1}\}$ is still a generating set for I and begin again. If we go on, we will end up with $\{LT(g_1), ..., LT(g_n), LT(g_{n+1}), ...\}$. And clearly $\{LT(g_1), ..., LT(g_n), LT(g_{n+1}), ...\} \in LT(I)$. What we will prove is that there exists $N \in \mathbb{N}$ such that if $i \geqslant N$ then $LT(g_i)$ is divisible by $LT(g_j)$, where $j < N$. *Hilbert Basis Theorem* implies that there are finitely many $LT(g_{i_1}), ..., LT(g_{i_n})$ that generates $LT(I)$ i.e., every monomial in $\{LT(g_1), ..., LT(g_n), LT(g_{n+1}), ...\}$ is divisible by $LT(g_{i_1}), ..., LT(g_{i_n})$. Choosing $N = max\{i_1, ..., i_n\}$ will do the work. □

Example 4.2.7. *Suppose* $I = (g_1, ..., g_m)$ *is a monomial ideal then by using Buchberger's Criterion to show* $\{g_1, ..., g_m\}$ *is a Gröbner Basis for* I*. If* $f \in I$ *then by proposition 4.1.4 each monomial term of* f *can be written as a multiple of some* g_i*'s and that shows* $\boldsymbol{S}(g_i, g_j) \equiv 0 \mod G$ *for* $i \neq j$*.*

A Gröbner Basis $g_1, ..., g_m$ for I where each $LT(g_i)$ is monic and where $LT(g_j)$ is not divisible by $LT(g_i)$ for $i \neq j$ is called *minimal Gröbner Basis*[4]. Next example shows minimal Gröbner Basis is not unique but the number of elements and their leading terms are unique.

Example 4.2.8. *Choose lexicographic ordering* $x > y$*. Let* $f_1 = x^3y - xy^2 + 1$ *and* $f_2 = x^2y^2 - y^3 - 1$*. Now check,*

$$\boldsymbol{S}(f_1, f_2) \equiv x + y = f_3 \mod G$$

$$\boldsymbol{S}(f_1, f_2) \equiv 0 \mod G$$

$$\boldsymbol{S}(f_2, f_3) \equiv y^4 - y^3 - 1 \mod G$$

$f_4 = y^4 - y^3 - 1$ *Therefore* $G' = f_1, f_2, f_3, f_4$ *is a Gröbner Basis. Also*

$$LT(I) = (x^3y, x^2y^2, x, y^4) = (x, y^4).$$

So $I = (x + y, y^4 - y^3 - 1)$ *is another Gröbner Basis.*

Previous example shows that Gröbner Basis is not unique.

Definition 4.2.9. *A Gröbner Basis for* I *is called reduced Gröbner Basis if*

i) each g_i *has monic leading term i.e.,* $LT(g_i)$ *is monic*

ii) no term in g_j *is divisible by* $LT(g_i)$ *for* $i \neq j$*.[4]*

Note that if $\{g_1, ..., g_m\}$ is a reduced Gröbner basis for I then by definition of minimal Gröbner Basis it is also a minimal Gröbner Basis.

Proposition 4.2.10. $\{g_1, ..., g_m\}$ *is a minimal Gröbner basis for* I *if and only if* $\{LT(g_1), ..., LT(g_m)\}$ *is a minimal generating set for* $LT(I)$.

Proof. Assume $F = \{LT(g_1), ..., LT(g_m)\}$ is not a minimal generating set for $LT(I)$. Let $F' \in F$ be the minimal generating set. Without lost of generality we can assume $F' = F - LT(g_i)$ is the minimal generating set for $LT(I)$. By *Proposition 4.2.3* $G' = \{g_1, ..., g_m\} - \{g_i\}$ for some $i \leqslant m$ is Gröbner Basis for I. $g \in G$ then by Buchberger's Criterion $\exists g_k, g_j \in G$ where $j, k \neq i$ such that $\mathbf{S}(g_k, g_j) = g_i$ but g_i is not in G' so G' is not a Gröbner Basis.

For the converse if $F = \{LT(g_1), ..., LT(g_m)\}$ is a minimal generating set for $LT(I)$ by *Proposition 4.2.3* $G = \{g_1, ..., g_m\}$ is a Gröbner Basis for I. We want to show that G is the minimal Gröbner Basis. Since F is the minimal generating set there is no subset of F that generates $LT(I)$, i.e., for any $LT(g_i) \in F$, $LT(g_i)$ does not divide $LT(g_j)$ for $i \neq j$. Therefore G is a minimal Gröbner Basis.

□

Proposition 4.2.11. *Leading terms of the minimal Gröbner Basis for I are uniquely determined and the number of elements in any two minimal Gröbner Bases for I is the same.*

Proof. Let $G = \{g_1, ..., g_t\}$ and $H = \{h_1, ..., h_m\}$ where m, n are positive integers. For $h_1 \in I$ $\exists LT(g_i)$ such that $LT(g_i)$ divides $LT(h_1)$. Without lost of generality we may assume $i = 1$ hence $LT(g_1)$ divides $LT(h_1)$. Also $g_1 \in I$ and since H is a Gröbner Basis for I, $\exists LT(h_j)$ such that $LT(h_j)$ divides divides $LT(h_1)$ but H is a minimal Gröbner Basis so $j = 1$. Thus $LT(g_1) = LT(h_1)$.

By the same way; $h_2 \in I$ where $\exists LT(g_i)$ such that $LT(g_i)$ divides $LT(h_2)$. Without loss of generality we may assume $i = 2$ i.e., $LT(g_2)$ divides $LT(h_2)$. Also $g_2 \in I$ where $\exists LT(h_j)$ such that $LT(h_j)$ divides $LT(g_2)$. Hence $LT(h_j)$ divides $LT(h_2)$ but H is a minimal Gröbner Basis so $j = 2$. Thus $LT(g_2) = LT(h_2)$.

If we proceed that way till all the $g_i's$ *and* $f_i's$ are used, then we will clearly see that $t = m$ and $LT(g_i = LT(h_i))$ $i = 1, ..., m$.

□

Next proposition shows that Reduced Gröbner Basis is unique for every ideal $I \subseteq k[x_1, x_2, ..., x_n]$.

Theorem 4.2.12. *There is a unique reduced Gröbner Basis for every I.[4]*

Proof. By *Proposition 4.2.11* two minimal Gröbner bases have the same number of elements and the same leading terms. This also holds for two reduced Gröbner Basis. by definition of reduced Gröbner Basis. Let $G = \{g_1, ..., g_m\}$ and $G' = \{g'_1, ..., g'_m\}$ be two reduced bases for I. By possible rearrangement we may assume $LT(g_i) = LT(g'_i)$=h_i for $i = 1, ..., m$. Now for any fixed i, consider the polynomial $f_i = g_i - g'_i$. If f_i is nonzero, then since $f_i \in I$ then it must be divisible by some of the h_j. By definition of a reduced Gröbner Basis h_j for $j \neq i$ does not divide any of the terms in either g_i or g'_i, hence does not divide $LT(f_i)$. But also does not divide $LT(f_i)$ since all the the terms in f_i have smaller multi degree. Therefore $f_i = 0$ and $g_i = g'_i$ for every i=1,...,m.

□

Example 4.2.13. *Choose Lex ordering $x > y$. Let $I = (h_1, h_2, h_3)$ with $h_1 = x^2 + xy^5 + y^4$, $h_2 = xy^6 - xy^3 + y^5 - y^2$ and $h_3 = xy^5 - xy^2 \in k[x, y]$. After doing some calculations, we will end up with*

$$x^2 + xy^5 + y^4, xy^6 - xy^3 + y^5 - y^2, xy^5 - xy^2, y^5 - y^2$$

which is a Gröbner Basis for I. Thus $LT(I) = (x^2, xy^6, xy^5, y^5)$. Since y^5 divides xy^6 and xy^5 we may remove h_2 and h_3 from the Gröbner Basis and we have $G = \{x^2 + xy^5 + y^4, y^5 - y^2\}$ for I. The second term in the first generator is divisible by the leading term y^5 of the second generator, in order to obtain reduced Gröbner Basis apply general polynomial division and replace $x^2 + xy^5 + y^4$ by its remainder $x^2 + xy^2 + y^4$ after division by $x^2 + xy^5 + y^4$. Therefore we are left with the reduced Gröbner Basis $\{x^2 + xy^2 + y^4, y^5 - y^2\}$. [4]

4.3 Elimination

Let $\{x_1, ..., x_n\}$ and $\{y_1, ..., y_n\}$ be two set of variables. Assume that monomials in the x variables and monomials in the y variables are ordered by some monomial orders $<_x, <_y$ respectively. We will define a monomial order on the monomials in x, y variables as follows.

Definition 4.3.1. *For X_1X_2 monomials in the x variables and Y_1, Y_2 monomials in the y variables, we define[3]*

$$X_1Y_1 < X_2Y_2 \Longleftrightarrow \begin{cases} X_1 <_x X_2 \\ or \\ X_1 = X_2 \quad and \;\; Y_1 <_y Y_2. \end{cases}$$

This ordering is called an elimination order with the x variables larger than the y variables.

Elimination order can be seen as a Lex ordering between two different sets of variables. Also we do not need to consider the order within the two sets.

Theorem 4.3.2. *Let I be a non-zero ideal of $k[y_1, ..., y_n, x_1, ..., x_m]$ and $<$ be an elimination order with the x variables larger than the y variables. Let $G = \{g_1, ..., g_t\}$ be a Gröbner Basis for this ideal. Then $G \cap k[y_1, ..., y_n]$ is a Gröbner Basis for the ideal $I \cap k[y_1, ..., y_n]$.[3]*

Proof. Clearly $G \cap k[y_1, ..., y_n] \subseteq I \cap k[y_1, ..., y_n]$. Conversely, let $0 \neq f(y_1, ..., y_n) \in I \cap k[y_1, ..., y_n]$. G is a Gröbner Basis for I $\exists i$ such that $LT(g_i)$ divides $LT(f_i)$. Since f_i is in y variables $LT(g_i)$ is in y variables. And also g_i is in y variables because of the elimination order. Therefore $g_i \in G \cap k[y_1, ..., y_n]$. □

The ideal $I \cap k[y_1, ..., y_n]$ is called the *Elimination ideal* since the x variables are eliminated. We will discuss this in the *Integer Programming and Polynomial Maps* Sections again.

Chapter 5

APPLICATIONS OF GRÖBNER BASIS

5.1 The n-Coloring Problem

Ω is a finite graph of size N, set of vertices $i \in \{1, ..., N\}$ and collection of edges (i, j) connecting vertex i with vertex j. An n-coloring of Ω is an assignment of one of n-colors to each vertex in such a way that vertices connected by an edge have distinct colors. Coloring need not be unique.

Our purpose is to find the coloring of graph Ω by using Gröbner Basis. To do it first we have to represent the rules we are given with polynomials. There are two ways, in the first way we are going to represent colors as elements from a field and in the second way we will use root of unities.

Now let $\mathbb{F}$ be any field containing at least n elements and S be the set of n-colors. We will assign x_i for each vertex i and represent n colors by choosing elements from $\mathbb{F}$. The n-coloring of Ω,

$$x_i \to \alpha_i \quad for \quad each \quad i = 1, ..., N \quad and \quad \alpha_i \in \mathbb{F}.$$

Therefore the polynomial that represents our first rule which is coloring each vertex with a color from our set S is

$$f(x) = \prod_{\alpha_i \in S} (x - \alpha_i).$$

This is a polynomial in $F[x]$ whose degree is n and roots are the elements from S. For a special case $n = p$ for some prime number p, by Fermat's little theorem we have $f(x) = x^p - x$.

Our second rule is, vertices connected by an edge must have distinct colors. Now assume x_i and x_j are two vertices and $n = p$ and they are colored. Therefore $f(x_i) =$

$f(x_j)$ and

$$x_i^p - x_i = x_j^p - x_j$$

$$(x_i - x_j)(x_i^{p-1} + x_i^{p-2}x_j + ... + x_j^{p-1} - 1) = 0.$$

Let $h = (x_i - x_j)$ and $k = (x_i^{p-1} + x_i^{p-2}x_j + ... + x_j^{p-1} - 1)$. We have three cases;

case1: Let $h = 0$ *and* $k = 0$. That means $x_i = x_j$ and k becomes $k = px_i^{p-1} - 1 = 0$. Thus $px_i^{p-1} \equiv 1 \mod p$ but this can not happen. Therefore this case wont happen.

case2: $h = 0$ and $k \neq 0$

case3: $h \neq 0$ and $k = 0$

The other cases show that polynomial k is taking value according to the vertices being connected or not. Hence we can use k for representing our rule. Let's call $k = g(x_i, x_j)$.

Now we will discuss our second way. First we let $\xi = e^{\frac{2\pi i}{n}} \in \mathbb{C}$ be n^{th} root of unity. We represent n-colors by $1, \xi, \xi^2, ..., \xi^{n-1}$ the n- distinct n^{th} root of unity. As before we let $x_i, i = 1..n$ be variables representing the distinct vertices. Each vertex is to be assigned one of the n colors. This will be represented as follows, $f(x) = x^n - 1$ and for any vertex $x_i, i = 1, ..., n$

$$f(x_i) = x_i^n - 1 = 0.$$

We have a second rule which says vertices which are connected need to have different color.

To represent it, consider the vertices x_i and x_j. Since $f(x_i) = f(x_j)$ we have $x_i^n = x_j^n$. Therefore

$$(x_i - x_j)(x_i^{n-1} + x_i^{n-2}x_j + ... + x_j^{n-1}) = 0.$$

Let $h = (x_i - x_j)$ and $k = (x_i^{n-1} + x_i^{n-2}x_j + ... + x_j^{n-1})$. We have three cases as we did before;

case1: Let $h = 0$ *and* $k = 0$. That means $x_i = x_j$ and k becomes $k = nx_i^{n-1} = 0$ but this can not happen. Therefore this case wont happen.

case2: $h = 0$ and $k \neq 0$

case3: $h \neq 0$ and $k = 0$ The other cases show that polynomial k is taking value according to the vertices being connected or not. Hence we can use k for representing our rule. Let's call $k = g(x_i, x_j)$.

As a result the n-coloring of the graph Ω is equivalent to solving the system of equations

$$f(x_i) = 0 \quad for \quad i = 1, ..., n$$

and

$$g(x_i, x_j) = 0 \quad for \quad all \quad edges \quad (i, j) \in \Omega.$$

By *Proposition 3.4.5* that system of equations has a solution, i.e., the graph Ω has n-coloring, unless the Gröbner Basis for I which is the ideal in $F[x_1, ..., x_N]$ generated by polynomials $f(x_i) = 0 \quad i = 1, ...N \quad and \quad g(x_i, x_j) = 0 \quad for \quad all \quad edges \quad (i, j) \in \Omega.$, is simply $\{1\}$.

Example 5.1.1. *Consider the 3-coloring of Ω with 8 vertices and edges*

(1,3), (1,4),(1,5),(2,4),(2,7),(2,8),(3,6),(3,8),(4,5),(5,6), (6,7),(6,8),(7,8). Now take $F = \mathbb{F}_3 = \{0, 1, 2\}$ and suppose $x_1 \to 0$.

$$f(x) = x(x-1)(x-2) = x(x-1)(x+1) = x^3 - x \in \mathbb{F}_3$$

and

$$g(x_i, x_j) = x_i^2 + x_i x_j + x_j^2 - 1.$$

If

$$I = (\{x_1, x_i^3 - x_i; i = 2, ..., 8, g(x_i, x_j); \quad for \quad the \quad edges \quad (i, j) \in \Omega\})$$

$= (\{x_1, x_2^3 - x_2, x_3^3 - x_3, x_4^3 - x_4, x_5^3 - x_5, x_6^3 - x_6, x_7^3 - x_7, x_8^3 - x_8, x_1^2 + x_1x_3 + x_3^2 - 1, x_1^2 + x_1x_4 + x_4^2 - 1, x_1^2 + x_1x_5 + x_5^2 - 1, x_2^2 + x_2x_4 + x_4^2 - 1, x_2^2 + x_2x_7 + x_7^2 - 1, x_2^2 + x_2x_8 + x_8^2 - 1, x_3^2 + x_3x_6 + x_6^2 - 1, x_3^2 + x_3x_8 + x_8^2 - 1, x_4^2 + x_4x_5 + x_5^2 - 1, x_5^2 + x_5x_6 + x_6^2 - 1, x_6^2 + x_6x_7 + x_7^2 - 1, x_6^2 + x_6x_8 + x_8^2 - 1, x_7^2 + x_7x_8 + x_8^2 - 1\})$

One can show the reduced Gröbner Basis with respect to the lexicographic monomial ordering with the help of CoCoA (see appendix B.1) is

$$\{x_1, x_2, x_3 + x_8, x_4 + 2x_8, x_5 + x_8, x_6, x_7 + x_8, x_8^2 + 2\}.$$

This result means vertex x_1, x_2, x_6 *are colored by* 0. *Also*

$$x_8^2 + 2 = 0, x_8^2 = -2$$

$$x_8^2 \equiv -2 \mod 3 \Longrightarrow x_8 \equiv 1 \mod 3 \text{ or } x_8 = -1 \equiv 2 \mod 3$$

If we assign $x_8 = 1$, *then*

$$x_3 = -1 \equiv 2 \mod 3 \quad x_4 = -2 \equiv 1 \mod 3$$

$$x_5 = -1 \equiv 2 \mod 3 \quad x_7 = -1 \equiv 2 \mod 3.$$

If we assign $x_8 = 2$, *then*

$$x_3 = -2 \equiv 1 \mod 3 \quad x_4 = -4 \equiv -1 \equiv 2 \mod 3$$

$$x_5 = -2 \equiv 1 \mod 3 \quad x_7 = -2 \equiv 1 \mod 3.$$

Therefore there are two different coloring for the graph Ω. *If the edge (3,7) is added that means* $g(x_3, x_7) = x_3^2 + x_3x_7 + x_7^2 - 1$ *is added to our basis. Consider the first coloring of* Ω. *If* $x_8 = 1$, *then* $x_3 = 2$ *and* $x_7 = 2$. *Hence* $g(x_3, x_7) = g(2, 2) = 11 \equiv 2 \mod 3$ *since (2,2) is not a root of* $g(x_i, x_j)$ $x_8 = 1$ *is not a solution. Now lets consider the second coloring where* $x_8 = 2$. *We found that* $x_3 = 1$ *and* $x_7 = 1$ *therefore* $g(x_3, x_7) = g(1, 1) \equiv 2 \mod 3$. *But still (1,1) is not a root of* $g(x_i, x_j)$. *Thus* Ω *is not 3-colorable if the edge (3,7) is added. Since the Gröbner Basis shows that* x_3 *and* x_7 *must have the same coloring. Adding the edge (3,7) makes* $V(I) = \emptyset$ *and* $G = \{1\}$ *Hence by* Proposition 3.4.5 *graph* Ω *in not 3-colorable.*

Example 5.1.2. *Now take* $F = \mathbb{F}_5$ *with four colors* $1, 2, 3, 4 \in \mathbb{F}_5$, *so* $f(x) = x^4 - 1$ *and we may use* $g(x_i, x_j) = x_i^3 + x_i^2x_j + x_ix_j^2 + x_j^3$. *One can show that the graph* G *with five vertices and nine edges,* $\{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5), (4,5)\}$ *can be 4-colored. Since by the help of CoCoA (see appendix B.2) one can show that the reduced Gröbner Basis for the ideal* I, *which is generated by* $f(x_i : i = 1, ..., 4)$ *and* $g(x_i, x_j)$ *where* $(i, j) \in \Omega$, *is*

$$\{x_4^3+x_4^2x_5+x_4x_5^2-1, x_5^4-1, x_3^2+x_3x_4+x_4^2+x_3x_5+x_4x_5+x_5^2, x_2+x_3+x_4+x_5, x_1+x_3+x_4+x_5\}$$

Clearly 1 *is not in the reduced Gröbner Basis. Thus by* Proposition 3.4.5 *this graph is 4-colorable. But it is not 3-colorable because by the help of CoCoA (see appendix B.3)the reduced Gröbner Basis is* $G = \{1\}$.

Example 5.1.3. *The graph* Ω *with nine vertices and 22 edges*

$(1,4),(1,6),(1,7),(1,8),(2,3),(2,4),(2,6),(2,7),(3,5),(3,7),(3,9),$

$(4,5),(4,6),(4,7),(4,9),(5,6),(5,7),(5,8),(5,9),(6,7),(6,9),(7,8)$ *is four colorable up to the permutations of colors (see appendix B.4).*

The reduced Gröbner Basis for the ideal I which is generated by polynomials as in the previous example, is

$\{x_4 + x_5 + x_6 + x_9, x_7 - x_9, x_8^3 + x_8^2x_9 + x_8x_9^2 + x_9^3, x_1 - x_5, x_2 - x_5, x_5x_6 + x_6^2 - x_5x_8 - x_8^2 + x_6x_9 - x_8x_9, x_3^2 + x_3x_5 - x_5x_8 - x_8^2 + x_3x_9 - x_8x_9, x_6^3 + x_6^2x_9 + x_6x_9^2 + x_9^4 - 1, x_5^2 + x_5x_8 + x_8^2 + x_5x_9 + x_8x_9 + x_9^2\}$ *But it is not 3-colorable because by the help of CoCoA (see appendix B.5)the reduced Gröbner Basis is* $G = \{1\}$.

5.2 Polynomial Maps

A $k-$algebra homomorphism is a ring homomorphism

$$\varphi : k[y_1, ...y_m] \longmapsto k[x_1, ...x_n]$$

which is also a $k-$vector space linear transformation. Such a map is uniquely determined by

$$\varphi : y_i \longmapsto f_i,$$

where $f_i \in k[x_1, ...x_n]$, $1 \leq i \leq n$. That is, if we let $h(y_1, ...y_m) \in k[y_1, ..., y_m]$, say $h = \sum_\alpha c_\alpha y_1^{\alpha_1}, ...y_m^{\alpha_m}$ where $c_\alpha \in k$, $\alpha = (\alpha_1, ..., \alpha_m) \in \mathbb{N}^m$, and only finitely many $c'_\alpha s$ are non-zero, then we have

$$\varphi(h) = \sum_\alpha c_\alpha f_1^{\alpha_1}, ...f_m^{\alpha_m} = h(f_1, ..., f_m) \in k[x_1, ...x_n].$$

In this section we are going to determine if any given $f_i \in k[x_1, ...x_n]$ is in the $\operatorname{Im}\varphi$ or not. In order to do it, first we will use the theory of *Elimination* to determine

$\operatorname{Ker}\varphi$ or more precisely, a Gröbner Basis for $\operatorname{Ker}\varphi$. And also $\operatorname{Im}\varphi$ more precisely an algorithm to decide whether a polynomial f is in the image of φ and a map like φ is surjective or not. Before we start this process we will prove a very useful lemma.

Lemma 5.2.1. *Let $a_1, ..., a_n, b_1, ..., b_n$ be elements of a commutative ring R. Then the element $a_1a_2...a_n - b_1b_2...b_n$ is in the ideal $(a_1 - b_1, ..., a_n - b_n)$.*

Proof. We will use mathematical induction on the index of variables. For $n = 1$ it is clear. Now let's assume that the equation holds for $n - 1$ variables and prove for n variables. To do it, we will use

$$a_1a_2...a_n - b_1b_2...b_n = a_1(a_2...a_n - b_2...b_n) + b_2...b_n(a_1 - b_1).$$

By induction hypothesis $(a_2...a_n - b_2...b_n)$ is in the ideal generated by $(a_2 - b_2, ..., a_n - b_n)$ and so it is an element of $(a_1 - b_1, ..., a_n - b_n)$ and also $a_1 - b_1 \in (a_1 - b_1, ..., a_n - b_n)$. Therefore $a_1a_2...a_n - b_1b_2...b_n \in (a_1 - b_1, ..., a_n - b_n)$.

□

Theorem 5.2.2. *Set $K = (y_1 - f_1, ..., y_m - f_m) \subseteq k[y_1, ..., y_m, x_1, ..., x_n]$. Then* $\operatorname{Ker}(\varphi) = K \cap k[y_1, ..., y_m]$.

Proof. If $g \in K \cap k[y_1, ..., y_m]$, then

$$g(y_1, ..., y_m) = \sum_{i=1}^{m} (y_i - f_i)h_i(y_1, ..., y_m, x_1, ..., x_n).$$

If we substitute $(f_1, ..., f_m)$ instead of $(y_1, ..., y_m)$ we will end up with

$$\varphi(g) = g(f_1, ..., f_m) = 0.$$

Hence $g \in \operatorname{Ker}\varphi$. For the converse, if $g \in \operatorname{Ker}\varphi$, $g = \sum_\alpha c_\alpha y_1^{\alpha_1}...y_m^{\alpha_m}$ where $c_\alpha \in k$, $\alpha = (\alpha_1, ..., \alpha_m) \in \mathbb{N}^m$ and $\varphi(g) = g(f_1, ..., f_m) = 0$. Now let

$$\begin{aligned} g &= g - g(f_1, ..., f_m) \\ &= \sum_\alpha c_\alpha (y_1^{\alpha_1}...y_m^{\alpha_m} - f_1^{\alpha_1}...f_m^{\alpha_m}) \end{aligned}$$

By *Lemma 5.2.1* $g \in (y_1 - f_1, ..., y_m - f_m) = K$. Therefore $g \in K \cap k[y_1, ..., y_m]$.

□

Now recall the section about *Elimination* and *Theorem 4.3.2* about the elimination ideal. We already have the tools to calculate the Gröbner Basis of $\mathrm{Ker}(\varphi)$. First we will calculate the Gröbner Basis for the ideal $K = (y_1 - f_1, ..., y_m - f_m) \subseteq k[y_1, ..., y_m, x_1, ..., x_n]$ with respect to the elimination order which the x variables larger than the y variables then we will find the intersection of this Gröbner Basis elements and $k[y_1, ..., y_m]$. The Gröbner Basis for the $\mathrm{Ker}(\varphi)$ is $G \cap k[y_1, ..., y_m]$. K acts as an elimination ideal as we saw in the *Theorem 4.3.2*

Theorem 5.2.3. *Let* $K = (y_1 - f_1, ..., y_m - f_m) \subseteq k[y_1, ..., y_m, x_1, ..., x_n]$ *and* G *be the reduced Gröbner Basis for* K *with respect to the elimination order* x *variables larger than* y *variables. Then* $f \in k[x_1, ..., x_n]$ *is in the image of* φ *if and only if* $\exists h \in k[y_1, ..., y_m]$ *such that* $f \equiv h \mod G$. *In this case* $f = \varphi(h) = h(f_1, ..., f_m)$.

Proof. If $f \in \mathrm{Im}\,\varphi$, then $\exists g \in k[y_1, ..., y_m]$ such that $f = \varphi(g(y_1, ..., y_m) = g(f_1, ..., f_m)$. Clearly $f - g \in k[y_1, ..., y_m, x_1, ..., x_n]$. Consider,

$$\begin{aligned} f(x_1, ..., x_n) - g(y_1, ..., y_m) &= g(f_1, ..., f_n) - g(y_1, ..., y_m) \\ &= g - g(y_1, ..., y_m). \end{aligned}$$

By *lemma 5.2.1* $f(x_1, ..., x_n) - g(y_1, ..., y_m) \in K$. Since G is the Gröbner Basis for K, $f(x_1, ..., x_n) - g(y_1, ..., y_m) \equiv 0 \mod G$ and that means $f \equiv g \mod G$. Now $g \in k[y_1, ..., y_m]$, by definition of Gröbner Bases and our elimination order, $g \equiv h \mod G$ where $h \in k[y_1, ..., y_m]$ and therefore $f \equiv h \in k[y_1, ..., y_m]$.

Conversely, if $f \equiv h \mod G$ where $h \in k[y_1, ..., y_m]$, then $f - g \in K$. Consider,

$$f(x_1, ..., x_n) - h(y_1, ..., y_m) = \sum_{i=1}^{m} g_i(x_1, ..., x_n, y_1, ..., y_m)(y_i - f_i)$$

where $g_i \in K$ for $i = 1, ..., m$. Recall that $\varphi(h) = h(f_1, ..., f_m)$. If we substitute $(f_1, ..., f_m$ instead of $(y_1, ..., y_m)$ we will end up with,

$$\begin{aligned} f(x_1, ..., x_n) - h(f_1, ..., f_m) &= \sum_{i=1}^{m} g_i(x_1, ..., x_n, f_1, ..., f_m)(f_i - f_i) = 0 \\ f - \varphi(h) &= 0 \\ f &= \varphi(h). \end{aligned}$$

Hence $f \in \operatorname{Im} \varphi$. □

For any given $f \in k[x_1, ..., x_n]$, this theorem gives an algorithm to determine whether f is in the image or not.

- Find the Gröbner Basis G of K with respect to an elimination order
- Do the reduction of f with respect to G.
- f is in the image of φ if and only if $f \equiv h \mod G$ where $h \in k[y_1, ..., y_m]$.

Also we can can generalize this theorem and determine if φ is onto or not. Next theorem shows that finding some specific polynomials in G is enough to do that.

Theorem 5.2.4. *Let $K = (y_1 - f_1, ..., y_m - f_m) \subseteq k[y_1, ..., y_m, x_1, ..., x_n]$ and G be the reduced Gröbner Basis for K with respect to the elimination order x variables larger than y variables. φ is onto if and only if for each $i = 1, .., n$ $\exists g_i \in G$ such that $g_i = x_i - h_i$ where $h_i \in k[y_1, ..., y_m]$.*

Proof. Assume φ is onto and without loss of generality assume the order is $x_1 < x_2 < ... < x_n$. Since φ is onto, by previous theorem x_1 is in the image and $\exists h_1 \in k[y_1, ..., y_m]$ such that $x_1 \equiv h_1' \mod G$. Therefore $x_1 - h_1' \in K$. Hence $\exists g_1 \in G$ such that $LT(g_1)$ divides $LT(x_1 - h_1) = x_1$. By the elimination order the only terms smaller than x_1 are in y variables, therefore $g_1 = x_1 - h_1$ for some $h \in k[y_1, ..., y_m]$. Similarly,x_2 is in the image, by *Theorem 5.2.3* $\exists h_2 \in k[y_1, ..., y_m]$ such that $x_2 \equiv h_2' \mod G$. Thus $\exists g_2$ such that $LT(g_2)$ divides $LT(x_2 - h_2') = x_2$. Since the only terms strictly smaller

then x_2 are the y variables and x_1 and G is the reduced Gröbner basis and any term involving x_1 could be reduced by $g_1 = x_1 - h_1$, we must have $g_2 = x_2 - h_2$ for some $h_2 \in k[y_1, ..., y_m]$. We can proceed this way until the x_i for $i = 1, .., m$ are consumed. For the converse, assume $x_i - h_i \in G$ where $h_i \in k[y_1, ..., y_m]$, we have $x_i - h_i \equiv 0$ mod G. Therefore $x_i \equiv h_i \mod G$ and by *Theorem 5.2.3* x_i is in the Im φ. □

Now we will give an easy example to illustrate the idea, we have been dealing.

Example 5.2.5. *Let,*

$$\begin{aligned} \varphi : \mathbb{Q}[u, v, w] &\longmapsto \mathbb{Q}[x] \\ u &\longmapsto x^4 + x \\ v &\longmapsto x^3 \\ w &\longmapsto x^5. \end{aligned}$$

φ is a well defined map. In order to determine if this map is onto or not we are going to calculate the Gröbner Basis for the ideal $K = (u - x^4 - x, v - x^3, w - x^5)$ with respect to the elimination order (as we discussed that elimination ordering can be seen as a Lex ordering), $x > u > v > w$ and with the help of CoCoA (see appendix B.6) programming. Result is

$$\begin{aligned} G = \{&x - uv^2 + uv - u + w^2, v^5 - w^3, -uw + v^3 + v^2, -uv^3 + uw^2 + w^2, \\ &-u^2v + v^2w + 2vw + w, u^3 - v^4 - 3v^3 - 3v^2 - v\} \end{aligned}$$

If we check the Gröbner Basis we will see that we have $x - uv^2 + uv - u + w^2$. So by the Theorem 5.2.4*we can say φ is onto. Also*

$$x = (\varphi(uv^2 + uv - u + w^2)) = (x^4 + x)x^6 - (x^4 + x)x^3 + x^4 + x - x^{10}$$

shows that the pre-image of x is $uv^2 + uv - u + w^2$.

Now we will extend the above results to quotient rings of polynomial rings. We will refer this section when we construct a way to determine the solutions of integer programming problem **Case 2**(see, next section).

Definition 5.2.6. *An k-algebra is called an affine k-algebra if it is isomorphic as a k-algebra to $k[x_1, ..., x_n]/I$ for some ideal I of $k[x_1, ..., x_n]$*

If we consider the mapping φ

$$\varphi : k[y_1, ..., y_m] \longmapsto k[x_1, ..., x_n]$$

$$y_i \longmapsto f_i$$

$k[f_1, ..., f_n]$ is an affine k-algebra, since it is isomorphic to $k[y_1, ..., y_m]/\operatorname{Ker}\varphi$.

Now, let

$$\begin{aligned} \varphi : k[y_1, ..., y_m] &\longmapsto k[x_1, ..., x_n]/I \\ y_i &\longmapsto f_i + I \end{aligned}$$

where I is an ideal of $k[x_1, ..., x_n]$ and $f_i \in k[x_1, ..., x_n]$. Clearly this map is well-defined. Next we will show that $\operatorname{Ker}\varphi = K \cap k[y_1, ..., y_m]$.

Theorem 5.2.7. *If $K = (I, y_1 - f_1, ..., y_m - f_m) \subseteq k[y_1, ..., y_m, x_1, ..., x_n]$, then* $\operatorname{Ker}(\varphi) = K \cap k[y_1, ..., y_m]$.

Proof. If $g' \in K \cap k[y_1, ..., y_m]$, then

$$g'(y_1, ..., y_m) = \sum_{i=1}^{m} (y_i - f_i)h_i(y_1, ..., y_m, x_1, ..., x_n) + w(y_1, ..., y_m, x_1, ..., x_n).$$

where

$$w(y_1, ..., y_m, x_1, ..., x_n) = \sum_j c_j(y_1, ..., y_m, x_1, ..., x_n)d(x_1, ..., x_n)$$

$h_i, c_i \in k[y_1, ..., y_m, x_1, ..., x_n]$ and $d \in I$. If we substitute $(f_1, ..., f_m)$ instead of $(y_1, ..., y_m)$ we will end up with

$$\varphi(g') = g'(f_1, ..., f_m) + I = w + I = 0.$$

Hence $g \in \operatorname{Ker}\varphi$. For the converse, if $g \in \operatorname{Ker}\varphi$, $g = \sum_\alpha c_\alpha y_1^{\alpha_1}...y_m^{\alpha_m}$ where $c_\alpha \in k$, $\alpha = (\alpha_1, ..., \alpha_m) \in \mathbb{N}^m$ and $\varphi(g) = g(f_1, ..., f_m) = 0$. Now let

$$\begin{aligned} g &= g - g(f_1, ..., f_m) \\ &= \sum_\alpha c_\alpha (y_1^{\alpha_1}...y_m^{\alpha_m} - f_1^{\alpha_1}...f_m^{\alpha_m}) \end{aligned}$$

By *Lemma 5.2.1* $g \in (y_1 - f_1, ..., y_m - f_m) \subseteq K$. Therefore $g \in K \cap k[y_1, ..., y_m]$.

□

Theorem 5.2.8. *Let $K = (I, y_1 - f_1, ..., y_m - f_m) \subseteq k[y_1, ..., y_m, x_1, ..., x_n]$ and G be the reduced Gröbner Basis for K with respect to the elimination order x variables larger than y variables. $f \in k[x_1, ..., x_n]$ is in the image of φ if and only if $\exists h \in k[y_1, ..., y_m]$ such that $f + I \equiv h \mod G$.*

Proof. If $f + I \in \operatorname{Im}\varphi$, then $\exists g \in k[y_1, ..., y_m]$ such that $f + I = \varphi(g(y_1, ..., y_m)) = g(y_1, ..., y_m)$. Clearly $f(x_1, ..., x_n) - g(f_1, ..., f_m) \in k[y_1, ..., y_m, x_1, ..., x_n]$. Consider,

$$f(x_1, ..., x_n) - g(y_1, ..., y_m) = g(f_1, ..., f_m) - g(y_1, ..., y_m) + (f(x_1, ..., x_n) - g(f_1, ..., f_m))$$

By *Lemma 5.2.1* $f(x_1, ..., x_n) - g(y_1, ..., y_m) \in K$. Since G is the Gröbner Basis for K, $f(x_1, ..., x_n) - g(y_1, ..., y_m) \equiv 0 \mod G$ and that means $f \equiv g \mod G$. Now $g \in k[y_1, ..., y_m]$, by definition of Gröbner Bases and our elimination order, $g \equiv h \mod G$ where $h \in k[y_1, ..., y_m]$ and therefore $f + I \equiv h \in k[y_1, ..., y_m]$.

Conversely, if $f \equiv h \mod G$ where $h \in k[y_1, ..., y_m]$, then $f - h \in K$. Consider,

$$f(x_1, ..., x_n) - h(y_1, ..., y_m) = \sum_{i=1}^{m} g_i(x_1, ..., x_n, y_1, ..., y_m)(y_i - f_i) + w(y_1, ..., y_m, x_1, ..., x_n).$$

where

$$w(y_1, ..., y_m, x_1, ..., x_n) = \sum_j c_j(y_1, ..., y_m, x_1, ..., x_n) d(x_1, ..., x_n)$$

$g_i, c_j \in k[y_1, ..., y_m, x_1, ..., x_n]$ and $d \in I$. If we substitute $(f_1, ..., f_m)$ instead of $(y_1, ..., y_m)$ we will end up with

$$f - h(f_1, ..., f_m) = f - \varphi(h(y_1, ..., y_m)) \in I.$$

Hence $\varphi(h) = f + I$. □

Theorem 5.2.9. *Let $K = (I, y_1 - f_1, ..., y_m - f_m) \subseteq k[y_1, ..., y_m, x_1, ..., x_n]$ and G be the reduced Gröbner Basis for K with respect to the elimination order x variables larger than y variables. φ is onto if and only if for each $i = 1, .., n$ $\exists g_i \in G$ such that $g_i = x_i - h_i$ where $h_i \in k[y_1, ..., y_m]$.*

Proof. Assume φ is onto and without loss of generality assume the order is $x_1 < x_2 < ... < x_n$. Since φ is onto by *Theorem 5.2.8*, $x_1 + I$ is in the image and $\exists h_1' \in k[y_1, ..., y_m]$ such that $x_1 \equiv h_1' \mod G$. Therefore $x_1 - h_1' \in K$. Hence $\exists g_1 \in G$ such that $LT(g_1)$ divides $LT(x_1 - h_1') = x_1$. By the elimination order the only terms smaller than x_1 are in y variables, therefore $g_1 = x_1 - h_1$ for some $h_1 \in k[y_1, ..., y_m]$. Similarly,$x_2 + I$ is in the image, by the previous theorem $\exists h_2' \in k[y_1, ..., y_m]$ such that $x_2 \equiv h_2' \mod G$. Thus $\exists g_2$ such that $LT(g_2)$ divides $LT(x_2 - h_2') = x_2$. Since the only terms strictly smaller then x_2 are the y variables and x_1 and G is the reduced Gröbner basis and any term involving x_1 could be reduced by $g_1 = x_1 - h_1$, we must have $g_2 = x_2 - h_2$ for some $h_2 \in k[y_1, ..., y_m]$. We can proceed this way until the x_i for $i = 1, .., m$ are consumed. For the converse, assume $x_i - h_i \in G$ where $h_i \in k[y_1, ..., y_m]$, we have $x_i - h_i \equiv 0 \mod G$. Therefore $x_i \equiv h_i \mod G$ and by *Theorem 5.2.8* x_i is in the $\operatorname{Im} \varphi$.

□

5.3 Integer Programming

In this section we will use a great deal deal of the theory that is developed at the previous section. Our main aim is to calculate a solution for the following equation

system given,

$$\begin{aligned} &a_{11}\sigma_1 + a_{12}\sigma_2 + ... + a_{1m}\sigma_m = b_1 \\ &a_{21}\sigma_1 + a_{22}\sigma_2 + ... + a_{2m}\sigma_m = b_2 \\ &\vdots \\ &a_{n1}\sigma_1 + a_{n2}\sigma_2 + ... + a_{nm}\sigma_m = b_n \end{aligned} .$$

which minimizes the "cost function"

$$c(\sigma_1, ..., \sigma_m) = \sum_{j=1}^{m} c_j\sigma_j$$

where a_{ij}'s and b_i's are integers and $(\sigma_1, ..., \sigma_m) \in \mathbb{N}^m$ is the solution of the system. First we will ignore the "cost function" when solving this equation system.

We want to convert this problem into a polynomial mapping problem and the solutions of this polynomial mapping problem into the integer programming problem. Well, we will discuss this in two cases. In the first case we will restrict ourselves where all a_{ij}'s and b_i's are positive integers which is an relatively easier case. The second case is the case where all a_{ij}'s and b_i's are just integers.

CASE 1:

In this case we will just consider the integer programming problem where all a_{ij}'s and b_i's are positive integers. First we will introduce a new variable for each equation, say $x_1, ..., x_n$ and a new variable for each unknown σ_i, say $y_1, ..., y_m$. We will now represent each equation as follows,

$$x_i^{a_{i1}\sigma_1 + a_{i2}\sigma_2 + ... + a_{im}\sigma_m} = x_i^{b_i}$$

for $i = 1, ..., n$. Hence the system becomes,

$$x_1^{a_{11}\sigma_1 + a_{12}\sigma_2 + ... + a_{1m}\sigma_m} ... x_n^{a_{n1}\sigma_1 + a_{n2}\sigma_2 + ... + a_{nm}\sigma_m} = x_1^{b_1} ... x_n^{b_n}.$$

And also we can write,

$$(x_1^{a_{11}} x_2^{a21} ... x_n^{a_{n1}})^{\sigma_1} ... (x_1^{a_{1m}} x_2^{a2m} ... x_n^{a_{nm}})^{\sigma_m} = x_1^{b_1} ... x_n^{b_n}.$$

Now is the time to use our new represented variables y_is. $(x_1^{a_{i1}} x_2^{ai1} ... x_n^{a_{i1}})$ for $i = 1, ..m$ can be viewed as the image of y_i for $i = 1, ..m$ under the following map,

$$\begin{aligned} \varphi : k[y_1, ..., y_m] &\longmapsto k[x_1, ..., x_n] \\ y_i &\longmapsto x_1^{a_{i1}} x_2^{ai1} ... x_n^{a_{i1}} \end{aligned}$$

Therefore $x_1^{b_1}...x_n^{b_n}$ becomes the image of $y_1^{\sigma_1}...y_m^{\sigma_m}$ under φ. Hence there exists a solution $(\sigma_1, ..., \sigma_m) \in \mathbb{N}^m$ of this integer programming problem if and only if $x_1^{b_1}...x_n^{b_n} \in \operatorname{Im}\varphi$ and if it is in the image then $x_1^{b_1}...x_n^{b_n} = \varphi(y_1^{\sigma_1}...y_m^{\sigma_m})$. By *Theorem 5.2.3* $x_1^{b_1}...x_n^{b_n} \in \operatorname{Im}\varphi$ if and only if $x_1^{b_1}...x_n^{b_n} \equiv h \mod G$ where $h \in k[y_1, ..., y_m]$. But there are more things that we should prove, since we want h to be a monomial(power product of $y_i's$). Now recall the construction of the ideal K in the previous section,it is generated by differences of two monomials(power products). Therefore Buchberger Algorithm (construction of S-polynomials) forces the Gröbner basis G to consist of differences of two monomials(power products). Since reduction of a power product by differences of power products gives a power product. $x_1^{b_1}...x_n^{b_n} \equiv h \mod G$, therefore h is a power product. Thus we have "Algorithm" to solve this problem.

1)Calculate the Gröbner Basis with respect to the elimination order where x variables are larger than the y variables, for the ideal K.

2)Look for h where $x_1^{b_1}...x_n^{b_n} \equiv h \mod G$ if h is not in $k[y_1, ..., y_m]$ then this means this problem does not have a solution if $h \in k[y_1, ..., y_m]$ and $h = y_1^{\sigma_1}...y_m^{\sigma_m}$, then $(\sigma_1, ..., \sigma_m) \in \mathbb{N}^m$ is a solution of the system.

Let us give an example to show this method.

Example 5.3.1.

$$\begin{aligned} 3\sigma_1 + 2\sigma_2 + \sigma_3 &= 10 \\ 4\sigma_1 + 3\sigma_2 + \sigma_3 &= 4 \end{aligned} .$$

Now we are looking for the pre-image of $x_1^{10}x_2^4$ *where*

$$\begin{aligned} \varphi : \mathbb{Q}[y_1, y_2, y_3] &\longmapsto \mathbb{Q}[x_1, x_2] \\ y_1 &\longmapsto x_1^3 x_2^4 \\ y_2 &\longmapsto x_1^2 x_2^3 \\ y_3 &\longmapsto x_1 x_2 \end{aligned}$$

Clearly $K = (y_1 - x_1^3x_2^4, y_2 - x_1^2x_2^3, y_3 - x_1x_2) \in \mathbb{Q}[x_1, x_2, y_1, y_2, y_3]$. *The Gröbner Basis for* K *(see appendix B.7)is,*

$$G = \{y_3 - x_1x_2, y_2 - x_2y_3^2, x_1y_2 - y_3^3, y_1 - y_2y_3\}.$$

One can see that G *does not contain elements like* $x_1 - h_1$ *and* $x_2 - h_2$ *where* $h_i \in \mathbb{Q}[y_1, y_2, y_3]$. *By* Theorem 5.2.4 *this means* φ *is not an onto map. Clearly this does not mean* $x_1^{10}x_2^4$ *is not an element of* $\operatorname{Im}\varphi$. *But in this case* $x_1^{10}x_2^4 \equiv x_1^6y_3^4 \mod G$ *and* $x_1^6y_3^4$ *is not an element of* $\mathbb{Q}[y_1, y_2, y_3]$. *Therefore this system does not have a solution.*

In the following case we will discuss a general solution method for the integer programming problem.

CASE 2: In this case we will consider the same problem without any constraints on a_{ij}'s and b_i's. But that means we have negative exponents on the x variables and this is the main problem if we want to work with the polynomial ring $k[x_1, ..., x_n]$. To deal with this problem, we will first introduce a new variable w where one can consider $w = 1/x_1, ..., x_n$ and then work in the ring $k[x_1, ..., x_n, w]/I$ where $I = (x_1...x_nw - 1)$. We want to convert negative integers to a non-negative ones to work with the polynomial rings. To do it, first we will choose non-negative integers a'_{i_j} and α_j for each $j = 1, ..., m$ and $i = 1, ..., n$ such that for each j we have,

$$(a_{1j}, ..., a_{nj}) = (a'_{1j}, ..., a'_{nj}) + \alpha_j(-1, ..., -1).$$

So the coset

$$x_1^{a_{1j}}...x_n^{a_{nj}} + I = x_1^{a'_{1j}}...x_n^{a'_{nj}}w^{\alpha_j} + I.$$

Similarly, use β instead of α

$$x_1^{b_1}...x_n^{b_n} + I = x_1^{b'_1}...x_n^{b'_n}w^{\beta_j} + I.$$

Now consider,

$$\begin{aligned} \varphi : k[y_1, ..., y_m] &\longmapsto k[x_1, ..., x_n]/I \\ y_i &\longmapsto x_1^{a'_{i1}}x_2^{a'_{i1}}...x_n^{a'_{i1}}w^{\alpha_i} + I \end{aligned}$$

Therefore $x_1^{b'_1}...x_n^{b'_n}w^{\beta_j} + I$ becomes the image of $y_1^{\sigma_1}...y_m^{\sigma_m}$ under φ.Hence we can say there exists a solution $(\sigma_1, ..., \sigma_m) \in \mathbb{N}^m$ of this integer programming problem if and only if $x_1^{b'_1}...x_n^{b'_n}w^{\beta_j} + I \in \operatorname{Im}\varphi$ and if it is in the image then $x_1^{b'_1}...x_n^{b'_n}w^{\beta_j} = \varphi(y_1^{\sigma_1}...y_m^{\sigma_m})$. By *Theorem 5.2.8* $x_1^{b'_1}...x_n^{b'_n}w^{\beta_j} + I \in \operatorname{Im}\varphi$ if and only if $x_1^{b'_1}...x_n^{b'_n}w^{\beta_j} + I \equiv h \mod G$ where $h \in k[y_1, ..., y_m]$. As in the previous case there are extra things that we should prove, since we want h to be a monomial(power product of $y'_i s$). Recall the construction of the ideal K in the Polynomial Mapping section,it is generated by differences of two monomials(power products). Therefore as in Case1 $x_1^{b_1}...x_n^{b_n}w^{\beta_j} \equiv h \mod G$, h is a power product. Thus the "Algorithm" solve this integer programming problem here is similar to the one in case1 to,

1)Calculate the Gröbner Basis for K with respect to the elimination order where x variables are larger than the y variables and where $K = (I, y_i - f_i : i = 1, .., m)$.

2)Look for h, where $x_1^{b'_1}...x_n^{b'_n}w^{\beta_j} + I \equiv h \mod G$ if h is not in $k[y_1, ..., y_m]$ then this means this problem does not have a solution if $h \in k[y_1, ..., y_m]$ and $h = y_1^{\sigma_1}...y_m^{\sigma_m}$, then $(\sigma_1, ..., \sigma_m) \in \mathbb{N}^m$ is a solution of the system.

Let us give an example to show this method.

Example 5.3.2.

$$\begin{aligned} 2\sigma_1 + \sigma_2 - 3\sigma_3 + \sigma_4 &= 4 \\ -3\sigma_1 + 2\sigma_2 - 2\sigma_3 - \sigma_4 &= -3 \end{aligned} .$$

First we will convert the negative exponents of x into a positive ones.

$$(2, -3, 0) = (5, 0, 1) + 3(-1, -1, -1), \quad x_1^2x_2^{-3} + I = x_1^5w + I$$

$$(1, 2, 0) = (1, 2, 0) + 0(-1, -1, -1), \quad x_1x_2^2 + I = x_1x_2^2 + I$$

$$(-3, -2, 0) = (0, 1, 1) + 3(-1, -1, -1), \quad x_1^{-3}x_2^{-2} + I = x_2w + I$$

$$(1, -1, 0) = (2, 0, 1) + (-1, -1, -1), \quad x_1x_2^{-1} + I = x_1^2w + I$$

$$(4, -3, 0) = (7, 0, 1) + 3(-1, -1, -1), \quad x_1^4x_2^{-3} + I = x_1^7w + I$$

We will look for the pre-image of $x_1^7w + I$ *where* $I = (x_1x_2w - 1)$ *and the map is,*

$$\begin{aligned} \varphi : \mathbb{Q}[y_1, y_2, y_3, y_4] &\longmapsto \mathbb{Q}[x_1, x_2, w]/I \\ y_1 &\longmapsto x_1^5w + I \\ y_2 &\longmapsto x_1x_2^2 + I \\ y_3 &\longmapsto x_2w + I \\ y_4 &\longmapsto x_1^2w + I \end{aligned}$$

Clearly $K = (x_1x_2w-1, y_1-x_1^5w, y_2-x_1x_2^2, y_3-x_2w, y_4-x_1^2w) \in \mathbb{Q}[x_1, x_2, w, y_1, y_2, y_3, y_4]$. *We used CoCoa to determine the Gröbner Basis and also to do the division algorithm in order to find the pre-image of* $x_1^7w + I$ *(see appendix B.8). The result was* $x_1^7w + I \equiv y_2^2y_3y_4^5 \in \mathbb{Q}[y_1, y_2, y_3, y_4]$. *Therefore a solution of this problem is* $(0, 2, 1, 5)$.

Now we will go back to the original problem and find a solution that minimizes the "cost function",$c(\sigma_1, ..., \sigma_m) = \sum_{j=1}^m c_j\sigma_j$. *First we will define a term order,*

Definition 5.3.3. *A monomial order* $<_c$ *on the y variables is said to be compatible with the cost function c and the map* φ *if*

$$\left.\begin{array}{l} \varphi(y_1^{\sigma^1}...y_m^{\sigma_m}) = \varphi(y_1^{\sigma'_1}...y_m^{\sigma'_m}) \\ \textit{and} \\ c(\sigma_1, ..., \sigma_m) = (\sigma'_1, ..., \sigma'_m) \end{array}\right\} \implies y_1^{\sigma^1}...y_m^{\sigma_m} <_c y_1^{\sigma'_1}...y_m^{\sigma'_m}.$$

Proposition 5.3.4. *Let* G *be a Gröbner Basis for* K *with respect to the elimination order* x *and* w *variables larger than the* y *variables and order* $<_c$ *on the* y *variables compatible with the cost function* c *and the map* φ. *If* $x_1^{b'_1}...x_m^{b'_m}w^\beta \equiv y_1^{\sigma^1}...y_m^{\sigma_m} \mod G$ *then* $(\sigma_1, ..., \sigma_m)$ *is a solution which minimizes the cost function.*

Proof. Let $x_1^{b'_1}...x_m^{b'_m}w^\beta \equiv y_1^{\sigma^1}...y_m^{\sigma_m} \mod G$ and $(\sigma_1, ..., \sigma_m)$ be a solution of the system. Now assume there is another solution $(\sigma'_1, ..., \sigma'_m)$ such that $\sum_{j=1}^m c_j\sigma'_j < \sum_{j=1}^m c_j\sigma_j$. Since they are both solutions

$$\varphi(y_1^{\sigma_1}...y_m^{\sigma_m}) = \varphi(y_1^{\sigma'_1}...y_m^{\sigma'_m}) = x_1^{b'_1}...x_m^{b'_m}w^\beta + I$$

$y_1^{\sigma_1}...y_m^{\sigma_m} - y_1^{\sigma'_1}...y_m^{\sigma'_m} \in \operatorname{Ker}\varphi \subseteq K$. Hence $y_1^{\sigma_1}...y_m^{\sigma_m} - y_1^{\sigma'_1}...y_m^{\sigma'_m} \equiv 0 \mod G$. Since $y_1^{\sigma_1}...y_m^{\sigma_m} >_c y_1^{\sigma'_1}...y_m^{\sigma'_m}$ by tour assumption, $LT(y_1^{\sigma_1}...y_m^{\sigma_m} - y_1^{\sigma'_1}...y_m^{\sigma'_m}) = y_1^{\sigma_1}...y_m^{\sigma_m}$. But $y_1^{\sigma_1}...y_m^{\sigma_m}$ is reduced with respect to G, and therefore $y_1^{\sigma_1}...y_m^{\sigma_m} - y_1^{\sigma'_1}...y_m^{\sigma'_m}$ can not reduce to 0 by G.

□

Chapter 6

BORDER BASES

In this chapter we will discuss another bases which we can apply to the problems where Gröbner Basis don't give the kind of results we want or we need a better(faster) algorithm than Buchberger's Algorithm. This is described as the theory of border bases of zero-dimensional polynomial ideals[11]. We will discuss the advantages and disadvantages of using Gröbner Bases or Border Bases on examples at chapter eight. We will start this chapter by giving the notations and definitions we will use through the rest of the thesis.

Let k be a field and $R = k[x_1, ..., x_n]$. We will denote the set of monoid terms in R with $\mathbb{T}^n$. Also we have $T_1^n.\mathbb{T}_1^n....\mathbb{T}_1^n = (\mathbb{T}^n)^k = \mathbb{T}_k^n$.

Definition 6.0.5. *Let I be an ideal of R if R/I is a finite dimensional vector space then I is called a zero-dimensional ideal.*

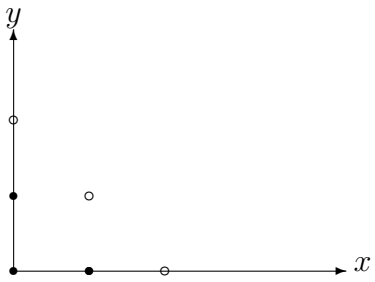
Definition 6.0.6. *A non-empty set of terms $\mathcal{O} \subseteq \mathbb{T}^n$ is called an order ideal if $t \in \mathcal{O}$, then $t' \in \mathcal{O}$ or every t' dividing t. The border of $\mathcal{O}$ is the set of the terms*

$$\partial\mathcal{O} = \mathbb{T}_1^n.\mathcal{O}\backslash\mathcal{O} = (x_1\mathcal{O} \cup ... \cup x_n\mathcal{O})\backslash\mathcal{O}$$

and the first border closure of $\mathcal{O}$ is $\overline{\partial\mathcal{O}} = \mathcal{O} \cup \partial\mathcal{O}$. For every $k \geqslant 1$, we inductively define the (k+1)st border $\partial^{k+1}\mathcal{O} = \partial(\overline{\partial^k\mathcal{O}})$ and the (k+1)st border closure $\overline{\partial^{k+1}\mathcal{O}} = \overline{\partial^k\mathcal{O}} \cup \partial^{k+1}\mathcal{O}$. We let $\partial^0\mathcal{O} = \overline{\partial^0\mathcal{O}} = \mathcal{O}$. [8]

Let us give an example to visualize the idea.

Example 6.0.7. *Let $\mathcal{O} = \{1, x, y\} \subseteq \mathbb{T}^n$. Clearly $\mathcal{O}$ is a order ideal with border $\partial\mathcal{O} = \{x^2, y^2, xy\}$. In the diagram disks represent the elements of the order ideal and the circles represent the elements of the border.*



Next proposition shows the properties of the border of an order ideal.

Proposition 6.0.8. *Let $\mathcal{O}$ be an order ideal.*

i)For every $k \geqslant 1$, we have disjoint union $\partial^k\mathcal{O} = \cup_{i=0}^{k}\partial^i\mathcal{O}$. Consequently, we have a disjoint union $\mathbb{T}^n = \cup_{i=0}^{\infty}\partial^i\mathcal{O}$.

ii)For every $k \geqslant 1$, we have $\partial^k\mathcal{O} = \mathbb{T}_k^n.\mathcal{O}\backslash\mathbb{T}_{<k}^n.\mathcal{O}$.

iii) A term $t \in \mathbb{T}^n$ is divisible by a term in $\partial\mathcal{O}$ if and only if $t \in \mathbb{T}^n\backslash\mathcal{O}$.

Proof. i)By definition of border we have

$$\overline{\partial\mathcal{O}} = \mathbb{T}_1^n\mathcal{O} \cup \mathcal{O} = \mathcal{O} \cup \partial\mathcal{O}$$

$$\overline{\partial^2\mathcal{O}} = \overline{\partial\mathcal{O}} \cup \mathbb{T}_1^n\overline{\partial\mathcal{O}} = \overline{\partial\mathcal{O}} \cup \mathbb{T}_2^n\mathcal{O} = \overline{\partial\mathcal{O}} \cup \partial^2\mathcal{O} = \mathbf{0} \cup \partial\mathcal{O} \cup \partial^2\mathcal{O}$$

$$\overline{\partial^3\mathcal{O}} = \overline{\partial^2\mathcal{O}} \cup \mathbb{T}_1^n\overline{\partial^2\mathcal{O}} = \overline{\partial^2\mathcal{O}} \cup \mathbb{T}_3^n\mathcal{O} = \overline{\partial^2\mathcal{O}} \cup \partial^3\mathcal{O} = \mathbf{0} \cup \partial\mathcal{O} \cup \partial^2\mathcal{O} \cup \partial^3\mathcal{O}$$

$\dots$

$$\overline{\partial^k\mathcal{O}} = \overline{\partial^{k-1}\mathcal{O}} \cup \mathbb{T}_1^n\overline{\partial^{k-1}\mathcal{O}} = \overline{\partial^{k-1}\mathcal{O}} \cup \mathbb{T}_k^n\mathcal{O} = \overline{\partial^{k-1}\mathcal{O}} \cup \partial^k\mathcal{O} = \mathbf{0} \cup \partial\mathcal{O} \cup \partial^2\mathcal{O} \cup \dots \cup \partial^k\mathcal{O}$$

Therefore

$$\overline{\partial^k\mathcal{O}} = \mathbf{0} \cup \partial\mathcal{O} \cup \partial^2\mathcal{O} \cup \partial^3\mathcal{O} \cup \dots \cup \partial^k\mathcal{O} = \bigcup_{i=0}^{k}\partial^i\mathcal{O}.$$

And clearly $\mathbb{T}^n = \cup_{i=0}^{\infty}\partial^i\mathcal{O}$.

ii) From the definition of border basis we know that

$$\partial^{k+1}\mathcal{O} = \partial(\overline{\partial^k\mathcal{O}}) = \mathbb{T}_1^n\overline{\partial^k\mathcal{O}}\backslash\overline{\partial^k\mathcal{O}}$$

and also

$$\overline{\partial^{k+1}\mathcal{O}} = \overline{\partial^k\mathcal{O}} \cup \partial^{k+1}\mathcal{O}.$$

As a consequence of these $\partial^{k+1}\mathcal{O} = \overline{\partial^{k+1}\mathcal{O}}\backslash\overline{\partial^k\mathcal{O}}$. We also have $\overline{\partial^{k+1}\mathcal{O}} = \mathbb{T}_{k+1}^n\mathcal{O}$ and $\overline{\partial^k\mathcal{O}} = \mathbb{T}_k^n$. Therefore $\partial^{k+1}\mathcal{O} = \mathbb{T}_{k+1}^n.\mathcal{O}\backslash\mathbb{T}_k^n\mathcal{O}\mathcal{O}$.

iii) Let $t \in \mathbb{T}^n$ and $t \neq 0$. Assume t is divisible by $t'' \in \partial\mathcal{O}$. That is $t'' \in \mathbb{T}^n\backslash\mathcal{O}$. If $t \in \mathcal{O}$, then since $\mathcal{O}$ is an order ideal $t'' \in \mathcal{O}$. But then $t'' \in \partial\mathcal{O} \cap \mathcal{O} = \emptyset$. Therefore $t \in \mathbb{T}^n\backslash\mathcal{O}$. For the converse assume $t \in \mathbb{T}^n\backslash\mathcal{O}$. If $t \in \mathbb{T}^n\backslash\mathcal{O} = \cup_{i=0}^{\infty}\partial^i\mathcal{O}\backslash\mathcal{O}$, then there exists $k \in \mathbb{N}$ such that $t \in \partial^k\mathcal{O}\backslash\mathcal{O} = \mathbb{T}_k^n\partial\mathcal{O}\backslash\mathcal{O}$. Therefore $\exists t'' \in \partial\mathcal{O}$ such that $t = t't''$. □

The properties of border of the order ideal lead us to measure the "distance" of a term from an order ideal. To do this we define $ind_{\mathcal{O}}(t) = min\{k \geqslant 0 : t \in \overline{\partial^k\mathcal{O}}\}$ for every term $t \in \mathbb{T}^n$,which is unique, and call it the *index* of t with respect to $\mathcal{O}$. Given a non-zero polynomial $f = c_1t_1+...+c_st_s \in R$ where $c_1, ..., c_s \in k\backslash\{0\}$ and $t_1, ..., t_s \in \mathbb{T}^n$, we order the terms in the support of f such that $ind_{\mathcal{O}}(t_1) \geqslant ind_{\mathcal{O}}(t_2) \geqslant ... \geqslant ind_{\mathcal{O}}(t_s)$. Then we call $ind_{\mathcal{O}}(f) = ind_{\mathcal{O}}(t_1)$ the index of f.[8]

Now we will prove a useful lemma and then we will show the properties of the index.

Lemma 6.0.9. *For any $f, g \in R$ we have $Supp(f + g) \subseteq Supp(f) \cup Supp(g)$.*

Proof. Let $f = \sum_{i=1}^{n} c_it_i$ and $g = \sum_{j=1}^{n'} c'_jt'_j$ where $c'_j, c_i \in k$, $n, n' \in \mathbb{N}$ and $t, t' \in \mathbb{T}^n$. If we take the sum, we will have

$$f + g = \sum_{t\in\mathbb{T}^n}(\sum_{i:t_i=t} c_i + \sum_{j:t_j=t} c'_j)t.$$

Therefore $Supp(f + g) \subseteq Supp(f) \cup Supp(g)$.

□

Proposition 6.0.10. *Let $\mathcal{O} \subseteq \mathbb{T}^n$ be an order ideal.*

i) *For a term $t \in \mathbb{T}^n$, the number $k = ind_{\mathcal{O}}(t)$ is the smallest natural number such that $t = t't''$ with $t' \in \mathbb{T}^n_k$ and $t' \in \mathcal{O}$.*

ii)*Given two terms $t, t'' \in \mathbb{T}^n$ we have $ind_{\mathcal{O}}(tt') \leqslant deg(t) + ind_{\mathcal{O}}(t')$.*

iii)*For a non-zero polynomials $f, g \in R$ such that $f+g \neq 0$, we have the inequality $ind_{\mathcal{O}}(f+g) \leqslant max\{ind_{\mathcal{O}}(f), ind_{\mathcal{O}}(g)\}$.*

iv)*For a non-zero polynomials $f, g \in R$, we have the inequality*

$$ind_{\mathcal{O}}(fg) \leqslant min\{deg(f) + ind_{\mathcal{O}}(g), deg(g) + ind_{\mathcal{O}}(f)\}$$

Proof. **i)**Let $k = ind_{\mathcal{O}}(t)$. Then

$$\begin{aligned} t \in \partial^k\mathcal{O} &= \partial(\overline{\partial^{k-1}\mathcal{O}}) \\ &= \mathbb{T}^n_1\overline{\partial^{k-1}\mathcal{O}}\backslash\overline{\partial^{k-1}\mathcal{O}} \\ &= \mathbb{T}^n_k\mathcal{O}\backslash\overline{\partial^{k-1}\mathcal{O}} \\ &= \mathbb{T}^n_k\mathcal{O}\backslash \cup_{i=0}^{k-1} \partial^i\mathcal{O}. \end{aligned}$$

Therefore there exists $t' \in \mathbb{T}^n_k$ and $t'' \in \mathcal{O}$ such that $t = t't''$. Since k is unique it is the smallest number that satisfy the previous equation.

ii) Let $ind_{\mathcal{O}}(tt') = k$. Then

$$tt' \in \mathbb{T}^n_k\mathcal{O}\backslash\overline{\partial^{k-1}\mathcal{O}} = \mathbb{T}^n_{k-1}\partial\mathcal{O}\backslash\overline{\partial^{k-1}\mathcal{O}} = ... = \mathbb{T}^n_1\partial^{k-1}\mathcal{O}\backslash\overline{\partial^{k-1}\mathcal{O}}.$$

Let $deg(t) \geqslant m$, $m \in \mathbb{N}$. Then $tt' \in \mathbb{T}^n_m\partial^{k-m}\mathcal{O}\backslash\overline{\partial^{k-1}\mathcal{O}}$ and $ind_{\mathcal{O}}(t') = k-m$. Therefore $k = ind_{\mathcal{O}}(tt') \leqslant ind_{\mathcal{O}}(t') + deg(t)$.

iii)Let $t_f \in Supp(f)$ and $t_g \in Supp(g)$. And recall lemma 6.0.9.

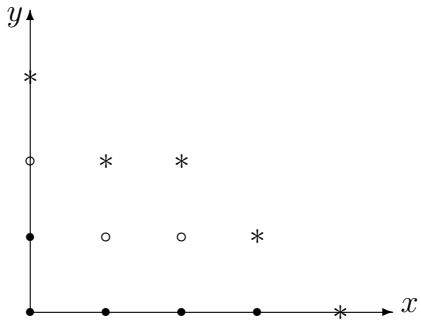
$$\begin{aligned} ind_{\mathcal{O}}(f+g) &= max\{ind_{\mathcal{O}}(t) : t \in Supp(f+g)\} \\ &\leqslant \{ind_{\mathcal{O}}(t) : t \in Supp(f) \cup Supp(g)\} \\ &\leqslant max\{ind_{\mathcal{O}}(t_f), ind_{\mathcal{O}}(t_g)\} \\ &= max\{ind_{\mathcal{O}}(f), ind_{\mathcal{O}}(g)\} \end{aligned}$$

iv) Clearly we have $Supp(fg) \subseteq \{t_f t_g : t_f \in Supp(f), t_g \in Supp(g)\}$.

$$\begin{aligned} ind_{\mathcal{O}}(fg) &= max\{ind_{\mathcal{O}}(t_f t_g) : t_f t_g \in Supp(fg)\} \\ &\leqslant \{ind_{\mathcal{O}}(t_f t_g) : t_f \in Supp(f), t_g \in Supp(g)\} \\ &\leqslant min\{ind_{\mathcal{O}}(t_f) + deg(t_g), ind_{\mathcal{O}}(t_g) + deg(t_f)\} \end{aligned}$$

□

Example 6.0.11. *Let $\mathcal{O} = \{1, x, x^2, y\} \subseteq \mathbb{T}^n$. Clearly $\mathcal{O}$ is a order ideal with border $\partial\mathcal{O} = \{x^3, xy, y^2, x^2y\}$ and $\partial^2 = \{x^4, x^2y^2, xy^2, x^3y, y^3\}$. In the diagram disks represent the elements of the order ideal and the circles represent the elements of the first and stars represent the elements of the second border.*



If we consider index as an order, we will have a problem with multiplication. Since $x^2 \in \mathcal{O}$, $ind_{\mathcal{O}}(x^2) = 0$ and since $xy \in \partial\mathcal{O}$, $ind_{\mathcal{O}}(xy) = 1$. We have

$$ind_{\mathcal{O}}(x^2) < ind_{\mathcal{O}}(xy).$$

If we multiply x^2 and xy with x^2, we will end up with

$$ind_{\mathcal{O}}(x^2x^2) = ind_{\mathcal{O}}(x^2xy) = 2.$$

That example implies that index is not compatible with multiplication. However it is not compatible with multiplication, it allows us to measure a distance of term from the order ideal and also it gives a partial ordering on the set of the terms. Therefore it allows us to introduce a new algorithm that takes place of the Division Algorithm which uses term ordering.

6.1 The Border Division Algorithm

Before giving the algorithm we will a give the definition of $\mathcal{O}-$border prebasis which took an essential part in the Border division algorithm.

Definition 6.1.1. *Given an order ideal $\mathcal{O} \subseteq \mathbb{T}^n$ with border $\partial\mathcal{O} = \{b_1, ..., b_\upsilon\}$, a set of polynomials $\{g_1, ..., g_\upsilon\}$ be an $\mathcal{O}-$border prebasis if the polynomials have the form $g_i = b_i - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ where $\alpha_{ij} \in k$ for $1 \leqslant i \leqslant \mu$ and $t_i \in \mathcal{O}$. [8]*

Proposition 6.1.2 (*The Border Division Algorithm*)**.** *Let $\mathcal{O} = \{t_1, ..., t_\mu\}$ be an order ideal, let $\partial\mathcal{O} = \{b_1, ..., b_\upsilon\}$ be its border, and let $\{g_1, ..., g_\upsilon\}$ be an $\mathcal{O}-$border prebasis. Given a polynomial $f \in R$, consider the following instructions.*

1. *Let $f_1 = f_2 = ... = f_\upsilon = 0$, $c_1 = ... = c_\mu = 0$ and $h = f$.*

2.*If $h = 0$ then return $(f_1, ..., f_\upsilon, c_1, ..., c_\mu)$ and stop.*

3.*If $ind_{\mathcal{O}}(h) = 0$ then find $c_1 = ... = c_\mu \in k$ such that $h = a_1c_1 + ... + a_\mu c_\mu$ and return $(f_1, ..., f_\upsilon, c_1, ..., c_\mu)$ and stop.*

4. *If $ind_{\mathcal{O}}(h) > 0$ then let $h = a_1h_1 + ... + a_sh_s$ with $a_1, ..., a_s \in k\backslash\{0\}$ and $h_1, ..., h_s \in \mathbb{T}^n$ such that $ind_{\mathcal{O}}(h_1) = ind_{\mathcal{O}}(h_1)$. Determine the smallest label $i \in \{1, ..., \upsilon\}$ such that h_1 factors as $h_1 = t'b_i$ with a term t' of degree $ind_{\mathcal{O}}(h) - 1$. Subtract $a_1t'g_i$ from h, add a_1t' to f_i and continue with step 2.*

This algorithm returns a tuple $(f_1, ..., f_\upsilon, c_1, ..., c_\mu) \in R^\upsilon \times k^\mu$ such that

$$f = f_1g_1 + ... + f_\upsilon g_\upsilon + c_1t_1 + ... + c_\mu t_\mu$$

and $deg(f_i) \leqslant ind_{\mathcal{O}}(f) - 1$ for all $i \in \{1, ..., \upsilon\}$ with $f_ig_i \neq 0$. This representation does not depend on the choice of the term h_1 in step D4. [8]

Proof. The instructions can be executed since in step **3** the fact that $ind_{\mathcal{O}}(h) = 0$ implies support of h is in $\mathcal{O}$. In step **4** we write h as a linear combination of terms and at least one of them, say h_1, has to have index $k = ind_{\mathcal{O}}(h) > 0$. By *Proposition*6.0.10a), there is a factorization $h_1 = t\ t_i$ with $t\ \in \mathbb{T}_k^n$ and $t_i \in \mathcal{O}$, and there is no such factorization with a term t of smaller degree. Since $k > 0$, we can write $t\ = t'x_j$ for some $t' \in \mathbb{T}^n$ and $j \in \{1, ..., n\}$. Then we have $deg(t') = k - 1$, and

the fact that t has the smallest possible degree implies $x_j t_i \in \partial\mathcal{O}$. Thus we see that $h_1 = t'(x_j t_i) = t' b_k$ for some $b_k \in \partial\mathcal{O}$.

This algorithm terminates after finitely many steps. In order to show it we will first check the subtraction $h - a_1 t' g_i$ in step **4**. By definition of the prebasis elements, we have

$$h - a_1 t' g_i = a_1 h_1 + ... + a_s h_s - a_1 t' b_i + a_1 t' \sum_{k=1}^{\mu} \alpha_{ki} t_k$$

where $\alpha_{ki} \in k$ for $k = 1, ..., \mu$. We had $ind_{\mathcal{O}}(h_1) = k$ with the highest index and $a_1 h_1 = a_1 t' b_i$. Therefore h is replaced by the terms with of the form $t' t_l \in \overline{\partial^{k-1}\mathcal{O}}$ which have smaller index. Therefore this algorithm terminates after finitely many steps, since there are only finitely many terms of smaller or equal index.

To prove the correctness of the equation, we will show

$$f = h + f_1 g_1 + ... + f_\upsilon g_\upsilon + c_1 t_1 + ... + c_\mu t_\mu$$

is invariant of the algorithm. A polynomial is only changed at step **4**. There the subtraction $h - a_1 t' g_i$ is compensated by the addition $(f_i + a_1 t') g_i$. The constants $c_1, ..., c_\mu$ are only changed in step **3** in which h is replaced by the expression $c_1 t_1 + ... + c_\mu t_\mu$. when the algorithm stops, we have $h = 0$. This proves the stated representation of f.

And also this representation does not depend on the choice of h_1 in step **4** since h_1 is replaced by terms of strictly smaller index. Thus the reduction of several terms of a given index in h, in step **4** do not interfere with one another and the final result is independent of the order in which they are taken care of. [8] □

Although Step **4** of the algorithm does not force us to choose the label i minimally in $h_1 = t' t_i$, we do this in order determine the representation of h uniquely. Therefore the result depends on the numbering of the elements of the border of the order ideal $\mathcal{O}$.

Now we will give an example to show how this Border Division Algorithm works.

Example 6.1.3. *Let* $R = \mathbb{Q}[x, y]$ *and let* $\mathcal{O} = \{1, x, y\}$. *Then the first border* $\partial\mathcal{O} = \{x^2, xy, y^2\}$, *where* $b_1 = x^2, b_2 = xy, b_3 = y^2$ *second border* $\partial^2\mathcal{O} = \{x^3, xy^2, x^2 y, y^3\}$

and the third border $\partial^3\mathcal{O} = \{x^4, x^3y, x^2y^2, xy^3, y^4\}$. *Let the* $\mathcal{O}$*-border prebasis be* $G = \{x^2 - x, xy - 1, y^2\}$ *where* $g_1 = x^2 - x, g_2 = xy - 1, g_3 = y^2$. *We apply border division algorithm to the polynomial* $f = x^2y^2 + xy^2 + y$

1) *Let* $f_1 = f_2 = f_3 = 0$ *and* $c_1 = c_2 = c_3 = 0$ *as well as* $h = f$.

2) $ind_{\mathcal{O}}(h) = 3$ *we have* $h_1 = x^2y^2 = t'(x_jt_i)$ *where* $x_j \in \{x, y\}$ *and* $t_i \in \mathcal{O}$ *and* $deg(t') = 2$. *Hence we have three options*

case1) *If* $t' = x^2$, *then we have* $h_1 = x^2(y^2)$ *where* $y^2 = b_3$ *and the label* $i = 3$.

case2) *If* $t' = y^2$, *then we have* $h_1 = y^2(x^2)$ *where* $x^2 = b_1$ *and the label* $i = 1$.

case3) *If* $t' = xy$, *then we have* $h_1 = xy(xy)$ *where* $xy = b_2$ *and the label* $i = 2$.

We will choose the label i *minimally in order to determine this step of the algorithm uniquely which implies we set* $h_1 = y^2b_1$. *As you will see that the result will depend on the numbering of the elements. Thus we let* $f_1 = y^2$ *and*

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

2)*The terms in the support* h *is* $2xy^2 + y$. *We have* $ind_{\mathcal{O}} = 2$, *and* $t' = x$ *or* $t' = y$. *As we did previously we will choose the minimal label. Setting* $t' = x$ *will make* $h = xb_3$ *and* $t' = y$ *will make* $h = yb_2$. *Hence we set* $h = yb_2$ *and* $f_2 = 2y$. *The terms in the support of* h *are* $3y \in \mathcal{O}$.

3) $ind_{\mathcal{O}} = 0$, *we have* $y = t_3$ *and* $c_3 = 3$.

Therefore the result is

$$f = y^2g_1 + 2yg_2 + 0g_3 + 3t_3.$$

Let us fix $\mathcal{G} = (g_1, ..., g_v)$ which makes the result of the Border Division Algorithm unique. So for an order ideal $\mathcal{O} = \{t_1, ..., t_\mu\}$ and $f \in R$ by the border division algorithm we will have $f = f_1g_1 + ... + f_vg_v + c_1t_1 + ... + c_\mu t_\mu$. Then $c_1t_1 + ... + c_\mu t_\mu = NR_{\mathcal{O},\mathcal{G}}$ is called the normal $\mathcal{O}$-remainder and it represent the same residue class with f modulo $(g_1, ..., g_v)$.

6.2 Existence and Uniqueness of Border Basis

Definition 6.2.1. *Let $G = \{g_1, ..., g_v\}$ be an $\mathcal{O}-$border prebasis, let $\mathcal{G}$ be the tuple $(g_1, ..., g_v)$ and let $I \subseteq R$ be an ideal containing G. The set G or the tuple $\mathcal{G}$ called an $\mathcal{O}$-border basis of I if one of the following equivalent conditions is satisfied.[11]*

a)The residue classes $\overline{\mathcal{O}} = \{\overline{t_1}, ..., \overline{t_\mu}\}$ form a $k-$vector space basis of R/I.

b)We have $I \cap \langle \mathcal{O} \rangle_k = 0$.

c)We have $R = I \oplus \langle \mathcal{O} \rangle_k$.

Proposition 6.2.2. *Let G be an $\mathcal{O}$-border basis of an ideal $I \subseteq R$. Then the ideal I is generated by G.*

Proof. By definition $(g_1, ..., g_v) \subseteq I$. For the converse we will use border division algorithm. Let $f \in I$ and apply border division algorithm to f we will end up with

$$f = f_1 g_1 + ... + f_v g_v + c_1 t_1 + ... + c_\mu t_\mu$$

where $f_i \in R$ and $c_i \in k$ and $\{t_1, ..., t_\mu\} = \mathcal{O}$. Since $\mathcal{G} \subseteq I$, $f_1 g_1 + ... + f_v g_v \in I$. Since $f \in I$ $c_1 t_1 + ... + c_\mu t_\mu \in I \cap \langle \mathcal{O} \rangle_k = \{0\}$. Therefore $I = (g_1, ..., g_v)$. □

For a given $f \in R$, recall that the remainder of the General Polynomial Division was not unique, unless we use Gröbner Basis. And also the result of the Border Division Algorithm was not unique. But similar to the General Polynomial Division, the result of the Border Division Algorithm is unique if we use the element of the Border Basis.

Definition 6.2.3. *Let k be a field $R = k[x_1, ..., x_n]$ a polynomial ring, $I \subseteq P$ an ideal of R and $k' \subseteq k$ be a subfield of k. I is* defined over *k' if there exists elements $k'[x_1, ..., x_n]$ which generate I as an ideal of R. k' is called a* field of definition *of I if I is defined over k' and there exists no proper subfield $k'' \subset k$ such that I is defined over k''.*

Proposition 6.2.4. *Let $\mathcal{O} = \{t_1, ..., t_\mu\}$ be an order ideal,$\partial\mathcal{O} = \{b_1, ..., b_v\}$ be its border, let $I \subseteq R$ be a zero-dimensional ideal and assume that the residue classes of the elements of $\mathcal{O}$ form a $k-$vector space basis of R/I.*

a)There exists a unique $\mathcal{O}$-border basis of I.

b)Let G be an order prebasis whose elements are in I. Then G is the $\mathcal{O}$-border basis of I.

c)Let k' be the field of definition of I. Then the $\mathcal{O}$-border basis of I is contained in $k'[x_1, ..., x_n]$.

Proof. **a)**By definition of border $\partial\mathcal{O} = \mathbb{T}^n\mathcal{O}\backslash\mathcal{O}$, i.e., b_i are not elements of $\langle\mathcal{O}\rangle_k$ which forms a $k-$vector space of R/I, and $b_i \in R/I$, hence they are linearly dependent. Therefore b_i can be written as $b_i = g_i + \sum_{j=1}^{\mu} \alpha_{ij}t_j$ and so $g_i = b_i - \sum_{j=1}^{\mu} \alpha_{ij}t_j \in I$ with $t_j \in \mathcal{O}$ and $\alpha_{ij} \in k\backslash\{0\}$. Then $G = \{g_1, ..., g_\upsilon\}$ is an $\mathcal{O}$-border prebasis of I which also implies G is a $\mathcal{O}$-border basis of I since $\mathcal{O}$ forms a vector space basis for R/I. Now we will prove the uniqueness. Assume there exists another $\mathcal{O}$-border basis $G' = \{g'_1, ..., g'_\upsilon\}$. There exists an index $i \in \{1, ..., \upsilon\}$ such that $g'_i = b_i - \sum_{j=1}^{\mu} \alpha'_{ij}t_j$ where $\alpha_{ij'} \neq \alpha_{ij}$. Then $0 \neq g_i - g'_i \in I$ with

$$Supp(g_i - g'_i) = t_{j\in\mathcal{O}}.$$

Therefore $g_i - g'_i \in I \cap \langle\mathcal{O}\rangle_k = 0$, i.e., $G = G'$.

b) $G = \{g_1, ..., g_\upsilon\}$ is a $\mathcal{O}-$border prebasis where $G \subseteq I$. Since the elements of $\overline{\mathcal{O}}$ forms a $k-$vector space basis for R/I, G is a $\mathcal{O}-$border basis and by part **a)** it is unique.

c) Let $R' = k'[x_1, ..., x_n]$, $I' = R' \cap I$ and σ be a a given term ordering. If G is a Gröbner basis of I' with respect to the term order σ, then G generates the ideal I' and the the set I' generates I since k' is the field of definition of I. Therefore G is the Gröbner Basis of I, too. And by definition of Gröbner Basis $LT\{I\} = LT\{I'\}$, and this implies $\mathbb{T}^n\backslash LT\{I\} = \mathbb{T}^n\backslash LT\{I'\}$ with respect to the σ. Therefore $dim(R'/I) = dim(R/I)$. The elements of $\mathcal{O}$ is contained in R' and they are linearly independent. Let G' be a $\mathcal{O}$-border basis of I'. Then G' is a $\mathcal{O}$-border prebasis and $G' \subseteq I$. By part **b)** G' is $\mathcal{O}$-border basis of I. □

Chapter 7

GRÖBNER BASIS VERSUS BORDER BASIS

The main reason the border basis is introduced was to get rid of the difficulties that is caused by the Buchberger Algorithm where the number of S-polynomials is getting so large and to keep the advantages that Gröbner basis has. Therefore, we can find similar and different properties between border bases and Gröbner basis. Hence we can characterize border bases similar to characterizations of Gröbner basis. And also additionally we will find a totally different characterization of border bases from Gröbner Basis.

7.1 Characterization of Border Bases That is Similar to The Characterization of Gröbner Bases

Proposition 7.1.1. *Let $G = \{g_1, ..., g_\upsilon\}$ be a $\mathcal{O}$-border prebasis where $\mathcal{O} = \{t_1, ..., t_\mu\}$ is an order ideal of a zero-dimensional ideal I that is genarated by G and $\partial\mathcal{O} = \{b_1, ..., t_\upsilon\}$ is the border. G is a $\mathcal{O}$-border basis if and only if the equivalent conditions are satisfied.*

i) *For every $f \in I\backslash\{0\}$ there exists $f_1, ..., f_\upsilon \in R$ such that $f = f_1g_1 + ... + f_\upsilon g_\upsilon$ and $deg(f_i) \leqslant ind_\mathcal{O}(f) - 1$ where $f_i \neq 0$.*

ii)*For every $f \in I\backslash\{0\}$ there exists polynomials $f_1, ..., f_\upsilon \in R$ such that $f = f_1g_1 + ... + f_\upsilon g_\upsilon$ and $max\{deg(f_i) : i \in \{1, ..., \upsilon\}, f_i \neq 0\} = ind_\mathcal{O}(f) - 1$.*

Proof. **i)** Assume G is a $\mathcal{O}$-border basis of I then we will show **i** holds. By border division algorithm we have $f = f_1g_1 + ... + f_\upsilon g_\upsilon + c_1t_1 + ... + c_\mu t_\mu$ where $t_i \in \mathcal{O}$, $g_i \in G$ and $deg(f_i) \leqslant ind_\mathcal{O}(f) - 1$ for every $i = \{1, ..., \upsilon\}$. Therefore $0 = c_1t_1 + ... + c_\mu t_\mu \in I \cap \langle\mathcal{O}\rangle_k$, i.e., $c_1 = ... = c_\mu = 0$.

ii) We have $ind_{\mathcal{O}}(f_i g_i) < deg(f_i) + ind_{\mathcal{O}}(g_i)$ where $g_i = b_i - \sum_{i=1}^{\mu} \alpha_{ij} t_i$. Since $b_i \in \partial\mathcal{O}$, $ind_{\mathcal{O}} = 1$. Hence

$$ind_{\mathcal{O}}(f_i g_i) \leqslant deg(f_i) + ind_{\mathcal{O}}(g_i) = deg(f_i) + 1 < ind_{\mathcal{O}}(f).$$

That implies $deg(f_i) < ind_{\mathcal{O}}(f) - 1$. Also we have $ind_{\mathcal{O}}(f+g) \leqslant max\{ind_{\mathcal{O}}(f), ind_{\mathcal{O}}(g)\}$ which implies

$$ind_{\mathcal{O}}(f) = ind_{\mathcal{O}}(f_1 g_1 + ... + f_\upsilon g_\upsilon) \leqslant max\{ind_{\mathcal{O}}(f_i g_i) : i = 1, ..., \upsilon\}.$$

Therefore there is at least one $i \in \{1, ..., \upsilon\}$ such that $max\{deg(f_i) : i \in \{1, ..., \upsilon\}, f_i \neq 0\} = ind_{\mathcal{O}}(f) - 1$.

iii) Now we will assume **ii)** holds and we will prove that G is $\mathcal{O}-$border basis for I by showing $I \cap \langle\mathcal{O}\rangle_k = \{0\}$. Assume $\exists f$ such that $f \in I \cap \langle\mathcal{O}\rangle_k$. So we can represent f as follows, $f = c_1 t_1 + ... + c_\mu t_\mu$ and also we have $f = f_1 g_1 + ... + f_\upsilon g_\upsilon$. From **ii)**

$$max\{deg(f_i) : i = 1, ..., \upsilon\} = ind_{\mathcal{O}}(f) - 1 = max\{ind_{\mathcal{O}}(t_i) : i = 1, ..., \mu\} = -1.$$

Therefore $f_i = 0$ for every $i = 1, ..., \upsilon$ and $c_j = 0$ for every $j = 1, ..., \mu$, i.e., $f = 0$. □

Definition 7.1.2. *Given $f \in R$, we write $f = a_1 u_1 + ... + a_s u_s$ with coefficients $a_1, ..., a_s \in k\backslash\{0\}$ and terms $u_1, ..., u_s \in \mathbb{T}^n$ satisfying $ind_{\mathcal{O}}(u_1) \geqslant ... \geqslant ind_{\mathcal{O}}(u_s)$.*

***a)** The polynomial $\mathrm{BF}_{\mathcal{O}}(f) = \sum_{\{i: ind_{\mathcal{O}}(u_i) = ind_{\mathcal{O}}(f)\}} a_i u_i \in R$ is called the* border form *of f with respect to $\mathcal{O}$. For $f = 0$, we let $\mathrm{BF}_{\mathcal{O}}(f) = 0$.*

***b)** Given an ideal $I \subseteq R$, the ideal $\mathrm{BF}_{\mathcal{O}}(I) = (\mathrm{BF}_{\mathcal{O}}(f) : f \in I)$ is called the* border form ideal *of I with respect to $\mathcal{O}$.*

Proposition 7.1.3. *The set G is an $\mathcal{O}-$border basis of I if and only if the following equivalent conditions are satisfied.*

***i)** For every $f \in I$, $Supp(\mathrm{BF}_{\mathcal{O}}(f)) \subseteq \mathbb{T}^n\backslash\mathcal{O}$*

***ii)** $\mathrm{BF}_{\mathcal{O}}(I) = (\mathrm{BF}_{\mathcal{O}}(g_1), ..., \mathrm{BF}_{\mathcal{O}}(g_\upsilon)) = (b_1, ..., b_\upsilon)$.*

Proof. First we will assume G is a border basis and then prove **i)** by showing the support of $BF_{\mathcal{O}}(f)$ does not contain any elements in $\mathcal{O}$. Suppose $\exists f \in I$ such that

$Supp(BF_{\mathcal{O}}(f))$ contains a term in $\mathcal{O}$, then by definition of border form every term is in $\mathcal{O}$, i.e., $f = c_1t_1 + ... + c_\mu t_\mu$ but G is a border basis and that forces $f = 0$ since $c_1t_1 + ... + c_\mu t_\mu \in I \cap \langle\mathcal{O}\rangle_k = \{0\}$.

Then we will assume **i)** and prove *ii)*. For any $g_i \in G$ we have $g_i \in I$, and $b_i = BF_{\mathcal{O}}(g_i) \in BF_{\mathcal{O}}(I)$. For the converse, let $f \in I$ where $BF_{\mathcal{O}}(f) \in BF_{\mathcal{O}}(I)$, i.e., $BF_{\mathcal{O}}(f) = a_1f_1 + ... + a_nf_n$ where $ind_{\mathcal{O}}(f_i) = ind_{\mathcal{O}}(f)$ where $f_i \in \mathbb{T}^n\backslash\mathcal{O}$. Therefore by *Proposition 6.0.8* $f_i's$ are divisible by $b_i\partial \in \mathcal{O}$, for every $i = 1, ..., n$ and that implies $BF_{\mathcal{O}}(f) \in (b_1, ..., b_n)$.

And finally, we will assume **ii** holds and prove G is a border basis by showing $I \cap \langle\mathcal{O}\rangle_k = \{0\}$. Suppose there exists $f \in I \cap \langle\mathcal{O}\rangle_k$, then f can be represented as follows, $f = c_1t_1 + ... + c_\mu t_\mu$. That implies $BF_{\mathcal{O}}(f) \in \mathcal{O}$. Therefore $BF_{\mathcal{O}}(f)$ is not divisible by any $b_i\partial \in \mathcal{O}$. But this contradicts $BF_{\mathcal{O}}(I) = (b_1, ..., b_\upsilon)$ unless $f = 0$.

□

Let $f \in R$ be a polynomial, let $t \in Supp(f)$ be a multiple of a border term $t = t'b_i$ and $c \in k$ be the coefficient of t in f. Then $h = f - ct'g_i$ doe not contain the term t anymore. We say that f reduces to h in one step using g_i and write $f \xrightarrow{G} h$. The reflexive, transitive closure of the relations $\xrightarrow{g_i}$, $i \in \{1, ..., \upsilon\}$, is called the rewrite relation associated to G and is denoted by $\xrightarrow{G}$. The equivalence relation generated by $\xrightarrow{G}$ is denoted by $\xleftrightarrow{G}$.[11]

Example 7.1.4. *Let $R = \mathbb{Q}[x, y]$ and $\mathcal{O} = \{1, x, x^2\}$. Then $\partial\mathcal{O} = \{y, xy, x^2y, x^3\}$ and the $\mathcal{O}-$order prebasis is $G = \{y, xy + y, x^2y, x^3 + 1\}$, where $g_1 = y, g_2 = xy + y, g_3 = x^2y, g_4 = x^3 + 1$ The following chain of reductions,*

$$x^3y \xrightarrow{g_4} y \xrightarrow{g_2} x^3y,$$

can be repeated infinitely and that implies $\xrightarrow{G}$ is not Noetherian.

Proposition 7.1.5. *Let $\xleftrightarrow{G}$ be the rewrite equivalence relation associated to an $\mathcal{O}-$border prebasis $G = \{g_1, ..., g_\upsilon\}$, and let $f_1, f_2, f_3, f_4 \in R$*

a)*If $f_1 \xleftrightarrow{G} f_2$ and $f_3 \xleftrightarrow{G} f_4$ then $f_1 + f_3 \xleftrightarrow{G} f_2 + f_4$.*

b)*If* $f_1 \overset{G}{\longleftrightarrow} f_2$ *then* $f_1 f_2 \overset{G}{\longleftrightarrow} f_2 f_3$.

c)*We have* $f_1 \overset{G}{\longleftrightarrow} f_2$ *if and only if* $f_1 - f_2 \in (g_1, ..., g_\upsilon)$

Proof. **a)** First we will show for any $f_1 \xrightarrow{g_i} f_2$ implies $f_1 + f_3 \xrightarrow{g_i} f_2 + f_3$ where $g_i \in G$. If $f_1 \xrightarrow{g_i} f_2$, then $f_2 = f_1 - at'g_i$ and $f_2 + f_3 = f_1 + f_3 - at'g_i$ where $a \in k$ and $t' \in \mathbb{T}^n$. If $t'g_i$ is not a factor of any $t \in Supp(f_3)$ then we are done. If it is not the case, $\exists t \in Supp(f_3)$ such that $t = a't'g_i$. We have two cases, If $a' = -a$, then $f_1 + f_3 = f_2 + f_3 + at'g_i = f_2 + f_3 - at'g_i$, then we can choose $f_4 = f_2 + f_3$. If $a' \neq a$, then $f_1 + f_3 = f_2 + f_3 + at'g_i = f_2 + f_3 + a't'g_i$. Hence $f_1 + f_3 = f_2 + f_3 + (a - a')t'g_i = f_4$. This holds for any g_i so we have, $f_1 \overset{G}{\longleftrightarrow} f_2$ implies $f_1 + f_3 \overset{G}{\longleftrightarrow} f_2 + f_3$. Hence, if $f_1 \overset{G}{\longleftrightarrow} f_2$ and $f_3 \overset{G}{\longleftrightarrow} f_4$, then we have $f_1 + f_3 \xrightarrow{G} f_2 + f_3$ and $f_2 + f_3 \overset{G}{\longleftrightarrow} f_4 + f_2$. Since this is an equivalence relation, we have $f_1 + f_3 \overset{G}{\longleftrightarrow} f_2 + f_4$.

b)We will first show, if $f_1 \overset{G}{\longleftrightarrow} f_2$, then $t_\alpha f_1 \overset{G}{\longleftrightarrow} t_\alpha f_2$ for any $t \in \mathbb{T}^n$. If $f_1 \xrightarrow{g_i} f_3$, then $f_2 = f_1 - at'g_i$ where $g_i \in G\, t' \in \mathbb{T}^n$ and for any $t \in Supp(f_1)$ if $t = t'g_i\, t$ vanishes. For $t_\alpha f_2 = t_\alpha f_1 - t_\alpha t'g_i$, clearly $t_\alpha t' \in Supp(tf_1)$ and $t_\alpha t'$ vanishes . Therefore we have $t_\alpha f_1 \overset{G}{\longleftrightarrow} t_\alpha f_2$, and this holds for every $t_\alpha \in \mathbb{T}^n$, and by previous result we have $f_1 f_3 \overset{G}{\longleftrightarrow} f_2 f_3$ where $f_3 = \sum_{i=1}^{n} a_i t_i$ for $a_i \in k$ and $t_i \in \mathbb{T}^n$.

c) If $f_1 \overset{G}{\longleftrightarrow} f_2$, then $f_2 = f_1 - a_1 g_1 - ... - a_\upsilon g_\upsilon$ and $f_1 - f_2 = a_1 g_1 - ... - a_\upsilon g_\upsilon \in (g_1, ..., g_\upsilon)$ where $a_i \in k$.

For the converse $f_1 - f_2 = a_1 g_1 - ... - a_\upsilon g_\upsilon \in (g_1, ..., g_\upsilon)$ then we have $f_1 \xrightarrow{g_1} f_{\alpha 1}$ where $f_{\alpha 1} = f_1 - a_1 g_1 = f_2 + a_2 g_2 - ... - a_\upsilon g_\upsilon$ and if we proceed this way we will end up with $f_1 \xrightarrow{g_1} ... \xrightarrow{g_\upsilon} f_{\alpha\upsilon}$ and $f_{\alpha\upsilon} = f_1 - a_1 g_1 - a_2 g_2 - ... - a_\upsilon g_\upsilon = f_2$, i.e., $f_1 \overset{G}{\longleftrightarrow} f_2$. □

Proposition 7.1.6. *The set* G *is an* $\mathcal{O}-$*border basis of* I *if and only if the following are equivalent*

i)*For* $f \in R$, *we have* $f \xrightarrow{G} 0$ *if and only if* $f \in I$.

ii) *If* $f \in I$ *is reducible with respect to* $\xrightarrow{G}$, *we have* $f = 0$.

iii)*For every* $f \in R$, *there exists an element* $h \in R$ *such that* $f \xrightarrow{G} h$ *and* h *is irreducible with respect to* $\xrightarrow{G}$. *The element* h *is uniquely determined.*

iv)*The rewrite relation* $\xrightarrow{G}$ *is confluent.*

Proof. First we will assume G is a border basis and prove **i**. Let $f \in R$, if $\xrightarrow{G} 0$, then $f \xrightarrow{g_i} f_i \longrightarrow ... \xrightarrow{g_v} 0$. That implies $f \in (g_1, ..., g_v) = I$, i.e., $f \in I$. For the converse, let $f \in I$ apply border division algorithm we have $f = f_1g_1 + ... + f_vg_v + c_1t_1 + ... + c_\mu t_\mu$. Since $f \in I$ and G is a border basis $c_1t_1 + ... + c_\mu t_\mu = 0$. Therefore $f \xrightarrow{G} 0$.

Now we will show **i** implies **ii**. Assume $f \in I$, which implies $f \xrightarrow{G} 0$ by **i)**. If f is irreducible $f = c_1t_1 + ... + c_\mu t_\mu$, then $c_1t_1 + ... + c_\mu t_\mu = 0$, i.e., $f = 0$.

We will assume **ii** holds and prove **iii**, that is $f \xrightarrow{G} h = NR_{\mathcal{O},\mathcal{G}}(f)$. Let $f \in R$ and apply border division algorithm we will end up with $f \xrightarrow{g_i} NR_{\mathcal{O},\mathcal{G}}(f)$ which is irreducible so there exists $NR_{\mathcal{O},\mathcal{G}}(f)$ and $f = f_1g_1 + ... + f_vg_v + NR_{\mathcal{O},\mathcal{G}}(f)$. If we have $f \xrightarrow{g_i} h$ irreducible, we have $f = f_1'g_1 + ... + f_v'g_v$, where $f_i, f_i' \in R$ for $i = \{1, ..., v\}$. Hence $NR_{\mathcal{O},\mathcal{G}}(f) - h \in I$ and also since they are both irreducible $NR_{\mathcal{O},\mathcal{G}}(f) - h \in \langle \mathcal{O} \rangle_k$. Since G is a border basis, $I \cap \langle \mathcal{O} \rangle_k = \{0\}$ and $NR_{\mathcal{O},\mathcal{G}}(f) = h$.

Assume (iii) holds, and let $f_1 \xrightarrow{G} f_2$ and $f_1 \xrightarrow{G} f_3$ where $f_1, f_2, f_3 \in R$. Also by definition of normal form we have $f_2 \xrightarrow{G} NR_{\mathcal{O},\mathcal{G}}(f_2)$ and $f_3 \xrightarrow{G} NR_{\mathcal{O},\mathcal{G}}(f_3)$ where both $NR_{\mathcal{O},\mathcal{G}}(f_3), NR_{\mathcal{O},\mathcal{G}}(f_2)$ are irreducible. That implies $f_1 \xrightarrow{G} NR_{\mathcal{O},\mathcal{G}}(f_3)$ and $f_1 \xrightarrow{G} NR_{\mathcal{O},\mathcal{G}}(f_2)$. By previous result we have $NR_{\mathcal{O},\mathcal{G}}(f_2) = NR_{\mathcal{O},\mathcal{G}}(f_3)$. Let $NR_{\mathcal{O},\mathcal{G}}(f_2) = NR_{\mathcal{O},\mathcal{G}}(f_3) = f_4$ Therefore $f_2 \xrightarrow{G} f_4$ and $f_3 \xrightarrow{G} f_4$.

Finally we will show if **iv** holds G is a border basis. Let $f_1, ..., f_t \in R$ such that $f = f_1$ and $f_t = 0$ and for $i \in \{1, ..., t-1\}$ either we have $f \xrightarrow{G} f_{i+1}$ or $f_{i+1} \xrightarrow{G} f_i$. Now choose the largest index $l \in \{1, ..., t-2\}$ such that $f_{l+1} \xrightarrow{G} f_l$. Then $f_{l+1} \xrightarrow{G} 0$ and also we have $f_{l+1} \xrightarrow{G} f_l$ by **iv)** we have $f_l \longrightarrow 0$. Now reduce the sequence to $f = f_1, ..., f_l, 0$. If we proceed this way we will end up with $f \longrightarrow h$, where $h \in \langle \mathcal{O} \rangle_k$ and $h = 0$ i.e., $f \in (g_1, ..., g_v)$ and also by *Proposition 7.1.5* ***c)*** $f \in I$ and $I \cap \langle \mathcal{O} \rangle_k = \{0\}$.

□

7.2 Characterization of Border Bases That is Totally Different From the Characterization of Gröbner Bases

Definition 7.2.1. *Let $\mathcal{O} = \{t_1, ..., t_\mu\}$ be an order ideal, $\partial\mathcal{O} = \{b_1, ..., b_\upsilon\}$ be its border, and $G = \{g_1, ..., g_\upsilon\}$ an $\mathcal{O}-$border prebasis with*

$$g_j = b_j - \sum_{m=1}^{\mu} \alpha_{mj} t_m \quad for \quad 1 \leqslant j \leqslant \upsilon.$$

For $1 \leqslant r \leqslant n$, define the rth formal matrix $\mathcal{X}_r = (\xi_{kl}^r)$ by

$$\xi_{kl}^{(r)} = \begin{cases} \delta_{ki} & if \quad t_i = x_r t_l \\ \alpha_{kj} & if \quad b_j = x_r t_l \end{cases}$$

Example 7.2.2. *Let $\mathcal{O} = \{1, x, y\}$ where $t_1 = 1$, $t_2 = x$ and $t_3 = y$. Then $\partial\mathcal{O} = \{x^2, xy, y^2\}$ where $b_1 = x^2$, $b_2 = xy$, $b_3 = y^2$ and the prebasis $g_i = b_i - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ where $\alpha_{ij} \in k$ for $1 \leqslant i \leqslant \mu$ and $t_i \in \mathcal{O}$, $G = \{x^2 + x + y, xy + y, y^2 + x + 1\}$ where*

$$g_1 = x^2 + xy + y = b_1 - \alpha_{21} t_2 - \alpha_{11} t_1; \quad \alpha_{21} = -1, \alpha_{11} = -1$$

$$g_2 = xy + y = b_2 - \alpha_{32} t_3; \quad \alpha_{32} = -1$$

$$g_3 = y^2 + x + 1 = b_3 - \alpha_{23} t_2 - \alpha_{13} t_1; \quad \alpha_{23} = -1, \alpha_{13} = -1$$

By the definition of first formal matrix, $\mathcal{X} = (\xi_{kl}^{(1)})$ by

$$\xi_{kl}^{(1)} = \begin{cases} \delta_{ki} & if \quad xt_l = t_i \\ \alpha_{kj} & if \quad xt_l b_j \end{cases}$$

Now we will calculate xt_i for every $t_i \in \mathcal{O}$.

$$l = 1, xt_1 = x = t_2$$

$$l = 2, xt_2 = x^2 = b_1$$

$$l = 3, xt_3 = xy = b_2.$$

$$k = 1, \xi_{11}^{(1)} = \delta_{12} \quad \xi_{12}^{(1)} = \alpha_{11} \quad \xi_{13}^{(1)} = \alpha_{12}$$

$$k = 2, \xi_{21}^{(1)} = \delta_{22} \quad \xi_{22}^{(1)} = \alpha_{21} \quad \xi_{23}^{(1)} = \alpha_{22}$$

$$k = 3, \xi_{31}^{(1)} = \delta_{32} \quad \xi_{32}^{(1)} = \alpha_{31} \quad \xi_{33}^{(1)} = \alpha_{32}$$

$$\mathcal{X} = \begin{pmatrix} \delta_{12} & \alpha_{11} & \alpha_{12} \\ \delta_{22} & \alpha_{21} & \alpha_{22} \\ \delta_{32} & \alpha_{31} & \alpha_{32} \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

Now we are going to construct $\mathcal{Y}$ therefore we will calculate yt_i for every $t_i \in \mathcal{O}$.

$$\xi_{kl}^{(2)} = \begin{cases} \delta_{ki} & if \quad yt_l = t_i \\ \alpha_{kj} & if \quad yt_l b_j \end{cases}$$

$$l = 1, yt_1 = y = t_3$$

$$l = 2, yt_2 = yx = b_2$$

$$l = 3, yt_3 y^2 = b_3.$$

$$k = 1, \xi_{11}^2 = \delta_{13} \quad \xi_{12}^{(2)} = \alpha_{12} \quad \xi_{13}^{(2)} = \alpha_{13}$$
$$k = 2, \xi_{21}^2 = \delta_{23} \quad \xi_{22}^{(2)} = \alpha_{22} \quad \xi_{23}^{(2)} = \alpha_{23}$$
$$k = 3, \xi_{31}^2 = \delta_{33} \quad \xi_{32}^{(2)} = \alpha_{32} \quad \xi_{33}^{(2)} = \alpha_{33}$$

$$\mathcal{Y} = \begin{pmatrix} \delta_{13} & \alpha_{12} & \alpha_{13} \\ \delta_{23} & \alpha_{22} & \alpha_{23} \\ \delta_{33} & \alpha_{32} & \alpha_{33} \end{pmatrix} = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}$$

What multiplication matrices do is, when we multiply an element in $\langle \mathcal{O} \rangle_k$ by indeterminate (in our case it is x or y) if the result is in the border, they keep the result in $\langle \mathcal{O} \rangle_k$. If G is an $\mathcal{O}-$border basis for a zero dimensional ideal , then $\overline{\mathcal{O}}$ is a k-vector space basis of R/I, and each matrix formal multiplication matrices defines $k-$linear maps,

$$\begin{aligned} \varphi_x : R/I &\longmapsto R/I \\ t_1 &\longmapsto xt_1 = x = t_2 \\ t_2 &\longmapsto xt_2 = x^2 = b_1 = \xi_{12}^{(1)} t_1 + \xi_{22}^{(1)} t_2 + \xi_{23}^{(1)} t_3 \\ t_3 &\longmapsto xt_3 = xy = b_2 = \xi_{13}^{(1)} t_1 + \xi_{23}^{(1)} t_2 + \xi_{33}^{(1)} t_3 \end{aligned}$$

and

$$\begin{aligned}
\varphi_y : R/I &\longmapsto R/I \\
t_1 &\longmapsto yt_1 = y = t_2 \\
t_2 &\longmapsto yt_2 = xy = b_2 = \xi_{12}^{(2)}t_1 + \xi_{22}^{(2)}t_2 + \xi_{23}^{(2)}t_3 \\
t_3 &\longmapsto yt_3 = y^2 = b_3 = \xi_{13}^{(2)}t_1 + \xi_{23}^{(2)}t_2 + \xi_{33}^{(2)}t_3
\end{aligned}$$

Clearly the map φ_x is multiplication by x and the map φ_y is multiplication by y. Therefore the formal multiplication matrices have to commute, as follows,

$$\mathcal{XY} = \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}.$$

$$\mathcal{YX} = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}.$$

Also $v = c_1t_1 + ... + c_\mu t_\mu \in \langle \mathcal{O} \rangle_k$ are encoded as column vectors $(c_1, ..., c_\mu)^{t_r} \in k^\mu$ and $x_r v$ is represented as $\mathcal{X}_r(c_1, ..., c_\mu)^{t_r}$. In our example the first column of $\mathcal{X}$ represents $xt_1 = t_2$ as,

$$\mathcal{X}(\mathbf{0}, \mathbf{1}, \mathbf{0})^{\mathbf{t_r}} = \begin{pmatrix} \delta_{12} \\ \delta_{22} \\ \delta_{32} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

Proposition 7.2.3. *G is a border basis if and only if the formal multiplication matrices commute, i.e.,if and only if $\mathcal{X}_r\mathcal{X}_s = \mathcal{X}_s\mathcal{X}_r$ for all $r, s \in \{1, ..., n\}$[11]*

Definition 7.2.4. *Let $b_i, b_j \in \partial\mathcal{O}$ be two distinct border terms.*

***i)** The border terms b_i and b_j are called* next-door neighbours *if we have $b_i = x_k b_j$ for some $k \in \{1, ..., n\}$.*

***ii)** The border terms b_i and b_j are called* across-the-street neighbours *if $x_k b_i = x_l b_j$ for some $k, l \in \{1, ..., n\}$.*

***iii)** The border terms b_i and b_j are called* neighbours *if they are next-door neighbours or across-the-street neighbours.[8]*

When we discussed Buchberger Criterion previous chapters we mentioned that the crucial idea in Buchberger Criterion is $S-$polynomials. Now we will prove Buchberger Criterion for Border basis analog of Buchberger's criterion in order to that we will define $S-$polynomials of two distinct elements $g_i, g_j \in G$ is defined by

$$S(g_i, g_j) = (lcm(b_i, b_j)/b_i)g_i - (lcm(b_i, b_j)/b_j)g_j.$$

Proposition 7.2.5 (*Buchberger Criterion for Border Bases*)**.** *The $\mathcal{O}-$border prebasis G is an $\mathcal{O}-$border basis if and only if one of the following equivalent conditions are satisfied.*

***i)** For all $1 \leqslant i \leqslant j \leqslant \upsilon$, the $S-$polynomial $S(g_i, g_j)$ reduces to 0 via $\xrightarrow{G}$.*

***ii)** For all neighbours b_i and b_j, the $S-$polynomial $S(g_i, g_j)$ reduces to 0 via $\xrightarrow{G}$.*

7.3 Border Division Algorithm

Lemma 7.3.1. *Let $d \in \mathbb{N}$, $\mathcal{L} = \mathbb{T}^n_{\leqslant d}$, V be a $k-$vector subspace of $\langle\mathcal{L}\rangle_k$ such that $(V + x_1V + ... + x_nV) \cap \langle\mathcal{L}\rangle_k = V$, let $\{v_1, ..., v_r\}$ be a $k-$basis of V, and let σ be a degree compatible term ordering. Consider the following sequence of instructions.*

***1)** Write $\mathcal{L} = \{l_1, ..., l_s\}$ such that $l_1 >_\sigma l_2 >_\sigma ... >_\sigma l_s$.*

***2)** For $i = 1, ..., r$, write $v_i = a_{i1}l_1 + ... + a_{is}l_s$ with $a_{ij} \in k$. Form the matrix $\mathcal{V} = (a_{ij}) \in Mat_{r,s}(k)$.*

***3)** Using row operations, transform $\mathcal{V}$ into row echelon form. Call the result $\mathcal{W}$.*

***4)** Let $\mathcal{O}$ be the set of terms in $\mathcal{L}$ corresponding to the columns of $\mathcal{W}$ in which no row $\mathcal{W}$ has its first non-zero entry. Return $\mathcal{O}$ and stop.*

This algorithm computes an order ideal $\mathcal{O} \subseteq \mathcal{L}$ such that the residue classes of the terms in $\mathcal{O}$ form a $k-$vector space basis of $\langle\mathcal{L}\rangle_k/V$ [11],[9].

Proof. The procedure is finite.Thus we prove correctness. The terms in $\mathcal{O}$ are linearly independent modulo V because a non-trivial element in $\langle\mathcal{O}\rangle_k \cap V$ would correspond to a row of $\mathcal{W}$ whose first non-zero position is in a column corresponding to a term of $\mathcal{O}$. To prove that $\mathcal{O}$ is an order ideal, it suffices to show that $l_i \in \mathcal{L}\backslash\mathcal{O}$ and $tl_i \in \mathcal{L}$ imply $tl_i \in \mathcal{L}\backslash\mathcal{O}$ for all $t \in \mathbb{T}^n$. Given a term $l_i \in \mathcal{L}\backslash\mathcal{O}$, there exists a vector $v \in V$ which corresponds to the row of $\mathcal{W}$ whose first non-zero entry is in position i. Thus we have $l_i = LT_\sigma(v)$. Now let $l_j = tl_i \in \mathcal{L}$ for some $t \in \mathbb{T}_n$. Then we see that $l_j = LT_\sigma(tv)$. Since σ is degree compatible, it follows that all elements of $Supp(tv)$ are in $\mathcal{L}$. Hence the term l_j corresponds to a column of the matrix $\mathcal{W}$ in which one of its rows has its first non-zero entry. Thus we have $tl_i \in \mathcal{L}\backslash\mathcal{O}$. [11]

□

Proposition 7.3.2 (*Border Division Algorithm*)**.** *Let $I \subseteq R$ be a zero-dimensional ideal generated by a set of non-zero polynomials $f_1, ..., f_s$, and let σ be a degree compatible term ordering. Consider the following sequence of instructions.*

1)*Let $V_0 \subseteq R$ be the $k-$vector subspace generated by $\{f_1, ..., f_s\}$.*

2) *Let $d = max\{deg(t) : t \in Supp(f_1) \cup ... \cup Supp(f_s)\}$ and $\mathcal{L} = \mathbb{T}^n_{\leqslant d}$.*

3)*For $i = 0, 1, ...$ compute $V_{i+1} = (V_i + x_1V_i + ... + x_nV_i) \cap \langle\mathcal{L}\rangle_k$ until $V_{i+1} = V_i$.*

4)*Using the lemma, compute an order ideal $\mathcal{O} \subseteq \mathcal{L}$ such that the residue classes of the terms in $\mathcal{O}$ form a $k-$vector space basis of $\langle\mathcal{L}\rangle_k/V_i$.*

5)*Check whether $\partial\mathcal{O} \subseteq \mathcal{L}$. If this is not the case, increase d by one, replace $\mathcal{L}$ by $\mathbb{T}^n_{\leq d}$, replace V_0 by V_i, and continue with step **3**.*

6)*Let $\mathcal{O} = \{t_1, ..., t_\mu\}$ and $\partial\mathcal{O} = \{b_1, ..., b_\upsilon\}$. For $j = 1, ..., \upsilon$, compute the representation $\overline{b_j} = \sum_{i=1}^{\mu} \alpha_{ij}t_i$ of $b_j \in \langle\mathcal{L}\rangle_k/V_i$ in terms of the basis $\{\overline{t_1}, ..., \overline{t_\mu}\}$ and let $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij}t_i$. Then let $G = \{g_1, ..., g_\upsilon\}$, return the pair $(\mathcal{O}, G)$, and stop.*

This algorithm returns the pair $(\mathcal{O}, G)$ where $\mathcal{O}$ is an order ideal and G is an $\mathcal{O}-$border basis of I. [11]

Proof. Since $V_i \subseteq V_{i+1}$ for $i \geqslant 0$ and since $dim_k(\langle\mathcal{L}\rangle_k) < \infty$, the sequence $V_0 \subseteq V_1 \subseteq ...$ is eventually stationary. Thus step **3)** involves only finitely many computations. To show that the loop in step **4)** and **5)**is finite, we have to prove that we eventually have $\mathcal{O} \subseteq \mathcal{L}$. Let σ be a degree compatible term ordering on $\mathbb{T}^n$, and let $H = \{h_1, h_2, ..., h_{s'}\}$ be the reduced Gröbner basis of I with respect to σ. For $j = 1, ..., s'$, there is a representation $h_j = p_{j1}f_1 + ... + p_{js}f_s$ with $p_{jk} \in R$. Let $d = max\{deg(p_{jk}f_k) : j \in \{1, ..., s\}\}$. By construction, we have $H \subseteq V_i$ after step **3)** has been performed for $\mathcal{L} = \mathbb{T}^n_{\leqslant d}$. Now we apply the algorithm of the lemma. It follows that none of the leading terms $LT_\sigma(h_j)$ is contained in $\mathcal{O}$. Thus we have $\mathcal{O} \subseteq \mathbb{T}^n \backslash LT_\sigma\{I\}$ and the number of the elements in $\mathcal{O}$ is smaller than the $dim_k(R/I)$. Therefore it suffices to repeat the loop until d is larger than its dimension in order to force $\mathcal{O} \subseteq \mathcal{L}$ and finiteness follows.

Next we prove the correctness. When the loop in step **3)**-**5)** finishes we have $\partial\mathcal{O} \subseteq \mathcal{L}$. Hence step **6)** can be performed and yields $G \subseteq V_i \subseteq I$. By construction, the set G is an $\mathcal{O}-$border prebasis. Given two neighbours $b_j, b_k \in \partial\mathcal{O}$, corresponding $S-$polynomial $S(g_j, g_k) - \sum_{l=1}^{\upsilon} c_l g_l$ has its support in $\mathcal{O}$. Since this polynomial is contained in V_i and $\mathcal{O}$ represents a $k-$vector space basis of $\langle\mathcal{L}\rangle_k/V_i$, it follows that $S(g_j, g_k) - \sum_{l=1}^{\upsilon} c_l g_l = 0$. Consequently, the $S-$polynomial $S(g_j, g_k)$ reduces to zero via $\xrightarrow{G}$, and Buchberger's Criterion for Border Bases proves that G is an $\mathcal{O}-$border basis of the ideal.

Finally we show $(g_1, ..., g_\upsilon) = I$. The inclusion $' \subseteq'$ was already observed above. For $j = 1, ..., s$, we have $f_j \in V_0 \subseteq V_i \subseteq \langle\mathcal{L}\rangle_k$. Every term in $\langle\mathcal{L}\rangle_k \backslash \mathcal{O}$ is a multiple of one of the terms $b_1, ..., b_\upsilon$. Therefore we can use $\xrightarrow{G}$ to reduce f_j to an element in $\langle\mathcal{O}\rangle_k$. But that element is also contained in V_i, and hence it is zero. In other words, we have $f_j \in (g_1, ..., g_\upsilon)$. [11] □

7.4 Application

In this section we will do some applications and mention some of the crucial properties of border basis and compare it with Gröbner Basis.

Let k be a field where $R = k[x_1, ..., x_n]$, $\mathcal{O}$ be a order ideal $(c_1, ..., c_s)$ be the minimal generating set for $\mathbb{T}^n \backslash \mathcal{O}$ which we also call corners of $\mathbb{T}^n \backslash \mathcal{O}$. Let I be a zero dimensional ideal which has an $\mathcal{O}-$border basis G and $\{g_1, ..., g_s\}$ be the elements in the border basis corresponding to $\{c_1, ..., c_s\}$. Let $J = (g_1, ..., g_s)$ and there exists a term ordering σ such that $LT_\sigma(g_i) = c_i$ where $i = 1, ..., s$.

First we will show that $dim_k(R/I) = dim_k(R/J)$. Clearly $J \subseteq I$ since $\{g_1, ..., g_s\} \in I$. We have $(c_1, ..., c(s)) = \mathbb{T}^n \backslash \mathcal{O}$ and $(c_1, ..., c(s)) \subseteq \partial\mathcal{O}$ and therefore $\{g_1, ..., g_s\}$ is a $\mathcal{O}-$border prebasis for J since $g_i = c_i - \sum_{j=1}^{\mu} \alpha_{ij} t_i$, for $i = 1, ..s$. Also G is a $\mathcal{O}-$border basis therefore $I \cap \langle \mathcal{O} \rangle_k = \{0\}$ and $J \subseteq I$, implies $J \cap \langle \mathcal{O} \rangle_k = \{0\}$. Hence $\mathcal{O}$ is a $k-$vector space basis for R/I and R/J and $dim_k(R/I) = dim_k(R/J)$.

Now we will show for $\mathcal{O}_\sigma(I)$, an order ideal $\mathbb{T}^n \backslash LT_\sigma\{I\}$ we have $\mathcal{O} = \mathcal{O}_\sigma(I)$. Macaluay Basis theorem implies that for ideal I if we denote the set of terms in $\mathbb{T}^n \backslash LT_\sigma\{I\}$ by $\mathcal{O}_\sigma(I)$, the residue classes of the elements of $\mathcal{O}_\sigma(I)$ defines $k-$vector space basis for R/I. And also $\mathcal{O}$ forms a $k-$vector space basis for R/I since G is a $\mathcal{O}-$border basis. Hence $dim(\mathcal{O}_\sigma(I)) = dim(\mathcal{O})$. Let $t \neq 0$ and $t \in \mathbb{T}^n \backslash \mathcal{O}_\sigma(I)$. Then t is not an element of $\mathcal{O}_\sigma(I)$, $t \in LT_\sigma\{I\} \subseteq I$. This implies t is not an element of $\mathcal{O}$ since $I \cap \langle \mathcal{O} \rangle_k = \{0\}$. Hence $\mathcal{O}_\sigma(I) \subseteq \mathcal{O}$ and $\mathcal{O}_\sigma(I) = \mathcal{O}$ by previous result $dim_k(R/I) = dim_k(R/J)$.

Finally we will show the crucial part which is, the set $\{g_1, ..., g_s\}$ is the reduced Gröbner basis of I. Let us show the reduced Gröbner Basis by G_σ. Notice that $\{c_1, ..., c_s\} \in \partial\mathcal{O}$. By definition of reduce Gröbner basis, an element from the reduced Gröbner basis has the form $c_i - h_i$ where $LT_\sigma\{g_i\} = c_i$ and $c_i \equiv h_i \mod G_\sigma$ where $h_i \in \mathbb{T}^n \backslash LT_\sigma\{I\}$. Therefore $h_i \in \langle \mathcal{O} \rangle_k = \langle \mathcal{O}_\sigma(I) \rangle_k$. But this is the form of an element in the $\mathcal{O}_\sigma(I)-$border basis G'. Hence G' is the reduced Gröbner basis.

Let us give an example that we can apply border basis algorithm,discuss the advantages of using it rather than Buchberger's Algorithm and show the border basis that is calculated by Border Basis Algorithm contains reduced Gröbner Basis concretely.

Example 7.4.1. *Let* $R = \mathbb{Q}[x, y]$. *Apply border basis algorithm to* $I = \{x^2 - xy + y^2, x^3 - x^2y, x^2y - xy^2, xy^2 - y^3, x^3 + y^3\}$. *By 7.3.2,*

1)Let $V_0 = \langle f_1, f_2, f_3, f_4, f_5\rangle_{\mathbb{Q}} = \langle x^2-xy+y^2, x^3-x^2y, x^2y-xy^2, xy^2-y^3, x^3+y^3\rangle_{\mathbb{Q}}$

2)Let $d = 3$ *and* $\mathcal{L} = \{x^3, x^2y, xy^2, y^3, x^2, xy, y^2, x, y, 1\}$.

3)$V_1 = \langle V_1+xV_1+yV_1\rangle_{\mathbb{Q}} \cap \langle\mathcal{L}\rangle_{\mathbb{Q}} = \langle f_1, f_2, f_3, f_4, f_5, xf_1, yf_1\rangle_{\mathbb{Q}} = \langle x^2-xy+y^2, x^3-x^2y, x^2y-xy^2, xy^2-y^3, x^3+y^3, x^3-x^2y+xy^2, x^2y-xy^2+y^3\rangle_{\mathbb{Q}}$. *Since* $deg(x_if_j) > 3$, $x_i \in \{x, y\}$ *and* $j = 2, 3, 4, 5$. *Therefore* $V_1 = V_2$.

4)Now we will form the matrix,

$$\mathcal{V} = \left(\begin{array}{c|cccccccccc} * & x^3 & x^2y & xy^2 & y^3 & x^2 & xy & y^2 & x & y & 1 \\ \hline f_1 & 0 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 & 0 \\ f_2 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ f_3 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ f_4 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ f_5 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ xf_1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ yf_1 & 0 & 1 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Notice that the original matrix is the matrix that is separated by the lines. The extra parts are only for to representing the notion. $\mathcal{V}$ *is not in echelon form, we will find the row echelon form of it.*

$$\mathcal{W} = \left(\begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2 & xy & y^2 & x & y & 1 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \textbf{\textit{-1}} & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

By the step 4 of the lemma*7.3.1* $\mathcal{O}$ *will be the set of the terms in* $\mathcal{L}$ *corresponding*

to the columns of $\mathcal{W}$ in which no row of $\mathcal{W}$ has its first non zero entry. Therefore we let $\mathcal{O} = \{1, x, y, y^2, xy\}$.

5)$\partial\mathcal{O} \in \mathcal{L}$.

6) $\partial\mathcal{O} = \{x^2, x^2y, xy^2, y^3\}$ and $\mathcal{O}-$border basis is $G = \{g_1, g_2, g_3, g_4\}$ where $g_1 = x^2y - xy + y^2 = f_1$, $g_2 = xy^2 = xf_1 - f_2$, $g_3 = x^2y = yf_1 - f_4$, $g_4 = y^3 = f_1 - 2f_4$. $G = \{x^2y - xy + y^2, xy^2, x^2y, y^3.\}$ Let G_σ be the reduced Gröbner basis and G' be Gröbner Basis of I. I we calculate G' we will have $G' = \{x^2 - xy + y^2, xy^2 - y^3, -y^3\}$ and the reduced Gröbner Basis (see appendix B.9) will be $G_\sigma = \{y^3, x^2 - xy + y^2, xy^2\}$. As we noted, $G_\sigma \subseteq G$.

The difference between Buchberger Algorithm and Border Basis Algorithm is, the Border Basis Algorithm requires only terms up to degree 3 but during the Buchberger Algorithm we came across to terms with larger degree as in x^4y^2 and x^3y^2. Therefore we end up with terms with degree 6 that has to be reduced. But Border Basis Algorithm avoids from redundant calculations that Buchberger Algorithm has.

If we start with a zero dimensional ideal I, we know that exists an order ideal. The order ideal that we calculate with Border Basis Algorithm is actually $\mathcal{O}_\sigma(I)$ which corresponds to $\mathbb{T}^n \backslash LT_\sigma\{I\}$ where σ is the given order. Therefore the border basis associated to $\mathcal{O}_\sigma(I)$ contains the reduced Gröbner Basis. But we can find other order ideals $\mathcal{O} \neq \mathcal{O}_\sigma(I)$ and border basis associated to them ,that may not contain reduced Gröbner Basis, with some nice properties. One of those nice properties we will discuss in this thesis is symmetry.

Let $R = k[x_1, ..., x_n]$ and $A \subseteq R$. We say that A is invariant under the action of of the symmetric group(or A is symmetric) if $f(x_1, ..., x_n) \in A$ then $f(x_{\pi(1)}, ..., x_{\pi(n)}) \in A$ for every permutation π of $\{1, ..., n\}$.[11] We will use $\pi(f(x_1, ..., x_n)) = f(x_{\pi(1)}, ..., x_{\pi(n)})$. Let $\mathcal{O} = \{t_1, ..., t_\mu\}$ be an order ideal in $\mathbb{T}^n$, and let $I \subseteq R$ be a zero-dimensional ideal. Assume that the residue classes or the elements form a $k-$vector space basis of R/I and both $\mathcal{O}$ and I are symmetric. Since $\mathcal{O}$ form a $k-$vector space basis G is a $\mathcal{O}-$border basis where $\partial\mathcal{O} = \{b_1, ..., b_v\}$ and$G = \{g_1, ..., g_v\}$. And any element $g_i \in G$

has the form

$$g_i = \{b_i - \sum_{j=1}^{\mu} \alpha_{ij} t_i\}$$

where $\sum_{j=1}^{\mu} \alpha_{ij} t_i\} \in \langle \mathcal{O} \rangle_k$. Clearly $\pi(g_i) \in I$ and $\pi(\sum_{j=1}^{\mu} \alpha_{ij} t_i\}) \in \langle \mathcal{O} \rangle_k$ since I and $\mathcal{O}$ are both symmetric. What about $\pi(b_i) \in \partial\mathcal{O}$? For any $b_i \in \partial\mathcal{O}$, $b_i = x_j t_i \neq 0$ for $x_j \in \{x_1, ..., x_n\}$ and $t_i \in \mathcal{O}$. Assume $\pi(b_i) = \pi(x_j t_i)$ is not an element of the border. Then $\pi(x_j t_i) \in \mathcal{O}$ and since $\mathcal{O}$ is symmetric $\pi^{-1}(\pi(x_j t_i)) = x_j t_i \in \mathcal{O}$. But that implies $x_j t_i \in \mathcal{O} \cap \partial\mathcal{O}$ which contradicts the definition or border and implies border is symmetric. Therefore $\pi(g_i) = \pi(\{b_i) - \pi(\sum_{j=1}^{\mu} \alpha_{ij} t_i)\}$ forms an element in a $\mathcal{O}-$border prebasis say G' and since the residue classes of the elements of $\mathcal{O}$ forms $k-$vector space G' is border basis and by uniqueness $G = G'$. As a result we can say if the zero-dimensional ideal and the order ideal are both symmetric, then the $\mathcal{O}-$border basis is symmetric.

Finally we will show another disadvantage of Gröbner Basis over Border Basis in an example.

Example 7.4.2. *Let* $R = \mathbb{C}[x, y]$, $f_1 = \frac{1}{4}x^2 + y^2 - 1$ *and* $f_2 = x^2 + \frac{1}{4}y^2 - 1$, $I = (f_1, f_2)$ *and let* $\mathcal{O}_\sigma(I)$ *be the order ideal* $\mathbb{T}^n \backslash LT_\sigma\{I\}$ *with respect to the term order* $\sigma =$*DegLex. Then* $LT_\sigma(I) = (x^2, y^2)$ *and* $\mathcal{O}_\sigma(I) = \{1, x, y, xy\}$ *and the border* $\partial\mathcal{O}_\sigma(I) = \{x^2, x^2y, xy^2 - \frac{4}{5}x, y^2 - \frac{4}{5}\}$. *The border basis*

$$G = \{x^2 - \frac{4}{5}, x^2y - \frac{4}{5}y, xy^2 - \frac{4}{5}x, y^2 - \frac{4}{5}\},$$

and the reduced Gröbner Basis of I *is,*

$$G_\sigma = \{x^2 - \frac{4}{5}, y^2 - \frac{4}{5}\}.$$

Now let $I^* = (\frac{1}{4}x^2 + y^2 + \epsilon xy - 1, x^2 + \frac{1}{4}y^2 + \epsilon xy - 1)$.

$\mathcal{O} = \{1, x, y, xy\}$ *is an order ideal of both* I *and* I^* *where* $\mathcal{O}_\sigma(I^*) = \{1, x, y, y^2\}$. *The reduced Gröbner Basis,* $\mathcal{O}$ *Border basis,*

$$G^* = \{x^2 + \frac{4}{5}\epsilon xy - \frac{4}{5}, x^2y - \frac{16\epsilon}{16\epsilon^2 - 25}x + \frac{20}{16\epsilon^2 - 25}y, xy^2 + \frac{20}{16\epsilon^2 - 25}x - \frac{16\epsilon}{16\epsilon^2 - 25}y, y^2 + \frac{4}{5}\epsilon xy - \frac{4}{5}\}$$

and the reduced Gröbner Basis is

$$G_\sigma^* = \{x^2 - y^2, xy + \frac{5}{4\epsilon}y^2 - \frac{1}{\epsilon}, y^3 - \frac{16\epsilon}{16\epsilon^2 - 25}x + \frac{20}{16\epsilon^2 - 25}y\}.$$

[11]

As seen, a small change made in the reduced Gröbner Basis caused a big change. However in Border Basis there is an ϵ succession and if we set $\epsilon = 0$ we will end up with the original border basis that we started.

Chapter 8

CONCLUSION

In this thesis we start with reviewing some commutative algebra. We recover fundamental theorems of Hilbert such as Hilbert Basis theorem and Nullstellensats that laid the foundations of commutative algebra. Then we introduce the relatively modern theory of Gröbner bases which provides indispensable tool for computational purposes. We go on to introduce two problems that are seemingly unrelated to commutative ring theory. These problems have background in combinatorics and optimization. We establish the link between these problems and the Grobner bases and demonstrate explicit solutions. These results are made precise in Chapter 6 and supported by the software (CoCoA) we use, see appendix. Last two chapters are devoted a trend that has emerged quite recently. Border bases are in some sense a generalization of Grobner bases. We present their theory extensively including the essential (border) polynomial division and construction algorithms that this theory relies on. We include evidence that suggests that border bases display better combinatorial behaviors. This enables them to be computed more efficiently.

Appendix A

A.1

CoCoA Code that calculates the Gröbner Basis,

```
Define Gbasis(J)
If Type(J)=LIST Then J:=Ideal(J) EndIf;
G:=Gens(J);
H:=[];
For A:=1 To Len(J)-1 Do
For B:=A+1 To Len(J) Do
If Not G[A]-G[B]=0 Then
Append(H,[G[A],G[B]]);
Else
Remove(G, B);
EndIf;
EndFor;
EndFor;
M:=1; While M¡=Len(H) Do
N:=LCM(LT(H[M][1]),LT(H[M][2]));
S:=((N/LT(H[M][1]))*H[M][1])-((N/LT(H[M][2]))*H[M][2]);
Q:=DivAlg(S,G);
M:=M+1;
If Not IsZero(Q.Remainder) Then
For A:=1 To Len(G) Do
Append(H,[Q.Remainder,G[A]]);
EndFor;
```

```
Append(G,Q.Remainder);
EndIf;
EndWhile;
Return G;
EndDefine;
```

Appendix B

B.1

R::=Z \(3)[x[1..8]], Lex;

Use R;

I:=Ideal($x_1, x_2^3 - x_2, x_3^3 - x_3, x_4^3 - x_4, x_5^3 - x_5, x_6^3 - x_6, x_7^3 - x_7, x_8^3 - x_8, x_1^2 + x_1x_3 + x_3^2 - 1, x_1^2 + x_1x_4 + x_4^2 - 1, x_1^2 + x_1x_5 + x_5^2 - 1, x_2^2 + x_2x_4 + x_4^2 - 1, x_2^2 + x_2x_7 + x_7^2 - 1, x_2^2 + x_2x_8 + x_8^2 - 1, x_3^2 + x_3x_6 + x_6^2 - 1, x_3^2 + x_3x_8 + x_8^2 - 1, x_4^2 + x_4x_5 + x_5^2 - 1, x_5^2 + x_5x_6 + x_6^2 - 1, x_6^2 + x_6x_7 + x_7^2 - 1, x_6^2 + x_6x_8 + x_8^2 - 1, x_7^2 + x_7x_8 + x_8^2 - 1$);

GB.Start-GBasis(I);

GB.Step(I);

GB.Complete(I);

I.GBasis;

($x_1, x_5^2+x_5x_6+x_6^2-1, -x_6-x_7-x_8, -x_3+x_7, -x_2-x_7-x_8, -x_7-x_8, x_8^2-1, -x_4-x_5$)

ReducedGBasis(I);

($x_7 + x_8, x_8^2 - 1, x_4 + x_5, x_1, x_5^2 - 1, x_6, x_3 + x_8, x_2$)

B.2

R::=Z\(5)[x[1..5]], Lex;

Use R;

I:=Ideal($x_1^4 - 1, x_2^4 - 1, x_3^4 - 1, x_4^4 - 1, x_5^4 - 1, x_1^3 + x_1^2x_3 + x_1x_3^2 + x_3^3, x_1^3 + x_1^2x_4 + x_1x_4^2 + x_4^3, x_1^3 + x_1^2x_5 + x_1x_5^2 + x_5^3, x_2^3 + x_2^2x_3 + x_2x_3^2 + x_3^3, x_2^3 + x_2^2x_4 + x_2x_4^2 + x_4^3, x_2^3 + x_2^2x_5 + x_2x_5^2 + x_5^3, x_3^3 + x_3^2x_4 + x_3x_4^2 + x_4^3, x_3^3 + x_3^2x_5 + x_3x_5^2 + x_5^3, x_4^3 + x_4^2x_5 + x_4x_5^2 + x_5^3$);

GB.Start-GBasis(I);

GB.Step(I);

GB.Complete(I);

I.GBasis;

($x_4^3 + x_4^2 x_5 + x_4 x_5^2 + x_5^3, x_5^4 - 1, -x_3^2 - x_3 x_4 - x_3 x_5 - x_4^2 - x_4 x_5 - x_5^2, -2x_2 - 2x_3 - 2x_4 - 2x_5, -2x_1 - 2x_3 - 2x_4 - 2x_5$)

ReducedGBasis(I);

($x_4^3 + x_4^2 x_5 + x_4 x_5^2 + x_5^3, x_5^4 - 1, x_3^2 + x_3 x_4 + x_3 x_5 + x_4^2 + x_4 x_5 + x_5^2, x_2 + x_3 + x_4 + x_5, x_1 + x_3 + x_4 + x_5$)

B.3

R::=Z\(3)[x[1..5]], Lex;

Use R;

I:=Ideal($x_1^3 - x_1, x_2^3 - x_2, x_3^3 - x_3, x_4^3 - x_4, x_5^3 - x_5, x_1^2 + x_1 x_3 + x_3^2 - 1, x_1^2 + x_1 x_4 + x_4^2 - 1, x_1^2 + x_1 x_5 + x_5^2 - 1, x_2^2 + x_2 x_3 + x_3^2 - 1, x_2^2 + x_2 x_4 + x_4^2 - 1, x_2^2 + x_2 x_5 + x_5^2 - 1, x_3^2 + x_3 x_4 + x_4^2 - 1, x_3^2 + x_3 x_5 + x_5^2 - 1, x_4^2 + x_4 x_5 + x_5^2 - 1$);

GB.Start-GBasis(I);

GB.Step(I);

GB.Complete(I);

I.GBasis;

[-1]

ReducedGBasis(I);

[1]

B.4

R::=Z\(5)[x[1..9]], Lex;

Use R;

I:=Ideal($x_1^4 - 1, x_2^4 - 1, x_3^4 - 1, x_4^4 - 1, x_5^4 - 1, x_6^4 - 1, x_7^4 - 1, x_8^4 - 1, x_9^4 - 1, x_1^3 + x_1^2 x_4 + x_1 x_4^2 + x_4^3, x_1^3 + x_1^2 x_6 + x_1 x_6^2 + x_6^3, x_1^3 + x_1^2 x_7 + x_1 x_7^2 + x_7^3, x_1^3 + x_1^2 x_8 + x_1 x_8^2 +$

$x_8^3, x_2^3+x_2^2x_3+x_2x_3^2+x_3^3, x_2^3+x_2^2x_4+x_2x_4^2+x_4^3, x_2^3+x_2^2x_6+x_2x_6^2+x_6^3, x_2^3+x_2^2x_7+$
$x_2x_7^2+x_7^3, x_3^3+x_3^2x_5+x_3x_5^2+x_5^3, x_3^3+x_3^2x_7+x_3x_7^2+x_7^3, x_3^3+x_3^2x_9+x_3x_9^2+x_9^3, x_4^3+$
$x_4^2x_5+x_4x_5^2+x_5^3, x_4^3+x_4^2x_6+x_4x_6^2+x_6^3, x_4^3+x_4^2x_7+x_4x_7^2+x_7^3, x_4^3+x_4^2x_9+x_4x_9^2+$
$x_9^3, x_5^3+x_5^2x_6+x_5x_6^2+x_6^3, x_5^3+x_5^2x_7+x_5x_7^2+x_7^3, x_5^3+x_5^2x_8+x_5x_8^2+x_8^3, x_5^3+x_5^2x_9+$
$x_5x_9^2+x_9^3, x_6^3+x_6^2x_7+x_6x_7^2+x_7^3, x_6^3+x_6^2x_9+x_6x_9^2+x_9^3, x_7^3+x_7^2x_8+x_7x_8^2+x_8^3$)

GB.Start-GBasis(I);

GB.Step(I);

GB.Complete(I);

ReducedGBasis(I);

($x_7-x_9, x_8^3+x_8^2x_9+x_8x_9^2+x_9^3, x_5^2+x_5x_8+x_5x_9+x_8^2+x_8x_9+x_9^2, x_4+x_5+$
$x_6+x_9, x_1-x_5, x_2-x_5, x_3^2+x_3x_5+x_3x_9-x_5x_8-x_8^2-x_8x_9, x_6^3+x_6^2x_9+x_6x_9^2+$
$x_9^3, x_9^4-1, x_5x_6-x_5x_8+x_6^2+x_6x_9-x_8^2-x_8x_9$)

B.5

R::=Z/(3)[x[1..9]], Lex;

Use R;

I:=Ideal($x_1^3-x_1, x_2^3-x_2, x_3^3-x_3, x_4^3-x_4, x_5^3-x_5, x_6^3-x_6, x_7^3-x_7, x_8^3-x_8, x_9^3-$
$x_9, x_1^2+x_1x_4+x_4^2-1, x_1^2+x_1x_6+x_6^2-1, x_1^2+x_1x_7+x_7^2-1, x_1^2+x_1x_8+x_8^2-1, x_2^2+$
$x_2x_3+x_3^2-1, x_2^2+x_2x_4+x_4^2-1, x_2^2+x_2x_6+x_6^2-1, x_2^2+x_2x_7+x_7^2-1, x_3^2+x_3x_5+$
$x_5^2-1, x_3^2+x_3x_7+x_7^2-1, x_3^2+x_3x_9+x_9^2-1, x_4^2+x_4x_5+x_5^2-1, x_4^2+x_4x_6+x_6^2-1, x_4^2+$
$x_4x_7+x_7^2-1, x_4^2+x_4x_9+x_9^2-1, x_5^2+x_5x_6+x_6^2-1, x_5^2+x_5x_7+x_7^2-1, x_5^2+x_5x_8+$
$x_8^2-1, x_5^2+x_5x_9+x_9^2-1, x_6^2+x_6x_7+x_7^2-1, x_6^2+x_6x_9+x_9^2-1, x_7^2+x_7x_8+x_8^2-1$)

GB.Start-GBasis(I);

GB.Step(I);

GB.Complete(I);

I.GBasis;

[-1]

ReducedGBasis(I);

[1]

B.6

Use S::=Q[x,u,v,w], Lex;

K:=Ideal($-x^4 - x + u, -x^3 + v, -x^5 + w$);

GB.Start-GBasis(K);

GB.Step(K);

GB.Complete(K);

K.GBasis;

($-u^3 + v^4 + 3v^3 + 3v^2 + v, u^2v - v^2w - 2vw - w, -uw + v^3 + v^2, -uv^3 + vw^2 + w^2, x - uv^2 + uv - u + w^2, v^5 - w^3$)

F:=x;

DivAlg(F,K.GBasis);

Record[Quotients = [0, 0, 0, 0, 1, 0], Remainder = $\mathbf{uv^2 - uv + u - w^2}$]

B.7

Let $y_1 = x_3, y_2 = x_4, y_3 = x_5$.

Use R::=Q[x[1..5]], Lex;

K:=Ideal($-x_1^3 x_2^4 + x_3\,, -x_1^2 x_2^3 + x_4\,, -x_1\,x_2 + x_5$);

GB.Start-GBasis(K);

GB.Step(K);

GB.Complete(K);

K.GBasis; [$-x_1\,x_2 + x_5\,, -x_2\,x_5^2 + x_4\,, x_1\,x_4 - x_5^3, x_3 - x_4\,x_5$]

F:=$x_1^{10} x_2^4$;

DivAlg(F,K.GBasis);

Record[Quotients = [$-x_1^3 x_2^4 + x_3\,, -x_1^2 x_2^3 + x_4\,, -x_1\,x_2 + x_5$],

Remainder =$x_1^6\,x_5^4$]

B.8

Let $x_3 = w, x_4 = y_1, x_5 = y_2, x_6 = y_3, x_7 = y_4$.

Use R::=Q[x[1..7]], Lex;

K:=Ideal($x_1 x_2 x_3 - 1, -x_1^5 x_3 + x_4, -x_1 x_2^2 + x_5, -x_2 x_3 + x_6, -x_1^2 x_3 + x_7$);

GB.StartGBasis(K);

GB.Step(K);

GB.Complete(K);

K.GBasis; [$-x_3 + x_6^2 x_7, -x_2 + x_5 x_6^2 x_7, -x_4 + x_5 x_7^3, -x_5 x_6^3 x_7^2 + 1, x_1 - x_5 x_6^2 x_7^2$]

F:=$x_1^{10} x_2^4$;

DivAlg(F,K.GBasis);

Record[Quotients = [$-x_1^7, 0, 0, -x_1^6 x_6 x_7 - x_1^5 x_7 - x_1^3 x_5 x_6 x_7^3 - x_1^2 x_5 x_7^3 - x_5^2 x_6 x_7^5, x_1^6 x_6^2 x_7 + x_1^5 x_6 x_7 + x_1^4 x_7 + x_1^3 x_5 x_6^2 x_7^3 + x_1^2 x_5 x_6 x_7^3 + x_1 x_5 x_7^3 + x_5^2 x_6^2 x_7^5$],

Remainder = $x_5^2 x_6 x_7^5$]

B.9

Use S::=Q[x,y], Lex;

K:=Ideal($x^2 - xy + y^2, x^3 - x^2 y, x^2 y - xy^2, xy^2 - y^3, x^3 + y^3$);

GB.Start-GBasis(K);

GB.Step(K);

GB.Complete(K);

K.GBasis;

$[x^2 - xy + y^2, xy^2 - y^3, -y^3]$

ReducedGBasis(K);

$[y^3, x^2 - xy + y^2, xy^2]$

BIBLIOGRAPHY

[1] T.W. Hungerford, Graduate Texts in Mathematics, Springer-Verlag 1974.

[2] M. Reid, Undergraduate Commutative Algebra, London Mathematical Society Student Texts 29,2002.

[3] W.W. Adams and P. Loustanou, An Introduction To Gröbner Bases, American Mathematical Society,1991.

[4] D.S. Dummit and R.M. Foote, Abstract Algebra, John Wiley and Sons Inc.,2004.

[5] B.Buchberger , Gröbner Bases: A Short Introduction for System Theorists.

[6] M. Kanuni Lecture Notes on Abstract Algebra, Bosphorus University, 2004.

[7] N. Lauritzen,Concrete Abstract Algebra From Numbers To Gröbner Bases, Cambridge University Press ,2003.

[8] A. Kehren, M. Kreuzer, Characterization of Border Basis, Journal of Pure and Applied Algebra ,196 (2005)251-270.

[9] A. Kehren, M. Kreuzer, Computing of Border Basis, Journal of Pure and Applied Algebra ,205 (2006)279-295.

[10] M. Kreuzer, L. Robbiano, Computational Commutative Algebra I, Springer-Verlag Berlin Heidelberg, 2000.

[11] M. Kreuzer, L. Robbiano, Computational Commutative Algebra II, Springer-Verlag Berlin Heidelberg, 2005.

[12] CoCoA Team, CoCoA: a system for doing Computations in Commutative Algebra, Available at http://cocoa.dima.unige.it