Thesis for the Degree of Master of Science

# Defining Equations of Rational Curves on a Rational Normal Surface Scroll $S(1,2)$


by

Woo-Young Jang

Department of Applied Mathematics

The Graduate School

Pukyong National University

August 2018

# Defining Equations of Rational Curves on a Rational Normal Surface Scroll $S(1,2)$

# 정규 유리곡면 $S(1,2)$위에 매립된 유리곡선들의 결정방정식에 관한 연구

Advisor : Prof. Wanseok Lee

by

Woo-Young Jang

A thesis submitted in partial fulfillment of the requirement
for the degree of

Master of Science

in the Department of Applied Mathematics, The Graduate School,
Pukyong National University

August 2018

# Defining Equations of Rational Curves on a Rational Normal Surface Scroll $S(1,2)$

A dissertation

by

Woo-Young Jang

Approved by :

_____

(Chairman) Yong-Soo Pyo, Ph. D.

_____ _____

(Member) Hyo-Seob Sim, Ph. D. (Member) Wanseok Lee, Ph. D.

August 24, 2018

# CONTENTS

# 정규 유리곡면 $S(1,2)$위에 매립된 유리곡선들의 결정방정식에 관한 연구

장 우 영

부경대학교 대학원 응용수학과

## 요 약

이 논문에서는 정규 유리곡면 $S(1,2)$ 위에 매립된 유리곡선들의 결정방정식에 관하여 연구하였다. 먼저 아핀다양체, 사영다양체, 정규 유리곡면, 정규 유리곡선 등 다항식들의 공통근으로 정의되는 대수적 집합의 성질을 살펴보고, 뇌터환의 원소를 계수로 가지는 다항식 환에서 힐베르트 기저정리가 성립함을 조사하였다. 또한 기약 대수적 집합과 유한개의 생성원을 가지는 가군, 체의 확대, 인테그랄 원소의 성질을 통하여 힐베르트 영점정리를 살펴보았고, 대수기하학의 기반이 되는 아이디얼들의 합과 곱, 교집합, 동차다항식이 가지는 성질, 다항식으로 이루어지는 사상 등 여러 가지 대수학의 기본 개념을 연구하였다.

정규 유리곡면 $S(1,2)$위에 매립된 유리곡선의 생성원을 구하기 위하여 'SINGULAR'프로그램을 이용하여 유리곡선들의 차수가 $5,6,7,8,9,10$일 때 각 차수에 대응하는 아이디얼의 생성원들을 계산하였다. 다음으로, 계산된 생성원들이 가지는 패턴을 이용하여 유리곡선의 일반적인 차수에 대하여 유리곡선을 정의하는 생성원들의 모양을 묘사하였고 실제 아이디얼을 생성함을 증명하였다. 80년대에 독일에서 처음 만들어진 컴퓨터 대수 계산 프로그램인 'SINGULAR'는 Gröbner Basis이론을 바탕으로 컴퓨터의 빠른 발달과 함께 대수기하학에서 정의되는 여러 가지 불변량들을 계산해준다.

# Chapter 1

# Preliminaries

In this chapter, we briefly introduce the fundamental definitions and concepts of commutative algebra based on two textbooks: Abstract Algebra [3] and Introduction to Commutative Algebra [1].

Through out this paper, a *ring* is a commutative ring with a multiplicative identity. A *domain* or *integral domain* is a ring without a zero divisor. A $field$ is a domain in which every non-zero element is a unit. That is, every non-zero element has a multiplicative inverse. When a non-empty subset $S$ of a ring $R$ is itself a ring under the addition and multiplication in $R$, then we say that $S$ is a *subring* of $R$. Note that a subring does not need to have a multiplicative identity to be sure.

A subring $I$ of $R$ is called an *ideal* of $R$ if $ar \in I$ for all $a \in I$ and $r \in R$. An ideal $M$ in $R$ is said to be *maximal* if $M \neq R$ and whenever $J$ is an ideal such that $M \subseteq J \subseteq R$ then $M = J$ or $J = R$. An ideal $P$ in $R$ is called prime, if $P \neq R$ and whenever $ab \in P$ then $a$ or $b$ in $P$. An ideal $I$ is said to be $finitely\ generated$ if $I = \{a_1r_1 + a_2r_2 + \cdots + a_nr_n \mid r_i \in R\}$ with for some $a_i \in I$, and denote by $(a_1, a_2, ..., a_n)$. If $I$ is generated by one element then we call $I$ is a *principal* ideal. A domain in which every ideal is principal is called a *principal ideal domain*, simply PID.

The ring of polynomials in $n$ variables over $R$ is written $R[X_1, ..., X_n]$. We call *monomials* that is the polynomial $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} \in R[X_1, ..., X_n]$, the degree of monomial is $i_1 + \cdots + i_n$. Take any polynomial $F$ in $R[X_1, ..., X_n]$, then $F$ has expression : $F = \sum a_{(i)}X^{(i)}$ with $X^{(i)}$ are the monomials, $a_{(i)} \in R$. Then we

can define *homogeneous* as a polynomial that is every terms have same degree. Any polynomial $F$ has a unique expression : $F = F_d + F_{d-1} + \cdots + F_0$ where $F_i$ are monomials of degree $i$, if $F_d$ is not zero then $d$ is the degree of $F$ and written $deg(F)$. For all $f \in R[X]$ where $R$ is a ring then $f$ is of the form: $f(X) = a_dX^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$, if $a_d \neq 0$ then $a_d$ is said to be leading coefficient of $f$, and denoted by $lc(f) = a_d$.

Let $R$ be a domain, $F$ and $G$ are homogeneous polynomials of ring $R[X_1, ..., X_n]$. Then $FG$ is still a homogeneous polynomial. Suppose that $deg(F) = s$ and $deg(G) = t$, and we have :

$$F = \sum a_{(i)}X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}, \qquad G = \sum b_{(j)}X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n},$$

where $i_1 + \cdots i_n = s$ and $j_1 + \cdots j_n = t$. Then clearly every terms of $FG$ are monomials of degree $s + t$, hence any finite product of homogeneous polynomials is a homogeneous polynomial.

If every ideal in a ring $R$ is finitely generated, then $R$ is said to be *noetherian* ring.

**Proposition 1.1**. *If $R$ is a noetherian ring and let $S$ be the set of leading coefficient of all polynomials in ideal $I$ in $R[X]$. Then $S$ is an ideal in $R$.*

**Proof.** First prove that $S$ is a subgroup of $R$. Consider for all $a$, $b$ in $S$ then there exist a polynomials $f$ and $g$ in $R[X]$ such that $lc(f) = a$, $lc(g) = b$, and $deg(f) = deg(g)$, then there exist $-f$, $-g$ are in $I$ and clearly $(f - g)$ is in $I$. Focus on there leading coefficien.

$$\begin{aligned} f(X) &= aX^d + \cdots + a_0, \\ g(X) &= bX^d + \cdots + b_0, \\ (f-g)(X) &= (a-b)X^d + \cdots + (a_0 - b_0). \end{aligned}$$

Thus $lc(f - g) = (a - b) \in S$, and hence $S$ is a subgroup of $R$.

Second, prove the ideal property. Take for all $n \in R$, for every $a \in S$, then $a = lc(f)$ for some polynomial $f \in I$. Consider the polynomial $bf$. Since $I$ is an ideal, $bf \in I$. Thus $lc(bf) = ab \in S$. Furthermore, $S$ is an ideal of $R$.

**Lemma 1.2.** *Suppose that $R$ is an noetherian. If $I$ is an ideal of ring $R[X]$, then $S_m = \{lc(f) \mid f \in I,\ deg(f) \leq m\}$ is an ideal of $R$ with $m$ is a positive integer.*

**Proof.** Clearly $S_m$ is a subset of $R$. We must show that $S_m$ is a subgroup of $R$ and satisfy the ideal property on $R$. Let $a, b$ be an elements of $S_m$, then $a = lc(f)$ and $b = lc(g)$ for some polynomials $f$, $g \in I$ with $deg(f) = d_1 \leq m$ and $deg(g) = d_2 \leq m$.

$$f(X) = aX^{d_1} + a_{d_1-1}X^{d_1-1} + \cdots + a_0,$$
$$g(X) = bX^{d_2} + b_{d_2-1}X^{d_2-1} + \cdots + b_0.$$

Since $I$ is an ideal, there exists $-g(X) \in I$ such that

$$-g(X) = -bX^{d_2} - b_{d_2-1}X^{d_2-1} - \cdots - b_0.$$

Assume that $d_1 \geq d_2$. If $d_1 = d_2$ then $(a - b) \in S_m$, we are done. Therefore suppose that $d_1 > d_2$ Consider $-g(X)X^{d1-d2}$ :

$$\begin{aligned} -g(X)X^{d_1-d_2} &= (-bX^{d_2} - b_{d_2-1}X^{d_2-1} - \cdots - b_0)X^{d_1-d_2} \\ &= -bX^{d_1} - b_{d_2-1}X^{d_1-1} - \cdots - b_0X^{d_1-d_2}. \end{aligned}$$

This polynomial has degree $d_1$ and leading coefficient $-b$. Then polynomial

$$\begin{aligned} f(X) - g(X)X^{d_1-d_2} &= aX^{d_1} + a_{d_1-1}X^{d_1-1} + \cdots + a_0 \\ &\quad - bX^{d_1} - b_{d_2-1}X^{d_1-1} - \cdots - b_0X^{d_1-d_2} \\ &= (a-b)X^{d_1} + (a_{d_1-1} - b_{d_2-1})X^{d_1-1} + \cdots . \end{aligned}$$

Therefore, $f(X) - g(X)X^{d_1-d_2} \in I$ and degree $d_1 \leq m$, and hence $(a - b) \in S_m$. Thus $S_m$ is a subgroup of $R$.

Now show that ideal property. Let $a$ be an element of $S_m$ and let $b$ be an element of $R$. Then $a = lc(f)$ for some polynomial $f \in I$ with $deg(f) \leq m$. Then $bf(X) \in I$ and $deg(bf) = deg(f)$. Therefore $lc(bf) = ab \in S_m$. Consequently, $S_m$ is an ideal of $R$.

A domain $R$ is said to be a *unique factorization domain* provided that every non-zero, non-unit element of $R$ is the product of irreducible elements, and this factorization is unique, written UFD. If $R$ is UFD, then $R[X]$ is also a UFD. Therefore $k[X_1, ..., X_n]$ is a UFD for any field $k$.

A field $k$ is said to be *algebraically closed* if any non-constant polynomial $F \in k[X]$ has a same number of root as degree of $F$. The field $\mathbb{C}$ of compelx numbers is an algebraically closed field.

Let $k$ be any field, then there are infinite number of irreducible monic polynomials in $k[X]$. Suppose that there are finitely many monic polynomials $F_1, ..., F_n$ in $k[X]$. We may assume that $F_i \neq 1$ for all $i$. Let $G$ be an irreducible factor of the monic polynomial $F_1F_2 \cdots F_n + 1$, then leading coefficient of $G$ must be a unit by multiplying $G$ by the inverse of its leading coefficient. We may assume that $G$ is monic. Thus $G = F_i$ for some $i$. Hence $F_i$ divides $F_1F_2 \cdots F_n + 1$ hence $F_i$ divides 1. Since $F_i \neq 1$ and hence $F_i$ does not divides $F_1F_2 \cdots F_n + 1$. This contradicts the assumption.

Any algebraically closed field is infinite. The irreducible polynomials are of the form $X - a$ where $a \in k$. However there are an infinite number of these polynomials by above discussion, hence there must be infinitely many $a \in k$.

[The first isomorphism theorem] Let $R$ be a ring, and let $\varphi : R \to S$ be a ring homomorphism. Then the image of $\varphi$ is isomorphic to the quotient ring $R/Ker(\varphi)$. If $\varphi$ is surjective then $S$ is isomorphic to $R/Ker(\varphi)$.

Let $I$ be an ideal of a ring $R$. Then $I$ is a prime ideal if and only if $R/I$ is domain. Let $I$ be an ideal of a ring $R$. Then $I$ is a maximal ideal if and only if $R/I$ is a field.

**Lemma 1.3.** *Let $I$ be an ideal of a PID $R$ and if $I$ is a prime ideal of $R$ that is not zero and whole ring. Then $I$ is generated by an irreducible element and $I$ is a maximal ideal of $R$.*

**Proof.** Since $I$ is principal, then $I = (g)$. Suppose that $g = ab$, then $ab \in I$ and since $I$ is prime $a$ or $b$ in $I$, if $a$ in $I$ then $a = gc$ for some $c \in R$. Thus $g = ab = gcb$, and hence $cb = 1$. Therefore $I$ becomes the whole. This is a contradiction. Therefore $g$ is an irreducible element of $R$. To show that $I$ is maximal, suppose that there exists ideal $J \in R$ such that $I \subseteq J \subseteq R$. Since $I$, $J$ is principal, $I = (i)$, $J = (j)$ with $i$, $j \in R$. Thus $i \in J$, then there exists $a$ in $R$ such that $i = ja$. Since generator of $I$ is irreducible, hence $j = 1$ or $a = 1$.if $j = 1$ then $J = R$, if $a = 1$ then $I = J$. Thus $I$ is maximal ideal of $R$.

**Lemma 1.4.** *For an infinie field $k$, a polynomial $F \in k[X_1, ..., X_n]$. If $F(a_1, ..., a_n) = 0$ with for every $a_1, ..., a_n \in k$, then $F = 0$.*

**Proof.** Use induction on $n$, $n = 1$ then for all $F \in k[X_1] - \{0\}$ have a finite roots. Suppose that is true for polynomials in $(n-1)$ variables. $F = \sum_i F_i X_n^i$ where $F_i \in k[X_1, ..., X_{n-1}]$. Then there exits $(b_1, ..., b_{n-1}) \in k$ such that $F_i(b_1, ..., b_{n-1}) \neq 0$. Then consider, the polynomial $F(b_1, ..., b_{n-1}, X_n) \neq 0$ has a finite number of roots. Therefore there are infinitely many choices for the variable $X_n$ such that $F(b_1, ..., b_{n-1}, X_n) \neq 0$. Hence the only polynomial that vanish on every points in $k$ is the zero polynomial.

# Chapter 2

# Affine algebraic set

This chapter is devoted to prove Hilbert's basis theorem and Hilbert' Nullstellensatz. For this aim, we investigate the basic notions and definitions of algebraic geometry based on the textbook: Algebraic Curves-An Introduction to Algebraic Geometry [2]

## 2.1 Hilbert's Basis Theorem

### 2.1.1 Affine algebraic sets

**Definition 2.1**. Let $k$ be any field. The cartesian product of $k$ with $n$ times:

$$\mathbb{A}^n(k) = \underbrace{k \times \cdots \times k}_{n-times};$$

we call $\mathbb{A}^n(k)$ an affine space over $k$, and its elements call points.

A point $P = (a_1, ..., a_n) \in \mathbb{A}^n(k)$ is called a *zero* of $f$ if $f(P) = f(a_1, ..., a_n) = 0$ with $f \in k[X_1, ..., X_n]$. And if $f$ is not a constant, the set $V(f) = \{(a_1, ..., a_n) \mid f(a_1, ..., a_n) = 0$ with $(a_1, ..., a_n) \in \mathbb{A}^n(k)\}$ is called the hypersurface defined by $f$. If $f$ is a polynomial of degree one, $V(f)$ is called a hyperplane in $\mathbb{A}^n(k)$.

Let $S$ be a set of polynomials in $k[X_1, ..., X_n]$, then $V(S)$ is defined as follows: $V(S) = \{(a_1, ..., a_n) \in \mathbb{A}^n(k) \mid f(a_1, ..., a_n) = 0$, for all $f \in S\}$.

**Definition 2.2**. The set $X \subset \mathbb{A}^n(k)$ is called an affine algebraic set, if $X = V(S)$ for some S.

By definition 2.2, we may regard that an algebraic set as a set of common root of polynomials.

**Proposition 2.3**. *Let $I$ be the ideal of $k[X_1, ..., X_n]$ generated by the set of polynomial $S$, then $V(S) = V(I)$.*

**Proof.** Let $(a_1, ..., a_n)$ be a point of $V(I)$, then $f(a_1, ..., a_n) = 0$ for all $f \in I$. Since $S \subseteq I$ and $g(a_1, ..., a_n) = 0$ for all $g \in S$. Thus $V(I) \subseteq V(S)$. Show that $V(I) \supseteq V(S)$, let $(a_1, ..., a_n)$ be a point of $V(S)$ and $g \in I$ such that $g = \sum f_i h_i$ where $f_i \in S$ and $h_i \in k[X_1, ..., X_n]$. Since $f_i(a_1, ..., a_n) = 0$, $g(a_1, ..., a_n) = g = \sum f_i(a_1, ..., a_n)h_i(a_1, ..., a_n) = 0$ for all $i$. Therefore $V(I) \supseteq V(S)$, and hence $V(S) = V(I)$.

Therefore every algebraic set is equal to $V(I)$ for some ideal $I$. Thus, instead of thinking about $V(S)$, we can think of the property of ideal $V(I)$.

**Proposition 2.4**. *If $\{I_\alpha\}$ is any collection of ideals then $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$.*

**Proof.** Let $(a_1, ..., a_n)$ be a point in $V(\cup_\alpha I_\alpha)$, then for all $\alpha$ and all $f \in I_\alpha$ we have $f(a_1, ...a_n) = 0$, thus $(a_1, ...a_n) \in \cap_\alpha V(I_\alpha)$. Therefore $V(\cup_\alpha I_\alpha) \subset \cap_\alpha V(I_\alpha)$. Let $(a_1, ..., a_n)$ be a point in $\cap_\alpha V(I_\alpha)$, then for all $\alpha$ and for all $f \in I_\alpha$ we have $f(a_1, ..., a_n) = 0$, thus $(a_1, ..., a_n) \in V(\cup_\alpha I_\alpha)$, and hence $V(\cup_\alpha I_\alpha) \supset \cap_\alpha V(I_\alpha)$. Consequently, $V(\cup_\alpha I_\alpha) = \cap_\alpha V(I_\alpha)$.

Proposition 2.4 give us, every algebraic set is written by the intersection of any collection of algebraic sets, without whether the collection is infinite or not.

**Proposition 2.5**. *If ideal $I$ is a subset of ideal $J$, then $V(I) \supseteq V(J)$.*

**Proof.** Let $(a_1, ..., a_n)$ be a point in $V(J)$. Then $F(a_1, ..., a_n) = 0$ for all $F \in J$. Since $I \subseteq J$ we know that $G(a_1, ..., a_n) = 0$ for all $G \in I$, and hence $V(I) \supseteq V(J)$.

**Proposition 2.6**. *Let $F$, $G$ be a polynomials in $k[X_1, ..., X_n]$, then $V(FG) = V(F) \cup V(G)$; $V(I) \cup V(J) = V(\{FG \mid F \in I,\, G \in J\})$.*

**Proof.** Let $(a_1, ..., a_n)$ be a point in $V(I) \cup V(J)$. Then $F(a_1, ..., a_n) = 0$ for all $F \in I$ or $G(a_1, ..., a_n) = 0$ for all $G \in J$. Then $(FG)(a_1, ..., a_n) = 0$ for all

$F \in I$ and $G \in J$ since $F(a_1, ..., a_n) = 0$. Therefore $V(I) \cup V(J) \subseteq V(\{FG \mid F \in I,\ G \in J\})$. Let $(a_1, ..., a_n)$ be a point in $V(\{FG \mid F \in I,\ G \in J\})$. Then $(FG)(a_1, ..., a_n) = 0$ for all $F \in I$ and $G \in J$. If $G(a_1, ..., a_n) = 0$ for all $G \in J$ then $(a_1, ..., a_n) \in V(J) \subseteq V(I) \cup V(J)$. Otherwise if $G(a_1, ..., a_n) \neq 0$. Then $(FG)(a_1, ..., a_n) = 0$ for all $F \in I$, and hence $F(a_1, ..., a_n) = 0$ for all $F \in I$. Thus $(a_1, ..., a_n) \in V(I) \subseteq V(I) \cup V(J)$. Therefore $V(\{FG \mid F \in I,\ G \in J\}) \subseteq V(I) \cup V(J)$.

**Proposition 2.7**. $V(0) = \mathbb{A}^n(k)$, $V(1) = \varnothing$, $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\}$ *with* $a_i \in k$.

**Proof.** If $V(0) \neq \mathbb{A}^n(k)$ then there exists $(a_1, ..., a_n) \in \mathbb{A}^n(k)$ such that $0(a_1, ..., a_n) \neq 0$. But it is impossible, and hence $V(0) = \mathbb{A}^n(k)$. And if $V(1) \neq \varnothing$ then there exists $(a_1, ..., a_n) \in \mathbb{A}^n(k)$ such that $1(a_1, ..., a_n) = 0$, this is also impossible. Thus $V(1) = \varnothing$. By definition of algebraic set, $V(X_1 - a_1, ..., X_n - a_n) = \{(a_1, ..., a_n)\}$ is clear.

Consider the number of algebraic sets on $\mathbb{A}^1(k)$, Let $X$ be an algebraic set of $\mathbb{A}^1(k)$, then $X = V(S)$ for some set of polynomials $S$. If $S = 0$ then $X = V(0) = \mathbb{A}^1(k)$. If not there exists $F$ in $V(S)$, then $F$ has at most $deg(F)$ roots, and hence $V(S) \subset V(F)$. Therefore $V(S) = X$ has finite numbers of points. Therefore the algebraic subsets of $\mathbb{A}^1(k)$ are the finite subsets, together with $\mathbb{A}^1(k)$ itself.

Let $F$ be a nonconstant polynomial in $k[X_1, ..., X_n]$, $k$ algebraically closed. Then $\mathbb{A}^n(k) - V(F)$ is infinite if $n \geq 1$, and $V(F)$ is infinite if $n \geq 2$. Use indction on $n$. If $n = 1$ $\mathbb{A}^1(k) - V(F)$ then clearly $\mathbb{A}^n(k) - V(F)$ is infinite. Since any algebraic set of $\mathbb{A}^1(k)$ is finite subset of $\mathbb{A}^1(k)$. Suppose that the claim holds for polynomial in $n-1$ variables. Consider $F(X_1, X_2, ..., X_{n-1}, 1)$. This is a polynomial in $n-1$ variables and thus there are infinitely many points that are not solutions to the equation $F(X_1, X_2, ..., X_{n-1}, 1) = 0$ and therefore infinitely points that are not solutions to the equation $F(X_1, X_2, ..., X_n) = 0$. For the second part, for any $a_1, ...a_{n-1} \in k$ the polynomial $F(a_1, ...a_{n-1}, X_n) = 0$ has at least one

solution. Since there are infinitely many choices for $a_1, ...a_{n-1}$ there are infinitely solutions to $F(X_1, ..., X_n) = 0$. The conclusion follows since any algebraic set $V(I)$ choose $F \in I$ then $V(I) \subseteq V(F)$. Thus the complement of any proper algebraic set is infinite.

**Lemma 2.8** *Let $X$ and $Y$ be an algebraic sets of $\mathbb{A}^n(k)$ and $\mathbb{A}^m(k)$ respectively. Then it satisfies the following :*

$$X \times Y = \{(x_1, ..., x_n, y_1, ..., y_m) \mid (x_1, ..., x_n) \in X,\ (y_1, ..., y_m) \in Y\}$$

*is an algebraic set in $\mathbb{A}^{n+m}(k)$. It is called the product of $X$ and $Y$.*

**Proof.** $X = V(S)$ and $Y = V(T)$ for some set of polynomials $S$, $T$. Rename the variable in $T$ so that they begin at $X_{n+1}$ and end at $X_{n+m}$ then $X \times Y = V(X \cup Y)$.

### 2.1.2 The ideal of a set of points

**Definition 2.9**. Let $X$ be a subset of $\mathbb{A}^n(k)$. Then the set $I(X)$ is defined as follows:

$$I(X) = \{f \in k[X_1, ..., X_n] \mid F(a_1, ..., a_n) = 0 \text{ for all } (a_1, ..., a_n) \in X\}.$$

**Lemma 2.10.** *Under the situation as above, $I(X)$ is an ideal of $k[X_1, ..., X_n]$, and $I(X)$ is called the ideal of a set of points.*

**Proof.** for all $f$, $g \in I(X)$, then for all $(a_1, ..., a_n) \in X$ consider $(f - g)$ :

$$(f - g)(a_1, ..., a_n) = f(a_1, ..., a_n) - g(a_1, ..., a_n) = 0$$

Thus $I(X)$ is a subgroup of $k[X_1, ..., X_n]$. And for all $f \in I(X)$, for all $g \in k[X_1, ..., X_n]$, then for all $(a_1, ..., a_n) \in X$

$$\begin{aligned}(fg)(a_1, ..., a_n) &= f(a_1, ..., a_n)g(a_1, ..., a_n) \\ &= 0 \cdot g(a_1, ..., a_n) = 0\end{aligned}$$

Therefore $fg \in I(X)$, and hence $I(X)$ is an ideal of $k[X_1, ..., X_n]$.

**Proposition 2.11**. *If $X$ is a subset of $Y$, then $I(X) \supset I(Y)$.*

**Proof.** Let $F$ be a polynomial in $I(Y)$ then $F(a_1, ..., a_n) = 0$ for all $(a_1, ..., a_n) \in Y$. Since $X$ is a subset of $Y$ we know $F(b_1, ..., b_n) = 0$ for all $(b_1, ..., b_n) \in X$. Thus $F$ is an element of $I(X)$.

**Proposition 2.12**. *$I(\varnothing) = k[X_1, ..., X_n]$ and $I(\mathbb{A}^n(k)) = (0)$ if $k$ is an infinite field.*

**Proof.** $I(\varnothing) = k[X_1, ..., X_n]$ is clear. Show that $I(\mathbb{A}^n(k)) = (0)$ if $k$ is an infinite field. Suppose that $F \in I(\mathbb{A}^n(k))$ and nonzero polynomial, then $F(a_1, ..., a_n) = 0$ with for all $(a_1, ..., a_n) \in \mathbb{A}^n(k)$. Therefore we can take the set $\{(x_1, 0, ..., 0)\} \subset \mathbb{A}^n(k)$, then $F(x_1, 0, ..., 0) = 0$ for all $x_1 \in k$. Since $F(x_1, 0, ..., 0)$ is a one variable polynomial, hence $F(x_1, 0, ..., 0)$ is satisfying the fundermental theorem of algebra. Then $F(x_1, 0, ..., 0)$ have must finite numbers of roots, but $F(x_1, 0, ..., 0)$ has infinitely many zeros, this is a contradiction. Thus $F = 0$.

**Proposition 2.13**. *$I(\{(a_1, ..., a_n)\}) = (X_1 - a_1, ..., X_n - a_n)$ with $a_i \in k$.*

**Proof.** $I(\{(a_1, ..., a_n)\}) \supset (X_1 - a_1, ..., X_n - a_n)$ is clear. Show that $I(\{(a_1, ..., a_n)\})$ $\subset (X_1 - a_1, ..., X_n - a_n)$. Suppose that for all $F \in I(\{(a_1, ..., a_n)\})$, then $F(a_1, ..., a_n)$ $= 0$. Therefore $F = \sum_{i=1}^{n} (X_i - a_i)G_i$, and hence $F \in (X_1 - a_1, ..., X_n - a_n)$. Therefore $I(\{(a_1, ..., a_n)\}) = (X_1 - a_1, ..., X_n - a_n)$.

**Proposition 2.14**. *Let $S$ be a subset of $k[X_1, ..., X_n]$, then $I(V(S)) \supset S$. And let for all $X$ be a subset of $\mathbb{A}^n(k)$ then $V(I(X)) \supset X$.*

**Proof.** Suposse that for all $S \subset k[X_1, ..., X_n]$ then we can make the set $V(S) = \{p \in \mathbb{A}^n(k) \mid F(p) = 0, \text{ for all } F \in S\}$. If $V(S) = \varnothing$, then $I(V(S)) = I(\varnothing) = k[X_1, ..., X_n] \supset S$. If not, consider definition of $I(V(S))$ : is the set of polynomials that vanish on $V(S)$. Since every element of $S$ vanish on $V(S)$, hence $I(V(S)) \supset S$.

**Proposition 2.15**. *Let for all $S$ be a subset of $k[X_1, ..., X_n]$, then $V(I(V(S))) = V(S)$. And let for all $X$ be a subset of $\mathbb{A}^n(k)$ then $I(V(I(X))) = I(X)$.*

**Proof.** Take for all $P \in V(I(V(S)))$, then point $P$ is the root of for every polynomials in $I(V(S))$. It means $P \in V(S)$ since $I(V(S))$ is the set of polynomials that vanish on $V(S)$. Thus $V(I(V(S))) \subset V(S)$. Suppose that for all $P \in V(S)$ and show that $P \in V(I(V(S)))$. Clearly $P$ is root of every polynomials in $I(V(S))$. Thus $P \in V(I(V(S)))$, and hence $V(I(V(S))) = V(S)$.

Shows that $I(V(I(X))) = I(X)$. First $I(V(I(X))) \subset I(X)$, let $F$ be a polynomial in $I(V(I(X)))$, then $F(P) = 0$ for all $P \in V(I(X))$. Since $P$ is the root of every polynomials in $I(X)$, thus $P \in X$, and hence $F \in I(X)$. Second $I(V(I(X))) \supset I(X)$, take any polynomial $F$ in $I(X)$, then there exists $P \in V(I(X))$ such that $G(P) = 0$ with for all $G \in I(X)$. And any polynomial in $I(V(I(X)))$ vanish on $P$, thus $F \in I(V(I(X)))$. Therefore $I(V(I(X))) = I(X)$.

**Definition 2.16**. Let $I$ be an ideal of $R$. Define $Rad(I) = \{a \in R \mid a^n \in I\}$ where integer $n > 0$. We called $Rad(I)$ the radical of $I$. If $I = Rad(I)$ then $I$ is said to be a radical ideal.

**Proposition 2.17**. *$Rad(I)$ is an ideal of ring $R$, $I \subset Rad(I)$.*

**Proof.** Clearly $Rad(I)$ is an subset of $R$. Take for all $a$, $b \in Rad(I)$ then there exist $n$, $m$ such that $a^n$, $b^m \in I$, if $m$ is even, then $b^m = (-b)^m$. Thus $-b \in Rad(I)$. If not, there exists $-b^m \in I$ and $-b^m = (-b)^m$, therefore $-b \in Rad(I)$. Then consider as follow equation :

$$(a-b)^{n+m} = \binom{n+m}{0} a^0(-b)^{m+n} + \binom{n+m}{1} a^1(-b)^{m+n-1} + \cdots + a^{m+n}$$

Every terms of above equation are elements of $I$, Thus $(a-b) \in Rad(I)$, and hence $Rad(I)$ is a subgroup of $R$. And show that ideal property. Take $a \in Rad(I)$, $r \in R$, then there exists $a^n \in I$ and clearly $(a^n)(r^n) = (ar)^n \in I$. Therefore $Rad(I)$ is an ideal of $R$, and for all $a \in I$ is in $Rad(I)$ consider as $a^1$. As a result, $Rad(I)$ is an ideal of $R$ that contains $I$.

**Proposition 2.18**. *For all $X \subset \mathbb{A}^n(k)$ then $I(X)$ is a radical ideal.*

**Proof.** $I(X) \subset Rad(I(X))$ is clear. Show that $I(X) \supset Rad(I(X))$. Take $F \in Rad(I(X))$, then there exits $m$ such that $F^m \in I(X)$, and $F^m(P) = 0$ for all $P \in X$. Since $k$ has no zero divisors, hence $F(P) = 0$ and then $F \in I(X)$.

Let $X$, $Y$ be algebraic sets in $\mathbb{A}^n(k)$ and then $X = Y$ if and only if $I(X) = I(Y)$. Proof is simple, if $X = Y$ then $I(X) = I(Y)$ is clear. Now suppose that $I(X) = I(Y)$ then $X = V(I(X)) = V(I(Y)) = Y$ as required.

**Proposition 2.19**. *Let $I$ be a prime ideal of ring $R$, then $I$ is a radical ideal.*

**Proof.** Suppose that $I$ is a prime ideal of ring $R$, and $Rad(I)$ is radical of $I$. Since $I \subset Rad(I)$ is clear. Thus we must show that $I \supset Rad(I)$. For all $a \in Rad(I)$ then there exists $a^n \in I$. Since $I$ is a prime ideal, $a^n = aa^{n-1}$ if $a \in I$ then we are done. Thus we assume that $a^{n-1} \in I$, then $aa^{n-2} \in I$,etc. This process will surely end, and hence $a \in I$, and $I \supset Rad(I)$.

**Lemma 2.20.** *Any ideal $J$ of $k[X_1, ..., X_n]$, $V(J) = V(Rad(J))$ and $Rad(J) \subset I(V(J))$.*

**Proof.** Since $J \subset Rad(J)$, we have $V(J) \supset V(Rad(J))$. Take $p \in V(J)$, $F \in Rad(J)$, then there exists $F^m \in J$. Then $F^m(p) = 0$. Since $k$ has no zero divisors, then $F(p) = 0$. Therefore $p \in V(Rad(J))$. Take $p \in V(I)$, for all $F \in Rad(J)$, then there exists $F^m \in I$. Then $F^m(p) = 0$. Hence $F(p) = 0$, therefore $F \in I(V(J))$.

**Proposition 2.21**. *$I = (X_1 - a_1, ..., X_n - a_n)$ is an maximal ideal of $k[X_1, ..., X_n]$, and the natural homomorphism from $k$ to $k[X_1, ..., X_n]/I$ is an isomorphism.*

**Proof.** Suppose that $I \subsetneq J \subset k[X_1, ..., X_n]$. Take $F \in J - I$, then $F(a_1, ..., a_n) \neq 0$.

$$F = \sum_{(i)} \alpha_{(i)} (X_1 - a_1)^{i_1} (X_2 - a_2)^{i_2} \cdots (X_n - a_n)^{i_n}.$$

We can take $G \in I$ :

$$G = \sum_{(i)\neq(0,...,0)} \alpha_{(i)}(X_1 - a_1)^{i_1}(X_2 - a_2)^{i_2} \cdots (X_n - a_n)^{i_n}.$$

Then $F - G \in J$. Since every terms of $F$ and $G$ are same except the constant term, thus $F - G = \alpha_{(0,...,0)} \in J$. If $\alpha_{(0,...,0)} = 1$ then $J = k[X_1, ..., X_n]$. If not, we can take another polynomial $F' \in J - I$ and $G' \in I$ as follows:

$$F' = \sum_{(i)} \beta_{(i)}(X_1 - a_1)^{i_1}(X_2 - a_2)^{i_2} \cdots (X_n - a_n)^{i_n},$$
$$G' = \sum_{(i)\neq(0,...,0)} \beta_{(i)}(X_1 - a_1)^{i_1}(X_2 - a_2)^{i_2} \cdots (X_n - a_n)^{i_n},$$

where $\beta_{(0,...,0)} = \frac{1}{\alpha_{(0,...,0)}}$, since $k$ is a field. Then $F' - G' = 1/\alpha_{(0,...,0)} \in J$. Then clearly $(F - G)(F' - G') = \alpha_{(0,...,0)}\frac{1}{\alpha_{(0,...,0)}} = 1 \in J$. Therefore $J = k[X_1, ..., X_n]$, and hence $I = (X_1 - a_1, ..., X_n - a_n)$ is an maximal ideal of $k[X_1, ..., X_n]$. Let $\varphi$ be the nautral homomorphism from $k$ to $k[X_1, ..., X_n]/I$. Consider $0_k \longmapsto \varphi(0_k) = 0_k + I$, thus $0_k \in Ker(\varphi)$ and any other element of $k$ does not in $Ker(\varphi)$ by the natural condition, and hence $\varphi$ is injective. Suppose that for all $F \in k[X_1, ..., X_n]$ then $F$ has the form :

$$F = \sum_{(i)} \alpha_{(i)}(X_1 - a_1)^{i_1}(X_2 - a_2)^{i_2} \cdots (X_n - a_n)^{i_n}.$$

Then consider $F + I \in k[X_1, ..., X_n]/I$ with $I = (X_1 - a_1, ..., X_n - a_n)$. Since every terms of $F$ are factorized into $(X_1 - a_1)$, ..., $(X_n - a_n)$, they are all element of $I$. Therefore on $k[X_1, ..., X_n]/I$ they are zero, except constant term. Thus $F + I = \alpha_{(0,...,0)} + I \in k[X_1, ..., X_n]/I$ with $\alpha_{(0,...,0)} \in k$. Since $k[X_1, ..., X_n]/I$ is a field, for all $\bar{a} \in k[X_1, ..., X_n]/I$ then there exists $a \in k$ such that $\varphi(a) = \bar{a}$. Consequently, $\varphi$ is an isomorphism.

### 2.1.3 Hilbert's Basis Theorem

We know that every algebraic set is equal to for some intersection of hypersurface. But this time you'll see that a finite number of hypersurfaces is enough. This is the beginning, we have any hypersurface $V(S)$ with $S$ is a set of polynomials in $k[X_1, ..., X_n]$. Then there exists ideal $I \in k[X_1, ..., X_n]$ such that $V(I) = V(S)$. If $I$ is finitely generated by $g_1, ..., g_r \in k[X_1, ..., X_n]$ then clearly $V(S) = V(I) = V(g_1, ..., g_r) = V(g_1) \cap \cdots \cap V(g_r)$. Thus, if $k[X_1, ..., X_n]$ is a noetherian ring, our claim is over. This can be confirmed by Hilbert's basis theorem.

**The Hilbert Basis Theorem.** If $k$ is a noetherian ring, then $k[X_1, ..., X_n]$ is a noetherian ring.

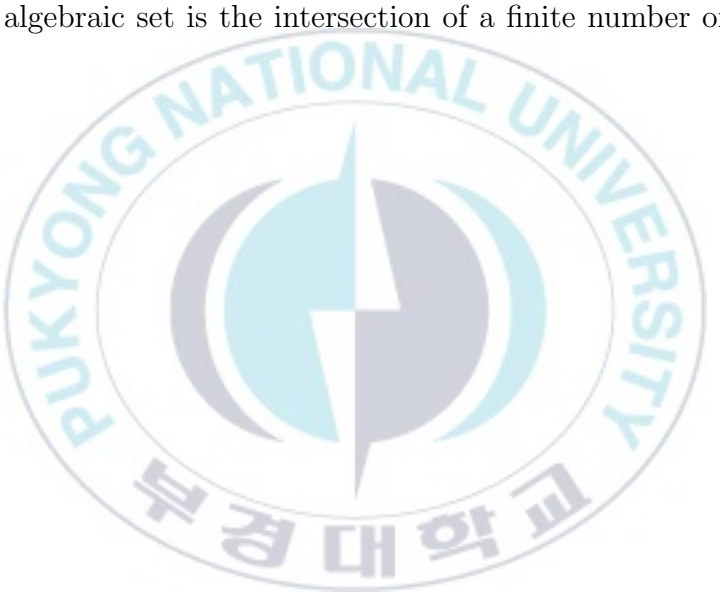
**Proof.** If we can prove that $k$ is a noetherian then $k[X]$ is a noeterian, since $k[X_1, ..., X_n] \cong k[X_1, ..., X_{n-1}][X_n]$ it is enough to show the theorem. Thus shows that $k$ is a noetherian then $k[X]$ is a noeterian. Let $I$ be an ideal of $k[X]$, our claim is for some ideal $I'$ of $k[x]$ is finitely generated and it is same as $I$. Consider ideal $J$ of $k$, defined by $J = \{lc(f) \mid \text{for all } f \in I\}$ by proposition1.1. Since $k$ is a noetherian ring, $J = (g_1, ..., g_r)$ with $g_i \in k$. Then there exist a polynomials $G_1, ..., G_r \in k[X]$ such that $lc(G_i) = g_i$. Take an integer $N > max(deg(G_1), ..., deg(G_r))$, for each $m \leq N$, $J_m = \{lc(f) \mid f \in k[X] \text{ and } deg(f) \leq m\}$ is an ideal of $k$ by Lemma1.2, and $J_m = (g_{m1}, ..., g_{ml})$ sinc $k$ is a noetherian. Then we can find polynomials $G_{m1}, ..., G_{ml} \in k[X]$ such that $lc(G_{mi}) = g_{mi}$. Suppose that $I'$ is generated by $G_1, ..., G_r$ and $G_{m1}, ..., G_{ml}$, and show that $I = I'$. Clearly, $I' \subset I$ since $I$ contains every generators of $I'$. Take a polynomial $H \in I - I'$ such that $deg(H) \leq deg(F)$ for all $F \in I - I'$. If $deg(H) > N$, then we can find polynomial $Q_i$ such that $\sum Q_i G_i$, $deg(\sum Q_i G_i) = deg(H)$ and $lc(\sum Q_i G_i) = lc(H)$. Consider the degree of $(H - \sum Q_i G_i)$, it is lower than $deg(H)$, thus $(H - \sum Q_i G_i) \in I'$ and $H \in I'$. Second, if $deg(H) \leq N$ then then we can find polynomial $Q_i$ such

that $\sum Q_i G_{mi}$, $deg(\sum Q_{mi} G_i) = deg(H)$ and $lc(\sum Q_{mi} G_i) = lc(H)$. According to the above method, $(H - \sum Q_i G_{mi}) \in I'$ and $H \in I'$. Therefore $H$ can not exist, and hence $I = I'$. As a result if $k$ is a noetherian ring, then $k[X_1, ..., X_n]$ is a noetherian ring.

**Corollary 2.22.** If $k$ is any field, then $k[X_1, ..., X_n]$ is a noetherian ring.

**Proof.** Every field is PID, therefore field $k$ is a noetherian ring. By the hilbert basis theorem, corollary is done.

Therefore every algebraic set is the intersection of a finite number of hypersurfaces.



## 2.2 Hilbert's Nullstellensatz

The aim of this section is to prove Hilbert's Nullstellensatz. We begin with the following basic concepts.

### 2.2.1 Module

**Definition 2.23.** Let $R$ be a ring. An *R-module* is a abelian group $(M, +)$ together with a scalar multiplication($R \times M \longrightarrow M$ defined by $(a, b) \longmapsto ab$) satisfying:

1. $(a + b)m = am + bm$ with $a$, $b \in R$, $m \in M$.
2. $a(m + n) = am + an$ with $a \in R$, $m$, $n \in M$.
3. $(ab)m = a(bm)$ with $a$, $b \in R$, $m \in M$.
4. $1_R m = m$ with $m \in M$, $1_R$ is the multiplicative identity of $R$.

A subgroup $S$ of an *R-module* $M$ is called a *submodule* if $sm \in S$, for all $s \in R$, for every $m \in S$, then $S$ is an $R - module$. Suppose that $G \subset$ *R-module* $M$, the submodule generated by $G$ is defined by $\{\sum r_i g_i \mid r_i \in R,\ s_i \in G\}$, then it is the smallest submodule of $M$ that contains $G$. The module $M$ is said to be finitely generated if $M = \sum Rg_i$ for some $g_1, ...g_n \in M$.

Let $S$ be a ring with subring $R$. We say that $S$ is module-finite over $R$ if $S$ is finitely generated as an *R-module*. We say that $S$ is ring-finite over $R$ if $S = R[v_1, ..., v_n] = \{\sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n}\}$ for some $v_1, ..., v_n \in S$, it is the smallest ring contains ring $R$ and $v_1, ..., v_n$. Note that module-finite implies ring-finite, but the converse is false. If $L$ is ring-finite over $K$, with $L$, $K$ fields, then $L$ is a finite extension of $K$.

**Proposition 2.24.** *Let $S$ be a ring with subring $R$. If $S$ is module-finite over $R$, then $S$ is ring-finite over $R$.*

**Proof.** The ring $S$ is module-finite over $R$, then write $S = \sum Rv_i$ for some $v_1, ..., v_n \in S$. And if $S$ is ring-finite, $S = \sum Rv_1^{i_1}v_2^{i_2}\cdots v_n^{i_n}$. Thus any element of ring-finite over $R$ is in the module-finite over $R$.

**Proposition 2.25.** *Let $K$, $L$ be a fields. If $L$ is ring-finite over $K$, then $L$ is a finitely generated field extension of $K$.*

**Proof.** $L$ is ring-finite over $K$, thus $L = K[v_1, ..., v_n]$ for some $v_1, ..., V_n \in L$, and clearly $L = K[v_1, ..., v_n] \subseteq K(v_1, ..., v_n)$. Since $K(v_1, ..., v_n)$ is the smallest field containing $v_1, ..., v_n$ we know that $L = K[v_1, ..., v_n] = K(v_1, ..., v_n)$ since $L$ is a field.

**Proposition 2.26.** *If $L = K(X)$ is a finitely generated field extension of $K$, but $L$ is not ring-finite over $K$.*

**Proof.** Suppose that $L = K[v_1, ..., v_n]$ for some $v_i \in L$, and $f(X) \in K[X] = L$ such that $f = b_1 \cdots b_n$ with $v_i = a_i/b_i$($a_i$, $b_i$ are relatively prime). Choose $g(X) \in K[X]$ such that $g \nmid f^m$ for all $m \in \mathbb{N}$. then there exists $\frac{1}{g} \in k[v_1, ..., v_n] = L$ :

$$\frac{1}{g} = \sum_{(i)} \alpha_{(i)} v_1^{i_1} \cdots v_r^{i_r}$$

Multiply by $f^N$ on both sides of the displayed equation for sufficiently large $N$ so that the denominators on the left hand side are all cleared if $N = \sum_{(i)}(i_1 + \cdots i_r)$ will do. Then $\frac{f^N}{g} \in K[X]$, a contradiction as $g$ does not divide $f^N \in K[X]$.

**Proposition 2.27.** *Let $R$ be a subring of $S$ and $S$ a subring of $T$.*

1. *If $S = \sum Rv_i$, $T = \sum Sw_j$ then $T = \sum Rv_iw_j$.*
2. *If $S = R[v_1, ..., v_n]$, $T = S[w_1, ..., w_m]$ then $T = R[v_1, ..., v_n, w_1, ..., w_m]$.*
3. *If $R$, $S$, $T$ are fields, and $S = R(v_1, ..., v_n)$, $T = S(w_1, ..., w_m)$ then $T = R(v_1, ..., v_n, w_1, ..., w_m)$.*

**Proof.** Prove the first condition, $T \supset \sum Rv_iw_j$ is clear. we must shows that $T \subset \sum Rv_iw_j$. Since $R$ is subring of $T$ and $v_i$, $w_j \in T$ for all $i$, $j$. Take for all $t \in T$, then $t = \sum_j \lambda_j w_j$ with $\lambda \in S$. Then $\lambda_j = \sum_i \xi_{ij} v_i$ for all $j$.

$$t = \sum_j \lambda_j w_j = \sum_j \sum_i \xi_{ij} v_i w_j = \sum_{i,j} \xi_{ij} v_i w_j \in \sum_{i,j} Rv_i w_j$$

Therefore $T = \sum Rv_iw_j$. Prove the second condition, $T \supset R[v_1, ..., v_n, w_1, ..., w_m]$ is clear. shows that $T \subset R[v_1, ..., v_n, w_1, ..., w_m]$. Take for all $t \in T$ then $t = \sum_{(i)} s_{(i)} w_1^{i_1} \cdots w_m^{i_m}$ with $s_{(i)} \in S$, and $s_{(i)} = \sum r_{(j)} v_1^{j_1} \cdots v_n^{j_n}$

$$\begin{aligned} t &= \sum_{(i)} s_{(i)} w_1^{i_1} \cdots w_m^{i_m} \\ &= \sum_{(i)} \sum_{(j)} r_{(j)} v_1^{j_1} \cdots v_n^{j_n} w_1^{i_1} \cdots w_m^{i_m} \\ &= \sum_{(i),(j)} r_{(j)} v_1^{j_1} \cdots v_n^{j_n} w_1^{i_1} \cdots w_m^{i_m} \end{aligned}$$

Therefore $t \in R[v_1, ..., v_n, w_1, ..., w_m]$, and hence $T = R[v_1, ..., v_n, w_1, ..., w_m]$. Prove the third condition, $S$ is the smallest field containing $R$ and $v_1, ...v_n$, and $T$ is the smallest field containing $S$ and $w_1, ...w_m$. Then

$$\begin{aligned} T &= S(w_1, ..., w_m) \\ &= R(v_1, ..., v_n)(w_1, ..., w_m) \\ &= R(v_1, ..., v_n, w_1, ..., w_m) \end{aligned}$$

Thus the three finiteness conditions impose a transitive relation.

### 2.2.2 Integral elements

Let $R$ be a subring of a ring $S$. We say that $v \in S$ is integral over $R$ if there is a monic polynomial $f = X^d + a_1 X^{d-1} + \cdots + a_d$ in $R[X]$ satisfy that $f(v) = 0$,and if $R$, $S$ are fields, we say that $v$ is algebraic over $R$.

**Proposition 2.28.** *If $R$ is a subring of domain $S$, and $v \in S$, then the following are equivalent:*

*(1) $v$ is integral over $R$.*

*(2) $R[v]$ is module-finite over $R$.*

*(3) There is a subring $R'$ of $S$ containing $R[v]$ that is module-finite over $R$.*

**Proof.** $1 \Rightarrow 2$ : Since $v$ is integral over $R$, there exists monic polynomial $F \in R[X]$ such that $F(v) = v^d + a_{d-1}v^{d-1} \cdots + a_0 = 0$, then $v^d \in \sum_{i=0}^{d-1} Rv^i$. It means $v^n \in \sum_{i=0}^{d-1} Rv^i$ for all $n$, since $v \in R$. thus $R[v] = \sum_{i=0}^{d-1} Rv^i$.

$2 \Rightarrow 3$ : we just take $R' = R[v]$, then we are done.

$3 \Rightarrow 1$ : If $R' = \sum_{i=1}^{n} Rw_i$, then $vw_i = \sum_{j=1}^{n} a_{ij}w_j$ for some $a_{ij} \in R$. Then $\sum_{j=1}^{n}(\xi_{ij}v - a_{ij})w_j = 0$ for all i, where $\xi_{ij} = 0$ if $i \neq j$ and $\xi_{ij} = 1$. If we consider these equations in the quotient field of $S$, we see that $(w_1, ..., w_n)$ is a nontrivial solution, thus $det(\xi_{ij}v - a_{ij}) = 0$. Since $v$ appears only in the diagonal of the matrix, this determinant has the form $v^n + a_{n-1}v^{n-1} + \cdots + a_0$, $a_i \in R$. Therefore $v$ is integral over $R$.

**Corollary 2.29.** The set of elements of $S$ that are integral over $R$ is a subring of $S$ containing $R$.

**Proof.** If $a$, $b$ are integral over $R$, then $b$ is integral over $R[a] \supset R$, thus $R[a, b]$ is module-finite over $R$. And $a \pm b$, $ab \in R[a, b]$, therefore they are integral over $R$.

If every element of $S$ is integral over $R$, then $S$ is said to be integral over $R$. And if $S$, $R$ are a fields, $S$ is algebraic over $R$.

**Proposition 2.30.** *Let $L$ be ring-finite over $K$. Then $L$ is module-finite over $K$ if and only if $L$ is integral over $K$.*

**Proof.** ($\Rightarrow$) Suppose that $L = \sum Kv_i$ with $v_1, ..., v_n \in L$. Since $L$ is module-finite over $K$ and $K[v_i] \subset L$, thus $v_i$ is integral over $K$ by Proposition 3 to 1. By the corollary 5, $K \subset S = \{a \in L \mid a \text{ is integral over } K\} \subset L$. Since $S$ is subring of

$L$ and containing $v_1, ..., v_n$ and $K$, and for all $z \in L$ has the form : $z = \sum k_i v_i$. Thus every terms of $z$ is in $S$. therefore $S = L$. ($\Leftarrow$) Suppose that $L$ is integral over $K$. By the Proposition (1) to (3), clearly $L$ is module-finite over $K$.

**Proposition 2.31.** *Let $L$, $K$ be fields such that $K \subset L$ and $K$ is an algebraically closed.* (1) *Then the set $S = \{v \in L \mid v$ is algebraic over $K\} \subset K$.* (2) *And $K$ has no module-finite field extensions except itself.*

**Proof.** (1) : Let $v \in L$ be algebraic over $K$. Sice $K$ is algebraically closed, therefore every root of any polynomial $F \in K[X]$ is already in $K$. (2) Suppose that $L$ is module-finite over $K$. then we know that $L$ is algebraic over $K$. By (1) $L = K$.

**Proposition 2.32.** *Let $R$ be a subring of $S$ and $S$ is a subring $T$. If $S$ is integral over $R$, and $T$ is integral over $S$. Then $T$ is integral over $R$.*

**Proof.** Suppose that $z \in T$, $R' = R[a_1, ..., a_n]$ and $R'' = R[a_1, ..., a_n, z]$ where the $a_i \in S$ are the coefficients of a monic polynomial which vanish on $z$. Using part (2) of proposition 21 repeatedly we see that $R'$ is moudle finite over $R$. The ring $R''$ is module finite over $R'$ sice $R'' = \sum_{i=0}^{n-1} R' z^i$. By transitivity $R''$ is module finite over $R$. Since $R''$ is a subset of $T$ containing $R[z]$ that is module-finite over $R$, we can use part (3) of proposition 21 to conclude $z$ is integral over $R$.

**Proposition 2.33.** *Let $K$ be a field, $L = K(X)$ the field of rational functions in one variable over $K$. Then* (1) *$z \in L$ such that $z$ is integral over $K[X]$ is already in $K[X]$, and* (2) *there is no non-zero element $F \in K[X]$ such that for all $z \in L$, $F^n z$ is integral over $K[X]$ for some $n > 0$.*

**Proof.** proof (1), Suppose that $z \in L$ be integral over $K[X]$. Then there exists monic polynomial $H$ such that $H(z) = 0$, write $H(z) = z^n + a_1 z^{n-1} + \cdots = 0$. Since $z$ is an element of the field of rational functions $L = K(X)$, thus $z = F/G$

with $F$, $G \in K[X]$ are relatively prime. Then

$$\begin{aligned} G^n H(z) &= G^n(z^n + a_1 z^{n-1} + \cdots) = 0, \\ G^n H(F/G) &= G^n((F/G)^n + a_1(F/G)^{n-1} + \cdots) = 0 \\ &= F^n + a_1 G F^{n-1} + \cdots = 0. \end{aligned}$$

Since $G$ divides $F^n$, therefore $G$ must divides $F$. But this is contradiction to $G$ and $F$ are relatively prime. Thus $z \in L$ is integral over $K[X]$, then $z \in K[X]$.
proof (2) Choose $C(X) \in K[X]$ such that $C$ does not divide any power of $F$. Then setting $z = 1/C$ we can conclude that $F^n/C$ is integral over $K[X]$, then there exists some $a_i \in K[X]$ such that

$$\left(\frac{F^n}{C}\right)^d + \sum_{i=0}^{d-1} a_i \left(\frac{F^n}{C}\right)^i = 0.$$

Clearing denominators gives

$$F^{nd} = \sum_{i=0}^{d-1} a_i C^{d-i} F^{ni}$$

and since $C$ divides every term in the right hand side it must divide $F^{nd}$, a contradiction.

Zariski lemma can be proved by combining the results so far.

**Proposition 2.34.** *If a field $L$ is ring-finite over a subfield $K$, then $L$ is module-finite over $K$.*

**Proof.** Suppose that $L = K[v_1, ..., v_n]$. We use induction on $n$. The case $n = 1$, $L = K(v_1)$, consider the homomorphism $\xi : K[X_1] \to L = k(v_1)$ defined by $X_1$ to $v_1$. Then by the first isomorphism theorem, $Im(\xi) = K[v_1] \cong K[X_1]/Ker(\xi)$. Since $K[X_1]$ is PID, we can write $Ker(\xi) = (F)$ for some $F \in K[X_1]$ and $K[v_1]$ is a domain, hence $(F)$ is a prime ideal. By the property of $PID$, $(F)$ is maximal in $K[X_1]$. Thus $K[X_1]/(F)$ is a field, and hence $K[v_1] = K(v_1)$. And $F(v_1) = 0$,

thus $v_1$ is algebraic over $K$ and $L = K[v_1]$ is module-finite over $K$ by Proposition 21, 1 to 2. Assume that the claim is true for $n-1$. Then $L = K_n[v_1, ..., v_{n-1}]$ is moudle-finite over $K_n$ with $K_n = K(v_n)$. If $v_n$ is algebraic over $K$ then we are done by Proposition 20-1. Hence suppose that $v_n$ is not algebraic over $K$. Then each $v_i$ satisfies an equation $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots = 0$ where $a_{ij} \in K_n$. Then we take $\beta \in K[v_n]$ that is a multiple of all the denominators of the $a_{ij}$. Multiply both sides of the above equation by $\beta^{n_i}$ : $(\beta v_i)^{n_i} + a_{i1}\beta(\beta v_i)^{n_i-1} + \cdots = 0$, it means $\beta v_i$ is algebraic over $K[v_n]$. Consider subring $S = \{a \in L \mid a \text{ is integral over } K\}$, by corollary $K \subset K[V_n] \subset S \subset L$. Therefore for all $z \in L = K[X_1, ..., X_n]$, there is an $N$ such that $\beta^N z$ is integral over $K[V_n]$ ($\beta v_i$, $v_n \in S$). In particular this must hold for $z \in K(v_n) \subset L$. Since $K(v_n)$ is isomorphic to the field of rational function $K(X)$, this is contradiction by Proposition 25-(2).

### 2.2.3 Hilbert's Nullstellensatz

**Weak Hilbert's Nullstellensatz.** If $K$ is algebraically cloed and $I$ is a proper ideal in $K[X_1, ..., X_n]$, then $V(I) \neq \varnothing$.

**Proof.** We may assume that $I$ is a maximal ideal of $K[X_1, ..., X_n]$, because any proper ideal contained for some maximal ideal. Suppose that $L = K[X_1, ..., X_n]/I$ is a field. Then $L$ is ring-finite over $K$ and since $K$ is algebraically closed, $L = K$ by the above propositions. Then each $i$ there is an $v_i \in K$ that the $I$-residue of $X_i$ is $v_i$ or $X_i - v_i \in I$ for some $v_i \in L$. But we know that $(X_1 - v_1, ..., X_n - v_n)$ is maximal ideal, therefore $V(I) = (v_1, ..., v_n) \neq \varnothing$.

**Hilbert's Nullstellensatz.** If $k$ is algebraically cloed and $I$ is an ideal of $k[X_1, ..., X_n]$, then $I(V(I)) = Rad(I)$.

**Proof.** Take $p \in V(I)$, for all $F \in Rad(J)$, then there exists $F^m \in I$. Then $F^m(p) = 0$, thus $F(p) = 0$ and $F \in I(V(J))$. Thus $I(V(I)) \supset Rad(I)$. Let's show

the opposite direction. Suppose that $I = (F_1, ..., F_r)$ with $F_i \in K[X_1, ..., X_n]$ and take $G \in I(V(I))$, then $G = A_1F_1 + \cdots + A_nF_n$ for some $A_i \in K[X_1, ..., X_n]$. Consider ideal $J = (F_1, ..., F_n, X_{n+1}G - 1)$ in $K[X_1, ..., X_{n+1}]$. Since $F_i$ and $X_{n+1}G - 1$ has no common zeros, $V(J) = \varnothing$. By the Weak Nullstellensatz, $J$ is whole ring $K[X_1, ..., X_{n+1}]$. It implies $1 \in J$, therefore we have an equation :

$$1 = \sum B_i(X_1, ..., X_{n+1})F_i + C(X_1, ..., X_{n+1})(X_{n+1}G - 1),$$

where $B_i, C \in K[X_1, ..., X_{n+1}]$. Let setting $Y = \frac{1}{X_{n+1}}$. Then multiply the equation by a high power of $Y$ :

$$Y^N = \sum D_i(X_1, ..., X_n, Y)F_i + E(X_1, ..., X_n, Y)(G - Y).$$

Substituting $G$ for $Y$ then

$$\begin{aligned} G^N &= \sum D_i(X_1, ..., X_n, G)F_i \\ &= \sum H_i(X_1, ..., X_n)F_i \end{aligned}$$

Thus $G^N \in I \Rightarrow G \in Rad(I)$. Therefore $I(V(I)) \subset Rad(I)$.

**Corollary 2.35.** Let $I$ be a radical ideal of $k[X_1, ..., X_n]$, then $I(V(I)) = I$.

Therefore $\{radical\ ideal\} \overset{1-1}{\longleftrightarrow} \{algebraic\ set\}$.

**Corollary 2.36.** Let $I$ be a prime ideal of $k[X_1, ..., X_n]$, then $V(I)$ is irreducible.

Thus $\{prime\ ideal\} \overset{1-1}{\longleftrightarrow} \{irreducible\ algebraic\ set\}$, and the maximal ideals correspond to points.

# Chapter 3

# Projective algebraic set

Let $k$ be algebraically closed field. We denote $\mathbb{P}^n$ the quotient of $k^{n+1} - \{0\}$ by the operation of the group $k^* : \mathbb{P}^n := (k^{n+1} - \{0\})/\sim$, where $\sim$ is the equivalence relation defined by: $(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n)$ if there is a non-zero element $\lambda$ in $k$ such that $(x_0, \cdots, x_n) = (\lambda y_0, \cdots, \lambda y_n)$. $\mathbb{P}^n$ is roughly the set of the lines in $k^{n+1}$ passing through the origin.

If we want to refer to the projective space of one -dimensional subspaces of a vector space $V$ over the field $k$ without specifying an isomorphism of $V$ with $K^{n+1}$, denote it by $\mathbb{P}(V)$ or simply $\mathbb{P}V$.

Let's look at the point of $\mathbb{P}^n$ now. It is usually written as a homogeneous vector $[Z_0, ..., Z_n]$, by which we mean the line generated by $(Z_0, ..., Z_n) \in k^{n+1}$. Let $v$ be any non-zero vector in $V$, then $\alpha v \in V$ for all scalar multiplication $\alpha$ is a same point in $\mathbb{P}V \cong \mathbb{P}^n$.

An affine variety $X \subset \mathbb{A}^n$ is defined by the common zero locus of a collection of polynomials in $k[X_1, ..., X_n]$. However, a projective variety is not defined as the common zero locus of a collection of polynomials but is defined as the common zero locus of a collection of homogeneous polynomials.

Let $U_i \subset \mathbb{P}^n$ be the subset of points $[Z_0, ..., Z_n]$ with $Z_i \neq 0$. Then on $U_i$ the ratios $z_j = Z_j/Z_i$ are well-defined and give a bijection $U_i \cong \mathbb{A}^n$. If $X$ is variety of $\mathbb{P}^n$, then the intersection $X_i = X \cap U_i$ is an affine variety. The following two definitions will clarify our thinking.

**Definition 3.1**. Let K be a domain. Take any polynomial $f \in K[X_1, ..., X_n]$ of

degree $d$, then we can write $f$ as follow:

$$f = f_0 + f_1 + \cdots + f_d,$$

where $f_i$ is a form of degree $i$, and let's define $f^*$ :

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + X_{n+1} f_{d-1} + f_d = X_{n+1}^d f\left(\frac{X_1}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}}\right).$$

Then $f^* \in K[X_1, ..., X_{n+1}]$ is a form of degree $d$.
We call this process *Homogenization*.

**Definition 3.2**. Let K be a domain. Take any form $F \in K[X_1, ..., X_{n+1}]$, let's define $F_*$ :

$$F_* = F(X_1, ..., X_n, 1)$$

Then $F_* \in K[X_1, ..., X_n]$. We call this process *Dehomogenization*.

The purpose of the dehomogenization is to eliminate some $X_i$. Therefore, 1 may be substituted anywhere. Consider the homogeneous polynomial $F \in k[X_1, ..., X_{n+1}]$ with $deg(F) = d$. Then we can dehomogenization against $X_i$ of $F$ :

$$\begin{aligned} X_1 &\Rightarrow F(1, X_2, ..., X_{n+1}), \\ X_2 &\Rightarrow F(X_1, 1, X_3, ..., X_{n+1}), \\ &\vdots \\ X_n &\Rightarrow F(X_1, X_2, ..., X_{n-1}, 1, X_{n+1}), \\ X_{n+1} &\Rightarrow F(X_1, X_2, ..., X_n, 1). \end{aligned}$$

Thus projective space is the union of affine spaces, and every projective variety is the union of affine varieties. In particular, a subset $X$ in $\mathbb{P}^n$ is a projective variety if and only if $X_i = X \cap U_i$ are all affine varieties, following propositions are propoerties of homogenization and dehomogenization.

**Proposition 3.3**. $(FG)_* = F_*G_*$ *and* $(fg)^* = f^*g^*$.

**Proof.** Suppose that $F$, $G \in K[X_1, ..., X_{n+1}]$ are a forms, then clearly $FG$ is a form. Consider $(FG)_*$ :

$$\begin{aligned}(FG)_* &= (FG)(X_1, ..., X_n, 1) \\ &= F(X_1, ..., X_n, 1)G(X_1, ..., X_n, 1) \\ &= F_*G_*.\end{aligned}$$

Therefore $(FG)_* = F_*G_*$.

Assume that $f, g \in K[X_1, ..., X_n]$ with $deg(f) = d_1$, and $deg(g) = d_2$. Then $fg$ is a polynomial of $K[X_1, ..., X_n]$ with degree $d_1 + d_2$. Consider the following :

$$\begin{aligned}(fg)^* &= X_{n+1}^{d_1+d_2}(fg)\left(\frac{X_1}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}}\right) \\ &= X_{n+1}^{d_1+d_2} f\left(\frac{X_1}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}}\right) g\left(\frac{X_1}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}}\right) \\ &= X_{n+1}^{d_1} f\left(\frac{X_1}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}}\right) X_{n+1}^{d_2} g\left(\frac{X_1}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}}\right) \\ &= f^*g^*\end{aligned}$$

**Proposition 3.4**. $(f^*)_* = f$ *and* $X_{n+1}^h(F_*)^* = F$ *where* $F \neq 0$, *and* $h$ *is the highest power that satisfy following* $X_{n+1}^h \mid F$.

**Proof.** Assume that $f$ is any polynomial of $K[X_1, ..., X_n]$, and $deg(f) = d$. Then

$$f* = X_{n+1}^d f\left(\frac{X_1}{X_{n+1}}, ..., \frac{X_n}{X_{n+1}}\right)$$

And consider $(f_*)^*$ :

$$\begin{aligned}(f_*)^* &= (f_*)(X_1, ..., X_n, 1) \\ &= f\left(\frac{X_1}{1}, ..., \frac{X_n}{1}\right) = f\end{aligned}$$

Suppose that $F \in K[X_1, ..., X_{n+1}]$ a form of degree $d$ and $r$ is the highest power of $X^{n+1}$ that divides $F$ :

$$\begin{aligned} F &= \sum a_{(i_1,i_2,...,i_{n+1})} X_1^{i_1} \cdots X_{n+1}^{i_{n+1}} \\ &= X_{n+1}^r \sum a_{(i_1,i_2,...,i_{n+1})} X_1^{i_1} \cdots X_{n+1}^{i_{n+1}-r}, \end{aligned}$$

where $i_1 + i_2 + \cdots + i_{n+1} = d$. Then $F_*$ is a polynomial of $K[X_1, ..., X_n]$, and it has a form as follow:

$$F_* = \sum a_{(i_1,i_2,...,i_n)} X_1^{i_1} \cdots X_n^{i_n},$$

where $a_{(i_1,i_2,...,i_n)} \in K$, and degree of $F_*$ is $d - r$. Now Consider $(F_*)^*$,

$$(F_*)^* = X_{n+1}^{d-r} \sum a_{(i_1,i_2,...,i_n)} \left(\frac{X_n}{X_{n+1}}\right)^{i_1} \cdots \left(\frac{X_n}{X_{n+1}}\right)^{i_n}.$$

Finally, let's look at the following :

$$\begin{aligned} X_{n+1}^r (F_*)^* &= X_{n+1}^r X_{n+1}^{d-r} \sum a_{(i_1,i_2,...,i_n)} \left(\frac{X_n}{X_{n+1}}\right)^{i_1} \cdots \left(\frac{X_n}{X_{n+1}}\right)^{i_n} \\ &= X_{n+1}^d \sum a_{(i_1,i_2,...,i_n)} \left(\frac{X_n}{X_{n+1}}\right)^{i_1} \cdots \left(\frac{X_n}{X_{n+1}}\right)^{i_n}. \end{aligned}$$

Since $i_1 + i_2 + \cdots + i_n = d - i_{n+1}$

$$\begin{aligned} X_{n+1}^r (F_*)^* &= X_{n+1}^d \sum a_{(i_1,i_2,...,i_n)} \frac{(X_1^{i_1} \cdots X_n^{i_n})}{X_{n+1}^{d-i_{n+1}}} \\ &= \sum a_{(i_1,i_2,...,i_n)} X_1^{i_1} \cdots X_{n+1}^{i_{n+1}} \\ &= F. \end{aligned}$$

**Proposition 3.5**. $(F + G)_* = F_* + G_*$.

**Proof.** Suppose that $F$ and $G \in K[X_1, ..., X_{n+1}]$ are forms. Then

$$\begin{aligned}(F+G)_* &= (F+G)(X_1, ..., X_n, 1) \\ &= F(X_1, ..., X_n, 1) + G(X_1, ..., X_n, 1) \\ &= F_* + G_*.\end{aligned}$$

**Proposition 3.6**. *$X_{n+1}^t(f+g)^* = X_{n+1}^r f^* + X_{n+1}^s g^*$, where $r = deg(g)$, $s = deg(f)$, and $t = r + s - deg(f+g)$.*

**Proof.** Assume that $f, g \in K[X_1, ..., X_n]$ are polynomials of degree $s$, $r$ respectively. Then $(f+g)^* =$

$$X_{n+1}^{deg(f+g)} f_0 + \cdots + X_{n+1}^{deg(f+g)-s} f_s + X_{n+1}^{deg(f+g)} g_0 + \cdots + X_{n+1}^{deg(f+g)-r} g_r.$$

Consider $X_{n+1}^t(f+g)^* = X_{n+1}^{r+s-deg(f+g)}(f+g)^*$

$$\begin{aligned}&= X_{n+1}^{r+s} f_0 + X_{n+1}^{r+s-1} f_1 + \cdots + X_{n+1}^r f_s + X_{n+1}^{r+s} g_0 + \cdots + X_{n+1}^s g_r \\ &= X_{n+1}^r (X_{n+1}^s f_0 + X_{n+1}^{s-1} f_1 + \cdots + f_s) + X_{n+1}^s (X_{n+1}^r g_0 + \cdots + g_r) \\ &= X_{n+1}^r f^* + X_{n+1}^s g^*.\end{aligned}$$

**Corollary 3.7**. Up to powers of $X_{n+1}$, factoring a form $F \in K[X_1, ..., X_{n+1}]$ is the same as factoring $F_* \in K[X_1, ..., X_n]$. In particular, if $F \in K[X, Y]$ is a form, $K$ algebraically closed, then $F$ factors into a product of linear factors.

**Proof.** First claim, Suppose that any form $F \in K[X_1, ..., X_{n+1}]$. If $F = F_1 \cdots F_l$ and $F = X_{n+1}^r G$ where $r$ is the highest power that divides $F$. Then

$$\begin{aligned}F &= X_{n+1}^r (F_*)^* \\ &= X_{n+1}^r \{(F_1 \cdots F_l)_*\}^* \\ &= X_{n+1}^r \{(F_1)_* \cdots (F_l)_*\}^* \\ &= X_{n+1}^r \{(F_1)_* \cdots (F_l)_*\}^* \\ &= X_{n+1}^r \{(F_1)_*\}^* \cdots \{(F_l)_*\}^*.\end{aligned}$$

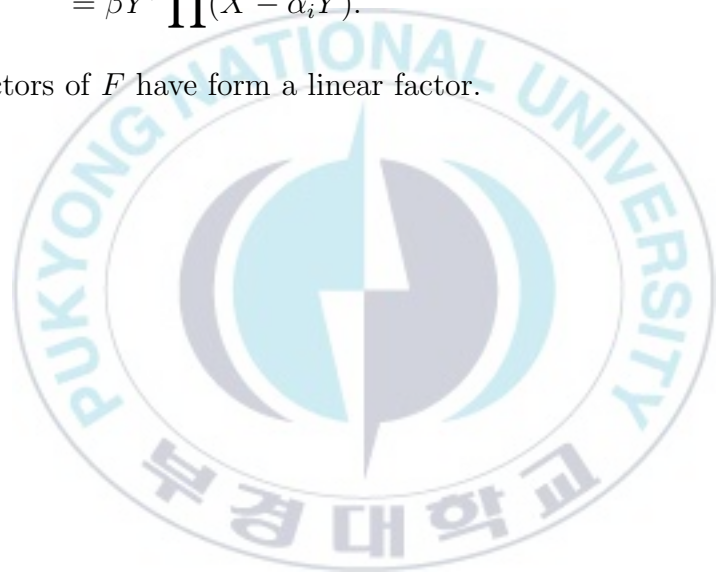
Second claim, Assume that $F \in K[X,Y]$ and $K$ algebraically closed. Then $F = Y^t H$, where $Y \nmid H$. Therefore, $F_* = H_*$ and since $K$ is algebraiclly closed,

$$F_* = H_* = \beta \prod (X - \alpha_i).$$

Consider $F = Y^r (F_*)^*$

$$\begin{aligned} F = Y^r (F_*)^* &= \beta Y^r \left\{ \prod (X - \alpha_i) \right\}^* \\ &= \beta Y^r \prod (X - \alpha_i Y). \end{aligned}$$

Therefore every factors of $F$ have form a linear factor.



# Chapter 4

# Defining equations of rational curves on S(1,2)

In this chapter, we completely determine the minimal generators of rational curves on a rational normal surface scroll S(1,2) in $\mathbb{P}^4$

**Definition 4.1**. The rational normal curve $C \subset \mathbb{P}^d$ is defined to be the image of the map $v_d : \mathbb{P}^1 \longrightarrow \mathbb{P}^d$ given by $v_d : [X_0 : X_1] \longmapsto [X_0^d, X_0^{d-1}X_1, \ldots X_1^d]$. It is well-known that the rational normal curve $C$ is defined by $(2 \times 2) - minors$ of the matrix as follow :

$$\begin{bmatrix} X_0 & X_1 & X_2 & \cdots & X_d - 1 \\ X_1 & X_2 & X_3 & \cdots & X_d \end{bmatrix}$$

If $Q_{ij} = X_iX_{j+1} - X_{i+1}X_j$ with $i \neq j$ and $0 \leq i,\ j \leq d$ ($i, j$ are the column numbers of the matrix). Then $C$ is generated by the set $S = \{Q_{ij} \mid 0 \leq i,\ j \leq d$ and $i \neq j\}$.

Let define $C_d \subset \mathbb{P}^4$, is the rational curve as follow :

$$C_d = \{[s^d(P) : s^{d-1}t(P) : s^2t^{d-2}(P) : st^{d-1}(P) : t^d(P)] \mid P \in \mathbb{P}^1\}.$$

In this chapter, $C_d$ always means the above the rational curve.

If $\mathbb{P}^a \cap \mathbb{P}^b = \varnothing$ then $\nu_a : \mathbb{P}^1 \hookrightarrow \mathbb{P}^a$ by setting $[s, t] \longmapsto [s^a : s^{a-1}t : \cdots : t^a]$. $\nu_b : \mathbb{P}^1 \hookrightarrow \mathbb{P}^b$ by setting $[s, t] \longmapsto [s^b : s^{b-1}t : \cdots : t^b]$. We know that $\nu_b(\mathbb{P}^1), \nu_a(\mathbb{P}^1)$ are normal rational curves in $\mathbb{P}^{a+b+1}$ and $\mathbb{P}^1 \cong \nu_b(\mathbb{P}^1) \cong \nu_a(\mathbb{P}^1)$.

**Definition 4.2**. $S(a, b) = \cup\overline{\nu_a(p)\nu_b(p)}, p \in \mathbb{P}^1$. We call S(a,b) is rational normal scroll S(a,b).

**Definition 4.3**. Rational normal surface scroll (1,2) It is well-known that the rational normal surface scrolls $S(1,2) \subset \mathbb{P}^4$ is defined by $(2 \times 2) - minors$ of the matrix

$$\begin{bmatrix} X_0 & X_2 & X_3 \\ X_1 & X_3 & X_4 \end{bmatrix}$$

Thsu $S(1,2)$ is generated by $X_0X_3 - X_1X_2$, $X_0X_4 - X_1X_3$, $X_2X_4 - X_3^2$.

**Lemma 4.4**. *$C_d$ is smooth and of degree $d$.*

**Proof**. The case where $d = 4$, then $C_d$ is rational normal curve. Suppose that $d > 4$, then we can see that the parametrization comes from the embedding $\nu_d : \mathbb{P}^1 \to \mathbb{P}^d$ by

$$P \hookrightarrow [s^d(P) : s^{d-1}t(P) : \cdots : st^{d-1}(P) : t^d(P)] \text{ for } P \in \mathbb{P}^1$$

of a projective line $\mathbb{P}^1$. More precisely, we denote $\widetilde{C}_d$ the image of $\mathbb{P}^1$ by the map $\nu_d$ and let $\mathbb{L}$ be a $(d-3)$-dimensional linear subspace of $\mathbb{P}^d$ spanned by $(d-4)$ standard coordinate points

$$\{[0,0,1,0,\ldots,0,0],[0,0,0,1,0,\ldots,0,0],\ldots,[0,0,\cdots,0,1,0,0,0]\}.$$

Then $C_d$ is obtained by the linear projection map $\pi_{\mathbb{L}} : \widetilde{C}_d \to \mathbb{P}^4$ of $\widetilde{C}_d$ from $\mathbb{L}$. Since $\mathbb{L} \subset \mathbb{P}^r \setminus C_d^2$, the map $\pi_{\mathbb{L}}$ is an isomorphism. Thus $C_d$ is a smooth rational curve of degree $d$.

**Proposition 4.5**. *The curve $C_d$ is contained in the rational normal surface scroll $S(1,2)$.*

**Proof.** If we want to prove $C_d \subset S(1,2)$, it is enough to see $I_{C_d} \supset I_{S(1,2)}$. It means $F(p) = 0$ with for every $p \in C_d$ and for all $F \in I_{s(1,2)}$. Since $S(1,2)$ is generated by $Q_1 = X_0X_3 - X_1X_2$, $Q_2 = X_0X_4 - X_1X_3$ ,$Q_3 = X_2X_4 - X_3^2$, we just show that $Q_1$, $Q_2$, $Q_3$ vanishes on for all $p = [s^d, s^{d-1}t, s^{d-2}t^2, st^{d-1}, t^d] \in C_d$. On $Q_1$ for example

$$Q_1(p) = s^d st^{d-1} - s^{d-1}ts^2t^{d-2} = s^{d+1}t^{d-1} - s^{d+1}t^{d-1} = 0.$$

In the same way, $Q_2(p)$, $Q_3(p)$ are zero. Thus $C_d \subset S(1,2)$.

**Example 4.6**. For $d = 5,6,7,8,9,10$, let $C_d \subset \mathbb{P}^4$ be curves defined as the parametrization : $C_d = \{[s^d(P) : s^{d-1}t(P) : s^2t^{d-2}(P) : st^{d-1}(P) : t^d(P)] \mid P \in \mathbb{P}^1\}$. We looked up the set $M_d$ of generators of $C_d$ through the Computer Algebra System Singulatr[4] as follows :

$$Q_1 = X_2X_4 - X_3^2, \quad Q_2 = X_0X_4 - X_1X_3, \quad Q_3 = X_0X_3 - X_1X_2;$$

and $Q_1, Q_2, Q_3$ are fixed.

$$\begin{aligned}
M_5 &= \{Q_1, Q_2, Q_3, X_1X_4 - X_2^2, X_0^2X_2 - X_1^3\} \\
M_6 &= \{Q_1, Q_2, Q_3, X_1X_4^2 - X_2^2X_3, X_1X_3X_4 - X_2^3, X_0X_2^2 - X_1^2X_4, X_0^3X_2 - X_1^4\} \\
M_7 &= \{Q_1, Q_2, Q_3, X_1X_4^2 - X_2^3, X_0^2X_2^2 - X_1^3X_4, X_0^4X_2 - X_1^5\} \\
M_8 &= \{Q_1, Q_2, Q_3, X_1X_4^3 - X_2^3X_3, X_1X_3X_4^2 - X_2^4, X_0X_2^3 - X_1^2X_4^2, X_0^3X_2^2 - X_1^4X_4, \\
&\qquad X_0^5X_2 - X_1^6\} \\
M_9 &= \{Q_1, Q_2, Q_3, X_1X_4^3 - X_2^4, X_0^2X_2^3 - X_1^3X_4^2, X_0^4X_2^2 - X_1^5X_4, X_0^6X_2 - X_1^7\} \\
M_{10} &= \{Q_1, Q_2, Q_3, X_1X_4^4 - X_2^4X_3, X_1X_3X_4^3 - X_2^5, X_0X_2^4 - X_1^2X_4^3, X_0^3X_2^3 - X_1^4X_4^2, \\
&\qquad X_0^5X_2^2 - X_1^6X_4, X_0^7X_2 - X_1^8\}
\end{aligned}$$

Consider the case of when $d$ is odd or even numbers.
Case1. $d = 2n + 1$ with $n \geq 2$.

$$\begin{aligned}
M_5 &= \{Q_1, Q_2, Q_3, X_1X_4 - X_2^2, X_0^2X_2 - X_1^3\} \\
M_7 &= \{Q_1, Q_2, Q_3, X_1X_4^2 - X_2^3, X_0^2X_2^2 - X_1^3X_4, X_0^4X_2 - X_1^5\} \\
M_9 &= \{Q_1, Q_2, Q_3, X_1X_4^3 - X_2^4, X_0^2X_2^3 - X_1^3X_4^2, X_0^4X_2^2 - X_1^5X_4, X_0^6X_2 - X_1^7\}.
\end{aligned}$$

Case2. $d = 2n$ with $n > 2$.

$$M_6 = \{Q_1, Q_2, Q_3, X_1X_4^2 - X_2^2X_3, X_1X_3X_4 - X_2^3, X_0X_2^2 - X_1^2X_4, X_0^3X_2 - X_1^4\}$$
$$M_8 = \{Q_1, Q_2, Q_3, X_1X_4^3 - X_2^3X_3, X_1X_3X_4^2 - X_2^4, X_0X_2^3 - X_1^2X_4^2, X_0^3X_2^2 - X_1^4X_4,$$
$$X_0^5X_2 - X_1^6\}$$
$$M_{10} = \{Q_1, Q_2, Q_3, X_1X_4^4 - X_2^4X_3, X_1X_3X_4^3 - X_2^5, X_0X_2^4 - X_1^2X_4^3, X_0^3X_2^3 - X_1^4X_4^2,$$
$$X_0^5X_2^2 - X_1^6X_4, X_0^7X_2 - X_1^8\}.$$

We have found the following pattern in the above equations of each case:

$$Q_1 = X_2X_4 - X_3^2, \quad Q_2 = X_0X_4 - X_1X_3, \quad Q_3 = X_0X_3 - X_1X_2$$

In all cases, $Q_1$, $Q_2$, and $Q_3$ are fixed.

Case1. $d = 2n$ with $n \geq 2$, then

$$M_d = \{Q_1, Q_2, Q_3, F_{[n,n]}, F_{[n+1,n-1]}, \cdots, F_{[2n-2,2]}, F_{[2n-1,1]}\}$$

where $F_{[2n-i,i]} = X_0^{2n-2i}X_2^i - X_1^{2n-2i+1}X_4^{i-1}$ for $1 \leq i \leq n$.

Case2. $d = 2n$ with $n > 2$, then

$$M_d = \{Q_1, Q_2, Q_3, G_{[n,0]}, G_{[n,1]}, F_{[n,1]}, F_{[n+1,2]}, \cdots, F_{[n+j-1,j]}\}$$

where

$$G_{[n,i]} = X_1X_3^iX_4^{n-i-1} - X_2^{n+i-1}X_3^{1-i} \text{ with } j = 0, 1.$$

and

$$F_{[n+j-1,j]} = X_0^{2j-1}X_2^{n-j} - X_1^{2j}X_4^{n-j-1} \text{ for } 1 \leq j \leq n-1.$$

These examples and the observations about the pattern of the minimal generators of defining ideals $I_{C_d}$ enable us to pose the following theorem.

**Remark 4.7.** [**Minimal set of generators of an ideal**]

Let $Z \subset \mathbb{P}^r$ be a nondegenerate projective irreducible curve and let $I_Z$ be the homogeneous ideal of $Z$ in $R$. Then we can choose the minimal set of homogeneous generators for $I_Z$ as $I_Z$ is finitely generated. For the convenience of the reader, we revisit the notion of minimal set of generators of an ideal $I_Z$. Let

$$M = \{G_{i,j} \in K[X_0, X_1, \ldots, X_r] \quad | \quad G_{i,j} \in I_Z \quad \text{for } 2 \leq i \leq m \text{ and } 1 \leq j \leq \ell_i\}$$

be the set of homogeneous polynomials of degree $\deg(G_{i,j}) = i$. Let $(I_Z)_{\leq t}$ be the ideal generated by the homogeneous polynomials in $I_Z$ of degree at most $t$. Then $M$ is the minimal set of generators of $I_Z$ if and only if the following three conditions hold:

(*i*) $I_Z$ is generated by the polynomials in $M$ (i.e., $I_Z = \langle M \rangle$).

(*ii*) $G_{i,1}, G_{i,2}, \ldots, G_{i,\ell_i}$ are $\mathbb{K}$-linearly independent forms of degree $i$ for each $2 \leq i \leq m$.

(*iii*) $G_{i,j} \notin (I_Z)_{\leq i-1}$ for each $2 \leq i \leq m$.

**Main Theorem 4.8.** Let the rational curve $C_d$ be defined as

$$C_d = \{[s^d(P) : s^{d-1}t(P) : s^2t^{d-2}(P) : st^{d-1}(P) : t^d(P)] \mid P \in \mathbb{P}^1\}.$$

Then the defining ideal $I_{C_d}$ of $C_d$ is minimally generated as follows:

$$Q_1 = X_2X_4 - X_3^2, \quad Q_2 = X_0X_4 - X_1X_3, \quad Q_3 = X_0X_3 - X_1X_2;$$

and $Q_1, Q_2, Q_3$ are fixed all the case.

Case1. $d = 2n + 1$ with $n \geq 2$, then

$$I_{C_d} = \left\langle Q_1, Q_2, Q_3, F_{[n,n]}, F_{[n+1,n-1]}, \cdots, F_{[2n-2,2]}, F_{[2n-1,1]} \right\rangle$$

where $F_{[2n-i,i]} = X_0^{2n-2i}X_2^i - X_1^{2n-2i+1}X_4^{i-1}$ for $1 \leq i \leq n$.

Case2. $d = 2n$ with $n > 2$, then

$$I_{C_d} = \langle Q_1, Q_2, Q_3, G_{[n,0]}, G_{[n,1]}, F_{[n,1]}, F_{[n+1,2]}, \cdots, F_{[n+j-1,j]} \rangle$$

where

$$G_{[n,i]} = X_1X_3^iX_4^{n-i-1} - X_2^{n+i-1}X_3^{1-i} \text{ with } i = 0, 1;$$

$$F_{[n+j-1,j]} = X_0^{2j-1}X_2^{n-j} - X_1^{2j}X_4^{n-j-1} \text{ for } 1 \leq j \leq n-1.$$

**Proof.** During the proof, $Q_1$, $Q_2$, and $Q_3$ are the same as the above theorem. We must show that the three condition of above Remark. We want to prove the theorem in the following order: (1) $M_d \subset I_{C_d}$, (2) condition $(ii)$ of the Remark 1, (3) condition $(iii)$ of the Remark 1, (4) $\langle M_d \rangle = I_{C_d}$ by using the result of the theorem[5].

Now we start (1). If $M_d \subset I_{C_d}$ is ture, implies that any point in $C_d$ kill all the polynomial in $M_d$. Since we have coordinate of $C_d$, thus we just substitution $X_0$ to $s^d$, $X_1$ to $s^{d-1}t$ etc, and check that every polynomial is zero. And it work.

Next, let's prove (2). We must first prove $Q_1, Q_2$ and $Q_3$ before prove the case 1 and case 2. But this is easy, for example $Q_2$ and $Q_3$ are $\mathbb{K}$-linearly independent and $Q_1$ is not. Then $Q_1 = Q_2A_1 + Q_3A_2$ for some constant $A_i$. Since $Q_1 = Q_2A_1 + Q_3A_2$ is an identity equation, therefore we can assign a point $p = [0, 0, 0, X_3, 0] \in \mathbb{P}^4$ in the formula. Then $-X_3^2 = 0$, this is a contradiction, since $Q_1 = Q_2A_1 + Q_3A_2$ is an identity equation. In the same way, $Q_2$ and $Q_3$ can be proved easily.

Now let us consider two cases : $d = 2n + 1$ and $d = 2n$. If $d = 2n + 1$, then we have : $Q_1, Q_2, Q_3, F_{[n,n]}, F_{[n+1,n-1]}, \cdots, F_{[2n-2,2]}, F_{[2n-1,1]}$. Since every $F_{[2n-i,i]}$ has a different degree, thus we only need to think about $deg(F_{[2n-i,i]}) = 2$. It implies that $n = 2$, we have $Q_1, Q_2, Q_3, F_{[2,2]}, F_{[3,1]}$. Show that $Q_1, Q_2, Q_3$ and $F_{[2,2]}$ are $\mathbb{K}$-linearly independent forms of degree 2. Since $Q_1, Q_2, Q_3$ are $\mathbb{K}$-linearly

independent. Hence suppose that $F_{[2,2]}$ and $Q_1, Q_2, Q_3$ are not $\mathbb{K}$-linearly independent. Then we have an identity equation $F_{[2,2]} = Q_1A_1 + Q_2A_2 + Q_3A_3$. Take $p = [0, 0, X_2, 0, 0] \in \mathbb{P}^4$, then $F_{[2,2]}(p) = X_2^2 = Q_1(p)A_1(p) + Q_2(p)A_2(p) + Q_3(p)A_3(p) = 0 : X_2^2 = 0$. This can not happen. Thus $Q_1, Q_2, Q_3, F_{[2,2]}$ are $\mathbb{K}$-linearly independent. Now suppose that $d = 2n$, since $Q_1, Q_2, Q_3$ are $\mathbb{K}$-linearly independent, and every $F_{[n+j-1,j]}$ has a different degree. Therefor we have to show that $G_{[n,0]}$, $G_{[n,1]}$ and $F_{[n,1]}$ are $\mathbb{K}$-linearly independent. First step, show that $G_{[n,0]}$ $G_{[n,1]}$ are $\mathbb{K}$-linearly independent. If not, then we have an identity equation $G_{[n,0]} = G_{[n,1]}A_1$ for some constant $A_1 : X_1X_4^{n-1} - X_2^{n-1}X_3 = (X_1X_3X_4^{n-2} - X_2^n)A_1$. We can not create the term $X_2^{n-1}X_3$ by multiplying the right side by a constant, thus $G_{[n,0]}$ are $G_{[n,1]}$ $\mathbb{K}$-linearly independent. Now consider $G_{[n,0]}$, $G_{[n,1]}$ and $F_{[n,1]}$. Suppose that $G_{[n,0]}$, $G_{[n,1]}$ and $F_{[n,1]}$ are not $\mathbb{K}$-linearly independent. Then we have $F_{[n,1]} = X_0X_2^{n-1} - X_2^2X_4^{n-2} = (X_1X_4^{n-1} - X_2^{n-1}X_3)A_1 + (X_1X_3X_4^{n-2} - X_2^n)A_2 = G_{[n,0]}A_1 + G_{[n,1]}A_2$ for some constant $A_i$. However, since $X_2^n$ can not be canceled, this formula can not be established. Therefore $G_{[n,0]}$, $G_{[n,1]}$ and $F_{[n,1]}$ are $\mathbb{K}$-linearly independent form of degree $n$.

Prove (3). Assume that $d = 2n + 1$, we know that $F_{[n,n]} \notin \langle Q_1, Q_2, Q_3 \rangle$. So, prove that $F_{[2n-k,k]} \notin \langle Q_1, Q_2, Q_3, F_{[n,n]}, F_{[n+1,n-1]}, \cdots, F_{[2n-k-2,k+2]}, F_{[2n-k-1,k+1]} \rangle$ for $1 \leq k < n$. Now suppose that

$$F_{[2n-k,k]} \in \langle Q_1, Q_2, Q_3, F_{[n,n]}, F_{[n+1,n-1]}, \cdots, F_{[2n-k-2,k+2]}, F_{[2n-k-1,k+1]} \rangle$$

for $1 \leq k < n$. Then we have an identity equation : $F_{[2n-k,k]} = Q_1A_1 + Q_2A_2 + Q_3A_3 + F_{[n,n]}B_0 + F_{[n+1,n-1]}B_1 + \cdots + F_{[2n-k-2,k+2]}B_{n-k-1} + F_{[2n-k-1,k+1]}B_{n-k}$ for

some $A_i, B_j \in k[X_0, \cdots, X_n]$. Then

$$\begin{aligned} X_0^{2n-2k}X_2^k - X_1^{2n-2k+1}X_4^{k-1} =& (X_2X_4 - X_3^2)A_1 + (X_0X_4 - X_1X_3)A_2 + \\ & (X_0X_3 - X_1X_2)A_3 + (X_2^n - X_1X_4^{n-1})B_0 + \\ & (X_0^2X_2^{n-1} - X_1^3X_4^{n-2})B_1 + \cdots + \\ & (X_0^{2n-2k-4}X_2^{k+2} - X_1^{2n-2k-3}X_4^{k+1})B_{n-k-1} + \\ & (X_0^{2n-2k-2}X_2^{k+1} - X_1^{2n-2k-1}X_4^k)B_{n-k}. \end{aligned}$$

Take point $p = [1, 0, X_2, 0, 0] \in \mathbb{P}^4$, and let substituting $p$ in the equation above. Then we have an identity equation : $X_2^k = X_2^n B'_0 + X_2^{n-1}B'_1 + \cdots + X_2^{k+2}B'_{n-k-1} + X_2^{k+1}B'_{n-k}$. The equations do not hold because the degree of all terms on the right is greater than $k$. Thus

$$F_{[2n-k,k]} \notin \langle Q_1, Q_2, Q_3, F_{[n,n]}, F_{[n+1,n-1]}, \cdots, F_{[2n-k-2,k+2]}, F_{[2n-k-1,k+1]} \rangle.$$

Suppose that $d = 2n$. We know that $G_{[n,0]}, G_{[n,1]}, F_{[n,n]}$ are $\mathbb{K}$-linearly independent. Now we take $k$ for $1 \leq k \leq n-1$, and shows that
$F_{[n+k-1,k]} \notin \langle Q_1, Q_2, Q_3, G_{[n,0]}, G_{[n,1]}, F_{[n,1]}, F_{[n+1,2]}, \cdots, F_{[n+k-3,k-2]}, F_{[n+k-2,k-1]} \rangle$.
Suppose not, then we have an identity equation :

$$\begin{aligned} X_0^{2k-1}X_2^{n-k} - X_1^{2k}X_4^{n-k-1} =& (X_2X_4 - X_3^2)A_1 + (X_0X_4 - X_1X_3)A_2 \\ & + (X_0X_3 - X_1X_2)A_3 + (X_1X_4^{n-1} - X_2^{n-1}X_3)B_0 \\ & + (X_1X_3X_4^{n-2} - X_2^n)B_1 + (X_0X_2^{n-1} - X_1^2X_4^{n-2})C_1 \\ & + (X_0^3X_2^{n-2} - X_1^4X_4^{n-3})C_2 \\ & + \cdots + (X_0^{2k-3}X_2^{n-k+1} - X_1^{2k-2}X_4^{n-k})C_{k-1}. \end{aligned}$$

Take $p = [1, 0, X_2, 0, 0] \in \mathbb{P}^4$ and put into above equation. Then we have :

$$X_2^{n-k} = -X_2^n B'_1 + X_2^{n-1}C'_1 + X_2^{n-2}C'_2 + \cdots + X_2^{n-(k-2)}C'_{k-2} + X_2^{n-(k-1)}C'_{k-1}.$$

Since the degree of the right side is $n - (k-1)$ when it is smallest, but the degree of the left side is $n - k$, this is a contradiction. Therefore $F_{[n+k-1,k]} \notin \langle Q_1, Q_2, Q_3, G_{[n,0]}, G_{[n,1]}, F_{[n,1]}, F_{[n+1,2]}, \cdots, F_{[n+k-3,k-2]}, F_{[n+k-2,k-1]} \rangle$.

The number of minimal generators of $I_{C_d}$ can be known from the results of the theorem[5] and compared with the number of generators of $M_d$, then $I_{C_d} = \langle M_d \rangle$ and $M_d$ is the set of minimal generators of $I_{C_d}$.

# References


[1] M.F.Atiyah, I.G.Macdonald, *Introduction to Commutative algebra*, Addison-Wesley Publishing Company, 1969.

[2] William Fulton, *Algebraic Curves: An introduction to Algebraic Geometry*, Addison-Wesley Publishing Company, 2008.

[3] Thomas W.Hungerford, *Abstract Algebra: An Introduction*, Brooks/Cole, Cengage Learning, 2013.

[4] Gert-Martin Greuel, Gerhard Pfister et al *Singular 3.0, a computer algebra system for polynomial computations*, Center for Computer Algebra, University of Kaiserslautern (2005) (http://www.singular.uni-kl.de).

[5] W. Lee and E. park, *On curves lying on a rational normal surface scroll, preprint.*

[6] Thomas W.Hungerford, *Algebra: Graduate texts in mathematics*, Springer, 2000.

[7] Karean E. Smith, Lauri Kahanpaa, Pekka Kekalainen, William Traves, *An Inviation to Algebraic Geometry*, Springer, 2000.