



## 저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Thesis for the Degree of Master of Science

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



Shuai-Ling Yang

Department of Applied Mathematics

The Graduate School

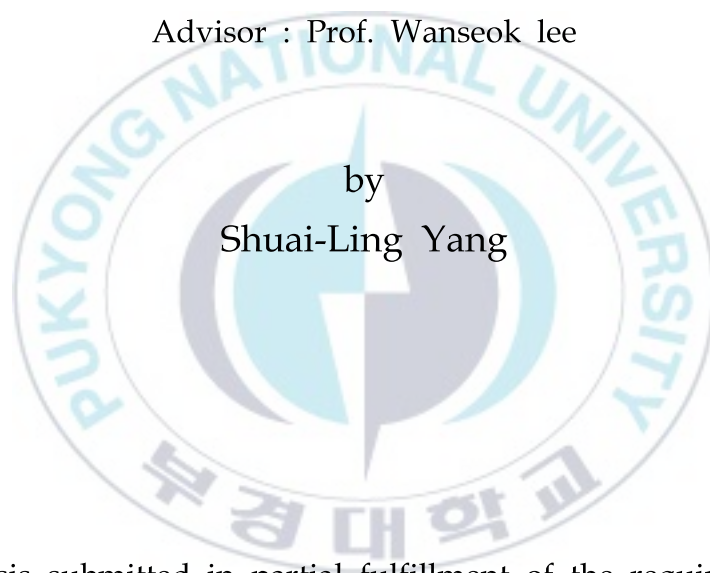
Pukyong National University

August 2018

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

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

Advisor : Prof. Wanseok lee



by  
Shuai-Ling Yang

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

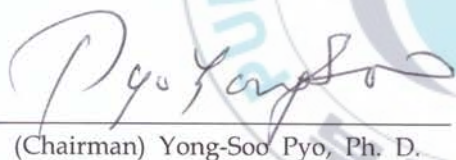
Master of Science

in Department of Applied Mathematics, The Graduate School,  
Pukyong National University  
August 2018

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

A dissertation  
by  
Shuai-Ling Yang


Approved by:



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



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



(Member) Wanseok Lee, Ph. D.

August 24, 2018

## CONTENTS

|  |    |
|--|----|
| Abstract(Korean) .....                                     | ii |
| 1. Preliminaries .....                                     | 1  |
| 2. Affine varieties .....                                  | 7  |
| 3. Projective varieties .....                              | 19 |
| 4. Defining equations of rational curves on $S(1,1)$ ..... | 25 |
| References .....   | 30 |

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

양 수 령

부경대학교 대학원 응용수학과

요 약

사영공간에 매립된 사영다영체를 정의하는 결정방정식에 관한 연구는 사영대수기하학의 매우 중요하고 어려운 문제 중의 하나이다. 이 논문에서는 3차원 사영공간  $\mathbb{P}^3$ 에 차수가  $d$ 인 Veronese 동형사상으로부터 유도된 매개변수들로 정의되는 유리곡선  $C_d$ 들의 결정방정식을 연구하였다.

먼저 유리곡선  $C_d$ 들이 정규 유리곡면  $S(1, 1)$ 위에 여차원이 1인 부분다양체가 됨을 보였고 이러한 기하적인 사실과 컴퓨터 대수 계산 프로그램(Computer Algebra System, CAS)인 'SINGULAR'를 이용하여 유리곡선  $C_d$ 들의 결정방정식들을 완벽하게 묘사하였다. 유리곡선  $C_d$ 를 정의하는 동차 아이디얼  $I_{C_d}$ 는 2차 동차 방정식  $X_0X_3 - X_1X_2$ 와  $(d-1)$  개의 차수가  $d$ 인 동차 방정식  $F_{d,i} = X_0^{d-i-1}X_2^i - X_1^{d-i}X_3^{i-1}$ ,  $1 \leq i \leq d-1$ 을 최소 생성원으로 생성됨을 보였다. 제1 장에서는 가환환, 아이디얼의 연산과 관련된 여러 가지 대수학의 기본 개념들을 정리하였다. 제2 장에서는 대수기하학의 기본적인 개념과 본 연구에 필요한 중요한 정리들을 조사하였다. 제3 장에서는 'SINGULAR' 프로그램을 통하여 유리곡선들의 차수가 5, 6, 7, 8, 9, 10일 때 유리곡선  $C_d$ 의 결정방정식들의 모양을 계산하였고 이러한 예제들을 기반으로 일반적인 경우에 대하여  $C_d$ 의 최소 결정방정식을 완벽하게 묘사하였다.

# Chapter 1

## Preliminaries

### 1.1 Rings and Ideals

Much of algebraic geometry comes from the fact that geometric problems can be translated into algebraic problems. In this chapter, we construct some fundamental algebraic concepts might be different to general algebraic concepts. For details, see [2] [3] [8]. If we talk about a ring then it means that the ring is commutative and with identity.

**Definition 1.1.1.** A *ring* is a set with two binary operations (addition and multiplication ) such that

- (1)  $A$  is abelian group with respect to addition.
- (2) Multiplication is associative and distributive over addition.
- (3)  $xy = yx$  for all  $x, y$  in  $A$ .
- (4) There exist  $1$  in  $A$  such that  $x1 = 1x = x$  for all  $x$  in  $A$  the identity element is the unique.

**Definition 1.1.2.** A *ring homomorphism* mapping  $f$  of a ring  $A$  into a ring  $B$  such that

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

**Definition 1.1.3.** A subset  $S$  of a ring  $A$  is a *subring* of  $A$ . If  $S$  is closed under addition and multiplication and contain the identity element of  $A$ .

Let  $Id$  be a map from  $S$  to  $A$  by settling  $Id(x) = x$  for all  $x$  in  $S$ , then it is

easy to verify  $Id$  is a ring homomorphism.

**Definition 1.1.4.** An *ideal*  $I$  of a ring  $A$  is a subset of  $A$  which is an addition subgroup and is such that  $AI$  is a subset of  $I$ .

**Proposition 1.1.5.** *There is a one-to-one order-preserving correspondence between the ideals  $J$  of  $A$  which contain  $I$  and the ideal  $\bar{J}$  of  $A/I$ .*

**Definition 1.1.6.** (1) A *zero-divisor* in ring  $A$  is a nonzero element  $x$  which there exists  $y \neq 0$  in  $A$  such that  $xy = 0$ .

(2) A ring with no zero-divisor is called an *integral domain*.

(3) An element  $x$  of  $A$  is called *nilpotent*, if  $x^n = 0$  for some  $n > 0$ .

(4) The multiples  $ax$  of an element  $x \in A$  form a *principal ideal* denote by  $\langle x \rangle$ .

**Proposition 1.1.7.** (1) *If  $x$  is nilpotent, then  $x$  is zero-divisor.*

(2) *Let  $S$  be a set of units in  $A$ , then  $S$  is an abelian group.*

(3)  *$x$  is a unit if and only if  $\langle x \rangle = A$ .*

**Proposition 1.1.8.** *Let  $A$  be a non-zero ring, then the following are equivalent:*

(1)  *$A$  is a field.*

(2) *The only ideals in  $A$  are  $\langle 0 \rangle$  and whole ring  $A$ .*

(3) *Every homomorphism of  $A$  into a non-zero ring  $B$  is injective.*

**Proof.** (1) $\Rightarrow$ (2) Let  $a$  be a nonzero ideal in  $A$ . there exist a nonzero element  $x$  in  $a$ , then  $x$  is unit, hence  $\langle x \rangle = A$  is a subset of  $a$ , hence  $a$  is whole ring.

(2) $\Rightarrow$ (3) Let  $\phi$  be a ring homomorphism from  $A$  to  $B$ . Then  $\ker \phi$  is a proper ideal in  $A$  and  $B$  is non-zero ring. Therefore  $\ker \phi = 0$ , hence  $\phi$  is injective.

(3) $\Rightarrow$ (1) Let  $x$  be an element of which is not unit. Then  $\langle x \rangle$  is a proper ideal, hence  $B = A / \langle x \rangle$  is not 0. Let  $\phi$  be a natural map from  $A$  to  $B$ . Then  $\phi$  is a homomorphism. By hypothesis  $\phi$  is injective. Therefore  $\langle x \rangle = 0$ , hence  $x = 0$ .



## 1.2 Prime ideals and maximal ideals

**Definition 1.2.1.** An ideal  $p$  in  $A$  is *prime*, if  $p$  is not whole ring  $A$ ,  $xy$  is an element in  $p$ , then  $x$  in  $p$  or  $y$  in  $p$ .

**Definition 1.2.2.** An ideal  $m$  in  $A$  is *maximal*, if  $m$  is not whole ring and if there is no ideal  $a$  such that  $m \subsetneq a \subsetneq A$ .

**Proposition 1.2.3.** If  $f$  is a ring homomorphism from  $A$  to  $B$  and  $q$  is a prime ideal in  $B$ . Then  $f^{-1}(q)$  is a prime ideal in  $A$ .

But if  $m$  is a maximal ideal in  $B$ . It is not necessarily true that  $f^{-1}(m)$  is maximal in  $a$ . For true that  $f^{-1}(n)$  is prime.

**Definition 1.2.4.** A *partial order* on a set  $S$  is a relation  $\leq$  on  $S$  which is

- (1) For all  $x$  in  $S$ , there is  $x \leq x$ .
- (2) For all  $x, y$  in  $S$ , if  $x \leq y$ ,  $y \leq x$ , then  $x = y$ .
- (3) For all  $x, y, z$  in  $S$ , there is  $x \leq y$ ,  $y \leq z$ , then  $x \leq z$ .

**Definition 1.2.5.** (1) A partial order " $\leq$ " on a set  $S$  is *total order*, if for any  $x, y \in S$ , either  $x \leq y$  or  $y \leq x$ . In particular, if  $\leq$  is a partial order on a set  $S$  and  $C$  is a subset of  $S$ , then we say that set  $C$  is a *chain* if  $\leq$  is a total order on  $C$ .

(2) Let  $\leq$  be a partial order on a set  $S$ . Let  $A$  be a subset of  $S$ . An *upper bound* to the set  $A$  is an element  $s$  of  $S$  such that  $a \leq s$  for all  $a \in A$ .

Let  $\leq$  be a partial order on a set  $S$ .  $m$  is an element of  $S$  is called a maximal element of  $S$  if there is no element  $s \in S$  and  $s$  is not  $m$  such that  $m \leq s$ .

**Theorem 1.2.6.** [Zorn's Lemma] Let  $\leq$  be a partial order on a non-empty set  $S$ . If every chain in  $S$  has an upper bound in  $S$ , then  $S$  contain a maximal element.

**Theorem 1.2.7.** For every ring  $A$ , If  $A$  is not 0, then  $A$  has at least one maximal ideal.

**Proof.** Since  $A$  is a non-zero ring. Then we can take a set  $S$  is all proper ideals in  $A$ . Since  $\langle 0 \rangle$  is a proper ideal, so  $S$  is not an empty set. Let  $C$  be a chain consisting of ideals in  $S$ . The union  $U$  of all ideals in the chain  $C$ . Then for all ideals in chain  $C$  is always contained in  $U$ . Let  $a, b$  be elements of  $U$ . Then there exists  $I, J$  in  $C$  such that  $a$  is an element of  $I$ ,  $b$  is an element of  $J$ . Since  $C$  is chain, therefore  $I$  is a subset of  $J$  or  $J$  is a subset of  $I$ , We can suppose  $I$  is a subset  $J$ . That means  $a, b$  are in  $J$ . Hence  $a - b$  is in  $J$ , therefore  $a - b$  is an element of  $U$ . Let  $a$  be an element of  $U$ , and let  $r$  be in  $A$ . Then there exists  $I$  in  $C$  such that  $a$  is in  $I$ . That means  $ar$  is an element of  $I$  in  $U$ . Therefore  $U$  is an ideal in  $C$ . Since  $1$  is not in any of the ideals in the chain  $C$ , so  $1$  is not in  $U$ . Therefore  $U$  is a proper ideal, then  $U$  is in  $C$ . By Zorn's Lemma,  $S$  has a maximal element which in turn is a maximal ideal of ring  $A$ .

**Corollary 1.2.8.** *If  $a$  is a proper ideal, there exists a maximal ideal of  $A$  containing  $a$ .*

**Corollary 1.2.9.** *Every non-unit of  $A$  is contained in a maximal ideal.*

**Definition 1.2.10.** A ring  $A$  with exactly one maximal ideal  $m$  is called a *local ring*.

**Proposition 1.2.11.** (1) *Let  $A$  be a ring and  $m$  is a proper ideal of such that for every  $x \in A/m$  is a unit in  $A$ . Then  $A$  is a local ring and  $m$  its maximal ideal.*

(2) *Let  $A$  be a ring and  $m$  is a maximal ideal of  $A$ , such that every element of  $1 + m$  is a unit in  $A$ . Then  $A$  is local ring.*

**Proof.** (1) Every proper ideal consists of non-units, hence every non-units are contained in  $m$ , therefore  $m$  is the only maximal ideal of  $A$ .

(2) Let  $x$  be an element of  $A/m$ . Since  $m$  is a maximal ideal. That means  $\langle x \rangle + m = A$ . Hence there exists an element  $y$  in  $A$  and an element  $t$  in  $m$  such that  $xy + t = 1$ . Hence  $xy = 1 - t$  is in  $1 + m$ . Therefore  $x$  is unit. By (1)  $A$  is local ring.

## 1.3 Nilradical and Jacobson radical

**Proposition 1.3.1.** *The set  $\mathfrak{n}$  of all nilpotent elements in a ring  $A$  is an ideal and  $A/\mathfrak{n}$  has no nilpotent element ( $\neq 0$ ).*

**Proof.** If  $x$  is an element of  $\mathfrak{n}$ , then  $ax$  is in  $\mathfrak{n}$  for all  $a \in A$ . Let  $x, y$  be in  $\mathfrak{n}$ , then  $x^m = 0, y^n = 0$ . By the binomial theorem (valid in any commutative ring). We have  $(x + y)^{m+n-1}$  is a sum of integer multiples of products  $x^r y^t$ , where  $r + t = m + n - 1$ . We can not have both  $r < m$  and  $s < n$ , then  $x^r y^t = 0$ . Therefore  $(x + y)^{m+n-1} = 0$ . Hence  $x + y \in \mathfrak{n}$ . Therefore  $\mathfrak{n}$  is an ideal, Let  $\bar{x}$  be in  $A/\mathfrak{n}$  be represented by  $x$  is an element of  $A$ . Then  $\bar{x}^n$  is represented by  $x^n$ . If  $\bar{x}^n = 0$ , then  $x^n \in \mathfrak{n}$  that means  $(x^n)^k = 0$  for some  $k > 0$ . Hence  $x$  is in  $\mathfrak{n}$ , therefore  $\bar{x} = 0$ .

**Definition 1.3.2.**  $\mathfrak{n}$  is a set of all nilpotent elements of  $A$  is called the *nilradical* of  $A$ .

**Proposition 1.3.3.** *The nilradical of  $A$  is the intersection of all prime ideals of  $A$ .*

**Proof.** Let  $\mathfrak{n}'$  denote the intersection of all prime ideals of  $A$ . If  $f$  is nilpotent of  $A$  and if  $P$  is a prime ideal, then  $f^n = 0$  is in  $P$  for some  $n > 0$ . Hence  $f$  is in  $P$ . Hence  $f$  is in  $\mathfrak{n}'$ . If  $f$  is not nilpotent. Let  $\Sigma$  be the set of ideals  $a$  with the property  $n > 0$ , then  $f^n$  is not in  $a$ .  $0$  is in  $\Sigma$  and  $\Sigma$  is not an empty set. As in Zorn's lemma can be applied to the setting  $\Sigma$  order by inclusion. Therefore  $\Sigma$  has a maximal element. Let  $p$  be a maximal element of  $\Sigma$ . Let  $x, y$  be not in  $p$ , then  $p$  is a proper subset of  $\langle x \rangle + p$ , and  $\langle y \rangle + p$ , for some  $m, n$ . That means  $\langle x \rangle + p, \langle y \rangle + p$  are not in  $\Sigma$ . Hence  $f^m$  and  $f^n$  are in  $\langle x \rangle + p, \langle y \rangle + p$  respectively, for some  $m, n$ . It follows that  $f^{m+n}$  is in  $p + \langle xy \rangle$ . That means  $p + \langle xy \rangle$  are not in  $\Sigma$ . Hence  $xy$  is not in  $p$ . Therefore  $p$  is a prime ideal and  $f$  is not in  $p$ . Therefore  $f$  is not in  $\mathfrak{n}'$ .

**Definition 1.3.4.** The *Jacobson radical*  $\mathfrak{R}$  is defined to be the intersection of all the maximal ideals of  $A$ .

**Proposition 1.3.5.**  $x \in \mathfrak{R}$  if and only if  $1 - xy$  is a unit in  $A$  for all  $y \in A$ .

**Proof.** Suppose  $1 - xy$  is not unit. Since  $m$  is a maximal ideal, then  $1 - xy$  is an element of  $m$ . But  $x$  is in  $\mathfrak{R}$ , and  $\mathfrak{R}$  is a subset of  $m$ , that means  $xy$  is in  $m$ . Then  $1$  is in  $m$ , which is absurd. Conversely, suppose  $x$  is not in  $\mathfrak{R}$ , then  $x$  is not in  $m$ , for some maximal ideal  $m$ . Then  $\langle x \rangle + m = A$ , there exists an element  $u$  in  $m$  and an element  $y$  in  $A$  such that  $u + xy = 1$ , then  $1 - xy$  is in  $m$ ,  $1 - xy$  is not a unit.



# Chapter 2

## Affine varieties

### 2.1 Algebraic sets and Hilbert Basis Theorem

In algebraic geometry, we study the common zero sets of polynomials. We work over algebraically closed  $k$  with an arbitrary characteristic. In this chapter we construct some fundamental concept in algebraic geometry. For details, we refer [7] [9].

**Definition 2.1.1.**  $n$ -dimensional *affine space* is  $\mathbb{A}^n := k^n = k \times \cdots \times k$ .

If  $f \in k[x_1, \dots, x_n]$  is a polynomial,  $f$  defines a function from  $\mathbb{A}^n$  to  $K$  setting by  $f(a_1, \dots, a_n)$ , for every point in  $\mathbb{A}^n$ . If  $f \in k[x_1, \dots, x_n]$  and  $p$  is in  $\mathbb{A}^n$  such that  $f(p) = 0$ , then  $p$  is called a zero of  $f$ . If  $f \in k[x_1, \dots, x_n]$  is not a constant,  $Z(f)$  is a set of all zero of  $f$ ,  $Z(f)$  is called a hyperplane define by  $f$ . Degree of  $f$  is one is called hyperplane. If  $f$  is a linear form in  $k[x_1, \dots, x_n]$ ,  $Z(f)$  is isomorphic to  $(n - 1)$ -dimensional linear space.

**Definition 2.1.2.** Let  $S$  be a set of  $k[x_1, \dots, x_n]$ , then  $Z(S)$  is defined by all zero of all polynomials in  $S$ .  $X$  is called an *affine algebraic set* in  $\mathbb{A}^n$ , if there exists a subset of  $S$  in  $k[x_1, \dots, x_n]$  such that  $X = Z(S)$ .

**Proposition 2.1.3.** Let  $S, T$  be subsets of polynomials in  $k[x_1, \dots, x_n]$ .

- (1) If  $S$  is a subset of  $T$ , then  $Z(T)$  is a subset  $Z(S)$ .
- (2) If  $I$  is an ideal in  $k[x_1, \dots, x_n]$  generated by  $S$ , then  $Z(S) = Z(I)$ .

**Proof.** (1) If  $p$  is in  $Z(T)$ , then  $f(p) = 0$ , for any  $f$  of  $T$  and  $S$  is a subset of

$T$ . It implies for any polynomial  $g$  of  $S$  is in  $T$ . Then  $g(p) = 0$ , therefore  $p$  is an element of  $Z(S)$ .

(2) Let  $I$  be an ideal generated by  $S$ , then  $S$  is a subset of  $I$ . That means  $Z(I)$  is a subset of  $Z(S)$ . Therefore for every  $p$  is in  $Z(S)$  and  $f$  is in  $S$ , there is  $f(p) = 0$ . If  $g$  is in  $I$ , then  $g$  can be expressed by a finite sum of  $f_i g_i$  for some  $g_i$  are polynomials of  $k[x_1, \dots, x_n]$ . We know  $g(p) = \sum (f_i g_i)(p) = f_i(p) g_i(p) = 0$ , then  $p \in Z(S)$ . Therefore  $Z(S) = Z(I)$ .

If we declare the affine algebraic sets are as the closed sets. Then we may regard the affine space as topological spaces. For the set of all affine algebraic set, we can give an induced topology to it.

**Proposition 2.1.4.** (1)  $\{S_\alpha\}_{\alpha \in A}$  is a family of subsets of  $k[x_1, \dots, x_n]$ , then  $\cap_\alpha Z(S_\alpha) = Z(\cup_\alpha S_\alpha)$ .

(2) If  $S, T \subseteq k[x_1, \dots, x_n]$ , then  $Z(S) \cup Z(T) = Z(ST)$ ,  $ST$  is a set of  $fg$ , for  $f \in S$  and  $g \in T$ .

(3)  $Z(0)$  is whole space and  $Z(1)$  is an empty set.

**Proof.** (1) By definition  $p$  is in  $\cap_\alpha Z(S_\alpha)$  if and only if  $f(p) = 0$ , for all  $f$  in any of the  $S_\alpha$ , then  $p$  is in  $Z(\cup_\alpha S_\alpha)$ .

(2) Let  $p$  be in  $Z(S) \cup Z(T)$  and  $f$  is a polynomial of  $S$ ,  $g$  is a polynomial of  $T$ . Since  $f(p) = 0$  or  $g(p) = 0$ , then  $fg(p) = f(p)g(p) = 0$ . Therefore  $p \in Z(ST)$ . Let  $p$  be a point of  $Z(ST)$ , assume  $p$  is not in  $Z(S)$ . Then there exist a polynomial  $f$  of  $S$  such that  $f(p)$  is not 0. Since  $g$  is a polynomial of  $T$ . Then  $fg$  is in  $ST$ .  $fg(p) = f(p)g(p) = 0$  and  $f(p)$  is not 0, hence  $g(p) = 0$ . Therefore  $p$  is a point of  $Z(T)$ .

**Definition 2.1.5.** We defined *zariski topology* on  $\mathbb{A}^n$  is taking the closed subsets to algebraic sets.

If  $A$  is a subset of  $\mathbb{A}^n$ , we can give the induced topology on it. In particular, if  $X$  is an algebraic set, Then induced Zariski topology on  $X$ , if we take the closed



sets to algebraic subsets in  $X$ .

**Definition 2.1.6.** Let  $X$  be a subset of  $\mathbb{A}^n$ . The ideal of  $X$  is defined by a set of polynomials of  $k[x_1, \dots, x_n]$ , if take  $f \in I(X)$  and every point  $p$  in  $X$ , then  $f(p) = 0$ . The ideal of  $X$  is denoted by  $I(X)$ . That is  $I(X)$  is the ideal of all polynomials vanishing on  $X$ . In particular, if  $X$  is an affine algebraic set, then  $Z(I(X)) = X$ .

If  $X$  is an affine algebraic set in  $\mathbb{A}^n$ . Then  $X$  can be expressed by some finite set  $S$  of polynomials in  $k[x_1, \dots, x_n]$  by Hilbert Basis Theorem. Geometric consequences for an algebraic set. Every affine algebraic set can be decomposed into a finite number of "pieces".

**Lemma 2.1.7.** Let  $R$  be a ring, the following are equivalent:

- (1) Every ideal  $I$  of  $R$  is finite generated.
- (2)  $R$  satisfies the ascending chain condition: If  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$  chain of ideal, then it becomes stationary. If  $R$  fulfills the properties,  $R$  is called Noetherian.

**Proof.** (1)  $\Rightarrow$  (2) Let  $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$  be a chain of ideal in  $R$ . Put  $I := \cup_{i \geq 0} I_i$ , then  $I$  is an ideal. By (1) we can write  $I = \langle f_1, \dots, f_k \rangle$ . Each  $f_i$  lies in  $I_{i_i}$  for some  $i_i > 0$ . Let  $N = \max\{i_1, \dots, i_k\}$ , then  $f_1, \dots, f_k$  are in  $I_N$ , that means  $I$  is a subset of  $I_N$ . Since  $I_N$  is also a subset of  $I$ . Therefore  $I_N = I_{N+1}$ .

(2)  $\Rightarrow$  (1) Let  $I$  be an ideal of  $R$ , assume  $I$  is not finite generator, take  $f_1$  is in  $I$  and  $f_2$  is in  $I \setminus \langle f_1 \rangle$ , inductively we take  $f_{n+1}$  is not in  $\langle f_1, \dots, f_n \rangle$ . So we have an ideal chain :  $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \dots \subsetneq \langle f_1, \dots, f_k \rangle \subsetneq \dots$ . Infinite chain where does not become stationary.

**Theorem 2.1.8. [Hilbert Basis Theorem]** Let  $R$  be a Noetherian ring, then  $R[x_1, \dots, x_n]$  is Noetherian.

**Proof.** Since  $R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$ . That is enough to prove (by induction), if  $R$  is Noetherian ring, then  $R[x]$  is Noetherian. Let  $I$  be an ideal

in  $R[x]$  is not finite generated. let  $f_1 \in I \setminus \{0\}$  such that  $\deg(f_1)$  is minimal. let  $f_2 \in I \setminus \{f_1\}$  be a polynomial of minimal degree. Inductively  $f_{n+1} \in I \setminus \{f_1, \dots, f_n\}$  is a polynomial of minimal degree.  $n_i = \deg(f_i)$ ,  $a_i \in R \setminus \{0\}$  is leading coefficient of  $f_i$ . Notice:  $n_1 \leq n_2 \leq n_3 \leq \dots$  and  $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset \dots$ . Assume  $\langle a_1, \dots, a_k \rangle = \langle a_1, \dots, a_k, a_{k+1} \rangle$ . It implies  $a_{k+1}$  is an element of  $\langle a_1, \dots, a_k, a_{k+1} \rangle$ . We can write  $a_{k+1} = \sum_{i=1}^k b_i a_i$ , for some  $b_i$  is in  $R$ . Let  $g := f_{k+1} - \sum_{i=1}^k b_i x^{n_{k+1}-n_i} \cdot f_i = f_{k+1} - (b_1 x^{n_{k+1}-n_1} \cdot f_1 + b_2 x^{n_{k+1}-n_2} \cdot f_2 + \dots + b_k x^{n_{k+1}-n_k} \cdot f_k)$ .  $g$  is in  $I \setminus \langle f_1, \dots, f_k \rangle$ , All sums of  $g$  have degree  $n_{k+1}$ , and the sum of leading term is  $a_{k+1} - \sum_{i=1}^k a_i b_i = 0$ , then  $\deg(g) < n_{k+1}$ . This is a contradiction with the way that take  $f_{k+1}$ . Hence the chain does not become stationary. Therefore  $R$  is not Noetherian.

**Corollary 2.1.9.** *Every affine algebraic set  $X \subseteq \mathbb{A}^n$  is intersection of finitely many hypersurfaces.*

**Proof.**  $I(X)$  is an ideal of  $k[x_1, \dots, x_n]$ .  $k$  is a field, it implies  $k[x_1, \dots, x_n]$  is Noetherian. By Hilbert Basis Theorem, we have  $I(X) = \langle f_1, \dots, f_k \rangle$ .  $Z(I(X)) = X$ . Then  $X = Z(f_1) \cap \dots \cap Z(f_k)$ .

## 2.2 Irreducible components

A topological space may be the union of some smaller topological space. A topological space  $X$  is called reducible, if we can write  $X = X_1 \cup X_2$ , for  $X_1, X_2$  are closed sets of  $X$  and  $X_1 \subsetneq X, X_2 \subsetneq X$ .  $X$  is called irreducible, if it is not reducible.

**Proposition 2.2.1.** *Let  $X$  be an irreducible topological space and  $U$  is a nonempty open subset, then  $U$  is dense in  $X$ .*

**Proof.**  $X = (X \setminus U) \cup \bar{U}$ ,  $X$  is irreducible. Then  $X = X \setminus U$  or  $X = \bar{U}$ . Since  $U$  is nonempty,  $X$  is not  $X \setminus U$ , therefore  $X = \bar{U}$ .



**Example 2.2.2.** (1) A point  $p \in \mathbb{A}^n$  is irreducible.  
(2)  $Z(XY) \subset \mathbb{A}^2$  is reducible. Since  $Z(XY) = Z(X) \cup Z(Y)$ .

**Definition 2.2.3.** A topological space  $X$  is called *Noetherian* if every descending chain  $X \supset X_1 \supset X_2 \supset \dots$  of closed subsets becomes stationary.

**Proposition 2.2.4.** (1) Any subspace  $Y$  of a Noetherian topological space  $X$  is Noetherian. (2)  $\mathbb{A}^n$  is a Noetherian topological space.

**Proof.** (1) A descending chain of closed subset.  $Y \supset Y_1 \supset Y_2 \supset \dots$ , then for all  $i$  there exist  $Y_i = X_i \cap Y$ ,  $X$  is closed subset of  $X_i$ . Put  $x'_i = \bigcap_{j \leq i} X_j$  and  $X_i \cap Y = Y_i$ . Then we have  $X'_1 = X_1, Y_1 = Y \cap X_1 = Y \cap X'_1$ . Then we have a descending chain of a closed set of  $X$ :  $X \supset X'_1 \supset X'_2 \supset \dots$ . Since  $X$  is Noetherian topological space, then there exist integer  $N$  such that  $X'_N = X_{N+1} = \dots$ . Then also  $Y \supset Y_1 \supset Y_2 \supset \dots$  becomes stationary. Therefore  $Y$  is a Noetherian topological space.

(2) Let  $\mathbb{A}^n = X_1 \supset X_2 \supset \dots$  be the chain of closed subsets in  $\mathbb{A}^n$ . Then  $I(X_1) \subset I(X_2) \subset \dots$  is an ascending chain of ideals in  $k[x_1, \dots, x_n]$ . Thus it becomes stationary,  $I(X_N) = I(X_{N+1}) = \dots$ . Therefore  $\mathbb{A}^n$  is a Noetherian topological space.

**Theorem 2.2.5** Let  $X$  be Noetherian space. (1)  $X$  is a union of finitely many irreducible closed subsets :  $X = X_1 \cup \dots \cup X_r$ . (2) If we require  $X_j \not\subset X_i$  for  $i \neq j$ , then this decomposition is unique, up to reorder.

**Proof.** (1) Assume  $X$  does not have a decomposition into finitely many irreducible closed subsets. Then  $X$  is not irreducible (if  $X$  is irreducible, then  $X = X$  has finitely irreducible decomposition.) Then we can write  $X = X_1 \cup Y_1$   $X_1, Y_1$  is a closed subset and  $X_1, Y_1 \neq X$ . Then at least there is one of  $\{X_1, Y_1\}$  does not have a decomposition into finitely many irreducible closed subsets. We use the same statement as the assumption about  $X_1$ , repeat argument,  $X_1 = X_2 \cup Y_2 \dots$ . We get descending chain  $X \supsetneq X_1 \supsetneq X_2 \supsetneq \dots$ . This chain does not

become stationary which is a contradiction to  $X$  being Noetherian.

(2) Let  $X = X_1 \cup \dots \cup X_r = Y_1 \cup \dots \cup Y_s$  and  $X_i \not\subseteq X_j, Y_i \not\subseteq X_j$  for  $i \neq j$ . We can write  $X_i = X \cap X_i = \cup_{j=1}^s (Y_j \cap X_i)$ , ( $X_i \cap Y_j$  is closed.) Since  $X_i$  is irreducible, then  $X_i = X_i \cap Y_j$  for some  $j$ . (i.e.,  $X_i \subset Y_j$ ). Similarly  $Y_j \subset X_k$  for some  $k$ . Then  $X_i \subset Y_j \subset X_k$ , it means  $X_i = X_k$  and  $Y_j = X_i$ . So each  $X_i$  is equal to one of  $Y_j$ , and each  $Y_j$  is equal to one of  $X_i$ . Hence  $r = s$ . Then this decomposition is unique, up to reorder.

In the future we mostly consider only irreducible an algebraic set.

**Definition 2.2.6.** An affine *variety* is a irreducible affine algebraic set.

**Proposition 2.2.7.** Let  $X$  be a subset of  $\mathbb{A}^n$  is an affine algebraic set.  $X$  is irreducible if and only if  $I(X)$  is a prime ideal.

**Proof.** Let  $f, g$  be polynomials of  $k[x_1, \dots, x_n]$  such that  $fg$  is in  $I(X)$ , then  $X$  is a subset of  $Z(fg) = Z(f) \cup Z(g)$ . Hence  $X = (X \cap Z(f)) \cup (X \cap Z(g))$  and  $(X \cap Z(f)), (X \cap Z(g))$  are closed subsets of  $X$ . Then  $X = (X \cap Z(f))$  or  $X = (X \cap Z(g))$ . Therefore  $X \subset Z(f)$  or  $X \subset Z(g)$ . Assume  $X$  is not irreducible We can write  $X = X_1 \cup X_2$  and  $X_i$  are closed subsets of  $X$ .  $Z(I(X_1)) = X_1$  is a subset of  $X = Z(I(X))$ , then  $I(X)$  is a proper subset of  $I(X_1)$ . Similar:  $I(X)$  is a proper subset of  $I(X_2)$ , let  $f$  be in  $I(X_1) \setminus I(X)$  and  $g$  is in  $I(X_2) \setminus I(X)$ .  $fg$  vanishes on  $X_1 \cup X_2 = X$ , then  $fg$  is in  $I(X)$ , therefore  $I(X)$  is not irreducible.

**Example 2.2.8.**  $\mathbb{A}^n$  is irreducible.

**Definition 2.2.9.** Let  $X \neq \emptyset$  be an irreducible topological space. the *dimension* of  $X$  is the largest integer  $n$  such that there is an ascending chain  $\emptyset \neq X_0 \subsetneq X_1 \subsetneq X_2 \subsetneq \dots \subsetneq X_n = X$  of irreducible closed subsets of  $X$ . If  $X$  is a Noetherian topological space then  $\dim(X)$  is defined to be the maximum of the dimensions of the irreducible components of  $X$ .

**Example 2.2.10.** (1) points have dimension 0. (2)  $\mathbb{A}^1$  has dimension 1. Only irreducible closed subsets of  $\mathbb{A}^1$  are points and  $\mathbb{A}^1$ . (3)  $\mathbb{A}^n$  has dimension  $n$  (In

the moment can not prove). It is easy to verify that  $\dim(\mathbb{A}^n) \geq n$ . Because ascending chain:  $\{0\} \subsetneq Z(x_2, \dots, x_n) \subsetneq Z(x_3, \dots, x_n) \subsetneq \dots \subsetneq Z(x_n) \subsetneq \mathbb{A}^n$ ,  $\mathbb{A}^0 \subsetneq \mathbb{A}^1 \subsetneq \dots \subsetneq \mathbb{A}^n$ .

## 2.3 Hilbert Nullstellensatz

If  $K$  is algebraically closed field and  $f(x)$  is a polynomial of  $K[x_1, \dots, x_n]$ . We knew the zero set of  $f(x)$  is not an empty set.

The question is we are not looking at a single polynomial, we looking a bunch of polynomials, even be finite and we are not looking at polynomials in one variable, we working on several variable polynomial ring. We want to get the similar result like above at the more general case. The weak Nullstellensatz tell we can get the same result by the just one condition, if  $k$  is a algebraically closed field and  $f(x)$  is a polynomial of  $K[x_1, \dots, x_n]$ , then the zero set of  $f(x)$  is not an empty set.

**Theorem 2.3.1. [Weak Nullstellensatz]** *If  $I$  is a proper ideal in  $K[x_1, \dots, x_n]$ , then  $Z(I) \neq \emptyset$ .*

**Proof.** We may assume that  $I$  is a maximal ideal for there is a maximal ideal  $J$  containing  $I$ , and  $Z(J)$  is a subset of  $Z(I)$ . So  $L = K[x_1, \dots, x_n]/I$  is a field, and  $K$  is isomorphic to  $K + I$ . Suppose we knew that  $K = L$ . Then for each  $x_i$ , there is an  $a_i \in K$  such that  $x_i + I = a_i + I$  if and only if  $x_i - a_i \in I$ . Since  $(x_1 - a_1, \dots, x_n - a_n)$  is a maximal ideal. So  $I = (x_1 - a_1, \dots, x_n - a_n)$  and  $Z(I) = \{(a_1, \dots, a_n)\}$  is not an empty set.

We will show that by two step:

- (1)  $L, K$  are field and  $K$  is  $L$  a subfield. If  $L$  is ring-finite over  $K$ , then  $L$  is module-finite over  $K$ .
- (2) If  $K$  is an algebraic closed field. If  $L$  is module-finite over  $K$ , then  $L = K$ .

**Definition 2.3.2.** Let  $R, S$  be rings, and  $R$  is a subring of  $S$ . (1)  $S$  is said to be *module-finite* over  $R$ , if  $S$  is finitely generated as  $R$ -module,  $S = \sum_{i=1}^n R s_i$ ,  $s_i \in S$ . If  $S$  and  $R$  are fields,  $S$  is a vector space over  $R$  dimension by  $[S : R]$ . (2)  $S$  is called *ring-finite* over  $R$ , if  $S = R[v_1, \dots, v_n]$  for some  $v_1, \dots, v_n \in S$ . (3)  $S$  is called *finitely generated field extension* of  $R$ , if  $S = R(v_1, \dots, v_n)$  for some  $v_1, \dots, v_n \in S$ .

**Definition 2.3.3.** Let  $R$  be a subring of a ring  $S$ . An element  $v \in S$  is said to be integral over  $R$ , if there is a monic polynomial.  $F = x^n + a_1 x^{n-1} + \dots + a_n \in R[x]$ , such that  $F(v) = 0$ . If  $R, S$  are fields, we say that  $v$  is *algebraic over  $R$* . (If  $v$  is integral over  $R$ .)

**Proposition 2.3.4.** Let  $R$  be a subring of a domain  $S$ .  $v \in S$ . 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) Let  $v$  be integral over  $R$ . Then there exist a monic polynomial.  $F = x^n + a_1 x^{n-1} + \dots + a_n$  such that  $F(v) = v^n + a_1 v^{n-1} + \dots + a_n = 0$ . Then we have a equation  $v^n = -a_1 v^{n-1} - \dots - a_n$ ,  $a_i \in R$  it implies  $v^n \in \sum_{i=0}^{n-1} R v^i$ . it follows that  $v^m$  is in  $\sum_{i=0}^{n-1} R v^i$  for all  $m$ . So  $R[v] = \sum_{i=0}^{n-1} R v^i$ .

(2) $\Rightarrow$ (3) Take  $R' = R[v]$ .

(3) $\Rightarrow$ (1) If  $R' = \sum_{i=1}^n R w_i$ ,  $w_i \in R$ . Since  $R[v]$  is a subset of  $R'$ , then

$$\begin{aligned} v w_1 &= a_{11} w_1 + \dots + a_{1n} w_n, \\ &\vdots \\ v w_n &= a_{n1} w_1 + \dots + a_{nn} w_n. \end{aligned}$$

Since  $S$  is a domain, we can consider these equations in the quotient field of  $S$ .

Let

$$\mathbf{A} = \begin{pmatrix} v - a_{11} & \cdots & -a_{1n} \\ \vdots & & \vdots \\ -a_{n1} & \cdots & v - a_{nn} \end{pmatrix}.$$

We see that  $(w_1, \dots, w_n)$  is a nontrivial solution. So  $\det(A) = 0$ . This determination has form  $v^n + a_1 v^{n-1} + \cdots + a_n = 0$ ,  $a_i \in R$ . So  $v$  is integral over  $R$ .

**Corollary 2.3.5.** *The set of elements of  $S$  that are integral over  $R$  is a subring of  $S$  containing  $R$ .*

**Proof.**  $a, b$  are integral over  $R$ , then  $b$  is integral over  $R[a]$ . So  $R[a, b]$  is module finite over  $R$ , and  $a \pm b, ab \in R[a, b]$ . Since  $R[ab], R[a \pm b] \subseteq R[a, b]$  module-finite over  $R$ . Therefore  $ab, a \pm b$  is integral over  $R$ .

**Definition 2.3.6.**  $S$  is *integral over  $R$*  if every element of  $S$  is integral over  $R$ .

**Proposition 2.3.7.** *Let  $L$  be a field,  $K$  is an algebraically closed subfield of  $L$ .*

- (1) *Show that any element of  $L$  that is algebraic over  $K$  is already in  $K$ .*
- (2) *An algebraically closed field has no module-finite field extensions except itself.*

**Proof.** (1) Let  $a$  be an element of  $L$  and  $a$  is algebraic over  $K$ . Then there exist a monic polynomial  $f \in K[x]$  such that  $f(a) = 0$ . Since  $K$  is algebraically closed. Therefore  $a$  is in  $K$ .

(2) Suppose  $L$  is module finite over  $K$ . Then  $L = Kv_1 + \cdots + Kv_n \subseteq K[v_1, \dots, v_n]$  is a subset of  $L$   $v_i$  is in  $L$ . Therefore  $L$  is ring-finite over  $K$ . That means  $v_1, \dots, v_n$  are algebraic over  $K$ , then  $v_1, \dots, v_n \in K$ , therefore  $L = K$ .

Suppose  $K$  is subfield of a field  $L$ , and  $L = K(v)$ , for some  $v \in L$ . Let  $\phi$  be a map from  $k[x]$  to  $L = k(v)$ . By setting  $\phi(x) = v$ . Since  $K[x]$  is PID, let

$\ker\phi = (F)$   $F \in K[x]$ , then  $K[x]/(F)$  be isomorphic to  $K[v]$ , therefore  $(F)$  is a prime ideal.

case (1),  $F = 0$ . Then  $k[x]$  is isomorphic to  $K[v]$ . So  $K(v) = L$  is isomorphism to  $k(x)$ . In this case  $L$  is not ring-finite over  $K$ .

case (2),  $F \neq 0$ . We may assume  $F$  is monic. Then  $(F)$  is a prime ideal, then  $F$  is irreducible, hence  $(F)$  is maximal, then  $K[x]/(F)$  is a field, we can know  $K[v] = K(v)$  is a field. Since  $F$  is in  $\ker\phi$ , then  $F(v) = 0$ . Then  $v$  is algebraic over  $K$ . By proposition 2.3.4. We have  $L = K[v] = k(v)$  is module-finite over  $K$ . **Theorem 2.3.8.**[Zariski] If a field  $L$  is ring-finite over a subfield  $K$ , then  $L$  is module-finite over  $K$ .

**Proof.** Suppose  $L = K[v_1, \dots, v_n]$ . The case  $n = 1$  is taken care of by the above discussion. Assume the result for all extensions generated by  $n - 1$  element. Let  $K_1 = K(v_1)$ , by induction  $L = k_1[v_2, \dots, v_n]$  is module finite over  $K_1$ , Assume  $v_1$  is not algebraic over  $K$ . (If not the proof finished). Each  $v_i$  satisfies equations:

$$\begin{aligned} v_2^{n_2} + a_{21}v_2^{n_2-1} + \dots + a_{2,n_2} &= 0, \\ \vdots \\ v_n^{n_n} + a_{n1}v_n^{n_n-1} + \dots + a_{n,n_n} &= 0. \end{aligned}$$

Take  $a \in K[v_1]$  such that multiply of all denominators of  $a_{ij}$ , we get equations:

$$\begin{aligned} (av_2)^{n_2} + aa_{21}(av_2)^{n_2-1} + \dots + a^{n_2}a_{2,n_2} &= 0, \\ \vdots \\ (av_n)^{n_n} + aa_{n1}(av_n)^{n_n-1} + \dots + a^{n_n}a_{n,n_n} &= 0. \end{aligned}$$

Hence  $av_2, \dots, av_n$  is integral over  $K[v_1] \forall z \in L = K[v_1, \dots, v_n]$ . By Corollary 5, there is an  $N \in \mathbb{N}$ , such that  $a^N z$  is integral over  $k[v_1]$ . Since  $k(v_1)$  is a subset of  $L$ , this must hold for  $z$  is in  $K(v_1)$ . But  $K(v_1)$  is isomorphic to the field of rational function in one variable over  $K$ , that is impossible.



If  $I$  is a subset of  $k[x_1, \dots, x_n]$  is an ideal, then  $Z(I)$  is an affine algebraic set in  $\mathbb{A}^n$ . If  $X$  is an affine algebraic set, then  $I(X)$  is an ideal in  $k[x_1, \dots, x_n]$ .

We know that if  $X$  is an affine algebraic set, then  $Z(I(X)) = X$ .

But it is not true  $I(Z(J)) = J$ ,  $J$  is an ideal in  $k[x_1, \dots, x_n]$ . But clear we know  $J$  is a subset of  $I(Z(J))$ .

If  $I$  is an ideal in  $k[x_1, \dots, x_n]$  such that  $Z(I)$  is empty if and only if a unit is in  $I$ , when  $k$  is algebraic closed, otherwise this theorem is false.

**Definition 2.3.9.** Let  $I$  be an ideal in ring  $R$ . The *radical* of  $I$  is a set of for some positive  $n$  and  $r$  is  $R$  such that  $r^n$  is in  $I$ . The radical of  $I$  denote by  $\sqrt{I}$ .  $I$  is called a radical ideal, if  $I = \sqrt{I}$ .

**Proposition 2.3.10.** If  $X \subset \mathbb{A}^n$  is an affine algebraic set, then  $I(X)$  is a radical ideal.

**Proof.** Let  $f$  be a polynomial of  $k[x_1, \dots, x_n]$  with  $f^n \in I(X)$ , then  $f^n$  is in  $I(X)$ , it implies  $f^n(p) = 0$ .  $f^n(p) = f(p)^n = 0$ , that means  $f(p) = 0$ . Therefore  $f$  is in  $I(X)$ .

**Theorem 2.3.11.[Strong Hilbert Nullstellensatz]** Let  $I \subset k[x_1, \dots, x_n]$  be an ideal, then  $I(Z(I)) = \sqrt{I}$ .

**Proof.** While  $I$  is an ideal and generated by  $f_1, \dots, f_r$ . We know  $I(Z(I))$  is a radical ideal containing  $I$ , then  $I(Z(I))$  is a subset of  $\sqrt{I}$ . Let  $J$  be a ideal of  $k[x_1, \dots, x_n, t]$  and  $J$  is generated by  $I \cup ft - 1$ . Let  $(p, a)$  be in  $\mathbb{A}^{n+1}$  and  $p$  is in  $\mathbb{A}^n$ ,  $a$  is in  $k$ .  $(p, a) \in Z(J)$  if and only if  $p$  is in  $Z(I)$ ,  $f(p) \cdot a = 1$  if and only if  $f_1(p) = f_2(p) = \dots = f_r(p) = 0$ . Since  $p$  is a point of  $Z(I)$ , then  $f(p) \cdot a = 0 = 1$  this is impossible. Hence  $Z(J)$  is an empty set. By weak Hilbert Nullstellensatz.  $1$  is in  $J$ , then  $J = k[x_1, \dots, x_n, t]$ . Let  $1 = g_0(ft - 1) + \sum_{i=1}^r g_i f_i$ ,  $g_0, \dots, g_r \in k[x_1, \dots, x_n, t]$ . Back to  $k[x_1, \dots, x_n]$  with

$k(x_1, \dots, x_n)$ . Define ring homomorphism  $\phi$  from  $k[x_1, \dots, x_n, t]$  to  $k(x_1, \dots, x_n)$  by  $\phi((x_1, \dots, x_n, t)) = g(x_1, \dots, x_n, \frac{1}{f})$ . Apply  $\phi$  to  $1 = g_0(ft - 1) + \sum_{i=1}^r g_i f_i$ ,  $g_0, \dots, g_r \in k[x_1, \dots, x_n, t]$ , then  $\phi(1) = \phi(g(f \cdot \frac{1}{f} - 1)) + \sum_{i=1}^r \phi(g_i)\phi(f_i)$  in  $k(x_1, \dots, x_n)$   $1 = \sum_{i=1}^r \phi(g_i)f_i$ .

There exists  $n_i \in \mathbb{Z}^+$ , such that  $\phi(g_i) = \frac{G_i}{f^{n_i}}$ ,  $G_i \in k[x_1, \dots, x_n]$ . Let  $N = \max\{n_1, \dots, n_r\}$ , multiply by  $f^N$ .  $f^N = \sum_{i=1}^r G_i f^{N-n_i} \cdot f_i \in I$ . Thus  $I(Z(I))$  is a subset of  $\sqrt{I}$ . Therefore  $I(Z(I)) = \sqrt{I}$ .

**Corollary 2.3.12.** *We have mutually inverse inclusion-reversing bijection between affine algebraic sets in  $\mathbb{A}^n$  to radical ideals in  $k[x_1, \dots, x_n]$ .*

**Corollary 2.3.13.** (1) *If  $I$  is a prime ideal in  $k[x_1, \dots, x_n]$ , then  $Z(I)$  is irreducible.*

(2) *If  $f$  is irreducible in  $k[x_1, \dots, x_n]$ , then  $Z(f)$  is irreducible.*

**Proof.** (1) Let  $I$  be a prime ideal, we know  $I$  is a subset of  $\sqrt{I}$ . Let  $f$  be a polynomial of  $\sqrt{I}$ , then  $f^N$  is in  $I$ . Since  $I$  is a prime ideal. then  $f$  is in  $I$ . Hence  $I = \sqrt{I}$ , then  $I = I(Z(I))$ .  $I(X)$  is prime if and only if  $X$  is irreducible.

(2)  $k[x_1, \dots, x_n]$  is a UFD, if  $f$  is in  $k[x_1, \dots, x_n]$  is irreducible. then  $\langle f \rangle$  is a prime ideal. Hence  $Z(f) = Z(\langle f \rangle)$  is irreducible.



# Chapter 3

## Projective varieties

### 3.1 Projective algebraic sets

In this chapter we construct some basic concept in projective geometry. For details, see [10].

Let  $(X, d)$  is a metric space and  $S$  is a subset of  $X$ . If  $S$  is a subset of  $\{O_\alpha \mid O_\alpha \text{ are open sets of } X\}$ , then  $\cup_{\alpha \in A} O_\alpha$  is called an open cover of  $S$ , and  $S$  is called a compact set, if for all open cover  $O_\alpha$  of  $S$ , there exist  $\alpha_1, \dots, \alpha_m$  are elements of  $A$  such that  $S \subseteq \cup_{i=1}^m O_{\alpha_i}$ .

We define an equivalence relation on  $k^{n+1} \setminus \{0\}$ .  $(a_0, \dots, a_n)$  is relative to  $(b_0, \dots, b_n)$  if and only if there exists a non-zero real number  $\lambda$  such that  $(a_0, \dots, a_n) = \lambda(b_0, \dots, b_n)$ . Denote by  $[a_0, \dots, a_n]$  for equivalence class.  $n$ -dimensional projective space is a quotient set  $\mathbb{P}^n := (k^{n+1} \setminus \{0\}) / \sim$ .

Let  $U_i := \{[a_0, \dots, a_n] \in \mathbb{P}^n \mid a_i \neq 0, i = 0, \dots, n\}$ . The map  $\varphi_i$  is between  $U_i$  to  $\mathbb{A}^n$ , by  $\varphi([a_0, \dots, a_n]) = (\frac{a_0}{a_i}, \dots, \frac{\hat{a_i}}{a_i}, \dots, \frac{a_n}{a_i})$  is obviously bijective with the inverse  $u_i$  is from  $\mathbb{A}^n$  to  $U_i$ , setting by  $u_i(b_0, \dots, \hat{b_i}, \dots, b_n) = [b_0, \dots, 1, \dots, b_n]$ .  $\frac{a_j}{a_i}$  is called the affine coordinates of  $p = [a_0, \dots, a_n]$  with respect to  $U_i$ .

Usually we fix  $i = 0$ , we want to know  $\mathbb{A}^n$  as a subset of  $\mathbb{P}^n$ , by identifying the point  $(a_1, \dots, a_n) \in \mathbb{A}^n$  with  $[1, a_1, \dots, a_n] \in \mathbb{P}^n$ . In particular,  $\mathbb{P}^n = \mathbb{A}^n \cup H_\infty = U_0 \cup H_\infty$ , with  $H_\infty := \mathbb{P}^n \setminus U_0 = \{[a_0, \dots, a_n] \mid a_0 = 0\}$ ,  $H_\infty$  is called the hyperplane at infinity. We want to define a projective algebraic set  $\subset \mathbb{P}^n$  as zero set of polynomials in  $k[x_0, \dots, x_n]$ . Since  $f(a_0, \dots, a_n) \neq f(\lambda a_0, \dots, \lambda a_n), f \in k[x_0, \dots, x_n]$ . Thus  $f$  does not define a function. If  $f$  is homogeneous,  $f$  can define a function from  $\mathbb{P}^n$  to  $k$ .

If  $f \in k[x_0, \dots, x_n]$  is homogeneous of degree  $d$ , then for all  $\lambda \in k$ . There is  $f(\lambda a_0, \dots, \lambda a_n) = \lambda^d f(a_0, \dots, a_n)$ . Whether  $g(a_0, \dots, a_n) = 0$  depends only on  $[a_0, \dots, a_n]$ .

**Definition 3.1.1.** Let  $g \in k[x_0, \dots, x_n]$  be homogeneous, a point  $p = [a_0, \dots, a_n]$  is a zero of  $g$  ( $g(p) = 0$ ) if and only if  $g[a_0, \dots, a_n] = 0$ . By the above this is independent of the representative  $(a_0, \dots, a_n)$ . Let  $S \subset k[x_0, \dots, x_n]$  be a set of homogeneous polynomials, the projective zero set of  $S$ .  $Z(S) := \{p \in \mathbb{P}^n \mid f(p) = 0, \forall f \in S\}$  is called a *projective algebraic set*.

**Example 3.1.2.** (1)  $\emptyset = Z(1)$ ,  $\mathbb{P}^n = Z(\emptyset)$ .  
(2) If  $p = [a_0, \dots, a_n] \in \mathbb{P}^n$ , then  $\{p\} = Z(a_1x_0 - a_0x_1, a_2x_0 - a_0x_2, \dots, a_nx_0 - a_0x_n)$ .

**Definition 3.1.3.** Any polynomial  $f \in k[x_0, \dots, x_n]$  can be written in a unique way as a sum  $f = f^{(0)} + \dots + f^{(d)}$  of forms  $f^{(i)}$  of degree  $i$ .  $f^{(i)}$  are called *homogeneous components* of  $f$ .

**Definition 3.1.4.** An ideal  $I \subset k[x_0, \dots, x_n]$  is called *homogeneous ideal* if for  $f \in I$  all the homogeneous components  $f^{(i)}$  are in  $I$ .

**Proposition 3.1.5.** An ideal  $I \in k[x_0, \dots, x_n]$  is homogeneous if and only if it is generated by homogeneous elements.

**Proof** Assume  $I$  is homogeneous. Let  $\{f_\alpha\}_\alpha$  be a set of generators of  $I$ . Then  $\{f_\alpha^{(i)}\}_{(\alpha,i)}$  are a set of homogeneous generators. Let  $I$  be generated by homogeneous polynomials  $\{g_i\}$ , let  $f$  be a polynomial in  $I$ . We can write  $f = \sum_i a_i g_i$ ,  $a_i \in k[x_0, \dots, x_n]$ . By  $g_i$  is homogeneous, thus the homogeneous part of  $a_i g_i$  of degree  $d$  is just  $a_i^{(d-\deg(g_i))} \cdot g_i$ , then  $f^{(d)} = \sum_i a_i^{(d-\deg(g_i))} \cdot g_i \in I$  (since  $g_i \in I$ ).

**Definition 3.1.6.** Let  $I \subset k[x_0, \dots, x_n]$  be a homogeneous ideal. The projective zero set of  $I$  is defined by  $Z_p(I) = Z(I) = \{p \in \mathbb{P}^n \mid f(p) = 0\}$  for all homogeneous  $f \in I$ . For a subset  $X$  in  $\mathbb{P}^n$ , the *homogeneous ideal of  $X$*  is

defined by  $I_H(X) = I(X) := \langle \{f \in k[x_0, \dots, x_n] \mid f : \text{homogeneous}, f(p) = 0, \text{ for all } p \in X\} \rangle$ , by definition this is a homogeneous ideal.

If  $f = f^{(0)} + f^{(1)} + \dots + f^{(d)}$  is the decomposition into homogeneous component, then  $Z(f) = \cap_{i=0}^d Z(f^{(i)})$ . If  $f$  have non-zero constant part, then  $Z(f)$  is an empty set.

## 3.2 Zariski topology of projective varieties

Many properties on affine space is also hold on projective space, such as :

- (1) If  $X \subset Y$ ,  $\mathbb{P}^n$  are projective algebraic sets, then  $I(X) \supset I(Y)$ .
- (2) If  $Y \subset \mathbb{P}^n$  is a projective algebraic set, then  $Z(I(X)) = X$ .
- (3)  $I \subset k[x_0, \dots, x_n]$  is homogeneous ideal,  $I(Z(I)) \supset I$ .
- (4) If  $S \subset k[x_0, \dots, x_n]$  is a set of homogeneous  $Z(S) = Z(\langle S \rangle)$ .
- (5) For a family  $\{S_\alpha\}_\alpha$  of a set of homogeneous polynomials.  $Z(\langle \cup_\alpha S_\alpha \rangle) = Z(\cup_\alpha S_\alpha) = \cap_\alpha Z(S_\alpha)$ .
- (6) If  $S, T \subset k[x_0, \dots, x_n]$  set of homogeneous polynomial  $ST = \{fg \mid f \in S, g \in T\}$ , then  $Z(ST) = Z(S) \cup Z(T)$ .

Then we know that arbitrary intersections and finite unions of projective algebraic sets are projective algebraic set  $\emptyset$ ,  $\mathbb{P}^n$  are projective algebraic sets, now we can define a topology on projective space.

**Definition 3.2.1.** The *Zariski topology* on  $\mathbb{P}^n$  is the topology whose closed sets are projective algebraic set. If  $X \subset \mathbb{P}^n$  is a subset give it the induce topology. (The Zariski topology on  $X$ .)

**Definition 3.2.2.** A projective variety is an *irreducible projective algebraic set*. A quasi-projective algebraic set is an open subset of a projective variety. A variety is a locally closed subvariety of  $\mathbb{A}^n$ , or  $\mathbb{P}^n$ .

**Proposition 3.2.3.**  $k[x_0, \dots, x_n]$  is Noetherian, then the same proof as in affine case shows  $\mathbb{P}^n$  is Noetherian topological space.

**Proof.** If  $x_1 \supset x_2 \supset \dots$  chain of closed subsets of  $\mathbb{P}^n$ , then  $I(x_1) \subset I(x_2) \subset \dots$  is a chain of ideals in  $k[x_0, \dots, x_n]$ . Thus  $k[x_0, \dots, x_n]$  is Noetherian. As  $x_i = Z(I(x_i))$ , also the original chain  $x_1 \supset x_2 \supset \dots$  become stationary.

Every subspace of  $\mathbb{P}^n$  is Noetherian, in particular quasi-projective variety is Noetherian. That means quasi-projective variety has a unique decomposition into irreducible components.

If we use the identification:  $\mathbb{A}^n = U_0 = \{[1, a_1, \dots, a_n] \in \mathbb{P}^n\} \subset \mathbb{P}^n$ , we get  $\mathbb{A}^n = \mathbb{P}^n \setminus Z(x_0)$  is an open subset of  $\mathbb{P}^n$ . (i.e.,  $\mathbb{A}^n$  is a quasi-projective variety.) Any affine algebraic sets are quasi-projective algebraic sets.

### 3.3 Affine cones and the projective Nullstellensatz

Projective varieties of Nullstellensatz is also hold on projective space. In other words we have bijective from closed sets of  $\mathbb{P}^n$  to homogeneous ideals in  $k[x_0, \dots, x_n]$ .

$$\begin{aligned} \{\text{projective algebraic set in } \mathbb{P}^n\} &\xrightarrow{I} \{\text{homogeneous ideals in } k[x_0, \dots, x_n]\} \\ \{\text{projective algebraic set in } \mathbb{P}^n\} &\xleftarrow{Z} \{\text{homogeneous ideals in } k[x_0, \dots, x_n]\} \end{aligned}$$

We will prove by reducing to the case of  $\mathbb{A}^{n+1}$  making use of affine cones.

**Definition 3.3.1.** A non-empty affine algebraic set  $X \subset \mathbb{A}^{n+1}$  is called a *cone*, if for all  $p = (a_0, \dots, a_n) \in X$  and all  $\lambda \in k$ ,  $\lambda p = (\lambda a_0, \dots, \lambda a_n) \in X$ .

**Example 3.3.2.** The projective variety  $X = Z(x^2 + y^2 - z^2) \subset \mathbb{P}^2$  is called a conic curve.

If  $X \subset \mathbb{P}^n$  is a projective algebraic set the affine cone over  $X$  is  $C(X) := \{(a_0, \dots, a_n) \in \mathbb{A}^{n+1} \mid [a_0, \dots, a_n] \in X\} \cup \{0\}$  is a cone.

**Lemma 3.3.3.** *Let  $X$  be a nonempty projective algebraic set.*

- (1)  $X = Z_p(I)$  for  $I$  is a homogeneous ideal in  $k[x_0, \dots, x_n]$ , then  $C(X) = Z(I)$  is a subset of  $\mathbb{A}^{n+1}$  (in particular affine algebraic set).
- (2)  $I(C(X)) = I_H(X)$ .

**Theorem 3.3.4.** [Projective Nullstellensatz] *Let  $I$  be a homogeneous ideal of  $k[x_0, \dots, x_n]$ , then (1)  $Z_p(I)$  is an empty set if and only if  $I$  contain all forms of degree  $\geq N$  for some  $N$ . (2) If  $Z_p(I)$  is a nonempty set, then  $I(Z_p(I)) = \sqrt{I}$ .*

**Proof.** (1) Let  $X = Z_p(I)$ ,  $X$  be an empty set if and only if  $C(X) = \{0\}$ ,  $C(X) = Z(I) \cup \{0\}$ . Thus  $X$  is an empty set if and only if  $Z(I)$  is an empty set or  $Z(I) = \{0\}$ . By affine Nullsteensatz  $\sqrt{I} = k[x_0, \dots, x_n]$  or  $\sqrt{I} = \langle x_0, \dots, x_n \rangle$ , then  $\langle x_0, \dots, x_n \rangle$  is a subset of  $I(C(X)) = \sqrt{I}$ . Therefore for each  $i = 0, \dots, n$ , there exists  $j_i$  with  $x_i^{j_i} \in I$ . We can take  $N = j_0 + \dots + j_n$ .

(2) Let  $X = Z_p(I)$  be a non-empty set, then  $I_H(X) = I(C(X)) = I(Z_p(I)) = \sqrt{I}$ .

So we get a very similar version of the Nullstellensatz, only the ideal  $\langle x_0, \dots, x_n \rangle$  lead to exceptions. It is called the irrelevant ideal.

**Corollary 3.3.5.**  $I_H$  and  $Z_p$  are mutually inverse bijection between non-irrelevant homogeneous radical ideals  $I \subset k[x_0, \dots, x_n]$  and projective algebraic set  $X \subset \mathbb{P}^n$ . i.e.,

$$\begin{aligned} \{\text{projective algebraic set in } \mathbb{P}^n\} &\xrightarrow{I_H} \{\text{homogeneous ideals in } k[x_0, \dots, x_n]\} \\ \{\text{projective algebraic set in } \mathbb{P}^n\} &\xleftarrow{Z_p} \{\text{homogeneous ideals in } k[x_0, \dots, x_n]\} \end{aligned}$$

**Proposition 3.3.5.** (1) *A projective algebraic set  $X \subset \mathbb{P}^n$  is a projective variety if and only if  $X = Z_p(I)$   $I \subset k[x_0, \dots, x_n]$  is a homogeneous prime ideal.*

(2)  $f \in k[x_0, \dots, x_n]$  is homogeneous and irreducible if and only if  $Z_p(f)$  is irreducible in  $\mathbb{P}^n$ .

**Proof.** (1) Assume  $X$  is reducible. Then  $X = X_1 \cup X_2$  for closed subset  $X_1, X_2$  is a proper subset of  $X$ . Hence  $C(X) = C(X_1) \cup C(X_2)$  is a reducible subset of  $\mathbb{A}^{n+1}$ . Therefore  $I_{N(X)} = I_{C(X)}$  is not a prime ideal.

Assume  $I := I_H(X)$  is not a prime ideal. Then there exists  $f, g$  is in  $k[x_0, \dots, x_n] \setminus I$ , and  $fg$  is in  $I$ . Let  $i, j \in \mathbb{Z}^+$  be minimal with  $f^{(i)}, g^{(j)}$  is not in  $I$ . Subtracting homogeneous component of lower degree of  $f$  and  $g$ . We can assume  $f$  starts in degree  $i$ ,  $g$  starts in degree  $j$ .  $f^{(i)}g^{(j)}$  is homogeneous component of minimal degree in  $fg \in I$ , ( $I$  is homogeneous ideal.) then  $f^{(i)}g^{(j)} \in I$ . Let  $X_1 = Z_p(I \cup f^{(i)}) = Z_p(I) \cap Z(f^{(i)})$ ,  $X_2 = Z_p(I \cup g^{(j)}) = Z_p(I) \cap Z(g^{(j)})$ . Hence  $X_1, X_2 \subsetneq X$ , and  $X = X_1 \cup X_2$ . Therefore  $X$  is reducible.

(2) Follows in the same way as in the affine case.



# Chapter 4

## Equations defining rational curves on a rational surface scroll $S(1,1)$

In this chapter, we would like to focus our interest on the problem to describe the equations defining the rational curves. As a beginning of this problem we study the rational curve  $C_d \subset \mathbb{P}^3$  parameterized as

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

This parametrization of  $C_d$  is a kind of generalization of the rational normal curve  $C \subset \mathbb{P}^3$  of degree 3. Then the curve  $C_d$  is a smooth rational curve of degree  $d$  contained in a smooth rational normal surface scroll  $S(1,1)$ . These investigations enable us to determine the precise shapes of the minimal generators of the homogenous ideal  $I_{C_d}$  of  $C_d$ . The following is our main result.

**Theorem 4.1.1.** *Let  $C_d \subset \mathbb{P}^3$  be a rational curve defined as the parametrization*

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

*where  $d \geq 3$ . Then*

- (1) The curve  $C_d$  is a smooth rational curve of degree  $d$  contained in the rational normal surface scroll  $S(1,1)$ .
- (2) The defining ideal  $I_{C_d}$  of  $C_d$  is minimally generated as following:

$$I_{C_d} = \langle X_0X_3 - X_1X_2, F_{d,1}, F_{d,2}, \dots, F_{d,d-1} \rangle$$

where  $F_{d,i} = X_0^{d-i-1}X_2^i - X_1^{d-i}X_3^{i-1}$  for  $1 \leq i \leq d-1$ .

**Notation and Remark 4.1.2.** (1) Let  $S(1, 1) \subset \mathbb{P}^3$  be the rational normal surface scroll of degree 2. Let  $S = \mathbb{k}[X_0, X_1, X_2, X_3]$  be the homogeneous coordinate ring of  $\mathbb{P}^3$ . Then  $S(1, 1)$  is defined by the quadratic equation  $X_0X_3 - X_1X_2$ . (2) Let  $C \subset \mathbb{P}^3$  be a rational normal curve of degree 3. Then  $C$  can be defined by the parameterization

$$C = \{[s^3(P) : s^2t(P) : st^2(P) : t^3(P)] \mid P \in \mathbb{P}^1\}$$

and the ideal  $I_C$  of  $C$  is generated by the following three quadratic equations:

$$\{X_0X_2 - X_1^2, \quad X_1X_3 - X_2^2, \quad X_0X_3 - X_1X_2\}.$$

Thus  $C$  is contained in the rational normal surface scroll  $S(1, 1)$ .

## 4.1 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

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

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)  $G_{i,1}, G_{i,2}, \dots, G_{i,\ell_i}$  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  $2 \leq i \leq m$ .

## 4.2 Proof of Main Theorem

This section is devoted to proving Theorem . We keep the notations in the previous section. Let  $C_d \subset \mathbb{P}^3$  ( $d \geq 3$ ) be a rational curve defined as the parametrization

$$(0.1) \quad C_d = \{[s^d(P) : s^{d-1}t(P) : st^{d-1}(P) : t^d(P)] \mid P \in \mathbb{P}^1\}.$$

**Lemma 4.2.1.** *Let  $C_d$  be a curve just stated as above. Then  $C_d$  is smooth and of degree  $d$ .*

**Proof.** The case where  $d = 3$  follows from Notation and Remark .(2). Suppose that  $d > 3$ . Then we can see that the parametrization (0.1) comes from the embedding  $\nu_d : \mathbb{P}^1 \rightarrow \mathbb{P}^d$  by

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

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

$$\{[0, 0, 1, 0, \dots, 0, 0], [0, 0, 0, 1, 0, \dots, 0, 0], \dots, [0, 0, \dots, 0, 1, 0, 0]\}.$$

Then  $C_d$  is obtained by the linear projection map  $\pi_{\mathbb{L}} : \tilde{C}_d \rightarrow \mathbb{P}^3$  of  $\tilde{C}_d$  from  $\mathbb{L}$ . Since  $\mathbb{L} \subset \mathbb{P}^r \setminus C_d^2$ , the map  $\pi_{\mathbb{L}}$  is an isomorphism by Notation and Remark .(3). Thus  $C_d$  is a smooth rational curve of degree  $d$ .

**Proposition 4.2.2.** *Let  $C_d$  be as in Lemma . Then the curve  $C_d$  is contained in the rational normal surface scroll  $S(1, 1)$ .*

**Proof.** Consider the parametrization (0.1) of  $C_d$ . Then it is easy to see that the defining ideal  $I_{C_d}$  of  $C_d$  contains the quadratic equation  $X_0X_3 - X_1X_2$  and hence  $C_d$  is a subvariety of  $S := S(1, 1)$  by Notation and Remark .(1).

**Example 4.2.3.** For  $d = 4, 5, 6, 7, 8, 9, 10$ , let  $C_d \subset \mathbb{P}^3$  be curves defined as the parametrization (0.1). For the simplicity, put

$$F_{d,i} = X_0^{d-i-1} X_2^i - X_1^{d-i} X_3^{i-1}$$

for  $4 \leq d \leq 10$  and  $1 \leq i \leq d-1$ . Then by means of the Computer Algebra System Singular [6], the defining ideal  $I_{C_d}$  for  $d = 4, 5, 6, 7, 8, 9, 10$  are respectively minimally generated as followings:

$$(i) \ I_{C_4} = \langle X_0 X_3 - X_1 X_2, F_{4,1}, F_{4,2}, F_{4,3} \rangle,$$

$$(ii) \ I_{C_5} = \langle X_0 X_3 - X_1 X_2, F_{5,1}, F_{5,2}, F_{5,3}, F_{5,4} \rangle$$

$$(iii) \ I_{C_6} = \langle X_0 X_3 - X_1 X_2, F_{6,1}, F_{6,2}, F_{6,3}, F_{6,4}, F_{6,5} \rangle$$

$$(iv) \ I_{C_7} = \langle X_0 X_3 - X_1 X_2, F_{7,1}, F_{7,2}, F_{7,3}, F_{7,4}, F_{7,5}, F_{7,6} \rangle$$

$$(v) \ I_{C_8} = \langle X_0 X_3 - X_1 X_2, F_{8,1}, F_{8,2}, F_{8,3}, F_{8,4}, F_{8,5}, F_{8,6}, F_{8,7} \rangle$$

$$(vi) \ I_{C_9} = \langle X_0 X_3 - X_1 X_2, F_{9,1}, F_{9,2}, F_{9,3}, F_{9,4}, F_{9,5}, F_{9,6}, F_{9,7}, F_{9,8} \rangle$$

$$(vii) \ I_{C_{10}} = \langle X_0 X_3 - X_1 X_2, F_{10,1}, F_{10,2}, F_{10,3}, F_{10,4}, F_{10,5}, F_{10,6}, F_{10,7}, F_{10,8}, F_{10,9} \rangle.$$

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

**Proposition** *Let  $C_d$  be as in Lemma . Then the defining ideal  $I_{C_d}$  of  $C_d$  is minimally generated as following:*

$$I_{C_d} = \langle X_0 X_3 - X_1 X_2, F_{d,1}, F_{d,2}, \dots, F_{d,d-1} \rangle$$

where  $F_{d,i} = X_0^{d-i-1}X_2^i - X_1^{d-i}X_3^{i-1}$  for  $1 \leq i \leq d-1$ .

**Proof.** If  $d = 3$ , then  $C_d$  is a rational normal curve (see Notation and Remark .(2)). So we may assume that  $d \geq 4$ . Put  $M_d = \{X_0X_3 - X_1X_2, F_{d,1}, F_{d,2}, \dots, F_{d,d-1}\}$ . Then since  $C_d \subset S(1,1)$  by Proposition . (1), we can see that  $X_0X_3 - X_1X_2 \in I_{C_d}$ . Also it can be shown that  $F_{d,i}([s^d : s^{d-1}t : st^{d-1} : t^d]) = 0$  for all  $1 \leq i \leq d-1$  as the parametrization (0.1). This shows that  $M_d \subset I_{C_d}$ . Now we will show that  $I_{C_d} = \langle M_d \rangle$  by verifying the three conditions (ii), (iii) and (i) in subsection 2. 2 hold for the set  $M_d$  in tern. For the condition (ii), it suffices to show that  $\{F_{d,i}\}$  are  $\mathbb{K}$ -linearly independent polynomials of degree  $d-1$ . To do this, consider the degree of  $X_0$  in each  $F_{d,i}$  for  $1 \leq i \leq d-1$ . Then one can see that  $F_{d,i}$  for each  $i$  can not be written by a linear combination of the other  $F'_{d,j}$ s.

Let  $\langle M_d \rangle = I \subseteq I_{C_d}$  and.  $Q = X_0X_3 - X_1X_2$ . We claim that  $F_{d,i} \notin \langle Q \rangle$   $1 \leq i \leq d-1$ . Let  $F \in \langle Q \rangle$ , then  $F = (X_0X_3 - X_1X_2) \cdot \sum a_j X_0^{i_0} X_1^{i_1} X_2^{i_2} X_3^{i_3} = \sum a_m X_0^{i_0+1} X_1^{i_1} X_2^{i_2} X_3^{i_3+1} + \sum a_k X_0^{i_0} X_1^{i_1+1} X_2^{i_2+1} X_3^{i_3}$   $i_0, i_1, i_2, i_3 \geq 0, j, m, k \in \mathbb{Z}^+$ ,  $a_j, a_m, a_k \in k \setminus \{0\}$ . That means F has a monomial always has varieties  $X_0, X_3$ . Therefore  $F_{d,i} \notin \langle Q \rangle$   $1 \leq i \leq d-1$  To show that (i) (iii) hold, we use [4, Theorem 4.8] or [5, Theorem 5.1]. In these papers the authors provided the number of minimal generators of the defining ideal  $I_{C_d}$  of  $C_d$ . Indeed one can verity that the number of polynomials in M is same with the number of minimal generators of the defining ideal  $I_{C_d}$  of  $C_d$ .

## References

- [1] W. Fulton, *Algebraic Curves An introduction to Algebraic Geometry*, 2008.
- [2] J.J. Watkins, *Topics in Commutative Ring Theory*, 2007.
- [3] M.F. Atiyah and I.G. Macdonald, *Introduction to Commutative algebra*, 1969.
- [4] S. Giuffrida and Maggioni, *On the resolution of a curve lying on a smooth cubic surface in  $\mathbb{P}^3$*  Trans. Am.Math.Soc 331(1992),181-201.
- [5] W. Lee and E. Park, *On curves lying on a rational normal surface scroll*, submitted.
- [6] M. Decker, G.M. Greuel and H. Schönemann, Singular 3–1–2 – A computer algebra system for polynomial computations. <http://www.singular.uni-kl.de> (2011).
- [7] S. Lang, *Algebra*, 2002.
- [8] T.M. Hungerford, *Algebra*, 1980.
- [9] J. Harris, *Algebraic Geometry A First Course*, 1992.
- [10] K.E. Smith, L. Kahanpää, P. Kekäläinen and W. Traves, *An Invitation to Algebraic Geometry*, 1998.