# Lectures on
# Geometry of Plane Curves
# An Introduction to Algegraic Geometry

ANANT R. SHASTRI
Department of Mathematics
Indian Institute of Technology, Mumbai

Spring 1999

# Contents


1 Introductory Remarks 3

2 Affine Spaces and Projective Spaces 6

3 Homogenization and De-homogenization 8

4 Defining Equation of a Curve 10

5 Relation Between Affine and Projective Curves 14

6 Resultant 17

7 Linear Transformations 21

8 Simple and Singular Points 24

9 Bezout's Theorem 28

10 Basic Inequalities 32

11 Rational Curve 35

12 Co-ordinate Ring and the Quotient Field 37

13 Zariski Topology 39

14 Regular and Rational Maps 43

15 Closed Subspaces of Projective Spaces 48

16 Quasi Projective Varieties 50

17 Regular Functions on Quasi Projective Varieties 51

**18 Rational Functions** **55**

**19 Product of Quasi Projective Varieties** **58**

**20 A Reduction Process** **62**

**21 Study of Cubics** **65**

**22 Inflection Points** **69**

**23 Linear Systems** **75**

**24 The Dual Curve** **80**

**25 Power Series** **85**

**26 Analytic Branches** **90**

**27 Quadratic Transforms:** **92**

**28 Intersection Multiplicity** **94**

# Chapter 1

# Introductory Remarks

Lecture No. 1
$31^{st}$ Dec. 98

The present day algebraic geometry has several aspects to it. Let us illustrate two of the main aspects by some examples:
(i) *Solve geometric problems using algebraic techniques:* Here is an example. To find the possible number of points of intersection of a circle and a straight line, we take the general equation of a circle and substitute for $X$ (or $Y$) using the general equation of a straight line and get a quadratic equation in one variable. Since this equation can have at most two roots, we conclude that there are at most two points of intersection.
(ii) *Determine whether the polynomial $x^2 + y^2 - 1$ can be factored over reals:* We draw a picture of the locus of zeros of the above polynomial and see that the 'curve' has one 'component' only and hence the polynomial cannot be factored.

The examples given above are too simplistic. We happen to know the solution of each of the problem both by purely algebraic as well as purely geometric methods. However, often this may not be the case. Most often, it is algebra which provides the ultimate solution, whereas the geometry suggests the result and sometimes even an approach to a problem. This course is going to be an elementary introduction to bring out these two themes.

In what follows $k$ will denote a field which is infinite. Often, we are working with the field $\mathbb{R}$ or $\mathbb{C}$. However, unless specifically mentioned, the results and proofs will hold in the general case also. We write $k = \bar{k}$ to mean that $k$ is algebraically closed.

In this course, our aim is to introduce some of the important concepts of Algebraic Geometry through the study of plane algebraic curves.

**Definition 1.1** A *plane affine algebraic curve* $C$ is the locus of a polynomial equation

$$F(X, Y) = 0$$

where $F(X, Y) \in k[X, Y]$ is a non constant polynomial.

This simply means that $C$ is the subset of $k^2$ consisting of all points $(x, y)$ such that $F(x, y) = 0$.

The first question that arises to our mind is: Is $C$ non empty? We immediately notice that the answer to this depends very much on the nature of the ground field itself. Fixing an equation, the same question can be considered over larger and larger fields, till the locus becomes non empty. Changing the coefficient fields from smaller to a larger one or vice versa, is another important method in algebraic geometry. The following result is a small step toward the study of curves.

**Theorem 1.1** *Let $k = \bar{k}$ and $F(X, Y)$ be a non constant polynomial. Then the curve $\Gamma := F(X, Y) = 0$, has infinitely many solutions. Also, there are infinitely many points $(x, y) \in k^2$ which are not on the curve.*

**Proof:** Write $F = a_0(X) + a_1(X)Y + \cdots + a_n(X)Y^n$, with $a_i(X) \in k[X], a_n(x) \neq 0,\ n \geq 1$. Choose $x \in k$ such that $a_n(x) \neq 0$. There are infinitely many choices, since $k$ is infinite and a polynomial in 1-variable can have only finitely many solutions. Now since $k = \bar{k}$, there exists $y \in k$ such $F(x, y) = 0$. Also, since there can be only $n$ such solutions there exists $y' \in k$ such that $F(x, y') \neq 0$. ♠

A curve defined over reals may not have any real points. Typical example is

$$X^2 + Y^2 + 1 = 0.$$

Nevertheless, one can often say quite a lot about the points of a curve over the smaller field with the knowledge of points over a larger field. The following lemma illustrates this point.

**Lemma 1.1** The real points of a complex line lie on a real line.

**Proof:** Write

$$L := (a_1 + \imath a_2)X + (b_1 + \imath b_2)Y + (c_1 + \imath c_2) = 0, \tag{1.1}$$

with at least one of the numbers $a_1 + \imath a_2$ and $b_1 + \imath b_2$ is not zero. If $(x, y) \in (\mathbb{R} \times \mathbb{R}) \cap L$, then $(x, y)$ satisfies

$$a_1X + b_1Y + c_1 = 0; \quad a_2X + b_2Y + c_2 = 0.$$

Since, at least one of these two equations defines a genuine real line, we are done. ♠

Observe that, the lemma does not say whether the set of real points of (1.1) is non empty or not.

**Exercise 1.1** Determine when the equation (1.1) has
(i) a unique real point;
(ii) many real points;
(iii) no real points.

**Definition 1.2** We say a polynomial is irreducible if it cannot be factored. Obviously, we should fix the field before making any sense out of this terminology. For, if we enlarge fields, the irreducibility of a polynomial gets affected. For instance, any polynomial in one variable is the product of linear ones over an algebraically closed field. However, it is also clear that a polynomial which is irreducible over a larger field is irreducible over a smaller one also.

**Example 1.1** Take $F(X,Y) = X^2+Y^2-1$ over $\mathbb{C}$. Let us prove that this is irreducible. If not, say $F = F_1F_2$, where $f_i$ are linear polynomials. Therefore the real points of the curve $X^2+Y^2 = 1$ are contained in the union of the two lines $F_1 = 0$ and $F_2 = 0$. Since the real points of these two lines themselves are contained in real lines, by the above lemma, it follows that the unit circle in $\mathbb{R}^2$ is contained in the union of two real lines. But we have seen that a circle and a line can have at most two points whereas there are infinitely many points on the circle. This contradiction proves that $F$ is irreducible over $\mathbb{C}$. We have given a geometrical argument here. You are welcome to write down a purely algebraic proof, which is indeed easier, in this case.

**Exercise 1.2**
(i) Show that the curve $Y^2 - X^2 - X^3 = 0$ is met by any line in at most three points.
(ii) Determine the irreducibility of the above curve over $\mathbb{R}$ as well as over $\mathbb{C}$.
(iii) Determine whether $X^2 + Y^2 + 1$ is irreducible over $\mathbb{C}$.

# Chapter 2

# Affine Spaces and Projective Spaces

Lecture No. 2
$5^{th}$ Jan 99

In the earlier lecture, we studied some properties of plane curves. The plane itself constituted of set of ordered pairs $(x, y)$ of points of the ground field $k$. One can think of this as a 2-dimensional vector space over $k$. However, in geometry, we do not want to specify any point as a special point such as the origin in a vector space. Thus, the notion of *affine space* is introduced. An affine plane over $k$ is nothing but $k^2$ in which we have forgotten which point is the origin. So, we shall also have a different notation for it. Thus the affine plane is denoted by $\mathbb{A}^2_k$. Likewise the $n$-dimensional affine space over $k$ is denoted by $\mathbb{A}^n_k$. When the ground field $k$ is understood, without confusion, we shall use the notation $\mathbb{A}^n$.

Given two plane curves, we would like to know their common points. In particular, we know that generally two distinct lines meet in a point. Of course two distinct points determine a line. These two properties are in a sense dual to each other. However, whereas the second statement is true always, the first statement is not true for so called parallel lines. We wish that parallel lines also met in a point and hence, intuitively say that they meet at a point at infinity. In order to make this intuitive notion concrete, we now introduce the notion of the projective plane. Of course, there are many other motivations for us to introduce this concept. The advantages of this notion are many, as we shall learn in due course.

**Definition 2.1** Consider the Cartesian product $k^{n+1}$ of $(n+1)$-copies of $k$. Remove the point $(0, 0 \ldots, 0)$ from it and define the equivalence relation on the resulting set:

$$(x_0, \ldots, x_n) \sim \lambda(x_0, \ldots, x_n), \quad \forall\ \lambda \in k \setminus \{0\}.$$

Denote the set of equivalence classes by $\mathbb{P}^n_k$. This is called the $n-$dimensional projective space over $k$.

**Remark 2.1**

(i) $\mathbb{P}^n_k$ can be thought of as the space of all lines in vector space $k^{n+1}$, passing through the origin. An element of $\mathbb{P}^k$ is denoted by $[x_0, \ldots, x_n]$.

(ii) We identify $\mathbb{A}^n$ with a subset of $\mathbb{P}^n$ through the map

$$(x_1, \ldots, x_n) \mapsto [1, x_1, \ldots, x_n].$$

(iii) The set of points

$$\{[x_0, x_1, x_2, \ldots, x_n] \in \mathbb{P}^n \ : \ x_0 = 0\}$$

is called the $(n-1)-$plane at infinity. Observe that it can be identified with $\mathbb{P}^{n-1}$. Of course, $\mathbb{P}^0$ is nothing but a singleton. There is only one point in $\mathbb{P}^1$ which does not correspond to $\mathbb{A}^1$ under the mapping given in (ii). This point is called the point at infinity ($\infty$) in $\mathbb{P}^1$. Likewise, we have the 'line at infinity $l_\infty$, in $\mathbb{P}^2$ the plane at $\infty$ $\mathbb{P}^2_\infty$ in $\mathbb{P}^3$ and so on. Thus we see that

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}_\infty.$$

(iv) There are other ways to identify $\mathbb{A}^n$ with a subset of $\mathbb{P}^n$. The most common ones being the co-ordinate inclusions as in the above case:

$$(x_1, x_2, \ldots, x_n) \mapsto [x_1, x_2, \ldots, x_i, 1, x_{i+1}, \ldots, x_n].$$

We shall denote the image of these mappings by $\mathbb{A}^n_i$. It follows that $\mathbb{P}^n = \cup_{i=0}^n \mathbb{A}^n_i$.

# Chapter 3

# Homogenization and De-homogenization

Given a polynomial $f \in k[X_1, \ldots, X_n]$ of degree $d$, the *homogenization $F$ of $f$ through a new variable $X_0$* is defined as follows: Write $f = f_d + f_{d-1} + \cdots + f_1 + f_0$ where, $f_i$ are homogeneous of degree $i$. (We call $f_i$, the $i^{th}$ homogeneous component of $f$.) Then take

$$F(X_0, \ldots, X_n) = f_d + X_0 f_{d-1} + \cdots + X_0^{d-1} + X_0^d f_0.$$

The *de-homogenization* of a homogeneous polynomials $G(X_0, \ldots, X_n)$ with respect to $X_i$ is obtained by simply substituting $X_i = 1$ in $G$. Recall that a polynomial $G$ is homogeneous of degree $d$ if

$$G(\lambda X_0, \lambda X_1, \ldots, \lambda X_n) = \lambda^d G(X_0, X_1, \ldots, X_n)$$

for all $\lambda \in k$. Thus it vanishes on a point $(x_0, \ldots, x_n)$ iff it does so on all $\lambda(x_0, \ldots, x_n)$. Hence, it makes sense to talk about the zero set of a homogeneous polynomial in the projective space.

**Example 3.1** A homogeneous polynomial of degree $d$ in two variables over an algebraically closed field is a product of homogeneous linear factors. Each homogeneous linear polynomial defines a point in the projective space $\mathbb{P}^1$. Of course if one polynomial is a non zero multiple of the other, they define the same zero set in the projective space. Thus a homogeneous polynomial of degree $d$ defines exactly $d$ points on $\mathbb{P}^1$, counted with appropriate multiplicities.

**Example 3.2** Let us determine the intersection points of a curve

$$\Gamma := F(X_0, X_1, X_2) = 0$$

and a line

$$L := a_0X_0 + a_1X_1 + a_2X_2 = 0$$

in $\mathbb{P}^2$. We may assume that $a_2 \neq 0$. And eliminate $X_2$ from the two equations, by putting $X_2 = -\dfrac{a_0X_0 + a_1X_1}{a_2}$ in $F$. This is equivalent to carrying out division of $F$ by the monic polynomial $L_1 = L/a_2$. So, let us say,

$$F(X_0, X_1, X_2) = L_1G + H$$

where $H$ is a polynomial independent of $X_2$. Retaining only the homogeneous components of degree $d$ on either side, it follows that we may assume that $H$ is homogeneous of degree $d$. (Indeed, this is true always, but you need not prove this!) Now it follows that $(x_0, x_1, x_2)$ is a point of intersection of $\Gamma$ and $L$ only if $H(x_0, x_1) = 0$. Conversely, if $H(x_0, x_0) = 0$ then we get a unique point $x_2 = -\dfrac{a_0x_0 + a_1x_1}{a_2}$ such that $[x_0, x_1, x_2]$ is on $\Gamma \cap L$. Therefore, the number of intersection points is in one-to-one correspondence with the solutions of $H(X_0, X_1) = 0$. Since this is homogeneous of degree $d$, it has exactly $d$ roots in $\mathbb{P}^1$ if $k = \bar{k}$. Of course, we have to count these roots with appropriate multiplicities.

# Chapter 4

# Defining Equation of a Curve

Observe that the zero set of any polynomial $F$ and that of $F^n$ are the same. (Later on we shall have devices to distinguish between these.) More generally, we have,

**Theorem 4.1** *Let $k = \bar{k}$, and $\Gamma$ be a plane curve given by $F = 0$, where, $F = cF_1^{r_1}F_2^{r_2}\cdots F_n^{r_n}, c \neq 0, r_i \geq 1$ with each $F_i$ being non constant irreducible and $F_i, F_j$ being non associates for $i \neq j$. Let $G$ be such that $G = 0$ also defines the curve $\Gamma$. Then $G = c'F_1^{s_1}\cdots F_n^{s_n}$ for some $c' \neq 0$, and $s_i \geq 1$.*

In order to understand and prove this theorem, all that we need to know is some algebra. Two elements $x, y$ of a ring $R$ are called *associates* if $x = \lambda y$ for some unit $\lambda$ in the ring $R$. An element $x \in R$ is called *reducible* if there exist $y, z \in R$ which are non units such that $x = yz$. Any element which is not reducible is called *irreducible.* The ring is called a *unique factorization domain* (UFD) if every element in $R$ can be expressed as finite product of irreducible ones unique up to associates and a permutation. An immediate consequence of this is:

**Lemma 4.1** Let $R$ a UFD, and $x \in R$ be irreducible. Then $x$ divides $yz$ implies that $x$ divides at least one of $y$ and $z$.

We shall prove a more primitive result in some sense than the above theorem, viz., assuming $F$ is irreducible and that the zeros of $F$ are contained in the curve $G = 0$ we shall prove that $f$ divides $G$. recall that if $f$ were a linear polynomial, then we already know this result, by simple application of division algorithm or equivalently, eliminating one of the variables. We situation here is somewhat more complicated and needs a subtle handling. The important fact about $k[X_0, X_1, X_2]$ that we need here is that it is a UFD. And the tool is Gauss Lemma. Explicitly, we shall prove:

**Lemma 4.2** Let $F$ be a homogeneous irreducible polynomial of positive degree. Let $G$ is another homogeneous polynomial not divisible by $F$. Consider the three points $[0,0,1],[0,1,0]$ and $[1,0,0]$. Then for each of these points, there are finitely many lines the union of which contains the points of intersection of $F=0$ and $G=0$. In particular, there are only finitely many points common to the curves $F=0$ and $G=0$.

**Proof:** First observe that the gcd of $F$ and $G$ is a unit since $F$ is irreducible and does not divide $G$. Viewing $k[X_0,X_1,X_2]$ as $k[X_0,X_1][X_2]$, i.e., a polynomial ring in one variable $X_2$ over the polynomial ring in the two variables $X_0$ and $X_1$, we pass to the larger ring $k(X_0,X_1)[X_2]$, where, $K=k(X_0,X_1)$ denotes the quotient field of $k[X_0,X_1]$. From Gauss's lemma, it follows that the gcd of $F$ and $G$ is a unit even in this ring. Since $K[X_2]$ is a principle ideal domain, it follows that we can write $1=\alpha F+\beta G$ where $\alpha,\beta\in K$. By clearing the denominators, we get,

$$H(X_0,X_1)=P(X_0,X_1,X_2)F(X_0,X_1,X_2)+Q(X_0,X_1,X_2)G(X_0,X_1,X_2)$$

for some polynomials $H,P$ and $Q$. By retaining only the homogeneous component of maximal degree on either side, we may assume that all these polynomials are homogeneous. Clearly $H(X_0,X_1)=0$ represents a finite set of lines passing through $[0,0,1]$. Similar statement holds for $[1,0,0]$ and $[0,1,0]$. This completes the first part. Now we observe that the three points $[1,0,0],[0,1,0]$ and $[0,0,1]$ are non collinear. Therefore, given a point $Q$ such that $F(Q)=0=G(Q)$, we three lines $L_1,L_2,L_3$ respectively passing through these three points and through $Q$. Since three lines cannot be the same $Q$ is on the intersection of at least two distinct lines. Since such pairs of lines are finite in number, the number of points $Q$ is also finite. ♠

**Remark 4.1** For future use, it is important to observe that the all these lines that we have used are defined over the same field $k$ -there is no need to go to any larger field.

As an immediate corollary, we get

**Lemma 4.3** Let $F,G$ be homogeneous and $F$ irreducible. If $G$ vanishes identically on the curve $F=0$, then $F$ divides $G$.

The theorem now follows from this lemma immediately. This lemma and theorem 4.1 are both true in the affine case also. Moreover, these results are true in higher dimension as well. However, the earlier lemma is not true as stated and needs some modification.

It is interesting to prove the above lemma directly. Observe that we may assume that $deg_{X_2} F > 0$. Let

$$F = a_m X^m + \text{ lower degree terms.}$$

Choose $[x_0, x_1]$ such that $a_m(x_0, x_1)H(x_0, x_1) \neq 0$. Now pick up $x_2$ such that $F(x_0, x_1, x_2) = 0$. Now in the equation, $H = PF + QG$, if we evaluate the two sides at $(x_0, x_1, x_2)$ the LHS does not vanish. Therefore $Q(x_0, x_1, x_2)G(x_0, x_1, x_2) \neq 0$. This gives a direct proof of the above lemma.

**Definition 4.1** Given a curve a $\Gamma$ defined by $F = 0$ where $F = cF_1^{r_1} \cdots F_n^{r_n}$ as above, we say $F_1 \cdots F_n = 0$ as the defining equation of the curve $\Gamma$. It is well defined up to a non zero scalar multiple. Its degree is called the order of $\Gamma$.

**Definition 4.2** A curve $\Gamma$ is said to be *reducible* if $\Gamma = \Gamma_1 \cup \Gamma_2$, where $\Gamma_i$ are both curves not equal to $\Gamma$ itself. A curve which is not reducible is called *irreducible.*

Typical example of a reducible curve is a pair of lines such as given by $XY = 1$. A line is certainly an irreducible curve.

**Theorem 4.2** *Let $\Gamma$ be a curve given by $F = 0$. Then $\Gamma$ is irreducible iff $F = cF_1^r$ for some irreducible polynomial $F_1$, $r \geq 1$ and $c$ is a non zero constant.*

**Proof:** Assume that the defining equation for $\Gamma$ is $F_1 \cdots F_n = 0$, $n \geq 2$. Put

$$\Gamma_1 = \{P \ : \ F_1(P) = 0\}$$

and

$$\Gamma_1' = \{P \ : \ F_2(P) \cdots F_n(P) = 0\}.$$

Since $F_1$ does not divide $F_j, j \neq i$, it follows that $F_1$ vanish completely on $\Gamma_1'$. Hence $\Gamma_1 \not\subset \Gamma_1'$. Likewise, we obtain that $\Gamma_1' \not\subset \Gamma_1$. Since $\Gamma = \Gamma_1 \cup \Gamma_1'$, it follows that $\Gamma$ is reducible.

Conversely, suppose $\Gamma = \Gamma_1 \cup \Gamma_2$ is a decomposition of $\Gamma$. Let $F_i$ be the defining equations of $\Gamma_i$. Then clearly $F_1$ and $F_2$ are non associates. Also, each of the irreducible factors of $F_i$ divide $F$. Hence both $F_1$ and $F_2$ divide $F$. ♠

**Exercise 4.1**

(1) Let $\Gamma_i$ be irreducible curves with defining equations $F_i = 0$. Show that $\Gamma_1 = \Gamma_2$ iff $F_1$ and $F_2$ associates.

(2) Suppose an irreducible curve is contained in the union of two curves. Then, it is contained in at least one of them.

(3) If $\Gamma_i$ are irreducible curves such that $\Gamma_1 \subset \Gamma_2$, then show that $\Gamma_1 = \Gamma_2$.

The following theorem is an immediate consequence of the discussion that we had so far.

**Theorem 4.3** *A curve can be written as a finite union of irreducible ones in a unique way.*

# Chapter 5

# Relation Between Affine and Projective Curves

Let us consider the homogenization and de-homogenization process once again. Given $f \in k[X_1, X_2]$ we shall denote its homogenization through $X_0$ by $F \in k[X_0, X_1, X_2]$. Observe that $X_0$ does not divide $F$. Clearly, the assignment $f \mapsto F$ defines a one-to-one correspondence between degree $d$ polynomials in $X_1, X_2$ and homogeneous polynomials of degree $d$ in $X_0, X_1, X_2$ which are **not** divisible by $X_0$. One checks that
(i) If $h = fg$ then $H = FG$.
(ii) $f$ is irreducible iff $F$ is.
(iii) If $f = f_1^{r_1} \cdots f_n^{r_n}$ is a decomposition of $f$, then $F = F_1^{r_1} \cdots F_n^{r_n}$ is the decomposition of $F$ into homogeneous factors.

**Definition 5.1** Given an affine curve $\gamma$ defined by $f = 0$, its projective completion $\Gamma$ is defined to be the curve in $\mathbb{P}^2$ given by $F = 0$.

Clearly
(iv) Two affine curves $\gamma_1$ and $\gamma_2$ are equal iff their projective completions $\Gamma_1 = \Gamma_2$.
(v) $\gamma$ is irreducible, iff $\Gamma$ is.

**Example 5.1** Consider the hyperbola given by $X_1X_2 = 1$. Its projective completion is given by $X_1X_2 - X_0^2 = 0$. Let us study the real points of this curve. We understand the affine portion of the curve in the $X_1X_2$ plane very well. It has two 'connected components', even though the defining equation is irreducible. This phenomenon defies our intuition! Some explanation may be possible if we study the projective completion.

The line at infinity $X_0 = 0$ intersects this curve at $[0, 0, 1]$ and $[0, 1, 0]$. How does it behave near these two points. To answer this question, we draw the picture of this curve

in the affine plane $X_0X_1$ say. For this purpose, we must now de-homogenize $X_1X_2 - X_0^2$ with respect to $X_2$ and obtain the equation of the parabola $X_1 - X_0^2 = 0$. We could also do this in the affine $X_0X_2$ plane. Now it is not difficult to see that the space of real points of the curve in $\mathbb{P}^2$ is actually connected.(Work it out carefully.) So, after all it is only one single curve.

It follows that it is impossible to give only one branch of the hyperbola by a polynomial equation.

**Exercise 5.1**

(1) Find the points at which the projective completion of each of the following curves meets the line at infinity:

(a) $X^3 - 6X^2Y + 11XY^2 - 6Y^3 + 1 = 0$;

(b) $Y^4 + X^4 + 3Y^2 + X + 1 = 0$;

(c) $1 + X + Y + XY + X^2 + Y^2 = 0$.

(2) Sketch the projective completions of the curves:

(a) $Y - X^3 = 0$; (b) $Y^2 - X^3 = 0$; (c) $X^2 - Y^2 - X^3 = 0$.

(3) Show that there exists two points $P, Q$ in $\mathbb{P}^2_{\mathbb{C}}$ such that the projective completion of every circle in $\mathbb{R}^2$ passes through them. Find these points.

(4) Let $F, G$ be homogeneous in $k[X_0, X_1, X_2]$. Let $deg\, F \geq deg\, G$ and $F(1, X_1, X_2) = G(1, X_1, X_2)$. Show that $F = X_0^s G$ where $s = deg\, F - \deg\, G$.

(5) Show that the determinant of a $n \times n$ matrix whose entries are all variables is irreducible. (Do it for $n = 2$ and $n = 3$ first.)

[**Solution to 5)** We prove a lemma:

**Lemma 5.1** *Let $R$ be an UFD, $f, g \in R$ be such that they have no common factors. Then $Xf + Yg \in R[X, Y]$ is irreducible.*

**Proof:** This $Xf + Yg$ is linear in $X, Y$ one of its factors must be an element of $R$. Now if $r \in R$ divides $Xf + Yg$ going modulo $X$ or $Y$ it follows that $r$ divides both $g$ and $f$ contradiction to the fact that $f$ and $g$ have no common factors. ♠

Repeated application of the above lemma yields that if $f_i$ are irreducible in $R$ then in $R[X_1, \ldots, X_n]$ the element $\sum_{i=1}^n X_i f_i$ is irreducible. Also, it is easily seen that if $c \in R$ is an irreducible element, then so it is in $R[T]$.

Now we complete the proof of 5) by induction on $n$. Assume the statement being true for $n - 1$. Let $X = [X_{ij}]$ be the $n \times n$ matrix. Expand $det\, X$ along the first row to

write

$$det\, X = \sum_j X_{1j} f_{1j}$$

where $f_{1j}$ is the $(1, j)^{th}$ cofactor. By induction it follows that each $f_{ij}$ is irreducible in the polynomial ring

$$R = k[\{X_{ij} \ : \ 2 \leq i \leq n, \ 1 \leq j \leq n\}.$$

Now the proof is completed by appealing to the lemma above.]

# Chapter 6

# Resultant

Lect. No. 3
$7^{th}$ Jan 99

Let us follow the practice of denoting a bunch of variables by a single letter. Thus $X$ would stand for the set of variables $X_1, X_2, \ldots,$ a finite number of them, the actual number being understood by the contest. So, $k[U, V, X]$ denotes the polynomial ring over $k$ in the variables $U_1, U_2 \ldots, V_1, V_2 \ldots, X_1, X_2 \ldots$.

Consider two polynomials,

$$f = U_0 X^n + U_1 X^{n-1} + \cdots + U_n; \quad g = V_0 X^m + V_1 X^{m-1} + \cdots + V_m.$$

Here $f \in \mathbb{Z}[U, X]$, $g \in \mathbb{Z}[V, X]$ where $X$ denotes a single variable, whereas $U$ stands for $U_0, \ldots, U_n$ and $V$ stands for $V_0, \ldots, V_m$. Both $f$ and $g$ may be viewed as elements of $\mathbb{Z}[U, V, X]$.

**Definition 6.1** We define the *resultant* $\mathcal{R}_X(f, g)$ with respect to the variable $X$ to be the determinant of the $(m+n) \times (m+n)$ matrix

$$M_X(f,g) = \begin{bmatrix} U_0, & U_1, & \cdots & \cdots & \cdots & \cdots, & U_n, & 0, & \cdots & \cdots & \cdots & 0 \\ 0, & U_0, & \cdots & \cdots & \cdots & \cdots, & U_{n-1}, & U_n, & \cdots & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & \cdots & \cdots & \cdots & \cdots & U_0, & U_1, & \cdots & \cdots & \cdots & U_{n-1}, & U_n \\ V_0, & V_1, & \cdots & \cdots & \cdots & \cdots & V_m, & 0, & \cdots & \cdots & 0, & 0 \\ 0, & V_0, & \cdots & \cdots & \cdots & \cdots & V_{m-1}, & V_m, & 0, & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0, & \cdots & \cdots & \cdots & \cdots & V_0, & V_1, & \cdots & \cdots & \cdots & V_{m-1}, & V_m \end{bmatrix}$$

**Remark 6.1** Observe that there are $m$ rows of $U_i$'s followed by $n$ rows of $V_j$'s in the matrix $M$. The following observations are immediate.
(i) $\mathcal{R}_X(f,g) \in \mathbb{Z}[U,V]$, with each coefficient equal to $\pm 1$.
(ii) $\mathcal{R}_X(f,g)$ is homogeneous of degree $m$ in the variables $U$. This is easily seen by replacing $U_i$ by $\lambda U_i$ and observing that $\lambda$ can be pulled out of the first $m$ rows. Likewise it is homogeneous of degree $n$ in the variables $V$.
(iii) One of the monomials is $U_0^m V_m^n$. (Look at the main diagonal.)

**Lemma 6.1** There exist $P, Q \in \mathbb{Z}[U,V,X]$ such that

$$Pf + Qg = \mathcal{R}_X(f,g).$$

**Proof:** Let $C_{ij}$ denote the cofactors of $M_X(f,g)$. Take

$$P = C_{1,m+n}X^{m-1} + C_{2,m+n}X^{m-2} + \cdots C_{m,m+n};$$

and

$$Q = C_{m+1,m+n}X^{n-1} + \cdots + C_{m+n.m+n}$$

and verify the required identity.

<u>Alternatively,</u> in the matrix $M$, multiply the $j^{th}$ column by $X^{m+n-j}$ for all $j \leq m+n-1$ and add them to the last column. Now observe that the first $m$ entries in last column are multiples of $f$ whereas the remaining ones are multiples of $g$. Now expand for the determinant along the last column. ♠

**Corollary 6.1** Suppose $\phi : \mathbb{Z}[U,V] \longrightarrow R$ be a ring homomorphism. Let us denote the induced ring homomorphism $\mathbb{Z}[U,V][X] \longrightarrow R[X]$ also by $\phi$. Assume that $\phi(f)$ and $\phi(g)$ have a common root in $R$. Then $\mathcal{R}_X(\phi(f), \phi(g)) = 0$.

**Proof:** Observe that whether you substitute first for the variables in the matrix and then take the determinant or first take the determinant and then substitute for the variables, the two results are the same. Thus,

$$\mathcal{R}_X(\phi(f), \phi(g)) = \phi(\mathcal{R}_X(f,g)) = \phi(Pf + Qg) = \phi(P)\phi(f) + \phi(Q)\phi(g).$$

Now evaluate this last expression at the common root $X = x \in R$. ♠

We shall now proceed toward a proof of a converse to the above corollary. Let now $T$ and $S$ be any two sets of distinct variables. Consider the polynomials

$$F(U_0, T, X) = U_0(X - T_1)\cdots(X - T_n);\ G(V_0, S, X) = V_0(X - S_1)\cdots(X - S_m).$$

If $\sigma_{i,r}$ denotes the elementary symmetric function of degree $i$ in $r$ variables, then we can rewrite

$$F = U_0X^n + U_1X^{n-1} + \cdots + U_n; \quad G = V_0X^m + V_1X^{m-1} + \cdots + V_m$$

with

$$U_i = (-1)^i U_0 \sigma_{i,n}(T), i > 0; \quad V_j = (-1)^j V_0 \sigma_{j,m}(S).$$

Observe that $F$ and $G$ are now elements of $\mathbb{Z}[T, S, X]$.

**Theorem 6.1** *With $F$ and $G$ etc. as above we have,*

$$\mathcal{R}_X(F, G) = U_0^m V_0^n \prod_{\substack{1\le i\le n \\ 1\le j\le m}} (T_i - S_j) = V_0^n \prod_{i=1}^{n} G(T_i) = (-1)^{mn} U_0^m \prod_{j=1}^{m} F(S_j). \tag{6.1}$$

**Proof:** The second and third equalities follow directly from the definition of $F$ and $G$. So, let us prove the first equality. Temporarily, write $\mathcal{R}_X(F, G) = \mathcal{R}$ and let $\mathcal{S}$ denote the second term in the above formula. Since the first $m$ rows of $M(F, G)$ have a common factor $U_0$, it follows that $U_0^m$ divides $\mathcal{R}$. Likewise $V_0^n$ also divides $\mathcal{R}$. For a fixed $(r, s)$, consider the ring homomorphism

$$\phi : \mathbb{Z}[T, S] \longrightarrow \mathbb{Z}[T_1, \ldots, \widehat{T_r}, \ldots T_n; S]$$

defined by

$$\phi(T_i) = T_i, \quad i \neq r; \quad \phi(T_r) = S_s; \quad \phi(S_j = S_j, \ \forall\ j.$$

Then the polynomials $\phi(F)$ and $\phi(G)$ have a common root. Hence $\phi(\mathcal{R}) = 0$. This is the same as saying that $\mathcal{R}$ belongs to the ideal generated by $T_r - S_s$ in $\mathbb{Z}[T, S]$. Since this is true for all pairs $(r, s)$, we have proved that $\mathcal{S}$ divides $\mathcal{R}$. To complete the proof, we use the second and third equalities. Observe that $\mathbb{Z}[U, V, X] \subset \mathbb{Z}[T, S, X]$ and we can think of $F, G$ as elements of $\mathbb{Z}[U, V, X]$. Now, since $F$ is homogeneous linear in $U$ each of $F(S_j)$ are also so. Hence their product is homogeneous of degree $m$ in $U$. Therefore $\mathcal{S}$ is homogeneous of degree $m$ in $U$. Likewise, it is homogeneous of degree $n$ in $V$. Since this property is true for $\mathcal{R}$ also, it follows that $\mathcal{R}$ is a constant multiple of $\mathcal{S}$. Finally to see that this constant is equal to 1, we compare the coefficients of $U_0^m V_m^n$ on either side. ♠

**Theorem 6.2** *Let $R$ be a domain and $f, g \in R[X]$. Then $\mathcal{R}_X(f, g) = 0$ iff they have a common root in some ring $R' \supset R$.*

**Proof:** Let the degree of $f$ and $g$ be $n$ and $m$ respectively, with the coefficient of the top degree terms being $a_0, b_0$ respectively. Let $K$ be a field which contains all roots $t_1, \ldots, t_n$ of $f$ and $s_1, \ldots, s_m$ of $g$. Let $\phi : \mathbb{Z}[U, V] \longrightarrow K[t, s]$ be the ring homomorphism such that

$$\phi(U_i) = \text{ coefficient of } X^{n-i} \text{ in } f$$

and

$$\phi(V_j) = \text{ coefficient of } X^{m-j} \text{ in } g.$$

Then, in $K[t, s][X]$, we have, $\mathcal{R}_X(f, g) = \phi(\mathcal{R}_X(F, G))$ which is equal to $a_0^m b_0^n \prod(t_i - s_j)$. Now, the result follows easily. ♠

**Remark 6.2** *The special case when $g = f'$ is of utmost interest. Then the above theorem gives the well known criterion for a polynomial to have a repeated root. The* discriminant *$\Delta(f)$ is defined by*

$$\Delta(f) = (-1)^{n(n-1)/2} \prod_{i \neq j} (t_i - t_j).$$

*The following theorem is immediate.*

**Theorem 6.3** $\mathcal{R}_X(f, f') = (-1)^{n(n-1)/2} a_0^{2n-2} \Delta(f)$.

**Proof:** We have, $\mathcal{R}_X(f, f') = a_0^{n-1} \prod_{i=1}^n f'(t_i)$. Since

$$f = a_0(X - t_1) \cdots (X - t_n),$$

it follows that

$$f' = a_0(\sum_i (X - t_1) \cdots \widehat{(X - t_i)} \cdots (X - t_n)).$$

Therefore, $f'(t_i) = a_0(t_i - t_1) \cdots \widehat{(t_i - t_i)} \cdots (t_i - t_n)$. The result follows. ♠

**Exercise 6.1**

(1) Compute the discriminants of

(i) $a_0X^2 + a_1X + a_2$. (ii) $a_0X^3 + a_1X^2 + a_2X + a_3$.

(2) Show that $\mathcal{R}_X(F_1F_2; G) = \mathcal{R}_X(F_1, G)\mathcal{R}_X(F_2, G)$.

# Chapter 7

# Linear Transformations

Lect. No. 4
$12^{th}$ Jan 99

Consider $A \in GL(3,k)$ where $GL(3,k)$ denotes the group of all invertible $3 \times 3$ matrices with entries in $k$. The action of $A$ on $k^3$ defines an action on $\mathbb{P}^2$ in an obvious way. Moreover, for any non zero element $\lambda \in k$ $\lambda A$ has the same action on $\mathbb{P}^2$ so that we may treat $A$ and $\lambda A$ as equivalent. These equivalence classes are called '*projective linear transformations* or simply as *linear transformations on* $\mathbb{P}^2$. The set of these equivalence classes is denoted by $\mathbb{P}GL(3,k)$. Check that the group operation on $GL(3,k)$ goes down to define a group operation on $\mathbb{P}GL(3,k)$ also.

$GL(3,k)$ also acts on the set of homogeneous polynomials in three variables over $k$. However, we carefully choose this action defined as follows: First of all, we are treating element of $k^3$ as column vectors and then take a $3 \times 3$ matrix $A = ((a_{ij}))$ to operate on it by left multiplication. This action is then carried onto elements of $\mathbb{P}^2$ as well. On the other hand, we treat a polynomial as a function on $k^3$ and define $AP := P \circ A^{-1}$. Verify that this defines an action. [ i.e., $B(AP) = (BA)P$, etc.] Also, this action is the same as substituting for $X_0, X_1, X_2$ respectively the linear homogeneous polynomials $\sum_j a_{0j}X_j, \sum_j a_{1j}X_j, \sum_j a_{2j}X_j$.

The advantage of this action is that if $C$ is a curve defined by a homogeneous polynomial $F = 0$, then for any $A \in GL(3,k)$, $AC$ is the curve defined by $AF = 0$ viz., $F \circ A^{-1} = 0$. In this sense, the two actions of $GL(3,k)$ are compatible. Obviously, several geometric properties of the curves are preserved under this action. In particular, irreducibility, associateship, coprimeness, and degree of homogeneous polynomials are preserved. Likewise the order of a curve, i.e., the degree of a minimal defining equation is also preserved.

**Definition 7.1** We say a set of points $S$ in $\mathbb{P}^2$ is in general position, if no three points of $S$ are collinear.

**Theorem 7.1** *Given two sets of four points $\{a_0, a_1, a_2, a_3\}$ and $\{b_0, b_1, b_2, b_3\}$ in general position, there exists a unique projective linear transformation $\phi$ sending $a_i$ onto $b_i$.*

**Proof:** We may assume that $a_0 = [1,1,1], a_1 = [1,0,0], a_2 = [0,1,0], a_3 = [0,0,1]$. Pick up representative points $B_i$ in $k^3$ for $b_i$ and form the matrix $A = (B_1, B_2, B_3)$ where $B_i$ are treated as columns of size 3. Clearly, $Aa_i = b_i, i = 1,2,3$. So, we try to modify $A$ so that $Aa_0 = b_0$. Now observe that since $B_1, B_2, B_3$ have to be linearly independent ($b_1, b_2, b_3$ are non collinear), it follows that a representative for $b_0$ can be written as $\sum_1^3 \lambda_i B_i$. Now each $\lambda_i$ are non zero, for otherwise, $b_0$ will be collinear with two other points in $\{b_1, b_2, b_3\}$. Therefore, we can take $\phi = (\lambda_1 B_1, \lambda_2 B_2, \lambda_3 B_3)$. Then clearly, $\phi(a_i) = b_i$ for $i = 0,1,2,3$. The uniqueness of $\phi$ as an element of $\mathbb{P}GL(3,k)$ is clear. ♠

**Remark 7.1**
(1) We can now define an affine transformation to be a projective transformation, which preserves the affine subspace $\mathbb{A}^2_0$. This condition is the same as saying that the line at infinity $X_0 = 0$ is preserved. Such transformations can be represented by matrices $A = ((a_{ij}))$, where, $a_{01} = a_{02} = 0$. It is straight forward to check that a mapping $\phi : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ is an affine transformation, iff $\phi = \mathbf{v} + L$ where $L$ is a linear isomorphism and $\mathbf{v}$ is a fixed 2-vector. (Ex. Write down the expressions for $\mathbf{v}$ and $L$ in terms of entries of $A$.
(2) Projective linear transformations can be used to simplify the study of the curves by suitably choosing our co-ordinates. This will be exploited in what follows to a large extent. As a beginning let us prove the following:

**Theorem 7.2** *All irreducible conics in $\mathbb{P}^2_{\mathbb{C}}$ are equivalent under projective linear transformations.*

**Proof:** Let $\Gamma$ be an irreducible conic. First choose three distinct points on $\Gamma$ which are non collinear and map them to $[1,0,0], [0,1,0]$ and $[0,0,1]$ respectively. Thus without loss of generality we may assume that $\Gamma$ passes through these three points. If $F = 0$ is the defining quadratic, it follows that it does not involve ther terms $X_1^2$ and $X_2^2$. Therefore

$$F = c_0 X_1 X_2 + c_1 X_0 X_2 + c_2 X_0 X_1.$$

Observe that $c_i \neq 0$ for otherwise $F$ will have a non trivial factor. Now consider the transformation $X_i' = X_i/c_i,\ i = 0, 1, 2$. Thus, starting with an arbitrary irreducible curve we have projectively transformed it onto the curve

$$X_1X_2 + X_0X_2 + X_0X_1 = 0.$$

This completes the proof. ♠

**Exercise 7.1**

(1) Recall that a homogeneous quadratic polynomial $f$ in three variables can be represented by a $3 \times 3$ symmetric matrix $M_f = ((m_{ij}))$, defined by

$$m_{ij} = \begin{cases} \text{coeffecient of } X_iX_j/2 \text{ in f} & \text{if} \quad i \neq j \\ \text{coefficient of } X_i^2 \text{ in f} & \text{if} \quad i = j. \end{cases}$$

One obtains $f$ from $M_f$ by simply taking $(X_0, X_1, X_2)M_f(X_0, X_1, X_2)^t$. Under a projective linear transformation $A$, how does the corresponding matrix change? Show that $f$ is irreducible iff the rank of $M_f$ is 3.

(2) Let $k = \bar{k}$. Given two projective curves $\Gamma$ and $\Delta$ in $\mathbb{P}^2$ having no common components, and a point $P \in \mathbb{P}^2$, show that $\Gamma \cap \Delta$ is contained in the union of finitely many lines passing through $P$. From this deduce that $\Gamma \cap \Delta$ is finite.

# Chapter 8

# Simple and Singular Points

Lect. No. 5
$14^{th}$ Jan 99.

Let $F(X_0, X_1, X_2)$ be a homogeneous polynomial representing a plane curve $\Gamma$. Let $P, Q \in \mathbb{P}^2$ be any to points. Then the line joining $P$ and $Q$ is parameterized by $\lambda \mapsto P + \lambda Q$, (except for the point $Q$). How to obtain the points of intersection of this line with the curve $\Gamma$? We shall always assume that $Q$ does not belong to $\Gamma$. So, we simply substitute the co-ordinates of this parameterization into $F$ obtain an equation in the variable $\lambda$ and solve for $\lambda$. If $\lambda_i$ is such a solution, then clearly, $P + \lambda_i Q$ is a point on the curve and vice versa. So, write $F(P + \lambda Q) = \sum_{j=0}^{d} f_j(P, Q)\lambda^j$ where $f_i(P, Q) \in k$. Observe that $f_j$ are actually polynomial functions of the variables which are co-ordinates of $P$ and $Q$ (i.e., in all six variables.) They are homogeneous in $P$ and $Q$ separately.
(i) Suppose now that $P \in \Gamma$. Since this corresponds to the value $\lambda = 0$, it follows that $f_0(P, Q) = 0$. From now onward, we shall fix $P \in \Gamma$ and therefore consider $f_i$ etc. as polynomials in $Q$ only.
(ii) Write $Q = [Q_0, Q_1, Q_2]$. Put $G(\lambda) = F(P + \lambda Q)$. Use chain rule to see that

$$f_1(Q) = Q_0 \frac{\partial F}{\partial X_0}(P) + Q_1 \frac{\partial F}{\partial X_1}(P) + Q_2 \frac{\partial F}{\partial X_2}(P).$$

It follows that this polynomial is identically zero iff

$$\frac{\partial F}{\partial X_0}(P) = 0; \ \frac{\partial F}{\partial X_1}(P) = 0; \ \frac{\partial F}{\partial X_2}(P) = 0.$$

(iii) Further, suppose that $f_j(Q) \equiv 0, 0 \leq j \leq s - 1$ and $f_s(Q) \not\equiv 0$ as polynomials in $Q$. We say $P$ is a *simple point* of $\Gamma$ if $s = 1$. Otherwise, $P$ is called a *multiple point* or *singular point.* In any case, $s$ is called the *multiplicity* of $P$ on $\Gamma$ or the multiplicity of $\Gamma$ at $P$ and we write $\mu(\Gamma, P) = s$. If every point on a given curve is simple then we say

that the curve is *smooth* or *non singular*.
(iv) Now consider a special point $Q$. What happens if $f_j(Q) = 0$ for all $j$?. This is the same as saying that for all $\lambda$, $F(P + \lambda Q) = 0$ and hence the line is a component of the curve $\Gamma$. We are interested in those lines which are not components of $\Gamma$ and hence we must have that for point $Q$ on such lines $f_j(Q)$ is not zero for some $j$. Let $t$ be the least such that $f_t(Q) \neq 0$. We call $t$ to be the *intersection multiplicity* of $\Gamma$ and the line

$$L_{PQ} := \lambda \mapsto P + \lambda Q$$

at the point $P$ and write $i(\Gamma, L_{PQ}; P) = t$. Clearly this number is greater than or equal to the multiplicity $\mu(\Gamma; P)$ of the curve $\Gamma$ at $P$. Observe that as we vary the point $Q$ we obtain all the lines passing through $P$. Thus for any line $L$ passing through $P$, which is not a component of the curve $\Gamma$, we have,

$$i(\Gamma, L; P) \geq \mu(\Gamma, P).$$

(v) We say a line through $P$ is a *tangent* to $\Gamma$ if $i(\Gamma, L; P) > \mu(\Gamma; P)$. For instance, if $P$ is a smooth point then $L$ is a tangent at $P$ iff $i(\Gamma, L; P) > 1$. This is the same as saying that $Q$ satisfies the linear equation $f_1(Q) = 0$. Therefore, there is only one tangent line and that is given by $f_1(Q) = 0$. As seen in (ii) above, the equation of the tangent line is

$$\frac{\partial F}{\partial X_0}(P)X_0 + \frac{\partial F}{\partial X_1}(P)X_1 + \frac{\partial F}{\partial X_2}(P)X_2 = 0.$$

We shall consider the case when $P$ is a multiple point a little later.
(vi) If we know the point $P$ before hand, in order to study the multiplicity behavior etc. at $P$, we may assume, by making a linear change of coordinates, that $P = [1, 0, 0]$. Further, we may also assume that the line at infinity is not a component of $\Gamma$ and hence pass into the affine space by de-homogenizing with respect to $X_0$. Thus we have to study a polynomial $f(X, Y)$ in two variables and without a constant term. Also, we can now substitute $y = mx$ in $f(x, y)$ to determine $s$. It turns out that $s$ is the order of $X$ in $f(X, mX)$. This is the same as the degree of the non zero homogeneous component $f_s$ of $f(X, Y)$ of the least degree. In particular, $(0, 0)$ is a simple point iff $f_1 \neq 0$. Once again, for special values of $m$, the least $t$ for which the coefficient of $X^t$ is non zero will be equal to $i(\Gamma, L_m; (0, 0))$ where $L_m$ denotes the line with slope $m$.
(vii) Now suppose $\mu(\Gamma, P) > 1$. Assume that $L_m$ is a tangent to $\Gamma$ at $P$. It follows that $f_s(X, mX) = 0$. Thus the tangent lines to $\Gamma$ at the origin $P$ have the slope given by the solution of the equation $f_s(X, mX) = 0$. Of course, this does not include the case of the curve $X = 0$ itself, which may be reflected in the fact that if we write

$f_s(X, mX) = \alpha(m)X^s$ then the degree of $\alpha$ in $m$ may not be less than $s$. This is same as saying that $X$ itself is a factor of $f(X, Y)$. All this is resolved easily by simply observing that $f_s(X, Y)$ being a homogeneous polynomial, factors into linear ones, which in turn define the equations of various tangent lines to the curve at the origin. Thus, writing

$$f_s(X, Y) = \prod_{j=1}^{s} (a_j X + b_j Y)$$

the tangent lines at $P$ are given by $a_j X + b_j Y = 0, \quad 1 \leq j \leq s$. In general, there are $s$ tangents to the curve at a point of multiplicity $s$. It may happen that some of them are repeated.

**Example 8.1**

(1) Let us find the intersection points of $25X_0^2 - X_1^2 - X_2^2 = 0$ and the line joining $P = [1, 7, 1], Q = [1, -1, 7]$. Putting $X_0 = 1+\lambda, X_1 = 7-\lambda, X_2 = 1+7\lambda$ in the equation, we get,

$$25(1 + \lambda)^2 - (7 - \lambda)^2 - (1 + 7\lambda)^2 = 0.$$

We see that $\lambda = 1$. Thus $[1, 3, 4]$ is the only point of intersection. We would expect that a line should intersect a quadratic in two points. This is reflected in the fact that $\lambda = 1$ is a double root of the equation. Verify that the point $[1, 3, 4]$ is a smooth point. (Indeed the curve itself is smooth). Therefore the line is a tangent to the curve. Let us make a projective transformation $X_0' = X_0, X_1' = X_1 + 3X_0, X_2' = X_2 + 4X_0$. Under this, the point $[1, 3, 4]$ goes to $[1, 0, 0]$ and the equation of the curve becomes

$$X_1^2 + 6X_0X_1 + X_2^2 + 8X_0X_2 = 0.$$

Since $X_0$ is not a factor of this, we can now de-homogenize this to obtain the affine equation

$$X^2 + 6X + Y^2 + 8Y = 0.$$

Clearly, the tangent line is given by $3X + 4Y = 0$. Upon substituting $Y = -3X/4$, we see that the quadratic term does not vanish. Hence the intersection multiplicity is equal to 2.

(2) Consider the curve $\Gamma := X_0^4 + X_1^4 + X_2^4 = 0$. Let us show that every point on this curve is simple. Let $P = [P_0, P_1, P_2]$ be a point on the curve. For a general point $Q = [Q_0, Q_1, Q_2]$, putting $(X_0, X_1, X_2) = P + \lambda Q$ we get

$$(P_0 + Q_0)^4 + (P_1 + Q_1)^4 + (P_2 + Q_2)^4 = 0.$$

Upon simplification, this becomes

$$(4\sum_i P_i^3 Q_i)\lambda + \text{ higher degree terms in } \lambda.$$

Therefore $s = 1$ and hence $P$ is a simple point.

# Chapter 9

# Bezout's Theorem

Lect. No. 6
$19^{th}$ Jan 99 We have seen that any two distinct lines meet in a sinlge point. We have also seen that a line will meet a curve of degree $n$ in $n$ points, counted appropriately. So, if a curve of degree $m$ is union of $m$ lines then it would meet any other curve in $mn$ points. Based on these observations we could make a guess for a formula for the number of points of intersection of two curves and arrive at the famous classical theorem:

**Theorem 9.1** *Let $\Gamma$ and $\Delta$ be two projective plane curves of degree $n$ and $m$ respectively. Suppose that they do not have any common components. Then there are at most $mn$ points common to both the curves. If $k = \bar{k}$ then there are exactly $mn$ points, counted with appropriate multiplicities.*

**Proof:** If we assume $k = \bar{k}$ and prove the latter part, the former part follows automatically. We know that $\Gamma \cap \Delta$ is finite. Therefore, we can only draw a finitely many lines through pairs of points of $\Gamma \cap \Delta$. Thus we can choose $P \in \mathbb{P}^2$ which does not lie on any of these lines, and declare co-ordinates for $\mathbb{P}^2$ such that $P = [0, 0, 1]$. It follows that if $F$ and $G$ are the defining polynomials for $\Gamma$ and $\Delta$ then
$F(X_0, X_1, X_2) = a_0(X_2^n + a_1(X_0, X_1)X_2^{n-1} + \cdots + a_n(X_0, X_1))$
$G(X_0, X_1, X_2) = b_0(X_2^m + b_1(X_0, X_1)X_2^{m-1} + \cdots + b_m(X_0, X_1))$
with $a_0 \neq 0 \neq b_0$ and each $a_i, b_i$ homogeneous of degree $i$. Therefore, the resultant of $F$ and $G$ is of the form

$$\mathcal{R}_{X_2}(F, G) = a_0^m b_0^n H(X_0, X_1).$$

We claim that $H$ is homogeneous of degree $mn$. To see this observe that if $M = ((m_{ij}))$ is the resultant matrix $M_{X_2}(F, G)$ then each $m_{ij}$ is either 0 or we have

$$deg\, m_{ij} = \begin{cases} j - i & \text{for } i \leq m \\ j - i + m & \text{for } i \geq m + 1. \end{cases}$$

Therefore the degree of each monomial which occurs in $det\,((m_{ij}))$ is equal to

$$\sum_{i=1}^{m+n} (\sigma(i) - i) + mn,$$

where $\sigma$ is some permutation of $\{1, 2, \ldots, m + n\}$. This is clearly equal to $mn$.

Why $H$ is non zero? For otherwise, for every $(x_0, x_1) \in k^2$, there would exist $x_2 \in k^2$ such that $[x_0, x_1, x_2]$ is in $\Gamma \cap \Delta$ contradicting the finiteness of this set. So, set $H = \prod_{j=1}^{r}(x_{1j}X_0 - x_{0j}X_1)^{s_j}$ where $s_j \geq 1$, be the factorization of $H$ into linear factors with $x_{ij} \in k$. Clearly $\sum_1^r s_j = mn$ and $1 \leq r \leq mn$. It follows that for each $1 \leq j \leq r$, there exists at least one $x_{2j} \in k$ such that $P_j = [x_{0j}, x_{1j}, x_{2j}] \in \Gamma \cap \Delta$. If there is one more such $x'_{2j}$ say, then it is seen that both points $P_j = [x_{0j}, x_{1j}, x_{2j}], P'_j = [x_{0j}, x_{1j}, x'_{2j}]$ are on a line passing through $P$. This contradicts our choice of $P$ and hence we conclude that for each $i$ there is precisely one point $P_i$ on $\Gamma \cap \Delta$.

Finally, it is clear that we should count $P_i$ with multiplicity $s_i$. With this definition of multiplicity, the proof of Bezout's theorem is complete!

The only (and a serious one at that) objection that we have against this proof is that the definition of multiplicity should be shown to be independent of the choice of co-ordinates. Thus, our task is to define the intersection multiplicity of a common point of the two curves properly.

**Definition 9.1** Let $\Gamma, \Delta$ be any two projective plane curves. We say, $\Gamma, \Delta$ are in permissible position if $[0, 0, 1]$ is not in $\Gamma \cap \Delta$ and not on any line joining two distinct points of $\Gamma \cap \Delta$. We also say that a co-ordinate system chosen in this way, is a permissible co-ordinate system for the pair of curves $\Gamma, \Delta$.

If we define $i(\Gamma, \Delta; P_j) = s_j$ where $s_j$ is defined as above, we then have to show that $s_j$ are independent of such a co-ordinate choice. Explicitly, suppose $A$ is a projective linear transformation, which takes the first permissible co-ordinate system to the second. We should show that $i(A\Gamma, A\Delta; AP_j) = s_j$. Thus we consider $\mathcal{R}_{X_2}(FA^{-1}, GA^{-1})$ and its factorization into linear factors. Since set theoretically, it is obvious that $AP_j$ are in the intersection of $A\Delta$ and $A\Gamma$, it follows that

$$\mathcal{R}_{X_2}(FA^{-1}, GA^{-1}) = \prod_{j=1}^{r}(x'_{1i}X_0 - x'_{0i}X_i)^{s'_j}$$

where, $A[x_{0j}, x_{1j}, x_{2j}] = [x'_{0j}, x'_{1j}, x'_{2j}]$. It remains to prove that $s_j = s'_j$ for all $1 \leq j \leq r$.

We now use one of the strong tools in algebraic geometry. We take a large field $K$ containing $k$, prove that the result is true there and come back and see that it implies the result in $k$ as well. This time $K$ is the algebraic closure of the rational function field $k(L)$ where $L$ denotes a bunch of nine variables written in a $3 \times 3$ array:

$$L = \begin{pmatrix} L_{00} & L_{01} & L_{02} \\ L_{10} & L_{11} & L_{12} \\ L_{20} & L_{21} & L_{22} \end{pmatrix}.$$

The idea is to think of $L$ (why have another notation?) as an invertible $3 \times 3$ matrix over this field and hence a projective linear transformation on $\mathbb{P}^2_K$. Also, we would like to consider $\mathcal{R}_{X_2}(FL^{-1}, GL^{-1})$ over $K$. First of all observe that the same equation $F = 0$ defines a curve $\Gamma_K$ in $\mathbb{P}^2_K$ such that $\Gamma_K \cap \mathbb{P}^2_k = \Gamma$ etc. Crucial to our argument is the result:

**Lemma 9.1** $\Gamma_K \cap \Delta_K = \Gamma \cap \Delta$.

**Proof:** It is enough to prove that $\Gamma_K \cap \Delta_K \subset \Gamma \cap \Delta$. Recall that while proving that the intersection of two curves having no common component is a finite set, we had actually proved that given any point $Q \in \mathbb{P}^2$, there exist a finite set $S_i$ of lines passing through $Q$ such that $\Gamma \cap \Delta$ is contained in the union of these lines, defined over $k$ itself. If we take three non collinear points, $Q_1, Q_2, Q_3$ in $\mathbb{P}^2$, then each point $Z \in \Delta_K \cap \Gamma$ belongs to the intersection two distinct lines in $\mathbb{P}^2_K$ which are any way defined over $k$ itself. Hence the unique point of intersection of these two lines viz. $Z$ belongs to $\mathbb{P}^2_k$. This proves $\Delta_K \cap \Gamma_K \subset \mathbb{P}^2_k$. The rest of the argument is easy. ♠

Next we need:

**Lemma 9.2** $\Delta_K$ and $\Gamma_K$ are in permissible position.

**Proof:** Clearly $[0, 0, 1] \notin \Delta_K \cap \Gamma_K$. If $Q_1, Q_2$ are any two points of $\Gamma_K \cap \Delta_K$, then by the above lemma, they are points of $\mathbb{P}^2_k$ and hence the equation of the line passing through them will be defined over $k$. This violates the permissibility of $\Gamma$ and $\Delta$. ♠

We are now in a position to study $\mathcal{R}_{X_2}(FL^{-1}, GL^{-1})$ over the field $K$. Observe that $\{LP_j : 1 \leq j \leq r\}$ are the only points of intersection of $FL^{-1} = 0$ and $GL^{-1} = 0$. Therefore,

$$\mathcal{R}_{X_2}(FL^{-1}, GL^{-1})$$
$$= \lambda \prod_{j=1}^{r} [X_1(L_{00}x_{j0} + L_{01}X_{j1} + L_{02}x_{j2}) - X_0(L_{10}x_{j0} + L_{11}X_{j1} + L_{12}x_{j2})]^{t_j} \qquad (9.1)$$

where $\lambda = \dfrac{q(L)}{det\, L)^u}$ for some polynomial $q(L)$. Thus we see that we are actually inside the rational function field $k(L)$. We now once again appeal to commutativity of the two operations of substituting and taking the resultant. This means that to obtain the expressions for left hand side of (9.1), different values of $L$, we have to plug those values of $L$ in the right hand side of (9.1). In particular, it follows that the corresponding exponents that occur in (9.1) are the same for all values of $L$. Of course, $L$ may take the value $Id$ and any $A$ which corresponds to a permissible change of co-ordinates. This proves the claim and thereby the proof of Bezout's theorem is complete. ♠

**Exercise 9.1** Let $\Gamma_i, i = 1, 2, 3$ be plane curves having pair-wise no common components. Show that for any point $P$, $i(\Gamma_1 \cup \Gamma_2, \Gamma_3; P) = i(\Gamma_1, \Gamma_3; P) + i(\Gamma_2, \Gamma_3; P)$.

# Chapter 10

# Basic Inequalities

Lect.No.7
$21^{st}$ Jan 99

**Theorem 10.1** *Let $\Gamma, \Delta$ be any two plane curves without common components and let $P \in \Gamma \cap \Delta$. Then $i(\Gamma, \Delta; P) \geq 1$ and equality holds iff $P$ is a smooth point of both $\Gamma$ and $\Delta$ and the tangents to $\Gamma$ and $\Delta$ at $P$ are distinct.*

**Proof:** We assume that $\Gamma$ and $\Delta$ are in permissible position. We may also assume that $P = [1, 0, 0]$ and pass onto the affine space. Let then $\Gamma$ and $\Delta$ be given by

$$\begin{aligned} F(X,Y) &:= a_{10}X + a_{01}Y + \text{higher order terms} = 0 \\ G(X,Y) &:= b_{10}X + b_{01}Y + \text{ higher order terms} = 0 \end{aligned}$$

respectively. Then the resultant matrix $M_Y(F, G)$ looks like

$$\begin{pmatrix} a_{10}X + \cdots, & a_{01} + \cdots, & \cdots & \cdots & \cdots & \cdots \\ 0, & a_{10}X + \cdots, & a_{01} + \cdots, & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots, & \cdots, & \cdots & \cdots \\ b_{10}X + \cdots, & b_{01} + \cdots, & \cdots & \cdots & \cdots & \cdots \\ 0, & b_{10}X + \cdots, & b_{01} + \cdots, & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots, & \cdots, & \cdots & \cdots \end{pmatrix} \tag{10.1}$$

Use Laplace's rule to expand the determinant along the first two columns. One of the terms of the expansion will be

$$\begin{vmatrix} a_{10}X + \cdots, & a_{01} + \cdots \\ b_{10}X + \cdots, & b_{01} + \cdots \end{vmatrix} C(X)$$

which corresponds to the row pair $(1, m+1)$, where $C(X)$ is the corresponding cofactor. Hence this is divisible by $X$. The other four non zero terms are easily seen to be divisible by $X^2$. Therefore, $X$ divides $\mathcal{R} := \mathcal{R}_Y(F, G)$. This means that $i(\Gamma, \Delta; P) \geq 1$.

Now we have to determine the exact order to which $X$ divides $\mathcal{R}$. This order will be equal to 1 iff $C(X)$ is not divisible by $X$ and $a_{10}b_{01} - a_{01}b_{10} \neq 0$. This latter condition means that $P$ is a smooth point of both $\Gamma$ and $\Delta$ and the tangent lines to these curves at $P$ are distinct. So, assuming that $P$ is a smooth point of both $\Gamma$ and $\Delta$ and the tangents are distinct, to show that $i(\Gamma, \Delta; P) = 1$, it remains to prove that the cofactor $C(X)$ is not divisible by $X$. This is the same as saying that $C(0) \neq 0$.

Define

$$\alpha(X, Y) = \frac{F(X, Y) - F(X, 0)}{Y}; \quad \beta(X, Y) = \frac{G(X, Y) - G(X, 0)}{Y}.$$

Observe that $C(X)$ is nothing but the $Y-$resultant of $\alpha$ and $\beta$. Thus we want to compute $\mathcal{R}_Y(\alpha(0, Y), \beta(0, Y))$. Observe that the solutions of $F(0, Y) = 0$ correspond to the point of $\Gamma \cap \{X = 0\}$ and likewise $G(0, Y) = 0$ correspond to $\Delta \cap \{X = 0\}$. If there were any common points amongst them other than $P = (0, 0)$ it would violate the permissibility of $\Gamma$ and $\Delta$. Thus the only common root of $F(0, Y)$ and $G(0, Y)$ is $Y = 0$.

Now if possible let $Y = y$ be a common root of $\alpha(0, Y)$ and $\beta(0, Y)$. If $y \neq 0$, then $y$ will be a common root of $F(0, Y)$ and $G(0, Y)$. Hence $y = 0$. But then this implies that $a_{01} = 0 = b_{0,1}$. But then the $Y-$ axis is a common tangent to both $\Gamma$ and $\Delta$. This contradicts permissibility of $\Gamma \cap \Delta$. Hence $C(0) \neq 0$. This completes the proof. ♠

Exactly following the line of argument in the above theorem, but working out through a little more complicated computations, we can prove:

**Theorem 10.2** *Let $\Gamma, \Delta$ be two plane curves without any common components and let $P$ be a point of multiplicity $r$ and $s$ respectively on them. Then $i(\Gamma, \Delta; P) \geq rs$ and equality holds iff $\Gamma$ and $\Delta$ have no common tangent at $P$.*

**Lemma 10.1** Let $P$ be a simple point of a curve $\Gamma$ and let $L$ be the tangent to $\Gamma$ at $P$. Let $\Delta$ be any other curve with no common component with $\Gamma \cup L$. Then
(a) $i(\Gamma, \Delta; P) \geq \min\{i(\Gamma, L; P), i(\Delta, L; P)\}$.
(b) If one of the numbers $i(\Gamma, \Delta; P)$, $i(\Delta, L; P)$ is less than $i(\Gamma, L; P)$ then so is the other and the two are equal.

**Proof:** As usual, we may assume that $P = [1, 0, 0]$ $\Gamma, \Delta$ are in permissible position and pass onto the affine plane. We can further assume that $L$ is given $Y = 0$. Let us write

(see lemma 6.1)

$$\mathcal{R}_Y(F,G) = A(X,Y)F(X,Y) + B(X,Y)G(X,Y).$$

Since the left hand side is independent of $Y$, we may rewrite

$$\mathcal{R}_Y(F,G) = A(X)F(X,0) + B(X)G(X,0).$$

Since the order of $F(X,0)$ and $G(X,0)$ give the numbers $i(\Gamma, L; P), i(\Delta, L; P)$ respectively, and the order of left hand side gives the $i(\Gamma, \Delta; P)$, (a) follows.

In order to prove (b), suppose $i(\Gamma, \Delta; P) < i(\Gamma, L; P)$. Then by (a), we have $i(\Gamma, \Delta; P) \geq i(\Delta, L; P)$ and hence $i(\Delta, L; P) < i(\Gamma, L; P)$. Hence, we may assume that $i(\Delta, L; P) < i(\Gamma, L; P)$ and prove that $i(\Gamma, \Delta; P) = i(\Delta, L; P)$. Let the order of $P$ on $\Delta$ be $s$. If $L$ is not a tangent to $\Delta$ at $P$, then we know that $i(\Gamma, \Delta; P) = 1.s = s = i(\Delta, L; P)$. Therefore, it follows that $L$ is a tangent to $\Delta$ at $P$. We now expand the determinant for the resultant along the first two columns as in the proof of the above theorem. Let

$$F = a_0(X) + a_1(X)Y + \cdots; \quad G = b_0(X) + b_1(X)Y + \cdots$$

Since, we have assumed that $(0,0)$ is a smooth point of $\Gamma$, and $Y = 0$ is the tangent line $L$, it follows that the order of $a_0(X)$ is greater than one, and $a_1(0) \neq 0$. Similarly it follows that order of $b_0(X)$ is greater than $s \geq 1$. Indeed, since $ord_X\,(a_0(X)) = i(\Gamma, L; P)$, $ord_X\,(b_0(X)) = i(\Delta, L; P)$, it also follows that $ord_X\,(a_0(X)) > ord_X\,(b_0(X))$. Therefore, the minor of least order amongst the five possible non zero minors from the first two columns of (10.1) is equal to the order of $a_0b_1 - b_0a_1$. This in turn is equal to $ord\,(b_0(X))$. It remains to observe that the order of the cofactor of this term in the matrix is zero, i.e., $C(0) \neq 0$. The proof of this is exactly the same as that in the earlier theorem, using the fact that $\Gamma$ and $\Delta$ are in permissible position. ♠

# Chapter 11

# Rational Curve

The notion is predominantly from number theory, wherein one wants to find rational solutions (if any, or all) of Diophantine equations.

We say a curve $f(x, y) = 0$ is *rational* if there exists two rational functions $\phi(t)$ and $\psi(t)$ of one variable such that $f(\phi(t), \psi(t)) = 0$ for all $t$. Recall that by a rational function of one variable we mean a function of the kind $\alpha(t)/\beta(t)$, where both $\alpha$ and $\beta$ are polynomials. Obviously, finitely many points at which the denominator $\beta$ vanishes has to be avoided. Before proceeding with this notion any further, let me sketch an application of this in number theory:

Assume that $f(x, y)$ is a polynomial with rational coefficients and that it defines a rational curve where even the co-ordinate functions $\phi(t)$ and $\psi(t)$ are also defined over the rational numbers. Then the parameterization $x = \phi(t), y = \psi(t)$ will give all (except finitely many) rational solutions of $f(x, y) = 0$, as $t$ runs over all the rational numbers. This idea is exploited in a small way in the following special case of an *irreducible quadratic.*

Let $(x_0, y_0)$ be a known point on the curve, $f(x, y) = 0$. The line through $(x_0, y_0)$ with slope $t$ has the form

$$y - y_0 = t(x - x_0). \tag{11.1}$$

Substituting this in $f(x, y) = 0$ yields a quadratic in $x$, of which $x = x_0$ is a solution. This of course corresponds to the point $(x_0, y_0)$ on the curve. After cutting down the factor $(x - x_0)$, the remaining term is linear in $x$ and hence the solution is a rational function of $t$ (as well as $x_0, y_0$). Substituting it in (11.1) gives $y$ as a rational function of $t$.

We have just described a method to parameterise a quadratic, which yields a rational parameterization. On the way, we observed that if we had started with a rational point

$(x_0, y_0)$, then all the points $(x, y)$ corresponding to rational values of the parameter $t$ would give all but finitely many rational solutions of the equation $f(x, y) = 0$.

Thus given a rational quadratic finding one rational solution is quite good since that would give us all but finitely many rational solutions. Of course, even finding this one solution could be a delicate problem, which has been answered by Legendre's theorem, for instance. I shall not speak about this purely number theoretic result.

There are of course other applications of the parameterizations, such as in computing integrals etc.. which we shall not discuss here. Now let us show that a curves of higher degree need not be a rational curve in general. We shall prove:

**Theorem 11.1** *The curve given by*

$$x^n + y^n = 1 \tag{11.2}$$

*is not rational if $n > 2$. (and $n$ not divisible by $ch(k)$.*

**Proof:** : Let $x = \phi(t) = \dfrac{p(t)}{r(t)}, \quad y = \psi(t) = \dfrac{q(t)}{r(t)}$ be a parameterization of (11.2). Here we assume that $p, q, r$ have no common factors of positive degree. Let us say degree of $p, q, r$ are $a, b, c$ respectively. Then

$$p^n + q^n - r^n = 0 \tag{11.3}$$

Upon differentiation and cutting down $n$, we get,

$$p^{n-1}p' + q^{n-1}q' - r^{n-1}r' = 0 \tag{11.4}$$

The above two equations can be thought of as saying that $(p^{n-1}, q^{n-1}, r^{n-1})$ is a solution of the system of linear equation

$$\begin{aligned} pX + qY + rZ &= 0 \\ p'X + q'Y + r'Z &= 0. \end{aligned}$$

Therefore, by Cramer's rule, we have,

$$\frac{p^{n-1}}{qr' - rq'} = \frac{q^{n-1}}{rp' - pr'} = \frac{r^{n-1}}{pq' - qp'}. \tag{11.5}$$

But since $p, q, r$ do not have any common factors, it follows that $p^{n-1}$ should divide $qr' - rq'$, etc.. Hence $(n-1)a \leq b + c - 1, (n-1)b \leq a + c - 1, (n-1)c \leq a + b - 1$. Adding these three inequalities together, we see that $n \leq 2$. ♠

# Chapter 12

# Co-ordinate Ring and the Quotient Field

In Mathematics, we almost always study both *objects* and *morphisms* hand in hand. Here we would like to consider what are the maps on the algebraic curves. First of all let us only concentrate on field valued maps. Certainly, on $A$ and $A^2$, we have the rings $k[X]$ and $k[X, Y]$ respectively. On plane curves therefore, we merely take the restriction maps, i.e, given any polynomial in two variables $X, Y$, we consider the function defined by this polynomial on $A^2 \longrightarrow k$ and then restrict it to the set $C$ of points defined $f(X, Y) = 0$. Obviously, different polynomials may define the same map in this way on the curve $C$. For instance the polynomial $f$ itself defines the 0 map on $C$. Also, for any $g \in k[X, Y]$ all polynomials $g + hf$ define the same function on $C$. Therefore, it follows that the set of all so called 'regular functions' on $C$ can be identified with $k[X, Y]/(f)$. It inherits the structure of a ring in two different ways; check that the two structures are the same.

This ring is called the *co-ordinate ring* of the curve $C$. It is a nightmare of the beginner that this ring is also denoted by $k[C]$. However, once you get familiar with these notations and jargon, you will start appreciating the benefits of this notation.

Our approach being strongly algebraic in nature, we would like to perform the operation of dividing one regular function by the other. This would require the construction of the field of fractions, which in turn is possible only if $k(C)$ is a domain, i.e., $f$ is irreducible. So we make this assumption, without loss of generality, and proceed to consider $k(C)$, the field of fractions $k[C]$. Elements of $k(C)$ are called *rational functions on $C$*.

**Example 12.1**

*1) Let us consider a simple case first, where $C$ is the $X$-axis given by $Y = 0$. Then the co-ordinate ring is $k[X, Y]/(Y) = k[X]$.*
*2) Now let $C$ be any rational curve with a parameterization $T \mapsto (\phi(T), \psi(T))$. Putting $X = \phi(T), Y = \psi(T)$ yields a mapping $k[X, Y] \longrightarrow k[T]$. Check that $f$ goes to $0$ under this mapping and hence we get a mapping of $k(C) \longrightarrow k[T]$ which in turn yields a mapping of the quotient fields $k(C) \longrightarrow k(T)$. We claim that this mapping is an injective, if the field $k$ is infinite. This follows from the theorem below:*

**Theorem 12.1** *If $f, g \in k[X, Y]$ have infinitely many common zeros, then they have a common factor.*

[Reading this result from some book may be taken as one of the exercises.]

So far, we have been able to identify $k(C)$ with a subfield of $k(T)$ which obviously contains the field $k$. A simple application of Noether's normalisation theorem, will tell you that $k(C)$ itself is isomorphic to a rational function field in one variable.(Lüroth's theorem).
3) Let us work this out in a special case. Consider the circle $C : X^2 + Y^2 = 1$. Take $(x_0, y_0) = (0, 1)$ and consider the stereographic projection onto the line $Y = 0$. This yields the parameterization $X = \dfrac{2T}{T^2+1}, y = \dfrac{T^2-1}{T^2+1}$ for the circle. The field of rational functions $k(C)$ is thus identified with the subfield generated by

$$x = \frac{2T}{T^2+1}, \quad y = \frac{T^2-1}{T^2+1}$$

in $k(T)$. However , the inverse of the parameterization now tells you that $T = \dfrac{x}{1-y}$ which shows that the image of $k(C)$ is the whole of $k(T)$.

# Chapter 13

# Zariski Topology

**Definition 13.1** *Consider the set $k^n = k \times \cdots \times k$ the cartesian product of $n$ copies of $k$. We shall define a special topology on $k^n$ called* Zariski Topology. *Together with this topology, the space will be called the* Affine n-space *over $k$ and is denoted by $\mathbb{A}^n_k$ Often when the ground field $k$ is understood, we shall merely write $\mathbb{A}^n$.*

*The Zariski topology is defined by declaring the closed subsets: $A \subseteq k^n$ is said to be* closed *if it is the set of common zeros of a finite number of polynomials in $n$ variables $T_1, \ldots, T_n$. We shall often lazily denote the $n$ variables by a single letter $T$. Thus $k[T]$ is supposed to signify $k[T_1, \ldots, T_n]$.*

Let $X = \{t \in k^n \ : \ F_\lambda(t) = 0, \ \forall \ \lambda \in \Lambda\}$. Let $\mathfrak{a}$ be the ideal generated by $\{F_\lambda \ : \ \lambda \in \Lambda\}$. Then it follows easily that $X = \{t \in k^n \ : \ F(t) = 0 \text{ for all } F \in \mathfrak{a}\}$. Moreover, by Hilbert basis theorem, we know that there exist $F_1, \ldots, F_k \in \mathfrak{a}$ generating $\mathfrak{a}$, i.e., such that $(F_1, \ldots, F_k) = \mathfrak{a}$. Hence it follows that $X = \{t \in k^n \ : \ F_1(t) = \cdots = F_k(t) = 0\}$ is a closed subset of $\mathbb{A}^n$. From this it follows easily that arbitrary intersection of closed sets is closed. To verify that finite union of closed sets is closed, we observe that if $X$ is given as above and $Y$ is given by

$$Y = \{t \in k^n \ : \ G_1(t) = \cdots = G_l(t) = 0\}$$

then $X \cup Y$ is given by

$$X \cup Y = \{t \in k^n \ : \ F_i(t)G_j(t) = 0, i = 1, \ldots, k; j = 1, \ldots, l.\}$$

Clearly the entire set $k^n$ is defined by the 0 polynomial and the empty set is defined by the constant polynomial 1.

In general, a closed subset defined by a single non constant equation is called a *hyper surface.*

**Example 13.1**

*1) Clearly, $\mathbb{A}^1$ of which the underlying set is $k$ has co-finite topology: the only proper closed subsets are finite sets. For, a set of non zero polynomials in one variable have either no common factor, in which case the set of common zeros is emptyset OR they have a common factor, in which case the common zeros of them is the set of common zeros of the GCD, which is clearly a finite set. Also, every finite set $\{a_1, \ldots, a_r\}$ is the zero set of*

$$(T - a_1) \cdots (T - a_r) = 0.$$

*2) Let us determine the Zariski Topology on $\mathbb{A}^2$. Consider the set*

$$X = \{t_1, t_2) \ : \ F_1(t_1, t_2) = \cdots = F_k(t_1, t_2) = 0\}.$$

*Let $G$ be the GCD and write $F_i = GH_i$. Then as observed above, $X = Y \cup Z$ where $Y$ is the curve given by $G(t_1, t_2) = 0$ and $G_2$ is the common zeros of $H_i$. Since $H_i$ have no common factors, it follows that $Z$ is finite( $k$ is infinite). It may happen $G$ is a unit and then of course, $Y$ is empty. Thus we see that a proper closed subset of $\mathbb{A}^2$ is a union of a curve and a finite set of points. All such subsets are clearly closed sets any way.*

*3) An important observation to make is that the product topology on $\mathbb{A}^n \times \mathbb{A}^m$ does not coincide with $\mathbb{A}^{m+n}$. [To this, you may consider the simplest case when $m = 1 = n$. In the product topology, the proper closed subsets will be finite union of lines parallel to the two axes and a finite set. However, we know that there are other close subsets such as parabolas and circles, in $\mathring{A}^2$.] This could be the one of the strongest reason to adopt a notation different from simpler cartesian product notation for the affine space with the Zariski topology.*

*4) Having made the above negative observation, it is now worth noting that if $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are closed then the product set $X \times Y$ is closed in $\mathbb{A}^{n+m}$. To see this, we first write*

$$X = \{t \in k^n \ : \ F_1(t) = \cdots = F_k(t) = 0\};$$

$$Y = \{s \in k^m \ : \ G_1(s) = \cdots = G_l(s) = 0\}.$$

*Then we can think of $F_i$ and $G_j$ as elements of $k[R_1, \ldots, R_{n+m}]$ via the assignment*

$$T_i \mapsto R_i, \ i = 1, \ldots, n; \quad S_j \mapsto R_{n+j}, j = 1, \ldots, m.$$

*It follows that the common zeros of $F_i$ in $\mathbb{A}^{n+m}$ is nothing but $X \times \mathbb{A}^m$ and that of $G_j$ is precisely $\mathbb{A}^n \times Y$. Therefore,*

$$X \times Y = \{(t, s) \in k^n \times k^m \ : \ F_i(t) = 0 \ \& \ G_j(s) = 0\}$$

*which is the intersection of these closed sets.*
*5) Finally, consider the co-ordinate inclusion* $\mathbb{A}^n \hookrightarrow \mathbb{A}^{n+m}$ *given by* $t \mapsto (t, s)$ *for a fixed* $t$*. We shall show that the induced topology on the image is the same as the Zariski topology on* $\mathbb{A}^n$*. Clearly, the above argument shows that if* $X \subset \mathbb{A}^n$ *is closed then so is* $X \times \{s\}$ *is* $\mathbb{A}^{n+m}$*. To see the converse, Let* $W = \{(t, s) \ : \ H_i(t, s) = 0, i = 1, \ldots, k\}$*. We wish to prove that* $\{t \ : \ (t, s) \in W\}$ *is a closed subset of* $\mathbb{A}^n$*. Indeed, for this consider the specialisations* $F_i(T) = H_i(T, s)$ *as polynomials in* $T$*. Then we have,*

$$\{t \ : \ (t, s) \in W\} = \{t \ : \ F_i(t) = 0\}.$$

*6) There is a close relation between the set of ideals in* $k[T]$ *and the closed subsets of* $\mathbb{A}^n$ *which can be termed as 'dual': Let* $X = \{t \ : \ F(t) = 0, \ \forall! F \in \mathfrak{a}\}$ *and* $Y = \{t \ : \ F(t) = 0 \ \forall \ F \in \mathfrak{b}\}$*. Now* $\mathfrak{a} \subseteq \mathfrak{b}$ *implies that* $Y \subseteq X$*. On the other hand, given a closed set* $X$ *let us define an ideal* $\mathfrak{a}_X = \{F \in k[T] \ : \ F(t) = 0 \ \forall \ t \in X\}$*. Then it is easily seen that* $\mathfrak{a} \subseteq \mathfrak{a}_X$*. The equality may not be true in general. Thus in particular, even if* $\mathfrak{a} \subset \mathfrak{b}$ *it may happen that* $Y = X$*. We shall investigate this problem in more detail later on. However, it is true that* $V(\mathfrak{a}_X) := \{t \ : \ F(t) = 0 \ \forall F \in \mathfrak{a}_X\} = X$*. Verify this. [If* $t \in X$ *by the very definition of* $\mathfrak{a}_X$ *we have* $F(t) = 0$ *for all* $F \in \mathfrak{a}_X$*. To see the converse, we use the fact* $\mathfrak{a} \subseteq \mathfrak{a}_X$ *and hence* $V(\mathfrak{a}_x) \subseteq V(\mathfrak{a}) = X$*.] From this it follows that if* $Y$ *is a proper subset of* $X$*, then* $\mathfrak{a}_X$ *is a proper subideal of* $\mathfrak{a}_Y$*.*

**Definition 13.2** *Given a closed or an open subset* $F$ *of* $\mathbb{A}^n$*, we give the induced topology on* $F$ *and call it the Zariski topology on* $F$*.*

**Remark 13.1**
*1) Observe that when the ground field* $k$ *is* $\mathbb{R}$ *or* $\mathbb{C}$*, there is the usual topology on* $\mathbb{A}^n$ *and all Zariski closed subsets are closed in the usual topology. However, the convention is that we are using the Zariski topology, whenever any topological reference is made, unless specifically mentioned otherwise.*
*2) All non empty open subsets in the Zariski topology are open and dense in the usual topology (when* $k = \mathbb{R}$*, or* $\mathbb{C}$*). It is enough to check this for the complement of a hypersurface. Write out the details, as an exercise.*

**Definition 13.3** *We say a closed subset* $F$ *of* $\mathbb{A}^n$ *is reducible if we can write* $F = F_1 \cup F_2$ *where both* $F_i$ *are non empty proper closed subsets. A closed set which is not reducible will be called* irreducible*.*

Typical example of a reducible set is the union of the two axis. It is straight forward to check that a plane curve is irreducible iff the defining polynomial is. For instance, the union of two axes is reducible in $\mathbb{A}^2$. The space $\mathbb{A}^n$ itself is irreducible. Try to prove this. Of course, this will follow from a result that we are going to prove soon, once you observe that $\mathbb{A}^1$ is irreducible.

**Theorem 13.1** *Every closed subset is the union of a finite number of irreducible ones in a unique way.*

**Proof:** Suppose that this is false. Then we get a strictly decreasing sequence of closed sets which in turn yields an increasing sequence of ideals. By Noetherianness of $k[T]$ the sequence of ideals terminates and hence the sequence of closed sets should also terminate, which is a contradiction.

To show the uniqueness, let us write $F = F_1 \cup \cdots \cup F_k$ and let $G$ be any irreducible closed subset of $F$. Then it follows that $G = (F_1 \cap G) \cup \cdots \cup (F_k \cap G)$ and hence $G = F_i$ for some $i$. From this the uniqueness follows easily. ♠

**Remark 13.2** *Such a representation is often called the* in-contractible representation *and $f_i$ are called the* irreducible components of $F$.

**Theorem 13.2** *Product of two irreducible closed sets is irreducible.*

**Proof:** The correct statement that is implied by the above statement is as follows: Suppose $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are irreducible. Then $X \times Y$ is irreducible in $\mathbb{A}^{n+m}$. [This is stronger than saying that $X \times Y$ is irreducible in its product topology.] Let us write down the proof of this carefully.

Assume that $X \times Y = F_1 \cup F_2$ a union of two closed subsets. For any $y \in Y$ the subspace $X \times y$ being homeomorphic to $X$ is an irreducible subspace of $X \times Y$ and hence it is either contained in $F_1$ or in $F_2$. Suppose, we show that the subspaces $G_i = \{y \ : \ X \times y \subset F_i\}$ are closed in $\mathbb{A}^m$. Then it follows that $Y = G_1 \cup G_2$ and since $Y$ is irreducible, either $Y = G_1$ or $Y = G_2$. From this it follows that $X \times Y$ is either equal to $F_1$ or $F_2$ respectively. This would complete the proof.

Of course the proof that $G_1$ is closed will be similar to that for $G_2$ and so we prove the former one. Fix a $x \in X$. Now consider the set $Y_x = \{y \in Y \ : \ (x, y) \in F_1\}$. This is homeomorphic to $x \times Y \cap F_1$ under $y \mapsto (x, y)$. Hence it is a closed subset of $Y$. Therefore $\cap_x Y_x$ is also a closed subset. But this is precisely the set $G_1$. ♠

# Chapter 14

# Regular and Rational Maps

**Definition 14.1** *Let $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ be closed subsets. A set theoretically defined function $f : X \longrightarrow Y$ is called a* regular *map, if there are $k$-valued regular functions on $f_i : X \longrightarrow k$ such that $f = (f_1, f_2, \ldots, f_m)$. If it has an inverse which is also regular, then $f$ is called an isomorphism. Two closed subsets of affine spaces are said to be* isomorphic *to each other if there exists an isomorphism between them.*

**Remark 14.1**
*1) Given $m$ regular functions $f_i$ on $X$, in order to see that $f = (f_1, f_2, \ldots, f_m)$ defines a regular map on into $Y$, all that we have to do is to check that the substitutions $T_i = f_i$ satisfy the equations of $Y$.*
*2) Clearly, a regular function $X \longrightarrow \mathbb{A}^1$ is the same as an element of $k[X]$.*
*3) The mapping $t \mapsto (t^2, t^3)$ is a regular mapping of $\mathbb{A}^1$ into the plane curve given by $Y^2 = X^3$. It is easily checked that it is one a one mapping. However, it is not an isomorphism, since the inverse is of the form $Y/X$ which is not regular.*
*4) It is fairly easy to see that if $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ are regular, then the composite $g \circ f : X \longrightarrow Y$ is a regular mapping.*
*5)* **Frobeneous Mapping:** *Let now the field $k$ be of characteristic $p$. Then we have the identity $(T_1 + T_2)^p = T_1^p + T_2^p$. From this it follow that for any $F \in k[T]$, we have, $F(t_1^p, t_2^p, \ldots, t_n^p) = (F(t_1, \ldots, t_n))^p$. Consider the regular mapping $\phi : \mathbb{A}^n \longrightarrow \mathbb{A}^n$ defined by $(t_1, \ldots, t_n) \mapsto (t_1^p, \ldots, t_n^p)$. It follows from the above observation that if $X \subset \mathbb{A}^n$ is any closed subset then $\phi(X) \subset X$ and hence defines a regular mapping $\phi : X \longrightarrow X$. We call this the Frobeneous mapping. Its importance in problems over fields of non zero characteristic cannot be over-emphasised. Here is one such instance: suppose that the defining equations of $X$ all have coefficients in $\mathbb{F}_p \subset k$. Since the only points of $k$ that satisfy the equation $T^p = T$ are precisely those of $\mathbb{F}_p$, it follows that the set of points*

*of $X$ which have co-ordinates inside $\mathbb{F}_p$ are precisely the fixed points of the Frobeneous mapping.*

Let us now examine the relationship with the co-ordinate rings. Let $f : X \longrightarrow Y$ be a regular mapping. Since the co-ordinate functions of $f$ are represented by polynomials, it follows that if $\alpha \in k[Y]$ then $\alpha \circ f \in k[X]$. Thus the assignment $\alpha \mapsto \alpha \circ f$ defines an algebra homomorphism $f^\star : k[Y] \longrightarrow k[X]$. It has the usual functorial property that $(g \circ f)^\star = f^\star \circ g^\star$ and $Id^\star = Id$.

Moreover, given any algebra homomorphism $\gamma : k[Y] \longrightarrow k[X]$, we claim that there exists a regular mapping $f : X \longrightarrow Y$ such that $f^\star = \gamma$. We shall first do this for the simpler case when $X = \mathbb{A}^n$ and $Y = \mathbb{A}^m$. Observe that $\gamma$ is completely defined by its values on $Y_i, i = 1, 2, \ldots, m$. Put $F_i = \gamma(Y_i)$. Then clearly, $F_i$ defines a regular mapping $\mathbb{A}^n \longrightarrow \mathbb{A}^1$. Hence, $F = (F_1, F_2, \ldots, F_m)$ is a regular mapping of $\mathbb{A}^n \longrightarrow \mathbb{A}^m$. It remains to show that $F^\star = \gamma$. To see this it is enough to prove that $\gamma(Y_i) = F^\star(Y_i) = Y_i \circ F = F_i$ which is true by the very choice.

We now take up the general case, where $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ are any two closed subsets and $\gamma : k[Y] \longrightarrow k[X]$ is an algebra homomorphism. First of all, we shall show that that there is a commutative diagram of algebra homomorphisms:

$$\begin{tikzcd}
k[Y_1, \ldots, Y_m] \arrow[r, "\Gamma"] \arrow[d] & k[X_1, \ldots, X_n] \arrow[d] \\
k[Y] \arrow[r, "\gamma"] & k[X]
\end{tikzcd}$$

We shall denote elements of $k[Y_1, \ldots, Y_m]$ and $k[X_1, \ldots, X_n]$ by capital letters and their images in $k[Y] = k[Y_1, \ldots, Y_m]/\mathfrak{b}$ and $k[X] = k[X_1, \ldots, X_n]/\mathfrak{a}$ by the corresponding small case letters. Put $\gamma(y_i) = f_i$, where $f_i$ is the image of a polynomial $F_i \in k[Y_1, \ldots, Y_m]$ in $k[Y]$. Consider the map $\Gamma : k[Y_1, \ldots, Y_m] \longrightarrow k[X_1, \ldots, X_n]$ defined by $\Gamma(Y_i) = F_i$. Then we have the following commutative diagram given above.

Let $\Phi : \mathbb{A}^n \longrightarrow \mathbb{A}^m$ be the regular map defined by $\Gamma$, i.e., $\Phi^\star = \Gamma$. We consider the restriction of this map to the closed subset $X$ and denote it by $\phi$. Now all that we have to do is to check that $\phi(X) \subset Y$. This is the same as checking that for each $x = (x_1, \ldots, x_n) \in X$, the point $(F_1(x), \ldots, F_m(x)) \in Y$. For this we have to see that $q(F_1(x), \ldots, F_m(x)) = 0$ for all $q \in \mathfrak{b}$. But from the above commutative diagram, we

have $\Gamma(\mathfrak{b}) \subset \mathfrak{a}$. This means that, for every $q \in \mathfrak{b}$, $G = q(F_1, \ldots, F_m) \in \mathfrak{a}$, and hence, $G(x) = 0$.

It follows from the above considerations that two closed subsets of affine spaces are isomorphic iff their co-ordinate rings are isomorphic (as $k$-algebras). It may be worth noting that isomorphism implies homeomorphism of the underlying Zariski topological spaces. Indeed, in case of $k = \mathbb{R}, \mathbb{C}$, the same is true with respect to the usual topology also.

We may be also interested in the weaker equivalence relation amongst the closed subsets of affine spaces, viz., *bi-rational equivalence*. Clearly, the corresponding algebraic problem is then the isomorphism of the function fields. A natural question then is: what kind of rings and fields arise as co-ordinate rings or function fields of affine spaces? This question is answered easily:

**Theorem 14.1** *A $k-$ algebra $R$ is the co-ordinate ring of a closed subset of an affine space $X$ iff it is finitely generated; such a $X$ is irreducible iff $R$ has no non trivial zero-divisors. A field extension $K$ of $k$ is a function field iff it is finitely generated over $k$.*

Finally, we shall now state the result which cuts down the ambient dimension.

**Theorem 14.2** *Every irreducible closed subset $X$ of an affine space is birationally isomorphic to a hypersurface, in some other affine space.*

The proof of the above theorem is heavily algebraic and depends upon Abel theorem of existence of *primitives*. We sketch the rest of the proof here: Let $k(X) = k(t_1, \ldots, t_n)$ and let $d$ be maximal such that $t_1, \ldots, t_d$ be algebraically independent over $k$. Then $t_{d+1}$ a root of a polynomial $f \in k(t_1, \ldots, t_d)[T_{d+1}]$ and we can assume that $f$ is irreducible. In particular, it follows that $f'(T_{d+1}) \neq 0$. [This is not true in general, in case the characteristic of $k$ is non zero. However, this can arranged.] Thus $t_{d+1}$ is *seperable* over $k(t_1, \ldots, t_d)$. Now $t_{d+2}$ is also algebraic over $k(t_1, \ldots, t_d)$. Under these conditions, Abel's theorem says that we can find an element $y \in K$ such that $k(t_1, \ldots, t_{d+2}) = k(t_1, \ldots, t_d, y)$. Proceeding this way, we can finally show that $K = k(z_1, \ldots, z_{d+1})$. This is the same as saying that $X$ is bi-rational to a hypersurface in $\mathbb{A}^{d+1}$.

**Example 14.1**

*1) The mapping $t \mapsto (t, t^2)$ defines an isomorphism of the affine line with the parabola $Y = X^2$. One can also compute the co-ordinate ring directly. It is $k[X, Y]/(Y - X^2) =$*

$k[X]$.

*2) Consider the hyperbola $H$ given by $XY = 1$. The co-ordinate ring $k[H]$ is then equal to $k[X,Y]/(XY-1) = k[T,T^{-1}]$, the ring of Laurent polynomials in one variable. However, the function field is isomorphic to $k(T)$ only.*

*3) As a typical relationship between the co-ordinate ring and the closed subsets, suppose $f : X \longrightarrow Y$ be a regular map. If $f$ is surjective, it is easily checked that $f^\star : k[Y] \longrightarrow k[X]$ is injective. Let us look at the converse now. Assume that $f^\star$ is injective. This implies that given any regular function $\alpha$ on $Y$ such that restrict to $f(Y)$ if it is zero then it is identically zero. Of course, any regular (continuous) function that vanishes on $f(X)$ will automatically vanish on $\overline{f(X)}$. Thus, we cannot expect $f$ to be surjective but we may only hope that $\overline{f(X)} = Y$. So, let us try to prove this. Suppose this is not the case. Then $Z = \overline{f(X)}$ is a proper closed subset of $Y$ and hence there exists a non zero regular map $\alpha$ on $Y$ which vanishes on $Z$. (This is so, because the defining ideal of $Y$ must be strictly smaller than that of $Z$ and $\alpha$ could be taken to be any element in the set-theoretic difference of these two ideals.) But then $\alpha \in Ker f^\star$.*

We shall now compute the co-ordinate ring $X \times Y$ for any two closed subsets $X, Y$ of affine spaces. Once again, in the simplest case, when $X = \mathbb{A}^n$ and $Y = \mathbb{A}^m$. The rings are $k[Y_1, \ldots, Y_n$ and $k[X_1, \ldots, X_m]$ respectively and for $X \times Y$ we have the ring $k[T_1, \ldots, T_{m+n}]$ which we know is the tensor product of the first two rings, over the field $k$ (tensor product as vector spaces). So, we expect that similar statement should hold in the general case also and let us try it out. There is an obvious map

$$\tau : k[X] \otimes_k k[Y] \longrightarrow k[X \times Y]$$

given by

$$\tau(\sum_{i,j} f_i \otimes g_j)(x,y) = \sum_{i,j} f_i(x) g_j(y).$$

Verify that it is indeed a ring homomorphism. It is easily seen that all the co-ordinate functions are in the image of $\tau$ and hence it is surjective. To verify the injectivity, it suffices to assume that $\{f_i\}$ and $\{g_j\}$ are independent finite subsets of vector spaces $k[X], k[Y]$ respectively, and verify that $\{\tau(f_i \otimes g_j)\}_{i,j}$ is an independent set in $k[X \times Y]$. So suppose, $0 = \sum_{i,j} c_{ij} \tau(f_i \otimes g_j)(x,y) = \sum_{i,j} c_{ij} f_i(x) g_j(y) = 0$ for all $(x,y) \in X \times Y$. This implies for each fixed $x \in X$, we have $\sum_j (\sum_i c_{ij} f_i(x)) g_j(y) = 0$ for all $y \in Y$, i.e., $\sum_j (\sum_i c_{ij} f_i(x)) g_j = 0$ Hence, from the independence of $\{g_j\}$ in $k[Y]$, $\sum_i c_{ij} f_i(x) = 0$ for all for all $j$. Since this is true for all $x \in X$, by the independence of $\{f_i\}$ in $k[X]$, it follows that $c_{ij} = 0$ for all $i, j$.

Thus we have proved that

**Theorem 14.3** *The co-ordinate ring of $X \times Y$ is isomorphic to $k[X] \otimes_k k[Y]$.*

We end this section with a local criterion for a rational function to be regular, the proof of which will employ Hilbert's Nullstellensatz.

**Definition 14.2** *Let $X$ be a closed subset of an affine space. A rational function $\phi$ on $X$ is said to be* regular at $x \in X$ *if we can find $f, g \in k[X]$ such that $g(x) \neq 0$ and $\phi(x) = f(x)/g(x)$.*

**Theorem 14.4** *A rational function on an irreducible closed set $X$ is regular iff it is regular at every point $x \in X$.*

**Proof:** We have to prove only the 'if' part. So, let $\phi(x) = f_x(x)/g_x(x), g_x(x) \neq 0$. Let $\mathfrak{a}$ be the ideal generated by all the $g_x,\ x \in X$, and let $g_1, \ldots, g_k$ be a finite generating set, where $g_i = g_{x_i}$. Observe that $\mathfrak{a}$ does not have any common zero in $X$ and hence by HN, it follows that $\mathfrak{a} = (1)$. Write $1 = \sum u_i g_i$. Then $\phi = \sum_i \phi g_i u_i = \sum_i f_{x_i} u_i \in k[X]$, since $\phi g_i = \phi g_{x_i} = f_{x_i}$. ♠

# Chapter 15

# Closed Subspaces of Projective Spaces

Almost in a similar fashion to the study of closed subsets of affine spaces, we can carry out the study of closed subsets of projective spaces. However, there are a few points at which these two concepts differ and we would like to note them carefully.

Recall that the $n-$ dimensional projective Space $\mathbb{P}^n$ is defined to be the set of equivalence classes of elements of $\mathbb{A}^{n+1} \setminus \{0\}$ upto scalars. We denote them by $[x_0, \ldots, x_n]$ where $x_i \in k$, with at least one of the $x_i \neq 0$.

**Definition 15.1** *Given a polynomial $f \in k[X_0, \ldots, x_n]$ we say $f$ vanishes at $p = [x_0, \ldots, x_n]$, if $f$ vanishes on the entire line represented by $p$, i.e., $f(\lambda x_0, \ldots, \lambda x_n) = 0$ for all $\lambda \in k$. We shall express this as $f(p) = 0$. A subset $X \subset \mathbb{P}^n$ is said to be a* closed *subset if it is the common zero of a finite set of polynomials in $X_0, \ldots, X_n$.*

Once again, starting with a closed subset $X$ we can consider the set of all polynomials that vanish at all the points of $X$. It will form an ideal $\mathfrak{a}_X$ of $k[X_0, \ldots, X_n]$ and is called the ideal of $X$.

**Remark 15.1** *Given a polynomial $f$, writing $f = f_0 + \cdots + f_d$ as the sum of its homogeneous components, we see that this condition $f(p) = 0$ is equivalent to say that each $f_i(x_0, \ldots, x_n) = 0, i = 0, \ldots, d$. (Here we have to use the fact that $k$ is infinite.) This leads us to consider the concept of homogeneous ideals.*

**Definition 15.2** *By a homogeneous ideal of $k[X]$ we mean an ideal $\mathfrak{a}$ which is generated by homogeneous elements. This condition is the same as saying that $f \in \mathfrak{a}$ iff each of its homogeneous components $f_i \in \mathfrak{a}$.*

The defining ideal of a closed subset of $\mathbb{P}^n$ is a homogeneous ideal. Moreover, they are all finitely generated by homogeneous elements. Thus every closed subset of $\mathbb{P}^n$ is defined by a finite set of homogeneous equations.

Conversely, each homogeneous ideal defines a closed subset viz., the common zeros of all elements of in it. However, this set may be empty, even if $k$ is assumed to be algebraically closed, unlike in the case of affine closed subsets. The reason is very simple: we have taken equivalence classes of only non zero elements of $\mathbb{A}^{n+1}$. Let us examine this phenomenon a little closely. For instance, ideal $(X_0, \ldots, X_n)$ defines the element $0 \in \mathbb{A}^{n+1}$ and hence the emptyset in $\mathbb{P}^n$. Indeed for any $s \geq 1$ if $I_s$ is the ideal of all elements of $k[X]$ degree $\geq s$ (and 0), then it defines the empty set in $\mathbb{P}^n$ since it contains $X_i^s$ the common zero of which is the $\{0\}$. We have:

**Lemma 15.1** *A homogeneous ideal $\mathfrak{a}$ defines the empty set $\mathbb{P}^n$ iff it contains $I_s$ for some $s$.*

It remains to see the 'only if' part. Let $F_i,\ i = 1, \ldots, m$ be a set of homogeneous polynomials generating $\mathfrak{a}$. We shall show that for a suitable $s$ all $X_i^s \in \mathfrak{a}$. Consider the polynomials $F_i(1, T_1, \ldots, T_n)$. These have no common roots (for if there were any, by putting $T_j = X_j/X_0$, it would follow that $F_i(X_0, \ldots, X_n)$ have a non zero common root). By Hilbert Basis Theorem, it follows that there exists $G_i \in k[T_1, \ldots, T_n]$ such that $\sum_i F_i(1, T_1, \ldots, T_n)G_i(T_1, \ldots, T_n) = 1$. Substitute in these equations $T_j = X_j/X_0$ and clearing the denominator, it follows that $X_0^{m_0} \in \mathfrak{a}$. Likewise, we can show that $X_j^{m_j} \in \mathfrak{a}$. Take $m = max\{m_j\}$ and $s = m(n+1) + 1$. Then if $\alpha$ is a monomial of degree $\geq s$ it follows that it is divisible by one of the $X_j^m$ and hence is in $\mathfrak{a}$. Therefore $I_s \subset \mathfrak{a}$. ♠

**Lemma 15.2** *The mapping $(x_1, \ldots, x_n) \mapsto [1, x_1, \ldots, x_n]$ from $\mathbb{A}^n \longrightarrow \mathbb{P}^n$ is a homeomorphism and defines $\mathbb{A}^n$ as an open subspace of $\mathbb{P}^n$.*

**Proof:** The image of the map clearly consists of points defined by $X_0 \neq 0$ which is an open set in $\mathbb{P}^n$. The mapping is a homeomorphism follows from the homogenisation and de-homogenisation process that we have seen before. ♠.

The image of this mapping is denoted by $\mathbb{A}_0^n$. Likewise, we could consider open sets $\mathbb{A}_i^n$ defined by the condition $X_i \neq 0$. Clearly $\mathbb{P}^n = \cup_i \mathbb{A}_i^n$.

Now given any projective closed subset $X \subset \mathbb{P}^n$, we can consider the open subsets $U_i = \mathbb{A}_i^n \cap X$ of $X$. These are called *affine open subsets* of $X$. From the above considerations, they are closed subsets in $\mathbb{A}^n$.

# Chapter 16

# Quasi Projective Varieties

We shall now combine these notions into one single definition.

**Definition 16.1** *A* quasi projective variety *is an open subset of a closed projective set.*

Clearly, all closed projective sets are quasi projective. All closed subsets of an affine space are quasi projective: for if $X$ is closed in $\mathbb{A}^n$ then it can be thought of as a closed subset of $\mathbb{A}^n_0$ say, and its closure $\overline{X}$ in $\mathbb{P}^n$ is such that $\overline{X} \cap \mathbb{A}^n_0 = X$. Thus, it follows that all closed subsets and all open subsets of a quasi projective variety are also quasi projective.

**Definition 16.2** *By a* subvariety *of a quasi projective variety $X \subset \mathbb{P}^n$, we mean a subset $Y \subset X$ which is a quasi projective variety on its own in $\mathbb{P}^n$.*

This is equivalent to say that $Y$ is the difference $Z_1 \setminus Z_2$ of two closed subsets $Z_i$ of $X$.

# Chapter 17

# Regular Functions on Quasi Projective Varieties

As usual, we begin with the parent space $\mathbb{P}^n$. We immediately perceive a difficulty here. For no non constant polynomial can be regarded as a genuine function on $\mathbb{P}^n$. (Exercise). Let that be so and let us pass onto consider the analogue of rational functions. Even here the difficulty remains. For in order that a rational function $F/G$ to make sense at a point $p \in \mathbb{P}^n$, we need to have $F(\lambda p)/G(\lambda p)$ to take the same value for all $\lambda \neq 0$. This is possible if $F$ and $G$ are homogeneous of the same degree, i.e, we should consider only homogeneous rational functions of degree 0. In that case, $F/G$ defines a set theoretic $k$-valued function at least on the open subset $G \neq 0$ of $\mathbb{P}^n$. Thus given a quasi-projective variety $X$ we say the mapping $f : X \longrightarrow k$ is regular, if for each $x \in X$ we can find homogeneous rational functions $F, G$ of the same degree such that in a nbd of $x$, $f = F/G$. The collection of all regular functions on $X$ will be denoted by $k[X]$. It is verified easily that this forms a ring and contains the field $k$.

But we must verify that the new definition of $k[X]$ coincides with the old one in case $X$ is an irreducible closed subset of an affine space $\mathbb{A}^n$. But this precisely the content of theorem 14.4, if we merely adopt the method of homogenisation and de-homogenisation.

As indicated above it is possible that $k[X] = k$ as in the case of $X = \mathbb{P}^n$ for instance. Indeed this is the case for all closed subsets of a projective space, as we shall see later on. On the other hand, there are examples of quasi projective varieties $X$ with $k[X]$ not being a finitely generated $k$-algebra, as demonstrated by Nagata and Rees. Thus it is good to know that the co-ordinate ring is a good invariant only for affine closed subsets.

We can now define a regular mapping of $X$ into an affine space. Any such mapping will have $n$ co-ordinate functions. If all these co-ordinate functions are regular then we

say that the mapping is regular. Using this we now define mappings into quasi-projective varieties.

**Definition 17.1** *Let $f : X \longrightarrow \mathbb{P}^n$ be a set theoretic mapping. It is called a regular mapping if for each $x \in X$ and an affine open set $\mathbb{A}_i^n$ containing $f(x)$ there exists an open nbd $U$ of $x$ in $X$ such that $f(U) \subset \mathbb{A}_i^n$ and $f : U \longrightarrow \mathbb{A}_i^n$ is a regular mapping.*

One needs to check that this definition is unambiguous. So suppose if we choose a different affine space $\mathbb{A}_j^n$ containing $f(x)$. Then after restricting $f$ to a smaller open $V$ set if necessary the co-ordinates of $f : V \longrightarrow \mathbb{A}_j^n$ are obtained by the transformation from $\mathbb{A}_i^n \longrightarrow \mathbb{A}_j^n$ which is simply got by dividing all the other co-ordinates by $y_j \neq 0$. This is easily seen to be regular.

We shall now investigate how to express a regular mapping in terms of homogeneous co-ordinates. Say, for definiteness, $x \in U$ and $f : U \longrightarrow \mathbb{A}_0^m$ is given by regular functions $f_1, \ldots, f_m$. By definition, $f_i = P_i/Q_i$ where $P_i$ and $Q_i$ are both homogeneous polynomials of the same degree and $Q_i(x) \neq 0$. By taking a common denominator, we may write $f_i = F_i/F_0$ where $F_i$ are homogeneous of the same degree and $F_0(x) \neq 0$. Therefore, $f : U \longrightarrow \mathbb{P}^m$ is given by $f(x) = [F_0(x), \ldots, F_m(x)]$. We must note that the choice of $F_i$ is not unique here. Indeed if $G_i$ are such that $F_iG_j = F_jG_i$ then it follows that $f(x) = [G_0(x), \ldots, G_m(x)]$.

Thus we arrive at an alternate definition of a regular mapping on a quasi projective variety: A mapping $f : X \longrightarrow \mathbb{P}^m$ is regular if for each point $x \in X$ we can find $m$ forms $F_I$ such of the same degree such that at least one of them is not zero at $x$ and $f(x) = [F_0(x), \ldots, F_m(x)]$.

**Example 17.1** *We consider the projection of the circle $x^2 + y^2 = 1$ on the line from the point $p = (1, 0)$ and projectivise the whole picture: The circle is then given by the equation $U^2 + V^2 = W^2$. The point $p$ has co-ordinates $[1, 0, 1]$ and the projection takes values inside $\mathbb{P}^1$. Recall that the mapping was in affine co-ordinates was given by $t = y/x - 1$. Now in the projective co-ordinates $x = U/W$ and $y = V/W$ and $t = R/S$ say. Therefore the function can be written in the homogeneous co-ordinates by $f[U, V, W] = [R, S] = [U, V - W]$. Now this is not well defined at $[0, 1, 1]$. We can also write this mapping by the formula $f[U, V, W] = [V + W, -U]$ on the circle $U^2 + V^2 = W^2$ and in this representation, $[0, 1, 1]$ is sent to the point $[2, 0]$. Thus it follows that the projection map $C \longrightarrow \mathbb{P}^1$ is a regular mapping.*

Having defined what are regular mappings of qpv's, we can now have the concept of isomorphisms of these objects as usual. Any qpv that is isomorphic to a closed subset

of a projective space will be called a *projective variety.* It will be seen later on that being 'closed in a projective space' is an isomorphic invariant. Likewise, any qpv that is isomorphic to a closed subset of an affine space is called an *affine variety.* However the property of being 'closed in an affine space' is **not** an isomorphic invariant we may have a subset $Y \subset \mathbb{A}^n$ which is not closed yet it may be isomorphic to some other closed subset of an affine space. For example consider $Y = \mathbb{A}^1 \setminus \{0\}$. Under the mapping $t \mapsto (t, 1/t)$ it is isomorphic to the hyperbola $H : XY = 1$, in $\mathbb{A}^2$. Why is the above mapping regular?

[I now come to another point of irritant in algebraic geometry. Let me first state a result, which is purely a topological result. ]

**Lemma 17.1** *A subset $Y \subset X$ is closed iff given an open cover $X = \cup_\alpha U_\alpha$ of $X$, $Y \cap U_\alpha$ is closed in $U_\alpha$ for all $\alpha$.*

**Proof:** The only if part is obvious. To see the iff part, let $Z_\alpha$ be a closed set in $X$ such that $Y \cap U_\alpha = Z_\alpha \cap U_\alpha$ for every $\alpha$. Then we claim that $Y = \cap_\alpha(Z_\alpha \cup U_\alpha^c$ from which it would follow that $Y$ is closed. Let $y \in Y$. Given $\alpha$ if $y \in U_\alpha^c$ then well and good. Otherwise it is in $Y \cap U_\alpha$ and hence is in $Z_\alpha$. Therefore, $y \in Z_\alpha \cup U_\alpha^c$ for all $\alpha$. Conversely, since $X$ is covered by $U_\alpha' s$ we may assume that $y \in U_\alpha$ for some $\alpha$. But then $y \in Z_\alpha \cap U_\alpha$ and hence is in $Y$. ♠

**Remark 17.1** *A topological property is called* local *if the property hold for a set whenever it holds for in a nbd of every point of the set. Typical examples are continuity, differentiability, openness etc. of functions. The above lemma says that $Y \subset X$ being a closed subset of a space $X$ comes very close to being a local in this sense. The only difference is that the property should hold at all points of the space $X$ rather than for just points of $Y$ here. However, algebraic geometers call even such properties local. Also, it is worth noting here that there is yet another somewhat different notion of a locally closed set, which is quite useful in function theory.*

The following is a useful result while studying local properties of qpvs.

**Lemma 17.2** *Every point $x \in X$ has a nbd isomorphic to an affine variety.*

**Proof:** It suffices to show that $X \cap \mathbb{A}_i^n$ are affine varieties. Without loss of generality we may assume that $X$ itself is a qpv in $\mathbb{A}^n$ and prove the above result. By the definition, we have two closed subsets $Y_2 \subset Y_1 \subset \mathbb{A}^n$ such that $X = Y_1 \setminus Y_2$. Let $x \in X$ be any and let $F$ be a polynomial such that $F(x) \neq 0$ but $F = 0$ on $Y_2$, so that the open set $D(F) = \{y \in X \ : \ F(y) \neq 0\}$ is a nbd of $x$ in $X$. Ww claim that $D(F)$ is an affine

variety. For this, suppose $F_1, \ldots, F_m$ define the set $Y_1$ in $\mathbb{A}^n$. Consider the set $Z \subset \mathbb{A}^{n+1}$ defined by

$$F_1(x_1, \ldots, x_n) = \cdots = F_m(x_1, \ldots, x_n) = 0; \; F(x_1, \ldots, x_n).x_{n+1} = 1.$$

The mapping $(x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n)$ is clearly an isomorphism of $D(F)$ onto $Z$. ♠

**Remark 17.2** *The open sets of the type $D(f) = X \setminus V(f)$ in an affine variety, defined by a single equation are called* principal open sets. *They play an important role, since they are affine and every other open set is the finite union of principal open sets. Also, the co-ordinate ring of $D(f)$ is obtained by merely inverting the element $f$ in $k[X]$, i.e., $k[D(f)] = k[X][1/f]$. (Exercise).*

**Exercise:** A function $f : X \longrightarrow Y$ is called locally regular, if for every $x \in X$ and a regular function $\phi$ in a nbd of $f(x)$ the mapping $\phi \circ f$ is regular in a nbd of $x$. Show that $f$ is regular, iff it is continuous and locally regular.

# Chapter 18

# Rational Functions

In case of affine varieties a rational functions was defined to be a ratio of two regular (polynomial) functions. However, in this general situation, as we have observed, there may not be any regular functions other than constants. Let $X$ be an irreducible quasi-projective variety in $\mathbb{P}^n$ and $\mathcal{O}_X$ denote the set of all rational functions in homogeneous co-ordinates $X_0, \ldots, X_n$ of the form $P/Q$ where both $P$ and $Q$ are homogeneous polynomials of the same degree in $X_i's$. Of course, it is required that $Q$ does not vanish identically on $X$ and hence $Q \notin \mathfrak{a}_X$. Irreducibility of $X$ implies that $\mathcal{O}_X$ is a domain. (Exercise). Let $M_X$ denote the set of all $P/Q \in \mathcal{O}_X$ such that $P \in \mathfrak{a}_X$. Then $M_X$ is a maximal ideal and hence $\mathcal{O}_X/M_X =: k(X)$ is a field. This is called the *field of rational functions on* $X$.

Observe that if a homogeneous function vanishes on subset $Y$ of $X$ identically, then it vanishes on $\overline{Y}$ also. Hence $k(X) = k(\overline{X})$ and for any non empty open set $U$ of $X$ we have $k(U) = k(X)$. Thus while studying the field of rational functions, it is enough to consider only affine or projective varieties. Also, verify that in case of an affine variety, the above definition coincides with the old definition of the field of rational functions. Also, as in the earlier case, a rational functions on $X$ can be defined to be a function which is regular on a non empty open subset of $X$.

A rational mapping $f : X \longrightarrow \mathbb{P}^m$ is then a ratio of $m$ rational functions, such that, at least one of the forms is not identically zero on $X$.

Finally if $X$ and $Y \subset \mathbb{P}^m$ are quasi-projective varieties a rational mapping $f : X \longrightarrow Y$ is nothing but a regular mapping on an open set $U \subseteq X$ such that $f(U) \subseteq Y$. A rational mapping $g : Y \longrightarrow X$ is called inverse of $f$ if it is so restricted to some non empty open subset of $Y$.

**Theorem 18.1** *Two irreducible qpv $X$ and $Y$ birationally isomorphic iff they contain*

*isomorphic open subsets $U \subset X$ and $V \subset Y$.*

**Example 18.1**

*1)* **Projections:** *We have seen the so called projection from a point in $\mathbb{P}^n$. Let us now generalise this. Let $L_1, \ldots, L_{n-d}$ be independent linear forms in n+1 variables, and let $E$ be the set of common zeros of them in $\mathbb{P}^n$. Then $E$ is d-dimensional projective subspace of $\mathbb{P}^n$. Consider the mapping $\pi(x) = [L_1(x), \ldots, L_{n-d}(x)] \in \mathbb{P}^{n-d-1}$. Clearly, $\pi$ defines a regular mapping on any variety which does not intersect $E$. Of course, if the variety intersects $E$ but is not contained completely in $E$ then it defines a rational mapping. This is called the* projection with centre *$E$. Let us look at the geometric meaning of this map. As a model of $\mathbb{P}^{n-d-1}$ choose any $(n-d-1)$ dimensional projective subspace $H$ of $\mathbb{P}^n$ complementary to $E$. (This can be done for example by completing the above $L_i$ to a basis.) Then given any point $x \in \mathbb{P}^n$ the span of $E$ and $x$ is a $(d+1)$ dimensional subspace which intersects $H$ in a unique point; this point is $\pi(x)$.*

*2)* **Veronese mapping:** *Let us consider the space of all homogeneous polynomials of degree $m$ in the variables $X_0, \ldots, X_n$. Since the monomials of degree $m$ span them, this space is seen to be of dimension $\binom{n+m}{n}$. Therefore the corresponding projective space is of dimension $\nu_{n,m} := \binom{n+m}{n} - 1$. We shall index the co-ordinates of this space by monomials of degree $m$ in the variables $X_0, \ldots, X_n$. Only that we simplify this a little bit by writing $v_I$ where $I = i_0, \ldots, i_n$ is such that $i_0 + \cdots + i_n = m$, $i_j$ being non negative integers. We now consider the mapping $\nu : \mathbb{P}^n \longrightarrow \mathbb{P}^{\nu_{n,m}}$ by $[x_0, \ldots, x_n] \mapsto [\cdots, x^I, \cdots,]$ where the $I$-entry is the monomial $x^I$. Check that this is well defined (at least one of the co-ordinates is not zero) and it is a regular mapping. Check that it is injective. Finally, check that $v \in \mathbb{P}^{\nu_{n,m}}$ belongs to $\nu(\mathbb{P}^n)$ iff whenever $I, J, K, L$ are multi indices such that $i_r + j_r = j_r + l_r$ for all $r$ then $v_I v_J = v_K v_L$. ( One way is obvious. Given $v = [v_J] \in \mathbb{P}^{\nu_{n,m}}$, satisfying the above set of equations,without loss, assume that $v_I \neq 0$ for $I = (m, 0, \ldots, 0)$. Choose $x_0$ to be such that $x_0^m = v_I$. Then we are forced to choose $x_i$ so that $x_0^{m-1} x_i = v_{\{m-1,0,\ldots,0\}}$ Using the relations mentioned above, we then check that $\nu([x_0, \ldots, x_n]) = v$.) This shows that $\nu(\mathbb{P}^n)$ is a projective variety and $\nu$ is an isomorphism of $\mathbb{P}^n$ on to this Veronese variety, provided we show that $\nu$ is a clsoed mapping. This will follow from a theorem that we shall prove soon. Of course one can be prove this independently also.*

*The significance of the Veronese embedding is in the following. Suppose we have $F = \sum u_I X^I$ is a form of degree $m$ and $H$ is the hypersurface defined by it in $\mathbb{P}^n$. Then under the Veronese mapping $H$ is mapped onto the intersection of a hyperplane $\sum u_I v_I = 0$ and the variety $v(\mathbb{P}^n)$. Thus certain problems about hypersurfaces are converted into problems about hyper planes. This is an example of a powerful technique in Algebraic geometry,*

*viz.,* linearisation.

# Chapter 19

# Product of Quasi Projective Varieties

We have seen that while taking products we have to be a little careful. We shall now discuss how to think of a cartesian product of two qpvs as a qpv.

First consider the case when both $X$ and $Y$ are qpvs inside some affine spaces. Then we have $X = Z_1 \setminus Z_2$ and $Y = Z_3 \setminus Z_4$ say where $Z_2 \subset Z_1 \subset \mathbb{A}^n$ and $Z_4 \subset Z_3 \subset \mathbb{A}^m$ are closed. Clearly,

$$X \times Y = Z_1 \times Z_3 \setminus (Z_1 \times Z_4 \cup Z_2 \times Z_3)$$

and therefore, there is no problem in thinking of $X \times Y$ as a qpv. However, the situation is a little complicated in the general case, since, we have not yet defined what are closed subsets of $\mathbb{P}^n \times \mathbb{P}^m$. Indeed, we have to settle this problem in such a way that if $A_i \subset \mathbb{A}^{n_i}$ are qpvs then so is $A_1 \times A_2$ in $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2}$. We are also forced to define a topology on $\mathbb{P}^n \times \mathbb{P}^m$ in such a way that, restricted to any $\mathbb{A}^n_i \times \mathbb{A}^m_j$, it should give the topology that we have considered in the affine situation, i.e., each $\mathbb{A}^n_i \times \mathbb{A}^m_j$ should be isomorphic to $\mathbb{A}^{n+m}$. We also require that each $\mathbb{A}^n_i \times \mathbb{A}^m_j$, should be open in this topology. Since the collection of $\{\mathbb{A}^n_i \times \mathbb{A}^m_j\}_{i,j}$ covers the whole of $\mathbb{P}^n \times \mathbb{P}^m$, we see that these properties actually determine the topology uniquely, viz., give each $\mathbb{A}^n_i \times \mathbb{A}^m_j$ the topology through the isomorphism to $\mathbb{A}^{n+m}$ and declare a set $F \subset \mathbb{P}^n \times \mathbb{P}^m$ to be closed iff $F \cap \mathbb{A}^n_i \times \mathbb{A}^m_j$ is closed in $\mathbb{A}^n_i \times \mathbb{A}^m_j$ for each $i, j$.

By the usual trick of homogenisation and de-homogenisation, we see that

**Theorem 19.1** *A subset $F \subset \mathbb{P}^n \times \mathbb{P}^m$ is closed iff it is given as the set of common zeros of a finitely many polynomials $G_i(T, S)$ separately homogeneous in the variables $T = (T_0, \ldots, T_n)$ and $S = (S_0, \ldots, S_m)$. Moreover, a subset of $\mathbb{P}^n \times \mathbb{A}^m$ is closed iff it is given by a finite set of polynomials $g_j(T, S)$ homogeneous in the variables $T$.*

**Proof:** An alternate way of looking at this problem is to think of $\mathbb{P}^n \times \mathbb{P}^m$ as a closed subset of some $\mathbb{P}^N$ in some natural way and then consider the induced topology. The following result does this job.

**Theorem 19.2** *The mapping $\nu$ defined by*

$$([t],[s]) \mapsto [w_{ij}]$$

*where $w_{ij} = t_i s_j$ is an embedding of $\mathbb{P}^n \times \mathbb{P}^m$ onto a closed subset of $\mathbb{P}^N$, where $N = (n+1)(m+1)-1$.*

**Proof:** That the mapping is well defined is clear. Also, it is easy to see that the image set is given by the equations

$$W_{ij}W_{kl} = W_{kj}W_{il}.$$

To verify that the mapping is regular, we may assume that $w_{00} \neq 0$ say. Then $t_0 \neq 0$ and $s_0 \neq 0$ and we have the mapping given by $(t,s) \mapsto (w_{ij})$, where now we have simply put $t_0 = 1 = s_0$ in the above formula. It easy to see that this mapping is injective. To see that it is an embedding, it remains to see that if $\Gamma$ is closed set in $\mathbb{P}^m \times \mathbb{P}^m$, then $\nu(\Gamma)$ is closed in $\mathbb{P}^{(n+1)(m+1)-1}$. So, let $F(T,S)$ be a polynomial homogeneous in $T$ of degree $a$ and homogeneous in $S$ of degree $b$. Assume for definiteness sake that $a \geq b$ and let $c = a - b$. Now consider the polynomials $S_j^c F(T,S)$ which is homogeneous of degree $a$ in both $T$ and $S$ seperately. It follows that there exists $G_j(W)$ homogeneous in $W_{ij}'s$ such that if we substitute $W_{ij} = T_i S_j$ then we get $S_j^c F$. Verify that the common zeros of $G_j$ intersected with the image of $\nu$ is equal to the image of the zero set of $F$. ♠

**Remark 19.1** *The above mapping can be written in terms of matrices: Take $[t]$ as a $(n+1)\times 1$ matrix and $[s]$ as a $1 \times (m+1)$ matrix and take $w$ to be the $(n+1)\times(m+1)$ matrix which is the product of these to matrices. (Of course, you have to homogenise everywhere.) The conditions above simply say that we must take only matrices of rank at most one. Since at least one entry has to be nontrivial the rank is actually equal to one.*

Since the topology on the cartesian product is not the product topology, we should study some of the properties of this topology carefully.

**Lemma 19.1** *The diagonal $\Delta$ is closed in any $\mathbb{P}^n \times \mathbb{P}^n$.*

**Proof:** This is easy, since the diagonal is given by the equation $T_i = S_i, i = 0, \ldots, n$. ♠

**Remark 19.2** *You may have come across a result in point set topology, which says that the diagonal $\Delta$ is closed in $X \times X$ iff $X$ is a Hausdorff space. However, we definitely know that $\mathbb{P}^n$ is not Hausdorff. What is happening?*

**Lemma 19.2** *Let $X$ and $Y$ be any two qpvs, $f : X \longrightarrow Y$ be a regular mapping. Then the graph $\Gamma_f$ is closed in $X \times Y$.*

**Proof:** We first reduce this to the case when $Y = \mathbb{P}^m$. Suppose $Y \subset \mathbb{P}^m$. Consider $g : X \longrightarrow \mathbb{P}^m$, $g =\hookrightarrow \circ f$. Now $\Gamma_f = \Gamma_g \cap X \times Y$. So, we assume that $Y = \mathbb{P}^m$. Now consider the mapping $\phi : (x, y) \mapsto (f(x), y)$ from $X \times \mathbb{P}^m \longrightarrow \mathbb{P}^m \times \mathbb{P}^m$. Clearly $\Gamma_f = \phi^{-1}(\Delta)$ and $\phi$ is a regular mapping. By the lemma above $\Delta$ is closed and hence $\Gamma_f$ is closed. ♠

**Theorem 19.3** *Let $X$ be projective variety and $Y$ be a qpv. Then the projection map $\pi : X \times Y \longrightarrow Y$ is a closed mapping.*

**Proof:** Once again we first reduce the proof of the theorem to a simpler situation. First notice that if $X \subset \mathbb{P}^n$ is closed then it is enough to prove the theorem for $\mathbb{P}^n$ in place of $X$. Next, since the property of being closed is 'local', we can cover $Y$ with affine varieties and then it is enough to prove the theorem under the assumption that $Y$ is affine. Now suppose $Y \subset \mathbb{A}^m$ is closed, then given a closed subset $F$ of $\mathbb{P}^n \times Y$ it can be treated as a closed subset of $\mathbb{P}^n \times \mathbb{A}^m$ and then $\pi(F)$ is closed in $\mathbb{A}^m$ implies it is closed in $Y$ also. Thus it is enough to prove the result for $Y = \mathbb{A}^m$.

Let now $F$ be a closed subset of $\mathbb{P}^n \times \mathbb{A}^m$ defined by the equations $g_i(T, S) = 0, i = 1, \ldots, k$ where each $g_i$ is a polynomial homogeneous in the variables $T$. A point $s \in \mathbb{A}^m$ belongs to $\pi(F)$ iff the equations $g_i(T, s) = 0$ have a non zero solution in $T$. As seen before, this is equivalent to say that the ideal $\mathfrak{a} := \mathfrak{a}_s := (\{g_i(T, s)\})$ does not contain any of the ideals $I_r \subset k[T]$, $r \geq 1$. Let $X_r$ be the set of all $s \in \mathbb{A}^m$ such that the ideal $\mathfrak{a}_s$ does not contain $I_r$. It is enough to show that $X_r$ is closed for each $r \geq 1$. For then, $\pi(F) = \cap_{r\geq 1} X_r$ will be also closed.

Now $\mathfrak{a}$ contains $I_r$ iff it contains all the monomials in $T$ of degree $r$. Let us say the degree of $g_i(T, s) = d_i$. It follows that $I_r \subset \mathfrak{a}$ iff for each monomial $T^\beta$ of degree $r$, we have $T^\beta = \sum g_i(T, s) f_{\beta,i}(T)$ where each $f_{\beta,i}$ is a homogeneous polynomial of degree $r - d_i$. Obviously, in this summation those $g_i$ for which $d_i > r$ do not occur. For simplicity, we may assume that each $d_i \leq r$. In the vector space of all homogeneous polynomials in $T$, of degree $r$, which is of dimension $d = \binom{n+r}{r}$, we consider the elements $v_{i,\gamma} := g_i(T, S)T^{\gamma_i}$, where $i = 1, 2 \ldots, k$ and $T^\gamma$ varies over all monomials of degree $r - d_i$. Now fixing some

order on all the monomials of degree $r$, each element $\alpha_{i,\gamma}$ can be thought of as a row-vector whose entries are polynomials in $S$. Putting these row vectors one below the other we get a matrix $M$.

Now each monomial $T^\beta$ is a linear combination of $v_{i,\gamma}$ iff the rank of $M$ is $d$. (The rank cannot be greater than $d$.) Thus the negation of this is the same as saying that all $d \times d$ minors of $M$ should vanish, each of which is a polynomial in $S$. The common zeros of these polynomials is precisely the set $X_r$. ♠

We can now prove what we were aiming at:

**Theorem 19.4** *Let $f : X \longrightarrow Y$ be a regular mapping, where $X$ is projective. Then $f(X)$ is closed in $Y$.*

**Proof:** Clearly $f(X) = \pi(\Gamma_f)$. ♠

As an immediate corollary, we have,

**Theorem 19.5** *For any irreducible projective variety $X$, we have $k[X] = k$. Further if $Y$ is any affine variety then any regular map $f : X \longrightarrow Y$ is a constant.*

**Proof:** Let $f : X \longrightarrow \mathbb{A}^1$ be a regular function. We can then think of $f$ as a regular mapping into $\mathbb{P}^1$ also. Then the image $f(X)$ is a closed subset of $\mathbb{P}^1$. Since it cannot be the whole set $\mathbb{P}^1$, it must be a finite set. If it contains more than one point, then we can write $X$ as a disjoint union of proper closed sets which contradicts the irreducibility of $X$. Hence $f(X)$ is a singleton.

The latter part follows by applying the former result to each co-ordinate map. ♠

As a final application of this theorem, let us prove:

**Theorem 19.6** *Under the Veronese mapping, the set $R$ of all points $\theta \in \mathbb{P}^{\nu_{n,m}}$ corresponding to reducible polynomials forms a closed subset of $\mathbb{P}^{\nu_{n,m}}$.*

**Proof:** Consider the mapping $\psi : \mathbb{P}^{\nu_{n,j}} \times \mathbb{P}^{\nu_{n,m-j}} \longrightarrow \mathbb{P}^{\nu_{n,m}}$ given by the multiplication of two homogeneous polynomials of degree $j$ and $m - j$. Clearly this mapping is regular and hence the image is a closed subset. Taking the union over all $1 \leq j \leq m - 1$ we get all the set $R$. ♠.

**Remark 19.3** *Thus we have seen that after fixing the degree, the set of all reducible hyper surfaces is a thin set as compared to the set of all irreducible ones. On the other hand each reducible one corresponds to a finite (more than two) collection of irreducible ones. Does it not sound paradoxical?*

# Chapter 20

# A Reduction Process

$23^{th}$ Feb 99

We shall begin this section again with some more properties about the resultant.

**Lemma 20.1** *Let $F = U_0X^n + U_1X^{n-1} + \cdots + U_n$; $G = V_0X^m + \cdots + V_m$ be as before. Then the resultant $\mathcal{R}_X(F, G) \in k[U, V]$ is irreducible.*

**Proof:** The proof is by a double induction on $m$ and $n$. Verify the statement directly for the cases $(m, n) = (1, 1), (2, 1)$ or $(1, 2)$, and assume that it holds for all cases when the sum of the degrees is less than $m + n$, $m, n \geq 2$. Now observe that

$$\mathcal{R}(F, G)|_{V_0=0} = U_0\mathcal{R}(F, G|_{V_0=0})$$

and $\mathcal{R}(F, G|_{V_0=0})$ is non zero and irreducible. Likewise, we have,

$$\mathcal{R}(F, G)|_{U_0=0} = (-1)^m V_0\mathcal{R}(F, G|_{U_0=0})$$

and $\mathcal{R}(F, G|_{U_0=0})$ non zero and irreducible.

Now suppose $\mathcal{R}(F, G) = PQ$ is a non trivial factorisation, with both $P$ and $Q$ homogeneous in $U$ and $V$. Denoting the specializations at $V_0 = 0$ by putting a bar, we first observe that $\bar{H}$ cannot be a non zero constant for any non constant homogeneous polynomial $H$. We now have, $U_0\mathcal{R}(F, \bar{G}) = \overline{\mathcal{R}(F, G)} = \bar{P}\bar{Q}$. Without loss of generality we may assume that
$\bar{P} = \mathcal{R}(F, \bar{G})$ and $\bar{Q} = U_0$, i.e., $P = \mathcal{R}(F, \bar{G}) + V_0P_1; Q = U_0 + V_0Q_1$. Thus we have proved that

$$\mathcal{R}(F, G) = (\mathcal{R}(F, G_1) + V_0P_1)(U_0 + V_0Q_1)$$

where $G_1 = \bar{G}$ and $P_1, Q_1$ are some homogeneous polynomials.

Now going modulo $U_0$, and denoting the results by 'bar', we have,

$$(-1)^m V_0 \mathcal{R}(\bar{F}, G) = ((-1)^{m-1} V_0 \mathcal{R}(\bar{F}, G_1) + V_0 \bar{P}_1) V_0 \bar{Q}_1.$$

This contradicts the irreducibility of $\mathcal{R}(\bar{F}, G_1)$. ♠

**Lemma 20.2** *For any $H(X_0, X_1)$ there exists a $c \in k$ such that*

$$Res_X(F, G) = c\mathcal{R}_X(F, G - HF).$$

**Proof:** We may consider $H$ itself as a variable and consider $A = \mathcal{R}_{X_2}(F, G), B = \mathcal{R}_{X_2}(F, G - HF) \in k[U, V, H]$ as homogeneous polynomials of degree $m + n$. Then an element in the zero set of $A$ corresponds to a common root the specialization of $F$ and $G$ and hence is also a common root of $F$ and $G - HF$. Hence this element is contained in the zero set of $B$. But since $A$ is irreducible, it follows that $A$ divides $B$ in $k[U, V, H]$. Hence this is also true in $k[X_0, X_1]$. But in this ring the polynomials are of the same degree and hence the result. ♠

**Theorem 20.1** *Let $\Gamma, \Delta$ be any two plane curves of degree $n, m$ respectively. Suppose $L$ is a line and $\Gamma \cap L$ consists of points $\{P_1, P_2, \ldots, P_n\}$ where, it is understood that a particular point $P_i$ is being repeated as often as the multiplicity $i(\Gamma, L; P_i)$ in the above enumeration. Suppose that $\{P_1, \ldots, P_n\}$ is contained in $\Delta$ also. Then there exists a plane curve $\Delta_1$ of degree $m - 1$ such that the $n(m - 1)$ points of intersection of $\Gamma \cap \Delta_1$ correspond to the rest of the intersection points of $\Gamma$ and $\Delta$.*

**Proof:** Let $F$ and $G$ be the defining polynomials of $\Gamma$ and $\Delta$. Without loss of generality, we may assume that $L$ is given by $X_2 = 0$. We should find $G_1$ such that the curve $X_2 G_1(X_0, X_1, X_2) = 0$ has intersection pattern with $\Gamma$ exactly as $\Delta$ has.

Observe that if $m < n$ then the hypothesis implies that $L$ must be a component of $\Delta$ which is the same as saying that $G = X_2 G_1$ and we are done. So, we shall assume that $m \geq n$.

Since the zeros of the homogeneous polynomial $F(X_0, X_1, 0)$ are contained in the zeros set of $G(X_0, X_1, 0)$ (with multiplicities) it follows that

$$F(X_0, X_1, 0) H(X_1, X_2) = G(X_0, X_1, 0). \tag{20.1}$$

for some homogeneous polynomial $H$ of appropriate degree. Therefore, there exists $G_1$ such that

$$G(X_0, X_1, X_2) - F(X_0, X_1, X_2) H(X_0, X_1) = X_2 G_1(X_0, X_1, X_2).$$

Since both sides have to be homogeneous of degree $m$, it follows that $G_1$ is homogeneous of degree $m-1$. It follows from this equation that the set of common zeros of $F$ and $G$ is the same that of common zeros of $F$ and $X_2G_1$. In order to see that even the multipicities are the same we use appeal to the fact that $\mathcal{R}_{X_2}(F,G) = \mathcal{R}_{X_2}(F, G-FH) = \mathcal{R}_{X_2}(F, X_2G_1)$. ♠

# Chapter 21

# Study of Cubics

$25^{th}$ Feb. 99

We shall now give an extremely important application of this result. Let $\Gamma$ be a non singular plane cubic. On the set of points of $\Gamma$, we shall define an additive structure. Choose $O \in \Gamma$ as the reference point. Let $A, B$ be any two points on $\Gamma$ (with repetition allowed). Consider the line $AB$ (this being a tangent if $A = B$.) Let this line intersect $\Gamma$ again in $\tau(A, B)$. Now consider the line through $O$ and $\tau(A, B)$ and consider the point of intersection of this line with $\Gamma$ and call it $A + B$. It is clear that this operation is commutative. Also, if $A = O$ then clearly, $A + B = B$ and hence $O$ is the identity element. Also, in order to construct the negative of $A$, we first draw a tangent at $O$ to $\Gamma$ and let it intersect the curve again at $O'$. We then join $A$ and $O'$ and then the point of intersection of this with $\Gamma$ will be clearly equal to $-A$. The only difficulty is in proving that this operation is associative and this is where the result that we proved in the above theorem comes handy.

Let $A, B, C$ be any three points on $\Gamma$. Put $\tau(A, B) = P, \tau((A+B), C) = Q, \tau(B, C) = R$. We must show that $\tau(A, (B+C)) = Q$ in order to show that $A+(B+C) = (A+B)+C$. This is the same as showing that $A, B + C, Q$ are collinear.

Consider the cubic which is the product of the three lines $ABP, C(A + B)Q$ and $O(B + C)R$. This intersects $\Gamma$ in nine points. Amongst these nine points, observe that $CBR$ are collinear. Therefore, by a previous theorem, there exists a conic $\Delta$ such that

$$\Gamma \cap \Delta = \{A, O, , B + C, A + B, P, Q\}.$$

Once again, $O, A + B, P$ are collinear. Hence, there must exist a line $L$ that contains the remaining three points. ♠.

**Exercise:**

(1) On a non singular cubic, work out

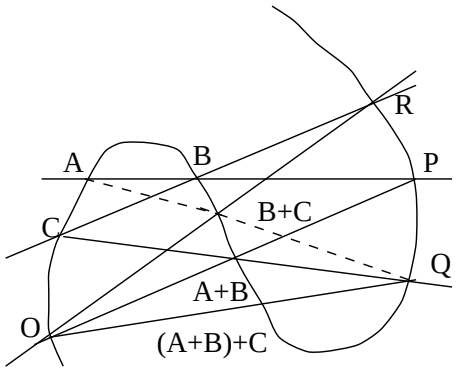


**Fig. 1**

(i) how to construct $P + P$ for any $P$.

(ii) what happens if $O$ is an inflection point.

(2) Show that a plane cubic can have at most one singular point, and that too of multiplicity 2 only.

(3) Show that if $D$ is a singular point on a cubic $\Gamma$ then $\Gamma \setminus \{D\}$ forms an abelian group, the additive operation being defined in the same fashion.

(4) Show that three points $A, B, C$ on a cubic are collinear iff $A + B + C = 0$.

(5) Of course other varieties also admit group structure. Let $\Gamma$ be an irreducible conic and $0, 1, \infty$ be three points on it. Then $\Gamma \setminus \{\infty\}$ admits a commutative group law written additively $A + B$ defined as in the following figure. Likewise $\Gamma \setminus \{0, \infty\}$ forms a multiplicative commutative group $X.Y$, defined as in the fugure below. Verify these statements.

$4^{th}$ March 99

**Theorem 21.1** *The operations of addition and taking the negative on a non singular cubic are regular functions.*

**Proof:** Let $\Gamma$ be a non singular cubic, $\alpha : \Gamma \times \Gamma \longrightarrow \Gamma$ be the operation of addition and let $\eta : \Gamma \longrightarrow \Gamma$ be the operation of taking negative, i.e., $\alpha(A, B) = A + B; \eta(A) = -A$. We have to show that these mappings are regular. Let us define $\tau : \Gamma \times \Gamma \longrightarrow \Gamma$ as follows: Given $A, B$ let $\tau(A, B)$ denote the third point of intersection of the line joining

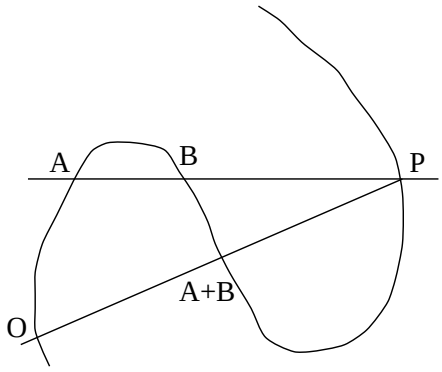


**Fig. 2**

$A, B$ with $\Gamma$. Then we know that $\alpha(A, B) = \tau(\tau(A, B), O)$. Therefore, if we show that $\tau$ is a regular function, then it follows that $\alpha$ is also regular. Similarly, $\eta(A) = \tau(A, A_0)$ where $A_0$ is the third point of intersection of the tangent line at $O$. Hence, it would follow that $\eta$ is also regular.

Now the line joining $A$ and $B$ is represented by $\lambda A + \mu B$ for $[\lambda, \mu] \in \mathbb{P}^1$. The points of intersection of this line with the cubic are given by the solutions of $F(\lambda A + \mu B) = 0$ which is a homogeneous polynomial of degree 3 in $\lambda, \mu$ and with coefficients which are polynomials in $A, B$. When $A, B \in \Gamma$, it must have two of its factors equal to $\lambda$ and $\mu$ respectively. This means that

$$F(\lambda A + \mu B) = \lambda\mu\gamma(\lambda, \mu)(modF) \tag{21.1}$$

for some homogeneous linear polynomial $\gamma(\lambda, \mu) = a(A, B)\lambda + b(A, B)\mu$ say where $a, b$ are elements of the algebraic closure of the function field $k(X_0, X_1, X_2)$. But then comparing the coefficients on either side of (21.1), it follows that $a, b$ are actually polynomials in $A, B$. By the homogeneity of $F$, it follows that we can choose $a, b$ to be homogeneous of the same degree. Therefore $\tau(A, B) = [b(A, B)A - a(A, B)B]$ is regular. ♠

**Remark 21.1** *A variety with a group law wherein the multiplication and the inverse are regular maps is called a group variety. They are no doubt topological groups ( indeed, Lie groups). It turns out that on a projective variety, we can only have commutative*

*group laws. Hence, they are called abelian varieties. Thus what we have seen just now amounts to saying that a non singular cubic forms an abelian variety.*

# Chapter 22

# Inflection Points

Given a projective plane curve $\Gamma$, defined by $F(X_0, X_1, X_2) = 0$, let us now study the inflection points on them. For any two points $\mathbf{x} = (x_0, x_1, x_2), \mathbf{y} = y_0, y_1, y_2)$, write

$$F(\mathbf{x} + \lambda\mathbf{y}) = F(\mathbf{x}) + \lambda(\sum_i \frac{\partial F}{\partial x_i} y_i) + \lambda^2(\sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j} y_i y_j) + \cdots$$

Here $\dfrac{\partial F}{\partial x_i}$ denotes $\dfrac{\partial F}{\partial X_i}|X = \mathbf{x}$, etc. Now, $\mathbf{x} \in \mathbf{\Gamma}$ iff $F(\mathbf{x}) = 0$. Further, it is a simple point iff $\sum_i \frac{\partial F}{\partial x_i} Y_i \not\cong 0$ and then $\sum_i \frac{\partial F}{\partial x_i} Y_i$ gives the equation of the tangent line at $X = \mathbf{x}$. Moreover, the order of tangency is $\geq 2$, iff $\sum_i \frac{\partial F}{\partial x_i} Y_i$ divides $\sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j} Y_i Y_j$. Thus, we have obtained an algebraic condition for a particular point on $\Gamma$ to be an inflection point.

The second quantity is a degree 2 homogeneous polynomial. Recall from your school geometry that a conic is reducible (i.e., a product of two st. lines) iff the determinant of the coefficient matrix vanishes. Thus $X = \mathbf{x}$ is an inflection point implies that it satisfies the equation,

$$\begin{vmatrix} \dfrac{\partial^2 F}{\partial X_0^2} & \dfrac{\partial^2 F}{\partial X_0 X_1} & \dfrac{\partial^2 F}{\partial X_0 X_1} \\ \dfrac{\partial^2 F}{\partial X_1 X_0} & \dfrac{\partial^2 F}{\partial X_1^2} & \dfrac{\partial^2 F}{\partial X_1 X_2} \\ \dfrac{\partial^2 F}{\partial X_2 X_0} & \dfrac{\partial^2 F}{\partial X_2 X_1} & \dfrac{\partial^2 F}{\partial X_2^2} \end{vmatrix} = 0.$$

This is called the *Hessian* of $F$ and denote it by $H_F$.

We first observe that the property of being a point of inflection on a curve is a projective invariant, i.e., if $A$ is a projective transformation then $\mathbf{x}$ is a point of inflection of $\Gamma$ iff $A\mathbf{x}$ is a point of inflection on $A\Gamma$. For, first of all, $\mathbf{x}$ is a simple point of $\Gamma$ iff $A\mathbf{x}$ is so on $A\Gamma$. Then for the tangent line $L$ at $\mathbf{x}$, we have $i(\Gamma, L; \mathbf{x}) = i(A\Gamma, AL; A\mathbf{x})$ by the projective invariance of the local multiplicity.

We claim that the vanishing of the Hessian is a criterion for an inflection point.

**Theorem 22.1** *Over an algebraically closed field of characteristic* 0, *a simple point* $\mathbf{x}$ *of a projective plane curve* $\Gamma$ *is an inflection point iff it satisfies* $H_F(\mathbf{x}) = 0$.

**Proof:** Multiply the columns of $H$ by $X_i$ respectively and add them to the first one, and use Euler's formula to see that

$$X_0 H = \begin{vmatrix} (n-1)\dfrac{\partial F}{\partial X_0} & \dfrac{\partial^2 F}{\partial X_0 \partial X_1} & \dfrac{\partial^2 F}{\partial X_0 \partial X_2} \\ (n-1)\dfrac{\partial F}{\partial X_1} & \dfrac{\partial^2 F}{\partial^2 X_1} & \dfrac{\partial^2 F}{\partial X_1 \partial X_2} \\ (n-1)\dfrac{\partial F}{\partial X_2} & \dfrac{\partial^2 F}{\partial X_2 \partial X_1} & \dfrac{\partial^2 F}{\partial^2 X_2} \end{vmatrix}$$

Now multiply the rows of this matrix by $X_i$ and add them to the first row to obtain

$$X_0^2 H = \begin{vmatrix} n(n-1)F & (n-1)\dfrac{\partial F}{\partial X_1} & (n-1)\dfrac{\partial F}{\partial X_2} \\ (n-1)\dfrac{\partial F}{\partial X_1} & \dfrac{\partial^2 F}{\partial^2 X_1} & \dfrac{\partial^2 F}{\partial X_1 \partial X_2} \\ (n-1)\dfrac{\partial F}{\partial X_2} & \dfrac{\partial^2 F}{\partial X_2 \partial X_1} & \dfrac{\partial^2 F}{\partial^2 X_2} \end{vmatrix}$$

Let us now make some simplifying projective transformations. Assume that $\mathbf{x} = [1, 0, 0]$ and $Y = 0$ is the tangent at this point. If $\mathbf{x}$ is not an inflection point, then we have

$$F(1, X, Y) = aY + cX^2 + \cdots,$$

with $ac \neq 0$. This means that

$$H(1,0,0) = \begin{vmatrix} 0 & 0 & n-1 \\ 0 & 2c & \cdots \\ (n-1)a & \cdots & \cdots \end{vmatrix} = -2ac(n-1)^2 \neq 0.$$

Thus the Hessian does not vanish at $[1, 0, 0]$. ♠

**Corollary 22.1** *Every non singular cubic has at least one point of inflection.*

**Proof:** For, the Hessian is a homogeneous polynomial of degree 3 and any two prjective curves have to intersect. ♠

**Remark 22.1** *Observe that we have not yet asserted that the Hessian is non zero. so far, this was not necessary, and soon, it will follow as a consequence of what we prove.*

**Lemma 22.1** *Every non singular cubic over an algebraically closed field is projectively equivalent to a standard one, such as*

$$Y^2Z - X(X-Z)(X-cZ) = 0$$

where $0 \neq c \in k$.

**Proof:** We shall start with an arbitrary non singular cubic and apply a number of projective linear transformations to bring it to the above form. First we map an inflection point onto the point $[0,0,1]$. Putting $Y = 1$, the cubic then looks like

$$f_3(X,Z) + f_1(X,Z)Z + \lambda Z = 0,$$

where $\lambda \in k$ is non zero, $f_1$ is homogeneous linear and $f_3$ is homogeneous cubic not divisible by $Z$. Dividing out by $\lambda$ we may as well assume that $\lambda = 1$. Going back to the homogeneous form we now have

$$f_3(X,Z) + f_1(X,Z)YZ + ZY^2 = 0.$$

Now make the transformation $X = X', Y' = Y + tX, Z = Z'$ for a suitable $t \in k$ so that the $XYZ$ term disappears. Next, make the transformation $X = X', Y' = Y + sX$ and $Z' = Z$ so that the $YZ$ term also disappears. Now the equation has taken the form $g_3(X,Z) + Y^2Z = 0$. We now observe that the linear factors of $g_3$ are distinct, since the curve is non singular. Hence the equation is of the form

$$Y^2 - d(X-aZ)(X-bZ)(X-cZ) = 0.$$

Replace $X$ by $rX$ where $r^3 = d$, and assume that $d = 1$. Finally, take the transformation which maps $[0,0,1],[1,a,0],[1,b,0]$ to $[0,0,1],[1,0,0],[1,1,0]$. This will map the cubic to the required form. ♠

We shall now compute the Hessian of this 'standard form' of the cubic. This is equal to

$$\begin{vmatrix} -2cX & -2cZ + 2(1+c)X & 2Y \\ -2cZ + 2(1+c)X & -6X + 2(1+c)Z & 0 \\ 2Y & 0 & 2Z \end{vmatrix}$$

$$= 8[cZX(3X - (1+c)Z) - Z(cZ + (1+c)X)^2 + Y^2(3X - (1+c)Z)]$$

At the inflection point $P = [0,0,1]$, we see that this cubic takes the form

$$3X - (1+c)Z + \text{ higher degree terms.}$$

Therefore, $P$ is a smooth point of the Hessian and the tangent at this point is different from the tangent to $\Gamma$ (which is given by $Z = 0$.) Hence, it follows that $i(F,H;P) = 1$. Due the remark that the intersection number is a projective invariant, we have proved:

**Theorem 22.2** *The Hessian of $\Gamma$ cuts $\Gamma$ at an ordinary point of inflection with multiplicity one.*

Combining with Bezout's theorem, we conculde:

**Theorem 22.3** *There are exactly nine points of inflection on a non singular cubic.*

**Remark 22.2** *As promised earlier, we now see that the Hessian of a smooth cubic is never identically zero. The theorem 22.2 is true for Hessian of a smooth curve of higher degree also, viz., it cuts the curve at an inflection point with multiplicity 1. (Indeed, it is possible to extract a proof of this fact from the arguments given above. We leave this to you as an optional exercise.) Since, the entries of the Hessian matrix are homogeneous of degree n-2, the Hessian itself is of order 3(n-2). Therefore, there are precisely 3n(n-2) points of inflection on a smooth curve of degree n.*

$9^{th}$ March. 99

**Theorem 22.4** *A smooth cubic does not admit any rational parameterization.*

**Proof:** We may assume that $k = \bar{k}$. We have seen that projectively any smooth cubic is equivalent to

$$Y^2Z - X((X-1)(X-c), \qquad c \in k \setminus \{0,1\}.$$

So, it suffices to show that the affine curve

$$Y^2 - X(X-1)(X-c) = 0 \tag{22.1}$$

does not admit any rational parameterizations. So, begin with a parameterisation $t \mapsto (f(t), g(t))$ of (22.1) with $f = p/q$ and $g = r/s$ say where $p, q, r, s$ are in $k[t]$ with $(p, q) = (1)$ and $(r, s) = (1)$ and plan to show that $p, q, r$ and $s$ are all constants.

Substituting in (22.1) and clearing the denominators we obtain

$$r^2q^3 = p(p-q)(p-cq)s^2 \tag{22.2}$$

By the co-primeness, we see that $q^3 = \alpha s^2$. It follows that $q = \alpha(s/q)^2$ is a square in $k[t]$. Also, it follows that $r^2 = \alpha^{-1}p(p-q)(p-cq)$ and once again due to co-primeness, we obtain that each of $p, p-q, p-cq$ is a square in $k[t]$. Now the proof is completed by the following lemma which is version of Fermat's method of *Infinite Descent* in the polynomial ring $k[t]$.

**Lemma 22.2** *Let $k = \bar{k}$, and $p, q \in k[t]$ be any two co-prime elements. Assume that four linear combinations of $\lambda_i p + \mu_i q$ are squares in $k[t]$ where the ratios $[\lambda_i, \mu_i] \in \mathbb{P}^1_k$ are distinct. Then $p, q \in k$.*

**Proof of the lemma:** Assume that that there do exist such polynomials at least one of which is of positive degree. Then we can pick one such pair $p, q$ for which $\max\{deg\, p, deg\, q\} > 0$ is minimum. Since both the hypothesis and the conclusion are not affected by a non singular linear transformation, we may assume that $p, q, p-q, p-\lambda q$ are all squares in $k[t]$. (Ex. Give full details of this step.) Let then $p = u^2, q = v^2, u, v \in k[t]$ being co-prime. Clearly,

$$\max\{deg\, u, deg\, v\} < \max\{deg\, p, deg\, q\}.$$

Since both

$$p - q = u^2 - v^2(u - v)(u + v)$$

and

$$p - \lambda q = u^2 - \lambda v^2 = (u - \alpha q)(u + \alpha q)$$

where $\alpha = \sqrt{\lambda}$ are squares in $k[t]$, due to the co-primeness of $u$ and $v$, it follows that all the four $u - v, u + v, u - \alpha q, u + \alpha q$ are squares in $k[t]$. This contradicts the minimality of $\max\{deg\, p, deg\, q\}$ thereby completing the proof of the lemma. ♠

So, the proof of the theorem is also complete. ♠

In contrast, one can parameterise any irreducible cubic with a singularity. Consider the case of a cubic with a cusp. We may assume that the cups is at the origin and $Y = 0$ is the tangent. Then the cubic takes the form $Y^2 = f_3(X, Y)$ in the affine co-ordinates $X, Y$ where $f_3$ is homogeneous of degree 3 and not divisible by $Y$. Therefore the homogenisation of this looks like $ZY^2 = f_3(X, Y)$. Now de-homogenise this with respect to $Y$ to obtain an affine cubic in $X, Z$ co-ordinate plane. This curve has the form

$$Z = f_3(X, 1) \tag{22.3}$$

which is obviously parameterized by $t \mapsto (f_3(t, 1), t))$. In order to get back a parameterisation of the original affine curve, we can now reverse the process of homogenisation and de-homogenisation as follows. First of all, the homogenisation of the parameterization of (22.3) is given by

$$[t, s] \mapsto [f_3(t, s), ts^2, s^3]$$

So, now de-homogenise domain with respect to $s$ and co-domain with respect to $Z$ to obtain

$$t \mapsto \left( \frac{t}{f_3(t,1)}, \frac{1}{f_3(t,1)} \right).$$

Likewise, we can carry out the discussion of an irreducible cubic with an ordinary double point also.

**Remark 22.3**

*(1) For the cuspidal curve $Y^2 = X^3$, we could directly take $t \mapsto (t^2, t^3)$ as a parameterization. Compare this with parameterization obtained from the above method. Similarly, for the nodal curve $Y^2 - X^2 = X^3$, we can directly take $t \mapsto (t^2 - 1, t(t^2 - 1)^2)$ as a parameterization. Compare this with the one obtained by the above method.*

*(2) There is a subtle reason why we kept changing the affine planes. Even though our aim is to give a rational parameterization, our mind usually hunts for polynomial parameterizations. This is certainly not possible in general. Indeed, a necessary condition for the existence of a polynomial parameterization of an affine curve is that its closure in the projective space should have only one extra point. That is, the corresponding projective curve should have only 'one point at infinity.'*

# Chapter 23

# Linear Systems

In this section, we shall really have a lively game with points, lines, conics and cubics. For any $d \geq 1$, let us introduce the notation

$$S_d = \{0\} \cup \{\text{forms of degree d in } X, Y, Z\}$$

Also for $d = 0$, we shall define $S_0 := k$.

Let us sum up some of the basic facts about $S_d$.

(1) Recall that by a 'form' we mean a homogeneous polynomial. We know that $S_d$ is a vector space over the ground field $k$. Since there are precisely $\binom{d+2}{2}$ monomials of degree $d$, which form a $k$-basis for $S_d$, the dimension of this vector space is $\binom{d+2}{2.}$ A non zero element $F$ of $S_d$ defines a curve of degree $d$ in $\mathbb{P}^2$. Indeed any non constant multiple also defines the same curve. Nevertheless, we shall use the same symbol to denote the form and the corresponding curve, whenever there is no confusion.

(2) Now let $P_1, \ldots, P_n \in \mathbb{P}^3_k$ be any $n$ points.

$$S_d(P_1, \ldots, P_n) = \{f \in S_d \ : \ f_d(P_i) = 0, \ i = 1, \ldots, n\} \cup \{0\}.$$

This just means that $P_i$ is a point on the curve $F = 0$ for $F \in S_d(P_1, \ldots, P_n)$. Observe that it is possible that some of the $P_i$ are repeated also. Since no point can be of multiplicity greater than $d$ on a curve of degree $d$, we should assume that *there are no* $(d+1)$*-fold repetitions in* $P_1, \ldots, P_n$. (Another way is to define $S_d(P_1, \ldots, P_n) = 0$ if the above condition is not fulfilled.) Since for each $P_i$, the condition that $F(P_i) = 0$ is a linear one for $F$, it follows that $S_d(P_1, \ldots, P_n)$ is a subspace of $S_d$ of dimension $\geq \binom{d+2}{2} - n$ OR $S_d(P_1, \ldots, P_n) = (0)$.

(3) (From now on, assume that $k$ is an infinite field.)

**Theorem 23.1 Pealing Off Lemma**: *Let $C$ be any irreducible form of degree $m \leq d$. $P_1, \ldots, P_r \in C$ and $P_{r+1} \ldots, P_n \notin C$, for some $r > md$. Then*

$$S_d(P_1, \ldots, P_n) = C \cdot S_{d-m}(P_{r+1}, \ldots, P_n).$$

**Proof:** For, if $F \in S_d(P_1, \ldots, P_n)$ then by Bezout's theorem $F \cap C$ has at most $md$ points, unless $C$ is a factor of $F$. This gives $S_d(P_1, \ldots, P_n) \subset C \cdot S_{d-m}(P_{r+1}, \ldots P_n)$. The other way containment is obvious. ♠

(4) Let us consider the properties of $S_1$. Clearly dim $S_1 = 3$ and dim $S_1(P) = 2$. If $P_1, P_2$ are distinct then dim $S_1(P_1, P_2) = 1$. For $n \geq 3$, if $P_i$ are all collinear, then $\dim S_1(P_1, \ldots, P_n) = 1$; otherwise $S_1 = (0)$.

(5) Let us now study $S_2$.

**Theorem 23.2** *Let $n \leq 5$ and $P_1, \ldots, P_n$ be distinct points such that no four of them are collinear. Then* dim $S_2(P_1, \ldots, P_n) = 6 - n$.

**Proof:** We have only to prove that $\dim S_2(P_1, \ldots, P_n) \leq 6 - n$. First consider the case $n = 5$. By Bezout's theorem, if $C_1$ and $C_2$ are linearly independent irreducible conics, then they cannot have more than four points in common. Now assume that one of $C_1, C_2$, say $C_1$ is a product of two lines, $C_1 = L_1.L_2$. One of these $L_i$ should contain at least three of the $P_j$ and hence is a factor of $C_2$. This means that $C_2$ is also reducible $C_2 = L_1.L_3$, say. But then $L_3$ should contain two other points which are not on $L_1$, it follows that $L_3 = L_2$. Therefore, $C_1$ and $C_2$ are linearly dependent. Hence the result.

Now, suppose $n < 5$. Choose additional points $P_{n+1}, \ldots, P_5$ so that no four of $P_1, \ldots, P_5$ are on the same line. Then

$$1 = \dim\ S_2(P_1, \ldots, P_5) \geq \dim\ S_2(P_1, \ldots, P_n) - (5 - n)$$

from which the claim follows. ♠

(6) Given any arbitrary six points in $\mathbb{P}^2_k$, there may not be any conic passing through them. Try to give at least one specific example.

$11^{th}$ March 99

(7) Let us now make a definition. By a *pencil* of $d$ forms we mean the family

$\lambda F + \mu G$ of $d$-forms where $F, G$ are any two linearly independent elements of $S_d$ and $\lambda, \mu \in k$. Thus a pencil is nothing but a 2-dimendionl subsapce of $S_d$. If we think them of curves then they actually form a 1-dimensional family (in $\mathbb{P}S_d$) and is refered as a pencil of curves of degree $d$. There are a number of interesting geometric properties of

pencils. To begin with we may want to know whether there are any irreducible elements in it, or the number of common points or actualy to find out what are these common points and so on.

**Theorem 23.3** *Given any pencil of conics, either all the conics in it are reducible or at most three of them are; over the field of real numbers, there is at least one reducible one.*

**Proof:** Let us denote the determinant of the symmetric matrix corresponding to a conic $C$ by $det(C)$. Then observe that

$$g(\lambda, \mu) = det(\lambda F + \mu G)$$

is a homogeneous polynomial in $\lambda, \mu$ of degree 3. If this is not identically zero, it can have at most three linear factors. Over the field of real numbers, it should have at least one linear factor. ♠

**Example 23.1** *Start with any four points $P_1, \ldots, P_4$, no three of them are collinear. As seen above* dim $S_2(P_1, \ldots, P_4) = 2$. *Hence there is a unique pencil of conics such that each member of it passes through these points. Such a pencil is simply called a* pencil through $P_1, P_2, P_3, P_4$. *Out of these, exactly three members are degenerate (reducible). If we denote the line through $P_i, P_j$ by $L_{i,j}$ then these conics are: $L_{1,2}.L_{3,4}, L_{1,3}.L_{2,4}, L_{1,4}.L_{2,3}$. Indeed, we can represent every member of the pencil by*

$$\lambda L_{1,2}.L_{3,4} + \mu L_{1,3}.L_{2,4}.$$

**Example 23.2** *Let us consider the problem of finding the points of intersection of a pencil generated by two (distinct) conics $C_1, C_2$. Clearly these points will be nothing but the four points of intersection of $C_1$ with $C_2$. Certain special cases of this could be of specific interest in some areas of mathematics and applications. Let us take a very special case:*

$$C_1 : Y^2 + 2aY + 2bX + c = 0; \; C_2 : Y - X^2 = 0.$$

*We first find three values of $[\lambda, \mu]$ for which the conic $\lambda C_1 + \mu C_2$ is reducible. This is the same as solving the cubic*

$$0 = g(\lambda, \mu) = \left| \lambda \begin{bmatrix} 0 & 0 & b \\ 0 & 1 & a \\ b & a & c \end{bmatrix} + \mu \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{bmatrix} \right|.$$

*Corresponding to these three values of* $[\lambda, \mu]$, *we get three conics which represent pair of st. lines. Put* $a = 1, b = 1$ *and* $c = 5/4$. *Then*

$$g(\lambda, \mu) = 4\lambda^3 + \lambda^2\mu - 4\lambda\mu^2 - \mu^3 = (4\lambda + \mu)(\lambda + \mu)(\lambda - \mu).$$

*Taking* $[\lambda, \mu] = [1, -4], [1, -1]$ *we get two quadratics which can be easily factored. We have to write down the factorisations of any two of these conics now. The next step is to find the intersection points. The computational details are left to you as an exercise.*

*Historically, the theme that we discussed just now has its genesis in the solution of quartics. The substitution* $y = x^2$ *first converted the problem into finding the common solutions of* $y = x^2$ *and another quadratic.*

(8) Let us now turn our attention to cubics again. Let us say that a finite set of points are *conconic,* if they lie on a conic.

**Theorem 23.4** *Suppose* $P_1, \ldots, P_8$ *are distinct points of* $\mathbb{P}^2$ *no four of them collinear and no seven of them conconic. Then* $\dim S_3(P_1, \ldots P_8) = 2$.

**Proof:** Once again we have only to prove that $\dim S_3(P_1, \ldots P_8) \leq 2$. We assume this is not true and arrive at a contradiction. We have to consider various cases:
**Case 1**: Suppose no three of $P_i$ are collinear and no six are conconic. Choose two points $P_9, P_{10}$ on the line $P_1P_2$ and distinct from all the $P_1, \ldots, P_8$. Then

$$\dim S_3(P_1, \ldots, P_{10}) \geq \dim S_3(P_1, \ldots, P_8) - 2 \geq 1.$$

So choose a cubic non zero cubic $F$ passing through the ten points. By the Pealing Off Lemma 23.1, we have, $F = L.G$ for a conic $G$ passing through the six points $P_3, \ldots, P_8$. This is a contradiction.
**Case 2**: Suppose three of the points are collinear, say a line $L$ passes through $P_1, P_2, P_3$. Choose $P_9$ on this line distinct from all the other points. Then again

$$\dim S_2(P_4, \ldots, P_8) = \dim S_3(P_1, \ldots, P_9) \geq 2.$$

Since no four of $P_4, \ldots, P_8$ are collinear, this contradicts theorem 23.2.
**Case 3**: Suppose six of the points are conconic, say $C$ is a conic passing through $P_1, \ldots, P_6$. Choose $P_9$ as earlier on $C$ and then we obtain that $\dim S_1(P_7, P_8) \geq 2$ which is again a contradiction. ♠

Let us have some interesting consequences:

**Corollary 23.1** Suppose two cubics $F_1, F_2$ intersect in exactly nine distinct points. Then any other cubic which passes through eight of the points passes through the nineth also.

**Proof:** Observe that the two cubics cannot have any common components. From this it follows that any eight points of intersection satisfy the hypothesis of the earlier theorem. (For, if any four of them are collinear, then the line passing through these points is contained in both cubics. Likewise, if seven of them were conconic, then a conic will be contained in both of them.) Therefore, dim $S_3(P_1, \ldots, P_8) = 2$. This means that every other cubic in $S_3(P_1, \ldots, P_8)$ is a linear combination of $F_1$ and $F_2$. The result follows.♠

**Corollary 23.2 Pascal's Theorem** Let $A, B, C, D, E, F$ be six points no three of them collinear. Extend all the six sides of the hexagon suitably so that the pair of opposite sides of the hexagon meet at $P, Q, R$. Then $P, Q, R$ are collinear iff $ABCDEF$ are conconic.

**Proof:** Consider the two cubics, $AB + CD + EF$ and $BC + DE + FA$ which intersect exactly in nine points $A, B, C, D, E, F, P, Q, R$. (Why $P, Q, R$ are distinct and distinct from the given six points?) Now suppose $P, Q, R$ lie on a line $L$. Choose a conic $H$ passing through $A, B, C, D$ and $E$. Then $L.H$ is a cubic which passes through eight of the nine points and hence it must pass through $F$ also. This means that $H$ passes through the given six points. The converse is proved similarly. ♠

There are of course several proofs of this ancient result. Prove this using Peeling Off theorem directly.

# Chapter 24

# The Dual Curve

Let $\Gamma$ be an irreducible projective plane curve of degree $m \geq 2$, given by $F = 0$. At a smooth point of $P \in \Gamma$, the equation of the tangent is given by

$$\sum_i \frac{\partial F}{\partial p_i} Y_i = 0.$$

Therefore, the rational mapping $\mathcal{T}$

$$[X_0, X_1, X_2] \mapsto \left[\frac{\partial F}{\partial X_0}, \frac{\partial F}{\partial X_1}, \frac{\partial F}{\partial X_2}\right]$$

takes the smooth points of the curve $\Gamma$ to the points in the dual space $\widehat{\mathbb{P}^2}$ that represent the tangent lines to $\Gamma$ at the respective points. Let $\widehat{\Gamma}$ denote the closure of $\mathcal{T}(\Gamma)$. It turns out that $\widehat{\Gamma}$ is again a curve and we call it the *dual curve* of $\Gamma$. Let us prove that $\widehat{\Gamma}$ is also a curve. Consider first the case when $\Gamma$ is smooth. It follows that in this case, $\mathcal{T}$ is a regular mapping. We then know that at the co-0rdinate ring level the induced map $\mathcal{T}^\star : k[\widehat{\Gamma}] \longrightarrow k[\Gamma]$ is injective. Therefore, the transcendence degree of $k[\widehat{\Gamma}]$ has to be at most one. Thus it remains to see that this degree is not equal to 0. Observe that since $\Gamma$ is irreducible, it follows that so is $\widehat{\Gamma}$. Thus we have to show that $\widehat{\Gamma}$ is not a singleton. Assuming on the contrary, suppose this singleton is $[y_0, y_1, y_2]$. Consider the line $L : \sum_i y_i X_i = 0$. Now, the Euler's formula

$$mF(X_0, X_1, X_2) = \sum_i \frac{\partial F}{\partial X_i} X_i$$

tells us that if $[X_0, X_1, X_2] \in \Gamma$ then $L(X_0, X_1, X_2) = 0$ which is a contradiction to the fact $\Gamma$ is an irreducible curve of degree $m \geq 2$.

In the general case, $\mathcal{T}$ will not be defined at the singularities of $\Gamma$ and it is only a rational mapping. Nevertheless the above arguments go through if we work directly with the function fields instead of co-ordinate rings.

Why did we choose to give such a 'proof' of this fact instead of trying write down an equation for the dual curve. The reason is, let alone get an explicit equation, even to show the existence of such a curve algorithmically seems to be a very difficult task. Let us try to understand this by some simple examples. Consider the curve $C$

$$X_0^m + X_1^m + X_2^m = 0$$

which is clearly a smooth curve( $ch\,(k) = 0$). The dual curve consists of points

$$[mx_0^{m-1}, mx_1^{m-1}, mx_2^{m-1}], \quad [x_0, x_1, x_2] \in C.$$

Thus the equation of the dual curve is obtained by 'rationalising'

$$(Y_0^{1/m-1})^m + (Y_1^{1/m-1})^m + (Y_2^{1/m-1})^m = 0$$

that is not easy. For $m = 2$ however, it is already a polynomial equation

$$Y_0^2 + Y_1^2 + Y_2^2 = 0.$$

Even for $m = 3$ we can do this without much trouble. Take one of the terms on one side and then take squares. We then have all terms except one are free from fractional exponents. Now take this exceptioanl term to one side, again take squares and obtain

$$Y_0^6 + Y_1^6 + Y_2^6 - 2(Y_0^3Y_1^3 + Y_1^3Y_2^3 + Y_0^2Y_0^3) = 0.$$

For higher degrees this task becomes more and more difficult.

The degree of the dual curve is called the *class* of the curve. Thus we see that the quadratic and cubic above are of class 2 and 6 respectively. It can be seen that the class of a curve of degree $m$ cannot be greater than $m(m-1)$. For, given any point $P$ in the plane, we can draw at most $m(m-1)$ tangents to a curve of degree $m$. This means that the dual curve intersects the dual line $L_P$ in at most $m(m-1)$ points. The class may actually drop. Indeed, this is invariably the case for a singular curve. Before that, let us see what happens to a smooth curve. Suppose that $Q = [q_0, q_1, q_0]$ is a point of $\Gamma$ and a line through $P = [p_0, p_1, p_2]$ is tangential to $\Gamma$. This means that

$$F(q_0, q_1, q_2) = 0; \quad \sum_i \frac{\partial F}{\partial q_i} p_i = 0.$$

Therefore the point $Q$ is on the intersection $\Gamma$ and the curve given by

$$\sum_i \frac{\partial F}{\partial X_i} p_i = 0. \tag{24.1}$$

The latter curve is called the *polar curve* of $\Gamma$ with respect to the point $P$. Its degree is obviously $m-1$. Of course, we define the polar of a curve with respect to a point $P$ which is not on the curve and then the lhs of 24.1 does not vanish identically(why?).

Hence the two curves can have at most $m(m-1)$ points of intersection.

In order to study the intersection pattern of these two curves at any of the intersection point $Q$, we may assume that $Q = [1, 0, 0]$. We may also assume that the tangent at $Q$ is given by $X_2 = 0$ and $P = [0, 1, 0]$. Therefore the equation of the polar is $\dfrac{\partial F}{\partial X_1} = 0$. Passing on to affine co-ordinates $X, Y$, the equation of the curve $\Gamma$ and that of the polar are respectively

$$F(1, X, Y) = f(X, Y) = Y + f_2(X, Y) + \cdots + f_m(X, Y) = 0; \quad \sum_{i \geq 2} \frac{\partial f_i}{\partial X} = 0,$$

where $f_i(X, Y)$ are homogeneous of degree $i$.

Now we know that $i(\Gamma, \mathcal{P}; Q) = 1$ iff the tangent to the polar at $Q = (0, 0)$ is not on the $X$-axis. This is the same as saying that $Y$ does not divide $f_2$. This, in turn is the same as saying that $Q$ is not an inflection point of $\Gamma$.

We also know that any smooth curve has only finitely many inflection points. Take the union $A$ of all the tangents at all inflection points and let now $P$ be a point not on $A$. Then it follows that the polar $\mathcal{P}$ with respect to $P$ of $\Gamma$ intersects $\Gamma$ in exactly $m(m-1)$ points. This proves that

**Theorem 24.1** *The class of a smooth curve of degree $m$ is equal to $m(m-1)$.*

In particular, dual of a smooth conic is again a conic. Now consider the case of a singular curve. Before discussing the general case, let us take up an example. Consider the standard cuspidal curve $C$ :

$$X_0 X_2^2 - X_1^3 = 0.$$

The co-ordinates of the dual curve are $[x_2^2, -3x_1^2, 2x_0x_2]$ for $[x_0, x_1, x_2] \in C$. We put

$$Y_0 = x_2^2, \quad Y_1 = -3x_1^2, \quad Y_2 = 2x_0x_2$$

and eliminate $x_i$. We see that $Y_1^3 = -27x_1^6 = -27(x_0x_2^2)^2 = (-27/4)Y_2^2Y_0$. Thus

$$4Y_1^3 + 27Y_0Y_2^2 = 0$$

is the equation of the dual curve. This is again a cuspidal cubic. Thus we see that in case of a singular curve the class can go down quite drastically. We shall leave it you to work out the equation of the dual of the standard nodal cubic $Z(Y^2 - X^2) = X^3$ and see that it is of degree 4. Indeed, we have

**Theorem 24.2 Plücker's Formula** *Let $\Gamma$ be a plane curve of degree $m$ with $s$ ordinary double points and $t$ ordinary cusps and no other singularities. Then the class of $\Gamma$ is equal to $m(m-1)-2s-3t$.*

**Proof:** As before we must count the number of distinct points of intersection of $\Gamma$ with its polar curve w.r.t a generic point. The discussion above holds verbatim in case the intersection of the two curves is a smooth point, viz, $i(\Gamma, \mathcal{P}; Q) = 1$ whenever $Q \in \Gamma$ is smooth and $P$ is taken sufficiently generic. We also see that at any singular point the partial derivatives vanish identically and hence every polar curve passes through every singular point. So, we shall choose $P$ in such a way that
(i) $P$ does not lie on any of the tangent lines to $\Gamma$ at a point $Q$ which an inflection point, or a singularity.
(ii) For each ordinary double point singularity $Q \in \Gamma$, the the tangent to the polar at $Q$ is different from the two tangents to $\Gamma$.
(iii) For each cups $Q \in \Gamma$, the tangent to to the polar at $Q$ is of order 2.

For suppose that we have done such a choice for $P$. It then follows that

$$i(\Gamma, \mathcal{P}; Q) = \begin{cases} 1 & \text{if } Q \text{ is a smooth point} \\ 2 & \text{if } Q \text{ is node} \\ 3 & \text{if } Q \text{ is cusp.} \end{cases}$$

Now let us count the number of tangent lines from $P$ to $\Gamma$. For each smooth point $Q_i \in \Gamma \cap \mathcal{P}$ we get $PQ$ is a tangent and also $i(\Gamma; \mathcal{P}; Q) = 1$. For each node $Q$, the line $PQ$ is not a tangent whereas $i(\Gamma, \mathcal{P}; Q) = 2$. Likewise for a cusp $Q$, we have $i(\Gamma, \mathcal{P}, Q) = 3$ whereas $PQ$ is not a tangent. Thus if $r$ is the number of smooth points in $\Gamma \cap \mathcal{P}$, then by Bezouts' theorem, $r + 2s + 3t = m(m-1)$, whereas the number of tangents to $\Gamma$ from $P$ is equal to $r$.

In order to justify that the choice of $P$ is possible and indeed is generic, we begin with the first condition, which we have already seen is generic. Now choose the line at infinity to be such that it does not pass through any of the singularities. Then given a singularity $Q$ let us choose it to be the origin $Q = (0, 0)$. Now suppose $Q$ is a node and the affine equation of $\Gamma$ is of the form

$$Y^2 - X^2 + f_3(X, Y) + \cdots = 0.$$

Then for any point $P = [0, p_1, p_2]$ the linear term of the polar equation is of the form

$$2p_2Y - 2p_1X.$$

Therefore, if we choose $P$ so that $[p_1, p_2] \neq [1, \pm 1]$, then it satisfies (ii).

Next assume that $Q$ is an ordinary cusp so that

$$Y^2 + f_3(X, Y) + \cdots = 0$$

is the affine equation of $\Gamma$. In this case, we see that the line $Y = 0$ is a tangent to both $\Gamma$ and $\mathcal{P}$. However, we can choose $P$ in such a way that the degree 2 term in $\mathcal{P}$ is not divisible by $Y$. This is possible since $Q$ is an ordinary cusp and hence the cubic term in $\Gamma$ is not divisible by $Y$. Again, all that we have to do is to choose $p_1 \neq 0$. This completes the proof. ♠

As an application of he concept of dual curve, we can deduce the following theorem from Pascal's theorem.

**Theorem 24.3 Brianchon's Theorem:** *Given any hexagon in in the plane, the three diagonals are concurrent iff we can inscribe a conic in it.*

**Proof:** We have seen that the dual of a smooth conic is again a smooth conic.

Let us see what Pascal's theorem taken in the dual plane $\mathbb{P}^2$ means in the usual plane. Giving six points in $\mathbb{P}^2$ corresponds to giving six lines in $\widehat{\mathbb{P}^2}$. Taking the intersection of pairs of opposite sides corresponds to joining the opposite vertices of the hexagon formed by the six lines. That these three points are collinear corresponds to say that the three diagonals are concurrent. That the given six points lie on a conic corresponds to say that the six lines are tangential to a conic (the dual one). Thus we indeed see that Pascal's theorem and Brianchon's theorem are dual to each other. Hence one is true iff the other is. ♠

**Remark 24.1** *It is a fact that the dual of the dual curve is actually the given curve itself. we have not proved this statement. Also, it should be noted that we need use this fact in the proof of the above theorem.*

# Chapter 25

# Power Series

$25^{th}$ March 99

Consider a simple case of an irreducible affine plane curve $\Gamma$ given by $F(X,Y)=0$. Let us assume that $(0,0)$ is a simple point on the curve with $X$-axis as the tangent. We can then write $F(X,Y)=0$ as

$$Y = G(X,Y) \tag{25.1}$$

for some polynomial $G$ of order $\geq 2$. By substituting the expression on the rhs for $Y$, we get

$$Y = G(X, G(X,Y)) \tag{25.2}$$

This means that on the curve $\Gamma$, (25.2) is also satisfied. Since $\Gamma$ is irreducible, this means that

$$Y - G(X, G(X,Y)) = (Y - G(X,Y))H(X,Y) \tag{25.3}$$

for some polynomial $H$. It is also clear that $H(0,0)=1$. Thus (25.2) represents a curve with $\Gamma$ as the only one of its components passing through $(0,0)$.

We can keep playing this game again, by substituting for $Y$ on the rhs of (25.2) and the rhs the resulting equation and so on. The above conclusion will hold for all equations that we get successively

$$Y = G(X, G(X, \cdots G(X,Y)\cdots). \tag{25.4}$$

Since $Y$ terms in $G$ occur only terms of degree $\geq 2$, it follows that that in rhs of (25.2) they occur only in terms of degree $\geq 3$. Thus after repeating the process $n$-times the $Y$-term will occur only after $n+2$ degrees. If we ignore these terms, then we get a

curve which is an approximation to $\Gamma$ near $(0,0)$ and has the property that the rhs is now free from the $Y$-term. What we would like to do is not to ignore anything. So we keep repeating this process and in the limiting case, get a power series $f(X)$ in $X$ on the rhs:

$$Y = f(X). \tag{25.5}$$

This has both the properties:(i) the rhs is a function of $X$ alone and (ii) the component that passes through $(0,0)$ is precisely the curve $\Gamma$. Of course, we are lead to consider the question of convergence of the power series $f(X)$ also.

Recall that a formal power series in $n$ variables over a field $k$ consists of a formal sum

$$F(X) = \sum_i F_i(X) \tag{25.6}$$

where each $F_i$ is a homogeneous polynomial of degree $i$. The collection of all formal power series is denoted by $k[[X]]$ and forms a $k$-algebra in an obvious way, of which the polynomial ring $k[X]$ is a sub-algebra. The *order* or the *subdegree* of a power series $F$ is the smallest $i$ for which $F_i \neq 0$. Let us denote it by $\operatorname{ord} F$. Clearly,

$$\operatorname{ord}(F+G) \geq \min\{\operatorname{ord} F, \operatorname{ord} G); \quad \operatorname{ord} FG = (\operatorname{ord} F)(\operatorname{ord} G).$$

From the last property, it follows that, $k[[X]]$ is a domain. The quotient field is denoted by $k((X))$.

It is possible to define infinite sums of formal power series in certain cases. For instance suppose $F_\alpha$ is a family of formal power series such that for any $i$ there are only finitely many of $F_\alpha$ such that $\operatorname{ord} F_\alpha = i$. We may refer to this property by saying that the family is *order finite.* Then

$$\sum_\alpha F_\alpha := \sum_i G_i,$$

where $G_i$ is the sum of $i^{th}$ components of all the $F_\alpha' s$.

**Theorem 25.1** *The units in $k[[X]]$ are precisely those of order* 0.

**Proof:** If $FG = 1$, then $0 = \operatorname{ord} 1 = \operatorname{ord} F + \operatorname{ord} G$ and hence $\operatorname{ord} F = \operatorname{ord} G = 0$. Conversely, given $\operatorname{ord} F = 0$, write

$$F(X) = a(1-G)$$

where $0 \neq a \in k$ and $\operatorname{ord} G > 0$. This means that the family $\{G^i\}$ is order finite and hence $\sum_i G^i$ makes sense. Moreover, it is directly verified that $(1-G)(\sum_{i\geq 0}) = 1$. ♠

**Theorem 25.2** *The polynomial ring $k[[X]]$ is a unique factorisation domain.*

We shall prove this only for the case when $X$ is a single variable. The proof for the general case is much more involved and is beyond the scope of this course. We first have:

**Lemma 25.1** *A power series $a_0 + a_1X + a_2X^2 + \cdots$ in one variable is a unit iff $a \neq 0$.*

The proof of this is straight forward. It follows that every $f(X)$ can be written as $X^dG$ where $d = \operatorname{ord} F$ and $G$ is a unit. From this the unique factorisation in the power series in 1-varaible follows. Moreover, from the standard results about UFD, it now follows that $k(X)[[T]]$ and $k[X][[T]]$ are unique factorisation domains. (This is enough for our present purpose.)

**Theorem 25.3 Implicit Function Theorem:** *Let $F(X, Y) = 0$ be the equation of a curve $\Gamma$ passing through $(0, 0)$. Suppose that $(0, 0)$ is a smooth point and the tangent is not vertical. Then given a power series $g(X) = \sum_{i\geq 1} g_iX^i$ in $X$ which is of positive order, there exists a unique power series $p(X)$ of positive order such that*

$$F(x, p(X)) = g(X). \tag{25.7}$$

**Proof:** We may assume that $F(X, Y) = Y + aX+$ higher degree terms. Suppose $p(X) = \sum_{i\geq 1} p_iX^i$, $q(X) = \sum_{i\geq 1} q_iX^i$ both satisfy (25.7). Comparing the coefficients of $X$ on either side of the identity

$$F(X, p(X)) = F(X, q(X)) \tag{25.8}$$

we see that $p_1 = q_1$. Now assume that you have shown $p_k = q_k$ for $k \leq n$. Put $s(X) \sum_{k=1}^n p_kX^k = \sum_{k=1}^n q_kX^k$. Then observe that the coefficient of $X^{n+1}$ on the LHS is $p_{n+1}+$ coefficient of $X^{n+1}$ in $F_2(X, s(X) + F_3(X, s(X)) + \cdots$. On the RHS the same is given by $q_{n+1}+$ coefficient of $X^{n+1}$ in $F_2(X, s(X)+F_3(X, s(X))+\cdots$. Hence $p_{n+1} = q_{n+1}$. This proves the uniqueness of $p$. Now choose $p_1 = g_1 - a$. Inductively, suppose you have chosen $p_k$ for $k \leq n$ so that

$$F(X, s(X)) = g_1X + g_2X^2 + \ldots + g_nX^n + \alpha_{n+1}X^{n+1} + \text{higher degree terms.}$$

Now choose $p_{n+1} = g_{n+1} - \alpha_{n+1}$. Verify that

$$F(X, s(X)) = g_1X + g_2X^2 + \ldots + g_{n+1}X^{n+1} + \alpha_{n+2}X^{n+2} + \text{higher degree terms.}$$

In the limiting case this implies $F(X, p(X)) = g(X)$. ♠

**Remark 25.1** *In case $\mathbb{K} = \mathbb{C}$, it can be shown that $p$ has positive radius of convergence. Also, in the proof of the theorem, $\mathbb{K}$ need not be algebraically closed. In particular, if $\mathbb{K} = \mathbb{R}$, then $p \in \mathbb{R}[[X]]$. It follows that near a simple point the curve is bi-analytically equivalent to an open subset of $\mathbb{C}$ or $\mathbb{R}$ as the case may be. Thus*

**Theorem 25.4** *Let $\Gamma$ be a curve over $\mathbb{C}$ or $\mathbb{R}$. Then the set of smooth points on $\Gamma$ form a 1-dimensional $\mathbb{C}$ (or $\mathbb{R}$) manifold.*

Now, since $Y = p(X)$ is a solution of $F(X, Y) = 0$ in $k[[X]]$, it follows that $F(X, Y) = (Y - p(X))H(X, Y)$ for some $G \in k[[X]][Y]$. Comparing order on either side it follows that $\operatorname{ord} H(X, Y) = 0$. Therefore, $\operatorname{ord} F(X, 0) = \operatorname{ord} p$. Thus we have proved:

**Theorem 25.5** *The intersection multiplicity $i(\Gamma, \{Y = 0\}; O) = ord p$.*

More generally, we have,

**Theorem 25.6** *Let $\Gamma : F(X, Y) = 0$ be an affine plane curve with $O = (0, 0)$ as a smooth point and with tangent line at this point non vertical. Let $p(X)$ be the unique power series such that $F(X, p(X)) = 0$. Then for any $\Delta : G(X, Y) = 0$ is another curve passing through $O$, we have, $i(\Gamma, \Delta; O) = ord G(X, p(X))$.*

**Proof:** We assume that $\Gamma, \Delta$ are in permissible position. In particular, there are no points of $\Gamma \cap \Delta$ on the $Y$-axis. We have to count the multiplicity of $X$-factor in $\mathcal{R}_Y(F, G)$. We have

$$\begin{aligned} \mathcal{R}_Y(G, F) &= \mathcal{R}_Y(G, (Y - p(X))H(X, Y)) \\ &= G(X, p(X))\mathcal{R}_Y(G, H). \end{aligned}.$$

Therefore, it suffices to show that $X$ does not divide $\mathcal{R}_Y(G, H)$. This is the same as showing that $\mathcal{R}_Y(G(0, Y), H(0, Y)) \neq 0$. But $F(0, Y) = YH(0, Y)$, and hence we should show that $\mathcal{R}_Y(G(0, Y), F(0, Y)/Y) \neq 0$. This follows from the fact that $\Gamma, \Delta$ are in the permissible position, and $F(0, Y)/Y$ does not vanish at $Y = 0$. ♠

**Theorem 25.7 Inverse Function Theorem** *Let $p \in k[[t]]$ be of order 1. Then there exists a unique $q \in k[[t]]$ such that $p(q(t)) = t$.*

**Proof:** Let $p(t) = \sum_{i \geq 1} p_i t^i, p_1 \neq 0$. We want to find $q(t) = \sum_{i \geq 1} q_i t^i$ such that

$$p_1(q_1 t + q_2^2 + \cdots + p_2(q_1 t + q_2 t^2 + \cdots)^2 + \cdots = t.$$

(Observe why we have taken $q$ also to be order $\geq 1$.) This means we have to solve for the system of equations in for $q_i$ :

$$\begin{array}{lcl} p_1 q_1 & = & 1 \\ p_1 q_2 + p_2 q_1^2 & = & 0 \\ \cdots\cdots & & \cdots \\ p_1 q_n + \text{ terms involving } q_1, \ldots, q_{n-1} & = & 0 \\ \cdots\cdots & & \cdots \end{array}$$

The solution is obviously is obtained by solving for $q_i$ successively and is unique. ♠

**Remark 25.2** *The non symmetric nature of the system of equations do not help us to conclude that of $p(q(t) = t$ then $q(p(t)) = t$. To see this we should work a little harder.*

**Theorem 25.8** *Let $p(t) \in k[[t]]$ be any. Then the substitution $\tau = p(t)$ defines an automorphism $\mathcal{T} : k[[\tau]] \longrightarrow k[[t]]$ given by $q(\tau) \mapsto q(p(t))$ iff $\operatorname{ord} p = 1$. Moreover, every $k$-algebra automorphism of $k[[t]]$ is obtained by a substitution of order* 1.

**Proof:** Verify that $\mathcal{T}$ is an algebra homomorphism. Let now $\operatorname{ord} p = 1$. From the inverse function theorem it follows that $\mathcal{T}$ is surjective. If $\operatorname{ord} q = d$ then it is easily seen that $\operatorname{ord} q(p(t)) = d$ and hence $\mathcal{T}$ is injective. The converse is proved easily by examining the identity $q(p(t)) = t$ carefully. To see the last part let $\lambda$ be any $k$-algebra homomorphism, let $\lambda(\tau) = p(t)$ say. Then it follows that $\lambda(\tau^n) = p(t)^n$. It follows that for any polynomial $q(\tau)$, we have $\lambda(q) = q(p(t))$. Clearly $\lambda$ maps units into units. That is elements of order zero go inti elements of order zero. Since $\lambda$ is an automorphism it should map elements of positive order into elements of positive order. Since an automorphism preserves irreducible elements, it also preserves the number of irreducible factors up to units. This means that it maps order 1 elements to order 1 element. In particular, we have $\operatorname{ord} p = 1$. It still remains to see why $\lambda(q) = q(p(t))$ for all power series $q$. Write $q(t) = Q(t) + R_m(t)$ $Q(t)$ is the sum of first $m$ terms and $\operatorname{ord} R_m > m$. Then it follows that $\lambda(q) = \lambda(Q) + \lambda(R_m) = Q(p(t)) + \lambda(R_m) = q(p(t)) - R_m(p(t)) + \lambda(p(t))$. Therefore, it follows that $\lambda(q) - q(p(t))$ is an element of order $\geq m$ where $m$ is arbitrary. This means $\lambda(q) - q(p(t)) = 0$. ♠

**Remark 25.3** *Now if $\mathcal{T} : k[[\tau]] \longrightarrow k[[t]]$ is given by the substitution $\tau = p(t)$, then to say $q(p(t)) = t$ is the same as saying $\mathcal{T}(q(\tau)) = t$. Therefore $\mathcal{T}^{-1}(t) = q(\tau)$, which mens that $\mathcal{T}^{-1}$ is given by the substitution $t = q(\tau)$. But then $\mathcal{T}^{-1}(p(t)) = \tau$ implies $p(q(\tau)) = \tau$.*

# Chapter 26

# Analytic Branches

$30^{th}$ March 99.

We shall now stick to the case when the ground field is $k = \bar{k}$. As seen before, the tool for the local study of a curve is the power series. Thus, given a polynomial curve $F(X, Y) = 0$ passing through $(0, 0)$, in order to study the properties of it at the point $(0, 0)$, we should consider $F$ as an element of $k[[X, Y]]$. But then we may as well study the properties of a power series $F$ of positive order. When $k = \mathbb{C}$, we may restrict our attention to those which have positive radius of convergence and look out for the locus of points $(x, y)$ such that $F(x, y) = 0$. In the general situation, there is no way to look at the locus. So, before looking at this general case, first study polynomial equations using power series.

**Definition 26.1** *Let $\Gamma$ be a curve defined by $F$ over $k$. Let $k \subset K$ be a field. By a* generic point *of $\Gamma$ we mean a point $[a, b, c] \in \mathbb{P}^2_K \setminus \mathbb{P}^2_k$ such that $F(a, b, c) = 0$.*

Observe that since we have assumed that $k = \bar{k}$the extension $K$ of $K$ is transcendental. Often we choose $K = k((t))$ the field of fractions of the power series ring in one variable over $k$. Recall that an element of $k((t))$ looks like $\sum_{j \geq m} \alpha_j t^j$ where $m$ is some integer.

**Definition 26.2** *By a* branch representation *of $\Gamma$ with* center *$P$, we mean a generic point $[a, b, c]$ of $\Gamma$ where $K = k((t))$ such that $P = [a(0), b(0), c(0)]$. Assuming that $P = [1, 0, 0]$ and passing to affine co-ordinates, we see that a branch representation of $\Gamma$ at $(0, 0)$ is a pair of elements, $(p, q)$ where $p, q \in k[[t]]$ such that at least one of them is non constant. (As such, $p, q \in k((t))$ but since they are defined at $(0, 0)$ means that they must be of non negative order.)*

We introduce a further equivalence of branch representations: Two branch representations $(p, q), (p', q')$ are said to be *equivalent* if there exists an automorphism $\mathcal{T}$ of $k[[t]]$ such that $\mathcal{T}(p) = p', \mathcal{T}(q) = q'$. This is the same as saying that there exists a power series $\alpha(t)$ of positive order such that $p(\alpha(t)) = p'(t)$ and $q(\alpha(t)) = q'(t)$. An equivalence class of branch representations of $\Gamma$ is called a *branch* of the curve $\Gamma$. Observe that the center is the same for all branch representations in the same class and is called the center of the branch.

**Theorem 26.1** *If $P = (0, 0)$ is a smooth point then $\Gamma$ has exactly one branch centered at $P$.*

**Proof:** Assuming that the $X$-axis is the tangent to $\Gamma$, we have seen that there exist a power series of positive order such that $(t, p(t))$ is a branch representation for $\Gamma$ centered at $(0, 0)$. To see the uniqueness, suppose $\xi, \eta \in k[[t]]$ are of positive order and $F(\xi(t), \eta(t)) = 0$. Since we have $F(X, Y) = (Y - p(X))H(X, Y)$, it follows that

$$0 = F(\xi, \eta) = (\eta - p(\xi))H(\xi, \eta).$$

Since $H \in k[[X]][Y]$ has a non zero constant term, it follows that $H(\xi, \eta)$ is a unit in $k[[t]]$. Hence $\eta = p(\xi)$. Therefore, $\operatorname{ord} \xi = 1$. So, $\xi = tu(t)$ where $u(t)$ is a unit. Hence, after dividing out by $u(t)$, we may assume that $\xi(t) = t$. But then $\eta = p$. ♠

**Exercise:** Two irreducible curves cannot have same branch.

# Chapter 27

# Quadratic Transforms:

In order to study the behaviour of a curve at a singular point, we now introduce the concept of quadratic transforms. Consider the substitution

$$X' = X; \quad Y' = Y/X. \tag{27.1}$$

This is called a *local quadratic transform* with *center* $(0,0)$. Clearly, it not defined only on the line $X = 0$. Consider the mapping $Q : \mathbb{A}^2 \longrightarrow \mathbb{A}^2$ defined by $(X', Y') \mapsto (X', X'Y')$. This is nothing but the inverse of (27.1). Observe that $Q(X = 0) = (0,0)$ and $Q : \mathbb{A}^2 \setminus \{X = 0\} \longrightarrow \mathbb{A}^2 \setminus \{(0,0)\}$ is an isomorphism. Given a curve $\Gamma$ in $\mathbb{A}^2$ its *total transform* is defined to be $Q^{-1}(\Gamma)$ whereas its *proper transform* is defined to be the closure of $Q^{-1}(\Gamma \setminus \{(0,0)\})$. If $F(X,Y) = 0$ is the equation of the curve $\Gamma$ then clearly, the substitution (27.1) yields the equation of the total transform. It is easily seen that if the order of $F$ at $(0,0)$ is $r$, then $F(X', X'Y')$ is divisible by $X'^r$. Therefore, it follows that the equation of the proper transform is $F(X', X'Y')/X'^r = 0$. The mapping $Q$ is also referred to as *blowing down* and the transform (27.1) a *blow-up*. Here we are blowing-down the line $X' = 0$ to a single point or under the inverse, blowing-up the point $(0,0) \in \mathbb{A}^2$ into a line.

Let us now consider the projectivised version of the quadratic transformation. Consider the quadratic hypersurface $M$ in $\mathbb{P}^2 \times \mathbb{P}^1$ given by

$$M = \{([X_0, X_1, X_2], [U_1, U_2] \in \mathbb{P}^2 \times \mathbb{P}^1 \ : \ X_1U_2 = X_2U_1\}.$$

Restrict the projection map $\pi : \mathbb{P}^2 \times \mathbb{P}^1 \longrightarrow \mathbb{P}^2$ to $M$. Clearly, the line $L := [1,0,0] \times \mathbb{P}^1$ is contained in $M$ and is mapped to the single point $[1,0,0]$ by $\pi$. On the other hand for every other point $[x_0, x_1, x_2] \in \mathbb{P}^2$, there is a unique point viz., $([x_0, x_1, x_2], [x_1, x_2]) \in M$ mapped on to this point by $\pi$. Therefore, it follows that $M \setminus L$ is isomorphic to the

qpv $\mathbb{P}^2 \setminus \{[1,0,0]\}$ under $\pi$. Given a curve $\Gamma$ in $\mathbb{A}^2$ its *total transform* in $M$ is just the inverse image $\pi^{-1}(\Gamma)$ whereas, the *proper transform* form is defined to be the closure of $\pi^{-1}(\Gamma \setminus \{(0,0)\})$.

On the other hand, consider the mapping $\psi : \mathbb{A}^2 \longrightarrow M$

$$(t,s) \mapsto [1,t,ts][1,s].$$

Clearly this defines an embedding of $\mathbb{A}^2$ into $M$ and the image consists precisely those points of $M$ for which $X_0 \neq 0; U_1 \neq 0$. The composite $\pi \circ \psi$ can be identified with (27.1).

**Theorem 27.1** *$Q$ establishes a one-to-one correspondence between the set of lines $Y' = m$ in the affine $X', Y'$ space and the set of lines $Y = mx$ in the affine $X, Y$ space.*

**Theorem 27.2** *If $\Gamma \neq \{X = 0\}$ is irreducible, then so is its proper transform.*

**Proof:** Observe that $Q$ defines an isomorphism $Q^\star$ of the rings $k[X, X^{-1}][Y] \longrightarrow k[X', X'^{-1}][Y]$. If $F(X,Y)$ is irreducible and is not the line $X = 0$ then it is irreducible in $k[X, X^{-1}][Y]$. Hence $Q^\star(F)$ is irreducible in $k[X', X'^{-1}][Y']$. Hence $F' = Q^\star / X'^r$ is irreducible $k[X', X'^{-1}][Y']$. So, $F'$ is irreducible in $k[X', Y']$ also. ♠

**Theorem 27.3** *Let $\Gamma$ be curve not having $X = 0$ as tangent at $(0,0)$. Let $\Gamma'$ be the transform of $\Gamma$ under (27.1). Then there is a one-to-one correspondence between the branches of $\Gamma$ centered at $(0,0)$ and the branches of $\Gamma'$ centered at finite distance on the $Y$-axis.*

**Proof:** Since neither of $\Gamma, \Gamma'$ has $X = 0$ as a component, it follows that all branches in question have the first co-ordinate not equal to 0. Further, if $(\xi, \eta)$ is a branch of $\Gamma$, then $F(\xi, \eta) = 0$. Therefore, $(\xi, \eta/\xi)$ satisfies $F(X, XY) = 0$ and hence $F(X, XY)/X^r = 0$ also. The converse is also easy to see. It remains to see that none of the branches of $\Gamma$ escapes to infinity. This can happen only if a branch $(\xi, \eta)$ has $X = 0$ as a tangent. Recall that this means that $\operatorname{ord} \xi > \operatorname{ord} \eta > 0$. On the other hand, since $\Gamma$ does not have $X = 0$ as a tangent, it follows that the order form $F_r(X,Y)$ is not divisible by $X$.

Now for any homogeneous component $F_i(X,Y)$ of $F$, it is clear that the least degree term in $t$ will be contributed by the pure $Y$-term. Since $F_r$ has a non zero pure $Y$-term, its contribution will be of the smallest degree amongst all $F_i, i \geq r$. Therefore

$$\operatorname{ord} F(\xi, \eta) = \operatorname{ord} F_r(\xi, \eta) = \operatorname{ord} \eta^r = r(\operatorname{ord} \eta).$$

Hence $\operatorname{ord} F(\xi, \eta) = r(\operatorname{ord} \eta) < \infty$. This is a contradiction, since $F(\xi, \eta) = 0$. ♠

# Chapter 28

# Intersection Multiplicity

We shall now use the techniques of power series to study the intersection multiplicity. Indeed, this is will be only a small consequence of what we can achieve through this technique.

**Definition 28.1** *Let $\gamma = (\xi, \eta)$ be a branch at $P = (0,0)$ and $\Gamma := F(X,Y) = 0$ be a curve through $P$. We define*

$$j(\Gamma, \gamma; P) = ord_t\, F(\xi(t), \eta(t)).$$

*Observe that this definition is independent of the choice of representation of the branch and we could have even defined this directly with the projective co-ordinates at any point $P$ of the curve $\Gamma$.*

In this notation, theorem 25.6 says that if $\Gamma$ is smooth at $P$ and $\Delta$ is any curve passing through $P$, then

$$i(\Gamma, \Delta; P) = j(\Delta, \gamma; P). \tag{28.1}$$

In order to extend this result to the general situation, it is necessary for us to prove the existence of branches through non smooth points also. This leads us to the following:

**Theorem 28.1** *Let $P = (0,0)$ be an ordinary $r$-fold point on $\Gamma$. Then there are exactly $r$ distinct branches of $\Gamma$ through $P$.*

**Proof:** We may assume that $X = 0$ is not tangential to $\Gamma$ at $P$ so that

$$F(X,Y) = \prod_{i=1}^{r}(Y - m_i X) + \text{ higher degree terms}$$

where $m_i$ are distinct numbers. The QDT of $\Gamma$ would then be given by

$$F'(X,Y) = \prod_{i=1}^{r}(Y - m_i) + X(\cdots).$$

Hence $\Gamma'$ has simple points at $(0, m_i)$, $i = 1, \ldots, r$. At each of these points $\Gamma'$ has a unique branch which gives distinct branch of $\Gamma$ at $P$. ♠

In order to prove the existence of a branch in general, we may as well assume that $\Gamma$ is irreducible. We would like to blow-up at an r-fold point and look at the *infinitely near points* viz., the points of intersection of $\Gamma'$ with $X' = 0$. Even if one of these points is of multiplicity $< r$ on $\Gamma'$, we can then apply induction on this multiplicity to conclude that there is a branch at $P$. So we have to only consider the case when at $P$ there is only one tangent to $\Gamma$. Nevertheless we can look at the transformed curve $\Gamma'$ and look at its multiplicity at the unique infinitely nearby point $P'$. It may happen that the multiplicity at $P'$ for $\Gamma'$ may be again equal to $r$ (it is never greater than $r$) and is again of the same type. This may continue to be the situation even after we blow-up once more and so on. Thus it remains to show that this is not the case.

Let us write $\Gamma_0 = \Gamma$ and $\Gamma_i$ for the transform of $\Gamma_{i-1}$. Let us also write $P_0 = P$ and $P_i$ as the infinitely nearby point to $P_{i-1}$. Clearly, $P_i = (0, m_i)$ for some $m_i \in k$. Observe that after successive blow-ups, $X = 0$ is never a tangent, since the order term always involves a $Y$-term. Thus we can perform blow-ups at points $P_i = (0, m_i)$ using transformations

$$X' = X'; \quad Y' = (Y - m_i)/X$$

without performing any linear change of co-ordinates. For a fixed $i$, let us write

$$F(X,Y) = \sum_{pq} \alpha_{pq} X^p (Y - m_1 X - m_2 X^2 \cdots - m_i X^i)^q + X^{h_i} g_i(X). \tag{28.2}$$

with $\alpha_{pq} \in k$, $g_i \in k[X]$ with $g_i(0) \neq 0$. (This is nothing but the division algorithm through the monic polynomial $Y - m_1 X - m_2 X^2 \cdots - m_i X^i$.) Then $\alpha_{pq} = 0$. It is easily seen that $\alpha_{pq} = 0$ for $p + q < r$ and $h_i(F) = h_i \geq r$. Now

$$F'(X,Y') = \sum_{q>0} \alpha_{pq} X^{a+b-r} (Y' - m_1 - m_2 X \ldots m_{i-1} X^{i-1})^b + X^{h_i - r} g_i(X). \tag{28.3}$$

From this it follows that $h_{i-1}(F') = h_i(F) - r$. Repeated application of this shows that $h_i(F) \geq ir$. Since this is true for all $i$,

$$F(X,Y) = \sum_{q>0} \alpha_{pq} X^a Q^b, \tag{28.4}$$

where $Q = Y - m_1X - m_2X \ldots \in k[[X]][Y]$. Therefore, taking $\xi = t$ and $\eta = m_1t + m_2t^2 + \cdots$ we see that $F(\xi, \eta) = 0$. Thus we have proved:

**Theorem 28.2** *Every curve has a branch through a given point.*

The crux of the fact is that we can use this to actually prove that the above sequence of r-fold points is finite.

Since $\Gamma$ is irreducible, it follows that the branch $\gamma = (t, m_1t + m_2t^2 + \cdots)$ is not a branch of any other curve through $(0, 0)$. So, we consider the curve $\Gamma_y := \dfrac{\partial F}{\partial Y} = 0$ which has a $(r-1)$-fold point at $P$. Similarly, we also consider the curve $\Gamma'_{y'} := \dfrac{\partial F'}{\partial Y'}$ passing through $(0, m_1)$. Observe that $\gamma'(t, m_1 + m_2t + m_3t^2 + \cdots)$ is a branch of $\Gamma'$ at $P_1 = (0, m_1)$. Now if $Q$ denotes the QDT $(x', y') \mapsto (x', x'y')$, then by chain rule

$$\frac{\partial F \circ Q}{\partial Y'} = \left(\frac{\partial F}{\partial Y} \circ Q\right) \frac{\partial Y}{\partial Y'}.$$

Therefore,

$$\frac{\partial F}{\partial Y} \circ Q = \frac{1}{X'} \frac{\partial F \circ Q}{\partial Y'}.$$

Therefore,

$$\frac{\partial F}{\partial Y} \circ Q = X'r - 1 \frac{\partial}{\partial Y'} \left(\frac{1}{X'^r} F \circ Q\right).$$

Hence

$$\begin{aligned}
j(\Gamma_y; \gamma; P) &= \operatorname{ord}_t \frac{\partial F}{\partial Y}(t, t + m_1t^2 + \cdots) \\
&= \operatorname{ord}_t \frac{\partial F}{\partial Y} \circ Q(t, m_1 + m_2t + m_3t^2 + \cdots) \\
&= ord_t \left(t^{r-1} \frac{\partial}{\partial Y'} \left(\frac{1}{X'^r} F \circ Q\right)(t, m_1 + m_2t + m_3t^2 + \cdots)\right) \\
&= r - 1 + j(\Gamma'_{y'}, \gamma'; P_1).
\end{aligned}$$

Thus, under the assumption that $r > 1$, we see that

$$j(\Gamma_y, \gamma; P) > j(\Gamma'_{y'}; \gamma'; P_1) > 0.$$

The situation repeats from $\Gamma'$ and so on producing a strictly decreasing sequence of positive integers $\cdots > j((\Gamma_i)_y; \gamma_i; P_i) > \cdots$ which is absurd.

Thus we have proved:

**Theorem 28.3** *Given a plane curve $\Gamma$, there exists a finite set of QDT's applied at some points of $\Gamma$ and its transforms and so on, so that the final transform of $\Gamma$ is smooth. In*

*particular, $\Gamma$ has at least one and at most finitely many distinct branches at any of its points. The total number of branches at any point is not greater than the number of irreducible components of $\Gamma$ through that point.*

**Definition 28.2** *Let $\Gamma_1, \Gamma_2$ be any two curves and $\phi : \Gamma_1 \longrightarrow \Gamma_2$ be a bi-rational isomorphism. We say $\phi$ is a* resolution of singularities *of $\Gamma_2$ if $\Gamma_1$ is smooth. Thus we have proved that every plane curve admits a resolution of singularity, which is actually a composite of finitely many QDT's.*

**Remark 28.1** *The resolution of singularity is an extremely powerful tool in algebraic geometry, since it can be used to reduce the general problem about a variety to that of a smooth variety. This definitely so if the property under consideration is a bi-rational invariant. Otherwise one is lead to study the behaviour of a given property under such transformations. Hence, it is necessary to know the exact nature of a resolution of singularity. In higher dimension, the extremely difficult problem existence and the description of resolution of singularity for characteristic 0 was solved by Hironaka. The positive characteristic is still open and partial result are known.*

We now return to the study of intersection multiplicity. Let $\Gamma := F(X, Y) = 0; \Delta := G(X, Y) = 0$ be curves passing through $P$. We define

$$j(\Gamma; \Delta; P) = \sum_{\delta} j(\Gamma, \delta; P) \tag{28.5}$$

where the summation is taken over all distinct branches of $\Delta$ through $P$. As such it is not even clear that $j(\Delta; \Gamma; P) = j(\Gamma, \Delta; P)$. Our aim is to show that the $j$ function is nothing but the intersection number $i$.

**Theorem 28.4** *Let $\Gamma := F(X, Y) = 0; \Delta := G(X, Y) = 0$ be curves having $r$-fold and $s$-fold points at $P = (0.0)$. Assume that $X = 0$ is not tangential to either of them. Let $\Gamma'$, etc denote the transform of $\Gamma$ etc under the QDT: $X' = X;\ Y' = Y/X$. Let $P_1, \ldots, P_l$ be the points of intersection of $\Gamma'$ and $\Delta'$ on the $Y'$ axis. Then*

$$j(\Gamma, \Delta; P) = rs + \sum_{i=1}^{l} j(\Gamma'; \Delta'; P_i). \tag{28.6}$$

[Suppose that we have proved this theorem. Then from, (28.1), resolution of singularity and a simple induction on the number of QDT's involved, we obtain a proof of the fact that $i(\Gamma, \Delta; P) = j(\Gamma, \Delta; P)$. ]

**Proof:** First observe that the intersection multiplicity of $X = 0$ with the transformed curve $\Delta'$ is precisely $s$ which is the multiplicity of the point $P$ on $\Delta$. (This can be seen as follows: If $G(X, Y) = \prod_{i=1}^{s}(Y - m_i X)+$ higher degree terms, then the equation of $\Delta'$ is given by $G'(X, Y') = \prod_{i=1}^{s}(Y' - m_i) + X(\cdots)$. So, upon putting $X = 0$ we get the result.) Now,

$$\begin{aligned} j(\Gamma, \Delta; P) &= \sum_{\delta} j(\Gamma; \delta; P) \\ &= \sum_{\delta} \operatorname{ord}_{\delta} F(X, Y) \\ &= \sum_{\delta'} \operatorname{ord}_{\delta'} X^r F'(X, Y') \\ &= r \sum_{\delta'} \operatorname{ord}_{\delta'} X + \sum_{\delta'} \operatorname{ord}_{\delta'} F'(X, Y') \\ &= rs + \sum_{i=1}^{l} j(\Gamma'; \Delta; P_i) \end{aligned}$$

This completes the proof. ♠