Inflexion Points on Plane Algebraic Curves

Bachelor Thesis of Andreas Steiger
Supervised by Prof. Richard Pink and Patrik Hubschmid

November 18, 2008

In this thesis we will have a look at algebraic curves in the projective plane over an arbitrary algebraically closed field k. Using the resultant of polynomial rings over k we define intersection multiplicities and prove Bézout's Theorem for effective divisors. We define singularities and inflexion points and count their number depending on the degree of the curve, using the Hessian of a curve.

0 Introduction

Algebraic geometry is a very active branch in modern mathematics. The language of schemes, introduced by Grothendieck in the middle of the twentieth century, is enormously powerful and allows the mathematician to get geometric insight into facts from different fields such as algebra and number theory, where there are no obvious analogies at the first glance. However, a concept which opens a vast amount of possibilities often demands its tribute by being difficult to understand, and beginners often struggle. This is the case for the language of schemes.

As important as schemes are in current research, one can still use classical algebraic geometry to understand the basic concepts. One can even try to work with algebraic geometry with using as little algebra as possible.

When I started to write this thesis, I felt shiftless with the algebra involved in algebraic geometry. Thus the thesis turned out to use only very basic concepts of commutative algebra.

In the first chapter we introduce the projective plane over a field and define algebraic curves in the plane. This concept is easily generalised to projective varieties. The important results are the properties that curves over algebraically closed fields contain infinitely many points (Theorem 1.11), and the equivalence of topological and algebraic irreducibility (Theorem 1.16), as well as its consequence that there exists a unique decomposition into irreducible components. (Theorem 1.17)

In the second chapter we study intersections of curves. The crucial point is the introduction of intersection multiplicities, which allows us to prove Bézout's famous Theorem.

The intersection multiplicity is introduced via the resultant (Definition 2.9), which simplifies the proof of Bézout's Theorem (Theorem 2.14) greatly. However, this definition has its drawbacks: At first glance, the only purpose of this definition seems to be the simplification mentioned above. It looks arbitrary, and it is not easy to calculate intersection multiplicities of complicated curves. Nevertheless it has the properties that are known for the definition using local rings. Unfortunately, we were not able to find a proof for the very important independence of the choice of coordinates, Theorem 2.10. A proof for the case $k = \mathbb{C}$ can be found in Fischer [1].

The next topic are then singularities and tangents. We give two equivalent definitions of the order of a point on a curve, using the Taylor expansion for an algebraic insight (Definition 3.1) and observing intersection multiplicities of lines in that point to get a geometric intuition (Proposition 3.5). The second notion is closely related to the tangents at that point (Corollary 3.7). Two very important tools, the Euler Formula (Proposition 3.11) and the Jacobi Criterion (Proposition 3.12), will be proven. The first application is the proof that a curve only has finitely many singularities (Proposition 3.15). This result can be improved to an upper bound depending on the degree of the curve (Proposition 3.21 and Corollary 3.22).

The fourth chapter then finally deals with the main topic, inflexion points of curves. Nearly all results proven before are required to prove that the Hessian of a curve (Definition 4.4) intersects the curve exactly in flexes and singular points (Theorem 4.8). As a conclusion we give examples where and how the theorem works, and that it can be wrong in fields of non-zero characteristic.

1 Projective Algebraic Curves in the Plane

Let k be an algebraically closed field and $k[X_0, X_1, X_2]$ be the polynomial algebra over k with variables in X_0, X_1, X_2. Throughout this thesis we will mostly be working in the projective plane $\mathbb{P}^2_k$ over the field k. The reason for this choice is that there are a lot of theorems which show their full beauty only if we can use the so-called "points at infinity".

Definition 1.1. The *projective r-space* $\mathbb{P}^r_k$ over k of dimension r is given by the set of $(r+1)$-tuples $(x_0, \ldots, x_r) \in k^{r+1} \setminus \{0\}$ modulo the equivalence relation

$$(x_0, \ldots, x_r) \sim (y_0, \ldots, y_r) : \Longleftrightarrow \ \exists \alpha \in k^* : \alpha \cdot (y_0, \ldots, y_r) = (x_0, \ldots, x_r).$$

Note that $\mathbb{P}^r_k$ actually describes the lines in k^{r+1} through the origin.

Definition 1.2. A polynomial $F \in k[X_0, X_1, X_2]$ is called *homogeneous* of degree n if it is a linear combination of monomials in $k[X_0, X_1, X_2]$ of degree $n < \infty$.

Remark 1.3. The zero polynomial is a polynomial of every degree.

Remark 1.4. If F is a homogeneous polynomial of degree n, then

$$F(\lambda X_0, \lambda X_1, \lambda X_2) = \lambda^n F(X_0, X_1, X_2) \quad \forall \lambda \in k.$$

Therefore, if $P = (x_0 : x_1 : x_2) \in \mathbb{P}_k^2$, the property $F(x_0, x_1, x_2) = 0$ does not depend on the particular representing element, but only on the equivalence class of P. We will write $F(P) = 0$ in these cases.

Definition 1.5. The *variety* or *zero set* of a homogeneous polynomial $F \in k[X_0, X_1, X_2]$ is the set

$$V(F) := \{P \in \mathbb{P}_k^2 \mid F(P) = 0\}.$$

Definition 1.6. A subset $C \subset \mathbb{P}_k^2$ is called a *plane projective algebraic curve* if there is a non-zero homogeneous polynomial $F \in k[X_0, X_1, X_2]$ with $\deg F \geq 1$, such that $C = V(F)$. A polynomial of least degree defining C is called a *minimal polynomial* for C, and its degree is called the degree of C.

From now on, a curve shall be a plane projective algebraic curve.

Note that the minimal polynomial is not uniquely defined, as multiplication of a constant $\lambda \in k^*$ with a polynomial gives a different polynomial with the same variety. We shall see later that up to multiplication with a constant factor, the minimal polynomial is actually unique.

Example. The curves of degree 1 are called *projective lines*. One sees immediately that they are defined by a linear equation

$$a_0X_0 + a_1X_1 + a_2X_2 = 0, \qquad (a_0 : a_1 : a_2) \in \mathbb{P}_k^2.$$

Two projective lines always intersect. The intersection consists of one point if and only if the lines are different, as the equation

$$\begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix} = 0$$

has exactly one non-trivial solution up to a constant factor if and only if the coefficient matrix has rank 2. Otherwise, $(a_0 : a_1 : a_2) = (b_0 : b_1 : b_2)$ and the intersection is the whole line.

Definition 1.7. A mapping $\tau : \mathbb{P}_k^2 \to \mathbb{P}_k^2$ is called a *projective coordinate transformation* if there is a matrix $T \in GL_3(k)$, such that

$$\tau(x_0 : x_1 : x_2) = (x_0 : x_1 : x_2) \cdot T, \qquad \forall (x_0 : x_1 : x_2) \in \mathbb{P}_k^2.$$

Note that T is uniquely determined by its induced mapping τ, up to a constant factor $\lambda \in k^*$:

Proof. Suppose that both S and $T \in GL_3(k)$ give the same transformation τ. Then

$$\tau(x_0 : x_1 : x_2) = (x_0 : x_1 : x_2)S = (x_0 : x_1 : x_2)T, \qquad \forall (x_0 : x_1 : x_2) \in \mathbb{P}_k^2.$$

Multiplication by T^{-1} gives

$$(x_0 : x_1 : x_2)ST^{-1} = (x_0 : x_1 : x_2), \qquad \forall (x_0 : x_1 : x_2) \in \mathbb{P}_k^2.$$

By explicit calculation we get

$$(1,0,0)ST^{-1} = (\lambda_1, 0, 0), \quad (0,0,1)ST^{-1} = (0, \lambda_2, 0), \quad (0,0,1)ST^{-1} = (0, 0, \lambda_3)$$

for some λ_1, λ_2, $\lambda_3 \in k^*$. Furthermore,

$$(1,1,1)ST^{-1} = (1,0,0)ST^{-1} + (0,1,0)ST^{-1} + (0,0,1)ST^{-1} = (\lambda_1, \lambda_2, \lambda_3).$$

This point is in the same equivalence class in $\mathbb{P}^2_k$ as $(1,1,1)$ if and only if $\lambda_1 = \lambda_2 = \lambda_3$. Thus $ST^{-1} = \lambda \cdot E$, where $\lambda \in k^*$ and E denotes the unit matrix, and furthermore $S = \lambda T$. Obviously, multiplication of the matrix with a constant factor does not change the equivalence class of a point in the image. □

From now on, any coordinate transformation τ shall be identified with its matrix, i.e. τ itself is a matrix.

If a curve C is given by the homogeneous polynomial F and T is a projective coordinate transformation, then

$$F^T(X_0, X_1, X_2) := F((X_0, X_1, X_2) \cdot T^{-1})$$

is a homogeneous polynomial with $\deg F^T = \deg F$. This gives us the transformed curve

$$T(C) = V(F^T),$$

which has the same degree as C. We often will transform curves such that our objects of interest satisfy special conditions to simplify calculations.

Until now, we have used $\mathbb{P}^2_k$ as a somewhat independent space, i.e. with no relations other than to the field k. But actually, it is an extension of the affine plane $\mathbb{A}^2_k$ by the canonical embedding

$$\begin{array}{rccc} i & : & \mathbb{A}^2_k & \to & \mathbb{P}^2_k \\ & & (x_1, x_2) & \mapsto & (1 : x_1 : x_2). \end{array}$$

We identify $\mathbb{A}^2_k$ with its image under i. Note that $\mathbb{P}^2_k \setminus i(\mathbb{A}^2_k)$ is a projective line $V(X_0) = \{(0 : x_1 : x_2) \in \mathbb{P}^2_k\}$, called the *line at infinity* of $\mathbb{P}^2_k$. Its points are called *points at infinity*. The primary usage of this embedding lies in the homogenisation of polynomials in two variables:

Definition 1.8. Given a polynomial $f \in k[X, Y]$ with $\deg f = n$, the *homogenisation* $\hat{f} \in k[X_0, X_1, X_2]$ of f is given by

$$\hat{f}(X_0, X_1, X_2) := X_0^n \cdot f\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right).$$

Then $\hat{f}$ is a homogeneous polynomial of degree n. Conversely, to any homogeneous polynomial $F \in k[X_0, X_1, X_2]$ we associate the *dehomogenisation* $f \in k[X, Y]$ of F with respect to X_0, by

$$f(X, Y) := F(1, X, Y).$$

If X_0 is not a factor of F, then $\deg F = \deg f$.

Remark 1.9. Let $f \in k[X,Y]$ be a polynomial defining an *affine* algebraic curve C by its zero set. Then $i(V(f)) \subset V(\hat{f})$, and the only missing points of the embedding in the projective space are those at infinity, i.e. $i(V(f)) = V(\hat{f}) \cap i(\mathbb{A}^2_k)$.

Theorem 1.10 (Homogeneous form of the Fundamental Theorem of Algebra)**.** *Every non-zero homogeneous polynomial $F \in k[X,Y]$ has a decomposition into linear factors.*

Proof. Let $F = \sum_{i=0}^{n} c_i X^i Y^{n-i}$ be any non-zero homogeneous polynomial in two variables X, Y of degree d over k. Let e be the highest power of X dividing F, and let $G = \prod_{i=e}^{d} c_i X^{i-e} Y^{n-i}$, i.e. $F = X^e \cdot G$. Dehomogenising G with respect to X gives a polynomial in Y:

$$g = \sum_{i=0}^{n-e} c_{i+e} Y^{n-e-i}.$$

By the Fundamental Theorem of Algebra, g has the (not necessarily different) zeros $b_{e+1}, \ldots, b_n \in k$. Then we can write g as

$$g = c' \cdot \prod_{i=1}^{n-e} (Y - b_{i+e}).$$

for some $c' \in k^*$. Homogenising each factor gives

$$G = \hat{g} = c' \cdot \prod_{i=e+1}^{n} (Y - b_i X) \Rightarrow F = \prod_{i=1}^{n} (a_i Y - b_i X),$$

for some $a_i \in k$ with $a_1 = \ldots = a_e = 0$. □

Theorem 1.11. *Every curve C consists of infinitely many points.*

Proof. Let $C = V(F)$, $\deg F =: n$, and write F as

$$F = A_0 + A_1 X_2 + \ldots + A_p X_2^p,$$

where $A_i \in k[X_0, X_1]$ are homogeneous polynomials of degree $n - i$ and $A_p \neq 0$.

- $p = 0$:

  Then $F = A_0 = \sum_{i=0}^{n} c_i X_0^i X_1^{d-i}$ for some $c_i \in k$. By Theorem 1.10, there exists a decomposition into linear factors $F = \prod_{i=1}^{n} (a_i X_1 - b_i X_0)$. For each pair (a_i, b_i) we get the solution set $L_i = \{(a_i : b_i : x) \mid x \in k\}$, which is a projective line. Since we are working in algebraically closed field each line consists of infinitely many points.

- $p \neq 0$:

  The polynomial A_p has at most finitely many zeros in $\mathbb{P}^1_k$. Thus there exist infinitely many points $P \in \mathbb{P}^1_k$, such that $A_p(P) \neq 0$. For each such point P, the polynomial F is nonconstant in X_2, and thus has at least one zero. Hence we have found infinitely many zeros and C consists of infinitely many points.

□

Definition 1.12. The *ideal* $I(C) \subset k[X_0, X_1, X_2]$ of a curve C is the ideal generated by all homogeneous polynomials that vanish at all points of C.

Therefore, it is a homogeneous ideal.

Theorem 1.13 (Hilbert's Nullstellensatz, homogeneous form)**.** *Let k be an algebraically closed field and $\mathfrak{a} \subseteq k[X_0, \ldots, X_r]$ be a homogeneous ideal. Let $V(\mathfrak{a}) = \{P \in \mathbb{P}_k^r \mid \forall F \in \mathfrak{a} : F(P) = 0\}$, then $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*

Proof. See Zariski–Samuel [3], Theorem VII.4.15, page 171f. □

Theorem 1.14. *The minimal polynomial of a curve C is uniquely determined by C up to a constant factor $\lambda \in k^*$. It generates the ideal $I(C)$.*

Proof. Assume $C = V(F) = V(G)$ for two minimal polynomials F, G of C. Obviously, $V((F)) = V(F) = V(G) = V((G))$. Thus, by the homogeneous form of Hilbert's Nullstellensatz, $\sqrt{(G)} = I(V(G)) = I(V(F)) = \sqrt{(F)}$. Since F and G are minimal polynomials for their zero sets, there are no polynomials of lower degree, having the same zero sets. Thus, $(F) = \sqrt{(F)} = I(C) = \sqrt{(G)} = (G)$, and $I(C)$ is generated by any minimal polynomial. Thus F and G have the same degree, and so $(F) = (G)$ is only possible if there is a constant factor $\lambda \in k^*$, such that $F = \lambda G$. □

From now on, if we say a curve C is given by a polynomial F, we always choose F to be the minimal polynomial.

Definition 1.15. A curve C is called *irreducible* if every decomposition $C = C_1 \cup C_2$ into two curves implies $C = C_1$ or $C = C_2$, i.e. C is not the union of two different curves.

Theorem 1.16. *The following three statements are equivalent:*

i. C is irreducible.

ii. The minimal polynomial of C is irreducible.

iii. $I(C)$ is a homogeneous prime ideal.

Proof. We show i. ⇒ ii. ⇒ iii. ⇒ i.

i. ⇒ ii. Let C be irreducible and F be a minimal polynomial of C. Suppose that $F = F_1F_2$ for some $F_i \in k[X_0, X_1, X_2]$. Then the F_i are homogeneous. Furthermore, $V(F_1) \cup V(F_2) = V(F) = C$, because $F(P) = 0 \iff F_1(P) = 0$ or $F_2(P) = 0$ for any $P \in \mathbb{P}_k^2$. But C is irreducible, hence without loss of generality assume $V(F_1) = C$. We get that $\deg F = \deg F_1$, since $\deg F_1 \leq \deg F$ by $F = F_1F_2$ and $\deg F_1 \geq \deg F$ by minimality of F. This yields $\deg F_2 = \deg F - \deg F_1 = 0$ and F_2 is constant. Hence, F is irreducible.

ii. ⇒ iii. By Theorem 1.14, $I(C)$ is generated by the minimal polynomial, which is irreducible and homogeneous. Hence $I(C)$ is a homogeneous prime ideal.

iii. $\Rightarrow$ i. Let $C = C_1 \cup C_2$ be a decomposition into two curves with minimal polynomials F_1 and F_2, respectively. Write $F := F_1F_2$, then $F \in I(C)$, since F is homogeneous and vanishes at all points of C. Furthermore, since $I(C)$ is a prime ideal, without loss of generality suppose $F_1 \in I(C)$. But then F_1 vanishes at all points of C, so $C \subset V(F_1) = C_1$ and we get $C = C_1$.

□

Theorem 1.17. *Every curve C has a unique (up to order) representation*

$$C = C_1 \cup \cdots \cup C_l,$$

where the C_i are pairwise distinct irreducible curves. They are in one-to-one-correspondence with the irreducible factors of a minimal polynomial for C.

Proof. Let F be the minimal polynomial of C and let $F = F_1 \cdot \ldots \cdot F_l$ be the decomposition into irreducible factors, which is unique up to constant factors and ordering. Then $F(P) = 0$ if and only if there is a polynomial F_i such that $F_i(P) = 0$. Thus, $C = V(F) = V(F_1) \cup \cdots \cup V(F_l)$. Since each F_i is irreducible, they are minimal polynomials of their respective varieties. By Theorem 1.16 an irreducible minimal polynomial determines an irreducible curve, thus $C_i = V(F_i)$ gives a decomposition

$$C = C_1 \cup \cdots \cup C_l$$

of of C into irreducible curves.

Let

$$C = D_1 \cup \ldots \cup D_l'$$

be any decomposition of C into distinct irreducible curves. Then the respective minimal polynomials G_i, such that $D_i = V(G_i)$, are irreducible. But then $V(G_1 \cdot \ldots \cdot G_l') = V(F)$. This is only possible if $G_1 \cdot \ldots \cdot G_l'$ is the minimal polynomial itself. Since the decomposition of a polynomial into irreducible factors is unique, l equals l' and the G_i are just a permutation of the F_j. □

This leads us to an algebraic structure on the set of curves:

Definition 1.18. The *divisor group* $\mathcal{D}$ of $\mathbb{P}^2_k$ is the free abelian group on the set of all irreducible curves. An element D of $\mathcal{D}$ is called a *divisor*. It is represented as a formal linear combination

$$D = \sum_{C \text{ irred.}} n_C \cdot C, \quad n_C \in \mathbb{Z}, n_C \neq 0 \text{ for only finitely many } C.$$

A divisor is an *effective divisor* if $n_C \geq 0$ for all irreducible curves C. The *degree* of an effective divisor is given by $\deg D = \sum_{C \text{ irred.}} n_C \cdot \deg C$. For an effective divisor, the *support* of D is the set

$$\operatorname{Supp} D := \bigcup_{n_C > 0} C.$$

If $D \neq 0$ this is a curve. An effective divisor is a *reduced curve*, if furthermore $n_C \leq 1$ for all irreducible curves C.

2 Intersections of Curves

With the basic properties of curves we are now able to work towards one of the most important results of elementary curve theory, namely Bézout's Theorem. It relates the number of intersections of two curves with their degrees.

Let us first consider the most simple case, the intersection of a curve with a line.

Proposition 2.1. *Let $C = V(F)$ be a curve of degree n and L be a line in $\mathbb{P}^2_k$. If L does not completely in C, then the number of intersections $C \cap L$ is at most n.*

Proof. By coordinate transformation, choose L to be given by $X_2 = 0$. Thus, for any point $P = (x_0 : x_1 : x_2)$ in the intersection, we need $F(P) = 0$ and $x_2 = 0$, which is equivalent to solving $F(x_0, x_1, 0) = 0$.

Decompose F in terms of X_2, i.e.

$$F(X_0, X_1, X_2) = F_0 X_2^n + F_1 X_2^{n-1} + \cdots + F_n,$$

where $F_i \in k[X_0, X_1]$ and F_i is homogeneous of degree i. Then $F(x_0, x_1, 0) = 0$ is equivalent to $F_n(x_0, x_1) = 0$. If F_n is the zero polynomial, then F is a multiple of X_2 and $L \subset C$. Otherwise, $\deg F_n = n$ and by the homogeneous form of the Fundamental Theorem of Algebra F_n has a decomposition

$$F_n = (b_1 X_0 - a_1 X_1)^{k_1} \cdot \ldots \cdot (b_m X_0 - a_m X_1)^{k_m}, \qquad k_j \in \mathbb{N}^*, (a_j : b_j) \in \mathbb{P}^1_k,$$

where all $(a_j : b_j)$ are distinct and $m \leq n$. Thus, F_n has at most d zeros. □

Note that powers k_j do not depend on the particular choice of coordinates, but only on C and L. Thus, the intersection multiplicity defined below is indeed well-defined:

Definition 2.2. Let C be a curve and L be a line, which intersect at a point P. Using the construction in the proof above, let $k = k_j$ for $P = (a_j : b_j : 0)$ after a coordinate transformation. Then the *intersection multiplicity* of C and L at P is given by

$$\mu_P(C, L) := k.$$

Corollary 2.3. *A line L which is not contained in a curve C of degree n has exactly n intersection points with C, counted with multiplicity.*

Of course we want to generalise this result to arbitrary curves. As curves are just zero sets of polynomials, we can use the resultant, which relates the coefficients of two polynomials with its common zeros. We present the following results, following Fischer [1]:

Definition 2.4. Let A be a commutative ring with unit, and

$$f = a_0 X^m + \cdots + a_m, \quad g = b_0 X^n + \cdots + b_n, \quad f, g \in A[X],$$

with $a_0 \neq 0$ and $b_0 \neq 0$. The *resultant* of f and g is defined by

$$R_{f,g} = \det \begin{pmatrix} a_0 & & \cdots & \cdots & & a_m & & \\ & \ddots & & & & & \ddots & \\ & & a_0 & & \cdots & \cdots & & a_m \\ b_0 & \cdots & \cdots & b_n & & & & \\ & & \ddots & & & \ddots & & \\ & & & & b_0 & \cdots & \cdots & b_n \end{pmatrix} \in A. \quad \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \begin{matrix} n \text{ rows} \\ \\ \\ \\ m \text{ rows} \\ \\ \end{matrix}$$

Lemma 2.5. If A is an integral domain and $f, g \in A[X]$, then $R_{f,g} = 0$ in A if and only if there exist polynomials $\varphi, \psi \in A[X]$, not both zero, with $\deg \varphi < \deg f$ and $\deg \psi < \deg g$, such that $\psi f + \varphi g = 0$.

Proof. In the vector space V of polynomials in $K[X]$ of degree $< n + m$, we look at the elements

$$X^{n-1}f, \ldots, Xf, f, X^{m-1}g, \ldots, Xg, g.$$

Then each row of the resultant matrix is the linear representation in the base X^{m+n-1}, X^{m+n-2}, …, X, 1 of V. Thus, $R_{f,g} = 0$ if and only if the vectors are linearly dependent, i.e. there exists a non-trivial relation

$$\begin{aligned} 0 = &\quad \mu_0 X^{n-1} f + \cdots + \mu_{n-1} f &&+ \lambda_0 X^{m-1} g + \ldots + \lambda_{m-1} g \\ = &\quad (\mu_0 X^{n-1} + \cdots + \mu_{n-1}) f &&+ (\lambda_0 X^{m-1} + \ldots + \lambda_{m-1}) g \\ = &\quad \psi f &&+ \varphi g. \end{aligned}$$

It is possible that ψ or φ do not have coefficients in A itself, but only in its quotient field K. If this is the case, we simply multiply ψ and φ with the common denominator of their coefficients, giving coefficients in A. □

Proposition 2.6. *Let A be a factorial ring and $f, g \in A[X]$ as above, with $a_0 \neq 0$ and $b_0 \neq 0$. Then, the following are equivalent:*

i) f and g have a common divisor in $A[X]$ of degree ≥ 1,

ii) $R_{f,g} = 0$ in A.

Proof. By Lemma 2.5, $R_{f,g} = 0$ if and only if there exist φ, ψ of the above form with $\psi f + \varphi g = 0$.

- i) ⇒ ii):

  Let h be common factor of f and g. Then $f = f_1 h$ and $g = g_1 h$. Choose $\varphi := f_1$ and $\psi := -g_1$. Then $\deg \varphi < \deg f, \deg \psi < \deg g$, and not both are zero. Furthermore, $\psi f + \varphi g = -g_1 f_1 h + f_1 g_1 h = 0$. Thus $R_{f,g} = 0$.

- ii) $\Rightarrow$ i):

  Decompose $f\psi = -g\varphi$ into prime factors

  $$f_1 \cdot \ldots \cdot f_r \cdot \psi_1 \cdot \ldots \cdot \psi_k = -g_1 \cdot \ldots \cdot g_s \cdot \varphi_1 \cdot \ldots \cdot \varphi_l,$$

  where factors of degree zero in X can show up. Up to units, each factor g_i must show up on the left hand side of the equation. Since $\deg \psi < \deg g$, at least one factor g_σ of degree ≥ 1 is a prime factor of f, thus f and g have a common factor of degree ≥ 1.

□

Proposition 2.7. *Let k be a field, $A = k[Y_1, \ldots, Y_r]$, and $f, g \in A[X]$ with*

$$f = a_0 X^m + \cdots + a_m, \quad g = b_0 X^n + \cdots + b_n,$$

where $a_0 \neq 0$, $b_0 \neq 0$, all a_i, b_j homogeneous of degree i and j, respectively. Then $R_{f,g}$ is in A, homogeneous of degree $m \cdot n$, or $R_{f,g} = 0$.

Proof. A polynomial $a \in k[Y_1, \ldots, Y_r]$ is homogeneous of degree d if and only if

$$a(TY_1, \ldots, TY_r) = T^d a(Y_1, \ldots, Y_r) \text{ in } k[Y_1, \ldots, Y_r, T].$$

If we calculate $R_{f,g}(TY_1, \ldots, TY_r)$, then the entries of the matrix are multiplied by the following powers of T:

$$\begin{vmatrix}
0 & 1 & & & & m & & & \\
 & 0 & & & & & m & & \\
 & & \ddots & & & & & \ddots & \\
 & & & 0 & & & & & m \\
0 & 1 & & & n & & & & \\
 & 0 & & & & n & & & \\
 & & \ddots & & & & \ddots & & \\
 & & & \ddots & & & & \ddots & \\
 & & & & 0 & & & & n
\end{vmatrix}$$

If we further multiply each row with the power of T given on the left, we get the following powers of T:

$$\begin{array}{c|}
\begin{matrix}
1: & 1 & 2 & & & & m & & & & \\
2: & & 2 & & & & & m+1 & & & \\
\vdots & & & \ddots & & & & & \ddots & & \\
n: & & & & n & & & & & & m+n \\
1: & 1 & 2 & & & n+1 & & & & & \\
2: & & 2 & & & & n+2 & & & & \\
\vdots & & & \ddots & & & & & \ddots & & \\
\vdots & & & & \ddots & & & & & \ddots & \\
m: & & & & & m & & & & & n+m
\end{matrix}
\end{array}.$$

We can get this result in a different way, namely by multiplying the i-th column of $R_{f,g}$ with T^i. Thus, with $p = (1 + \cdots + n) + (1 + \cdots + m)$ and $q = (1 + \ldots + (m + n))$,

$$T^p R_{f,g}(TY) = T^q R_{f,g}(Y).$$

But $q - p = m \cdot n$, thus $R_{f,g}$ is homogeneous of degree $m \cdot n$, if it is not zero. □

Theorem 2.8. *Let C_1, C_2 be curves of degree m, n, respectively, with no common components. Then the number of intersections $C_1 \cap C_2$ is at most $n \cdot m$.*

We prove the Theorem in two steps:

Claim 1: $C_1 \cap C_2$ is finite.

Proof. Let $C_1 = V(F_1)$ and $C_2 = V(F_2)$. By coordinate transformation assume that $q = (0 : 0 : 1)$ is neither in C_1 nor in C_2. For each point $x = (x_0 : x_1 : 0)$ let L_x be the line connecting q and x, i.e. $L_x \setminus \{q\} = \{(x_0 : x_1 : t) \mid t \in k\}$. Just as in Theorem 2.1 we decompose F_1 and F_2 along X_2:

$$\begin{aligned} F_1 &= a_0 X_2^m + a_1 X_2^{m-1} + \cdots + a_m, \\ F_2 &= b_0 X_2^n + b_1 X_2^{n-1} + \cdots + b_n, \end{aligned}$$

with $a_i, b_j \in k[X_0, X_1]$, homogeneous, and $\deg a_i = i$, $\deg b_j = j$. Since $a_i(q) = 0 = b_j(q)$ for all $i, j > 0$ and $q \notin C_1 \cup C_2$, the coefficients a_0 and b_0 are both not zero.

Let $G = R_{F_1,F_2}$ be the resultant of F_1 and F_2. The curves C_1 and C_2 have no common components by requirement, therefore F_1 and F_2 have no common factors when viewed as polynomials in X_2 with coefficients in $k[X_0, X_1]$. Hence G is non-zero by Proposition 2.6. Furthermore it is homogeneous of degree $n \cdot m$ by Proposition 2.7.

Suppose $G(x_0, x_1) = 0$. For fixed x_0, x_1, we know that F_1 and F_2 are just polynomials in X_2. Since $G(x_0, x_1) = 0$ they must have a common zero (x_0, x_1, x_2) which lies on L_x, hence C_1 and C_2 intersect on L_x. Otherwise, if $G(x_0, x_1) \neq 0$, then F_1 and F_2 have no common zero for that particular x_0, x_1, hence C_1 and C_2 do not intersect on L_x. So $G(x_0, x_1) = 0$ if and only if C_1 and C_2 intersect each other on L_x.

Since $q \in L_x \setminus (C_1 \cup C_2)$, the line L_x can not be a component of C_1 or C_2, respectively. Thus, for any fixed x the line L_x intersects C_1 and C_2 only in finitely many points. Since G is of finite degree $C_1 \cap C_2$ consists of finitely many points. □

Claim 2: $|(C_1 \cap C_2)| \leq n \cdot m$.

Proof. Between finitely many intersection points, there are only finitely many lines connecting such points. By coordinate transformation, choose q such that none of these lines contains q. Then, by the same construction, each line L_x contains at most one intersection point. Thus $C_1 \cap C_2$ cannot consist of more than $\deg G = n \cdot m$ points. □

Again, we want to improve the result by counting multiplicities.

Definition 2.9. Let $C_1 = V(F_1)$, $C_2 = V(F_2)$ be two curves without common components, such that they do not contain $q = (0 : 0 : 1)$, and each line through q contains at most one intersection point of C_1 and C_2. Let $G = R_{F_1,F_2}$. If $P = (p_0 : p_1 : p_2) \in C_1 \cap C_2$ is an intersection point, let $P' := (p_0 : p_1)$, and define the *intersection multiplicity* of C_1 and C_2 at P, $\mu_P(C_1, C_2)$, to be the order of the zero of G in P'.

Note that this definition is consistent with the definition of intersection multiplicity of a curve and a line. If $C_2 = V(X_2)$, then the resultant is just $G = \pm a_m$, using the same notation as above.

Obviously, for each pair of curves C_1, C_2, there exist several coordinate transformations, such that the transformed curves fulfill the conditions of the definition of intersection multiplicity. However, it is not clear at all that every transformation yields the same multiplicities:

Theorem 2.10. *If C_1 and C_2 are curves satisfying the conditions of 2.9 and T is a coordinate transformation, such that the transformed curves $T(C_1)$, $T(C_2)$ also satisfy these conditions, then*

$$\mu_P(C_1, C_2) = \mu_{PT}(T(C_1), T(C_2)) \qquad \forall P \in C_1 \cap C_2.$$

In particular, for any two curves not satisfying the conditions of 2.9, any coordinate transformation, such that the transformed curves do satisfy the conditions, yields the same intersection multiplicities.

As mentioned in the introduction, we did not succeed in finding a proof within reasonable time, and thus decided to leave this gap open.

With a further result about the resultant, we are even able to calculate intersection multiplicities of effective divisors:

Proposition 2.11. *Let A be an integral ring and let $f, g \in A[X]$, such that there exist $c_1, \ldots, c_m, d_1, \ldots, d_n \in A$ satisfying*

$$f = \prod_{i=1}^{m}(X - c_i), \quad g = \prod_{j=1}^{n}(X - d_j).$$

Then

$$\begin{aligned} R_{f,g} &= \prod_{i=1}^{m}\prod_{j=1}^{n}(c_i - d_j) = \prod_{i=1}^{m} g(c_i) \\ &= (-1)^{mn}\prod_{j=1}^{n} f(d_j) = (-1)^{mn} \cdot R_{g,f}. \end{aligned}$$

Proof. Let $B = \mathbb{Z}[Y_1, \ldots, Y_m, Z_1, \ldots, Z_n]$, and define the polynomials $F, G \in B[X]$ by

$$\begin{aligned} F &:= \prod_{i=1}^{m}(X - Y_i) = \sum_{i=0}^{m} F_i X^{m-i}, \\ G &:= \prod_{j=1}^{n}(X - Z_j) = \sum_{j=0}^{n} G_j X^{n-j}, \end{aligned}$$

where F_i and G_j are the elementary symmetric polynomials of $Y_1, \ldots, Y_m$ and $Z_1, \ldots, Z_n$ respectively. Each of them is homogeneous if degree i or j, respectively. Define

$$R := R_{F,G} \in B, \quad S := \prod_{i=1}^{m}\prod_{j=1}^{n}(Y_i - Z_j) \in B.$$

Both R and S are homogeneous polynomials of degree $n \cdot m$.

We need to show that $R = S$. Fortunately, we do not need to calculate the determinant: If we substitute Z_j by Y_i in G, then F and G have a common linear factor. Thus R is zero for $Z_j = Y_i$, and $(Y_i - Z_j)$ must be a divisor of R. We can do this for any pair (i, j), thus S is a divisor of R. Since both have the same degree, there is a factor $a \in \mathbb{Z}$ such that $R = aS$.

To show that $a = 1$ we have a look at the summand $(-1)^{mn}(Z_1 \cdot \ldots \cdot Z_n)^m$ of R. This is the diagonal of the resultant matrix, and can not appear otherwise in its determinant. But it also is a summand of S, thus $a = 1$.

If we now substitute Y_i and Z_j by the constant polynomials $Y_i = c_i$ and $Z_j = d_j$, the statement follows. □

Corollary 2.12. *Let $f_1, f_2, g \in A[X]$ be polynomials. Then*

$$R_{f_1 \cdot f_2, g} = R_{f_1, g} \cdot R_{f_2, g} \in A.$$

Proof. If all 3 polynomials are monic, then applying Proposition 2.11 in the common splitting field of f_1, f_2, g over the quotient field of A gives the result.

Any polynomial is a multiple of a monic polynomial in its splitting field. By taking the polynomials to the algebraic closure, we can write the polynomials as $f_1 = a_1 h_1$, $f_2 = a_2 h_2$ and $g = b h'$, i.e.

$$\begin{aligned} f_1 &= a_1 \left(\sum_{i=0}^{m_1} f_{1i} X^{m_1 - i} \right), \quad a_1 \neq 0, \\ f_2 &= a_2 \left(\sum_{i=0}^{m_2} f_{2i} X^{m_2 - i} \right), \quad a_2 \neq 0, \\ g &= b \left(\sum_{j=0}^{n} g_j X^{n-j} \right), \quad b \neq 0. \end{aligned}$$

Then the resultants become

$$\begin{aligned} R_{f_1,g} &= a_1^n b^{m_1} R_{h_1,h'} \\ R_{f_2,g} &= a_2^n b^{m_2} R_{h_2,h'} \\ R_{f_1 f_2,g} &= (a_1 a_2)^n b^{m_1+m_2} R_{h_1 h_2,h'}. \end{aligned}$$

Thus the formula holds for every polynomial in $A[X]$. □

Proposition 2.13. *Let $C = V(F)$, $C' = V(F')$ and $D = V(G)$ be curves, all containing the point P, such that P does not lie on a common component of $C + C' := V(F \cdot F')$ and D. Then*

$$\mu_P(C + C', D) = \mu_P(C, D) + \mu_P(C', D).$$

Proof. By Corollary 2.12, the resultant is multiplicative, thus zero orders are additive. □

Theorem 2.14 (Bézout's Theorem)**.** *For effective divisors C_1 and C_2 of degree m and n, respectively, with no common components,*

$$\sum_{P \in C_1 \cap C_2} \mu_P(C_1, C_2) = m \cdot n.$$

Proof. By the Proposition 2.13 it suffices to show the theorem for reduced curves.

Using the same construction as in Theorem 2.8, if necessary via coordinate transformation, we get at most $m \cdot n$ lines through q, containing intersection points. But since we count intersection multiplicities in exactly the same way as we count zeros of G with multiplicities, those numbers must be equal. Thus,

$$\sum_{P \in C_1 \cap C_2} \mu_P(C_1, C_2) = \deg G = m \cdot n.$$

□

3 Singularities and Tangents

The notion of counting intersection multiplicities is clearly a local matter. We can study local properties more easily if we reduce to the affine case. Let $C = V(F)$, and let $f \in k[X, Y]$ be the dehomogenisation of F, and let $P = (1 : x : y)$ be a finite point (i.e. not on the line at infinity). Then we can substitute $X = x + (X - x)$ and $Y = y + (Y - y)$, resulting in a new representation of $f(X, Y)$:

$$f(X, Y) = \sum_{m=0}^{\deg F} f_{(m)}, \text{ where } f_{(m)} = \sum_{\mu+\nu=m} a_{\mu\nu} (X - x)^\mu (Y - y)^\nu,$$

where $a_{\mu\nu} = (D_X^\mu D_Y^\nu f)(x, y)$ and D_X, D_Y are the k-linear Hasse differentials

$$\begin{array}{rcccc} D_X^\mu & : & k[X,Y] & \to & k[X,Y] \\ & & X^m & \mapsto & \binom{m}{\mu} X^{m-\mu}, \\ & & Y & \mapsto & Y, \end{array} \qquad \begin{array}{rcccc} D_Y^\nu & : & k[X,Y] & \to & k[X,Y] \\ & & X & \mapsto & X, \\ & & Y^n & \mapsto & \binom{n}{\nu} Y^{n-\nu}. \end{array}$$

Definition 3.1. We define the *order* of $P = (1 : x : y) \in \mathbb{P}^2_k$ with respect to C to be

$$m_P(C) := \min\{m : f_{(m)} \neq 0\}.$$

Definition 3.2. A point $P \in C$ is called a *simple* or *regular* point of C if $m_P(C) = 1$. Then the curve C is called *smooth* or *regular* at P. If $m_P(C) > 1$, then P is called a *multiple* or *singular* point or a *singularity* of C. A curve that has no singularities is called *smooth* or *nonsingular*. We denote the set of all singular points with $\mathrm{Sing}(C)$, and the set of all regular points with $\mathrm{Reg}(C)$.

Remark 3.3. Obviously, projective coordinate transformations do not change the order of a point. Thus we can define the order of a point at infinity independently of the chosen projective coordinates.

Lemma 3.4. Let C be a curve and P a point in $\mathbb{P}^2_k$.

1. $0 \leq m_P(C) \leq \deg C$,
2. $m_P(C) = 0 \iff P \notin C$.

Proof. 1. This is obvious from the definition of $m_P(C)$.

2. $m_P(C) = 0 \iff f_{(0)} = f(x, y) \neq 0 \iff P \notin C$.

□

Proposition 3.5. *The order of a point $P \in C = V(F)$ is also given by*

$$m_P(C) = \min\{\mu_P(C, L) \mid L \text{ is a line through } P\}.$$

Proof. Let $m := m_P(C)$ and $n := \deg C$. Without loss of generality, reduce to the following, affine case: Let L be a line through P, given by $L = V(pX_0 + qX_1 + rX_2)$. Apply a coordinate transformation, such that P maps to $(1 : 0 : 0)$ and $L = V(aX_1 - X_2)$ for some $a \in k$. Now dehomogenise F with respect to X_0, i.e. $f(X, Y) = F(1, X, Y)$. Hence L is now given by $V(Y - aX)$.

If we write f as the sum of its homogeneous components, $f = f_0 + \ldots + f_n$, we know that $f_i = 0$ for $i < m$, because in that case $f_i = f_{(i)} = 0$. Thus

$$f(X, aX) = X^m \sum_{i=m}^{n} X^{i-m} f_i(1, a).$$

By embedding the curve into the projective space again, we see that $\mu_P(C, L) \geq m$ by definition 2.2. Furthermore, $f_m(1, a)$ is a non-zero polynomial in a, thus there exists a line $L' = V(Y - a'X)$ with $\mu_P(C, L') = m$. □

Definition 3.6. A line L through a point P of a curve C is called a *tangent* if

$$\mu_P(C, L) > m_P(C).$$

This definition is due to Kunz [2], and we shall see immediately how useful the definition is.

Corollary 3.7. *A point P on a curve $C = V(F)$ of order $m := m_P(C)$ has at least one and at most m tangents. If $P = (1 : 0 : 0)$, they are given by the linear decomposition*

$$f_{(m)} = \prod_{j=1}^{m} (a_j X - b_j Y).$$

Proof. We know that $f_m(1, a)$ from the proof of 3.5 is a polynomial of degree m in a, thus has, counted with multiplicity, m zeros.

Let a_j be a zero of $f_m(1, a)$. Thus the line $V(Y - a_j X)$ is tangent to P. Since $P = (1 : 0 : 0)$, the projective coordinate tansformation that we applied in the proof is only necessary if the line $V(X)$ is tangent to C. Thus we get that the collection of all tangents in P is given by the zero set of

$$\prod_{j=1}^{m} (a_j X - b_j Y) = f_{(m)}.$$

□

Corollary 3.8. *If $C = V(F)$ and $F = \prod_{k=1}^{n} F_k$, where each F_k is irreducible, then*

$$m_P(C) = \sum_{k=1}^{n} m_P(V(F_k)).$$

Proof. Assuming $P = (0, 0)$ and the line at infinity is not contained in C, the dehomogenisation f of F has a factorisation $f = \prod_{k=1}^{n} f_k$. Let $m_k := m_P(F_k)$. Applying the procedure of the proof of Proposition 3.5 to the factors f_k of f, we get

$$\begin{aligned} f(X, aX) &= \prod_{k=1}^{n} \left(X^{m_k} \left(\sum_{l=m_k}^{\deg f_k} X^{l-m_k} f_{k,l}(1, a) \right) \right) \\ &= X^{\sum_{k=1}^{n} m_k} \cdot \prod_{k=1}^{n} \left(\sum_{l=m_k}^{\deg f_k} f_{k,l}(1, a) \right). \end{aligned}$$

Thus, $m_P(C) = \sum_{k=1}^{n} m_P(V(F_k))$. □

Corollary 3.9. *A simple point P on C does not lie on two distinct components of C.*

Proof. By corollary 3.8, a point that lies on two components $C_1 \neq C_2$ must have

$$m_P(C) \geq m_P(C_1) + m_P(C_2) \geq 2.$$

□

Corollary 3.10. *Every smooth plane projective curve is irreducible.*

Proof. A reducible curve consists of at least two components. By Bézout's Theorem, these must intersect, thus the curve has a multiple point. □

Proposition 3.11 (Euler Formula)**.** *Any homogeneous polynomial F satisfies*

$$X_0\frac{\partial F}{\partial X_0} + X_1\frac{\partial F}{\partial X_1} + X_2\frac{\partial F}{\partial X_2} = F \cdot \deg F.$$

Proof. Decompose F into all its summands $F_i = a_i X_0^{b_i} X_1^{c_i} X_2^{d_i}$, with $b_i + c_i + d_i = \deg F$. Then

$$\begin{aligned} X_0\frac{\partial F_i}{\partial X_0} + X_1\frac{\partial F_i}{\partial X_1} + X_2\frac{\partial F_i}{\partial X_2} &= a_i \cdot (b_i + c_i + d_i) \cdot X_0^{b_i} X_1^{c_i} X_2^{d_i} \\ &= F_i \cdot \deg F. \end{aligned}$$

□

Proposition 3.12 (Jacobi Criterion)**.** *A point $P = (x_0 : x_1 : x_2) \in C = V(F)$ is singular if and only if*

$$F_{X_i}(P) := \frac{\partial F}{\partial X_i}(x_0, x_1, x_2) = 0, \quad \textit{for all } i = 0, 1, 2.$$

Proof. By coordinate transformation, assume $x_0 = 1$. Now consider the Taylor series of F at $(1 : x_1 : x_2)$:

$$F = F(1, x_1, x_2) + (X_0 - 1)F_{X_0}(P) + (X_1 - x_1)F_{X_1}(P) + (X_2 - x_2)F_{X_2}(P) + \cdots$$

The first summand vanishes, since $F(P) = 0$. Dehomogenise with respect to X_0, and set $X := X_1 - x_1$, $Y := X_2 - x_2$. Then we get an affine polynomial corresponding to F, in a coordinate system where $P = (0, 0)$. It has the form

$$X \cdot F_{X_1}(P) + Y \cdot F_{X_2}(P) + (\text{terms of higher order}).$$

By definition 3.1, $m_P(C) > 1$ if and only if $F_{X_1}(P) = F_{X_2}(P) = 0$. Furthermore, the Euler Formula tells us that

$$1 \cdot F_{X_0}(P) + x_1 \cdot F_{X_1}(P) + x_2 \cdot F_{X_2}(P) = F(1, x_1, x_2) \cdot \deg F = 0,$$

thus $m_P(C) > 1 \iff F_{X_0}(P) = F_{X_1}(P) = F_{X_2}(P) = 0$. □

Proposition 3.13. *If two curves C, C' intersect at a point P, we have*

$$\mu_P(C, C') \geq m_P(C) \cdot m_P(C').$$

Equality holds if and only if the curves do not have common tangents in P.

The proof of this strong statement requires a large set of local methods. Instead of providing these methods, we prove a weaker version, which satisfies our needs.

Lemma 3.14. If P is a singular point on $C = V(F)$, any intersection at P with a different curve $C' = V(G)$ has a multiplicity of at least 2.

Proof. Let n be the degree of C, m the degree of C', and by a coordinate transformation assume $P = (1:0:0)$. Write F and G in terms of X_2, i.e.

$$\begin{aligned} F(X_0, X_1, X_2) &= a_0 X_2^n + a_1 X_2^{n-1} + \ldots + a_n, \\ G(X_0, X_1, X_2) &= b_0 X_2^m + b_1 X_2^{m-1} + \ldots + a_m. \end{aligned}$$

Since $F(P) = G(P) = 0$, we know that $a_n(1,0) = b_m(1,0) = 0$. Furthermore, by the Jacobi Criterion, $\frac{\partial F}{\partial X_2}(P) = a_{n-1}(1,0) = 0$ and $\frac{\partial a_n}{\partial X_0}(1,0) = \frac{\partial a_n}{\partial X_1}(1,0) = 0$ and $(1,0)$ is a double zero of a_n. Thus the resultant matrix looks like

$$R_{F,G} = \det \begin{pmatrix} a_0 & \cdots & \cdots & a_{n-2} & 0 & 0 & & & \\ & \ddots & & & \ddots & \ddots & \ddots & & \\ & & \ddots & & & \ddots & a_{n-1} & a_n & \\ & & a_0 & & \cdots & & a_{n-2} & a_{n-1} & a_n \\ b_0 & \cdots & & b_{m-1} & b_m & & & & \\ & \ddots & & & & \ddots & \ddots & & \\ & & & & & & b_{m-1} & b_m & 0 \\ & & & b_0 & & \cdots & & b_{m-1} & b_m \end{pmatrix}$$

The last two columns guarantee, that every summand in the determinant has one of the factors a_n or $b_m \cdot a_{n-1}$. Thus we get at least a double zero at the point $(1,0)$, i.e. $\mu_P(C, C') \geq 2$. □

Proposition 3.15. *A curve $C = V(F)$ has only finitely many singularities.*

By the Jacobi Criterion and Bézout's Theorem we only need to prove that F and its partial derivatives do not vanish and have no common factors.

Claim 1: F has at least one non-vanishing partial derivative.

> *Proof.* If $\operatorname{char} k = 0$, this obviously holds, since F has a positive degree.
>
> If $\operatorname{char} k = p$ and all three partial derivatives vanish, then every appearing power of X_0, X_1 and X_2 must be a multiple of p. Thus
>
> $$F(X_0, X_1, X_2) = G(X_0^p, X_1^p, X_2^p) = G(X_0, X_1, X_2)^p,$$
>
> contradicting the minimality of F. □

Claim 2: F and its non-vanishing partial derivatives have no common factors.

Proof. By claim 1 and a choice of coordinates assume that $\frac{\partial F}{\partial X_1} \neq 0$ and the line at infinity is not contained in C. Thus only finitely many points at infinity can be singularities and we can reduce to the affine case.

Let $f = \prod_i f_i$ be the decomposition of f into irreducible factors. Then

$$\frac{\partial f}{\partial X_1} = \sum_i \frac{\partial f_i}{\partial X_1} \prod_{j \neq i} f_j.$$

Any factor f_{i_0} of f certainly divides all summands containing f_{i_0} itself. But it does not divide $\frac{\partial f_{i_0}}{\partial X_1} \prod_{j \neq i_0} f_j$, since it has higher degree than $\frac{\partial f_{i_0}}{\partial X_1}$ and each f_j is irreducible. □

Remark 3.16. In particular, a curve $C = V(F)$ of degree n has at most $n(n-1)$ singularities, since $V(\frac{\partial F}{\partial X_1})$ is a curve of degree $n-1$. Our next task is to improve this (weak) bound.

Definition 3.17. The vector space $V_{m,n} \subset k[X_0, \ldots, X_m]$ is the vector space of homogeneous polynomials of degree n in $m+1$ variables.

Lemma 3.18.

$$\dim V_{m,n} = \binom{n+m}{m}.$$

Proof. There are $\binom{n+m}{n}$ different monomials of degree n in $m+1$ variables. □

Thus, $(V_{2,n} \setminus \{0\})/k^*$ is isomorphic to $\mathbb{P}_k^N$, where $N := \dim V_{2,n} - 1$.

Up to the end of this chapter we set $N = \binom{n+2}{n} - 1 = \frac{n(n+3)}{2}$.

Remark 3.19. Any element of $\mathbb{P}_k^N$ defines an effective divisor of $\mathbb{P}_k^2$ of degree n via the associated polynomial.

Lemma 3.20. For any N not necessarily different points, there is a curve of degree $\leq n$ containing all these points.

Proof. Let $ev_{P_1,P_2,\ldots,P_m} : V_{2,n} \to k^m$ be the evaluation map of a polynomial at the points $P_1, \ldots, P_m$, i.e. $ev_{P_1,P_2,\ldots,P_m}(F) = (F(P_1), \ldots, F(P_m))$. Obviously this is a linear map of k-vectorspaces, thus we can use results from general linear algebra.

Our goal is to prove that there exists a curve which contains some specified points. This is equivalent to proving that the kernel of the evaluation map at these points is non-trivial. But finding the kernel means just solving an equation system in N variables and m equations. If we set $m = N$ we know that the kernel is non-trivial and the lemma is proven. □

Proposition 3.21. *An irreducible curve C of degree n has at most*

$$\gamma(n) := \binom{n-1}{2} = \frac{(n-1)(n-2)}{2}$$

singularities.

Proof. For $n = 1$ and $n = 2$, this is obviously true, since lines and quadrics are smooth. Thus we can assume $n \geq 3$. Suppose C has at least $\gamma(n)+1$ singularities. We specifiy up to $n-3$ additional points on the curve, totalling to $\frac{(n-2)(n+1)}{2}$. Hence there is a curve C' of degree $m \leq n-2$, that contains all these points. Counting intersection multiplicities using Lemma 3.14, we get

$$\sum_{P \in C \cap C'} \mu_P(C, C') \geq 2(\gamma(n)+1) + n - 3 = n(n-2) + 1.$$

The curve C is irreducible and C' is of lower degree, thus they have no common components and we can use Bézout's Theorem, which tells us that

$$\sum_{P \in C \cap C'} \mu_P(C, C') = n \cdot m \leq n \cdot (n-2).$$

Thus we have found a contradiction. □

Corollary 3.22. *A curve C of degree n has at most $n(n-1)/2$ singularities. A curve which has this maximum of possible intersections is the union of n pairwise distinct lines.*

Proof. If C is irreducible, Proposition 3.21 is a far better bound.

Assume the corollary is true for some curve C. Then the upper bound for the number of singularities of the union of C with an irreducible curve D of degree m is

$$\begin{aligned} |\operatorname{Sing}(C)| + |\operatorname{Sing}(D)| + |C \cap D| &\leq \frac{n(n-1) + (m-1)(m-2)}{2} + mn \\ &= \frac{n^2 - n + m^2 - 3m + 2 + 2mn}{2} \\ &\leq \frac{n^2 - n + m^2 - m + 2mn}{2} \\ &= \frac{(m+n)(m+n-1)}{2}. \end{aligned}$$

Equality holds if and only if $m = 1$. The statement now follows by induction over the number of irreducible components. □

4 The Hessian of a Curve

Definition 4.1. A point P on a curve C is called a *flex* or *inflexion point*, if P is simple and the unique tangent L to P satisfies $\mu_P(C, L) > 2$. The tangent is then called a *flex tangent*. If the tangent is not a component of C, then P is called a *proper flex*.

Remark 4.2. Since the definitions of the order of a point and intersection multiplicity are independent of the choice of coordinates, this also holds for the definition of a flex.

Example. On a line L, any point $P \in L$ is an improper flex. Furthermore, a curve C of degree 2 can not have any proper flexes, since any line intersects C with a multiplicity of at most 2, by Bézout's Theorem.

In the following, assume that a curve C has a degree $n \geq 3$, and that a point $P \in C$ is simple. Furthermore, apply a projective coordinate transformation, such that P maps to $(1:0:0)$, and that the tangent L to P is given by $L = V(X_2)$. If we dehomogenise F to f now, we get the following lemma:

Lemma 4.3. A point P is an improper flex of C if and only if Y is a factor of f. Otherwise, there exists $\phi \in k[X]$, $\psi \in k[X,Y]$, $\mu \in \mathbb{N}$ satisfying $\phi(0) \neq 0$, $\psi(0,0) \neq 0$, $\mu = \mu_P(C,L)$, such that f can be written as

$$f(X,Y) = X^\mu \phi(X) + Y \cdot \psi(X,Y).$$

Proof. The case of an improper flex is obvious. For the second case, observe that we always can decompose f in this manner, if we forget about the restrictions. Thus we have to show that the property of P being a proper flex implies $\phi(0) \neq 0$, $\psi(0,0) \neq 0$.

We know that $\mu_P(C,L) \geq 3$ and P is proper, thus f satisfies

$$f(X,0) = X \cdot \sum_{k=1}^{n} X^{k-1} f_k(1,0),$$

where $f_1(1,0) = f_2(1,0) = 0$. Decompose $f(X,0)$ to $X^\mu \cdot \phi(X)$, such that $\phi(0) \neq 0$. Then $\mu \geq 2$. Thus we have a decomposition

$$f(X,Y) = X^\mu \phi(X) + \varphi(X,Y),$$

where $\varphi(0,0) = 0$, otherwise $f(0,0) \neq 0$. Furthermore, every monomial of φ must have Y as a factor, otherwise it would be part of $X^\mu \cdot \phi(X)$. Thus, $\varphi(X,Y) = Y \cdot \psi(X,Y)$. Since the line $X = 0$ is not a tangent, $f(0,Y) = Y \cdot \psi(0,Y)$ must have a zero of order 1 in $(0,0)$. Hence $\psi(0,0) \neq 0$. □

Definition 4.4. The *Hessian determinant* of a homogeneous polynomial F is given by

$$H_F := \det\left(\frac{\partial^2 F}{\partial X_i \partial X_j}\right)_{i,j=0,1,2}.$$

If $C = V(F)$ and $H_F \neq 0$, then the *Hessian curve* of C is given by $H_C := V(H_F)$.

Lemma 4.5. H_C is independent of the choice of coordinates.

Proof. Applying the chain rule to $F^T(X_0, X_1, X_2)$ gives

$$H_{F^T}(X_0, X_1, X_2) = (\det T)^2 \cdot H_F((X_0, X_1, X_2) \cdot T^{-1}).$$

□

Let $F_{X_i} := \frac{\partial F}{\partial X_i}$ and $F_{X_i X_j} := \frac{\partial^2 F}{\partial X_i \partial X_j}$.

Lemma 4.6. For $n := \deg F$ we always have

$$X_0^2 \cdot H_F = \begin{vmatrix} n(n-1)F & (n-1)F_{X_1} & (n-1)F_{X_2} \\ (n-1)F_{X_1} & F_{X_1X_1} & F_{X_1X_2} \\ (n-1)F_{X_2} & F_{X_1X_2} & F_{X_2X_2} \end{vmatrix}.$$

Proof. Multiplying the first row of H_F by X_0 and adding X_1 times the second row and X_2 times the third row gives

$$X_0 \cdot H_F = \begin{vmatrix} X_0 \cdot \sum_{j=0}^{2} F_{X_0X_j} & X_1 \cdot \sum_{j=0}^{2} F_{X_1X_j} & X_2 \cdot \sum_{j=0}^{2} F_{X_2X_j} \\ F_{X_0X_1} & F_{X_1X_1} & F_{X_1X_2} \\ F_{X_0X_2} & F_{X_1X_2} & F_{X_2X_2} \end{vmatrix}.$$

Euler's Formula now tells us, that

$$(n-1)F_{X_i} = \sum_{j=0}^{2} F_{X_iX_j} \cdot X_j, \quad i = 0, 1, 2.$$

Thus we get

$$X_0 \cdot H_F = \begin{vmatrix} (n-1)F_{X_0} & (n-1)F_{X_1} & (n-1)F_{X_2} \\ F_{X_0X_1} & F_{X_1X_1} & F_{X_1X_2} \\ F_{X_0X_2} & F_{X_1X_2} & F_{X_2X_2} \end{vmatrix}.$$

Applying the same procedure to columns instead of rows finally results in

$$X_0^2 \cdot H_F = \begin{vmatrix} n(n-1)F & (n-1)F_{X_1} & (n-1)F_{X_2} \\ (n-1)F_{X_1} & F_{X_1X_1} & F_{X_1X_2} \\ (n-1)F_{X_2} & F_{X_1X_2} & F_{X_2X_2} \end{vmatrix}.$$

□

Corollary 4.7. *Every singular point P of $C = V(F)$ lies on its intersection with H_C. Also, $H_F = 0$ if $\operatorname{char} k$ divides $n - 1$.*

The following Theorem tells us, how we can compute inflexion points easily:

Theorem 4.8. *Let $C = V(F)$ be a curve of degree $n \geq 3$. Let p be the characteristic of k, and assume that either $p = 0$ or $p > n$. Then H_F and H_C have the following properties:*

1. *H_F is a multiple of F if and only if C is a union of lines.*
2. *If H_F is not a multiple of F, then the intersection of C with its Hessian H_C consists of the singular points of C and the flexes of C.*
3. *For every point P of C whose tangent L is not a component of C we have*

$$\mu_P(C, L) = \mu_P(C, H_C) + 2.$$

Proof. Let P be a regular point of C with tangent L. By choice of coordinates, assume that $P = (1 : 0 : 0)$ and $L = V(Y)$. Let f be the dehomogenisation of F. By Lemma 4.6, $H_F(P)$ is given by the determinant

$$\Delta := \begin{vmatrix} n(n-1)f & (n-1)f_X & (n-1)f_Y \\ (n-1)f_X & f_{XX} & f_{XY} \\ (n-1)f_X & f_{XY} & f_{YY} \end{vmatrix}.$$

If P is an improper flex of C, then Y is a divisor of f. But then

$$\begin{aligned} f_X(P) &= 0 \cdot \frac{\partial\psi(0,0)}{\partial X} + 0 \cdot \psi(0,0) = 0 \\ f_{XX}(P) &= 0 \cdot \frac{\partial^2\psi(0,0)}{\partial X^2} + 2 \cdot 0 \cdot \frac{\partial\psi(0,0)}{\partial X} + 0 \cdot \psi(0,0) = 0. \end{aligned}$$

Thus the first row of H_F is zero, therefore $H_F(P) = 0$. If C is the union of lines, then C only has improper flexes, and every point on C is on H_C. Thus H_F is a multiple of F.

Now suppose P is a regular point, lying on a component of degree ≥ 2. Then its tangent is not a component of C. Remember that, by Lemma 4.3, we can write f as

$$f(X, Y) = X^\mu\phi(X) + Y \cdot \psi(X, Y).$$

Calculating partial derivatives gives

$$\begin{aligned} f_X &= \mu X^{\mu-1}\phi + X^\mu\phi' + Y \cdot \psi_X, \\ f_{XX} &= \mu(\mu-1)X^{\mu-2}\phi + 2\mu X^{\mu-1}\phi' + X^\mu\phi'' + Y \cdot \psi_{XX}, \\ f_Y &= \psi + Y \cdot \psi_Y, \\ f_{YY} &= 2\psi_Y + Y \cdot \psi_{YY}, \\ f_{XY} &= \psi_X + Y \cdot \psi_{XY}. \end{aligned}$$

Inserting P now gives

$$\begin{aligned} \Delta &= \begin{vmatrix} 0 & 0 & (n-1)\psi(P) \\ 0 & f_{XX}(P) & \psi_X(P) \\ (n-1)\psi(P) & \psi_X(P) & 2\psi_Y(P) \end{vmatrix} \\ &= (n-1)^2 \cdot \psi(P)^2 \cdot f_{XX}(P). \end{aligned}$$

Observe that

$$f_{XX}(P) = \begin{cases} 2\phi(P), & \text{if } \mu = 2 \\ 0, & \text{otherwise} \end{cases}.$$

Thus $\Delta = 0$ if and only if $\mu > 2$. This is equivalent to L being a flex tangent, thus a regular point P is a flex if and only if $P \in C \cap H_C$.

Furthermore, H_F has a decomposition

$$H_F = X_1^{\mu-2}\tilde{\phi}(X_0, X_1) + X_2 \cdot \tilde{\psi}(X_0, X_1, X_2),$$

where $\tilde{\phi}(1,0) \neq 0$. Thus $\mu_P(H_C, L) < \mu_P(C, L)$, hence P lies on a component of C, which is not in H_C. Thus H_F is not a multiple of F.

By calculating the resultat R_{F,H_F}, we see that each summand has the factor $X_1^{\mu-2}$. But there is also a summand of the form $X_1^{\mu-2} \cdot (a_{n-1})^{3n(n-2)} b_0^{n-1}$, and since $m_P(C) = 1$ we have $a_{n-1}(P) \neq 0$. Thus there is a zero of order $\mu - 2$, and the third part of the theorem is proven. □

Example. The assumption about the characteristic of k can not be dropped easily. Suppose $\operatorname{char} k = 3$, and let $F = X_0^2 X_2 - X_1^3$ define the curve C. This curve is irreducible, its only point at infinity is the singularity $(0:0:1)$, and $H_F = 0$. The regular points are all at finite distance and satisfy $Y = X^3$. Thus we have a proper flex at $(0,0)$. But even more, any point (a,b) on the curve at finite distance satisfies

$$Y - X^3 = Y - X^3 - (b - a^3) = Y - b - (X - a)^3.$$

Therefore, any regular point is a flex.

Corollary 4.9. *Unter the assumptions of 4.8 let C be irreducible of degree n with s singularities. Then C has at most $3n(n-2) - 2s$ flexes.*

Proof. By 4.8, the Hessian H_C is non-empty and has no common component with C. Thus Bézout's Theorem tells us that

$$\sum_P \mu_P(C, H_C) = \deg C \cdot \deg H_C = 3n(n-2).$$

But in this sum, s terms come from singularities, and by Lemma 3.14 each intersection at a singularity has a multiplicity of at least two. □

Example. For $n \geq 3$ and $\operatorname{char} k \not| n$, let $F(X_0, X_1, X_2) = X_0^n + X_1^n + X_2^n$. Its associated curve is called the *Fermat curve*. Since $\frac{\partial F}{\partial X_i} = n X_i^{n-1}$ for all i, the partial derivatives never vanish coincidentally, thus the curve is smooth. The Hessian is given by

$$\begin{aligned} H_F &= \det \begin{pmatrix} n(n-1)X_0^{n-2} & 0 & 0 \\ 0 & n(n-1)X_1^{n-2} & 0 \\ 0 & 0 & n(n-1)X_2^{n-2} \end{pmatrix} \\ &= n^3(n-1)^3 (X_0 X_1 X_2)^{n-2}. \end{aligned}$$

Thus an intersection point must have at least one vanishing coordinate. On the other hand, if a point has two vanishing coordinates, it can not lie on the curve, since its third coordinate would have to vanish as well.

Since everything is symmetric, we only have to take a look at the case $P = (0:y:1)$. Then the polynomial equation reduces to $y^n = -1$, and its solutions are the n odd powers of the $2n$-th root of unity. Thus the curve has $3n$ proper inflexion points, and by Corollary 4.9 the Hessian intersects the Fermat curve with multiplicity $n - 2$.

References

[1] Gerd Fischer. *Ebene algebraische Kurven.* vieweg, 1994.

[2] Ernst Kunz. *Introduction to Plane Algebraic Curves.* Birkhäuser, 2005.

[3] Oscar Zariski and Pierre Samuel. *Commutative Algebra, Volume II.* Van Nostrand, 1960.