Abstract

In this thesis we state and give elementary proofs for some fundamental results about intersections of algebraic curves, namely Bezout's, Max Noether's, Pappus's, Pascal's and Chasles' theorems. Our main tools are linear algebra and basic ring theory. We conclude the thesis by applying the results to elliptic curves.

Keywords: Bezout's theorem, Max Noether's fundamental theorem, Pappus's theorem, Pascal's theorem, Chasles' theorem, algebraic curves, elliptic curves

Contents

Introduction

The main motivation for this thesis is to rigorously define addition on elliptic curves and to show that the resulting structure is an abelian group. In order to do this, we use Bezout's theorem and Chasles' theorem, which we also state and prove. Since the latter relies on Max Noether's theorem in its proof, we deduce that theorem as well.

In the first chapter we show a weak version of Bezout's theorem (1.10), namely that two curves of degree n_1 and n_2, respectively, intersect in at most $n_1 n_2$ distinct points, under suitable conditions. We do this by first showing the weak theorem for the affine plane and then strengthening it by performing a number of projective coordinate changes. Along the way we develop the basic correspondence between the affine and projective plane.

The second chapter is concerned with intersection multiplicities, since these are needed in the strong version of Bezout's theorem. The chapter is introduced with an affine definition, followed by properties thereof that will be used in the subsequent chapters. We then show that the definition extends to the projective plane, and that we can make linear changes of variables without affecting multiplicities.

After dealing with intersection multiplicities we state and prove Bezout's theorem (3.1) in Chapter 3, which is the result that any two curves of degree n_1 and n_2, respectively, intersect at exactly $n_1 n_2$ points, under certain conditions and counting multiplicities. Our proof is mostly a detailed version of the outline given in Appendix A Section 4 in Silverman and Tate 1992, albeit in a different order. We have deviated somewhat from the outline by proving Lemma 1.18 in the first chapter, although we only need it for a result which we could have given a more direct proof of. The lemma is not part of the outline in Silverman and Tate 1992, but is instead inspired by the proof of Max Noether's theorem in Fulton 2008.

Before stating and proving Max Noether's theorem we introduce simple points, and deduce some consequences necessary for subsequent chapters.

With all the preparation in the earlier chapters, the proof of Max Noether's theorem (5.1) in Chapter 5 is two lines. In this chapter we also introduce intersection cycles to simplify bookkeeping of intersections. Before continuing we cite a proposition that will allow us to use Max Noether's theorem in the proceeding chapter.

The goal of Chapter 6 is to prove Chasles' theorem (6.6). Due to the amount of work spent on developing the fundamentals in previous sections, the proof is quite short, so we fill out the section by deducing two other interesting consequences of Max Noether's theorem, namely Pappus's and Pascal's theorem. These results date back to the fourth and seventeenth century respectively. For a more detailed reference see David Eisenbud and Harris 1996.

Finally, in the last chapter we use the theorems shown to give a definition of addition on elliptic curves, and to show that the curve endowed with this addition constitutes an abelian group.

We assume the reader is familiar with the definition of the projective plane, $\mathbb{P}_k^2$ over a given base field. Furthermore, the reader is assumed to be accustomed to linear algebra and elementary ring theory.

Notation

$\|A\|$	The cardinality of the set A.
$A \subseteq B$	The set A is a subset of B.
$A \subset B$	The set A is a proper subset of B.
k	A field.
$\mathbb{P}_k^2$	The projective plane over k.
$\dim V$	The dimension of the vector space V over k.
$U \oplus V$	The direct sum of U and V.
$R[x_1, \ldots, x_n]$	The polynomial ring in n variables over R.
$R(x_1, \ldots, x_n)$	The field of fractions over $R[x_1, \ldots, x_n]$.
R/I	The quotient ring R modulo the ideal I.
(a, b)	Coordinates in k^2.
$[A, B, C]$	Homogeneous coordinates in $\mathbb{P}_k^2$.
$\varphi\|_S$	The restriction of the map φ to the set S.
f_i'	The partial derivative of f w.r.t. the i:th argument.
∇f	The gradient of f, i.e. $(f_1', \ldots, f_n')$.

1 A Weak Form of Bezout's Theorem

In this first section we set out to prove a weak form of Bezout's theorem. Before formulating it, we will state and prove lemmas used in its proof.

Through the entirety of this text, we let k be a field. Whenever we find the need to introduce extra conditions on k, those conditions will be stated.

The next lemma is a solution to exercise 2.42(a) in Fulton 2008.

Lemma 1.1. *Let R be a ring and suppose that I and J are ideals in R such that $I \subseteq J$. Then*

$$\varphi : R/I \ni r + I \mapsto r + J \in R/J$$

is a well-defined surjective homomorphism.

Proof. Suppose that $r_1 + I = r_2 + I$. Then $r_1 - r_2 \in I$ so that the assumption gives $r_1 - r_2 \in J$. Thus, $r_1 + J = r_2 + J$, showing that φ is well-defined.

Because

$$\varphi(a + I) + \varphi(b + I) = (a + J) + (b + J) = a + b + J = \varphi(a + b + I)$$

and

$$\varphi(a + I)\varphi(b + I) = (a + J)(b + J) = ab + J = \varphi(ab + I)$$

φ is a homomorphism.

For any element $r + J \in R/J$ one can take one of its preimages $r \in R$ and get $\varphi(r + I) = r + J$. Hence, φ is surjective. $\square$

Lemma 1.2. *Let R be a ring that contains k as a subring. Suppose that I and J are ideals in R such that $I \subseteq J$. Then*

$$\dim(J/I) = \dim J - \dim I.$$

In particular, if $\dim J$ is finite, then $\dim(J/I)$ and $\dim I$ are finite.

Proof. If $I = J$, then

$$\dim(J/I) = 0 = \dim J - \dim J = \dim J - \dim I.$$

Otherwise, it may be assumed that $I \subset J$. If $s \in k \cap I$ with $s \neq 0$, then s is invertible in R, so that $1 = s^{-1}s \in I$, and consequently $I = R$ contradicting that $I \subset J$. Thus, $k \cap I = \{0\}$. Consider the natural homomorphism $\varphi : R \to R/I$. If $s, t \in k$ then

$$\begin{aligned} \varphi(s) = \varphi(t) &\implies \varphi(s - t) = 0 \\ &\implies s - t \in k \cap I \\ &\implies s - t = 0 \\ &\implies s = t \end{aligned}$$

showing that the restriction of $\varphi|_k$ is an isomorphism $k \cong \varphi(k)$. Hence, one may identify k with $\varphi(k)$.

Consider $\varphi|_J : J \to J/I$. Suppose that $s, t \in k$ and that $f, g \in J$. Because $s, t \in R$ one has $sf + tg \in J$ due to J being an ideal in R, and

$$\varphi(sf + tg) = \varphi(s)\varphi(f) + \varphi(t)\varphi(g) = s\varphi(f) + t\varphi(g).$$

This shows that $\varphi|_J$ is a linear transformation. The rank-nullity theorem gives

$$\dim \operatorname{im}(\varphi|_J) + \dim \ker(\varphi|_J) = \dim J \iff \dim(J/I) = \dim J - \dim I. \quad \square$$

Lemma 1.3. *Let R be a ring containing k as a subring. Let I, J and K be ideals in R such that $I \subseteq J \subseteq K$. Then*

$$\dim(K/J) = \dim(K/I) - \dim(J/I).$$

In particular, if $\dim(K/I)$ *is finite, then* $\dim(K/J)$ *and* $\dim(J/I)$ *are finite.*

Proof. If $I = R$, the equality to prove is $0 = 0 - 0$. Otherwise, one may as in the proof of Lemma 1.2 assume that $I \subset R$, with the natural homomorphism $\varphi : R \to R/I$ being an isomorphism when restricted to k. Thus, we may regard k as a subring of R/I. By the third isomorphism theorem J/I and K/I are ideals in R/I, and $J/I \subseteq K/I$. Furthermore, the same theorem gives

$$(K/I)/(J/I) \cong K/J$$

whence applying Lemma 1.2 completes the proof. □

We first define algebraic curves in k^2. Curves in the projective plane $\mathbb{P}^2_k$ are defined analogously. It is easy to verify that the relation $\sim$ on $k[x, y]$ defined by $f \sim g$ if and only if $f = \lambda g$ for some $\lambda \in k$ with $\lambda \neq 0$ is an equivalence relation. The equivalence classes of non-constant polynomials under $\sim$ are called algebraic curves. If f is a representative of C then f is called the defining polynomial of C and one writes $C : f = 0$. It is clear that the set

$$\{(a, b) \in k^2 \ ; \ f(a, b) = 0\}$$

does not depend on the representative f of C. Thus, every algebraic curve induces a unique point set in k^2. The reverse does not hold as is seen by the fact that the distinct algebraic curves $x = 0$ and $x^2 = 0$ induce the same point set. If $f(P) = 0$ one writes $P \in C$. Similarly, we will treat algebraic curves as point sets whenever necessary. For example $C \cap D$ means the set of intersection points of the curves C and D.

An irreducible polynomial $g \in k[x, y]$ is said to be a component of $C : f = 0$ if $g \mid f$. It follows that the curves $C_1 : f_1 = 0$ and $C_2 : f_2 = 0$ have no components in common if and only if $\gcd(f_1, f_2) = 1$.

To relate points of the affine plane k^2 with points of $\mathbb{P}^2_k$ the usual injection

$$k^2 \ni (a, b) \mapsto [a, b, 1] \in \mathbb{P}^2_k$$

is used. To pass from algebraic curves in k^2 to their projective counterparts in $\mathbb{P}^2_k$ consider the map $\xi : k[x, y] \ni f \mapsto F \in k[X, Y, Z]$ defined by

$$F = \sum_{i+j \leq n} a_{i,j} X^i Y^j Z^{n-i-j} \quad \text{where} \quad f = \sum_{i+j \leq n} a_{i,j} x^i y^j.$$

where $\deg f = n$. Because ξ maps polynomials to polynomials and $f \sim g$ if and only if $\xi(f) \sim \xi(g)$, ξ can be seen as a map between algebraic curves.

The map ξ has the desirable property that it respects the induced point sets in the sense that if $C : f = 0$ and $\widetilde{C} : F = 0$ is the projective counterpart with $F = \xi(f)$, then

$$(a, b) \in C \iff [a, b, 1] \in \widetilde{C}.$$

This follows from that $f(a, b) = F(a, b, 1)$.

It shall be shown that the mapping of curves from k^2 to $\mathbb{P}^2_k$ is injective and respects multiplication. In order to simplify this two lemmas are stated. The proofs, which are trivial, have been left out.

Lemma 1.4. *Suppose that R is a subring of $k[x_1, \dots, x_n]$ and let S be a commutative ring that contains k as a subring. If $s_1, \dots, s_n$ are some fixed elements of S, then the evaluation map*

$$R \ni f \mapsto f(s_1, \dots, s_n) \in S$$

is a homomorphism.

Lemma 1.5. *Suppose that R is a subring of $k[x_1, \dots, x_n]$ and that S is a commutative ring containing k as a subring. Assume that $s_1, \dots, s_n \in S$ are algebraically independent over k, i.e.*

$$f(s_1, \dots, s_n) = 0 \implies f = 0$$

for all $f \in k[x_1, \dots, x_n]$. Then

$$R \ni f \mapsto f(s_1, \dots, s_n) \in S$$

is an injective homomorphism.

Note that X/Z and Y/Z are algebraically independent elements of $k(X, Y, Z)$ over k. Also note that the map $f \mapsto F$ above can be written as

$$\xi : k[x, y] \ni f \mapsto Z^m f(X/Z, Y/Z) \in k[X, Y, Z], \quad \deg f = m. \tag{1.1}$$

Because

$$Z^m f(X/Z, Y/Z) \cdot Z^n g(X/Z, Y/Z) = Z^{m+n}(fg)(X/Z, Y/Z)$$

by Lemma 1.5 and $\deg(fg) = m + n$, $\xi(f)\xi(g) = \xi(fg)$ so that ξ respects multiplication. If $Z^m f(X/Z, Y/Z) = Z^n g(X/Z, Y/Z)$, then by comparing degrees of the sides one gets that $\deg f = \deg g$. Thus, $f(X/Z, Y/Z) = g(X/Z, Y/Z)$ and Lemma 1.5 gives $f = g$, showing that ξ is injective and respects multiplication.

That ξ is not a homomorphism is for example seen by the fact that $f = x$ and $g = y^2$ map to $F = X$ and $G = Y^2$, respectively, but $f + g = x + y^2$ maps to $XZ + Y^2 \neq F + G$.

Because ξ is injective and respects multiplication g is a component of C if and only if the homogenization G is a component of the corresponding projective curve $\widetilde{C}$. We may now dispense with the tildes and pass between k^2 and $\mathbb{P}^2_k$ without notice. We have shown how to pass from affine curves to projective curves. The next lemma shows when we may pass from a projective curve to an affine one using the maps introduced.

Lemma 1.6. *Let $C : F = 0$ be a projective curve, where F is a homogeneous polynomial in $k[X, Y, Z]$. If the line at infinity, $Z = 0$, is not a component of C, then $F = \xi(f)$ for some $f \in k[x, y]$.*

Proof. Let $n = \deg F$. Note that

$$F = Z^n F(X/Z, Y/Z, 1).$$

By setting $f = F(x, y, 1)$ one has

$$F = Z^n f(X/Z, Y/Z)$$

and $\deg f \le \deg F = n$. Suppose toward a contradiction that $\deg f < n$ and let $m = \deg f$. Then $Z^m f(X/Z, Y/Z) \in k[X, Y, Z]$ and

$$Z \mid Z^{n-m} \implies Z \mid Z^{n-m} Z^m f(X/Z, Y/Z) \iff Z \mid F$$

contradicting the assumption. Thus, $\deg f = n$ and $F = \xi(f)$. □

From now on we fix the notation $R = k[x, y]$.

Lemma 1.7. *Let $\{P_i\}_{i=1}^m$ be a set of m points of k^2. Then for each i there exists a polynomial $h_i \in R$ such that $h_i(P_j) = \delta_{ij}$ where δ_{ij} is the Kronecker delta.*

Proof. Let i be given and let $P_j = (x_j, y_j)$ for all j. For each j let K_j be the kernel of

$$k^3 \ni (a, b, c) \mapsto ax_j + by_j + c \in k.$$

Suppose $K_j \subseteq K_i$. Then because $(1, 0, -x_j) \in K_j$ one has $(1, 0, -x_j) \in K_i$ so that

$$x_i - x_j = 1 \cdot x_i + 0 \cdot y_i + (-x_j) = 0$$

showing that $x_i = x_j$. Similarly, $y_i = y_j$. Thus, $P_i = P_j$ so that $i = j$. Therefore, one may for each $j \neq i$ take a $\mathbf{v}_j = (a_j, b_j, c_j) \in k^3$ such that $\mathbf{v}_j \in K_j$ in but $\mathbf{v}_j \notin K_i$ and let

$$g_i(x, y) = \prod_{j \neq i} (a_j x + b_j y + c_j).$$

By construction $g_i(P_j) = 0$ for all $j \neq i$ and $g_i(P_i) \neq 0$. Now $h_i = (g_i(P_i))^{-1} g_i$ satisfies the requirements. □

We are now in a position to formulate a weak form of Bezout's theorem. The assumption that the line at infinity is not a component of either curve will be lifted later on.

Theorem 1.8. *If the projective curves C_1 and C_2, of degree n_1 and n_2 respectively have no common component and the line at infinity is not a component of either curve, then C_1 and C_2 intersect at at most $n_1 n_2$ points of k^2.*

Proof. By Lemma 1.6 one may let $f_1, f_2 \in R$ such that the affine parts can be written as $C_1 : f_1 = 0$ and $C_2 : f_2 = 0$.

Let $(f_1, f_2) = Rf_1 + Rf_2$ be the ideal in R generated by f_1 and f_2. The theorem follows whenever it has been shown that

$$|C_1 \cap C_2 \cap k^2| \le \dim(R/(f_1, f_2)) \le n_1 n_2. \tag{1.2}$$

For each $d \in \mathbb{Z}$ define

$$\phi(d) = \binom{d+2}{2} = \frac{1}{2}(d+1)(d+2) \quad \text{and} \quad R_d = \{f \in R\ ;\ \deg f \le d\}.$$

R_d is a linear space over k for all d. Let

$$W_d = R_{d-n_1} f_1 + R_{d-n_2} f_2.$$

Now W_d is a vector space over k such that $W_d \subseteq (f_1, f_2)$ and $W_d = \{0\}$ if $d < \min\{n_1, n_2\}$.

Because each polynomial $f \in R_d$ has a unique representation

$$f = \sum_{i+j \leq d} c_{i,j} x^i y^j$$

with $c_{i,j} \in k$ the monomials $\{x^i y^j\}_{i+j \leq d}$ form a basis for R_d. There are

$$\phi(e) - \phi(e-1) = \frac{1}{2}((e+1)(e+2) - e(e+1)) = \frac{1}{2}(e+1)(e+2-e) = e+1$$

monomials of degree $e \leq d$ in R_d. Therefore, there are

$$\phi(d) = \phi(d) - \phi(-1) = \sum_{e=0}^{d} (\phi(e) - \phi(e-1))$$

monomials in R_d showing that $\dim R_d = \phi(d)$.

Suppose that $d \geq n_1 + n_2$. If $h \in R_{d-n_1-n_2} f_1 f_2$ then $h = g f_1 f_2$ for some $g \in R$ with $\deg g \leq d - n_1 - n_2$. Thus,

$$h = (g f_1) f_2 = (g f_2) f_1$$

with $\deg(g f_1) = \deg g + \deg f_1 \leq d - n_2$ and $\deg(g f_2) \leq d - n_1$, from which $h \in R_{d-n_1} f_1 \cap R_{d-n_2} f_2$ follows. Conversely suppose that $h \in R_{d-n_1} f_1 \cap R_{d-n_2} f_2$. Then

$$h = g_1 f_1 = g_2 f_2$$

for some $g_1, g_2 \in R$ with $\deg g_i \leq d - n_i$. It follows that $f_1 \mid g_2 f_2$, but because $\gcd(f_1, f_2) = 1$ one has $f_1 \mid g_2$, so that $g_2 = g f_1$ for some $g \in R$. It follows that $h = g f_1 f_2$ with

$$d - n_2 \geq \deg g_2 = \deg g + \deg f_1 \implies \deg g \leq d - n_1 - n_2,$$

so that $h \in R_{d-n_1-n_2} f_1 f_2$ showing that

$$R_{d-n_1} f_1 \cap R_{d-n_2} f_2 = R_{d-n_1-n_2} f_1 f_2$$

for all $d \geq n_1 + n_2$.

For all non-zero $f \in R$, the map

$$R_d \ni g \mapsto g f \in R_d f$$

is a linear bijection. It is clearly surjective. If $gf = hf$ for some $g, h \in R$, then because R is an integral domain one has $g = h$. The linearity follows from

$$(ag + bh) f = a(gf) + b(hf)$$

for all $a, b \in k$ and $g, h \in R$. Thus,

$$\dim(R_d f) = \dim R_d = \phi(d).$$

Because $\dim(U + V) = \dim U + \dim V - \dim(U \cap V)$ for all subspaces of a finite dimensional subspace one has that

$$\dim W_d = \dim(R_{d-n_1} f_1) + \dim(R_{d-n_2} f_2) - \dim(R_{d-n_1-n_2} f_1 f_2)$$

for all $d \geq n_1 + n_2$. Analogously with Lemma 1.2 it follows that

$$\begin{aligned}\dim(R_d/W_d) &= \dim R_d - \dim W_d \\ &= \phi(d) - \phi(d-n_1) - \phi(d-n_2) + \phi(d-n_1-n_2) \\ &= n_1 n_2,\end{aligned} \tag{1.3}$$

where the last equality follows from a simple but lengthy calculation.

Now suppose $r > n_1 n_2$ and suppose $g_1, \ldots, g_r$ are polynomials in R. Take $d = \max\{\deg g_1, \ldots, \deg g_r, n_1 + n_2\}$. Then $g_i \in R_d$ for all i and $d \geq n_1 + n_2$. Due to (1.3) there are $c_1, \ldots, c_r \in k$ not all zero such that that

$$\begin{aligned}\sum_{i=1}^{r} c_i g_i \equiv 0 \pmod{W_d} &\iff \sum_{i=1}^{r} c_i g_i \in W_d \\ &\implies \sum_{i=1}^{r} c_i g_i \in (f_1, f_2) \\ &\iff \sum_{i=1}^{r} c_i g_i \equiv 0 \pmod{(f_1, f_2)}.\end{aligned}$$

This shows that any collection of more than $n_1 n_2$ polynomials in R are linearly dependent modulo (f_1, f_2), or in other words that

$$\dim(R/(f_1, f_2)) \leq n_1 n_2. \tag{1.4}$$

This proves the latter inequality of (1.2).

Suppose that $\{P_i\}_{i=1}^{m} \subseteq C_1 \cap C_2 \cap k^2$ and take for each i an $h_i \in R$ such that $h_i(P_j) = \delta_{ij}$. Suppose that

$$\sum_{i=1}^{m} c_i h_i \equiv 0 \pmod{(f_1, f_2)}$$

for some $c_1, \ldots, c_m \in k$. Then

$$\sum_{i=1}^{m} c_i h_i = g_1 f_1 + g_2 f_2$$

for some $g_1, g_2 \in R$ and it follows that

$$c_j = \sum_{i=1}^{m} c_i \delta_{ij} = \sum_{i=1}^{m} c_i h_i(P_j) = g_1(P_j) f_1(P_j) + g_2(P_j) f_2(P_j) = 0$$

for each j by construction and the assumption on P_j. Hence, $h_1, \ldots, h_m$ are linearly independent modulo (f_1, f_2) showing that

$$m \leq \dim(R/(f_1, f_2)).$$

Since $\dim(R/(f_1, f_2))$ is finite by (1.4), it follows that so is $C_1 \cap C_2 \cap k^2$ and one may therefore let $\{P_i\}_{i=1}^{m} = C_1 \cap C_2 \cap k^2$. Then

$$|C_1 \cap C_2 \cap k^2| = m \leq \dim(R/(f_1, f_2))$$

completing the proof of (1.2). $\square$

Corollary 1.9. *If the projective curves C_1 and C_2 have no common component and the projective line L is not a component of either curve, then C_1 and C_2 intersect at at most n_1n_2 points of $\mathbb{P}_k^2 \setminus L$.*

Proof. Given any invertible matrix $M \in k^{3\times 3}$ the space $\mathbb{P}_k^2$ is transformed with

$$\mathbb{P}_k^2 \ni \begin{bmatrix} A \\ B \\ C \end{bmatrix} \mapsto M \begin{bmatrix} A \\ B \\ C \end{bmatrix} \in \mathbb{P}_k^2.$$

It is clear that this map is a well-defined bijection. If $C : F = 0$ is an algebraic curve, then the transformed curve C' must satisfy

$$P \in C \iff MP \in C'$$

where MP is the point acquired by applying M to the homogeneous coordinates of P. Due to this the polynomial F' defining C' satisfies

$$F'(MP) = F(P) \iff F'(P) = F(M^{-1}P).$$

Polynomials are therefore transformed with

$$k[X, Y, Z] \ni F \mapsto F\left(M^{-1}\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}\right) \in k[X, Y, Z]. \tag{1.5}$$

Because the inverse of this map is acquired by replacing M^{-1} with M, the map is a bijection. By Lemma 1.4 the map is an isomorphism. If two integral domains are isomorphic, then so are their fields of fractions. Thus,

$$k(X, Y, Z) \ni \Phi \mapsto \Phi\left(M^{-1}\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}\right) \in k(X, Y, Z) \tag{1.6}$$

is an isomorphism. Hence, a linear transformation of $\mathbb{P}_k^2$ induces an isomorphism on the set of rational expressions on $k(X, Y, Z)$.

Let L be any projective line that is a component of neither C_1 nor C_2. Considering the geometric configurations as part of the U, V, W projective plane one can write L as

$$L : aU + bV + cW = 0$$

for some $a, b, c \in k$, not all zero. Since the space k^3 is three dimensional, there are vectors (m_{11}, m_{12}, m_{13}) and (m_{21}, m_{22}, m_{23}) in k^3 such that the matrix

$$M = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ a & b & c \end{bmatrix}$$

is invertible. By considering the transformation

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = M \begin{bmatrix} U \\ V \\ W \end{bmatrix}$$

one has

$$Z = 0 \iff aU + bV + cW = 0$$

so that the line at infinity in the X, Y, Z plane is mapped to L in the U, V, W plane. This map induces an isomorphism between the X, Y, Z and U, V, W planes, and their curves, respectively. Since L is a component of neither C_1 nor C_2 the line at infinity is not a component of any of the curves corresponding to C_1 and C_2 in the X, Y, Z plane. An application of Theorem 1.8 completes the proof. □

To apply the corollary one must have a line that is not a component of either curve at disposal. We shall strengthen Corollary 1.9 considerably by not requiring the existence of such a line. However, to do this we will require that k is infinite.

Theorem 1.10. *Let k be an infinite field. If the projective curves C_1 and C_2 have no common component, then $|C_1 \cap C_2| \leq (\deg C_1)(\deg C_2)$*

To deduce Theorem 1.10 from Corollary 1.9 one only needs to find a line L that is a component of neither C_1 nor C_2 and does not meet any of their intersections. We now set out to show the existence of such a line using the infinitude of k.

Lemma 1.11. *Let $C_1, \ldots, C_r$ be any finite collection of curves in $\mathbb{P}^2_k$ where k is infinite. Then there exists a line L that is not a component of any of the curves in the collection.*

Proof. Since the degree of each algebraic curve C_i is finite, there are only finitely many lines L_{ij} that are components of C_i. Therefore the set of all such components $\{L_{ij}\}_{i,j}$ is finite. However, the set of all lines is infinite, because the map

$$k \ni a \mapsto \{[X, Y, Z] \in \mathbb{P}^2_k \; ; \; aX + Y + Z = 0\}$$

is injective. Therefore there exists a line that is not a component of any of $C_1, \ldots, C_r$. □

Using the lemma, take a line L_1 that is not a component of either C_1 and C_2. Next, take another line L_2 that is not a component of any of L_1, C_1 and C_2. Because L_1 and L_2 are distinct lines, they intersect at exactly one point, i.e. $|L_1 \cap L_2| = 1$. By some set theoretic manipulation one has

$$C_1 \cap C_2 = C_1 \cap C_2 \cap \mathbb{P}^2_k = C_1 \cap C_2 \cap ((\mathbb{P}^2_k \setminus L_1) \cup (\mathbb{P}^2_k \setminus L_2) \cup (L_1 \cap L_2))$$

By distributing $C_1 \cap C_2$ over the intersection, taking cardinality on both sides and using Corollary 1.9 one gets

$$|C_1 \cap C_2| \leq n_1 n_2 + n_1 n_2 + 1,$$

whence $C_1 \cap C_2$ is finite. This finding we summarize in a lemma.

Lemma 1.12. *Suppose that the projective curves C_1 and C_2 share no component. Then $C_1 \cap C_2$ is finite.*

Proof. If the base field k is finite, $C_1 \cap C_2$ is finite by virtue of being a subset of $\mathbb{P}^2_k$, which is finite. Otherwise, k is infinite and the discussion prior to the lemma suffices as proof. □

Lemma 1.13. *Suppose that S is a finite subset of $\mathbb{P}^2_k$ where k is infinite. Then there are infinitely many projective lines not meeting any of the points of S.*

Proof. It is shown that there exist infinitely many lines L not intersecting S and $\{[0,1,0]\}$, from which the desired result follows.

Suppose toward a contradiction that there are only a finite number, n, of lines not meeting any of the points. Any point $[A,B,C] \in \mathbb{P}^2_k$ with $C \neq 0$ can be written as $[A/C, B/C, 1]$. On the other hand if $C = 0$ and $A \neq 0$ the point has a unique representation $[1, B/A, 0]$. Lastly, if $C = 0$ and $A = 0$ the point can be uniquely represented as $[0,1,0]$. Thus, it is possible to uniquely write

$$S \cup \{[0,1,0]\} = \{[A_1, B_1, 1], \ldots, [A_r, B_r, 1], [1, D_1, 0], \ldots, [1, D_q, 0], [0,1,0]\}$$

for some $A_1, \ldots, A_r, B_1, \ldots, B_r, D_1, \ldots, D_q \in k$.

Let $\mathcal{A}$ be a finite subset with $n+1$ elements of $k \setminus \{A_1, \ldots, A_r\}$. For each $A \in \mathcal{A}$ choose an $a \in k$ such that

$$a \neq 0, \quad a \neq \frac{B_i}{A_i - A} \quad \text{and} \quad a \neq D_j$$

for all $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, q\}$. This is possible to do since k is infinite. Now the line

$$L_A : X - \frac{1}{a}Y - AZ = 0$$

does not meet any point of $S \cup \{[0,1,0]\}$, as is now shown. If $[A_i, B_i, 1] \in L$ then

$$A_i - \frac{1}{a}B_i - A = 0 \implies a = \frac{B_i}{A_i - A}$$

contrary to the construction. If $[1, D_j, 0] \in L$ then

$$1 - \frac{1}{a}D_j = 0 \implies a = D_j$$

which also contradicts the construction. Clearly, $[0,1,0] \notin L$.

If $L_A = L_{A'}$, then since $[A,0,1] \in L_A$ one also has $[A,0,1] \in L_{A'}$ so that $A - A' = 0$ after insertion into the equation of $L_{A'}$. This shows that the map $A \mapsto L_A$ is injective, but then there are $n+1$ lines not meeting any of the points of S. This contradicts the supposition, whence there are infinitely many lines not meeting S. $\square$

Using this lemma the proof of Theorem 1.10 is a simple manoeuvre.

Proof of Theorem 1.10. There are only finitely many components of C_1 and C_2. By the lemma there is a line L that is not a component of either C_1 and C_2 and does not meet $C_1 \cap C_2$. Now one has

$$\begin{aligned} C_1 \cap C_2 &= C_1 \cap C_2 \cap \mathbb{P}^2_k \\ &= C_1 \cap C_2 \cap ((\mathbb{P}^2_k \setminus L) \cup L) \\ &= (C_1 \cap C_2 \cap (\mathbb{P}^2_k \setminus L)) \cup (C_1 \cap C_2 \cap L) \\ &= (C_1 \cap C_2 \cap (\mathbb{P}^2_k \setminus L)), \end{aligned}$$

so after taking the cardinality on both sides and using Corollary 1.9 one gets

$$|C_1 \cap C_2| \leq n_1 n_2$$

completing the proof of Theorem 1.10. $\square$

By the next lemma we may apply Theorem 1.10 to any algebraically closed field.

Lemma 1.14. *Any algebraically closed field is infinite.*

Proof. Suppose toward a contradiction that an algebraically closed field k is finite. Then by listing the elements one has $k = \{a_1, \dots, a_n\}$. Now

$$f = \prod_{i=1}^{n}(x - a_i) + 1$$

is a polynomial without any zero in k, contrary to the assumption that k is algebraically closed. This completes the proof. $\square$

To further strengthen the theorem one needs to introduce intersection multiplicities. Before doing so, we show that (1.4) is in fact an equality under the assumption that k is algebraically closed and that C_1 and C_2 do not meet at infinity. As we have seen, the latter condition can be erased by applying a suitable linear change of variables, after which the equality holds in the entirety of $\mathbb{P}^2_k$.

The following lemmas are more general than necessary at the moment, but the additional generality will pay off greatly in the proof of Max Noether's fundamental theorem.

Lemma 1.15. *For all $F \in k[x_1, \dots, x_d]$ there exist unique homogeneous polynomials $F_i \in k[x_1, \dots, x_d]$ of degree i where at most a finite number of the F_i's are non-zero, such that $F = \sum_{i\in\mathbb{N}} F_i$.*

Proof. Let

$$F = \sum_{j_1+\cdots+j_d\leq n} c_{j_1,\dots,j_d} x_1^{j_1} \cdots x_d^{j_d}.$$

The existence is seen by rearranging the terms so that

$$F = \sum_{i=0}^{n} \underbrace{\sum_{j_1+\cdots+j_d=i} c_{j_1,\dots,j_d} x_1^{j_1} \cdots x_d^{j_d}}_{F_i} = \sum_{i\in\mathbb{N}} F_i$$

where $F_i = 0$ for $i > n$.

For the uniqueness suppose that $F = \sum_{i\in\mathbb{N}} F_i = \sum_{i\in\mathbb{N}} G_i$ where F_i and G_i are homogeneous and at most finitely many F_i's and G_i's are non-zero. Let

$$n = \max\{i \in \mathbb{N}\ ;\ F_i \neq 0 \text{ or } G_i \neq 0\}.$$

Then

$$F = \sum_{i=0}^{n} F_i = \sum_{i=0}^{n} G_i \implies \sum_{i=0}^{n}(F_i - G_i) = 0$$

We now show by induction that if $\sum_{i=0}^{n} H_i = 0$ for some homogeneous polynomials H_i of degree i then $H_i = 0$ for $i \leq n$, from which the result follows. For

$n = 0$ the assumption directly yields the desired result. Assume that the result is true for n and that $\sum_{i=0}^{n+1} H_i = 0$. It then follows that

$$-H_{n+1} = \sum_{i=0}^{n} H_i$$

but the left hand side is either 0 or has degree $n + 1$. However, the right hand side has degree at most n. Thus, $H_{n+1} = 0$ and $\sum_{i=0}^{n} H_i = 0$. The induction hypothesis gives that $H_i = 0$ for $i \leq n$ completing the induction step. By the induction principle the proof is complete. $\square$

For any polynomial $F \in k[X, Y, Z]$ define $F_0 = F(X, Y, 0)$.[1]

Lemma 1.16. *Suppose that k is an algebraically closed field. If $F = 0$ and $G = 0$ are projective curves not meeting at infinity, then* $\gcd(F_0, G_0) = 1$.

Proof. Let $\deg F = m$ and set

$$F = \sum_{i_1+i_2+i_3=m} c_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3}.$$

By rearranging the terms one has

$$F = \sum_{i+j=m} c_{i,j} X^i Y^j + Z \sum_{\substack{i_1+i_2+i_3=m \\ i_3 \geq 1}} c_{i_1,i_2,i_3} X^{i_1} Y^{i_2} Z^{i_3-1}$$

with $c_{i,j} = c_{i,j,0}$. Thus,

$$F_0 = \sum_{i+j=m} c_{i,j} X^i Y^j$$

is a homogeneous polynomial in $k[X, Y]$. Because k is algebraically closed one has that

$$F_0 = \prod_{i=1}^{m} (a_i X + b_i Y)$$

for some $a_i, b_i \in k$. Similarly, $G_0 = \prod_{j=1}^{n} (a'_j X + b'_j Y)$ for some $a'_j, b'_j \in k$. If F_0 and G_0 share a common factor, then they share a factor on the form $aX + bY$. It then follows that F_0 and G_0 have common zeros at $(tb, -ta)$ for all $t \in k$, but then $[b, -a, 0]$ is a common zero of F and G that lie on the line at infinity, which contradicts the assumption. Hence, F_0 and G_0 share no factor and $\gcd(F_0, G_0) = 1$ follows as desired. $\square$

Lemma 1.17. *Suppose that k is an algebraically closed field. Let $F = 0$ and $G = 0$ be projective curves not meeting at infinity. Let $H, A, B \in k[X, Y, Z]$. If $ZH = AF + BG$, then $H = A'F + B'G$ for some $A', B' \in k[X, Y, Z]$.*

Proof. By passing to the homomorphism $J \mapsto J_0$ one has $A_0 F_0 + B_0 G_0 = 0$. Lemma 1.16 gives that $\gcd(F_0, G_0) = 1$ and it follows that $F_0 \mid B_0$ so that $B_0 = EF_0$ for some $E \in k[X, Y]$. Consequently, $A_0 = -EG_0$. Let $A_1 = A + EG$ and $B_1 = B - EF$. Note that $ZH = A_1 F + B_1 G$. Because Z is a monic

[1] This F_0 is of course different from the F_0 in Lemma 1.15.

polynomial one may divide A_1 by viewing it as a polynomial in Z over $k[X, Y]$. Doing this one gets

$$A_1 = ZA' + S$$

for some $A' \in k[X, Y, Z]$ and $S \in k[X, Y]$. By passing to the homomorphism $J \mapsto J_0$ one sees that

$$S = (A_1)_0 = A_0 + EG_0 = 0$$

so $A_1 = ZA'$. Similarly, $B_1 = ZB'$ for some $B' \in k[X, Y, Z]$. Now

$$ZH = ZA'F + ZB'G$$

and the result follows by canceling Z. □

Lemma 1.18. *Let $F = 0$ and $G = 0$ be projective curves with no intersections on the line at infinity. Suppose that H is a homogeneous polynomials in $k[X, Y, Z]$. Let $f = F(x, y, 1)$, $g = G(x, y, 1)$ and $h = H(x, y, 1)$. If $h = af + bg$ for some $a, b \in R$, then $H = AF + BG$ for some homogeneous polynomials $A, B \in k[X, Y, Z]$ with $\deg A = \deg H - \deg F$ and $\deg B = \deg H - \deg G$.*

Proof. Let

$$n = \max\{\deg H, \deg a + \deg F, \deg b + \deg G\}$$

and

$$r + \deg H = \deg a + r_a + \deg F = \deg b + r_b + \deg G = n.$$

By passing to the isomorphism $j \mapsto j(X/Z, Y/Z)$ and multiplying by Z^n one has

$$Z^r H = AF + BG$$

where $A = Z^{\deg a + r_a} a(X/Z, Y/Z)$ and $B = Z^{\deg b + r_b} b(X/Z, Y/Z)$. By repeated use of Lemma 1.17 one has that

$$H = A'F + B'G$$

for some $A', B' \in k[X, Y, Z]$.

By virtue of Lemma 1.15 let $A' = \sum A_i$ and $B' = \sum B_j$ with A_i and B_j homogeneous of degree i and j, respectively. Set $s = \deg H - \deg F$ and $t = \deg H - \deg G$. It is possible to write

$$\sum_{i \neq s} A_i F + \sum_{j \neq t} B_j G = \sum_{l \neq \deg H} C_l$$

where C_l are homogeneous polynomials of degree l. Since

$$A_s F + B_t G - H + \sum_{l \neq \deg H} C_l = 0$$

where the first part is homogeneous of degree $\deg H$ one has by the uniqueness of Lemma 1.15 that $H = A_s F + B_t G$, completing the proof. □

It is now shown that

$$R_d \cap (f_1, f_2) = W_d \tag{1.7}$$

for all $d \geq n_1 + n_2$. Firstly, if $f \in W_d$, then $f = g_1 f_1 + g_2 f_2$ for some $g_1, g_2 \in R$ with $\deg g_i \leq d - n_i$. In particular $f \in (f_1, f_2)$ and it also follows that

$$\deg f \leq \max_{i \in \{1,2\}} \deg(g_i f_i) = \max_{i \in \{1,2\}} (d - n_i + n_i) = d$$

which means $f \in R_d$. Thus, $f \in R_d \cap (f_1, f_2)$.

Conversely, suppose $f = g_1 f_1 + g_2 f_2$ with $\deg f \leq d$ and $g_1, g_2 \in R$. Letting $F = \xi(f)$ and $F_i = \xi(f_i)$ and applying Lemma 1.18 one has that

$$F = G_1' F_1 + G_2' F_2, \quad \deg G_i' = \deg F - \deg F_i,$$

for some homogeneous polynomials $G_i' \in k[X, Y, Z]$. By applying the homomorphism $J \mapsto J(x, y, 1)$ one gets

$$f = g_1' f_1 + g_2' f_2$$

where $g_i' = G_i'(x, y, 1)$ and consequently

$$\deg g_i' \leq \deg G_i' = \deg F - \deg F_i = \deg f - \deg f_i \leq d - n_i.$$

Finally, $f \in W_d$ which shows (1.7)

Take $d \geq n_1 + n_2$. Let $r = n_1 n_2$. By (1.3) there exist $g_1, \ldots, g_r \in R_d \subseteq R$ that are linearly independent modulo W_d. Suppose that

$$g = \sum_{i=1}^{r} c_i g_i \equiv 0 \pmod{(f_1, f_2)}$$

where $c_i \in k$. This means by definition that $g \in (f_1, f_2)$. Because R_d is a k-vector space one also has $g \in R_d$. Since $R_d \cap (f_1, f_2) = W_d$, it follows that $g \in W_d$, but then

$$\sum_{i=1}^{r} c_i g_i \equiv 0 \pmod{W_d}$$

and $c_1 = \cdots = c_r = 0$ by construction. This shows that $g_1, \ldots, g_r$ are linearly independent as elements of R modulo (f_1, f_2). Hence, $\dim(R/(f_1, f_2)) \geq n_1 n_2$ and (1.4) is indeed an equality. We record this finding as a lemma for referencing later on.

Lemma 1.19. *Suppose that k is algebraically closed. Let C_1 and C_2 be projective curves of degree n_1 and n_2, respectively, with no common component. Assume that the curves do not meet at infinity. If $f_i = 0$ is the affine part of C_i, then* $\dim(R/(f_1, f_2)) = n_1 n_2$.

2 Intersection Multiplicities

With notation as in the previous section, the intersection multiplicity of C_1 and C_2 at $P \in k^2$ shall be defined. From now on let $K = k(x, y)$ be the field of fractions over R. A rational expression $f/g \in K$ is said to be defined at P if $g(P) \neq 0$. Let the local ring of P,

$$\mathcal{O}_P = \{f/g \in K \; ; \; g(P) \neq 0\},$$

be the set of defined fractions at P. Because $k \subseteq \mathcal{O}_P$ one has $\mathcal{O}_P \neq \varnothing$. If $f_1/g_1, f_2/g_2 \in \mathcal{O}_P$ then

$$(g_1 g_2)(P) = g_1(P) g_2(P) \neq 0$$

due to k being a field. Thus

$$\frac{f_1}{g_1} - \frac{f_2}{g_2} = \frac{f_1 g_2 - f_2 g_1}{g_1 g_2} \quad \text{and} \quad \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}$$

are defined at P, showing that $\mathcal{O}_P$ is a subring of K.

Proposition 2.1. *The evaluation*

$$\mathcal{O}_P \ni \phi \mapsto \phi(P) \in k$$

is a surjective homomorphism which induces the identity map on k. With M_P being the kernel of this homomorphism one has $\mathcal{O}_P/M_P \cong k$ and $\mathcal{O}_P = k \oplus M_P$.

Proof. The map is well-defined since the denominator of ϕ is by definition non-zero at P. That evaluation is a homomorphism is trivial. For all constant expressions $a \in k$ one has $a(P) = a$, from which it follows that the map induces the identity map on k. In particular, the homomorphism is surjective. The first isomorphism theorem gives $\mathcal{O}_P/M_P \cong k$. Note that $k \cap M_P = \{0\}$ since all constant expression that are zero at P must be identically zero. If $\phi \in \mathcal{O}_P$, then

$$\phi = \phi(P) + (\phi - \phi(P)) \in k + M_P.$$

Consequently, $\mathcal{O}_P = k \oplus M_P$. □

Proposition 2.2. *$\phi \in \mathcal{O}_P$ has a multiplicative inverse if and only if $\phi \notin M_P$.*

Proof. Suppose $\phi \in \mathcal{O}_P$ has a multiplicative inverse $\psi \in \mathcal{O}_P$. Evaluation yields $\phi(P)\psi(P) = 1$ showing that $\phi(P) \neq 0$, or equivalently that $\phi \notin M_P$. Conversely, suppose $\phi \notin M_P$. Then $\phi = f/g$ for some $f, g \in R$ where $f(P) \neq 0$. It follows by definition of $\mathcal{O}_P$ that $\psi = g/f \in \mathcal{O}_P$, but then $\phi\psi = 1$, so that ϕ has a multiplicative inverse. □

Proposition 2.3. *M_P is the unique maximal ideal in $\mathcal{O}_P$.*

Proof. Let I be an ideal in $\mathcal{O}_P$. If I contains an invertible element, then $I = \mathcal{O}_P$. Otherwise, no element in I is invertible, or in other words $I \subseteq M_P$. □

Define $(f_1, f_2)_P = \mathcal{O}_P f_1 + \mathcal{O}_P f_2$ to be the ideal in $\mathcal{O}_P$ generated by f_1 and f_2. We are now ready to define the intersection multiplicity.

Definition 2.4. With notation as before, the intersection multiplicity of the curves C_1 and C_2 at $P \in k^2$ is defined as

$$I_P(C_1, C_2) = \dim(\mathcal{O}_P/(f_1, f_2)_P).$$

We continue this section by showing a few consequences of the definition. It is clear that $(f_1, f_2)_P = (f_2, f_1)_P$. The next proposition is a consequence of this.

Proposition 2.5. *$I_P(C, D) = I_P(D, C)$ for all curves C and D and points $P \in k^2$.*

Proposition 2.6. *If $P \notin C_1 \cap C_2$, then $I_P(C_1, C_2) = 0$.*

Proof. Suppose that $P \notin C_1 \cap C_2$. Then at least one of $f_1(P) \neq 0$ and $f_2(P) \neq 0$. Without loss of generality, it might be assumed that $f_1(P) \neq 0$. Then $f_1^{-1} \in \mathcal{O}_P$ so that

$$1 = f_1^{-1} f_1 + 0 \cdot f_2 \in (f_1, f_2)_P.$$

It follows that $(f_1, f_2)_P = \mathcal{O}_P$, and consequently that $I_P(C_1, C_2) = 0$. $\square$

Proposition 2.7. *If $P \in C_1 \cap C_2$, then*

$$I_P(C_1, C_2) = 1 + \dim\left(\frac{M_P}{(f_1, f_2)_P}\right).$$

Proof. If $P \in C_1 \cap C_2$, then $f_1(P) = f_2(P) = 0$ so that $(f_1, f_2)_P \subseteq M_P \subseteq \mathcal{O}_P$. Lemma 1.3 gives that

$$\dim\left(\frac{\mathcal{O}_P}{(f_1, f_2)_P}\right) = \dim\left(\frac{\mathcal{O}_P}{M_P}\right) + \dim\left(\frac{M_P}{(f_1, f_2)_P}\right)$$

but since $\mathcal{O}_P/M_P \cong k$ the result follows. $\square$

Note that the dimension of the space $\mathcal{O}_P/(f_1, f_2)_P$ might be infinite, in which case we will consider $I_P(C_1, C_2) = \infty$. This implies that I_P in general has range $\mathbb{N} \cup \{\infty\}$. However, for the curves we are mostly intereseted in, infinite multiplicities need not be considered, which is a result of the next proposition.

Proposition 2.8. *Suppose that C_1 and C_2 are affine curves with no component in common and set $n_i = \deg C_i$. Then $I_P(C_1, C_2) \leq n_1 n_2$ for all $P \in k^2$.*

Proof. It is shown that

$$\dim(\mathcal{O}_P/(f_1, f_2)_P) \leq \dim(R/(f_1, f_2))$$

after which inequality (1.4) completes the proof. Suppose that $\phi_1, \ldots, \phi_r \in \mathcal{O}_P$ are linearly independent modulo $(f_1, f_2)_P$. Take $g_1, \ldots, g_r, h \in R$ with $h(P) \neq 0$ such that $\phi_i = g_i/h$ for $i = 1, \ldots, r$. Because

$$\begin{aligned}
\sum_{i=1}^r c_i g_i \in (f_1, f_2) &\iff \sum_{i=1}^r c_i g_i = h_1 f_1 + h_2 f_2 \text{ for some } h_1, h_2 \in R \\
&\iff \sum_{i=1}^r c_i \frac{g_i}{h} = \frac{h_1}{h} f_1 + \frac{h_2}{h} f_2 \text{ for some } h_1, h_2 \in R \\
&\implies \sum_{i=1}^r c_i \phi_i = \psi_1 f_1 + \psi_2 f_2 \text{ for some } \psi_1, \psi_2 \in \mathcal{O}_P \\
&\iff \sum_{i=1}^r c_i \phi_i \in (f_1, f_2)_P \\
&\implies c_1 = \cdots = c_r = 0
\end{aligned}$$

$g_1, \ldots, g_r$ are linearly independent as elements of R modulo (f_1, f_2), completing the proof. $\square$

The finiteness of the intersection multiplicity implies a characterization of the local ring that will be useful later on in the proof of Bezout's theorem.

Lemma 2.9. *$\mathcal{O}_P = R + (f_1, f_2)_P$ whenever* $\gcd(f_1, f_2) = 1$.

Proof. The assumption together with Proposition 2.8 guarantees the existence of a finite collection $g_1/h, \ldots, g_r/h$, with $g_1, \ldots, g_r, h \in R$ and $h(P) \neq 0$, that span $\mathcal{O}_P$ modulo $(f_1, f_2)_P$. This means that given any $\phi \in \mathcal{O}_P$ there exists $c_1, \ldots, c_r \in k$ and $\psi \in (f_1, f_2)_P$ such that

$$\frac{\phi}{h} = \sum_{i=1}^{r} c_i \frac{g_i}{h} + \psi$$

because $\phi/h \in \mathcal{O}_P$. It follows that

$$\phi = \sum_{i=1}^{r} c_i g_i + h\psi$$

where $\sum_{i=1}^{r} c_i g_i \in R$ and $h\psi \in (f_1, f_2)_P$ due to the latter being an ideal. Since ϕ is arbitrary this shows $\mathcal{O}_P \subseteq R + (f_1, f_2)_P$. The inclusion $\supseteq$ is trivial. □

If $C : f = 0$ and $D : g = 0$ are affine curves, we denote by CD the affine curve whose equation is $fg = 0$. The proof of the next proposition is merely a detailed version of the proof found in Fulton 2008.

Proposition 2.10. *If C is a curve sharing no component with either D or E, then $I_P(C, DE) = I_P(C, D) + I_P(C, E)$ for all $P \in k^2$.*

Proof. Let $C : f = 0$, $D : g = 0$ and $E : h = 0$. It shall be shown that the map

$$\alpha : \mathcal{O}_P/(f, h)_P \ni \phi + (f, h)_P \mapsto g\phi + (f, gh)_P \in \mathcal{O}_P/(f, gh)_P$$

is a well-defined linear injection. To show that it is well-defined, it is sufficient to show that

$$\phi \in (f, h)_P \implies g\phi \in (f, gh)_P,$$

for all $\phi \in \mathcal{O}_P$. This is clear since if $\phi = \psi_1 f + \psi_2 h$ for some $\psi_1, \psi_2 \in \mathcal{O}_P$, then

$$g\phi = \psi_1 gf + \psi_2 gh \in (f, gh)_P.$$

The map is obviously linear. To prove the injectivity, it is sufficient to show

$$g\phi \in (f, gh)_P \implies \phi \in (f, h)_P,$$

for all $\phi \in \mathcal{O}_P$. Thus, suppose that $g\phi \in (f, gh)_P$. Then $g\phi = f\psi_1 + gh\psi_2$ for some $\psi_1, \psi_2 \in \mathcal{O}_P$. Choose an $e \in R$ with $e(P) \neq 0$ such that $\phi e \in R$, $\psi_1 e \in R$ and $\psi_2 e \in R$, and set $a = \phi e$, $b = \psi_1 e$ and $c = \psi_2 e$. It follows that

$$g(a - hc) = fb$$

so the assumption that $\gcd(f, g) = 1$ gives that $a - hc = df$ for some $d \in R$. Finally

$$\phi = \frac{a}{e} = \frac{d}{e} f + \frac{c}{e} h \in (f, h)_P.$$

For α the following identity holds

$$\operatorname{im}\alpha = (f,g)_P/(f,gh)_P,$$

since firstly $g\phi + (f,gh)_P \in \operatorname{im}\alpha$ implies that $g\phi + (f,gh)_P \in (f,g)_P/(f,gh)_P$. Conversely, if $\psi + (f,gh)_P \in (f,g)_P/(f,gh)_P$, then

$$\psi + (f,gh)_P = \psi_1 f + \psi_2 g + (f,gh)_P = \psi_2 g + (f,gh)_P$$

for some $\psi_1, \psi_2 \in \mathcal{O}_P$ and consequently $\psi + (f,gh)_P \in \operatorname{im}\alpha$.

The map

$$\beta : \mathcal{O}_P/(f,gh)_P \ni \phi + (f,gh)_P \mapsto \phi + (f,g)_P \in \mathcal{O}_P/(f,g)_P$$

is a well-defined surjective homomorphism by Lemma 1.1.

Suppose that $\phi + (f,gh)_P \in \ker\beta$. Then $\phi \in (f,g)_P$ and it follows that $\phi + (f,gh)_P \in (f,g)_P/(f,gh)_P$. Conversely, if $\phi + (f,gh)_P \in (f,g)_P/(f,gh)_P$, then $\phi \in (f,g)_P$ so that $\phi \in \ker\beta$ and

$$\ker\beta = (f,g)_P/(f,gh)_P.$$

This shows that $\operatorname{im}\alpha = \ker\beta$.

The rank-nullity theorem gives that

$$\begin{aligned} I_P(C,DE) &= \dim(\mathcal{O}_P/(f,gh)_P) \\ &= \dim\operatorname{im}\beta + \dim\ker\beta \\ &= \dim(\mathcal{O}_P/(f,g)_P) + \dim\operatorname{im}\alpha \\ &= \dim(\mathcal{O}_P/(f,g)_P) + \dim(\mathcal{O}_P/(f,h)_P) \\ &= I_P(C,D) + I_P(C,E). \end{aligned}$$ □

Proposition 2.11. *Let $C : f = 0$ and $D : g = 0$ be affine curves without a common component. If E is an affine curve whose defining polynomial is $af + g$ for some $a \in R$, then $I_P(C,E) = I_P(C,D)$.*

Proof. We show that $(f, af+g)_P = (f,g)_P$, from which the proposition follows. If $\phi \in (f, af+g)_P$, then

$$\phi = \psi_1 f + \psi_2(af+g) = (\psi_1 + a\psi_2)f + \psi_2 g$$

for some $\psi_1, \psi_2 \in \mathcal{O}_P$ so that also $\phi \in (f,g)_P$ and $(f, af+g)_P \subseteq (f,g)_P$. Because there are no restrictions on $a \in R$ the reverse inclusion follows from

$$(f,g)_P = (f, (-a)f + af + g)_P \subseteq (f, af+g)_P.$$ □

Before continuing with the proof of Bezout's theorem, we first show how the definition carries over to the projective plane, and second show that it is invariant under a linear change of variables. This will allow us to make simplifying assumptions in proving Bezout's theorem.

To be able to define the local ring for a point in the projective plane we introduce a counterpart of K. Consider the set

$$\widetilde{K} = \{F/G \in k(X,Y,Z) \; ; \; F \text{ and } G \text{ are homogeneous of the same degree}\}.$$

All elements $\Phi \in \widetilde{K}$ satisfy

$$\Phi(tA, tB, tC) = \frac{F(tA, tB, tC)}{G(tA, tB, tC)} = \frac{t^n F(A, B, C)}{t^n G(A, B, C)} = \frac{F(A, B, C)}{G(A, B, C)} = \Phi(A, B, C)$$

for all $t \neq 0$ and $[A, B, C] \in \mathbb{P}^2_k$, which means all $\Phi \in \widetilde{K}$ are well-defined functions in $\mathbb{P}^2_k$.

We want to define the function

$$\eta : K \ni \frac{f}{g} \mapsto \frac{Z^n f(X/Z, Y/Z)}{Z^n g(X/Z, Y/Z)} \in k(X, Y, Z) \tag{2.1}$$

where $n = \max\{\deg f, \deg g\}$. The next proposition verifies that $\widetilde{K}$ is indeed the projective counterpart of K.

Proposition 2.12. *The map η defined in* (2.1) *is a well-defined isomorphism $K \to \widetilde{K}$.*

Proof. The proof is completed whenever all of the following assertions have been shown:

(i) η is a well-defined function.
(ii) $\eta(K) \subseteq \widetilde{K}$.
(iii) η respects addition.
(iv) η respects multiplication.
(v) η is injective.
(vi) η is surjective.

(i) Firstly $n = \max\{\deg f, \deg g\} \in \mathbb{N}$ because $g \neq 0$ implies $\deg g \geq 0$. Suppose that $f_1/g_1 = f_2/g_2$. Let $n_i = \max\{\deg f_i, \deg g_i\}$. Now

$$\frac{f_1(X/Z, Y/Z)}{g_1(X/Z, Y/Z)} = \frac{f_2(X/Z, Y/Z)}{g_2(X/Z, Y/Z)} \iff \frac{Z^{n_1} f_1(X/Z, Y/Z)}{Z^{n_1} g_1(X/Z, Y/Z)} = \frac{Z^{n_2} f_2(X/Z, Y/Z)}{Z^{n_2} g_2(X/Z, Y/Z)}$$

shows that η is a well-defined function.

(ii) It is clear that $F = Z^n f(X/Z, Y/Z)$ is homogeneous of degree n, and similarly for $G = Z^n g(X/Z, Y/Z)$. Thus, F and G are homogeneous of the same degree so that $F/G \in \widetilde{K}$.

(iii) By Lemma 1.4 one has

$$\begin{aligned}
\eta\left(\frac{f_1}{g_1}\right) + \eta\left(\frac{f_2}{g_2}\right) &= \frac{Z^m f_1(X/Z, Y/Z)}{Z^m g_1(X/Z, Y/Z)} + \frac{Z^n f_2(X/Z, Y/Z)}{Z^n g_2(X/Z, Y/Z)} \\
&= \frac{Z^{m+n}(f_1 g_2 + f_2 g_1)(X/Z, Y/Z)}{Z^{m+n}(g_1 g_2)(X/Z, Y/Z)} \\
&= \frac{Z^l (f_1 g_2 + f_2 g_1)(X/Z, Y/Z)}{Z^l (g_1 g_2)(X/Z, Y/Z)} \\
&= \eta\left(\frac{f_1 g_2 + f_2 g_1}{g_1 g_2}\right) \\
&= \eta\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right).
\end{aligned}$$

for $l = \max\{\deg(f_1 g_2 + f_2 g_1), \deg(g_1 g_2)\} \geq 0$.

(iv) Another use of Lemma 1.4 gives

$$\begin{aligned}
\eta\left(\frac{f_1}{g_1}\right)\eta\left(\frac{f_2}{g_2}\right) &= \frac{Z^m f_1(X/Z,Y/Z)}{Z^m g_1(X/Z,Y/Z)}\cdot\frac{Z^n f_2(X/Z,Y/Z)}{Z^n g_2(X/Z,Y/Z)} \\
&= \frac{Z^{m+n}(f_1f_2)(X/Z,Y/Z)}{Z^{m+n}(g_1g_2)(X/Z,Y/Z)} \\
&= \frac{Z^l(f_1f_2)(X/Z,Y/Z)}{Z^l(g_1g_2)(X/Z,Y/Z)} \\
&= \eta\left(\frac{f_1f_2}{g_1g_2}\right) \\
&= \eta\left(\frac{f_1}{g_1}\cdot\frac{f_2}{g_2}\right),
\end{aligned}$$

for $l = \max\{\deg(f_1f_2), \deg(g_1g_2)\} \geq 0$.

(v) Suppose that $\eta(f_1/g_1) = \eta(f_2/g_2)$. Then by definition

$$\frac{Z^m f_1(X/Z,Y/Z)}{Z^m g_1(X/Z,Y/Z)} = \frac{Z^n f_2(X/Z,Y/Z)}{Z^n g_2(X/Z,Y/Z)}$$

so that after multiplying with the denominators and applying the homomorphism part of Lemma 1.4 one has

$$Z^{m+n}(f_1g_2)(X/Z,Y/Z) = Z^{m+n}(f_2g_1)(X/Z,Y/Z).$$

Canceling Z^{m+n} and applying Lemma 1.5 one finally has

$$f_1g_2 = f_2g_1 \iff \frac{f_1}{g_1} = \frac{f_2}{g_2}$$

completing the proof of the injectivity.

(vi) Take $F/G \in \widetilde{K}$. By definition $F/G \in k(X,Y,Z)$ with F and G homogeneous of the same degree n. Let $f = F(x,y,1)$ and $g = G(x,y,1)$. Then $f,g \in R$,

$$F = Z^n F(X/Z,Y/Z,1) = Z^n f(X/Z,Y/Z),$$

and similarly for G. Finally,

$$\frac{F}{G} = \frac{Z^n f(X/Z,Y/Z)}{Z^n g(X/Z,Y/Z)} = \frac{Z^l f(X/Z,Y/Z)}{Z^l g(X/Z,Y/Z)} = \eta\left(\frac{f}{g}\right)$$

where $l = \max\{\deg f, \deg g\}$ completing the proof. □

If $P \in \mathbb{P}^2_k$ we now define

$$\widetilde{\mathcal{O}}_P = \left\{\frac{F}{G} \in \widetilde{K}\ ;\ G(P) \neq 0\right\}.$$

Firstly, $\mathcal{O}_P$ is a subring of $\widetilde{K}$. This follows from an argument similar to the one before that showed that $\mathcal{O}_P$ is a subring of K.

Proposition 2.13. *$\eta|_{\mathcal{O}_P}$ is an isomorphism $\mathcal{O}_P \cong \widetilde{\mathcal{O}}_P$ for all $P = [a,b,1] \in k^2$.*

Proof. One only needs to show that $\eta(\mathcal{O}_P) = \widetilde{\mathcal{O}}_P$ since all other properties follow from the corresponding properties of η.

Suppose that $f/g \in \mathcal{O}_P$ and let $n = \max\{\deg f, \deg g\}$. Now

$$G = Z^n g(X/Z, Y/Z) \implies G(P) = G(a, b, 1) = g(a, b) \neq 0$$

showing that $\eta(f/g) \in \widetilde{\mathcal{O}}_P$.

Conversely, if $F/G \in \widetilde{\mathcal{O}}_P$, then by letting

$$n = \deg G, \quad f = F(x, y, 1) \quad \text{and} \quad g = G(x, y, 1)$$

one has

$$Z^n g(X/Z, Y/Z) = Z^n G(X/Z, Y/Z, 1) = G$$

and consequently $g(a, b) \neq 0$ by insertion of $(X, Y, Z) = (a, b, 1)$. Now $f/g \in \mathcal{O}_P$ and $\eta(f/g) = F/G$. $\square$

With $P = [a, b, 1]$, take $\Phi = F/G \in \widetilde{\mathcal{O}}_P$ and its preimage $\phi = f/g \in \mathcal{O}_P$. Then

$$\phi(a, b) = \frac{f(a, b)}{g(a, b)} = \frac{F(a, b, 1)}{G(a, b, 1)} = \Phi(a, b, 1)$$

showing that the values of the expressions are preserved upon passing between $\mathcal{O}_P$ and $\widetilde{\mathcal{O}}_P$.

For all $P \in \mathbb{P}^2_k$ define $\widetilde{M}_P = \{\Phi \in \widetilde{\mathcal{O}}_P \ ; \ \Phi(P) = 0\}$.

Proposition 2.14. *$\eta|_{M_P}$ is an isomorphism $M_P \cong \widetilde{M}_P$ for all $P \in k^2$.*

Proof. As before one only needs to show that $\eta(M_P) = \widetilde{M}_P$. For all $\phi \in \mathcal{O}_P$ and $\Phi \in \widetilde{\mathcal{O}}_P$ with $\Phi = \eta(\phi)$ one has

$$\phi \in M_P \iff \phi(P) = 0 \iff \Phi(P) = 0 \iff \Phi \in \widetilde{M}_P.$$

It follows directly that $\eta(M_P) \subseteq \widetilde{M}_P$. Surjectivity of $\eta|_{\mathcal{O}_P}$ implies that regardless of $\Phi \in \widetilde{M}_P$ there is a $\phi \in \mathcal{O}_P$ such that $\eta(\phi) = \Phi$. Thus, one may read the above chain of equivalences from right to left for all $\Phi \in \widetilde{M}_P$ and the proposition follows. $\square$

Proposition 2.15. *Let $\widetilde{R}$ be the set of homogeneous polynomials in $k[X, Y, Z]$. Suppose $F_1, F_2 \in \widetilde{R} \setminus \{0\}$ and let $P \in \mathbb{P}^2_k$. Then $(F_1, F_2)_P$ defined by*

$$(F_1, F_2)_P = \left\{ \frac{F}{G} \in \widetilde{\mathcal{O}}_P \ ; \ F = H_1 F_1 + H_2 F_2 \textit{ for some } H_1, H_2 \in \widetilde{R} \right\}$$

is an ideal in $\widetilde{\mathcal{O}}_P$.

Proof. $0/1 \in (F_1, F_2)_P$ so (F_1, F_2) is non-empty.

Let $F/G, F'/G' \in (F_1, F_2)_P$. If either $F = 0$ or $F' = 0$ it is clear that $F/G - F'/G' \in (F_1, F_2)_P$. Otherwise, one may by definition take $H_i, H_i' \in \widetilde{R}$ such that $F = H_1 F_1 + H_2 F_2$ and $F' = H_1' F_1 + H_2' F_2$. If $H_1 = 0$ or $H_1' = 0$, then clearly $H_1 G' - H_1' G$ is homogeneous. Otherwise

$$\deg H_1 + \deg F_1 = \deg F = \deg G \quad \text{and} \quad \deg H_1' + \deg F_1 = \deg F' = \deg G'$$

and it follows that

$$\begin{aligned}\deg H_1 + \deg G' &= \deg H_1 + \deg H_1' + \deg F_1 \\ &= \deg H_1' + \deg H_1 + \deg F_1 = \deg H_1' + \deg G.\end{aligned}$$

Therefore $H_1G' - H_1'G$ is homogeneous. Similarly it is shown that $H_2G' - H_2'G$ is homogeneous. Now

$$\begin{aligned}\frac{F}{G} - \frac{F'}{G'} &= \frac{(H_1F_1 + H_2F_2)G' - G(H_1'F_1 + H_2'F_2)}{GG'} \\ &= \frac{(H_1G' - H_1'G)F_1 + (H_2G' - H_2'G)F_2}{GG'} \in (F_1, F_2)_P.\end{aligned}$$

Furthermore, if $F/G \in \widetilde{\mathcal{O}}_P$ and $F'/G' \in (F_1, F_2)_P$, then

$$\frac{F}{G} \cdot \frac{F'}{G'} = \frac{F(H_1'F_1 + H_2'F_2)}{GG'} = \frac{FH_1'F_1 + FH_2'F_2}{GG'} \in (F_1, F_2)_P,$$

where FH_1' and FH_2' are clearly homogeneous. This shows that $(F_1, F_2)_P$ is an ideal in $\widetilde{\mathcal{O}}_P$. □

Recall the map ξ, defined in (1.1), that is used to transform affine curves to their projective counterparts. Before presenting the last proposition needed to define intersection multiplicities in the projective plane, a lemma is needed.

For all $F \in \widetilde{R}$ such that $F \neq 0$, let

$$d(F) = \max\{n \in \mathbb{N} \ ; \ Z^n \mid F\}.$$

Lemma 2.16. *For all $F \in \widetilde{R}$ with $F \neq 0$ there exists an $f \in R$ such that $F = Z^{d(F)}\xi(f)$.*

Proof. Because $Z^{d(F)} \mid F$ one has that $F = Z^{d(F)}G$ for some $G \in \widetilde{R}$. By construction $Z \nmid G$. Lemma 1.6 gives $G = \xi(f)$ for some $f \in R$. □

The next proposition is the last piece needed to carry the definition of intersection multiplicity over to the projective plane. However simple the proposition might seem, its proof is quite cumbersome.

Proposition 2.17. *Let $P \in k^2$. If $f_1, f_2 \in R \setminus \{0\}$ and $F_i = \xi(f_i)$, then $\eta|_{(f_1,f_2)_P}$ is an isomorphism $(f_1, f_2)_P \cong (F_1, F_2)_P$.*

Proof. The proof is carried out by showing that $\eta((f_1, f_2)_P) = (F_1, F_2)_P$.

Take

$$\phi = \frac{h_1}{g} \cdot f_1 + \frac{h_2}{g} \cdot f_2 \in (f_1, f_2)_P,$$

with $h_1, h_2, g \in R$. It shall be shown that $\eta(\phi) \in (F_1, F_2)_P$. Let $n_i = \deg f_i$, $m = \deg g$ and $l_i = \deg h_i$. Set $r = \max\{l_1 + n_1, l_2 + n_2, m\}$. If both $h_i = 0$, then clearly $\eta(\phi) = 0 \in (F_1, F_2)_P$ since $(F_1, F_2)_P$ is an ideal. Note that

$$h_i \neq 0 \implies H_i = Z^{r-n_i} h_i(X/Z, Y/Z) = Z^{r-l_i-n_i} Z^{l_i} h_i(X/Z, Y/Z) \in \widetilde{R}.$$

If exactly one of $h_1 \neq 0$ and $h_2 \neq 0$ one may without loss of generality assume that $h_1 \neq 0$ and $h_2 = 0$. Then

$$\begin{aligned}\eta(\phi) &= \frac{Z^r(h_1f_1)(X/Z,Y/Z)}{Z^rg(X/Z,Y/Z)} \\ &= \frac{Z^{r-n_1}h_1(X/Z,Y/Z)Z^{n_1}f_1(X/Z,Y/Z)}{Z^rg(X/Z,Y/Z)} \\ &= \frac{H_1F_1 + 0F_2}{G} \in (F_1,F_2)_P\end{aligned}$$

where $G = Z^rg(X/Z,Y/Z)$. Similarly, if $h_1 \neq 0$ and $h_2 \neq 0$, one has

$$\begin{aligned}\eta(\phi) &= \frac{Z^q(h_1f_1 + h_2f_2)(X/Z,Y/Z)}{Z^qg(X/Z,Y/Z)} \\ &= \frac{Z^r(h_1f_1 + h_2f_2)(X/Z,Y/Z)}{Z^rg(X/Z,Y/Z)} \\ &= \frac{H_1F_1 + H_2F_2}{G} \in (F_1,F_2)_P\end{aligned}$$

where H_i and G are as before and

$$q = \max\{\deg(h_1f_1 + h_2f_2), \deg g\} \leq r.$$

In any case $\eta(\phi) \in (F_1,F_2)_P$.

Conversely, let $F/G \in (F_1,F_2)_P$. By definition $F = H_1F_1 + H_2F_2$ for some $H_1, H_2 \in \widetilde{R}$. If it can be shown that there exist $\phi_1, \phi_2 \in (f_1,f_2)_P$ such that $\eta(\phi_i) = H_iF_i/G$, then it follows that

$$\frac{H_1F_1 + H_2F_2}{G} = \frac{H_1F_1}{G} + \frac{H_2F_2}{G} = \eta(\phi_1) + \eta(\phi_2) = \eta(\phi_1 + \phi_2)$$

since η is an isomorphism $\mathcal{O}_P \to \widetilde{\mathcal{O}}_P$. Because $(f_1,f_2)_P$ is an ideal it follows that $\phi_1 + \phi_2 \in (f_1,f_2)_P$ so that $F/G \in \eta((f_1,f_2)_P)$. Therefore one only needs to find a $\phi_1 \in (f_1,f_2)_P$ such that $\eta(\phi_1) = H_1F_1/G$, to show that $F/G \in \eta((f_1,f_2)_P)$, since finding ϕ_2 is similar.

For $H_1 = 0$ it is clear that $\phi_1 = 0$ suffices. Thus, assume $H_1 \neq 0$. Then $H_1 = Z^{d(H_1)}\xi(h_1)$ and $G = Z^{d(G)}\xi(g)$ for some $h_1, g \in R$, so

$$\frac{H_1F_1}{G} = \frac{Z^{d(H_1)}\xi(h_1)\xi(f_1)}{Z^{d(G)}\xi(g)} = \frac{Z^{d(H_1)}\xi(h_1f_1)}{Z^{d(G)}\xi(g)} = \frac{Z^a\xi(h_1f_1)}{Z^b\xi(g)}$$

where $a = 0$ or $b = 0$. By definition of $\widetilde{\mathcal{O}}_P$ it holds that

$$a + \deg(h_1f_1) = a + \deg\xi(h_1f_1) = b + \deg\xi(g) = b + \deg g.$$

If $a = 0$, then $\max\{\deg(h_1f_1), \deg g\} = \deg(h_1f_1)$ so that

$$\begin{aligned}\eta\left(\frac{h_1f_1}{g}\right) &= \frac{Z^{\deg(h_1f_1)}(h_1f_1)(X/Z,Y/Z)}{Z^{\deg(h_1f_1)}g(X/Z,Y/Z)} \\ &= \frac{Z^{\deg(h_1f_1)}(h_1f_1)(X/Z,Y/Z)}{Z^bZ^{\deg g}g(X/Z,Y/Z)} \\ &= \frac{\xi(h_1f_1)}{Z^b\xi(g)} \\ &= \frac{H_1F_1}{G}.\end{aligned}$$

If $b = 0$, then $\max\{\deg(h_1 f_1), \deg g\} = \deg g$, and it follows that

$$\begin{aligned}
\eta\left(\frac{h_1 f_1}{g}\right) &= \frac{Z^{\deg g}(h_1 f_1)(X/Z, Y/Z)}{Z^{\deg g} g(X/Z, Y/Z)} \\
&= \frac{Z^a Z^{\deg(h_1 f_1)}(h_1 f_1)(X/Z, Y/Z)}{Z^{\deg g} g(X/Z, Y/Z)} \\
&= \frac{Z^a \xi(h_1 f_1)}{\xi(g)} \\
&= \frac{H_1 F_1}{G}.
\end{aligned}$$

Anyhow $\eta(\phi_1) = H_1 F_1/G$, where $\phi_1 = h_1 f_1/g \in (f_1, f_2)_P$ and the proof is complete. □

By the propositions one has

$$\dim(\mathcal{O}_P/(f_1, f_2)_P) = \dim(\widetilde{\mathcal{O}}_P/(F_1, F_2)_P), \quad P \in k^2,$$

showing that one may extend the definition of intersection multiplicity from the affine plane to the projective plane using the following definition. Due to the propositions shown we will dispense with the tildes and transport the relevant structure from k^2 to $\mathbb{P}_k^2$.

Definition 2.18. The intersection multiplicity at the point $P \in \mathbb{P}_k^2$ of the projective curves C_1 and C_2, whose equations are $F_1 = 0$ and $F_2 = 0$, respectively, is defined as

$$I_P(C_1, C_2) = \dim(\mathcal{O}_P/(F_1, F_2)_P).$$

Recall the induced linear transformation defined in (1.6), and call it φ. We now show that the intersection multiplicity is invariant under φ. This will allow us to apply a suitable linear transformation of the projective plane to simplify the proof of Bezout's theorem.

Note that $G(P) \neq 0$ if and only if $G(M^{-1}MP) \neq 0$, that is $\varphi(G)(MP) \neq 0$. This means that $\varphi(\mathcal{O}_P) \subseteq \mathcal{O}_{MP}$, since φ also preserves the degrees of polynomials as is easily seen. By considering the inverse transformation φ^{-1} one has similarly that $\varphi^{-1}(\mathcal{O}_{MP}) \subseteq \mathcal{O}_P$. Thus, $\varphi|_{\mathcal{O}_P}$ is an isomorphism $\mathcal{O}_P \cong \mathcal{O}_{MP}$.

To finally show that the definition of intersection multiplicity is invariant under linear changes of variables, it must be shown that the transformation of $(F_1, F_2)_P$ to $(F_1', F_2')_{MP}$, where F_i' is the image of F_i under φ, is an isomorphism. Suppose that $\Phi \in (F_1, F_2)_P$. Then $\Phi = F/G$ with F and G homogeneous of the same degree and $F = H_1 F_1 + H_2 F_2$ for some homogeneous H_1 and H_2. Because φ preserves the degrees of polynomials

$$\varphi(F) = \varphi(H_1)F_1' + \varphi(H_2)F_2'$$

is homogeneous with $\varphi(H_i)$ homogeneous. Thus,

$$\varphi(\Phi) = \frac{\varphi(F)}{\varphi(G)} \in (F_1', F_2')_{MP},$$

showing that $\varphi((F_1, F_2)_P) \subseteq (F_1', F_2')_{MP}$. The reverse inclusion follows by replacing φ with its inverse. This shows that $\varphi|_{(F_1,F_2)_P}$ is an isomorphism $(F_1, F_2)_P \cong (F_1', F_2')_{MP}$.

3 Bezout's Theorem

Throughout this section we let k be an algebraically closed field and let the curves C_1 and C_2 have affine parts $f_1 = 0$ and $f_2 = 0$, respectively, with $\gcd(f_1, f_2) = 1$. After the endeavor of the previous section, we are finally ready to show Bezout's theorem.

Theorem 3.1 (Bezout's Theorem)**.** *If the projective curves C_1 and C_2, of degrees n_1 and n_2 respectively, have no common component, then C_1 and C_2 intersect at exactly $n_1 n_2$ points of $\mathbb{P}^2_k$ counting multiplicity, i.e.*

$$\sum_{P \in C_1 \cap C_2} I_P(C_1, C_2) = n_1 n_2.$$

In the rest of this section, let for notional purposes $\mathcal{P} = C_1 \cap C_2 \cap k^2$.

Lemma 3.2. *If $P \in \mathcal{P}$ and $r \geq I_P(C_1, C_2)$, then $\prod_{i=1}^r t_i \in (f_1, f_2)_P$ for all $t_1, \ldots, t_r \in M_P$.*

Proof. Define the ideals $J_1, \ldots, J_{r+1}$ in $\mathcal{O}_P$ by

$$J_q = \left(\prod_{i=1}^q t_i \right) \mathcal{O}_P + (f_1, f_2)_P \quad \text{and} \quad J_{r+1} = (f_1, f_2)_P$$

where $1 \leq q \leq r$. If $\psi \in J_{r+1}$, then because $0 \in \mathcal{O}_P$ one has

$$\psi = \left(\prod_{i=1}^r t_i \right) \cdot 0 + \psi \in J_r.$$

If $\gamma \in J_{q+1}$ for some $1 \leq q < r$, then $\gamma = \prod_{i=1}^{q+1} t_i \phi + \psi$ for some $\phi \in \mathcal{O}_P$ and $\psi \in (f_1, f_2)_P$, but because $\mathcal{O}_P$ is a ring one has $t_{q+1}\phi \in \mathcal{O}_P$ and

$$\gamma = \prod_{i=1}^q t_i (t_{q+1}\phi) + \psi \in J_q.$$

Hence,

$$(f_1, f_2)_P = J_{r+1} \subseteq J_r \subseteq J_{r-1} \subseteq \cdots \subseteq J_1 \subseteq M_P.$$

Firstly Lemma 1.3 gives that

$$\dim \left(\frac{M_P}{J_{q+1}} \right) = \dim \left(\frac{M_P}{J_q} \right) + \dim \left(\frac{J_q}{J_{q+1}} \right) \tag{3.1}$$

for all $1 \leq q \leq r$. Assume that

$$\dim \left(\frac{M_P}{J_{q+1}} \right) = \dim \left(\frac{M_P}{J_1} \right) + \sum_{i=1}^q \dim \left(\frac{J_i}{J_{i+1}} \right). \tag{3.2}$$

Note that (3.2) is true for $q = 1$ by (3.1). Together (3.1) and (3.2) give

$$\dim \left(\frac{M_P}{J_{q+2}} \right) = \dim \left(\frac{M_P}{J_{q+1}} \right) + \dim \left(\frac{J_{q+1}}{J_{q+2}} \right) = \dim \left(\frac{M_P}{J_1} \right) + \sum_{i=1}^{q+1} \dim \left(\frac{J_i}{J_{i+1}} \right)$$

so that one by induction has that (3.2) is true for $q = r$. Thus, by Proposition 2.7 one has

$$r \geq 1 + \dim\left(\frac{M_P}{(f_1, f_2)_P}\right) \geq 1 + \sum_{i=1}^{r} \dim\left(\frac{J_i}{J_{i+1}}\right).$$

Because all $r + 1$ terms in the right hand sides are natural numbers and their sum is at most r, one term is zero. Therefore $J_q = J_{q+1}$ for some $1 \leq q \leq r$. If $q = r$ then

$$\prod_{i=1}^{r} t_i = \prod_{i=1}^{r} t_i \cdot 1 + 0 \in \left(\prod_{i=1}^{r} t_i\right) \mathcal{O}_P + (f_1, f_2)_P = (f_1, f_2)_P,$$

as desired. Otherwise

$$\prod_{i=1}^{q} t_i = \prod_{i=1}^{q} t_i \cdot 1 + 0 \in \left(\prod_{i=1}^{q} t_i\right) \mathcal{O}_P + (f_1, f_2)_P = \left(\prod_{i=1}^{q+1} t_i\right) \mathcal{O}_P + (f_1, f_2)_P$$

so that

$$\prod_{i=1}^{q} t_i = \left(\prod_{i=1}^{q+1} t_i\right) \phi + \psi$$

for some $\phi \in \mathcal{O}_P$ and $\psi \in (f_1, f_2)_P$. It follows that

$$\left(\prod_{i=1}^{q} t_i\right) (1 - t_{q+1}\phi) = \psi \in (f_1, f_2)_P,$$

but because $t_{q+1} \in M_P$ implies

$$(1 - t_{q+1}\phi)(P) = 1 - t_{q+1}(P)\phi(P) = 1 - 0 \cdot \phi(P) = 1$$

one has $(1 - t_{q+1}\phi)^{-1} \in \mathcal{O}_P$. Since $(f_1, f_2)_P$ is an ideal in $\mathcal{O}_P$ one has that $\prod_{i=1}^{q} t_i \in (f_1, f_2)_P$, and finally $\prod_{i=1}^{r} t_i \in (f_1, f_2)_P$. □

Lemma 3.3. *Let $P \in \mathcal{P}$ and $\phi \in \mathcal{O}_P$. Then there exists a $g \in R$ such that*

$$g \equiv \phi \pmod{(f_1, f_2)_P} \quad \textit{and} \quad g \equiv 0 \pmod{(f_1, f_2)_Q}$$

for all $Q \in \mathcal{P}$ such that $Q \neq P$.

Proof. Define $\mathcal{Q} = \{Q \in \mathcal{P} \ ; \ Q \neq P\}$. By Lemma 1.12 the sets $\mathcal{P}$ and $\mathcal{Q}$ are finite. By Lemma 1.7 there is a polynomial $h \in R$ such that $h(P) = 1$ and $h(Q) = 0$ for all $Q \in \mathcal{Q}$. This means that $h^{-1} \in \mathcal{O}_P$ and $h \in M_Q$ for $Q \in \mathcal{Q}$. Let

$$r = \max_{Q \in \mathcal{Q}} I_Q(C_1, C_2).$$

By Lemma 3.2 $h^r \in (f_1, f_2)_Q$. Trivially, $h^{-r} \in \mathcal{O}_P$. Since $\phi h^{-r} \in \mathcal{O}_P$ and $\mathcal{O}_P = R + (f_1, f_2)_P$, by Lemma 2.9, there is an $f \in R$ and a $\psi \in (f_1, f_2)_P$ such that $\phi h^{-r} = f + \psi$, but then $f \equiv \phi h^{-r} \pmod{(f_1, f_2)_P}$. Set $g = fh^r$. Then

$$g \equiv \phi h^{-r} h^r = \phi \pmod{(f_1, f_2)_P} \quad \text{and} \quad g \equiv 0 \pmod{(f_1, f_2)_Q},$$

for all $Q \in \mathcal{Q}$. □

Lemma 3.4. *Let M be an ideal in R such that $(f_1, f_2) \subseteq M \subseteq R$ and $1 \notin M$. Suppose that p is a polynomial in R. Then there exists an $s \in k$ such that*

$$1 \notin M + R(p - s).$$

Proof. By Lemma 1.3, $m = \dim(R/M)$ is finite. Thus, $1, p, p^2, \ldots, p^m$ are linearly dependent modulo M, so there exist $b_0, \ldots, b_m \in k$, not all zero, such that

$$\sum_{i=0}^{m} b_i p^i \in M.$$

By setting $n = \max\{i \in \{1, \ldots, m\} \ ; \ b_i \neq 0\}$ and $c_i = b_i/b_n$ for $0 \leq i \leq n$ one has

$$p^n + c_{n-1}p^{n-1} + \cdots + c_1 p + c_0 = \sum_{i=0}^{n} c_i p^i = \frac{1}{b_n} \sum_{i=0}^{n} b_i p^i = \frac{1}{b_n} \sum_{i=0}^{m} b_i p^i \in M.$$

Because k is algebraically closed there exist $s_1, \ldots, s_n \in k$ such that

$$\prod_{i=1}^{n} (p - s_i) = \sum_{i=0}^{n} c_i p^i \in M. \tag{3.3}$$

Suppose toward a contradiction that $1 \in M + R(p - s_i)$ for all i. For each i, take $h_i \in M$ and $g_i \in R$ such that $1 = h_i + g_i(p - s_i)$. It now follows that

$$1 = \prod_{i=1}^{n} (h_i + g_i(p - s_i)) \in M$$

because upon expansion of the product, all terms are on the form

$$h_{i_1} \cdots h_{i_r} g_{i_{r+1}} (p - s_{i_{r+1}}) \cdots g_{i_n} (p - s_{i_n}).$$

More precisely, any term that includes an h_i belongs to M due to the latter being an ideal and the term $g_1 \cdots g_n (p - s_1) \cdots (p - s_n)$ belongs to the ideal by (3.3). This is a contradiction, so $1 \notin M + R(p - s_i)$ for some i. $\square$

Lemma 3.5. $R/(f_1, f_2) \cong \prod_{P \in \mathcal{P}} (\mathcal{O}_P/(f_1, f_2)_P)$.

Proof. Consider the homomorphism

$$\alpha : R \ni f \mapsto (f \bmod (f_1, f_2)_P)_{P \in \mathcal{P}} \in \prod_{P \in \mathcal{P}} \frac{\mathcal{O}_P}{(f_1, f_2)_P}.$$

Any element in the codomain of α can be written as $(\phi_P \bmod (f_1, f_2)_P)_{P \in \mathcal{P}}$ with $(\phi_P)_{P \in \mathcal{P}} \in \prod_{P \in \mathcal{P}} \mathcal{O}_P$. To show that α is surjective, take any such $(\phi_P)_{P \in \mathcal{P}}$. For each $P \in \mathcal{P}$ there is by Lemma 3.3 a $g_P \in R$ such that

$$g_P \equiv \phi_P \pmod{(f_1, f_2)_P} \quad \text{and} \quad g_P \equiv 0 \pmod{(f_1, f_2)_Q}$$

for all $Q \in \mathcal{P}$ with $Q \neq P$. Now let $f = \sum_{Q \in \mathcal{P}} g_Q$. For any $P \in \mathcal{P}$ one now has

$$f = \sum_{Q \in \mathcal{P}} g_Q \equiv g_P \equiv \phi_P \pmod{(f_1, f_2)_P}$$

As a consequence of this, α is surjective. Let $J = \ker \alpha$. The first isomorphism theorem gives $R/J \cong \prod_{P \in \mathcal{P}}(\mathcal{O}_P/(f_1, f_2)_P)$. The proof is completed by showing that $J = (f_1, f_2)$.

Because $(f_1, f_2) \subseteq (f_1, f_2)_P$ for all $P \in \mathcal{P}$, one has $(f_1, f_2) \subseteq J$. To show the reverse inclusion, let f be an arbitrary polynomial in J and set

$$L = \{g \in R \; ; \; gf \in (f_1, f_2)\}.$$

Whenever it has been shown that $1 \in L$, the proof is complete.

First it is shown that L is an ideal in R satisfying $(f_1, f_2) \subseteq L \subseteq R$. The inclusions being obvious, only the first part is shown. Because of the inclusion L is non-empty. If $g_1, g_2 \in L$, then $g_1 f, g_2 f \in (f_1, f_2)$ so that

$$(g_1 - g_2)f = g_1 f - g_2 f \in (f_1, f_2)$$

because the latter is a ring. Thus, $g_1 - g_2 \in L$. If $h \in R$ and $g \in L$, then, since (f_1, f_2) is an ideal in R, one has

$$(hg)f = h(gf) \in (f_1, f_2)$$

showing that $hg \in L$. Hence, L is an ideal in R.

Secondly, it is shown that for all $P \in k^2$ there is a polynomial $g \in L$ such that $g(P) \neq 0$. By definition $f \in J$ means that

$$f \equiv 0 \pmod{(f_1, f_2)_P} \quad \text{for all} \quad P \in \mathcal{P}.$$

If $P \in \mathcal{P}$ this means that there exist polynomials $g_1, g_2, h \in R$ such that

$$f = \frac{g_1}{h} f_1 + \frac{g_2}{h} f_2 \iff hf = g_1 f_1 + g_2 f_2 \implies hf \in (f_1, f_2)$$

and $h(P) \neq 0$. Otherwise, if $P \notin \mathcal{P}$, then $f_1(P) \neq 0$ or $f_2(P) \neq 0$. Without loss of generality assume that the first holds. Then one has $f_1 f \in (f_1, f_2)$. This completes the proof of the second property.

Using these two properties of L it shall be shown that $1 \in L$. Assume toward a contradiction that $1 \notin L$. By applying Lemma 3.4 on $M = L$ and $p = x$ one gets the existence of an $a \in k$ such that $1 \notin L + R(x - a)$. Applying the lemma again, but this time with $M = L + R(x-a)$ and $p = y$ one can find a $b \in k$ such that $1 \notin L + R(x - a) + R(y - b)$. Let $g \in L$ be arbitrary. Since the polynomial $y - b$ is monic, divison of g as a polynomial in y over $k[x]$ is admissible with

$$g = g_2(y - b) + r$$

for some $g_2 \in k[x, y]$ and $r \in k[x]$. Dividing r by $x - a$ in $k[x]$ gives

$$r = g_1(x - a) + c$$

for some $c \in k$. Thus,

$$g = g_1(x - a) + g_2(y - b) + c.$$

If $c \neq 0$, then

$$1 = \frac{1}{c} \cdot c = \frac{1}{c}\left(g - g_1(x - a) - g_2(y - b)\right),$$

but the latter clearly belongs to $L+R(x-a)+R(y-b)$, which is a contradiction. Therefore $c=0$ and one gets

$$g(a,b)=g_1(a,b)(a-a)+g_2(a,b)(b-b)=0,$$

but since $g\in L$ is arbitrary this contradicts that there exists a $g\in L$ such that $g(a,b)\neq 0$. Hence, the assumption that $1\notin L$ is false, completing the proof. $\square$

Finally, the proof of Bezout's theorem is merely putting the pieces together.

Proof of Bezout's Theorem. As in the proof of Theorem 1.10 we can find a line L that does not meet $C_1\cap C_2$ and that is a component of neither C_1 nor C_2. Because the intersection multiplicities do not change with a linear change of coordinates, we may apply a linear transformation that maps L to the line at infinity. Therefore we assume that C_1 and C_2 do not meet at infinity and that the line at infinity is not a component of either curve. This assumption gives that $\mathcal{P}=C_1\cap C_2$. Lemma 3.5 and Lemma 1.19 give

$$\sum_{P\in C_1\cap C_2} I_P(C_1,C_2)=\dim\left(\prod_{P\in C_1\cap C_2}(\mathcal{O}_P/(f_1,f_2)_P)\right)=\dim\frac{R}{(f_1,f_2)}=n_1n_2,$$

completing the proof. $\square$

4 Simple Points

Before stating and proving Max Noether's theorem and its consequences we introduce simple points in this separate section.

Definition 4.1. A point P on an affine curve $C:f=0$ is said to be simple if ∇f does not vanish at P.

In other words, a point (a,b) on an affine curve is simple if $f_1'(a,b)\neq 0$ or $f_2'(a,b)\neq 0$, where f_1' and f_2' are the partial derivatives of f. Because we will have reason to consider simple points on the line at infinity, we need a projective definition as well. Note that if $F\in k[X,Y,Z]$ is homogeneous of order n, then the partial derivatives F_i', $i=1,2,3$, are homogeneous of order $n-1$. This is what makes the projective definition good.

Definition 4.2. A point P on a projective curve $C:F=0$ is said to be simple if $\nabla F(P)\neq 0$. If this is the case the tangent of C at P is defined as the line

$$F_1'(P)X+F_2'(P)Y+F_3'(P)Z=0,$$

the definition being independent of the representative for P.

Note that by Euler's theorem (Fulton 2008, p. 3) the tangent intersects C at P. As usual we must verify the following properties prior to making simplifying assumptions:

(i) If (a,b) is a simple point on the affine curve $f=0$, then $[a,b,1]$ is a simple point on the projective curve $F=0$, where F is the homogenization of f.

(ii) If F is the homogenization of f and $[a,b,1]$ is a simple point on $F=0$, then (a,b) is a simple point on $f=0$.

(iii) Linear coordinate changes map simple points to simple points.

We now show these assertions.

(i) Suppose that (a,b) is a simple point on $f=0$. Then $f_i'(a,b)\neq 0$ for some $i\in\{1,2\}$. Let $F=Z^n f(X/Z,Y/Z)$, where $n=\deg f$, be the homogenization of f. Then

$$F_i' = Z^n f_i'(X/Z,Y/Z)\cdot\frac{1}{Z} = Z^{n-1} f_i'(X/Z,Y/Z),$$

so that $F_i'(a,b,1)=f_i'(a,b)$ showing that $[a,b,1]$ is a simple point on $F=0$.

(ii) Let $[a,b,1]$ be a simple point on $F=0$ where $F=Z^n f(X/Z,Y/Z)$ for some $f\in k[x,y]$ with $\deg f=n$. Then $F_i'(a,b,1)=f_i'(a,b)$ for $i\in\{1,2\}$ as above, and a computation shows that

$$F_3' = nZ^{n-1}f(X/Z,Y/Z) - Z^{n-2}(Xf_1'(X/Z,Y/Z)+Yf_2'(X/Z,Y/Z)),$$

so insertion gives

$$F_3'(a,b,1) = -af_1'(a,b) - bf_2'(a,b)$$

since $f(a,b)=0$. If both $f_1'(a,b)=0$ and $f_2'(a,b)=0$, then $F_i'(a,b,1)=0$ for all $i\in\{1,2,3\}$, contradicting the assumption, so (a,b) must be a simple point.

(iii) Suppose that P is a simple point on $F=0$ and suppose that points of $\mathbb{P}_k^2$ are transformed with $P\mapsto MP$ where M is an invertible 3×3 matrix. Then polynomials are mapped with the map given in (1.5) on page 11, which we will here denote by $F\mapsto F\circ M^{-1}$. It is easy to verify that

$$\nabla(F\circ M^{-1}) = \left(M^{-1}\right)^t(\nabla F)\circ M^{-1}$$

from which it follows that

$$\nabla(F\circ M^{-1})(MP) = \left(M^{-1}\right)^t\cdot\nabla F(P)\neq 0$$

by the assumption on P and the fact that $\left(M^{-1}\right)^t$ is invertible.

It is clear that given two distinct points there is a unique line passing through them. If we dispense with the assumption that the points are distinct, we arrive at the following proposition.

Proposition 4.3. *Assume that k is an infinite field. Suppose that P is a simple point on C. The tangent of C at P is the unique line L such that $I_P(C,L)\geq 2$.*

Proof. We first show that we without loss of generality can work in the affine plane with P being the origin and $x=0$ being the tangent. We start in the U,V,W projective plane. Let $C: F=0$, $P=[U_0,V_0,W_0]$ and $m_{1i}=F_i'(P)$. Set $\mathbf{m}_1=(m_{11},m_{12},m_{13})$. Let K be the kernel of the map

$$(a,b,c)\mapsto aU_0+bV_0+cW_0.$$

Since $\dim K=2$ and $\mathbf{m}_1\in K$ there is a vector $\mathbf{m}_2\in K$ such that $\mathbf{m}_1$ and $\mathbf{m}_2$ are linearly independent. Since C has only finitely many linear components it is possible to choose a vector (a,b,c) from k^3 that does not lie in K, such that $aU+bV+cW$ is not a component of C. Set $\mathbf{m}_3=(a,b,c)/(aU_0+bV_0+cW_0)$.

Take M to be the 3×3 matrix whose rows are $\mathbf{m}_1$, $\mathbf{m}_2$ and $\mathbf{m}_3$. By applying the projective transformation

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = M \begin{bmatrix} U \\ V \\ W \end{bmatrix}$$

we see that P maps to the origin and the tangent line $m_{11}U + m_{12}V + m_{13}W = 0$ is mapped to $X = 0$. Furthermore, the line at infinity is by construction not a component of the transformed curve, so we may consider C an affine curve and work in the affine plane.

We first show that the tangent line actually satisfies the given requirements. Note that $M = Rx + Ry$ is the ideal in R consisting of all curves intersecting the origin, and $M_P = \mathcal{O}_P x + \mathcal{O}_P y$. We have $f \in M$, where $C : f = 0$. The construction implies that

$$f = x + g$$

where $g = \sum_{2 \leq i+j \leq n} c_{ij} x^i y^j$ are the higher terms. (To simplify notation we here take the liberty to identify the curves with their defining polynomials.) By Proposition 2.11, $I_P(x, f) = I_P(x, g)$. The same proposition can be applied as long as there is a term in g with a factor x to finally get $I_P(x, f) = I_P(x, g(0, y))$. If $g(0, y) = 0$ the intersection multiplicity is infinite and we are done. Otherwise let $m \geq 2$ be the largest integer such that $g(0, y) = y^m h$ for some h. By construction $h(0) \neq 0$ so Propositions 2.6 and 2.10 give $I_P(x, h) = 0$, and

$$I_P(x, f) = I_P(x, y^m h) = I_P(x, y^m) + I_P(x, h) = I_P(x, y^m).$$

After m further applications of Proposition 2.10 one has

$$I_P(x, f) = m I_P(x, y).$$

By Proposition 2.7 one finally has $I_P(x, f) = m \geq 2$.

Lastly, to show the uniqueness suppose $L : ax + by + c = 0$ is any line such that $I_P(L, C) \geq 2$ where $C : f = x + g$. Firstly, $c = 0$ by Proposition 2.6. Suppose toward a contradiction that $b \neq 0$. Then we can make the linear change of variables

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a & b \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

and let $\widetilde{L} : v = 0$ and $\widetilde{C} : \widetilde{f} = u + \widetilde{g} = 0$, where $\widetilde{g}$ are the higher terms, be the images of L and C, respectively. Write $\widetilde{g} = v\widetilde{h} + u^2 \widetilde{r}$ where $\widetilde{h} \in k[u, v]$ and $\widetilde{r} \in k[u]$. A computation using the same propositions as before shows that

$$\begin{aligned} I_P(v, \widetilde{f}) &= I_P(v, u + v\widetilde{h} + u^2 \widetilde{r}) \\ &= I_P(v, u(1 + u\widetilde{r})) \\ &= I_P(v, u) + I_P(v, 1 + u\widetilde{r}) \\ &= I_P(v, u) \\ &= 1 < 2 \end{aligned}$$

contrary to the assumption. Thus, $b = 0$ and the line is $L : x = 0$ as desired. □

A curve is said to be non-singular if all its points are simple.

Proposition 4.4. *A non-singular curve over an algebraically closed field is irreducible.*

Proof. Let C be a non-singular curve and suppose that it is reducible. Then $C = DE$ for some curves D and E. Let $C : F = 0$, $D : G = 0$ and $E : H = 0$. Differentiation yields

$$F_i' = GH_i' + G_i'H.$$

D and E intersect at some point P. If they do not have a component in common Bezout's theorem guarantees this, and else it is obvious. Inserting this point in the above identity gives $F_i'(P) = 0$, so that P is not a simple point on C, contrary to the assumption, whence C must be irreducible. $\square$

The example $x^2 - y^3 = 0$ shows that there are irreducible singular curves.

5 Max Noether's Fundamental Theorem

In this and all subsequent sections, we let k be an algebraically closed field.

Max Noether's fundamental theorem is a key part in the proof of Chasles theorem. Luckily, with the work that has been done in the proof of Bezout's theorem, the proof becomes very slick. There is a shorter formulation of the theorem that does not require the assumption that the curves C and D do not meet at infinity, but to use such a formulation one would need to replace the homomorphism $J \mapsto J(x, y, 1)$ with something that works on the line at infinity. Because the extra generality will not be necessary in this text, the assumption is kept.

Theorem 5.1 (Max Noether's Fundamental Theorem)**.** *Let $C : F = 0$ and $D : G = 0$ be projective curves with no common component. Assume that C and D do not meet at infinity. Suppose that H is a homogeneous polynomials in $k[X, Y, Z]$. Let $f = F(x, y, 1)$, $g = G(x, y, 1)$ and $h = H(x, y, 1)$. If $h \in (f, g)_P$ for all $P \in C \cap D$, then $H = AF + BG$ for some homogeneous polynomials $A, B \in k[X, Y, Z]$ with $\deg A = \deg H - \deg F$ and $\deg B = \deg H - \deg G$.*

Proof. Lemma 3.5 gives that $h \in (f, g)$ so that $h = af + bg$ for some $a, b \in R$. The result follows by an application of Lemma 1.18. $\square$

To use Max Noether's theorem we will utilize the following proposition, the proof of which requires more theory than is given in this text, so we refer the reader to Proposition 1 of §5.5 in Fulton 2008. The proposition given here is not as general as the cited one, but the extra generality will not be needed here.

Proposition 5.2. *Let $C : f = 0$, $D : g = 0$ and $E : h = 0$ be affine curves. If P is a simple point on C and $I_P(C, E) \geq I_P(C, D)$ then $h \in (f, g)_P$.*

It is easily seen that

$$\mathcal{G} = \left\{ (n_P)_{P \in \mathbb{P}_k^2} \in \prod_{P \in \mathbb{P}_k^2} \mathbb{Z} \; ; \; n_P \neq 0 \text{ for at most a finite number of } P \in \mathbb{P}_k^2 \right\}$$

form an additive group under element-wise addition. We denote an element $(n_P)_{P \in \mathbb{P}_k^2} \in \mathcal{G}$ with the formal sum $\sum_{P \in \mathbb{P}_k^2} n_P P$. Usually the index is clear from context, and will be dispensed with. If $m_P \geq n_P$ for all $P \in \mathbb{P}^2_k$ we write $\sum m_P P \geq \sum n_P P$.

Given two curves C and D that have no component in common we define their intersection cycle to be

$$C \cdot D = \sum I_P(C, D)P.$$

Given curves C, D and E such that C and DE do not intersect at infinity, Proposition 2.10 translates to

$$C \cdot DE = C \cdot D + C \cdot E.$$

By performing a suitable linear change of coordinates one sees that the identity holds even if C and DE do meet at infinity.

Similarly Proposition 2.11 translates to

$$C \cdot E = C \cdot D$$

whenever $C : F = 0$, $D : G = 0$ and $E : AF + G = 0$.

We are now in a position to give a detailed proof of the following corollary, which is an instance of the Corollary of §5.5 in Fulton 2008.

Corollary 5.3. *Let C, D and E be projective plane curves such that C and DE do not have a common component. If all points of $C \cap D$ are simple points on C and $C \cdot E \geq C \cdot D$, then there is a curve B such that $C \cdot B = C \cdot E - C \cdot D$.*

Proof. Firstly, if C and DE meet at infinity we can make a linear coordinate change so that the line at infinity does not meet any of the intersection points of C and DE. We may therefore assume that C and DE do not meet at infinity.

Let $C : F = 0$, $D : G = 0$ and $E : H = 0$. Set f, g and h as in the formulation of Max Noether's theorem. The assumption $C \cdot E \geq C \cdot D$ gives that $I_P(C, E) \geq I_P(C, D)$ for all $P \in C \cap D$. Since all these points are simple and C and D do not meet at infinity, Proposition 5.2 gives that $h \in (f, g)_P$ for all $P \in C \cap D$. An application of Max Noether's theorem gives that $H = IF + JG$ for some homogeneous polynomials I and J. Let $B : J = 0$. Now

$$C \cdot E = C \cdot BD = C \cdot B + C \cdot D$$

so that the result follows from rearranging the terms. □

6 Pappus's, Pascal's and Chasles' Theorems

As an applications of Max Noether's theorem and its corollary we show three results which are due to Pappus, Pascal and Chasles, respectively. These results are stated and proved briefly in Fulton 2008. The proofs given here are basically the same, but more detailed.

Note that Bezout's theorem states that

$$C \cdot D = \sum_{i=1}^{mn} P_i$$

where $\deg C = m$, $\deg D = n$ and the points P_i are not necessarily distinct, whenever C and D do not share a component. We first state a lemma that will be used in the upcoming proofs.

Lemma 6.1. *Let C and D be curves. If P is a simple point on C and $P \notin D$, then P is a simple point on CD.*

Proof. Let $C : f = 0$ and $D : g = 0$. Then by definition $CD : fg = 0$ so that by differentiating and inserting P one has

$$(fg)'_1(P) = f'_1(P)g(P) + f(P)g'_1(P) = f'_1(P)g(P)$$

by the assumption that $P \in C$. Similarly $(fg)'_2(P) = f'_2(P)g(P)$ and consequently $\nabla(fg)(P) = \nabla f(P)g(P)$. The assumption that $P \notin D$ gives that $g(P) \neq 0$ and it follows that P is a simple point on CD. □

Proposition 6.2. *Let C_1 and C_2 be cubics with no common component, such that $C_1 \cdot C_2 = \sum_{i=1}^{9} P_i$ where all P_i's are simple points on C_1. Suppose that D is a conic with no components in common with C_1, and $C_1 \cdot D = \sum_{i=1}^{6} P_i$. Then P_7, P_8 and P_9 are collinear.*

Proof. Because $C_1 \cdot C_2 \geq C_1 \cdot D$ there is by Corollary 5.3 a curve L such that

$$C_1 \cdot L = C_1 \cdot C_2 - C_1 \cdot D = P_7 + P_8 + P_9.$$

L must be a line. Therefore P_7, P_8 and P_9 lie on the same line, as desired. □

Corollary 6.3 (Pappus's Theorem)**.** *Let L and L' be two distinct projective lines. Suppose that P_1, P_2, P_3 and P'_1, P'_2, P'_3 are distinct points on $L \setminus L'$ and $L' \setminus L$ respectively. Let L_{ij} be the line through P_i and P'_j for $i, j \in \{1, 2, 3\}$ with $i \neq j$. Then the three intersection points $L_{ij} \cdot L_{ji}$ for $i \neq j$ lie on a straight line.*

Proof. Let C_1 be the cubic $L_{12}L_{23}L_{31}$ and $C_2 = L_{13}L_{21}L_{32}$. Furthermore let D be the conic LL'. When the hypotheses of Proposition 6.2 have been shown, the proof is complete.

We first show that C_1 and C_2 do not share a component. Suppose toward contradiction that C_1 and C_2 have a component in common. Then two lines L_{ij} and L_{kl} are the same line where $j - i \equiv 1 \pmod 3$ and $l - k \equiv 2 \pmod 3$. If $i \neq k$ then P_i and P_k both lie on the line L_{ij} so $L_{ij} = L$. It follows that $P'_j \in L$ contradicting the construction. Otherwise, if $i = k$, then $j \neq l$ so that P'_j and P'_l lie on L_{kl} and it follows that $L' = L_{kl}$ contradicting that $P_k \notin L'$. Hence, C_1 and C_2 do not share a component.

Similarly, if C_1 and D share a component then without loss of generality $L = L_{ij}$ for some i and j, but this contradicts that $P'_j \notin L$. Thus, C_1 and D do not have a common component.

Let $R_1 = L_{12} \cdot L_{21}$, $R_2 = L_{13} \cdot L_{31}$ and $R_3 = L_{23} \cdot L_{32}$. By construction

$$C_1 \cdot C_2 = \sum_{i=1}^{3} P_i + \sum_{i=1}^{3} P'_i + \sum_{i=1}^{3} R_i.$$

It shall be shown that P_1, P_2, P_3, P'_1, P'_2, P'_3 and R_1, R_2, R_3 are simple points on C_1.

Suppose toward a contradiction that $P_1 \in L_{23}$. Then L_{23} goes through both P_1 and P_2 so that $L_{23} = L$. It then follows that $P'_3 \in L$, but this contradicts the assumption that $P'_3 \in L' \setminus L$. Thus, $P_1 \notin L_{23}$, and $P_1 \notin L_{31}$ is shown similarly. Since P_1 is a simple point on L_{12} it follows P_1 is a simple point on C_1 by Lemma 6.1. Similarly, $P_2, P_3, P'_1, P'_2, P'_3$ are simple points one C_1.

We only show that R_1 is a simple point on C_1. That also R_2 and R_3 are simple points is shown similarly.

Note that if $R_1 = P_2$, then $P_1, P_2 \in L_{12}$ so that $L_{12} = L$, which contradicts that $P_2' \notin L$. Thus, $R_1 \neq P_2$. Similarly $R_1 \neq P_1'$.

Suppose first that $R_1 \in L_{23}$. Then R_1, P_2 lie on both L_{21} and L_{23} and it follows that $L_{21} = L_{23}$. Now both P_1' and P_3' lie on L_{23} and it follows that $L_{23} = L'$, but this contradicts that $P_2 \notin L'$. Suppose next that $R_1 \in L_{31}$. Then R_1, P_1' lie on both L_{31} and L_{21} so that $L_{31} = L_{21}$. Now one gets the contradiction that $P_1' \in L$. Therefore $R_1 \in L_{12}$, $R_1 \notin L_{23}$ and $R_1 \notin L_{31}$ Lemma 6.1 gives that R_1 is a simple point on C_1. □

The next named result we will show is Pascal's theorem, and to show it we will utilize a property of conics. To keep the proof of Pascal's theorem relatively clean we state the result as a lemma.

Lemma 6.4. *If three distinct points of a conic are collinear, then it is reducible.*

Proof. Let L be the line through the distinct points, and let C be the conic. If L and C do not share a component, then the weak form of Bezout's theorem states that they intersect in at most two points, but since they intersect in three points the curves must have a common component. Because the only component of L is L itself, it is a component of C, showing that C is reducible. □

The very short formulation of this the next corollary affords the clarification that the sides might need to be extended outside the conic.

Corollary 6.5 (Pascal's Theorem)**.** *Suppose that a hexagon is inscribed in an irreducible conic. Then the intersections of the opposite sides are collinear.*

Proof. Let D be the conic and let $P_1, \dots, P_6$ be the distinct points on the hexagon. Define L_i to be the line through P_i and P_{i+1} for $i = 1, \dots, 5$ and L_6 the line through P_6 and P_1. Set $C_1 = L_1L_3L_5$ and $C_2 = L_2L_4L_6$.

First it is shown that C_1 and C_2 do not share a component. If $L_i = L_j$ for any two i and j, then three distinct points of D are collinear. An application of the previous lemma gives that D is reducible contrary to the assumption. Thus, $L_i \neq L_j$ for all $i \neq j$.

Let $R_i = L_i \cdot L_{i+3}$ be the intersections of the opposite sides. By construction

$$C_1 \cdot C_2 = \sum_{i=1}^{6} P_i + \sum_{i=1}^{3} R_i,$$

and $C_1 \cdot D = \sum_{i=1}^{6} P_i$. It only remains to show that the points are simple points on C_1 to be allowed to use Proposition 6.2, after which the result is immediate.

It is shown that P_1 is a simple point on C_1. That $P_2, \dots, P_6$ are simple points is shown similarly. First suppose that $P_1 \in L_i$ for some $i \in \{3, 5\}$. Then the points P_1, P_i, P_{i+1} of D lie on a line. The lemma gives that D is reducible, contrary to the assumption. Hence, $P_1 \in L_1$, but $P_1 \notin L_3$ and $P_1 \notin L_5$. Lemma 6.1 gives that P_1 is a simple point.

We now show that $R_i \neq P_j$ for all meaningful i and j. Suppose toward a contradiction that $R_i = P_j$ for some i and j. Note that $R_i \in L_i$ and $R_i \in L_{i+3}$. It holds that

$$(j \neq i \wedge j \neq i+1) \vee (j \neq i+3 \wedge j \neq l)$$

where $l = i + 4$ if $i \neq 3$ or $l = 1$ otherwise. It follows that three distinct points of D are collinear, so that D is reducible, but this is impossible, so $R_i \neq P_j$ as desired.

We show that R_1 is a simple point, but the same procedure applies to R_2 and R_3. If $R_1 \in L_3$, then the distinct points R_1 and P_4 lie on both L_3 and L_4, whence $L_3 = L_4$, which is a contradiction. If $R_1 \in L_5$, then the distinct points R_1 and P_5 lie on both L_4 and L_5, whence $L_4 = L_5$, which is also contradiction. Thus, R_1 belongs to exactly one of L_1, L_3 and L_5 so Lemma 6.1 gives that R_1 is a simple point on C_1.

By an application of Proposition 6.2 the proof is complete. □

The next theorem is given in Fulton 2008 with weaker conditions, namely that the curve C is only assumed to be irreducible and not non-singular. We have opted for including the restriction that C be non-singular to simplify both the formulation and the proof. This theorem is the same as the Cubic Cayley-Bacharach theorem given in Silverman and Tate 1992.

Theorem 6.6 (Chasles' Theorem). *Suppose that C is a non-singular cubic such that $C \cdot C' = \sum_{i=1}^{9} P_i$ for some cubic C' and not necessarily distinct points P_i. If $C \cdot C'' = \sum_{i=1}^{8} P_i + Q$ for some cubic C'', then $Q = P_9$.*

Proof. Assume toward a contradiction that $P_9 \neq Q$. Let L be a line that passes through P_9, but not through Q. Bezout's theorem gives that $C \cdot L = P_9 + R + S$ for some not necessarily distinct points R and S. By using Proposition 2.10 one has that

$$C \cdot C''L = \sum_{i=1}^{8} P_i + Q + P_9 + R + S = C \cdot C' + Q + R + S.$$

The assumption gives that all involved points are simple, so an application of Corollary 5.3 guarantees the existence of a curve L' (necessarily a line) such that $C \cdot L' = Q + R + S$. If R and S are distinct L and L' have two points in common so $L = L'$. Otherwise one gets that $L = L'$ by using the uniqueness of Proposition 4.3. It finally follows that $P_9 = Q$, contradicting the assumption, whence $P_9 = Q$. □

7 Addition on Elliptic Curves

In this last section we apply the results shown to show that addition on an elliptic curve gives rise to an abelian group. We will use the following definition of elliptic curves.

Definition 7.1. An elliptic curve is a non-singular cubic curve.

Let C be any elliptic curve. Given any two points $P, Q \in C$ there is by Bezout's theorem and Proposition 4.3 a unique line L such that $C \cdot L = P + Q + R$. We define the binary composition $*$ on C by $P * Q = R$.

Take any point $\mathcal{O} \in C$. We define addition on C by $P + Q = \mathcal{O} * (P * Q)$. That $(C, +)$ is an abelian group is verified by the next four propositions.

Proposition 7.2. *$P + Q = Q + P$ for all $P, Q \in C$.*

Proof. It is clear that $P * Q = Q * P$, since there is only one line containing both P and Q, counting multiplicity. The result follows from this. $\square$

Proposition 7.3. *$P + \mathcal{O} = P$ for all $P \in C$.*

Proof. Let L be the line containing P and $\mathcal{O}$ and let $C \cdot L = P + \mathcal{O} + R$. By definition $P * \mathcal{O} = R$, but then $P + \mathcal{O} = \mathcal{O} * R$. The definition gives $\mathcal{O} * R = P$, completing the proof. $\square$

Proposition 7.4. *For all $P \in C$ there exists a $Q \in C$ such that $P + Q = \mathcal{O}$.*

Proof. Let $R = \mathcal{O} * \mathcal{O}$, and let L_1 be the line such that $C \cdot L_1 = 2\mathcal{O} + R$. We claim that $Q = P * R$ meets the requirements. Let L_2 be the line such that $C \cdot L_2 = P + Q + R$. By definition we now have

$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * R = \mathcal{O}. \qquad \square$$

Proposition 7.5. *$P + (Q + R) = (P + Q) + R$ for all $P, Q, R \in C$.*

Proof. We will use parentheses to distinguish between addition in intersection cycles and addition on the cubic. Let $L_1, \dots, L_6$ be the lines such that

$$\begin{aligned} C \cdot L_1 &= Q + R + Q * R, \\ C \cdot L_2 &= \mathcal{O} + Q * R + (Q + R), \\ C \cdot L_3 &= P + (Q + R) + P * (Q + R), \\ C \cdot L_4 &= P + Q + P * Q, \\ C \cdot L_5 &= \mathcal{O} + P * Q + (P + Q), \\ C \cdot L_6 &= (P + Q) + R + (P + Q) * R. \end{aligned}$$

By letting $C' = L_1 L_3 L_5$ and $C'' = L_2 L_4 L_6$ one sees that

$$C \cdot C' = \mathcal{O} + P + Q + R + P * Q + Q * R + (P + Q) + (Q + R) + P * (Q + R)$$

and

$$C \cdot C'' = \mathcal{O} + P + Q + R + P * Q + Q * R + (P + Q) + (Q + R) + (P + Q) * R.$$

By an application of Chasles' theorem, $P * (Q + R) = (P + Q) * R$, so that

$$P + (Q + R) = \mathcal{O} * (P * (Q + R)) = \mathcal{O} * ((P + Q) * R) = (P + Q) + R. \quad \square$$

References

David Eisenbud, Mark Green and Joe Harris (June 1996). "Cayley-Bacharach Theorems and Conjectures". In: *Bulletin (New Series) of the American Mathematical Society* 33.3, pp. 295–324.

Fulton, William (2008). *Algebraic Curves (An Introduction to Algebraic Geometry)*. URL: http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf.

Silverman, Joseph H. and John Tate (1992). *Rational Points on Elliptic Curves (Undergraduate Texts in Mathematics)*. Ed. by J.H. Ewing, F.W. Gehring, and P.R. Halmos. Springer-Verlag. ISBN: 0-387-97825-9.