SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Bezout's Theorem

av

Caroline Björk

2026 - No K4

Bezout's Theorem

Caroline Björk

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Sofia Tirabassi

2026

Table of Contents

Contents

Abstract

This thesis will investigate how many points two algebraic curves intersects in and what the multiplicity is of each point. We will come to a result which is called Bezout's theorem which is important for more advanced studies in algebraic geometry.

I dethär självständiga arbete utforskar vi alla punkter som två algebraiska kurvor skär i varandra och vad multipiciteten är för varje sådan punkt. Vi kommer även komma fram till ett resultat som kallas för Bezout's theorem vilket är ett viktigt resultat som grundar mer avancerade studier inom algebraisk geometri.

Introduction

Given F(x,y)=0 and G(x,y)=0 where F and G are two polynomials in x and y, suppose you have a system of equations

$$\begin{cases} F(x,y) = 0 \\ G(x,y) = 0 \end{cases}$$

How many solutions can their system of equation have ?

Algebraically, this is the same as asking how many pairs (x,y) satisfies both equations F(x,y)=0 and G(x,y)=0. We will translate this problem into working with algebraic curves and then investigate in how many points they intersect in and provide an estimation of how they touch eachother in each such point, which we call the multiplicity of this point in respect to these two curves.

There are many problems that arise when trying to find these points. For example, the curves might intersect at infinity which we are not able to see or count. Therefore we also need to develop certain tools and procedures that will aid us in this regard which we will do using projective geometry.

The main body of the work will be to prove Bezout's theorem which gives us a simple method to estimate how many intersection points two curves can have in an algebraically closed field together with their multiplicities, including points of infinity.

For this paper the reader is recommended to have background knowledge in group theory and ring theory aswell as basic knowledge in topology, calculus, linear algebra, set theory and combinatorics.

It is also recommended to have knowledge of the polynomial division algorithm in one variable as we need to extend it to multiple variables to be able to calculate the number of intersection points including their multiplicities. The extension of the division algorithm is in preliminaries for those who have not encountered it before.

1 Preliminaries

We will need to extend the division algorithm in $K[x]$ to $K[x_1, .., x_n]$. All information in this section is from Ideals, Varieties and Algorithms by David A. Cox, John little and Donal O'Shea [2].

Definition 1.1. Monomial Ordering
Recall first that a monomial in $x_1, .., x_n$ is a product of the form $x_1^{\alpha_1} * x_2^{\alpha_2} * .. * x_n^{\alpha_n}$, $a_n \neq 0$. The total degree of a monomial is the sum $\alpha_1 + .. + \alpha_n$. Now the monomial $x^\alpha = x_1^{\alpha_1} * ... * x_n^{a_n}$ gives a tuple $\alpha = (\alpha_1, ..., \alpha_n) \in Z_{\geq 0}^n$, so we have a one to one correspondence between monomials in $K[x_1, .., x_n]$ and $Z_{\geq 0}^n$.

We can therefore define a monomial ordering on $K[x_1, ..., x_n]$ as a relation $>$ on $Z_{\geq 0}^n$, which will give us a relation on the set of monomials $x^\alpha, \alpha \in Z_{\geq 0}^n$ such that

1) $>$ is a total ordering on $Z_{\geq 0}^n$

2) If $\alpha > \beta$ and $\gamma \in Z_{\geq}^n$ then $\alpha + \gamma > \beta + \gamma$

3) $>$ is a well-ordering on $Z_{\geq 0}^n$.

It follows that $x^\alpha > x^\beta$ if $\alpha > \beta$. By the total ordering we know that exactly one of these three statements holds for every pair of x^α and x^β:

$$x^\alpha > x^\beta$$
$$x^\alpha = x^\beta$$
$$x^\beta > x^\alpha$$

A total order is also transitive, so if $x^\alpha > x^\beta$ and $x^\beta > x^\alpha$ then $x^\alpha > x^\gamma$.

Now the ordering we will use further on for examples is called the lexicographic order.

Definition 1.2. Lexicographic Order
Let $\alpha = (\alpha_1, ..., \alpha_n)$ and $\beta = (\beta_1, .., \beta_n)$ be in $Z_{\geq 0}^n$. We say that $\alpha >_{lex} \beta$ if the leftmost nonzero entry of the vector difference $\alpha - \beta \in Z^n$ is positive. If so, then $x^\alpha >_{lex} x^\beta$, otherwise $x^\beta > x^\alpha$ by reversal of the statement.

An example of lexicographic ordering is $(1, 2, 0) >_{lex} (0, 3, 4)$ since $\alpha - \beta = (1, -1, -4)$.

Note that the variables $x_1, .., x_n$ under the lexicographic order gives them the order

$$(1, 0, 0, .., 0) >_{lex} (0, 1, 0, .., 0) >_{lex} (0, 0, ..., 0, 1)$$

and so $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$ since for each x_i, we get $1 - 0$ for the x_j next to it on the right, so by transitivity the statement follows.

Proposition 1.3. *The lex ordering on $Z_{\geq 0}^n$ is a monomial ordering.*

Proof. By definition of comparing the first nonzero difference of the vectors, $\alpha >_{lex} \beta$ is a total order since $Z_{\geq 0}$ is a total order. Now if $\alpha >_{lex} \beta$ then their first nonentry in $\alpha - \beta$ is positive. So for any γ

$$(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$$

which tells us that $\alpha + \gamma >_{lex} \beta + \gamma$.

To see that it is a well-ordering, assume by contradiction that it is not. A set is well-ordered if and only if there does not exist a strictly infinite descending sequence of elements under the order. By contradiction, there must exist an infinite sequence $\alpha^{(1)} >_{lex} \alpha^{(2)} >_{lex} .....$

Now consider the first entries of all $\alpha^{(i)}$. This will be the first non-negative integer in the first entry, and together they create a subset of $Z^n_{\geq 0}$. As it is strictly descending, $\alpha^{(i_1)} >_{lex} \alpha^{(i_1+1)}$. Under the lexicographic order, this translates to the first integer entry of the left being larger than the first integer entry of the right so we have a strictly decreasing subset of $Z^n_{\geq}$. As $Z^n_{\geq}$ is well-ordered, we know that any non-increasing sequence of non-negative integers must stabilize, hence we conclude that the first entry of all $\alpha^{(i)}$ must become constant.

Now by using the same argument for all other entries, we can see that all entries eventually become constant, contradicting the fact that we have a strictly descending sequence. So $>_{lex}$ is well-ordered.

□

Definition 1.4. Let $f = \sum_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $K[x_1, .., x_n]$ and let $>$ be a monomial order:

1) The multidegree of f is multideg(f) = $\max\{\alpha \in Z^n_{\geq 0} : a_\alpha \neq 0\}$.

2) The leading coefficient of f is LC(f) = $a_{multideg(f)} \in K$.

3) The leading monomial of f is LM(f) = $x^{multideg(f)}$

4) The leading term of f is LT(f) = LC(f) $\cdot$ LM(f)

A monomial $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ divides another monomial $x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}$ if and only if $\alpha_i \leq b_i \; \forall \, i$ under the monomial order.

Theorem 1.5. *Division Algorithm in $K[x_1, .., x_n]$ Let $>$ be a monomial order on $Z^n_{\geq 0}$ and let $F = (f_1, .., f_s)$ be an ordered s-tuple of polynomials in $K[x_1, .., x_n]$. Then every $f \in K[x_1, .., x_n]$ can be written as*

$$f = q_1 f_1 + .. + q_s f_s + r$$

where $q_i, r \in K[x_1, .., x_n]$, and either $r = 0$ or r is a linear combination with coefficients in K of monomials such that none of them are divisible by any of the leading terms from f_i. r is called a remainder of f by division by F. Also, if $q_i f_i \neq 0$ then multideg(f) $\geq$ multideg($q_i f_i$).

For an example of how to calculate the division algorithm, we will divide $f = x^3y + x^2y^2 + xy + y^3$ by $f_1 = xy - 1$, $f_2 = x - y$, $f_3 = y^2 - 1$ under the lexicographic ordering.

Now since we are looking for polynomials q_1, q_2, q_3 and r $\in K[x, y]$ such that r does not divide any of the leading terms of f_i, we can set up a table:

$$\begin{array}{rl} q_1: & \\ q_2: & \\ q_3: & \\ xy-1 & \\ x-y & \overline{)x^3y + x^2y^2 + xy + y^3} \\ y^2-1 & \end{array}$$

Now we start checking for divisibility of the leading terms starting with f_1. LT(f) $= x^3y$ and LT(f_1) $= xy$. Now xy divides x^3y and $\frac{x^3y}{xy} = x^2$. So the first quotient term for f_1 is x^2 and we put it in the row for q_1 and subtract $x^2 * f_1 = x^2 * (xy - 1) = x^3y - x^2$ from f. So now our new dividend is $d_1 = (x^3y + x^2y^2 + xy + y^3) - (x^3y - x^2) = x^2y^2 + x^2 + xy + y^3$

$$\begin{array}{rl} q_1: & x^2 + xy \\ q_2: & \\ q_3: & \\ xy-1 & \\ x-y & \overline{)x^3y + x^2y^2 + xy + y^3} \\ y^2-1 & \\ & \underline{x^3y - x^2} \\ & x^2y^2 + x^2 + xy + y^3 \end{array}$$

Now repeat but with our new dividend. LT(d_1) $= x^2y^2$. LT(f_1) $= xy$ so again we can divide $\frac{x^2y^2}{xy} = xy$. Add xy to q_1 and subtract $xy * f_1$ from d_1 to get our new dividend $d_2 = x^2 + 2xy + y^3$.

$$\begin{array}{rll} q_1: & x^2 + xy & \\ q_2: & & \\ q_3: & & r \\ xy-1 & & \\ x-y & \sqrt{x^3y + x^2y^2 + xy + y^3} & \\ y^2-1 & & \\ & \underline{x^3y - x^2} & \\ & x^2y^2 + x^2 + xy + y^3 & \\ & \underline{xy(xy-1)} & \\ & x^2 + 2xy + y^3 & \end{array}$$

We continue in this fashion until we find that the leading term of any f_i is not divisible by the leading term of the dividend. We move that term to the remainder list, and repeat the process to check if any leading term of f_i divides the new leading term of the dividend. Continue until the process stops and no f_i can divide any term of the dividend.

Once the process have stopped, collect the quotients and remainders and rewrite f $= f_1 * q_1 + f_2 * q_2 + f_3 * q_3 + r$.

We will continue from where we stopped in our example.

LT(d_2) = x^2. LT(f_2) = x and $\frac{x^2}{x} = x$. Add x to q_2 and d_2= d_2 - $x^* f_2 = 3xy - y^3$.

LT(d_3)= $3xy$. LT(f_1)=xy. $\frac{3xy}{xy} = 3$. Add 3 to q_1 and d_4=d_3-$3 * f_1 = y^3 + 3$.

LT(d_4) = y^3. $LT(f_3) = y^2$. $\frac{y^3}{y^2} = y$. Put y to q_3 and d_5=d_4-$y * f_3$=$y + 3$.

Hence, no leading term of any f_i can divide LT(d_5)=y. Put y to the remainder r. The new dividend is $d_6 = 3$ and we can also see that no leading term of f_i can divide 3 either, so 3 is added to r. In algorithmic way, this will be

$$
\begin{array}{rll}
q_1: & x^2 + xy + 3 & \\
q_2: & x & \\
q_3: & y & r \\
xy - 1 & & \\
x - y & \sqrt{x^3y + x^2y^2 + xy + y^3} & \\
y^2 - 1 & & \\
 & x^3y - x^2 & \\
 & \hline
 & x^2y^2 + x^2 + xy + y^3 & \\
 & xy(xy - 1) & \\
 & \hline
 & x^2 + 2xy + y^3 & \\
 & x \cdot (x - y) & \\
 & \hline
 & 3xy - y^3 & \\
 & 3 \cdot (x - y) & \\
 & \hline
 & y^3 + 3 & \\
 & y \cdot (y^2 - 1) & \\
 & \hline
 & y + 3 & \to y + 3
\end{array}
$$

So we have that

$$
\begin{aligned}
q_1 &= x^2 + xy + 3 \\
q_2 &= x \\
q_3 &= y \\
r &= y + 3
\end{aligned}
$$

and $f = (x^2 + xy + 3)f_1 + xf_2 + y^2 f_3 + y + 3$.

So now that we have the extended division algorithm, we are also going to regard Gröbner bases which will be used for computations.

Definition 1.6. Gröbner Basis
Fix a monomial order on the polynomial ring $K[x_1, .., x_n]$. A finite subset $G = \{g_1, ..., g_n\}$ of an ideal I is said to be a Gröbner basis if $(LT(g_1), .., LT(g_i)) = LT(I)$ where LT(I) denotes the ideal generated by leading terms of the polynomials in I.

Equivalently we can restate this as a set $\{g_1, .., g_n\} \subset I$ is a Gröbner basis if and only if the leading term of any element of I is divisible by one of the $LT(g_i)$.

Corollary 1.7. *Fix a monomial order. Then every ideal $I \subset K[x_1, .., x_n]$ has a Gröbner basis. Furthermore, any Gröbner basis of I is also a basis of I so (G) = (I).*

Lemma 1.8. *Let G be a Gröbner basis of $I \subset K[x_1, ..., x_n]$. Let $p \in G$ be a polynomial such that $LT(p) \in (LT(G \setminus \{p\}))$. Then $G \setminus \{p\}$ is also a Gröbner basis for I.*

Proof. If LT(p) $\in (LT(G \setminus \{p\}))$ then we know that LT(p) can be written as a combination of the leading terms of the other elements in G, so (LT(G $\setminus\{p\}$)) $= LT(G)$. Since we know that (LT(G)) = LT(I) we can conclude that $(LT(G \setminus \{p\})) = LT(I)$. □

Gröbner bases are important as they allow us to fully extend the division algorithm in order to receive unique remainders.

Proposition 1.9. *Properties of Gröbner Basis*

Let $I \subset K[x_1, .., x_n]$ be an ideal and let $G = \{g_1, ..., g_i\}$ be a basis for I. Then given $f \in K[x_1, .., x_n]$, there is a unique $r \in K[x_1, .., x_n]$ with the following properties:

1) No term of r is divisible by any of $LT(g_1), .., LT(g_i)$.

2) There is $g \in I$ such that $f = g + r$.

In particular, r is the unique remainder on division of f by G no matter how the elements are listed when using the division algorithm.

Definition 1.10. Reduced Gröbner basis, page 93 [2]
A reduced Gröbner basis for a polynomial ideal I is a Gröbner basis for I such that:

1) LC$(p) = 1 \ \forall \ p \in G$

2) $\forall \ p \in G$, no monomial of p lies in $(LT(G) \setminus \{p\})$.

Theorem 1.11. *Reduced Gröbner Basis is Unique, page 93 [2]*

Let $I \neq \{0\}$ be a polynomial ideal. Then for a given monomial ordering, I has a reduced Gröbner basis and the reduced Gröbner basis is unique.

We will now calculate how to find a Gröbner basis for every ideal I.

Definition 1.12. Definition 4 Let $f, g \in K[x_1, .., x_n]$ be nonzero polynomials.

1) If multideg(f) $= \alpha$ and multideg(g) $= \beta$ then let $\gamma = (\gamma_1, .., \gamma_n)$ where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^γ the least common multiple of LM(f) and LM(g), written $x^\gamma =$ lcm$(LM(f), LM(g))$

2) The S-polynomial of f and g is the combination

$$S(f, g) = \frac{x^\gamma}{LT(f)} * f - \frac{x^\gamma}{LT(g)} * g$$

Note now that if $I = (f, g)$ then $S(f, g) \in I$ since the right hand side is a polynomial multiple of f and g.

Theorem 1.13. *Theorem 6: Buchberger's Criterion[2], page 86*

Let I be a polynomial ideal. Then a basis $G = \{g_1, .., g_i\}$ of I is a Gröbner Basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G listed in some order is zero.

Theorem 1.14. *Theorem 2: Buchberger's Algorithm [2], page 91*

Let $I = (f_1, ..., f_n) \neq \{0\}$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps.

1) *Given your inital set of generators $f_1, .., f_n$, create a set $F = \{f_1, .., f_n\}$ and then for every possible pair of different polynomials in F compute their S-polynomial.*

2) *Divide every S-polynomial with elements in F to find remainders r and check reductions modulo I.*

3) *If $r = 0$ then do nothing, if $r \neq 0$ then add it to the set F. Note that $r \in I$ since divison by F means that $S(f_i, f_j) = \sum_i g_i f_i + r$. So $r = S(f_i, f_j) - \sum_i g_i f_i \in I$.*

4) *If any r was added to the set F, then repeat the process from step 2. Stop when no new polynomials are added.*

When no new polynomials are produced this way, the final set is a Gröbner basis for I. For optimization purposes, we wish to reduce the basis to get a reduced Gröbner basis. Note that this process must terminate as each time a new polynomial is added, the leading term is a strictly smaller monomial in the given monomial ordering which is well-founded.

Example.

Under the lexicographic ordering, let I = $(x^2 - y, xy - 1)$ and $F = \{x^2 - y, xy - 1\}$.

To compute their S-polynomial, we will first find $LM(x^2 - y) = x^2$ and $LM(xy - 1) = xy$. Now $\text{lcm}(x^2, xy) = x^2y$ since $\max_1(2, 1) = 2$ and $\max_2(0, 1) = 1$ of their multideg.

So

$$\begin{aligned} S(x^2 - y, xy - 1) &= \frac{x^2y}{x^2} \cdot (x^2 - y) - \frac{x^2y}{xy} \cdot (xy - 1) \\ &= y \cdot (x^2 - y) - x \cdot (xy - 1) \\ &= yx^2 - y^2 - x^2y + x = x - y^2 \end{aligned}$$

We can see that $x - y^2$ can not be divided by any of the leading terms of $x^2 - y$ and $xy - 1$, since neither x^2 or xy divides x. So the S-polynomial is its own remainder, and $x - y^2 \neq 0$ so it must be added to F.

Now we have that F = $\{x^2 - y, xy - 1, x - y^2\}$. We must now check $S(x - y^2, x^2 - y)$

and $S(x-y^2, xy-1)$. Thus

$$\begin{aligned} S(x-y^2, x^2-y) &= \frac{x^2}{x} \cdot (x-y^2) - \frac{x^2}{x^2} \cdot (x^2-y) \\ &= x(x-y^2) - (x^2-y) \\ &= x^2 - xy^2 - x^2 + y = y - xy^2 = y(xy-1 \end{aligned}$$

Note that $(xy-1) \in I$ so this is reduced to 0 modulo I. So r $= 0$ and nothing needs to be added. Further:

$$\begin{aligned} S(x-y^2, xy-1) &= \frac{xy}{x} \cdot (x-y^2) - \frac{xy}{xy} \cdot (xy-1) \\ &= y(x-y^2) - (xy-1) \\ &= xy - y^3 - xy + 1 = 1 - y^3 \end{aligned}$$

By indivisibility again, this must be added to F, and so F $= \{x^2-y, xy-1, x-y^2, 1-y^3\}$ and we repeat the process again:

$$\begin{aligned} S(1-y^3, x^2-y) &= \frac{x^2y^3}{y^3} \cdot (1-y^3) - \frac{x^3y^3}{x^2} \cdot (x^2-y) \\ &= x^2(1-y^3) - y^3(x^2-y) \\ &= x^2 - x^2y^3 - x^2y^3 + y^4 \\ &= x^2 - 2x^2y^3 + y^4 \end{aligned}$$

Now we can reduce using $1-y^3$ since $1-y^3 \in I$ implying that $y^3 = 1 \mod I$. Thus

$$\begin{aligned} x^2 - 2x^2y^3 + y^4 &= x^2 - 2x^2y^3 + y^4 \\ &= x^2 - 2x^2 + y^4 \\ &= -x^2 + y^4 \end{aligned}$$

Since we also have that $x - y^2 \in I$, then $x = y^2$ mdd I so $y^4 = y^2 * y^2 = x * x = x^2$, and thus $-x^2 + y^4 = -x^2 + x^2 = 0 \mod I$. Hence, $r = 0$. Now,

$$\begin{aligned} S(1-y^3, xy-1) &= \frac{xy^3}{y^3} * (1-y^3) - \frac{xy^3}{xy} * (1-xy) \\ &= x(1-y^3) - y^2(xy-1) \\ &= x - xy^3 - xy^3 + y^2 \\ &= x - 2xy^3 + y^2 \end{aligned}$$

By using $y^3 = 1$ we get that $x - 2xy^3 + y^2 = x - 2x + y^2 = -x + y^2$. By $x = y^2$ we get $-x + x = 0$ mod I. So $r = 0$ again. Further,

$$\begin{aligned} S(1-y^3, x-y^2) &= \frac{xy^3}{y^3} * (1-y^3) - \frac{xy^3}{x} * (x-y^2) \\ &= x(1-y^3) - y^3(x-y^2) \\ &= x - xy^3 - xy^3 + y^5 \\ &= x - 2xy^3 + y^5 \end{aligned}$$

By the same reductions as used above we receive

$$\begin{aligned} x - 2xy^3 + y^5 &= x - 2x + y^5 \\ &= -x + y^5 \\ &= -y^2 + y^5 \\ &= -y^2 + y^2 * y^3 \\ &= -y^2 + y^2 = 0 \mod I \end{aligned}$$

Thus, $r = 0$ again.

Since $r = 0$ for all the new S-polynomials, our process has terminated and our Gröbner basis is F = $\{x^2 - y, xy - 1, x - y^2, 1 - y^3\}$. We shall now find the reduced Gröbner basis.

Following definition 4) we can see that 1) is satisfied for all polynomials in F so we start with $x^2 - y$ and the ideal $(F \setminus (x^2 - y))$. In this ideal we see that the relations $x = y^2, xy = 1, y^3 = 1$ holds and so

$$\begin{aligned} x^2 - y &= x * x - y \\ &= xy^2 - y \\ &= y^2 * y^2 - y \\ &= y^4 - y = y^3 * y - y \\ &= y - y = 0 \end{aligned}$$

Thus $x^2 - y$ reduces to 0 modulo the others, implying we can remove this polynomial.

Consider $xy - 1$ modulo $(F \setminus \{xy - 1\})$. By the relations $y^3 = 1$ and $x = y^2$ we calculate

$$xy - 1 = y^2 * y - 1 = y^3 - 1 = y^3 - y^3 = 0$$

So $xy - 1$ is also removed.

For $1 - y^3$ and $x - y^2$ we easily see that we can not reduce them by each others relations as they do not have any common factors. So our reduced Gröbner basis is F' = $\{1 - y^3, x - y^2\}$.

1.1 Gröbner bases in K[[x,y]], the ring of formal power series

As we move on to $K[[x, y]]$, we can already see that the division algorithm we extended for $K[x, y]$ might not terminate anymore as we work with infinite power series. Note that $K[x, y] \subset K[[x, y]]$ so every polynomial can be seen as a finite power series.

The following information is from [4]

Given a monomial ordering on $k[[x, y]]$ and the machinery we have already gone through, to find a Gröbner basis for an ideal (F,G) we need to use trunctation to avoid that the division algorithm might not terminate with infinite polynomials. This implies given any polynomial f, truncated at order M $\in N$ is f without all its monomials of degree $> M$.

The Buchberg algorithm for truncation is then:

1 Pick a truncation order M

2 Take the generators of the ideal F and G, truncate them to degree M.

3 Compute the usual algorithm with the S-polynomials and reduce module the truncated basis to get new elements up to degree $\leq M$ until we have a Gröber basis.

4 Pick trunction order M+1 and repeat the process to find a Gröber basis of this degree.

5 If the process terminates at some degree M, that is no new elements get added to the basis as $M \to \infty$ then we have a finite Gröbner basis with elements of finite degree, as there are only finitely many monomials $x^i y^j$ such that i+j $\leq M$.

6 If the process do not terminate then we are getting an infinite Gröbner basis of infinite degree.

We are interested in the case of step 5. If this case has accured, note that the Gröbner basis is now a subset of $K[x, y]$. As we have that (F,G) = (G) $\subset K[x, y]$ we can continue calculations in $K[x, y]$ of the ideal (F,G) which we will do further on.

For now, all that remains is to show that this does not depend on the chosen monomial ordering for the calculations of a Gröbner basis. Therefore we need to show that all the cosets are the same but with a different representative.

Proof. Given $I \subset K[x_1, .., x_n]$ and two Gröbner basis G, G' for two different monomial orderings and any $f \in K[x_1, .., x_n]$ we know that $f = \sum_{i=1}^{m} q_{i_i} + r$, $g_i \in G$ and

$$f = \sum_{i=1}^{n} q'_j g'_j + r', \; g'_j \in G'$$

Therefore, $f - r \in I$, $f - r' \in I$ as both sums are in I by definition of the division algorithm. So we have that $f = r \mod I$ and $f = r' \mod I$. So the cosets remain the same no matter the monomial ordering. □

2 Affine Varieties

Throughout the rest of this work, the book that has been used is Plane Algebraic Curves by Andreas Gathmann .

We will always assume rings to be commutative with a multiplicative element 1.

Let K be a field. For $n \in N$ we call $A^n = A^n_K$ the affine n-space over a field K. The elements in A^n are called points which are from the underlying set K^n.

Given a subset S of $K[x_1, ..., x_n]$, the affine zero locus of S is the set V(S) = $\{P \in A^n : f(P) = 0 \ \forall f \in S\}$ which is a subset of A^n. An affine variety K is a subset of A^n such that $K = V(S)$ for S $\subset K[x_1, .., x_n]$.

If S = $\{f_1, .., f_k\} \subset K[x_1, ..., x_n]$ is a finite set, then we will write V(S) = $(\{f_1, ..., f_k\}) = V(f_1, .., f_k)$.

Lemma 2.1. *Affine varieties are the closed sets of a topology.*

Proof. We wish to equip A^n_K with a topology. First, we see that for any two polynomials $f, g \in K[x_1, .., x_n]$, we have that (Andreas Gathmann[1], page 8):

1) $V(f) \cup V(g) = V(fg)$

2) $V(f) \cap V(G) = V(f, g)$

For 1) to hold, we need that $fg(P) = 0 \leftrightarrow f(P) = 0$ or $g(P) = 0$.

To see that the above statement holds, recall the evaluation map $ev_P : K[x_1, .., x_n] \to K$ where $ev_P(f) \to f(P)$. As the evaluation map is a ring homomorphism, we know that it respects addition and multiplication, so $ev_P(f + g) = ev_P(f) + ev_P(g)$ and $ev_P(fg) = ev_P(f) * ev_P(g)$.

Let $(fg)(P) = 0$. Then $f(P) \cdot g(P) = 0$ by the evaluation map. Since K is a field, it is an integral domain so either $f(P) = 0$ or $g(P) = 0$. If $f(P)$ or $g(P) = 0$, then again by the evaluation map multiplication we have that $(fg)(P) = 0$.

For 2) we can see that this holds by definition as $V(f, g) = \{P \in A^n : f(P) = 0$ and $g(P) = 0\}$, so if P $\in V(f, g)$ then $f(P) = 0$ and $g(P) = 0$.

Note that this give us that the union and intersection of two varieties is a variety aswell.
Now we will extend these properties for any family $(S_i)_i \subset K[x_1, .., x_n]$ by showing that $\cup V(S_i) = V(\prod_i S_i)$ and $\cap V(S_i) = V(\cup S_i)$.

For the first statement, let $x \in \cup V(S_i)$. Then we know that there exists an i such that $f(x) = 0 \ \forall f \in S_i$. In $\prod_i S_i$, we know then that for this x any $\prod_i f_i(x) = 0$ since the product is 0 if and only if at least one factor is 0 as shown above, which it is for the i-th coordinate since for every $f \in S_i$, $f(x) = 0$. So $x \in V(\prod_i S_i)$. Now let $x \in V(\prod_i S_i)$. Assume x is not in $\cup_i V(S_i)$. That means x is not in $V(S_i)$ $\forall i$, therefore there exist for every i a polynomial $f_i \in S_i$ such that $f_i(x) \neq 0$. Consider the element $f = \prod_i f_i$ of these polynomials. Evaluated at x we get $f(x) = \prod_i f_i(x) \neq 0$ but this implies then that x is not in $V(\prod_i S_i)$ which gives us a contradiction.

For the second statement, let $x \in \cap V(S_i)$. By definition $V(\cup_i S_i) = \{x \in A^n : f(x) = 0 \; \forall f \in \cup_i S_i\}$, therefore $V(\cup S_i)$ is the set of all x such that $f_i = 0$ for all $f_i \in S_i so x must then be in \mathrm{V}(\cap S_i)$ as well. Conversely, let $x \in V(\cup_i S_i)$. So $f_i(x) = 0$ for all $f_i \in S_i$, but then x must be in $\cap_i V(S_i)$.

Therefore we also have now that any arbitrary union and intersection of varieties is again a variety.

We can now introduce a topology on the affine n-space, called the Zariski topology, where the closed sets are the affine varieties and the open sets are the complements of these.

First we will see that the varieties satisfy the closed set axioms. Note that $\emptyset$ is closed because we can write it as V(1). The constant polynomial 1 has no solution so its zero set is empty. The whole space A_n^k is the zero set of the zero polynomial because f(x)=0 $\forall x \in A_n^k$.

Let F be a finite collection of varieties, so F = $\{V(S_i) \subset A_n^k : S_i \subset K[x_1, ..., x_n]\}$. We want to see that it is closed under finite union. We know now that $\cup_i V(S_i) = V(\prod_i S_i)$ which is a variety as we have seen, so it is closed. Now let F instead be any arbitrary collection of varieties. We want to see that it is closed under intersection. Since $\cap V(S_i) = V(\cup_i S_i)$ we have that the intersection is a variety, so it is closed as well.

To see that the topology axioms are satisfied, note first that $A_n^k = A_n^k \setminus \emptyset$ is an open set and $\{\emptyset\} = \{\emptyset\} \setminus A_n^k$ is also an open set since we saw that A_n^k, $\emptyset$ are closed. So the first axiom of a topology is satisfied.

Now we need to see that they are closed under arbitrary unions. So let $\{U_i\}$ be any family of open sets. By definition, U_i open implies that $A_n^k \setminus U_i$ is closed. Consider U = $\cup_i U_i$ and $A_n^k \setminus U$. By De Morgan's Law this is just $A_n^k \setminus \cup_i U_i = \cap_i (A_n^k \setminus U_i)$. We know this is a variety, so it is a closed set. Therefore U is open so any arbitrary union of open sets are open.

Furthermore, take any finite family of open sets $\{U_i\}_i$ and consider $A_n^k \setminus \cap_i^n U_i$. By De Morgan's law again we have that $A_n^k \setminus \cap_i U_i = \cup_i (A_n^k \setminus U_i)$ where each $A_n^k \setminus U_i$ is closed so we have a finite union of varieties which we know is again a variety so we get that any finite intersection of open sets is open.

As the topology axioms are satisfied, we may conclude that the Zariski topology is a topology on the affine n-space. $\square$

3 Affine Curves

Definition 3.1. Definition 1.5, Andreas Gathmann[1], page 8

1) An affine plane curve is a non-constant polynomial F $\in K[x, y]$ modulo the equivalence relation $F \sim G$ if F $= \lambda G$ for some $\lambda \in F^*$.

2) The degree of a curve is its degree as a polynomial. Note that the degree is well-defined since deg(F) $= \max \{i + j : x^i y^j \in F\}$ where the coefficient is nonzero and multiplying by a scalar does not change the degree of a polynomial, only the coefficient.

3) A curve F is called irreducible if it is as a polynomial, and reducible otherwise. If F $= F_1^{a_1} F_2^{a_2} ... F_k^{a_k}$ is the irreducible decomposition of F as a polynomial, we will also call this the irreducible decomposition of the curve F. The curves $F_1, ..., F_k$ are then the irreducible components of F and $a_1, ...a_k$ their multiplicity. If all multiplicities are 1, F is called reduced.

We need to check that the irreducibility is well-defined. Since $K[x_1, ..., x_n]$ is a Unique Factorization Domain, we know that every nonzero non-unit can be factored as a product of irreducible elements and the factorization is unique up to units. So what we need to do is to show that the units of $K[x_1 1, .., x_n]$ is $K^* = K \setminus \{0\}$.

Proof. Let $\lambda \in K^*$, then $\lambda^{-1} \in K^*$ because K is a field so every nonzero element has an inverse and we have that $\lambda * \lambda^{-1} = 1$, so it is also a unit. Now assume $f \in K[x_1, .., x_n]$ is a unit and $\deg(f) > 0$. Then there exists a g such that $fg = 1$. Note however that $0 = \deg(fg) = \deg(f) + \deg(g) \neq 0$. This can not hold so f is not a unit, therefore the only units are K^*. From 1) we now have that they are the same polynomial so it is well-defined. □

In the field K=$\mathbb{R}$ we will usually visualize a curve F by drawing its set of points V(F) in the plane as shown in the Figure 1 below: (Andreas Gathmann, page 9)

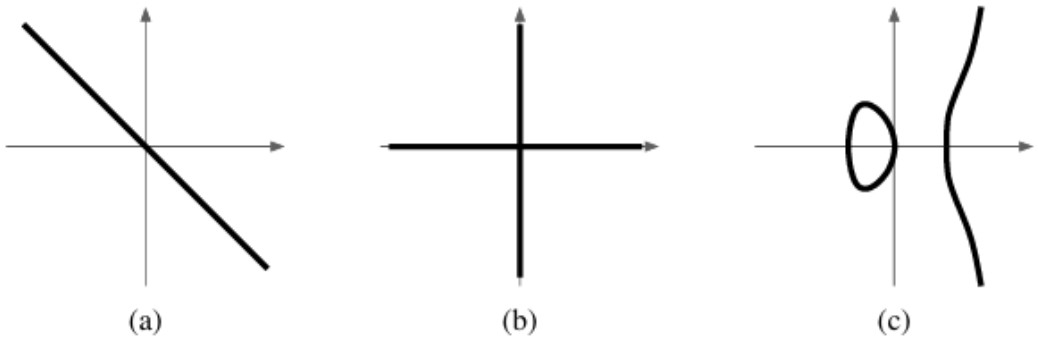


Figure 1

Here we have the curves a) $x + y$, b) xy and c) $y^2 + x - x^3$, K = $\mathbb{R}$.

Even though curves are defined to be a polynomial modulo scalars, we would like to think of a curve as a geometric object as in Figure 1. However, the zero set is not unique to a specific polynomial F and different multiplicities give the same zero set, an example of that may be $(x - y)$ and $(x - y)^2$. Non-vanishing functions also give the same zero set, for instance V(1) = V($x^2 + y^2 + 1$) in $\mathbb{R}$.

What we want to see, and will see is that these are essentially the only two situations that can arise given the same zero set if we work over algebraically closed fields.

Remark 1.9 Algebraically closed fields (Andreas Gathmann[1],page 9)

A field K is called algebraically closed if every non-constant polynomial F $\in K[x]$ has a zero. An example of an algebraically closed field is $K = \mathbb{C}$.

Every field is contained in an algebraically closed one, so that only considering curves over algebraically closed fields is not a serious constriction.

Construction 1.10 Quotient fields (Andreas Gathmann[1], page 9).

For any integral domain R there is an associated quotient field QuotR = $\{\frac{a}{b} : a, b \in R,\ b \neq 0\}$ where the fraction $\frac{a}{b}$ denotes the equivalence class $(a, b) \sim (a', b') \leftrightarrow ab' = a'b$.

In this work we will use the field R = K[$x_1, .., x_n$] for which the quotient field QuotR is denoted by K($x_1, .., x_n$) and will be the field of rational polynomials over K. For example, if we take R = K[x_1, x_2] then $\frac{x_1+x_2}{x_1-x_2} \in K(x_1, x_2)$.

Lemma 3.2. *Lemma 1.11, Andreas Gathmann[1], page 10*
Let F be an affine curve.

1) *If K is algebraically closed then V(F) is infinite.*

1) *If K is infinite then $A^2_K \setminus V(F)$ is infinite.*

Proof. For 1) let F be an affine curve. Since it is not a constant polynomial by definition, it has positive degree in at least one of the variables x and y. W.L.O.G assume it is in x. Then we can rewrite F as F = $a_n x^n + \ldots + a_0$ for some $a_0, \ldots, a_n \in K[y]$ with n $> 0, a_n \neq 0$. So we look at F as a polynomial in x with coefficients that are polynomials in y.

As a_n is a polynomial in $K[y]$ it has at most finitely many deg(a_n) zeroes. We now wish to prove that an algebraically closed field K is infinite.

Assume K is finite and K is algebraically closed. Let $|K| = q < \infty$. Define the polynomial $f(x) = \prod_{a \in K}(x - a) + 1 \in K[x]$ which we know exists since K is finite, $degf(x) = q$. Note that every element $a \in$ K vanishes on $(x - a)$, however this polynomial will never be zero from any element in K so this polynomial does not have a zero. This contradicts the fact that K is algebraically closed. Therefore K must be infinite.

So as there are infinitely many $k \in K$ such that $a_n(k) \neq 0$. For each such k, consider

F(x,k) where k is fixed. This is a polynomial in $K[x]$ and since K is algebraically closed there must be some $k' \in K$ such that $F(k', k) = 0$. Therefore

$$(k', k) \in V(F)$$

for each such k and V(F) is infinite since there is infinitely many such k.

For 2) we continue with each such k from 1) such that $a_n(k) \neq 0$, we get that F(x,k) is a non-constant polynomial in $K[x]$ so there are only finitely many $k' \in K$ such that $F(k', k) = 0$. Therefore there are infinitely many $z \in K$ such that $F(z, k) \neq 0$. So the complement of V(F) is infinite. □

Proposition 3.3. *Proposition 1.12, Finiteness of the intersection of curves, Andreas Gathmann[1], page 10 Let F and G be two curves without a common component.*

1) *The ideal (F,G) in K[x,y] contains a non-zero polynomial that depends only on x (and by symmetry, also a non-zero polynomial that depends only on y)*

2) *The intersection V(F,G) of the two curves is finite.*

Proof. Following the proof of Andreas Gathmann[1], for 1) we can see that because F and G have no common component, F and G are coprime. We also wish to see that they are coprime in $K(x)[y]$.

As $K[y] \subset K(y)$, we can embed any polynomial in y (or any variables) into their representative class of rational function. Again, consider F and G as polynomials in $K[y]$ with coefficients in $K[x]$, and then embed them into K(y). So F $= a_n y^n + \ldots + a_0$ and G $= b_m y^m + \ldots + b_0$ for $a_n, \ldots, a_0, b_m, \ldots, b_0 \in K(x)$. Assume they are not coprime in $K(x)[y]$, so they share a common component H in $K(x)[y]$ and we have $F = HF'$, $G = HG'$. As $H \in K(x)[y]$, it has denominators in its coefficients from $K[x]$, so after clearing all denominators we would have $aF = H'F'$ and $aG = H'G'$ for some $F', G', H' \in K[x, y]$ and $a \in K[x]$ such that a is the polynomial consisting of the denominators from H that we cleared.

From $aF = H'F$, $aG = H'G$ we can see that every irreducible factor of a must divide H' or both F', G'. So we will get a new decomposition depending on which it can divide, where $F = H''F'$, $G = H''G'$ or $F = H''F'$, $G = H'G''$ where $H'', F'', G'' \in K[x, y]$. However, then as we can see that they are no longer coprime as they share the same factor H" or H' which is a contradiction. Therefore they must stay coprime in $K(x)[y]$.

Now $K(x)[y]$ is a PID because K(x) is a field and we have that if F is a field then $F[x]$ is a PID. As F,G are coprime in $K(x)[y]$ we can write 1 as a linear combination of F and G with coefficients in $K(x)[y]$. This follows from the fact that in a PID every ideal is generated by one element d, so $(F, G) = (d)$. Now $d = 1$ because F, G are coprime and the generator of an ideal in a PID must be a divisor of the other elements in the ideal since by definition, $(F, G) = (d) = \{r * d : r \in K(x)[y]\}$. By the fact that $F, G \in (F, G)$, d must divide both F and G. Therefore we have $1 = aF + bG$, $a, b \in K(x)[y]$. Note that since the left hand side is 1 which is independent of y and has degree 0, the right hand side must also degree 0 therefore the y-variables must be cancelled out. After clearing denominators from a and b, which are in $K[x]$, we get $c = DF + EG \in K[x]$.

For 2) let P $\in V(F, G)$. Then the c from a) would give us

$$c(P) = D(P)F(P) + E(P)G(P) = 0$$

So if $G(P), F(P) = 0$ then it must also be a root of c. Hence, any point in $V(F, G)$ is restricted to the finitely many zeroes of $c \in K[x]$. Since a) also held symmetry, there can also only be finitely many choices for the y-coordinate. So V(F,G) is finite. □

Corollary 3.4. *Corollary 1.13, Andreas Gathmann[1], page 10 Let F be a curve over an algebraically closed field. Then for any irreducible curve G we have $G \mid F \leftrightarrow V(G) \subset V(F)$.*

In particular, the irreducible components of F but not their multiplicities can be recovered from V(F).

Proof. $\Rightarrow$ Assume $F = GH$ for some curve H. If $P \in V(G)$, then we also have that $F(P) = G(P)H(P) = 0$, so $P \in V(F)$.

$\Leftarrow$ Assume $V(G) \subset$ V(F). Then $V(F, G) = V(G)$ is infinite since we are in an algebraically closed field. Since $V(F, G)$ is infinite, F and G must contain a common component since we already saw if they do not share a common component, $V(F, G)$ is finite.

We must now see that $G \mid F$. Factor F into its irreducible factors $(F_i)_i$ such that F $= F_1 * F_2 * \ldots * F_n$. Then $V(F) = V(F_1) \cup V(F_2) \cup \ldots \cup V(F_n)$. As G is irreducible we also have that $V(G)$ is irreducible, therefore $V(G) \subset V(F)$ implies that $V(G) = V(F_i)$ for some i. This follows from the fact that $V(G)$ is irreducible if it is as a polynomial, therefore it cannot be factored into smaller non-constant polynomials so translated to curves this implies $V(G)$ cannot be written as a union of smaller curves.

As $V(G) = V(F_i)$ for some i, we have that as polynomials $G = uF_i$ for some constant $u \in K^*$. From this we get that $G \mid F_i$ and $F_i \mid G$ as we know that in a UFD two irreducibles divide eachother if and only if $G = uF_i$ for some unit u. From $G \mid F_i$ it follows that $G \mid F$. □

So now we get that if two polynomials F and G have the same zero set, $V(F) = V(G)$ such that $V(F), V(G) \neq 0$ over an algebraically closed field then they can only be the same polynomial up to different multiplicity. To see that this follows, note that if $V(F) = V(G)$ then $V(G) \subset V(F)$ and $V(F) \subset V(G)$. Factor F and G into their irreducible components, $F = \prod_i F_i$, $G = \prod_j G_j$ so $V(F) = \cup_i V(F_i)$ and $V(G) = \cup_j V(G_j)$.

As $\cup_j V(G_j) = \cup_i V(F_i)$ and every G_j is irreducible, $V(G_j)$ corresponds to some $V(F_i)$ in $\cup_i V(F_i)$. Then we get that $F_i \mid G_j$ and $G_j \mid F_i$ so they differ only up to a unit. Do this for every irreducible factor, which we can do by the subset inclusions of both curves, we can conclude that F and G are the same polynomial up to units and therefore only differs by some multiplicity on the factors.

Remark 1.14 Specifying a curve by its set of points. (Andreas Gathmann [1], page 11)

So now we know that over an algebraically closed field we can specify a curve by its set of points by drawing them out in A^2 together with a multiplicity on each irreducible component to distinguish them. For example in the picture below we have $(x^2 + y^2 - 1)(x - y)^2$, K $= \mathbb{R}$.

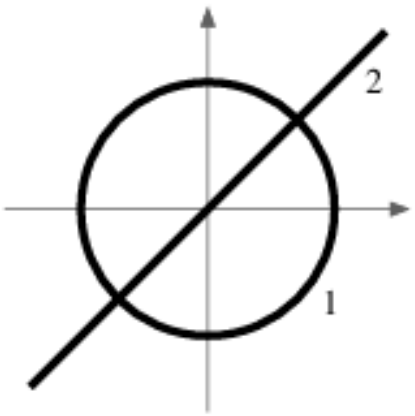


Figure 2

4 Intersection Multiplicities

We will now introduce the concept of intersection multiplicity. This is a generalization of the multiplicity of a zero of a univariate polynomial on the x-axis to any other point where two polynomials intersects as shown below in Figure 3 (K= $\mathbb{R}$). (Andreas Gathmann, page 12).

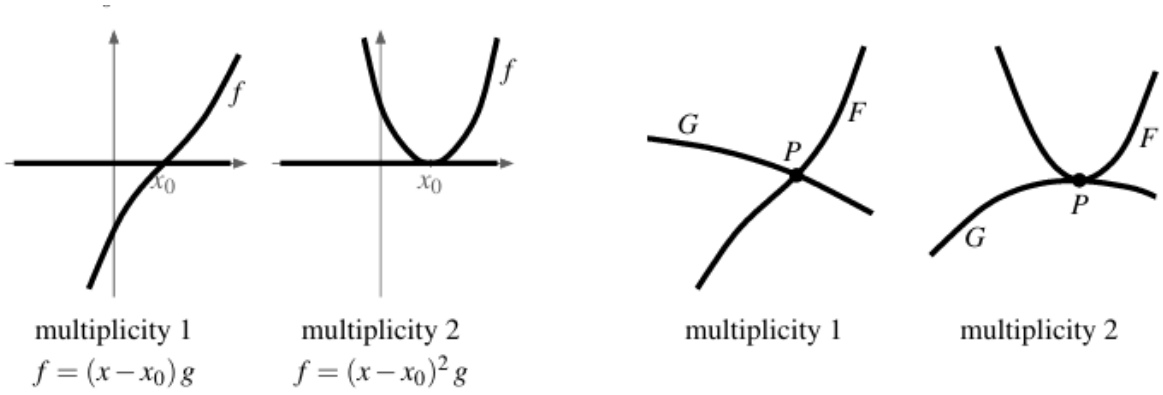


Figure 3

Now we will recall the definition of the univariate case of multiplicity of a zero to build up some geometric intuition. Let $f \in K[x]$ and $x_0 \in K$ is such that $f = (x - x_0)^m * g$ for a polynomial $g \in K[x]$ where $g(x_0) \neq 0$, then f has multiplicity m at x_0.The multiplicity is an approximation of how similar the graph is to the x-axis around the point x_0 when $f(x_0) = 0$.

Note that the multiplicity in the factorization of a polynomial in definition 3.1 and the multiplicity of the intersection f with the x-axis are the same number in the univariate case, the first definition with factorization is an algebraic viewpoint while the behaviour of the graph is the geometric viewpoint.

A multiplicity of 1 means that the graph of f intersects the x-axis transversely, while a

multiplicity of 2 means the graph of f is tangent to the x-axis at x_0. In general, as $m \to \infty$, the curve of F looks more and more like the x-axis at the point p, and if multiplicity is ∞ then f and the x-axis look exactly the same in a neighborhood around p.

Definition 4.1. Definition 2.1, Local rings of A^2, Andreas Gathmann[1], page 11

Let $P \in A^2$ be a point. The local ring of A^2 at P is defined as

$$O_P = \mathcal{O}_{A^2,P} = \left\{ \frac{f}{g} : f, g \in K[x,y], g(P) \neq 0 \right\}$$

This is a subring of K(x,y).

Proof. It contains 0 and 1 since

$$1 = \frac{1}{1}$$
$$0 = \frac{0}{1}$$

We also have that it is closed under addition and multiplication since

$$\frac{f}{g} + \frac{h}{k} = \frac{fk + gh}{gk}$$

$fk + gh \in K[x,y]$ as $K[x,y]$ is a ring, and

$$(gk)(P) = g(P)k(P) \neq 0$$

So $f + g \in O_P$. We can also see that $\frac{f}{g} * \frac{h}{k} = \frac{fh}{gk}$, where $fh \in K[x,y]$ and $(gk)(P) \neq 0$ so $fg \in O_P$ □

We also have a well-defined ring homomorphism $\mathcal{O}_\mathcal{P} \to K$, $\frac{f}{g} \to \frac{f(P)}{g(P)}$ which we call the evaluation map of the local ring at the point P. Its kernel is denoted by

$$I_P = I_{A^2,P} = \left\{ \frac{f}{g} : f, g \in K[x,y], f(P) = 0, g(P) \neq 0 \right\}$$

which is a subset of $\mathcal{O}_P$.

Proof. It is a homomorphism because

$$\mathrm{ev}_P\left(\frac{f}{g} + \frac{h}{k}\right) = \mathrm{ev}_P\left(\frac{fk + gh}{gk}\right) = \frac{fk(P) + gh(P)}{g(P)k(P)} = \frac{f(P)}{g(P)} + \frac{h(P)}{k(P)}$$

via the operations defined in $K[x,y]$.

To check well-defined, let $\frac{f}{g} = \frac{f'}{g'}$ in O_P. Then $fg' = f'g$ in K$[x,y]$. Evaluation at P gives us $f(P)g'(P) = f'(P)g(P)$, but then $\frac{f(P)}{g(P)} = \frac{f'(P)}{g'(P)}$ as wanted.

The kernel follows from definition, it is the set

$$\left\{ \frac{f}{g} \in O_P : \frac{f(P)}{g(P)} = 0 \right\}$$

which gives us that $f(P) = 0$, $g(P) \neq 0$.

□

Geometrically, the local ring $\mathcal{O}_P$ is the ring of rational functions that are well-defined at P where we can see how they behave in a small neighborhood of p.

Algebraically, $\mathcal{O}_P$ is a subring of $K(x,y)$ that also contains $K[x,y]$, because if $f \in K[x,y]$ then $f = \frac{f}{1}$. As a subring of a field, it is an integral domain and its units are precisely the fractions $\frac{f}{g}$ for which both f and g are non-zero at P, as then $\frac{f}{g}, \frac{g}{f} \in \mathcal{O}_P$ and $\frac{f}{g} * \frac{g}{f} = 1$

In a different view, we can regard $\mathcal{O}_P$ as the localization of $K[x,y]$ with the multiplicatively closed set $S = K[x,y] \setminus I_P$ where we have that I_P is the ideal $(x - x_0, y - y_0)$ for $P = (x_0, y_0)$, it is denoted $K[x,y]_{(x-x_0,y-y_0)}$. Note that this is the set

$$\left\{ \frac{f}{g} : f \in K[x,y], g \in S \} = \{ \frac{f}{g} \in K[x,y] : g(P) \neq 0 \right\}$$

which is the same as what we defined $\mathcal{O}_P$ to be.

Definition 4.2. Definition 2.3, Intersection multiplicities, Andreas Gathmann[1], page 13
For a point $P \in A^2$ and two curves F, G we define the intersection multiplicity of F and G at P to be

$$\mu_P(F,G) = \dim \mathcal{O}_P/(F,G) \in N \cup \{\infty\}$$

where dim denotes the dimension as a vector space over K.

The intuition is the same as in the univariate case with the x-axis, but now the multiplicity approximates how similar the graphs are to each other around the point they intersect in where a multiplicity of 1 implies that they traverse each other and as $m \to \infty$, the graphs looks more alike. If $m = \infty$, they look exactly the same around a small neighbourhood of the point.

Example calculation

Let $F = y$ and $G = y - x^2$ in $K[x,y]$. We can see that they intersect at $(0,0)$. Consider $O_{(0,0)} \setminus (F,G)$ where

$$(F,G) = \{a * y + b * (y - x^2) : a, b \in O_0\}$$

As $(F,G) = (y, y - x^2)$, in $O_0 \setminus (F,G)$ we have that $y = x^2$ since $y - x^2 = 0$ therefore we can rewrite (F,G) to (x^2). Note that only terms of 1 and x survive, as every term of y is modded out to 0, as well as every term of x^n for $n \geq 2$ since $x^n = x^{n-2} * x^2$ which is 0 in the quotient.

So we get that $\mu_0(y, y - x^2) = \dim \mathcal{O}_0/(y, y - x^2) = 2$

Example general calculation

As every element in $O_p/(F,G)$ can be embedded into $K[[x,y]]$, the formal power series ring around the origin (0,0) after a coordinate translation of the point p, we can now see the general calculations using Gröbner basis from the preliminaries.

W.L.O.G we will continue with the example from the preliminaries with $F = x^2 - y$ and $G = xy - 1$, as we either have that the calculations of its Gröbner basis is equivalent to the Gröbner basis of $(F, G) \in K[[x, y]]$ or the dimension is infinite as shown in the preliminaries.

We have $(F, G) = (x^2-y, 1-xy)$ and we can see that they intersect in the point $(1, 1)$. By the calculations from preliminaries a reduced Gröbner basis for the ideal is $F' = \{1-y^3, x-y^2\}$. Therefore every element $H \in K[x, y]$ can be written as $H = a*F+b*G+r$ for $a, b \in K[x, y]$ and $r = 0$, or r does not divide the leading term of any element in the Gröbner basis of $1 - y^3$ and $x - y^2$.

Now $LT(1 - y^3) = y^3$, $LT(x - y^2) = x$ by the $x >_{lex}$ ordering. We see that the only monomials that do not divide any of the leading terms are 1, y and y^2. Note that these remainders are exactly the representatives of the cosets in $K[x, y]/(F, G)$, which is a vector space by definition of the quotient being a ring (so it is an abelian group) and we have for all $k \in K$ that

$$k * (f + I) = (kf) + I$$

which give us a scalar action. In this case,

$$\mu_{(1,1)}(F, G) = \dim O_{(1,1)}/(F, G) = 3$$

Therefore, for any two curves $F, G \in K[x, y]$ find the Gröbner basis for their ideal (F, G) in $K[[x, y]]$, then calculate the remainders modulo the leading terms of the Gröbner basis to get the dimension of $O_P/(F, G)$ as shown above. If the Gröbner basis is infinite, the dimension is infinite.

Remark 2.4. (Andreas Gathmann[1], page 13)

1) The invertible affine coordinate transformation (x,y) to $(x', y') = (ax+by+c, dx+ey+f)$ for $a, b, c, d, e, f \in K$ with $ae - bd \neq 0$ is an isomorphism between the local rings O_p and $O_{p'}$.

   As this map let us evaluate every polynomial from (x, y) to (x', y'), it follows that we get an induced isomorphism of $O_P \setminus (F, G)$ to $O_{P'} \setminus (F', G')$ where F' and G' are F, G expressed in the new coordinates x' and y'. Note that this is the same quotient group but viewed from another perspective.

2) The intersection multiplicity is symmetric, so $\mu_P(F, G) = \mu_P(G, F)$ for all F and G.

3) For all F, G, H we have $(F, G + FH) = (F, G)$, so $\mu_P(F, G + FH) = \mu(F, G)$.

Proof. For the second statement we can see that as K is a field it is a commutative ring therefore $K[x, y]$ is a commutative ring so we have that

$$(F, G) = \{aF + bG : a, b \in K[x, y]\} = \{bG + aF : a, b \in K[x, y]\} = (G, F)$$

It follows by definition of quotient calculations that

$$\begin{aligned} &= (f + g) + \mathcal{O}_{\mathcal{P}} \\ &= (g + f) + \mathcal{O}_{\mathcal{P}} \\ &= (g + \mathcal{O}_{\mathcal{P}}) + (f + \mathcal{O}_{\mathcal{P}}) \end{aligned}$$

As for the third statement, take any $h \in (F, G)$. Then

$$\begin{aligned} h &= aF + bG \\ &= aF + b(G + FH - FH) \\ &= aF + b(G + FH) - bFH \\ &= (a - bH)F + b(G + FH) \end{aligned}$$

So $(F, G) \subset (F, G + FH)$. Now for any $h \in (F, G + FH)$ we have

$$\begin{aligned} h &= aF + b(G + FH) \\ &= aF + bG + bFH \\ &= (a + bH)F + bG \end{aligned}$$

So $(F, G + FH) \subset (F, G)$. Therefore we have that

$$\mathcal{O}_{\mathcal{P}} \setminus (F, G) = \{f + (F, G) : f \in \mathcal{O}_{\mathcal{P}}\} = \{f + (F, G + FH) : f \in \mathcal{O}_{\mathcal{P}}\}$$

as the ideals contain the same elements. □

Construction 2.9. Short exact sequences. (Andreas Gathmann[1], page 14)

A sequence $0 \to U \xrightarrow{\phi} V \xrightarrow{\psi} W \to 0$ of linear maps between vector spaces, where 0 denotes the zero vector space, is exact if the image of each map equals the kernel of the next.

In other words, it is exact if $\ker \phi = 0$, so ψ is injective, and $\operatorname{im} \phi = \ker \psi$ and $\operatorname{im} \psi = W$, so ψ is surjective.

We also get a dimension formula $\dim V = \dim U + \dim W$. Note that this comes from the dimension formula for vectors spaces where

$$\begin{aligned} \dim V &= \dim \ker \psi + \dim \operatorname{im} \psi \\ &= \dim \operatorname{im} \phi + \dim W \\ &= \dim U + \dim W \end{aligned}$$

since ϕ is surjective and $\ker(\phi) = \operatorname{im}(\psi) \cong U$ by injectivity.

Proposition 4.3. *Proposition 2.10, Additivity of intersection multiplicities (Andreas Gathmann[1], page 14)*

Let $P \in A^2_K$ and let F, G, H be three curves.

1) If F and G have no common component through P there is an exact sequence

$$0 \to O_P \setminus (F, H) \xrightarrow{G} O_P \setminus (F, GH) \xrightarrow{\pi} O_P \setminus (F, G) \to 0$$

where π is the natural quotient map and G is the multiplication map by G, so $f + (F, H) \to Gf + (F, GH)$

2) We have that $\mu_P(F, GH) = \mu_P(F, G) + \mu_P(F, H)$.

Proof. Following Gathmann we can see that for 1), as we know that π is well-defined, we only need to check that G is a well-defined map. First we need to see that it is a homomorphism.

$$\begin{aligned} G((a + (F, H) + (b + (F, H))) &= G((a + b) + (F, H)) \\ &= G(a + b) + (F, GH) \\ &= Ga + Gb + (F, GH) \\ &= (Ga + (F, GH) + (Gb + (F, H)) \end{aligned}$$

since $O_P \setminus (F, GH)$ is a ring. Let $f + (F, H) = f' + (F, H)$. Then $f - f' \in (F, H)$. $G(f - f') = aFG + bHG = (aG)F + b(GH) \in (F, GH)$, therefore $G(f - f') = 0$, but this is the same as $G(f) - G(f') = 0$ as G is a homomorphism, so $G(f) = G(f')$.

To see that this is an exact sequence, first we need that G is injective. Assume $\frac{f}{g}$ is in the kernel, so $\frac{f}{g} * G = \frac{f'}{g'} * F + \frac{f''}{g''} * GH$ for some $f', f'', g', g'' \in K[x, y]$ with $g'(P)$, $g''(P)$ nonzero. W.L.O.G we can assume all three fractions have the same denominator. Multiplying by this denominator we obtain the equation $fG = f'F + f''GH \in \mathcal{O}_\mathcal{P}$. From $fG = f'F + f''GH$ we get $G(f - f''H) = f'F$. As G divides the lefthand side, it must also divide the righthand side. Therefore it must also divide $f'F$ but since G and F have no common component G must divide f'. So $f' = aG$ for some $a \in K[x, y]$. We then get $fG = aFG + f''GH$. Divide by G and we have $f = aF + f''H$, so f must be in (F, H) in $O_P \setminus (F, H)$, that is f is zero. So the kernel is trivial.

Now we want that im $G = \ker \pi$. By definition, we want that

$$\text{im } G = \{Gf + (F, GH) : f \in O_P\}$$

is equal to the kernel of π which are all elements $Gf + (F, GH)$ such that

$$\pi(Gf + (F, GH)) = Gf + (F, G) = 0 + (F, G)$$

For the first inclusion, im G $\subset$ ker π, note that as G is already in (F, G), we get that $Gf \in (F, G)$ for all $f \in O_p$. For the second inclusion, ker $\pi \subset$ im G, let f $\in$ ker π. So f = f' + (F,GH) such that f' $\in (F, G)$. Therefore f' = aF + bG for $a.b \in \mathcal{O}_\mathcal{P}$. Then we get that

$$\begin{aligned} f &= (aF + bG) + (F, GH) \\ &= (aF + (F, GH)) + (bG + (F, GH)) \\ &= bG + (F, GH) \end{aligned}$$

Note that this is in im G for b $\in \mathcal{O}_\mathcal{P}$, therefore any element in the kernel of π can be written as an elements in the image of G.

The map π we already know is surjective. So exactness is showed.

For 2) by taking dimensions we get that

$$\dim O_P \setminus (F, GH) = \dim O_P \setminus (F, H) + \dim O_P \setminus (F, G)$$

If $\mu_P(F, GH)$ is finite, we can use construction 3.9 with exact sequences immediately, by plugging in the dimension formula $\dim V = \dim W + \dim U$ on the given function in 1).

If $\mu_p(F, GH)$ is infinite, we first need to solve exercise 3.10.

Lemma 3.10 (Exercise 3.10) Let F and G be two curves that pass through the origin.

1): If F and G have no common component, then the family $(F^n)_{n\in N}$ is linearly independent in $O_0 \setminus (F, G)$,

Suppose by contradiction that there exists coefficients $a_0, .., a_n$ not all zero such that

$$a_0 + a_1 * F + \ldots + a_n * F \in (G)$$

and let k be the smallest index such that $a_k \neq 0$. Then we can rewrite it to

$$F^k(a_k + a_{k+1} + \ldots + a_n * F^{n-k} \in (G)$$

Now we know that F^k is not divisible by G since they share no common component, so we can conclude that $a_k + a_{k+1}F + \ldots + a_nF^{n-k} \in (G)$.

As $F(0, 0) = 0$, evaluating $a_k + a_{k+1}F + \ldots + a_nF^{n-k}$ at $(0, 0)$ gives us a_k. However, anything in (G) must vanish at the origin since G does. Therefore $a_k = 0$, which gives us a contradiction. We can then conclude that all coefficients $a_i = 0$ and the family is linearly independent.

2): If F and G have a common component that passes through the origin then $\mu_0(F, G) = \infty$.

Assume F and G have a common component H passing through the origin. Rewrite $F = H * F'$, $G = H * G'$ for some F', G' in $K[x, y]$.

Now we can consider the quotient ring homomorphism

$$\phi : O_0 \setminus (F, G) \to O_0 \setminus (H)$$

where $f + (F, G) \to f + (H)$. As that $(F, G) \subset (H)$ as (F) $\subset (H), (G) \subset (H)$ so we get that this is a well-defined map. Note that if f+(F,G) = g+(F,G) then f-g $\in (F, G)$, as (F,G) $\subset (H)$ we get that f-g $\in (H)$ so f+(H) = g+(H). Surjectivity follows by definition of the map.

Therefore we can conclude

$$\dim O_0 \setminus (F, G) \geq \dim O_0 \setminus (H)$$

All we need to do is to find a curve F with no common component with H, to get a family $\{F^n\}_{n\in N}$ that is linearly independent in $O_0 \setminus (H)$, which will give us that the dimension is infinite. As H is a polynomial of degree d, we know it can have at most d linear factors since multiplying the factors must result in degree d again. Now any line through L is determined by its direction given by the equation $y = \lambda x$, $\lambda \in K$, and we know there are infinitely many, so after excluding finitely many that is included in H, we can choose any other line. Denote this line as F and apply 1) to get that we have a linearly independent family $\{F^n\}_n$.

Note that as they are linearly independent, each F^n give a unique coset and therefor dim $O_0 \setminus (H) = \infty$ and we have that dim $O_0 \setminus (F, G)$ is infinite aswell, and we get that $\infty = \infty$.

Going back to 2) we now have that if $\mu_P(F, GH) = \infty$ then F must share a common component with GH. Therefore $F = LF'$ and $GH = LK$ for some polynomials F', K. Factorize L into its irreducible components. Then each factor of L must divide either G or H. W.L.O.G take one factor that divides G. Then G and F shares this common factor of L. Now apply the steps in exercise 3.10 with H replaced with this factor and we get our statement. $\square$

5 Projective Curves

We will now go from local intersection to the global situation, where we are interested in the quuestion of how many intersection points can two curves have in total, or in other words how many common zeroes can we find for two polynomials $F, G \in K[x, y]$ where we count each zero with its intersection multiplicity. For this, we shall work in the projective plane.

3.1. Projective plane

Remark 5.1. Remark 3.1, (Andreas Gathmann[1], page 21) Geometric idea

The idea for adding points at infinity is to first embed the affine space A^n in the vector space K^{n+1} by $(x_1, \ldots, x_n) \to (1, x_1, \ldots, x_n)$, where the first coordinate is set to 1.

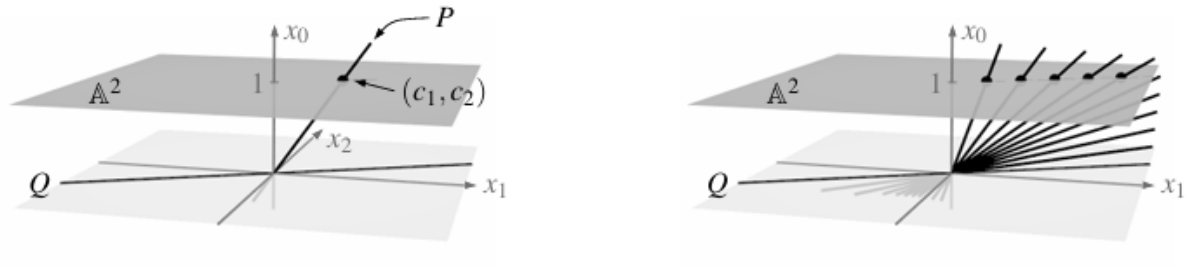


Figure 4

In Figure 4 we can see that a point (c_1, c_2) in A^2 corresponds to the line through origin and $(1, c_1, c_2)$ in K^3.

The projective plane is defined to be the set of all such 1-dimensional linear subspaces in K^3 together with the lines through origin contained in the coordinate $x_0 = 0$ as seen in the picture above.

The lines where $x_0 = 0$ are going to be our points of infinity in the projective plane. Note that the picture on the right illustrates that these lines can be seen as limits of lines coming from an unbounded sequence of points in A^2.

Definition 5.2. Definition 3.2, Projective Spaces (Andreas Gathmann [1], page 22)
For $n \in \mathbb{N}$ we define the projective n-space over K as the set of all 1-dimensional linear subspaces of K^{n+1}, and is denoted P^n_K or P^n

Now, $P^n = (K^{n+1} \setminus 0)/\sim$, where $\sim$ is

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) \leftrightarrow x_i = \lambda y_i$$

for some $\lambda \in K^*$, $\lambda \neq 0$ and all i. This is due to the fact that a 1-dimensional linear subspace of K^{n+1} is uniquely determined by a spanning non-zero vector in K^{n+1} where two vectors give the same linear subspace if and only if they are scalar multiples of each other.

The elements are therefore equivalence classes and will be denoted by $(x_0 : x_1 : \ldots : x_n)$ from now on.

Remark 3.4 Geometric interpretation of P^n. (Andreas Gathmann[1], page 22)

Our first interpretation is that we may regard P^n as $A^n \cup P^{n-1}$ where A^n is the affine part of P^n, and P^{n-1} the infinite part of P^n. In our case, this is how we will mostly regard P^n when working in it.

As we can embed A^n into P^n by the map $(x_1, \ldots, x_n) \to (1 : x_1 : \ldots : x_n)$, we can consider A^n to be a subset of P^n as its image of this map which is the set $U = \{(x_0 : x_1 : \ldots : x_n) : x_0 \neq 0\}$. The remaining points are $(0 : x_1 : \ldots : x_n)$ and correspond to a set that is naturally isomorphic with the set of 1-dimensional linear subspaces of K^n; merely disregard the 0 and send $(0 : x_1 : \ldots : x_n) \to (x_1 : \ldots : x_n)$.

An example of this is P^2 where we have that $P^2 = A^2 \cup P^1$ where P^1 is the set of all 1-dimensional subspaces of K^2.

The second interpretation is that we can split P^n into n different copies of A^n. This will be done by constructing so called patches defined as $U_i = \{(x_0 : \ldots : x_n) : x_i \neq 0\}$. We will show that it is naturally bijective to A^n for each i.

For any fixed i, divide by x_i to get $(\frac{x_0}{x_i} : \ldots : 1 : \ldots : \frac{x_n}{x_i})$. Note that equivalence classes under this division will correspond to only one point in A^n. To see this, consider let $(x_1 : \ldots : x_i : \ldots : x_n)$ and $(\lambda x_1 : \ldots : \lambda x_i : \ldots : \lambda x_n)$. As they are both nonzero in the i-th place we can divide to get 1, so we have $(\frac{x_1}{x_i} : \ldots : 1 : \ldots : \frac{x_n}{x_i})$ and $(\frac{\lambda x_1}{\lambda x_i} : \ldots : 1 : \ldots : \frac{\lambda x_n}{\lambda x_i})$. Then we can see that λ cancels out and we have the same point. As we let x_i range over all elements of K, U_i will be naturally isomorphic to A^n.

As in chapter 2, we would like to work with subsets of P^n defined by polynomial equations, However, polynomials in general are not well-defined functions on P^n, as two points in the same equivalence class can give different images. For instance, let $f = x_0^2 + x_1$, then if we take the equivalence class $(-1 : 1) \in P^n$ we have that $f(-1, 1) = 2$ and $(1, -1) = 0$.

Remark 3.7 Homogeneous polynomials (Andreas Gathmann[1], page 23)

Let

$$f = \sum_{i_0+\ldots+i_n=d} a_{i_0,\ldots,i_n} \lambda^{i_0+\ldots+i_n} x_0^{i_0} \ldots x_n^{i_n} \in K[x_0, \ldots, x_n]$$

be a homogeneous polynomial of degree d. This means that every term has degree d.

Then we have that

$$f(\lambda x_0, \ldots, \lambda x_n) = \sum_{i_0+\ldots+i_n=d} a_{i_0,\ldots,i_n} \lambda^{i_0+\ldots+i_n} x_0^{i_0} \ldots x_n^{i_n} = \lambda^d f(x_0, \ldots, x_n)$$

From this we can see that $f(\lambda x_0, \ldots, \lambda_n) = 0 \Leftrightarrow f(x_0, \ldots, x_n) = 0$ for all $\lambda \in K^*$. So if f is a homogeneous function, it's zero locus is well-defineda as $0 = 0 * \lambda^d$ for all $\lambda \in K^*$.

We can also see that if g is another homogeneous polynomial of degree d then

$$\frac{f(\lambda x_0, \ldots, \lambda x_n)}{g(\lambda x_0, \ldots, \lambda x_n)} = \frac{\lambda^d f(x_0, \ldots, x_n)}{\lambda^d g(x_0, \ldots, x_n)} = \frac{f(x_0, \ldots, x_n)}{g(x_0, \ldots, x_n)}$$

We conclude that the quotient $\frac{f}{g}$ is a well-defined function on the subset of P^n as long as g does not vanish.

Definition 5.3. Definition 3.8, Projective varieties (Andreas Gathmann[1], page 23)
For a subset $S \subset K[x_0, \ldots, x_n]$ of homogeneous polynomials we call

$$V(S) = \{P \in P^n : f(P) = 0 \forall f \in S\} \subset P^n$$

the projective zero locus of S. Subsets of P^n that are of this form are called projective varieties. To distinguish this from the affine zero locus, we can denote it by $V_P(S) \subset P^n$, and the affine zero locus as $V_a(S)$.

Remark 3.9 (Andreas Gathmann[1], page 24)

For any two homogeneous polynomials $f, g \in K[x, y, z]$ we have that $V(f) \cup V(g) = V(fg)$ and $V(f) \cap V(g) = V(f, g)$, following from Remark 1.4 by restricting us to homogeneous polynomials in $K[x, y, z]$ as well as the identities from De Morgan Laws established in the affine space, as the zero sets of homogeneous polynomials in P^n are well-defined as shown above.

We can also introduce the Zariski topology in the projective space with the closed sets being the projective varieties, which is the topology we will work with and it is shown to be a topology exactly the same as we saw for the affine case by the restriction to homogeneous polynomials.

Lemma 3.11 (Exercise 3.11)

1) If $F, G \in K[x_1, \ldots, x_n]$ are polynomials such that $F \mid G$, G homogeneous then F is homogeneous.

As F divides G, we have that $G = F * H$ for some $H \in K[x_1, \ldots, x_n]$. Every polynomial can be decomposed into its homogeneous parts since every monomial have a well-defined degree. Therefore we can write $F = \sum_i F_i$ and $H = \sum_j H_j$ for their corresponding homogeneous decomposition.

Then $G = FH = \sum_{i,j} F_i * H_j$. As G is homogeneous, all terms are of the same degree d. Therefore $i + j = d$ for all i and j.

We claim that i is the same number for all terms. If not, let i, i' be such that $i \neq i'$. Then in the product, when we multiply F_i and $F_{i'}$ with the same H_j we get that

$$\deg F_i * H_j \neq \deg F_{i'} * H_j$$

that is $i + j \neq i' + j$. But then only one of those are of degree d, so G contains a term with a degree $\neq d$, which is a contradiction.

2) Every homogeneous polynomial in two variables over an algebraically closed field is a product of linear terms.

Let K be algebraically closed and $f \in K[x, y]$ be a homogeneous polynomial. We shall use that over $K[x]$, every f splits into a factor of linear products. To see this, note that as K is algebraically closed, it has a root. We can then rewrite $f = (x - a) * f'$ where $f' \in K[x]$ and deg f' <deg f. Since K is algebraically closed, we have that $f' = (x - b) * f''$ for some

$f'' \in K[x]$ with deg f'' < deg f. So $f = f'' * (x-a)(x-b)$. Repeating the process until the degree terminates, we shall receive a product of linear terms.

Let $F(x,y) \in K[x,y]$ be homogeneous of degree n. If $y \neq 0$ then set $y = 1$ to get the univariate polynomial $F(x,1) = F(t) \in K[x]$. By the proof above, we can factor $F(t)$ into a product of linear terms

$$f(t) = \prod_{i=1}^{n}(t - a_i), \text{ for } a_1, \ldots, a_n \in K$$

Now we want to reintroduce the y variable to lift F back up to a homogeneous polynomial. Set $t = \frac{x}{y}$, and we get that $t - a_i = \frac{x - a_i y}{y}$. Thus

$$\begin{aligned} F(x,y) &= \{ \text{ by homogeneity } \} \\ &= y^n F(\frac{x}{y}, 1) \\ &= y^n F(\frac{x}{y}) \\ &= y^n \prod_{i=1}^{n}(\frac{x}{y} - a_i) \\ &= \prod_{i=1}^{n}(x - a_i y) \end{aligned}$$

Therefore it is a product of linear terms and we have what we wanted.

Definition 5.4. Definition 3.12, Projective curves (Andreas Gathmann[1], page 24)

1) A projective plane algebraic curve over K is a non-constant homogeneous polynomial $F \in K[x,y,z]$ modulo units. We call $V(F) = \{P \in P^2 : F(P) = 0\}$ its set of points.

2) The degree of a projective curve is its degree as a polynomial

3) The notions of irreducible, reducible and reduced curves, as well as of irreducible components and their multiplicities, are defined in the same way as for affine curves in Definition 1.5

Well-definedness follows from the same proof as in the affine case, therefore the degree is well-defined up to scalars as well as irreducibility.

To study projective curves, we would often like to relate them to affine curves. To do this, we need the following construction.

Construction 3.13 Homogenization and dehomogenization. (Andreas Gathmann[1], page 24).

1) For a nonzero polynomial $f = \sum_{i+j \leq d} a_{i,j} x^i y^j \in K[x,y]$ of degree d we define the homogenization of f as

$$f^h = \sum_{i+j \leq d} a_{i,j} x^i y^j z^{d-i-j} \in K[x,y,z]$$

Here we multiply with the variable z to make the polynomial homogeneous in $K[x, y, z]$ of degree d. For example, $x^3 + y^2 + 3 \in K[x, y]$ and the degree of f is 3. Its homogenization is $x^3 + yz^2 + 3z^3$ and the degree is still 3.

Note that f^h is homogeneous of degree $f^h = degf = d$ and that z does not divide f^h since f contains a term with $i + j = d$, as we keep the leading term in $K[x, y]$ so it is not divisible by z.

2) For a non-zero homogeneous polynomial

$$f = \sum_{i+j+k=d} a_{i,j,k} x^i y^j z^k \in K[x, y, z]$$

of degree d we define the dehomogenization of f to be

$$f^i = f(z = 1) = \sum_{i+j+k=d} a_{i,j,k} x^i y^j \in K[x, y]$$

Here we just set $z = 1$ to get a polynomial in $K[x, y]$. In general, f^i will be an inhomogeneous polynomial. We also have a bijective correspondence between polynomials of degree d in $K[x, y]$ with homogeneous polynomials of degree d in $K[x, y, z]$ not divisible by z via the maps $f \to f^h$ and $f^i \to f$.

Proof. Let f $\in K[x, y]$ such that f is of degree d. After homogenization it will be a polynomial in $K[x, y, z]$ with degree d with its leading term not divisible by z. So f^h is homogeneous of degree d $\in K[x, y, z]$ not divisible by z. Let f $\in K[x, y, z]$ homogenenous of degree d not divisible by z. Then some term of f must be a monomial in $K[x, y]$ of degree d. Then f^i is a polynomial in $K[x, y]$ of degree d. Therefor we have inclusions both ways and surjectivity follows. Now it is easy to see that if f=f' in $K[x, y, z]$ not divisible by z, $f^i = f'^i$ so injectivity follows. □

Construction 3.15. Affine parts and projective closures. (Andreas Gathmann[1], page 25)

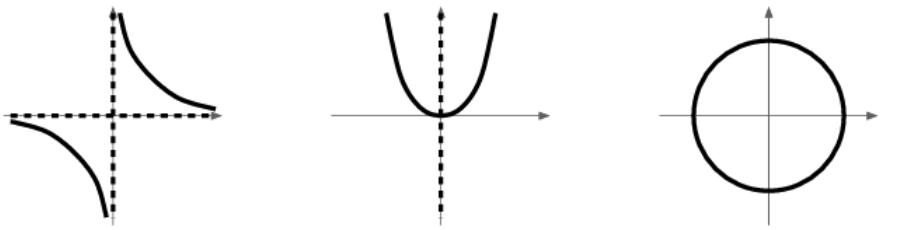
1) For a projective curve F, its affine set of points is $V_P(F) \cap A^2 = V_a(F(z = 1)) = V_a(F^i)$. So F^i is the affine part of F, and the points of infinity are given by $V_P(F(z = 0)) \subset P^1$ as in the picture in Remark 3.1 when we constructed projective plane.

2) For an affine curve F we call F^h its projective closure. It is the smallest projective curve that contains the original affine curve, so it is what we get after adding missing points at infinity.

Example 3.16. Visualization of projective curves. (Andreas Gathmann[1], page 25).

To visualize a projective curve F, we can just draw its affine set of points $V_a(F^i)$ and if it has a point at infinity, we will draw out the direction of it in A^2. As every equivalence class has a representative in A^2, the curve will look the same as in the affine part except with a point at infinity, which by construction is a direction in P^1.

For Figure 5 below (K=$\mathbb{R}$, following construction 3.15 we can see in (a) that the curve of $F = xy - 1$ is $xy - 1 = 0$, $xy = 1$. $x = 1/y$, $y = 1/x$, and after the projective closure, the point at infinity is $xy - z^2 = 0$, $x = 0$, $y = 0$. So the points at infinity is equivalence class



(a) hyperbola
$F = xy - 1$
$F^{\mathrm{h}} = xy - z^2$
points at infinity: $xy = 0$

(b) parabola
$F = y - x^2$
$F^{\mathrm{h}} = yz - x^2$
points at infinity: $x^2 = 0$

(c) ellipse
$F = x^2 + y^2 - 1$
$F^{\mathrm{h}} = x^2 + y^2 - z^2$
points at infinity: $x^2 + y^2 = 0$

Figure 5

$(0 : 1 : 0)$ and $(1 : 0 : 0)$. Hence we have two points of infinity in P^1.

For (b) we have that the curve of $F = y - x^2 = 0$ is $y = x^2$, and its point of infinity on $F^h = yz - x^2$ is $F^h(z = 0) = -x^2 = 0$ so $x = 0$. So then we have $(0 : 1 : 0)$, the whole y-axis.

For (c) we have $F = x^2 + y^2 - 1$ so $x^2 + y^2 - 1 = 0$ which gives us $x^2 + y^2 = 1$. So the curve is the circle. Now $F^h = x^2 + y^2 + z^2$, so the points on infinity $z = 0$ is $x^2 + y^2 = 0$. Hence, the points of infinity is the set of points $(x : y : 0)$ that satisfy this equation.

Remark 3.18. Finiteness of zero locus. (Andreas Gathmann[1], page 26).

Let F and G be two projective curves. The finiteness results of Lemma 1.11 also holds for the affine parts of F and G which we will see by using that $V(F) = V_a(F) \cup \{\text{points at infinity}\}$. For the first statement, if $V_a(F)$ is infinite then adding more points is still infinite.

We wish to see now that the points of infinity for any projective curve is a finite set of points. As the points of infinity of a given curve F is given by z=1, we have seen before that finding them comes down to the equation $f^i(x, y) = 0 \in K[x, y]$. This is a polynomial in two variables, by lemma 3.11 we have that in an algebraically closed field it can be written as a product of linear terms. Therefore, $f^i(x, y) = \prod_{i=1}^{d}(a_i x + b_j y)$. Each linear factor give rise to a root $(x : y) \in P^1$ satisfying $a_i x + b_j y = 0$. Therefore, there are at most the degree of F many roots which we know is finite.

For the second statement, if $P^2_K \setminus V_a(F)$ is infinite, as the points of infinity are only finitely many, removing them aswell from an infinite set will not change anything.

We can also see that statement 2 of Proposition 1.12 also holds since $V(F, G) = V_a(F, G) \cup \{$ common points at infinity $\}$, which is a union of finite points therefore it is finite.

We can now restate a result from chapter 2, but for projective curves.

Remark 3.19 Recovering F from $V(F)$. (Andreas Gathmann[1], page 26).

Recall from chapter 2 that in an algebraically closed field, every polynomial sharing the same zero set must be a multiple of F or F with different multiplicities on components. We want to do the same but in the projective case.

Assume $V(F), V(G) \subset P^2$ and $V(F) = V(G)$. Consider F^i and G^i. Then it follows that $V(F^i) = V(G^i) \in A^2$. Then we know that F^i and G^i are the same polynomial up to different multiplicities. Therefore we can write $F^i = c\prod_j (G^i_j)^{a_j}$ where G^i_j are the irreducible components of G^i with their multiplicities.

Now we wish to see that homogenization preserves factorization. Let f and g be two polynomials such that f = $\sum a_{ij]x^iy^j}$ with i+j=d, h = $\sum b_{k,l}x^ky^l$ with k+l = d'. Then

$$f^h = \sum a_{i,j}x^iy^jz^{d-(i+j)}$$

by the definition of homoenization. Likewise,

$$g^h = \sum b_{k,l}x^ky^lz^{d'-(k+l)}$$

Then

$$\begin{aligned}(f^h)(g^h) &= (a_{ij}x^iy^jz^{d-(i+j)})(b_{kl}x^ky^lz^{d'-(k-l)}) \\ &= \sum a_{ij}b_{kl}x^{i+k}y^{k+l}z^{d+d'-(i+k+j+l)}\end{aligned}$$

Also $fg = \sum a_{ij}b_{kl}x^{i+k}y^{j+l}$ with degree $i+k+j+l = d+d'$, so

$$(fh)^h = \sum a_{ij}b_{kl}x^{i+k}y^{j+l}z^{(d+d'-(i+j+k+l))}$$

So we have that $f^h * g^h = (fg)^h$ and factors are preserved. Therefore we can conclude that F and G are the same polynomial up to different multiplicities again if their zero set coincide in the projective space.

Construction 3.20. Local rings of P^2. (Andreas Gathmann[1], page 26)

For $P \in P^2$ we define the local ring of P^2 at P as

$$O_{P^2,P} = O_P = \left\{ \frac{f}{g} : f, g \in K[x,y,z] \right\}$$

homogeneous of the same degree with $\{g(P) \neq 0\} \cup \{0\} \subset K(x,y,z)$.

As in definition 2.1, these rings admit a well-defined evaluation map $O_P \to K, \frac{f}{g} \to \frac{f(P)}{g(P}$ with kernel

$$I_P = I_{P^2,P} = \left\{ \frac{f}{g} \in O_P : f(P) = 0 \right\} \subset O_P$$

Proof. So let $\frac{f}{g} \sim \frac{f'}{g'}$. Using the localization view of O_P so we can see that $\frac{f}{g} \sim \frac{f'}{g'}$ if and only if there exist a $h \in S = K[x,y] \setminus I_P$ such that $h * (fg' - f'g) = 0$, $h(P) \neq 0$.

As $h(P)(f(p)g'(P) - f'(P)g(P)) = 0 \in K$, and $h(P) \neq 0$ we get that $f(P)g'(P) - f'(P)g(P) = 0$ so $\frac{f(P)}{g(P)} = \frac{f'(P)}{g'(P)}$.

□

For a point $P = (x_0 : y_0 : 1)$ in the affine part of P^2 there is an isomorphism

$$O_{P^2,(x_0:y_0:1)} \to O_{A^2,(x_0,y_0)}$$

where $\frac{f}{g} \to \frac{f^i}{g^i}$ which is compatible with the evaluation maps as we can easily see as we already know that $f(x, y, 1) = f^i(x, y)$.

Therefore we are given a commutative diagram:

$$\begin{array}{ccc} \mathcal{O}_{P^2,(x_0:y_0:1)} & \longrightarrow & \mathcal{O}_{A^2,(x_0,y_0)} \\ \downarrow eval & & \downarrow eval \\ K & \xrightarrow{inclusion} & K \end{array}$$

Note further that this also maps $I_{P^2,(x_0:y_0:1)}$ to $I_{A^2,(x_0,y_0)}$.

Construction 3.21 Intersection multiplicites. (Andreas Gathmann[1], page 26)

A the homogeneous polynomials of $K[x, y, z]$ are not elements of O_{P^2}, we must first define the ideal

$$(F_1, \ldots, F_k) = \left\{ \begin{array}{l} \frac{f_i}{g_i} * F_1 + \cdots + \frac{f_k}{g_k} * F_k : f_i = 0 \text{ or } f_i, g_i \in K[x, y, z] \text{ homogeneous with} \\ g_i(P) \neq 0 \text{ and } \deg(f_i F_i) = \deg(g_i) \forall i \end{array} \right\} \subset O_P$$

Then we can define the intersection multiplicity of two projective curves F and G at a point $P \in P^2$ as $\mu_P(F, G) = \dim O_P \setminus (F, G) \in N \cup \{\infty\}$.

Note that for any point P $= (x_0 : y_0 : 1)$ we have that

$$\mu_{(x_0:y_0:1)}(F, G) = \mu_{(x_0,y_0)}(F^i, G^i).$$

Proof. We want to see that for any two curves F and G, under the isomorphism ϕ of construction 3.20 we have that for a point $(x_0 : y_0 : 1) \in P^2$, $\phi((F, G)) = (F^i, G^i)$. Now any element of (F,G) is of the form $\frac{f_1}{g_1} * F + \frac{f_2}{g_2} * G$. Then $\phi(\frac{f_1}{g_1} * F + \frac{f_2}{g_2} * G) = \frac{f_1^i}{g_1^i} * F^i + \frac{f_2^i}{g_2^i} * G^i$ which is an element of $(F^i, G^i) \subset O_{A^2,(x_0,y_0)}$. Therefore $\phi((F, G)) \subset (F^i, G^i)$. Take any element $\frac{f_1^i}{g_1^i} * F^i + \frac{f_2^i}{g_2^i} * G^i$. By the equation $(f^i)^h = f$ we get $\frac{f_1}{g_1} * F + \frac{f^i}{g^i} * G$ which we know is in (F,G) therefore it is in $\phi((F, G))$.

□

Therefore intersection multiplicities in the affine part can be computed precisely as in chapter 2. For the points at infinity, as one of its i-th coordinate must be nonzero we can use the U_i patch construction to make it an affine point, hence all computations will always follow from chapter 2.

Also, like in the affine case, intersection multiplicities are invariant under projective transformations. To see this, we will do exercise 3.10.

Lemma 3.10. (Exercise 3.10). Let $P_1, .., P_{n+2} \in P^n$ be points such that any $n + 1$ of them are linearly independent in K^{n+1}, and the same way for $Q_1, \ldots, Q_{n+2}$. Then there is

a projective coordinate transformation f with $f(P_i) = Q_i \ \forall \ i = 1, \ldots, n+2$.

Let $(P_i)_i$ and $(Q_i)_i$ be such points, $i = 1, \ldots, n+2$. As they are projective points, $P_i = [v_i]$ and $Q_i = [w_i]$ for $v_i, w_i \in K^{n+1}$. By assumption, any $n+1$ of them are linearly independent vectors in K^{n+1} so $(v_i)_i$, $(w_i)_i$ forms respectively basis of K^{n+1}.

As they form a basis, we have that the remaining vector $v_{n+2} = a_1 v_1 + \ldots + a_n v_{n+1}$ where not all $a_i = 0$. Similarly for w_{n+2}. Recall that in the projective space we can rearrange the scalars without changing the point, as we have that $[v_i] = [\lambda v_i]$. Therefore we can rewrite the equation of v_{n+2} to $v_{n+2} = v_1 + \ldots + v_{n+1}$ aswell as for w_{n+2}.

Now let $f : K^{n+1} \to K^{n+1}$ be the unique linear map sending basis elements to basis elements $v_i \to w_i$. Then we get that

$$f(v_{n+2}) = f(v_1 + \ldots + v_{n+1}) = w_1 + \ldots + w_n = w_{n+2}$$

This will induce a projective transformation $g : P^n \to P^n$, $g([v]) = [f(v)]$. Then we have that $g(P_i) = g([v_i]) = [f(v_i)] = [w_i] = Q_i \ \forall i$.

6 Bezout's Theorem

For an ideal $I \subset R$, the radical of I denoted $\sqrt{I}$ is defined as $\sqrt{I} = \{r \in R : r^n \in I\}$ for some positive integer n.

Let $X \subset A_K^n$, the vanishing ideal of X is defined as $I(X) = \{f \in K[x_1, .., x_n] : f(p) = 0 \forall p \in X\}$. It is the set of polynomials that vanish on X.

Fact 4.1. Hilbert's Nullstellensatz. (Andreas Gathmann[1], page 29)

The weak Hilbert Nullstellensatz states that if K is algebraically closed field and $V(I) = \emptyset$ then I = (1).

This statement corresponds to the fact that if f has no zero in an algebraically closed field then f must be constant. To see this, assume $V(\{f\}) = \emptyset$ for some f $\in K[x_1, .., x_n\}$. By the weak Hilbert Nullstellensatz we get that (f) = (1). Therefore $1 \in (f)$ so there exist some g such that f*g=1 which implies that f is a unit. As we have seen before, the only units of $K[x_1, .., x_n]$ are K^* so f must be constant.

The strong Hilbert Nullstellensatz states that if K is an algebraically closed field then I(V(I)) = $\sqrt{I}$. The vanishing ideal of the zero set for some subset I is exactly the radical of I.

Lemma 2.7. (Exercise 2.7). Let F and G be two curves without a common component through origin. Then there is a number $n \in N$ such that

$$(x - x_i)^n = (y - y_i)^n = 0 \in O_{p_i} \setminus (F, G)$$

for all i.

Let $I = (F, G) \subset O_0$. Since F and G do not have a common component, we can find an isolated neighborhood of $(0, 0)$. To see this, note that $V(F, G)$ as is finite we can exclude $(0, 0)$ from V(F,G) and then create a subset of $K[x_1, ., x_n]$ of polynomials that vanishes at the points of $V(F, G) \setminus \{(0, 0\}$ to get a closed set, and then use its complement as the neighbourhood of $(0, 0)$. For example, f = $\prod_i (x - a_i)$ for $a_i \neq 0 \in V(F, G)$. Then V(f) is a closed set, $(0, 0) \notin V(f)$.

Therefore, $V((F, G)) = V(I) = \{(0, 0)\}$ in a neighbourhood of $(0, 0)$. The ideal of all polynomials vanishing at origin is (x,y) so $I(V(I)) = (x, y)$. By the strong Hilbert Nullstellensatz we get that (x,y) = $\sqrt{(F, G)}$. By the definition of radical ideal we now know there is some k and l such that $x^k, y^l \in (F, G)$. Note now that $x^n = (x^k)x^{n-k}$ and $y^n = (y^l)y^{n-l}$, which both are in (x, y). So we have that

$$x^n = 0, y^n = 0 \in O_0 \setminus (F, G)$$

Note also by translation by Remark 2.4a) we can move it to any other point p to get that this result holds for $(x - x_p)^n, (y - y_p)^n$.

Lemma 6.1. *Lemma 4.2, Summing up intersection multiplicities (Andreas Gathmann[1], page 29)*
Let F and G be two affine curves over K with no common component. Consider the natural ring homomorphism

$$\phi : K[x, y] \setminus (F, G) \to \prod_{P \in F \cap G} O_P \setminus (F, G)$$

such that $[f] \to ([f]_P)_{P \in F \cap G}$.

1) The morphism ϕ *is surjective.*

2) If K *is algebraically closed then* ϕ *is an isomorphism.*

Proof. We follow the proof of Gathmann, for 1) and first show surjectivity. Let $F \cap G = \{P_0, .., P_m\}$ with $P_i = (x_i, y_i)$ for $i = 1, .., m$. We know this is a finite set as F and G have no common component by Remark 3.18 so there exists $n \in N$ such that

$$(x - x_i)^n = (y - y_i)^n = 0 \in O_{p_i} \setminus (F, G)$$

for all i.

For the polynomial

$$f = \prod_{i: x_i \neq x_0} (x - x_i)^n * \prod_{i: x_i \neq x_0} (y - y_i)^n \in K[x, y]$$

we have that $f(P_0) \neq 0$. Note that $f(P_0) = ([f]_{P_0}, 0, 0, 0, .., 0)$ since for all other i, $(x - x_i)^n$ appears and therefor $[f]_{p_i}$ becomes 0 in $O_{p_i} \setminus (F, G)$.

Recall that $O_p \setminus (F, G)$ can be embedded into $K[[x, y]]$, so every element has a corresponding power series. As this can be infinite, to ensure surjectivity we need to show that every element of $O_p \setminus (F, G)$ has a polynomial representative.

Exercise 2.7*b*). Let F and G be two curves without a common component through the origin. For every equivalence class in $O_0 \setminus (F, G)$ choose a representative element. Represent this element as its power series in $K[[x, y]]$, so

$$h(x, y) = \sum_{i, i \geq 0} a_{ij} x^i y^j$$

From exercise 2.7*a*) we have that in $O_0 \setminus (F, G)$ that $x^i y^j = 0$ whenever i $\geq n$, $j \geq n$. Therefore mod (F,G) we get

$$h = \sum_{0 \leq i, j < n} a_{ij} x^i y^j$$

which is a finite polynomial of total degree $< 2n$ and h $\in K[x, y]$.

As $f(P_0) \neq 0$, we know that it is a unit in $O_{P_0} \setminus (F, G)$ in view of localization, so there is a polynomial representative $g \in K[x, y]$ for $\frac{1}{f} \in O_{P_0} \setminus (F, G)$. Now the polynomial $fg \in K[x, y]$ is then mapped by ϕ to $(1, 0, 0, ..., 0)$, as $f = 0 \in O_{p_i} \setminus (F, G)$, i $\neq 0$, therefore $[fg] = [f][g] = 0 * [g]$ in these coordinates aswell.

By symmetry, we can find in the same way for all i, a polynomial that is mapped by ϕ to 1 in the P_i component and 0 to all others. As the image of ϕ is a subring, it follows that ϕ is surjective.

For 2) we need only to check injectivity. Let $f \in K[x, y]$ be such that $\phi(f) = 0$, so $[f]_{P_i} = 0 \forall i$. We want to show that $f = 0 \in K[x, y] \setminus (F, G)$.

Consider the ideal $I = \{g \in K[x,y] : gf \in (F,G)\}$. This is an ideal that contains (F,G). To see this, let h $\in (F,G)$ so h = aF + bG, a,b, $\in K[x,y]$. Multiply with f to get hf = (aF+bG)f = afF + bfG $\in (F,G)$, therefore $(F,G) \subset I$. Now we want to show that $V(I) = \emptyset$ so we can use the weak Nullstellensatz.

By contradiction, assume there is a point $P \in V(I)$. As F, G is in I, we know that $P \in F \cap G$ by the definition of the zero set of I. Therefore P is one of the target coordinates of ϕ, so $[f]_P \in (F,G)$ as $f \in \ker \phi$. But then $f = \frac{a}{g}F + \frac{b}{g}G$ for some polynomials $a, b, g \in K[x,y]$ with $g(P) \neq 0$ in $O_P \setminus (F,G)$. Therefore $gf = aF + bG$, so $g \in I$ and $g(P) = 0$ as P was from $V(I)$. This is a contradiction, so $V(I) = \emptyset$.

We have now that $I = K[x,y]$ from Nullstellensatz. This implies $f \in (F,G)$ as $1 \in I$ therefore 1*f = f $\in (F,G)$. So we get that $f = 0 \in K[x,y] \setminus (F,G)$ and the kernel is trivial. □

Note that from this, we also now have that

$$\sum_p \mu_p(F,G) \leq \dim\ K[x,y] \setminus (F,G)$$

with equality if K is algebraically closed. This follows as the dimension of a product vector space is the sum of each individual dimension, and the surjectivity guarantees the dimension of $K[x,y] \setminus (F,G)$ is bigger or equal to the product, while the injectivity gives equality as it is then a bijection.

Lemma 6.2. *Lemma 4.4, (Andreas Gathmann[1], page 30)*
Let F and G be two affine curves of degree $m = \deg F$, $n = \deg G$ such that their leading parts F_m and G_n have no common component.

Then every $f \in (F,G) \subset K[x,y]$ of degree $d = \deg f$ can be written as $f = aF + bG$ for two polynomials a, b with $\deg a \leq d - m$ and $\deg b \leq d - n$.

Proof. Following the proof of Gathmann, as f $\in (F,G)$, f = aF+bG for some a,b $\in K[x,y]$. Choose a representation with degree a minimal. Aassume for contradiction that deg $a > d-m$ or deg $b > d - n$. Then aF or bG contains a term of degree bigger than d. W.L.O.G assume it is aF. So

$$\deg\ (af) = \deg\ a + \deg\ F > d - m + m = d.$$

Since deg f = deg $aF + bG = d$, and aF has degree $> d$, the leading terms of aF and bG must cancel in f. Denote the leading terms of a and b as $a*, b*$. Then by cancellation we get that $a * F_m = -b * G_n$.

By assumption, G_n and F_m have no common component, and as F_m divides the right hand side of our equation, it must divide the left hand side too. Therefore $b*$ must be divisible by F_m, so $b* = cF_m, c \in K[x,y]$. From $a * F_m = -b * G_n$ we substitute in our new expression for $b*$ to get $a * F_m = -(-cF_m)G_n$. Then we get $a* = cG_n$ after cancellation of F_m. Note now that we can rewrite f as

$$f = aF + bG = aF - cGF + bG + cGF = (a - cG)F + (b + cF)G$$

We can see that the leading term $a*$ of a cancels the leading term cG_n of cG. Therefore we get that deg $(a - cG) <$ deg a, which contradicts the minimality of deg a. □

Lemma 6.3. *Lemma 4.5 (Andreas Gathmann[1], page 31)*
Let F and G be affine curves with no common component of degrees $m = \deg F$, $n = \deg G$.

1) *dim $K[x,y] \setminus (F,G) \leq mn$*

2) *If the leading parts F_m and G_n have no common component either, then equality holds in* 1)

Proof. We follow the proof of Gathmann, for 1) start with considering for all $d \geq m+n$, the sequence of vector space homomorphisms

$$K[x,y]_{\leq d-m} \times K[x,y]_{\leq d-n} \xrightarrow{\alpha} K[x,y]_{\leq d} \xrightarrow{\pi} K[x,y] \setminus (F,G)$$

where α takes $(a,b) \to aF + bG$ and π is the quotient map mod (F,G).

Note that for any $a \in K[x,y]_{\leq d-m}$,

$$\deg\,(aF) = \deg\, a + \deg\, F \leq d - m + m = d$$

and similarly for bG. The kernel of α is all pairs (a,b) such that $aF + bG = 0$. So we need that $aF = -bG$. As F and G have no common component, as described in Lemma 4.4. we have that $a = cG$ and $b = -cF$ for some $c \in K[x,y]_{\leq d-m-n}$. This bound on the degree from c follows from

$$\deg\,(a) = \deg\,(cG) = \deg\, c + \deg\, G = \deg\, c + n$$

As $\deg a \leq d - m$ we get that $\deg c \leq d - m - n$. Similar calculations for $\deg b$ gives the same result.

We can conclude that

$$\ker\, \alpha = K[x,y]_{\leq d-m-n} * (G, -F).$$

We see also that $\text{im}\ \alpha \subset \ker\, \pi$, as $\text{im}\ \alpha$ is of the form $aF + bG$ belonging to the ideal (F,G), which is the kernel of π.

We shall use the dimension theorem to calculate the dimension. First, we note that the space of $K[x,y]_{\leq d}$, for any d, is spanned by all monomials $x^i y^j$ with $i,j > 0$ and $i + j \leq d$, which will be a basis and span the space. To find its dimension, we need to count how many such polynomials there are.

Note that for each fixed $k = i + j$, where $k = 0, 1, 2, ..., d$, we get $k + 1$ choices of possible pairs (i,j), since each k determines what the other number is. That is, $(0,k)$, $(1,k-1)$, $(2,k-2)$, ..., $(k,0)$. We get a total number of monomials of degree $\leq d$ to be

$$\sum_{k=0}^{d}(k+1) = 1 + 2 + ... + (d+1) = \frac{(d+1)((d+1)+2)}{2} = \frac{(d+1)(d+2)}{2} = \binom{d+2}{2}$$

We can see this holds because

$$\binom{d+2}{2} = \frac{(d+2)!}{2!(d+2-2)!} = \frac{(d+2)!}{2!d!} = \frac{(d+2)(d+1)d!}{2d!} = \frac{(d+2)(d+1)}{2}$$

So now we can conclude that:

- dim $K[x,y]_{\leq d} = \binom{d+2}{2}$
- dim $K[x,y]_{\leq d-m} = \binom{d-m+2}{2}$
- dim $K[x,y]_{\leq d-n} = \binom{d-n+2}{2}$
- dim ker $\alpha = \binom{d-m-n+2}{2}$ since dim ker $\alpha = K[x,y]_{\leq d-m-n} * (G, -F)$

This gives us that

$$\dim \text{ im } \alpha = \dim K[x,y]_{\leq d-m} \times K[x,y]_{d-n} - \ker \alpha = \binom{d-m+2}{2} + \binom{d-n+2}{2} - \binom{d-m-n+2}{2}$$

So now we get with the dimension theorem that

$$K[x,y] \setminus (F,G) = \dim \pi = \dim K[x,y]_{\leq d} - \dim \ker \pi \leq \dim K[x,y]_{\leq d} - \dim \text{ im } \alpha$$

because im $\alpha \subset \ker \pi$, but this is just equal to

$$\binom{d+2}{2} - \binom{d-m+2}{2} - \binom{d-n+2}{2} + \binom{d-m-n+2}{2} = mn$$

For 2) note that it is enough to see that ker $\pi \subset$ im α. Ker $\pi = (F,G) \cap K[x,y]_{\leq d}$. By lemma 4.4 we already have $f = aF + bG$ for polynomials a with deg $\leq d-m$ and b with deg $\leq d-n$. □

Corollary 6.4. *Corollary 4.6, Bezout's Theorem (Andreas Gathmann[1], page 31)*
Let F and G be projective curves without a common component over an infinite field K. Then $\sum_{P \in F \cap G} \mu_P(F,G) \leq \deg F * \deg G$. If K is algebraically closed then equality holds.

Proof. We follow the proof of Gathmann and recall that as K is infinite we know the complement of $V(F,G)$ is infinite, and as they do not have a common component, then $V(F,G)$ is finite. So we can then pick a point Q and a line through it which does not intersect $F \cap G$. Therefor we can pick a point Q $\notin V(F,G)$ and a line through it which does not intersect $F \cap G$.

To see the above statement, note that given such a point Q, $Q = (x_0 : y_0 : z_0)$ and $P = (x_1 : y_1 : z_1)$ in P^2, given any projective line $aX + bY + cZ = 0$, solve the linear system $ax_0 + by_0 + cz_0 = 0$, $ax_1 + by_1 + cz_1 = 0$ and we will get the unique solution $(a : b : c) \in P^2$. Geometrically, as each point on the line in the projective plane is a line through the origin in K^3, the collection of all those lines corresponding to each point creates a plane in K^3 through the origin, therefore their intersection is a line through the origin in K^3 which is the solution point of this equation system.

As we only have finitely many points in the intersection, we get finitely many lines L through Q that passes through these points, so we still have infinitely many points left to choose from such that the line does not pass through $F \cap G$. □

We also want that L is not a component of F or G. As F is nonzero and must have a finite degree d it can at most be factored into d linear terms when divided out, so only finitely many distinct linear forms can divide F, and similarly for G, therefore we only have finitely many points $(a : b : c)$ which we do not want our line to contain to avoid that it is a factor of F or G. Again, as we have infinitely many lines we can choose from such that

it is not a component of F or G as altogether we have only a union of finitely many bad values.

Therefor by lemma 3.10 we can make a projective coordinate transformation so that L becomes the line at infinity. Note now by the choice of L, neither F or G has infinity as a component.

Now we can apply lemma 4.2 to F^i and G^i to get that

$$\sum_{P \in F \cap G} \mu_P(F, G) = \sum_{P \in F^i \cap G^i} \mu_P(F^i, G^i) \leq \dim\, K[x, y] \setminus (F^i, G^i)$$

By lemma 4.5 we then get that

$$\dim\, K[x, y] \setminus (F^i, G^i) \leq \deg\, F^i * \deg\, G^i = \deg\, F * \deg\, G$$

So we have that $\sum_{P \in F \cap G} \mu_P(F, G) \leq \deg\, F \cdot \deg\, G$.

If K is algebraically closed then the first inequality from lemma 4.2 is an equality. All we need now for the second inequality to be an equality from 4.5, is to show that the leading parts of F^i and G^i have no common component.

As F^i_m and G^i_n are homogeneous polynomials in two variables we get by lemma 3.11 that, over an algebraically closed field, they are a product of linear polynomials. Note now that these products corresponds to the points at infinity. By our choice of construction however, they cannot have any common points as the points of infinity lie on L, and L does not intersect F or G. Therefore, there is no common component, and equality holds.

Hence, we get our desired result that $\sum_{P \in F \cap G} \mu_P(F, G) = \deg\, F \cdot \deg\, G$.

Remark 4.7 (Andreas Gathmann[1], page 32)

In the proof of Bezout's Theorem we needed an infinite field K. However, the inequality in the theorem still holds for finite fields. This is where we use that every field has an algebraic closure. We can embed the finite field into the algebraic closure and compute the intersection of F and G in the algebraic closure instead. Note that in the algebraic closure, we can get more points that satisfy $F(p) = 0$, $G(p) = 0$, than what we have in the original field. However we can see that the inequality still holds. Equality holds if there are no more such points after the embedding.

Remark 3.8 (Andreas Gathmann[1], page 32)

If F and G have an intersection point, from Bezout's Theorem it follows that as every point has atleast multiplicity 1, they can intersect in at most $\deg\, F \cdot \deg\, G$ points. We can also have that they intersect in no points here and by the inequality the result still follows.

If K is algebraically closed, by the equality of Bezout's Theorem, we can conclude that they actually must intersect in atleast one point. We can immediately see that this is false without algebraic closure, as we then have no guarantee that there exists any point in either $V(F)$ or $V(G)$.

Lemma 4.9 (Exercise 4.9)

For the following complex affine curves F and G, determine the points at infinity of their projective closures and use Bezout's Theorem to read off the intersection multiplicities at all points of $F \cap G$.

a) $F = x + y^2$, $G = x + y^2 - x^3$.

Since Bezout's Theorem uses projective curves, we will first have to homogenize the curves so we can see all their possible intersection points. So $F^h = xz + y^2$ and $G^h = xz^2 + zy^2 - x^3$.

For the points at infinity, we have that $F(x, y, 0) = 0$ implies that $y^2 = 0$, so $y = 0$. This tells us that F has $[1 : 0 : 0]$ as a point of infinity. Meanwhile, $G(x, y, 0) = -x^3 = 0$, so G has the point $[0 : 1 : 0]$ as a point of infinity. Hence, they do not intersect at infinity.

Now we look at the intersections in the affine part. We need to solve the equation system

$$\begin{aligned} x + y^2 &= 0 \\ x + y^2 - x^3 &= 0 \end{aligned}$$

Subtracting the first equation from the second give us that $-x^3 = 0$. We are now given that $(0, 0)$ is their only intersection point. By Bezout's theorem, we are also given that the multiplicity of $(0, 0)$ is $\deg F \cdot \deg G$ which is $2 \cdot 3 = 6$.

b) $F = y^2 - x^2 + 1$, $G = (y + x + 1)(y - x + 1) = y^2 - x^2 + 2y + 1$.

First, we homogenize again to give us $F^h = y^2 - x^2 + z^2$ and $G^h = y^2 - x^2 + 2yz + z^2$. Then we see that $F(x, y, 0) = y^2 - x^2$ and $G(x, y, 0) = y^2 - x^2$. Both have the same points of infinity given by $y^2 = x^2$ so $y = x$ or $y = -x$, which gives us the points $[1 : 1 : 0]$ and $[1 : -1 : 0]$. The curves thus intersect at two points of infinity.

For their affine intersection points we have the equation system

$$\begin{aligned} y^2 - x^2 + 1 &= 0 \\ y^2 - x^2 + 2y + 1 &= 0 \end{aligned}$$

Subtracting the first one with the second gives $2y = 0$, so $y = 0$. Then we have that $x^2 + 1 = 0$ so $x^2 = -1$, which tells us that $x = \pm 1$. So the affine intersection points are $(1, 0)$ and $(-1, 0)$.

By Bezout's theorem we have that the sum of the intersection points multiplicity is $\deg F \cdot \deg G = 2 * 2 = 4$. Note now that we have exactly 4 intersection points so each one of them must have multiplicity 1.

Lemma 4.10 (Exercise 4.10)
Deduce the following real version of Bezout's Theorem from the complex case: If F and G are two real projective curves without common component then

$$\sum_{P \in F \cap G} \mu_P(F, G) = \deg F * \deg G \bmod 2.$$

In particular, two real projective curves of odd degree always intersect in at least one point.

First, by definition, P^2_C is the projective space made up of complex lines in C^3. We know that

$R^3 \subset C^3$ and a real point in P^2_C is any equivalence class $[x : y : z]$ such that its equivalence class contains a point where x, y, z are real simultaneously. This tells us that the complex line intersects R^3. A complex point in P^2_C is then a line which does not intersect R^3, so it contains no such triple of real numbers.

We also have that if $P = [x : y : z]$ is a real point in P^2_C, then $[x : y : z]$- conjugate $= [x : y : z]$. The conjugate of any real number is itself, however this does not hold for any complex point in P^2_C as the conjugate of complex numbers are different complex numbers. We also have that if P is a complex point, and $F(P) = 0$ then $F(\overline{P}) = 0$ as well. Therefore we have that if F and G only have complex intersection points then

$$\sum_{P \in F \cap G} \mu_P(F, G) = \deg F * \deg G \bmod 2 = 0$$

Rewriting it give us

$$\sum_{P \in F \cap G} \mu_P(F, G) = \sum_{P \text{ complex} \in F \cap G} \mu_P(F, G) + \sum_{P \text{ real} \in F \cap G} \mu_P(F, G)$$

then mod 2 we have that only the real points are counted modulo 2 as the question wanted. Now note that if $\deg F * \deg G$ is odd then we get atleast 1 real point.

7 Multiplicity of a point of a curve

From seeing how similar two curves can be at intersection points, we shall now instead regard a little about how they look individually at points and see some different properties curves can have at a point.

We are going to start in the affine space to develop the theory and, as done previously, embed it to the projective plane.

Definition 7.1. Definition 2.18, Tangents and multiplicities of points (Andreas Gathmann[1], page 17

Let F be an affine curve. Write F = $\sum_i F_i$ where each F_i is homogeneous

1) The smallest $m \in N$ for which the homogeneous part F_m is non-zero is called the multiplicity $m_0(F)$ at the origin. Any linear factor L of F_m is called a tangent to F at the origin. The direction of the tangent is given by L = 0

2) For a general point $P = (x_0, y_0) \in A^2$, tangents at P and the multiplicity $m_p(F)$ are defined by first shifting coordinates to $x' = x - x_0$ and $y' = y - y_0$, and then applying a) to the origin.

Lemma 2.19 (Exercise 2.19).

Given a linear coordinate transformation that maps the origin to itself and a curve F to F', show that $m_0(F) = m_0(F')$ and that the transformation maps any tangent of F to any tangent of F'.

By remark 2.4, an affine coordinate transformation (x, y) to (x', y') is given by $(ax + by + e, cx + dy + f)$ for $a, b, c, d, e, f \in K$ with $ae - bd \neq 0$. As we are mapping from the origin to the origin, $e = 0$, $f = 0$. Given the curve $F = (x, y)$, rewrite it in terms of its homogeneous parts so we can get that $m_0(F) = m$ for some m $\in N$. Given the linear coordinate transformation, consider $F(x', y') = F(ax + by, cx + dy)$. For any monomial $x^i y^j \in F$, after the variable change we can see that

$$x^i y^j = (ax + by)^i * (cx + dy)^j$$

has the same degree which is $i + j$. So the degree does not change by coordinate transformation, therefor we have that $m_0(F) = m_0(F') = m$ as the degree of the homogeneous parts remains unchanged. From this it also follows that any tangent, which is a line, is mapped to another line by the degree invariance.

Definition 7.2. Definition 2.20, Smooth and singular points (Andreas Gathmann[1], page 17
Let F be an affine curve.

1) A point P $\in F$ is called a smooth or regular point if $m_P(F) = 1$. Note then that F has a unique tangent at P which will be dented by $T_P F$.

If P is not a smooth point, so $m_P(F) > 1$, then P is a singular point or a singularity of F. A special case of this arises when $m_P(F) = 2$, as then in an algebraically closed field F has exactly two different tangents, and this is called a node.

2) The curve F is said to be smooth or regular if all its points are smooth. Otherwise F is called singular.

Example 2.21. (Andreas Gathmann[1], page 18)

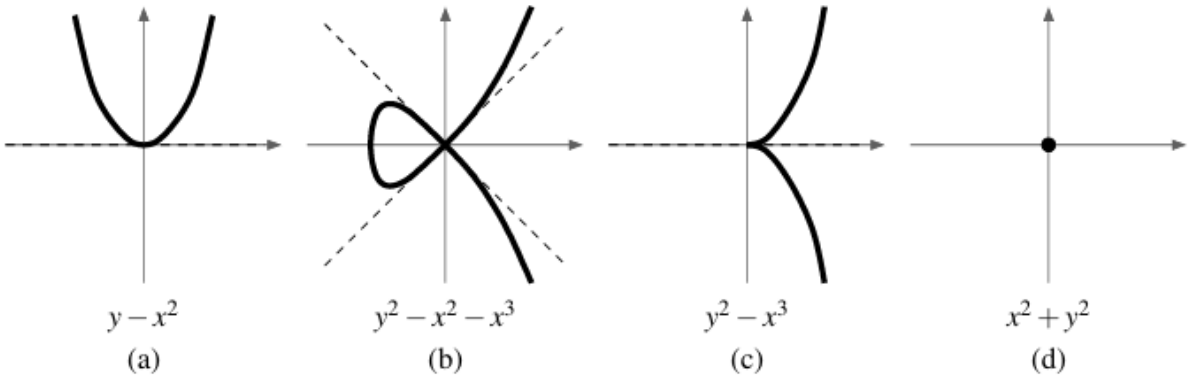


Figure 6

In Figure 6 we have four curves in $\mathbb{R}[x,y]$ and we will check the multiplicity of each curve at the origin.

a) $F = y - x^2$. We can see that $F_1 = y$, so $m_0(F) = 1$ and it is a smooth point. The tangent is given by $y = 0$ by definition 2.18 *a*), so $T_P F$ is the x-axis

b) $F = y^2 - x^2 - x^3$. We have $F_2 = y^2 - x^2$ and $m_0(F) = 2$. Therefore, we have a node and we can see that the tangents are given by $y^2 - x^2 = (y-x)(y+x) = 0$. So we get $y = x$ and $y = -x$ as its tangent lines.

c) $F = y^2 - x^3$. Then $F_2 = y^2$ and $m_0(F) = 2$. The tangent is given by $y^2 = 0$ which is again the x-axis.

d) $F = x^2 + y^2$. Here we have $m_0(F) = 2$ but we have no tangent lines since $x^2 + y^2 = 0$ has no solution in R.

As we can see in the picture, the tangents give us information to an extent on how the curves behave at the origin.

Note that for *d*) above we would get that $x^2 + y^2 \in R = x^2 + y^2$ in its algebraic closure C, and we have two linear factors $(x+iy)(x-iy)$. However, as $V(F)$ changes when we move from R to C, we can not use that information geometrically, so $m_P(F)$ is only used to visualise the "thickness" of the points in the field we originally considered, as shown in the picture above.

Proposition 7.3. *Proposition 2.24, Affine Jacobi Criterion (Andreas Gathmann[1], page 18)*

1) P is a singular point of F if and only if

$$\frac{\delta F}{\delta x}(P) = \frac{\delta F}{\delta y}(P) = 0$$

2) If P is a smooth point of F the tangent to F at P is given by

$$T_P F = \frac{\delta F}{\delta x}(P) * (x - x_0) + \frac{\delta F}{\delta y}(P) * (y - y_0)$$

We will now go over to the projective plane.

Construction 3.23. Tangents and multiplicities. (Andreas Gathmann[1], page 27)

For a point $P = (x_0 : y_0 : 1) \in P^2$ in the affine part A^2 we define $m_P(F) = m_{(x_0,y_0)}(F^i)$. Then we can see that a tangent to F at P is the projective closure of a tangent to F^i at (x_0, y_0).
If P is not in the affine part, then choose a different coordinate for the line at infinity, thus we can switch charts and get the point to an affine part. Therefor we can always work with the curve in the affine space to observe how it behaves at points.

As in the affine case, $P \in F$ is a smooth or regular point if $m_P(F) = 1$ and its unique tangent is denoted $T_P F$, otherwise it is singular. If all points of F are smooth then F is smooth, otherwise we call F singular.

Proposition 7.4. *Proposition 3.25, Projective Jacobi Criterion (Andreas Gathmann[1], page 27)*
Let P be a point on a projective curve F.

1) P is a singular point if and only if

$$\frac{\delta F}{\delta x}(P) = \frac{\delta F}{\delta y}(P) = \frac{\delta F}{\delta z}(P) = 0$$

2) If P is a smooth point of F the tangent to F at P is given by

$$T_P F = \frac{\delta F}{\delta x}(P) * x + \frac{\delta F}{\delta y}(P) * y + \frac{\delta F}{\delta z}(P) * z$$

Lemma 4.11 (Exercise 4.11)

Let F be a complex irreducible projective curve of degree d, and let $P \in P^2$ be a point. Let $m = m_P(F) \in N$.

Show that for all but finitely many lines $L \in P^2$ through P, the intersection $F \cap L$ consists of exactly $d - m$ points $\neq P$.

Given $P \in P^2$, we can do a coordinate and affine chart change to let it be $(0,0)$. By assumption, F has degree d so by Bezout's theorem we have that

$$\sum_{P \in F \cap L} \mu_P(F, L) \leq d \cdot 1 = d$$

for any line L, as the degree of lines are 1. As we are in C, which is algebraically closed, we have that equality holds.

Given $m = m_P(F) \in N$, we can write F as a sum of its homogeneous parts. So $F = F_m + ... + F_n$, where F_m is its first nonzero homogeneous part. A line through P in the affine chart has an equation of the form $y = \lambda x$, $\lambda \in C$.

By parametrizing the line into F we get

$$F(x, \lambda x) = F_m(x, \lambda x) + ... + F_n(x, \lambda x)$$

As F_m is homogeneous we can rewrite $F_m(x, \lambda x) = x^m * F_m(1, \lambda)$. Note now that this implies that $\mu_P(F, L) = m$, as long as $F(1, \lambda) \neq 0$. If $F(1, \lambda) = 0$ then the term vanishes at the next nonzero term and has degree $> m$.

Note that $F(1, \lambda)$ is a univariate polynomial in $\lambda, \lambda \in C$ of degree $\leq m$. Since C is algebraically closed, we know it has at most m roots. So there are only finitely many solutions to when this is equal to 0. For each such solution, we remove the corresponding line, and we have only finitely many lines remaining which we do not wish to have. By Bezout's theorem again, we get that for all but finitely many lines,

$$\sum_{P \in F \cap G} \mu_P(F, L) = d - m$$

Now we want to see how many of these lines have exactly $d - m$ distinct points where they intersect F. This translates to exclude lines that has intersection points with multiplicity > 1 with F. We will use Corollary 2.22, which tells us that $\mu_P(F, L) = 1$ if and only if P is a smooth point of both F and L, and $T_P F \neq T_P L$.

By Proposition 2.24 we get that P is a singular point of F if and only if

$$\frac{\delta F}{\delta x}(P) = \frac{\delta F}{y}(P) = F(P) = 0$$

This is an overdetermined system of equations, as we have more equations than unknowns x and y, so we know that there are either no solutions or a finite number of solutions. We can conclude that F has only finitely many singular points, as we know that for each of these singular points, only one line through origin is passing through that point and P simultaneously, implying that we may remove finitely many bad lines.

We finally need that for the remaining smooth points of F, each one of them have a unique $T_P F$ such that $L = T_P L \neq T_P F$. As we know we are dealing with at most $d - m$ points left that are smooth, therefore they have a unique tangent line, there are only finitely many lines we need to remove to avoid that $T_P F = L$.

Taking the union of these lines we have removed, which is just a union of finitely many lines, we still have a finite set. We can therefore see that for all but finitely many lines, $F \cap L$ consists of exactly $d - m$ points $\neq P$.

8 Bibliography

References

[1] Andreas Gathmann. *Plane Algebraic Curves*. Class notes, RPTU Kaiserslautern, 2023

[2] Cox et. al. *Ideals, Varieties and Algorithms*, Fourth Edition. Springer International Publishing Switzerland, 2015

[3] A. Chambert-Loir *(Mostly) Commutative Algebra*. Springer Nature Switzerland AG, 2021

[4] Kobayashi, H., Furukawa, A., Sasaki, T. (1986). Grobner bases of ideals of convergent power series. *SYMSAC86: Proceedings of the Symposium on Symbolic and Algebraic Manipulation*, 225-227. https://doi.org/10.1145/32439.32484

Found Mistakes

April 5, 2026

1. In Corollary 4.6 proof of Bezouts Theorem I forgot to say I am showing there is a unique line between any two points in the proof of statement 1.

2. To correct the statement made on page 15, "We are interested in the case of step 5. If this case has accured, note that the Gröbner basis is now a subset of K[x, y]. As we have that (F,G) = (G) K[x, y] we can continue calculations in K[x, y] of the ideal (F,G) which we will do further on", we instead need to show that the division algorithm terminates in $k[[x, y]]$ so we can get remainders for the use of Gröbner basis in the calculations. Therefore we must show that there will be a well-defined limit to the division process.

This is done by implementing a metric to $k[[x, y]]$ to make it a metric space, show that the division algorithm induces a Cauchy sequence and then if this metric is complete we get the limit which will be the remainder.

Following information is from PlanetMath [1], Stanford [2] and McGill School of Computer Science [3].

First choose a monomial ordering for the variables. Then we define the order of a power series f to be { min i+j | $a_ij \neq 0$}, the minimal degree of the monomials of f.

The metric is defined to be $d(f, g) = 2^{-ord(f-g)}$, it is inspired from the p-acid metric form.

To see completeness, recall that a sequence $(f_n)_n$ is Cauchy in $k[[x, y]]$ iff $\forall\epsilon > 0, \exists N : m, n \geq N \rightarrow d(f_m, f_n) < \epsilon$. Take such a sequence and fix $\epsilon = 2^{-k}$.T Then we can see that for all m,n $\geq M$ for this ϵ, ord$(f_m - f_n) >= k$ by definition of the metric. This implies that the terms of degree $< k$ must agree as $f_m - f_n$ cancels the terms up to k. Therefor their monomials and coefficients must be equal up to degree k.

If we let $k \rightarrow \infty$ we can apply this argument as the distance for f_m and f_n is $2^{-\infty} = 0$ so they must agree on all terms and coefficents eventually. Therefor define the limit function of this Cauchy sequence to be f = $\sum_{i,j} a_{i,j}x^iy^j$ where

each $a_{i,j}x^iy^j$ is the term that all f_n agrees with for $n \geq N$. Then $f_n \to f$ in this metric, and f $\in k[[x, y]]$.

All we need to do now is to see that the division algorithm produces a Cauchy sequence of remainders. Recall that in the division algorithm, at each step we will have removed atleast one step of the highest degree term. Therefor the order of the remainder is bigger or equal to the previous one, ord$(r_n) \leq$ ord(r_{n+1}). Note also that the ord $r_k \to \infty$ as $k \to \infty$. So for any fixed k, we can find that for all $n, m \geq k$, the order of r_n, r_m is bigger than k. Now we can see that $d(r_n, r_m) = 2^{-ord(r_n, r_m)} < 2^{-k}$ as the order of $f_n - f_m > k$ since they do not have any terms of degree $<$ k. The cauchy definition follows.

Note also that depending on monomial ordring and the different choices of which polynomials to divide with in the list we can still get different remainders when we divide. This only got us that the remainders exists. Calculations for the quotient group continue instead exactly as explained except the remainders can now be infinite too.

1 Bibliography

References

[1] mathcam, *I-adic topology*. `https://planetmath.org/iadictopology`, 2013

[2] Church, B and Lerner-Brecher, Matthew. *Introduction to p-adic Numbers*. Stanford, 2022.

`https://web.stanford.edu/~bvchurch/assets/files/talks/p-adics.pdf`

[3] Edward Chernysh, *A Brief Note on p-adic Analysis, p-Adic Topology and Ostrowski's Theorem*. McGill School of Computer Science, 2017.

`https://www.cs.mcgill.ca/~echern2/repo/padic.pdf`

Found Mistakes

April 5, 2026

1. In Corollary 4.6 proof of Bezouts Theorem I forgot to say I am showing there is a unique line between any two points in the proof of statement 1.

2. To correct the statement made on page 15, "We are interested in the case of step 5. If this case has accured, note that the Gröbner basis is now a subset of K[x, y]. As we have that (F,G) = (G) K[x, y] we can continue calculations in K[x, y] of the ideal (F,G) which we will do further on", we instead need to show that the division algorithm terminates in $k[[x, y]]$ so we can get remainders for the use of Gröbner basis in the calculations. Therefore we must show that there will be a well-defined limit to the division process.

This is done by implementing a metric to $k[[x, y]]$ to make it a metric space, show that the division algorithm induces a Cauchy sequence and then if this metric is complete we get the limit which will be the remainder.

Following information is from PlanetMath [1], Stanford [2] and McGill School of Computer Science [3].

First choose a monomial ordering for the variables. Then we define the order of a power series f to be { min i+j | $a_ij \neq 0$}, the minimal degree of the monomials of f.

The metric is defined to be $d(f, g) = 2^{-ord(f-g)}$, it is inspired from the p-acid metric form.

To see completeness, recall that a sequence $(f_n)_n$ is Cauchy in $k[[x, y]]$ iff $\forall\epsilon > 0, \exists N : m, n \geq N \rightarrow d(f_m, f_n) < \epsilon$. Take such a sequence and fix $\epsilon = 2^{-k}$.T Then we can see that for all m,n $\geq M$ for this ϵ, ord$(f_m - f_n) >= k$ by definition of the metric. This implies that the terms of degree $< k$ must agree as $f_m - f_n$ cancels the terms up to k. Therefor their monomials and coefficients must be equal up to degree k.

If we let $k \rightarrow \infty$ we can apply this argument as the distance for f_m and f_n is $2^{-\infty} = 0$ so they must agree on all terms and coefficents eventually. Therefor define the limit function of this Cauchy sequence to be f = $\sum_{i,j} a_{i,j}x^iy^j$ where

each $a_{i,j}x^iy^j$ is the term that all f_n agrees with for $n \geq N$. Then $f_n \to f$ in this metric, and f $\in k[[x, y]]$.

All we need to do now is to see that the division algorithm produces a Cauchy sequence of remainders. Recall that in the division algorithm, at each step we will have removed atleast one step of the highest degree term. Therefor the order of the remainder is bigger or equal to the previous one, ord$(r_n) \leq$ ord(r_{n+1}). Note also that the ord $r_k \to \infty$ as $k \to \infty$. So for any fixed k, we can find that for all $n, m \geq k$, the order of r_n, r_m is bigger than k. Now we can see that $d(r_n, r_m) = 2^{-ord(r_n, r_m)} < 2^{-k}$ as the order of $f_n - f_m > k$ since they do not have any terms of degree $<$ k. The cauchy definition follows.

Note also that depending on monomial ordring and the different choices of which polynomials to divide with in the list we can still get different remainders when we divide. This only got us that the remainders exists. Calculations for the quotient group continue instead exactly as explained except the remainders can now be infinite too.

1 Bibliography

References

[1] mathcam, *I-adic topology*. `https://planetmath.org/iadictopology`, 2013

[2] Church, B and Lerner-Brecher, Matthew. *Introduction to p-adic Numbers*. Stanford, 2022.

`https://web.stanford.edu/~bvchurch/assets/files/talks/p-adics.pdf`

[3] Edward Chernysh, *A Brief Note on p-adic Analysis, p-Adic Topology and Ostrowski's Theorem*. McGill School of Computer Science, 2017.

`https://www.cs.mcgill.ca/~echern2/repo/padic.pdf`