A proof of Bézout's theorem using the euclidean algorithm

Hulst, R.P.

R. P. Hulst

rhulst@math.leidenuniv.nl

A proof of Bézout's theorem using the Euclidean algorithm

Bachelor thesis, August 30th 2011

Supervisor: Prof. Dr. S. J. Edixhoven

Mathematisch Instituut, Universiteit Leiden

Table of Contents

Introduction

Bézout's theorem (Theorem 3.1) states that the number of common points of two algebraic plane curves is either infinite or equal to the product of their degrees. The theorem holds if we count points at infinity in the projective plane and intersection multiplicities.

History

In circa the year 300 BC Euclid of Alexandria (∼325–∼265 BC) wrote the treatise *The Elements* consisting of thirteen books. Book seven is an introduction to number theory and it contains the Euclidean algorithm to find the greatest common divisor of two integers. This algorithm is one of the oldest in history and is still in common use.

In the year 1748 Leonhard Euler (1707–1783) and Gabriel Cramer (1704–1752) already stated Bézout's theorem, but neither of them succeeded in completing a proof. A few years later, in the year 1764, Étienne Bézout (1730–1783) gave the first satisfactory proof as a result of earlier work of Colin Maclaurin (1698–1746). In actual fact, this proof was incomplete in the count of multiple points. The proper count of multiplicities was settled more then one hundred years later, in the year 1873, by Georges-Henri Halphen (1844–1889). This historical information can be found in [7] and [1].

Two years ago, in 2009, Jan Hilmar and Chris Smyth finished their article [5] and in this work they proved Bézout's theorem using the Euclidean algorithm. This bachelor thesis is based on the article [5], but we will expand the matter a bit more precisely. Firstly, in Remark 4 of Section 3.3 [5], Hilmar and Smyth admit that they *"have brazenly taken for granted that certain polynomials* [...] *are homogeneous; so as not to interrupt the flow of the paper"*. In Lemma 3.5 of this bachelor thesis we will prove that these certain polynomials are indeed homogeneous. Secondly, in the appendix of [5] Hilmar and Smyth refer to Fulton [2] for the definition of the intersection multiplicity. So actually, alongside the Euclidean algorithm, Hilmar and Smyth use commutative algebra in order to prove Bézout's theorem as well. Using Proposition 2.5, I will prove Bézout's theorem without any use of commutative algebra. Finally I will be more extensive in giving definitions and proving properties.

Content

The aim of this bachelor thesis is to prove Bézout's theorem using the Euclidean algorithm. Let k be a field and let $\overline{k}$ be its algebraic closure. Let k^* denote the unit group of k.

In the first section we will define the projective plane over $\bar{k}$. After that we will define homogeneous polynomials, whose solutions have nice properties over the projective plane. With these homogeneous polynomials, we will be able to define curves in the projective plane and formulate and prove Bézout's theorem.

The second section consists of a definition and some important properties of the intersection multiplicity in a common point of two plane curves. Hereby we can define the intersection cycle of two homogeneous polynomials. The proof of the finiteness of intersection multiplicities is deferred to section 3.

The last section is about Bézout's theorem and its proof. For this proof we use an algorithm which reminds us strongly of the Euclidean algorithm mentioned above. After applying this algorithm, it is sufficient to prove a weaker version of Bézout's theorem. We will finish the proof by induction on the minimum x-degree of two homogeneous polynomials.

1 Curves and divisors of homogeneous polynomials

In this section we will first define the projective plane and thereafter homogeneous polynomials and their curves. We can study homogeneous polynomials over the projective plane, which give us curves in the projective plane. Since Bézout's theorem is about curves in the projective plane, we need these definitions and properties in order to formulate and prove the theorem.

The projective plane

Recall that k is a field. We start with a definition of the projective plane over k, using an equivalence relation.

Definition 1.1. Let $\sim$ be the equivalence relation on $\bar{k}^3 - \{0\}$ defined by $x \sim y$ if and only if there exists a λ in $\bar{k}^*$ such that the equality $x = \lambda y$ holds. The *projective plane* is defined as the set

$$\mathbb{P}^2\left(\bar{k}\right) := \left(\bar{k}^3 - \{0\}\right) / \sim .$$

We will write $\mathbb{P}^2$ instead of $\mathbb{P}^2\left(\bar{k}\right)$.

Example 1.2. Consider the field of real numbers $\mathbb{R}$. The points $(1,1,1)$ and $(2,2,2)$ in $\mathbb{R}^3$ are not equal to one another, but they are elements of the same equivalence class modulo the equivalence relation $\sim$ defined above.

Notation 1.3. Let $q : \bar{k}^3 - \{0\} \longrightarrow \mathbb{P}^2$ be the quotient map. For all points (a_1, a_2, a_3) in $\bar{k}^3 - \{0\}$ write $q(a_1, a_2, a_3) = (a_1 : a_2 : a_3)$. These are called homogeneous coordinates.

Remark 1.4. For every point a in $\mathbb{P}^2$ the projective plane, there either exist unique elements x and y in $\bar{k}$ such that a is of the form $(x : y : 1)$ or there exists a unique element x in $\bar{k}$ such that a is of the form $(x : 1 : 0)$ or a is equal to $(1 : 0 : 0)$. Therefore, there are two disjoint subsets of the projective plane; the subset consisting all points of the form $(x : y : 1)$ and the subset consisting all points of the form $(x : y : 0)$. Analogously, the latter subset consists of two disjoint subsets. Hence, the projective plane is a disjoint union of affine spaces

$$\mathbb{P}^2 = \bar{k}^2 \sqcup \bar{k} \sqcup \{\text{one point}\}.$$

We will write every point of the projective plane in one of the above mentioned forms.

Homogeneity

Since multiples of points in the projective plane are equal to one another, it would make sense if there is a relationship between their values when substituted in a polynomial. We will define so called homogeneous polynomials and subsequently we will show some of their properties, which will become very useful in the proof of Bézout's theorem.

Definition 1.5. Let $f \in k[x,y,z]$ be a polynomial. One says that f is a *homogeneous polynomial of degree* $n \in \mathbb{Z}_{\geq 0}$ if f is of the form

$$f = \sum_{i+j \leq n} f_{ij} x^i y^j z^{n-i-j},$$

with coefficients $f_{ij} \in k$ for all i, j and one writes $f \in k[x,y,z]_n$. If f is a nonzero polynomial, then ∂f denotes the degree of f and $\partial_x f$ denotes the x-degree of f. Logically, ∂_y and ∂_z are defined analogously.

Remark 1.6. Let $f \in k[x, y, z]$ be a homogeneous polynomial of degree n and let point (a_1, a_2, a_3) be in $\left(\bar{k}\right)^3$. For all λ in $\bar{k}^*$ the equality $f(\lambda a_1, \lambda a_2, \lambda a_3) = \lambda^n f(a_1, a_2, a_3)$ holds.

Remark 1.7. The polynomial ring $k[x, y, z]$ is equal to the following direct sum of k-vector spaces

$$k[x, y, z] = \bigoplus_{i \geq 0} k[x, y, z]_i.$$

Hence, if $f \in k[x, y, z]$ is a polynomial, then it is a unique finite sum of homogeneous polynomials,

$$f = \sum_{i=0}^{N} f_i$$

for some positive integer N and with homogeneous polynomials $f_i \in k[x, y, z]_i$ for all i.

Remark 1.8. From Remark 1.6 it follows that if one finds a nonzero solution to the equation $f = 0$ for some homogeneous polynomial $f \in k[x, y, z]$, then one finds a line through 0 in $\bar{k}^3$ such that every point in this line is a solution to the equation. From the definition of the projective plane it follows that we may say that the projective plane is the set of one-dimensional subspaces of $\bar{k}^3$.

Example 1.9. Consider the field of real numbers $\mathbb{R}$ and let $f \in \mathbb{R}[x, y, z]$ be the homogeneous polynomial given by $x + y - z$. It is easy to see that point $(1, 1, 2)$ in $\mathbb{R}^3$ is a solution of the equation $f = 0$. Since f is homogeneous and since $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, one has that for all λ in $\mathbb{C}^*$ the point $\lambda(1, 1, 2)$ is a solution of the equation in $\mathbb{C}[x, y, z]$. Hence, we find point $(\frac{1}{2} : \frac{1}{2} : 1)$ in the projective plane $\mathbb{P}^2$ as a solution of the equation.

Lemma 1.10. Let $f, g \in \bar{k}[x, y, z]$ be two nonzero polynomials such that g divides f. If f is homogeneous, then so is g.

Proof. Let $g, h \in \bar{k}[x, y, z]$ be two nonzero polynomials such that the product $f := gh$ is a homogeneous polynomial and suppose that g is not homogeneous. From Remark 1.7 it follows that there exist strictly positive integers M and N such that

$$g = \sum_{i=0}^{M} g_i, \quad h = \sum_{j=0}^{N} h_j \quad \text{and} \quad f = \sum_{s=0}^{M+N} f_s$$

with homogeneous polynomials $g_i \in \bar{k}[x, y, z]_i$, $h_j \in \bar{k}[x, y, z]_j$ and $f_s \in \bar{k}[x, y, z]_s$ for all i, j, s. Define the following indices

$$i_0 := \min\{i : g_i \neq 0\},\ i_1 := \max\{i : g_i \neq 0\},\ j_0 := \min\{j : h_j \neq 0\},\ j_1 := \max\{j : h_j \neq 0\}.$$

Hence, one has that both $f_{i_0+j_0} = g_{i_0} h_{j_0}$ and $f_{i_1+j_1} = g_{i_1} h_{j_1}$ are nonzero homogeneous polynomials. One has that $i_0 \neq i_1$, otherwise g would be a homogeneous polynomial. It follows that one has that $i_0 + j_0 < i_1 + j_1$, so f is not homogeneous. This is in contradiction with the assumption. Therefore, it follows that if f is homogeneous, then so is g. $\square$

Lemma 1.11. Let $f \in k[x, y, z]$ be a nonzero homogeneous polynomial. There exists a unique factorization modulo k^* of f in $k[x, y, z]$ such that one has

$$f = c \cdot \prod_{i \in I} f_i^{e_i}$$

for some constant c in k^* and finite index set I, such that for all i one has that $f_i \in k[x, y, z]$ is an irreducible homogeneous polynomial and $e_i \in \mathbb{Z}_{>0}$ is the multiplicity of f_i and for all i, j one has that $f_i = f_j$ modulo k^* if and only if $i = j$.

Proof. Since k is a field, k is a factorial ring (definition: [6], p. 144) or in different words an unique factorization domain. Hence, $k[x]$ is a factorial ring ([6], Theorem 6.9, p. 148) and analogously it follows that $k[x, y, z]$ is a factorial ring. So for all nonzero polynomials $f \in k[x, y, z]$ there exists a unique factorization modulo k^*. It follows from Lemma 1.10 that f_i is homogeneous for all i. $\square$

Remark 1.12. Let $f \in k[x, y, z]$ be a nonzero homogeneous polynomial. Since $k[x, y, z]$ is a subset of $\bar{k}[x, y, z]$ and since $\bar{k}$ is a field as well, one can consider the factorization of f either in $k[x, y, z]$ or in $\bar{k}[x, y, z]$.

Example 1.13. Consider the field of real numbers $\mathbb{R}$. Let $f \in \mathbb{R}[x, y, z]$ be the homogeneous polynomial given by $x^2 + y^2$. Since f is irreducible in $\mathbb{R}[x, y, z]$, the factorization of f in $\mathbb{R}[x, y, z]$ is given by $(x^2 + y^2)^1$. Now consider the field of complex numbers $\mathbb{C}$ which is the algebraic closure of $\mathbb{R}$. The factorization of f in $\mathbb{C}[x, y, z]$ is given by $(x - iy)^1(x + iy)^1$.

Notation 1.14. Let $f, g \in k[x, y, z]$ be two nonzero homogeneous polynomials and let their factorizations in $\bar{k}[x, y, z]$ be given as in Lemma 1.11. The *greatest common divisor* or *gcd* of f and g is a common divisor of f and g such that if polynomial h is a divisor of both f and g, then h divides the gcd of f and g. If for all i, j one has that $f_i \neq g_j$ modulo k^*, then one says that f and g are coprime and one writes $\gcd(f, g) = 1$.

Remark 1.15. Note that using the Euclidean algorithm for polynomials in one variable ([6], Theorem 1.6, p. 113) it can be shown that f and g are coprime in $\bar{k}[x, y, z]$ if and only if f and g are coprime in $k[x, y, z]$.

Curves of homogeneous polynomials

Given a homogeneous polynomial one can define its curve in the projective plane. Theorem 3.1 (Bézout's theorem) tells us about the number of intersection points of these so called curves.

Definition 1.16. Let $f \in k[x, y, z]$ be a nonzero homogeneous polynomial. The *curve of* f is the subset of $\mathbb{P}^2$ defined as the zero locus $\mathrm{Z}(f) := \{a \in \mathbb{P}^2 : f(a) = 0\}$.

Remark 1.17. Since $\bar{k}$ is algebraically closed it follows that if f is not constant, then $\mathrm{Z}(f)$ is infinite.

Example 1.18. Let $f, g \in \mathbb{R}[x, y, z]$ be two nonzero homogeneous polynomials given by xy and xy^2 respectively. The curves of f and g are both equal to the union of $\mathrm{Z}(x)$, the y-axis and $\mathrm{Z}(y)$, the x-axis.

The following lemma is fundamental for both the formulation and the proof of Bézout's theorem.

Lemma 1.19. Let $f, g \in k[x, y, z]$ be two nonzero coprime homogeneous polynomials. One has that the intersection of their curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$ is finite.

Proof. Let $f, g \in k[x, y, z]$ be two nonzero coprime homogeneous polynomials. From Remark 1.4 it follows that we can split $\mathrm{Z}(f) \cap \mathrm{Z}(g)$ into two disjoint subsets, the points which are elements of $\bar{k}^2$ and the remaining points.

Consider the former subset. All its elements are of the form $(a_1 : a_2 : 1)$. Hence, it is equivalent to study common vanishing points in $\bar{k}^2$ of the polynomials $f(x, y, 1)$ and $g(x, y, 1)$ in $k[x, y]$. Note that f and g are polynomials in one variable x with coefficients in the polynomial ring $k[y]$. Since $k[y]$ is a factorial ring with quotient field $k(y)$ it follows from

Gauss's lemma that f and g are coprime in $k(y)[x]$. Hence, there exist two rational functions $r_1, r_2 \in k(y)[x]$ such that the equality $r_1 f + r_2 g = 1$ holds. Multiplying this equation by a common (nonzero) multiple of the denominators of r_1 and r_2, say the polynomial $h \in k[y]$, shows that h is an element of the ideal (f, g) generated by $f(x, y, 1)$ and $g(x, y, 1)$ in $k[x, y]$. Hence, for all points (a_1, a_2) in $\bar{k}^2$ one has that if the equalities $f(a_1, a_2, 1) = g(a_1, a_2, 1) = 0$ hold, then one has that h vanishes at a_2. Hence, there exist only finitely many points a_2 in $\bar{k}$ such that the equalities $f(a_1, a_2, 1) = g(a_1, a_2, 1) = 0$ hold. Analogously, there exist only finitely many points a_1 in $\bar{k}$ such that the equalities $f(a_1, a_2, 1) = g(a_1, a_2, 1) = 0$ hold. It follows that there exist only finitely many points in in the intersection curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$ of the form $(a_1 : a_2 : 1)$.

Now consider the latter subset. Since there is only one point in this subset of the form $(1 : 0 : 0)$, it is sufficient to prove that there exist only finitely many points of the form $(b : 1 : 0)$. Note that at least one of the polynomials $f(x, 1, 0)$ and $g(x, 1, 0)$ in $k[x]$ is nonzero, otherwise z is a common divisor of f and g. Without loss of generality, assume that $f(x, 1, 0)$ is nonzero. There exist only finitely many points b in $\bar{k}$ such that the equality $f(b, 1, 0) = 0$ holds. Hence, there exist only finitely many points in the intersection of curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$ of the form $(b : 1 : 0) = 0$.

It follows that $\mathrm{Z}(f) \cap \mathrm{Z}(g)$ is finite. □

Lemma 1.20. Let $f, g \in k[x, y, z]$ be two nonzero homogeneous polynomials such that the curve of g is a subset of the curve of f; $\mathrm{Z}(g) \subset \mathrm{Z}(f)$. If g is irreducible, then g divides f and one writes $g|f$.

Proof. Let $f, g \in k[x, y, z]$ be two nonzero homogeneous polynomials with g irreducible and such that $\mathrm{Z}(g) \subset \mathrm{Z}(f)$. Assume that $g \nmid f$ so that f and g are coprime. From Lemma 1.19 it follows that $\mathrm{Z}(g) \cap \mathrm{Z}(f)$ is finite and so $\mathrm{Z}(g)$ is finite. Hence, from Remark 1.17 it follows that, g is constant and so g divides f. This is in contradiction with the assumption so g divides f. □

Corollary 1.21. Let $f, g \in k[x, y, z]$ be two nonzero irreducible homogeneous polynomials. If f and g have the same curve, then the equality $f = g$ modulo k^* holds.

Divisors of homogeneous polynomials

From Example 1.18 it follows that it is possible for two nonzero homogeneous polynomials, distinct up to k^*, to have the same curve in the projective plane. Hence, given a curve there does not exist one unique polynomial modulo k^* with this curve. We will now define divisors of homogeneous polynomials. Given a divisor, it follows from Corollary 1.21 that there exists a nonzero homogeneous polynomial, unique modulo k^*, giving this divisor.

Definition 1.22. A *prime divisor* in $\mathbb{P}^2$ is a subset of $\mathbb{P}^2$ of the form $\mathrm{Z}(f)$ with $f \in \bar{k}[x, y, z]$ a homogeneous irreducible polynomial.

Definition 1.23. Let $f \in \bar{k}[x, y, z]$ be a nonzero homogeneous polynomial and let the factorization of f be given as in Lemma 1.11. The *divisor of* f is defined by

$$\sum_{i \in I} e_i \cdot \mathrm{Z}(f_i) \quad \text{in} \quad \left\{ \{\text{prime divisors of } \mathbb{P}^2\} \xrightarrow{\varphi} \mathbb{Z} : \varphi \text{ has finite support} \right\}.$$

We will not use the divisor of a nonzero homogeneous polynomial in our computations. Later, in Definition 2.15 we will define the intersection cycle of two nonzero coprime homogeneous polynomials. This definition is rather similar to the definition above.

2 Intersection of curves

In this section we will define the intersection cycle of two nonzero coprime homogeneous polynomials. This intersection cycle is a way to write down common points of the curves of those two polynomials. In the definition of a divisor one can see that points have a form of multiplicity. In order to define these multiplicities we will first define the intersection multiplicity of two nonzero coprime homogeneous polynomials in a point of the projective plane. When we prove Bézout's theorem, we will use the intersection cycle in an algorithm to compute those common points and their multiplicities.

Definition of intersection multiplicity

We will first give a definition of the intersection multiplicity using the local ring of rational functions of zero degree modulo one of its ideals. Thereafter, we will prove some properties of the intersection multiplicity.

Definition 2.1. Let a be a point in the projective plane $\mathbb{P}^2$. The *local ring of rational functions of zero degree at the point a* is defined as

$$R_a := \left\{ \frac{s}{t} \in \bar{k}(x,y,z) : s,t \in \bar{k}[x,y,z] \text{ homogeneous of the same degree, } t(a) \neq 0 \right\}.$$

Definition 2.2. Let $f_1, \dots f_n \in \bar{k}[x,y,z]$ be homogeneous polynomials and let a be a point in the projective plane $\mathbb{P}^2$. The *ideal $(f_1,\dots,f_n)_a \subset R_a$ generated by $f_1,\dots,f_n$* is defined as the ideal ([6], p. 87) generated by the rational functions of zero degree $f_i/(t^{\partial f_i})$ for all i and with $t \in \{x,y,z\}$ such that t does not vanish at a. Hence,

$$(f_1,\dots,f_n)_a := \left\{ \frac{s}{t} \in R_a : \exists p_1,\dots,p_n \in \bar{k}[x,y,z] \text{ homogeneous}, s = p_1 f_1 + \dots + p_n f_n \right\}.$$

Definition 2.3. Let $f, g \in \bar{k}[x,y,z]$ be two nonzero coprime homogeneous polynomials and let a be a point in the projective plane $\mathbb{P}^2$. The *intersection multiplicity $i(a, f \cap g)$ of f and g at a* is defined as the dimension of the $\bar{k}$-vector space $R_a/(f,g)_a$. Hence

$$i(a, f \cap g) := \dim\left(R_a/(f,g)_a\right) \qquad \text{in} \qquad \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$

Remark 2.4. From the axioms of a $\bar{k}$-vector space it is easy to check that R_a is a $\bar{k}$-vector space with addition $R_a \times R_a \to R_a$ and scalar multiplication $\bar{k} \times R_a \to R_a$ defined by $(f,g) \mapsto f+g$ and $(v,f) \mapsto vf$ respectively. Hence, $R_a/(f,g)_a$ is indeed a $\bar{k}$-vector space and the intersection multiplicity $i(a, f \cap g)$ is well defined. Note that it is not obvious that this dimension is finite, although in [5] Hilmar and Smyth did not mention anything regarding the finiteness of the intersection multiplicity.

Properties of intersection multiplicity

In [5] the intersection multiplicity is defined in the same way as in this bachelor thesis. For a proof of Proposition 2.5 below, Hilmar and Smyth refer to [2]. In [2] Fulton uses another strategy to define the intersection multiplicity defined in Definition 2.3. He starts with describing the properties an intersection multiplicity should satisfy, including the properties given in this section. Thereafter, he proves that there exists only one definition of an intersection multiplicity having these properties. He uses Hilbert's Nullstellensatz ([2], page 20) and more commutative algebra to prove that the $\bar{k}$-vector space given in the definition above is finite dimensional. In order to avoid Hilbert's Nullstellensatz, we will prove Proposition 2.5 as part of Bézout's theorem in Section 3. The properties of the intersection multiplicity mentioned in this section will help us later in proving some computational tools of the intersection cycle, as defined at the end of said section.

Proposition 2.5. In the situation of Definition 2.3 above, the $\bar{k}$-vector space $R_a/(f,g)_a$ is finite dimensional.

Lemma 2.6. Let a be a point in the projective plane $\mathbb{P}^2$ and let $f, g \in k[x,y,z]$ be two nonzero coprime homogeneous polynomials. The intersection multiplicity $i(a, f \cap g)$ is strictly positive if a is an element of the intersection of curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$ and zero otherwise.

Proof. Let a be a point in the projective plane $\mathbb{P}^2$ and assume that a is not an element of in the intersection of curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$. Let s/t be a rational function of zero degree in R_a with nonzero $t(a)$. It follows that either the homogeneous polynomial ft or the homogeneous polynomial gt does not vanish at point a or neither of them does. Without loss of generality, assume that ft does not vanish at point a. Hence, one has that the rational function s/t is equal to fs/ft and so it follows that s/t is an element of the ideal $(f,g)_a$. So the local ring of rational functions of zero degree R_a is a subset of its own ideal $(f,g)_a$. Hence, the ideal generated by f and g is equal to R_a. It follows that for the intersection multiplicity of f and g at point a one has that

$$i(a, f \cap g) = \dim(R_a/R_a) = \dim(0) = 0.$$

Suppose that a is an element of the intersection of curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$. Let s/t be a rational function of zero degree in the ideal $(f,g)_a$ with nonzero $t(a)$, so s is a linear combination of f and g. Since a is an element of the intersection of curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$, one has that s/t vanishes at point a. Hence, all elements of $(f,g)_a$ vanish at a. Since $1 = 1/1$ is an element of the polynomial ring $\bar{k}[x,y,z]$, but 1 does not vanish at a, one has that $(f,g)_a$ is not equal to R_a. Thus, for the intersection multiplicity of f and g at point a, it follows that

$$i(a, f \cap g) = \dim(R_a/(f,g)_a) > 0.$$

$\square$

Lemma 2.7. Let a be a point in the projective plane $\mathbb{P}^2$ and let $f, g \in k[x,y,z]$ be two nonzero coprime homogeneous polynomials. For the intersection multiplicity of f and g at point a one has that $i(a, f \cap g) = i(a, g \cap f)$.

Proof. Let a be a point in the projective plane $\mathbb{P}^2$ and let $f, g \in k[x,y,z]$ be two nonzero homogeneous polynomials such that f and g are coprime. It follows directly from Definition 2.2 that one has that $(f,g)_a = (g,f)_a$. Hence, the equality $i(a, f \cap g) = i(a, g \cap f)$ holds. $\square$

In order to prove Lemma 2.10 we will first prove the following two lemmas.

Lemma 2.8. Let A be a ring and let $v, w \in A$ be two of its elements such that the maps $v\cdot, w\cdot : A \longrightarrow A$ given by $x \longmapsto vx$ and $x \longmapsto wx$ respectively are injective. One has that $w\cdot$ induces a morphism of A-modules $A/(v) \longrightarrow A/(vw)$ and the sequence

$$0 \longrightarrow A/(v) \xrightarrow{w\cdot} A/(vw) \xrightarrow{q} A/(w) \longrightarrow 0$$

is exact, with q the quotient map.

Proof. Let A be a ring and let $v, w \in A$ be two of its element such as in the lemma. Since A is a ring, A is an abelian group. We can define the map $A \times A \longrightarrow A$ given by $(y,x) \longmapsto yx$ which defines A as an A-module ([6], p. 192). Since $(v), (vw)$ and (w) are submodules of A-module A, one can construct the factor modules $A/(v), A/(vw)$ and $A/(w)$ respectively. Let ψ and φ be the two maps induced by the map $w\cdot$ and the quotient map q respectively. Hence,

$$\begin{aligned} \psi : A/(v) &\longrightarrow A/(vw) \\ \overline{x} &\longmapsto \overline{wx} \end{aligned} \quad \text{and} \quad \begin{aligned} \varphi : A/(vw) &\longrightarrow A/(w) \\ \overline{x} &\longmapsto \overline{x} \end{aligned} .$$

Note that both ψ and φ are morphisms of A-modules. It is sufficient to prove that the sequence

$$0 \longrightarrow A/(v) \xrightarrow{\psi} A/(vw) \xrightarrow{\varphi} A/(w) \longrightarrow 0 \tag{1}$$

is exact.

Claim 1: The map ψ is injective. Let x be an element of A such that $\psi(\overline{x}) = \overline{wx}$ vanishes in $A/(vw)$. It follows that one has that $\psi(\overline{x}) = \overline{n(vw)} = \overline{w(nv)}$ in $A/(vw)$ for some element n in A. Since $w\cdot$ is injective, the equality $x = nv$ holds. One has that $\overline{nv}$ vanishes in $A/(v)$, which proves that the kernel of ψ is trivial and so that ψ is injective.

Claim 2: The map φ is surjective. This is because φ is the quotient map.

Claim 3: The image of ψ is equal to the kernel of φ. Let y be an element A such that $\overline{y}$ in $A/(vw)$ is an element of the image of ψ. Hence, there exists an element x in A such that one has that $y = wx$ in A. It follows that $\varphi(\overline{y})$ is equal to $\overline{wx}$ which vanishes in $A/(w)$. This implies that $\overline{y}$ is an element of the kernel of φ and so the image of ψ is a subset of the kernel of φ. Now, let y be an element of A such that $\overline{y}$ in $A/(vw)$ is an element of the kernel of φ. Hence, there exists an element x in A such that y is equal to wx in A. One has that $\psi(\overline{x})$ is equal to $\overline{wx}$ in $A/(vw)$ and so it is equal to $\overline{y}$, which implies that $\overline{y}$ is an element of the image of ψ and so the image of ψ is a subset of the kernel of φ. This proves that the image of ψ is equal to the kernel of φ.

From Claim 1, 2 and 3 it follows that the sequence (1) is exact, which completes the proof of this lemma. □

Lemma 2.9. Let

$$0 \longrightarrow U \xrightarrow{e} V \xrightarrow{p} W \longrightarrow 0 \tag{2}$$

be an exact sequence of $\bar{k}$-vector spaces. One has that

$$\dim U + \dim W = \dim V.$$

Proof. Let $(u_i)_{i\in I}$ and $(w_j)_{j\in J}$ be two bases of U and W respectively. Note that these bases may be infinite. Let e be the embedding of U into V and let p be a projection of V onto W. Let $(v_j)_{j\in J}$ be elements of V such that for all j one has that the equality $p(v_j) = w_j$ holds. It is sufficient to prove the following claim. Claim: $(e(u_i)_{i\in I}, (v_j)_{j\in J})$ is a base of V. Firstly, let v be an element of V. There exist unique elements $\{\lambda_j\}_{j\in J}$ in $\bar{k}$ such that the equality $p(v) = \sum_{j\in J} \lambda_j w_j$ holds. One has that

$$p\left(\sum_{j\in J} \lambda_j v_j\right) = \sum_{j\in J} \lambda_j w_j. \text{ Hence, } p\left(v - \sum_{j\in J} \lambda_j v_j\right) = p(v) - p\left(\sum_{j\in J} \lambda_j v_j\right)$$

vanishes in W. It follows that $v - \sum_{j\in J} \lambda_j v_j$ is an element of the kernel of p and since (2) is exact, it is an element of the image of e as well. This implies that there exists a unique element u in U such that $e(u)$ is equal to $v - \sum_{j\in J} \lambda_j v_j$. Secondly, there exist unique elements $\{\mu_i\}_{i\in I}$ in $\bar{k}$ such that the equality $u = \sum_{i\in I} \mu_i u_i$ holds. Hence, e maps u into $\sum_{i\in I} \mu_i e(u_i)$. It follows that one has that

$$v = \sum_{i\in I} \mu_i e(u_i) + \sum_{j\in J} \lambda_j w_j.$$

Since the elements $\{\lambda_j\}_{j\in J}$ $\{\mu_i\}_{i\in I}$ are unique, the latter proves the claim and so the lemma. □

Using Lemma 2.8 and Lemma 2.9 we can prove the following lemma.

Lemma 2.10. Let a be a point in the projective plane $\mathbb{P}^2$ and let $f, g, h \in k[x, y, z]$ be three nonzero homogeneous polynomials such that f is coprime with both g and h. For the intersection multiplicity of f and gh at a one has that $i(a, f \cap gh) = i(a, f \cap g) + i(a, f \cap h)$.

Proof. Let A be the ring $R_a/(f)_a$ and let its elements v and w be equal to $g/(t^{\partial g})$ and $h/(t^{\partial h})$ respectively with t in $\{x, y, z\}$ such that t does not vanish at a. The mapping $v\cdot$ defined as in Lemma 2.8 is injective, since if there exist three elements p_1, p_2, q in A such that both the equalities $vp_1 = q$ and $vp_2 = q$ hold, then it follows that one has $p_1 = p_2$. Likewise one can prove that the mapping $w\cdot$ defined as in Lemma 2.8 is injective. Hence, from this same lemma it follows that $w\cdot$ induces a morphism of A-modules $A/(v) \longrightarrow A/(vw)$ and the sequence of $\bar{k}$-vector spaces

$$0 \longrightarrow R_a/(f, g)_a \longrightarrow R_a/(f, gh)_a \longrightarrow R_a/(f, h)_a \longrightarrow 0$$

is exact. From Lemma 2.9 it follows that one has that

$$\dim(R_a/(f, g)_a) + \dim(R_a/(f, h)_a) = \dim(R_a/(f, gh)_a)$$

which completes the proof. □

Lemma 2.11. Let a be a point in the projective plane $\mathbb{P}^2$ and let $f, g, h \in k[x, y, z]$ be three nonzero homogeneous polynomials such that f and g are coprime and such that fh and g have the same degrees. For the intersection multiplicity of f and $g + fh$ one has that $i(a, f \cap (g + fh) = i(a, f \cap g)$.

Proof. Let a be a point in the projective plane $\mathbb{P}^2$ and let $f, g, h \in k[x, y, z]$ be three nonzero homogeneous polynomials such that f and g are coprime and such that fh and g have the same degrees. Let $t \in \{x, y, z\}$ such that t does not vanish at a. One has that

$$(f, g + fh)_a = \left(\frac{f}{t^{\partial f}}, \frac{g}{t^{\partial g}} + \frac{f}{t^{\partial f}} \cdot \frac{h}{t^{\partial h}}\right)_a = \left(\frac{f}{t^{\partial f}}, \frac{g}{t^{\partial g}}\right)_a = (f, g)_a.$$

Hence, for the intersection multiplicity of f and $g+fh$ one has $i(a, f \cap (g+fh) = i(a, f \cap g)$. □

Lemma 2.12. Let $l, m \in k[x, y, z]$ be two nonzero distinct modulo k^* homogeneous polynomials of degree 1 given by $l_1x + l_2y + l_3z$ and $m_1x + m_2y + m_3z$ respectively. For the intersection of their curves one has that $\mathrm{Z}(l) \cap \mathrm{Z}(m) = \{p_\times\}$ with intersection multiplicity $i(p_\times, l \cap m) = 1$. The point $p_\times$ of the projective plane is given by

$$p_\times := \left(\begin{vmatrix} l_2 & l_3 \\ m_2 & m_3 \end{vmatrix}, \begin{vmatrix} l_3 & l_1 \\ m_3 & m_1 \end{vmatrix}, \begin{vmatrix} l_1 & l_2 \\ m_1 & m_2 \end{vmatrix} \right).$$

Proof. Let $l, m \in k[x, y, z]$ be two nonzero distinct homogeneous polynomials of degree 1 given by $l_1x + l_2y + l_3z$ and $m_1x + m_2y + m_3z$ respectively. From Cramer's rule it follows that the unique point on both lines is indeed $p_\times$ defined as in the lemma. Since l and m are distinct, it follows that they are independent, and since the dimension of k^3 is equal to 3, there exist elements n_1, n_2, n_3 in k such that the matrix

$$J := \begin{pmatrix} l_1 & l_2 & l_3 \\ m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{pmatrix}$$

has nonzero determinant. Let $n \in k[x, y, z]$ be the nonzero homogeneous polynomial of degree 1 given by $n_1x + n_2y + n_3z$. Since the equality $J \begin{pmatrix} x & y & z \end{pmatrix}^T = \begin{pmatrix} l & m & n \end{pmatrix}^T$ holds, it follows that the equality $\begin{pmatrix} x & y & z \end{pmatrix}^T = J^{-1} \begin{pmatrix} l & m & n \end{pmatrix}^T$ holds as well. Hence, all polynomials in $\bar{k}[x, y, z]$ can be written as polynomials in $\bar{k}[l, m, n]$. Let q be a rational function of zero degree in $R_{p_\times}$. For some positive integer r there exist two homogeneous polynomials s_2, t_2 in $\bar{k}[l, m, n]$ both of degree $r-1$ and two homogeneous polynomials s_1, t_1 in $\bar{k}[m, n]$ both of degree $r-1$ and two elements s_0, t_0 in $\bar{k}$ with nonzero t_0 such that the equality

$$q = \frac{ls_2 + ms_1 + s_0 n^r}{lt_2 + mt_1 + t_0 n^r}$$

holds. Note that both $(lt_2 + mt_1 + t_0 n^r)$ and t_0 do not vanish at the point $p_\times$. One has that

$$q - \frac{s_0}{t_0} = \frac{l(s_2 t_0 - s_0 t_2) + m(s_1 t_0 - s_0 t_1)}{lt_0 t_2 + mt_0 t_1 + t_0^2 n^r}$$

is an element of the ideal $(l, m)_{p_\times}$. Since $\frac{s_0}{t_0}$ is an element of $\bar{k}$, one has that the dimension of $R_{p_\times}/(l, m)_{p_\times}$ is equal to 1. Hence, for the intersection multiplicity, one has $i(p_\times, l \cap m) = 1$. $\square$

Intersection cycle

In order to define the intersection cycle we will first define the intersection function. The definition of the intersection cycle reminds us strongly of the definition of a divisor. After the definition of the intersection cycle of two nonzero coprime homogeneous polynomials we will formulate a proposition with computational tools for the intersection cycle. Its proof will follow directly from the properties of the intersection multiplicity mentioned in the previous section.

Definition 2.13. Let $f, g \in k[x, y, z]$ be two nonzero coprime homogeneous polynomials. The *intersection function of f and g* is defined as

$$i(f, g) : \mathbb{P}^2 \longrightarrow \mathbb{Z}_{\geq 0} \cup \{\infty\} \quad \text{with} \quad a \longmapsto i(a, f \cap g).$$

Later we will see that as a consequence of Bézout's theorem, for all a the intersection multiplicity $i(a, f \cap g)$ is in $\mathbb{Z}$.

Lemma 2.14. The intersection function defined above has finite support.

Proof. Since f and g are coprime it follows from Lemma 1.19 that the intersection of their curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$ is finite. From Lemma 2.6 it follows that points a in the projective plane $\mathbb{P}^2$ have zero intersection multiplicity $i(a, f \cap g)$ if and only if a is not an element of the intersection of the curves $\mathrm{Z}(f) \cap \mathrm{Z}(g)$. Hence, the intersection function has finite support. $\square$

Definition 2.15. Let $f, g \in k[x, y, z]$ be two nonzero coprime homogeneous polynomials. The *intersection cycle of f and g* is defined as

$$f \cap g := \sum_{a \in \mathbb{P}^2} i(a, f \cap g) a \quad \text{in} \quad \left\{ \mathbb{P}^2 \xrightarrow{\varphi} \mathbb{Z} \cup \{\infty\} : \varphi \text{ has finite support} \right\}.$$

Let the sum of the intersection multiplicities of all points a in the projective plane $\mathbb{P}^2$

$$\#(f \cap g) := \sum_{a \in \mathbb{P}^2} i(a, f \cap g) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$$

denote the *intersection number of f and g*.

Note that from Definition 2.13 and Lemma 2.14 it follows that both the intersection cycle of f and g and the intersection number of f and g are well defined and that $\#(f \cap g)$ is in $\mathbb{Z}$ if all $i(a, f \cap g)$ are in $\mathbb{Z}$.

Proposition 2.16. Let $f, g, h \in k[x, y, z]$ be three nonzero homogeneous polynomials such that f and g are coprime. The following properties of their intersection cycles and intersection numbers hold.

(i) $f \cap g = g \cap f$;

(ii) If f and h are coprime, then $f \cap (gh) = f \cap g + f \cap h$;

(iii) If $\partial g = \partial(fh)$, then $f \cap (g + fh) = f \cap g$;

(iv) If f and g are two distinct homogeneous polynomials of degree 1, then $\#(f \cap g) = 1$.

Proof. Properties (i), (ii), (iii) and (iv) follow directly from the proofs of Lemma 2.7, 2.10, 2.11 and 2.12 respectively. □

3 Bézout's theorem

With the definition of the intersection number of two nonzero coprime homogeneous polynomials given in the previous section, we can now finally formulate Bézout's theorem. Subsequently, we will examine an example where one uses this theorem. In order to proof Bézout's theorem, we will simplify the theorem to the situation where one of the polynomials is a union of lines. Proposition 3.3 is a proof for this simplified problem. In order to finish the proof of Bézout's theorem we will introduce an algorithm which reminds us strongly of the Euclidean algorithm to find the greatest common divisor of two integers. This algorithm uses the properties of the intersection cycle given in Proposition 2.16 in order to simplify the intersection cycle of two arbitrary nonzero coprime homogeneous polynomials. In the end, the proof of Bézout's theorem will be a concise proof by induction.

Theorem 3.1 (Bézout (1730 - 1783))**.** Let $f, g \in k[x, y, z]$ be two nonzero coprime homogeneous polynomials of degrees m and n respectively. For all points a in the projective plane $\mathbb{P}^2$ the intersection multiplicity $i(a, f \cap g)$ is finite. The intersection number of f and g is given by $\#(f \cap g) = mn$.

Example 3.2. *Consider the field of real numbers $\mathbb{R}$ and let the two homogeneous polynomials $f, g \in k[x, y, z]$ be given by $y^2z - x^3$ and $y^2z - x^2(x + z)$ respectively. Compute all intersection points of f and g in the projective plane and their multiplicities. In other words, determine the intersection $Z(f) \cap Z(g)$ of the curves of f and g.*

Note that f and g are coprime. Hence, we can examine the intersection cycle $f \cap g$. From Proposition 2.16(i) it follows for the intersection cycle of f and g that one has that $f \cap g = g \cap f$. Interpret f and g as two polynomials in one variable x with coefficients in $\mathbb{R}[y, z]$. Use polynomial long division ([6], Theorem 1.6, p. 113) to divide f through by g. One obtains that f is equal to $1 \cdot g + x^2z = x^2z + g \cdot 1$ and so for the intersection cycle of g and f one has that

$$g \cap f = g \cap (x^2z + g \cdot 1).$$

It follows from Proposition 2.16(iii) that for the latter intersection cycle the equality

$$g \cap (x^2z + g \cdot 1) = g \cap (x^2z)$$

holds. From Proposition 2.16(ii) it follows that for the intersection cycle of g and x^2z one has that

$$g \cap (x^2z) = 2(g \cap x) + g \cap z.$$

Finally, using Proposition 2.16(ii) and (iii) again, one computes the intersection cycles

$$g \cap x = (y^2z) \cap x = 2(y \cap x) + z \cap x = 2(0 : 0 : 1) + (0 : 1 : 0)$$

and

$$g \cap z = (x^3) \cap z = 3(x \cap z) = 3(0:1:0).$$

Hence, one obtains that

$$f \cap g = 4(0:0:1) + 5(0:1:0).$$

Note that the intersection number of f and g is equal to 9, which follows as well from Bézout's theorem.

Intersecting with a union of lines

In this subsection we will proof Bézout's theorem for a simplified situation, the situation stated in Proposition 3.3. This is the first step of the proof by induction of Bézout's theorem.

Proposition 3.3. Let $f \in k[x,y,z]$ and $g \in k[y,z]$ be two nonzero coprime homogeneous polynomials of degrees m and n respectively. For all points a in the projective plane $\mathbb{P}^2$ one has that the intersection multiplicity $i(a, f \cap g)$ is finite. The intersection number of f and g is given by $\#(f \cap g) = mn$.

Proof. Let $f \in k[x,y,z]$ and $g \in k[y,z]$ be two coprime homogeneous polynomials of degrees m and n respectively. We will prove the proposition for two different cases.

Firstly, assume that the polynomial g has zero y-degree as well. Hence, one has that g is an element of $k[z]$ so g is of the form $g = \lambda z^n$ for some element λ in k^*. There exists a homogeneous polynomial $f' \in k[x,y,z]$ of degree $m-1$ such that one has that

$$f(x,y,z) = f(x,y,0) + zf'(x,y,z).$$

Note that $f(x,y,0)$ is nonzero since z and f are coprime and that $f(x,y,0)$ and f' are both homogeneous polynomials of degree m and $m-1$ respectively. Hence, it follows from Proposition 2.16(iii) that for the intersection cycle of f and z one has that

$$f \cap z = (f(x,y,0) + zf'(x,y,z)) \cap z = f(x,y,0) \cap z.$$

Since $f(x,y,0)$ is a homogeneous polynomial of degree m it follows from Lemma 1.11 and Remark 1.12 that one can factorize $f(x,y,0)$ into $\mu \prod_{i=1}^{m} f_i$ with element μ in k^* and homogeneous irreducible polynomials f_i in $\bar{k}[x,y]$. Choose an order to the f_i's such that $f_1, \ldots, f_t$ are elements of $\bar{k}[y]$ with zero x-degree and $f_{t+1}, \ldots, f_m$ are elements of $\bar{k}[x,y]$ with nonzero x-degree for some constant t with $0 \leq t \leq m$. From Proposition 2.16(ii) it follows that for the intersection cycle of polynomials $f(x,y,0)$ and z one has that

$$f(x,y,0) \cap z = \left(\mu \prod_{i=1}^{m} f_i\right) \cap z = \sum_{i=1}^{m} (f_i \cap z).$$

For all i in $\{1, \ldots, t\}$ note that f_i is of the form $\nu_i y$ with element ν_i in $\bar{k}^*$, so it follows that for the intersection cycle of f_i and z one has that $f_i \cap z = y \cap z = (1:0:0)$. For all i in $\{t+1, \ldots, m\}$ one has that homogeneous polynomial f_i has degree 1, so f_i is a line in $\bar{k}[x,y]$. Let $\alpha_{t+1}, \ldots, \alpha_m$ in $\bar{k}$ be the (not necessarily distinct) roots of the polynomials $f_{t+1}(x,1), \ldots, f_m(x,1)$ respectively. Since these are homogeneous polynomials of degree 1 with nonzero x-degree it follows that for all i in $\{t+1, \ldots, m\}$ one has that f_i is equal to $(x - \alpha_i y)$. Hence, for these f_i one has that the intersection cycles with z are given by $f_i \cap z = (x - \alpha_i y) \cap z = (\alpha_i : 1 : 0)$. Hence, for the intersection cycle of f and g one has that

$$\begin{aligned} f \cap g &= f \cap (\lambda z^n) = n(f \cap z) = n\,(f(x,y,0) \cap z) = n\left(\sum_{i=1}^{m} (f_i \cap z)\right) \\ &= n\left(t(1:0:0) + \sum_{i=t+1}^{m} (\alpha_i : 1 : 0)\right). \end{aligned}$$

Since the intersection cycle $f \cap g$ given above is a finite sum it follows that for all points $a \in \mathbb{P}^2$ in the projective plane the intersection multiplicity $i(a, f \cap g)$ is finite and that the intersection number of f and g is given by $\#(f \cap g) = mn$.

Secondly, assume that polynomial g has nonzero y-degree. Just as the factorization of $f(x, y, 0)$ in the situation above, one can factorize g into $\lambda \prod_{i=1}^{n} g_i$ with element λ in k^* and homogeneous irreducible polynomials $g_1, \ldots, g_r$ equal to z modulo $\bar{k}^*$ and homogeneous irreducible polynomials $g_{r+1}, \ldots, g_n$ of the form $y - \beta_i z$ with (not necessarily distinct) roots $\beta_{r+1}, \ldots, \beta_n$ in $\bar{k}$ for some constant r with $0 \leq r \leq n$. Note that for the former types of g_i, the situation is analogue to the situation above, so one has that

$$f \cap z = f(x, y, 0) \cap z = q(1 : 0 : 0) + \sum_{i=q+1}^{m} (\alpha_i : 1 : 0)$$

for some constant q. There exists a homogeneous polynomial $f' \in k[x, y, z]$ of degree $m - 1$ such that for any element β in $\bar{k}$ and the homogeneous polynomial f the equality

$$f = f(x, \beta z, z) + (y - \beta z) f'(x, y, z)$$

holds. It follows from Proposition 2.16(iii) that for any element β in $\bar{k}$ the intersection cycle of f and line $(y - \beta z)$ is given by

$$f \cap (y - \beta z) = (f(x, \beta z, z) + (y - \beta z) f'(x, y, z)) \cap (y - \beta z) = f(x, \beta z, z) \cap (y - \beta z).$$

Again, analogous to the factorizations of $f(x, y, 0)$ and g above, for all i in $\{r + 1, \ldots, n\}$ one can factorize $f(x, \beta_i z, z)$ into $\mu_i \prod_{j=1}^{m} f_{ij}$ with elements μ_i in k^* and homogeneous irreducible polynomials $f_{i1}, \ldots, f_{is_i}$ in $\bar{k}(\beta_i)[z]$ with zero x-degree and homogeneous irreducible polynomials $f_{i(s_i+1)}, \ldots, f_{im}$ in $\bar{k}(\beta)[x, z]$ with nonzero x-degree for some constants s_i with $0 \leq s_i \leq m$. Hence, the homogeneous irreducible polynomials $f_{i1}, \ldots, f_{is_i}$ are equal to z modulo $k(\beta_i)^*$. For any element β in $\bar{k}$ it follows from Proposition 2.16(iii) that for the intersection cycle of these homogeneous polynomials f_{ij} and line $(y - \beta z)$ one has that

$$f_{ij} \cap (y - \beta z) = z \cap (y - \beta z) = z \cap y = (1 : 0 : 0).$$

Otherwise, if j is an element of $\{s_i + 1, \ldots, m\}$, then f_{ij} is a homogeneous polynomial of degree 1 in $\bar{k}(\beta)[x, z]$ with nonzero x-degree. For all i, j let elements γ_{ij} in $\bar{k}(\beta_i)$ be the root of the polynomial $f_{ij}(x, 1)$. Hence, one has that $f_{ij}(x, z)$ is equal to $(x - \gamma_{ij} z)$. It follows that for these polynomials and for all elements β in $\bar{k}$ one has that

$$f_{ij} \cap (y - \beta z) = (x - \gamma_{ij} z) \cap (y - \beta z) = (\gamma_{ij} : \beta : 1).$$

Hence, for the intersection cycle of $f \in k[x, y, z]$ and $g \in k[y, z]$ with nonzero x-degree one has that

$$\begin{aligned}
f \cap g &= f \cap \left(\lambda \prod_{i=1}^{n} g_i \right) = \sum_{i=1}^{n} (f \cap g_i) = \sum_{i=1}^{t} (f \cap z) + \sum_{i=t+1}^{n} (f \cap (y - \beta_i z)) \\
&= \sum_{i=1}^{t} (f \cap z) + \sum_{i=t+1}^{n} (f(x, \beta_i z, z) \cap (y - \beta_i z)) \\
&= \sum_{i=1}^{t} (f \cap z) + \sum_{i=t+1}^{n} \left[\left(\mu_i \prod_{j=1}^{m} f_{ij} \right) \cap (y - \beta_i z) \right] \\
&= \sum_{i=1}^{t} (f \cap z) + \sum_{i=t+1}^{n} \left[\sum_{j=1}^{m} (f_{ij} \cap (y - \beta_i z)) \right] \\
&= \sum_{i=1}^{t} (f \cap z) + \sum_{i=t+1}^{n} \left[s_i (1:0:0) + \sum_{j=s_i+1}^{m} (\gamma_{ij} : \beta_i : 1) \right] \\
&= \sum_{i=1}^{t} \left[q(1:0:0) + \sum_{i=q+1}^{m} (\alpha_i : 1 : 0) \right] + \sum_{i=t+1}^{n} \left[s_i (1:0:0) + \sum_{j=s_i+1}^{m} (\gamma_{ij} : \beta_i : 1) \right].
\end{aligned}$$

Since the intersection cycle $f \cap g$ given above is a finite sum it follows that for all points $a \in \mathbb{P}^2$ in the projective plane the intersection multiplicity $i(a, f \cap g)$ is finite and that the intersection number of f and g is given by $\#(f \cap g) = mn$. $\square$

The Euclidean Algorithm

In this section we will define an algorithm which reminds us strongly of the Euclidean algorithm to compute the greatest common divisor of two integers. Given two nonzero homogeneous polynomials of arbitrary degrees, the algorithm simplifies the computation of their intersection cycle. Instead of computing this intersection cycle, we can compute intersection cycles of two polynomials of which at least one has zero x-degree. Proposition 3.3 gives us the proof of Bézout's theorem for these intersection cycles, thus we can finish the proof by induction on the minimum of the x-degrees of f and g.

Algorithm 3.4. INPUT: Two nonzero coprime homogeneous polynomials $f, g \in k[x, y, z]$ of degree n and m respectively such that the inequality $\partial_x f \geq \partial_x g \geq 1$ holds.

OUTPUT: Four homogeneous polynomials $r, g', h, c \in k[x, y, z]$ such that one has the equation of intersection cycles $f \cap g = r \cap g' - h \cap g' + f \cap c$ holds and such that for the x-degrees one has that $\partial_x r < \partial_x g' = \partial_x g$ and $\partial_x h = \partial_x c = 0$.

Note that all homogeneous polynomial of zero x-degree in $\bar{k}[y, z]$ are products of homogeneous polynomials of degree 1. In the previous subsection we proved Bézout's theorem for the situation where at least one of the homogeneous polynomials is such a product.

Step (1) Find the unique rational functions $Q, R \in k(y, z)[x]$ with $0 \leq \partial_x R < \partial_x g$ and $R \neq 0$ and $f = Qg + R$.

Step (2) Define the homogeneous polynomial $\widetilde{h} \in k[y, z]$ as the least common multiple of the denominators of the rational functions Q and R to get $\widetilde{h} f = \widetilde{q} g + \widetilde{r}$, with homogeneous polynomials $\widetilde{q} = Q\widetilde{h}$ and $\widetilde{r} = R\widetilde{h}$ in $k[x, y, z]$.

Step (3) Define the homogeneous polynomial $c := \gcd(g, \widetilde{r}) = \gcd(g, \widetilde{h}) \in k[x, y, z]$ and divide through by c to get $hf = \widetilde{q} g' + r$, where $g = g'c$, $\widetilde{h} = hc$ and $\widetilde{r} = rc$ are homogeneous polynomials.

Step (4) Now one has four homogeneous polynomials $r, g', h, c \in k[x, y, z]$ such that the equation of intersection cycles

$$f \cap g = r \cap g' - h \cap g' + f \cap c$$

holds and such that for the x-degrees one has that $\partial_x r < \partial_x g' = \partial_x g$ and $\partial_x h = \partial_x c = 0$.

Proposition 3.6 states that the algorithm above is correct. In order to prove this proposition, we need the following lemma.

Lemma 3.5. The polynomials $\widetilde{h}, \widetilde{q}$ and $\widetilde{r} \in k[x, y, z]$ given in the algorithm are homogeneous.

Proof. Note that $\bar{k}[x, y, z]$ is both a ring and a $\bar{k}$-vectorspace with the same group structures in such a manner that the axiom $(\lambda a)b = a(\lambda b) = \lambda(ab)$ is satisfied for all elements λ in $\bar{k}$ and a, b in $\bar{k}[x, y, z]$. Hence, $\bar{k}[x, y, z]$ is a $\bar{k}$-*algebra* ([4], p. 3). The group $\bar{k}^*$ acts on the $\bar{k}$-algebra $\bar{k}[x, y, z]$ as follows

$$\bar{k}^* \times \bar{k}[x, y, z] \longrightarrow \bar{k}[x, y, z], \quad (\lambda, f) \longmapsto \lambda \star f$$

where for $\lambda \in \bar{k}^*$

$$\bar{k}[x, y, z] \longrightarrow \bar{k}[x, y, z], \quad f \longmapsto \lambda \star f$$

is the $\bar{k}$-algebra automorphism given by $x \mapsto \lambda x$, $y \mapsto \lambda y$, $z \mapsto \lambda z$ and $a \mapsto a$ for all a in $\bar{k}$. This induces a $\bar{k}$-algebra automorphism $\lambda\star$ on $\bar{k}(x, y, z)$ and in particular on $\bar{k}(y, z)[x]$. For the equation in Step (1) one has that

$$\lambda \star f = (\lambda \star Q) \cdot (\lambda \star g) + \lambda \star R.$$

Note that for all polynomials $p \in \bar{k}[x, y, z]$ one has that $\lambda \star p$ is equal to $\lambda^d p$ for all $\lambda \in \bar{k}^*$ if and only if p is a homogeneous polynomial of degree d. Since both f and g in Algorithm 3.4 are homogeneous polynomials of degrees n and m respectively, it follows that both the equalities $\lambda \star f = \lambda^n f$ and $\lambda \star g = \lambda^m g$ hold. Firstly, one has that

$$\lambda^n f = (\lambda \star Q) \cdot (\lambda^m g) + \lambda \star R. \tag{3}$$

Since the equality $f = Qg + R$ is a division with remainder, it follows that (3) is a division with remainder as well. Secondly one has that

$$\lambda^n f = \lambda^n Q g + \lambda^n R = (\lambda^{n-m} Q) \cdot (\lambda \star g) + \lambda^n R. \tag{4}$$

Since (4) is also a division with remainder, it follows from the uniqueness of division with remainder that the equalities $\lambda \star Q = \lambda^{n-m} Q$ and $\lambda \star R = \lambda^n R$ hold.

Write $R = R_1/R_2$ with the unique polynomials R_1 in $\bar{k}[x, y, z]$ and R_2 in $\bar{k}[y, z]$ such that $\gcd(R_1, R_2) = 1$ and with $y^i z^j$ the greatest monomial of R_2 according to the graded lexicographic monomial order ([3], Example 2.5, p. 13). In other words, R_2 is monic for the graded lexicographic monomial order. One has that $\lambda \star R = (\lambda \star R_1)/(\lambda \star R_2)$ and that $\lambda \star R = \lambda^n R = \lambda^n (R_1/R_2)$. Therefore it follows that the equality

$$\frac{\lambda \star R_1}{\lambda \star R_2} = \lambda^n \frac{R_1}{R_2} \tag{5}$$

holds. Since $y^i z^j$ is a homogeneous monomial, one has that $\lambda\star(y^i z^j) = \lambda^{i+j} y^i z^j$. Therefore, and from (5), it follows that both the equalities

$$\lambda \star R_2 = \lambda^{i+j} R_2 \quad \text{and} \quad \lambda \star R_1 = \lambda^{n+i+j} R_2$$

hold. Hence, both R_1 and R_2 are homogeneous polynomials. Just as R, write $Q = Q_1/Q_2$ with the same requirements to Q_1 in $\bar{k}[x, y, z]$ and Q_2 in $\bar{k}[x, y, z]$ as R_1 and R_2 respectively. Analogously to R_1 and R_2, one can prove that both Q_1 and Q_2 are homogeneous polynomials.

Since $\tilde{h}$ in Algorithm 3.4 is the least common multiple of Q_2 and R_2 and since the factorizations of Q_2 and R_2 as in Lemma 1.11 consist of homogeneous polynomials, it follows that $\tilde{h}$ is a homogeneous polynomial as well. Let d be the degree of $\tilde{h}$ so the equality $\lambda \star \tilde{h} = \lambda^d \tilde{h}$ holds. One has that

$$\lambda \star \widetilde{r} = (\lambda \star R)(\lambda \star \widetilde{h}) = \left(\frac{\lambda^{n+i+j} R_1}{\lambda^{i+j} R_2} \right) (\lambda^d \widetilde{h}) = \lambda^{n+d} \left(\frac{R_1 \widetilde{h}}{R_2} \right) = \lambda^{n+d} R \widetilde{h} = \lambda^{n+d} \widetilde{r}.$$

Since R_2 divides $\widetilde{h}$, one has that $\widetilde{r}$ is an element of $k[x, y, z]$. Hence, $\widetilde{r}$ is a homogeneous polynomial in $k[x, y, z]$. Analogously to $\widetilde{r}$, one can prove that $\widetilde{q}$ is a homogeneous polynomial in $k[x, y, z]$. □

Proposition 3.6. Algorithm 3.4 is correct.

Proof. Firstly, note that since $\partial_x h = \partial_x c = 0$, it follows from Proposition 3.3 that the intersection cycles $h \cap g'$ and $f \cap c$ are finite. In Step (1) one can find the unique rational functions Q, R given in the algorithm by polynomial long division of polynomials in x with coefficients in $k(y, z)$ ([6], Theorem 1.6, p. 113) of f through by g. Note that since f and g are coprime it follows that R is nonzero. In Lemma 3.5 we proved that the polynomials $\widetilde{h}$, $\widetilde{q}$ and $\widetilde{r}$ in Step (2) are indeed homogeneous. Since the polynomials $\widetilde{h}$ and f are homogeneous, it follows that $\widetilde{h}f$ is a homogeneous polynomial. Hence, $\widetilde{q}g$ and $\widetilde{r}$ have the same degree which means that c in Step (3) is well defined. Since f and g are coprime it follows that the equality $\gcd(g, \widetilde{r}) = \gcd(g, \widetilde{h})$ holds. Therefore, one has that the polynomials g', h and r in $k[x, y, z]$ are homogeneous. Step (4) follows from the properties of intersection cycles given in Proposition 2.16:

$$\begin{aligned} f \cap g \quad &= \quad f \cap (g'c) \overset{(ii)}{=} f \cap g' + f \cap c = h \cap g' + f \cap g' - h \cap g' + f \cap c \\ &\overset{(ii)}{=} \quad (hf) \cap g' - h \cap g' + f \cap c = (\widetilde{q}g' + r) \cap g' - h \cap g' + f \cap c \\ &\overset{(iii)}{=} \quad r \cap g' - h \cap g' + f \cap c. \end{aligned}$$

One has that c and h are both homogeneous polynomials and both divisors of the homogeneous polynomial $\widetilde{h}$ in $k[y, z]$. Hence, h and c have zero x-degree and the x-degree of g' is equal to the x-degree of g. As well one has for the x-degreed of R and r that $\partial_x R \leq \partial_x r < \partial_x g$. Therefore, one has that $\partial_x r < \partial_x g'$. □

Remark 3.7. If one wishes to compute the intersection cycle of two nonzero coprime homogeneous polynomials f and g in $k[x, y, z]$, the algorithm gives us the opportunity to compute simpler intersection cycles of coprime homogeneous polynomials instead. After applying the algorithm once, one obtains: two intersection cycles $h \cap g'$ and $f \cap c$, such that one of the two polynomials has zero x-degree; and one intersection cycle $r \cap g'$ where one polynomial has the same x-degree equal to $\partial_x f$, while the other polynomial has x-degree lower then $\partial_x g$. Since all x-degrees are finite one can apply the algorithm recursively to $r \cap g'$ until one obtains a sum of intersection cycles of the form $\pm f \cap g$ with $f \in k[x, y, z]$ and $g \in k[y, z]$. In Proposition 3.3 we all ready proved Bézout's these intersection cycles. Hence, we an finish the proof by induction.

Proof by induction on the x-degree of g

With Proposition 3.3 we have all the ingredients to complete this bachelor thesis with a proof of Bézout's theorem.

Proof. Let $f, g \in k[x, y, z]$ be two nonzero coprime homogeneous polynomials of degrees m and n respectively.

If g has zero x-degree, then it follows from Proposition 3.3 that for all points a in the projective plane $\mathbb{P}^2$ the intersection multiplicity $i(a, f \cap g)$ is finite and the intersection number of f and g is given by $\#(f \cap g) = mn$.

Induction hypothesis: assume that Bézout's theorem holds for all nonzero homogeneous polynomials $f, g \in k[x, y, z]$ with the x-degree of g smaller then N for some strictly positive integer N.

Suppose that the x-degree of g is equal to N. After running Algorithm 3.4 once we find four homogeneous polynomials $r, g', h, c \in k[x, y, z]$ such that for the intersection cycles the equality

$$f \cap g = r \cap g' - h \cap g' + f \cap c$$

holds. Since the x-degree of r is strictly smaller than the x-degree of g, $\partial g = N$, and since h and c have zero x-degree, it follows from the induction hypothesis that for all points a in the projective plane $\mathbb{P}^2$ the intersection multiplicity $i(a, f \cap g)$ is finite.

Hence, for the intersection number of f and g one has that

$$\#(f \cap g) = \#(r \cap g') - \#(h \cap g') + \#(f \cap c).$$

From Algorithm 3.4 it follows that for the x-degrees of r and g one has that $\partial_x r < \partial_x g = N$. Hence, it follows from the induction hypothesis that for the intersection number of homogeneous polynomials r and g' one has that $\#(r \cap g')$ is equal to $\partial r \partial g'$. Further, from Algorithm 3.4 it follows that h and c have zero x-degrees. Hence, from the induction hypothesis it follows that for both the intersection cycles of $h \cap g'$ and $f \cap c$ the intersection number is equal to $\partial h \partial g$ and $\partial f \partial c$ respectively. Since the polynomials hf and r in Step 2 of Algorithm 3.4 are homogeneous, it follows that the equality $\partial r - \partial h = \partial f$ holds. Analogously it follows that the equalily $\partial g' + \partial c = \partial g$ holds. Hence, for the intersection number of f and g one has that

$$\begin{aligned}
\#(f \cap g) &= \partial r \partial g' - \partial h \partial g' + \partial f \partial c = (\partial r - \partial h)\partial g' + \partial f \partial c \\
&= \partial f \partial g' + \partial f \partial c = \partial f(\partial g' + \partial c) = \partial f \partial g = mn.
\end{aligned}$$

This proves Theorem 3.1. □

Bibliography

[1] John J. O'Connor and Edmund F. Robertson, *The MacTutor History of Mathematics archive*, `http://www-history.mcs.st-andrews.ac.uk/index.html`, JOC/EFR, April 2011.

[2] W. Fulton, *Algebraic Curves*, W. A. Benjamin, New York, 1969.

[3] Brendan Hassett, *Introduction to Algebraic Geometry*, Cambridge Univesity Press, New York, 2007.

[4] M. Hazewinkel, N. Gubareni and V.V. Kirichenko, *Algebras, Rings and Modules, Volume 1*, Kluwer Academic Publishers, Dordrecht, 2004.

[5] Jan Hilmar and Chris Smyth, *Euclid meets Bézout: Intersecting algebraic plane curves with the Euclidean algorithm*, American Mathematical Monthly, vol. 117, no. 3, pp. 250-260, 2010.

[6] Serge Lang, *Undergraduate Algebra*, Springer, New York, Third Edition, 2005.

[7] Uta C. Merzbach and Carl B. Boyer, *A History of Mathematics*, John Wiley & Sons, Inc., Hoboken, New Jersey, Third edition, 2011.