Bézout's theorem

Toni Annala

Contents

Chapter 1

Introduction

The topic of this thesis is Bézout's theorem. The classical version considers the number of points in the intersection of two algebraic plane curves. It states that if we have two algebraic plane curves, defined over an algebraically closed field and cut out by multivariate polynomials of degrees n and m, then the number of points where these curves intersect is exactly nm if we count "multiple intersections" and "intersections at infinity". In Chapter 2 we define the necessary terminology to state this theorem rigorously, give an elementary proof for the upper bound using resultants, and later prove the full Bézout's theorem. A very modest background should suffice for understanding this chapter, for example the course "Algebra II" given at the University of Helsinki should cover most, if not all, of the prerequisites.

In Chapter 3, we generalize Bézout's theorem to higher dimensional projective spaces. This chapter is more technical, and more background is needed. Section 3.1 defines the main tool of this chapter: the Hilbert polynomial. Section 3.2 tries to summarize enough of the modern theory of schemes for later use. In Section 3.3 we first give partial extensions of the Bézout's theorem in the higher dimensional case. The section culminates in the full extension of Bézout's theorem, which states that given r projective hypersurfaces in the projective n-space $\mathbb{P}^n$ whose defining polynomials define a *regular sequence*, the intersection consists of finitely many *components* of dimension $n-r$, and if these components are counted correctly, the number of these components is the product of the degrees of the defining polynomials.

The two later sections, 3.4 and 3.5, consider intersections of subvarieties in $\mathbb{P}^n$. The Section 3.4 begins by showing how the Hilbert polynomial behaves in "reduction to diagonal" type of situations. Then we define the *geometric multiplicity* of X, $n(X)$, as the sum of the degrees of the irreducible components of X. Finally we show that $n(X \cap Y) \leq n(X) \cdot n(Y)$, where no assumptions are made for X, Y, or the properness of the intersection.

The topic of Section 3.5 is Serre's Tor-formula. The main result of this section is that the multiplicities given by Serre's formula satisfy Bézout's theorem in proper intersection of equidimensional subvarieties of $\mathbb{P}^n$. This is achieved by looking at the situation globally: we use the graded variants of the usual Tor-functors and the properties of Hilbert polynomials, to show that multiplicities defined in a slightly different way satisfy Bézout's theorem. Finally we show that these two multiplicities coincide.

I would like to thank my supervisor Kari Vilonen for this topic, which turned out to be more interesting than its initial expression. I also thank him for his patience during this time.

Chapter 2

Bézout's theorem

2.1 Affine plane curves

Let k be a field. The affine n-space (over k) is denoted by $\mathbb{A}^n_k$, or just $\mathbb{A}^n$ if k is clear from the context. Its points are exactly the elements of k^n; the reason for a different denotation is to make distinction between different kinds of objects. The affine space $\mathbb{A}^n$ is an object of algebraic geometry, while k^n is an algebraic object. It should be thought as the place where the elements of $k[x_1, ..., x_n]$, the polynomials of n indeterminates over k, live: a setting for the theory of objects cut out by polynomial equations.

If $a = (a_1, ..., a_n)$ is a point of $\mathbb{A}^k$, then $f \in \mathbb{A}^n$ is said to *vanish* at a if $f(a) = f(a_1, ..., a_n)$ is zero. The set of the points of A^n where f vanishes, $V(f)$, is said to be *the vanishing set* of f. The vanishing set $V(f)$ is said to be *cut out* by f. If S is a (possibly infinite) set of polynomials in $k[x_1, ..., x_n]$, then we denote by $V(S)$ the set of all points of $\mathbb{A}^n$ where all polynomials of S vanish. Such subsets of A^n are called *algebraic sets.* The following properties are trivial from the definitions, or from the properties stated before:

- $V(S) = V(I)$, where I is the ideal of $k[x_1, ..., x_n]$ generated by the elements of S.
- $V(S) \cap V(T) = V(S \cup T)$.
- $V(I) \cap V(J) = V(I + J)$, when I and J are ideals.
- $V(fg) = V(f) \cup V(g)$, when f and g are polynomials.

It is easy to visualize what kind of sets the algebraic sets of $\mathbb{R}^2$ or $\mathbb{R}^3$ might look like. There is the sphere, the circle, lines, a weird surface cut out by a weird polynomial... What all of these have in common, is that they are very small subsets of $\mathbb{R}^n$. This is true in a more general situation, as we will see next.

Proposition 2.1.1. *Let $f_1, ..., f_m$ be nonzero polynomials in $k[x_1, ..., x_n]$. If k is infinite, then there is a point $a \in \mathbb{A}^n$ where none of the f_i vanishes.*

Proof. The case $n = 1$ is easy: as there are only finitely many polynomials, which have only finitely many roots, there must be a point where none of them vanishes. If $n > 1$, then each of the polynomials may be written as $f_i = f_{i,r_i} x_n^{r_i} + f_{i,r_i-1} x_n^{r_i-1} + ... + f_{i,0}$, where $f_{i,j}$ are polynomials in $k[x_1, ..., x_{n-1}]$. By the inductive assumption, we may choose $a_1, ..., a_{n-1}$ in such a way that each $f_i(a_1, ..., a_{n-1}, x_n)$ is a nonzero polynomial in $k[x_n]$. The claim then follows from the case $n = 1$. □

The above proposition fails if k is finite. If $a_1, ..., a_r$ are the elements of k in some order, then $(x - a_1) \cdots (x - a_r)$ is a polynomial which vanishes at all points of $\mathbb{A}^1$.

The affine 2-space $\mathbb{A}^2$ is called *the affine plane*. An *affine plane curve* is a subset of $\mathbb{A}^2$ cut out by a nonconstant polynomial. We already know that when k is infinite, the affine plane curves are small subsets of $\mathbb{A}_k^2$ in the sense that $\mathbb{A}_k^2$ cannot be given as a finite union of them. On the other hand, in good situations these sets are not *too small*: they are not finite.

Proposition 2.1.2. *Let f be a nonconstant polynomial in $k[x_1, ..., x_n]$, $n \geq 2$. If k is algebraically closed, then $V(f)$ is infinite.*

Proof. Let us write $f = f_r x_n^r + f_{r-1} x^{r-1} + ... + f_0$, where f_i are polynomials in $k[x_1, ..., x_{n-1}]$, and f_r is not the zero polynomial. Assume first that $r \neq 0$. As algebraically closed fields are infinite, we know that there must be infinitely many points $a = (a_1, ..., a_{n-1}) \in \mathbb{A}^{n-1}$, where f_r does not vanish. Therefore $f(a_1, ..., a_{n-1}, x_n) \in k[x_n]$ is a nonzero polynomial and hence has a root. This takes care of the first case.

On the other hand, if $r = 0$, then by induction there must be $a_1, ..., a_{n-1} \in k$ such that $f(a_1, ..., a_{n-1}, x_n)$ is he zero polynomial. This takes care of the second case, concluding the proof. □

It is necessary to assume that k is algebraically closed for the above theorem to hold. If for example $k = \mathbb{R}$, then the polynomial $x^2 + y^2$ cuts out a single point, namely the origin. This is not the whole truth however, as for any k not algebraically closed the affine space $\mathbb{A}_k^n$ is not "the most natural" place for the elements of $k[x_1, ..., x_n]$ to live. One should instead think of, as one indeed does in the theory of schemes, the structure consisting of the points of n-tuples of $\overline{k}/\sim$: the algebraic closure of k after identifying elements with the same minimal polynomials. For real numbers this would mean taking the complex numbers, and then identifying complex conjugates with each other. This point of view would make most of the theorems in this chapter to work over any k, not just infinite or algebraically closed ones.

We say that algebraic plane curves F and G, cut out by f and g respectively, have a *common component* if f and g have a nontrivial common factor. In our case of interest, which is the case where k is algebraically closed, this is independent of the choice of f and g, as the next proposition shows.

Proposition 2.1.3. *Let k be an algebraically closed field, $f, g \in k[x, y]$ nonconstant polynomials. The set $V(f) \cap V(g)$ is infinite if and only if f and g share a nontrivial factor.*

Proof. If f and g share a nontrivial factor, say h, then $V(f) \cap V(g)$ contains $V(h)$, which is infinite. On the other hand, if f and g share no nontrivial factors in $k[x, y] = k[x][y]$, then by Gauss' lemma they do not share nontrivial factors in $k(x)[y]$ either. As $k(x)[y]$ is a principal ideal domain, we have such $\alpha, \beta \in k(x)[y]$ that $\alpha f + \beta g = 1$, and therefore such $a, b \in k[x, y]$ that $af + bg \in k[x]$. Thus, there are only finitely many values of x where $V(f)$ and $V(g)$ can intersect. As this process can be repeated with y, we see that the number of intersections must be finite. □

The reader should note that if f and g share no nontrivial factors, then $V(f) \cap V(g)$ is known to be finite for any k, not just infinite or algebraically closed ones. This is because our proof above did not need any such assumptions for k.

Let f and g be polynomials in $k[x, y]$ sharing no nontrivial factors. As the number of intersection points is known to be finite, one is naturally led to the following question: is there a simple way to estimate the number of points in the intersection if f and g are known? This is exactly the kind of question that Bézout's theorem concerns.

Theorem 2.1.4. ***Bézout's theorem, first formulation.*** *Let f and g be two polynomials in $k[x, y]$ of degrees n and m respectively. The intersection $V(f) \cap V(g)$ has at most nm points.*

One would hope that some notion of *multiplicity* of intersection points could make this estimation equality, i.e., if we would count the points of intersection *with multiplicity*, then the intersection would have exactly nm points. After all, this works well for polynomials over algebraically closed field: a nonzero polynomial $f \in k[x]$ has exactly $\deg(f)$ roots, if the roots are counted with multiplicity. This time, however, multiplicity can not save us. The most simple way to see this, is to note that parallel lines never meet. If we want the equality to hold we must at least fix this. One cure, which is also the topic of the next section, is the projective plane.

2.2 Projective plane curves

From this section on, unless otherwise stated, we assume that we are working over an algebraically closed field k. The reason for this is that many theorems will need the hypothesis, and restating it whenever it is needed is tiresome. Many statements hold without this hypothesis; in these cases the proof doesn't usually use the hypothesis at all.

To make all distinct lines meet, one needs to add some points to $\mathbb{A}^2$. To motivate the following definition, we give the following mental image. Imagine that you are standing on an infinite plane. There is a railroad track of infinite length, running across the plane, and you are standing right between the rails. These rails are parallel, and the farther you look, the closer they seem to get, until, "at infinity", they seem to intersect. On the other hand, if the rails were not parallel, then the illusion would break, and the rails would no longer seem to intersect at infinity. If you turn 180 degrees, then the rails, if assumed to be parallel again, intersect again at infinity. If we want the rails to intersect at exactly one point, we must think these two "infinities", even thought they are on the opposite sides of the plane, as the same point.

Therefore, it would make sense to add new points to $\mathbb{A}^2$ corresponding bijectively to equivalence classes of lines in $\mathbb{A}^2$, where two lines would be considered equivalent if they are parallel. In this way we get exactly the projective plane $\mathbb{P}^2$, as we shall see next.

One defines the projective n-space $\mathbb{P}^n_k$ as follows. If a and b are elements of $k^{n+1}\backslash\{0\}$, then we say that a and b are equivalent if there is a nonzero $r \in k$ such that $ra = b$. The points of $\mathbb{P}^n_k$ are exactly the elements of $k^{n+1}\backslash\{0\}$ under this identification. We use the *homogeneous coordinates* to talk about the points of $\mathbb{P}^n_k$, i.e., we denote the equivalence class of $(a_0, ..., a_n)$ by $[a_0 : ... : a_n]$.

The affine n-space $\mathbb{A}^n$ can easily be thought as a subset of the projective space $\mathbb{P}^n$. We identify the points $(a_1, ..., a_n)$ with the points $[1 : a_1, ..., a_n]$; the points of the form $[0 : a_1 : ... : a_n]$ are called *points at infinity.* It is clear, that the points at infinity are in bijective correspondence with the equivalence classes of parallel lines in $\mathbb{A}^n$, so the construction coincides with our mental image. Moreover, as the homogeneous coordinate set to 1 can be chosen arbitarily, one sees that $\mathbb{P}^n$ can be covered with $n+1$ "isomorphic copies" of $\mathbb{A}^n$, a fact that will be surprisingly useful in the near future.

In order to do algebraic geometry on $\mathbb{P}^n$, we need to have well behaved set of "polynomial functions" on it. More specifically, we want polynomials $f \in k[x_0, ..., x_n]$ for which $f[a_0 : ... : a_n] = 0$ is a well defined relation, i.e., if $f(a_0, ..., a_n) = 0$, then for all nonzero $r \in k$ we have that $f(ra_0, ..., ra_n) = 0$. The *homogeneous polynomials* are those polynomials where all monomials with nonzero coefficients have the same degree. If f is a homogeneous polynomial of degree n, then $f(ra_0, ..., ra_1) = r^n f(a_0, ..., a_1)$, so the homogeneous polynomials are well behaved in our sense. We take the homogeneous polynomials of $k[x_0, ..., x_n]$ to be "the polynomials" on $\mathbb{P}^n$.

Now we can finally check that the *projective plane* $\mathbb{P}^2$ does what we wanted it to do, i.e., that any two distinct lines in $\mathbb{P}^2$ intersect at a point. A *projective line* is a subset of $\mathbb{P}^2$ cut out by a homogeneous polynomial of degree one.

Proposition 2.2.1. *Any two distinct lines in $\mathbb{P}^2$ intersect at a point.*

Proof. The lines are subsets of $\mathbb{P}^2$ cut out by equations of form $a_0x_0 + a_1x_1 + a_2x_2$. If we think $\mathbb{A}^3$ as a three-dimensional vector space, then such an equation defines a two-dimensional linear subspace of $\mathbb{A}^3$. By dimensionality, the intersection of two distinct two-dimensional subspaces of a three-dimensional vector space has dimension 1. As it is clear, that a one-dimensional linear subspace of $\mathbb{A}^3$ corresponds to a single point of $\mathbb{P}^2$, we are done. □

Let $\psi : k^{n+1} \to k^{n+1}$ be a linear isomorphism. This map induces a function $\overline{\psi} : \mathbb{P}^n \to \mathbb{P}^n$ defined by $[a] \mapsto [\psi(a)]$. This map is well defined: by linearity of ψ we see that the equivalence class of a maps into the equivalence class of $\psi(a)$, and by injectivity no nonzero element of k^{n+1} maps to 0. This map is bijective as well: surjectivity is trivial, and if $[\psi(a)] = [\psi(b)]$, then $\psi(a) = r\psi(b)$, i.e., $\psi(a) = \psi(rb)$, which by the injectivity of ψ shows that $[a] = [b]$. Such a map $\mathbb{P}^n \to \mathbb{P}^n$ is called a *linear change of coordinates.*

A linear change of coordinates can be expressed as $[x_0 : ... : x_n] \mapsto [L_0(x_0, ..., x_n) : ... : L_n(x_0, ..., x_n)]$, where L_i are homogeneous polynomials of degree one. Now we can *pull back* homogeneous polynomials on the changed coordinates to homogeneous polynomials on the original coordinates by setting $(\psi^{-1}f)(x_0, ..., x_n) = f(L_0(x_0, ..., x_n), ..., L_n(x_0, ..., x_n))$. The pullback map satisfies the following properties:

Proposition 2.2.2. *Let ψ be as above.*

1. $(\psi^{-1}f)[a] = 0$ *if and only if* $f(\overline{\psi}[a]) = 0$.
2. *If $S \subset k[x_0, ..., x_n]$, then the vanishing set of $\{\psi^{-1}f \mid f \in S\}$ is exactly the preimage of $V(S)$ under the induced map $\mathbb{P}^n \to \mathbb{P}^n$.*

Proof. It is clear that the second claim follows from the first. On the other hand, we have that $(\psi^{-1}f)(a_0, ..., a_n) = f(L_0(a_0, ..., a_n), ..., L_n(a_0, ..., a_n)) = f(\psi(a_0, ..., a_n))$, which proves the first claim. □

On the other hand, if we want to transfer polynomials from the original coordinates to the new coordinates, we may use the pullback map induced to ψ^{-1}. It is clear from the above proposition that, for example, the number of points of an algebraic set does not change in linear change of coordinates.

As $\mathbb{A}^n$ can be thought as a subset of $\mathbb{P}^n$, one would hope to be able to transfer polynomials in $k[x_1, ..., x_n]$ to homogeneous polynomials in $k[x_0, ..., x_n]$, and vice versa. There are simple ways to do both of these, called *homogenization* and *dehomogenization.* If f has degree n, then one multiplies each monomial of f by x_0^r, where r is chosen in a way that makes the product monomial have degree n. This way one obtains a homogeneous polynomial $\text{ho}_0(f) \in k[x_0, ..., x_n]$. It is clear that $\text{ho}_0(f)(1, x_1, ..., x_n) = f(x_1, ..., x_n)$, so this transformation preserves the points where f vanishes. Furthermore, the map $f \mapsto \text{ho}_0(f)$ respects multiplication. The proof of the following proposition is easy.

Proposition 2.2.3. *The maps $f \mapsto \text{ho}_0(f)$ and $g \mapsto \text{de}_0(g)$, where $\text{de}_0(g)$ denotes the polynomial $g(1, x_1, ..., x_n)$, satisfy the following properties:*

1. $\text{de}_0(\text{ho}_0(f)) = f$, *for* $f \in k[x_1, ..., x_n]$.

2. $x_0^r \cdot \text{ho}_0(\text{de}_o(g)) = g$, *for any homogeneous* $g \in k[x_0, ..., x_n]$, *where* x_0^r *denotes the highest power of* x_0 *dividing* g.

The maps ho_0 and de_0 are called *homogenization* and *dehomogenization* in respect to x_0. Let $f \in k[x, y]$ is homogeneous. Using the previous proposition, as well as the fact that k is algebraically closed, we see that f splits into a product of linear terms. Geometrically this tells us that the algebraic sets of $\mathbb{P}^1$ are finite collections of points.

It is clear that one can define homogenization and dehomogenizations in respect to other variables as well. Thus we obtain the maps ho_i and de_i, which satisfy the earlier proposition as well. With the help of dehomogenizations de_i, one can reduce the study of set $V(f) \subset \mathbb{P}^n$ to the study of the $n+1$ subsets $V(\text{de}_i(f)) \subset \mathbb{A}^n$. First of all, we obtain the following lemma.

Lemma 2.2.4. *Let f and g be homogeneous polynomials in $k[x_0, ..., x_n]$. If $\text{de}_0(f)$ and $\text{de}_0(g)$ are coprime, then the greatest common divisor of f and g is of form x_0^r.*

Proof. First of all, any factor of a homogeneous polynomial is homogeneous as the multiplication of a nonhomogeneous polynomial with any nonzero polynomial is never homogeneous. Thus, if h divides both f and g, then by the assumptions $\text{de}_0(h)$ is constant. Hence h is a homogeneous polynomial in $k[x_0]$, so it is of the form ax_0^r. □

Using the previous lemma, we see that the coprimality of two polynomials f and g can be checked *affine locally*, which in this case means that it can be checked on the standard cover of $\mathbb{P}^n$ by $\mathbb{A}^n$.

Proposition 2.2.5. *Let f and g be nonzero homogeneous polynomials on $\mathbb{P}^n$. They are coprime if and only if $\text{de}_i(f)$ and $\text{de}_i(g)$ are coprime for all $i = 0..n$.*

Proof. As homogenization respects multiplication and $x_i^r \cdot \text{ho}_i(\text{de}_i(f)) = f$, we see that if f and g are coprime, then so are $\text{de}_i(f)$ and $\text{de}_i(g)$. On the other hand, if $\text{de}_i(f)$ and $\text{de}_i(g)$ are coprime for all i, then by the last lemma, we have that f and g have greatest common divisors of form x_0^r and $x_1^{r'}$. The only way this is possible, is that f and g are coprime, so we are done. □

A *projective plane curve* is a nontrivial subset of $\mathbb{P}^2$ cut out by a single homogeneous polynomial. Using the results of this and the previous chapter, we obtain the following:

Proposition 2.2.6. *Let f and g be two homogeneous polynomials on $\mathbb{P}^2_k$. The intersection $V(f) \cap V(g)$ is finite if and only if f and g do not share a nontrivial factor.*

Proof. It is clear that the intersection $V(f) \cap V(g)$ is finite if and only if $V(\mathrm{de}_i(f)) \cap V(\mathrm{de}_i(g))$ is finite for $i = 0, 1, 2$. On the other hand, by the analogous statement of the previous section, this is equivalent to the fact that $\mathrm{de}_i(f)$ and $\mathrm{de}_i(g)$ are coprime. The claim then follows from the previous proposition. □

Thus we have a simple algebraic characterization to tell when the intersection of two projective plane curves, defined over an algebraically closed field, is finite. The main reason to introduce the projective plane was to make the Bézout's theorem more elegant, and indeed, with the help of a suitable notion of multiplicity, one can formulate the Bézout's theorem as follows:

Theorem 2.2.7. ***Bézout's theorem*** *Let f and g be two homogeneous plane curves of degree n and m respectively. If f and g are coprime, then the number of points in the intersection $V(f) \cap V(g)$ is exactly nm, if the points are counted with multiplicity.*

One should note that 2.1.4 follows from the above, but a weaker version would suffice: it would follow if we knew that the intersection of $V(f)$ and $V(g)$ has at most $\deg(f)\cdot\deg(g)$ points in the projective case. This is exactly what we are going to prove in the next section. In the section following that, we define the multiplicity of an intersection point.

2.3 An elementary proof for the upper bound

In this section we are going to prove the upper bound version of Bézout's theorem. The proof, which uses elementary properties of resultants, is based on the ones given in [1] and [2].

The resultant of two polynomials is a surprisingly useful tool. The concept follows naturally from the following question: *when do two univariate polynomials, say f and g, share a root?* As k is algebraically closed, this is equivalent to the fact that f and g share a nontrivial factor. By unique factorization, this is equivalent to the existence of such nonzero a and b in $k[x]$ that $\deg(a) < \deg(g)$, $\deg(b) < \deg(f)$ and $af + bg = 0$. This is then equivalent to the linear dependence of $f, xf, ..., x^{\deg(g)-1}f, g, xg, ..., x^{\deg(f)-1}g$ over k.

Let $f = a_n x^n + a_{n-1}x^{n-1} ... + a_0$ and $g = b_m x^m + b_{m-1}x^{m-1} + ... + b_0$. Now we may form the *Sylvester matrix*

$$
Syl(f,g) = \begin{pmatrix}
a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & \cdots & 0 \\
0 & a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \cdots & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_1 & a_0 \\
b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & \cdots & 0 \\
0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \cdots & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0
\end{pmatrix}
$$

This is an $(n+m) \times (n+m)$ matrix, and it has the property that its determinant is zero exactly when f and g share a common root. This determinant is called the *resultant* of f and g. If we are working over a field k that is not algebraically closed, then the resultant is zero if and only if f and g have a nontrivial common factor.

The full power of resultants is not fully apparent from the univariate case. If f and g are nonzero polynomials in $k[x_1, ..., x_n]$, then they are expressible as $f = f_r x_n^r + f_{r-1} x_n^{r-1} + ... + f_0$ and $g = g_{r'} x_n^{r'} + g_{r'-1} x_n^{r'-1} + ... + g_0$, where the coefficients are elements of $k[x_1, ..., x_{n-1}]$ and the leading terms are assumed to be nonzero. We can form the Sylvester matrix, where instead of constant coefficients, we have polynomials in $n-1$ indeterminates as coefficients. The determinant of this matrix, $Res(f, g, x_n)$, is a polynomial in $k[x_1, ..., x_{n-1}]$, and the vanishing set of this polynomial clearly contains all the points $(a_1, ..., a_{n-1})$ where it is possible to find such an $a_n \in k$ that both f and g vanish at $(a_1, ..., a_n)$. Such an a_n may not exist for all the points of $V(Res(f, g, x_n))$, but it is clear that this can only happen at the points where at least one of the leading terms $f_r, g_{r'}$ vanishes.

Let f and g be coprime homogeneous polynomials on $\mathbb{P}^2$. As their intersection is finite, we may find a point of $\mathbb{P}^2$ where neither f nor g vanishes, and which is not contained in any line between any two distinct points of the intersection $V(f) \cap V(g)$. Using a linear change of coordinates, we may assume that this point is exactly $[1 : 0 : 0]$. Now no two distinct points of the intersection lie on the same line from $[1 : 0 : 0]$. Write $f = f_n x_0^n + f_{n-1} x_0^{n-1} + ... + f_0$ and $g = g_m x_0^m + g_{m-1} x_0^{m-1} + ... + g_0$. Now $n = \deg(f)$ and $m = \deg(g)$, otherwise all the coefficients f_i of f (respectively g_i of g) would be nonconstant homogeneous polynomials in $k[x_1, x_2]$ and thus f (resp. g) would vanish at $[1 : 0 : 0]$.

Lemma 2.3.1. *If f and g are assumed to be as above, then $R \equiv Res(f, g, x_0)$ is a nonzero homogeneous polynomial of degree nm.*

Proof. To see that R is nonzero, we first note that the resultant polynomial is just the normal resultant if we think f and g as elements of $k(x_1, x_2)[x_0]$. If this would be zero, then f and g would have a nontrivial common factor as elements of $k(x_1, x_2)[x_0]$, and hence by Gauss' lemma they would have a nontrivial common factor as elements of $k[x_0, x_1, x_2]$, which would contradict our assumptions.

To prove that R is a homogeneous polynomial of degree nm, we need to show that for all permutations $\sigma \in S_{n+m}$, the product

$$\prod_{i=1..m+n} Syl(f,g)_{i,\sigma(i)}$$

has degree nm whenever it is nonzero. First of all, note that the degree of a nonzero coefficient f_i is $n-i$, and similalrly for g_i it is $m-i$. Now the degree of the homogenous polynomial $Syl(f,g)_{i,j}$, assuming it is nonzero, is

$$\begin{cases} j-i, & \text{if } i = 1..m \\ j-(i-m), & \text{if } i = m+1..m+n \end{cases}$$

Therefore the degree of the product, if assumed nonzero, is

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

which concludes the proof. □

As k is algebraically closed, the polynomial R splits to a product of nm linear terms of the form $ax_1 + bx_2$. Each $V(ax_1 + bx_2)$ is a line going trough $[1:0:0]$, and we know that these lines cover all the points of the intersection. Moreover, by our previous assumptions, no two points of the intersection lie on the same line. Therefore we may conclude that the intersection can have at most nm points.

2.4 Intersection numbers

In this section, we define the "suitable notion of multiplicity" needed by Bézout's theorem. The definition is based on the one given in [3]. How could one define the multiplicity of a point in intersection? The definition should be *local* in the sense that the intersection number at a point a should only depend on the things happening near a. One way to do this is to look at the *local ring* at a, which describes the structure of an "algebro-geometric" structure (scheme in the modern theory) near a, and forgets everything that is "too far" from a.

Let $a = (a_1, a_2)$ be a point of $\mathbb{A}^2$. The ideal p generated by $x_1 - a_1$ and $x_2 - a_2$ is a maximal ideal as it is the kernel of the map $f \mapsto f(a_1, a_2)$. The local ring at a is the localization of $k[x_1, x_2]$ at p, denoted by $k[x_1, x_2]_p$. This ring consists of elements of form f/g, where $f \in k[x_1, x_2]$ is arbitrary and $g \in k[x_1, x_2]$ does not belong to p. One way to think about this ring is to think it as the subring of rational functions, consisting of those rational functions that are well defined at a. The map $f/g \mapsto f(a)/g(a)$ is a well defined homomorphism of rings and its kernel is a meximal ideal of $k[x_1, x_2]_p$. As it turns out, this is the only maximal ideal of the ring. (One says that a ring is *local* if it has only one maximal ideal, hence the name "local ring at a".) This is because all nonunits of $k[x_1, x_2]_p$ are of form f/g, where $f \in p$, so $f(a)/g(a) = 0$ for all $g \notin p$.

We define the intersection number of $f, g \in k[x_1, x_2]$ at a, $I(f \cap g, a)$, as the dimension of the k-vector space $k[x_1, x_2]_p/(f, g)$. It is clear that if either one of the f or g does not vanish at a, then the intersection number is zero, as the ideal (f, g) is the whole ring. It is also clear, that for any polynomial h, we have $I(f \cap g, a) = I((f + hg) \cap g, a)$. We would like to prove that the intersection number $I(f \cap g, a)$ is finite if and only if f and g do not share a common factor vanishing at a. The other direction is much easier:

Proposition 2.4.1. *If f and g share a factor vanishing at a, then $I(f \cap g, a) = \infty$.*

Proof. Let h be a common nontrivial factor, which vanishes at a. Now h generates an ideal containing (f, g), so it is enough to prove that $k[x_1, x_2]_p/(h)$ is infinite-dimensional as a vector space. If h is not a polynomial in x_1, i.e., if $h \notin k[x_1]$, then $x_1, x_1^2, x_1^3, ...$ is a k-free sequence. On the other hand, if $h \notin k[x_2]$ then $x_2, x_2^2, x_2^3, ...$ is free. As h is not constant, it cannot be both in $k[x_1]$ and in $k[x_2]$, so at least one of the above cases must be true. Thus $k[x_1, x_2]_p/(h)$ is infinite-dimensional, proving the claim. □

It is well known, and easy to verify, that localization commutes with taking quotients. This means that, if we denote by p' the prime ideal $p/(f, g)$ of $k[x_1, x_2]$, then the ring $k[x_1, x_2]_p/(f, g)$ is isomorphic to the ring $(k[x_1, x_2]/(f, g))_{p'}$ (recall, that localizations are a little bit more complicated in the case of rings that are not integral domains). Therefore we can flip our order: first we take the quotient by (f, g), and after that we localize at a. This is a fruitful strategy, as we will see next.

Lemma 2.4.2. *If f and g share no nontrivial factors, then $k[x_1, x_2]/(f, g)$ is a finite dimensional k-vector space.*

Proof. Recall, that in the proof of 2.1.3 we showed the existence of such $\alpha, \beta \in k[x_1, x_2]$, that $m_1 = \alpha f + \beta g \in k[x_1]$ is nonzero. Similarly we may find a nonzero $m_2 \in k[x_2] \cap (f, g)$. As $k[x_1, x_2]/(m_1, m_2)$ surjects onto $k[x_1, x_2]/(f, g)$, and as it is clearly finite dimensional k-vector space, we are done. □

Thus $A = k[x_1, x_2]/(f, g)$ is a finite dimensional k-algebra, and hence every element s of A is algebraic over k. Denote by m_s the minimal polynomial of s over k. This polynomial tells surprisingly much about s. Suppose first that m_s has nonzero constant term, so we can assume that $m_s = c_n x^n + ... + c_1 x + 1$. Now s is invertible in A as $-(c_n s^{n-1} + c_{n-1} s^{n-2} ... + c_1)s = 1$. On the other hand, if the constant term of m_s is zero, then m_s can be written as $x^m m'_s$, where x^m is the highest power of x dividing m_s. If we furthermore assume that s is not nilpotent, then m'_s is not constant and can be written as $m'_s = c_n x^n + ... + c_1 x + 1$ where $n > 0$. When we localize with a multiplicatively closed set S containing s, we see that $m'_s(s)$ becomes zero. Hence $-(c_n s^{n-1} + c_{n-1} s^{n-2} ... + c_1)$ is the inverse of s in $S^{-1}A$. From this we can conclude the following: if S is a multiplicative subset of A not containing zero, and hence no nilpotents, then the natural map $A \to S^{-1}A$ is surjective, and hence the dimension of $S^{-1}A$ as a k-vector space is smaller than that of A.

Corollary 2.4.3. *The intersection number $I(f \cap g, a)$ at a is finite if and only if f and g share no nontrivial factors vanishing at a.*

Proof. Indeed, if f and g share no nontrivial factors vanishing at a, then we can assume that they do not share any nontrivial factors at all. This is because any such factor becomes invertible in $k[x_1, x_2]_p$, so getting rid of that factor does not change the ideal $(f, g) \subset k[x_1, x_2]_p$. Everything else has already been taken care of, so we are done. □

Next we are going to figure out what is the intersection number of $I(fg \cap h, a)$, or more precicely, is there a simple way to derive it from $I(f \cap h, a)$ and $I(g \cap h, a)$. The answer, as we shall see next, is yes: $I(fg \cap h, a)$ is just the sum of $I(f \cap h, a)$ and $I(g \cap h, a)$! Before proving this, it is good to note that *unique factorization is preserved under localization.* Let f be a prime element of a UFD A not turned unit by localization. As localization commutes with taking quotients, and as f is prime exactly when quotient by f is integral domain, we see that $f/1$ is a prime element in the localized ring $S^{-1}A$. Therefore each element of $S^{-1}A$ can be expressed as a product of prime elements and a unit, i.e., $S^{-1}A$ is an unique factorization domain.

Proposition 2.4.4. *$I(fg \cap h, a) = I(f \cap h, a) + I(g \cap h, a)$.*

Proof. If either f or g shares a nontrivial factor with h, then the statement is clear, so we may assume that this is not the case. Recall, that a sequence of linear maps

$$0 \to A' \to A \to A'' \to 0$$

of k-vector spaces is called *exact* if $A' \to A$ is an injective map surjecting onto the kernel of $A \to A''$ which is surjective. From the basic properties of dimension, one has

$dim(A) = dim(A') + dim(A'')$. Denote by A the ring $k[x_1, x_2]$. As one may have already guessed, we are trying to form an exact sequence

$$0 \to A_p/(f,h) \to A_p/(fg,h) \to A_p/(g,h) \to 0.$$

Define a map $A_p/(f,h) \to A_p(fg,h)$ by $[w] \to [gw]$. This map is clearly well defined. It is also an injection: if $gw = \alpha fg + \beta h$, then $(w - \alpha f)g = \beta h$ and hence h divides $w - \alpha f$. Therefore $w \in (f,h)$, i.e., $[w] = 0$. Moreover, the image of this map is clearly (g).

We define the map $A_p/(fg,h) \to A_p/(g,h)$ to be the canonical projection (clearly $(fg,h) \subset (g,h)$). The kernel of this map is (g) as $(g) + (fg,h) = (g,h)$. Therefore we have our exact sequence, which proves our claim. □

Before extending our definition to the projective plane, we need to check one property. It is clear that if we have two degree one polynomials f and g, defining nonparallel lines intersecting at a, then the intersection number $I(f \cap g, a)$ should be 1. This is indeed true, as the following proposition shows.

Proposition 2.4.5. *Let f and g be as above. Now $I(f \cap g, a) = 1$.*

Proof. By using translation, we may assume that a is the origin. Thus $f = \alpha_1 x_1 + \alpha_2 x_2$ and $g = \beta_1 x_1 + \beta_2 x_2$, moreover these are linearly independent over k. Therefore x_1 and x_2 are in $(f,g) \subset A_p$, and as they generate the maximal ideal, we have that $A_p/(f,g) = k$, whose dimension is clearly 1, so we are done. □

Let $a = [a_0 : a_1 : a_2]$ be a point in the projective plane, f and g homogeneous polynomials. We define the projective intersection number of f and g at a, $I(f \cap g, a)$, by the affine intersection number at the corresponding point after dehomogenization. So if $a_0 \neq 0$, then we set $a' = (a_1/a_0, a_2/a_0)$ and take the intersection number $I(f(1, x_1, x_2) \cap g(1, x_1, x_2), a')$. We would like to show that this is independent of the choice of the variable x_i, respect which we dehomogenize. Without any loss of generality, we may assume that a_0 and a_1 are nonzero, and that we are proving that

$$I(f(1, x_1, x_2) \cap g(1, x_1, x_2), (a_1/a_0, a_2/a_0)) = I(f(x_0, 1, x_2) \cap g(x_0, 1, x_2), (a_0/a_1, a_2/a_1))$$

Denote $p = (x_1 - a_1/a_0, x_2 - a_2/a_0)$ and $p' = (x_0 - a_0/a_1, x_2 - a_2/a_1)$. We define a map of between the local rings $k[x_1, x_2]_p$ and $k[x_0, x_2]_{p'}$ by sending x_1 to $1/x_0$ and x_2 to x_2/x_0. If h is any element of $k[x_1, x_2]_p$, then the value of its image at $(a_0/a_1, a_2/a_1)$ is $h(1/(a_0/a_1), (a_2/a_1)/(a_0/a_1)) = h(a_1/a_0, a_2/a_0)$. As the right side is known to be well defined, by our earlier characterization for local rings at a point as the ring of rational functions that are well defined at that point, we see that our definition gives a well defined map $k[x_1, x_2]_p \to k[x_0, x_2]_{p'}$. By symmetry, sending x_0 to $1/x_1$ and x_2 to x_2/x_1, gives a well defined homomorphism $k[x_0, x_2]_{p'} \to k[x_1, x_2]_p$. These maps are inverses of each other, so we have just described an isomorphism.

Denote by f' the polynomial $f(1, x_1, x_2)$ and by f'' the polynomial $f(x_0, 1, x_2)$ (and define g' and g'' in a similar way). The image of f' in our map is $f(1, 1/x_0, x_2/x_0)$. Let N be the degree of the original homogeneous polynomial f. If we multiply by x_0^N, then by looking at each monomial, we see that we obtain $f(x_0, 1, x_2)$. Thus the image of f' differs from f'' only by multiplication with a unit. Hence the image of (f', g') is exactly (f'', g''), i.e., $k[x_1, x_2]_p(f', g') \to k[x_0, x_2]_{p'}/(f'', g'')$ is an isomorphism. This proves that the projective intersection number is well defined in the sense that it doesn't depend on the variable x_i in respect which we dehomogenize.

Many of the properties we have proved for the affine intersection number now extend easily to the projective case. For example, if f and g are homogeneous polynomials of degree one defining distinct lines intersecting at a, then $I(f \cap g, a) = 1$. Another example is that $I(fg \cap h, a) = I(f \cap h, a) + I(g \cap h, a)$. Moreover, if h is a homogeneous polynomial having degree $\deg(f) - \deg(g)$, then $I((f + hg) \cap g, a) = I(f \cap g, a)$ as dehomogenization maps respect both multiplication and addition.

2.5 Proof of Bézout's theorem

In this section, we are going to prove the full Bézout's theorem using the properties of the intersection number proved in the last section. Our proof is based on the one given in [4]. The proof uses the properties of *extended Eucliedan algorithm*, which is introduced shortly. Recall, that for a polynomial ring $k[x]$ over any field k, and any polynomials $f, g \in k[x]$, we may express f in a unique way as $cg + r$, where $c \in k[x]$ and r is a polynomial, whose degree is strictly smaller than that of g. For the algorithmic purposes below, we denote r by $f\%g$ and c by $f//g$.

The *Euclidean algorithm* uses the remainder operator to find a greatest common divisor for f and g. The pseudocode for the algorithm is given below:

```
gcd(f,g)
  if g divides f
    return g
  else
    return gcd(g, f%g)
```

The *extended Euclidean algorithm* finds, in addition to the greatest common divisor h, such polynomials a and b that $af + bg = gcd(f, g)$. This is a simple modification of the above algorithm, namely:

```
extended-gcd(f,g)
  if g divides f
    return (g,0,1)
  else
   (h,a',b')=extended-gcd(g, f%g)
    return (h, b', a'-b'(f//g))
```

Verifying that these algorithms halt, and that they produce the right output, is straightforward and therefore omitted. The recursive nature of the extended Euclidean algorithm allows easy estimation for the degrees of a and b.

Lemma 2.5.1. *Let f, g, a, b be as above. If we furthermore assume that either f or g is not constant, then the degrees of a and b satisfy the following bounds:*

$$\begin{cases} \deg(a) < \deg(g) - \deg(gcd(f,g)) \\ \deg(b) < \deg(f) - \deg(gcd(f,g)) \end{cases}$$

Proof. This is clear if g divides f (recall, that the degree of the zero polynomial is taken to be $-\infty$). Otherwise, we may assume that $\deg(g) \leq \deg(f)$, and that neither f nor g is constant. Let r, c be as above, i.e., $f = cg + r$ and $\deg(r) < \deg(g)$. Let a' and b' be given by the recursive call of the extended Euclidean algorithm. Assume that the claim already holds for them, i.e.,

$$\begin{cases} \deg(a') < \deg(r) - \deg(gcd(g,r)) \\ \deg(b') < \deg(g) - \deg(gcd(g,r)). \end{cases}$$

As $a = b'$ and $b = a' - cb'$, where the degree of cb' is strictly smaller than

$$\deg(f) - \deg(g) + \deg(g) - \deg(gcd(g,r)) = \deg(f) - \deg(gcd(f,g)),$$

we see that

$$\begin{cases} \deg(a) & < \deg(g) - \deg(gcd(g,r)) = \deg(g) - \deg(gcd(f,g)) \\ \deg(b) & < max\{\deg(r) - \deg(gcd(g,r)), \deg(f) - \deg(gcd(f,g))\} \\ & = \deg(f) - \deg(gcd(f,g)), \end{cases}$$

which proves the claim. □

Let f and g wo homogeneous polynomials in $k[x_0, x_1, x_2]$. Using the extended Euclidean algorithm, we may find such $a, b \in k[x_0, x_1, x_2]$ that $af + bg \in k[x_0, x_1]$. As f and g are known to be homogeneous, and as homogeneous polynomials of different degrees are linearly independent over k, we may assume that a and b, and thus also $af+bg$, are homogeneous. Moreover, if $\deg_{x_2}(f) \geq \deg_{x_2}(g)$ (the degrees as elements of $k(x_0,x_1)[x_2]$), then $\deg_{x_2}(a) < \deg_{x_2}(f)$. Before proving the Bézout's theorem, we need one final lemma.

Lemma 2.5.2. *Let f and g be homogeneous polynomials, of degrees n and m respectively, that do not share prime factors. If f and g split into linear factors, then*

$$\sum_{a\in\mathbb{P}^2} I(f\cap g,a) = nm$$

Proof. Let $f=\prod_{i=1..n} f_i$ and $g=\prod_{j=1..m} g_i$ be the factorization to linear factors. By the properties of intersection number proved in the last section, we have

$$\sum_{a\in\mathbb{P}^2} I(f\cap g,a) = \sum_{a\in\mathbb{P}^2}\sum_{i,j} I(f_i\cap g_j,a) = \sum_{i,j}\sum_{a\in\mathbb{P}^2} I(f_i\cap g_j,a).$$

As f_i and g_j are coprime, they intersect at exactly one point with multiplicity one, so we have that $\sum_a I(f_i\cap g_j,a)=1$. This proves the claim. □

The proof of the Bézout's theorem 2.2.7. We prove that if f and g are two homogeneous polynomials of degree n and m respectively, then $\sum_a I(f\cap g,a)=nm$. This is done by the following recursive argument: let f and g be homogeneous polynomials in $k[x_0,x_1,x_2]$, $\deg(f)=n$ and $\deg(g)=m$. We may assume that the x_2-degree of f is at least as much as the x_2-degree of g, otherwise we can just swap f and g. Now we can use the extended Euclidean algorithm to find such homogeneous $\alpha,\beta\in k[x_0,x_1,x_2]$, that $\alpha f+\beta g\in k[x_0,x_1]$, and the x_2-degree of a is strictly smaller than that of f.

Now we have that

$$\sum_a I(\alpha\cap g,a)+\sum_a I(f\cap g,a)=\sum_a I(\alpha f\cap g,a)=\sum_a I((\alpha f+\beta g)\cap g,a),$$

so

$$\sum_a I(f\cap g,a)=\sum_a I((\alpha f+\beta g)\cap g,a)-\sum_a I(\alpha\cap g,a).$$

Define a partial order relation $\leq$ on $\mathbb{N}^2$ by setting $(n_1,n_2)\leq(n_1',n_2')$ when $n_1\leq n_1'$ and $n_2\leq n_2'$. Note that the pairs x_2-degrees on the right side are strictly smaller than the pair $(\deg_{x_2}(f),\deg_{x_2}(g))$. In the case $(0,0)$, the polynomials split into linear factors, and this case has already been taken care of by the previous lemma. As the order relation $\leq$ we just defined is clearly well-founded, we can use induction to see that

$$\begin{aligned}\sum_a I(f\cap g,a) &= \deg(\alpha f+\beta g)\cdot\deg(g)-\deg(\alpha)\cdot\deg(g)\\ &= (\deg(\alpha)+\deg(f))\cdot\deg(g)-\deg(\alpha)\cdot\deg(g)\\ &= \deg(f)\cdot\deg(g),\end{aligned}$$

which proves the claim. □

Note that we have also proved the following theorem in the affine case:

Corollary 2.5.3. *Let f and g be polynomials in $k[x_1, x_2]$, $\deg(f) = n$ and $\deg(g) = m$. Now*

$$\sum_{a \in \mathbb{A}^2} I(f \cap g, a) \leq nm.$$

The equality holds whenever $V(\mathrm{ho}_0(f)) \cap V(\mathrm{ho}_0(g))$ contains no points at infinity, i.e., points of form $[0 : a_1 : a_2]$.

Chapter 3

Intersections in $\mathbb{P}^n$

In this chapter, we no longer assume that k is algebraically closed, but we still assume it to be infinite.

3.1 The Hilbert series and the Hilbert polynomial

A *graded* ring $R_\bullet$ is a ring with grading, i.e., as an abelian group it is the direct sum of R_i, where $i \in \mathbb{N}$, which satisfy $R_iR_j \subset R_{i+j}$. Elements r belonging to R_i for some $i \in \mathbb{N}$ are called *homogeneous of degree i*. A *homogeneous ideal* I of $R_\bullet$ is an ideal that can be generated by homogeneous elements of $R_\bullet$, or equivalently, an ideal I of $R_\bullet$ where from $r \in I$ follows that all "homogeneous parts" of r are in I. It is clear that $R_\bullet/I$ inherits in a natural way the graded ring structure of $R_\bullet$ whenever I is homogeneous.

A *graded k-algebra* is a graded ring $R_\bullet$, where $R_0 = k$. It is said to be *generated in degree one* if it is generated by the elements of R_1 as an k-algebra. It is straightforward to verify that any graded k-algebra finitely generated in degree one is of form $k[x_1, ..., x_n]/I$, where I is an homogeneous ideal.

A *graded $R_\bullet$-module* is a module $M_\bullet$ together with grading $M_\bullet = \bigoplus_{i\in\mathbb{N}} M_i$ satisfying $R_iM_j \subset M_{i+j}$. A *graded submodule* of $M_\bullet$ is a submodule of $M_\bullet$ satisfying similar assumptions than homogeneous ideals, and similalrly to homogeneous ideals, we see that $M_\bullet/N_\bullet$ has a natural graded $R_\bullet$-module structure whenever $N_\bullet$ is a graded submodule of $M_\bullet$. A *morphism of graded modules* is a $R_\bullet$-linear map $\psi : M_\bullet \to N_\bullet$ respecting grading, i.e., $\psi M_i \subset N_i$. It is clear that the kernel and the image of ψ are graded submodules of $M_\bullet$ and $N_\bullet$ respectively. If $M_\bullet$ is any graded $R_\bullet$-module, then we may define the *shifted module*, $M[n]_\bullet$, by setting $M[n]_i = M_{n+i}$.

From now on we assume that $R_\bullet$ is a graded k-algebra finitely generated in degree one. It is clear that $\dim_k(R_i)$ is finite for all i, moreover, if $M_\bullet$ is a finitely generated graded

$R_\bullet$-module, then $\dim_k(M_i)$ is finite for all i as well. For any finitely generated graded $R_\bullet$-module $M_\bullet$, we define a function $\psi_{M_\bullet} : \mathbb{N} \to \mathbb{N}$ by setting $\psi_{M_\bullet}(i) = \dim_k(M_i)$. Now we can define an element $H_{M_\bullet}$ of $\mathbb{Z}[[x]]$, called the *Hilbert series* of $M_\bullet$, by $\sum_{i\in\mathbb{N}} \psi_{M_\bullet}(i)x^i$. This seemingly arbitrary definition is actually quite useful, as we will see shortly. Before that, however, we need some basic properties of the Hilbert series.

Lemma 3.1.1. *Let $0 \to M'_\bullet \to M_\bullet \to M''_\bullet \to 0$ be a short exact sequence of finitely generated graded $R_\bullet$-modules. Now $H_{M_\bullet} = H_{M'_\bullet} + H_{M''_\bullet}$.*

Proof. This follows directly from the fact that $\dim_k(M_i) = \dim_k(M'_i) + \dim_k(M''_i)$. □

Using the above lemma inductively, we obtain a very useful property for the Hilbert series in finite exact sequences.

Corollary 3.1.2. *Let $0 \to M^1_\bullet \to M^2_\bullet \to \cdots \to M^n_\bullet \to 0$ be an exact sequence of finitely generated graded $R_\bullet$-modules, $n \geq 3$. Now the Hilbert series for the modules satisfy*

$$H_{M^1_\bullet} - H_{M^2_\bullet} + ... + (-1)^n H_{M^n_\bullet} = 0.$$

Proof. The case $n = 3$ is already taken care of by the previous lemma. Denote by $N_\bullet$ the image of $M^{n-2}_\bullet$ in $M^{n-1}_\bullet$. We obtain the two exact sequences

$$0 \to M^1_\bullet \to M^2_\bullet \to \cdots \to M^{n-2}_\bullet \to N_\bullet \to 0$$

and

$$0 \to N_\bullet \to M^{n-1}_\bullet \to M^n_\bullet \to 0.$$

Now $H_{N_\bullet} = H_{M^{n-1}_\bullet} - H_{M^n_\bullet}$, so by induction we obtain

$$\begin{aligned} 0 &= H_{M^1_\bullet} - H_{M^2_\bullet} + ... + (-1)^{n-2} H_{M^{n-2}_\bullet} + (-1)^{n-1} H_{N_\bullet} \\ &= H_{M^1_\bullet} - H_{M^2_\bullet} + ... + (-1)^{n-2} H_{M^{n-2}_\bullet} + (-1)^{n-1} H_{M^{n-1}_\bullet} + (-1)^n H_{M^n_\bullet}, \end{aligned}$$

which proves the claim. □

Note that the proof of the above theorem generalizes for any *additive function*, from some "subcategory" of R-modules to some abelian group G. By an additive function, we mean a "function" ψ, associating for each module M in our chosen subclass an element $\psi(M)$ of G in such a way, that for all short exact sequences $0 \to M' \to M \to M'' \to 0$, where the maps are in the chosen subclass of maps, we have $\psi(M) = \psi(M') + \psi(M'')$. This is one of the reasons why exact sequences are so important in calculations: they may allow us to break more complicated structures into simpler pieces, and then calculate some invariant of the more complicated structure using the invariants calculated for the simpler ones. As examples of additive functions, besides of course the Hilbert series, we give the dimension of a finite dimensional k-vector space, rank of a finitely generated module over an integral domain, and the Hilbert polynomial, which is introduced later in this section.

Proposition 3.1.3. ***Hilbert-Serre theorem:*** *Let $R_\bullet$ and $M_\bullet$ be as above. Now the Hilbert series of $M_\bullet$ is a rational function of the form*

$$H_{M_\bullet} = \frac{f(x)}{(1-x)^d},$$

where $f \in \mathbb{Z}[x]$.

Proof. We proceed by induction on the number n of generators of the graded k-algebra $R_\bullet$. If $n = 0$, then any such $M_\bullet$ is a finite dimensional k-algebra, and hence $H_{M_\bullet}$ is a polynomial.

Assume then that $R_\bullet$ is generated by $r_1, ..., r_n \in R_1$. Denote by $K_\bullet$ the graded submodule of $M_\bullet$ annihilated by r_n. Now we have the following exact sequence of graded $R_\bullet$-modules

$$0 \to K_\bullet[-1] \to M_\bullet[-1] \xrightarrow{r_n} M_\bullet \to M_\bullet/r_nM_\bullet \to 0$$

It is clear that $H_{M[-1]_\bullet} = xH_{M_\bullet}$. Moreover, as r_n annihilates both $K_\bullet[-1]$ and $M_\bullet/r_nM_\bullet$, these can be thought as finitely generated graded $k[r_1, ..., r_{n-1}]$-modules, so the claim follows for those by induction. Using the preceding lemma, we see that

$$(1-x)H_{M_\bullet} = H_{M_\bullet/r_nM_\bullet} - xH_{K_\bullet},$$

from which the claim easily follows. □

We also obtained the following useful result: assume that the expression

$$H_{M_\bullet} = \frac{f(x)}{(1-x)^d},$$

is nondegenerate in the sense that the denominator and the nominator share no common factors. Now d is bound above by the number of elements r_i needed to generate $R_\bullet$ over k. In fact, even more is true. If we assume that $M_\bullet = R_\bullet$, then this number d is exactly the *transcendence degree* of $R_\bullet$ over k. Recall, that the transcendence degree of $R_\bullet$ is the maximum size of an algebraically independent subset of $R_\bullet$, i.e., a set whose elements do not satisfy any nontrivial multivariate polynomial over k. Before giving a proof for this, it is useful to talk about the *Hilbert polynomial.*

We know that $1/(1-x) = 1 + x + x^2 + ...$ in the ring $\mathbb{Z}[[x]]$ of formal power series. Therefore we obtain

$$\frac{1}{(1-x)^d} = \sum_{i\in\mathbb{N}} \binom{i+d-1}{d-1} x^i.$$

Using this identity, we obtain the following theorem.

Theorem 3.1.4. *Let $M_\bullet$ be a finitely generated graded $R_\bullet$-module. Now the coefficients $\psi_{M_\bullet}(i)$ of the Hilbert series $H_{M_\bullet}$ are given by a polynomial $h_{M_\bullet}$ for $i \gg 0$. This polynomial is known as the* Hilbert polynomial *of $M_\bullet$.*

Proof. We know that H_i is expressible as

$$H_{M_\bullet} = \frac{f(x)}{(1-x)^d}.$$

Let $f = c_m x^m + ... + c_1 x + c_0$. Now for $i \geq m$, we have that

$$\psi_{M_\bullet}(i) = \sum_{j=0..m} \binom{i-j+d-1}{d-1} c_j.$$

This is clearly a polynomial in i, so we are done. □

Lets again assume that the expression $f/(1-x)^d$ is nondegenerate in the sense that f and $(1-x)^d$ do not share common factors. If we know that M_i are nontrivial for arbitrarily large i, then d cannot be zero, so $f(1) = c_m + ... + c_1 + c_0$ cannot vanish. Thus we see from the proof of the previous theorem that the leading term of $h_{M_\bullet}$ is

$$\frac{c_m + ... + c_0}{(d-1)!} x^{d-1}.$$

We can now prove the result promised earlier:

Proposition 3.1.5. *Let*

$$H_{R_\bullet} = \frac{f(x)}{(1-x)^d}.$$

be the Hilbert series of $R_\bullet$. If f and $(1-x)^d$ are coprime, then d is exactly the transcendence degree of $R_\bullet$ over k.

Proof. By the homogeneous version of the Noether normalization lemma (see the Appendix 4.1), if n is the transcendence degree of $R_\bullet$, then we can choose n algebraically independent elements $r_1, ..., r_n$ of $R_\bullet$ in such a way that $R_\bullet$ becomes a finitely generated $A_\bullet \equiv k[r_1, ..., r_n]$-module. Moreover, as k is infinite, these r_i can be chosen to be homogeneous of degree 1. Therefore $A_\bullet$ has the structure of a graded ring, and we have $h_{A_\bullet}(i) = \binom{i+n-1}{n-1}$. As $R_\bullet$ is a finitely generated $A_\bullet$-module, and as $A_\bullet \subset R_\bullet$, we have such $c \in \mathbb{N}$ that

$$h_{A_\bullet}(i) \leq h_{R_\bullet}(i) \leq c \cdot h_{A_\bullet}(i)$$

holds for $i \gg 0$. By an asymptotic argument, we see that the degree of $h_{R_\bullet}$ must be the same as the degree of $h_{A_\bullet}$, i.e., it must be $n-1$. This proves the claim. □

Why then should one care about the transcendence degree of a finitely generated k-algebra A? If $A = k[x_1, ..., x_n]/I$ for an ideal I, then A is related to $V(I) \subset \mathbb{A}^n$ in the following way: there is a notion of *dimension* for algebraic sets that agrees with our intuition of what dimension should be (for example circle is one-dimensional and $\mathbb{A}^n$ is n-dimensional). As it turns out (see for example [7] Theorem 5.9), the transcendence degree of A is exactly the dimension of $V(I)$! If I is homogeneous, then it is intuitively clear that the dimension of $V(I) \subset \mathbb{P}^{n-1}$ is one smaller than the dimension of $V(I) \subset \mathbb{A}^n$ (this follows easily from the definition of dimension, and the fact that minimal primes over a homogeneous ideal are homogeneous), so the dimension of the projective algebraic set is exactly the degree of the Hilbert polynomial. Thus we have obtained a nice alternative description for the dimension, and this characterization has the advantage that it is easily computable.

If I is not homogeneous, then we cannot use the Hilbert series to compute the transcendence degree of $k[x_1, ..., x_n]/I$. This can be fixed: if we denote by $k[x_1, ..., x_n]_{\leq i}$ the subset of polynomials, whose degree is at most i, then we obtain a map $i \mapsto \dim_k(k[x_1, ..., x_n]_{\leq n}/I)$. This map is given by a polynomial for $i \gg 0$, this polynomial is called the *Samuel polynomial* of $k[x_1, ..., x_n]/I$. It can be shown that the degree of the Samuel polynomial is exactly the transcendence degree of $k[x_1, ..., x_n]/I$, for the details, see [7] Chapter 11 (note that there what we call the Samuel polynomial is called the Hilbert polynomial).

3.2 A brief overview of the modern theory

In this section we quickly summarize the parts of the theory of Schemes that will be necessary later. The details can be found from any book about modern algebraic geometry; two standard references are [5] and [6]. However, before modern theory, we need to introduce the classical theory properly. Good sources for the classical theory are for example [3] and [1] ([2] for a more computational point of view)no. Also [7], although a book about commutative algebra, contains many algebro-geometric results.

Let $A = k[x_1, ..., x_n]$. The algebraic set $V(I) \subset \mathbb{A}^n$ cut out by an ideal I of A has a natural ring of "polynomial functions" on it: if I' is the ideal consisting of all polynomials $f \in A$ that vanish at every point of $V(I)$, then the elements of A/I' have well defined values on $V(I)$, and if two elements coincide on the whole of $V(I)$, then they are the same element by the definition of I'. The vanishing set $V(I)$, together with the *coordinate ring* A/I', is an example of a *variety.*

A *morphism* between varieties $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$ is given by a "multi-coordinate polynomial map" $\mathbb{A}^n \to \mathbb{A}^m$ that sends the points of X to the points of Y. Similarly to the pullback defined for linear change of coordinates, a morphism of varieties induces a k-algebra homomorphism from the coordinate ring of Y to the coordinate ring of X. It can be shown that the morphisms of varieties are in bijective correspondence with the k-algebra morphisms of the coordinate rings, so the coordinate ring fully characterizes the variety.

Hilbert's famous Nullstellensatz states that the subvarieties of $\mathbb{A}^n$ correspond bijectively to *radical ideals* of its coordinate ring A. A variety is called *irreducible* if it cannot be given as a proper union of two of its subvarieties. A line and a circle would be examples of irreducible varieties, whereas the union of a line and a circle would be *reducible*. The theorem also states that the irreducible subvarieties of $\mathbb{A}^n$ correspond bijectively to the prime ideals of A, and that the points of $\mathbb{A}^n$ correspond bijectively with the maximal ideals of A. These statements no longer hold if we are working over a field that is not algebraically closed.

In the modern theory, we have an intristic definition of the objects of interest, i.e., we no longer think them as subobjects of some larger structure. For any commutative ring A, we assign a *ringed space* $SpecA$, called the *spectrum* of A. It is a topological space, together with a *sheaf* of *polynomial functions*; the sheaf contains the information of "polynomial functions" on $SpecA$, and "rational functions" which are defined only on some subset of $SpecA$, as well as the information about how these relate to each other. From the nullstellensatz one sees that we may have "points" that geometrically do not look like points, i.e., points that correspond to some "irreducible subset" of $SpecA$. These kinds of points are called *generic points*, and they are necessary for technical reasons.

Ringed spaces isomorphic to some $SpecA$ as *locally ringed spaces* are called *affine schemes*. A *scheme* is a ringed space formed by gluing together affine schemes. The ring of functions defined on some open subset U of a scheme X is denoted by $O_X(U)$. The points of the spectrum $SpecA$ are the prime ideals of A. When talking about affine schemes, one often uses the points and the prime ideals corresponding to that point interchangeably.

The *stalk* at a point p is a ring which contains information about the structure of the scheme near that point. For an affine scheme $SpecA$, the stalk at p is just the localization of A at p. For an arbitrary scheme X, one can first restrict to an *affine open subset* of X containing p, which means that the sheaf structure restructed to that open set looks like that of an affine scheme, and then take the localizaton at the prime ideal corresponding to p. The stalk of X at p is denoted by $O_{X,p}$. If a scheme X is finite and discrete as a topological space, as is the case with for example $Spec(k[x_1, x_2]/(f, g))$ whenever f and g are coprime, then the scheme is affine, $X \cong SpecA$, where A is the product of the stalks at the points of X. This result can be thought as a stronger version of the fact that for a finite k-algebra A, and its prime ideal p, the natural map $A \to A_p$ is surjective.

Given a graded ring $R_\bullet$, one can obtain the projective scheme $ProjR_\bullet$ using the following procedure. For each homogeneous $r \in R_\bullet$ we can localize the ring with r to obtain the ring $(R_\bullet)_r$, which has a graded structure (this time we usually have elements of negative degree as well). Taking only the degree 0 elements, we obtain the ring $((R_\bullet)_r)_0$, and gluing the spectra of these rings together, we get the projective scheme $ProjR_\bullet$. If $R_\bullet$ is $k[x_0, ..., x_n]$ with the usual grading, then the projective scheme $ProjR_\bullet$ is very similar to the classical projective n-space $\mathbb{P}^n_k$, which we defined earlier.

A commutative ring A is *Noetherian* if it satisfies the *ascending chain condition on ideals*, i.e., any ascending chain $I_1 \subset I_2 \subset ...$ eventually becomes constant. There are two very useful equivalent characterizations for this: every ideal of A is finitely generated, and every nonempty collection of ideals of A has a maximal element. Most of the rings of interest in algebraic geometry, for example $k[x_1, ..., x_n]$, are Noetherian. A module is Noetherian if it satisfies ascending chain condition on its submodules. A finitely generated module over a Noetherian ring is always Noetherian. The Noetherian property is preserved under taking quotients and localization.

3.3 Intersections of hypersurfaces in $\mathbb{P}^n$

By the properties of the Hilbert polynomial proved in the Section 3.1, if n is the degree of the Hilbert polynomial $h_{M_\bullet}$, then $n!$ times the leading term of $h_{M_\bullet}$ is a positive integer. We call this integer the *degree* of $M_\bullet$ and denote it by $e(M_\bullet)$. The first interesting property of the degree $e(R_\bullet)$ is the fact that it bounds the number of irreducible components of "maximum dimension" of $Proj(R_\bullet)$.

Proposition 3.3.1. *Let $R_\bullet$ be a graded k-algebra finitely generated in degree one, and $n = \dim(Proj(R_\bullet))$. If $p_1, ..., p_m$ are the primes of $R_\bullet$ such that $\dim(Proj(R_\bullet/p_i)) = n$ (they are necessarily minimal and homogeneous), then*

$$e(R_\bullet) \geq \sum_{i=1..m} e(R_\bullet/p_i),$$

so especially $m \leq e(R_\bullet)$.

Proof. As we remarked earlier, sending a graded module to its Hilbert polynomial is an additive function in the sense discussed in section 1. By the basic properties of dimension, we know that $p_i \not\subset p_j$ unless $i = j$. Therefore we have that $p_1 \cap \cdots \cap p_{i-1} \not\subset p_i$: this follows from the primeness of p_i and from the fact that $p_1 \cdots p_{i-1} \subset p_1 \cap \cdots \cap p_{i-1}$. From the basic properties of dimension, it follows that the dimension of $Proj(R_\bullet/(p_i + p_1 \cap \cdots \cap p_{i-1}))$ is strictly smaller than n.

Let M be a module over some ring, M_1 and M_2 its submodules. Using the well known short exact sequence

$$0 \to M_1 \cap M_2 \to M_1 \oplus M_2 \to M_1 + M_2 \to 0,$$

we see that for any homogeneous ideals I_1 and I_2 of $R_\bullet$, we have the following exact sequence:

$$0 \to I_1 \cap I_2 \to I_1 \oplus I_2 \to R_\bullet \to R_\bullet/(I_1 + I_2) \to 0.$$

Therefore the Hilbert polynomial of the intersection satisfies the following relation:

$$h_{I_1 \cap I_2} = h_{I_1} + h_{I_2} + h_{R_\bullet/(I_1+I_2)} - h_{R_\bullet}$$

To make the notation bearable, for the rest of the proof we denote $\lambda(M_\bullet) \equiv h_{M_\bullet}$. Expanding the above relation for the intersection, we obtain

$$\begin{aligned}\lambda(p_1 \cap \cdots \cap p_m) =& \lambda(p_m) - \lambda(R_\bullet) + \lambda(R_\bullet/(p_m + p_1 \cap \cdots \cap p_{m-1})) + \lambda(p_1 \cap \cdots \cap p_{m-1}) \\ =& \lambda(p_m) - \lambda(R_\bullet) + \lambda(R_\bullet/(p_m + p_1 \cap \cdots \cap p_{m-1})) + \\ & \lambda(p_{m-1}) - \lambda(R_\bullet) + \lambda(R_\bullet/(p_{m-1} + p_1 \cap \cdots \cap p_{m-2})) + \\ & \vdots \\ & \lambda(p_1)\end{aligned}$$

As $\lambda(R_\bullet) - \lambda(I) = \lambda(R_\bullet/I)$ for any homogeneous ideal I of $R_\bullet$, we have that

$$\begin{aligned}\lambda(R_\bullet) - \lambda(p_1 \cap \cdots \cap p_m) =& \lambda(R_\bullet/p_m) - \lambda(R_\bullet/(p_m + p_1 \cap \cdots \cap p_{m-1})) + \\ & \lambda(R_\bullet/p_{m-1}) - \lambda(R_\bullet/(p_{m-1} + p_1 \cap \cdots \cap p_{m-2})) + \\ & \vdots \\ & \lambda(R_\bullet/p_1).\end{aligned}$$

As the degrees of $\lambda(R_\bullet/(p_i + p_1 \cap \cdots \cap p_{i-1})$ are strictly smaller than n, they do not affect the leading term of the polynomial, so the claim follows from the above formula. We also see, that the inequality becomes equality whenever $\lambda(p_1 \cap \cdots \cap p_m)$ has strictly smaller degree than n. □

To show that the degree does not necessarily bound the number of components, we give the following example: the vanishing set of the homogeneous ideal $I = (xy, xz)$ in $\mathbb{P}^2$ is the union of the line $x = 0$ and the point $[1 : 0 : 0]$, and therefore it has 2 components. However, the Hilbert polynomial of $k[x, y, z]/I$ is $\binom{2+x}{2} - 2\binom{2+x-2}{2} + \binom{2+x-3}{2}$, and a direct calculation shows that the degree of $k[x, y, z]/I$ is one.

Whenever $Proj(R_\bullet)$ is *equidimensional*, i.e., when all of its irreducible components have the same dimension, we *do* have a bound for their number. However, unlike k-valued points, irreducible varieties can have degree greater than one, so to get a ”sensible” estimation one should really take into account the degrees of $R_\bullet/p$ as well. For example, if $R_\bullet = k[x_0, ..., x_n]$, and $f \in R_\bullet$ is a homogeneous polynomial of degree d, then the Hilbert polynomial of $R_\bullet/(f)$ is $\binom{n+x}{n} - \binom{n+x-d}{n}$, so the degree of $R_\bullet/(f)$ is d.

The degree can be calculated algorithmically: as it turns out, chosen *any* monomial ordering, the ideal J generated by the leading terms of the elements of a homogeneous ideal $I \subset k[x_0, ..., x_n] = R_\bullet$ has the property that the Hilbert polynomials of $R_\bullet/I$ and $R_\bullet/J$ coincide. The "inclusion-exclusion for dimensions" holds for homogeneous ideals generated by monomials, so the Hilbert polynomial of a monomial ideal can be easily computed algorithmically. For the details, see [2] Chapter 9.

As the degree bounds the number of components of maximum dimension, we would like to bound the degree next. Given a ring A, a sequence $a_1, ..., a_n$ is said to bee *regular* if a_i is not a zerodivisor in $A/(a_1, ..., a_{i-1})$ for any i. If A is taken to be a polynomial algebra, then the sequence f_1, f_2 is regular if and only if f_1 and f_2 do not share nontrivial factors, so this can be seen as a generalization of coprimeness (it can be shown that in good cases regularity is independent of the order of the sequence). Taking quotients by homogeneous nonzerodivisors changes the degree in a very manageable way.

Proposition 3.3.2. *Let $R_\bullet$ be a graded k-algebra finitely generated in degree one. If $a \in R_\bullet$ is homogeneous of degree d and not a zerodivisor, then $e(R_\bullet/(a)) = d \cdot e(R_\bullet)$.*

Proof. As a is not a zerodivisor, the Hilbert polynomial of (a) is $h_{R_\bullet}(i-d)$. As the Hilbert polynomial of $R_\bullet/(a)$ is $h_{R_\bullet} - h_{(a)}$, we are done. □

As an easy corollary, we obtain the following:

Corollary 3.3.3. *Let $R_\bullet = k[x_0, ..., x_n]$ and $f_1, ..., f_r$ a regular sequence of homogeneous polynomials of degrees $d_1, ..., d_r$ respectively. Now the degree of $R_\bullet/(f_1, ..., f_r)$ is $d_1 \cdots d_r$.*

When $r = n$, this translates to the following: the intersection of $V(f_1), ..., V(f_n)$ is finite and consists of at most $d_1 \cdots d_n$ points. It is well known that for a regular sequence $f_1, ..., f_r$ the vanishing set $V(f_1, ..., f_r)$ is equidimensional. Therefore, even when $r \neq n$, the formulation is quite simple: each component of $V(f_1, ..., f_r)$ has dimension $n - r$ and there are at most $d_1 \cdots d_r$ of them. This is a nice generalization of the upper bound version of the Bézout's theorem to higher dimension.

To have a proper extension of the Bézout's theorem, we must "fix" the inequality. If $n = r$ this is simple: for $f_1, ..., f_n \in k[x_1, ..., x_n]$, define the *intersection number* at point $a \in \mathbb{A}^n$ as the dimension of the k-vector space $k[x_1, ..., x_n]_p/(f_1, ..., f_n)$, where p is the prime ideal associated to a. This definition can be extended to the projective in a similar way to the case $n = 2$. If the intersection is finite, then it is known that $V(f_1, ..., f_n) = Spec(k[x_1, ..., x_n]/(f_1, ..., f_n)) \equiv SpecA$ is a discrete scheme, and therefore $A \cong \prod_{p \in SpecA} A_p$. Thus we conclude that the number of points in the intersection $V(f_1) \cap \cdots \cap V(f_n)$ is exactly $\dim_k(A)$ if we count them with multiplicity.

In the projective case, as $V(f_1) \cap \cdots \cap V(f_n)$ is finite, we can find a hyperplane (using linear change of coordinates we may assume that this plane is $V(x_0)$) not containing any of the points of intersection. This means that x_0 is almost a nonzerodivisor in $R_\bullet = k[x_0, ..., x_n]/(f_1, ..., f_n)$ (in the sense that elements killed by powers of x_0 are "so few" that they do not affect the Hilbert polynomial, see the Appendix 4.2 for details), and that $Proj(R_\bullet)$ is the affine scheme $Spec(O_{Proj(R_\bullet)}(D(x_0)))$. We claim that the dimension of $O_{Proj(R_\bullet)}(D(x_0))$ as a k-vector space is exactly the (constant) Hilbert polynomial of $R_\bullet$. This is because the multiplication by x_0 defines a bijection $R_i \to R_{i+1}$ for large enough i, so we can choose $j \in \mathbb{N}$ in a way that $\dim_k(O_{Proj(R_\bullet)}(D(x_0)) \cong x_0^{-j}R_j$. The dimension of the right side is clearly $h_{R_\bullet} = d_1 \cdots d_n$, so we obtain the following corollary:

Corollary 3.3.4. *Let $f_1, ..., f_n \in k[x_0, ..., x_n]$ be a regular sequence of homogeneous polynomials, which have degrees $d_1, ..., d_n$ respectively. Now the number of points in $V(f_1, ..., f_n)$, the intersection of $V(f_i) \subset \mathbb{P}^n$, is exactly $d_1 \cdots d_n$ if we count them with multiplicity (intersection number).*

The case $r \neq n$ is a bit harder as our current definition of multiplicity cannot be applied to irreducible components that are not points. The Proposition 3.3.1 gives us a hint of the definition of the "multiplicity" of a component of the intersection: an irreducible component of $Proj(R_\bullet)$ that is not a k-valued point can have "structural multiplicity" given by the degree of $R_\bullet/p$, where p is the minimal prime corresponding to the component. We define the *multiplicity* of the irreducible component corresponding to p to be

$$e(R_\bullet/p) \cdot l(O_{Proj(R_\bullet),p}), \tag{3.1}$$

where l denotes the *length* of a commutative ring, i.e., the length of a maximal chain of ideals of $O_{Proj(R_\bullet),p}$, or ∞ if no maximal chain exists (see for example [8] Section 2.4 for more details). If p is a generic point of an irreducible component of $Proj(R_\bullet)$, then $O_{Proj(R_\bullet),p}$ is zero-dimensional, and its length is known to be finite. Therefore, with the above definition, the multiplicities of components of intersections are always finite. If p corresponds to a k-valued point (if k is algebraically closed, then this is the same as a *closed point*, i.e., a point that is not a generic point), then $e(R_\bullet/p) = 1$ and the length of $e(R_\bullet/p)$ is known to be its dimension as a k-vector space. On the other hand, if p corresponds to an arbitrary closed point, we have that $e(R_\bullet/p) \cdot l(O_{Proj(R_\bullet),p})$ equals the dimension of $O_{Proj(R_\bullet),p}$ as a k-vector space. Therefore, our former definition of the intersection number is just a special case of this more general definition.

An *ascending filtration* of a k-algebra A is an ascending chain $k = A_0 \subset A_1 \subset A_2 \subset ...$ of finite dimensional k-vector subspaces of A satisfying $A_iA_j \subset A_{i+j}$, $\bigcup A_i = A$. An A-module M *with ascending filtration* is an A-module with ascending chain of finite-dimensional k-subspaces $M_0 \subset M_1 \subset M_2 \subset ...$ satisfying $A_iM_j \subset M_{i+j}$ and $\bigcup M_i = A$.

Let $a_1, ..., a_r$ generate A as an k-algebra and denote by V the k-vector space spanned by $1, a_1, ..., a_r$. If W, W' are k-subspaces of A, denote by WW' the k-space spanned by elements of form ww', where $w \in W$ and $w' \in W'$. This product is clearly both commutative and associative. Now $\bigcup V^i = A$, so the V^i give rise to an ascending filtration on A, called the V-adic filtration. An A-module with ascending filtration is called *V-good* if $VM_i = M_{i+1}$ for $i \gg 0$. Any quotient module of M has a naturally induced ascending filtration, given by the images of M_i in the canonical projection. If the original filtration on M is V-good, then so is the induced filtration on the quotient module as well.

Let A be a ring with V-adic ascending filtration. Now we can associate the graded ring $gr(A)$ to A as follows: $gr(A) = A_0 \oplus (A_1/A_0) \oplus (A_2/A_1) \oplus ...$, where the multiplication is defined in the obvious way. It is clear that $gr(A)$ is a graded k-algebra finitely generated in degree one. Similarly, to any A-module M with ascending filtration, we can associate the graded $gr(A)$-module $gr(M) = M_0 \oplus (M_1/M_0) \oplus (M_2/M_1) \oplus ...$ where the multiplication by $gr(A)$ is again defined in the obvious way. The reason for such a weird definition is to give the following characterization for V-good A-modules with ascending filtration:

Lemma 3.3.5. *An A-module M with an ascending filtration is V-good if and only if $gr(M)$ is a finitely generated graded $gr(A)$-module.*

Proof. If M is V-good, then $A_1(M_{i+1}/M_i) = M_{i+2}/M_{i+1}$ for large enough i, so we need to generate only finitely many M_{i+1}/M_i. All of them are finite dimensional k-vector spaces, so $gr(M)$ is indeed a finitely generated graded $gr(A)$-module.

If $gr(M)$ is finitely generated over $gr(A)$, then we may assume that it is finitely generated by homogeneous elements. If d is the highest degree of any of the chosen generators, then $(A_k/A_{k-1})(M_d/M_{d-1}) = M_{k+d}/M_{k+d-1}$, i.e., $A_1(M_i/M_{i-1}) = M_{i+1}/M_i$ for $i \geq d$. As A_1 contains 1, we know that $M_i \subset A_1 M_i$, so actually $A_1 M_i = M_{i+1}$ for $i \geq d$, proving the claim. □

Now we can prove the analogue of Artin-Rees lemma for ascending filtrations.

Proposition 3.3.6. ***Artin-Rees for ascending filtrations.*** *Let A have the V-adic filtration and M have a V-good filtration. For a submodule N of M, define an ascending filtration by setting $N_i = N \cap M_i$. This is a V-good filtration.*

Proof. As $gr(A)$ is a Noetherian ring and $gr(M)$ is a finitely generated $gr(A)$-module, we see that $gr(M)$ is a Noetherian module. The natural inclusion map $gr(N) \to gr(M)$ is injective, so $gr(N)$ is a Noetherian module as well. Therefore $gr(N)$ is finitely generated graded $gr(A)$-module, so by the previous lemma the filtration on N is V-good. □

The value of V-good filtrations lies in the asymptotic behaviour of $\dim(M_i)$. If a k-algebra A has the V-adic filtration, then $gr(A)$ is a graded k-algebra finitely generated in degree one, and therefore has a Hilbert polynomial. On the other hand, as $\dim(A_i) = \dim(A_i/A_{i-1}) + \dim(A_{i-1}/A_{i-2}) + ... + \dim(A_0)$, we see that $\dim(A_i)$ is given by a polynomial, say P_A, for large enough i. Let d be the degree of this polynomial. If we have an A-module $M \cong A$ with a V-good filtration, then we have that $|P_A(i) - \dim(M_i)| \in \mathcal{O}(i^{d-1})$. This can be seen as follows: let $m \in \mathbb{N}$ be the bound after which $A_1 M_i = M_{i+1}$ for all i, and let $n \in \mathbb{N}$ be such that A_n contains M_m. We may clearly assume that $n \geq m$. Now A_{n+i} contains M_{m+i} for all $i \geq 0$, so especially $P_A(n-m+i) \geq \dim(M_i)$ for large enough i. Thus

$$\dim(M_i) - P_A(i) \in \mathcal{O}(P_A(i+n-m) - P_A(i)) = \mathcal{O}(i^{d-1}).$$

On the other hand, we can find such $m' \geq m$ that $M_{m'}$ contains A_0. Thus $M_{m'+i}$ contains A_i for all positive i, and hence $\dim(M_i) \geq P(i-m')$ for large i, or put otherwise,

$$P_A(i) - \dim(M_i) \in \mathcal{O}(P_A(i) - P_A(i-m')) = \mathcal{O}(i^{d-1}).$$

So we truly have that $|P_A(i) - \dim(M_i)| \in \mathcal{O}(i^{d-1})$.

Before being able to make use of the above asymptotic behaviour, we need to recall some basic facts about Noetherian modules. If M is a finitely generated module over a Noetherian ring A, then we have such an ascending chain of submodules $0 = M_0 \subset M_1 \subset \ldots \subset M_l = M$ that $M_i/M_{i-1} = A/p_i$, where p_i is a prime ideal of A. Moreover, it is known that the minimal primes among the p_i are exactly the minimal primes in the support of M ([9] Section 1.7). If p is such a prime, then the length of M_p is known to be the number of distinct indices $i = 1..l$ such that $p = p_i$. Now we can see exactly what the degree of a projective scheme tells us:

Theorem 3.3.7. *Let $Proj R_\bullet$ be a d-dimensional projective scheme. Now the number of d-dimensional components of $Proj R_\bullet$, counted with multiplicity as defined in 3.1, is exactly $e(R_\bullet)$.*

Proof. As neither the sheaf structure of $Proj R_\bullet$ nor the Hilbert polynomial of $R_\bullet$ change by taking quotient with $R'_\bullet$, we may assume that the irrelevant ideal R_+ is not associated to $R_\bullet$ (see the Appendix 4.2). Thus there is a degree one homogeneous element $r \in R_\bullet$, which is not a zerodivisor. Recall that the prime ideals of $((R_\bullet)_r)_0$ are in natural bijective correspondence with the homogeneous prime ideals of $R_\bullet$ that do not contain r, so especially $Spec((R_\bullet)_r)_0$ contains all the generic points of the irreducible components of $Proj(R_\bullet)$. Moreover, recall that the leading coefficient of the Hilbert polynomial $h_{R_\bullet}$ is $e(R_\bullet)/d!$.

Denote by A the ring $((R_\bullet)_r)_0$. The grading on $R_\bullet$ gives us an ascending filtration on A: we simply set $A_i = r^{-i} R_i$. If we denote $V \equiv A_1$, then it is clear that the above filtration is just the V-adic filtration on A. As r was assumed not to be a zerodivisor, we have that the dimension of A_i is exactly the dimension of R_i, so the dimension of A_i is given by the Hilbert polynomial $h_{R_\bullet}(i)$ for large enough i. For a prime ideal p of A denote by p' the corresponding homogeneous prime ideal of $R_\bullet$. We know that there is a natural isomorphism between A/p and $(((R_\bullet/p')_r)_0)$, so if we denote by B the ring A/p and by V' the image of V in B, and if B is given the V'-adic filtration, then the dimensions of B_i are given by the Hilbert polynomial of $R_\bullet/p'$ for i large enough.

As A is a Noetherian ring, we have an ascending chain of ideals $0 = I_0 \subset I_1 \subset ... \subset I_l = A$, where $I_j/I_{j-1} \cong A/p_j$ for some prime ideal p_j. By the ascending version of Artin-Rees lemma, we know that the induced filtrations on $B^j = I_j/I_{j-1}$ are V-good. Moreover, by additivity of dimension, we know that $\dim(A_i) = \dim(B_i^1) + ... + \dim(B_i^l)$. By the previous discussions, if we denote by h_j the Hilbert polynomial giving the dimensions of B_i^j for large i, we know that $|h_j(i) - \dim(B_i^j)| \in \mathcal{O}(i^{d-1})$. Thus $|h_1(i) + ... + h_l(i) - h_{R_\bullet}(i)| \in \mathcal{O}(i^{d-1})$, which shows that the sums of the leading terms of h_j, where j runs over all indices $1..l$ where p_j cuts out a d-dimensional irreducible component of $Spec(A)$, must be the leading term of $h_{R_\bullet}$, i.e.,

$$\sum_{\dim(A/p_j)=d} e(R_\bullet/p'_j) = e(R_\bullet).$$

By the discussion preceding this theorem, the above sum is exactly the sum of the multiplicities of the d-dimensional components of $Proj(R_\bullet)$, so we are done. □

When $Proj R_\bullet$ is equidimensional, we see that the number of components, if counted with multiplicity, is exactly the degree $e(R_\bullet)$. As regular sequences of homogeneous polynomials cut out equidimensional varieties, we obtain the following generalization of Bézout's theorem.

Theorem 3.3.8. *Let $f_1, ..., f_r$ be a regular sequence of homogeneous polynomials in $k[x_0, ..., x_n]$, whose degrees are $d_1, ..., d_r$ respectively. Now the intersection $V(f_1) \cap ... \cap V(f_r) \subset \mathbb{P}^n$ is equidimensional of dimension $n - r$ and the number of components of the intersection is exactly $d_1 \cdots d_r$ if they are counted with multiplicity as defined in 3.1.*

3.4 Intersections of subvarieties in $\mathbb{P}^n$

Homogeneous ideals of $k[x_0, ..., x_n]$ cut out subvarieties of $\mathbb{P}^n$. In this section we look into intersections of arbitrary subvarieties, not just hypersurfaces as in the previous section. First we introduce an important technique: Serre's reduction to diagonal.

Suppose that we have two homogeneous ideals I and J of $k[x_0, ..., x_n]$. The intersection of $V(I)$ and $V(J)$ is given by the homogeneous ideal $I + J$. On the other hand, in order to get the intersection $V(I) \cap V(J)$, we may also form the product $V(I) \times V(J) \subset \mathbb{A}^{2n+2}$, and intersect it with the diagonal $\Delta(\mathbb{A}^{n+1}) \subset \mathbb{A}^{2n+2}$. This can be verified easily algebraically.

Let us have the coordinate ring $k[x_0, ..., x_n, x'_0, ..., x'_n]$. Let I' be the ideal generated by the elements of I in $k[x_0, ..., x_n]$ and J' be the ideal generated by the elements of

J thought as elements of $k[x'_0, ..., x'_n]$. From the right exactness of the tensor product, we see that the ring $k[x_0, ..., x_n, x'_0, ..., x'_n]/(I' + J')$ is isomorphic to the tensor product $(k[x_0, ..., x_n]/I) \otimes_k (k[x_0, ..., x_n]/J)$. If we identify each x_i with x'_i, i.e., take quotient by an ideal with generators of form $1 \otimes [x_i] - [x_i] \otimes 1$, then we clearly obtain $k[x_0, ..., x_n]/(I + J)$! Even though this may look like a more complicated way of getting the intersection, it makes computations much easier, as we shall see shortly.

Let $R_\bullet$ and $S_\bullet$ be graded k-algebras that are finitely generated in degree one. Now we can get a graded structure on their tensor product over k by setting $(R_\bullet \otimes_k S_\bullet)_n = \bigoplus_{i+j=n} R_i \otimes_k S_j$. From this definition, the following property is obvious:

Proposition 3.4.1. *The Hilbert Series of $R_\bullet \otimes_k S_\bullet$ is the product of $H_{R_\bullet}$ and $H_{S_\bullet}$.*

This translates to the following property of degree.

Proposition 3.4.2. $e(R_\bullet \otimes_k S_\bullet) = e(R_\bullet)e(S_\bullet)$.

Proof. Recall, that the Hilbert polynomials of $R_\bullet$ and $S_\bullet$ can be written in the form $f/(1-t)^{d_1}$ and $g/(1-t)^{d_2}$, where the denominators and nominator share no common factors. As fg and $(1-t)^{d_1+d_2}$ are coprime, we know that degree of the product $R_\bullet \otimes_k S_\bullet$ is the sum of coefficients of fg. On the other hand, this is clearly the product of the sums of coefficients of f and g, i.e., the product of $e(R_\bullet)$ and $e(S_\bullet)$. □

Before we come back to the intersections of subschemes, we need some basic results concerning dimension.

Proposition 3.4.3. *Let $R_\bullet$ be a graded k-algebra that is finitely generated in degree one, and that is also an integral domain. Let n be the dimension of $Proj R_\bullet$, and let r be a homogeneous element of $R_\bullet$. Now each component of $Proj(R_\bullet/(r))$ is $(n-1)$-dimensional.*

Proof. It follows from the Krull's principal ideal theorem (for example [9] III Corollary 4) that any prime ideal that is minimal over (r) (they are necessarily homogeneous) has height at most 1 (the height of p can be thought as the codimension of $V(p)$ in $Proj R_\bullet$). As $R_\bullet$ was assumed to be a domain, the height of all such primes is *exactly* 1. If $p \subset R_\bullet$ is such a minimal prime, as codimension and dimension work "as one would assume" in this situation (see [9] III Proposition 15), we see that the dimension of $Proj(R_\bullet/p)$ is exactly $n-1$. This is exactly what we needed to prove. □

Proposition 3.4.4. *Let $R_\bullet$ and $S_\bullet$ define projective schemes of dimensions n and m respectively. Now $Proj(R_\bullet \otimes_k S_\bullet)$ is equidimensional of dimension $n + m + 1$.*

Proof. We first reduce to the case where both the algebras are domains. Let p be a minimal prime ideal of $R_\bullet \otimes_k S_\bullet$. Now the pullback of p in the natural maps $R_\bullet \to R_\bullet \otimes_k S_\bullet$ and

$S_\bullet \to R_\bullet \otimes_k S_\bullet$ gives us homogeneous prime ideals $p_1 \subset R_\bullet$ and $p_2 \subset S_\bullet$. Now p contains $p_1 \otimes_k S_\bullet + R_\bullet \otimes_k p_2$, so its image in $(R_\bullet/p_1) \otimes_k (S_\bullet/p_2)$ is a minimal prime. Therefore we may assume that $R_\bullet$ and $S_\bullet$ are integral domains, and this case is taken care of by [9] III Lemma 6. □

As an immediate corollary, we obtain the following result concerning intersections:

Corollary 3.4.5. *Let I and J be homogeneous ideals of $k[x_0, ..., x_n]$ cutting out equidimensional projective schemes $V(I), V(J) \subset \mathbb{P}^n$ of dimensions d_1 and d_2 respectively. Now every component of the intersection $V(I) \cap V(J)$ is at least $d_1 + d_2 - n$ dimensional.*

Proof. We know that each component of $Proj(R_\bullet \otimes_k S_\bullet)$ has the dimension $d_1 + d_2 + 1$. For cutting out the diagonal, we need $n + 1$ relations, so each component in the intersection has the dimension of at least $d_1 + d_2 - n$. □

The previous result may be better understood in the terms of codimension. If d is the degree of an irreducible component of the intersection $V(I) \cap V(J)$, then the above theorem tells us that $(n - d) \leq (n - d_1) + (n - d_2)$, so the codimension behaves as one would naively expect. If each component of the intersection has exactly the degree $d_1 + d_2 - n$, then the intersection is called *proper*. Before stating a nice property of proper intersections, we need a lemma:

Lemma 3.4.6. *Let $Proj R_\bullet$ have dimension n, r a homogeneous element of $R_\bullet$ of degree d. If the dimension of $Proj(R_\bullet/(r))$ is $n - 1$, then the degree of the quotient ring is bound below by $d \cdot e(R_\bullet)$.*

Proof. Recall, that the Hilbert polynomial of the homogeneous ideal (r) is bound above by $h_{R_\bullet}(i - d)$. Therefore the Hilbert polynomial of $R_\bullet/(r)$ is bound below by $h_{R_\bullet}(i) - h_{R_\bullet}(i - d)$. As the Hilbert polynomial of $R_\bullet/(r)$ must have the same degree as $h_{R_\bullet}(i) - h_{R_\bullet}(i - d)$ by the assumption on dimension, we see that the claim holds. □

Using the above theorem inductively, we obtain:

Lemma 3.4.7. *Let I and J are homogeneous ideals of $k[x_0, ..., x_n]$ defining equidimensional projective schemes, which intersect properly. Now the degree of the graded k-algebra $k[x_0, ..., x_n]/(I + J)$ is bound* below *by the product of the degrees of $k[x_0, ..., x_n]/I$ and $k[x_0, ..., x_n]/J$.*

Proof. As each component of the intersection must have the "right" dimension, we may use the preceding lemma $n + 1$ times to obtain the claim. □

This inequality can be strict as the following example (a slightly modified version of the Example 14.4 found in [10]) shows. Lets look at the homogeneous ideals (xz, xw, yz, yw) and $(x - z, y - w)$ of $k[x, y, z, w, v]$. The first one is clearly the product of (x, y) and (y, z), and therefore it cuts out the union of two planes in $\mathbb{P}^4$. The second one cuts out a single plane in $\mathbb{P}^4$. The intersection $k[x, y, z, w, v]/(xz, xw, yz, yw, x - z, y - w)$ is clearly isomorphic to $k[x, y, v]/(x^2, xy, y^2)$, so the intersection is (topologically) a single point. Thus the subschemes intersect properly.

The ring $k[x, y, z, w, v]/(xz, xw, yz, yw)$ is contained in the algebra spanned by $k[x, y, v]$ and $k[z, w, v]$. As only the elements of $k[v]$ are "counted twice", we see that the Hilbert polynomial of $k[x, y, z, w, v]/(xz, xw, yz, yw)$ is $2\binom{2+i}{2} - 1$, so especially the degree of the ring is 2. On the other hand, the degree of $k[x, y, z, w, v]/(x-z, y-w) \cong k[x, y, z]$ is clearly 1, so the product of the degrees is 2. The Hilbert polynomial of $k[x, y, v]/(x^2, xy, y^2)$ is 3, as $k[x, y, v]/(x^2, xy, y^2)$ is the direct sum of $k[v]$, $xk[v]$ and $yk[v]$. As $3 > 2$, we see that the inequality can be strict.

This raises the following question: can a proper intersection of two equidimensional subvarieties of $\mathbb{P}^n$ have more components than the product of the degrees? The answer, as we shall see shortly, is *no*: the extra degree comes from "extra multiplicity" of components. There is a way to fix this: if we used multiplicities given by the Serre's Tor-formula, then the equality would hold. Proving this is the topic of the Section 3.5.

In [11] Vogel gives an affirmative answer to the following question by Kleiman: Let $V(I_1), ..., V(I_r) \subset \mathbb{P}^n$ be equidimensional subschemes of degrees $d_1, ..., d_r$ respectively. Is the number of components of the intersection $V(I_1) \cap ... \cap V(I_r)$ bound above by $d_1 \cdots d_r$? The answer is *yes*. This is proved in [11], and Vogel gives references to two other proofs. We are going to give a simple proof shortly. We first fix some terminology: by the *degree* of an irreducible subset X of $\mathbb{P}^n$, $\deg(X)$, we mean the degree of the graded k-algebra $k[x_0, ..., x_n]/p$, where p is the homogeneous prime ideal corresponding to the aforementioned irreducible subset.

Lemma 3.4.8. *Let us have an irreducible subset X of $\mathbb{P}^n$, which has dimension δ and degree d. Let us intersect X with a hyperplane H. Now three things may happen:*

- *If H contains X, then the intersection is X.*
- *If H doesn't contain X and $\delta > 0$, then the intersection has components $X_1, ..., X_r$, all of which have dimension $\delta - 1$, and the sum of $\deg(X_i)$ is at most $\deg(X)$.*
- *If H doesn't contain X and $\delta = 0$, then the intersection is empty.*

Proof. The first and the third cases are trivial, so we only need to prove the second one. Let p be the prime ideal corresponding to X, and r the nonzero element of $R_\bullet \equiv k[x_0, ..., x_n]$ corresponding to the hypersurface H. We already know that $Proj(R_\bullet/(r))$ is equidimensional, and that the degree of $R_\bullet/(r)$ is $\deg(r) \cdot e(R_\bullet) = 1 \cdot e(R_\bullet)$. The claim then follows from 3.3.1. □

Let X be any algebraic subset of $\mathbb{P}^n$. Denote by $n(X)$ the sum $\deg(X_1) + ... + \deg(X_r)$, where X_i runs over the irreducible components of X. We call this the *geometric multiplicity* of X. This can be thought as a number taking into account both the number of components of X, and the *capacity* of those components to split into multiple components in intersections. When X is equidimensional, we have $n(X) \leq e(X)$ by 3.3.1. The geometric multiplicity behaves remarkably well under intersection:

Theorem 3.4.9. *Let $X, Y \subset \mathbb{P}^n$ be algebraic subsets of $\mathbb{P}^n$. Now $n(X \cap Y) \leq n(X)n(Y)$.*

Proof. It is clear that we may break this into the intersection of irreducible algebraic sets, so we assume that X and Y are irreducible. Let p_1 and p_2 be the homogeneous prime ideals corresponding to X and Y. Now, by definition, the degrees of $k[x_0, ..., x_n]/p_1$ and $k[x_0, ..., x_n]/p_2$ are exactly the geometric multiplicities of X and Y respectively. We know that $(k[x_0, ..., x_n]/p_1) \otimes_k (k[x_0, ..., x_n]/p_2)$ is equidimensional, and that its degree is $n(X)n(Y)$, so $n(Z) \leq n(X)n(Y)$, where we denote by Z the "product" of X and Y in $\mathbb{P}^{2n+1}$. When we intersect Z with the diagonal, we are simply intersecting Z with $n+1$ hyperplanes. Therefore, we may use the previous lemma $n+1$ times to obtain the claim. □

This theorem generalizes trivially to intersections of more than n algebraic subsets of $\mathbb{P}^n$, and thus the answer to Kleiman's question follows immediately.

Corollary 3.4.10. *Let $V(I_1), ..., V(I_r) \subset \mathbb{P}^n$ be equidimensional subschemes of degrees $d_1, ..., d_r$ respectively. Now the number of components of the intersection $V(I_1) \cap ... \cap V(I_r)$ is bound above by $d_1 \cdots d_r$.*

Proof. As $n(V(I_i)) \leq d_i$, we see that $n(V(I_1) \cap ... \cap V(I_r)) \leq d_1 \cdots d_r$. As the number of components of an algebraic set X is bound above by $n(X)$, we are done. □

3.5 Serre's Tor-formula

In this section, we assume familiarity with the basics of homological algebra. The details can be found in for example the first three chapters of [12]. In [9] Serre defines the *intersection multiplicity* of two A-modules M and N as

$$\chi(M, N, p) = \sum_i (-1)^i l_{A_p}(\mathrm{Tor}_i^{A_p}(M_p, N_p)). \tag{3.2}$$

Due to its local nature, the formula generalizes trivially to (quasi-coherent) sheaves over a scheme, so especially we have a formula in the projective case as well. In this section, we will motivate the definition and prove some basic results.

Before beginning, we make the following remark concerning homological algebra. If we have a graded ring $R_\bullet$, then the graded modules over $R_\bullet$ form an abelian category. It is clear that this category has enough projectives, as any graded $R_\bullet$ module $M_\bullet$ can be given as a quotient of a direct sum of $R_\bullet[i]$, and such modules are projective. Therefore we may define the *graded Tor-functors* as left derived functors of the graded tensor product functor $M_\bullet \otimes_{R_\bullet}$. The usual properties of derived functors follow. As in the nongraded case, if we have the tensor product $M_\bullet \otimes_{R_\bullet} N_\bullet$, then we get the same Tor-modules $\mathrm{Tor}_i^{R_\bullet}(M_\bullet, N_\bullet)$ regardless of whether we take the projective resolution for $M_\bullet$ or $N_\bullet$. This can be proved by proving the next lemma, which we will need later:

Lemma 3.5.1. *Let $M_\bullet$ and $N_\bullet$ be graded $R_\bullet$-modules, $\mathcal{P}$ and $\mathcal{Q}$ some projective resolutions for $M_\bullet$ and $N_\bullet$ respectively. We may form the tensor product bicomplex $\mathcal{P} \otimes_{R_\bullet} \mathcal{Q}$ and take its total complex $\mathcal{T} = \mathrm{Tot}(\mathcal{P} \otimes_{R_\bullet} \mathcal{Q})$. Now $\mathcal{T}$ is quasi-isomorphic to the complexes $M_\bullet \otimes_{R_\bullet} \mathcal{Q}$ and $\mathcal{P} \otimes_{R_\bullet} N_\bullet$, so especially their homologies coincide.*

Proof. The proof of this is very similar to the case of nongraded modules, and the proof for that case can be found in any introductory book on homological algebra, at least if it discusses "balancing Tor". □

The reason we want to have graded Tor-functors is to be able to use Hilbert polynomials. The first property that we are going to prove is:

Proposition 3.5.2. *Let $R_\bullet$ be a graded k-algebra, and $M_\bullet$ a finitely generated graded $R_\bullet$-module. Now the polynomials*

$$\mathcal{H}_{(-)} = \sum_i (-1)^i h_{\mathrm{Tor}_i^{R_\bullet}(M_\bullet, -)}$$

define an additive function whenever the sum is finite.

Proof. Let us have the following short exact sequence

$$0 \to N'_\bullet \to N_\bullet \to N''_\bullet \to 0,$$

and assume that $\mathcal{H}_{N'_\bullet}$, $\mathcal{H}_{N_\bullet}$ and $\mathcal{H}_{N''_\bullet}$ are well defined. Using the long exact sequence

$$
\begin{array}{ccccccc}
 & & 0 & \longrightarrow & \mathrm{Tor}_n^{R_\bullet}(M_\bullet, N''_\bullet) & & \\
\mathrm{Tor}_{n-1}^{R_\bullet}(M_\bullet, N'_\bullet) & \longrightarrow & \cdots & & & & \\
 & & \cdots & \longrightarrow & \mathrm{Tor}_1^{R_\bullet}(M_\bullet, N''_\bullet) & & \\
\mathrm{Tor}_0^{R_\bullet}(M_\bullet, N'_\bullet) & \longrightarrow & \mathrm{Tor}_0^{R_\bullet}(M_\bullet, N_\bullet) & \longrightarrow & \mathrm{Tor}_0^{R_\bullet}(M_\bullet, N''_\bullet) & \longrightarrow & 0
\end{array}
$$

and the additivity of the Hilbert polynomial, we see that the polynomials $\mathcal{H}_{(-)}$ behave additively, so we are done. □

This is the motivation, we promised in the beginning. Taking higher Tor-modules into account by forming an alternating sum, we can save the additivity that gets lost in tensoring (after all, tensor product is only right-exact). Problems may arise if the sum was not finite, i.e., if infinitely many of the Tor-modules did not vanish. One case where this does *not* happen, is when at least the other "operand" is $R_\bullet/I$, where I can be generated by a homogeneous regular sequence.

Lemma 3.5.3. *Let $r_1, ..., r_n$ be a regular sequence of homogeneous elements of $R_\bullet$, $M_\bullet$ a finitely generated $R_\bullet$-module. Denote by $\mathcal{H}_i$ the polynomial*

$$\sum_i (-1)^i h_{\mathrm{Tor}_i^{R_\bullet}(M_\bullet, R_\bullet/(r_1,...,r_i))}.$$

Now these polynomials satisfy the relation $\mathcal{H}_i(x) = \mathcal{H}_{i-1}(x) - \mathcal{H}_{i-1}(x-1)$.

Proof. If $i = 0$, then the other operand is $R_\bullet$, and the higher Tor-modules vanish. Let then $i > 0$. Now, using the multiplication by r_i, we obtain the short exact sequence

$$0 \to R_\bullet/(r_1, ..., r_{i-1})[1] \xrightarrow{r_i} R_\bullet/(r_1, ..., r_{i-1}) \to R_\bullet/(r_1, ..., r_i) \to 0,$$

which gives the usual long exact sequence. By induction, we see that the Tor-modules $\mathrm{Tor}_j^{R_\bullet}(M_\bullet, R_\bullet/(r_1, ..., r_i))$ must vanish whenever $j > i$. Moreover, as $\mathrm{Tor}_j^{R_\bullet}(M_\bullet, N_\bullet[m]) = \mathrm{Tor}_j^{R_\bullet}(M_\bullet, N_\bullet)[m]$, we see that the relation $\mathcal{H}_i(x) = \mathcal{H}_{i-1}(x) - \mathcal{H}_{i-1}(x-1)$ holds. □

For the rest of the section, denote $A_\bullet = k[x_0, ..., x_n]$, $B_\bullet = A_\bullet \otimes_k A_\bullet$, and let I and J be homogeneous ideals of $A_\bullet$. Denote by Δ the "diagonal ideal" of $B_\bullet$. As $A_\bullet \cong B_\bullet/\Delta$, we can think any $A_\bullet$-module as a $B_\bullet$-module in a natural way. We can get the intersection ring $A_\bullet/(I+J) = \mathrm{Tor}_0^{A_\bullet}(A_\bullet/I, A_\bullet/J)$ by reducing to diagonal, but actually this is actually true for the higher Tor-modules as well.

Lemma 3.5.4. $\mathrm{Tor}_i^{A_\bullet}(M_\bullet, N_\bullet) \cong \mathrm{Tor}_i^{B_\bullet}(M_\bullet \otimes_k N_\bullet, B_\bullet/\Delta)$ *as graded $B_\bullet$-modules.*

Proof. Let $\mathcal{P}$ and $\mathcal{Q}$ be $A_\bullet$ projective resolutions for $M_\bullet$ and $N_\bullet$ respectively. Denote by $\mathcal{T}$ the total complex of the tensor product bicomplex of $\mathcal{P}$ and $\mathcal{Q}$. Now, by 3.5.1, the homologies of $\mathcal{T}$ are exactly $\mathrm{Tor}_i^k(M_\bullet, N_\bullet)$. Thus the homology at zero is $M_\bullet \otimes_k N_\bullet$, and the higher homologies vanish as both modules are free over k. This means that $\mathcal{T}$ is a $B_\bullet$-resolution of $M_\bullet \otimes_k N_\bullet$. In fact, it is a projective resolution as $P_\bullet \otimes_k Q_\bullet$ is a projective $B_\bullet$-module for any projective $A_\bullet$-modules $P_\bullet$ and $Q_\bullet$, and as the direct sum of projective modules is projective.

Now we know that the Tor modules $\mathrm{Tor}_i^{B_\bullet}(M_\bullet \otimes_k N_\bullet, B_\bullet/\Delta)$ are given by the homologies of the complex $\mathcal{T} \otimes_k (B_\bullet/\Delta)$. The tensor product $\mathcal{T} \otimes_k (B_\bullet/\Delta)$ is just the total complex of the bicomplex $(\mathcal{P} \otimes_k \mathcal{Q}) \otimes_k (B_\bullet/\Delta)$, which is clearly isomorphic to $\mathcal{P} \otimes_{A_\bullet} \mathcal{Q}$ thought as a complex of graded $B_\bullet$-modules. The homologies of this complex, and hence the homologies of $\mathcal{T} \otimes_k (B_\bullet/\Delta)$, are exactly the Tor-modules $\mathrm{Tor}_i^{A_\bullet}(M_\bullet, N_\bullet)$ by 3.5.1, which is exactly what we wanted to prove. □

Now we can use our previous lemmas to prove the following:

Corollary 3.5.5. *Let d_1 and d_2 be the dimensions of the projective vanishing sets $V(I)$ and $V(J)$, and let e_1, e_2 be the degrees of $A_\bullet/I$ and $A_\bullet/J$. Assume that $d_1 + d_2 - n \geq 0$. Now the leading term of the polynomial*

$$\sum_i (-1)^i h_{\mathrm{Tor}_i^{A_\bullet}(A_\bullet/I, A_\bullet/J)}$$

is exactly

$$\frac{e_1 e_2}{(d_1 + d_2 - n)!} x^{d_1 + d_2 - n}.$$

Proof. Recall that the degree of $(A_\bullet/I) \otimes_k (A_\bullet/J)$ is $e_1 e_2$. Using the previous lemma we can concentrate on the tor modules $\mathrm{Tor}_i^{A_\bullet \otimes_k A_\bullet}((A_\bullet/I) \otimes_k (A_\bullet/J), B_\bullet/\Delta)$, and as Δ can be generated by a regular sequence of $n+1$ elements, the claim follows immediately from 3.5.3. □

The above theorem did not need any assumptions on properness of the intersection, but in order for the formula to be of any use, we need to assume the properness of the intersecion. From now on $V(I)$ and $V(J)$ are assumed to be equidimensional of dimension d_1 and d_2, degree e_1 and e_2, and we assume that they intersect properly. Recall that a graded $A_\bullet$-module $M_\bullet$ defines a quasicoherent $O_{\mathbb{P}^n}$-module $\mathcal{F}_{M_\bullet}$ via the usual localization procedure. The annihilator of $M_\bullet$ is clearly homogeneous, and the homogeneous prime ideals in the support of $M_\bullet$ are in natural one-to-one correspondence with the points of $\mathbb{P}^n$ where the stalk of the sheaf $\mathcal{F}_{M_\bullet}$ does not vanish.

It is known that the support of $\mathcal{F}_{M_\bullet}$, the points where the stalk of the sheaf does not vanish, is a closed subset of $\mathbb{P}^n$. We call the dimension of this subset the *dimension* of the sheaf $\mathcal{F}_{M_\bullet}$. Now we may formulate the analogue of 3.3.7 for graded modules.

Proposition 3.5.6. *Let $\mathcal{F}_{M_\bullet}$ be a d-dimensional sheaf. Now the number of d-dimensional components of the support $Supp\mathcal{F}_{M_\bullet}$, counted with multiplicity*

$$e(A_\bullet/p) \cdot l_{O_{\mathbb{P}^n,p}}(\mathcal{F}_{M_\bullet,p}),$$

where p is the homogeneous prime ideal corresponding to the irreducible component, is exactly $e(M_\bullet)$.

Proof. The proof of 3.3.7 generalizes to this situation immediately. □

It is a basic fact of homological algebra, that the annihilator of $\mathrm{Tor}_i^{A_\bullet}(N_\bullet, M_\bullet)$ contains the annihilators of $N_\bullet$ and $M_\bullet$. Thus we see that $\mathrm{Tor}_i^{A_\bullet}(A_\bullet/I, A_\bullet/J)$ are annihilated by $I + J$, so especially their support cannot contain any homogeneous prime ideals that do not contain $I + J$. Therefore we can formulate a version of Bézout's theorem as follows:

Theorem 3.5.7. *If we count the number of components in the intersection $V(I) \cap V(J) \subset \mathbb{P}^n$ with multiplicity*

$$e(A_\bullet/p) \sum_i (-1)^i l_{O_{\mathbb{P}^n,p}}(\mathcal{F}_{\mathrm{Tor}_i^{A_\bullet}(A_\bullet/I, A_\bullet/J),p})$$

then there are exactly $e_1 e_2$ components.

Proof. We already know that

$$\sum_i (-1)^i e(\mathrm{Tor}_i^{A_\bullet}(A_\bullet/I, A_\bullet/J)) = e_1 e_2$$

where i runs over all such indices that $\mathrm{Tor}_i^{A_\bullet}(A_\bullet/I, A_\bullet/J)$ has the same dimension as $A_\bullet/(I + J)$. This, together with the previous lemma, proves the claim. □

We next show that the stalks of the "Tor-sheaf" are exactly the Tor-modules in Serre's formula, i.e., taking Tor-modules and taking stalks "commute".

Proposition 3.5.8. *The $O_{\mathbb{P}^n,p}$-modules $\mathcal{F}_{\mathrm{Tor}_i^{A_\bullet}(M_\bullet,N_\bullet),p}$ and $\mathrm{Tor}_i^{O_{\mathbb{P}^n,p}}(\mathcal{F}_{M_\bullet,p}, \mathcal{F}_{N_\bullet,p})$ are isomorphic.*

Proof. Let $a \in A_\bullet$ be a linear homogeneous polynomial. Denote by F the functor from the graded $A_\bullet$-modules, to $((A_\bullet)_a)_0$-modules, which sends $M_\bullet$ to $((M_\bullet)_a)_0$. It is known that this functor is exact, and that it preserves direct sums and tensor products. Moreover, $F(A_\bullet[i])$ is isomorphic to $F(A_\bullet) = ((A_\bullet)_a)_0$. Therefore F preserves projectivity: the projective graded $A_\bullet$ modules are direct summands of direct sums of $A_\bullet[i]$, and F sends such graded modules to direct summands of free $((A_\bullet)_a)_0$-modules, which are known to be projective.

Let $\mathcal{P}$ be a projective resolution of $M_\bullet$. Now $F\mathcal{P}$ is a projective resolution of $F(M_\bullet)$, and as $F(\mathcal{P} \otimes_{A_\bullet} M_\bullet) = F\mathcal{P} \otimes_{FA_\bullet} FM_\bullet$, we see that there is a canonical isomorphism between $(\mathrm{Tor}_i^{A_\bullet}(M_\bullet, N_\bullet)_a)_0$ and $\mathrm{Tor}_i^{((A_\bullet)_a)_0}(((M_\bullet)_a)_0, ((N_\bullet)_a)_0)$. On the other hand, as localization is exact and preserves projectivity, we see that there is a canonical isomorphism between $\mathrm{Tor}_i^{((A_\bullet)_a)_0}(((M_\bullet)_a)_0, ((N_\bullet)_a)_0)$ and $\mathrm{Tor}_i^{O_{\mathbb{P}^n,p}}(\mathcal{F}_{M_\bullet,p}, \mathcal{F}_{N_\bullet,p})$, which concludes the proof. □

This shows that the intersection numbers given by Serre's formula 3.2 satisfy Bézout's theorem in proper intersections.

Chapter 4

Appendix

4.1 Homogeneous Noether normalization

In this section, we prove a special version of the normal Noether normalization lemma. The proof is a slight modification of the proof of Theorem 8.19 in [7], and the proof of a somewhat similar statement is left as an exercise.

Theorem 4.1.1. *Let $R_\bullet$ be a graded k-algebra, where k is an infinite field, that is finitely generated in degree one. Now there are n homogeneous elements $x_1, ..., x_n$ of degree one, that are algebraically independent, and $R_\bullet$ is integral over $k[x_1, ..., x_n]$.*

Proof. We prove this by induction on the number n of homogeneous elements of degree one required for generating $R_\bullet$ as an k-algebra. The case $n = 0$ is trivial, so assume $n > 0$. Let $a_1, ..., a_n$ be degree one homogeneous elements that generate $R_\bullet$ over k.

If $a_1, ..., a_n$ are algebraically independent, then we are done. Otherwise, $a_1, ..., a_n$ satisfy an algebraic relation, i.e., $f(a_1, ..., a_n) = 0$ for some nonzero multivariate polynomial f. As $R_\bullet$ is a graded ring, the a_i must satisfy an homogeneous algebraic relation, meaning that we may assume that f is homogeneous. By permuting the indices if necessary, we may assume that $f(1, b_2, ..., b_n) \neq 0$ for some choice of b_i.

We claim that $R_\bullet$ is integral over the graded k-algebra $S_\bullet$ generated by $c_i = a_i - b_i a_1$, where $i = 2..n$. To show this, it is enough to show that a_1 is integral over $S_\bullet$, as the elements of $R_\bullet$ that are integral over $S_\bullet$ form a subalgebra. Set

$$g(x) = f(x, c_2 + b_2 x, ..., c_n + b_n x).$$

By definition $g(a_1) = 0$. Moreover, if d is the degree of f, then the leading term of g is $f(1, b_2, ..., b_n)x^d$, which shows that a_1 is a root of a monic polynomial with coefficients in $S_\bullet$. Thus $R_\bullet$ is integral over $S_\bullet$, which can be generated by $n-1$ elements over k. By the transitivity of integrality, the claim follows by induction. □

4.2 Primes associated to a graded module

For the rest of this section, we assume that $R_\bullet$ is a Noetherian graded ring and $M_\bullet$ is a finitely generated graded $R_\bullet$-module. We say that a prime ideal $p \subset A_\bullet$ is *associated* to $M_\bullet$ if there is a homogeneous element m of M whose annihilator p is. It is clear that such an ideal p must be homogeneous. Moreover, by utilizing the nongraded case, we see that the set $\mathrm{Ass}M_\bullet$ consisting of homogeneous primes associated to $M_\bullet$ is finite. The proof of the following proposition is essentially the same as in the nongraded case:

Proposition 4.2.1. *A homogeneous ideal maximal in the collection of annihilators of nonzero homogeneous elements of $M_\bullet$ is prime.*

From this, two properties immediately follow. Firstly, if $M_\bullet \neq 0$, then $\mathrm{Ass}M_\bullet$ is nonempty. Secondly, the set of elements of $A_\bullet$ which are zerodivisors of homogeneous elements of $M_\bullet$, is exactly the union $\bigcup \mathrm{Ass}M_\bullet$. We will also need an analogue of prime avoidance in the graded case.

Proposition 4.2.2. *Let $p_1, ..., p_r$ be homogeneous prime ideals of $A_\bullet$ and $I \subset A_\bullet$ any homogeneous ideal not containing degree zero homogeneous elements. If I is not contained in any of the p_i, then there is a homogeneous element of I not in any of the p_i.*

Proof. Only the other direction is unclear. If $r = 1$ then this is clear. Assume $r > 1$, and that the smaller cases have already been taken care of. By induction, we can find homogeneous elements $a_i \in I \backslash (p_1 \cup ... \cup \hat{p}_i \cup ... \cup p_r)$, and by taking powers we may assume that these are of the same degree. If there is some a_i that is not an element of p_i, we are done. Otherwise, let

$$b = \sum_{i=1..r} a_1 \cdots \hat{a}_i \cdots a_r.$$

By definition b is homogeneous. It is also clearly not in any p_i, so we are done. □

Let $R_\bullet$ be a finitely generated graded k-algebra generated in degree one. Recall, that the *irrelevant ideal* R_+ of $R_\bullet$ is the homogeneous ideal generated by the homogeneous elements of $R_\bullet$ of positive degree. Every proper homogeneous ideal of $R_\bullet$ is contained in the irrelevant ideal, a property strikingly similar to locality of a ring. If M is a finitely generated module over a local ring A, we know that there exists a nonzerodivisor of M if an only if the maximal ideal m_A is not associated to M. Analogously, in this situation we have:

Proposition 4.2.3. *Let $R_\bullet$ be as above. Now there is a homogeneous nonzerodivisor of $M_\bullet$ in R_+ if and only if R_+ is not associated to $M_\bullet$.*

Proof. Let $p_1, ..., p_r$ be the homogeneous primes associated to $M_\bullet$. A homogeneous $r \in R_\bullet$ is not a zerodivisor of $M_\bullet$ if and only if it is not in any of the associated primes p_i. By homogeneous prime avoidance, such an r must exist if none of the p_i contain R_+. But p_i contains R_+ exactly when $p_i = R_+$, so we are done. □

If k is assumed to be infinite, we obtain the following stronger result:

Proposition 4.2.4. *Now there is a degree one homogeneous nonzerodivisor of $M_\bullet$ in $R_\bullet$ if and only if R_+ is not associated to $M_\bullet$.*

Proof. Again, only the other direction is unclear. Let $p_1, ..., p_r$ be the primes associated to $M_\bullet$. If every degree one homogeneous element is a zerodivisor, then R_1 is the union of degree one parts of p_i. As k was assumed to be infinite, this means that $R_1 \subset p_i$ for some i. But as $R_\bullet$ is generated in degree one, this means that $p_i = R_+$, so we are done. □

Let $M'_\bullet$ denote the elements of $M_\bullet$ annihilated by some power of R_+. It is clear that $M'_\bullet$ is a graded submodule of $M_\bullet$. As $M_\bullet$ is Noetherian, we know that $M'_\bullet$ is generated by finitely many elements, and hence $M'_i = 0$ for large enough i. Therefore, we obtain the following corollary:

Corollary 4.2.5. *The Hilbert polynomials of $M_\bullet$ and $M_\bullet/M'_\bullet$ coincide.*

It is also clear that taking quotient by $M'_\bullet$ does not affect the sheaf structure of $\mathcal{F}_{M_\bullet}$ on $Proj R_\bullet$. The last property tells us that $M_\bullet/M'_\bullet$ behaves better than $M_\bullet$.

Proposition 4.2.6. *The irrelevant ideal R_+ is not associated to $M_\bullet/M'_\bullet$.*

Proof. This follows from a more general property: no nonzero element of $M_\bullet/M'_\bullet$ is annihilated by a power of R_+. Let $[m] \in M_\bullet/M'_\bullet$ be annihilated by a power of R_+, so $R_+^{n_1} m \subset M'_\bullet$ for some n_1. But as $R_+^{n_2} M'_\bullet = 0$ for large enough n_2, we see that $R_+^{n_1+n_2} m = 0$, i.e., $m \in M'_\bullet$ and thus $[m] = 0$. □

Bibliography

[1] Justin R. Smith: Introduction to Algebraic Geometry, Five Dimensions Press, 2014.

[2] David Cox, John Little, Donal O'Shea: Ideals, Varieties, and Algorithms, Third Edition, Springer, 2007.

[3] William Fulton: Algebraic Curves, Third Edition, 2008.

[4] Jan Hilmar, Chris Smyth: Euclid meets Bezout: Intersecting algebraic plane curves with the Euclidean algorithm, arXiv:0907.0361, 2009.

[5] Ravi Vakil: The Rising Sea - Foundations of Algebraic Geometry, December 30 2014 version

[6] Robin Hartshorne: Algebraic Geometry, 1st edition, Springer, 1977.

[7] Gregor Kemper: A Course in Commutative Algebra, Springer, 2011.

[8] David Eisenbud: Commutative Algebra: with a View Torward Algebraic Geometry, Springer.

[9] Jean-Pierre Serre: Local Algebra, Springer, 2000.

[10] Stacks Project: Intersection Theory, version 967ff45, 2016.

[11] Wolfgang Vogel: Lectures on results on Bézout's theorem, Springer, 1984.

[12] Charles Weibel: An introduction to homological algebra, Cambridge University Press, 1994.