Introductory Geometry

Course No. 100 351

Fall 2005

Second Part: Algebraic Geometry

Michael Stoll

Contents

1. What Is Algebraic Geometry?

Linear Algebra can be seen (in parts at least) as the study of systems of linear equations. In geometric terms, this can be interpreted as the study of linear (or affine) subspaces of $\mathbb{C}^n$ (say).

Algebraic Geometry generalizes this in a natural way be looking at systems of *polynomial* equations. Their geometric realizations (their solution sets in C^n, say) are called *algebraic varieties.*

Many questions one can study in various parts of mathematics lead in a natural way to (systems of) polynomial equations, to which the methods of Algebraic Geometry can be applied.

Algebraic Geometry provides a translation between *algebra* (solutions of equations) and *geometry* (points on algebraic varieties). The methods are mostly algebraic, but the geometry provides the intuition.

Compared to Differential Geometry, in Algebraic Geometry we consider a rather restricted class of "manifolds" — those given by polynomial equations (we can allow "singularities", however). For example, $y = \cos x$ defines a perfectly nice differentiable curve in the plane, but not an algebraic curve.

In return, we can get stronger results, for example a criterion for the existence of solutions (in the complex numbers), or statements on the number of solutions (for example when intersecting two curves), or classification results.

In some cases, there are close links between both worlds. For example, a compact Riemann Surface (i.e., a one-dimensional complex manifold) is "the same" as a (smooth projective) algebraic curve over $\mathbb{C}$.

As we do not have much time in this course, we will mostly look at the simplest nontrivial (but already very interesting case), which is to consider *one* equation in *two* variables. Such an equation describes a *plane algebraic curve.*

1.1. **Examples.** We will use x and y as the variables.

The simplest examples are provided by the equations $y = 0$ and $x = 0$; they describe the x-axis and y-axis, respectively. More generally, a *line* is given by an equation $ax + by = c$ with a and b not both zero.

The equation $x^2 + y^2 = 1$ describes the unit circle. Note that the set of its real points $(x, y) \in \mathbb{R}^2$ is compact, but its set of complex points is not — there are two "branches" extending to infinity, with x/y tending to i and to $-i$ respectively. It turns out that we can compactify the set of complex points by throwing in two additional points "at infinity" corresponding to these two directions.

More formally, we introduce the *projective plane* $\mathbb{P}^2$ as the set of points $(x : y : z)$ with $(x, y, z) \in \mathbb{C}^3 \setminus \{0\}$, where we identify $(x : y : z)$ and $(\lambda x : \lambda y : \lambda z)$ for $\lambda \in \mathbb{C} \setminus \{0\}$. We find the usual *affine plane* $\mathbb{A}^2 = \mathbb{C}^2$ within $\mathbb{P}^2$ as the subset of points $(x : y : 1)$; the points $(x : y : 0)$ form the "line at infinity", and there is one point for each direction in the affine plane. The unit circle acquires the two new points $(1 : i : 0)$ and $(1 : -i : 0)$.

A *projective* plane curve is now given by a *homogeneous* polynomial in the *three* variables x, y, z. To obtain it from the original affine equation, replace x and y by x/z and y/z, respectively and multiply by a suitable power of z to cancel the denominators. For the unit circle we obtain $x^2 + y^2 = z^2$; a general line in $\mathbb{P}^2$ is given by $ax+by+cz = 0$ with a, b, c not all zero. (The line at infinity has equation $z = 0$, for example.)

One of the great advantages of $\mathbb{P}^2$ over $\mathbb{A}^2$ is that in $\mathbb{P}^2$ any pair of distinct lines has exactly one common point — there is no need to separate the case of parallel lines; every pair of lines stands on the same footing.

The fact that two lines always intersect in exactly one point has a far-reaching generalization, known as *Bézout's Theorem.* It says that two projective plane curvers of degrees m and n intersect in exactly mn points (counting multiplicities correctly).

The first question towards a classification of algebraic curves one could ask is to order them in some way according to their complexity. Roughly, one would expect that the curve is more complicated when the degree of its defining polynomial is large. However, this is not true in general, for example, a curve $y = f(x)$ can be transformed to the line $y = 0$ by a simple substitution, no matter how large the degree of f is. But it is certainly true that a curve given by an equation of low degree cannot be very complicated.

It turns out that there is a unique discrete invariant of an algebraic curve: its *genus* g. The genus is a nonnegative integer, and for a plane curve of degree d, we have $g \le (d-1)(d-2)/2$. So lines ($d = 1$) and conic sections ($d = 2$) are of genus zero, whereas a general cubic curve ($d = 3$) will have genus one. Some cubic curves will have genus zero, however; it turns out that these are the curves having a *singular point*, where the curve is not smooth (not a manifold in the Differential Geometry sense). In general, there is a formula relating the degree d of a *projective* plane curve, its genus g and contributions δ_P associated to its singular points P:

$$g = \frac{(d-1)(d-2)}{2} - \sum_P \delta_P \,.$$

1.2. **Example.** [Iteration $z \mapsto z^2 + c$; to be added]

2. Affine Spaces and Algebraic Sets

In the following, we will do everything over the field $\mathbb{C}$ of complex numbers. The reason for this choice is that $\mathbb{C}$ is *algebraically closed*, i.e., it satisfies the "Fundamental Theorem of Algebra":

2.1. **Theorem.** *Let $f \in \mathbb{C}[x]$ be a non-constant polynomial. Then f has a root in $\mathbb{C}$.*

By induction, it follows that every non-constant polynomial $f \in \mathbb{C}[x]$ splits into linear factors:

$$f(x) = c\prod_{j=1}^{n}(x - \alpha_j)$$

where $n = \deg f$ is the degree, $c \in \mathbb{C}^\times$ and the $\alpha_j \in \mathbb{C}$.

Essentially everything we do would work as well over any other algebraically closed field (of characteristic zero).

The first thing we have to do is to provide the stage for our objects. They will be the solution sets of systems of polynomial equations, so we need the space of points that are potential solutions.

2.2. **Definition.** Let $n \geq 0$. *Affine n-space*, $\mathbb{A}^n$, is the set $\mathbb{C}^n$ of all n-tuples of complex numbers. Note that $\mathbb{A}^0$ is just one point (the empty tuple). $\mathbb{A}^1$ is also called the *affine line*, $\mathbb{A}^2$ the *affine plane.*

2.3. **Definition.**

(1) Let $S \subset \mathbb{C}[x_1, \dots, x_n]$ be a subset. The *(affine) algebraic set* defined by S is

$$V(S) = \{(\xi_1, \dots, \xi_n) \in \mathbb{A}^n : f(\xi_1, \dots, \xi_n) = 0 \text{ for all } f \in S\}\,.$$

If $I = \langle S \rangle$ is the ideal generated by S, then $V(S) = V(I)$. Note that $V(\emptyset) = V(0) = \mathbb{A}^n$ and $V(\{1\}) = V(\mathbb{C}[x_1, \dots, x_n]) = \emptyset$.

An non-empty algebraic set is called an *algebraic variety* if it is not the union of two proper algebraic subsets.

(2) Let $V \subset \mathbb{A}^n$ be a subset. The *ideal* of V is the set

$$I(V) = \{f \in \mathbb{C}[x_1, \dots, x_n] : f(\xi_1, \dots, \xi_n) = 0 \text{ for all } (\xi_1, \dots, \xi_n) \in V\}\,.$$

It is clear that $I(V)$ is indeed an ideal of $\mathbb{C}[x_1, \dots, x_n]$.

2.4. **Remark.** Note that the finite union and arbitrary intersection of algebraic sets is again an algebraic set — we have

$$\bigcap_{j \in J} V(S_j) = V\Big(\bigcup_{j \in J} S_j\Big)$$

$$V(S_1) \cup V(S_2) = V(S_1 S_2) \qquad \text{where } S_1 S_2 = \{fg : f \in S_1, g \in S_2\}.$$

Since the full $\mathbb{A}^n$ and the empty set are also algebraic sets, one can define a topology on $\mathbb{A}^n$ in which the algebraic sets are exactly the closed sets. This is called the *Zariski Topology.* Since algebraic sets are closed in the usual topology (the solution set of $f = 0$ is closed as a polynomial f defines a continuous function), this new topology is coarser than the usual toplogy.

2.5. **Remark.** We obviously have

$$S_1 \subset S_2 \Longrightarrow V(S_1) \supset V(S_2) \quad \text{and} \quad V_1 \subset V_2 \Longrightarrow I(V_1) \supset I(V_2)\,.$$

By definition, we have

$$S \subset I(V(S)) \qquad \text{and} \qquad V \subset V(I(V))\,.$$

Together, these imply

$$V(I(V(S))) = V(S) \qquad \text{and} \qquad I(V(I(V))) = I(V)\,.$$

This means that we get an inclusion-reversing bijection between algebraic sets and those ideals that are of the form $I(V)$. *Hilbert's Nullstellensatz* tells us what these ideals are.

Theorem. *Let I be an ideal, $V = V(I)$. If $f \in I(V)$, then $f^n \in I$ for some $n \geq 1$.*

We can deduce that

$$I(V(I)) = \operatorname{rad}(I) = \{f \in \mathbb{C}[x_1, \dots, x_n] : f^n \in I \text{ for some } n \geq 1\}$$

is the *radical* of I. Note that $\mathrm{rad}(I)$ is an ideal (Exercise). Hence $I = I(V(I))$ if and only if I is a *radical ideal*, which means that $I = \mathrm{rad}(I)$; equivalently, $f^n \in I$ for some $n \geq 1$ implies $f \in I$. Note that $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$ (Exercise).

So we see that $I \mapsto V(I)$, $V \mapsto I(V)$ provide an inclusion-reversing bijection between algebraic sets and radical ideals of $\mathbb{C}[x_1, \dots, x_n]$. Restricting this to algebraic varieties, we obtain a bijection between algebraic varieties and *prime ideals* of $\mathbb{C}[x_1, \dots, x_n]$ (i.e., ideals I such that $fg \in I$ implies $f \in I$ or $g \in I$).

Note that $\mathbb{C}[x_1, \dots, x_n]$ is a *noetherian* ring; therefore every ideal is finitely generated. In particular, taking S' to be a finite generating set of the ideal $\langle S \rangle$, we see that $V(S) = V(S')$ — every algebraic set is defined by a *finite* set of equations.

2.6. **Example.** Let us consider the algebraic sets and varieties in the affine line $\mathbb{A}^1$. An algebraic set is given by an ideal of $\mathbb{C}[x]$. Now $\mathbb{C}[x]$ is a principal ideal domain, hence every ideal I is generated by one element: $I = \langle f \rangle$. If $f = 0$, then the algebraic set is all of $\mathbb{A}^1$. So we assume now $f \neq 0$. Then the ideal is radical if and only if f has no multiple roots, and the algebraic set defined by it is just the finite set of points corresponding to the roots of f; these are n points, where n is the degree of f. (This set is empty when $n = 0$, i.e., f is constant.) So the algebraic sets in $\mathbb{A}^1$ are exactly the finite subsets and the whole line. It is then clear that the algebraic varieties in $\mathbb{A}^1$ are the whole line and single points (and indeed, the prime ideals of $\mathbb{C}[x]$ are the zero ideal and the ideals generated by a linear polynomial $x - \alpha$).

2.7. **Example.** Now consider the affine plane $\mathbb{A}^2$. The plane $\mathbb{A}^2$ itself is an algebraic set — $\mathbb{A}^2 = V(\emptyset)$. Any single point of $\mathbb{A}^2$ is an algebraic set (even an algebraic variety) — $\{(\xi, \eta)\} = V(x - \xi, y - \eta)$. Therefore all finite subsets of $\mathbb{A}^2$ are algebraic sets. Is there something in between finite sets and the whole plane? Yes: we can consider something like $V(x)$ or $V(x^2 + y^2 - 1)$. We get an algebraic set that is intuitively "one-dimensional". Here we look at ideals $\langle F \rangle$ generated by a single non-constant polynomial $F \in \mathbb{C}[x, y]$. Such an ideal is radical iff F has no repeated factors in its prime factorization (recall that $\mathbb{C}[x, y]$ is a unique factorization domain), and it is prime iff F is irreducible. We call $V(F)$ an *affine plane algebraic curve;* the curve is called *irreducible* if F is irreducible.

Simple examples of affine plane algebraic curves are the *lines* $V(ax + by - c)$ (with $(a, b) \neq (0, 0)$) or the "unit circle" $V(x^2 + y^2 - 1)$, which is a special case of a *quadric* or *conic section* — a curve $V(F)$, where F has (total) degree 2. Note that the "real picture" in $\mathbb{R}^2$ of the unit circle is misleading: it does not show the two branches tending to infiniy with asymptotes of slope i and $-i$!

One can show that a general proper algebraic subset of $\mathbb{A}^2$ is a finite union of irreducible curves and points.

Finally, we need to introduce two more notions that deal with the functions we want to consider on our algebraic sets. As this is algebra, the only functions we have at our disposal are polynomials and quotients of polynomials. If V is an algebraic set, $I = I(V)$ its radical ideal, then two polynomial functions will agree on V if and only if their difference is in I. This prompts the following definitions.

2.8. **Definition.** Let $V \subset \mathbb{A}^n$ be an algebraic set with ideal $I = I(V)$. The quotient ring $\mathbb{C}[V] := \mathbb{C}[x_1, \dots, x_n]/I$ is called the *affine coordinate ring* of V. If V is an algebraic variety (hence I is prime, hence $\mathbb{C}[V]$ is an integral domain), then the field of fractions $\mathbb{C}(V) := \operatorname{Frac}(\mathbb{C}[V])$ of the affine coordinate ring is called the *function field* of V.

The affine coordinate ring and function field are closely analogous with the ring of holomorphic functions and the field of meromorphic functions on a complex manifold.

2.9. **Definition.** Let $V \subset \mathbb{A}^n$ be an algebraic set. The elements of the coordinate ring $\mathbb{C}[V]$ are called *regular functions* on V. If $f \in \mathbb{C}[V]$ is a regular function and $P \in V$ is a point on V, then $f(P) \in \mathbb{C}$ makes sense: take a representative $F \in \mathbb{C}[x_1, \dots, x_n]$ of f, then $f(P) := F(P)$ is well-defined — if F and G both represent f, then their difference is in the ideal of V, hence vanishes on P.

Let $V \subset \mathbb{A}^n$ be an algebraic variety. The elements of the function field $\mathbb{C}(V)$ are called *rational functions* on V. If $f \in \mathbb{C}(V)$ is a rational function and $P \in V$ is a point on V, then f is *regular* at P if f can be written $f = g/h$ with $g, h \in \mathbb{C}[V]$ such that $h(P) \neq 0$. In this case, we can define $f(P) = g(P)/h(P) \in \mathbb{C}$. The regular functions on V are exactly the rational functions that are regular at all points of V.

3. Projective Spaces and Algebraic Sets

The affine space $\mathbb{A}^n$ has certain shortcomings. For example, its point set $\mathbb{C}^n$ is not compact (in the usual topology), and the same is true for any algebraic set that does not just consist of finitely many points. Or, looking at the affine plane, two lines in $\mathbb{A}^2$ may intersect in one point or not intersect at all. In order to get nicer objects and a nicer theory, we introduce a larger space. The price we have to pay is that the definition is more involved.

3.1. **Definition.** Let $n \geq 0$. *Projective n-space,* $\mathbb{P}^n$, is the quotient $(\mathbb{C}^{n+1} \setminus \{0\})/\sim$ of the set of non-zero points in $\mathbb{C}^{n+1}$ modulo the equivalence relation

$$(\xi_0, \dots, \xi_n) \sim (\eta_0, \dots, \eta_n) \iff \exists \lambda \in \mathbb{C}^\times : \eta_0 = \lambda\xi_0, \dots, \eta_n = \lambda\xi_n \,.$$

We write $(\xi_0 : \ldots : \xi_n)$ for the point represented by a tuple $(\xi_0, \dots, \xi_n)$.

Note that $\mathbb{P}^0$ is again just one point. Again, $\mathbb{P}^1$ is called the *projective line,* and $\mathbb{P}^2$ is called the *projective plane.*

We can find $\mathbb{A}^n$ inside $\mathbb{P}^n$ in a number of ways. Let U_j be the subset of $\mathbb{P}^n$ of points $(\xi_0 : \ldots : \xi_j : \ldots : \xi_n)$ such that $\xi_j \neq 0$. Then there is a bijection between $\mathbb{A}^n$ and U_j given by $\iota_j : (\xi_1, \dots, \xi_n) \mapsto (\xi_1 : \ldots : \xi_{j-1} : 1 : \xi_j : \ldots : \xi_n)$ and $(\xi_0 : \ldots : \xi_n) \mapsto (\frac{\xi_0}{\xi_j}, \dots, \frac{\xi_{j-1}}{\xi_j}, \frac{\xi_{j+1}}{\xi_j}, \dots, \frac{\xi_n}{\xi_j})$.

The complement of U_j is in a natural way a $\mathbb{P}^{n-1}$ (dropping the zero coordinate ξ_j), so we can write $\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$. In particular, the projective line $\mathbb{P}^1$ is $\mathbb{A}^1$ with one point "at infinity" added, and the projective plane $\mathbb{P}^2$ is $\mathbb{A}^2$ with a (projective) line "at infinity" added.

If we identify $t \in \mathbb{A}^1$ with the point $(t : 1) \in \mathbb{P}^1$, so that $(t : u) \in \mathbb{P}^1$ corresponds to $\frac{t}{u}$ (when $u \neq 0$), then approaching the "point at infinity" corresponds to letting the denominator tend to zero, keeping the numerator fixed (at 1, say). If we look at another "chart", that given by the coordinate $\frac{u}{t}$, then in this chart, we approach zero. In this way, we can consider the projective line as being "glued together" from two affine lines with coordinates t and u, identified on the complements of the origins according to $tu = 1$. In terms of complex points, this is exactly the construction of the *Riemann Sphere* $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$.

This shows that $\mathbb{P}^1$ is compact (in its complex topology). More generally, $\mathbb{P}^n$ is compact (with the quotient topology induced by the quotient map $\mathbb{C}^{n+1}\backslash\{0\} \to \mathbb{P}^n$, or equivalently, with the topology coming from the affine "charts" U_j).

3.2. **Definition.** A polynomial in $\mathbb{C}[x_0, \ldots, x_n]$ is called *homogeneous* (of degree d) if all its non-vanishing terms have the same total degree d. We will write

$$\mathbb{C}[x_0, \ldots, x_n]_d = \Big\{ \sum_{k_0+\cdots+k_n=d} a_{k_0,\ldots,k_n} x_0^{k_0} \cdots x_n^{k_n} : a_{k_0,\ldots,k_n} \in \mathbb{C} \Big\}$$

for the ($\mathbb{C}$-vector) space of homogeneous polynomials of degree d. (The zero polynomial is considered to be homogeneous of any degree d.)

Note that

$$\mathbb{C}[x_0, \ldots, x_n] = \bigoplus_{g \geq 0} \mathbb{C}[x_0, \ldots, x_n]_d$$

as $\mathbb{C}$-vector spaces: every polynomial is a (finite) sum of homogeneous ones; we write

$$f = f_0 + f_1 + \cdots + f_n$$

if f has (total) degree $\leq n$, where f_d is homogeneous of degree d. Regarding the multiplicative structure, we have that the product of two homogeneous polynomials of degrees d and d', respectively, is homogeneous of degree $d + d'$. (In algebraic terms, $\mathbb{C}[x_0, \ldots, x_n]$ is a *graded ring.* A graded ring is a ring R whose additive group is a direct sum $R = \bigoplus_{d \geq 0} R_d$ such that $R_d \cdot R_{d'} \subset R_{d+d'}$ for all $d, d' \geq 0$.)

3.3. **Definition.**

(1) Let $S \subset \mathbb{C}[x_0, \ldots, x_n]$ be a set of *homogeneous* polynomials. The *projective algebraic set* defined by S is

$$V(S) = \{(\xi_0 : \ldots : \xi_n) \in \mathbb{P}^n : F(\xi_0, \ldots, \xi_n) = 0 \text{ for all } F \in S\}.$$

$V(S) \neq \emptyset$ is a *projective algebraic variety* if it is not the union of two proper projective algebraic subsets.

(2) Let $V \subset \mathbb{P}^n$ be a subset. The *(homogeneous) ideal* of V is

$$I(V) = \bigoplus_{d \geq 0} \{F \in \mathbb{C}[x_0, \ldots, x_n]_d : F(\xi_0, \ldots, \xi_n) = 0 \text{ for all } (\xi_0 : \ldots : \xi_n) \in V\}.$$

3.4. **Remarks.** If F is homogeneous, then for $(\xi_0 : \ldots : \xi_n) \in \mathbb{P}^n$ it makes sense to ask whether $F(\xi_0, \ldots, \xi_n) = 0$, as this does not depend on the representative — $F(\lambda\xi_0, \ldots, \lambda\xi_n) = \lambda^d F(\xi_0, \ldots, \xi_n)$ if F is homogeneous of degree d.

An ideal is called *homogeneous*, if it is generated by homogeneous polynomials. $I(V)$ is the homogeneous ideal generated by all the homogeneous polynomials vanishing on all points of V.

We get again an inclusion-reversing bijection between projective algebraic sets and homogeneous radical ideals contained in the *irrelevant ideal* $I_0 = \langle x_0, \ldots, x_n \rangle$ (note that $V(I_0) = V(\{1\}) = \emptyset$), and between projective algebraic varieties and homogeneous prime ideals $\subsetneq I_0$.

Note that a projective algebraic set is compact (in the usual topology), since it is a closed subset of the compact set $\mathbb{P}^n$. In fact, a famous theorem due to Chow states:

Every connected compact complex manifold is complex-analytically isomorphic to a projective algebraic variety.

Even more is true: via this isomorphism, the field of meromorphic functions is identified with the function field of the algebraic variety (see below).

3.5. **Example.** Consider the (projective) algebraic subsets of $\mathbb{P}^1$. Any nonzero homogeneous polynomial $F(x, y)$ in two variables is a product of linear factors $\beta x - \alpha y$ (with α and β not both zero). Such a linear polynomial has the single point $(\alpha : \beta)$ as its algebraic set. The algebraic set defined by a general (squarefree) homogeneous polynomial is therefore again a finite set of points, and the same is true for a homogeneous ideal, since its algebraic set is the intersection of the algebraic sets of its generators. (In fact, the homogeneous ideals of $\mathbb{C}[x, y]$ are all generated by one element.)

3.6. **Example.** In the projective plane $\mathbb{P}^2$, we again have finite sets of points as algebraic sets (which are varieties when they consist of just one point). The whole plane $\mathbb{P}^2$ is a projective algebraic variety. As before, there are also "one-dimensional" algebraic sets and varieties; they are again defined by single equations, which are now given by (non-constant) homogeneous polynomials $F(x, y, z)$ in three variables. They are (surprisingly) called *projective plane algebraic curves.*

As before, we can define coordinate rings and function fields.

3.7. **Definition.** Let $V \subset \mathbb{P}^n$ be an algebraic set with homogeneous ideal $I = I(V)$. The quotient ring $\mathbb{C}[V] := \mathbb{C}[x_0, x_1, \ldots, x_n]/I$ is called the *homogeneous coordinate ring* of V.

If V is a projective algebraic variety, then the *function field* of V is defined as

$$\mathbb{C}(V) := \left\{ \frac{f}{g} : f, g \in \mathbb{C}[V], g \neq 0, \begin{array}{c} f \text{ and } g \text{ both have representatives} \\ \text{in } \mathbb{C}[x_0, \ldots, x_n]_d \text{ for some } d \geq 0 \end{array} \right\}.$$

It is something like the "degree zero part" of the field of fractions of $\mathbb{C}[V]$.

3.8. **Definition.** Let $V \subset \mathbb{P}^n$ be a projective algebraic variety. The elements of the function field $\mathbb{C}(V)$ are called *rational functions* on V. If $f \in \mathbb{C}(V)$ is a rational function and $P \in V$ is a point on V, then f is *regular* at P if f can be written $f = g/h$ with $g, h \in \mathbb{C}[V]$ such that $h(P) \neq 0$. In this case, we can define $f(P) = g(P)/h(P) \in \mathbb{C}$. Note that this is well-defined, since g and h are represented by homogeneous polynomials of the same degree d:

$$f\big((\lambda\xi_0 : \ldots : \lambda\xi_n)\big) = \frac{g(\lambda\xi_0, \ldots, \lambda\xi_n)}{h(\lambda\xi_0, \ldots, \lambda\xi_n)} = \frac{\lambda^d\, g(\xi_0, \ldots, \xi_n)}{\lambda^d\, h(\xi_0, \ldots, \xi_n)} = f\big((\xi_0 : \ldots : \xi_n)\big)$$

3.9. **Example.** The concept of a rational function on a projective algebraic variety is at first sight a bit involved. An example will help to clarify it. Consider the projective version of the unit circle, given by the equation $x^2 + y^2 - z^2 = 0$. Then $f = (y-z)/x$ defines a rational function (since numerator $y-z$ and denominator x have the same degree, and the denominator is not in the homogeneous ideal of the curve). Let us find out at which points of the curve f is regular. This is certainly the case for all points with $x \neq 0$. Let us look at the points where x vanishes. These are $(0 : 1 : 1)$ and $(0 : 1 : -1)$ (recall that projective coordinates are only determined up to scaling). At $(0 : 1 : -1)$, the numerator does not vanish, which implies that f is not regular (Exercise!). At $(0 : 1 : 1)$, the numerator and the denominator both vanish, so we have to find an alternative representation. Note that we have (in the function field)

$$\frac{y-z}{x} = \frac{(y-z)(y+z)}{x(y+z)} = \frac{y^2-z^2}{x(y+z)} = \frac{-x^2}{x(y+z)} = -\frac{x}{y+z}\,.$$

In this last representation, the denominator does not vanish at $(0 : 1 : 1)$, so f is regular there (and in fact takes the value zero).

There is an important result (which has some analogy to Liouville's Theorem in complex analysis, which can be formulated to say that any holomorphic function on a compact Riemann Surface is constant).

3.10. **Theorem.** *If $V \subset \mathbb{P}^n$ is a projective algebraic variety and $f \in \mathbb{C}(V)$ is regular everywhere on V, then f is constant.*

4. Projective Closure and Affine Patches

We now are faced with an obvious question: how do we go between affine and projective algebraic sets or varieties? There should be some correspondence related to the idea that going from affine to projective means to add some points in order to "close up" the algebraic set.

4.1. **Definition.** For a polynomial $f \in \mathbb{C}[x_1, \dots, x_n]$ of (total) degree d, we define

$$\tilde{f} = x_0^d f\Big(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\Big) \in \mathbb{C}[x_0, x_1, \dots, x_n]_d\,.$$

This operation corresponds to multiplying every term in f with a suitable power of x_0 in order to make the total degree equal to d. This process is sometimes called *homogenization.*

4.2. **Definition.** Let $V \subset \mathbb{A}^n$ be an affine algebraic set, with ideal $I = I(V) \subset \mathbb{C}[x_1, \dots, x_n]$. The *projective closure* $\tilde{V}$ of V (with respect to the embedding $\iota_0 : \mathbb{A}^n \to \mathbb{P}^n$) is the projective algebraic set given by the equations $\tilde{f} = 0$ for $f \in I$.

It can be shown that $\tilde{V}$ really is the topological closure (in both the usual and the Zariski topologies on $\mathbb{P}^n$) in $\mathbb{P}^n$ of $V \subset \mathbb{A}^n \subset \mathbb{P}^n$, thus justifying the name.

4.3. **Definition.** Let $V \subset \mathbb{P}^n$ be a projective algebraic set, given by equations $f = 0$ for $f \in S \subset \bigcup_d \mathbb{C}[x_0, x_1, \dots, x_n]_d$. Let $0 \le j \le n$. The *jth affine patch* of V is the affine algebraic set V_j given by the equations $f(x_0, \dots, x_{j-1}, 1, x_{j+1}, \dots, x_n) = 0$ for $f \in S$. (Here, we use $\mathbb{C}[x_0, \dots, x_{j-1}, x_{j+1}, \dots, x_n]$ as the coordinate ring of $\mathbb{A}^n$.)

The following is quite immediate.

4.4. **Proposition.** *If $V \subset \mathbb{A}^n$ is an affine algebraic set, then $(\tilde{V})_0 = V$.*

Proof. Exercise. □

The converse needs more care.

4.5. **Proposition.** *Let $V \subset \mathbb{P}^n$ be a projective algebraic variety such that V is not contained in the "hyperplane at infinity", i.e., the complement $\mathbb{P}^n \setminus U_0$. Then $\widetilde{(V_0)} = V$.*

Proof. Exercise. □

Note that $V_0 = \emptyset$ when V is contained in the hyperplane at infinity.

4.6. **Examples.** If we consider a line L in $\mathbb{A}^2$, given by the equation $ax + by = c$, say (with $(a, b) \neq (0, 0)$), then $\tilde{L}$ is given by $ax + by - cz = 0$ (writing z for the additional coordinate on $\mathbb{P}^2$). There is exactly one "point at infinity" in $\tilde{L} \setminus L$; it has coordinates $(b : -a : 0)$. This is the point common to all lines parallel to L.

Conversely, if we have a (projective) line $\Lambda \subset \mathbb{P}^2$, given by $ax + by + cz = 0$ (with $(a, b, c) \neq (0, 0, 0)$), then $\Lambda_0 \subset \mathbb{A}^2$ is given by $ax + by = -c$. If $(a, b) \neq (0, 0)$, this is an affine line, otherwise it is the empty set (since then $c \neq 0$).

Now consider the "unit circle" $C : x^2 + y^2 = 1$ in the affine plane. Its projective closure is $\tilde{C} : x^2 + y^2 - z^2 = 0$. The zeroth affine patch of this is of course again C. The first affine patch of $\tilde{C}$ is (set $x = 1$) $\tilde{C}_1 : z^2 = 1 + y^2$. So in this sense, the circle is "the same" as a hyperbola.

In the projective closure, the unit circle acquires the two new points "at infinity" with coordinates $(1 : i : 0)$ and $(1 : -i : 0)$ — they come from the factorization of the leading term $x^2 + y^2$ into a product of linear forms.

More generally, if we have any circle C in the affine plane, given by $(x - a)^2 + (y - b)^2 = r^2$, then $\tilde{C}$ still has the two points $(1 : i : 0)$ and $(1 : -i : 0)$: they are common to all circles!

This explains, by the way, why two circles intersect at most in two points (in $\mathbb{A}^2$), even though one would generically expect four points of intersection (since we are intersecting two curves of degree 2) — two of the intersection points are out at infinity (and not defined over $\mathbb{R}$ in addition to that).

4.7. **Proposition.** *Let $V \subset \mathbb{A}^n$ be an affine algebraic variety, $\tilde{V}$ its projective closure. Then the function fields $\mathbb{C}(V)$ and $\mathbb{C}(\tilde{V})$ are canonically isomorphic, and the affine coordinate ring $\mathbb{C}[V]$ can be identified with the set of rational functions on $\tilde{V}$ (or on V) that are regular everywhere on V.*

Proof. The proof of the first statement is an exercise. The second statement follows from the fact that $\mathbb{C}[V]$ is the subset of $\mathbb{C}(V)$ consisting of functions that are regular on all of V. □

5. Morphisms and Rational Maps

So far we have defined what our objects are (affine or porjective algebraic sets or varieties), and we have defined functions on them. But we also want to relate these objects with each other; in particular, we want to say when two such objects should be considered "the same". So we need to define a suitable class of maps between the objects.

In the affine case, this is quite straight-forward.

5.1. **Definition.** Let $V \subset \mathbb{A}^n$ and $W \subset \mathbb{A}^m$ be two affine algebraic sets. A *morphism* $V \to W$ is a map $\phi : V \to W$ that is given by polynomials: if $\mathbb{C}[x_1, \dots, x_n]$ is the coordinate ring of $\mathbb{A}^n$ and $\mathbb{C}[y_1, \dots, y_m]$ is the coordinate ring of $\mathbb{A}^m$, then there are polynomials $F_1, \dots, F_m \in \mathbb{C}[x_1, \dots, x_n]$ such that

$$\phi(\xi_1, \dots, \xi_n) = (F_1(\xi_1, \dots, \xi_n), \dots, F_m(\xi_1, \dots, \xi_n)) .$$

In order to make sure that the image is contained in W, it is necessary and sufficient that for every $G \in I(W)$, we have $G(F_1, \dots, F_m) \in I(V)$.

Note that the F_j are only determined modulo $I(V)$; therefore they can also be considered as elements of the coordinate ring $\mathbb{C}[V]$. The condition above then amounts to saying that ϕ corresponds to a ring homomorphism $\phi^* : \mathbb{C}[W] \to \mathbb{C}[V]$ that sends G to $G(F_1, \dots, F_m)$. (It is really a $\mathbb{C}$-algebra homomorphism, as it has to preserve the constants from $\mathbb{C}$.) Conversely, every such ring homomorphism leads to a morphism $V \to W$: the polynomials F_j are obtained (modulo $I(V)$) as the images of $y_1, \dots, y_m$.

As usual, a morphism is called an *isomorphism* if there is an inverse morphism; in this case V and W are called *isomorphic*, $V \cong W$. Note that it is not sufficient to require ϕ to be a bijective map between the points of V and W. This is analogous to the situation in topology, where a bijective continuous map is not necessarily a homeomorphism.

Note also that $V \cong W$ if and only if $\mathbb{C}[V] \cong \mathbb{C}[W]$ as $\mathbb{C}$-algebras.

It is clear how to compose morphisms; the composition of two morphisms is again a morphism.

5.2. **Example.** Let us show that what we consider a line in $\mathbb{A}^2$ really is isomorphic to the affine line $\mathbb{A}^1$. Let the line L be given by $y = ax + b$ (this excludes the case $x = c$, which can be dealt with in a similar way). Let $\mathbb{C}[t]$ be the coordinate ring of $\mathbb{A}^1$. We set up two morphims:

$$\phi : \mathbb{A}^1 \longrightarrow L\,, \quad t \longmapsto (t, at + b)\,; \qquad \psi : L \to \mathbb{A}^1\,, \quad (x, y) \longmapsto x$$

Both maps are given by polynomials, as required, and the image of the first is contained in L — it satisfies the equation. (There is nothing to check in this respect for the second map, as there is no equation to be satisfied.) It is then obvious that the two morphisms are inverses of each other, hence $L \cong \mathbb{A}^1$. In terms of coordinate rings, we have an isomorphism between $\mathbb{C}[x, y]/\langle y - ax - b\rangle$ and $\mathbb{C}[t]$, which comes essentially down to the fact that we can eliminate y.

5.3. **Example.** Now consider the *cuspidal cubic curve* $C : y^2 = x^3$ in $\mathbb{A}^2$. There is a morphism

$$\phi : \mathbb{A}^1 \longrightarrow C\,, \quad t \longmapsto (t^2, t^3)\,.$$

ϕ is even bijective on points — if $(x, y) \in C$ is not $(0, 0)$, then the unique t that maps to it is y/x, and $(0, 0)$ has the unique preimage 0 — but it is *not* an isomorphism. One way of checking this is to notice that the image of the corresponding $\mathbb{C}$-algebra homomorphism $\phi^* : \mathbb{C}[x, y]/\langle y^2 - x^3\rangle \to \mathbb{C}[t]$ does not contain t. In fact, there is no isomorphism between $\mathbb{A}^1$ and C, and this is a good thing, since the point $(0, 0)$ on C is bad (it is "singular"; we will come to that), but there are no bad points on $\mathbb{A}^1$.

The projective case is a little bit more involved.

5.4. **Definition.** Let $V \subset \mathbb{P}^n$ and $W \subset \mathbb{P}^m$ be two projective algebraic sets. A *morphism* $V \to W$ is a map $\phi : V \to W$ that is "locally given by homogeneous polynomials of the same degree". What this means is that there are $(m + 1)$-tuples $(F_0^{(j)}, \dots, F_m^{(j)})$ of homogeneous polynomials $F_k^{(j)} \in \mathbb{C}[x_0, \dots, x_n]_{d_j}$ of the same degree d_j, for j in some index set J, such that

(1) for all homogeneous $G \in I(W)$ and all $j \in J$, $G(F_0^{(j)}, \dots, F_m^{(j)}) \in I(V)$;
(2) for all $j, j' \in J$, $0 \le k < k' \le m$, we have $F_k^{(j)} F_{k'}^{(j')} - F_{k'}^{(j)} F_k^{(j')} \in I(V)$;
(3) for all $P \in V$, there is some $j \in J$ such that not all of $F_k^{(j)}(P)$ vanish, $0 \le k \le n$, and in this case

$$\phi(P) = (F_0^{(j)}(\xi_0, \dots, \xi_n) : \dots : F_n^{(j)}(\xi_0, \dots, \xi_n))\,,$$

if $P = (\xi_0 : \dots : \xi_n)$.

The first condition ensures that the image is contained in W. The second condition ensures that ϕ is well-defined at points where more than one tuple of polynomials would give a result. The third condition ensures that ϕ is defined everywhere.

We can again compose morphisms between projective algebraic sets (by plugging in; note that we may have to use all possible combinations of defining polynomials for both morphisms); the composition is again a morphism.

5.5. **Example.** In a similar way as for the affine case, one can show that a line $L : ax + by + cz = 0$ in $\mathbb{P}^2$ is isomorphic to the projective line $\mathbb{P}^1$.

Let us do something more interesting here: we show that $\mathbb{P}^1$ is isomorphic to the unit circle $C : x^2 + y^2 - z^2 = 0$. The geometric intuition behind this is the idea that one can "rationally parametrize" the points on the unit circle by fixing one point P on it and considering all the lines through P. The lines are parametrized by their slope, and each line intersects C in a unique second point. In this way, there is a correspondence between slopes and points on C. In formulas, this leads to the morphism

$$\phi : \mathbb{P}^1 \longrightarrow C\,, \quad (t : u) \longmapsto (t^2 - u^2 : 2\,tu : t^2 + u^2)\,.$$

The polynomials on the right hand side are homogeneous of the same degree 2. It is easy to see that the image is contained in C. Also, it suffices to give just this one set of defining polynomials, since they never vanish all three at the same time (recall that t and u do not both vanish for a point in $\mathbb{P}^1$).

What about the inverse? In the affine picture (where $z = 1$), the point P is $(-1, 0)$, and u/t is the slope of the line. So we should have $u/t = y/(x + 1)$. Writing this in homogeneous terms leads to

$$\psi : C \longrightarrow \mathbb{P}^1 , \quad (x : y : z) \longmapsto (x + z : y) .$$

But here we have a problem: at $P = (-1 : 0 : 1)$, both polynomials $x + z$ and y vanish, and the map is not defined. So we need to find an alternative representation that is defined at P. We can proceed as follows.

$$\begin{aligned}(x + z : y) &= ((x + z)(z - x) : y(z - x)) = (z^2 - x^2 : y(z - x)) \\ &= (y^2 : y(z - x)) = (y : z - x)\end{aligned}$$

This version is defined at P (and gives the image $(0 : 1)$), however, it is not defined at $(1 : 0 : 1)$. So we see that we really need two different sets of defining polynomials in this case.

5.6. **Remark.** There are no interesting morphisms from projective to affine algebraic sets. One can consider morphisms from affine to projective algebraic sets, however; they are defined in a similar way as above in the projective case, with the modification that the defining polynomials need not be homogeneous. For example, we can define a morphism from the affine unit circle $C' : x^2 + y^2 = 1$ to the projective line:

$$\psi' : C' \longrightarrow \mathbb{P}^1 , \quad (x, y) \longmapsto (x + 1 : y) \text{ or } (y : 1 - x)$$

In this sense, the canonical inclusion of an affine algebraic set V into its projective closure $\tilde{V}$ is a morphism.

Sometimes one wants to be less demanding and does not require the maps to be defined everywhere, as long as they are defined on a sufficiently large subset. This leads to the notion of rational map.

5.7. **Definition.** Let $V \subset \mathbb{P}^n$ and $W \subset \mathbb{P}^m$ be two projective algebraic varieties. A *rational map* $\phi : V \to W$ is defined in the same way as a morphism, with the exception that we do not require the last condition for *all* points $P \in V$, but just for at least *one* point. If P is a point that satisfies this condition, then we say that ϕ is *defined* at P. It is not hard to see that ϕ is defined on the complement of a proper algebraic subset of V.

Now it is not true that we can always compose rational maps: the image of the first map may be outside the (maximal) domain of definition of the second one. Therefore, we single out a subclass of rational maps that are better behaved in this respect. Consider some affine patch W' of W such that W' meets the image of ϕ. Then we can pull back regular functions on W' to rational functions on V via ϕ: we get a $\mathbb{C}$-algebra homomorphism $\mathbb{C}[W'] \to \mathbb{C}(V)$. We call ϕ *dominant* if this homomorphism is injective. (It can be shown that this does not depend on the affine patch chosen and that it is equivalent to saying that the image of ϕ is dense in the Zariski topology of W.) In this case, the homomorphism extends to a $\mathbb{C}$-algebra homomorphism $\phi^* : \mathbb{C}(W) = \operatorname{Frac}(\mathbb{C}[W']) \to \mathbb{C}(V)$. Explicitly, if ϕ is given by homogeneous polynomials $F_0, \dots, F_m$ of the same degree and $f = g/h$ is a quotient of homogeneous elements of $\mathbb{C}[W]$ of the same degree, then $\phi^*(f) = g(F_0, \dots, F_m)/h(F_0, \dots, F_m)$. Conversely, every such homomorphism $\mathbb{C}(W) \to \mathbb{C}(V)$ comes from a dominant rational map.

We can compose dominant rational maps; the composition is again a dominant rational map. More generally, if $\phi : V \to W$ is a dominant rational map and $\psi : W \to X$ is any rational map, then $\psi \circ \phi$ is defined and a rational map.

The (dominant) rational map ϕ is called *birational* or a *birational isomorphism* if there is an inverse (dominant) rational map. In view of the preceding discussion, this is equivalent to saying that the function fields of V and W are isomorphic (as $\mathbb{C}$-algebras). Intuitively speaking, a birational isomorphism between two algebraic varieties is an isomorphims "modulo proper algebraic subsets."

Since the function fields of an affine algebraic variety V and of its projective closure $\tilde{V}$ can be identified, we can extend the notion of rational maps to affine algebraic varieties.

5.8. **Example.** Let us look at the cuspidal cubic curve again and show that it is birationally isomorphic to the line. This time, we are looking at the projective situation. Then the cuspidal cubic is given by $C : x^3 - y^2 z = 0$ and the line is $\mathbb{P}^1$. We still have the morphism

$$\phi : \mathbb{P}^1 \longrightarrow C\,, \quad (t : u) \longmapsto (t^2 u : t^3 : u^3)\,,$$

but now we claim that it is invertible as a rational map. The inverse is

$$\psi : C \longrightarrow \mathbb{P}^1\,, \quad (x : y : z) \longmapsto (y : x)\,.$$

This is not a morphism, since it is not defined at $(0 : 0 : 1)$, but it is a rational map. It is easy to check that ϕ and ψ are inverses:

$$(t : u) \longmapsto (t^2 u : t^3 : u^3) \longmapsto (t^3 : t^2 u) = (t : u)$$
$$(x : y : z) \longmapsto (y : x) \longmapsto (xy^2 : y^3 : x^3) = (xy^2 : y^3 : y^2 z) = (x : y : z)$$

In terms of function fields, the isomorphism is given by identifying t/u with y/x.

6. Curves — Local Properties

Starting with this section, we will restrict ourselves to the consideration of plane algebraic curves. In this section, we will consider the behavior of a curve near one of its points.

6.1. **Definition.** Let $C : f(x, y) = 0$ be an affine plane algebraic curve, and let $P = (\xi, \eta) \in C$ be a point on C. Let $f_x = \partial f/\partial x$ and $f_y = \partial f/\partial y$ be the two partial derivatives of the polynomial f. We say that P is a *regular point* of C, and that C is *regular* or *smooth* or *nonsingular* at P, if $f_x(\xi, \eta)$ and $f_y(\xi, \eta)$ do not both vanish. In this case, the equation $f_x(\xi, \eta)(x - \xi) + f_y(\xi, \eta)(y - \eta) = 0$ describes a line through the point P; it is called the *tangent line* to C at P. If $f_x(\xi, \eta) = f_y(\xi, \eta) = 0$, we call P a *singular point* or a *singularity* of C, and we say that C is *singular* at P. We call the affine curve C *smooth* if it has no singular points.

Writing

$$f(x + \xi, y + \eta) = f_0(x, y) + f_1(x, y) + \cdots + f_d(x, y)$$

with f_j homogeneous of degree j, we have $f_0 = 0$ (since P is on C) and $f_1 = 0$ if and only if P is a singularity of C. We call the smallest j such that $f_j \neq 0$ the *multiplicity* of P. So a singular point is one with multiplicity at least 2. If the multiplicity is n, we speak of an *n-uple point* of C (e.g., double, triple point). If the point is regular, then $f_1(x - \xi, y - \eta) = 0$ gives the tangent line.

Intuitively, the local behavior of C near P is determined by the lowest order non-vanishing term f_n (where n is the multiplicity of P). If $n = 1$, then this lowest order term is linear, and the curve looks "like a line" near P; in particular, there is a well-defined tangent line. If $n > 1$, then we can factor f_n as a product of n linear forms, which correspond to the tangent directions of the various "branches" of the curve at P; these directions may occur with multiplicities. If f_n is a product of n pairwise non-proportional linear forms (so that there are n distinct tangent directions), we call the singularity *ordinary.* So an *ordinary double point* (also called a *node*) is a point of multiplicity 2 with two distinct tangent directions.

6.2. **Definition.** Let $C : F(x, y, z) = 0$ be a projective plane algebraic curve, $P \in C$ a point on C. Let C_i be an affine patch of C that contains P. Then we define the notions of regular/singular point etc. for $P \in C$ by those for $P \in C_i$. It is easy to check that this does not depend on the choice of affine patch when several are possible (Exercise). We say that C is *smooth* if it has no singular points.

It can be shown that $P \in C$ is singular if and only if $F_x(P) = F_y(P) = F_z(P) = 0$ (Exercise). Furthermore, if $P = (\xi : \eta : \zeta)$ is smooth on C, then the tangent line to C at P has equation

$$F_x(\xi, \eta, \zeta)x + F_y(\xi, \eta, \zeta)y + F_z(\xi, \eta, \zeta)z = 0$$

(Exercise).

6.3. **Example.** An affine line $ax + by = c$ $((a, b) \neq (0, 0))$ is smooth: the partial derivatives are a and b, and at least one of them is nonzero. Similarly, a projective line $ax + by + cz = 0$ $((a, b, c) \neq (0, 0, 0))$ is smooth.

6.4. **Example.** The affine and projective unit circles are smooth. Consider the affine circle $x^2 + y^2 - 1 = 0$. The partial derivatives are $2x$ and $2y$, so they vanish together only at the origin, but the origin is not on the curve. The same kind of argument works for the other affine patches of the projective unit circle.

6.5. **Example.** The reducible affine curve $xy = 0$ has an ordinary double point at the origin. Indeed, both partial derivatives y and x vanish there, and the first nonvanishing term in the local expansion is xy of degree 2, which factors into the two non-proportional linear forms x and y.

6.6. **Example.** Let us consider the *nodal cubic curve* $N : y^2 = x^2(x+1)$. Writing $f(x, y) = y^2 - x^3 - x^2$, the partial derivatives are $f_x = -3x^2 - 2x$ and $f_y = 2y$. If they both vanish, we must have $y = 0$ and then $x^2(x + 1) = x(3x + 2) = 0$, which implies $x = 0$. So the origin is singular. There we have $f_2 = y^2-x^2 = (y-x)(y+x)$ (and $f_3 = -x^3$), so we have an ordinary double point, with tangent directions of slopes 1 and -1.

6.7. **Example.** Now look at the *cuspidal cubic curve* $C : y^2 = x^3$. The partial derivatives are $-3x^2$ and $2y$, so the origin is again the only singularity. This time, $f_2 = y^2$ is a square, so there is only one tangent direction (in this case, along the x-axis). Such a singularity (where f_2 is a nonzero square and f_2 and f_3 have no common divisors) is called a *cusp.*

6.8. **Example.** Consider the affine curve $C : y = x^3$. It is smooth, since the y-derivative is constant 1. However, if we look at the projective closure $yz^2 - x^3 = 0$, we find that there is a singularity at $(0 : 1 : 0)$. Therefore it is not true that the projective closure of a smooth affine plane curve is again smooth.

Our next topic is the local behavior of rational functions on a curve.

6.9. **Definition.** Let C be an irreducible affine plane curve, $P \in C$ a smooth point, and consider a regular function $0 \neq \phi \in \mathbb{C}[C]$. We want to define the order of vanishing of ϕ at P. For this, let the equation of the curve be $f(x, y) = 0$ and assume (we can make a translation if necessary) that $P = (0, 0)$. Then

$$f(x, y) = ax + by + f_2(x, y) + \cdots + f_d(x, y)$$

with $(a, b) \neq (0, 0)$. Assume that $b \neq 0$ (otherwise interchange x and y). We define the *order of vanishing* or just *order* of ϕ at P to be

$$v_P(\phi) = \max\left\{ j : \frac{\phi}{x^j} \text{ is regular at } P \right\}.$$

Here ϕ/x^j is considered as a rational function on C. We set $v_P(0) = +\infty$.

The idea here is that in the situation described, $x = 0$ defines a line that meets the curve transversally at P (i.e., not in the tangent direction) and therefore x has a simple zero at P. So we should have $v_P(x) = 1$. Also, if ϕ is regular and non-zero at P, we want to have $v_P(\phi) = 0$. That the definition makes sense follows from the following result.

6.10. **Lemma.** *Consider the situation described in the definition above.*

(1) *If ϕ is regular at P and vanishes there, then $v_P(\phi) > 0$.*

(2) *Let $n = v_P(\phi)$. Then ϕ/x^n is regular at P and has a non-zero value there. This property determines n uniquely.*

(3) $v_P(\phi_1\phi_2) = v_P(\phi_1) + v_P(\phi_2)$.

(4) $v_P(\phi_1 + \phi_2) \geq \min\{v_P(\phi_1), v_P(\phi_2)\}$, *with equality if* $v_P(\phi_1) \neq v_P(\phi_2)$.

Proof.
(1) We have to show that ϕ/x is regular at P. By assumption, ϕ is represented by a polynomial without constant term. It is therefore sufficient to show that y/x is regular at P, since ϕ/x is represented by a polynomial (regular at P) plus a polynomial times y/x. Now we can write

$$f(x, y) = x(a + F(x, y)) + y(b + G(x, y))$$

where $F(0, 0) = G(0, 0) = 0$. Then

$$y(b + G(x, y)) \equiv -x(a + F(x, y)) \bmod f\,,$$

hence $y/x = -(a + F(x, y))/(b + G(x, y))$ in $\mathbb{C}(C)$, where the denominator does not vanish at $P = (0, 0)$ (and y/x takes the value $-a/b$).

(2) ϕ/x^n is regular at P by definition. If ϕ/x^n vanishes at P, then by part (1), ϕ/x^{n+1} is also regular, contradicting the definition of n. [The proof of part (1) also works for rational functions.] So $(\phi/x^n)(P) \neq 0$. It is clear that there can be at most one n such that ϕ/x^n is regular and non-vanishing at P.

(3) Let $n_1 = v_P(\phi_1)$ and $n_2 = v_P(\phi_2)$, then $\phi_1\phi_2/x^{n_1+n_2}$ is regular and non-vanishing at P, hence $v_P(\phi_1\phi_2) = n_1 + n_2$.

(4) Keep the notations from (3) and let $n = \min\{n_1, n_2\}$. Then $(\phi_1 + \phi_2)/x^n$ is regular at P, so $v_P(\phi_1 + \phi_2) \geq n$. If $n_1 < n_2$ (say), then ϕ_1/x^n is non-zero at P, whereas ϕ_2/x^n vanishes, so $(\phi_1 + \phi_2)/x^n$ is non-zero at P, and we have $v_P(\phi_1 + \phi_2) = n$. □

6.11. **Definition.** If C is an irreducible affine curve, $P \in C$ is a smooth point, and $\phi \in \mathbb{C}(C)$ is a rational function represented by the quotient f/g of regular functions, then we define the *order* of ϕ at P to be $v_P(\phi) = v_P(f) - v_P(g)$.

If C is an irreducible projective curve, $P \in C$ is a smooth point, and $\phi \in \mathbb{C}(C)$ is a rational function, then we define the *order* of ϕ at P to be the order of ϕ at P for any affine patch of C containing P.

It can be checked that the definitions do not depend on the choices made (of numerator and denominator or affine patch).

6.12. **Definition.** If $P \in C$ is a smooth point on an irreducible curve, then any rational function $t \in \mathbb{C}(C)$ such that $v_P(t) = 1$ is called a *uniformizing parameter* or *uniformizer* at P.

We then have again for all $0 \neq \phi \in \mathbb{C}(C)$ that

$$v_P(\phi) = n \iff \frac{\phi}{t^n} \text{ is regular and non-vanishing at } P.$$

6.13. **Lemma.** *Let C be an irreducible curve, $P \in C$ a smooth point and $\phi \in \mathbb{C}(C)$ a rational function. Then ϕ is regular at P if and only if $v_P(\phi) \geq 0$.*

Proof. We work in an affine patch containing P. Write $\phi = f/g$ as a quotient of regular functions, and let $m = v_P(f)$, $n = v_P(g)$. Let t be a uniformizer at P. Then $f = t^m f_0$ and $g = t^n g_0$ with f_0 and g_0 regular and non-vanishing at P. Hence $\phi = t^{m-n} f_0/g_0$, where f_0/g_0 is regular and non-vanishing at P. If $m - n = v_P(\phi) \geq 0$, then t^{m-n} and therefore ϕ is regular at P. If $m - n < 0$, then $\phi = f_0/(t^{n-m} g_0)$ is a quotient of regular functions such that the denominator vanishes at P, but the numerator does not, hence ϕ is not regular at P. □

6.14. **Example.** Let us see what these notions mean for the line (which, to satisfy the assumptions of the definitions, we can consider as being embedded in the plane, for example as a coordinate axis). Let t be the coordinate on $\mathbb{A}^1$, then a rational function is a quotient of polynomials $\phi = f(t)/g(t)$, which we can assume is in lowest terms. At a point $P = \tau$, a uniformizer is given by $t - \tau$, and we see that

$$v_P(f) = \max\{n : (t - \tau)^n \text{ divides } f\}$$

is the multiplicity of the zero τ of f. In particular,

$$\sum_{P \in \mathbb{A}^1} v_P(f) = \deg f \quad \text{and} \quad \sum_{P \in \mathbb{A}^1} v_P(\phi) = \deg f - \deg g\,.$$

Now let us consider $\mathbb{A}^1 \subset \mathbb{P}^1$ and find the order of ϕ at ∞. There, $1/t$ is a uniformizer, and a quotient $f(t)/g(t)$ is regular if and only if $\deg g \geq \deg f$. These facts together imply that $v_\infty(\phi) = \deg g - \deg f$ and therefore

$$\sum_{P \in \mathbb{P}^1} v_P(\phi) = 0\,.$$

This is a very important result: *a rational function has as many zeros as it has poles (counted with multiplicity).*

6.15. **Example.** Consider again the (affine) unit circle $C : x^2 + y^2 = 1$. At the point $P = (0, 1) \in C$, x is a uniformizer (since the tangent direction is horizontal, $x = 0$ intersects C transversally at P). So $v_P(x) = 1$. On the other hand, $2 = v_P(x^2) = v_P(y - 1) + v_P(y + 1) = v_P(y - 1)$. This shows again that $(y - 1)/x$ is regular at P and vanishes there.

6.16. **Remark.** Let V be an algebraic variety (affine or projective) and let $W \subset \mathbb{P}^m$ be a projective algebraic variety. Then every collection of rational functions $F_0, \dots, F_m \in \mathbb{C}(V)$, not all the zero function, determines a rational map $V \to W$ by evaluating $(F_0 : \ldots : F_m)$ (at points where $F_0, \dots, F_m$ all are regular and at least one of them does not vanish).

Conversely, every rational map can be written in this way (there is nothing to do when V is affine; in the projective case, the map is given by homogeneous polynomials of the same degree d, and we can just divide every polynomial by a fixed homogeneous polynomial of degree d that does not vanish on all of V.)

6.17. **Proposition.** *Let C be an irreducible plane algebraic curve and $\phi : C \to \mathbb{P}^m$ a rational map. Let $P \in C$ be a smooth point. Then ϕ is (or can be) defined at P.*

Proof. By the remark above, we can write $\phi = (F_0 : \ldots : F_m)$ with rational functions $F_0, \dots, F_m \in \mathbb{C}(C)$. Let t be a uniformizer at P, and let $n = \min\{v_P(F_j) : j = 0, \dots, m\}$. Then $\phi = (t^{-n}F_0 : \ldots : t^{-n}F_m)$ as well, and for all j, $v_P(t^{-n}F_j) = v_P(F_j) - n \geq 0$, with equality for at least one $j = j_0$. Hence $t^{-n}F_j$ is regular at P for all j, and $(t^{-n}F_{j_0})(P) \neq 0$. Therefore, we get a well-defined point $\phi(P) \in \mathbb{P}^m$. □

6.18. **Corollary.** *Let C be an irreducible smooth plane curve. Then every rational map $C \to \mathbb{P}^m$ is already a morphism.*

Proof. By the proposition, ϕ is defined on all of C. □

6.19. **Corollary.** *Let C be an irreducible smooth projective plane curve. Then there is a natural bijection between non-constant rational functions on C and dominant morphisms $C \to \mathbb{P}^1$.*

Proof. The map is given by associating to a rational function $\phi \in \mathbb{C}(C)$ the rational map $(\phi : 1)$. By the previous corollary, this rational map is already a morphism; it is dominant if ϕ is non-constant. Conversely, a dominant morphism gives rise to an injective $\mathbb{C}$-algebra homomorphism $\mathbb{C}[t] = \mathbb{C}[\mathbb{A}^1] \to \mathbb{C}(C)$; the corresponding rational function on C is the image of t under this homomorphism. □

6.20. **Example.** Consider again the nodal cubic curve $N : y^2 = x^2(x+1)$ and the rational function $y/x \in \mathbb{C}(N)$. It is *not* possible to extend it to the point $(0, 0)$ (which is a singular point of N): y/x is the slope of the line connecting $(0, 0)$ to (y, x), and so it will tend to 1 if you approach $(0, 0)$ within N along the branch where $y \approx x$, and it will tend to -1 along the branch where $y \approx -x$.

7. Bézout's Theorem

Bézout's Theorem is a very important statement on the intersection of two projective plane curves. It generalizes the statement that two distinct lines always intersect in exactly one point.

We begin with a simple case.

7.1. **Definition.** Let $C : F(x, y) = 0$ be a plane affine curve and $L : ax + by = c$ an affine line such that L is not contained in C. Let $P = (\xi, \eta) \in C \cap L$. If $b \neq 0$, then we set $(C \cdot L)_P$ equal to the multiplicity of the zero ξ of the polynomial $F(x, (c - ax)/b)$. If $a \neq 0$, we set $(C \cdot L)_P$ equal to the multiplicity of the zero η of the polynomial $F((c - by)/a, y)$. If $P \notin C \cap L$, then we set $(C \cdot L)_P = 0$. The number $(C \cdot L)_P$ is called the *intersection multiplicity* of C and L in P.

7.2. **Lemma.** *The intersection multiplicity is well-defined: if both a and b are nonzero in the above, then both definitions produce the same number.*

Proof. Let $f(x) = F(x, \frac{c-ax}{b})$ and $g(y) = F(\frac{c-by}{a}, y)$. Then $g(y) = f((c - by)/a)$, $f(x) = g((c-ax)/b)$, and the two maps $x \mapsto (c-by)/a$, $y \mapsto (c-ax)/b$ are inverse homomorphisms between the polynomial rings $\mathbb{C}[x]$ and $\mathbb{C}[y]$, mapping $x - \xi$ to $y - \eta$ (up to scaling) and conversely. Therefore the multiplicities agree. (Also note that f and g are nonzero, since the defining polynomial of C does not vanish everywhere on L.) □

7.3. **Definition.** Let C be a plane projective curve, $L \not\subset C$ a projective line, and $P \in \mathbb{P}^2$ a point. We define $(C \cdot L)_P$ to be the intersection multiplicity of $(C' \cdot L')_P$ for a suitable affine patch of $\mathbb{P}^2$ that contains P (and the corresponding affine patches C' and L' of C and L). (If L' is empty, the number is zero.)

It can be checked that the number does not depend on the affine patch chosen if there are several possibilities. Also, by homogenizing the affine situation, we see that $(C \cdot L)_P$ is the multiplicity of the linear factor $\eta x - \xi y$ in the homogeneous polynomial $F(x, y, -\frac{ax+by}{c})$, if $C : F(x, y, z) = 0$, $L : ax + by + cz = 0$ with $c \neq 0$, and $P = (\xi : \eta : \zeta)$. Similar statements are true when $a \neq 0$ or $b \neq 0$.

7.4. **Theorem.** *Let C be a projective plane curve of degree d and $L \subset \mathbb{P}^2$ a projective line that is not contained in C. Then*

$$C \cdot L := \sum_{P \in \mathbb{P}^2} (C \cdot L)_P = d\,.$$

In words, C and L intersect in exactly d points, counting multiplicities.

Proof. Let $C : F(x, y, z) = 0$ and $L : ax + by + cz = 0$. Without loss of generality, assume that $c \neq 0$. Consider the homogeneous polynomial

$$f(x, y) = F\Big(x, y, -\frac{ax + by}{c}\Big)$$

of degree d. Note that $f \neq 0$ since $L \not\subset C$. For a point $P = (\xi : \eta : \zeta) \in L$, we have that $(C \cdot L)_P$ is the multiplicity of $\eta x - \xi y$ in f (and P is uniquely determined by $(\xi : \eta)$). The sum of these multiplicities is d, since f is a product of d linear factors. For all other P, the multiplicity is zero. This proves the claim. □

Let us look more closely at the intersection multiplicities.

7.5. **Proposition.** *Let C be a plane affine curve and $P \in C$.*

(1) *If L is a line through P, then $(C \cdot L)_P \geq 1$.*
(2) *If P is smooth, then for all lines L through P, we have $(C \cdot L)_P = 1$, except for the tangent line to C at P, which has intersection multiplicity at least* 2 *with C at P.*
(3) *If P is not smooth, then for all lines L through P, $(C \cdot L)_P \geq m$, where m is the multiplicity of P as a point of C. We have equality except for the finitely many lines whose slopes are the tangent directions to C at P.*

Proof. It suffices to prove the last part. Without loss of generality, assume that $P = (0,0)$, and write

$$f(x,y) = f_1(x,y) + f_2(x,y) + \cdots + f_d(x,y)\,,$$

where $f(x,y) = 0$ is the equation of C, and f_j is homogeneous of degree j. The multiplicity m is the smallest j such that $f_j \neq 0$. If we plug in λx for y (to find the intersection multiplicity with the line $y = \lambda x$), then we get a polynomial in x that is divisible by x^m, hence $(C \cdot L)_P \geq m$. Similarly if we plug in 0 for x (when the line is the vertical $x = 0$). On the other hand, the polynomial in x will start $x^m f_m(1, \lambda)$ (plus higher order terms); therefore the intersection multiplicity will be exactly m unless λ is a slope corresponding to one of the tangent directions (and this extends to the vertical case). □

7.6. **Definition.** If C is a plane curve, $P \in C$ a smooth point, then P is called an *inflection point* or *flex point* or *flex* of C, if $(C \cdot L)_P \geq 3$, where L is the tangent line to C at P.

7.7. **Remark.** The property of a point $P \in C$ to be a flex point is not an "intrinsic" property — it depends on the embedding of the curve in the plane. For example, if C is a smooth projective cubic curve and P is any point on C, then there is an isomorphism of C with another smooth plane cubic curve C' such that the image of P on C' is a flex point.

7.8. **Theorem.** *Let $C : F(x,y,z) = 0$ be a projective plane curve. Define the* Hessian *of F to be*

$$H_F = \begin{vmatrix} \dfrac{\partial^2 F}{\partial x^2} & \dfrac{\partial^2 F}{\partial x\,\partial y} & \dfrac{\partial^2 F}{\partial x\,\partial z} \\[2ex] \dfrac{\partial^2 F}{\partial y\,\partial x} & \dfrac{\partial^2 F}{\partial y^2} & \dfrac{\partial^2 F}{\partial y\,\partial z} \\[2ex] \dfrac{\partial^2 F}{\partial z\,\partial x} & \dfrac{\partial^2 F}{\partial z\,\partial y} & \dfrac{\partial^2 F}{\partial z^2} \end{vmatrix}\,.$$

Then a smooth point $P \in C$ is an inflection point if and only if $H_F(P) = 0$.

Proof. Exercise. □

7.9. **Example.** If C is a smooth conic section (so of degree 2), then C does not have flex points. Indeed, the Hessian is constant and nonzero in this case.

7.10. **Example.** Consider $C : x^4 + z^4 - y^2z^2 = 0$. The partial derivatives of the defining polynomial are

$$(4\,x^3, -2\,yz^2, 4\,z^3 - 2\,y^2z)\,;$$

they all vanish at $P_0 = (0 : 1 : 0)$, which is therefore a singularity. The Hessian is

$$\begin{vmatrix} 12\,x^2 & 0 & 0 \\ 0 & -2\,z^2 & -4\,yz \\ 0 & -4\,yz & 12\,z^2 - 2\,y^2 \end{vmatrix} = -144\,x^2z^2(y^2 + 2\,z^2)\,.$$

If $x = 0$, then $z = 0$ (this gives the singularity P_0) or $y = \pm z$; this gives two flex points $(0 : \pm 1 : 1)$. (In these two points, the tangent line meets the curve even with multiplicity 4.) If $z = 0$, then $x = 0$, and we find P_0 again. Finally, if $y^2 = -2z^2$, then we obtain the equation $x^4 = -3z^4$, and we find eight more flex points $(i^k\sqrt[4]{-3} : \pm\sqrt{-2} : 1)$ (with $k = 0, 1, 2, 3$).

When looking at the intersection of a curve and a line, we could solve the equation of the line for one of the variables and then simply plug this into the equation of the curve. So we have eliminated one variable and reduced the problem to a one-dimensional one, which was easy.

If we intersect with a curve of higher degree, elimination is not so straight-forward. However, it is possible. The tool that comes in handy here is the *resultant.*

7.11. **Definition.** Let $f_1, \dots, f_n$ be polynomials of degree less than n with coefficients in a commutative ring. Write $f_i = a_{i1}x^{n-1} + a_{i2}x^{n-2} + \dots + a_{in}$. We set for the following

$$\det(f_1, \dots, f_n) = \det(a_{ij})\,.$$

Let $f = a_nx^n + \dots + a_1x + a_0$ and $g = b_mx^m + \dots + b_1x + b_0$ be two polynomials with coefficients in a commutative ring. The *resultant* of f and g (with respect to the variable x) is the $(n + m) \times (n + m)$ determinant

$$\operatorname{Res}(f, g) = \operatorname{Res}_x(n, m;\, f, g) = \det(x^{m-1}f, \dots, xf, f, x^{n-1}g, \dots xg, g)\,.$$

7.12. **Lemma.** *Keeping the notations of the definition above, assume that f is monic of degree n and that R is a field. Then $\operatorname{Res}(n, m;\, f, g)$ is the determinant of the endomorphism ϕ of the R-vector space $V = R[x]/\langle f\rangle$, that is given by $v \mapsto g \cdot v$.*

Proof. If h is a polynomial of degree $< n + m$, then by performing row operations on the matrix whose rows are the coefficient vectors of $x^{m-1}f, \dots, xf, f, h$, we can change the last row into r, where $h = qf + r$ and $\deg r < \deg f$. Applying this to $x^{n-1}g, \dots, xg, g$, and denoting by $\overline{h}$ the remainder of h mod f (r in the above), we see that

$$\operatorname{Res}(n, m;\, f, g) = \det(x^{m-1}f, \dots, xf, f, \overline{x^{n-1}g}, \dots, \overline{xg}, \overline{g}) = \det(\overline{x^{n-1}g}, \dots, \overline{xg}, \overline{g})\,.$$

(For the second equality, note that the matrix on the left is a block matrix whose upper left block is an upper triangular matrix with 1s on the diagonal and whose lower left block is a zero matrix.) The last matrix represents ϕ in the standard basis $\overline{x^{n-1}}, \dots, \overline{x}, 1$, whence the claim. □

7.13. **Corollary.** *Let f be a monic polynomial of degree n over a field, let g and h be polynomials of degree $\le m$ and $\le \ell$, respectively.*

(1) $\operatorname{Res}(n, m+k;\ f, g) = \operatorname{Res}(n, m;\ f, g)$ *for all* $k \ge 0$. *So we can just write* $\operatorname{Res}(n, *;\ f, g)$ *to denote* $\operatorname{Res}(n, k;\ f, g)$ *for any* $k \ge \deg g$.
(2) $\operatorname{Res}(n, *;\ f, g + hf) = \operatorname{Res}(n, *;\ f, g)$.
(3) $\operatorname{Res}(n, *;\ f, gh) = \operatorname{Res}(n, *;\ f, g) \operatorname{Res}(n, *;\ f, h)$.

Proof.
(1) By Lemma 7.12, both resultants are equal to the determinant of the same linear map.

(2) Since $\overline{g + hf} = \overline{g}$, both sides are again equal to the determinant of the same linear map.

(3) This follows from Lemma 7.12 and the multiplicativity of determinants. □

7.14. **Lemma.** *Let R be a general commutative ring, f and g as in the definition.*

(1) *For $c \in R$,* $\operatorname{Res}(n, m;\ cf, g) = c^m \operatorname{Res}(n, m;\ f, g)$.
(2) $\operatorname{Res}(n, m;\ f, g) = (-1)^{mn} \operatorname{Res}(m, n;\ g, f)$.

Proof.
(1) This is clear from the definition: we multiply the upper m rows of the matrix by c.

(2) The two determinants differ by the nth power of a cyclic permutation of the $(n+m)$ rows. The sign of this permutation is $(-1)^{n(n+m+1} = (-1)^{mn}(-1)^{n(n+1)} = (-1)^{mn}$ (since $n(n+1)$ is always even). □

7.15. **Proposition.** *Let R, f, g as before, and let h be a polynomial over R of degree $\le \ell$.*

(1) $\operatorname{Res}(n, m+\ell;\ f, gh) = \operatorname{Res}(n, m;\ f, g) \operatorname{Res}(n, \ell;\ f, h)$.
(2) *If f is monic of degree n, then* $\operatorname{Res}(n, m+k;\ f, g) = \operatorname{Res}(n, m;\ f, g) =: \operatorname{Res}(n, *;\ f, g) =: \operatorname{Res}(f, g)$ *for all* $k \ge 0$.
(3) *If f is monic of degree n, then* $\operatorname{Res}(n, *;\ f, g + hf) = \operatorname{Res}(n, *;\ f, g)$.

Proof. All identities are indentities between polynomials with integral coefficients in the coefficients of f, g, h. Consider all these coefficients as independent variables, and let K be the field of fractions of the polynomial ring P in all these variables over $\mathbb{Z}$. Let F, G, H be the polynomials over P whose coefficients are the corresponding variables. Then parts (2) and (3) are valid for F, G, H in place of f, g, h and over K, by Cor. 7.13. Part (1) is true over any field if f is monic of degree n. By Lemma 7.14, the statement continues to hold when f has nonzero leading coefficient (scale f to be monic and observe that both sides scale in the same way). Since the leading coefficient of our "generic polynomial" F is nonzero (it is a variable), part (1) holds for F, G, H over K.

Now since both sides of all the equalities are in P, they are also true over P. But this means that they hold in general. (For any ring R and polynomials f, g, h over R, there is a (unique) ring homomorphism $P[x] \to R[x]$ that sends F to f, G to g and H to h, hence it maps the identities that hold over P to the ones we want over R.) □

The most important property of the resultant is the following.

7.16. **Theorem.** *Let R be a Unique Factorization Domain and let f, g be polynomials over R of degrees $\leq n$ and $\leq m$, respectively. Then* $\operatorname{Res}(n, m;\, f, g) = 0$ *if and only if either* $\deg f < n$ *and* $\deg g < m$*, or f and g have a nonconstant common divisor in $R[x]$.*

Proof. If $\deg f < n$ and $\deg g < m$, then the resultant obviously vanishes, since the first column of the matrix is zero. So we can assume that (say) $\deg f = n$. Let F be the field of fractions of R; then we can write $f = cp_1 \cdots p_k \in F[x]$ with a constant $c \neq 0$ and irreducible monic polynomials p_j. By Prop. 7.15, we have

$$\operatorname{Res}(n, m;\, f, g) = c^m \operatorname{Res}(p_1, g) \cdots \operatorname{Res}(p_k, g)\,.$$

Now if $p \in F[x]$ is irreducible, then g is either invertible mod p or divisible by p. In the first case, multiplication by g on $F[x]/\langle p\rangle$ is an invertible map, hence has nonzero determinant. In the second case, we have the zero map. Therefore:

$$\operatorname{Res}(p_j, g) = 0 \iff p_j \mid g$$

So $\operatorname{Res}(n, m;\, f, g) = 0$ if and only if f and g have a nonconstant common divisor in $F[x]$. But by Gauss' Lemma, this is equivalent to the existence of a nonconstant common divisor in $R[x]$. □

In other words, the vanishing of the resultant indicates that f and g have a common root (in a suitable extension field).

Now we want to use the resultant to get information on the intersecion of two curves.

7.17. **Lemma.** *Let $f, g \in \mathbb{C}[x, y, z]$ be homogeneous of degree n and m, respectively. Then* $\operatorname{Res}_z(n, m;\, f, g)$ *is homogeneous of degree nm in the remaining two variables x and y.*

Proof. Consider the relevant matrix. The entry in the ith row and jth column is homogeneous in x and y of degree $j - i$ if $1 \leq i \leq m$ and of degree $m + j - i$ if $m < i \leq m + n$. Every term in the expansion of the determinant as a polynomial in the entries therefore is homogeneous of degree

$$\sum_{j=1}^{n+m} j - \sum_{i=1}^{m} i - \sum_{i=m+1}^{n+m} (i - m) = \frac{(n+m)(n+m+1)}{2} - \frac{m(m+1)}{2} - \frac{n(n+1)}{2} = nm\,.$$

□

7.18. **Corollary.** *Let C and D be two projective plane curves of degrees $n \geq 1$ and $m \geq 1$, respectively. Then $C \cap D$ is nonempty. If C and D do not have a component in common, then $\#(C \cap D) \leq nm$.*

Proof. Let $F(x, y, z) = 0$ and $G(x, y, z) = 0$ be the equations of C and D. After a linear change of variables, we can assume that $(0 : 0 : 1)$ is not in $C \cap D$. Let $R(x, y) = \operatorname{Res}_z(F, G)$; then R is homogeneous of degree nm by Lemma 7.17. If $R = 0$, then F and G have a nonconstant common factor by Thm. 7.16, i.e., C and D have a component in common. (Note that the coefficient of z^n in F or the coefficient of z^m in G is nonzero since $(0 : 0 : 1) \notin C \cap D$.) In this case, we certainly have $C \cap D \neq \emptyset$, hence we can assume that $R \neq 0$. Then R is a product of $nm \geq 1$ linear forms. Therefore, there is some $(\xi : \eta) \in \mathbb{P}^1$ such that $R(\xi, \eta) = 0$. But then by Thm. 7.16 again, the polynomials $F(\xi, \eta, z)$ and $G(\xi, \eta, z)$ in $\mathbb{C}[z]$ have a common root ζ. But this means that $(\xi : \eta : \zeta) \in C \cap D$.

Now assume that there are $nm+1$ distinct intersection points $P_1, \dots, P_{nm+1}$. After perhaps another linear change of variables, we can assume that $P_j = (\xi_j : \eta_j : \zeta_j) \neq (0 : 0 : 1)$ such that all $Q_j = (\xi_j : \eta_j)$ are distinct. Then $R(\xi_j, \eta_j) = 0$ for all j (note that ζ_j is a common root of $F(\xi_j, \eta_j, z)$ and $G(\xi_j, \eta_j, z)$). But R is homogeneous of degree nm, so this implies that $R = 0$, contradicting the assumption that C and D do not have a component in common. □

Now this prompts the following definition.

7.19. **Definition.** Let C and D be two projective plane curves without common component. Let $P \in C \cap D$. If necessary, make a linear change of variables as in the second part of the proof above; then we define the *intersection multiplicity* of C and D at P to be the multiplicity of the factor $\eta x - \xi y$ in $R(x, y)$, where $P = (\xi : \eta : \zeta)$. As before, we write $(C \cdot D)_P$ for that number. If $P \notin C \cap D$, we set $(C \cdot D)_P = 0$.

With this definition, the following theorem is immediate.

7.20. **Bézout's Theorem.** *Let C and D be projective plane curves of degrees n and m, without common component. Then*

$$C \cdot D := \sum_{P \in \mathbb{P}^2} (C \cdot D)_P = nm\,.$$

In words, C and D intersect in exactly nm points, if we count the points according to intersection multiplicity.

7.21. **Example.** Let us look at the points of intersection of the two circles with affine equations $C_1 : x^2 + y^2 = 1$ and $C_2 : (x-2)^2 + y^2 = 4$. The projective closures are given by the polynomials

$$F_1 = x^2 + y^2 - z^2 \quad \text{and} \quad F_2 = x^2 - 4xz + y^2\,.$$

We compute the resultant (with respect to z)

$$R = \begin{vmatrix} -1 & 0 & x^2+y^2 & 0 \\ 0 & -1 & 0 & x^2+y^2 \\ 0 & -4x & x^2+y^2 & 0 \\ 0 & 0 & -4x & x^2+y^2 \end{vmatrix} = -(x^2+y^2)(15x^2-y^2)\,.$$

Its zeros correspond to the points $(i : 1), (-i : 1), (1 : \sqrt{15}), (1 : -\sqrt{15}) \in \mathbb{P}^1$. We find the intersection points of intersection multiplicity 1

$$(i : 1 : 0)\,, \quad (-i : 1 : 0)\,, \quad (1 : \sqrt{15} : 4)\,, \quad (1 : -\sqrt{15} : 4)\,.$$

7.22. **Example.** Now consider two concentric circles $C_1 : x^2 + y^2 = 1$, $C_2 : x^2 + y^2 = 4$. This time,

$$R = \begin{vmatrix} -1 & 0 & x^2+y^2 & 0 \\ 0 & -1 & 0 & x^2+y^2 \\ -4 & 0 & x^2+y^2 & 0 \\ 0 & -4 & 0 & x^2+y^2 \end{vmatrix} = 9(x^2+y^2)^2\,.$$

R now has double zeros at $(\pm i : 1)$, and we get two intersection points $(\pm i : 1 : 0)$ of multiplicity 2: concentric circles touch at infinity!

7.23. **Example.** Let us look at our old friends, the nodal and cuspidal cubics. The projective equations are

$$N : x^3 + x^2 z - y^2 z = 0\,, \qquad C : x^3 - y^2 z = 0\,.$$

The point $(0 : 0 : 1)$ is on both curves, as is $(0 : 1 : 0)$, so we take the resultant with respect to x to avoid problems.

$$R = \begin{vmatrix} 1 & z & 0 & -y^2z & 0 & 0 \\ 0 & 1 & z & 0 & -y^2z & 0 \\ 0 & 0 & 1 & z & 0 & -y^2z \\ 1 & 0 & 0 & -y^2z & 0 & 0 \\ 0 & 1 & 0 & 0 & -y^2z & 0 \\ 0 & 0 & 1 & 0 & 0 & -y^2z \end{vmatrix} = -y^4 z^5\,.$$

The roots are at $(\eta : \zeta) = (0 : 1)$ and $(1 : 0)$, of multiplicities 4 and 5, respectively. So the intersection points are $(0 : 0 : 1)$ of intersection multiplicity 4 and $(0 : 1 : 0)$ of intersection multiplicity 5.

7.24. **Example.** It is true (Exercise) that the curve H given by the Hessian of a polynomial F defining the curve C meets C with multiplicity 1 (i.e., *transversally*) in a simple flex point (i.e., such that the intersection multiplicity of the tangent line and the curve is just 3 and not larger). If C is a smooth cubic curve, then any line meets C in at most three points (counting multiplicities), so there are only simple flex points. Therefore, H meets C only transversally, hence there are exactly 9 intersection points (H is also a curve of degree 3):

A smooth plane cubic curve has exactly nine inflection points.

If the coefficients of the polynomial defining C are real numbers, then exactly three of the inflection points are real (the other six come in three pairs of complex conjugates).

7.25. **Corollary.** *If C is a smooth plane projective curve, then C is irreducible.*

Proof. Otherwise, C would have at least two components C_1 and C_2, which would have to meet in some point P. But then P is a point of multiplicity at least 2 on C, hence a singularity. □

Now let us look at *bitangents* of quartic curves. A bitangent to a curve C is a line that meets C in two points with multiplicity at least 2. (As a boundary case, we include that the line meets C in some point with multiplicity at least 4; in this case, the two points of tangency can be thought of as coinciding.)

7.26. **Example.** As an example, consider the *Fermat Quartic* $F : x^4+y^4+z^4 = 0$. Let $P = (\xi : \eta : \zeta) \in F$ be a point; then the tangent line to K at P has equation

$$L : \xi^3 x + \eta^3 y + \zeta^3 z = 0\,.$$

For now, assume that $\zeta \neq 0$; then we can set $\zeta = 1$. We eliminate $z = -\xi^3 x - \eta^3 y$ from the equation for F; we get a homogeneous polynomial in x and y of degree 4 that is divisible by $(\eta x - \xi y)^2$. Dividing off this factor (one has to use that $\xi^4 + \eta^4 + 1 = 0$ in this computation), a quadratic polynomial remains whose discriminant is a constant times $\xi^2\eta^2(\xi^4 + \eta^4 + \xi^4\eta^4)$. Taking into account points at infinity leads to

$$G = x^2y^2z^2(x^4y^4 + y^4z^4 + z^4x^4)$$

such that the points of tangency of the bitangents are exactly the points of intersection of F with the curve defined by G. By Bézout, there are exactly $14 \cdot 4 = 56$ intersection points (counting multiplicity), and since every bitangent accounts for two points, there are 28 bitangents. There are twelve lines that intersect F fourfold in points like $(0 : \zeta^{1+2k} : 1)$, where $\zeta = e^{\pi i/4}$ is a primitive eighth root of unity. They correspond to the factors $x^2y^2z^2$ in G, and the lines are given by $y - \zeta^{1+2k}z = 0$. The other factors of G lead to points $(\tau^{1+3k} : \tau^{2+3\ell} : 1)$ and $(\tau^{2+3\ell} : \tau^{1+3k} : 1)$ with $\tau = e^{\pi i/6}$. They are the points of tangency of 16 other bitangents $i^a x + i^b y + z = 0$.

These considerations can be extended to arbitrary smooth plane quartic curves:

A smooth plane quartic curve has exactly 28 *bitangents.*