Chapter 5

Local Rings

In this chapter we will study the local rings $\mathcal{O}_P$; in particular we will see that the algebraic structure of $\mathcal{O}_P$ contains information about whether a point P is singular or not, and we will learn how to define intersection multiplicites using these rings.

5.1 Local Rings

Now fix a point $P \in \mathcal{C}_f$, and let $\mathcal{O}_P(\mathcal{C}_f)$ denote the set of all rational functions $g \in K(\mathcal{C}_f)$ that are defined at P.

Lemma 5.1.1. *The set $\mathcal{O}_P(\mathcal{C}_f)$ is a subring of $K(\mathcal{C}_f)$ containing the coordinate ring: $K \subseteq K[\mathcal{C}] \subseteq \mathcal{O}_P(\mathcal{C}_f) \subseteq K(\mathcal{C})$.*

Proof. If g_1 and g_2 are defined at P, then so are $g_1 \pm g_2$ and $g_1 g_2$: in fact, if $g_1 = a_1/b_1$ and $g_2 = a_2/b_2$ with $g_1(P), g_2(P) \neq 0$, then $g_1 + g_2 = (a_1 b_2 + a_2 b_1)/(b_1 b_2)$ and $g_1 g_2 = a_1 a_2/(b_1 b_2)$, and $b_1(P) b_2(P) \neq 0$ since $K[\mathcal{C}_f]$ is a domain. Note, however, that in general g_1/g_2 is not defined at P since we might have $g_2(P) = 0$.

Thus $\mathcal{O}_P(\mathcal{C}_f)$ is a subring of $K(\mathcal{C}_f)$. Moreover, elements in the coordinate ring are defined everywhere, hence are contained in $\mathcal{O}_P(\mathcal{C}_f)$ for any $P \in \mathcal{C}_f(K)$. $\square$

The ring $\mathcal{O}_P(\mathcal{C}_f)$ is called the **local ring** of $\mathcal{C}_f$ at P. Elements in the local ring at P can be evaluated there:

Lemma 5.1.2. *For $g \in \mathcal{O}_P(\mathcal{C}_f)$ with $g = \frac{a}{b}$ and $b(P) \neq 0$, the expression $g(P) = \frac{a(P)}{b(P)}$ is well defined.*

Proof. In fact, assume that $g = \frac{a}{b} = \frac{c}{d}$ and $b(P)d(P) \neq 0$. This means that, as polynomials, we have $ad - bc \in (f)$. Evaluation at P shows that $a(P)d(P) - b(P)c(P) = 0$ since $f(P) = 0$, and this implies that $a(P)/b(P) = c(P)/d(P)$, which is the claim. $\square$

Thus we can and will talk about values $g(P)$ for $g \in \mathcal{O}_P(\mathcal{C}_f)$.

Proposition 5.1.3. *The local rings $\mathcal{O}_P(\mathcal{C}_f)$ are Noetherian.*

Proof. Let I be an ideal in $\mathcal{O}_P(\mathcal{C}_f)$, and define $J = I \cap K[\mathcal{C}_f]$. Since $K[\mathcal{C}_f]$ is Noetherian, J is finitely generated, say $J = (f_1, \ldots, f_m)$ (strictly speaking we should write $f_1 + (f)$ etc.). We claim that $f_1, \ldots, f_m$ generate I. In fact, let $g \in I \subseteq \mathcal{O}_P(\mathcal{C}_f)$; since g is defined at P, there exist $a, b \in K[\mathcal{C}_f]$ with $g = a/b$ and $b(P) \neq 0$. Thus $bg \in K[\mathcal{C}_f] \cap I = J$, and thus $bg = r_1 f_1 + \ldots + r_m f_m$ with $r_i \in K[\mathcal{C}_f]$. This implies $g = (\sum r_j f_j)/b = \sum (r_j/b) f_j$, where $r_j/b \in \mathcal{O}_P(\mathcal{C}_f)$. ☐

We can get back $K[\mathcal{C}_f]$ from the local rings:

Proposition 5.1.4. *We have $K[\mathcal{C}_f] = \bigcap_P \mathcal{O}_P(\mathcal{C}_f)$.*

Proof. We have already proved that: the statement is equivalent to the claim that $\mathrm{dom}(g) = V$ for some $f \in K(V)$ is equivalent to $g \in K[V]$. Let us give the simple proof once more:

Let $g \in \bigcap_P \mathcal{O}_P(\mathcal{C}_f)$ and define $J_g = \{h \in K[X,Y] : hg + (f) \in K[\mathcal{C}_f]\}$. This is an ideal in $K[X,Y]$ containing (f). Note that if $g = \frac{a}{b}$, then $b \in J_g$, so the ideal J_g consists of the "denominators" of g. It is either the unit ideal or contained in some maximal ideal, which, by Hilbert's Nullstellensatz, has the form $(X - r, Y - s)$ for some $r, s \in K$.

If $J_g \subseteq (X - r, Y - s)$, then $h(r,s) = 0$ for all $h \in J_g$. But g is defined at $Q = (r,s)$, hence $g = \frac{a}{b}$ with $b(Q) \neq 0$, and $b \in J_g$: contradiction.

Thus $J_g = (1)$, and this implies that $g \in K[\mathcal{C}_f]$. ☐

We also have used the fact that every ideal is contained in some maximal ideal. This is in general a consequence of Zorn's Lemma, but can be deduced from the fact that $K[X,Y]$ is Noetherian (we have already seen that).

5.2 Local Rings are Local Rings

In commutative algebra, any ring R with the property that $R \setminus R^\times$ is an ideal is called a local ring. Let R denote a local ring in this sense and put $\mathfrak{m} = R \setminus R^\times$; then $\mathfrak{m}$ is clearly a maximal ideal because you cannot enlarge this ideal properly: adding a unit means you will get (1) as a result.

Proposition 5.2.1. *The ring $\mathcal{O}_P(\mathcal{C}_f)$ is a local ring. Its maximal ideal is the set of all functions vanishing at P: $\mathfrak{m} = \{g \in \mathcal{O}_P(\mathcal{C}_f) : g(P) = 0$.*

Proof. Consider the evaluation map $\mathcal{O}_P(\mathcal{C}_f) \longrightarrow K : g \to g(P)$ with kernel $\mathfrak{m}$. From algebra we know that if $\phi : R \longrightarrow S$ is a ring homomorphism, then $R/\ker\phi \simeq \mathrm{im}\,\phi$. In our situation this gives $\mathcal{O}_P(\mathcal{C}_f)/\mathfrak{m} \simeq K$ since evaluation is clearly surjective (evaluating the constant function $a \in K$ at P gives a). But this implies that $\mathfrak{m}$ is maximal. Moreover, every $g = \frac{a}{b} \in \mathcal{O}_P(\mathcal{C}_f) \setminus \mathfrak{m}$ is a unit since $a(P) \neq 0$ implies that $\frac{1}{g} = \frac{b}{a}$ is defined at P. Thus $\mathcal{O}_P(\mathcal{C}_f)$ is indeed a local ring with maximal ideal $\mathfrak{m}$. ☐

The situation is analogous to the following: for each prime p in $\mathbb{Z}$, define the ring $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$. This is a local ring, since the nonunits are those elements $\frac{a}{b}$ with $p \mid a$, and they form an ideal $(p) = p\mathbb{Z}_{(p)}$ (the multiples of p). We clearly have $\mathbb{Z} = \bigcap_p \mathbb{Z}_{(p)}$. The analog of the evaluation map is reduction modulo p: if $p \nmid b$, then $g(p) = \frac{a}{b} \bmod p$ is a well defined residue class modulo p. This is not really a function, since the domain depends on the point at which it is evaluated, but this is the best we can do. The kernel of the evaluation map is the set of all $\frac{a}{b} \in \mathbb{Z}_{(p)}$ with $p \mid a$, that is, the ideal $(p) \subset \mathbb{Z}_{(p)}$. It is a maximal ideal in $\mathbb{Z}_{(p)}$ because $\mathbb{Z}_{(p)}/(p) \simeq \mathbb{Z}/p\mathbb{Z}$ is a field.

The rings $\mathbb{Z}_{(p)}$ have all the properties of our local rings $\mathcal{O}_P(\mathcal{C}_f)$: the analog of the coordinate ring is $\mathbb{Z}$, the points $P \in \mathcal{C}_f$ correspond to the prime ideals in $\mathbb{Z}$, and the local rings $\mathcal{O}_P(\mathcal{C}_f)$ to the local rings $\mathbb{Z}_{(p)}$. Every ideal in this ring has the form (p^a) for some $a \geq 0$. This means that

- R is Noetherian: every ideal is finitely generated;
- R is a local ring: every ideal $\neq (1)$ is contained in the unique maximal ideal $\mathfrak{m} = (p)$;
- the unique maximal ideal $\mathfrak{m} = (p)$ is principal.

The common notion that contains both local rings of curves and rings such as $\mathbb{Z}$ is that of a scheme.

5.3 Discrete Valuation Rings

Proposition 5.3.1. *Let R be a domain which is not a field. Then the following statements are equivalent:*

1. *R is a Noetherian local ring whose maximal ideal is principal;*
2. *there is an irreducible element $t \in R$ such that every nonzero $r \in R$ can be written uniquely in the form $r = ut^n$, where $u \in R^\times$ is a unit and $n \geq 0$ some integer.*

As an example, consider the ring $R = \mathbb{Z}_{(p)}$. Here every nonzero element $r \in R$ has the form $r = up^a$ for some $u \in R^\times$.

If R is a field, then its only ideals are (0) and (1), so every field is Noetherian. Also, (0) is a maximal ideal since $R/(0) \simeq R$ is a field, hence fields are local rings whose maximal ideals are principal.

Proof. Assume that R is a Noetherian local ring whose maximal ideal is principal, say $\mathfrak{m} = (t)$. Let $r \in R$ be a nonunit; this implies that $r \in \mathfrak{m}$, hence $r = r_1 t$. If $r_1 \in R^\times$, we are done; otherwise $r_1 = r_2 t$, and we can continue. Assume this process does not stop. Then we have a chain of ideals $(r_1) \subset (r_2) \subset \ldots$; since R is Noetherian, this chain must terminate, say $(r_n) = (r_{n+1})$. But then r_{n+1} and r_n differ by a unit contradicting our construction. Thus the process terminates, and we have $r = ut^n$ for some unit u and some integer $n \geq 0$.

Assume now that $ut^n = vt^m$ for units $u, v \in R^\times$; then $ut^{n-m} = v$ is a unit, hence $n = m$ and $u = v$. Thus the representation is unique.

Now assume that every nonzero element has the form $r = ut^n$ and let $\mathfrak{m} = (t)$. Every element in $R \setminus \mathfrak{m}$ is a unit, hence R is local. Let $\mathfrak{a}$ be any ideal in R; if $\mathfrak{a} \neq (1)$, it is contained in the maximal ideal $\mathfrak{m}$. Let n be the maximal integer with $\mathfrak{a} \subseteq \mathfrak{m}^n$ and define $\mathfrak{b} = \{a \in R : t^n a \in \mathfrak{a}\}$; this is an ideal with $\mathfrak{a} = \mathfrak{b}(t^n)$. We claim that $\mathfrak{b} = (1)$; in fact, there is some $a \in \mathfrak{a}$ with $a = ut^n$ for some unit u, otherwise $\mathfrak{a} \subseteq \mathfrak{m}^{n+1}$. But then $u \in \mathfrak{b}$. This shows that every nonzero ideal in R has the form (t^n) for some $n \geq 0$, in particular every ideal is finitely generated. $\square$

We say that a ring R is a **discrete valuation ring** if R is a Noetherian local ring whose maximal ideal is principal. The reason for this name is that we can define a function $v : R \setminus \{0\} \longrightarrow \mathbb{N}$ by putting $v(r) = n$ for $r = ut^n$. This function has the following properties:

1. $v(r) \geq 0$ for all $r \in R$ (even for $r = 0$ if you put $v(0) = \infty$);
2. $v(r) \geq 1$ if and only if $r \in \mathfrak{m}$; $v(r) = 0$ if and only if r is a unit;
3. $v(rs) = v(r) + v(s)$ for all $r, s \in R$;
4. $v(r + s) \geq \min\{v(r), v(s)\}$.

The proofs are almost trivial; let us look at the last one and write $r = ut^n$, $s = vt^m$. If $n < m$, then $v(r + s) = n = \min\{v(r), v(s)\}$. If $n = m$, then $v(r + s) \geq n$. That's it.

More generally, a valuation of R is a map $v : R \longrightarrow \overline{\mathbb{R}}$ (where $\overline{\mathbb{R}}$ is the set of nonnegative reals with ∞ included) having the properties $v(rs) = v(r) + v(s)$ and $v(r + s) \geq \min\{v(r), v(s)\}$. The valuation is said to be discrete if the value set $v(R)$ is discrete in $\overline{\mathbb{R}}$, for example if $v(R) = \mathbb{N}$ as in the example above.

In less fancy terms, a discrete valuation ring is a ring with a unique prime p, and the valuation tells us how often an element is divisible by p.

Note that valuations may exist in rings other than discrete valuation rings; for example, the valuation attached to the discrete valuation ring $\mathbb{Z}_{(p)}$ is also a valuation on $\mathbb{Z}$. This means that for every prime p there is a p-adic valuation in $\mathbb{Z}$.

Lemma 5.3.2. *Let $P = (a, b)$ be a point on $\mathcal{C}_f : f(X, Y) = 0$. Then $\mathfrak{m}_P(\mathcal{C}_f) = (x - a, y - b)$, where $x = X + (f)$ and $y = Y + (f)$.*

Proof. Since x and y are defined everywhere, they are contained in $\mathcal{O}_P(\mathcal{C}_f)$, and since $x - a$ and $y - b$ vanish at P, they are contained in $\mathfrak{m}_P(\mathcal{C}_f)$.

Conversely, let $g = \frac{r}{s}$ be defined at P; then $g \in \mathfrak{m}_P$ means that $r(a, b) = 0$. Thus the Taylor expansion of $r \in K[X, Y]$ around (a, b) does not have a constant term, hence can be written in the form $r(X, Y) = (X - a)c + (Y - b)d$ for polynomials c, d (this is because all the terms of higher degree are divisible by $X - a$ or $Y - b$). But then $g = \frac{r}{s} = (x - a)\frac{c}{s} + (y - a)\frac{d}{s}$, and the quotients $\frac{c}{s}$, $\frac{d}{s}$ are elements of $\mathcal{O}_P$. Thus $g \in (x - a, y - b)$. $\square$

Theorem 5.3.3. *Let $\mathcal{C}_f : f(X,Y) = 0$ be an irreducible plane curve defined over some algebraically closed field K, and let $P \in \mathcal{C}_f(K)$, and assume that P is simple (i.e., nonsingular). Then $\mathcal{O}_P(\mathcal{C}_f)$ is a discrete valuation ring. If $L : aX + bY + c = 0$ is a line through P, the image ℓ of L in $\mathcal{O}_P(\mathcal{C}_f)$ is a uniformizer if and only if L is not a tangent.*

Proof. Changing coordinates we may assume that $P = (0,0)$ with tangent $Y = 0$, and that $L : X = 0$. We have to show that the maximal ideal $\mathfrak{m}_P(\mathcal{C}_f)$ is generated by $x = X + (f)$. From Lemma 5.3.2 we know that $\mathfrak{m}_P = (x,y)$. Since P is simple with tangent L, the Taylor expansion of f around P has the form $f(X,Y) = Y+$ terms of higher order; the terms of higher order are divisible by Y or by X^2, hence we can write $f(X,Y) = Yg - X^2h$ for polynomials g,h with $g(X,Y) = 1+$ terms of higher order and $h \in K[X]$. Reducing modulo f we find $yg = x^2h$ in $K(\mathcal{C}_f)$, hence $y = x^2h/g \in (x)$ because $g(P) = g(0,0) = 1 \neq 0$. Thus $\mathfrak{m}_P = (x,y) = (x)$. ☐

For simple points P we therefore have a valuation ord_P on the discrete valuation ring $\mathcal{O}_P(\mathcal{C}_f)$.

5.4 Multiplicities and Bezout

In this section we will define multiplicities of points, intersection multiplicities, and we will state Bezout's Theorem. Proofs will be given in the next section.

Let us start by defining the multiplicity of a point on a plane algebraic curve $\mathcal{C}_f : f(x,y) = 0$. By choosing our coordinate system properly we may assume that $P = (0,0)$; write $f = f_m + f_{m-1} + \ldots + f_n$, where $f_k \neq 0$ is homogeneous of degree k, and where $n = \deg f$. Then $m_P(f) = m$ is called the multiplicity of m. Points with multiplicity $m_P(\mathcal{C}_f) = 2$ are called double points, points with $m_P(\mathcal{C}_f) = 3$ triple points.

The fact that $f(P) = 0$ implies that f does not contain constant terms, hence $m_P(\mathcal{C}_f) \geq 1$. Moreover, P is singular if and only if all linear terms vanish, that is, if and only if $m_P(\mathcal{C}_f) \geq 2$. Finally, we obviously have $m_P(\mathcal{C}_f) \leq \deg f$.

As an example, consider $\mathcal{C}_f : f(x,y) = y^2 - x^3 - x^2 = 0$; here $f = f_2 + f_3$ with $f_2 = y2 - x^2$ and $f_3 = -x^3$, hence $m_P(\mathcal{C}_f) = 2$, and P is a double point.

For determining the multiplicity of the point at infinity on $\mathcal{C}_f$, we first homogenize: $Y^2Z - X^3 - X^2Z = 0$. The point at infinity has coordinates $P = [0:1:0]$. Now we dehomogenize with respect to Y (dehomogenizing with respect to Z means putting $Z = 1$; we dehomogenize with respect to Y by putting $Y = 1$) and find $Z - X^4 - X^2Z = 0$. The point P has coordinates $(0,0)$ in this coordinate system (the embedding of $\mathbb{A}^2K$ into the projective plane is given by $(x,z) \longmapsto [x:1:z]$ in this case), and clearly $m_P(\mathcal{C}_f) = 1$. Thus the point at infinity has multiplicity 1.

A basic result on multiplicities of points is the following

Theorem 5.4.1. *Let P be a point on the irreducible curve $\mathcal{C}_f : f(X,Y) = 0$. Then*

$$m_P(\mathcal{C}_f) = \dim_K {\mathfrak{m}_P}^n / {\mathfrak{m}_P}^{n+1}$$

for all sufficiently large n. In particular, the multiplicity of P only depends on the local ring $\mathcal{O}_P(\mathcal{C}_F)$.

The importance of this result lies with the fact that affine (or projective) coordinate changes induce isomorphisms of the coordinate rings, the local rings, and their maximal ideals. Thus every object defined in terms of $\mathcal{O}_P$ will be invariant under coordinate changes.

Intersection Multiplicities

Let $\mathcal{C}_f : f(x,y) = 0$ and $\mathcal{C}_g : g(x,y) = 0$ be two plane algebraic curves. We will assume that they do not have common components: curves are unions of irreducible curves, and the assumption made here is that no irreducible curve is simultaneously part of $\mathcal{C}_f$ and $\mathcal{C}_g$; for example, $f(x,y) = X^2 - 4$ and $g(x,y) = XY - 2Y$ have the line $X - 2 = 0$ as a common component. Note that irreducible curves have no common component if and only if they are distinct.

In such a situation we would like to count the number of intersection points. The weakest form of Bezout's theorem states that this number is at most $(\deg f)(\deg g)$; the strong form of Bezout's theorem states that this becomes an equality if we

1. work over an algebraically closed field (some points of intersection might not have coordinates in the base field);
2. work in the projective plane (some points of intersection might lie at infinity);
3. count with multiplicity (a tangent intersects a circle in exactly one point, which we have to count twice).

Now let P be a point of intersection of $\mathcal{C}_f$ and $\mathcal{C}_g$; this means that $f(P) = g(P) = 0$. We would like to interpret the multiplicity as an algebraic invariant of some object inside $\mathcal{O}_P$, the ring of functions in $K(x,y)$ defined at P. Note that $\mathcal{O}_P$ is a subring of the function field $K(x,y) = K(x,y)/(0)$ of the affine plane. It is a local ring with maximal ideal $\mathfrak{m}_P = \{f \in K(x,y) : f(P) = 0\}$. The

If $f(P) \neq 0$, we have $(f,g) = (1)$ in $\mathcal{O}_P$: in fact, since $\frac{1}{f}$ is defined at P, we have $1 = \frac{1}{f} \cdot f \in (f,g)$. This suggests looking at the quotient ring $\mathcal{O}_P/(f,g)$. First observe that this is a K-vector space: if h_1, h_2 represent elements in $\mathcal{O}_P/(f,g)$, i.e., are defined at P, then so do $c_1h_1 + c_2h_2$ for $c_1, c_2 \in K$. What we have seen above is that $\dim \mathcal{O}_P/(f,g) = 0$ if P is not a point of intersection of $\mathcal{C}_f$ and $\mathcal{C}_g$. We now define:

The intersection multiplicity of two plane algebraic curves $\mathcal{C}_f$ and $\mathcal{C}_g$ without common components is

$$I(P, \mathcal{C}_f \cap \mathcal{C}_g) = \dim \mathcal{O}_P/(f,g).$$

We now prove

Lemma 5.4.2. *If $P \in \mathcal{C}_f \cap \mathcal{C}_g$, then*

$$I(P, \mathcal{C}_f \cap \mathcal{C}_g) = 1 + \dim \mathfrak{m}_P/(f,g).$$

In particular, $I(P, \mathcal{C}_f \cap \mathcal{C}_g) \geq 1$ if and only if P is a point of intersection of $\mathcal{C}_f$ and $\mathcal{C}_g$.

Proof. Consider the exact sequence

$$0 \longrightarrow \mathfrak{m}_P \longrightarrow \mathcal{O}_P \longrightarrow K \longrightarrow 0$$

of K-vector spaces induced by the evaluation map $\mathcal{O}_P \longrightarrow K$ defined by mapping $h \in \mathcal{O}_P$ to $f(P) \in K$. Since $f(P) = g(P) = 0$, the evaluation map is 0 on the ideal (f,g), hence we get an induced exact sequence

$$0 \longrightarrow \mathfrak{m}_P/(f,g) \longrightarrow \mathcal{O}_P/(f,g) \longrightarrow K \longrightarrow 0$$

Now invoke the exercise that if U, V, W are K-vector spaces such that

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

is exact, then $V \simeq U \oplus W$, and $\dim V = \dim U + \dim W$. □

Two curves $\mathcal{C}_f$ and $\mathcal{C}_g$ are said to intersect transversally in P if $m_P(\mathcal{C}_f) = m_P(\mathcal{C}_g) = 1$, and if the tangents to $\mathcal{C}_f$ and $\mathcal{C}_g$ in P are distinct.

Using intersection multiplicities, we can even define tangents in singular points. Let P be a point on $\mathcal{C}_f$ with multiplicity $m = m_P(\mathcal{C}_f)$. Then any line will intersect $\mathcal{C}_f$ in P with multiplicity $\geq m$, and there is at least one line intersecting with multiplicity $= m$. Any line intersecting with multiplicity $> m$ will be called a tangent to $\mathcal{C}_f$ at P.

Consider e.g. the cubic $f(x,y) = y^2 - x^3 - x^2$ with the double point $P = (0,0)$. There are two lines intersecting the cubic in P with multiplicity > 2, namely $y = x$ and $y = -x$. A proof will require a lemma that we will only give in the next section, which is why we will discuss the details later.

The main result on intersection multiplicities is

Theorem 5.4.3. *Let K be an algebraically closed field. There exists exactly one function $I(P, \mathcal{C}_f \cap \mathcal{C}_g)$ defined for all plane curves $\mathcal{C}_f$, $\mathcal{C}_g$ and all points $P \in \mathbb{A}^2K$ with the following properties:*

1. *$I(P, \mathcal{C}_f \cap \mathcal{C}_g) \in \mathbb{N}$ whenever $\mathcal{C}_f$ and $\mathcal{C}_g$ do not have a common component passing through P (we put $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = \infty$ when this happens).*

2. *$I(P, \mathcal{C}_f \cap \mathcal{C}_g) = 0$ if and only if $P \notin \mathcal{C}_f \cap \mathcal{C}_g$. Moreover, $I(P, \mathcal{C}_f \cap \mathcal{C}_g)$ only depends on the components of $\mathcal{C}_f$ and $\mathcal{C}_g$ passing through P.*

3. *If T is an affine change of coordinates (a bijective linear map followed by a translation) and $T(Q) = P$, then $I(Q, \mathcal{C}_f^T \cap \mathcal{C}_g^T) = I(P, \mathcal{C}_f \cap \mathcal{C}_g)$.*

4. $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = I(P, \mathcal{C}_g \cap \mathcal{C}_f)$.

5. $I(P, \mathcal{C}_f \cap \mathcal{C}_g) \geq m_P(\mathcal{C}_f) m_P(\mathcal{C}_g)$, *with equality if and only if* $\mathcal{C}_f$ *and* $\mathcal{C}_g$ *have no tangent in common at* P.

6. *Let* $f = \prod f_j$ *and* $g = \prod g_k$. *Then* $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = \sum I(P, \mathcal{C}_{f_j} \cap \mathcal{C}_{g_k})$.

7. *Let* $h = g + af$ *for* $a \in K[x,y]$; *then* $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = I(P, \mathcal{C}_f \cap \mathcal{C}_h)$.

Moreover, this function is given by

$$I(P, \mathcal{C}_f \cap \mathcal{C}_g) = \dim_K \mathcal{O}_P/(f,g).$$

The proof will be given below. It will make use of the following lemma, which allows us to reduce some statements about $\mathcal{O}_P$ to statements about the polynomial ring $K[x,y]$:

Lemma 5.4.4. *Let* $f_1, \ldots, f_n \in K[x,y]$ *with* $\mathcal{V}(f_1, \ldots, f_n) = \{P\}$. *Then*

$$K[x,y]/(f_1, \ldots, f_n) \simeq \mathcal{O}_P/(f_1, \ldots, f_n).$$

Proof. The inclusion $K[x,y] \hookrightarrow \mathcal{O}_P$ induces a homomorphism

$$\lambda : K[x,y]/(f_1, \ldots, f_n) \longrightarrow \mathcal{O}_P/(f_1, \ldots, f_n).$$

Let us first see why λ is injective. Let $f \in \ker \lambda$. Then there are $g, g_1, \ldots, g_n \in K[x,y]$ such that $f = \sum \frac{1}{g} g_i f_i$ and $g(P) \neq 0$. Since $\mathcal{V}(f_1, \ldots, f_n) = \{P\}$, we have $\mathcal{V}(f_1, \ldots, f_n, g) = \varnothing$, so by Hilbert's Nullstellensatz we must have $(f_1, \ldots, f_n, g) = (1)$. Thus there exist polynomials $h_1, \ldots, h_n$ with $1 = hg + \sum h_i f_i$, hence

$$f = hgf + \sum h_i f f_i = \sum h g_i h_f + \sum h_i f f_i = \sum (h g_i + h_i f) f_i,$$

which means $f \in (f_1, \ldots, f_n)$.

Next we show that λ is surjective. In fact, let g be a polynomial with $g(P) \neq 0$; as above there exist $h, h_1, \ldots, h_n$ with $1 = hg + \sum h_i f_i$. But then $\lambda(h) = \frac{1}{g}$. □

As an application, we can compute the intersection multiplicity $I(P, \mathcal{C}_f \cap \mathcal{C}_g)$ for $P = (0,0)$, $f(x,y) = y - x$, and $g(x,y) = y^2 - x^3 - x^2$. In fact, it is easily seen that $\mathcal{V}(f,g) = \{P\}$, hence

$$\begin{aligned} I(P, \mathcal{C}_f \cap \mathcal{C}_g) &= \dim \mathcal{O}_P/(f,g) = \dim K[x,y]/(f,g) \\ &= \dim K[x,y]/(y - x, y^2 - x^3 - x^2) = \dim K[x,y]/(y - x, x^3) \\ &= \dim K[x]/(x^3) = \dim K \oplus Kx \oplus Kx^2 = 3. \end{aligned}$$

Here we have used $K[x,y]/(y - x, x^3) \simeq K[x]/(x^3)$.

A similar calculation shows that we also have $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = 3$ for the line $y = -x$. On the other hand, for the line $L : x = 0$ we get

$$I(P, \mathcal{C}_f \cap \mathcal{C}_L) = \dim \frac{K[x,y]}{(y^2 - x^3 - x^2, x)} = \dim K[y]/(y^2) = 2.$$

Note that it is not too difficult to derive this result without appealing to Lemma 5.4.4. In general, however, results like these are very useful to go from a problem in $\mathcal{O}_P$ to one in the polynomial ring $K[x,y]$, which we understand better. It is therefore of interest to generalize Lemma 5.4.4; this is indeed possible:

Proposition 5.4.5. *Let I be an ideal in $R = K[x_1, \ldots, x_n]$, and assume that $\mathcal{V}(I) = \{P_1, \ldots, P_d\}$. Then*

$$R/I \simeq \mathcal{O}_{P_1}/I \oplus \cdots \oplus \mathcal{O}_{P_d}/I.$$

Armed with this proposition, we can show that $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = 2$ for the lines $f(x,y) = y - tx$ with $t \neq \pm 1$. In fact, we have $\mathcal{V}(f,g) = \{P, Q\}$ with $P = (0,0)$ and $Q = (t^2 - 1, t^3 - t)$. Thus

$$3 = \dim K[x,y]/(f,g) = \dim \mathcal{O}_P/(f,g) + \dim \mathcal{O}_Q/(f,g).$$

We know that $\dim \mathcal{O}_Q/(f,g) = 1 + \dim \mathfrak{m}_Q/(f,g) \geq 1$, hence $\dim \mathcal{O}_P/(f,g) \leq 2$. On the other hand, since P is singular we must have $\dim \mathcal{O}_P/(f,g) \geq 2$, and we conclude that $y = tx$ intersects $\mathcal{C}_g$ at P with multiplicity 2 if $t \neq \pm 1$, and with multiplicity 3 if $t = \pm 1$. This shows that $\mathcal{C}_g$ has exactly two tangents in P.

Proof. Let $R_i = \mathcal{O}_{P_i}/I$. The natural injection $R \longrightarrow \mathcal{O}_i$ induces a ring homomorphism $\lambda : R/I \longrightarrow R_1 \oplus \cdots \oplus R_d$. The proof that λ is injective generalizes from the special case discussed in Lemma 5.4.4; the proof that λ is surjective is more difficult: see Fulton, p. 56. ☐

Let us finally observe a connection between the valuations on local rings and multiplicity:

Proposition 5.4.6. *Let P be a nonsingular point on $\mathcal{C}_f$, and let $v_{P,f}$ be the valuation on the local ring $\mathcal{O}_P(\mathcal{C}_f)$. Then $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = v_{P,f}(g)$.*

Bezout's Theorem

Now we can formulate

Theorem 5.4.7 (Bezout's Theorem)**.** *Let K be an algebraically closed field. Let $\mathcal{C}_f : f(x,y) = 0$ and $\mathcal{C}_g : g(x,y) = 0$ be two plane algebraic projective curves without common components. Then*

$$\sum I(P, \mathcal{C}_f \cap \mathcal{C}_g) = (\deg f)(\deg g).$$

Note that $I(P, \mathcal{C}_f \cap \mathcal{C}_g) > 0$ if and only if P is a point of intersection, hence the sum is actually only over such points.

Bezout's Theorem is very easy if one of the curves is a line; if one of the curves is a conic, there is also an elementary proof exploiting the parametrization of the conic. For the general case, one has to work hard, however.

Bezout's theorem has lots of nice corollaries, of which we only mention the most simple ones:

Corollary 5.4.8. *Singular conics are degenerate (reducible, i.e., a pair of lines).*

Proof. Let P be a singular point on the conic $\mathcal{C}$. Let $Q \neq P$ be another point on the conic. Then the line PQ intersects $\mathcal{C}$ with multiplicity $\geq m_P(\mathcal{C}) \geq 2$ in P and with multiplicity ≥ 1 in Q; this is only possible if $\mathcal{C}$ contains the line PQ as a component. $\square$

Corollary 5.4.9. *Irreducible cubics have at most one singular point.*

Proof. Assume that the cubic $\mathcal{C}$ has two singular points P and Q. Then the line PQ intersects $\mathcal{C}$ with multiplicity ≥ 2 in P and Q; thus the line PQ intersects $\mathcal{C}$ with multiplicity ≥ 4, which is only possible if PQ is a component of $\mathcal{C}$. But then $\mathcal{C}$ is reducible. $\square$

Corollary 5.4.10. *A curve of degree n with a point of multiplicity n consists of n lines going through P.*

Proof. Let $\mathcal{C}_g$ be an irreducible component of f (this means $g \mid f$, and g is irreducible). Let Q be any point on $\mathcal{C}_g \subseteq \mathcal{C}_f$ different from P. By the above argument, the line PQ is a component of $\mathcal{C}_g$, and since $\mathcal{C}_g$ is irreducible, we must have $\mathcal{C}_g = PQ$. Thus every irreducible component of f is a line, and since $\deg f = n$, we conclude that $\mathcal{C}_f$ consists of n lines (counted with multiplicity). $\square$

Singularities and the Genus

The last few results on singular curves of low degree can be generalized easily using the inequality $I(P, \mathcal{C}_f \cap \mathcal{C}_g) \geq m_P(\mathcal{C}_f) m_P(\mathcal{C}_g)$.

Proposition 5.4.11. *Let $\mathcal{C}$ be a curve of degree d in the complex plane, without multiple components. Then*

$$\sum_P m_P(C) \cdot (m_P(C) - 1) \leq d(d-1).$$

In particular, $\mathcal{C}$ has at most $\frac{d(d-1)}{2}$ singular points.

Proof. Let $\mathcal{C} : F(X, Y, Z) = 0$; not all three partials can vanish everywhere (otherwise F would be constant), so assume that $F_X \neq 0$, hence $\deg F_X = \deg F - 1$.

Consider the intersection of the curves $\mathcal{C}$ and $\mathcal{D} : F_X(X, Y, Z) = 0$. Since $\mathcal{C}$ and $\mathcal{D}$ do not have a common component (otherwise $\mathcal{C}$ would have multiple compoenents), there are at most $d(d-1)$ points of intersection, and we have $\sum I(P, \mathcal{C} \cap \mathcal{D}) = d(d-1)$.

Let $P \in \mathcal{C} \cap \mathcal{D}$; if P is singular, then $m_P(\mathcal{C}) = m_P(\mathcal{D}) + 1$, and we get $\sum I(P, \mathcal{C} \cap \mathcal{D}) \geq \sum m_P(\mathcal{C})(m_P(\mathcal{C}) - 1)$, where the sum on the right is over all singular points. Thus we find $\sum m_P(\mathcal{C})(m_P(\mathcal{C}) - 1) \leq d(d-1)$ as claimed.

Since only singular points contribute to the sum on the left, and since $m_P(\mathcal{C}) \geq 2$ for such points, there can be at most $\frac{d(d-1)}{2}$ singular points on $\mathcal{C}$. $\square$

The inequalitites in Prop. 5.4.11 cannot be improved in general: let $\mathcal{C}$ be the union of d distinct lines, no three of which have a common point of intersection. Then there are exactly $\binom{d}{2}$ points of intersection, and these are all singular with multiplicity 2 (check this!).

If the curve in question is irreducible, Prop. 5.4.11 can be sharpened:

Proposition 5.4.12. *Irreducible curves of degree d can have at most $\frac{(d-1)(d-2)}{2}$ singularities.*

Make sure you understand why these results have the following corollaries:

- A conic without multiple components has at most one double point.
- An irreducible conic is smooth.
- A cubic without multiple components has at most three double points.
- An irreducible cubic has at most one double point.
- A quartic without multiple components has at most 6 double points.
- An irreducible quartic has at most 3 double points.

You should also be able to construct curves for which these bounds are attained.

It is also true that curves of degree d with $\frac{(d-1)(d-2)}{2}$ singularities can always be parametrized. More generally, let $\mathcal{C}$ be an irreducible plane algebraic curve with at most double points as singularities. Let d denote the degree of $\mathcal{C}$ and r the number of double points. Then

$$g = \frac{(d-1)(d-2)}{2} - r$$

is called the genus of $\mathcal{C}$.

Our results above imply that $g \geq 0$; note that $g = 0$ for irreducible conics and singular cubics, and that $g = 1$ for smooth cubics.

The main property of the genus is

Theorem 5.4.13. *The genus is invariant under birational transformations.*

This is a deep and surprising fact; note that the degree and the number of singular points do change under birational transformations.

For example, the parametrization of the unit circle is a birational transformation changing the degree 2 of the circle into the degree 1 of the line; but both curves have genus 0. Similarly, parametrizations of singular cubics map a curve with degree 3 and one double point into a smooth line of degree 1.

As a corollary we see that curves of genus ≥ 1 cannot be properly parametrized, since there is no birational transformation from a curve of genus ≥ 1 to a line. Hilbert and Hurwitz have shown that curves of genus 1 over algebraically closed fields always can be parametrized.

5.5 Proofs

The proof will use a couple of lemmas. We will start with

Lemma 5.5.1. *Let $R = K[x, y]$ be a polynomial ring in two variables over some field K. Then, for any ideal I in R, the quotient ring R/I is a K-vector space.*

Proof. This is because R is a vector space (it has basis $\{1, x, y, x^2, xy, y^2, \ldots\}$ and because I is a subspace of R: it is closed under addition of vectors and under scalar multiplication by $K \subset R$. $\square$

Lemma 5.5.2. *Consider the ideal $I = (x, y)$ in $R = K[x, y]$. Then*

$$\dim_K K[x, y]/I^n = \frac{n(n+1)}{2}.$$

Proof. We claim that $B = \{1, x, y, x^2, xy, y^2, \ldots, x^{n-1}, x^{n-2}y, \ldots, y^{n-1}\}$ is a K-basis for $V = K[x, y]/I^n$. First let us show that these elements generate V. Given any polynomial f, we can reduce it modulo I^n by omitting any term $x^a y^b$ with $a + b \ge n$. The reduced polynomial is then a K-linear combination of elements in B.

Next we have to show that the elements in B are linearly independent. Assume therefore that $\sum_{i+j<n} a_{ij} x^i y^j \in I^n$. This means that $\sum_{i+j<n} a_{ij} x^i y^j = \sum_{i+j \ge n} b_{ij} x^i y^j$ for suitable $b_{ij} \in K$. But then the difference of both sides is the zero polynomial, and since there cannot occur any cancellation, we must have $a_{ij} = 0$. $\square$

Let $\mathcal{O}_P(\mathbb{A}^2)$ be the ring of all rational functions $g \in K(X, Y)$ such that $g = \frac{a}{b}$ with $b(P) \ne 0$. We clearly have $K[X, Y] \subseteq \mathcal{O}_P(\mathbb{A}^2)$. The map $\mathcal{O}_P(\mathbb{A}^2) \longrightarrow \mathcal{O}_P(\mathcal{C}_f); g \longmapsto g + (f)$ is well defined with kernel $(f)\mathcal{O}_P(\mathbb{A}^2)$.

Corollary 5.5.3. *We have $K[X, Y]/(I^n, f) \simeq \mathcal{O}_P(\mathbb{A}^2)/(I^n, f)$ for any polynomial $f \in K[X, Y]$.*

Proof of Thm. 5.4.1. Let $\mathcal{O} = \mathcal{O}_P(\mathcal{C}_f)$ and $\mathfrak{m} = \mathfrak{m}_P(\mathcal{C}_f)$. The exact sequence

$$0 \longrightarrow \mathfrak{m}^n/\mathfrak{m}^{n+1} \xrightarrow{f} \mathcal{O}/\mathfrak{m}^{n+1} \xrightarrow{g} \mathcal{O}/\mathfrak{m}^n \longrightarrow 0$$

shows that $\dim \mathfrak{m}^n/\mathfrak{m}^{n+1} = \dim \mathcal{O}/\mathfrak{m}^{n+1} - \dim \mathcal{O}/\mathfrak{m}^n$, hence it is sufficient to prove that

$$\dim \mathcal{O}/\mathfrak{m}^n = n \cdot m_P(\mathcal{C}_f) + s$$

for some constant s and all $n \ge m_P(\mathcal{C}_f)$.

We now assume that $P = (0,0)$; then $\mathfrak{m} = I\mathcal{O}$, where $I = (X, Y)$ is an ideal in $R = K[X, Y]$, and $\mathfrak{m}^n = I^n\mathcal{O}$. Now

$$R/(I^n, f) \simeq \mathcal{O}_P(\mathbb{A}^2)/(I^n, f) \simeq \mathcal{O}_P/I^n\mathcal{O} = \mathcal{O}/\mathfrak{m}^n.$$

In fact, the first isomorphism is Corollary 5.5.3, and the second is induced by the map $g + (I^n, f) \longmapsto (g + (f)) + I^n$. Thus we have to compute the dimension of $R/(I^n, f)$.

Let $m = m_P(\mathcal{C}_f)$. Then the Taylor expansion of f around $P = (0,0)$ does not have any terms of degree $< m$, hence $f \in I^m \setminus I^{m+1}$. Moreover we have $fg \in I^n$ whenever $g \in I^{n-m}$. Thus multiplication by f induces a K-linear map

$$\psi : R/I^{n-m} \longrightarrow R/I^m$$

(not a ring homomorphism, obviously, since $gh + I^{n-m}$ gets mapped to $ghf + I^n$, which is not equal to $(gf + I^n)(hf + I^n)$). We also have the projection

$$\pi : R/I^n \longrightarrow R/(I^n, f),$$

which of course is surjective. We now claim that the sequence

$$0 \longrightarrow R/I^{n-m} \xrightarrow{\ \psi\ } R/I^n \xrightarrow{\ \pi\ } R/(I^n, f) \longrightarrow 0$$

is exact. In fact, let $g + I^n \in \ker \pi$. Then $g \in (I^n, f)$, hence there exists a polynomial $h \in I^n$ such that $g + h \in (f)$; this implies $g + h = af$ for some $a \in R$, and now $\psi(a + I^{n-m}) = af + I^n = (g + h) + I^n = g + I^n$. Conversely, $\operatorname{im} \psi \subseteq \ker \pi$ since $\pi(af + I^n) = af + (I^n, f) = 0 + (I^n, f)$. Finally, injectivity of ψ is easily established: if $af \in I^n$, then $f \in I^m \setminus I^{m+1}$ shows that $a \in I^{n-m}$. In order to see this, write $a = a_0 + a_1 + \ldots + a_i$, where a_k is homogeneous of degree k, and $f = f_m + F_m$, where $f_m \neq 0$ is homogeneous of degree m, and where $F_m \in I^{m+1}$. Now $af = a_0 f_m +$ terms of degree $> m$; thus if $n > m$, then $a_0 = 0$. Next $af = a_1 f_m +$ terms of degree $> m+1$; thus if $n > m+1$, then $a_1 f_m = 0$ and therefore $a_1 = 0$. Continuing this way we find that $a_0 = a_1 = \ldots = a_{n-m-1} = 0$.

Now Lemma 5.5.2 tells us the dimensions of the first two terms in the exact sequence; this gives

$$\dim_K R/(I^n, f) = nm - \frac{m(m-1)}{2}$$

for all $n \ge m$. □

Corollary 5.5.4. *If $\mathcal{O}_P$ is a discrete valuation ring, then $m_P(\mathcal{C}_f) = 1$.*

In fact, the theorem shows that $m_P(\mathcal{C}_f) = \dim \mathfrak{m}^n/\mathfrak{m}^{n+1}$. Now $\mathfrak{m} = (t)$ for some $t \in \mathcal{O}_P$, hence the elements $g \in \mathfrak{m}^n$ are multiples of t^n, hence $\mathfrak{m}^n = t^n K \oplus \mathfrak{m}^{n+1}$ as K-vector spaces. This implies $\mathfrak{m}^n/\mathfrak{m}^{n+1} \simeq t^n K$, hence $\dim \mathfrak{m}^n/\mathfrak{m}^{n+1} = 1$.

Proof of Thm. 5.4.3. Let us first see that $I(P, \mathcal{C}_f \cap \mathcal{C}_g) = \dim_K \frac{\mathcal{O}_P}{(f,g)}$ has these properties. Since $I(P, \mathcal{C}_f \cap \mathcal{C}_g)$ only depends on the ideal (f,g) in $\mathcal{O}_P$, properties 2., 4., and 7. are clear. Similarly, affine coordinate changes induce isomorphisms of local rings, which gives 3. The fact that $I(P, \mathcal{C}_f \cap \mathcal{C}_g)$ is finite if $\mathcal{C}_f$ and $\mathcal{C}_g$ do not have a common component is a special case of Bezout's theorem.

We may now assume that $P = (0,0)$, and that all the components of $\mathcal{C}_f$ and $\mathcal{C}_g$ pass through P.

to be completed. □

Exercises

5.1 Let $\mathcal{C}$ be the union of two distinct lines in $\mathbb{P}^2K$. Show that the point of intersection is singular.

5.2 Let $\mathcal{C}$ be the union of three distinct lines in $\mathbb{P}^2K$. Show that the three points of intersection are singular, and that they have multiplicity 2.

5.3 Generalize the last exercise to unions of d lines, no three of which go through a single point.

5.4 Let $\mathcal{C}$ be the union of d distinct lines through a point P. Show that $m_P(\mathcal{C}) = n$.