Chapter 14

Local Rings

Here's what we know so far: given a plane affine algebraic curve $\mathcal{C}_f : f(x,y) = 0$ defined over K, we have constructed the coordinate ring $K[\mathcal{C}_f] = K[X,Y]/(f)$; polynomial maps $\mathcal{C}_f \longrightarrow \mathcal{C}_g$ between two curves then correspond to K-algebra homomorphisms $K[\mathcal{C}_g] \longrightarrow K[\mathcal{C}_f]$.

Now the problem is that many of the maps between algebraic curves that we have encountered so far (think of the parametrization of the unit circle, which is a map from the line to the circle) are not polynomial but rational, i.e., quotients of polynomials. Such maps will not induce K-algebra homomorphisms between coordinate rings becaus quotients of polynomials live in the field $K(X,Y)$ of rational functions rather than in $K[X,Y]$.

14.1 Function Fields

Now recall that a curve $\mathcal{C}_f$ is irreducible (as an algebraic variety) if and only if f is prime in $K[X,Y]$; thus f is irreducible if and only if its coordinate ring $K[\mathcal{C}_f]$ is a domain. Now domains have quotient fields; thus we can define, for irreducible curves, the function field $K(\mathcal{C}_f)$ as the quotient field of $K[\mathcal{C}_f] = K[X,Y]/(f)$. Its elements are represented by quotients $\frac{p}{q}$ of polynomials, where we are allowed to change p and q modulo f.

If $\mathcal{C}_f : Y = 0$ is a line, then $K[\mathcal{C}_f] \simeq K[X]$, hence its function field $K(\mathcal{C}_f) = K(X)$ is the field of rational functions.

The function field of more complicated curves are not as simple. Consider e.g. the function field of the unit circle defined by $f(X,Y) = X^2 + Y^2 - 1 = 0$, and consider the element $g(x,y) = \frac{1-x}{y} = \frac{X-1}{Y} + (f) \in K(\mathcal{C})$ (here and in the following, we will often use the abbreviation $x = X + (f)$). This function is defined for all points P on the unit circle except at $P = (\pm 1, 0)$. Note, however, that

$$\frac{1-x}{y} = \frac{(1-x)y}{y^2} = \frac{(1-x)y}{1-x^2} = \frac{y}{1+x},$$

hence the rational function $\frac{1-x}{y}$ is also defined at $P = (1, 0)$ and has the value 0 there!

The precise definition is as follows: an element $g \in K(\mathcal{C})$ is said to be defined at a point $P \in \mathcal{C}_f$ if $g = a/b$ for $a, b \in K[\mathcal{C}]$ and $b(P) \neq 0$. In the example above, g is defined at points with $y \neq 0$ since $g = \frac{x-1}{y}$, and at $P = (1, 0)$ since $g = \frac{y}{1+x}$.

The reason for this strange behavior is that the coordinate ring $K[\mathcal{C}]$ of the unit circle is not a unique factorization domain: we have $y^2 = (1-x)(1+x)$, and the factors y, $1-x$, $1+x$ are all irreducible, but, as the factorization shows, not prime.

Now recall that the unit circle can be parametrized; the parametrization

$$K \longrightarrow \mathcal{C}_f : t \longmapsto (x, y) \quad \text{with} \quad x(t) = \frac{1-t^2}{1+t^2},\ y(t) = \frac{2t}{1+t^2}$$

defined for all $t \in K \setminus \{\pm i\}$ actually allows us to define a ring homomorphism $\phi : K(\mathcal{C}_f) \longrightarrow K(t)$ via

$$\frac{a(x, y)}{b(x, y)} + (f) \longmapsto \frac{a(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})}{b(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})}.$$

In fact, since $f(x, y) = x^2 + y^2 - 1$ gets sent to 0, this is well defined.

The geometric parametrization also tells us that $t = \frac{y}{x+1}$, and in fact the element $\frac{y}{x+1} + (f)$ has image t, which means that ϕ is surjective. Actually the map $\psi : t \longrightarrow \frac{y}{x+1} + (f)$ defines a ring homomorphism $K(t) \longrightarrow K(\mathcal{C}_f)$, and the composition $\psi \circ \phi$ is the identity: this is because substituting $\frac{1-t^2}{1+t^2}$ for x and then substituting $\frac{y}{x+1}$ for t is the same thing as replacing x by

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

and a similar calculation shows that y gets replaced by y. You can also check that $\phi \circ \psi$ is the identity map, and this shows that ϕ and ψ are isomorphisms.

Thus although the coordinate rings of the parabola and the unit circle are different, their function fields are isomorphic. We will later see that this is connected with the fact that both can be parametrized.

The isomorphism between the function fields is not an accident: birational maps $\mathcal{C}_f \longrightarrow \mathcal{C}_g$ induce isomorpisms between the corresponding function fields (we will return to this later).

14.2 Noetherian Rings

Commutative algebra is the branch of mathematics dealing with the theory of commutative rings. It is not particularly difficult: the main problem is the horrifying amount of definitions one encounters here. Fields are relatively simple objects: they only have two ideals, namely (0) and (1). Rings, on the other hand, have usually lots of ideals, and there is a wealth of particular rings defined in terms of properties that their ideals have or do not have. Examples you already know include domains (rings without zero divisors) and principal ideal domains (rings in which every ideal is principal).

Below, we will have to introduce a lot of other classes of rings: local rings, discrete valuation rings, and Noetherian rings.

Recall that a Noetherian ring is a (commutative) ring with 1 in which every ascending chain of ideals terminates. In other words: if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ is an ascending chain of ideals, then there is some index n such that $I_n = I_{n+1} = \ldots$.

We also know:

Proposition 14.2.1. *A ring R is Noetherian if and only if every ideal in R is finitely generated.*

Corollary 14.2.2. *Principal ideal domains are Noetherian.*

As an example of a ring that is not Noetherian, consider the polynomial ring $R = \mathbb{Q}[X_1, X_2, X_3, \ldots]$ of infinitely many variables. The ideal $(X_2, X_3, \ldots)$ in R is not finitely generated; alternatively, the sequence

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \ldots$$

is an ascending chain of ideals that does not terminate. Note that the quotient field $K = \mathbb{Q}(X_1, X_2, X_3, \ldots)$ is Noetherian (any field is); since R is a subring of K, this shows that not every subring of a Noetherian ring is Noetherian. Actually, even the 'sandwich argument' does not work for Noetherian rings: we have $\mathbb{Q} \subset R \subset K$ with $\mathbb{Q}$ and K Noetherian, and yet R is not.

A big source of Noetherian rings are polynomial rings $K[X_1, \ldots, X_n]$:

Theorem 14.2.3 (Hilbert's Basis Theorem)**.** *If R is Noetherian, then so is $R[X]$.*

This is again a basic result in commutative algebra. Since $\mathbb{Z}$ and K are Noetherian, so are $\mathbb{Z}[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$.

A much simpler observation is

Proposition 14.2.4. *If I is an ideal in a Noetherian ring R, then R/I is Noetherian.*

Proof. Assume that J is an ideal in R/I. Define $A = \{r \in R : r + I \in J\}$ This is an ideal in R, hence it is finitely generated, say $A = (a_1, \ldots, a_m)$. We claim that $J = (a_1 + I, \ldots, a_m + I)$. Let $a + I \in J$; then $a \in A$, hence $a = r_1 a_1 + \ldots + r_m a_m$ for $r_i \in R$, hence $a + I = r_1(a_1 + I) + \ldots + r_m(a_m + I)$. □

14.3 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 14.3.1. *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 $P \in \mathcal{C}_f(K)$. □

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 14.3.2. *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. □

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

Proposition 14.3.3. *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 14.3.4. *We have $K[\mathcal{C}_f] = \bigcap_P \mathcal{O}_P(\mathcal{C}_f)$.*

Proof. 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).

14.4 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 14.4.1. *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 $R/\ker\phi \simeq \operatorname{im}\phi$. 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.

14.5 Discrete Valuation Rings

Proposition 14.5.1. *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 14.5.2. *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 $g \in (x - a, y - b)$. □

Theorem 14.5.3. *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 14.4.2 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 $\mathcal{O}_P(\mathcal{C}_f)$.