LECTURE 16, MONDAY APRIL 12, 2004

FRANZ LEMMERMEYER

1. Function Fields

Let K be an algebraically closed field and $f \in K[X,Y]$ an irreducible polynomial. The corresponding coordinate ring $K[\mathcal{C}] = K[X,Y]/(f)$ is a domain, hence has a quotient field $K(\mathcal{C})$ called the **function field** of $\mathcal{C}$. The function field of a line is, as we have seen above, just the field $K(X)$ of rational functions, and the same is true for the function field of the parabola.

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

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

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

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

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).

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. I am well aware of the fact that this

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 $I_n = I_{n+1} = \ldots$.

In order to give examples, we now prove

Proposition 2.1. *A ring R is Noetherian if and only if every ideal in R is finitely generated.*

Proof. Assume first that R is Noetherian and let I be an ideal of R. We have to show that I is finitely generated, i.e., that there exist elements $a_1, \ldots, a_n$ such that $I = (a_1, \ldots, a_n)$. If $I = (0)$, we are done. If $I \neq (0)$, then there is some $a_1 \in I$. If $I = (a_1)$, then we are done; if not, then there is some $a_2 \in I \setminus (a_1)$. If $I = (a_1, a_2)$, we are done, and if not, then there is some $a_3 \in I \setminus (a_1, a_2)$. We claim that this process must terminate. In fact, if it does not, then we can continue in this way and get an ascending chain of ideals $(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \ldots$. This contradicts the fact that R is Noetherian.

Conversely, assume that every ideal in R is finitely generated, and let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be an ascending chain of ideals. Let I denote the union of all the I_j. Then I is an ideal: for example, if $a, b \in I$, then $a \in I_j$, $b \in I_k$, hence $a, b \in I_{j+k}$ and therefore $a + b \in I_{j+k} \subseteq I$. Since every ideal in R is finitely generated, there are elements $a_i \in R$ with $I = (a_1, \ldots, a_n)$. This means that $a_1 \in I_{i_1}$, $\ldots$, $a_n \in I_{i_n}$ for indices $i_1, \ldots i_n$. Put $m = \max\{i_1, \ldots i_n\}$; then $a_1, \ldots, a_n \in I_m$, hence $I = (a_1, \ldots, a_m) \subseteq I_m$. But since $I_m \subseteq I$, this implies $I_m = I$. □

Corollary 2.2. *Principal ideal domains are Noetherian.*

This is because every ideal is principal, that is, generated by one element, and in particularly finitely generated. Thus fields or $\mathbb{Z}$ 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 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 $\mathbb{Q}$ are Noetherian, so are $\mathbb{Z}[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$.

A much simpler observation is

Proposition 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 $a + I = r_1(a_1 + I) + \ldots + r_m(a_m + I)$. □

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 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 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 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 $b(P) \ne 0$. 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 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 $(X - r, Y - s)$ 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 $b(Q) \ne 0$, and $b \in J_g$: contradiction.

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

Here we have used a special case of

Theorem 3.5 (Hilbert's Nullstellensatz)**.** *Let K be an algebraically closed field; then any maximal ideal in $K[X_1, \ldots, X_n]$ has the form $(X_1 - a_1, \ldots, X_n - a_n)$.*

It seems that you cannot avoid the Nullstellensatz for long when you start doing algebraic geometry using coordinate rings and function fields.

We also have used the fact that every ideal is contained in some maximal ideal. This is a consequence of Zorn's Lemma, which we discuss next (I didn't do this in class).

4. Interlude I: Zorn's Lemma

The ring $R = 0$ does not have a prime ideal, or even a maximal ideal: the only ideal is (0), and $R/(0) \simeq R$ is not a field since it only has one element. Are there any other rings without prime ideals? It turns out that the answer is no, at least if you believe in the axiom of choice, or in its incarnation as Zorn's Lemma.

Let Σ be a partially ordered set, that is, a set equipped with a transitive relation $<$ that allows us to compare certain (not necessarily all; that's why Σ is *partially* ordered). For example, the set $\mathbb{N}$ is partially ordered with respect to divisibility: we define $a < b$ if $a \mid b$. Then $2 < 6$ but 2 and 3 cannot be compared since $2 \nmid 3$ and $3 \nmid 2$. Similarly, the set $\operatorname{Spec} R$ of all prime ideals in R is partially ordered with respect to inclusion. In $\operatorname{Spec} \mathbb{Z}$, we have $(0) \subset (p)$ for all primes p, whereas the maximal prime ideals cannot be compared.

A maximal element of Σ is any $m \in \Sigma$ such that there is no $s \in \Sigma$ with $m < s$. A subset $S \subseteq \Sigma$ is totally ordered if for every pair $s, s' \in S$ we have $s \le s'$ or $s' \le s$. An upper bound of a totally ordered subset S of Σ is any $b \in S$ such that $s \le b$ for all $s \in S$. We call Σ inductively ordered if every non-empty totally ordered subset S of Σ has an upper bound.

Lemma 4.1 (Zorn's Lemma)**.** *Let Σ be a non-empty inductively ordered set. Then Σ has a maximal element.*

Proof. Zorn's Lemma is equivalent to the axiom of choice; here's the basic idea: since Σ is non-empty, there is an $s_1 \in \Sigma$. If s_1 is maximal, we're done, otherwise there is an $s_2 \in \Sigma$ with $s_1 < s_2$. If s_2 is maximal, we're done, if not then there is an $s_3 \in \Sigma$ such that $s_2 < s_3$. Continuing this way, we get a sequence of elements $s_1 < s_2 < s_3 < \dots$ in Σ. This sequence is a totally ordered subset, so it has an upper bound, that is, there is a $b \in \Sigma$ such that $s_i \leq b$ for all $i \geq 1$. If b is not maximal, the game goes on: but since at each step I have to make a choice, and since there are possibly infinitely many choices to make, we have to invoke the axiom of choice to guarantee we can do it. □

What is Zorn's Lemma good for? For one thing, it allows us to prove the existence of maximal ideals in any nontrivial ring:

Proposition 4.2. *Let R be a ring and $\mathfrak{a} \neq R$ an ideal; then there exists a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.*

Proof. Let Σ be the set of ideals $\mathfrak{b} \neq R$ containing $\mathfrak{a}$, partially ordered by inclusion. Then $\Sigma \neq \varnothing$ since $\mathfrak{a} \in \Sigma$. If $\{\mathfrak{a}_i\}_{i \in I}$ is a totally ordered subset of Σ, then $\mathfrak{A} = \bigcup \mathfrak{a}_i$ is an ideal containing $\mathfrak{a}$; also, $\mathfrak{A} \neq R$ since otherwise $1 \in \mathfrak{A}$, so $1 \in \mathfrak{a}_i$ for some index i, and we would have $\mathfrak{a}_i = R$ contradicting the construction of Σ. This shows that $\mathfrak{A} \in \Sigma$, and this ideal is clearly an upper bound for $\{\mathfrak{a}_i\}_{i \in I}$. Thus we may apply Zorn's Lemma and find a maximal element $\mathfrak{m} \in \Sigma$: this is an ideal containing $\mathfrak{m}$ but not contained in any other ideal in R containing $\mathfrak{a}$ and $\neq R$.

We claim that $\mathfrak{m}$ is a maximal ideal (note that all we know that it is maximal under the additional assumption that $\mathfrak{a} \subseteq \mathfrak{m}$). Assume not; then there is an ideal $\mathfrak{b}$ such that $\mathfrak{m} \subsetneq \mathfrak{b} \subsetneq R$. But then $\mathfrak{a} \subseteq \mathfrak{m} \subseteq \mathfrak{b}$, hence $\mathfrak{b} \in \Sigma$, and we have a contradiction. □

5. 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 because adding a unit means you will get (1) as a result.

Proposition 5.1. *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 $\mathbb{Z}_{(p)}$. The common notion that contains both curves and rings such as $\mathbb{Z}$ is that of a scheme.

6. Discrete Valuation Rings

Consider the ring $R = \mathbb{Z}_{(p)}$ for some prime p. Every ideal in this ring has the form (p^a) for some $a \ge 0$. This means that

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

In particular this means that coordinate rings of curves are Noetherian.

Proposition 6.1. *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 $n \ge 0$ 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 $n \ge 0$.

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 $\mathfrak{a} \ne (1)$, 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 $n \ge 0$, in particular every ideal is finitely generated. □