6. Local rings

Our last topic in commutative algebra is local rings. I first went over the basic definitions, talked about Nakayama's Lemma and I plan to do discrete valuation rings and then more general valuation rings and then return to places in fields. All rings are commutative with 1. They might not be Noetherian.

6.1. **Basic definitions and examples.**

Definition 6.1. A *local ring* is a ring R with a unique maximal ideal $\mathfrak{m}$.

Proposition 6.2. *A ring is local iff the nonunits form an ideal.*

Proof. Suppose first that R is local with maximal ideal $\mathfrak{m}$. Let x be any element not in $\mathfrak{m}$. Then x must be a unit. Otherwise, x generates an ideal (x) which is contained in a maximal ideal other than $\mathfrak{m}$.

Conversely, suppose that R is a ring in which the nonunits form an ideal I. Then every ideal in R must be contained in I since ideals cannot contain units. □

Example 6.3. An example is $\mathbb{Z}/(p)$, the integers localized at the prime ideal (p). Recall that $R_{\mathfrak{p}} = S^{-1}R$ is the set of all equivalence classes of fractions a/b where $a \in R$ and $b \in S$ where S is the complement of $\mathfrak{p}$. When R is an integral domain, $R_{\mathfrak{p}}$ is contained in the quotient field QR. So, it is easier to think about:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \text{ s.t. } p \nmid b \right\}$$

This is a local ring with unique maximal ideal

$$\mathfrak{m} = \left\{ \frac{a}{b} \in \mathbb{Q} \; s.t. \; p|a, p \nmid b \right\}$$

This is the unique maximal ideal since all of the other elements are clearly units. The quotient $\mathbb{Z}_{(p)}/\mathfrak{m}$ is isomorphic to $\mathbb{Z}/p$ although this is not completely trivial.

More generally we have:

Proposition 6.4. *If R is a ring and $\mathfrak{p}$ is a prime ideal then $R_{\mathfrak{p}} = S^{-1}R$ is a local ring with maximal ideal $S^{-1}\mathfrak{p}$.*

6.2. **Nakayama's Lemma.** You probably already know this but it is an very useful result which is also very easy to prove. There are two equivalent versions.

Lemma 6.5 (Nakayama's Lemma, version 1)**.** *Suppose that R is a local ring and M is a f.g. R-module. If $\mathfrak{m}M = 0$ then $M = 0$.*

Lemma 6.6 (Nakayama's Lemma, version 2)**.** *Suppose that R is a local ring and E is a f.g. R-module and $F \subseteq E$ is a submodule. If $E = F + \mathfrak{m}E = 0$ then $E = F$.*

First I showed that these are equivalent. The first version is obviously a special case of the second version: just let $F = 0$. To prove the second given the first let $M = E/F$. Then $E = F+\mathfrak{m}E$ implies that $M = \mathfrak{m}M$ which implies $M = E/F = 0$ which is the same as $E = F$.

Proof of Nakayama, 1st version. This will be by induction on the number of generators. If this number is zero, then $M = 0$ so the lemma is true. So, suppose that $x_1, \cdots, x_s$ is a minimal set of generators for M and $s \geq 1$. Since $x_s \in M = \mathfrak{m}M$, there exist $a_1, \cdots, a_s \in \mathfrak{m}$ so that

$$x_s = a_1x_1 + \cdots + a_sx_s$$

This gives:

$$(1 - a_s)x_s = a_1 + \cdots + a_{s-1}x_{s-1}$$

But $1-a_s$ is invertible since it is not an element of $\mathfrak{m}$ (if $1-a_s \in \mathfrak{m}$ then we would get $1 - a_s + a_s = 1 \in \mathfrak{m}$ which is not possible). Therefore,

$$x_s = (1 - a_s)^{-1}(a_1x_1 + \cdots + a_{s-1}x_{s-1})$$

which implies that $x_1, \cdots, x_{s-1}$ generate M. So, $M = 0$ by induction on s. □

Remark 6.7. Note that $M/\mathfrak{m}M$ is an $R\mathfrak{m}$-module. Since $R/\mathfrak{m}$ is a field (called the *residue field* of R), $M/\mathfrak{m}M$ is a vector space over the residue field. If $f : M \to N$ is a homomorphism of R-modules then we get an induced linear mapping

$$f_* : M/\mathfrak{m}M \to N/\mathfrak{m}N$$

given by $f_*(x + \mathfrak{m}M) = f(x) + \mathfrak{m}N$ (or $f_*(\overline{x}) = \overline{f(x)}$ if $\overline{x}$ denotes $x + \mathfrak{m}M$). This defines a functor from the category of R-modules to the category of vector spaces over $R/\mathfrak{m}$.

Definition 6.8. One definition of the *dimension* of a local ring R is the vector space dimension of $\mathfrak{m}/\mathfrak{m}^2$:

$$\dim R = \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$$

Proposition 6.9. *$x_1, \cdots, x_n$ are generators for the R-module M if and only if their images $\overline{x}_1, \cdots, \overline{x}_n$ span the vector space $M/\mathfrak{m}M$.*

Proof. ($\Rightarrow$) This direction is clear. Every element $x \in M$ can be written as $x = \sum a_i x_i$. So, any element $\overline{x} = x + \mathfrak{m}M$ of $M/\mathfrak{m}M$ can be written as $\overline{x} = \sum \overline{a}_i \overline{x}_i$.

(*neht*) Let N be the submodule of M generated by $x_1, \cdots, x_n$. If $\overline{x}_1, \cdots, \overline{x}_n$ span $M/\mathfrak{m}M$ then $N + \mathfrak{m}M = M$. Then $N = M$ by Nakayama. □

Corollary 6.10. *$x_1, \cdots, x_n$ is a minimal set of generators for M iff $\overline{x}_1, \cdots, \overline{x}_n$ form a basis for the vector space $M/\mathfrak{m}M$.*

Theorem 6.11. *Any finitely generated R-module M is projective if and only if it is free (isomorphic to R^n).*

Proof. It is clear that every free module is projective. So, suppose that M is projective. Let $x_1, \cdots, x_n$ be a minimal set of generators for M. Then we get an epimorphism $\phi : R^n \to M$ sending the i-th generator of R^n to x_i. Since M is projective by assumption, there is a section $s : M \to R^n$ of this homomorphism. I.e., $\phi \circ s = id_M$. This gives the following diagram:

$$\begin{array}{ccccc} M & \xrightarrow{s} & R^n & \xrightarrow{\phi} & M \\ \downarrow & & \downarrow & & \downarrow \\ M/\mathfrak{m}M & \xrightarrow{\overline{s}} & R^n\mathfrak{m}^n & \xrightarrow{\overline{\phi}} & M/\mathfrak{m}M \end{array}$$

Since $\phi \circ s$ is the identity on M, $\overline{\phi}/\overline{s}$ is the identity on $M.\mathfrak{m}M$. Therefore, $\overline{s} : M/\mathfrak{m}M \to R^n/\mathfrak{m}^n$ is a monomorphism. But $M/\mathfrak{m}M$ and $R^n/\mathfrak{m}^n$ have the same finite dimension over $R/\mathfrak{m}$. Therefore, $\overline{s}$ is an isomorphism. This implies that $s(M) + \mathfrak{m}^n = R^n$. By Nakayama this shows that $s(M) = R^n$. So, $M \cong R^n$ as we wanted to show. □

6.3. **Complete local rings.** If R is a local ring we get a sequence of ring homomorphisms:

$$\cdots \to R/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^n \to R/\mathfrak{m}^{n-1} \to \cdots \to R/\mathfrak{m}$$

The inverse limit $\lim_{\leftarrow} R/\mathfrak{m}^n$ is the set of all sequences $(a_n \in R/\mathfrak{m}^n)$ which are *compatible* in the sense that a_n maps to a_{n-1} under the homomorphism $R/\mathfrak{m}^n \to R/\mathfrak{m}^{n-1}$, i.e., $a_{n-1} = a_n + \mathfrak{m}^{n-1}$.

The inverse limit is defined by a universal condition. It is the universal object L with ring homomorphisms $f_n : L \to R/\mathfrak{m}^n$ so that the composition $L \to R/\mathfrak{m}^n \to R/\mathfrak{m}^{n-1}$ is f_{n-1}. In other words, given any other L' with homomorphisms $f'_n : L' \to R/\mathfrak{m}^n$, there exists a unique ring homomorphism $g : L' \to L$ so that $f_n \circ g = f'_n$ for all n. It is easy to see that the set of all compatible sequences (a_n) satisfies this universal property since $g(x) = (f'_n(x))$

Definition 6.12. R is a *complete* local ring if $R \cong \lim_{\leftarrow} R/\mathfrak{m}^n$.

Example 6.13. The *p-adic integers* $\mathbb{Z}_p$ form a complete local ring by definition. They are defined to by $\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$. I.e., it is the inverse limit of the sequence

$$\cdots \to \mathbb{Z}/p^n \to \mathbb{Z}/p^{n-1} \to \cdots \to \mathbb{Z}/p$$

In other words, $\mathbb{Z}_p$ is the set of all sequences (a_n) of integers a_n defined modulo p^n so that $a_n + p^{n-1}\mathbb{Z} = a_{n-1}$. There is a natural ring monomorphism $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ sending m to the sequence $(a_n = m)$ for all n. The unique maximal ideal is given by $a_1 = 0$, i.e., $\mathfrak{m}$ is the kernel of the epimorphism $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p$ given by $(a_n) \mapsto a_1$.

A typical element of $\mathbb{Z}_3$ has an infinite 3-nary expansion with digits $0, 1, 2$ to the left of the decimal place:

$$\cdots 2110220112.$$

p-adic integers do not have signs. They are all positive since, e.g.,

$$-1 = \cdots 2222222.$$

The maximal ideal is the set of all numbers with last digit equal to 0.

Problem: Show that there is a monomorphism of rings $\mathbb{Z}_{(p)} \hookrightarrow \mathbb{Z}_p$ which is not an epimorphism (since $\mathbb{Z}_p$ is a Cantor set and therefore uncountable whereas $\mathbb{Z}_{(p)}$ is countable, being a subset of $\mathbb{Q}$).

6.4. **Discrete valuation rings.** This is the last topic in commutative algebra.

6.4.1. *definition.* I gave two of the elementary definitions.

Definition 6.14 (1st definition)**.** A *discrete valuation ring* (DVR) is an integral domain R together with a mapping

$$v : QR^* \twoheadrightarrow \mathbb{Z}$$

called a *valuation* from the group of nonzero elements QR^* of the quotient field QR of R onto $\mathbb{Z}$ so that

(1) $v(ab) = v(a) + v(b)$ for all $a, b \in QR^*$
(2) $v(a + b) \geq \min(v(a), v(b))$ for all $a, b \in QR^*$
(3) $R^* = \{a \in QR^* \mid v(a) \geq 0\}$

I pointed out that the first conditions implies $v(1) = 0$ (since $v(1) = v(1) + v(1)$) and $v(a/b) = v(a) - v(b)$ (since $a = (a/b)b \Rightarrow v(a) = v(a/b) + v(b)$).

Example 6.15. Take $R = \mathbb{Z}_{(p)}$. Then $Q\mathbb{Z}_{(p)} = \mathbb{Q}$ and we can define

$$v_p : \mathbb{Q}^* \twoheadrightarrow \mathbb{Z}$$

by $v_p\left(\frac{a}{b}\right) = n$ where n is the number of times that p divides a/b. I.e.,

$$\frac{a}{b} = p^n \frac{c}{d}$$

where $p \nmid c$ and $p \nmid d$. It is easy to verify that the conditions are satisfied. We figured out in class that equality holds in (2) when $v(a) \neq v(b)$.

There is one thing I don't like about the first definition. The valuation is assumed to be defined outside of the original set R. The second definition restricts the valuation just to R^*.

Definition 6.16 (2nd definition)**.** A *DVR* is a domain R together with a mapping

$$v : R^* \twoheadrightarrow \{0, 1, 2, \cdots\}$$

so that

(1) $v(ab) = v(a) + v(b)$ for all $a, b \in R^*$
(2) $v(a + b) \geq \min(v(a), v(b))$ for all $a, b \in R^*$
(3′) $b|a \iff v(b) \leq v(a)$

Proposition 6.17. *These two definitions are equivalent.*

Proof. ($\Rightarrow$) If v is defined on QR^* we can just take the restriction of v to R^*. Then the only condition we need to check is $(3')$. If $b|a$ then $a = bc$ for some $c \in R^*$. So, $v(a) = v(b) + v(c) \geq v(b)$. Conversely, if $v(b) \leq v(a)$ then $v(a/b) = v(a) - v(b) \geq 0$.

($\Leftarrow$) Suppose we have v defined on R^*. Then we can extend it to QR^* by the equation

$$v\left(\frac{a}{b}\right) = v(a) - v(b)$$

This is well defined since $a/b = c/d$ implies $ad = bc$ which implies that

$$v(ad) = v(a) + v(d) = v(b) + v(c) = v(bc)$$
$$v(a) - v(b) = v(c) - v(d)$$

Conditions (1) is obvious. For condition (2):

$$\begin{aligned} v\left(\frac{a}{c} + \frac{b}{c}\right) = v\left(\frac{a+b}{c}\right) &= v(a+b) - v(c) \\ &\geq \min(v(a), v(b)) - v(c) \\ &= \min(v(a) - v(c), v(b) - v(c)) \\ &= \min\left(v(a/c), v(b/c)\right) \end{aligned}$$

For the last condition:

$$v(a/b) \geq 0 \iff v(a) \geq v(b) \iff b|a \iff a/b \in R$$

□

6.4.2. *properties.*

Proposition 6.18. *Suppose that R is a DVR with valuation v. Then*

1. *$a \in R$ is a unit iff $v(a) = 0$.*
2. *R is a local ring*
3. *$\mathfrak{m} = \{a \in R \,|\, v(a) \geq 1$ and $a \neq 0\}$*
4. *$\mathfrak{m} = (\pi)$ for any $\pi \in R$ so that $v(\pi) = 1$.*
5. *$\mathfrak{m}^n = (\pi^n)$.*

π is called the *uniformizer* of R.

Proof. For (1), a is a unit iff $a|1$ iff $v(a) \leq v(1) = 0$ iff $v(a) = 0$. This implies that the set of nonunits is $I = \{a \in R \,|\, v(a) \geq 0$ or $a = 0\}$. R is a local ring iff I is an ideal. But this is easy: I is closed under addition since

$$v(a+b) \geq \min(v(a), v(b)) \geq 1$$

and it is an ideal since, for any $a \in I, r \in R$ which are nonzero,

$$v(ra) = v(r) + v(a) \geq v(a) \geq 1$$

which implies $ra \in I$. Therefore, $I = \mathfrak{m}$ is the unique maximal ideal.

Now choose any $\pi \in R$ so that $v(\pi) = 1$. Then, π divides any element $a \in \mathfrak{m}$ since $v(\pi) \leq v(a)$. So, $\mathfrak{m} = (\pi)$.

Finally, it is clear that if π generates $\mathfrak{m}$ then π^n generates $\mathfrak{m}^n$. □

The converse to this is also true giving a 3rd definition of DVR:

Proposition 6.19. *If R is a local domain whose unique maximal ideal is principal, then R is a DVR.*

Proof. If π is a generator for $\mathfrak{m}$ then any nonzero element of R can be written uniquely as $\pi^n u$ where u is a unit. Then the valuation is given by $v(\pi^n u) = n$. □

6.4.3. *DVRs and Riemann surfaces.* The theorem is that there is a 1-1 correspondence between isomorphism classes of field extensions E of $\mathbb{C}$ of transcendence degree 1 and isomorphism classes of (compact) Riemann surfaces (complex curves). The points of the Riemann surface are given by the discrete valuations $v : E^* \twoheadrightarrow \mathbb{Z}$ associated to places in E which are DVRs.

I didn't prove this but I gave an example, the simplest possible example, which is $E = \mathbb{C}(X)$. This field corresponds to the Riemann sphere $S^2 = \mathbb{C} \cup \infty$. Any point $x_0 \in \mathbb{C}$ corresponds to the valuation $v_{x_0} : E^* \to \mathbb{Z}$ given by

$$v_{x_0}\left(\frac{f(X)}{g(X)}\right) = n$$

where n is the number of times that $X - x_0$ divides $f(X)/g(X)$. In other words,

$$\frac{f(X)}{g(X)} = (X - x_0)^n \frac{\phi(X)}{\psi(X)}$$

where $\phi(X), \psi(X)$ are not divisible by $X - x_0$. The condition that these are not divisible by $X - x_0$ is equivalent to the condition that $\phi(x_0) \neq 0$ and $\psi(x_0) \neq 0$. In other words, the function $f(X)/g(X)$ has a zero of order n at x_0. When $n < 0$, $f(X)/g(X)$ has a *pole* at x_0, i.e., $f(x_0)/g(x_0) = \infty$. The DVR is the set of all $f(X)/g(X)$ which does not have a pole at x_0. The maximal ideal is the set of all rational functions which are zero at x_0.

There is one other valuation on $E = \mathbb{C}(X)$ corresponding to the point at infinity. This should be the set of all rational functions $f(X)/g(X)$ which do not have a pole at ∞. This is equivalent to saying that $\deg(f) \leq \deg(g)$. So, the valuation at infinity is:

$$v_\infty(f(X)/g(X)) = \deg(g) - \deg(f).$$