Math 531

Notes from last time

- You do *not* need Zorn's lemma in anything we did yesterday. You *do* need Zorn's lemma to show that any ideal is contained in a maximal ideal.
- I made a slight error in the proof that the ascending chain condition implies that all ideals are finitely generated. I should have done this – let J be an ideal and let $\mathcal{S}$ be the set of all finitely generated ideals contained in J. Then this set has a maximal element and it must be J. Also, in general we will consider R to be an ideal of itself (we'll need this later). However, R is *not* considered to be a prime ideal of R.
- It is more standard to say that R is **locally principal** if $R_{\mathcal{P}}$ is a principal ideal domain for ever $\mathcal{P}$. This is equivalent to the definition I gave when R is Noetherian.

Some theorems from the book about localization. A quick note on prime ideals: we do not consider the whole ring R to be a prime ideal.

Lemma 4.1. *Let R be an integral domain. Let S be a multiplicative subset of R that does not contain 0. There is a bijection between the primes in R that do not intersect S and the primes in R_S.*

Proof. The idea was that for any prime $\mathcal{Q}$ in $S^{-1}R$, we know that $\mathcal{Q} \cap (R \cap S)$ is empty. Then, for any $\mathcal{P}$, we have that $S^{-1}R\mathcal{P}$ is a prime ideal in $S^{-1}R$. $\square$

Notation $S^{-1}R$ is often denoted as R_S.

Forming $S^{-1}R$ is called *localizing* R. We define a local ring to be a ring with only one maximal ideal, e.g. $\mathbb{Z}_{(p)}$ is a local ring.

Let's first show a weak unique factorization result that holds for all Noetherian rings.

Proposition 4.2. *(Poor man's unique factorization) Let R be a Noetherian ring and let I be an ideal in R. Then I has the property that there exist (not necessarily distinct) prime ideals $(\mathcal{P}_i)_{i=1}^n$ such that*

- *$\mathcal{P}_i \supset I$ for each i; and*
- $\displaystyle\prod_{i=1}^{n} \mathcal{P}_i \subset I$.

Proof. Let $\mathcal{S}$ be the set of ideals of R not having this property. Then $\mathcal{S}$ has a maximal element, call it I. We can assume I is not prime since prime ideals trivially have the desired property. Thus, there exist

$a, b \notin I$ such that $ab \in I$. The ideals $I + Ra$ and $I + Rb$ are larger than I, so must have prime ideals $\mathcal{P}_i$ and $\mathcal{Q}_j$ such that

$$\prod_{i=1}^{n} \mathcal{P}_i \subset I + Ra$$

with $\mathcal{P}_i \supset I + Ra \supset I$ and

$$\prod_{i=1}^{n} \mathcal{Q}_i \subset I + Rb$$

with $\mathcal{Q}_i \supset I + Rb \supset I$. Also, $(I + Ra)(I + Rb) \subset I$ so

$$\prod_{i=1}^{n} \mathcal{P}_i \prod_{i=1}^{n} \mathcal{Q}_i \subset I$$

and I does have the desired property after all. $\square$

There is no uniqueness at all here. Let's get a very, very weak uniqueness result for for local rings.

Proposition 4.3. *Let R be a local integral domain with maximal ideal $\mathcal{M}$. Then $\mathcal{M}^n \neq \mathcal{M}^{n+1}$ for $n \geq 1$.*

Proof. Since $\mathcal{M}^n \neq 0$ for any n, we may apply Nakayama's lemma below to $\mathcal{M}$ considered as an R-module. $\square$

Lemma 4.4. *(Nakayama's lemma) Let R be a local ring with maximal ideal $\mathcal{M}$ and let M be a finitely generated R-module. Suppose that $\mathcal{M}M = M$. Then $M = 0$.*

Proof. The proof is similar to that of the Cayley-Hamilton theorem. Let $m_1, \ldots, m_n$ generate M. Then $\mathcal{M}M$ will be the set of all sums $\sum_{j=1}^{n} a_j m_j$ where $a_j \in \mathcal{M}$. In particular, we can write

$$1 \cdot m_i = \sum_{j=1}^{n} a_{ij} m_j.$$

We form the matrix $T := I - [a_{ij}]$ as $n \times n$ matrix over A and treat as an endomorphism of M^n (as in Cayley-Hamilton). Then, as in Cayley-Hamilton $T(m_1, \ldots, m_n)^t = 0$ (i.e., T times the column vector with entries m_i), which means that $UT(m_1, \ldots, m_n)^t = 0$ which means that $(\det T)m_i = 0$ for each i, so $(\det T)M = 0$. Expanding out $\det T$, we note that all the a_{ij} are in $\mathcal{M}$ so we obtain

$$(1^n + 1^{n-1} + b_{n-1}1^{n-1} + \cdots + b_0)M = 0.$$

Now $1+b_{n-1}+\dots b_0$ is not in $\mathcal{M}$ so it must be a unit u. Then we have $uM=0$, so $u^{-1}uM=0$, so $1M=0$, so $M=0$. □

Earlier we said that we wanted to show that $\mathcal{O}_K$ had many of the same properties as $\mathbb{Z}$. What we will in fact show is that $\mathcal{O}_K$ is something called a *Dedekind domain.* A Dedekind domain is a simple kind of ring. Let us first define an even simpler kind of ring, a *discrete valuation ring*, frequently called a DVR.

Definition 4.5. A discrete valuation on a field K is a surjective homomorphism from K^* onto the additive group of $\mathbb{Z}$ such that

(1) $v(xy)=v(x)+(y)$;

(2) $v(x+y)\geq\min(v(x),v(y))$.

By convention, we say that $v(0)=\infty$.

Remark 4.6. Note that it follows from property 2 that if $v(x)>v(y)$, then $v(x+y)=v(y)$. To prove this we note that $v(-x)=v(x)$ and $v(y)=v(-y)$, so we have

$$v(y)\geq\min(v(x+y),v(-x))\geq v(x+y)$$

since $v(x)>v(y)$. Since $v(x+y)\geq\min(v(x),v(y))$ also, we must have $v(x+y)=v(y)$.

Example 4.7. Let v_p be the p-adic valuation on $\mathbb{Q}$. That is to say that $v_p(a)$ is the largest power dividing a for $a\in\mathbb{Z}$ and $v_p(a/b)=v_p(a)-v_p(b)$ for $a,b\in\mathbb{Z}$.

Definition 4.8. A discrete valuation R ring is a set of the form

$$\{a\in K\ \mid\ v(a)\geq 0\}$$

Note that since we have assumed that v is surjective a field is not a DVR. This is different from the terminology used in the book. The key fact about DVR's is that if we pick a π for which $v(\pi)=1$, then every element in a in R can be written as $u\pi^n$ for some $n\geq 0$. Indeed, this follows form the fact that $a/\pi^{v(a)}$ must have valuation 1 and therefore be a unit. Thus, Ra is the only maximal ideal in R.

Now, to define Dedekind domains.

Definition 4.9. A Dedekind domain is a domain R with the property that $R_{\mathcal{P}}$ is a DVR for every prime $\mathcal{P}$.

Example 4.10. Take the ring $\mathbb{Z}$. For any nozero prime (p), it is easy to check that $\mathbb{Z}_{(p)}$ is the DVR corresponding the p-adic valuation.