Definition 3.1. A ring A is said to be *Noetherian* if it satisfies the *ascending chain condition* which states that if there is a sequence of ideals I_m such that

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_m \subseteq \ldots$$

then there is an N such that for all $n \geq N$, we have $I_n = I_{n+1}$. In other word, the chain becomes stationary.

A quick word on maximality: an ideal I is maximal if there is no larger proper ideal J containing I. Maximal ideals are usually written as $\mathcal{M}$.

Lemma 3.2. *Let A be a Noetherian ring. Any subset $\mathcal{S}$ of ideals of A has a maximal element (here maximal means that there is no strictly larger ideal $I' \supset I$ in $\mathcal{S}$).*

Proof. Let $I_0 \in \mathcal{S}$. If I is not maximal in $\mathcal{S}$ there is a larger ideal $I_1 \in \mathcal{S}$ containing I_0. Similarly, if I_1 is not maximal there is a larger ideal $I_2 \in \mathcal{S}$ containing it and so on, so we have an ascending chain of ideals

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_m \subseteq \ldots,$$

which means that there is some N such that for all $n \geq N$, we have $I_n = I_{n+1}$ Then I_N is a maximal element of $\mathcal{S}$. □

Proposition 3.3. *R is Noetherian $\Leftrightarrow$ every ideal of R is finitely generated.*

Proof. ($\Rightarrow$) Let J be an ideal and let $\mathcal{S}_J$ be set of all finitely generated ideals contained in J. This set is nonempty since for any $a \in J$, the ideal $Ra \subset J$ is finitely generated. Let I be a maximal element of $\mathcal{S}_J$. If I is not equal to J, then there is some $b \in J$ such that $b \notin I$. But $I + Ra$ is also finitely generated and strictly larger than I, so this is impossible. Thus, $I = J$ and j is finitely generated.
($\Leftarrow$) Let

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_m \subseteq \ldots,$$

be an ascending chain of ideals. Then $\cup_{j=0}^{\infty} I_j$ is an ideal (easy to check) and is finitely generated, by, say, the set $a_1, \ldots, a_\ell$. Each a_i is in some I_j so there is an I_N containing all of the a_i. Thus, $I_N = \cup_{j=0}^{\infty} I_j$ and $I_{n+1} = I_n$ for every $n \geq N$.

□

Recall an ideal $\mathcal{P}$ is said to be prime if $ab \in \mathcal{P}$ implies that either $a \in \mathcal{P}$ or $b \in \mathcal{P}$.

Definition 3.4. The *dimension* of a ring is the largest n for which there exists a chain of prime ideals

$$\mathcal{P}_0 \subset \mathcal{P}_1 \subset \cdots \subset \mathcal{P}_n,$$

where the $\mathcal{P}_i$ are prime ideals and $\mathcal{P}_i \neq \mathcal{P}_{i+1}$ (for $i = 1, \ldots, n-1$).

Not all rings are finite dimensional, e.g. $k[(x_i)_{i=1}^{\infty}]$. This ring isn't Noetherian either. But furthermore, not all Noetherian rings are finite dimensional. However, all local Noetherian rings *are* finite dimensional.

Now, let's define localization... Let A be a domain and let $S \subset A$ be closed under multiplication and suppose that $0 \notin S$. Then, we can form a the ring $S^{-1}A$ which is the set of fraction of the form

$$\frac{a}{s}$$

where $a \in A$ and $s \in S$ subject to the equivalence relation

$$\frac{a}{s} = \frac{b}{t}$$

if $at = bs$. It is easy to check that is well-defined, e.g. that if $at = bs$ and $a't' = b's'$ then

$$\frac{a}{s}\frac{b}{t} = \frac{a'}{s'}\frac{b'}{t'}$$

and

$$\frac{a}{s} + \frac{b}{t} = \frac{a'}{s'} + \frac{b'}{t'}.$$

Note furthermore that s/s serves as 1 and that $0/s$ serves as 0. Also there is a natural map sending A into $S^{-1}A$ by fixing $s \in S$ and sending a to as/s.

Remark 3.5. Note that we need to change things slightly when S contains zero divisors. We say that $a/s = a'/s'$ if there exists some $t \in S$ such that $tas' = ta's$.

On the other hand, when A is a domain the map $A \longrightarrow S^{-1}A$ is always injective. Since $a/1 = 0/t$ implies that $at = 0$ which implies that $a = 0$.

When $\mathcal{P}$ is a prime elements than $A \setminus \mathcal{P}$ is multiplicatively closed set since $a, b \notin \mathcal{P}$ implies that $ab \notin \mathcal{P}$. This is the most important example of localization and in this case $S^{-1}A$ is written as $A_{\mathcal{P}}$. Examples...

Example 3.6. Localizing $\mathbb{Z}$ at the ideal (p) for p a prime number we get the set of elements of $\mathbb{Q}$ that can be written as a/s where s is not divisible by p.

Some more notation...people frequently write R_S rather $S^{-1}R$ simply because it is easier to write (for example, Janusz does this).

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 3.7. *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. Denote the map from R into R_S as ϕ. Every prime ideal $\mathcal{Q}$ in R_S pulls back to a prime ideal $\phi^{-1}(\mathcal{Q})$ of R. We also see that an ideal $\mathcal{P}$ in R is equal to $\phi^{-1}(\mathcal{Q})$ for some $\mathcal{Q}$ in R_S if $\phi(\mathcal{P})$ is a prime ideal and $\phi^{-1}(\phi(\mathcal{P})) = \mathcal{P}$. Now, if there is some $s \in S \cap \mathcal{P}$, then clearly $R_S\mathcal{P} = 1$, since $\frac{1}{s}s = 1$. So it only remains to show that if $\mathcal{P}$ is a prime that doesn't intersect S, then $R_s\mathcal{P}$ is a prime ideal. It is easy to see that $R_s\mathcal{P}$ consists of all a/s for which $a \in \mathcal{P}$ and $s \in S$. Now, suppose that

$$\frac{x}{t}\frac{y}{t'} = \frac{a}{s}$$

for $x, y \in R$, $t, t' \in S$ and $a/s \in R_S$. Then $xys = att'$, so $xy \in \mathcal{P}$ (since $s \notin \mathcal{P}$, so either x or y is in $\mathcal{P}$, so either x/t or y/t' is in $R_S\mathcal{P}$. Thus, $R_S\mathcal{P}$ is indeed a prime ideal. $\square$

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.

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 3.8. *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 3.9. *(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*
- *$\prod_{i=1}^{n} \mathcal{P}_i \subset I$.*

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. □

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

Proposition 3.10. *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. □

Lemma 3.11. *(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 $T(m_1, \dots, m_n)^t = 0$ (i.e., T times the column vector with entries m_i), which means that $UT(m_1, \dots, m_n)^t = 0$ 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 3.12. 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 3.13. 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 3.14. 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 $a, b \in \mathbb{Z}$.