Corollary 6.1. *Let R be a Noetherian ring of dimension 1. Then every nonzero ideal I is contained in finitely many prime ideals $\mathcal{P}$.*

Proof. Every prime ideal in R/I is maximal, so the proposition at the end of the previous lecture applies (using the bijection between primes of R containing I and primes of R/I, which you proved on your homework). $\square$

Lemma 6.2. *Let R be a integral domain, let $\mathcal{M}$ be a maximal ideal of R, let $n \geq q$, and let ϕ the quotient map $\phi : R \longrightarrow R/\mathcal{M}^n$ be the quotient map. Then $\phi(s)$ is a unit in $R/\mathcal{M}^n$ for every $s \in R \setminus \mathcal{M}$.*

Proof. Since $\mathcal{M}$ is maximal, we can have $Rs+\mathcal{M} = 1$ for $s \notin \mathcal{M}$. Thus, we can write $ax + m = 1$ for $a \in R$ and $m \in \mathcal{M}^n$ using facts about coprime ideals proved earlier. Thus $ax = 1 \pmod{\mathcal{M}^n}$, so $\phi(ax) = 1$. $\square$

Lemma 6.3. *Let R be a integral domain, let $\mathcal{M}$ be a maximal ideal of R, let $n \geq q$. Then*

$$R/\mathcal{M}^n \cong R_{\mathcal{M}}/(R_{\mathcal{M}}\mathcal{M}^n)$$

Proof. Since $1 \in R \setminus \mathcal{M}$, we can embed R into $R_{\mathcal{M}}$ by sending $r \in R$ to $r/1$. We have a map then from R to $R_{\mathcal{M}}/R_{\mathcal{M}}\mathcal{M}^n$ by composing this embedding with the quotient map. We show that this is well-defined on congruence classes of R modulo $\mathcal{M}^n$ since if $a - b \in \mathcal{M}$, then $a/1 - b/1 \in R_{\mathcal{M}}\mathcal{M}^n$. Thus, we obtain a map

$$\psi : R/\mathcal{M}^n \longrightarrow R_{\mathcal{M}}/(R_{\mathcal{M}}\mathcal{M}^n).$$

This map is easily seen to be surjective by the Lemma above, since for any $a/s \in R_{\mathcal{M}}$, there is a $t \in R$ such that $ts \equiv 1 \pmod{\mathcal{M}^n}$, which means that $ta \equiv a/s \pmod{R_{\mathcal{M}}\mathcal{M}^n}$. To see that the map is injective we note that $R_{\mathcal{M}}\mathcal{M}^n$ is the set of all m/s where $m \in \mathcal{M}^n$ and $s \in R \setminus \mathcal{M}$. So, if for some $t \in R$, we have $t/1 \in R_{\mathcal{M}}\mathcal{M}^n$, then we must have $t/1 = m/s$ for $m \in \mathcal{M}^n$ and $s \in R \setminus \mathcal{M}$. This means that $ts \in \mathcal{M}^n$. Since s is a unit modulo $\mathcal{M}^n$, this means that $t \in \mathcal{M}^n$. $\square$

Note in the following proof we do not simply mod out by I and factor 0. We mod out by an ideal smaller than I so that the projection of I onto each factor is not zero. That way we can apply Nakayama's lemma.

Theorem 6.4. *Let R be a Dedekind domain, let $I \subset R$ be a nonzero ideal, and let $\mathcal{P}_1, \ldots, \mathcal{P}_n$ be the set of primes that contain I. Then there* *exists a unique n-tuple* $e_1, \dots, e_n$ *of non-negative integers such that*

$$\prod_{j=1}^{n} \mathcal{P}_j^{e_j} = I.$$

Proof. There are positive integers f_j such that

$$\prod_{j=1}^{m} \mathcal{P}_j^{f_j - 1} \subset I$$

since R is Noetherian. Let's set up a bit of notation first. For each $j = 1, \dots, n$ we have the quotient map $\phi_j : R \longrightarrow R/\mathcal{P}_j^{f_j}$. Let ϕ be the map from R to $\bigoplus_{j=1}^n R/\mathcal{P}_j^{f_j}$ given by

$$\phi(r) = (\phi_1(r), \dots \phi_n(r)).$$

We'll denote $R/\mathcal{P}_j^{f_j}$ as R_j. Since $\phi(I)$ is an ideal, it has decomposition as above $\phi(I) = \bigoplus_{j=1}^n \phi_j(I)$. Each $\phi_j(I)$ is an ideal in $R/\mathcal{P}_j^{f_j}$. We know that $R/\mathcal{P}_j^{f_j}$ is isomorphic to $R_{\mathcal{P}_j}/\mathcal{P}_j^{f_j}$, so $\phi_j(I)$ must be a power of $\phi_j(\mathcal{P}_j)$; here we use the fact that $R_{\mathcal{P}_j}$ is a DVR. So we can write $\phi_j(I) = \mathcal{P}_j^{e_j}$ for some unique $e_j < f_j$ (since I was actually contained in the product of the $\mathcal{P}_i$ to the $f_i - 1$ power). Since

$$\phi(\mathcal{P}_j) = \bigoplus_{\ell \neq j} R_j \bigoplus \phi_j(\mathcal{P}_j)$$

(this follows from the Chinese Remainder theorem, in fact), we see then that

$$\prod_{j=1}^{n} \phi(\mathcal{P}_j^{e_j}) = \bigoplus_{j=1}^{n} \phi_j(\mathcal{P}_j) = \bigoplus_{j=1}^{n} \phi_j(I) = \phi(I).$$

Since all the $e_j \le f_j$, we have

$$\ker \phi = \prod_{j=1}^{n} \mathcal{P}_j^{e_j} \subset \prod_{j=1}^{n} \mathcal{P}_j^{f_j},$$

so

$$I = \phi^{-1}(\phi(I)) = \phi^{-1}(\prod_{j=1}^{n} \phi\left(\mathcal{P}_j^{e_j}\right)) = \prod_{j=1}^{n} \mathcal{P}_j^{e_j},$$

as desired. To see that the e_i are unique, recall that $\phi_j(I) = \phi_j(\mathcal{P}_j)^{e_j}$ for a unique e_j, so for $e'_j < e_j$, we have

$$\phi_j(\mathcal{P}_j)^{e_j} \not\subset \phi_j(I)$$

and for $e'_j > e_j$, we have

$$\phi_j(I) \not\subset \phi_j(\mathcal{P}_j)^{e_j}$$

(by Nakayama's Lemma), either of which forces the product

$$\prod_{j=1}^{n} \phi(\mathcal{P}_j) \neq \phi(I).$$

□

Now, for what are called fractional ideals

Definition 6.5. Let R be an integral domain with field of fractions K. A *fractional ideal* of R is an R-submodule $J \subset K$ for which there is some nonzero $x \in R$ such that $xJ \subset R$.

Definition 6.6. For a fractional ideal J, we define $(R : J)$ to be set

$$\{x \in K \mid xJ \subseteq R\}.$$

We say that J is invertible if $J(R : J) = R$.

A few remarks on the definition above. It is clear that $(R : R) = R$ since R contains 1 and is closed under multiplication. It follows that when $JN = R$, we must have $N = (R : J)$. Also note that $J(R : J)$ may not be all of R, as we'll see in some examples later.

If we consider the unit ideal R to be the identity, then we see that the invertible ideals of R form a group under fractional ideal multiplication, since it clear that if J and N are invertible, so is JN and that if J is invertible, then so is its inverse $(R : J)$ invertible, by definition.

We say, as usual, that a fractional ideal J is principal if there exists some y such that $Ry = J$. The principal fractional ideals of J are clearly invertible and form a subgroup of the group of invertible ideals.

We make the following definitions

$$\mathbf{F}(R) \text{ is the set of invertible fractional ideals of } R$$

$$\mathbb{P}(R) \text{ is the set of principal fractional ideals of } R$$

and

$$\mathrm{Pic}(R) = \mathbf{F}(R)/\mathbb{P}(R).$$

$\mathrm{Pic}(R)$ is called the Picard group of R.

We will show that if R is a DVR, then all of the fractional ideals of R are invertible. We'll also want a few facts about invertible ideals.

Lemma 6.7. *Let J be a finitely generated fractional ideal of an integral domain R with field of fractions K and let S be a multiplicative set S in R not containing 0. Then $S^{-1}R(R : J) = (S^{-1}R : S^{-1}RJ)$.*

We will prove this next time.