Math 430 Tom Tucker
NOTES FROM CLASS 09/16/24

I wanted to do a very quick proof of something from last time.

Theorem 6.1. *Let A be a Dedekind domain and let B be an integral extension of A that is an integral domain. Then B has dimension 1.*

Proof. We first show that if $\mathfrak{q} \subseteq \mathfrak{q}'$ satisfy $\mathfrak{q} \cap A = \mathfrak{q}' \cap A = \mathfrak{p}$ (for $\mathfrak{q}$, $\mathfrak{q}'$ primes of B), then $\mathfrak{q} = \mathfrak{q}'$. This follows immediately from applying Lemma 5.7 from last time to the extension $B/\mathfrak{q}$ of $A/\mathfrak{p}$ (using the fact that the image of $\mathfrak{q}'$ cannot intersect $A/\mathfrak{p}$ in the zero ideal unless this image is 0). This implies that the dimension of B is at most 1 since the dimension of A is 1. Now note that B has a nonzero maximal ideal since it cannot be a field as it cannot contain the field of fractions of A. Thus the dimension of B is 1. □

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.

Here is the idea: we don't truly have unique factoritzation in a ring like $R/\mathfrak{p}^m$ since if $\mathfrak{q}$ is the image of $\mathfrak{p}$ in $R/\mathfrak{p}^m$, then $R/\mathfrak{p}^n = 0$ for all $n \geq m$. But we do have unique factorization for powers of $\mathfrak{q}$ less than m. So what we want do to is take a product of primes contained in our ideal I so that I does not project onto 0 in any of the factors we get from the Chinese Remainder Theorem. That is the idea of the next proof.

Theorem 6.2. *Let R be a Dedekind domain, let $I \subset R$ be a nonzero ideal, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the set of primes that contain I. Then there exists a unique n-tuple $e_1, \ldots, e_n$ of non-negative integers such that*

$$\prod_{j=1}^{n} \mathfrak{p}_j^{e_j} = I.$$

Proof. There are positive integers f_j such that

$$\prod_{j=1}^{m} \mathfrak{p}_j^{f_j - 1} \subseteq I$$

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

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

We'll denote $R/\mathfrak{p}_j^{f_j}$ 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 $R/\mathfrak{p}_j^{f_j}$. We know that $R/\mathfrak{p}_j^{f_j}$ is isomorphic to $R_{\mathfrak{p}_j}/\mathfrak{p}_j^{f_j}$, so $\phi_j(I)$ must be a power of $\phi_j(\mathfrak{p}_j)$; here we use the fact that $R_{\mathfrak{p}_j}$ is a DVR. So we can write $\phi_j(I) = \mathfrak{p}_j^{e_j}$ for some unique $e_j < f_j$ (since I was actually contained in the product of the $\mathfrak{p}_i$ to the $f_i - 1$ power). Since

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

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

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

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

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

so

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

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

$$\phi_j(\mathfrak{p}_j)^{e_j} \not\subset \phi_j(I)$$

and for $e_j' > e_j$, we have

$$\phi_j(I) \not\subset \phi_j(\mathfrak{p}_j)^{e_j}$$

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

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

□

Now, for what are called fractional ideals

Definition 6.3. 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 6.4. 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

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

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

and

$$\text{Pic}(R) = \text{Inv}(R)/\mathbb{P}(R).$$

$\text{Pic}(R)$ 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 6.5. *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 $S^{-1}R(R : J) = (S^{-1}R : S^{-1}RJ)$.*

Proof. Since $xJ \subseteq R$ implies that $\frac{x}{s}J \subseteq S^{-1}R$ for any $s \in S$ it is clear that $S^{-1}R(R : J) \subseteq (S^{-1}R : S^{-1}RJ)$. To get the reverse inclusion, let $y \in (S^{-1}R : S^{-1}RJ)$ and let $m_1, \ldots, m_n$ generate J as an R-module. Since $yS^{-1}RJ \subseteq S^{-1}R$, we must have $ym_i \subset S^{-1}R$, so we can write $ym_i = r_i/s_i$ where $r_i \in R$ and $s_i \in S$. Since $(s_1 \cdots s_n y)m_i = (\prod_{j \neq i} s_j) r_i \in R$, this means that $s_1 \cdots s_n y \in (R : J)$. Thus, $y \in S^{-1}R(R : J)$. $\square$