Math 430 Tom Tucker
NOTES FROM CLASS 09/13/21

Lemma 5.1. *If $I + J_1 = 1$ and $I + J_2 = 1$, then $I + J_1 J_2 = 1$.*

Proof. Writing $a + b = 1$ for $a \in I$ and $b \in J_1$ and writing $a' + b' = 1$ for $a \in I$ and $b \in J_2$, we see that

$$1 = (a + b)(a' + b') = aa' + ab' + ba' + bb' \subseteq I + J_1 J_2.$$

□

Proposition 5.2. *(Chinese Remainder theorem) Let R be a ring and let $I_1, \dots, I_n$ be a set of ideals of R such that $I_j + I_k = 1$ for $j \neq j$. Then the natural map*

$$R \longrightarrow \bigoplus_{j=1}^{n} R/I_j$$

is surjective with kernel $I_1 \cdots I_n$.

Proof. We proceed by induction on n. If $n = 1$, then the result is obvious. Otherwise, write $I := I_1$ and $J := I_2 \cdots I_n$. Applying the lemmas above, $I + J = 1$ and the natural map

$$R \longrightarrow R/I \oplus R/J$$

is surjective with kernel IJ. Since the natural map

$$R \longrightarrow \bigoplus_{j=2}^{n} R/I_j$$

is surjective with kernel $I_2 \cdots I_n$ by the inductive hypothesis, we are done. □

One more criterion related to being a DVR.

Proposition 5.3. *Let A be a Noetherian local ring with maximal ideal $\mathcal{M}$. Let $I \subseteq M$ have the property that $I + \mathcal{M}^2 = \mathcal{M}$. Then $I = \mathcal{M}$.*

Proof. Let $N = \mathcal{M}/I$. Let $a \in \mathcal{M}$. Then there is a $b \in \mathcal{M}^2$ such that $a - b \in I$. Thus, $\mathcal{M}N = N$. By Nakayama's lemma (note that N is finitely generated since A is Noetherian), we have $N = 0$ so $I = \mathcal{M}$. □

Corollary 5.4. *Let A be a Noetherian local ring. Let $\mathcal{M}$ be its maximal ideal and let k be the residue field $A/\mathcal{M}$. Then*

$$\dim_k \mathcal{M}/\mathcal{M}^2 = 1$$

if and only if $\mathcal{M}$ is principal

Proof. One direction is easy: If $\mathcal{M}$ is generated by π, then $\mathcal{M}/\mathcal{M}^2$ is generated by the image of π modulo $\mathcal{M}^2$. To prove the other direction, suppose that $\mathcal{M}/\mathcal{M}^2$ has dimension 1. Then we can write $\mathcal{M} = Ra + \mathcal{M}^2$ for some $a \in \mathcal{M}$. Then the module $M = \mathcal{M}/a$ has the property that $\mathcal{M}M = M$, since any element in M can be written as $ca + d$ for $c \in R$ and $d \in \mathcal{M}^2$. By Nakayama's lemma, we thus have $M = 0$, so $\mathcal{M} = Ra$. □

Proposition 5.5. *Let R be a domain and let $S \subseteq R$ be a multiplicative subset not containing 0. Let $b \in K$, where K is the field of fractions of R. Then b is integral over $S^{-1}R \Leftrightarrow sb$ is integral over R for some $s \in S$.*

Proof. If b is integral over $S^{-1}R$, then we can write

$$b^n + \frac{a_{n-1}}{s_{n-1}} b^{n-1} + \cdots + \frac{b_0}{s_0} = 0.$$

Letting $s = \prod_{i=0}^{n-1} s_i$ and multiplying through by s^n we obtain

$$(sb)^n + a'_{n-1}(sb)^{n-1} + \cdots + a'_0 = 0$$

where

$$a'_i = s^{n-i-1} \prod_{\substack{j=1 \\ j \neq i}}^{n} s_i a_i$$

which is clearly in R. Hence sb is integral over R. Similarly, if an element sb with $b \in S^{-1}R$ and $s \in S$ satisfies an equation

$$(sb)^n + a_{n-1}(sb)^{n-1} + \cdots + a_0 = 0,$$

with $a_i \in R$, then dividing through by s^n gives an equation

$$b^n + \frac{a_{n-1}}{s} b^{n-1} + \cdots + \frac{a_0}{s^n},$$

with coefficients in $S^{-1}R$.

□

Corollary 5.6. *If R is integrally closed, then $S^{-1}R$ is integrally closed.*

Proof. When R is integrally closed, any b that is integral over R is in R. Since any element $c \in K$ that is integral over $S^{-1}R$ has the property that sc is integral over R for some $s \in S$, this means that $sc \in R$ for some $s \in S$ and hence that $c \in S^{-1}R$.

□

Lemma 5.7. *Let $A \subseteq B$ be domains and suppose that every element of B is algebraic over A. Then for every ideal nonzero I of B, we have $I \cap A \neq 0$.*

Proof. Let $b \in I$ be nonzero. Since b is algebraic over A and $b \neq 0$, we can write

$$a_n b^n + \cdots + a_0 = 0,$$

for $a_i \in A$ and $a_0 \neq 0$. Then $a_0 \in I \cap \mathbb{Z}$. □

Theorem 5.8. *Let α be an algebraic number that is integral over $\mathbb{Z}$. Suppose that $\mathbb{Z}[\alpha]$ is integrally closed. Then $\mathbb{Z}[\alpha]$ is a Dedekind domain.*

Proof. Since $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module, any ideal of $\mathbb{Z}[\alpha[$ is also a finitely generated $\mathbb{Z}$-module. Hence, any ideal of $\mathbb{Z}[\alpha]$ is finitely generated over $\mathbb{Z}[\alpha]$, so $\mathbb{Z}[\alpha]$ is Noetherian. Let $\mathcal{Q}$ be a prime in $Z[\alpha]$. Then, $\mathcal{Q} \cap \mathbb{Z}$ is a prime ideal (p) in $\mathbb{Z}$. Hence, $\mathbb{Z}[\alpha]/\mathcal{Q}$ is a quotient of $\mathbf{F}_p[X]/f(X)$ where $f(X)$ is the minimal monic satisfied by α. Since $\mathbf{F}_p[X]/f(X)$ has dimension 0 (Exercise 7 on the homework), this implies that $\mathbb{Z}[\alpha]/\mathcal{Q}$ is a field so $\mathcal{Q}$ must be maximal. □

Remark 5.9. The rings we deal with will *not* in general have this form.

Lemma 5.10. *Let R be a ring that has direct sum decomposition*

$$R = \bigoplus_{j=1}^{n} R_j.$$

Then every ideal in $I \subset R$ can be written as

$$I = \bigoplus_{j=1}^{n} I_j$$

for ideals $I_j \subset R_j$. If $\mathcal{P}$ is a prime of R then there is some j for which we can write

$$\mathcal{P} = \bigoplus_{\ell \neq j} R_\ell \bigoplus \mathcal{P}_j$$

Proof. We can view $R = \bigoplus_{j=1}^{n} R_j$ as the set of

$$(r_1, \ldots, r_n)$$

with $r_j \in R_j$. Let p_j be the usual projection from R onto its j-th coordinate and let i_j be the usual embedding of R_j into R obtained by sending $r_j \in R_j$ to the element of R with all coordinates 0 except for the j-th coordinate which is set to r_j. Since an ideal I of R must be a $i_j(R_j)$ module, the set of $p_j(r)$ for which $r \in I$ must form an ideal R_j ideal, call it I_j. It is easy to see that $I_j = p_j(I)$. Certainly, $I \subset \bigoplus p_j(I)$. Since we can multiply anything in I by $(0, \ldots, 1_j, 0, \ldots, 0)$ we see that $i_j p_j(I) \subset I$. Hence $\bigoplus p_j(I) \subset I$, and we are done with our description of ideals of $\bigoplus_{j=1}^{n} R_j$. For prime ideals, we note that if $\mathcal{P}$ is a prime then $(a_1, \ldots, a_n)(b_1, \ldots, b_n) \in \mathcal{P}$ implies that $a_j b_j \in p_j(\mathcal{P})$ for each j, so $p_j(\mathcal{P})$ must be a prime of R_j or all of R_j. Suppose we had $k \neq j$ with $p_j(\mathcal{P}) \neq R_j$ and $p_k(\mathcal{P}) \neq R_k$. Then choosing $a_j \in p_j(\mathcal{P})$, $a_k \in p_k(\mathcal{P})$ and $b_j \notin p_j(\mathcal{P})$, $b_k \notin p_k(\mathcal{P})$, we see that

$$(i_j(a_j) + i_j(b_k))(i_j(b_j) + i_k(a_k)) \in \mathcal{P},$$

but $(i_j(a_j)+i_j(b_k)), (i_j(b_j)+i_k(a_k)) \notin \mathcal{P}$, a contradiction, so $p_j(\mathcal{P}) = R_j$ for all but one j. Thus

$$\mathcal{P} = \bigoplus_{\ell \neq j} R_\ell \bigoplus \mathcal{P}_j$$

for some prime $\mathcal{P}_j$ of R_j. ☐

Corollary 5.11. *Let R be a Noetherian ring in which every prime ideal is maximal. Then R has only finitely many prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_n$ and can be written as*

$$R \cong \bigoplus_{j=1}^{n} R/\mathcal{P}_i^{w_i}.$$

Proof. Since R is Noetherian, there are prime ideals $\mathcal{P}_i$ such that $\prod_{j=1}^{n} \mathcal{P}_i^{w_i} = 0$ (remember that we can make the product be contained in 0 and 0 is the only element in $R0$). Then the natural map

$$R \longrightarrow \bigoplus_{j=1}^{n} R/\mathcal{P}_i^{w_i}$$

is surjective with kernel 0, hence it is an isomoprhism. Within each factor $R/\mathcal{P}_i^{w_i}$, the only prime ideal is the image of $\mathcal{P}_i$ under the quotient map ϕ, since the image of any other prime under ϕ is all of $R/\mathcal{P}_i^{w_i}$ by the Lemma above. Hence, $\phi(\mathcal{P}_i)$ is the only prime in $R/\mathcal{P}_i^{w_i}$. By the Lemma above, the only primes in R are of the form $\bigoplus_{\ell \neq j} R \bigoplus \phi(\mathcal{P}_i)$. ☐

Corollary 5.12. *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 above applies. ☐

Lemma 5.13. *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 $\phi(ax) = 1$. $\square$