Proposition 5.1. *Let R be a domain and let $S \subset R$ 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 5.2. *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 5.3. *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 $b \in A$ 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 5.4. *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 5.5. The rings we deal with will *not* in general have this form.

Now, a brief interlude on geometry and normality. Let $F(X,Y) = 0$ be a curve in the plane k^2 over an algebraically closed field k. We say that $F(X,Y)$ is *singular* at the point (a,b) is

$$\frac{\partial F}{\partial X}(a,b) = \frac{\partial F}{\partial Y}(a,b) = 0.$$

In other words if the tangent vector to $F = 0$ is 0 at (a,b), so that there is no notion of a tangent vector here. If the point (a,b) is not singular, we say that it is nonsingular.

Note that the primes $\mathcal{Q}$ of R correspond to points (a,b) such that $F(a,b) = 0$. If $\mathcal{Q}$ corresponds to the point (a,b) then $\mathcal{Q}$ is simply the image of $k[X,Y](X-a) + k[X,Y](Y-b)$ in R.

Lemma 5.6. *Let $\mathcal{Q}$ be a nonzero prime in the ring*

$$R = k[X,Y]/F(X,Y).$$

Then

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

if and only if the point (a,b) corresponding to $\mathcal{Q}$ is nonsingular.

Proof. Let $\mathcal{P}$ be prime in $k[X,Y]$ generated by $(X-a)$ and $(Y-b)$. Let θ be the map from $k[X,Y]$ to k^2 given by

$$\theta(G) = (\frac{\partial G}{\partial X}(a,b), \frac{\partial G}{\partial Y}(a,b)).$$

Then $\theta(X-a) = (1,0)$ and $\theta(Y-b) = (0,1)$, so the rank of the image of $\mathcal{P}$ is 2. It is easy to see that $\mathcal{P}^2$ is in the kernel of this map. So θ induces an isomorphism between $\mathcal{P}/\mathcal{P}^2$ and k^2. Now we have

$$\mathcal{Q}/\mathcal{Q}^2 \cong (\mathcal{P}/(\mathcal{P}^2 + F(X,Y)),$$

as a k-vector space since

$$\mathcal{P}^2 + F(X,Y) = \phi^{-1}(\mathcal{Q}^2)$$

where ϕ is the quotient map from $k[X,Y]$ to R. Counting dimensions we have

$$\dim_k \mathcal{P}/\mathcal{P}^2 = 2$$

if $\theta(F) = 0$ and and

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

otherwise. □

Lemma 5.7. *(Later in class we wil prove this more generally) We have*

$$\mathcal{Q}/\mathcal{Q}^2 \cong R_{\mathcal{Q}}\mathcal{Q}/(R_{\mathcal{Q}}\mathcal{Q})^2.$$

Lemma 5.8. *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. $\square$