Lect. 14. Integral extensions.

Lemma. $R \subset R'$ integral ext. of domains.
Then R' is a field $\Leftrightarrow$ R is a field.

Pf. Supp. R' is a field. Let $x \in R$, $x \neq 0$.
Then $\frac{1}{x} \in R'$, so sat. eqn.

$$\left(\frac{1}{x}\right)^n + a_1\left(\frac{1}{x}\right)^{n-1} + \cdots + a_n = 0.$$

Mult. by x^{n-1}, get

$$\frac{1}{x} = -(a_1 + a_2 x + \cdots + a_n x^{n-1}), \text{ so } \frac{1}{x} \in R.$$

Conv., supp. R is a field. Let $y \in R'$ be nonzero. Then y sat eqn.

$$y^n + a_1 y^{n-1} + \cdots + a_n = 0.$$

$$\text{So } y(y^{n-1} + \cdots + a_{n-1}) = -a_n$$

Take n minimal. Then $a_n \neq 0$,

$$\text{so} \quad \frac{1}{y} = -\frac{1}{a_n}(y^{n-1} + \cdots + a_{n-1}).$$

Def. Let $R \subset R'$, $\mathfrak{p} \subset R$ prime, $\mathfrak{p}' \subset R'$ prime.
Then $\mathfrak{p}'$ <u>lies over</u> $\mathfrak{p}$ if $\mathfrak{p}'$ contracts to $\mathfrak{p}$.
(i.e. $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$). (i.e. image of $\mathfrak{p}'$ is $\mathfrak{p}$ under $\operatorname{Spec} R' \to \operatorname{Spec} R$).

<u>Thm.</u> $R \subset R'$ integral ext, $\mathfrak{p} \subset R$ prime. Let $\mathfrak{p}' \subset \mathfrak{q}'$ primes in R', $\mathfrak{a}' \subset R'$ any ideal.

(1) (Maximality) Supp. $\mathfrak{p}'$ lies over $\mathfrak{p}$. Then $\mathfrak{p}'$ is maximal if and only if $\mathfrak{p}$ is.

(2) (Incomparability) Supp. $\mathfrak{p}', \mathfrak{q}'$ lie over $\mathfrak{p}$. Then $\mathfrak{p}' = \mathfrak{q}'$.

(3) (Lying over) There is a prime $\mathfrak{r}' \subset R'$ lying over $\mathfrak{p}$

(4) (Going up) Suppose $\mathfrak{a}' \cap R \subset \mathfrak{p}$. Then Can take $\mathfrak{r}'$ ~~to~~ in (3) to contain $\mathfrak{a}'$.

<u>Pf.</u> (1) follows from lemma

To prove (2), localize at $R \setminus \mathfrak{p}$, then get

$$\begin{tikzcd} R' \arrow[r] & R'_{\mathfrak{p}} \\ R \arrow[u] \arrow[r] & R_{\mathfrak{p}} \arrow[u] \end{tikzcd}$$

and $R_{\mathfrak{p}} \hookrightarrow R'_{\mathfrak{p}}$ is injective.

Thus $\mathfrak{p}' R'_{\mathfrak{p}} \subset \mathfrak{q}' R'_{\mathfrak{p}}$ are primes in $R'_{\mathfrak{p}}$. (bijection between primes). But $\mathfrak{p}' R'_{\mathfrak{p}}$ is max since lies over $\mathfrak{p} R_{\mathfrak{p}}$, so $\mathfrak{p}' R'_{\mathfrak{p}} = \mathfrak{q}' R'_{\mathfrak{p}}$. $\Rightarrow \mathfrak{p}' = \mathfrak{q}'$ (bij. between ideals).

To prove (3), again replace R by $R_{\mathfrak{p}}$, R' by $R'_{\mathfrak{p}}$. So we may assume R local and $\mathfrak{p}$ unique max ideal

Now, $\mathfrak{P}'$ has max ideal $\mathfrak{r}'$,
~~and $\mathfrak{r}' \ni \mathfrak{r}$ by (1). So $\mathfrak{r} = \mathfrak{p}$.~~
and $\mathfrak{r}'$ contracts to a max ideal $\mathfrak{r}$ in R by (1). Thus $\mathfrak{r} = \mathfrak{p}$.
Finally (4) foll from (3) by applying to $R/(\mathfrak{a}' \cap R) \subset R'/\mathfrak{a}'$. $\square$.

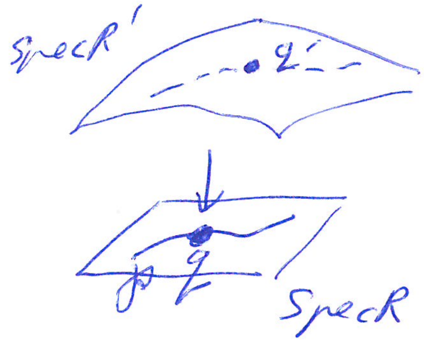
<u>Lemma</u>. $R \subset R'$ ring ext,
$f \in R[X]$ monic, $f = gh$, $g, h \in R'[X]$ monic.
Then the coeff. of g and h are integral over R.

<u>Pf.</u> $R_1 := R'[X]/\langle g \rangle$. Let x_1 be the image of X. Then $1, x_1, x_1^2, \ldots$ form a free basis of R_1 over R', so $R' \subset R_1$. Now, $g(x_1) = 0$, so $g = (X - x_1) g_1$, $g_1 \in R_1[X]$ monic of deg 1. less than g. Repeat, extending R_1.
Continuing, obtain $g(X) = \prod (X - x_i)$ and $h(X) = \prod (X - y_j)$, x_i, y_j are all in the ext of R'. Then x_i, y_j are integral over R since they are roots of f.
But coeff. of g, h are $\mathbb{Z}$-polyn. in x_i and y_j by Vieta thm. so they are also integral$/R$.

Prop. R normal domain, $K = \mathrm{Frac}(R)$
L/K a field ext. Let $y \in L$ be integral/R
$p \in K[X]$ its monic min. polyn.
Then $p \in R[X]$, so $p(y) = 0$ is an eqn of integral dep for y over R.

Pf. Since y integral, $\exists f \in R[X]$ monic s.t. $f(y) = 0$. Write $f = pq$ with $q \in K[X]$. Then by the above the coeff. of p are integral over R, so in R since R is normal.

Thm. (going down for integral extensions).
$R \subset R'$ domains, R' int/R, R normal
$p \subsetneq q$ primes in R, $q' \subset R'$ prime lying over q. Then $\exists$ a prime p' lying over p and contained in q'.



Pf. First show $\mathfrak{p}R'_{q'} \cap R = \mathfrak{p}$.

Given $y \in \mathfrak{p}R'_{q'} \cap R$, say $y = \frac{x}{s}$, $x \in \mathfrak{p}R'$, $s \in R' - q'$. Say $x = \sum_{i=1}^{m} y_i x_i$, $y_i \in \mathfrak{p}$, $x_i \in R'$, set $R'' = R'[x_1, \dots, x_n]$. Then R'' is module finite $/R'$ and $xR'' \subset \mathfrak{p}R''$. Let $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$ be the char. poly. of $\mu_x : R'' \circlearrowleft$. Then $a_i \in \mathfrak{p}^i \in \mathfrak{p}$ (sum of $i \times i$ minors), and $f(x) = 0$. Let $K = \mathrm{Frac}(R)$. Suppose $f = gh$ with $g, h \in K[x]$ monic. Since R is normal, coeff. of g and h lie in R (as R is normal). Also $f \equiv X^n \bmod \mathfrak{p}$. So $g \equiv X^r \bmod \mathfrak{p}$, $h \equiv X^{n-r} \bmod \mathfrak{p}$. (by unique fact in $\mathrm{Frac}(R/\mathfrak{p})[X]$) Hence all non-leading coe of g, h are in $\mathfrak{p}$. Replace f by a monic factor of min. degree. Then f is the min poly of x over K.

Recall that $s = \frac{x}{y}$. So s satisfies eqn.

(*) $s^n + b_1 s^{n-1} + \cdots + b_n = 0$, $b_i = \frac{a_i}{y_i} \in K$.

Conversely, any such eqn yields one of the same degree for x, as $y \in R \subset K$.

So (*) is the minimal poly of s over K.

So all b_i are in R by the above.

Suppose $y \notin \mathfrak{p}$. Then $b_i \in \mathfrak{p}$ as $a_i = b_i y^i \in \mathfrak{p}$. So $s^n \in \mathfrak{p}R' \subset qR' \subset q'$ ($q = \varphi^{-1}(q') = R \cap q'$, $\varphi : R \to R'$).

So $s \in q'$, a contradiction. Thus, $y \in \mathfrak{p}$, and $\mathfrak{p}R'_{q'} \cap R = \mathfrak{p}$.

Hence $\exists$ prime $\mathfrak{p}''$ of $R'_{q'}$ with $\mathfrak{p}'' \cap R = \mathfrak{p}$ by exercise 3.13 from before. So $\mathfrak{p}''$ lies in $q'R'_{q'}$ as this is the only max. ideal.

Set $\mathfrak{p}' = \mathfrak{p}'' \cap R'$. Then $\mathfrak{p}' \cap R = \mathfrak{p}$, and $\mathfrak{p}' \subset q'$ since $\mathfrak{p}'R'_{q'} \subset q'R'_{q'}$ (by inclusion-preserving bijection between primes).

<u>Lemma</u>. A min prime always consists of zero divisors.

<u>Pf.</u> R ring, $\mathfrak{p} \subset R$ min prime. Then $R_\mathfrak{p}$ has only one prime $\mathfrak{p}R_\mathfrak{p}$ ($R_\mathfrak{p}$ is local and all primes cont. $\mathfrak{p}R_\mathfrak{p}$)

So by Scheinnullstellensatz, $\mathfrak{p}R_\mathfrak{p}$ consists entirely of nilpotents. Hence, given $x \in \mathfrak{p}$, there is $s \in R \setminus \mathfrak{p}$ with $sx^n = 0$ for some $n \geq 1$. Take n minimal.

Then $sx^{n-1} \neq 0$. but $(sx^{n-1})x = 0$, so x is a zerodivisor.

<u>Thm.</u> (Going down for flat algebras).
Let R be a ring, R' a flat algebra, $\mathfrak{p} \subsetneq \mathfrak{q}$ nested primes, and $\mathfrak{q}'$ a prime of R' lying over $\mathfrak{q}$. Then there is a prime $\mathfrak{p}'$ lying over $\mathfrak{p}$ and contained in $\mathfrak{q}'$.

<u>Pf.</u> The canonical map $R_{\mathfrak{q}} \to R'_{\mathfrak{q}'}$ is faithf. flat:

<u>Lemma.</u> $\varphi: R \to R'$, R' flat R-algebra, $\mathfrak{p}' \subset R'$ prime, $\mathfrak{p} \subset R$ its contraction in R ($\mathfrak{p} = \varphi^{-1}(\mathfrak{p}')$). Then $R'_{\mathfrak{p}'}$ is faithfully flat over $R_{\mathfrak{p}}$.

<u>Pf.</u> $R'_{\mathfrak{p}}$ flat over $R_{\mathfrak{p}}$ by result before (localiz. preserves flatness). Also $R'_{\mathfrak{p}'}$ flat over $R'_{\mathfrak{p}}$ by further localiz. But a flat local homom. is faithfully flat.

<u>Another proof</u>: $R' \otimes_R R/\mathfrak{p}$ is flat over $R/\mathfrak{p}$ by cancellation in $\otimes$. So can replace R by $R/\mathfrak{p}$, R' by $R'/\mathfrak{p}R'$, and assume R is a domain and $\mathfrak{p} = 0$. The ideal $\mathfrak{q}'$ contains a min. prime $\mathfrak{p}'$ of R'.
Let's show $\mathfrak{p}'$ lies over 0, i.e. $\mathfrak{p}' \cap R = 0$.

Let $x \in R$, $x \neq 0$. Then $\mu_x : R \to R$ is injective. Since R' is flat$/R$, $\mu_x : R' \to R'$ is injective. So by lemma, x does not belong to the contraction of $\mathfrak{p}'$, as desired. (as mult. by a zero divisor can't be injective).

<u>Arbitrary normal rings</u>. Any ring R is <u>normal</u> if $R_{\mathfrak{p}}$ is a normal domain for every prime $\mathfrak{p}$. If R is a domain, this coincides with the previous def.