Math 711: Lecture of September 13, 2006

In the proof of the preceding Theorem, we used Chevalley's Lemma:

Theorem. *Let M be a finitely generated module over a complete local ring (R, m, K). Let $\{M_n\}_n$ be a decreasing sequence of submodules whose intersection is 0. Then for all $k \in \mathbb{N}$ there exists N such that $M_n \subseteq m^k M$.*

Proof. For all h, the modules $M_n + m^h M$ are eventually stable (we may consider instead their images in the Artinian module $M/m^h M$, which has DCC), and so we may choose n_h such that $M_n + m^h M = M_{n'} + m^h M$ for all $n, n' \geq n_h$. We may replace n_h by any larger integer, and so we may assume that the sequence n_h is increasing. We replace the original sequence by the $\{M_{n_h}\}_h$. Thus we may assume without loss of generality that $M_n + m^h M = M_{n'} + m^h M$ for all $n, n' \geq h$. We claim $M_k \subseteq m^k M$ for all k: if not, choose k and $v_k \in M_k - m^k M$. Now choose $v_{k+1} \in M_{k+1}$ such that $v_{k+1} \equiv v_k \bmod m^k M$, and, Recursively, for all $s \geq 0$ choose $v_{k+s} \in M_{k+s}$ such that $v_{k+s+1} \equiv v_{k+s} \bmod m^{k+s} M$: this is possible because $M_{k+s} \subseteq M_{k+s+1} + m^{k+s} M$. This gives a Cauchy sequence with nonzero limit. Since all terms are eventually in any given M_n, so is the limit (each M_n is m-adically closed), which is therefore in the intersection of the M_n. $\square$

We have been assuming that valuation domains V are integrally closed. It is very easy to see this: if f is in the fraction field L of V but not in V, then $x = 1/f$ is in the maximal ideal m of V. Some maximal $\mathcal{M}$ of the integral closure V' lies over m, and so x is not a unit of V', i.e., $f \notin V'$. Thus, $V' = V$.

It is also easy to see that if $K \subseteq L$ are fields and V is a valuation domain with fraction field L, then $V \cap K$ is a valuation domain with fraction field K. Moreover, if V is a DVR, then $V \cap K$ is a DVR or is K. For the first statement, each $f \in K - \{0\}$ has the property that f or $1/f$ is in V, and, hence, in $V \cap K$, as required. Now suppose that V is a DVR and that x generates the maximal ideal. Let $W = V \cap K \neq K$. Each nonzero element of the maximal ideal m of W has the form ux^k in V, where k is a positive integer. Choose an element y of the maximal ideal of W such that k is minimum. Then every $z \in m$ is a multiple of y in V, and the multiplier is in W. Thus, m is principal. It follows that every nonzero element m has the form uy^t, where $t > 0$, since it is clear that the intersection of the powers of m is zero.

We next want to prove:

Theorem. *Let R be a Noetherian domain. Then the integral closure R' of R is the intersection of the discrete valuation rings between R and its fraction field L.*

Proof. Let $f = b/a$ be an element of L not in R', where $a, b \in R$ and $b \neq 0$. It suffices to find a DVR containing R and not b/a: we may then intersect it with L. Localize at a prime of R in the support of the R-module $(R' + Rf)/R'$. Since localization commutes with integral closure we may assume that (R, m, K) is local. Nonzero elements of R are nonzerodivisors in $\widehat{R}$ by flatness, and so the fraction field of R embeds in the total quotient ring of $\widehat{R}$, and we may view b/a as an element of the total quotient ring of $\widehat{R}$. If $b + \mathfrak{p}$ is in the integral closure of $a(R/\mathfrak{p})$ for every minimal prime $\mathfrak{p}$ of $\widehat{R}$, then b is integral over $a\widehat{R}$. If the equation that demonstrates the integral dependence has degree n, we find that $b^n \in (b^{n-1}a,\, b^{n-2}a^2,\, \dots,\, ba^{n-1},\, a^n)\widehat{R}$, and since $\widehat{R}$ is faithfully flat over R, this implies that $b^n \in (b^{n-1}a,\, b^{n-2}a^2,\, \dots,\, ba^{n-1},\, a^n)R$ as well. Dividing by a^n then shows that b/a is integral over R, a contradiction. Thus, we can choose a minimal prime $\mathfrak{p}$ of $\widehat{R}$ such that $b+\mathfrak{p}$ is not integral over $a\widehat{R}/\mathfrak{p}$. It follows that $\overline{b}/\overline{a}$ is not integral over $\widehat{R}/\mathfrak{p}$, where the bars over the letters indicate images in $\widehat{R}/\mathfrak{p}$. Note that R injects into $\widehat{R}/\mathfrak{p}$. Thus, the integral closure $(\widehat{R}/\mathfrak{p})'$ of $\widehat{R}/\mathfrak{p}$ does not contain $\overline{b}/\overline{a}$, and since it is module-finite over $\widehat{R}/\mathfrak{p}$ by the last Theorem of the Lecture of September 11, it is a normal Noetherian ring. Thus, it is an intersection of DVR's by part (a) of the last Theorem of the Lecture of September 8, and we can choose a DVR V containing $(\widehat{R}/\mathfrak{p})'$ and not $\overline{b}/\overline{a}$, which is the image of b/a, so that V contains the isomorphic image of R but not the image of b/a. Now we may intersect V with the fraction field of R. $\square$

Theorem. *Let R be any ring and let $I \subseteq J$ be ideals of R.*

(a) *$r \in R$ is integral over I if and only if there exists an integer n such that $(I+rR)^{n+1} = I(I+rR)^n$. Thus, if J is generated over I by one element, then J is integral over R if and only if there exists an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$.*

(b) *If $J^{n+1} = IJ^n$ a with $n \in N$ then $J^{n+k} = I^k J^n$ for all $k \in \mathbb{N}$.*

(c) *If $J^{n+1} = IJ^n$ and $Q \supseteq J$ is an ideal and $r \in \mathbb{N}$ an integers such that $Q^{r+1} = JQ^r$, then $Q^{n+r+1} = IQ^{n+r}$.*

(d) *If J is integral over I and generated over I by finitely many elements, then there is an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$. If R is Noetherian then J is integral over I if and only if there exists an integer $n \in \mathbb{N}$ such that $J^{n+1} = IJ^n$.*

(e) *If R is a domain and M is a finitely generated faithful R-module such $JM = IM$ then J is integral over I. If R is a Noetherian domain, then J is integral over I if and only if there is a finitely generated faithful R-module M such that $JM = IM$.*

Proof. Note that

$$(I + rR)^n = I^n + rI^{n-1} + \cdots + r^t I^{n-t} + \cdots + r^n R.$$

Comparing the expansions for $(I + rR)^{n+1}$ and $I(I + rR)^n$, we see that the condition for equality is simply that r^{n+1} be in $I(I + rR)^n = r^n I + \cdots + I^{n+1}$, and this is precisely the condition for r to satisfy an equation of integral dependence on I of degree $n + 1$. This proves (a).

We prove (b) by induction on k. The result is clear if $k = 0$ and holds by hypothesis if $k = 1$. Assuming that $J^{n+k} = I^k J^n$, for $k \geq 1$ we have that

$$J^{n+k+1} = J^{n+k} J = (I^k J^n) J = I^k J^{n+1} = I^k I J^n = I^{k+1} J^n,$$

as required. This proves (b).

For (c), note that $Q^{r+n+1} = J^{n+1}Q^r = (IJ^n)Q^r = I(J^nQ^r) = IQ^{n+r}$.

It follows by induction on the number of elements needed to generate J over I that if J is finitely generated over I and integral over I then there is an integer n such that $J^{n+1} = IJ^n$.

Next, we want to show that if R is Noetherian and $J^{n+1} = IJ^n$ then J is integral over I. The condition continues to hold if we consider the images of I, J modulo a minimal prime of R, and so it suffices to consider the case where R is a domain. Moreover, if $I = (0)$ the result is immediate, and so we may assume that $I \neq 0$. Thus, J^n is a faithful R-module, and so the proof will be complete once we have established the first sentence of part (e).

Suppose that $JM = IM$ and let $u_1, \ldots, u_n$ be generators for M. Let r be an element of J. Then for every ν we can write $ru_\nu = \sum_{\mu=1}^{n} i_{\mu\nu}u_\mu$ where the $i_{\mu\nu} \in I$. Let $\mathbf{1}$ denote the size n identity matrix, and let B denote the size n matrix $(i_{\mu\nu})$. Let U be an $n \times 1$ column vector whose entries are the u_i. Then, in matrix notation, $rU = BU$, so that $(r\mathbf{1} - B)U = 0$. Let C be the transpose of the cofactor matrix of $r\mathbf{1} - B$. Then $C(r\mathbf{1} - B)$ is $D\mathbf{1}$, where $D = \det(r\mathbf{1} - B)$ is the characteristic polynomial of B evaluated at r. It is easy to see that the characteristic polynomial of a matrix with entries in I is I-special. Now, when we multiply the equation $(r\mathbf{1}-B)U = 0$ on the left by C we find that $D\mathbf{1}U = 0$, i.e., that $DU = 0$, and since D kills all the generators of M and M is faithful, it follows that $D = 0$, giving an equation of integral dependence for r on I. This proves the first sentence of part (e), and also completes the proof of (d).

Finally, if R is a Noetherian domain and J is integral over I, then if $I = (0)$ we have that $J = (0)$ and we may choose $M = R$, while if $I \neq (0)$ then $J \neq (0)$. In this case we can choose n such that $J^{n+1} = IJ^n$, and we may take $M = J^n$. $\square$