# LECTURE 4: GOING-DOWN THEOREM AND NORMAL RINGS

**Definition 0.1.** *Let $R$ be a domain. We say that $R$ is* normal (integrally closed) *if $R$ equals the integral closure in its fraction field $Q(R)$.*

**Proposition 0.2.** *Let $R$ be a ring and $S$ be a module finite $R$-algebra. Let $I$ be an ideal of $R$ and let $x \in IS$. Then there exists an integral dependence relation*

$$x^h + a_0 x^{h-1} + \cdots a_{h-1} x + a_h = 0,$$

*with $a_i \in I^i$ for all $i = 1, \dots, h$.*

*Proof.* Let us call the $R$-module generators of $S$ by $y_1, \dots, y_h$.

Since $x \in IS$, we see that $y_i x = \sum_{i=1}^{h} r_{ij} y_j$, with $r_{ij} \in I$, for all $j = 1, \dots, h$.

So, $\underline{y}(xI_h - A) = 0$, where $A = (r_{ji})$ and $\underline{y} = (y_1, \dots, y_h)$.

After multiplying by the adjunct of $xI_h - A$ both sides we get that $\det(xI_h - A)$ kills $\underline{y}$, which means that it kills each $y_1, \dots, y_h$. This means that $\det(xI_h - A)$ annihilates $S$ . Since $1 \in S$, therefore $\det(xI_h - A) = 0$.

Expanding $\det(xI_h - A) = 0$, and recall that $r_{ij} \in I$ we obtain an integral dependence of the required form.

□

**Proposition 0.3.** *Let $R \subseteq S$ be domains, $Q(R) = K \subseteq Q(S) = L$, and $s \in S$ be integral over $R$, with $R$ normal. Then the minimal polynomial $f$ of $s$ over $K$ has coefficients in $R$ and for every $g \in R[x]$ with $g(s) = 0$, $f|g$ in $R[x]$.*

*Moreover, if $S$ is module finite over $R$ and $s \in \mathfrak{p}S$, for a prime ideal $\mathfrak{p}$ in $R$, then the coefficients of $f$ belong to $\mathfrak{p}$.*

*Proof.* We can enlarge $S$ to a field extension, if needed. Let $f \in K[x]$ be the minimal polynomial for $s$ over $K$. Then $f = (x - s_1) \cdots (x - s_n)$, a decomposition in linear factors over an algebraic closure of $K$, with $s = s_1$. Let $F \in R[x]$ be a monic polynomial that gives the integral dependence of $s$ over $R$. So $f|F$ in $K[x]$. Then $F(s_i) = 0$ implies $s_i$ are integral over $R$ since $F \in R[x]$. But $f \in K[x]$ and all it coefficients are algebraic combinations of $s_1, ..., s_n$, and hence integral over $R$. But $R$ is normal so the coefficients of $f$ must belong to $R$, therefore $f \in R[x]$.

Let $g \in R[x]$, with $g(s) = 0$. Apply the division and remainder theorem over $R$ to obtain $g = qf + r$, with $q, r \in R[x]$, and $\deg r < \deg f$. Also, $g = q'f$ in $K[x]$ since $f$ is the minimal polynomial of $s$ over $K$. By the uniqueness of the division and remainder theorem over $K[x]$, we have $q = q'$, and $r = 0$.

If $s \in \mathfrak{p}S$, then by the above Proposition $s$ satisfies an integral dependence $F$ with coefficients in $\mathfrak{p}$. Consider again the roots of the minimal polynomial $f$: $s_1, \ldots, s_n$.

But $s$ can be mapped under an $K$-automorphism of the algebraic closure onto any of the conjugates of $s$, so the conjugates also satisfy the same integral dependence relation $F$. Therefore there exists $h$ such that $s_i^h \in \mathfrak{p}S$. But by the lying over property there exists $P$ prime in $S$ such that $P \cap R = \mathfrak{p}$, so $\mathfrak{p}S \subseteq P$ and $s_i \in P$. The coefficients of $f$ are in $R$ and are polynomial functions in $s_1, \ldots, s_n$ and so they belong to $P \cap R = \mathfrak{p}$.

□

**Theorem 0.4.** *(Going-Down) Let $R \subseteq S$ be an integral extension of domains with $R$ normal. Let $\mathfrak{p}, \mathfrak{q} \in Spec(R)$ with $\mathfrak{p} \subset \mathfrak{q}$, and let $Q \in Spec(S)$ with $Q \cap R = \mathfrak{q}$ (which it is known to exist under our hypotheses by the lying over property). Then $\exists\, P \in Spec(S)$ with $P \cap R = \mathfrak{p}$, and $P \subset Q$.*

*Proof.* Let $T = R \setminus \mathfrak{p}$, and $T' = S \setminus Q$, where both are multiplicative sets, so $T \cdot T'$ is also.

Let us show that $\mathfrak{p}S \cap TT' = \emptyset$ Let $x \in \mathfrak{p}S \cap TT'$. Then $x = uv$ with $u \in T$, and $v \in T'$. Since $x \in \mathfrak{p}S$, $x = \sum a_i s_i$ with $a_i \in \mathfrak{p}$, $s_i \in S$. We can replace $S$, $Q$, and $S \setminus Q$ by $S' = R[v, s_1, ..., s_k]$, $Q \cap S'$, and $S' \setminus (Q \cap S') = T''$, and assume $S$ is finitely generated as an $R$-algebra. But $S$ is integral, so $S$ is module-finite over $R$.

Let $f$ be the minimal polynomial of $v$ over $K = Q(R)$. Then $R$ normal implies $f \in R[x]$ (by above proposition) with $f = z^d + r_{d-1}z^{d-1} + \cdots + r_1 z + r_0$. Let $g = z^d + ur_{d-1}z^{d-1} + \cdots + u^{d-1}r_1 z + u^d r_0$. Then $g(uz) = u^d f(z) = 0$. But since $u \in R \setminus \{0\} \subseteq K \setminus \{0\}$, we have $K[uv] = K[v] \supseteq K$, with the degree of the extension equal to $\deg f$. Using that

$\deg g = d$, we conclude that $g$ is the minimal polynomial of $uv$ over $K$. But $x \in \mathfrak{p}S$, so by the above proposition we see that the coefficients of $g$ belong to $\mathfrak{p}$: we have that $u^i r_{d-1} \in \mathfrak{p}$. But $u \notin \mathfrak{p}$, so $r_0, ..., r_{d-1} \in \mathfrak{p}$. Since $f(v) = 0$ by definition of $f$, we conclude that $v^d \in \mathfrak{p}$, so $v \in \mathfrak{p} \subset \mathfrak{q} \subset Q$, a contradiction since $v \notin Q$. So $\mathfrak{p}S \cap TT' = \emptyset$.

Finally, take $\mathfrak{p}S \subseteq P$ with $P \cap TT' = \emptyset$, and $P \in \operatorname{Spec}(R)$. We know that this prime ideal exists from a previous result. Then $P \cap R = \mathfrak{p}$ because $\mathfrak{p} \subseteq \mathfrak{p}S \cap R \subseteq P \cap R$ and if $a \in P \cap R$, with $a \notin \mathfrak{p}$ then $a \in P \cap TT' = \emptyset$, and $P \cap T' = \emptyset$ implies $P \subseteq Q$ since $T' = S \setminus Q$. □

**Corollary 0.5.** *Under the hypotheses of the Going-Down Theorem, we have that* $\operatorname{ht}(Q) = \operatorname{ht}(Q \cap R)$, *for any prime ideal* $Q$ *in* $S$.

**Proposition 0.6.** *Let* $R \subset S$ *be an integral extension. Then* $T^{-1}R \subset T^{-1}S$ *is also integral, for any multiplicative set* $T$ *in* $R$.

*Proof.* Let $x = s/t$ with $s \in S, t \in T$. Since

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

for some $n\mathbb{N}$, and $a_1, \ldots, a_n \in R$, we see that

$$(s/t)^n + (a_1/t)(s/t)^{n-1} + \cdots a_n/t^n = 0$$

is an integral dependence relation of $x$ over $T^{-1}R$.

□

**Proposition 0.7.** *Let* $R$ *be a normal domain. Then for all* $T$ *multiplicative sets in* $R$, $T^{-1}R$ *is normal.*

*Proof.* First note that $T^{-1}R$ is a domain as well and $Q(T^{-1}R = Q(R)$

Let $x = r/s$ with $r \in R, s \in S$. Assume that $x$ is integral over $T^{-1}R$:

$$(r/s)^n + a_1/b_1(r/s)^{n-1} + \cdots + a_n/b_n = 0,$$

where $n \in \mathbb{N}$, $a_i, b_i \in R$, and $b_i \in T$.

Multiply this by $(b_1 \cdots b_n)^n$ to get that $(b_1 \cdots b_n)x$ is integral over $R$. So, $(b_1 \cdots b_n)x$ is in $R$ because $R$ is a normal. Then

$$x = b_1 \cdots b_n \cdot x \cdot \frac{1}{b_1} \cdots \frac{1}{b_n}$$

is an element of $T^{-1}R$ as needed.

$\square$

**Theorem 0.8.** *Let $R$ be a domain. Then the following assertions are equivalent:*

(1) *$R$ is normal;*
(2) *$T^{-1}R$ is normal for any multiplicative set $T \subset R$;*
(3) *$R_\mathfrak{p}$ is normal for any $\mathfrak{p}$ prime ideal of $R$;*
(4) *$R_\mathfrak{m}$ is normal for any $\mathfrak{m}$ maximal ideal of $R$.*

*Proof.* We have seen that (1) implies (2). Clearly (2) implies (3) and (3) implies (4).

Now let us assume (4). Let $x \in Q(R)$ integral over $R$. Note that for any maximal ideal $\mathfrak{m}$ of $R$, $x \in Q(R_\mathfrak{m}) = Q(R)$ and $x$ is integral over $R_\mathfrak{m}$. So, $x \in R_\mathfrak{m}$. But we know that $\cap_\mathfrak{m} R_\mathfrak{m} = R$ so $x \in R$ (to see the last equality, let $M = (R + Rx)/R$ which is an $R$-module. Note that $M_\mathfrak{m} = 0$ for any maximal ideal $\mathfrak{m}$ of $R$. So, $M = 0$. which means that $x \in R$.) $\square$

This last theorem justifies the following definition:

**Definition 0.9.** *Let $R$ be a reduced ring (i.e. $R$ has no nilpotents). We say that $R$ is normal if $R_\mathfrak{p}$ is a normal domain for every $\mathfrak{p}$ prime ideal in $R$.*

**Theorem 0.10.** *Let $(R, \mathfrak{m})$ be local domain which is not a field. the following assertions are equivalent:*

(1) *$R$ is a PID;*
(2) *$R$ is Noetherian and $\mathfrak{m}$ is principal;*
(3) $\cap_{k \geq 0} \mathfrak{m}^k = 0$ *and $\mathfrak{m}$ is principal;*
(4) *There is an element $u \in R$ such that every element of $R$ is of the form $su^t$, where $s$ is a unit and $t \geq 0$ (such an element is called an uniformising element of $R$).*

*Proof.* It is clear that (1) implies (2) and (2) implies (3) (by Krull's Intersection Theorem).

Assume (3). By Krull's Intersection Theorem, for all $x \in \mathfrak{m} = (u)$, there exists $t \geq 0$ maximal such that $x = su^t$. The maximality of $t$ shows that $s$ is not in $\mathfrak{m} = (u)$ so $s$ is a unit. Hence we have (4).

Now assume (4). Let $I$ be an ideal of $R$. Let $t$ minimum such that there exists $su^t \in I$ for some $s$ unit. Clearly $I = (u^t)$, so $R$ is PID, hence (1).

□

**Definition 0.11.** *A local PID which is not a field is called a* discrete valuation ring*, or for short* DVR*.*

**Corollary 0.12.** *Let $(R, \mathfrak{m})$ be a DVR. Then every ideal $I$ is a power of $\mathfrak{m}$.*

*Proof.* In course of (4) implies (1) we showed that $I = (u^t)$, for some $t$, so $I = (\mathfrak{m})^t$.

□