Commutative Algebra

Keerthi Madapusi

Contents

CHAPTER 1

Graded Rings and Modules I: Basics

chap:grm

1. Basic definitions

grm-graded-rings

DEFINITION 1.1.1. A $\mathbb{Z}$-*graded ring* R is a ring equipped with a direct sum decomposition into ideals $R = \bigoplus_{n\in\mathbb{Z}} R_n$ satisfying $R_n R_m \subset R_{n+m}$, for all pairs $(n, m) \in \mathbb{Z}^2$.

We say that the ring R is *positively graded* if $R_n = 0$, for all $n < 0$.

A *homomorphism* between graded rings R and S is a ring homomorphism $\phi : R \to S$ such that $\phi(R_n) \subset S_n$, for all $n \in \mathbb{Z}$.

We will usually refer to $\mathbb{Z}$-graded rings as just graded rings.

Observe that with this definition the ideal $R_0 \subset R$ is a ring in its own right. Also note that any ring R is a graded ring with the *trivial grading*: $R_0 = R$ and $R_n = 0$, for all $n \neq 0$.

DEFINITION 1.1.2. A *homogeneous* or *graded module* over a graded ring R is an R-module M equipped with a direct sum decomposition $M = \bigoplus_{n\in\mathbb{Z}} M_n$ of R_0-submodules of M such that $R_n M_m \subset M_{n+m}$, for all pairs $(n, m) \in \mathbb{Z}^2$.

A *graded submodule* of a graded submodule M is a graded R-module N such that $N_n \subset M_n$, for all $n \in \mathbb{Z}$.

An element $0 \neq x \in M$ is *homogeneous of degree* n if $x \in M_n$, for some $n \in \mathbb{Z}$. We denote the degree of x in this case by $\deg x$.

If $x \in M$ is any element, then we can express it uniquely as a sum $\sum_i x_i$, where each x_i is homogeneous. These x_i will be called the *homogeneous components* of x.

A *homogeneous* or *graded* ideal $I \subset R$ is just a graded R-submodule of R. We'll refer to $R^+ = \bigoplus_{n\neq 0} R_n$ as the *irrelevant ideal* of R.

Given any graded R-module M, and any R-submodule $N \subset M$, we set $N^* \subset M$ to be the R-submodule generated by all the homogeneous components of the elements of N. As we will see in the Proposition below, N^* is then a graded R-submodule of M.

The next two Propositions list some basic properties of homogeneous ideals and graded modules.

grm-graded-modules

PROPOSITION 1.1.3. *Let M be a graded R-module, and let $N \subset M$ be an R-submodule (not necessarily graded).*

(1) *M can be generated by homogeneous elements.*
(2) *If N is generated by homogeneous elements, then N contains the homogeneous components of each of its elements. In particular, $N = \bigoplus_{n\in\mathbb{Z}}(N \cap M_n)$ is a graded R-submodule of M.*
(3) *$N^* \subset N$ is the largest graded ideal of R contained in N.*

PROOF. (1) Just take the generators to be the elements of M_n, for each $n \in \mathbb{Z}$.

(2) Suppose $a = \sum_n a_n \in M$, with $a_n \in M_n$. Let M be generated by homogeneous elements $\{b_i : i \in I\}$. Then $a = \sum_i r_i b_i$, for $r_i \in R$ homogeneous. This means that

$$a_n = \sum_{\deg r_i + \deg b_i = n} r_i b_i \in M.$$

(3) It follows from (2) that N^* is graded. If $P \subset N$ is any other graded ideal, then P is generated by homogeneous elements, and is thus contained in N^*.

□

grm-pullback-homogeneous

LEMMA 1.1.4. *Let $\phi : R \to S$ be a homomorphism of graded rings. For any homogeneous ideal $I \subset S$, the contraction $\phi^{-1}(I) \subset R$ is also homogeneous. For any homogeneous ideal $J \subset R$, the extension $JS \subset S$ is again homogeneous.*

PROOF. If $I = \bigoplus_n I_n$, then $\phi^{-1}(I) = \bigoplus_n \phi^{-1}(I_n)$. The second statement follows from (2) of the previous Proposition, since JS is generated by homogeneous elements. □

grm-graded-ideals

PROPOSITION 1.1.5. *Let $I \subset R$ be an ideal.*

(1) *If I is graded, then R/I has a natural grading under which the natural map $R \to R/I$ is a homomorphism of graded rings.*
(2) *If I is graded, there is a one-to-one correspondence between homogeneous ideals containing I and ideals in R/I.*
(3) *If I is graded, then so is* $\operatorname{rad} I$.

PROOF. (1) Suppose $I = \bigoplus_n I_n$, where $I_n = I \cap R_n$. Give R/I the grading obtained from the direct sum decomposition $\bigoplus_n R_n/I_n$. It's clear that the map $R \to R/I$ is a homomorphism of graded rings.
(2) Follows immediately from the Lemma above, and the corresponding statement for rings.
(3) Suppose $a = \sum_n a_n \in \operatorname{rad} I$, with $a_n \in R_n$, and let $d = \max\{n : a_n \neq 0\}$. There is some $k \in \mathbb{N}$ such that $a^k \in I$. Since I contains all homogeneous components of its elements, this implies that $a_d^k \in I$, and so $a_d \in \operatorname{rad} I$. Now, subtract a_d from a and proceed inductively.

□

DEFINITION 1.1.6. A *morphism* between two graded R-module M and N is an R-module map $\varphi : M \to N$ such that $\varphi(M_n) \subset N_n$, for all $n \in \mathbb{Z}$.

This definition gives us a *category* of graded R-modules, which we will denote by $R^{\mathbb{Z}}$-mod.

DEFINITION 1.1.7. For any graded R-module M, and for any integer $n \in \mathbb{Z}$, we define $M(n)$ to be graded R-module with $M(n)_m = M_{n+m}$.

Given a collection $\{M_i : i \in I\}$ of graded R-modules, we define their *direct sum* to be the R-module $N = \bigoplus_i M_i$ equipped with the grading $N_r = \bigoplus_i (M_i)_r$.

A graded R-module M is *free* if there is a collection of integers $\{n_i : i \in I\}$ and an isomorphism

$$\phi : \bigoplus_{i \in I} R(n_i) \xrightarrow{\cong} M$$

of graded R-modules.

A collection of homogeneous elements $\mathscr{M} = \{m_i \in M : i \in I\}$ is *linearly independent* over R if, for every linear relation of the form $\sum_i a_i m_i = 0$, with a_i homogeneous, $a_i = 0$, for all i.

rm-graded-free-criterion

PROPOSITION 1.1.8. *Let M be a graded R-module; then M is free if and only if it is generated by a linearly independent collection of homogeneous elements.*

PROOF. Immediate. □

Observe that, for any R-module M, we have a surjection onto M from a graded free R-module: just choose any collection $\{m_i : i \in I\}$ of generators of M, with $\deg m_i = r_i$, and define a morphism

$$\bigoplus_{i\in I} R(-r_i) \to M$$
$$e_i \mapsto m_i,$$

where, for each i, e_i is a generator of $R(-r_i)$.

2. *Local Rings

grm-secn:star-local

Now we turn to the description of homogeneous primes in a graded ring

grm-homogeneous-primes

PROPOSITION 1.2.1. *If $\mathfrak{p} \subset R$ is any prime, then $\mathfrak{p}^*$ is also prime. Moreover, a homogeneous ideal $I \subset R$ is prime if and only if, for every pair of homogeneous elements $a, b \in R$, with $ab \in I$ and $a \notin I$, we have $b \in I$.*

PROOF. Suppose $a, b \in R$ are such that $ab \in \mathfrak{p}^*$. Let a' and b' be the homogeneous components of a and b respectively of highest degree. Then $a'b' \in \mathfrak{p}^* \subset \mathfrak{p}$; so either $a' \in \mathfrak{p}$ or $b' \in \mathfrak{p}$. Without loss of generality $a' \in \mathfrak{p}$ and hence $a' \in \mathfrak{p}^*$, since a' is homogeneous. If $b' \in \mathfrak{p}^*$, then $(a - a')(b - b') \in \mathfrak{p}^*$, and by an easy inductive argument we can conclude that one of $b - b'$ or $a - a'$ is in $\mathfrak{p}^*$, and so either a or b is in $\mathfrak{p}^*$. Otherwise, $(a - a')b \in \mathfrak{p}^*$, and, by the same argument, the highest degree term of $a - a'$ must be in $\mathfrak{p}^*$. Continuing this way, we find that $a \in \mathfrak{p}^*$. For the second statement, one implication is clear. For the other, just follow the proof of the first statement. □

With this in hand we enter the land of graded localization.

DEFINITION 1.2.2. Given any multiplicative subset $S \subset R$, and a graded R-module M, we define the *homogeneous localization* $(S)^{-1}M$ to be the module of fractions $U^{-1}M$, where $U \subset S$ is the multiplicative subset consisting of all homogeneous elements. This has a natural grading: for an element $\frac{m}{s}$, with $m \in M$ homogeneous and $s \in S$ also homogeneous, we set $\deg \frac{m}{s} = \deg m - \deg s$. One easily checks that this is well-defined.

If $S = R - \mathfrak{p}$, for some prime ideal $\mathfrak{p} \subset R$, we set $M_{(\mathfrak{p})} = (S)^{-1}M$. Observe that $M_{(\mathfrak{p}^*)} = M_{(\mathfrak{p})}$.

This leads naturally to the graded version of local rings.

DEFINITION 1.2.3. A graded ring R is **local* if it has a unique maximal homogeneous ideal $\mathfrak{m}$. We'll call $\mathfrak{m}$ a *maximal ideal.

REMARK 1.2.4. We've already seen some examples of *local rings. For any homogeneous prime $\mathfrak{p} \subset R$, $R_{(\mathfrak{p})}$ is *local with *maximal ideal $\mathfrak{p}R_{(\mathfrak{p})}$.

Also, if R is positively graded and R_0 is a local ring with maximal ideal $\mathfrak{m}_0$, then we see that $\mathfrak{m}_0 \oplus R^+$ is the unique *maximal ideal, and so R is again *local.

Observe that if $(R, \mathfrak{m})$ is *local with *maximal ideal $\mathfrak{m}$, then $R/\mathfrak{m}$ is a graded ring without any non-trivial graded ideals. The next Proposition describes such rings. They are the analogues of fields in the graded category.

grm-graded-fields

PROPOSITION 1.2.5. *The following are equivalent for a graded ring R:*

1. *The only homogeneous ideals of R are 0 and R.*
2. *Every non-zero homogeneous element is invertible.*
3. *$R_0 = k$ is a field, and either $R = k$, or $R = k[t, t^{-1}]$, for some indeterminate t of positive degree.*

PROOF. (3) $\Rightarrow$ (2) $\Leftrightarrow$ (1) is clear. So we only need to show (2) $\Rightarrow$ (3). Since every element of R_0 is invertible, we see that R_0 must be a field k. If $R = R_0 = k$, then we're done. Otherwise, let $t \in R$ be a homogeneous element of smallest positive degree d (this must exist, since if we had an element of negative degree, then its inverse would have positive degree). In this case, since t is invertible, we have a natural homomorphism

$$\phi : k[x, x^{-1}] \longrightarrow R,$$

where x is an indeterminate of degree d, that takes x to t. We'll show that this map is an isomorphism, which will finish our proof. So suppose $f = \sum_i a_i x^i \in \ker \phi$; then $\sum_i a_i t^i = 0$ in R, which implies that $a_i t^i = 0$, for all i, and so $f = 0$. This shows injectivity. Now, let $a \in R$ be a homogeneous element of degree i. If $i = 0$, then $a \in k$, and we're done. Otherwise, let $i = qd + r$, where $0 \leq r < d$. If $r > 0$, then at^{-q} has degree r, which contradicts the fact that t was the element with least positive degree. Hence $r = 0$, and $i = qd$; but in this case $at^{-q} \in k$, and so $a = ct^q = \phi(cx^q)$, for some $c \in k$. This shows surjectivity, and finishes our proof. □

The graded ring $k[t, t^{-1}]$ behaves like a field in another familiar way.

raded-modules-field-free

PROPOSITION 1.2.6. *Let M be a graded $k[t, t^{-1}]$-module. Then M is free; in particular, if M is finitely generated, then every minimal set of homogeneous generators for M has the same cardinality.*

PROOF. This is the usual Zorn's Lemma argument, applied to the collection of all linearly independent subsets of M. The only fact one needs is that if $\mathscr{M} \subset M$ is a linearly independent collection of homogeneous elements, then, for any homogeneous element $n \in M$, $\mathscr{M} \cup \{n\}$ is linearly dependent if and only if n is in the graded submodule generated by $\mathscr{M}$. But this follows immediately from the fact that every homogeneous element in $k[t, t^{-1}]$ is a unit. □

We are now in a position to present Nakayama's lemma for *local rings.

grm-graded-nakayama

PROPOSITION 1.2.7 (Graded Nakayama). *Let $(R, \mathfrak{m})$ be a *local ring, and let M be a finitely generated graded R-module.*

1. *If $N \subset M$ is a graded R-submodule such that $M = N + \mathfrak{m}M$, then $M = N$. In particular, if $\mathfrak{m}M = M$, then $M = 0$.*

(2) *The minimal number of homogeneous generators for M is uniquely determined by the rank of $M/\mathfrak{m}M$ over $R/\mathfrak{m}$.*

PROOF. (1) It suffices to prove the second statement. The first will follow by applying the second to the R-module M/N. Let $\{m_1, \dots, m_t\}$ be generators for M, with $\deg m_i = r_i$. Then we can find $a_j \in \mathfrak{m}$ with $\deg a_j = r_t - r_j$ such that $m_t = \sum_j a_j m_j$. Now, $(1 - a_t) \in R_0 \setminus \mathfrak{m}$ is homogeneous, and is thus invertible. This implies that we can express m_t as a linear combination of m_j, for $j < t$, with coefficients in $\mathfrak{m}$. So $M = (m_1, \dots, m_{t-1})$, and so we can induct on t to conclude that $M = 0$; the only thing we have to prove is the base case when $t = 1$. But then if $m_1 = am_1$, for some $a \in \mathfrak{m}_0$, we see immediately that, since $1 - a$ is invertible, $m_1 = 0$.

(2) Follows from (1) in standard fashion, using (1.2.6) and (1.2.5).

□

3. Finiteness Conditions

DEFINITION 1.3.1. A graded ring R is *finitely generated over* R_0 if it's a finitely generated R_0-algebra. It is *generated by* R_d *over* R_0 if there is an integer $d \in \mathbb{Z}$ such that $R_m = (R_d)^{m/d}$, for all $m \in \mathbb{Z}$, where $(R_d)^n$ is understood to be 0 if $n \notin \mathbb{Z}$.

A graded R-module M is *finitely generated* if it's finitely generated as an R-module.

nitely-generated-modules

PROPOSITION 1.3.2. *Let R be a positively graded ring, finitely generated over R_0, and let M be a finitely generated module over R.*

(1) *R is nilpotent if and only if there is $n_0 \in \mathbb{N}$ such that $R_n = 0$, for all $n \geq n_0$.*
(2) *There is $n_0 \in \mathbb{Z}$ such that $M_n = 0$, for $n \leq n_0$.*
(3) *For every $n \in \mathbb{Z}$, M_n is a finitely generated R_0-module.*
(4) *There is $m_0 \in \mathbb{Z}$ such that $M_{m_0+r} = R_r M_{m_0}$, for all $r \in \mathbb{N}$.*
(5) *There is $m \in \mathbb{Z}$ such that $R_{rm} = (R_m)^r$, for all $r \in \mathbb{N}$.*
(6) *For every $n \in \mathbb{N}$, there is an $m_0 \in \mathbb{Z}$ such that $R_m \subset (R^+)^n$, for all $m > m_0$.*

PROOF. Let $s_1, \dots, s_t$ be generators of R over R_0, with $\deg s_i = k_i$, and let $m_1, \dots, m_u$ be generators of M over R with $\deg m_i = l_i$. Let $\alpha = (\alpha_1, \dots, \alpha_t)$ be a t-tuple of positive integers; then we set

$$\mathbf{s}^\alpha = \prod_{i=1}^{t} s_i^{\alpha_i}.$$

Also, we define $|\alpha|$ to be the sum $\sum_{i=1} \alpha_i$. A *monomial of weight n* is a monomial $\mathbf{s}^\alpha$ with $|\alpha| = n$.

(1) R is nilpotent if and only if, for sufficiently large n, $s_i^n = 0$, for all i. Consider the t-tuples α with $\alpha_i < n$, for all i: there are only finitely many of them. Hence there are only finitely many monomials in $\mathbf{s}^\alpha$ with $\alpha_i < n$. So, in high enough degree, every monomial will be 0. This shows that if R is nilpotent, then it vanishes in large degrees; the other implication is more trivial, and is hence rather trivial indeed.
(2) Take $n_0 = \min_i l_i$.

(3) There are only finitely many monomials $\mathbf{s}^\alpha m_i \in M$ of degree n. These generate M_n over R_0.
(4) Let m be the l.c.m. of the integers $\{k_1, \ldots, k_t\}$, and let $g_i = s_i^{m/k_i}$. Hence $\deg g_i = m$, for all i. Now, there are only finitely many t-tuples α such that $\alpha_i < m/k_i$, for each i. In particular, there are only finitely many elements in M of the form $\mathbf{s}^\alpha m_i$, where $\alpha_j < m/k_j$, for all j. Let m_0 be the maximal of the degrees of such elements. Then, for $r > 0$, consider any monomial x of degree $m_0 + r$. Let $r = qm + r'$, where $q \geq 0$ and $0 \leq r' < m$; then we should be able to factor out q-many monomials of the form g_i till we end up with a monomial x' of degree $M_{m_0+r'}$, where $0 \leq r' < m$. If $r' = 0$, then we're done; otherwise, we can still factor out one additional factor of the form g_j, for some j, and reduce it still further to a monomial $y \in M_{m_0+r'-m}$, in which case we have expressed x' as an element of

$$R_m M_{m_0+r-m} = R_r \left(R_{m-r} M_{m_0+r-m}\right) \subset R_r M_{m_0}.$$

(5) Follows immediately from part (2): take $R = M$, and let $m = m_0$ as obtained in (2).
(6) There are only finitely many t-tuples α such that $|\alpha| < n$. Set

$$m_0 = \max_{|\alpha|<n} \left\{ \sum_j \alpha_j k_j \right\}.$$

Then, for $m > m_0$, any monomial $\mathbf{s}^\alpha$ of degree m will have weight at least n. This is equivalent to saying that $R_m \subset (R^+)^n$, for all $m > m_0$.

□

DEFINITION 1.3.3. A graded ring R is *Noetherian* if it is Noetherian as a ring.

m-noetherian-graded-ring

PROPOSITION 1.3.4. *The following are equivalent for a graded ring R:*

(1) *Every graded ideal of R is finitely generated.*
(2) *R is a Noetherian ring.*
(3) *R_0 is Noetherian, and R is a finitely generated R_0-algebra.*
(4) *R_0 is Noetherian, and both $S_1 = \bigoplus_{n\geq 0} R_n$ and $S_2 = \bigoplus_{n\leq 0} R_n$ are finitely generated R_0-algebras.*

PROOF. (4) ⇒ (3) ⇒ (2) ⇒ (1) is immediate. We prove (1) ⇒ (4): Let $M \subset R_n$ be an R_0-submodule; then $M' = \bigoplus_m R_m M$ is a graded ideal in R; moreover, $M' \cap R_n = M$. Let $M_0 \subset M_1 \subset \ldots$ be a chain of R_0-submodules in R_n; then we can extend this to a chain $M_0 R \subset M_1 R \subset \ldots$ of ideals in R. This chain of graded ideals has to stabilize, and so when we contract back to R_n, we see that the original chain of R_0-submodules must also stabilize. This shows that each R_n is a Noetherian R_0-module; in particular, R_0 is a Noetherian ring.

Consider the ideal $\mathfrak{n} = \bigoplus_{n\geq 1} R_n \subset S_1$; we claim that this is finitely generated. Since $\mathfrak{n}R$ is a finitely generated ideal of R by hypothesis, we see that we can find homogeneous elements $\{x_1, \ldots, x_r\}$ in $\mathfrak{n}$, which generate $\mathfrak{n}R$ over R. If $d = \max \deg x_i$, then any homogeneous element in $\mathfrak{n}$ of degree greater than d can be expressed as a linear combination of the x_i with coefficients in S_1. Since each R_n is finitely generated over R_0, we can pick finitely many homogeneous elements

generating $\bigoplus_{1\leq n\leq d} R_d$ over R_0, and these, together with the x_i, will generate $\mathfrak{n}$ over S_1.

So let $\{y_1, \ldots, y_s\}$ be a finite set of homogeneous generators for $\mathfrak{n}$ over S_1, and let $S' \subset S_1$ be the R_0-subalgebra generated by the y_i. We claim that $S' = S_1$. So for any homogeneous element $x \in S^1$, we need to show that $x \in S'$. We'll do this by induction on $\deg x$. If $\deg x = 0$, then this is clear. So assume $\deg x > 0$, and assume $y \in S'$, for all $y \in S^1$ with $\deg y < \deg x$. But $x = \sum_i a_i y_i$, where $\deg a_i < \deg x$, and so each $a_i \in S'$, from which it follows that $x \in S'$. □

4. Associated Primes and Primary Decomposition

aded-primes-annihilators

PROPOSITION 1.4.1. *Let R be a graded ring, and let M be a graded R-module.*

(1) *A prime $\mathfrak{p}$ is in* $\operatorname{Supp} M$ *if and only if $\mathfrak{p}^*$ is in* $\operatorname{Supp} M$.
(2) *If $m \in M$ is such that $\mathfrak{p} = \operatorname{ann}(m)$ is prime, then $\mathfrak{p}$ is in fact homogeneous, and we can find $m' \in M$ homogeneous, such that $\mathfrak{p} = \operatorname{ann}(m')$.*

PROOF. (1) It is clear that if $M_{\mathfrak{p}} = 0$, then $M_{\mathfrak{p}^*} = 0$. Conversely, suppose $M_{\mathfrak{p}^*} = 0$, and let $m \in M$ be homogeneous. There exists an element $r \in R \setminus \mathfrak{p}^*$ such that $rm = 0$. Since every homogeneous component of rm is also zero, we can assume that r is also homogeneous. But in that case $r \notin \mathfrak{p}$, since every homogeneous element of $\mathfrak{p}$ is in $\mathfrak{p}^*$. This shows that every homogeneous element of M maps to zero in $M_{\mathfrak{p}}$; but then $M_{\mathfrak{p}}$ must be 0.

(2) Suppose $r \in \mathfrak{p}$; we want to show that every homogeneous component of r is also in $\mathfrak{p}$. Equivalently, we will show that, for every homogeneous component r' of r, $r'm = 0$. By an inductive argument, it suffices to show that the homogeneous component t of r of lowest degree annihilates m. Now, suppose $m = \sum_{i=1}^k m_i$, where m_i is homogeneous of degree e_i and $e_p < e_q$, for $p < q$. Now, we have

$$0 = rm = tm_1 + \text{ higher degree terms.}$$

Hence $tm_1 = 0$. We will show $tm = 0$, by induction on k. The $k = 1$ case is already done. Now, observe that

$$tm = \sum_{i=2}^{k} tm_i$$

has fewer homogeneous terms than m. Let $I = \operatorname{ann}(tm)$; clearly $\mathfrak{p} \subset \operatorname{ann}(tm)$. If there exists $s \in I \setminus \mathfrak{p}$, then $stm = 0$, and so $st \in \mathfrak{p}$, which implies that $t \in \mathfrak{p}$. Otherwise $\mathfrak{p} = I$ is the annihilator of an element with fewer homogeneous components, and so is homogeneous by the inductive hypothesis.

Now, since $\mathfrak{p}$ is homogeneous, we see that $\mathfrak{p} \subset \operatorname{ann}(m_i)$, for all $1 \leq i \leq k$. Therefore, we have

$$\operatorname{ann}(m) = \mathfrak{p} \subset \bigcap_i \operatorname{ann}(m_i) \subset \operatorname{ann}(m).$$

Hence $\mathfrak{p} = \bigcap_i \operatorname{ann}(m_i)$, which implies that $\operatorname{ann}(m_i) = \mathfrak{p}$, for some i.

□

graded-associated-primes

COROLLARY 1.4.2. *Let R be a graded Noetherian ring, and let M be a finitely generated graded R-module.*

(1) *Every prime in* $\operatorname{Ass} M$ *is homogeneous. In particular, the minimal primes of R are homogeneous.*
(2) *Given any primary decomposition of a graded submodule $N \subset M$ of the form $N = \bigcap_{i=1}^{t} N_i$, the decomposition $N = \bigcap_{i=1}^{t} N_i^*$ is also a primary decomposition of N. In particular, we can choose the primary components of N to be homogeneous.*

PROOF. (1) Follows immediately from part (3) of the Proposition.
(2) Factoring out by N, and using part (1), it suffices to show that if $M_1 \subset M$ is a P-primary submodule, for some homogeneous prime $P \subset R$, then M_1^* is also P-primary. That is, we want to show that $\operatorname{Ass}(M/M_1^*) = \{P\}$. Now, suppose $Q \in \operatorname{Ass}(M/M_1^*)$; then, Q is homogeneous, and, by the Proposition, we can choose $m \in M \setminus M_1^*$ homogeneous such that $(M_1^* :_R m) = Q$. Now, since m is homogeneous, m is not in M_1 either, and so $Q \subset (M_1 :_R m) \subset P$. We claim that $(M_1 :_R m) = Q$: this will show that $Q = P$, and will thus finish our proof. Suppose $r = \sum_{i=1}^{s} r_i \in R$ is such that $rm \in M_1$. Then $r_i m \in M_1^*$, for each i, and so $r_i \in Q$, for each i. This shows that in fact $r \in Q$, and so we're done.

□

graded-associated-series

COROLLARY 1.4.3. *With the hypotheses as in the Corollary above, there is a descending chain of graded submodules*

$$M = M_n \supset M_{n-1} \supset M_{n-2} \supset \ldots \supset M_0 = 0,$$

such that, for all $1 \leq i \leq n$, there is a homogeneous prime $P_i \subset R$ and an integer $n_i \in \mathbb{Z}$ such that

$$M_i/M_{i-1} \cong (R/P_i)(n_i).$$

PROOF. Since M is finitely generated over a Noetherian ring, it is itself Noetherian and so has the ascending chain condition. Therefore, it's enough to find $M_1 \subset M$ such that $M_1 \cong (R/P_1)(n_1)$, for some $n_1 \in \mathbb{Z}$ and some homogeneous prime $P_1 \subset R$. For this, we can take P_1 to be any associated prime of M, and let $m \in M$ be any homogeneous element such that $P_1 = \operatorname{ann}(m)$. In this case, if $\deg m = r$, then for $n_1 = -r$, we have an isomorphism

$$(R/P_1)(n_1) \xrightarrow{\cong} Rm \subset M,$$

which sends 1 to m. □

We finish with the graded version of prime avoidance.

grm-prime-avoidance

PROPOSITION 1.4.4 (Prime Avoidance in the Graded Case). *Let R be a graded ring and let $P_1, \ldots, P_r \subset R$ be primes. If $J \subset R$ is a homogeneous ideal generated by elements of positive degree, such that $J \subset \bigcup_{i=1}^{r} P_i$, then there exists $i \in \{1, \ldots, r\}$ such that $J \subset P_i$.*

PROOF. Let $S = \oplus_{n \geq 0} R_n$; if $J \cap S \subset P_i \cap S$, then since J is generated by elements of positive degree $J \subset P_i$, we see that $J \subset P_i$. So, replacing R by S, we can assume that R is positively graded. Moreover, we can also replace P_i with P_i^*, and assume that each of the P_i is homogeneous.

Now, we'll prove the statement by induction on r. If $r = 1$, this is trivial; so we can assume that $r > 1$. Now, by induction, we can assume that J is not contained in a smaller union of primes. Then, for $1 \leq i \leq r$, there is a homogeneous element $a_i \in J$ such that $a_i \notin \bigcup_{j \neq i} P_j$, and so $a_i \in P_i$. Let $u, v \in \mathbb{N}$ be such that $u \deg a_1 = v\left(\sum_{i>1} \deg a_i\right)$, and set $a = a_1^u + \left(\prod_{i>1} a_2\right)^v$. Then, we find that $a \notin P_i$, for all i, which is a contradiction. □

5. The Category of Graded Modules

Definition 1.5.1. A *homomorphism* of graded R-modules M and N of degree m is an R-module homomorphism $\phi : M \to N$ such that $\phi(M_n) \subset N_{n+m}$, for each $n \in \mathbb{Z}$. We denote the group of such homomorphisms by ${}^*\operatorname{Hom}_R(M, N)$.

A *morphism* of graded R-modules M and N is just a homomorphism of degree 0. This gives us a category of graded R-modules, which we will denote by $R^{\mathbb{Z}}$-mod.

Note on Notation 1 (Warning!). A homomorphism between graded R-modules is *not* the same thing as a morphism in the category $R^{\mathbb{Z}}$-mod!

grm-graded-hom

Proposition 1.5.2. *The abelian group ${}^*\operatorname{Hom}_R(M, N)$ is naturally a graded R-module. If M is finitely generated, then ${}^*\operatorname{Hom}_R(M, N) \cong \operatorname{Hom}_R(M, N)$ as (ungraded) R-modules.*

Proof. Let ${}^*\operatorname{Hom}_R(M, N)_r$ be the set of homomorphisms between M and N of degree r. Then it's immediate that this is an R_0-module, and that if $\phi \in {}^*\operatorname{Hom}_R(M, N)_r$ and $r \in R_s$, then

$$r\phi \in {}^*\operatorname{Hom}_R(M, N)_{r+s}$$

(where we treat ${}^*\operatorname{Hom}_R(M, N)$ as an R-submodule of $\operatorname{Hom}_R(M, N)$).

Now, suppose M is generated by finitely many homogeneous elements $m_1, \ldots, m_k$. Let $n_{ij} \in N$ be homogeneous elements such that $\phi(m_i) = \sum_j n_{ij}$. Let ϕ_{ij} be the homomorphism from M to N defined by

$$\phi_{ij}(m_r) = \begin{cases} n_{ij}, \text{ if } i = r \\ 0, \text{ otherwise.} \end{cases}$$

It's immediate that $\phi_{ij} \in {}^*\operatorname{Hom}_R(M, N)_{r_{ij}}$, where $r_{ij} = \deg n_{ij} - \deg m_i$. Moreover, it also follows that $\phi = \sum_{i,j} \phi_{ij}$, since this identity is clearly true on the generators m_i. This finishes our proof. □

The tensor product $M \otimes_R N$ of two graded R-modules M and N is again naturally graded. We set $(M \otimes_R N)_n = \oplus_{i+j=n} M_i \otimes_{R_0} N_j$.

Definition 1.5.3. For $n \in \mathbb{Z}$, and a graded R-module M, we define $M(n)$ to be the graded R-module with $M(n)_m = M_{n+m}$. Observe that $M(n) = M \otimes_R R(n)$.

Remark 1.5.4. With this definition, we see that

$${}^*\operatorname{Hom}_R(M, N) = \oplus_{n \in \mathbb{Z}} \operatorname{Hom}_{R^{\mathbb{Z}}\text{-mod}}(M(n), N).$$

The next Proposition should be predictable.

r-hom-tensor-adjointness

Proposition 1.5.5. *Let R and S be graded rings, and let M be a graded (R, S)-bimodule (in the obvious sense). Then, for every graded R-module N and every graded S-module P, we have a natural isomorphism of abelian groups:*

$$\operatorname{Hom}_{R^{\mathbb{Z}}\text{-}mod}(M \otimes_S P, N) \cong \operatorname{Hom}_{S^{\mathbb{Z}}\text{-}mod}(P, {}^*\operatorname{Hom}_R(M, N)).$$

PROOF. Let $f : M \otimes_S P \to N$ be a morphism of graded R-modules. We define $\Phi(f) : P \to^* \mathrm{Hom}_R(M, N)$ by

$$\Phi(f)(p)(m) = f(m \otimes p),$$

for p and m homogeneous. If $\deg p = r$, then we see that $\Phi(f)(p)$ is a homomorphism of degree r. So $\Phi(f)$ is in fact a morphism of graded S-modules. Now, if $g : P \to^* \mathrm{Hom}_R(M, N)$ is a morphism of graded S-modules, we define $\Psi(g) : M \otimes_S P \to N$ by

$$\Psi(g)(m \otimes p) = g(p)(m),$$

for m and p homogeneous. If $\deg m = r$ and $\deg p = s$, then $\deg g(p) = s$, and so $\deg g(p)(m) = r + s = \deg m \otimes p$. This shows that $\Psi(g)$ is a morphism of graded R-modules. Now it's easy to check that Φ and Ψ are inverses to each other. □

grm-star-hom-star-tensor

COROLLARY 1.5.6. *With the hypotheses as in the Proposition, suppose $R = S$. We have an isomorphism of graded R-modules:*

$$^*\mathrm{Hom}_R(M \otimes_R P, N) \cong^* \mathrm{Hom}_R(P, ^*\mathrm{Hom}_R(M, N)).$$

PROOF. Follows from the Proposition and the fact that

$$^*\mathrm{Hom}_R(M, N) = \oplus_{n\in\mathbb{Z}} \mathrm{Hom}_{R^{\mathbb{Z}}\text{-mod}}(M(n), N).$$

□

REMARK 1.5.7. This shows that $R^{\mathbb{Z}}$-mod is a closed, symmetric, monoidal category if that's any use.

For the next Proposition, we'll need some definitions from [CT, **??**], [CT, **??**] and [CT, **??**].

es-grothendieck-category

PROPOSITION 1.5.8. *For any graded ring R, $R^{\mathbb{Z}}$-mod is a Grothendieck category. In particular, $R^{\mathbb{Z}}$-mod has enough injectives.*

PROOF. First, we must show that $R^{\mathbb{Z}}$-mod is abelian. For this, since a monomorphism (resp. an epimorphism) in $R^{\mathbb{Z}}$-mod is still a monomorphism (resp. an epimorphism) when viewed as a morphism in R-mod, it suffices to show that the kernel and the cokernel of every morphism $\phi : M \to N$ lies in $R^{\mathbb{Z}}$-mod. In fact, it's enough to show that the kernel is homogeneous, since $\mathrm{im}\,\phi = M/\ker\phi$ will then also be homogeneous, which implies that $\mathrm{coker}\,\phi = N/\mathrm{im}\,\phi$ will be homogeneous. To check that the kernel is homogeneous, it's enough to check that if $\phi(\sum_i m_i) = 0$, with m_i homogeneous of distinct degrees, then $\phi(m_i) = 0$. But this follows immediately from the fact that ϕ preserves degrees and from the direct sum decomposition of N.

Now, we will show that $R^{\mathbb{Z}}$-mod satisfies axiom Ab-3; that is, it has all small direct sums. This is immediate from the trivial observation that if $\{M_i\}$ is a collection of graded R-modules, then $\oplus_i M_i$ has a natural grading with the n^{th} component being $\oplus_i (M_i)_n$. It is also trivial that $R^{\mathbb{Z}}$-mod satisfies axiom Ab-5. It remains now to show that $R^{\mathbb{Z}}$-mod has a generator: for this, take $U = \oplus_{n\in\mathbb{Z}} R(n)$. If N, M are two graded R-modules, with $N \neq M$, then let $m \in M \setminus N$ be any homogeneous element. The morphism $R(-\deg m) \to M$ that takes 1 to m doesn't have its image in N. This finishes the proof of the first assertion. The second follows from [CT, **??**]. □

6. Dehomogenization: Preliminaries for Projective Geometry

This section will be fundamental in the construction of projective schemes.

DEFINITION 1.6.1. If $S = \{f^n : n \in \mathbb{N}\}$, for some homogeneous element $f \in R$, we will denote $(S)^{-1}M$ by M_f as usual, and denote the zeroth degree submodule of M_f by $M_{(f)}$. Note that $M_{(f)}$ is an $R_{(f)}$-module.

When $\deg f = 1$, then $R_{(f)}$ is very easy to describe. We'll do that in the next Lemma.

ogeneous-deg-one-element

LEMMA 1.6.2. *Let $f \in R$ be a homogeneous element of degree one. Then we have an isomorphism*

$$R_f = R_{(f)}[f, f^{-1}] \cong R_{(f)}[t, t^{-1}],$$

where t is an indeterminate. In particular, $R_{(f)} \cong R_f/(f-1)$; we call this a dehomogenization *of R_f.*

PROOF. Let $x =\in R_f$, with $\deg x = t$. Then $x = f^t y$, where $y = f^{-t}x \in R_{(f)}$. This shows that $R_f = R_{(f)}[f, f^{-1}]$. Consider now the natural surjection of graded rings

$$R_{(f)}[t, t^{-1}] \longrightarrow R_{(f)}[f, f^{-1}],$$

which sends t to f. This is also injective, since $\sum_i a_i t^i$ maps to 0 iff $a_i f^i = 0$, for all i iff $a_i = 0$ for all i. The second statement follows immediately from this. □

-loc-homogeneous-element

PROPOSITION 1.6.3. *Every homogeneous element $f \in R$ induces a functor from $R^{\mathbb{Z}}$-mod to $R_{(f)}$-mod which takes M to $M_{(f)}$. Here are some properties of this functor.*

1. *$M \mapsto M_{(f)}$ is an exact functor.*
2. *For two graded R-modules M and N, we have a natural injection*
$$M_{(f)} \otimes_{R_{(f)}} N_{(f)} \to (M \otimes_R N)_{(f)}.$$
If $\deg f = 1$, then this is in fact an isomorphism.
3. *If $\deg f = 1$, then for every $n \in \mathbb{Z}$, and every graded R-module M, $M(n)_{(f)} \cong M_{(f)}$. In particular, $R(n)_{(f)} \cong R_{(f)}$ is a free $R_{(f)}$-module of rank 1.*
4. *For two graded R-modules M and N, we have a natural homomorphism*
$$^* \operatorname{Hom}_R(M, N)_{(f)} \to \operatorname{Hom}_{R_{(f)}}(M_{(f)}, N_{(f)}).$$
If M is finitely presented, and $\deg f = 1$, then this is in fact an isomorphism.
5. *Let $\{M_i : i \in I\}$ be a filtered system of graded R-modules. Then*
$$(\operatorname{colim}_i M_i)_{(f)} \cong \operatorname{colim}_i (M_i)_{(f)}.$$
6. *Suppose now that f has positive degree. Pick an integer $d \in \mathbb{Z}$ and set $M^{\geq d} = \oplus_{n \geq d} M_n$. Then, the natural inclusion $M^{\geq d} \to M$ induces an isomorphism*
$$M^{\geq d}_{(f)} \cong M_{(f)}$$

PROOF. (1) We know that $M \mapsto M_f$ is an exact functor from $R^{\mathbb{Z}}$-mod to $R_f^{\mathbb{Z}}$-mod. Now, a sequence of morphisms in $R_f^{\mathbb{Z}}$-mod is exact iff it's exact in each graded component. This tells us that $M \mapsto M_{(f)} = (M_f)_0$ is also an exact functor.

(2) Observe that we have a natural isomorphism of graded R-modules

$$M_f \otimes_{R_f} N_f \cong (M \otimes_R N)_f.$$

Under this isomorphism $M_{(f)} \otimes_{R_{(f)}} N_{(f)}$ injects into $(M \otimes_R N)_{(f)}$. Now suppose $\deg f = 1$; we write down the natural map explicitly

$$\begin{aligned} M_{(f)} \otimes_{R_{(f)}} N_{(f)} &\longrightarrow (M \otimes_R N)_{(f)} \\ \frac{m}{f^r} \otimes \frac{n}{f^s} &\mapsto \frac{m \otimes n}{f^{r+s}}. \end{aligned}$$

To prove that it's surjective, it's enough to show that any element of the form $x = \frac{m \otimes n}{f^t}$ is in the image of the homomorphism. For this, observe that $\deg m + \deg n = t$; moreover by multiplying both halves of the fraction by suitable multiples of f, we can assume that both $\deg m = r$ and $\deg n = s$ are positive. Then, we see that $\frac{m}{f^r} \otimes \frac{n}{f^s}$ maps to x. The fact that $\deg f = 1$ was crucial for this splitting to be possible.

(3) From (2), we have

$$N(n)_{(f)} = (N \otimes_R R(n))_{(f)} \cong N_{(f)} \otimes_{R_{(f)}} R(n)_f.$$

So it suffices to show that $R(n)_f \cong R_{(f)}$. But observe that $R(n)_{(f)} = (R_f)_n$ is the free $R_{(f)}$-module generated by f^n and so is isomorphic to $R_{(f)}$ as an $R_{(f)}$-module.

(4) We always have a natural homomorphism of graded R_f-modules:

$$^* \operatorname{Hom}_R(M, N)_f \to^* \operatorname{Hom}_{R_f}(M_f, N_f).$$

If we look at the degree zero terms on both sides, we get a natural homomorphism of $R_{(f)}$-modules

$$^* \operatorname{Hom}_R(M, N)_{(f)} \to \operatorname{Hom}_{R_f^{\mathbb{Z}}\text{-mod}}(M_f, N_f),$$

which, via restriction, gives us a natural map

$$^* \operatorname{Hom}_R(M, N)_{(f)} \to \operatorname{Hom}_{R_{(f)}}(M_{(f)}, N_{(f)}).$$

Suppose now that $\deg f = 1$, and that M is finitely presented. By a standard argument (3.1.12), it suffices to prove that this map is an isomorphism for the case where $M = R(n)$, for some $n \in \mathbb{Z}$. But now we see that

$$\begin{aligned} \operatorname{Hom}_{R_{(f)}}(R(n)_{(f)}, N_{(f)}) &\cong \operatorname{Hom}_{R_{(f)}}(R_{(f)}, N_{(f)}) \\ &\cong N_{(f)} \\ &\cong N(-n)_{(f)} \\ &\cong^* \operatorname{Hom}_R(R(n), N)_{(f)}, \end{aligned}$$

where we've used twice the isomorphism from part (4).

(5) It suffices to show that

$$(\bigoplus_i M_i)_{(f)} \cong \bigoplus_i (M_i)_{(f)}.$$

But this follows immediately from the fact that localization commutes with infinite direct sums.

(6) We have an exact sequence of R-modules

$$0 \to M^{\geq d} \to M \to M/M^{\geq d} \to 0,$$

which gives us an exact sequence

$$0 \to M_{(f)}^{\geq d} \to M_{(f)} \to (M/M^{\geq d})_{(f)} \to 0.$$

Since f has positive degree and $(M/M^{\geq d})_n = 0$, for $n \geq d$, we see that every element in $M/M^{\geq d}$ is annihilated by some power of f, and so $(M/M^{\geq d})_f = 0$. This shows that the map on the left in the above sequence is actually an isomorphism.

□

As one can see from the previous Proposition, the situation where $\deg f = 1$ is nicer in all possible ways. But the other cases aren't completely hopeless. There is a little trick we can use to translate everything (not, however, with unblemished success) to this nice situation.

DEFINITION 1.6.4. Let R be a graded ring; for $d \in \mathbb{Z}$, the d^{th} Veronese subring is the ring $R^{(d)}$ defined as the graded ring with $R^{(d)}_n = R_{dn}$, with multiplication inherited from R.

This is almost, but not quite, a graded subring of R: the grading is scaled by d. Observe that we have a natural homomorphism of rings (though not of graded rings) from $R^{(d)}$ to R: this is just the inclusion map. Now, if $f \in R$ is a homogeneous element of degree d, then in $R^{(d)}$, f has degree 1! This lets us describe $R_{(f)}$ also as a dehomogenization of a certain ring as in the next Proposition.

grm-veronese-embedding

PROPOSITION 1.6.5. *Suppose $d \in \mathbb{Z}$, and let R and $R^{(d)}$ be as in the discussion above.*

(1) *If R is finitely generated over R_0, so is $R^{(d)}$. In particular, if R is Noetherian, then so is $R^{(d)}$.*
(2) *If $f \in R$ is a homogeneous element of degree md, for some $m \in \mathbb{Z}$, then the natural map of rings $R^{(d)} \to R$ induces an isomorphism from $R^{(d)}_{(f)}$ to $R_{(f)}$. In particular, if $\deg f = d$, then*

$$R_{(f)} \cong R^{(d)}_f/(f-1).$$

(3) *If R is positively graded and finitely generated over R_0, then there exists $d \in \mathbb{N}$ such that $R^{(d)}_n = (R^{(d)}_1)^n$, for all $n \in \mathbb{N}$. In other words, $R^{(d)}$ is generated by $R^{(d)}_1$ over R_0.*

PROOF. (1) The second statement will follow from the first via (1.3.4). So suppose R is finitely generated over R_0 by $x_1, \ldots, x_n$, with $\deg x_i = d_i$. Let $x_1^{r_1} \ldots x_n^{r_n}$ be any monomial such that $\sum_i r_i d_i = md$, for some $m \in \mathbb{Z}$. Write each r_i as $q_i d + s_i$, where $0 \leq s_i < |d|$. Then we find that we can express our monomial as

$$(x_1^{q_1 d} \ldots x_n^{q_n d})(x_1^{s_1} \ldots x_n^{s_n}),$$

where $d \mid \sum_i s_i d_i$. This shows that the finite set of monomials

$$\{x_1^{s_1} \ldots x_1^{s_i} : 0 \leq s_i \leq |d|, d \mid \sum_i s_i d_i\},$$

generates $R^{(d)}$ over R_0.

(2) The induced map is *a fortiori* injective. We only have to check that it's surjective. Suppose $x = \frac{a}{f^r} \in R_{(f)}$; then since $\deg x = 0$, we see immediately that $\deg a = rmd$, and so $a \in R^{(d)}$. For the second statement, use the fact that $\deg f = 1$ in $R^{(d)}$ combined with (1.6.2).

(3) Just apply part (3) of (1.3.2).

□

CHAPTER 2

Graded Rings and Modules II: Filtrations and Hilbert Functions

chap:hfm

1. Filtered Rings

hfm-secn:filtered-rings

1.1. Definitions. We'll be spending a lot of time just setting up the definitions, but there will be results soon.

NOTE ON NOTATION 2. We will treat 0 as a natural number in this section. That is, $0 \in \mathbb{N}$.

DEFINITION 2.1.1. A *filtration* on an R-module M is a collection $F^\bullet M = \{F^i M \subset M : i \in \mathbb{N}\}$ of R-submodules of M such that

(1) $F^0 M = M$.
(2) For $n \in \mathbb{N}$, $F^n M \supset F^{n+1} M$.

Let R be a ring equipped with a filtration $F^\bullet R$. A *filtered module* over R is a pair $(M, F^\bullet M)$, where M is an R-module and $F^\bullet M$ is a filtration on M such that, for each pair $(n, m) \in \mathbb{N} \times \mathbb{N}$, we have

$$F^n R F^m M \subset F^{n+m} M.$$

A *filtered ring* is a ring R equipped with a filtration $F^\bullet R$ such that $(R, F^\bullet R)$ is a filtered module over R. In general, we will only talk about filtered modules over filtered rings.

As always, we will talk about a filtered ring R, meaning implicitly the pair $(R, F^\bullet R)$, for some filtration $F^\bullet R$ that should either be clear from context or is not essential. Same deal holds for filtered modules.

REMARK 2.1.2. Given a filtered ring $(R, F^\bullet R)$ and any R-module M, we can equip M with a natural filtered R-module structure by setting $F^r M = F^r R \cdot M$, for each $r \in \mathbb{N}$. This is called the *natural filtration* on M.

Observe that every graded module M over a graded ring R has a filtration given by $F^n M = \bigoplus_{|m| \geq n} M_m$. So every graded ring has the natural structure of a filtered ring, over which any graded module can be given the structure of a filtered module.

DEFINITION 2.1.3. A *homomorphism* $\varphi : (R, F^\bullet R) \to (S, F^\bullet S)$ of filtered rings is a map of rings $\varphi : R \to S$ such that, for every $n \in \mathbb{N}$, $\varphi(F^n R) \subset F^n S$.

This definition gives us a category of filtered rings, which we will denote by FiltRing.

A *homomorphism* $\psi : (M, F^\bullet M) \to (N, F^\bullet N)$ between two filtered modules over a filtered ring R is a map of R-modules $\psi : M \to N$ such that, for every $n \in \mathbb{N}$, $\psi(F^n M) \subset F^n N$.

This gives us a category of filtered modules over R, which we will denote by R-filt.

DEFINITION 2.1.4. If M is a filtered R-module (implicit here is the assumption that R is a filtered ring) and $N \subset M$ is an R-submodule, then N has a natural filtration given by $F^r N = F^r M \cap N$, known as the *induced filtration* on N. With the induced filtration N is a filtered submodule of M.

Moreover, M/N also has a natural filtration given by

$$F^r(M/N) = F^r M/(N \cap F^r M);$$

this is called the *produced filtration*. With the the produced filtration the map $M \to M/N$ is clearly a homomorphism of filtered R-modules.

REMARK 2.1.5. With these filtrations in hand, for every homomorphism of filtered modules $\varphi : M \to N$, we can give $\ker\varphi$ and $\operatorname{coker}\phi$ natural filtered structures. More explicitly, the induces filtration on $\ker\varphi$ is

$$F^r(\ker\varphi) = \ker(\varphi|_{F^r M});$$

and the produced filtration on $\operatorname{coker}\varphi$ is

$$F^r(\operatorname{coker}\phi) = F^r N/(\varphi(M) \cap F^r N).$$

But the filtration on $M/\ker\varphi$ is given by

$$F^r\left(M/\ker\varphi\right) = F^r M/\ker(\varphi|_{F^r M}).$$

So it's not necessarily true that $M/\ker\varphi \cong \operatorname{im}\varphi$ as filtered R-modules. That is, R-filt is *not* an abelian category. Take any R-module M, and give it two distinct filtrations $F_1^\bullet M$ and $F_2^\bullet M$ such that $F_1^r M \subset F_2^r M$, for all $r \in \mathbb{N}$. Then, the identity map on M is a map of filtered modules from $(M, F_1^\bullet M)$ to $(M, F_2^\bullet M)$, and has zero kernel and cokernel; but if there is even one $r \in \mathbb{N}$ such that $F_1^r M \neq F_2^r M$, then it's not an isomorphism. The failure here is analogous to the failure of bijective, continuous maps to be homeomorphisms.

1.2. From Filtrations to Gradings. There are a few natural functors from FiltRing to GrRing, the category of graded rings. We'll describe them now.

DEFINITION 2.1.6. Let $(R, F^\bullet R)$ be a filtered ring. The *blow-up algebra* associated to R is the graded R-subalgebra of $R[t, t^{-1}]$ defined by

$$\mathcal{B}(F, R) = \bigoplus_{n\in\mathbb{N}} F^n R t^n;$$

and the *Rees algebra* associated to R is the graded R-subalgebra of $R[t, t^{-1}]$ defined by

$$\mathcal{R}(F, R) = \bigoplus_{n\in\mathbb{Z}} F^n R t^n,$$

where we set $F^n R = R$, for $n < 0$.

For any filtered R-module M, we define analogously the graded abelian groups $\mathcal{B}(F, M)$ and $\mathcal{R}(F, M)$; it's easy to see that these are modules over the blow-up algebra and the Rees algebra, respectively.

DEFINITION 2.1.7. Given a filtered ring $(R, F^\bullet R)$ and a filtered module $(M, F^\bullet M)$ over R, we define the *associated graded module* to be the graded abelian group

$$\mathrm{gr}_F(M) = \bigoplus_{n\in\mathbb{N}} F^n M/F^{n+1}M.$$

Note that, for every pair $(n, m) \in \mathbb{N} \times \mathbb{N}$, we have a natural bilinear map

$$\mathrm{gr}_F(R)_n \times \mathrm{gr}_F(M)_m \to \mathrm{gr}_F(M)_{n+m},$$

that takes a pair of elements $(a \pmod{F^{n+1}R}, b \pmod{F^{m+1}R})$ to the element $(ab \pmod{F^{n+m+1}M})$. It's easy to see that this is indeed well-defined and bilinear.

This shows that: (a) $\mathrm{gr}_F(R)$ is a graded ring, (b) For every filtered R-module M, $\mathrm{gr}_M(R)$ is a graded $\mathrm{gr}_F(R)$-module.

We call $\mathrm{gr}_F(R)$ the *associated graded ring* of the filtered ring R.

REMARK 2.1.8. It's clear that these constructions are functorial in M. Moreover, we have a natural map in called the *initial form* map.

$$\mathrm{in} : M \to \mathrm{gr}_F(M)$$
$$m \mapsto \begin{cases} m \pmod{F^{t+1}M}, \text{ if } t = \sup\{n \in \mathbb{N} : m \in F^n M\} < \infty \\ 0, \text{ if } t = \infty \end{cases}$$

There are natural relations between the Rees algebra and the graded associated algebra.

hfm-rees-gr-relations

PROPOSITION 2.1.9. *Let $(R, F^\bullet R$ be a filtered ring.*

1. $\mathscr{R}(F, R)_{t^{-1}} = R[t, t^{-1}]$.
2. $\mathscr{R}(F, R)/t^{-1}\mathscr{R}(F, R) = \mathrm{gr}_F(R)$.
3. *For $0 \neq a \in R$, $\mathscr{R}(F, R)/(t^{-1} - a)\mathscr{R}(F, R) = R$.*
4. *For $n \in \mathbb{N}$, we have $t^{-n}\mathscr{R}(F, R) \cap R = F^n R$.*

PROOF. Almost all the statements are immediate. We will prove (3). Observe that we have

$$R = R[t, t^{-1}]/(t^{-1} - a)R[t, t^{-1}] = \big(\mathscr{R}(F, R)/(t^{-1} - a)\mathscr{R}(F, R)\big)_{t^{-1}}$$

But $t^{-1} = a$ in the quotient ring on the right (before localization) is already invertible, and so we have our identity. □

DEFINITION 2.1.10. Let R be any ring and let $I \subset R$ be an ideal. The *I-adic* filtration on R is given by $F^n R = I^n$, for $n \in \mathbb{N}$. This gives R the structure of a filtered ring, which we will denote by (R, I).

Any filtered module M over (R, I) is called an *R-module with an I-adic filtration.*

NOTE ON NOTATION 3. If the filtration on M is the natural I-adic filtration (i. e. $F^n M = I^n M$), we denote $\mathrm{gr}_F(M)$, $\mathcal{B}(F, M)$ and $\mathcal{R}(F, M)$ by $\mathrm{gr}_I(M)$, $\mathcal{B}(I, M)$ and $\mathcal{R}(I, M)$ instead.

REMARK 2.1.11. In the I-adic case, it's easy to see that we have

$$\mathrm{gr}_I(M) \cong \mathscr{B}(I, M)/I\mathscr{B}(I, M).$$

We'll have reason to use this isomorphism in Chapter 10.

Now, if we consider the I-adic filtration on a ring R and suppose that $I = (x_1, \dots, x_d)$, then we find that $\mathrm{gr}_I(R)$ is generated over R/I by the images $\xi_i = \mathrm{in}(x_i) \in I/I^2$. Thus we have a surjection:

$$(R/I)[t_1, \dots, t_d] \to \mathrm{gr}_I(R)$$
$$t_i \mapsto \xi_i.$$

It is important to find general situations where this is an isomorphism. We'll find one in (2.3.25) and another very significant one in (10.3.13).

In fact, we can do this in a little more generality. Let M be any R-module; then we have a surjection:

$$\varphi_M^I : (M/IM)[t_1, \dots, t_d] \to \mathrm{gr}_I(M).$$

This map is obtained from rather general considerations: If N is a graded module over a graded ring S, then we have a natural map

qn:tensor-zero-generated

$$N_0 \otimes_{S_0} S \to N. \tag{1}$$

If N is generated by N_0 over S, then this is in fact a surjection, and so, if S is generated over S_0 by finitely many elements $x_1, \dots, x_d \in S_1$, we get a surjection

$$N_0[t_1, \dots, t_d] \to N.$$

In our specific case here, $N = \mathrm{gr}_I(M)$ and $S = \mathrm{gr}_I(R)$, whence our map. We'll investigate its properties in (2.3.25). In fact, under some flatness hypotheses, the surjection in (1) is an isomorphism in this situation. See (3.4.1) for more on that.

We end this section with a small definition.

hfm-shifted-filtration

Definition 2.1.12. Let $(M, F^\bullet M)$ be a filtered R-module. For $n \in \mathbb{N}$, we denote by $M(-n)$ the filtered R-module, whose underlying R-module is M, but whose filtration is given by

$$F^r M(-n) = \begin{cases} M, \text{ if } r \leq n \\ F^{r-n} M, \text{ if } r \geq n. \end{cases}$$

It's immediate that $\mathrm{gr}_F(M(-n)) \cong \mathrm{gr}_F(M)(-n)$.

1.3. More on the Initial Form Map. The initial form map $\mathrm{in} : M \to \mathrm{gr}_F(M)$, for a given filtered R-module $(M, F^\bullet M)$ is in general neither an additive nor a multiplicative homomorphism. The following Proposition tells us how close (or far) it is from being such a homomorphism.

hfm-initial-form-map

Proposition 2.1.13. *Let $(M, F^\bullet M)$ be a filtered R-module, and consider the initial form map* $\mathrm{in} : M \to \mathrm{gr}_I(M)$.

1. *For $m, n \in M$, we have either* $\mathrm{in}(m) + \mathrm{in}(n) = 0$, *or* $\mathrm{in}(m) + \mathrm{in}(n) = \mathrm{in}(m+n)$.
2. *For $m \in M$ and $r \in R$, we have either* $\mathrm{in}(r)\,\mathrm{in}(m) = 0$, *or* $\mathrm{in}(r)\,\mathrm{in}(m) = \mathrm{in}(rm)$.

Proof. (1) Suppose $\mathrm{in}(m) + \mathrm{in}(n) \neq 0$. If either $\mathrm{in}(m)$ or $\mathrm{in}(n)$ is 0, then we're done; so assume that both are non-zero. In this case, we can find $k, l \in \mathbb{N}$ such that k is the maximal number with $m \in F^k M$, and l is the maximal number with $n \in F^l M$. Without loss of generality, we can assume that $k \geq l$. First assume that $k > l$: in this case,

□

It is often the case that properties of $\mathrm{gr}_F(M)$ can be lifted to M using the initial form map. Before we give an example, we need a definition.

DEFINITION 2.1.14. A filtered module $(M, F^\bullet M)$ over a filtered ring $(R, F^\bullet R)$ is *separated* if we have

$$\bigcap_{n\in\mathbb{Z}} F^n M = 0.$$

A filtered ring $(R, F^\bullet R)$ is *separated* if it is separated as a module over itself.

fm-gr-domain-ring-domain

PROPOSITION 2.1.15. *Suppose $(R, F^\bullet R)$ is a separated filtered ring. If $\mathrm{gr}_F(R)$ is a domain, then so is R.*

PROOF. Assume that R is not a domain; then we can find $x, y \in R \setminus \{0\}$ such that $xy = 0$. Since R is separated, we see that $\mathrm{in}(x)$ and $\mathrm{in}(y)$ are non-zero, but their product is of course zero. □

EXAMPLE 2.1.16. The converse is not true. That is, R can be a domain without the property descending to $\mathrm{gr}_F(R)$. Consider the ring $R = k[x, y]/(x^2 - y^3)$ equipped with the filtration $F^n R = \mathfrak{m}^n$, where $\mathfrak{m} = (x, y)$. Then $\mathrm{in}(x) \neq 0$, but

$$\mathrm{in}(x)^2 = y^3 \pmod{\mathfrak{m}^3} = 0$$

Here's a result that we'll need later.

hfm-gr-quotient-ideal

PROPOSITION 2.1.17. *Let $J \subset I \subset R$ be a chain of ideals in R, and let M be an R-module; then we have*

$$\mathrm{gr}_I(M/JM) \cong \mathrm{gr}_I(M)/\,\mathrm{in}(J).$$

PROOF. Observe that $\mathscr{B}(I, M/JM) = \oplus_{n\geq 0} I^n M/\left(I^n M \cap JM\right)$. Consider this commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \oplus_{n\geq 0}\left(I^n M \cap JM\right) & \longrightarrow & \mathscr{B}(I, M) & \longrightarrow & \mathscr{B}(I, M/JM) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha'} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha''} & & \\
0 & \longrightarrow & K & \longrightarrow & \mathrm{gr}_I(M) & \longrightarrow & \mathrm{gr}_I(M/JM) & \longrightarrow & 0
\end{array}$$

Since the kernel of α surjects onto the kernel of α'', and since α and α'' are surjective, we find by the Snake Lemma that α' is also surjective. Namely, we find that the kernel of the natural surjection $\mathrm{gr}_I(M) \to \mathrm{gr}_I(M/JM)$ is

$$\oplus_{n\geq 0}\left(I^n M \cap JM\right) / \left(I^{n+1} M \cap JM\right).$$

It's easy to check now that this is precisely $\mathrm{in}(J)$. □

2. Finiteness Conditions: The Artin-Rees Lemma

DEFINITION 2.2.1. A filtered module M over a filtered ring R is *stable* if there exists $n_0 \in \mathbb{N}$ such that for $n \geq n_0$, we have $(F^{n-n_0} R)(F^{n_0} M) = F^n M$.

REMARK 2.2.2. Note that the natural filtration on any R-module is always stable.

hfm-pre-artin-rees

PROPOSITION 2.2.3. *Let $(R, F^\bullet R)$ be a filtered ring, and let M be a filtered R-module, finitely generated over R. Then the following are equivalent:*

(1) *M is stable.*

(2) $\mathcal{B}(F, M)$ *is a finitely generated module over* $\mathcal{B}(F, R)$.

PROOF. (1) $\Rightarrow$ (2)**:** In this case, $F^n M$ is a finitely generated R-module, for all $n \in \mathbb{N}$. Choose a set of generators $\{m_{ni} : 1 \leq i \leq r_n\}$. Let $n_0 \in \mathbb{N}$ be as in the definition of stability, and let $N' \subset \mathcal{B}(F, M)$ be the submodule generated by the elements $\{m_{ni}t^n : 1 \leq n \leq n_0, 1 \leq i \leq r_n\}$. Then we see that $N' = \mathcal{B}(F, M)$, proving one implication.
(2) $\Rightarrow$ (1)**:** The proof of this is contained in part (4) of (1.3.2).

□

DEFINITION 2.2.4. A filtered ring $(R, F^\bullet R)$ is *Noetherian* if the Rees algebra $\mathcal{R}(F, R)$ is a Noetherian ring.

m-noetherian-filtrations

PROPOSITION 2.2.5. *Let* $(R, F^\bullet R)$ *be a filtered ring. Then the following are equivalent.*

(1) $(R, F^\bullet R)$ *is Noetherian.*
(2) R *is Noetherian and* $\mathcal{R}(F, R)$ *is finitely generated over* R.
(3) R *is Noetherian and* $\mathcal{B}(F, R)$ *is finitely generated over* R.

PROOF. Follows from (1.3.4). □

hfm-artin-rees

THEOREM 2.2.6 (Artin-Rees). *Let* $(R, F^\bullet R)$ *be Noetherian, and let* M *be a stable filtered* R*-module, finitely generated over* R. *Let* $N \subset M$ *be any* R*-submodule. Then the induced filtration on* N *is also stable.*

PROOF. Just observe that if N is given the induced filtration, then $\mathcal{B}(F, N) \subset \mathcal{B}(F, M)$ is a $\mathcal{B}(F, R)$-submodule. Hence, if $\mathcal{B}(F, R)$ is Noetherian, then it's also finitely generated, which, by the Proposition above, shows that N is stable when endowed with the induced filtration. □

hfm-original-artin-rees

COROLLARY 2.2.7 (The Original Artin-Rees). *Suppose* R *is Noetherian, and* $I \subset R$ *is an ideal.*

(1) (R, I) *is Noetherian.*
(2) *If* M *is a finitely generated* R*-module equipped with the natural* I*-adic filtration, then, for any submodule* $N \subset M$*, there is* $n_0 \in \mathbb{N}$ *such that, for* $n \geq n_0$*,*

$$I^n M \cap N = I^{n-n_0}(I^{n_0} M \cap N).$$

PROOF. (1) Since I can be generated by finitely many elements, this follows from (2.2.5).
(2) Follows immediately from (2.2.6). Observe that the natural filtration on M is stable by definition.

□

hfm-krull-intersection

THEOREM 2.2.8 (Krull's Intersection Theorem). *If* R *is a Noetherian ring, and* M *is a finitely generated* R*-module, then, for any ideal* $I \subsetneq R$*, there is* $a \in I$ *such that*

$$(1 - a)\left(\bigcap_{n \in \mathbb{N}} I^n M\right) = 0.$$

PROOF. Let $E = \bigcap_{n\in\mathbb{N}} I^n M$; we will show that $IE = E$. The result will then follow from (4.1.1). For this, we use Artin-Rees above, to find $n_0 \in \mathbb{N}$ such that

$$E = I^{n_0+1}M \cap E = I(I_0^n M \cap E) = IE.$$

□

Here's the form in which this is mostly used.

hfm-krull-int-jacobson

COROLLARY 2.2.9. *If R is a Noetherian ring, and if $I \subset \mathrm{Jac}(R)$, then, for any finitely generated R-module M, we have*

$$\bigcap_{n\in\mathbb{N}} I^n M = 0.$$

PROOF. Follows from Nakayama's Lemma, since $IE = E$ implies $E = 0$. □

We also present a graded version.

hfm-krull-int-star-local

COROLLARY 2.2.10. *If $(R, \mathfrak{m})$ is a Noetherian *local ring, then, for any finitely generated graded R-module M, we have*

$$\bigcap_{n\in\mathbb{N}} \mathfrak{m}^n M = 0.$$

PROOF. Use the graded version of Nakayama's Lemma (1.2.7). □

3. The Hilbert-Samuel Polynomial

hfm-secn:hilbert-samuel

3.1. Functions of Polynomial Type.

DEFINITION 2.3.1. A polynomial $f(t) \in \mathbb{Q}[t]$ is *integer valued* if, for all $n \in \mathbb{Z}$, $f(n)$ is an integer.

For $k \in \mathbb{N}$, we define the polynomial $Q_k(t) \in \mathbb{Q}[t]$ via the formula

$$Q_k(t) = \frac{t(t-1)\dots(t-k+1)}{k!}.$$

For $k = 0$, we set $Q_0(t) = 1$.

The *difference operator* is the linear map $\Delta : \mathbb{Q}[t] \to \mathbb{Q}[t]$ that assigns to each polynomial $f(t)$, the polynomial $\Delta f(t) = f(t) - f(t-1)$.

Here are some elementary properties of the difference operator.

hfm-delta-prps

LEMMA 2.3.2. (1) *For every $k \in \mathbb{N}$, $\Delta Q_k(t) = Q_{k-1}(t)$.*
(2) *For every $k \in \mathbb{N}$, $Q_k(t)$ is integer valued.*
(3) *$\Delta f(t) = \Delta g(t)$ if and only if $f(t) - g(t)$ is a constant.*

PROOF. (1) Clear.
(2) By induction. Clearly Q_1 is integer valued. Moreover, for every $n \in \mathbb{Z}$, and $k > 1$, we have

$$Q_k(n) = \sum_{r=0}^{n} Q_{k-1}(r),$$

which proves our result.

(3) One direction is easy. For the other, observe that for every $n \in \mathbb{N}$, we have

$$f(n) = f(0) + \sum_{k=0}^{n} \Delta f(k),$$

and so $f(t) - f(0)$ and $g(t) - g(0)$ agree for infinitely many values in $\mathbb{Q}$. This of course means that they are equal in the ring of polynomials over $\mathbb{Q}$.

□

hfm-int-valued-poly

PROPOSITION 2.3.3. *Let $f(t) \in \mathbb{Q}[t]$ be a polynomial over $\mathbb{Q}$, and let $N \subset \mathbb{Q}[t]$ be the subspace spanned by the polynomials Q_k, $k \geq 0$, over $\mathbb{Z}$. Then the following are equivalent:*

(1) *$f(t) \in N$.*
(2) *$f(t)$ is integer valued.*
(3) *$f(n) \in \mathbb{Z}$, for all large enough $n \in \mathbb{Z}$.*
(4) *$\Delta f(t) \in N$ and there exists at least one $n \in \mathbb{Z}$ such that $f(n) \in \mathbb{Z}$.*

Moreover, we have $\deg f = \deg \Delta f + 1$.

PROOF. (1) $\Rightarrow$ (2)**:** Follows from the Lemma above.

(2) $\Rightarrow$ (3)**:** Obvious.

(1) $\Leftrightarrow$ (4)**:** From part (1) of the Lemma above, it follows that if $f(t)$ is in N, then so is $\Delta f(t)$. For the other direction, suppose $\Delta f(t) = \sum_{k=0}^{r} e_k Q_k(t)$; then we see from part (3) of the Lemma that

$$f(t) = c + \sum_{k=0}^{r} e_k Q_{k+1}(t),$$

for some constant $c \in \mathbb{Q}$. Since $f(t) - c$ is integer valued, and since there is some n such that $f(n)$ is integer valued, we find that $c \in \mathbb{Z}$, and so $f(t) \in N$.

(3) $\Rightarrow$ (1)**:** By induction on the degree of f. If $\deg f = 0$, then this is obvious. So assume $\deg f > 0$; then by the induction hypothesis Δf (which also has integer values for large enough n) will be in N. So we see that f satisfies the conditions in (4); but we've already shown that (4) $\Rightarrow$ (1).

The last assertion is obvious. □

REMARK 2.3.4. For every $k \in \mathbb{N}$, we have a nice map

$$e_k : N \to \mathbb{Z},$$

which takes an integer valued polynomial f to the coefficient of Q_k in its linear expansion. By part (1) of the Lemma, these maps satisfy the relation $e_{k-1} \circ \Delta = e_k$. Proceeding inductively, we find that, for every $k \in \mathbb{N}$, we have $e_k = e_0 \circ \Delta^k$. What this means is that, for every $f \in N$, the coefficient of Q_k in the linear expansion of f is just the constant term in $\Delta^k f$.

Also note that Q_k is a polynomial of degree k. So for an integer valued polynomial f of degree r, we have

$$r = \max\{k \geq 0 : e_k(f) \neq 0\},$$

and we have $f(t) = e_r \frac{t^r}{(r-1)!} +$ lower degree terms. So we see that $f(n) > 0$ for large enough n if and only if $e_r > 0$ if and only if $\Delta^r f > 0$.

DEFINITION 2.3.5. A function $f : \mathbb{Z} \to \mathbb{Q}$ is of *polynomial type* if there is an $n_0 \in \mathbb{N}$, and a polynomial $g(t) \in \mathbb{Q}[t]$, such that for all $n \geq n_0$, $f(n) = g(n)$.

Note that given any function f of polynomial type, there is a unique polynomial P_f that satisfies the above condition. Indeed, any two polynomials that agree with f for large enough n, must take the same value at infinitely many points, and must thus be equal. We define the *degree* of a function of polynomial type to be the degree of P_f, and we denote it by $\deg f$.

Let Poly be the space of all functions defined on $\mathbb{Z}$ of polynomial type. Then here again we have a *difference operator* Δ : Poly $\to$ Poly given by $\Delta f(n) = f(n) - f(n-1)$. It is clear that $P_{\Delta f} = \Delta P_f$.

A function of $f : \mathbb{Z} \to \mathbb{Q}$ is *integer valued* if $f(n) \in \mathbb{Z}$ for large enough $n \in \mathbb{Z}$. It is clear that if f is integer valued and is of polynomial type, then P_f is also integer valued (2.3.3). In this case, for $k \in \mathbb{N}$, we set $e_k(f) = e_k(P_f)$.

m-difference-fn-polytype

PROPOSITION 2.3.6. *Let $f : \mathbb{Z} \to \mathbb{Q}$ be an integer valued function. Then the following are equivalent:*

(1) *f is of polynomial type.*
(2) *Δf is of polynomial type.*
(3) *There exists $k \geq 0$ such that $\Delta^k f(n) = 0$, for large enough n.*

Moreover, we have $\deg f = \deg \Delta f + 1$.

PROOF. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) is immediate. We'll prove (3) $\Rightarrow$ (1) by induction on k. When $k = 0$, this is trivial; so suppose $k > 0$, and observe that $k - 1$ works for Δf. Therefore, Δf is of polynomial type. But now $g = \sum_{k \geq 0} e_k(\Delta f) Q_{k+1}$ is an integer valued polynomial. Consider now the function $h : n \mapsto f(n) - g(n)$. For n large, we have $\Delta h(n) = 0$, and so there exists a constant $r \in \mathbb{Z}$ such that for large enough n, $h(n) = r$. This implies that f is of polynomial type, and that $P_f(t) = g(t) + r$.

The last assertion now follows from (2.3.3). □

3.2. The Hilbert Function.

NOTE ON NOTATION 4. In this section, all our graded rings S will be finitely generated S_0-algebras, where S_0 is an Artinian ring.

Observe that if M is a finitely generated graded S-module, then, for each $n \in \mathbb{Z}$, M_n is a finitely generated S_0-module (1.3.2). Hence, for each $n \in \mathbb{Z}$, M_n has finite length. This leads to the following definition.

DEFINITION 2.3.7. Let M be a finitely generated, graded module over a graded ring S. The *Hilbert function* of M is the map

$$H(M, \_\_) : \mathbb{Z} \to \mathbb{N}$$
$$n \mapsto l(M_n).$$

The *Hilbert Series* of M is the Laurent series $P(M, t) = \sum_{n \in \mathbb{Z}} H(M, n) t^n$.

ert-series-rational-repn

PROPOSITION 2.3.8. *Let S be a graded ring generated over S_0 by $x_1, \ldots, x_s$, with $\deg x_i = k_i$, and let M be a finitely generated, graded S-module. Then, there exists a polynomial $f(t) \in \mathbb{Z}[t]$, with $\deg f \leq \sum_{i=1}^{s} k_i$, such that*

$$P(M, t) = \frac{f(t)}{\prod_{i=1}^{s} (1 - t^{k_i})}.$$

PROOF. We do this by induction on the number of generators. When $s = 0$, M is just a finitely generated S_0-module with bounded grading, and so $P(M,t)$ is already a polynomial. Suppose now that the statement of the proposition is valid for $r \leq s-1$. For $n \in \mathbb{Z}$, consider the following exact sequence:

$$0 \to \ker m_{x_s}(-k_s) \to M(-k_s) \xrightarrow{m_{x_s}} M \to \operatorname{coker} m_{x_s} \to 0,$$

where by m_{x_s}, we denote the map given by scalar multiplication by x_s on M.

Let $K = \ker m_{x_s}$, and let $L = \operatorname{coker} m_{x_s}$ be graded modules over S. Then we see that x_s has trivial action on both K and L, and so they're in fact graded modules over $S' = S_0[x_1, \ldots, x_{s-1}]$. By the inductive hypothesis, we can find polynomials $g(t), h(t) \in \mathbb{Z}[t]$, with $\deg g, \deg h \leq \sum_{i=1}^{s-1} k_i$, such that

$$P(K,t) = \frac{g(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})}, \tag{2}$$

$$P(L,t) = \frac{h(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})}. \tag{3}$$

Now, using the additivity of l, we see that

$$P(M,t) + t^{k_s}P(K,t) = t^{k_s}P(M,t) + P(L,t).$$

This implies that

$$\begin{aligned} P(M,t) &= \frac{P(L,t) - t^{k_s}P(K,t)}{1-t^{k_s}} \\ &= \frac{h(t) - t^{k_s}g(t)}{\prod_{i=1}^{s}(1-t^{k_i})} \\ &= \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})}, \end{aligned}$$

where $\deg f \leq \sum_{i=1}^{s} k_i$, as we had claimed. □

The most important application of this proposition is to the case where $k_i = 1$, for all i.

hfm-hilbert-fn-polytype

COROLLARY 2.3.9. *Let S be a graded ring finitely generated by S_1 over S_0 by $x_1, \ldots, x_s$. Then, for any finitely generated graded S-module M, the Hilbert function $H(M,n)$ is of polynomial type and its degree is at most $s-1$.*

PROOF. By the Proposition, we can express the Hilbert series as a rational function in the form

$$P(M,t) = \frac{f(t)}{(1-t)^s},$$

where $\deg f \leq s$.

After factoring out all powers of $(1-t)$ from $f(t)$, we can write

$$P(M,t) = g(t)(1-t)^{-d}$$

for some $d \in \mathbb{N}$, and some $g(t) \in \mathbb{Z}[t]$, with $\deg g = r \leq d$.

Now, $(1-t)^{-d} = \sum_{n=0}^{\infty} \binom{d+n-1}{d-1} t^n$. Suppose $g(t) = \sum_{m=1}^{r} g_m t^m$; then we see that

$$H(M,n) = \sum_{m=1}^{r} g_m \binom{d+n-m-1}{d-1},$$

where $\binom{k}{l} = 0$, for $k < l$. Set

$$\varphi(n) = \sum_{m=1}^{r} g_m Q_{d-1}(n + d - m - 1).$$

This is an integer valued polynomial of degree $d-1$ with $e_{d-1}(\varphi) = g(1) \neq 0$. Moreover, $\varphi(n) = H(M, n)$, for n large enough; so $H(M, \_\_)$ is of polynomial type of degree $d-1$. Since $d \leq s$, our proof is done. □

DEFINITION 2.3.10. With all the notation as in the Corollary above, we say that the polynomial associated do $H(M, n)$, which we also denote $H_M(n)$, is called the *Hilbert polynomial* of the graded S-module M.

ilbertfn-polynomial-ring

EXAMPLE 2.3.11. Suppose R is an Artinian ring; let M be a finitely generated R-module. Consider the graded $\widetilde{R} = A[t_1, \ldots, t_d]$-module $\widetilde{M} = M[t_1, \ldots, t_d]$. Since there are $\binom{d+n-1}{n}$ monomials of degree n, we see that the n^{th} graded component is isomorphic to $M^{\binom{d+n-1}{n}}$. If we take λ to be the length function, we see that

$$H(\widetilde{M}, n) = l(M)\binom{d+n-1}{d-1} = l(M)Q_{d-1}(d+n-1)$$

is a polynomial of degree $d-1$ with

$$\Delta^{d-1}H(M, n) = e_{d-1}(H(M, n)) = l(M).$$

Now, suppose $M = R = k$ is a field, and let $F \in \widetilde{k}_r$ be some homogeneous polynomial. Then, if $I = (F)$, I_{r+k}, for $k \geq 0$, is spanned by the product of F with all monomials of degree k. Hence, we see that, for $n \geq r$, we have

$$l(I_n) = \binom{d+n-r-1}{d-1} = Q_{d-1}(d+n-r-1),$$

which says that

$$\Delta^{d-1}H(I, n) = e_{d-1}(H(I, n)) = 1.$$

In fact, these calculations can be used to *characterize* polynomial rings

m-module-polynom-algebra

PROPOSITION 2.3.12. *With the notation as in the above example, let N be a graded $\widetilde{R}$-module, generated by N_0 over $\widetilde{R}$. Then, we have*

$$\Delta^{r-1}H(N, n) \leq l(N_0).$$

Moreover, the following statements are equivalent:

1. $\Delta^{d-1}H(N, n) = l(N_0)$.
2. $H(N, n) = l(N_0)\binom{d+n-1}{n}$.
3. *The natural map $N_0[t_1, \ldots, t_d] \to N$ is an isomorphism.*

PROOF. Let $\varphi : N_0[t_1, \ldots, t_d] \to N$ be the natural map considered in (3), and let $K = \ker \varphi$. Then, we see that $H(K, n) + H(N, n) = H(\widetilde{N_0}, n)$, and so we find that

$$\Delta^{d-1}\left(H(\widetilde{N_0}, n) - H(N, n)\right) = \Delta^{d-1}H(K, n).$$

Now, if $\deg H(K, n) = d-1$, then $\Delta^{d-1}H(K, n) > 0$, since the polynomial takes only positive values, for large enough n. If the degree is lower, then $\Delta^{d-1}H(K, n) = 0$. In either case, we find that

$$\Delta^{d-1}H(N, n) \leq \Delta^{d-1}H(\widetilde{N_0}, n) = l(N_0).$$

Now, we proceed to the proof of the equivalences. It's easy to see that (3) $\Rightarrow$ (2) $\Rightarrow$ (1), using the example above. We will show (1) $\Rightarrow$ (3): This will be done by showing that for any non-zero graded submodule K of $\widetilde{N_0}$, we have $\Delta^{d-1}H(K,n) \geq 1$. Given this, we see that $\Delta^{d-1}H(N,n) < l(N_0)$, whenever the kernel K of φ is non-zero. To prove our claim, take any composition series

$$0 = M_0 \subset M_1 \subset \ldots \subset M_s = N_0$$

of N_0. Then, for every i, $M_i/M_{i-1} \cong A/\mathfrak{m}_i$, for some maximal ideal $\mathfrak{m}_i \subset A$. Now, we get a filtration for K, by taking $F^iK = K \cap M_i[t_1, \ldots, t_d]$. Since $F^iK/F^{i-1}K \subset k[x_1, \ldots, x_d]$, where $k = A/\mathfrak{m}_i$, and $F^iK \neq F^{i-1}K$ for at least one i, it will suffice to show that $\Delta^{d-1}H(I,n) \geq 1$, where $0 \neq I \subset k[t_1, \ldots, t_d]$ is a homogeneous ideal. But now, I contains a homogeneous element f of, say, degree r, and we have

$$\Delta^{d-1}H(I,n) \geq \Delta^{d-1}H((f),n) = 1,$$

which is what we wanted to show. □

3.3. The Samuel Function.

NOTE ON NOTATION 5. From now on, R will be a Noetherian ring, and M will be a finitely generated module over R.

hfm-defn:ideal-of-defn

DEFINITION 2.3.13. An ideal $\mathfrak{q} \subset R$ is called an *ideal of definition* for the module M if $M/\mathfrak{q}M$ is an Artinian $R/\mathfrak{q}$-module.

REMARK 2.3.14. Observe that if $\mathfrak{q}$ is an ideal of definition for R, then it is an ideal of definition for every finitely generated R-module M. This is because $M/\mathfrak{q}M$ will be a finitely generated module over the Artinian ring $R/\mathfrak{q}$, and will thus be an Artinian module.

hfm-ideal-of-defn

LEMMA 2.3.15. *The following are equivalent for an ideal $\mathfrak{q} \subset M$.*

(1) *$\mathfrak{q}$ is an ideal of definition for M.*
(2) *$R/(\operatorname{ann} M + \mathfrak{q})$ is an Artinian ring.*
(3) *$\operatorname{Supp} M \cap V(\mathfrak{q})$ is a finite set consisting entirely of maximal ideals.*

PROOF. Observe that $M/\mathfrak{q}M$ is Artinian if and only if the ring $R/\operatorname{ann}(M/\mathfrak{q}M)$ is Artinian. Also observe that $\operatorname{ann}(M) + \mathfrak{q} \subset \operatorname{ann}(M/\mathfrak{q}M)$; so we have

$$\operatorname{Supp}(M/\mathfrak{q}M) = V(\operatorname{ann}(M/\mathfrak{q}M)) \subset V(\operatorname{ann}(M) + \mathfrak{q}) = \operatorname{Supp} M \cap V(\mathfrak{q}).$$

We will show equality. Indeed, let $P \in \operatorname{Supp}(M) \cap V(\mathfrak{q})$ be any prime. Then, we see that $M_P/\mathfrak{q}_P M_P \neq 0$, by Nakayama's Lemma. Hence $P \in \operatorname{Supp}(M/\mathfrak{q}M)$, which finishes our proof. □

REMARK 2.3.16. In the cases we'll be interested in, R will be a semilocal ring, that is a ring with only finitely many maximal ideals, and $\mathfrak{q}$ will be an ideal of definition for R, which is equivalent to saying that $\mathfrak{q}$ contains a power of $\operatorname{Jac}(R)$. There it's immediate that $\operatorname{Supp} M \cap V(\mathfrak{q})$ will contain only finitely many maximal ideals.

niteness-of-qadic-length

PROPOSITION 2.3.17. *Let $(R, \mathfrak{q})$ be the $\mathfrak{q}$-adic filtered ring, and let $(M, F^\bullet M)$ be a stable filtered module over $(R, \mathfrak{q})$. Then M/F^rM has finite length, for all $r \in \mathbb{N}$. Moreover, if $\mathfrak{q}$ is generated by s elements, the function $n \mapsto l(M/F^{n+1}M)$ is of polynomial type of degree at most s.*

PROOF. For every $r \in \mathbb{N}$, we have $F^r M \supset \mathfrak{q}^r M$. Hence, it suffices to show that $M/\mathfrak{q}^r M$ is Artinian, for every $r \in \mathbb{N}$. But this follows from the Lemma above, and the fact that $V(\mathfrak{q}) = V(\mathfrak{q}^r)$, for any $r \in \mathbb{N}$.

Consider the graded associated ring $\mathrm{gr}_{\mathfrak{q}}(R)$: this is generated in degree 1 by the s generators of $\mathfrak{q}$. Moreover, if $n_0 \in \mathbb{N}$ is such that $\mathfrak{q}F^n M = F^{n+1}M$, for all $n \geq n+0$ (this exists, since M is stable), then $\mathrm{gr}_F(M)$ is generated over $\mathrm{gr}_{\mathfrak{q}}(R)$ by the finitely generated $R/\mathfrak{q}$-submodule

$$M/F^1 M \oplus \ldots \oplus F^{n_0} M/F^{n_0+1}M,$$

and is hence finitely generated. So we are in a position to conclude, via (2.3.9) that the Hilbert function $H(\mathrm{gr}_F(M), \_\_)$ of M is of polynomial type of degree at most $s-1$. Now, observe that if $f_M : n \mapsto l(M/F^{n+1}M)$, then

$$\Delta f_M(n) = l(F^n M/F^{n+1}M) = H(\mathrm{gr}_F(M), n),$$

which is a function of polynomial type of degree at most $s-1$ by (2.3.9); so, by (2.3.6), f_M is a function of polynomial type of degree at most s. □

m-defn:samuel-polynomial

DEFINITION 2.3.18. Given a stable filtered module $(M, F^\bullet M)$ over $(R, \mathfrak{q})$, where $\mathfrak{q}$ is an ideal of definition for M, the *Hilbert polynomial* of M, denoted H^F_M, is the Hilbert polynomial associated to the graded module $\mathrm{gr}_F(M)$. As usual, if F is the natural $\mathfrak{q}$-adic filtration, we denote the polynomial by $H^{\mathfrak{q}}_M$

The *Samuel polynomial* of M, denoted χ^F_M, is the polynomial associated to the function of polynomial type f_M, where f_M is as in the proof of the Proposition above. Again, if F is the natural filtration, we denote this by $\chi^{\mathfrak{q}}_M$.

REMARK 2.3.19. Observe that we have $\Delta\chi^F_M = H^F_M$.

The next result shows how invariant χ^F_M is under different choices of $\mathfrak{q}$-adic filtration on M.

hfm-qadic-filtration

PROPOSITION 2.3.20. *Let $(M, F^\bullet M)$ be any stable filtered module over $(R, \mathfrak{q})$, and let $(M, \mathfrak{q})$ be the same underlying R-module equipped with the natural $\mathfrak{q}$-adic filtration. Suppose $\mathfrak{q}$ is an ideal of definition for M. Then, there exists a polynomial φ with $\deg\varphi < \deg\chi^{\mathfrak{q}}_M$ such that*

$$\chi^F_M - \chi^{\mathfrak{q}}_M = \varphi.$$

In particular, χ^F_M and $\chi^{\mathfrak{q}}_M$ have the same degree and leading coefficient.

PROOF. Observe that, by the stability of M, there exists $n_0 \in \mathbb{N}$ such that, for $n \geq n_0$,

$$\mathfrak{q}^n M \subset F^n M = \mathfrak{q}^{n-n_0} F^n_0 M \subset \mathfrak{q}^{n-n_0} M.$$

Hence, we see that, for $n > n_0$,

$$\chi^{\mathfrak{q}}_M(n-1) \geq \chi^F_M(n-1) \geq \chi^{\mathfrak{q}}_M(n-n_0-1).$$

One now gets the statement from the general result that if $p(t), q(t) \in \mathbb{Q}[t]$ are two polynomials such that there exists $n_0 \in \mathbb{N}$ with

$$p(n) \geq q(n) \geq p(n-n_0),$$

for $n \geq n_0$, then $\deg p = \deg q$, and they have the same leading coefficient. For this just observe that

$$\lim_{n\to\infty} \frac{q(n)}{p(n)} = 1.$$

□

REMARK 2.3.21. For most applications, we only care about the degree (in dimension theory), and the leading coefficient (in the study of multiplicities) of the Samuel polynomial. The above Proposition shows that, this being the case, we need only ever concern ourselves with the natural $\mathfrak{q}$-adic filtrations on our R-modules.

hfm-samuel-short-exctseq

COROLLARY 2.3.22. *Suppose we have an exact sequence of finitely generated R-modules*

$$0 \to M' \to M \to M'' \to 0.$$

Suppose also that $\mathfrak{q}$ is an ideal of definition for M. Then it is also an ideal of definition for M' and M'', and there is a polynomial φ, with $\deg \varphi < \deg \chi^{\mathfrak{q}}_{M'}$ such that

$$\chi^{\mathfrak{q}}_M - \chi^{\mathfrak{q}}_{M''} = \chi^{\mathfrak{q}}_{M'} + \varphi.$$

PROOF. Observe that $\operatorname{ann}(M) \subset \operatorname{ann}(M')$ and $\operatorname{ann}(M) \subset \operatorname{ann}(M'')$. Now, the first statement follows from (2.3.15).

For $r \in \mathbb{N}$, let $F^r M' = M'/(M' \cap \mathfrak{q}^r M)$; this is the filtration induced on M' by the $\mathfrak{q}$-adic filtration on M. By Artin-Rees (2.2.6), this is stable, and so by the Proposition we see that there is a polynomial φ, with $\deg \varphi < \deg \chi^{\mathfrak{q}}_{M'}$ such that

$$\chi^F_{M'} = \chi^{\mathfrak{q}}_{M'} + \varphi.$$

Now, we have the exact sequence

$$0 \to M'/(M' \cap \mathfrak{q}^n M) \to M/\mathfrak{q}^n M \to M''/\mathfrak{q}^n M'' \to 0.$$

This gives us the equality

$$\chi^{\mathfrak{q}}_M - \chi^{\mathfrak{q}}_{M''} = \chi^F_{M'} = \chi^{\mathfrak{q}}_M + \varphi.$$

□

The next Proposition shows that, to compute the Samuel polynomial, it suffices to be able to do it in the case where $(R, \mathfrak{m})$ is a local ring, and $\mathfrak{q} \subset \mathfrak{m}$ is a primary ideal.

hfm-samuel-local-ring

PROPOSITION 2.3.23. *Let M be a finitely generated R-module, and let $\mathfrak{q} \subset R$ be an ideal of definition for M. Suppose*

$$V(\mathfrak{q}) \cap \operatorname{Supp} M = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\},$$

and for $1 \leq i \leq r$, set $M_i = M_{\mathfrak{m}_i}$ and $\mathfrak{q}_i = \mathfrak{q}_{\mathfrak{m}_i}$. Then

$$\chi^{\mathfrak{q}}_M = \sum_{i=1}^{r} \chi^{\mathfrak{q}_i}_{M_i}.$$

PROOF. For each $n \in \mathbb{N}$, $M/\mathfrak{q}^n M$ is an Artinian module over the Artinian ring $R/(\mathfrak{q}^n + \operatorname{ann}(M))$, whose set of maximal ideals is precisely $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$. Then the identity falls out of the natural isomorphism

$$M/\mathfrak{q}^n M \cong \bigoplus_{i=1}^{r} M_i/\mathfrak{q}_i^n M_i,$$

and the fact that length is additive. □

Though the Samuel polynomial is linked with the pair $(\mathfrak{q}, M)$, where $\mathfrak{q}$ is an ideal of definition for a finitely generated module M, the next result shows that its *degree* is a somewhat coarse invariant. We will strengthen this result later in (6.2.14).

-ind-ideal-of-definition

PROPOSITION 2.3.24. *The degree of the Samuel polynomial $\chi_M^{\mathfrak{q}}$ depends only on the finite set* $\operatorname{Supp} M \cap V(\mathfrak{q})$ *and the module M.*

PROOF. Consider M as an S-module instead, where $S = R/\operatorname{ann}(M)$, and replace $\mathfrak{q}$ and $\mathfrak{q}'$ by $\mathfrak{q}S$ and $\mathfrak{q}'S$. In this case, we have $\operatorname{ann}(M) = 0$, and so $V(\mathfrak{q}) = V(\mathfrak{q}')$, which implies that $\operatorname{rad}(\mathfrak{q}) = \operatorname{rad}(\mathfrak{q}')$. Hence, we can find $n \in \mathbb{N}$ such that $\mathfrak{q}^n \subset \mathfrak{q}'$; and so

$$\chi_M^{\mathfrak{q}}(mn-1) \geq \chi_M^{\mathfrak{q}'}(m-1),$$

for all $m \in \mathbb{N}$. This shows that

$$\deg \chi_M^{\mathfrak{q}} \geq \deg \chi_M^{\mathfrak{q}'}.$$

We get the other inequality by symmetry. □

As we discussed in our introduction to I-adic filtrations and the associated graded ring, we have a natural surjective map

$$(M/\mathfrak{q}M)[t_0, \ldots, t_d] \to \operatorname{gr}_{\mathfrak{q}}(M),$$

where $\mathfrak{q}$ is some ideal of definition for M generated by d elements. The next Proposition looks at the behavior of this map and relates it to the leading coefficient of the Samuel polynomial $\chi_M^{\mathfrak{q}}$.

hfm-sop-quasiregular

PROPOSITION 2.3.25. *For any ideal of definition $\mathfrak{q} \subset R$, and any faithful, finitely generated R-module M, we have*

$$\Delta^d \chi_M^{\mathfrak{q}} \leq l(M/\mathfrak{q}M).$$

Equality above holds if and only if either of the following conditions is true:

1. $\chi_M^{\mathfrak{q}}(n) = l(M/\mathfrak{q}M)\binom{n+d}{d}$.
2. *The natural map*

$$(M/\mathfrak{q}M)[t_1, \ldots, t_d] \to \operatorname{gr}_{\mathfrak{q}}(M)$$

is an isomorphism.

PROOF. Observe that $\Delta\chi_M^{\mathfrak{q}}(n) = H(\operatorname{gr}_{\mathfrak{q}}(M), n)$, by definition. Hence we see that

$$\Delta^d \chi_M^{\mathfrak{q}} = \Delta^{d-1} H(\operatorname{gr}_{\mathfrak{q}}(M), n) \leq l(M/\mathfrak{q}M),$$

by Proposition (2.3.12). Now, the equivalences in the statement follow from the same Proposition, and the equivalences that we give right below.

$$\Delta^d \chi_M^{\mathfrak{q}} = l(M/\mathfrak{q}M) \Leftrightarrow \Delta^{d-1} H(\operatorname{gr}_{\mathfrak{q}}(M), n) = l(M/\mathfrak{q}M).$$

$$\chi_M^{\mathfrak{q}}(n) = l(M/\mathfrak{q}M)\binom{n+d}{d} \Leftrightarrow H(\operatorname{gr}_{\mathfrak{q}}(M), n) = l(M/\mathfrak{q}M)\binom{n+d-1}{d-1}.$$

For the equivalence with (2) just take $N = \operatorname{gr}_{\mathfrak{q}}(M)$, and $N_0 = M/\mathfrak{q}M$ in (3) of Proposition (2.3.12). □

CHAPTER 3

Flatness

chap:flat

NOTE ON NOTATION 6. In this chapter, R will denote a commutative ring

1. Basics

DEFINITION 3.1.1. An R-module M is *flat* if the functor

$$M \otimes_R \_\_ : R\text{-mod} \longrightarrow R\text{-mod}$$

is left exact; or, equivalently, if the functor above is exact.

An important characteristic of flat modules is that they commute with cohomology of complexes, in a sense that will be made clear in the following proposition.

flat-commutes-cohomology

PROPOSITION 3.1.2. *Let $C^\bullet$ be a chain complex of R-modules, and let M be a flat R-module. Then we have*

$$H^\bullet(C) \otimes_R M \cong H^\bullet(C \otimes_R M).$$

PROOF. All this is saying is that tensoring with M preserves kernels and cokernels. □

at-intersections-commute

COROLLARY 3.1.3. *Let M be an R-module, and let $\{M_i : i \in I\}$ be a collection of R-submodules of M. Let N be a flat R-module; then, we have a natural isomorphism*

$$(\bigcap_i M_i) \otimes_R N \cong \bigcap_i (M_i \otimes_R N) \subset M \otimes_R N.$$

PROOF. Observe that $\bigcap_i M_i$ is the kernel of the map $M \to \bigoplus_i M/M_i$, and that we have

$$(\bigoplus_i M/M_i) \otimes_R N = \bigoplus_i (M \otimes_R N)/(M_i \otimes_R N),$$

and use flatness of N again to get the result. □

flat-direct-sum

PROPOSITION 3.1.4. *Let $\{M_i : i \in I\}$ be a collection of R-modules. Then $M = \bigoplus_i M_i$ is flat if and only if each of the M_i is flat.*

PROOF. It's evident that tensoring by M preserves monomorphisms only if tensoring by each of the M_i does. For the other direction, use the fact that direct sum is an exact functor that commutes with tensor product. □

flat-projective

COROLLARY 3.1.5. *Any projective R-module is flat.*

PROOF. Any projective R-module is a direct summand of a free module, and the statement now follows from the Proposition above, since free modules are clearly flat. □

flat-base-change

PROPOSITION 3.1.6. *Let S be any commutative R-algebra, let M be a flat R-module, and let N be a flat S-module.*

(1) *$M \otimes_R N$ is flat over S.*
(2) *If S is flat over R, then so is N.*
(3) *If M is also an S-module, then $N \otimes_S M$ is flat over R.*

PROOF. (1) Observe that, for any S-module P, we have the natural isomorphism

$$(M \otimes_R N) \otimes_S P \cong M \otimes_R (N \otimes_S P)$$

Since the functors $N \otimes_S \_\_$ and $M \otimes_R \_\_$ are both exact, this tells us that $M \otimes_R N$ is flat over S.

(2) Similar to the first part: note that the functor $N \otimes_R \_\_$ is isomorphic to $N \otimes_S S \otimes_R \_\_$, which is the composition of two exact functors.

(3) Same kind of proof: observe that the functor in question is the composition $N \otimes_S M \otimes_R \_\_$ of exact functors.

□

REMARK 3.1.7. Of course, the commutativity hypothesis can be removed with a careful handling of right-left subtleties, but we won't need the more general assertion.

at-localization-quotient

COROLLARY 3.1.8. *Let M be a flat R-module.*

(1) *For any ideal $I \subset R$, M/IM is a flat R/I-module.*
(2) *For any multiplicative subset $S \subset R$, $S^{-1}M$ is flat over $S^{-1}R$.*

PROOF. Both follow immediately from the Proposition. □

at-iff-localization-flat

PROPOSITION 3.1.9. *The following are equivalent for an R-module M:*

(1) *M is flat.*
(2) *M_P is a flat R_P-module, for every prime $P \subset R$.*
(3) *$M_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module, for every maximal ideal $\mathfrak{m} \subset R$.*

PROOF. (1) ⇒ (2) ⇒ (3) follows immediately from part (2) of the previous Corollary. We will show (3) ⇒ (1). Observe that it's enough to show that tensoring by M preserves injections. So let $\varphi : P \to N$ be an injection, and consider the map

$$1 \otimes \varphi : M \otimes_R P \to M \otimes_R N.$$

For every maximal ideal $\mathfrak{m} \subset R$, we see that $(1 \otimes \varphi)_\mathfrak{m}$ is an injection. Therefore, $1 \otimes \varphi$ must also be an injection, thus finishing our proof. □

at-relative-localization

COROLLARY 3.1.10. *Let S be a commutative R-algebra, and let M be an S-module. Then the following are equivalent:*

(1) *M is flat over R*
(2) *For every prime $Q \subset S$, M_Q is flat over R_P, where $P = Q^c \subset R$.*
(3) *For every maximal ideal $Q \subset S$, M_Q is flat over R_P, where $P = Q^c \subset R$.*

PROOF. For (1) ⇒ (2), note that $M_Q \cong M_P \otimes_{S_P} S_Q$, where M_P is flat over R_P and S_Q is flat over S_P. The implication now follows from part (3) of (3.1.6). (2) ⇒ (3) is trivial, so we'll finish by proving (3) ⇒ (1). So suppose $N' \to N$ is a monomorphism of R-modules; then we'll be done if we show that $M \otimes_R N' \to M \otimes_R N$ is a monomorphism of S-modules. It suffices to show this after localizing

at a maximal ideal $Q \subset S$; but that this is true follows immediately from our hypothesis in (3). □

The next Proposition will be used often in the remainder of these notes.

-pres-hom-tensor-commute

PROPOSITION 3.1.11. *Let S be an R-algebra, let M and N be R-modules, with M finitely presented and let P be an S-module flat over R. Then, we have a natural isomorphism*

$$\Psi : \mathrm{Hom}_R(M, N) \otimes_R P \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R P).$$

PROOF. First let's define the map. Given a map $\varphi : M \to N$ and $p \in P$, we send $\varphi \otimes p$ to the map

$$\Psi(\varphi) : M \otimes_R SN \otimes_R P$$
$$m \otimes s \mapsto \varphi(m) \otimes sp.$$

One checks immediately that this assignment is well defined, and that the statement is true for $M = R$, and hence for $M = R^n$, for all $n \in \mathbb{N}$. Given this, and a finite presentation $R^n \to R^m \to M$, we have the following diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(M, N) \otimes_R P & \longrightarrow & \mathrm{Hom}_R(R^m, N) \otimes_R P & \longrightarrow & \mathrm{Hom}_R(R^n, N) \otimes_R P \\ & & \downarrow & & \downarrow \cong & & \downarrow \cong \\ 0 & \longrightarrow & \mathrm{Hom}_S(M \otimes_R S, N \otimes_R P) & \longrightarrow & \mathrm{Hom}_S(S^m, N \otimes_R P) & \longrightarrow & \mathrm{Hom}_S(S^n, N \otimes_R P) \end{array}$$

which tells us that the map on the left is also an isomorphism. We used the flatness of P to ensure that the top row is exact. □

fin-pres-hom-loc-commute

COROLLARY 3.1.12. *Let $U \subset R$ be a multiplicative set, and let M and N be R-modules, with M finitely presented. Then we have a natural isomorphism*

$$U^{-1} \mathrm{Hom}_R(M, N) \cong \mathrm{Hom}_{U^{-1}R}(U^{-1}M, U^{-1}N).$$

PROOF. Simply observe that $U^{-1}R$ is flat over R. □

REMARK 3.1.13. See also [RS, 4.16] for the corresponding statement for finitely presented sheaves.

2. Homological Criterion for Flatness

The most important characterization of flat modules is the following homological one.

at-homological-criterion

THEOREM 3.2.1 (Homological Criterion). *The following are equivalent for an R-module M*

1. *M is flat.*
2. *For every R-module N, and every $n \in \mathbb{N}$, $\mathrm{Tor}_n^R(N, M) = 0$.*
3. *For every ideal $I \subset R$, $\mathrm{Tor}^1(R/I, M) = 0$.*
4. *For every ideal $I \subset R$, the natural map*
$$I \otimes_R M \to M$$
is an injection.
5. *For every finitely generated R-module N, $\mathrm{Tor}_1^R(N, M) = 0$.*

(6) *For every injection $\varphi : N \to P$, with N and P finitely generated,*

$$\varphi \otimes 1 : N \otimes_R M \to P \otimes_R M$$

is also an injection.

PROOF. (1) $\Leftrightarrow$ (2)**:** Follows from the definition of the derived functor $\mathrm{Tor}^R_\bullet(\_\_, M)$.

(2) $\Rightarrow$ (3)**:** Trivial.

(3) $\Leftrightarrow$ (4)**:** Follows from the long exact sequence for $\mathrm{Tor}^R_\bullet(\_\_, M)$ associated to the short exact sequence

$$0 \to I \to R \to R/I \to 0.$$

(3) $\Rightarrow$ (5)**:** We will do this by induction on the number of generators of N. If N has a single generator, then $N \cong R/I$, for some ideal $I \subset R$, and so the statement follows. Otherwise, suppose N is generated by $\{n_1, \ldots, n_r\}$, and let $N' \subset N$ be the submodule generated by $\{n_1, \ldots, n_{r-1}\}$. We then have an exact sequence

$$0 \to N' \to N \to N/N' \to 0.$$

By induction, $\mathrm{Tor}^R_1(N', M) = \mathrm{Tor}^R_1(N/N', M) = 0$, and so from the long exact sequence associated to $\mathrm{Tor}^R_\bullet(\_\_, M)$, we see that $\mathrm{Tor}^R_1(N, M) = 0$.

(5) $\Rightarrow$ (6)**:** Easy. Use the long exact sequence for Tor.

(6) $\Rightarrow$ (1)**:** Suppose $\varphi : N \to P$ is an injection, and $x = \sum_{i=1}^t n_i \otimes m_i \in \ker(\varphi \otimes 1)$, where

$$\varphi \otimes 1 : N \otimes M \to P \otimes M.$$

Then, by replacing N by the submodule generated by the n_i and P by the submodule generated by the images $\varphi(n_i)$, we are back in the situation of (6), which tells us that $x = 0$.

□

lat-pid-iff-torsion-free

COROLLARY 3.2.2. *Any flat R-module is torsion free. If R is a principal ring, then an R-module is flat if and only if it is torsion free.*

PROOF. Follows immediately from characterization (4) above. □

flat-end-exact-sequence

COROLLARY 3.2.3. *For any R-module N, and any short exact sequence*

$$0 \to F' \to F \to F'' \to 0,$$

with F'' flat, the sequence

$$0 \to N \otimes_R F' \to N \otimes_R F \to N \otimes_R F'' \to 0$$

is also exact.

PROOF. Follows from the long exact sequence for $\mathrm{Tor}^R_\bullet(N, \_\_)$, along with the fact that $\mathrm{Tor}^R_1(N, F'') = 0$, which follows from flatness of F''. □

flat-short-exct-seq

COROLLARY 3.2.4. *Suppose we have a short exact sequence of R-modules:*

$$0 \to F' \to F \to F' \to 0.$$

Suppose F'' is flat. Then F' is flat if and only if F is flat.

PROOF. That F'' is flat tells us that $\mathrm{Tor}_n^R(F'', N)$ vanishes in all positive degrees and for all R-modules N. Hence, we find from the long exact sequence of $\mathrm{Tor}_n^R(\_\_, N)$ associated to the long exact sequence above that

$$\mathrm{Tor}_n^R(F', N) \cong \mathrm{Tor}_n^R(F, N),$$

for all R-modules N and for all $n \geq 1$. Now the statement follows from characterization (2) in the Theorem above. □

3. Equational Criterion for Flatness

t-equation-kernel-tensor

LEMMA 3.3.1. *Let M and N be R-modules, and suppose that $\{n_i : i \in I\}$ is a collection of generators for N. Then, an element $x \in N \otimes_R M$, written as a finite sum $\sum_{i\in I} n_i \otimes m_i$ is 0 if and only if there exist elements $m'_j \in M$ and $a_{ij} \in R$ such that*

$$\sum_j a_{ij} m'_j = m_i, \text{ for all } i;$$
$$\sum_i a_{ij} n_i = 0, \text{ for all } j.$$

PROOF. If such elements exist, then we have

$$\begin{aligned}\sum_{i\in I} n_i \otimes \left(\sum_j a_{ij} m'_j\right) &= \sum_j \left(\sum_i a_{ij} n_i\right) \otimes m'_j \\ &= \sum_j 0 \times m'_j = 0.\end{aligned}$$

Let G be a free module on the set I, and let $F \to G \to N \to 0$, be a presentation induced by the natural surjection $G \to N \to 0$, that sends a basis element $g_i \in G$ to $n_i \in N$. This induces a short exact sequence

$$F \otimes M \to G \otimes M \to N \otimes M \to 0.$$

Then we see that the element $\sum_i g_i \otimes m_i$ maps to 0 in $N \otimes M$, and hence is in the image of the map $F \otimes M \to G \otimes M$. So we can find $y_j \in \mathrm{im}(F \to G)$ and $m'_j \in M$ such that

$$\sum_i g_i \otimes m_i = \sum_j y_j \otimes m'_j.$$

Let $a_{ij} \in R$ be such that $y_j = \sum_i a_{ij} g_i$, for all j. Then we have

$$\sum_i g_i \otimes (m_i - \sum_j a_{ij} m'_j) = 0.$$

Since $G \otimes M$ is isomorphic to a direct sum of copies of M, this identity implies that $m_i = \sum_j a_{ij} m'_j$, for each i. Moreover, we find that $\sum_i a_{ij} n_i = 0$, since y_i is in the image of F, which is also the kernel of the surjection $G \to N$. □

lat-equational-criterion

THEOREM 3.3.2 (Equational Criterion). *The following are equivalent for an R-module M:*

(1) *M is flat.*

(2) *For every relation* $0 = \sum_i n_i m_i$*, with* $m_i \in M$ *and* $n_i \in R$*, there exist elements* $m'_j \in M$ *and* $a_{ij} \in R$ *such that*

$$\sum_j a_{ij} m'_j = m_i, \text{ for all } i;$$
$$\sum_i a_{ij} n_i = 0, \text{ for all } j.$$

(3) *For every map* $\beta : F \to M$ *with* F *a free module of finite rank, and for every finitely generated submodule* K *of* $\ker \beta$*, there is a commutative diagram*

$$\begin{array}{ccc} F & \xrightarrow{\gamma} & G \\ \| & & \downarrow \\ F & \xrightarrow{\beta} & M \end{array}$$

with G *free and with* $K \subset \ker \gamma$*.*

PROOF. (1) $\Leftrightarrow$ (2)**:** We observe simply that both (1) and (2) are equivalent to the statement that for every ideal $I \subset R$, the map $I \otimes_R M \to M$ is injective. The equivalence of this statement with (1) we showed in (3.2.1). For its equivalence with (2), note that the map $I \otimes_R M \to M$ is injective if and only if the following condition holds: A relation $\sum_i n_i \otimes m_i = 0$ holds in $I \otimes_R M$ if and only if the relation $\sum_i n_i m_i = 0$ holds in M. Now, the equivalence we need follows from the Lemma above.

(2) $\Rightarrow$ (3)**:** Let $\{g_i : 1 \leq i \leq r\}$ be a basis for F. Suppose K is generated by $\{f_k : 1 \leq k \leq s\}$. Let $n_i \in R$ be such that $f_1 = \sum_i n_i g_i$. Then, we find that

$$0 = \beta(a_1) = \sum_i n_i m_i,$$

where $m_i = \beta(g_i)$. Let $a_{ij} \in R$ and $m'_j \in M$ be the elements associated to this relation as in (2). Let G_1 be the free module on the elements m'_j with its natural map into M, and let $\gamma_1 : F \to G_1$ be the map given by the matrix (a_{ij}). Then, we find that

$$\gamma_1(f_1) = \sum_{i,j} (a_{ij} n_i)\, m'_j = 0.$$

Now we repeat this using the image of K in G_1, which is now generated by one fewer element, to define a map $\gamma_2 : F \to G_2$, which has both f_1 and f_2 in its kernel. Rinse and repeat. After each step, the number of generators that are non-zero strictly decreases, and so eventually all the generators of K will be in the kernel of $\gamma = \gamma_s$.

(3) $\Rightarrow$ (2)**:** Let F be the free module on the set $\{m_i\}$ and let $\beta : F \to M$ be the natural map. Then, the relation $\sum_i n_i m_i = 0$ gives an element $f \in \ker \beta$. The rest is just the argument in the first part of the proof of the last implication, only threaded backwards.

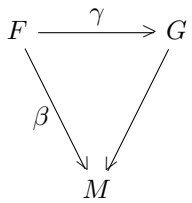
□

REMARK 3.3.3. What the equational criterion says is this: suppose we have a solution set to a finite bunch of linear equations in a flat module M. Then we can find elements $m'_1, \ldots, m'_k \in M$ such that these solutions lie in the submodule generated by the m'_i, and such that the coefficients of the m'_i in the linear expansion of the solutions can themselves be chosen to be solutions of the same linear equations in R.

t-finpres-iff-projective

COROLLARY 3.3.4. *A finitely presented R-module M is flat if and only if it is projective.*

PROOF. First assume that M is flat. Let $F' \to F \xrightarrow{\beta} M \to 0$ be a finite free presentation of M. This implies that $\ker\beta$ is finitely generated, and so by part (3) of the Theorem we can find a free module G and a map $\gamma : F \to G$ such that $\ker\beta \subset \ker\gamma$, and such that the following diagram commutes:



Since β is surjective, it follows that the map $G \to M$ is also surjective. Moreover, $\operatorname{im}\gamma$ maps isomorphically onto M, and so the surjection $G \to M$ in fact has a splitting, which makes M a direct summand of the free module G, and hence a projective R-module.

The other implication actually holds without any assumptions on M. See (3.1.5). □

flat-local-fingen-basis

COROLLARY 3.3.5. *Let $(R, \mathfrak{m})$ be a local ring, and let M be a flat R-module. If $x_1, \ldots, x_n \subset M$ are such that their images in $M/\mathfrak{m}M$ are linearly independent over $R/\mathfrak{m}$, then the x_i are linearly independent over R.*

PROOF. We'll do this by induction on n. If $n = 1$, then we have to show that $\operatorname{ann}(x_1) = 0$. But observe that if $ax_1 = 0$, for some $a \in R$, then we can find $b_j \in R$ and $m'_j \in M$ such that $x_1 = \sum_j b_j m'_j$ and $ab_j = 0$, for all j. By assumption $x_1 \notin \mathfrak{m}M$, and so there exists at least one j such that $b_j \notin \mathfrak{m}$ is a unit, which implies that $a = 0$.

Now, suppose $n > 1$, and suppose we have a relation $\sum_i a_i x_i = 0$. In this case, we can find $m'_j \in M$ and $b_{ij} \in R$ such that $x_i = \sum_j b_{ij} m'_j$, for all i, and such that $\sum_i a_i b_{ij} = 0$, for all j. Again, since $x_n \notin \mathfrak{m}M$, there is at least one j such that $b_{nj} \notin \mathfrak{m}$ is a unit. This implies that a_n is a linear combination of $a_1, \ldots, a_{n-1}$. So suppose $a_n = \sum_{i \le n-1} c_i a_i$; then we have

$$\begin{aligned} 0 &= \sum_{i \le n-1} a_i x_i + \sum_{i \le n-1} c_i a_i x_n \\ &= \sum_{i \le n-1} a_i (x_i + c_i x_n). \end{aligned}$$

But now, the images of $x_1 + c_1 x_n, \ldots, x_{n-1} + c_{n-1} x_n$ are linearly independent in $M/\mathfrak{m}M$, and so, by induction, this implies that $a_i = 0$, for all $i \le n-1$, which then implies also that $a_n = 0$, by our proof of the base case. □

at-finpres-kernel-fingen

LEMMA 3.3.6. *Suppose M is a finitely presented R-module, and let $\varphi : N \to M$ be a surjection with N finitely generated. Then* $\ker\varphi$ *is also finitely generated.*

PROOF. Let $F \to G \to M \to 0$ be a free presentation of M by free modules of finite rank. Then, $K = \ker(G \to M)$ is finitely generated, and we have the following picture:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K & \longrightarrow & G & \longrightarrow & M & \longrightarrow & 0 \\ & & \vdots & & \vdots & & \| & & \\ 0 & \longrightarrow & \ker\varphi & \longrightarrow & N & \xrightarrow{\varphi} & M & \longrightarrow & 0 \end{array}$$

The dotted map in the middle is the lifting to G obtained via its projectivity, and the dotted map at the left is obtained via the universal property of kernels. Now, by the Snake Lemma we see that

$$\operatorname{coker}(K \to \ker\varphi) \cong\cong \operatorname{coker}(G \to N)$$

is finitely generated. Since the image of K in $\ker\varphi$ is also finitely generated, we see that $\ker\varphi$ must also be finitely generated. □

flat-local-ring-free

PROPOSITION 3.3.7. *Let $(R, \mathfrak{m})$ be a local ring, and let M be a finitely generated R-module. Then the following are equivalent.*

1. *M is flat.*
2. *M is free.*

If M is finitely presented, then these are equivalent to

1. $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.
2. *The map $\mathfrak{m} \otimes M \to M$ is injective.*

PROOF. The first equivalence follows from (3.3.5), and from Nakayama's Lemma. The equivalence of the last two assertions is clear. We'll be done if we show that $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$, for a finitely presented R-module M, implies that M is free. For this, choose any minimal set $\{x_1, \ldots, x_n\}$ of generators for M, and let F be the free R-module on n generators. Then we have a short exact sequence

$$0 \to \ker\beta \to F \xrightarrow{\beta} M \to 0,$$

where β is the map taking the generators of F to the x_i. If we tensor this sequence with $R/\mathfrak{m}$, and use the fact about the vanishing of $\operatorname{Tor}_1^R(R/\mathfrak{m}, M)$, we obtain another short exact sequence

$$0 \to \ker\beta \otimes R/\mathfrak{m} \to F/\mathfrak{m}F \to M/\mathfrak{m}M \to 0.$$

But observe now that the map on the right is an isomorphism. Hence $\ker\beta \otimes R/\mathfrak{m} = 0$. But since M is finitely presented, $\ker\beta$ is finitely generated, by the Lemma above, and so, by Nakayama, $\ker\beta = 0$, showing that β was an isomorphism. □

t-fingen-iff-locallyfree

COROLLARY 3.3.8. *Let M be a finitely generated R-module. Then the following are equivalent:*

1. *M is flat.*
2. *M_P is a free R_P-module, for all primes $P \subset R$.*
3. *$M_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module, for all maximal ideals $\mathfrak{m} \subset R$.*

If, in addition, M is finitely presented, then these are also equivalent to:

(1) $\operatorname{Tor}_1^R(R/P, M) = 0$, *for all primes* $P \subset R$.
(2) $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$, *for all maximal ideals* $\mathfrak{m} \subset R$.

PROOF. This follows from the previous Proposition, (3.1.9), and the fact that Tor commutes with localizations. □

4. Local Criterion for Flatness

If we impose Noetherian conditions on our rings, we can obtain stronger results. The next Theorem and its corollaries are very important for geometric applications. We'll present the Theorem in rather broad generality, but it is mostly used in its incarnation as the local criterion for flatness, and the splicing criterion for flatness, which are the corollaries immediately following it.

Before we state the Theorem, we set up some notation. Let R be a Noetherian ring and let M be an R-module. For a given ideal $I \subset R$, we say that M is *I-adically ideal separated* if, for every ideal $\mathfrak{a} \subset R$, the module $\mathfrak{a} \otimes_R M$ is separated when equipped with the I-adic filtration. That is, if we have

$$\bigcap_{n \in \mathbb{N}} I^n(\mathfrak{a} \otimes_R M) = 0,$$

for every ideal $\mathfrak{a} \subset R$.

Now, for every $n \in \mathbb{N}$, we have a natural map

$$\alpha_n : \left(I^n/I^{n+1}\right) \otimes_A M \to I^n M/I^{n+1}M,$$

induced by the inclusion map $I^n/I^{n+1} \to A/I^{n+1}$.

Putting all these maps together gives us a morphism of graded $\operatorname{gr}_I(A)$-modules

$$\alpha : \operatorname{gr}_I(A) \otimes_A M \to \operatorname{gr}_I(M).$$

We're now ready to state the Theorem.

separated-filt-criterion

THEOREM 3.4.1. *Let R be a Noetherian ring, $I \subset R$ an ideal, and M an R-module that is I-adically ideal separated. Then the following are equivalent:*

(1) *M is flat over R.*
(2) *$\operatorname{Tor}_1^R(N, M) = 0$, for every R/I-module N.*
(3) *M/IM is flat over R/I, and $\operatorname{Tor}_1^R(R/I, M) = 0$.*
(4) *M/IM is flat over R/I, and $I \otimes_R M \to M$ is an injection.*
(5) *M/IM is flat over R/I, and α_n is an isomorphism, for all $n \geq 0$.*
(6) *M/IM is flat over R/I, and α is an isomorphism.*
(7) *$M/I^n M$ is flat over R/I^n, for every $n \geq 1$.*

In fact the sequence of implications

$$(1) \Rightarrow (2) \Leftrightarrow (3) \Leftrightarrow (4) \Rightarrow (5) \Leftrightarrow (6) \Rightarrow (7)$$

holds without any assumptions on M.

PROOF. So we begin with no assumptions on M.

(1) $\Rightarrow$ (2)**:** Immediate.
(2) $\Leftrightarrow$ (3)**:** For any monomorphism $N' \to N$ of R/I-modules, tensoring with M over R gives us an exact sequence

$$\operatorname{Tor}_1^R(N/N', M) \to N' \otimes_R M \to N \otimes_R M.$$

Now, since $N \otimes_R M \cong N \otimes_{R/I} (M/IM)$, we see that $\operatorname{Tor}_1^R(N/N', M) = 0$ if and only if

$$N' \otimes_{R/I} (M/IM) \to N \otimes_{R/I} (M/IM)$$

is also an injection. So we see that if (2) holds, then (3) follows immediately. Conversely, suppose (3) holds, and let N be any R/I-module; then we have an exact sequence

$$0 \to K \to F \to N \to 0,$$

where F is a free R/I-module. This gives us an exact sequence

$$\operatorname{Tor}_1^R(F, M) \to \operatorname{Tor}_1^R(N, M) \to K \otimes_R M \to F \otimes_R M.$$

But the map on the right is an injection, since M/IM is flat over R/I; therefore the map in the middle must be 0. Moreover, since tensor product commutes with direct sums, we find that $\operatorname{Tor}_1^R(F, M) = 0$, and so $\operatorname{Tor}_1^R(N, M) = 0$.

(3) $\Leftrightarrow$ (4)**:** Trivial.

(4) $\Rightarrow$ (5)**:** We'll show something stronger. Using induction, we'll show that $I^n \otimes_R M = I^n M$, for $n \in \mathbb{N}$. For $n = 1$, this is our hypothesis in (4). Suppose $n \geq 1$; then we have an exact sequence

$$0 \to I^{n+1} \to I^n \to I^n/I^{n+1} \to 0$$

Since, (4) is equivalent to (2), we have $\operatorname{Tor}_1^R(I^n/I^{n+1}, M) = 0$, and so the sequence

$$0 \to I^{n+1} \otimes_R M \to I^n \otimes_R M \to \left(I^n/I^{n+1}\right) \otimes_R M \to 0$$

is exact. Therefore, we see that

$$I^{n+1} \otimes_R M \to I^n \otimes_R M = I^n M$$

is an injection, where the equality holds by the induction hypothesis. This implies that $I^{n+1} \otimes_R M = I^{n+1} M$. Moreover, we also have

$$\left(I^n/I^{n+1}\right) \otimes_R M \cong \left(I^n \otimes_R M\right) / \left(I^{n+1} \otimes_R M\right) = I^n M / I^{n+1} M,$$

which is what we wanted.

(5) $\Leftrightarrow$ (6)**:** This is trivial.

(5) $\Rightarrow$ (7)**:** For $n \geq 0$, set $R_n = R/I^{n+1}$ and $M_n = M/I^{n+1}M$. We will show two things:

(1) $\operatorname{Tor}_1^{R_n}(R_n/IR_n, M_n) = 0$.

(2) M_n/IM_n is flat over R_n/IR_n.

Given these two facts, we find, using (2) $\Leftrightarrow$ (3), that $\operatorname{Tor}_1^{R_n}(N, M_n) = 0$, for all R_n/IR_n-modules N. Now, if P is any R_n-module, then IP is an R_{n-1}-module, and we have a short exact sequence

$$0 \to IP \to P \to P/IP \to 0.$$

Since P/IP is an R_n/IR_n-module, $\operatorname{Tor}_1^{R_n}(P/IP, M_n) = 0$. So to show that $\operatorname{Tor}_1^{R_n}(P, M) = 0$, it suffices to show $\operatorname{Tor}_1^{R_n}(IP, M) = 0$. This we can do by an inductive argument, where we assume that for any $k < n$, and any R_k-module N, we have $\operatorname{Tor}_1^{R_n}(N, M) = 0$. The base step follows from the fact that $R_n/IR_n \cong R/I$, and so, for any R_0-module N, we have $\operatorname{Tor}_1^{R_n}(N, M) = 0$.

So it now remains to prove assertions (1) and (2). Assertion (2) is immediate, since $M_n/IM_n \cong M/IM$ and $R_n/IR_n \cong R/I$. We only have to prove assertion (1). First observe that assertion (1) is equivalent to showing that the map

$$\sigma_n : IR_n \otimes_{R_n} M_n \to M_n$$

is a monomorphism, for all $n \in \mathbb{N}$. For this, we use induction on n. When $n = 0$, this is part of our hypothesis; so suppose $n \geq 1$. Consider the following short exact sequence:

$$0 \to I^n/I^{n+1} \to I/I^{n+1} \to I/I^n \to 0.$$

Tensor this with M to obtain the following diagram with exact rows:

$$\begin{array}{ccccccccc} & & \left(I^n/I^{n+1}\right) \otimes_R M & \longrightarrow & \left(I/I^{n+1}\right) \otimes_R M & \longrightarrow & (I/I^n) \otimes_R M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \sigma_n} & & \downarrow{\scriptstyle \sigma_{n-1}} & & \\ 0 & \longrightarrow & I^n M/I^{n+1}M & \longrightarrow & M_n & \longrightarrow & M_{n-1} & \longrightarrow & 0 \end{array}$$

By hypothesis, α_n is an isomorphism. Observe, moreover that, for all $n \geq 0$, we have

$$\left(I/I^{n+1}\right) \otimes_R M \cong IR_n \otimes_{R_n} M_n.$$

Therefore, by induction, σ_{n-1} is a monomorphism. Now, it's a simple application of the Snake Lemma to see that the map in the middle is also a monomorphism.

Now, assume that M is I-adically ideal separated.

(7) $\Rightarrow$ (1)**:** We will show that, for every ideal $\mathfrak{a} \subset R$, the map

$$\varphi : \mathfrak{a} \otimes_R M \to M$$

is an injection. We will do this by showing that

$$\ker \varphi \subset I^n(\mathfrak{a} \otimes_R M),$$

for all $n \in \mathbb{N}$. Once we've shown this, the hypothesis on M will tell us that $\ker \varphi = 0$, which is what we wanted to show.

Now, it suffices to show that, for all n, $\ker \varphi \subset \operatorname{im} \beta_n$, where

$$\beta_n : I^n \mathfrak{a} \otimes_R M \to \mathfrak{a} \otimes_R M,$$

By Artin-Rees (2.2.7), this is equivalent to showing that, for all $n \in \mathbb{N}$, $\ker \varphi \subset \operatorname{im} \gamma_n$, where

$$\gamma_n : (\mathfrak{a} \cap I^n) \otimes_R M \to \mathfrak{a} \otimes_R M,$$

But we have an exact sequence:

$$(\mathfrak{a} \cap I^n) \otimes_R M \xrightarrow{\gamma_n} \mathfrak{a} \otimes_R M \xrightarrow{\delta_n} (\mathfrak{a}/(\mathfrak{a} \cap I^n)) \otimes_R M \to 0.$$

So it suffices to show that $\ker \varphi \subset \ker \delta_n$, for all $n \in \mathbb{N}$. Now, observe that since M/I^nM is flat over R/I^n, the map

$$\eta_n : (\mathfrak{a}/(\mathfrak{a} \cap I^n)) \otimes_R M \xrightarrow{\cong} ((\mathfrak{a} + I^n)/I^n) \otimes_{R/I^n} (M/I^nM) \to M/I^nM$$

is injective. Consider the following diagram:

$$\begin{array}{ccc} \mathfrak{a} \otimes_R M & \xrightarrow{\delta_n} & (\mathfrak{a}/(\mathfrak{a} \cap I^n)) \otimes_R M \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \eta_n} \\ M & \xrightarrow{\pi_n} & M/I^n M \end{array}$$

From this diagram, we find that

$$\ker \varphi \subset \ker(\eta_n \circ \delta_n) = \ker \delta_n,$$

since η_n is injective. This finishes our proof.

□

flat-local-criterion

COROLLARY 3.4.2 (Local Criterion). *Suppose $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a local homomorphism of Noetherian local rings. Then, a finitely generated S-module M is flat over R if and only if $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.*

PROOF. We will show that M is $\mathfrak{m}$-adically ideal separated, and that characterization (3) above holds for M. The latter assertion is easy to show: $M/\mathfrak{m}M$ is always flat over $R/\mathfrak{m}$, for any R-module M, since $R/\mathfrak{m}$ is a field, and $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$, by hypothesis. So it suffices to prove the first assertion; for this, we observe that, for any ideal $\mathfrak{a} \subset R$, we have

$$\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n \left(\mathfrak{a} \otimes_R M\right) \subset \bigcap_{n \in \mathbb{N}} \mathfrak{n}^n \left(\mathfrak{a} \otimes_R M\right),$$

and the latter intersection is 0, by Krull's Intersection theorem (2.2.9). □

-infinitesimal-criterion

COROLLARY 3.4.3 (Infinitesimal Criterion). *Let $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of local Noetherian rings, and let M be a finitely generated S-module. Then M is flat over R if and only if $M/\mathfrak{m}^n M$ is flat over $R/\mathfrak{m}^n$, for all $n \in \mathbb{N}$.*

PROOF. As in the Corollary above, M is $\mathfrak{m}$-adically ideal separated. Moreover, it satisfies characterization (7) of the Theorem. Hence our result. □

See also (10.2.5) for another useful characterization of flatness.

5. The Graded Case

We will not give full proofs, since they are very similar to the ones in the ungraded case. In fact we could have assumed that everything was graded to start off, since, after all, ungraded rings are just trivially graded rings, but this adds a layer of unnecessary complexity; so we'll be presenting the graded case separately here, all in one place.

flat-graded-criterion

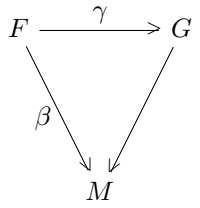
THEOREM 3.5.1 (The Graded Case). *Let R be a graded ring and let M be a graded R-module. Then the following are equivalent:*

(1) *M is flat.*
(2) *$\operatorname{Tor}_1^R(N, M) = 0$, for every graded R-module N.*
(3) *$\operatorname{Tor}_1^R(R/I, M) = 0$, for every homogeneous ideal $I \subset R$.*

(4) *For every homogeneous ideal $I \subset M$, the map $I \otimes M \to M$ is a monomorphism.*
(5) *Given any relation $\sum_i n_i m_i = 0 \in M$, with $n_i \in R$ and $m_i \in M$ homogeneous, we can find homogeneous elements $a_{ij} \in R$ and $m'_j \in M$ such that*

$$\sum_j a_{ij} m'_j = m_i, \text{ for all } i;$$
$$\sum_i a_{ij} n_i = 0, \text{ for all } j.$$

(6) *For every morphism $\beta : F \to M$ of graded modules, with F graded free, and every graded, finitely generated submodule $K \subset \ker \beta$, there is a graded free module G and a morphism $\gamma : F \to G$ of graded R-modules such that the following diagram commutes*



and such that $K \subset \ker \beta$.

PROOF. Most of this follows precisely how it did in (3.2.1) and (3.3.2). The only thing we will prove is (6) ⇒ (1). For this, we'll prove that the equational criterion as expressed in (3) of (3.3.2) holds for M. So suppose F is a free R-module of finite rank and let $\beta : F \to M$ be a map of R-modules. Suppose $g_1, \ldots, g_r$ is a basis for F and let $m_i = \beta(g_i) \in M$. Suppose $m_i = \sum_j m_{ij}$, where the $m_{ij} \in M$ are homogeneous, and let F' be the graded free module with generators g_{ij} satisfying $\deg g_{ij} = \deg m_{ij}$. Then, if $\beta' : F' \to M$ is the morphism of graded modules taking g_{ij} to m_{ij}, we have a map $\alpha : F \to F'$ taking g_i to $\sum_j g_{ij}$ such that $\beta = \beta' \circ \alpha$. It is clear that α is an injection. Now, given a finitely generated submodule $K \subset \ker \beta$, we get a finitely generated submodule $\alpha(K) \subset \ker \beta'$, and a graded free module G with a map $\gamma' : F' \to G$ such that $\alpha(K) \subset \ker \gamma'$ such that a diagram such as in (6) commutes. Now, take $\gamma = \gamma' \circ \alpha$ to finish the proof. □

We will not provide proofs of the next couple of results. The proofs are the same as in the ungraded case, but with Nakayama's Lemma replaced by its graded version (1.2.7), and of course, using the Theorem above instead.

-star-local-fingen-basis

COROLLARY 3.5.2. *Let $(R, \mathfrak{m})$ be a *local ring, and let M be a graded R-module. If $x_1, \ldots, x_n \in M$ are homogeneous elements such that their images in $M/\mathfrak{m}M$ are linearly independent over $R/\mathfrak{m}$, then the x_i are linearly independent over R.*

PROOF. □

lat-star-local-ring-free

PROPOSITION 3.5.3. *Let $(R, \mathfrak{m})$ be a *local ring, and let M be a finitely generated graded R-module. Then the following are equivalent.*

(1) *M is flat.*
(2) *M is free.*

If M is finitely presented, then these are equivalent to

(1) $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.
(2) *The map* $\mathfrak{m} \otimes M \to M$ *is injective.*

Using the Theorem, we can also present the graded counterpart for (3.4.1).

separated-filt-criterion

THEOREM 3.5.4. *Let R be a Noetherian graded ring, $I \subset R$ any ideal, and M a graded R-module. Suppose the following conditions hold:*

(1) *For every homogeneous ideal $J \subset R$, $J \otimes_R M$ is I-adically separated.*
(2) $\operatorname{Tor}_1^R(R/I, M) = 0$.
(3) *M/I is a flat R/I-module.*

Then M is flat over R.

PROOF. We basically need to prove the graded version of the implication (7) $\Rightarrow$ (1) in (3.4.1). This we do using the same proof; in this case, since we only need to prove that $J \otimes_R M \to M$ is a monomorphism for *homogenous* ideals $J \subset R$ (3.5.1), our assumption (1) is enough for the proof to go through. □

Using this, we can present a local criterion of flatness for *local rings. But first we need a lemma.

ar-local-faithfully-flat

LEMMA 3.5.5. *Let $(R, \mathfrak{m})$ be a Noetherian *local ring. Then, for any finitely generated graded R-module M, $M_\mathfrak{m} = 0$ if and only if $M = 0$.*

PROOF. One direction is trivial; so assume that $M_\mathfrak{m} = 0$. Then it follows that $\operatorname{Ass}_{R_\mathfrak{m}} M_\mathfrak{m} = \emptyset$. But we have

$$\operatorname{Ass}_{R_\mathfrak{m}} M_\mathfrak{m} = \{P_\mathfrak{m} : P \subset \mathfrak{m}\ , P \in \operatorname{Ass}_R M\}.$$

Moreover, since M is graded, we find from (1.4.2) that all the associated primes of M are homogeneous and are therefore contained in $\mathfrak{m}$. This means that $\operatorname{Ass}_R M = \emptyset$, and so $M = 0$. □

lat-star-local-criterion

COROLLARY 3.5.6. *Let $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a homomorphism between Noetherian *local rings, and let M be a finitely generated graded S-module. Then the following are equivalent:*

(1) *M is flat over R.*
(2) $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$.
(3) *$\mathfrak{m} \otimes_R M \to M$ is a monomorphism.*
(4) *$M_\mathfrak{n}$ is flat over $R_\mathfrak{m}$.*
(5) $\operatorname{Tor}_1^{R_\mathfrak{m}}(R_\mathfrak{m}/\mathfrak{m}_\mathfrak{m}, M_\mathfrak{n}) = 0$.
(6) *$\mathfrak{m}_\mathfrak{m} \otimes_{R_\mathfrak{m}} M_\mathfrak{n} \to M_\mathfrak{n}$ is a monomorphism.*

PROOF. Observe that, since f is a homomorphism of graded rings, $f(\mathfrak{m}) \subset \mathfrak{n}$. Using this, and the graded version of Krull's Intersection theorem (2.2.9), it's easy to show that M satisfies condition (1) in the Theorem above with respect to $\mathfrak{m}$. Condition (3) of the Theorem is trivially satisfied, since every graded $R/\mathfrak{m}$-module is free, by (1.2.5). So M is flat over R if and only if $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$. This gives us (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3).

(3) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5) follows from the Local Criterion for flatness (3.4.2). It's easy to see that (1) $\Rightarrow$ (4); so we'll be done if we show (5) $\Rightarrow$ (3). Let K be the kernel of the map in (3); then (5) says that $K_\mathfrak{n} = 0$. Hence, by the lemma above, $K = 0$, and our proof is done. □

6. Faithfully Flat Modules

lat-defn:faithfully-flat

DEFINITION 3.6.1. A flat R-module M is said to be *faithfully flat* if a chain complex $C^\bullet$ of R-modules is exact if and only if the complex $C^\bullet \otimes_R M$ is exact.

thfully-flat-base-change

PROPOSITION 3.6.2. *Let S be an R-algebra, let M be a faithfully flat R-module, and let N be a faithfully flat S-module. Then $M \otimes_R N$ is also a faithfully flat S-module.*

PROOF. Let $C^\bullet$ be a chain complex of S-modules such that $C^\bullet \otimes_S (N \otimes_R M)$ is exact. Then, since M is faithfully flat over R, we see that $C^\bullet \otimes_S N$ is exact, and since N is faithfully flat over S, we conclude that $C^\bullet$ is exact. □

fully-flat-loc-quotients

COROLLARY 3.6.3. *Let M be a faithfully flat R-module.*

1. *For every ideal $I \subset R$, M/IM is a faithfully flat R/I-module.*
2. *For every multiplicative set $S \subset R$, $S^{-1}M$ is a faithfully flat $S^{-1}R$-module.*

PROOF. Both follow from the Proposition and the fact that a ring is faithfully flat over itself. □

ithfully-flat-equiv-cond

THEOREM 3.6.4. *The following conditions are equivalent for a flat R-module M:*

1. *M is faithfully flat.*
2. *$M_\mathfrak{p}$ is a faithfully flat $R_\mathfrak{p}$-module, for all primes $\mathfrak{p} \subset R$.*
3. *For every prime ideal $\mathfrak{p} \subset R$, $k(\mathfrak{p}) \otimes_R M \neq 0$.*
4. *For every maximal ideal $\mathfrak{m} \subset R$, $M/\mathfrak{m}M \neq 0$.*
5. *For every proper ideal $I \subset R$, $M/IM \neq 0$.*
6. *For any non-zero R-module N, $M \otimes_R N \neq 0$.*

Moreover, if M is a faithfully flat R-module, then $\operatorname{Supp} M = \operatorname{Spec} R$.

PROOF. (1) ⇒ (2): Follows from (2) of the Corollary above.
(2) ⇒ (3): Suppose $k(\mathfrak{p}) \otimes_R M = 0$; then we have

$$k(\mathfrak{p}) \otimes_{R_\mathfrak{p}} M_\mathfrak{p} = 0.$$

But then we have $\mathfrak{p}_\mathfrak{p} M_\mathfrak{p} = M_\mathfrak{p}$, which means that $\mathfrak{p}_\mathfrak{p} = R_\mathfrak{p}$ (use the complex $0 \to \mathfrak{p} \to R$), which is absurd.
(3) ⇒ (4) is trivial.
(4) ⇒ (5): There is some maximal ideal $\mathfrak{m} \subset R$ with $I \subset \mathfrak{m}$, and since $M/\mathfrak{m}M$ is a quotient of M/IM, the result follows.
(5) ⇒ (6): Pick $0 \neq a \in N$; then $Ra \cong R/I$, where $I = \operatorname{ann}(M)$, and so $M \otimes_R Ra \neq 0$. But M is flat, and so $M \otimes_R Ra$ injects into $M \otimes_R N$, thus showing that $M \otimes_R N \neq 0$.
(6) ⇒ (1): Observe that $H^\bullet(C) = 0$ if and only if $H^\bullet(C) \otimes_R M = 0$. By (3.1.2), this will do.
As for the final statement, it's clear from characterization (2), that, whenever M is faithfully flat, we have $\operatorname{Supp} M = \operatorname{Spec} R$, since faithfully flat modules are in particular non-zero. □

cal-ring-faithfully-flat

COROLLARY 3.6.5. *Let $(R, \mathfrak{m})$ be a local ring, and let M be a finitely generated R-module. Then the following are equivalent:*

1. *M is free.*

(2) *M is flat.*
(3) *M is faithfully flat.*

PROOF. (1) $\Leftrightarrow$ (2) was shown in (3.3.7), and (3) $\Rightarrow$ (2) follows by definition. Moreover, it's clear that every free module is faithfully flat, which gives us (1) $\Rightarrow$ (3). □

lly-flat-spec-surjective

LEMMA 3.6.6. *Let $f : R \to S$ be a map of rings, and let M be an S-module, which is faithfully flat over R. Then the natural contraction map $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.*

PROOF. We need to show that, for every prime $\mathfrak{p} \subset R$, the ring $k(\mathfrak{p}) \otimes_R S \neq 0$. But observe that we have

$$0 \neq k(\mathfrak{p}) \otimes_R M = (k(\mathfrak{p}) \otimes_R S) \otimes_S M.$$

□

flat-defn-going-down

DEFINITION 3.6.7. We say that a map of rings $f : R \to S$ has the *going down property* when the following condition holds:

Given primes $\mathfrak{q} \subset S$ and $\mathfrak{p} \subset R$ such that $\mathfrak{q}^c = \mathfrak{p}$, and another prime $\mathfrak{p}^* \subsetneq \mathfrak{p}$, there is a prime $\mathfrak{q}^* \subset \mathfrak{q}$ such that $(\mathfrak{q}^*)^c = \mathfrak{p}^*$. In other words, the map $\operatorname{Spec} S_{\mathfrak{q}} \to \operatorname{Spec} R_{\mathfrak{p}}$ is surjective.

ithfully-flat-going-down

PROPOSITION 3.6.8 (Going Down for Flat Extensions). *Let $f : R \to S$ be a map of rings, and suppose there exists a finitely generated S-module M, which is flat over R. Then f has the going down property.*

PROOF. Suppose we have primes $\mathfrak{q} \subset S$ and $\mathfrak{p} \subset R$ such that $f^*(\mathfrak{q}) = \mathfrak{p}$. We have to show that the induced contraction map $\operatorname{Spec} S_{\mathfrak{q}} \to \operatorname{Spec} R_{\mathfrak{p}}$ is surjective. By the Lemma above, it's enough to show that $M_{\mathfrak{q}}$ is a faithfully flat $R_{\mathfrak{p}}$-module. Now, $M_{\mathfrak{q}}$ is flat over $R_{\mathfrak{p}}$ by (3.1.10). By (3.6.5), this implies that it is in fact faithfully flat over $R_{\mathfrak{p}}$, thus finishing our proof. □

faithfully-flat-algebras

PROPOSITION 3.6.9. *Let S be a flat R-algebra. Then the following are equivalent:*

(1) *S is faithfully flat over R.*
(2) *For every maximal ideal $\mathfrak{m} \subset R$, $\mathfrak{m}S \neq S$.*
(3) *For every non-zero R-module M, $M \otimes_R S \neq 0$.*
(4) *For every R-module M, the map $M \longrightarrow M \otimes_R S$ taking m to $m \otimes 1$ is injective.*
(5) *For every ideal $I \subset R$, we have $IS \cap R = I$.*
(6) *The induced map $\operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.*

PROOF. The equivalence of (1), (2) and (3) was part of (3.6.4). It's clear that (4) $\Rightarrow$ (3), and (5) $\Rightarrow$ (6) $\Rightarrow$ (2). We will show (3) $\Rightarrow$ (4) and (4) $\Rightarrow$ (5) to finish the proof. For (3) $\Rightarrow$ (4), observe that, for $0 \neq m \in M$, we can identify $S(m \otimes 1)$ with $(Rm) \otimes_R S$ using the following commutative diagram:

$$\begin{array}{ccccc} 0 & \longrightarrow & Rm & \longrightarrow & M \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & Rm \otimes_R S & \longrightarrow & M \otimes_R S \end{array}$$

But $(Rm) \otimes_R S \neq 0$ by (3), and so $m \otimes 1 \neq 0$.

For (4) $\Rightarrow$ (5), take $M = R/I$, and note that we have an injection $R/I \to S/IS$, which implies that $I \supset IS \cap R$. The other inclusion holds trivially. □

REMARK 3.6.10. In the language of schemes, one can rephrase this as saying: faithfully flat morphisms are the same as flat, surjective morphisms.

Here's a nice Corollary.

fully-flat-integral-extn

COROLLARY 3.6.11. *Suppose $R \subset S$ is a tower of domains, and suppose $K(R) = K(S)$. Then S is faithfully flat over R if and only if $S = R$.*

PROOF. One direction is trivial. For the other, suppose S is faithfully flat over R, and suppose $a = \frac{x}{y} \in S$, where $x, y \in R$. Let $I = (y) \subset R$, and observe that $x \in IS$. But $IS \cap R = I$, and so $x \in I$, showing that y divides x, and so $a \in R$. □

REMARK 3.6.12. Geometrically, this result is saying that a surjective, flat, birational morphism between two integral schemes is in fact an isomorphism.

CHAPTER 4

Integrality: the Cohen-Seidenberg Theorems

chap:iear

1. The Cayley-Hamilton Theorem

iear-cayley-hamilton

THEOREM 4.1.1 (Cayley-Hamilton). *Let $I \subset R$ be an ideal, and let M be an R-module generated by n elements over R. If $\phi \in \mathrm{End}_R(M)$ is such that $\phi(M) \subset IM$, then there are $a_j \in I^j$, for $0 \leq j < n$ such that*

$$\phi^n + a_{n-1}\phi^{n-1} + \ldots + a_1\phi + a_0 1_M = 0 \in \mathrm{End}_R(M).$$

Equivalently, there is a monic polynomial $p(t) \in R[t]$ of degree n such that $p(\phi) = 0$.

PROOF. We regard M as an $R[t]$-module, with t acting as ϕ. Let $\{m_1, \ldots, m_n\}$ be a generating set for M over R. Then, we can find a matrix $A = (a_{ij}) \in M_n(R)$ such that

$$\phi(m_i) = \sum_j a_{ij} m_j.$$

Letting $\mathbf{m}$ be the column vector with entries m_i, we now get the equation

$$(t1_M - A)\mathbf{m} = 0.$$

Multiplying on the left by the matrix of minors of $tI - A$, we get

$$\big(\det(t1_M - A)\big) I\mathbf{m} = 0$$

This implies that $\det(tI - A)m_i = 0$, for all i, and so we see that $\det(tI - A) = 0 \in \mathrm{End}_R(M)$. This gives us the result. □

Here's a clever, but immediate corollary that will be useful in the future.

ear-selfsurj-isomorphism

COROLLARY 4.1.2. (1) *Let $\varphi : M \to M$ be a surjective endomorphism of a finitely generated R-module M. Then φ is in fact an isomorphism.*

(2) *Let F be a free R-module of rank n. Then, any generating set for F consisting of exactly n elements is a basis.*

PROOF. (1) Treat M as an $R[t]$-module by setting $tm = \varphi(m)$, for all $m \in M$, and let $I = (t)$. Then, since φ is surjective, we find that $IM = M$. So now, by the Theorem, 1_M satisfies some polynomial identity over $R[t]$ of the form

$$1_M + a_{n-1}1_M + \ldots + a_0 1_M = 0,$$

where $a_i \in (t^i)$, for all i. This tells us that we can find a polynomial $p(t) \in R[t]$ such that $1_M = \varphi p(\varphi)$, which shows that φ is invertible.

(2) Let $s_1, \ldots, s_n \in F$ be generators of F over R. Define a map $\psi : F \to F$ that maps a basis of F to the s_i. This is surjective by hypothesis, and hence is an isomorphism by part (1). So $s_1, \ldots, s_n$ do indeed form a basis for F.

□

iear-monic-free

COROLLARY 4.1.3. *Let $J \subset R[t]$ be an ideal, and let $S = R/J$.*

(1) *S is finitely generated over R by d elements if and only if J contains a monic polynomial of degree d. In fact, if J contains a monic polynomial of degree d, then S is generated by the images of t^r, for $0 \leq r < d$.*
(2) *S is free of rank d over R if and only if J is generated by a monic polynomial of degree d. In fact, if J is generated by a monic polynomial of degree d, then the images of $1, t, \ldots, t^{d-1}$ in S form a basis over R.*

PROOF. (1) If J contains a monic polynomial $p(t) = t^d + q(t)$, with $\deg q < d$, then the image of t^r in S, for $r \geq n$, can be expressed as a linear combination of the images of $1, t, \ldots, t^{d-1}$. Conversely, if S is finitely generated by d elements, then, by the Cayley-Hamilton theorem, applied in the case where ϕ is multiplication by t, there is a monic polynomial $p(x) \in R[x]$ of degree d such that $p(t)$ acts as 0 on S: this is equivalent to saying that $p(t) \in J$.

(2) First suppose $J = (p(t))$ is generated by a monic polynomial $p(t)$ of degree d, and let β be the image of t in S. We want to show that $1, \beta, \ldots, \beta^{d-1}$ form a basis for S. So suppose $\sum_{i=1}^{d-1} a_i \beta^i$ is a relation over R; this implies that $q(t) = \sum_{i=1}^{d-1} a_i t^i \in J$. But $\deg q < \deg p$, which, since J is generated by $p(t)$, and $p(t)$ is monic, implies that $q = 0$.

Conversely, suppose S is a free R-module of rank d; then by part (1) there is a monic polynomial $p(t) \in J$ of degree d, and S is generated over R by $1, \beta, \ldots, \beta^{d-1}$. By part (2) of (4.1.2), this means that $\{1, \beta, \ldots, \beta^{d-1}\}$ is in fact a basis for S over R. Now, let $f \in J$ be any element, and let q be such that $\deg q < \deg p$ and $f \equiv q \pmod{p(t)}$. Then $q \in J$ will give a relation between β^i, for $0 \leq i < d$ in S, which shows that $q = 0$, and so $f \in (p(t))$.

□

2. Integrality

DEFINITION 4.2.1. Let $R \subset S$ be a tower of rings. Then, an element $s \in S$ is *integral* over R, if there is a monic polynomial $p(t) \in R[t]$ such that $p(s) = 0$.

S is *integral* over R if every element of S is integral over R.

iear-equiv-integral

PROPOSITION 4.2.2. *Let $R \subset S$ be a tower of rings, and let $s \in S$. Then the following statements are equivalent:*

(1) *s is integral over R.*
(2) *$R[s]$ is a finitely generated R-module.*
(3) *$R[s]$ is contained in a subring $T \subset S$ with T a finitely generated R-module.*
(4) *There is a faithful $R[s]$-module M that's finitely generated as an R-module.*

PROOF. (1) ⇒ (2): There is a monic polynomial $p(t) \in R[t]$ of degree r such that $p(s) = 0$. Now the result follows from part (1) of (4.1.3).

(2) ⇒ (3): Take $T = R[s]$.

(3) ⇒ (4): Take $M = T$.

(4) ⇒ (1): Note that $sM \subset M$. Now apply Cayley-Hamilton to see that s satisfies a monic polynomial over R. We need faithfulness, because we want the map $R[s] \to \mathrm{End}_R(M)$ to be injective. □

This has a number of corollaries.

r-fingen-integral-finite

COROLLARY 4.2.3. *Let R, S be as above, and let $s_1, \ldots, s_n \in S$ be integral elements over R. Then $R[s_1, \ldots, s_n]$ is a finitely generated R-module.*

PROOF. Follows by induction on n, using (2) of the Proposition. □

integral-elts-subalgebra

COROLLARY 4.2.4. *Let R, S be as in the Proposition. Then the set of R-integral elements in S is a subalgebra of S. In particular, if S is generated as an R-algebra by R-integral elements, then S is integral over R.*

PROOF. Let $s_1, s_2 \in S$ be integral elements over R. Consider $R[s_1, s_2] \subset S$: this is a finitely generated R-module by the last Corollary. Moreover, it contains $R[s_1 s_2]$, $R[r_1 s_1 + r_2 s_2]$, for any $r_i \in R$. So, by part (3) of the Proposition, we see that both $s_1 s_2$ and $r_1 s_1 + r_2 s_2$ are integral over R. This proves the first statement. The second follows immediately. □

REMARK 4.2.5. Corollary (4.2.3) shows that any finitely generated R-algebra that's also integral over R is a finitely generated R-module.

ar-integral-transitivity

COROLLARY 4.2.6. *Let $R \subset S \subset T$ be a tower of rings, with S integral over R and T integral over S. Then T is integral over S.*

PROOF. Let $t \in T$ satisfy a monic equation

$$t^n + s_{n-1} t^{n-1} + \ldots + s_0 = 0,$$

over S. Then $R[s_0, \ldots, s_{n-1}, t] = T'$ is integral over $S' = R[s_0, \ldots, s_{n-1}]$, and is thus a finitely generated S'-module. But S' is a finitely generated R-module. Hence $R[t]$ is contained in T', which is a subring of T that's a finitely generated R-module. So, we see by the Proposition that t is integral over T. □

iear-loc-normality

PROPOSITION 4.2.7. *Let $R \subset S$ be a tower of rings with S integral over R. Let $I \subset S$ be an ideal, and let $J = I \cap R$. Let $U \subset R$ be a multiplicative set.*

1. *S/I is integral over R/J.*
2. *$U^{-1}S$ is integral over $U^{-1}R$.*

PROOF. Both statements are easy. For the second, note that if $s/u \in U^{-1}S$, and s satisfies the monic equation

$$s^n + a_{n-1} s^{n-1} + \ldots + a_0 = 0$$

over R, then s/u satisfies the monic equation

$$(s/u)^n + (a_{n-1}/u)(s/u)^{n-1} + \ldots + a_0/u^n = 0$$

over $U^{-1}R$. □

3. Integral Closure and Normality

3.1. Reduced Rings.

DEFINITION 4.3.1. We will say that a ring R is of *dimension* 0 if every maximal ideal of R is also minimal.

Reduced rings of dimension 0 are easy to describe.

r-reduced-local-dim-zero

LEMMA 4.3.2. *The only reduced local rings of dimension* 0 *are fields.*

PROOF. Clearly, every field is a reduced local ring of dimension 0. So suppose R is a local ring of dimension 0 with maximal ideal $\mathfrak{m}$. Observe that $\mathfrak{m}$ is also minimal, and hence $\operatorname{Nil} R = \mathfrak{m}$. So, if R is reduced, then $\mathfrak{m} = 0$, and so R is a field. □

iear-reduced-dim-zero

PROPOSITION 4.3.3. *Every reduced ring of dimension* 0 *is a product of fields.*

PROOF. Follows from the lemma above, and the fact that any artinian ring is isomorphic to a direct product of its localizations. □

We now give a characterization of reduced rings.

ar-reducedness-criterion

PROPOSITION 4.3.4. *A Noetherian ring R is reduced iff it satisfies the following conditions:*

R_0**:** *The localization of R at every height* 0 *prime is a field*
S_1**:** *All the associated primes of R are minimal.*

PROOF. First suppose that R is reduced. Then, so is every localization of R. In particular, every localization of R at a minimal prime is a reduced local ring of dimension 0. So, by Lemma (4.3.2), we see that R satisfies condition R_0. Moreover, since $\operatorname{Nil} R = 0$, we see that 0 is an intersection of minimal primes. Hence, by primary decomposition, all the associated primes of R are minimal.

Conversely, suppose R satisfies condition R_0. Then, $\operatorname{Nil} R_P = 0$, for every minimal prime $P \subset R$. If R also satisfies S_1, then the associated primes are all minimal, and so $(\operatorname{Nil} R)_P = \operatorname{Nil} R_P = 0$, for all primes $P \in \operatorname{Ass} R$. So $\operatorname{Nil} R = 0$, and R is reduced. □

iear-loc-of-tqr-reduced

PROPOSITION 4.3.5. *If R is reduced, and $P \in \operatorname{Spec} R$, then*

$$K(R_P) \cong K(R)_P$$

Recall that $K(R)$ is the total quotient ring of R.

PROOF. If R is reduced, then all its associated primes are minimal, by Proposition (4.3.4). Since all the primes in $K(R)$ are the primes contained in the associated primes of R, we see that all the primes in $K(R)$ are minimal. Thus, $K(R)$ is a reduced ring of dimension 0, and so, by Proposition (4.3.3), it is a product of fields. To be more specific, it's isomorphic to $\prod_{Q \in \operatorname{Ass} R} K(R)_Q$. Now, observe that since R_Q is a field, and $K(R)_Q$ is a localization of R_Q, $K(R)_Q \cong R_Q$. Moreover, if $Q \nsubseteq P$, for some prime $P \subset R$, then $(R_Q)_P = 0$. We can see this by observing that, since $Q_Q = 0$,

$$(R_Q)_P \cong (R_Q/Q_Q)_P \cong (R_P/Q_P)_Q = 0.$$

The last inequality follows from the fact that $Q \nsubseteq P$, and so $Q_P = R_P$.

So

$$K(R)_P \cong \prod_{\substack{Q \in \operatorname{Ass} R \\ Q \subset P}} R_Q \cong \prod_{Q \in \operatorname{Ass} R_P} R_Q.$$

Similarly, we have

$$K(R_P) \cong \prod_{Q \in \operatorname{Ass} R_P} R_Q \cong K(R)_P.$$

□

We found a good description of $K(R)$ in the proof. Let's record it here.

r-tqr-reduced-prodstruct

COROLLARY 4.3.6. *If R is a reduced ring, then*

$$K(R) = \prod_{\text{ht } Q=0} (R/Q)_Q$$

PROOF. Just observe that R_Q is a field, and hence $Q_Q = 0$. □

Now, we present a useful criterion for checking when an element of $K(R)$ is actually in R. Suppose R is reduced, and assume that we have $x = \frac{a}{u} \in K(R)$, and $x \notin R$. Then, this means that $a \notin (u)$. In other words, $a \neq 0$ in the ring $R/(u)$. This means that there is a $P \in \operatorname{Ass} R/(u)$, such that $a \neq 0$ in $R_P/(u)_P$; which means that the image of x in $K(R_P) = K(R)_P$ is not in R_P. This gives us the following proposition.

iear-elt-in-R-criterion

PROPOSITION 4.3.7. *Suppose R is reduced. Then, an element $x \in K(R)$ is in R iff the image of x in $K(R)_P$ lies in R_P for every prime P associated to a non zero divisor of R.*

PROOF. Done above. □

3.2. Normality.

DEFINITION 4.3.8. If $R \subset S$ is a tower of rings, then the *integral closure* $T \subset S$ of R is the subalgebra of S that consists of the elements of S that are integral over R.

If $R = T$, then R is *integrally closed* in S.

egral-closure-int-closed

PROPOSITION 4.3.9. *Let R, S, T be as in the definition above. Then T is integrally closed in S.*

PROOF. Suppose $s \in S$ is integral over T; then by (4.2.6), it's also integral over R and is hence in T. □

iear-defn-normal

DEFINITION 4.3.10. A ring R is *normal* if it is reduced and is integrally closed in its total quotient ring $K(R)$.

The following Proposition gives us a ready bank of normal domains.

iear-ufd-normal

PROPOSITION 4.3.11. *Every UFD is normal.*

PROOF. Let R be a UFD, and let $r/s \in K(R)$ be integral over R satisfying a monic equation

$$(r/s)^n + a_{n-1}(r/s)^{n-1} + \ldots + a_0 = 0.$$

We can assume that r/s is reduced so that r and s are relatively prime. Now, multiply the equation above by s^n to get

$$r^n + a_{n-1} s r^{n-1} + \ldots + a_0 s^n = 0,$$

which implies that $r \in (s)$, contradicting the fact that r and s are relatively prime. □

-normality-loc-preserved

PROPOSITION 4.3.12. *Let R, S, T be as in the definition above, and let $U \subset R$ be a multiplicative set. Then $U^{-1}T$ is the integral closure of $U^{-1}R$ in $U^{-1}T$.*

PROOF. We know by (4.2.7) that $U^{-1}T$ is integral over $U^{-1}R$. Now, suppose $s/u \in U^{-1}S$ is integral over $U^{-1}R$. Then it satisfies a monic equation

$$s^n + (a_{n-1}/u_{n-1})s^{n-1} + \ldots + a_0/u_0 = 0$$

over $U^{-1}R$.

Multiply this by $(\prod_i u_i)^n$ to see that $(\prod_i u_i)s$ is integral over R, and hence is in T. □

ear-normal-loc-criterion

PROPOSITION 4.3.13. *A reduced ring R is normal if and only if R_P is normal for every prime $P \subset R$.*

PROOF. Let S be the integral closure of R in $K(R)$, and consider the inclusion map $R \hookrightarrow S$. R is normal if and only if this is an isomorphism. Observe that R is reduced; we see by (4.3.5), that $K(R_P) = K(R)_P$, and so S_P is the integral closure of R_P in $K(R_P)$ by (4.3.12). Hence, we see that R is normal if and only if $R \hookrightarrow S$ is an isomorphism if and only if $R_P \hookrightarrow S_P$ is an isomorphism for every prime $P \subset R$ if and only if R_P is normal for every prime $P \subset R$. □

More generally, given a tower of rings $R \subset S$, and an ideal $I \subset R$, we can consider the set of all elements in S that are integral over I, in the sense that they satisfy a monic equation with coefficients in I. We'll call this the *integral closure* of I in S.

iear-int-closure-ideal

PROPOSITION 4.3.14. *Let R, S, I be as in the above paragraph. Then, the integral closure of I in S is the ideal* $\mathrm{rad}(IS)$. *In particular, it's closed under addition and multiplication.*

PROOF. Let $s \in S$ be an element integral over I. Then, it satisfies an equation

$$s^n + a_{n-1}s^{n-1} + \ldots + a_0 = 0,$$

with $a_i \in I$. So we see that $s^n \in IS$, and so $s \in \mathrm{rad}(IS)$.

Conversely, suppose $s \in \mathrm{rad}(IS)$. Then, $s^n = \sum_{i=1}^r a_i s_i$, for some $a_i \in I$ and $s_i \in S$. In that case, $s^n S' \subset IS'$, where $S' = R[s_1, \ldots, s_r]$. Since S' is a finitely generated R-module, we see by Cayley-Hamilton, that s^n satisfies a monic equation with coefficients in I, which of course implies that s also does. □

The next result is useful in number theory.

mal-polynomial-over-ring

COROLLARY 4.3.15. *Suppose $R \subset S$ is an integral extension, with R, S domains and R normal. Then, if $x \in S$ is integral over an ideal $I \subset R$, its minimal polynomial over $K(R)$ has all its coefficients in* $\mathrm{rad}(I)$.

PROOF. Let $x_1, \ldots, x_n$ be the conjugates of x in $K(S)$; then each of them satisfies the same monic polynomial with coefficients in I that x also satisfies, and hence each of them lies in $\mathrm{rad}(I)$, by (4.3.14). But the coefficients of the minimal polynomial are polynomials in the x_i, and so they also lie in $\mathrm{rad}(I)$. □

ynomial-integral-closure

PROPOSITION 4.3.16. *Suppose $R \subset S$ is integrally closed in S. Then $R[x] \subset S[x]$ is integrally closed in $S[x]$.*

PROOF. Let $f(x) = \sum_i a_i x^i \in S[x]$ be an element integral over $R[x]$ satisfying some monic equation

$$f^n + p_1 f^{n-1} + \ldots + p_n = 0,$$

over $R[x]$. Let $R' \subset R$ be the subring generated by the coefficients of each of the p_i. So R' is finitely generated and hence Noetherian. Now, $M = R'[x][f] \subset S[x]$ is a finitely generated $R'[x]$-module, since f is integral over $R'[x]$. So if $I \subset S$ is the ideal generated by the coefficients of all the elements of M, then I is generated over R' by the coefficients of the generators of M over $R'[x]$, and is thus finitely generated. Let a_n be the leading coefficient of f; then $R'[a_n] \subset I$, and so is again finitely generated over R'. This implies that a_n is integral over R' (since R' is Noetherian), and so $a_n \in R$. But then $a_n x^n$ is integral over $R[x]$, and, using induction on the degree of f, we find that $f \in R[x]$. □

l-normal-iff-ring-normal

COROLLARY 4.3.17. *A domain R is normal if and only if $R[x]$ is normal.*

PROOF. First observe that $K(R)[x]$ is factorial, and hence normal. So $R[x]$ is normal if and only if it's integrally closed in $K(R)[x]$. This implies that if R is normal, then so is $R[x]$, using the Proposition above. Conversely, if $R[x]$ is integrally closed in $K(R)[x]$, and $a \in K(R)$ is integral over R, then it's also integral over $R[x]$, and hence lies in $R[x]$. But then it's in fact in R, and so R is also normal. □

3.3. Normality in the Noetherian Case.

rmal-loc-noeth-criterion

LEMMA 4.3.18. *A reduced Noetherian ring R is normal if and only if R_P is normal for every prime $P \subset R$ associated to a non zero divisor.*

PROOF. It's easy to see that any localization of a normal ring is normal. See (4.2.7).

Suppose now that $x \in K(R)$ is integral over R. Then its image in $K(R_P)$ is integral over R_P, for every prime P. Now, Proposition (4.3.7) tells us that $x \notin R$ if and only if $x \notin R_P$, for some prime P associated to a non zero divisor. So if R is not normal, then R_P is also not normal, for some P associated to a non zero divisor. □

Now we give a criterion for a domain to be normal.

iear-normality-criterion

PROPOSITION 4.3.19. *A Noetherian domain R is normal if and only if, for every prime P associated to a principal ideal, P_P is principal.*

PROOF. Suppose first that R is normal, and $a \in R - 0$. Let P be a prime associated to a. We want to show that P_P is principal. Now, there is a $b \in R \setminus (a)$ such that $bP \subset (a)$. We localize at P to find that $bP_P \subset (a)_P$. We set

$$P_P^{-1} = (R_P :_{K(R_P)} P_P) \subset K(R_P).$$

Observe now, that since $bP_P \subset (a)_P$, we have $b/a \in P_P^{-1}$. By hypothesis $b \notin (a)$, which implies that $b/a \notin R_P$, and hence $P_P^{-1} \nsubseteq R_P$. Moreover, we have $P_P \subset P_P^{-1} P_P \subset R_P$. Since P_P is maximal, this means that either $P_P^{-1} P_P = P_P$ or $P_P^{-1} P_P = R_P$. If the former is true, then we find, by a version of Nakayama, that P_P^{-1} is integral over R_P. But R_P is normal, and so $P_P^{-1} \subset R_P$, which contradicts what we showed at the beginning of the paragraph. So we must have $P_P^{-1} P_P = R_P$. If $cP_P \subset P_P$, for all $c \in P_P^{-1}$, then, by the locality of R_P, we see that $P_P^{-1} P_P \subset P_P$. Therefore, there is some $c \in P_P^{-1}$ such that $cP_P = R_P$, which means that $P_P = c^{-1} R_P \cong R_P$ is principal.

Conversely, suppose for every prime P associated to a principal ideal, P_P is principal. Then, the localization R_P is a local domain whose maximal ideal is

principal. So R_P is a DVR and is thus normal. Observe now, that by Proposition (4.3.7), $R = \cap_P R_P$, where the intersection is taken over all primes associated to a principal ideal. Since R_P is integrally closed in $K(R_P)$, and $K(R_P) = K(R)$, for all primes $P \subset R$, we see that R must also be integrally closed in $K(R)$. □

Here's an easy characterization of normal rings.

-normal-characterization

PROPOSITION 4.3.20. *Every Noetherian normal ring is a product of normal domains.*

PROOF. Let R be a Noetherian normal ring. Then, in particular, R is reduced. So by Corollary (4.3.6), we see that

$$K(R) \cong \prod_i (R/Q_i)_{Q_i},$$

where $\operatorname{ht} Q_i = 0$, for all i.

Let e_i be the unit in $K_i = (R/Q_i)_{Q_i}$. Then, e_i is idempotent in $K(R)$, and so satisfies the monic equation $x^2 - x = 0$ over R. But R is integrally closed in $K(R)$, and so $e_i \in R$. Moreover, we see that for $i \neq j$, $e_i e_j = 0$, and that $\sum_i e_i = 1$. Hence, we have that $R \cong \prod_i Re_i$, with $K(Re_i) = K_i$. Since R is integrally closed in $K(R)$, we see that Re_i must be integrally closed in K_i, and is thus a normal domain (it's a sub-ring of a field). □

3.4. Integral Closure in the Graded Case. Now, we consider the graded case.

gral-components-integral

LEMMA 4.3.21. *Let $A \subset B$ be an inclusion of graded rings, with A Noetherian. If $s \in B$ is integral over A, then every homogeneous component of s is integral over A.*

PROOF. Observe that $T = A[s]$ is a subring of S that is finitely generated as an A-module. Now, let $N \subset T$ be the graded A-submodule generated by the highest degree components of the elements of T, and let s' be the highest degree component of s. Suppose $t \in N$ is of the form $\sum_i a_i t_i$, where each $a_i \in A$ and each t_i is the highest degree component of some element $b_i \in T$; then, for each i, $s't_i$ is the highest degree component of $s'b_i$, which implies that $s't$ is also in N. Thus, we find that $s'N \subset N$. To show that s' is integral over s, it suffices to show that N is a finitely generated A-module.

Choose finitely many generators $b_1, \ldots, b_r$ for T as an A-module, and let $M \subset T$ be the graded A-submodule generated by the homogeneous components of the b_i. Pick $b \in T$ and express it as a sum of the form $\sum_i a_i b_i$, where $a_i \in A$, for all i. Then it's immediate that the highest degree term of b is an A-linear combination of some homogeneous components of the b_i, and hence lies in N. This shows that $N \subset M$, and since A is Noetherian, and M is finitely generated, N must also be finitely generated over A.

Now, subtract s' from s and proceed inductively. □

-integral-closure-graded

PROPOSITION 4.3.22. *The integral closure S' of any graded domain S in its quotient field has a natural grading so that the inclusion $S \subset S'$ is a map of graded rings.*

PROOF. Let L be the ring of fractions of S obtained by inverting all homogeneous, non-zero elements of S. Then S' satisfies the hypotheses of part (3) of

Proposition (1.2.5) and is thus either a field or of the form $k[t, t^{-1}]$, for some field k. First suppose L is a field; then every element in S must have been homogeneous to begin with, which means that S is trivially graded. In this case, the inclusion of S in any ring is always a map of graded rings.

Suppose now that $L = k[t, t^{-1}]$: then L is normal. To see this, just observe that it is a UFD. Hence $S' \subset L$, and we will be done now if we show that the integral closure of every graded ring in a graded extension is a homogeneous subring of he extension. So let A and B be graded rings with a graded inclusion $A \subset B$. Suppose $s \in B$ is an element integral over A, and let $p(t) \in A[t]$ be a monic polynomial such that $p(s) = 0$. We want to show that each homogeneous component of s is integral over A. Let $A' \subset A$ be the graded subring generated by the homogeneous components of the coefficients of $p(t)$; then A' is Noetherian. It is enough to show that every component of s is integral over A'. This reduces us to the case of the Lemma, and so our proof is done. □

3.5. Finiteness of Integral Closure. We'll prove here that the integral closure of a normal domain R in a finite, separable extension of its quotient field is finite over R. Later, in Chapter 8, we'll see that the integral closure of any affine domain in any finite extension is finitely generated as a module over the domain. Also, in Chapter 7, we'll see that the integral closure of any Noetherian domain of dimension 1 is again Noetherian of dimension 1.

ness-of-integral-closure

THEOREM 4.3.23. *Let R be a normal domain, and let $L/K(R)$ be a finite separable extension of its function field. Let $R' \subset L$ be the integral closure of R in L. Then R' is contained in a finitely generated R-submodule of L. In particular, if R is Noetherian, then R' is finite over R.*

PROOF. The second assertion follows immediately from the first. Since L is separable, we can replace it by its Galois closure, and assume $L/K(R)$ is a Galois extension. Now, consider the trace form $\mathrm{tr}_{L/K(R)} : L \times L \to K(R)$: this is a non-degenerate bilinear form on L since $L/K(R)$ is separated. We can find a basis $\{b_1, \ldots, b_n\} \subset R'$ for L over $K(R)$. Let $\{b_1^*, \ldots, b_n^*\}$ be its dual basis under the trace form. Then, for $a \in R'$, we have $a = \sum_i a_i b_i^*$, for some $a_i \in K(R)$. But observe now that

$$\mathrm{tr}_{L/K(R)}(ae_j) = \sum_i \mathrm{tr}_{L/K(R)}(a_i \delta_{ij}) = a_i \in R.$$

Hence it follows that $R' \subset \sum_i Re_i^*$. □

4. Lying Over and Going Up

iear-secn-going-up

-iff-integral-extn-field

PROPOSITION 4.4.1. *Let $R \subset S$ be an integral extension. Then R is a field if and only if S is a field.*

PROOF. First suppose R is a field; then every element $s \in S$ is algebraic over R, and thus has an inverse in $R[s]$.

Now, suppose S is a field, and suppose $s \in S$ is the inverse of an element $r \in R$. Then, s satisfies a monic equation

$$s^n + a_{n-1}s^{n-1} + \ldots + a_0 = 0.$$

Multiplying this by r^{n-1}, we find that

$$s = -(a_{n-1} + a_{n-2}r + \ldots + a_0 r^{n-1}) \in R.$$

□

ear-contract-max-iff-max

COROLLARY 4.4.2. *Let $f : R \to S$ be an integral map; then an ideal $\mathfrak{q} \subset S$ is maximal if and only if $\mathfrak{p} = f^{-1}(\mathfrak{q}) \subset R$ is maximal.*

PROOF. This is equivalent to the statement that $S/\mathfrak{q}$ is a field if and only if $R/\mathfrak{p}$ is one, which follows immediately from the Proposition above. □

iear-defn-going-up

DEFINITION 4.4.3. We say that a map of rings $f : R \to S$ has the *going up property* when the following condition holds:

Given primes $\mathfrak{q} \subset S$ and $\mathfrak{p} \subset R$ such that $\mathfrak{q}^c = \mathfrak{p}$, and another prime $\mathfrak{p}^* \supsetneq \mathfrak{p}$, there is a prime $\mathfrak{q}^* \supset \mathfrak{q}$ such that $(\mathfrak{q}^*)^c = \mathfrak{p}^*$. In other words, the map $\operatorname{Spec} S/\mathfrak{q} \to \operatorname{Spec} R/\mathfrak{p}$ is surjective.

It has the *lying over* property if the map $\operatorname{Spec} S \to \operatorname{Spec} R/\ker f$ is surjective.

DEFINITION 4.4.4. We say that a map $f : R \to S$ of rings is *integral* if S is an integral extension of $f(R)$.

iear-extn-going-up

PROPOSITION 4.4.5. *Let $f : R \to S$ be an integral map. Then it has the lying over and going up properties.*

PROOF. We need to show that the map $\operatorname{Spec} S \to \operatorname{Spec} R/\ker f$ is surjective, and that the maps $\operatorname{Spec} S/\mathfrak{q} \to \operatorname{Spec} R/\mathfrak{p}$ are surjective for primes $\mathfrak{p} \subset R$, $\mathfrak{q} \subset S$, with $\mathfrak{q}^c = \mathfrak{p}$. Replacing R with $R/\ker f$, we can assume that we have an integral extension $R \subset S$. Since, by (4.2.7), $R/\mathfrak{p} \subset S/\mathfrak{q}$ is also an integral extension, it suffices to show that $\operatorname{Spec} S \to \operatorname{Spec} R$ is surjective. So suppose $\mathfrak{p} \in \operatorname{Spec} R$, and consider the integral extension $R_\mathfrak{p} \subset S_\mathfrak{p}$. Let $\mathfrak{m} \subset S_\mathfrak{p}$ be any maximal ideal. Then we have another integral extension

$$R_\mathfrak{p}/(\mathfrak{m} \cap R) \subset S_\mathfrak{p}/\mathfrak{m},$$

with $S_\mathfrak{p}/\mathfrak{m}$ a field. So, by the last Proposition, we see that $R_\mathfrak{p}/(\mathfrak{m} \cap R)$ is also a field, which implies that $\mathfrak{m} \cap R = \mathfrak{p}$, and so the map $\operatorname{Spec} S \to \operatorname{Spec} R$ is indeed surjective. □

iear-defn-incomp

DEFINITION 4.4.6. We say that two primes $\mathfrak{p}_1, \mathfrak{p}_2 \subset R$ are *incomparable* if they are incomparable in the prime lattice of R.

A map of rings $f : R \to S$ has the *incomparability property* if, given a prime $\mathfrak{p} \subset R$, and two distinct primes $\mathfrak{q}_1, \mathfrak{q}_2 \subset S$ such that $\mathfrak{q}_i^c = \mathfrak{p}$, for $i = 1, 2$, $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are incomparable. In other words, if all the primes in $S \otimes k(\mathfrak{p})$ are maximal.

Integral extensions also satisfy the incomparability property.

iear-extn-incomp

PROPOSITION 4.4.7. *Let $f : R \to S$ be an integral map. Then it has the incomparability property.*

PROOF. As always, replacing R with its image, we can assume $R \subset S$ is an integral extension. Let $\mathfrak{p} \subset R$ be a prime. Now, for any prime $\mathfrak{q} \subset S$ contracting to $\mathfrak{p}$, we see that we have an integral extension $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \subset S_\mathfrak{p}/\mathfrak{q}_\mathfrak{p}$. Since $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$ is a field, we see that $\mathfrak{q}_\mathfrak{p} \subset S_\mathfrak{p}$ must also be maximal. In particular, this implies that all the primes in $S \otimes k(\mathfrak{p})$ are maximal, thus showing that f has the incomparability property. □

5. Finite Group Actions

In this section, we present a few generalities on finite group actions on rings that will prove useful in the number theoretic context.

DEFINITION 4.5.1. Let R be a ring, and let G be a finite subgroup of $\mathrm{Aut}(R)$. The *norm* $N_G(a)$ of an element $a \in R$ is the product $\prod_{\sigma \in G} \sigma(a)$. Evidently, $N_G(a)$ lives in R^G, the sub-ring of G-invariant elements.

-finite-group-transitive

PROPOSITION 4.5.2. *Let R be a ring, G a finite subgroup of $\mathrm{Aut}(R)$, and $R^G \subset R$ the fixed sub-ring of G.*

1. *R is integral over R^G.*
2. *If $P \subset R^G$ is any prime, then G acts transitively on the set of primes in R contracting to P.*

PROOF. (1) Let $x \in R$, and consider the polynomial

$$p(t) = \prod_{\sigma \in G} (t - \sigma(x)).$$

This is a monic polynomial that vanishes at x; moreover, it's also invariant under the action of G, and hence is a polynomial over R^G. This shows that x is integral over R^G.

(2) Let $Q_1, Q_2 \subset R$ be primes contracting to P, and pick $x \in Q_1$. Consider the norm $N_G(x)$: this lies in $Q_1 \cap R^G = P$, and hence also in Q_2. This implies that $\sigma(x) \in Q_2$, for some $\sigma \in G$, and so we have

$$Q_1 \subset \bigcup_{\sigma \in G} \sigma(Q_2).$$

By prime avoidance, there exists $\sigma \in G$ such that $Q_1 \subset \sigma(Q_2)$. Now, by incomparability (4.4.7), we have $Q_1 = \sigma(Q_2)$.

□

DEFINITION 4.5.3. With the notation as in the above Proposition, the stabilizer of a prime $Q \subset R$ is called the *decomposition group* of Q.

The fixed sub-ring $R^{\mathrm{Dec}(Q)} \subset R$ of $\mathrm{Dec}(Q)$ is called the *decomposition ring* of Q.

REMARK 4.5.4. If $Q \cap R^G = Q' \cap R^G = P$, then the transitivity of the group action on the fiber over P tells us that $\mathrm{Dec}(Q)$ and $\mathrm{Dec}(Q')$ are conjugate subgroups of G.

Also observe that if $Q' = R^{\mathrm{Dec}(Q)} \cap Q$, then Q is the only prime in R lying over Q'. This again follows from the transitivity of the action of $\mathrm{Dec}(Q)$ on the fiber over Q'.

The next lemma basically says that flat base change preserves group invariants.

-action-flat-base-change

LEMMA 4.5.5. *Let R and A' be A-algebras, and suppose A' is flat over A. If G is a finite sub-group of $\mathrm{Aut}_A(R)$, then we have a natural isomorphism*

$$R^G \otimes_A A' \cong (R \otimes_A A')^G,$$

where the action of G is extended naturally to $R \otimes_A A'$, by letting it act trivially on A'.

PROOF. We have:

$$R^G = \mathrm{Hom}_{A[G]}(A, R),$$
$$(R \otimes_A A')^G = \mathrm{Hom}_{A[G]\otimes_A A'}(A \otimes_A A', R \otimes_A A'),$$

where $A[G]$ is the group ring of G over A, and A is given the natural $A[G]$-module structure via the augmentation map. The desired isomorphism is now immediate from (3.1.11). □

roup-action-localization

COROLLARY 4.5.6. *With the notation and hypotheses of (4.5.2), let $S \subset R^G$ be a multiplicative set. Then, under the natural action of G on $S^{-1}R$, we have $(S^{-1}R)^G = S^{-1}(R^G)$.*

PROOF. Take $A = R^G$ and $A' = S^{-1}(R^G)$ in the lemma above. □

ition-ring-residue-field

PROPOSITION 4.5.7. *With the notation and hypotheses of (4.5.2), let $Q \subset R$ be a prime lying over $P \subset R^G$, and let R^D be the decomposition ring of Q. If $Q' = Q \cap R^D$, then the natural inclusion $k(P) \hookrightarrow k(Q')$ is an isomorphism.*

PROOF. By (4.5.6), we have $(R^G)_P = (R_P)^G$. Note that $\mathrm{Dec}(Q)$ is unaffected by localization. Using (4.5.6) again, we see that $(R^D)_P = (R_P)^D$. Therefore, we can replace R with R_P and R^G with $(R^G)_P$, and assume that P is maximal. In this case, both Q and Q' are maximal, by (4.4.2) and (4.5.2).

So what we need to show is that $R/P \hookrightarrow R^D/Q'$ is surjective. That is, given $x \in R^D \setminus Q'$, we need to find $y \in R \setminus P$ such that $x - y \in Q'$.

For $\sigma \in G$, we set $Q'_\sigma = \sigma(Q) \cap R^D$; note that if $\sigma \notin \mathrm{Dec}(Q)$, then $Q'_\sigma \neq Q'$, since Q is the only prime in R contracting to Q'. Since $\{Q'_\sigma : \sigma \in G\}$ is a finite collection of maximal ideals in R^D, using the Chinese remainder theorem, we can find $z \in R^D$ such that $z - x \in Q'_1 = Q'$ and such that $z - 1 \in Q'_\sigma$, for $\sigma \notin \mathrm{Dec}(Q)$. In particular, $z \equiv x \pmod{Q}$, and $\sigma(z) \equiv 1 \pmod{Q}$, for all $\sigma \notin \mathrm{Dec}(Q)$.

Now consider $y = z\prod_{\sigma\notin \mathrm{Dec}(Q)} \sigma(z)$: this lies in R^G, and also satisfies the condition $y \equiv x \pmod{Q}$. But both y and x lie in R^D, and so we must have $x - y \in Q'$. This finishes our proof. □

Observe now that any element $\sigma \in \mathrm{Dec}(Q)$ induces a natural automorphism on R/Q over R^G/P, and hence on $k(P)$ over $k(Q)$. The next Proposition says that *all* automorphisms of $k(P)$ over $k(Q)$ are obtained in this fashion.

-surjection-automorphism

PROPOSITION 4.5.8. *We maintain the notation and hypotheses of the previous Proposition. The extension $k(Q)/k(P)$ is normal algebraic, and the natural map $\mathrm{Dec}(Q) \to \mathrm{Aut}_{k(P)}(k(Q))$ is surjective.*

PROOF. Just as in (4.5.7) we reduce to the case where P, and hence Q, is maximal. In this case, let $\overline{a} \in R/Q$ be an element, and let $a \in R$ be an element mapping to $\overline{a}$. Then a is a zero of the monic polynomial $\prod_{\sigma\in G}(t - \sigma(a))$ over R^G, and so $\overline{a}$ is a zero of the polynomial $\prod_{\sigma\in G} t - \overline{\sigma(a)}$ over $k(P)$. This polynomial splits completely in R/Q, and so we see that $k(Q)$ is normal over $k(P)$. That it's algebraic is of course an easy consequence of what we have shown.

For the second assertion, first observe that, by (4.5.7), we can replace R^G with R^P and P with $Q' = R^D \cap Q$, and assume that $G = \mathrm{Dec}(Q)$. Let $k^s/k(P)$ be the maximal separable sub-extension of $k(Q)/k(P)$; then we can find $\overline{a} \in k^s$ such that

$k^s = k(P)[\overline{a}]$. Now, an automorphism φ of $k(Q)$ over $k(P)$ is completely determined by where it sends $\overline{a}$. But any conjugate of $\overline{a}$ is of the form $\overline{\sigma(a)}$, for some $a \in R$ mapping to $\overline{a}$ and some $\sigma \in G$. Now we find that φ is the image of σ under the natural map from G to $\mathrm{Aut}_{k(P)}(k(Q))$. □

DEFINITION 4.5.9. The kernel of the natural surjection $\mathrm{Dec}(Q) \to \mathrm{Aut}_{k(P)}(k(Q))$ is called the *inertia group* of Q and will be denoted $I(Q)$. This consists of all elements in $\mathrm{Dec}(Q)$ that induce the trivial action on the quotient R/Q.

REMARK 4.5.10. If $k(Q)$ is separable over $k(P)$ (which happens, for example, when $k(P)$ is finite), then we get an exact sequence of groups:

$$1 \to I(Q) \to \mathrm{Dec}(Q) \to \mathrm{Gal}(k(Q)/k(P)) \to 1.$$

Thus $[\mathrm{Dec}(Q) : I(Q)] = [k(Q) : k(P)]$.

DEFINITION 4.5.11. Given an A-algebra ring R and a field K, a *K-valued point of R over A* is just a map of A-algebras $R \to K$. We denote the set of K-valued points of R over A by $R_A(K)$.

REMARK 4.5.12. If R has a left action by a group G, then that automatically induces a right action of G on $R_A(K)$ by the formula $(\varphi\sigma)(a) = \varphi(\sigma(a))$.

ansitive-k-valued-points

COROLLARY 4.5.13. *We keep the hypotheses of (4.5.2). For any field K equipped with a map $R^G \to K$, the action of G on $R_{R^G}(K)$ is transitive.*

PROOF. Given two maps $\varphi_1, \varphi_2 : R \to K$ that agree on R^G, we can replace φ_2 by a suitable translate and assume that $\ker \varphi_1 = \ker \varphi_2 = Q$. Now, $\mathrm{im}\, \varphi_1$ and $\mathrm{im}\, \varphi_2$ differ by an automorphism of R/Q over R^G/P, and thus by an automorphism of $k(Q)$ over $k(P)$. But by the Proposition above, D surjects onto $\mathrm{Aut}_{k(Q)}(k(P))$, and so we can find a $\sigma \in D$ such that $\varphi_1 = \varphi_2 \circ \sigma$. □

REMARK 4.5.14. Suppose that in the corollary above, we take $L = R$ to be a field; then L^G is the fixed field of G. Then we find that G acts transitively on $L_{L^G}(L)$. But this is the same as saying that G acts transitively on $\mathrm{Aut}_{L^G}(L)$, which is the same as saying that $G = \mathrm{Aut}_{L^G}(L)$. This leads to a quick proof that any field is always Galois over the fixed sub-field of any finite group of automorphisms.

6. Going Down for Normal Domains

This section is devoted to showing that integral extensions of normal domains have the going down property. See (3.6.7) for the definition. First we need a few auxiliary results, the last of which is a consequence of Galois theory.

ly-inseparable-bijective

LEMMA 4.6.1. *Let $R \subset S$ be a tower of domains, with $K(S)/K(R)$ a purely inseparable extension. Then, for every prime $P \subset R$, $\mathrm{rad}(PS)$ is again prime. In particular, contraction induces a bijective correspondence between the primes of S and the primes of R.*

PROOF. Let $a, b \in S$ be such that $ab \in \mathrm{rad}(PS)$; then we can find $n \in \mathbb{N}$ such that $(ab)^{p^n} \in P$, $a^{p^n}, b^{p^n} \in R$. Suppose $a \notin \mathrm{rad}(PS)$; then $a^{p^n} \notin P$, and so $b^{p^n} \in P$, implying that $b \in \mathrm{rad}(PS)$. □

normal-extn-transitivity

THEOREM 4.6.2. *Let R be a normal domain, $L/K(R)$ a normal extension, and S the integral closure of R in L. Then, for every prime $P \subset R$, $\mathrm{Aut}(L/K(R))$ acts transitively on the primes in S contracting to P.*

PROOF. By the lemma above, we can assume that $L/K(R)$ is separable, and hence Galois.Let $Q_1, Q_2 \subset S$ be two primes contracting to P. For every sub-extension $L'/K(R)$ of L, we set

$$F(L') = \{\sigma \in \mathrm{Gal}(L/K(R)) : \ \sigma(Q_1 \cap L') = Q_2 \cap L'\}.$$

For any sub-extension $L'/K(R)$, let $R_{L'}$ be the integral closure of R in L'. If $L'/K(R)$ is Galois, we have $R_{L'}^{\mathrm{Gal}(L'/K(R))} = R_{L'} \cap K(R)$, and since R is normal, we have $R_{L'}^{\mathrm{Gal}(L'/K(R))} = R$. So, if $L'/K(R)$ is a finite Galois extension, then, by (4.5.2), we find that $F(L') \neq \emptyset$. Moreover, observe that if $L^{(1)}/K(R)$ and $L^{(2)}/K(R)$ are two finite Galois sub-extensions, then so is their composite $L^{(1)}L^{(2)}/K(R)$. Moreover, we find that

$$\emptyset \neq F(L^{(1)}L^{(2)}) \subset F(L^{(1)}) \cap F(L^{(2)}).$$

We set

$$\mathscr{F} = \{F(L') \subset \mathrm{Gal}(L/K(R)) : \ L'/K(R) \text{ a finite Galois sub-extension of } L/K(R)\}.$$

We have shown above that $\mathscr{F}$ has the finite intersection property.

Now, equip $G = \mathrm{Gal}(L/K(R))$ with the Krull topology. We'll need two topological facts:

(1) G is compact in the Krull topology.
(2) For every finite Galois sub-extension $L'/K(R)$, $F(L')$ is closed in G.

Given these two properties, and the fact that $\mathscr{F}$ has the finite intersection property, we find that $\bigcap_{L' \in \mathscr{F}} F(L') \neq \emptyset$. So choose $\sigma \in \bigcap_{L' \in \mathscr{F}} F(L')$; it's now immediate that $\sigma(Q_1) = Q_2$. □

oing-down-normal-domains

COROLLARY 4.6.3. *Let $R \subset S$ be a tower of domains, with R normal and S integral over R. Then the inclusion $R \hookrightarrow S$ has the going down property.*

PROOF. Let L be the normal closure of $K(S)$, and let T be the integral closure of R in L (and hence also the integral closure of S in L). Let $\mathfrak{p}^* \subsetneq \mathfrak{p}$ be a chain of primes in R, let $\mathfrak{q} \subset S$ be a prime lying over $\mathfrak{p}$, and let $\widetilde{\mathfrak{q}} \subset T$ be a prime lying over $\mathfrak{q}$. By lying over and going up (4.4.5), there is a prime $\mathfrak{q}_1 \subset T$ lying over $\mathfrak{p}^*$ and another prime $\mathfrak{q}_2 \supset \mathfrak{q}_1$ lying over $\mathfrak{p}$. Since $L/K(R)$ is normal, the Theorem above gives us a $\sigma \in \mathrm{Aut}(L/K(R))$ such that $\sigma(\mathfrak{q}_2) = \widetilde{\mathfrak{q}}$. Let $\mathfrak{q}^* = \sigma(\mathfrak{q}_1) \cap S$; we see that $\mathfrak{q}^* \subset \mathfrak{q}$ and that $\mathfrak{q}^* \cap R = \mathfrak{q}_1 \cap R = \mathfrak{p}^*$. □

7. Valuation Rings and Extensions of Homomorphisms

DEFINITION 4.7.1. A domain R is a *valuation ring* if, for every $x \in K(R)$, either $x \in R$ or $x^{-1} \in R$.

luation-rings-basic-prps

PROPOSITION 4.7.2. *Let R be a valuation ring.*

(1) *The ordering $x \leq y$ if and only if $x \in (y)$ induces a total ordering on R.*
(2) *R is a local ring.*
(3) *R is normal.*
(4) *If $R \subset S \subset K(R)$ is a tower of rings, then S is also a valuation ring.*

PROOF. For (1), it suffices to show that every two elements of R are comparable. Suppose $x, y \in R$ are such that $x \notin (y)$; then $\frac{x}{y} \notin R$, and so $\frac{y}{x} \in R$, which implies $y \in (x)$.

Let $\mathfrak{m} \subset R$ be the set of all non-units. To show that R is local, it suffices to show that $\mathfrak{m}$ is closed under addition. So pick $x, y \in \mathfrak{m}$, and observe that either $xy^{-1} \in R$ or $x^{-1}y \in R$. Without loss of generality, assume $xy^{-1} \in R$. In this case, we see that $x + y = (1 + xy^{-1})y \in \mathfrak{m}$.

For normality, pick $z \in K(R)$, and assume that it satisfies some monic polynomial $p(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ over R. If $z \notin R$, then $z^{-1} \in R$, and we can write

$$z = -(a_{n-1} + a_{n-2}z^{-1} + \ldots + a_0 z^{-n+1}),$$

and hence $z \in R$.

Part (4) is obvious. □

CHAPTER 5

Completions and Hensel's Lemma

chap:comp

1. Basics

In this section, we fix a filtered ring $(R, F^\bullet R)$.

DEFINITION 5.1.1. Let $(M, F^\bullet M)$ be a filtered R-module; then we define the *completion* of M to be the filtered R-module

$$\hat{M}_F = \varprojlim_{n\in\mathbb{N}} (M/F^n M),$$

equipped with the natural map $\varepsilon_M : M \to \hat{M}_F$ given by the universal property of the inverse limit, and the filtration $F^\bullet \hat{M}_F$ given by

$$F^n \hat{M}_F = \varprojlim_{m\in\mathbb{N}} \left(F^n M/F^{n+m} M\right),$$

which makes ε_M a homomorphism of filtered R-modules.

A filtered R-module M is *complete* if ε_M is an isomorphism of filtered R-modules.

We denote by R-comp the full subcategory of R-filt that consists of complete R-modules.

REMARK 5.1.2. If the filtration $F^\bullet M$ is clear from context or is unambiguous we will suppress F and write the completion simply as $\hat{M}$.

REMARK 5.1.3. Note that, in the definition of the filtration on $\hat{M}$, we have used the fact that inverse limits preserve monomorphisms. In particular, $F^n\hat{M}$ is indeed an R-submodule of $\hat{M}$.

REMARK 5.1.4. It's also clear that ε_M is an injection if and only if M is separated; so, in particular, complete modules are separated.

mp-completion-reflection

PROPOSITION 5.1.5. *The assignment $M \mapsto \hat{M}_F$ is a functor from R-filt to R-comp that is a left adjoint to the forgetful functor from R-comp to R-filt. Equivalently, R-comp is a reflective subcategory of R-comp with the reflection given by the completion functor.*

PROOF. First we show that $\hat{M}$ is complete. We see immediately that we can write every element in $\hat{M}$ as the sum of an element in $F^n\hat{M}$, and another element which has 0 in its m^{th} co-ordinate, for all $m > n$. Hence, we find that $\hat{M}/F^n\hat{M} \cong M/F^n M$. From this, it follows at once that $\hat{M}$ is complete. It's clear that $M \mapsto \hat{M}$ is in fact a functor.

Now, suppose $\varphi : M \to N$ is a homomorphism of filtered R-modules, where N is complete. This induces, for every $n \in \mathbb{N}$, a map $\varphi_n : M/F^n M \to N/F^n N$, and hence a map $\widetilde{\varphi} : \hat{M} \to N$, since N is complete. By construction $\widetilde{\varphi}$ satisfies $\varphi = \widetilde{\varphi} \circ \varepsilon_M$. It's also easily checked that this factoring is uniquely determined. □

REMARK 5.1.6. In a similar vein, one may define the *separation* of M as being the module $M/\cap_{n\geq 0} F^n M$, which will give us a reflection into the subcategory of separated modules. But we won't need this.

comp-gr-completion

COROLLARY 5.1.7. *Let $(M, F^\bullet M)$ be a filtered R-module, and let $\hat{M}$ be its completion. Then we have*

$$\mathrm{gr}_F(\hat{M}) \cong \mathrm{gr}_F(M).$$

PROOF. Falls out immediately from the proof of the Proposition above. □

EXAMPLE 5.1.8. The p-adic integers $\hat{\mathbb{Z}}_p$ are obtained by completing $\mathbb{Z}$ equipped with the p-adic filtration (where, by abuse of notation, we are identifying the ideal (p) with the number p). The power series ring $R[[x_1, \ldots, x_n]]$ over any ring R is the completion of $R[x_1, \ldots, x_n]$ equipped with the $(x_1, \ldots, x_n)$-adic filtration.

DEFINITION 5.1.9. Let $(M, F^\bullet M)$ be a filtered R-module, and let $N \subset M$ be an R-submodule. The *closure* of N is the submodule

$$\overline{N} = \cap_{n\in\mathbb{N}} \left(N + F^n M\right).$$

If $N = \overline{N}$, then we say that N is *closed*. Observe that N being closed is equivalent to M/N being separated under the produced filtration.

omp-completion-exactness

PROPOSITION 5.1.10. *Let M be a filtered R-module, and let $N \subset M$ be an R-submodule. Let N be equipped with the induced filtration, and M/N with the produced filtration, so that the sequence*

$$0 \to N \to M \to M/N \to 0$$

is exact in R-filt.

1. *The map $\hat{N} \to \hat{M}$ is injective, and the filtration on $\hat{N}$ agrees with the induced filtration.*
2. *The sequence*
$$0 \to \hat{N} \to \hat{M} \to \widehat{M/N} \to 0$$
is also exact in R-comp. In particular, $\widehat{M/N} \cong \hat{M}/\hat{N}$, where $\hat{M}/\hat{N}$ is equipped with the produced filtration.
3. *$\hat{N} \cong \overline{\varepsilon_M(N)}$ is a closed submodule of M.*

PROOF. Before we begin, observe that we cannot just use the left adjointness of the completion functor to say that it is left exact, since the categories involved are not abelian. We will instead use the properties of left adjoints on a more basic level.

1. We use the fact that $N/F^n N$ includes into $M/F^n M$, for every n: indeed, $F^n N = N \cap F^n M$, by definition. Since inverse limits preserve monomorphisms, we're done. In particular, we find that $\hat{N}$ lives inside $\hat{M}$ as the set of coherent sequences that have as their co-ordinates images of elements in N. From this, the conclusion about the filtrations on $\hat{N}$ immediately follows.
2. Note that $\{N/F^n N\}$ is an inverse system satisfying the weak Mittag-Leffler condition ([CT, **??**]), and so $\lim^1 N/F^n N = 0$; this immediately gives us the statement.

(3) Now, observe that since $\hat{M}/\hat{N}$ is complete, and hence separated, $\hat{N}$ is a closed submodule of $\hat{M}$. So it suffices to show that $\hat{N} \subset \overline{\varphi_M(N)}$; or, equivalently, that $\hat{N} \subset \varphi_M(N) + F^n M$, for all $n \in \mathbb{N}$. So suppose $s \in \hat{N}$, and let $s_n \in N/(F^n M \cap N)$ be its n^{th} co-ordinate. Let $t \in N$ be any element which maps onto s_n. Then it's clear that $s - \varphi_M(t)$ belongs to $F^n M$.

□

Now, given a filtered R-module M, we have the natural maps

$$\alpha_M^n : R/F^n R \otimes_R M \to M/F^n M,$$

which is an isomorphism for all $n \in \mathbb{N}$, if the filtration on M is the natural filtration. This give us a natural map $\alpha_M : \hat{R} \otimes_R \to \hat{M}$ given by the composition

$$\hat{R} \otimes_R M \to \varprojlim (R/F^n R \otimes_R M) \xrightarrow{\lim \alpha_M^n} \hat{M}.$$

Let's see how this map looks in concrete terms. An element on the left hand side is a linear sum of elements of the form $s \otimes m$, where s is a coherent sequence and m is an element in M. Then, we send $s \otimes m$ to the coherent sequence with co-ordinates $s_n \otimes m$ under the first map, and then to the coherent sequence with co-ordinates $s_n m$ in $\hat{M}$.

It's easy to see that α_R is an isomorphism, which, since both completions and tensor products respect direct sums, implies that α_{R^n} is an isomorphism, for all $n \in \mathbb{N}$. We'll see in (5.3.3) that this is also an isomorphism for most modules we care about.

DEFINITION 5.1.11. Suppose $(M, F^\bullet M)$ and $(M, F'^\bullet M)$ are two filtered R-modules with the same underlying R-module M. We say that these two are *equivalent* if there exists $n_0 \in \mathbb{N}$ such that for all $r \geq n_0$, we can find $N(r), N'(r) \in \mathbb{N}$ such that $F^{N(r)} M \subset F'^r M$ and $F'^{N'(r)} M \subset F^r M$.

lent-completion-isomorph

PROPOSITION 5.1.12. *If $(M, F^\bullet M)$ and $(M, F'^\bullet M)$ are equivalent filtered R-modules, then $\hat{M}_F$ and $\hat{M}_{F'}$ are isomorphic as R-modules.*

PROOF. For $r \in \mathbb{N}$ large enough, let $k(r)$ be the maximal integer such that $F^r M \subset F'^{k(r)} M$. Set $\widetilde{F}^r M = F'^{k(r)} M$; we then have an exact sequence of inverse systems, which, at the r^{th} level, looks like:

$$0 \to \widetilde{F}^r M / F^r M \to M/F^r M \to M/\widetilde{F}^r M \to 0.$$

Now, since, for a given $r \geq 0$, we have $\widetilde{F}^s M \subset F^r M$, for all s large enough, we find that the image of $\widetilde{F}^s M/F^s M$ in $\widetilde{F}^r M/F^r M$ is 0, for all s large enough. From this it's immediate that $\{\widetilde{F}^r M/F^r M\}$ is an inverse system satisfying the Mittag-Leffler condition [CT, **??**], and also that $\lim \widetilde{F}^r M/F^r M$ is 0. So we have an isomorphism

$$\hat{M}_F \cong \varprojlim M/\widetilde{F}^r M.$$

By a similar argument, we also have

$$\varprojlim M/\widetilde{F}^r M \cong \hat{M}_{F'},$$

and so our proof is done. □

comp-stable-filtrations

COROLLARY 5.1.13. *Let $(M, F^\bullet M)$ be a stable filtered module over R, and let $F'^\bullet M$ be the natural filtration on M. Then $\hat{M}_F \cong \hat{M}_{F'}$.*

PROOF. By hypothesis, there exists $n_0 \in \mathbb{N}$ such that, for all $r \geq 0$, $F^{n_0+r}M = F^r R \cdot F^{n_0} M$. Therefore, for all $s \geq n_0$, we have $F^s M \subset F'^{s-n_0} M$. Since, by definition, $F'^s M \subset F^s M$, the Proposition now gives us the result. □

We finish this section with a few definitions.

DEFINITION 5.1.14. The *I-adic completion*of a ring R is the completion of the filtered ring (R, I); that is, of R equipped with the natural I-adic filtration.

We say that a ring R is *complete with respect to an ideal I* if (R, I) is complete.

A local ring $(R, \mathfrak{m})$ is *complete* if it is complete with respect to $\mathfrak{m}$.

REMARK 5.1.15. Let $\hat{R}$ be the I-adic completion of R; then we see from the definition that $F^n\hat{R}$ is simply $\hat{I^n}$, the I-adic completion of the ideal I^n. In particular, if $(R, \mathfrak{m})$ is a local ring, then $\hat{R}$ is again local, and its maximal ideal is $\hat{\mathfrak{m}}$.

DEFINITION 5.1.16. Let $(R, F^\bullet R)$ be a filtered ring; then the *ring of restricted power series* over R is the subring $R\{t\}$ of $R[[t]]$ given by:

$$R\{t\} = \{f = \sum_i f_i t^i \in R[[t]] : \text{ for all } n \in \mathbb{N}\text{ , there exists } r \in \mathbb{N} \text{ such that } f_m \in F^n M \text{ for } m \geq r\}$$

Observe that an element $f \in R[[t]]$ is in $R\{t\}$ if and only if, for every $n \in \mathbb{N}$, its image in $(R/F^n R)[[t]]$ is a polynomial. Now, equip the polynomial ring $R[t]$ with the natural filtration; then we see immediately that

$$\widehat{R[t]} = \varprojlim (R/F^n R)[t]$$

is the ring of restricted power series over R. This gives us the following result.

-restricted-power-series

PROPOSITION 5.1.17. *Let R be a complete ring; then the completion of $R[t]$, where this ring is equipped with the natural filtration as an R-module, is $R\{t\}$, the ring of restricted power series over R. In particular, $R\{t\}$ is again complete.*

2. Convergence and some Finiteness Results

Many of the notions we have encountered so far have their origins in topology (completion, closure, etc.), and in fact this entire treatment could have been conducted in topological terms by treating filtrations of a module as a neighborhood basis for 0. Taking further inspiration from such considerations, we can define a notion of convergence and continuity for filtered modules.

DEFINITION 5.2.1. An element $m \in M$ is a *limit* of a sequence $\{m_n : n \in \mathbb{N}\}$ of elements in a filtered R-module M if there exists an $m \in M$, such that, for all $r \in \mathbb{N}$, there is $N(r) \in \mathbb{N}$ such that $m_n \in F^r M$, whenever $n \geq N(r)$.

A sequence $\{m_n : n \in \mathbb{N}\}$ of elements in a filtered R-module M is *convergent* if it has a unique limit $m \in M$. In this case, we say that the sequence *converges* to m, and denote this by $\lim_{n\to\infty} m_n = m$.

A sequence $\{m_n : n \in \mathbb{N}\}$ in a filtered R-module M is *Cauchy* if, for all $r \in \mathbb{N}$, there is $N(r) \in \mathbb{N}$ such that $m_k - m_l \in F^r M$, whenever $k, l \geq N(r)$.

REMARK 5.2.2. It's clear that M is separated if and only if every sequence has at most one limit.

The next Proposition tells us that complete modules behave the way we would expect them to, given our topological intuitions.

comp-completion-complete

PROPOSITION 5.2.3. *A filtered R-module M is complete if and only if every Cauchy sequence is convergent.*

PROOF. Suppose every Cauchy sequence converges: we'll first show that M is then separated. Indeed, given $m \in \bigcap_n F^n M$, we observe that setting $m_n = m$ gives us a Cauchy sequence in M. Now we see that both 0 and m are limits of this sequence, which then, since $\{m_n\}$ is convergent, tells us that $m = 0$.

So we can assume that M is separated and show that $\varepsilon_M : M \to \hat{M}$ is a surjection if and only if every Cauchy sequence in M is convergent.

In one direction, let $s \in \hat{M}$ be a coherent sequence; then, for $r \in \mathbb{N}$, we can find $m_r \in M$ such that the image of m_r in $M/F^r M$ equals s_r, and so $s - \varepsilon_M(m_r) \in F^{r+1}\hat{M}$. Observe now that, for $t \geq r$, $m_t - m_r \in F^r M$: that is, $\{m_n : n \in \mathbb{N}\}$ is a Cauchy sequence in M and hence converges to some element $m \in M$. Then, it follows that $\{\varepsilon_M(m_n)\}$ converges to $\varepsilon_M(m)$ in $\hat{M}$. But $\hat{M}$ is separated and s is also a limit of this sequence; therefore, $s = \varepsilon_M(m)$.

Conversely, let $\{m_n : n \in \mathbb{N}\}$ be a Cauchy sequence, and consider the coherent sequence $s \in \hat{M}$ given by $s_n = \pi_n(m_n)$, where $\pi_n : M \to M/F^n M$ is the natural surjection. Then it's clear that s is a limit of the sequence $\{\varepsilon_M(m_n)\}$ in $\hat{M}$. Let $m \in M$ be such that $s = \varepsilon_M(m)$; then, for every $r \in \mathbb{N}$, $\varepsilon_M(m - m_k) \in F^r \hat{M}$, for k large enough. This implies that $m - m_k \in F^r M$, for k large enough, which shows that $\{m_n\}$ converges to m in M. □

REMARK 5.2.4. We'll usually employ this property of complete modules to talk about the convergence of series of the form $\sum_{n=1}^{\infty} m_n$, where, given any $r \in \mathbb{N}$, for n large enough, $m_n \in F^r M$. In this case, we define $\sum_{n=1}^{\infty} m_n$ to be the limit $\lim_{r\to\infty} \sum_{n=1}^{r} m_n$.

p-ideal-jacobson-radical

PROPOSITION 5.2.5. *Let $(R, F^\bullet R)$ be a complete filtered ring; then $F^1 R$ is contained in* $\operatorname{Jac} R$.

PROOF. It will suffice to show that, for every $a \in F^1 R$, $1 - a$ is a unit. Observe that the series $\sum_{n=1}^{\infty} a^n$ converges: indeed, for every $n \in \mathbb{N}$, $a^n \in F^n R$. Now it's easy to check that this convergent series gives us the inverse for $1 - a$. □

As we saw earlier, certain properties can be lifted from the associated graded ring of a filtered ring to the ring itself. The next Theorem uses this philosophy to study the relative case.

mp-gr-completion-surjinj

THEOREM 5.2.6. *Let M and N be filtered R-modules, and suppose $\varphi : M \to N$ is a map of filtered modules. Denote by* $\operatorname{gr}\varphi$ *the map induced from* $\operatorname{gr}_F(M)$ *to* $\operatorname{gr}_F(N)$.

1. *If M is separated and* $\operatorname{gr}\varphi$ *is a monomorphism, then φ is a monomorphism.*
2. *If M is complete, N is separated, and* $\operatorname{gr}\varphi$ *is a surjection, then φ is also a surjection*

PROOF. Let φ_n be the map induced from $M/F^n M$ to $N/F^n N$, and let α_n be the map induced from $F^n M/F^{n+1} M$ to $F^n N/F^{n+1} N$. Observe that $\alpha_n = (\operatorname{gr}\varphi)_n$.

(1) Let m be an element of $\ker\varphi$; then, since M is separated, there is a maximal $r \in \mathbb{N}$ such that $m \in F^r M$, but $m \notin F^{r+1}M$, and so we see that $m \in \ker\alpha_r$, which contradicts our assumption about $\operatorname{gr}\varphi$.
(2) Choose $n \in N$; since N is separated, there is a maximal $r \in \mathbb{N}$ such that $n \in F^r N$ but $n \notin F^{r+1}N$. So $\operatorname{in}(n) \in F^r N/F^{r+1}N$ can be expressed as a linear combination $\sum_i a_i(\operatorname{gr}\varphi)(\operatorname{in}(m_i))$, where $m_i \in M$. Set $m^{(1)} = \sum_i a_i m_i$; we see that $m^{(1)} \in F^r M$ and also that $n - \varphi(m^{(1)}) \in F^{r+1}M$. Now, repeating the same procedure with $n - \varphi(m^{(1)})$, we can find $m^{(2)} \in F^{r+1}M$ such that $n - \varphi\left(m^{(1)} + m^{(2)}\right)$ is in $F^{r+2}M$. Proceeding inductively, for $t \in \mathbb{N}$, we can find $m^{(t)} \in F^{r+t}M$ such that $n - \varphi\left(\sum_{k=1}^{t} m^{(k)}\right)$ lies in $F^{r+t+1}M$. Since M is complete the series $\sum_{t=1}^{\infty} m^{(t)}$ converges to an element $m \in M$. Now, we simply observe that

$$n - \varphi(m) \in \bigcap_{k=1}^{\infty} F^k N = 0,$$

and so $\varphi(m) = n$.

□

This has a number of corollaries.

comp-gr-fingen-fingen

COROLLARY 5.2.7. *Let R be a complete ring and let M be a separated filtered R-module; then M is finitely generated over R if and only if $\operatorname{gr}_F(M)$ is finitely generated over $\operatorname{gr}_F(R)$.*

PROOF. Let $m_1, \ldots, m_r \in M$ be such that $\operatorname{in}(m_1), \ldots, \operatorname{in}(m_r)$ generate $\operatorname{gr}_F(M)$ over $\operatorname{gr}_F(R)$. Set $e_i = \deg\operatorname{in}(m_i)$ and consider the free, filtered R-module $F = \oplus_i R(-e_i)$ (see (2.1.12) for the notation): we can define a map $\varphi : F \to M$ by sending the generator of $R(-e_i)$ to m_i. It's immediate that this is a map of filtered R-modules; moreover the induced map $\operatorname{gr}\varphi$ is surjective by our assumption about the m_i. Hence, by the Proposition above, φ is also surjective, and so M is finitely generated over R. □

Here's a special case of the above corollary that strengthens one of the main consequences of Nakayama's lemma.

p-nakayama-complete-case

COROLLARY 5.2.8 (Nakayama in the Complete Case). *Let R be a ring complete with respect to some ideal $I \subset R$, and let M be an R-module separated when equipped with the natural I-adic filtration. If $m_1, \ldots, m_r \in M$ are such that their images in M/IM generate M/IM over R/I, then they in fact generate M over R. In particular, M is finitely generated over R if and only if M/IM is finitely generated over R/I.*

PROOF. Just observe that $\operatorname{gr}_I(M)$ is finitely generated over $\operatorname{gr}_I(R)$ whenever M/IM is finitely generated over R/I: indeed, $I^n/I^{n+1} \otimes_{R/I} M/IM$ surjects onto $I^n M/I^{n+1}M$, for every $n \in \mathbb{N}$. Now use the corollary above (and its proof) to obtain the result. □

REMARK 5.2.9. The power of this result stems from the fact that we don't need M to be *a priori* finitely generated for it to be applicable.

For the next Corollary, recall that a Noetherian filtered ring $(R, F^\bullet R)$ is one for which the blow-up algebra $\mathscr{B}(F, R)$ is a Noetherian ring.

mp-noetherian-completion

COROLLARY 5.2.10. *A complete filtered ring (R, F) is Noetherian if and only if $\mathrm{gr}_F(R)$ is a Noetherian ring. In particular, if (R, F) is any Noetherian filtered ring, then its completion $\hat{R}$ is again Noetherian.*

PROOF. Let $I \subset R$ be any ideal, and equip it with the induced filtration; so, for any $r \in \mathbb{N}$, $F^r I = I \cap F^r R$. We claim that $\mathrm{gr}_F(I)$ is finitely generated over $\mathrm{gr}_F(R)$. Indeed, for every $n \in \mathbb{N}$, we find that

$$(F^n R \cap I) \,/\, \big(F^{n+1} R \cap I\big) \cong (F^n R \cap I) + F^{n+1} R / F^{n+1} R \subset F^n R / F^{n+1} R.$$

Therefore, $\mathrm{gr}_F(I) \subset \mathrm{gr}_F(R)$ is an ideal and is thus finitely generated over $\mathrm{gr}_F(R)$ (which is Noetherian since it's a quotient of the blow-up algebra). Now, using (5.2.7), we find that I is finitely generated over R, and so R is also Noetherian.

The second statement follows from the first assertion and the fact that $\mathrm{gr}_F(R) \cong \mathrm{gr}_F(\hat{R})$ (5.1.7). □

3. The Noetherian Case

In the last section we showed that the completion of a Noetherian filtered ring is also Noetherian (as a ring). Now we'll investigate some more consequences of the Noetherian assumption. For the rest of this section, we fix a Noetherian filtered ring (R, F).

NOTE ON NOTATION 7. Given any R-module M, we equip M with the natural filtration $F^r M = F^r R \cdot M$, and we denote by $\hat{M}$ the completion of M with respect to this filtration.

comp-stable-completion

LEMMA 5.3.1. *Let $(M, F^\bullet M)$ be a stable filtered module over R; then $\hat{M}_F \cong \hat{M}$.*

PROOF. This is a restatement of (5.1.13). □

therian-completion-exact

THEOREM 5.3.2. *Suppose we have a short exact sequence*

$$0 \to M' \to M \to M'' \to 0$$

of R-modules, with M' finitely generated. Then we obtain another exact sequence

$$0 \to \hat{M}' \to \hat{M} \to \hat{M}'' \to 0.$$

In particular, $M \mapsto \hat{M}$ gives us an exact functor from R-mod to $\hat{R}$-mod.

PROOF. Equip M with the natural filtration. It's easy to check that the produced filtration on M'' agrees with the natural filtration. By the Artin-Rees lemma (2.2.6), the induced filtration on M' is stable. Now the result follows from (5.1.10) and the lemma above. □

Now, given an R-module M, we have the natural maps

$$\alpha_M^n : R/F^n R \otimes_R M \to M/F^n M,$$

which is an isomorphism for all $n \in \mathbb{N}$ (the filtration on M is the natural filtration). This give us a natural map $\alpha_M : \hat{R} \otimes_R \to \hat{M}$ given by the composition

$$\hat{R} \otimes_R M \to \varprojlim (R/F^n R \otimes_R M) \xrightarrow{\lim \alpha_M^n} \hat{M}.$$

Let's see how this map looks in concrete terms. An element on the left hand side is a linear sum of elements of the form $s \otimes m$, where s is a coherent sequence and m is an element in M. Then, we send $s \otimes m$ to the coherent sequence with co-ordinates

$s_n \otimes m$ under the first map, and then to the coherent sequence with co-ordinates $s_n m$ in $\hat{M}$.

It's easy to see that α_R is an isomorphism, which, since both completions and tensor products respect direct sums, implies that α_{R^n} is an isomorphism, for all $n \in \mathbb{N}$. We are now ready for our first corollary to the theorem above.

comp-noetherian-tensor

COROLLARY 5.3.3. *Let M be a finitely generated R-module, and let $I \subset R$ be an ideal.*

(1) *$\alpha_M : M \otimes_R \hat{R} \to \hat{M}$ is an isomorphism.*
(2) *If R is complete, then so is M.*
(3) *$I\hat{M} = \widehat{IM}$ is the closure of $\varepsilon_M(IM)$ in $\hat{M}$. So we have*
$$\widehat{M/IM} = \hat{M}/\widehat{IM} = \hat{M}/I\hat{M}$$
(4) *$\hat{R}$ is flat over R.*
(5) *If $(R, \mathfrak{m})$ is a local ring equipped with the $\mathfrak{m}$-adic filtration, then $\hat{R}$ is faithfully flat over R.*
(6) *If $(R, \mathfrak{m})$ is a complete local ring equipped with the $\mathfrak{m}$-adic filtration, and $(S, \mathfrak{n})$ is a local ring that's a finite R-module, then S is also complete.*

PROOF. (1) Choose a finite presentation
$$R^n \to R^m \to M \to 0$$
for M. By the Theorem, we then have the following diagram with exact rows:
$$\begin{array}{ccccccc} \hat{R} \otimes_R R^n & \longrightarrow & \hat{R} \otimes_R R^m & \longrightarrow & \hat{R} \otimes_R M & \longrightarrow & 0 \\ \downarrow{\scriptstyle \alpha_{R^n}} & & \downarrow{\scriptstyle \alpha_{R^m}} & & \downarrow{\scriptstyle \alpha_M} & & \\ \hat{R^n} & \longrightarrow & \hat{R^m} & \longrightarrow & \hat{M} & \longrightarrow & 0 \end{array}$$
Here, α_{R^n} and α_{R^m} are isomorphisms as we noted above. Hence α_M is also an isomorphism.

(2) Just note that
$$\hat{M} \cong M \otimes_R \hat{R} = M \otimes_R R = M.$$

(3) That $\widehat{IM}$ is the closure of $\varepsilon_M(IM)$ follows from (5.1.10). By the Theorem, we have $\widehat{IM} = IM \otimes_R \hat{R}$ is the image of $I \otimes_R \hat{M}$ in $\hat{M}$, and so we're done.

(4) This we can deduce from (3.2.1) and part (2). Indeed, if $I \subset R$ is any ideal, then $I \otimes_R \hat{R}$ is isomorphic to $\hat{I}$, which embeds into $\hat{R}$.

(5) Note that $\mathfrak{m}\hat{R} = \hat{\mathfrak{m}}$ is the maximal ideal in $\hat{R}$. Now our result follows from (3.6.9).

(6) S is definitely complete with respect to the $\mathfrak{m}$-adic filtration; so it suffices to find $n \in \mathbb{N}$ such that $\mathfrak{n}^n \subset \mathfrak{m}$. For this, observe that $S/\mathfrak{m}S$ is a finitely generated $R/\mathfrak{m}$-module, and thus is Artinian. In particular, there is a power of $\mathfrak{n}$ contained in $\mathfrak{m}$.

□

REMARK 5.3.4. The finite generation hypothesis is crucial. For the simplest counterexample, let R be a complete ring, and consider the polynomial ring $R[t]$

as an R-module: its completion, as we found in (5.1.17), is $R\{t\}$, but its tensor product with R is of course itself.

an-power-series-quotient

COROLLARY 5.3.5. *Let R be equipped with the I-adic filtration, and suppose $I = (a_1, \ldots, a_n)$. Then there is an isomorphism of complete rings*

$$R[[x_1, \ldots, x_n]]/(x_1 - a_1, \ldots, x_n - a_n) \cong \hat{R}$$

PROOF. When $A = R[x_1, \ldots, x_n]$ is equipped with the natural filtration induced by the ideal $(x_1, \ldots, x_n)$, we see that the natural surjection $R[x_1, \ldots, x_n] \to R$ is a map of filtered A-modules with kernel $(x_1 - a_1, \ldots, x_n - a_n)$. Now our result follows from part (3) of (5.3.3). □

REMARK 5.3.6. One can show directly that $R[[x_1, \ldots, x_n]]$ is Noetherian whenever R is Noetherian by essentially the same proof as that of the Hilbert Basis theorem. So the Noetherianness of $\hat{R}$ can also be deduced from the Corollary above.

rian-commutes-hom-tensor

COROLLARY 5.3.7. *Let M and N be finitely generated R-modules.*

(1) $\widehat{M \otimes_R N} \cong \hat{M} \otimes_{\hat{R}} \hat{N}$.
(2) $\widehat{\mathrm{Hom}_R(M, N)} \cong \mathrm{Hom}_{\hat{R}}(\hat{M}, \hat{N})$.

PROOF. (1) follows immediately from (5.3.3), and (2) follows from (5.3.3) coupled with (3.1.11). □

The next Proposition can be rephrased as saying that completion reflects isomorphisms between finitely generated modules in the Noetherian case.

an-reflects-isomorphisms

PROPOSITION 5.3.8. *Let M and N be finitely generated R-modules; then $\hat{M} \cong \hat{N}$ if and only if $M \cong N$.*

PROOF. Let $\psi : \hat{M} \to \hat{N}$ be an isomorphism; From part (2) of (5.3.7), we see that we can find $r \in \hat{R}$ and $\varphi \in \mathrm{Hom}_R(M, N)$ such that $\psi = r\hat{\varphi}$. We can find a unit $u \in R$ such that $\psi - u\hat{\varphi}$ has its image in $F^1\hat{R} \cdot \hat{N}$. Replacing φ by $u\varphi$ we might as well assume that $\psi - \hat{\varphi}$ has its image in $F^1\hat{R} \cdot \hat{N}$.

By (5.2.5), $F^1\hat{R} \subset \mathrm{Jac}\, R$. So now, Nakayama's lemma tells us that $\hat{\varphi}$ is surjective. Since $\hat{R}$ is faithfully flat over R (5.3.3), this implies that φ is also surjective. In sum, we've shown that if there is an isomorphism from $\hat{M}$ to $\hat{N}$, then there is a surjection from M to N.

So we get surjections $\varphi : M \to N$ and $\varphi' : N \to M$. But then $\varphi\varphi' : N \to N$ and $\varphi'\varphi : M \to M$ are both surjections and are hence isomorphisms, by (4.1.2). This finishes our proof. □

REMARK 5.3.9. What this Proposition lets us do is transfer questions about modules over a local Noetherian ring to those about modules over its completion with respect to its maximal ideal. As we'll see towards the end of this chapter, complete local rings have a particularly simple description, which is why this result is greatly useful.

4. Hensel's Lemma and its Consequences

4.1. Hensel's Lemma: The Jazzed Up Version. For the first version of Hensel's lemma, which is a generalization of Newton's method of approximation, we will need certain facts about maps between power series rings.

DEFINITION 5.4.1. Let $A_m = R[[x_1, \dots, x_m]]$, and let $\mathbf{f} = (f_1, \dots, f_n)$ be an element of A_m^n. The *Jacobian* $J_\mathbf{f}$ of $\mathbf{f}$ is the matrix over A_m whose $(i,j)^{th}$ entry is $\frac{\partial f_i}{\partial x_j}$.

p-maps-power-series-ring

LEMMA 5.4.2. *Let R be any ring and S an R-algebra complete with respect to some filtration $F^\bullet S$.*

(1) *For every n-tuple of elements $(a_1, \dots, a_n)$ in $F^1 S$, there is a unique map of R-algebras*

$$\varphi : R[[x_1, \dots, x_n]] \to S$$
$$x_i \mapsto a_i$$

(2) *For every n-tuple $\mathbf{f}$ of elements in $(x_1, \dots, x_n)R[[x_1, \dots, x_n]]$, the unique map of R-algebras*

$$\varphi_\mathbf{f} : R[[x_1, \dots, x_n]] \to R[[x_1, \dots, x_n]]$$
$$x_i \mapsto f_i$$

is an isomorphism if and only if $\det J_\mathbf{f}(0) \in R$ is a unit.

(3) *For every choice of $\mathbf{f} \in R[[x_1, \dots, x_n]]^n$, and every $\mathbf{a} \in R^n$, there is an automorphism ψ of $R[[x_1, \dots, x_n]]$ fixing R such that*

$$f(\mathbf{a} + e\psi(\mathbf{x})) = f(\mathbf{a}) + eJ_\mathbf{f}(\mathbf{a}) \cdot \mathbf{x},$$

where $e = \det J_\mathbf{f}(\mathbf{a})$.

PROOF. (1) Equip $A = R[x_1, \dots, x_n]$ with the natural $(x_1, \dots, x_n)$-filtration; then every n-tuple $\mathbf{a}$ of elements in S, there is a unique map of R-algebras from A to S taking x_i to a_i. If the elements are chosen in $F^1 S$, then this map is in fact a map of filtered rings (and in fact filtered A-modules). Hence, since S is complete, by (5.1.5), there is a unique map from $R[[x_1, \dots, x_n]]$ to S of A-modules that satisfies our requirement. One easily checks that this is also a map of R-algebras.

(2) By (5.2.6), $\varphi_\mathbf{f}$ is an isomorphism if and only if $\operatorname{gr} \varphi_\mathbf{f}$ is an isomorphism. Let t_i be the image of x_i in $\operatorname{gr}_{(x_1,\dots,x_n)} R[[x_1, \dots, x_n]]$; then $\operatorname{gr} \varphi_\mathbf{f}$ is just the map

$$R[t_1, \dots, t_n] \to R[t_1, \dots, t_n]$$
$$t_i \mapsto \sum_{j=1}^{n} \frac{\partial f_i(0)}{\partial x_j} t_j.$$

This map is an isomorphism if and only if $\det J_\mathbf{f}(0)$ is a unit.

(3) By Taylor's formula, we can write

$$\mathbf{f}(\mathbf{a} + e\mathbf{x}) = \mathbf{f}(\mathbf{a}) + eJ_\mathbf{f}(\mathbf{a})(\mathbf{x}) + e^2\mathbf{g}(\mathbf{x}),$$

for some n-tuple $\mathbf{g}$ of elements in $(x_1, \dots, x_n)^2 R[[x_1, \dots, x_n]]$.

Let M be the matrix of minors of $J_\mathbf{f}(\mathbf{a})$, so that $J_\mathbf{f}(\mathbf{a})M = eI$. Then we can write

$$\mathbf{f}(\mathbf{a} + e\mathbf{x}) = \mathbf{f}(\mathbf{a}) + eJ_\mathbf{f}(\mathbf{a})\left(\mathbf{x} + M\mathbf{g}(\mathbf{x})\right)$$

Consider the map φ from $R[[x_1, \dots, x_n]]$ to itself induced by the n-tuple $\mathbf{h} = \mathbf{x} + eM\mathbf{g}(\mathbf{x})$; then by part (2), φ is an isomorphism. Now take $\psi = \varphi^{-1}$ to prove the statement.

□

DEFINITION 5.4.3. Let $\mathbf{f}$ be an n-tuple of polynomials in $R[x_1, \ldots, x_n]$, and let $I \subset R$ be an ideal. A *solution* for $\mathbf{f}$ is an n-tuple $\mathbf{a}$ of elements in R such that $\mathbf{f}(\mathbf{a}) = 0$. An *approximate solution* for $\mathbf{f}$ is an n-tuple $\mathbf{a}$ of elements in R such that

$$f_i(\mathbf{a}) \equiv 0 \pmod{e^2 I},$$

for $1 \leq i \leq n$, where $e = \det J_{\mathbf{f}}(\mathbf{a})$.

comp-hensel-two

THEOREM 5.4.4 (Hensel's Lemma). *Let (R, I) be a complete ring, $\mathbf{f}$ an n-tuple of polynomials in $R[x_1, \ldots, x_n]$, and $\mathbf{a}$ an approximate solution for $\mathbf{f}$. Set $e = \det J_{\mathbf{f}}(\mathbf{a})$.*

(1) *There exists a solution $\mathbf{b}$ for $\mathbf{f}$ such that*

$$b_i \equiv a_i \pmod{eI},$$

for $1 \leq i \leq n$.

(2) *If $J_{\mathbf{f}}(\mathbf{a})$ is injective (or, equivalently, if $e \notin \mathcal{Z}(R)$), then there is a unique solution $\mathbf{b}$ for $\mathbf{f}$ satisfying the condition in* (1).

PROOF. (1) Let M be the matrix of minors of $J_{\mathbf{f}}(\mathbf{a})$, so that $J_{\mathbf{f}}(\mathbf{a})M = eI$. Choose $\mathbf{c} \in \oplus_{i=1}^n I$ so that $\mathbf{f}(\mathbf{a}) = e^2\mathbf{c}$. Set $\mathbf{d} = -M\mathbf{c}$, and let $\alpha : R[[x_1, \ldots, x_n]] \to R$ be the unique map such that $\alpha(x_i) = d_i$ (5.4.2). Let ψ be the automorphism of $R[[x_1, \ldots, x_n]]$ such that

$$f(\mathbf{a} + e\psi(\mathbf{x})) = f(\mathbf{a}) + eJ_{\mathbf{f}}(\mathbf{a}) \cdot \mathbf{x}$$

Applying α to this identity, we find

$$\begin{aligned} f\left(\mathbf{a} + e\alpha\left(\psi(\mathbf{x})\right)\right) &= f(\mathbf{a}) - eJ_{\mathbf{f}}(\mathbf{a})M\mathbf{c} \\ &= f(\mathbf{a}) - e^2\mathbf{c} = 0. \end{aligned}$$

Now, we'll be done by taking $\mathbf{b} = \mathbf{a} + e\alpha\left(\psi(\mathbf{x})\right)$.

(2) Suppose $\mathbf{c}, \mathbf{c}' \in \oplus_{i=1}^n I$ are two n-tuples such that

$$f(\mathbf{a} + e\mathbf{c}) = f(\mathbf{a} + e\mathbf{c}') = 0.$$

Let β, β' be the unique maps from $R[[x_1, \ldots, x_n]]$ to R such that $\beta(x_i) = c_i$ and $\beta'(x_i) = c_i'$, respectively. Set $\gamma = \beta \circ \psi^{-1}$ and $\gamma' = \beta' \circ \psi^{-1}$; then we find that

$$0 = f(\mathbf{a} + e\mathbf{c}) = f\left(\mathbf{a} + e\gamma\left(\psi(\mathbf{x})\right)\right) = f(\mathbf{a}) + eJ_{\mathbf{f}}(\mathbf{a})(\gamma(\mathbf{x})).$$

There's also a similar identity involving $\mathbf{c}'$ giving us the equality

$$eJ_{\mathbf{f}}(\mathbf{a})(\gamma(\mathbf{x})) = eJ_{\mathbf{f}}(\mathbf{a})(\gamma'(\mathbf{x})).$$

Since $J_{\mathbf{f}}(\mathbf{a})$ is injective, e is a non-zero divisor, and we find that $\gamma = \gamma'$, and so $\mathbf{c} = \mathbf{c}'$, which is what we wanted to show.

□

mp-implicit-function-thm

COROLLARY 5.4.5 (Implicit Function Theorem). *Let (R, I) be a complete ring, $\mathbf{f}$ an s-tuple of elements in $R[x_1, \ldots, x_r, y_1, \ldots, y_s]$, and $M_{\mathbf{f}}$ the $s \times s$-matrix whose $(i,j)^{th}$ entry is $\frac{\partial f_i}{\partial y_j}$. Suppose $\mathbf{a} \in R^r$ and $\mathbf{b} \in R^s$ are such that $\mathbf{f}(\mathbf{a}, \mathbf{b}) = 0$, and suppose that $e = \det M_{\mathbf{f}}(\mathbf{a}, \mathbf{b})$ is a unit. Then, we can find an s-tuple $\mathbf{g}$ of elements in $R[[x_1, \ldots, x_r]]$ such that $\mathbf{g}(\mathbf{a}) = \mathbf{b}$ and $\mathbf{f}(\mathbf{x}, \mathbf{g}(\mathbf{x})) = 0$.*

PROOF. By replacing x_i with $x_i - a_i$, we can assume that $\mathbf{a} = 0$. Now, set $A = R[[x_1, \ldots, x_r]]$, and view $\mathbf{f}$ as an s-tuple in $A[y_1, \ldots, y_s]$. We find that $\det J_{\mathbf{f}} = e$ is a unit, and so by hypothesis $\mathbf{b}$ is an approximate solution for $\mathbf{f}$ (where $I = (x_1, \ldots, x_n)$). By the Theorem, there now exists a solution $\mathbf{g} \in A^s$ for $\mathbf{f}$ such that $\mathbf{g} \equiv \mathbf{b} \pmod{(x_1, \ldots, x_n)}$, which is equivalent to saying that $\mathbf{g}(0) = \mathbf{b}$. □

For convenience, we present the one-dimensional version of these results separately.

comp-hensel-two-one-dim

COROLLARY 5.4.6. *Let (R, I) be a complete ring.*

(1) *Let $f \in R[x]$ be a polynomial, and let $a \in R$ be such that*
$$f(a) \equiv 0 \pmod{f'(a)^2 I}.$$
Then, there exists $b \in R$ such that $f(b) = 0$ and $a - b \in f'(a)I$. If $f'(a)$ is a non-zero divisor, then there is a unique such $b \in R$.

(2) *Let $g \in R[x, y]$ be a polynomial, and let $a, b \in R$ be such that $g(a, b) = 0$, and such that $\frac{\partial g}{\partial y}(a, b)$ is a unit. Then, there is a power series $h \in R[[x]]$ such that $h(a) = b$, and $f(x, h(x)) = 0$.*

We isolate a very special, but useful case of the one-dimensional version.

p-hensel-one-simple-root

COROLLARY 5.4.7. *Let (R, I) be a complete ring, let $F \in R[t]$ be a polynomial, and suppose $a \in R$ is such that $F(a) \equiv 0 \pmod{I}$, and such that $F'(a)$ is a unit in R. Then, there exists a unique $b \in R$ such that $F(b) = 0$ and $a \equiv b \pmod{I}$.*

PROOF. Follows immediately from the Corollary above. □

EXAMPLE 5.4.8. As an application of Hensel's lemma, we will now present a criterion for deciding whether a unit in $\hat{\mathbb{Z}}_p$ is an n^{th} power. So let $u \in \hat{\mathbb{Z}}_p$ be a unit; then to say that u is an n^{th} power is equivalent to saying that there is a solution to $f(x) = x^n - u$. Let v_p be the p-adic valuation, and let $r = v_p(n)$. Suppose $w \in \hat{\mathbb{Z}}_p$ is such that $f(w) \equiv 0 \pmod{p^{2r+1}}$. Observe that $p \nmid w$, for, if this were not the case, then $p \mid u$, which contradicts the assertion that u is a unit. Hence $f'(w) = p^r b$, where $p \nmid b$, and so we find that w is an approximate solution for f. The Corollary above tells us that there is in fact a solution for f, and thus an n^{th} root for u in $\hat{\mathbb{Z}}_p$. So u has an n^{th} root in $\hat{\mathbb{Z}}_p$ if and only if it has a root modulo $p^{2v_p(n)+1}$.

For example, if we take $n = 2$, then u has a square root in $\hat{\mathbb{Z}}_p$ if and only if n has a square root module $p^{2v_p(2)+1}$. If $p \neq 2$, then we see that u has a square root in $\hat{\mathbb{Z}}_p$ if and only if $\left(\frac{u}{p}\right) = 1$. If $p = 2$, then u has a square root if and only if it has a square root modulo 8. But the only odd square module 8 is 1, and so u has a square root if and only if $u \equiv 1 \pmod{8}$.

The same argument of course applies verbatim to any local field with finite residue field.

4.2. Hensel's Lemma: The Classical Version. What follows is a more classical version of Hensel's Lemma.

comp-hensel-one

THEOREM 5.4.9 (Classical Hensel's Lemma). *Let R be a ring complete with respect to an ideal I, and let $F \in R[t]$ be a polynomial. Suppose we have polynomials $g_1, g_2 \in R[t]$, and suppose* $\mathrm{Res}(g_1, g_2) \notin I^{s+1}$. *If we have*
$$F \equiv g_1 g_2 \pmod{I^{2s+1}},$$

and suppose the leading coefficient of F is the product of the leading coefficients of g_1 and g_2; then we can find polynomials $G_1, G_2 \in R[t]$ satisfying the following conditions:

(1) $G_i \equiv g_i \pmod{I^{s+1}}$, *for* $i = 1, 2$.
(2) $\deg G_i = \deg g_i$, *for* $i = 1, 2$.
(3) *The leading coefficient of G_i is the same as the leading coefficient of g_i, for* $i = 1, 2$.
(4) $F = G_1 G_2$.

If, moreover, $\operatorname{Res}(g_1, g_2)$ *is a non-zero divisor, then the G_i satisfying these conditions are in fact uniquely determined.*

PROOF. We'll call a pair (H_1, H_2) of polynomials a *solution* to our problem if it satisfies the conditions listed above.

Suppose $g_1(t) = \sum_{i=0}^{r} a_i t^i$, with $a_r \neq 0$, $g_2(t) = \sum_{j=0}^{s} b_j t^j$, with $b_s \neq 0$, and $F(t) = \sum_{k=0}^{n} c_k t^k$, so that $r + s = n = \deg F$. Now consider the n-tuple of polynomials $\mathbf{f} \in R[x_0, \ldots, x_{r-1}, y_0, \ldots, y_{s-1}]$ given by

$$f_t(\mathbf{x}, \mathbf{y}) = \sum_{i+j=t} x_i y_j - a_r y_{t-r} - b_s x_{t-s} c_t, \qquad \text{for } 0 \leq t \leq n-1.$$

Here, we follow the convention that $y_t = x_t = 0$, for $t < 0$. It's easy to check that

$$e = J_{\mathbf{f}}(\mathbf{a}, \mathbf{b}) = \operatorname{Res}(g_1, g_2)$$

The following congruence is then just a consequence of our hypotheses:

$$\mathbf{f}(\mathbf{a}, \mathbf{b}) \equiv g_1 g_2 \pmod{e^2 I}.$$

Observe that by our construction the pair of polynomials $(\sum_{i=0}^{r} a'_i t_i, \sum_{j=0}^{s} b'_j t^j)$, where $a'_r = a_r$ and $b'_s = b_s$, is a solution to our problem if and only if the $r+s$-tuple $(\mathbf{a}', \mathbf{b}') = (a'_0, \ldots, a'_{r-1}, b'_0, \ldots, b'_{s-1})$ is such that

$$\mathbf{f}(\mathbf{a}', \mathbf{b}') = 0;$$
$$(\mathbf{a}', \mathbf{b}') \cong (\mathbf{a}, \mathbf{b}) \pmod{I^{s+1}}.$$

Now, by our jazzed up Hensel's lemma (5.4.4), we immediately obtain existence of a solution, and also its uniqueness, when e is a non-zero divisor. □

REMARK 5.4.10. In most cases we encounter, one of the g_i will be a monic polynomial, and the Theorem then assures us that G_i will also be monic in that case.

5. Lifting of Idempotents: Henselian Rings

comp-lifting-idempotents

THEOREM 5.5.1 (Lifting of Idempotents). *Let (R, I) be a complete Noetherian ring, and suppose A is a finite, central R-algebra (not necessarily commutative); then any finite set of orthogonal idempotents of A/IA can be lifted to a set of orthogonal idempotents of A. If A is commutative, then this lifting is unique.*

PROOF. Suppose first that $e \in R$ is such that $\overline{e} \in R/I$ is idempotent. Consider the polynomial $f(x) = x^2 - x$; we claim that $f'(e) = 2e - 1$ is a unit. Indeed, we find that $f'(e)^2 \equiv 1 \pmod{I}$, and is hence a unit by (5.2.5). Hence, by (5.4.7), there exists a unique idempotent $\widetilde{e} \in R$ that maps to $\overline{e}$ in R/I.

Now let $\{\overline{e}_1, \ldots, \overline{e}_n\}$ be a set of orthogonal idempotents in A/IA. First suppose that A is commutative; then, by part (2) of (5.3.3), A is itself complete with respect

to the ideal IA. Hence we can assume that $A = R$; in this case, as we showed in the first paragraph, for each i, there is a unique idempotent $\widetilde{e}_i \in R$ such that $\overline{\widetilde{e}}_i = \overline{e}_i$. We will show that the set $\{\widetilde{e}_1, \ldots, \widetilde{e}_n\}$ is orthogonal. Indeed $\widetilde{e}_i\widetilde{e}_j \in I$, for all pairs (i, j), with $i \neq j$. By idempotence, it follows that $\widetilde{e}_i\widetilde{e}_j \in \bigcap_{n\geq 0} I^n$, for these pairs (i, j). Since R is complete, it's in particular separated, and so we see that $\widetilde{e}_i\widetilde{e}_j = 0$.

It's time to discard the commutativity hypothesis. We will lift $\overline{e}_i$ to A by induction on n. If $n = 1$, then we can replace A by the commutative R-subalgebra generated by e_1, and so we'll be done by our proof of the commutative case. If $n > 1$, by induction, we can lift $\overline{e}_i$ to idempotents $\widetilde{e}_i \in A$, for $1 \leq i \leq n-1$, orthogonal to each other. Let $f = 1 - \sum_{i=1}^{n-1} \widetilde{e}_i$, and set $e = fe_nf$. We find that $ee_i = e_ie = 0$, for $1 \leq i \leq n-$. Moreover

$$\overline{e} = \overline{f}\overline{e}_n\overline{f} = \overline{e}_n\overline{f} = \overline{e}_n.$$

So we can restrict our attention to the R-subalgebra A' of A generated by $\widetilde{e}_1, \ldots, \widetilde{e}_{n-1}, e$. This is a commutative ring, and so we're again done by our proof of the commutative case. □

EXAMPLE 5.5.2. The uniqueness does in fact fail in the non-commutative case. Consider the ring A of 2×2 matrices over $k[[t]]$, and the matrices

$$\begin{pmatrix} 1 & 0 \\ tr(t) & 0 \end{pmatrix}$$

where $r(t)$ is any power series over k. Each of these matrices is idempotent and reduces modulo t to the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

The following Corollary gives a structure theorem for finite algebras over a complete local ring.

rian-lifting-idempotents

COROLLARY 5.5.3. *Let $(R, \mathfrak{m})$ be a complete Noetherian local ring, and let A be a commutative R-algebra finite over R. Then A has only finitely many maximal ideals $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$. Moreover, $A_{\mathfrak{m}_i}$ is also a complete Noetherian local ring, for all i, and $A = \prod_{i=1}^n A_{\mathfrak{m}_i}$.*

PROOF. Observe that $A/\mathfrak{m}A$ is a finitely generated $R/\mathfrak{m}$-module and is thus Artinian. So there is a complete set of orthogonal idempotents $\{\overline{e}_1, \ldots, \overline{e}_n\} \subset A/\mathfrak{m}A$. By the Theorem above, these can be lifted to a complete set of orthogonal idempotents $\{e_1, \ldots, e_n\} \subset A$. Let $A_i = Ae_i$; then we see that $A = \prod_{i=1}^n A_i$, where $A_i/\mathfrak{m}A_i$ is a local Artinian ring, for all i. Moreover, since A_i is a direct summand of A as an R-module, it's also finite over R.

Let $\mathfrak{n} \subset A_i$ be a maximal ideal; then $\mathfrak{n} \cap R$ is again a maximal ideal, by (4.4.5). Hence every maximal ideal of A_i contains $\mathfrak{m}A_i$. Since $A_i/\mathfrak{m}A_i$ is a local ring, we see therefore that A_i is also a local ring. Let $\mathfrak{n}_i \subset A_i$ be the maximal ideal and let $\mathfrak{m}_i \subset A$ be the maximal ideal that's the pre-image of $\mathfrak{n}_i$ under the projection $A \to A_i$. Then it's clear that $A_i \cong A_{\mathfrak{m}_i}$. Now, any maximal ideal in A contains $\mathfrak{m}A$ by the argument at the beginning of this paragraph, and thus corresponds to a maximal ideal of $A/\mathfrak{m}A$. But the maximal ideals of $A/\mathfrak{m}A$ are precisely the images of the $\mathfrak{m}_i$ in $A/\mathfrak{m}A$. □

This Corollary inspires the following definition.

DEFINITION 5.5.4. A local Noetherian ring $(R, \mathfrak{m})$ is *Henselian* if every commutative finite R-algebra can be decomposed into a finite direct product of local R-algebras.

REMARK 5.5.5. The Corollary above shows that all complete Noetherian local rings are Henselian.

The next Theorem shows that the Henselian property is equivalent to a somewhat weak Hensel's Lemma type result. It is in fact true that it is equivalent to the strong form of Hensel's Lemma (5.4.4), but we will not prove this till Chapter 16.

nselian-characterization

THEOREM 5.5.6. *Let $(R, \mathfrak{m})$ be a local Noetherian ring, and set $k = R/\mathfrak{m}$. Then the following are equivalent:*

1. *R is Henselian.*
2. *Every free R-algebra of finite rank can be decomposed into a finite product of local R-algebras.*
3. *For every monic polynomial $p(t) \in R[t]$, $R[t]/(p(t))$ can be decomposed into a finite product of local R-algebras.*
4. *For every monic polynomial $F(t) \in R[t]$, and every pair of monic polynomials $g_1(t), g_2(t) \in R[t]$ satisfying the following conditions:*
   (a) $F(t) \equiv g_1(t)g_2(t) \pmod{\mathfrak{m}}$.
   (b) $\mathrm{Res}(g_1(t), g_2(t)) \notin \mathfrak{m}$,
   we can find monic polynomials $G_1(t), G_2(t) \in R[t]$ such that $F(t) = G_1(t)G_2(t)$ and such that $G_i(t) \equiv g_i(t) \pmod{\mathfrak{m}}$, for $i = 1, 2$.

PROOF. (1) $\Rightarrow$ (2) is trivial, and (2) $\Rightarrow$ (3) follows from (4.1.3).

For (3) $\Rightarrow$ (4), consider the R-algebra $R[t]/(F(t))$: this is a free R-algebra of finite rank (4.1.3), and so can be decomposed into a product of local R-algebras, by hypothesis. Given g_1, g_2 satisfying the given conditions, we find that $\overline{F} = \overline{g}_1\overline{g}_2 \in k[t]$, and that

$$k[t]/(\overline{F}(t)) \cong k[t]/(\overline{g}_1(t)) \times k[t]/(\overline{g}_2(t)).$$

Since $R[t]/(F(t))$ is decomposed into a product of local R-algebras, we see that $R[t]/(F(t)) = S_1 \times S_2$, where $S_i/\mathfrak{m}S_i \cong k[t]/(\overline{g}_i(t))$, for $i = 1, 2$. Now, since S_i is projective over R, it is in fact free over R (7.1.3), and its rank is $\deg g_i$. But then, by (4.1.3), $S_i = R[t]/(G_i(t))$, for some monic polynomial $G_i(t) \in R[t]$. It's clear now that the G_i satisfy our requirements. □

6. More on Actions by Finite Groups

Let S be a ring, let G be a finite group acting on S via ring automorphisms and let $R = S^G$ be the ring of invariants of this action. By (4.5.6), we can localize S and R at any prime ideal of R and still preserve the same hypotheses. In other words, we can assume that R is a local ring with maximal ideal $\mathfrak{m}$. By the same argument, we can also replace S and R with their completions along $\mathfrak{m}$. By (5.5.3) and (4.5.2), S decomposes into a direct product of its localizations at the primes lying over $\mathfrak{m}$. Now, suppose $S = \prod_{i=1}^{r} S_i$, where $S_i = S_{\mathfrak{n}_i}$, for some maximal ideal $\mathfrak{n}_i \subset S$, and let $D_i \leq G$ be the decomposition group of $\mathfrak{n}_i$. This sub-group acts on S_i, and the ring of invariants of this action contains R. It is moreover a local R-algebra, whose residue field is the same as that of R (4.5.7), and therefore must be equal to R. We summarize this in the following

omp-finite-group-actions

PROPOSITION 5.6.1. *Let S be a ring, let G be a finite group acting on S via ring automorphisms and let $R = S^G$ be the ring of invariants of this action. Let $\mathfrak{p} \subset R$ be a prime, and let $\hat{S}$ and $\hat{R}$ be the completions of S and R along $\mathfrak{p}$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_d$ be the primes of S lying over $\mathfrak{p}$; then we have*

$$\hat{S} = \prod_{i=1}^{d} S_i,$$

where $S_i = \widehat{S_{\mathfrak{q}_i}}$. Moreover, if $D_i \leq G$ is the decomposition group of $\mathfrak{q}_i$, then $S_i^{D_i} = \hat{R}$.

CHAPTER 6

Dimension Theory I: The Main Theorem

chap:dt

1. Krull Dimension and the Hauptidealsatz

dt-secn:krull-theorem

The cleanest definition of dimension, valid for all rings, is the following.

DEFINITION 6.1.1. The *Krull dimension* $\dim R$ of a ring R is the maximal length of a chain of primes

$$P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_r$$

in R.

Obviously, it need not be finite.

DEFINITION 6.1.2. The *Krull dimension* $\dim M$ of a finitely generated R-module M is the Krull dimension of the quotient ring $R/\operatorname{ann}(M)$.

REMARK 6.1.3. There's a lot of information in this definition. Recall that a prime $P \subset R$ contains $\operatorname{ann}(M)$ if and only if $P \in \operatorname{Supp} M$ if and only if $M_P \neq 0$. So the Krull dimension of M is the longest chain of primes such that M localized at each prime is non-zero.

The dimension 0 case is easy to take care of.

dt-dimension-zero

PROPOSITION 6.1.4. *A finitely generated R-module M is Artinian if and only if* $\dim M = 0$.

PROOF. Observe that M is Artinian if and only if $R/\operatorname{ann}(M)$ is an Artinian ring. So it suffices to show that a ring R is Artinian if and only if it has dimension 0. But observe that a Noetherian ring R is Artinian if and only if all its prime ideals are maximal. This is exactly equivalent to the fact that $\dim R = 0$. □

The first and the prettiest finiteness result about Krull dimension is the Hauptidealsatz. Geometrically, it says that, by introducing an extra equation, you can cut down the dimension of the solution space by at most one.

dt-hauptidealsatz

THEOREM 6.1.5 (Krull's Hauptidealsatz). *If R is a Noetherian ring, and $\mathfrak{p} \subset R$ is a prime minimal over a principal ideal (a), then* $\dim R_{\mathfrak{p}} \leq 1$.

PROOF. We can assume right away that R is local with maximal ideal $\mathfrak{p}$. We want to show that $\dim R \leq 1$. By quotienting out by a minimal prime, we can also assume R is a domain. We wish to show that there are no primes between 0 and $\mathfrak{p}$. So assume to the contrary that we have a chain of primes $0 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. Now, $R/(a)$ is a local Artinian ring, and so the descending chain:

$$(a) + \mathfrak{q} \supset (a) + \mathfrak{q}^{(2)} \supset \ldots \supset (a) + \mathfrak{q}^{(n)} \supset \ldots$$

stabilizes, where $\mathfrak{q}^{(n)} = (\mathfrak{q}_{\mathfrak{q}}^n)^c$, is the symbolic n^{th} power of $\mathfrak{q}$. So there is n such that $\mathfrak{q}^{(n)} \subset (a) + \mathfrak{q}^{(n+1)}$. Observe now that $\mathfrak{q}^{(n)}$ is $\mathfrak{q}$-primary: so if $ar \in \mathfrak{q}^{(n)}$ for

some $r \in R$, then in fact $r \in \mathfrak{q}^{(n)}$ (since $a \notin \mathfrak{q}$). Hence $\mathfrak{q}^{(n)} = a\mathfrak{q}^{(n)} + \mathfrak{q}^{(n+1)}$. But $a \in \mathfrak{p}$, and so by Nakayama, $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+1)}$. This means that in $R_{\mathfrak{q}}$, we have $\mathfrak{q}_{\mathfrak{q}}^n = \mathfrak{q}_{\mathfrak{q}}^{n+1}$; so another application of Nakayama tells us that $\mathfrak{q}_{\mathfrak{q}}^n = 0$. But $R_{\mathfrak{q}}$ is a domain! Hence $\mathfrak{q}_{\mathfrak{q}} = 0$, which implies that $\mathfrak{q} = 0$, contradicting our assumption that it wasn't. □

DEFINITION 6.1.6. We define the *height* $\operatorname{ht}\mathfrak{p}$ of a prime $\mathfrak{p} \subset R$ to be $\dim R_{\mathfrak{p}}$.

REMARK 6.1.7. Krull's theorem says that for any prime $\mathfrak{p}$ minimal over a principal ideal, we have $\operatorname{ht}\mathfrak{p} \leq 1$.

This theorem has a number of corollaries.

dt-nzd-ht-by-one

COROLLARY 6.1.8. *If, in the theorem above, a is not in any minimal prime, in particular, if a is a non zero divisor, then* $\operatorname{ht}\mathfrak{p} = 1$.

PROOF. From the hypothesis, it's evident that $\mathfrak{p}$ is not minimal. Hence $\operatorname{ht}\mathfrak{p} > 0$, and the theorem gives us the result. □

dt-min-primes-height

COROLLARY 6.1.9. *If R is a Noetherian ring, and $\mathfrak{p} \subset R$ is a prime minimal over an ideal $(x_1, \ldots, x_r)$ generated by r elements, then* $\operatorname{ht}\mathfrak{p} \leq r$.

PROOF. We prove this by induction on r. The case $r = 1$ is Krull's theorem above. By localizing, we can assume R is a local ring with maximal ideal $\mathfrak{p}$. Let $\mathfrak{q} \subsetneq \mathfrak{p}$ be a prime such that there are no primes between $\mathfrak{q}$ and $\mathfrak{p}$. Now, $\mathfrak{q}$ cannot contain all the x_i; so we can assume without loss of generality, that $x_1 \notin \mathfrak{q}$. In this case, $\mathfrak{p}$ is minimal over $(x_1) + \mathfrak{q}$, and hence, by applying Krull's theorem to $R/\mathfrak{q}$, we see that $\operatorname{ht}\mathfrak{p} \leq \operatorname{ht}\mathfrak{q} + 1$.

Since $(x_1) + \mathfrak{q}$ is $\mathfrak{p}$-primary, we see that there is $n \in \mathbb{N}$ such that $x_i^n \in (x_1) + \mathfrak{q}$, for all i. For $2 \leq i \leq n$, let $y_i \in \mathfrak{q}$ be such that $x_i^n - y_i \in (x_1)$. Then, if $I = (y_2, \ldots, y_{r-1})$, we see that in R/I, $\mathfrak{p}/I$ is minimal over $(\overline{x}_1)$, and so, by Krull's theorem, $\operatorname{ht}\mathfrak{p}/I \leq 1$. But then $\operatorname{ht}\mathfrak{q}/I = 0$, which implies that $\mathfrak{q}$ is minimal over I, and so, by inductive hypothesis, $\operatorname{ht}\mathfrak{q} \leq r - 1$, giving us $\operatorname{ht}\mathfrak{p} \leq r$. □

dt-krull-thm-converse

COROLLARY 6.1.10. *If $\operatorname{ht}\mathfrak{p} = r$, then we can find an ideal I generated by r elements such that $\mathfrak{p}$ is minimal over I.*

PROOF. We prove this by induction. When $\operatorname{ht}\mathfrak{p} = 0$, there's nothing to show. So assuming $\operatorname{ht}\mathfrak{p} > 0$, we can find a prime $\mathfrak{q} \subset \mathfrak{p}$ with $\operatorname{ht}\mathfrak{q} = r - 1$, and so there is an ideal J generated by $r - 1$ elements over which $\mathfrak{q}$ is minimal. Now, let $P_1, \ldots, P_t$ be the primes in R minimal over J, and choose $x \in \mathfrak{p} \setminus \bigcup_i P_i$. Let $I = J + (x)$; then $\mathfrak{p}$ is minimal over I, and so I is the ideal we were looking for. □

Using the notion of height, we can give now a useful property of normal domains.

l-heightone-intersection

COROLLARY 6.1.11. *A normal, Noetherian domain R is the intersection of its localizations R_P taken over all primes P of height* 1.

PROOF. By (4.3.7), we have $R = \cap_P R_P$, where the intersection is taken over all primes P associated to a principal ideal. By (4.3.19), we see that every such prime has height 1. □

2. The Main Theorem of Dimension Theory

We now specialize to the case of *semilocal*, Noetherian rings. So consider a ring R with finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. We set $\mathfrak{m} = \cap_i \mathfrak{m}_i$; this is the Jacobson radical of R.

In this case, we'll be able to prove that the dimension of a finitely generated module is always finite. For this, we need a different measure of dimension, so to speak, that we know is *a priori* finite. For, after all, the main problem with Krull dimension is that it's not clear at all if it is ever finite.

DEFINITION 6.2.1. A *system of parameters* for an R-module M is a subset $\{x_1, \ldots, x_n\}$ of $\mathfrak{m}$ such that $\mathfrak{q} = (x_1, \ldots, x_n)$ is an ideal of definition for M; that is, $\mathfrak{q}$ is such that $M/\mathfrak{q}M$ is Artinian.

Here's another candidate for the dimension of a semilocal ring.

DEFINITION 6.2.2. For an R-module M, we set $\delta(M)$ to be the minimal size of a system of parameters for M.

REMARK 6.2.3. The reason that this should be a good measure of dimension is this: suppose we consider the scheme $\operatorname{Spec} R$ and we look at the closed subscheme $\operatorname{Spec} R/\mathfrak{q}$, for some ideal of definition: this is supported in a discrete closed subspace, and so we can consider the generators $x_1, \ldots, x_n$ of $\mathfrak{q}$ as giving us 'co-ordinates' on $\operatorname{Spec} R$ upto finite ambiguity.

For simplicity, suppose R is a k-algebra, where k is algebraically closed. Then, what we're saying is that given any n-tuple $(a_1, \ldots, a_n) \in k^n$, there are only finitely many points at which the global section $x_1 - a_1, \ldots, x_n - a_n$ all vanish together. We will see later that even this finite ambiguity disappears when we are dealing with so-called *regular* local rings. In fact, in some sense, the lack of ambiguity characterizes such local rings.

dt-del-m-del-ann

LEMMA 6.2.4. *A set $\{x_1, \ldots, x_n\}$ is a system of parameters for M if and only if it is a system of parameters for $R/\operatorname{ann}(M)$. In particular, $\delta(M) = \delta(R/\operatorname{ann}(M))$.*

PROOF. We showed in (2.3.15) that $\mathfrak{q}$ is an ideal of definition for M if and only if $V(\mathfrak{q}) \cap \operatorname{Supp} M$ was a finite set consisting entirely of maximal ideals. Since $\operatorname{Supp} M = \operatorname{Supp}(R/\operatorname{ann}(M))$, we are done. □

We will now use the Hilbert and Samuel functions to define another version of dimension. This is the most easily computable version, albeit somewhat unintuitive. We maintain our hypothesis that R is a semilocal ring with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ and Jacobson radical $\mathfrak{m}$.

Recall from (2.3.18), the definition of the Samuel polynomial $\chi_M^{\mathfrak{q}}$ associated to a module M over the filtered ring $(R, \mathfrak{q})$, where $\mathfrak{q}$ is some ideal of definition for M. We showed in (2.3.24) that the degree of this polynomial depends only on the set $\operatorname{Supp} M \cap V(\mathfrak{q})$. If now, R is semilocal and $\mathfrak{q}$ is generated by a system of parameters for R, then $V(\mathfrak{q}) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ is just the collection of maximal ideals of R. So $V(\mathfrak{q})$ and hence $\operatorname{Supp} M \cap V(\mathfrak{q})$ is independent of choice of $\mathfrak{q}$. This lets us formulate the following definition.

DEFINITION 6.2.5. The *Poincaré dimension* $d(M)$ of an R-module M is the degree of the Samuel polynomial $\chi_M^{\mathfrak{q}}$, where $\mathfrak{q} \subset \mathfrak{m}$ is any ideal of definition for R contained in $\mathfrak{m}$; or, equivalently, where $\mathfrak{q}$ is an ideal generated by a system of parameters for R.

dt-hfm-polynomial-ring

EXAMPLE 6.2.6. To make this definition a little more palatable, we will compute this number in a very special and simple case. Consider the polynomial ring $R = k[x_1, \ldots, x_n]$ and its localization $R_{\mathfrak{m}}$ at the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. Then, it's easy to see that $\mathrm{gr}_{\mathfrak{m}}(R_{\mathfrak{m}}) \cong R$. Hence we can compute the Hilbert polynomial associated to the filtered ring $(R_{\mathfrak{m}}, \mathfrak{m})$ quite easily. Indeed, $H^{\mathfrak{m}}_{R_{\mathfrak{m}}}(r) = \dim_k R_r$, but R_r is just the space of all homogeneous polynomials of degree r, and this is spanned by all the monomials in the x_i of degree r. So $\dim_k R_r = \binom{n+r-1}{n-1}$; and we see that $H^{\mathfrak{m}}_{R_{\mathfrak{m}}} = Q_{n-1}$, in the notation of Section 3. Hence $\deg H^{\mathfrak{m}}_{R_{\mathfrak{m}}} = n-1$, and so $\deg \chi^{\mathfrak{m}}_{R_{\mathfrak{m}}} = n$, which shows that $d(R_{\mathfrak{m}}) = n$.

Of course, the choice of the maximal ideal $\mathfrak{m}$ here was arbitrary. We could have chosen any other maximal ideal and obtained the same result (though things would be a little hairier in the case where k is not algebraically closed). In fact, using the main theorem of dimension theory, which we will prove very soon, this 'shows' that $\dim k[x_1, \ldots, x_n] = n$. We will find a different (and more rigorous!) proof of this fact in a later section (6.6.3).

The following lemma is crucial.

LEMMA 6.2.7. *If we have an exact sequence of finitely generated R-modules*

$$0 \to M' \to M \to M'' \to 0,$$

then the polynomials associated to the functions $\chi^{\mathfrak{q}}_M - \chi^{\mathfrak{q}}_{M''}$ and $\chi^{\mathfrak{q}}_{M'}$ have the same degree and leading coefficient. In particular, we have

$$d(M) = \max\{d(M'), d(M'')\}.$$

PROOF. See (2.3.22). □

Now, we can present the most fundamental result of dimension theory.

dt-main-thm-dim-theory

THEOREM 6.2.8 (Main Theorem of Dimension Theory). *Any finitely generated module M over a semilocal, Noetherian ring R has finite Krull dimension. Moreover, we have*

$$\delta(M) = \dim M = d(M).$$

PROOF. We will show

$$d(M) \geq \dim M \geq \delta(M) \geq \mathrm{d}(M)$$

Since we know that $d(M)$ and $\delta(M)$ are finite, but are not sure about $\dim M$, we will prove the first inequality by induction on $d(M)$. If $d(M) = 0$, then $\dim M/\mathfrak{m}^n M$ is a constant for large enough n. This implies that $\mathfrak{m}^n M = \mathfrak{m}^{n+1} M$, and by Nakayama, we have $\mathfrak{m}^n M = 0$, for large enough n. Hence M is of finite length, and so $\dim M = 0$. Now, assume $d(M) > 0$, and pick $x \notin \mathcal{Z}(M)$. Then, by Corollary (6.2.12), we see that $\dim M' = \dim M - 1$, where $M' = M/xM$. But we also have the exact sequence:

$$0 \to M \xrightarrow{x} M \to M' \to 0.$$

This tells us, via the lemma above, that $d(M') \leq d(M) - 1$. By the induction hypothesis, we then have

$$d(M) \geq d(M') + 1 \geq \dim M' + 1 = \dim M.$$

Now, we turn to the second inequality: by (6.2.4), we see that

$$\delta(M) = \delta(R/\operatorname{ann}(M)).$$

Since, by definition, $\dim M = \dim(R/\operatorname{ann}(M))$, it suffices to prove the inequality for the case where M is itself the semilocal ring R. We do this by induction on $\dim R$. If $\dim R = 0$, then (0) is an ideal of definition, and so $\delta(R) = 0$. Suppose $\dim R > 0$, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the minimal primes of R such that $\dim R/\mathfrak{p}_i = \dim R$. Then none of the $\mathfrak{p}_i$ is maximal; therefore $\mathfrak{m} \nsubseteq \mathfrak{p}_i$, for all $1 \leq i \leq n$. So there exists, by prime avoidance, $x \in \mathfrak{m} \setminus \bigcup_i \mathfrak{p}_i$. Let $R' = R/(x)$; then we have

$$\dim R' = \dim R - 1.$$

Now, by the induction hypothesis, we have

$$\delta(R') \leq \dim R' = \dim R - 1.$$

So, to finish up, it suffices to show that $\delta(R') \geq \delta(R) - 1$. Indeed, if $\{x_1, \ldots, x_r\}$ is a set of elements of R such whose images form a system of parameters in R', then $\{x, x_1, \ldots, x_r\}$ is a system of parameters in R.

Now, for the last and easiest inequality: We have an ideal of definition $\mathfrak{q} \subset \mathfrak{m}$ generated by a system of parameters for M of size exactly $\delta(M)$. Any system of parameters for R generating an ideal of definition for M must, by the definition of $\delta(M)$, have at least $\delta(M)$ elements. From (2.3.9), we then see that $d(M) \leq \delta(M)$. □

Remark 6.2.9. From now on, for any finitely generated module M over a semilocal ring R, we will refer to any of the following quantities as the dimension of M and denote them all by $\dim M$:

Krull dimension: The maximal length of a chain of primes in $R/\operatorname{ann}(M)$.
Chevalley dimension: The minimal size of a system of parameters for M.
Poincaré dimension: The degree of the Samuel polynomial $\chi_M^{\mathfrak{q}}$, where $\mathfrak{q}$ is any ideal of definition for R.

The Main Theorem assures us that they are all indeed the same thing.

Remark 6.2.10. One can actually deduce the Hauptidealsatz as a Corollary of the main theorem: simply localize at the prime minimal over a non-zero divisor, and observe that the non-zero divisor is now a system of parameters in the localization.

However, the Hauptidealsatz is a fundamental result, and it seems to me an independent proof is well worth it, especially when it's as elegant as Krull's.

dt-dim-decreasing

Corollary 6.2.11. *If $x_1, \ldots, x_n \in R$ then we have*

$$\dim M/(x_1, \ldots, x_n)M \geq \dim M - n$$

Proof. It's easy to check inductively that

$$\delta(M/(x_1, \ldots, x_n)) \geq \delta(M) - n.$$

Now, we get our result from the Proposition. □

dt-nzd-dim-dec-by-one

Corollary 6.2.12. *If $x \notin \mathcal{Z}(M)$, then* $\dim M/xM = \dim M - 1$.

Proof. From the last Corollary, it follows that we only have to show $\dim M/xM < \dim M$. Since $x \notin \mathcal{Z}(M)$, it follows that $x \notin \mathcal{Z}(R/\operatorname{ann}(M))$, and so x is not in any minimal prime over $\operatorname{ann}(M)$. We showed in (2.3.15) that

$$V(\operatorname{ann}(M/xM)) = V((x) + \operatorname{ann}(M)).$$

Hence, the primes minimal over $\operatorname{ann}(M/xM)$ are precisely the primes minimal over $(x) + \operatorname{ann}(M)$. Since x is not in any minimal prime over $\operatorname{ann}(M)$, this implies that

every minimal prime over $\operatorname{ann}(M/xM)$ has height at least 1 in $R/\operatorname{ann}(M)$. This shows that

$$\dim(M/xM) = \dim(R/\operatorname{ann}(M/xM)) < \dim(R/\operatorname{ann}(M)) = \dim M.$$

□

REMARK 6.2.13 (Warning). This is only true when R is a semilocal ring. For a counterexample, consider the ring $R = k[u,v,w]/(uv,uw)$, and let $x = u-1$. Then

$$R/(u-1) = k[u,v,w]/((u-1)+(uw,vw)) = k[u,v,w]/(u-1,v,w) = k.$$

So we see that $\dim R = 2$ (the prime (u,v) has height 2), while $\dim R/(u-1) = 0$. The geometric picture here should be clear.

The next Corollary finishes what we started in (2.3.24), and shows that the degree of the Samuel polynomial is indeed a very coarse invariant.

-of-defn-supp-dependence

COROLLARY 6.2.14. *Let R be any Noetherian ring (not necessarily semilocal), let M be a finitely generated R-module, and let $\mathfrak{q} \subset R$ be an ideal of definition for M. Then the degree of the Samuel polynomial $\chi_M^{\mathfrak{q}}$ depends only on the finite set* $\operatorname{Supp} M \cap V(\mathfrak{q})$.

PROOF. We showed in (2.3.24) that the degree depended on *both* the set $\operatorname{Supp} M \cap V(\mathfrak{q})$, and the module M. We remove the dependence on the module now.

First, we will show that

$$\deg \chi_M^{\mathfrak{q}} = \deg \chi_{R/\operatorname{ann}(M)}^{\mathfrak{q}}. \tag{1}$$

From (2.3.23) (and using the notation therein), we see that

$$\deg \chi_M^{\mathfrak{q}} = \max_{1 \le i \le r} \{\deg \chi_{M_i}^{\mathfrak{q}_i}\}.$$

So, to prove our statement, by replacing R by $(R/\operatorname{ann}(M))_{\mathfrak{m}_i}$, we can assume that $(R,\mathfrak{m})$ is a local ring, that $\mathfrak{q} \subset \mathfrak{m}$ is a primary ideal and that M is a faithful R-module. In this case, observe that we have

$$\deg \chi_M^{\mathfrak{q}} = \dim M = \dim R = \deg \chi_R^{\mathfrak{q}}.$$

Now, suppose $\operatorname{Supp} M \cap V(\mathfrak{q}) = \operatorname{Supp} M' \cap V(\mathfrak{q})$, for some other finitely generated R-module M'. In this case, we see that

$$V(\operatorname{ann}(M)+\mathfrak{q}) = V(\operatorname{ann}(M/\mathfrak{q}^n M)) = V(\operatorname{ann}(M'/\mathfrak{q}^n M')) = V(\operatorname{ann}(M')+\mathfrak{q})$$

and so

$$\operatorname{rad}(\operatorname{ann}(M)+\mathfrak{q}) = \operatorname{rad}(\operatorname{ann}(M')+\mathfrak{q}).$$

This, by an argument similar to the one in (2.3.24), will show that

$$\deg \chi_{R/\operatorname{ann}(M)}^{\mathfrak{q}} \ge \deg \chi_{R/\operatorname{ann}(M')}^{\mathfrak{q}},$$

and the other inequality will follow by symmetry. This, coupled with equation (1) above, gives us what we wanted. □

3. Regular Local Rings

Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then, by (6.2.8), $\dim R$ is the smallest number of elements generating an $\mathfrak{m}$-primary ideal.

DEFINITION 6.3.1. Let $(R, \mathfrak{m})$ be a Noetherian local ring; then the number $\varepsilon(R) = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) - \dim R$ is called the *embedded dimension* of R.

A Noetherian local ring $(R, \mathfrak{m})$ is *regular* if $\mathfrak{m}$ can be generated by $\dim R$ many elements; that is, if it has embedded dimension 0.

dt-regular-local-domain

PROPOSITION 6.3.2. *Every regular local ring is an integral domain.*

PROOF. Let R be a regular local ring. We'll prove the statement by induction on $\dim R$. If $\dim R = 0$, then $\mathfrak{m} = 0$, and so R is a field.

Now, suppose $\dim R > 1$, and let $P_1, \ldots, P_s$ be the minimal primes of R. Then, we can find

$$x \in \mathfrak{m} \setminus ((\bigcup_i P_i) \cup \mathfrak{m}^2).$$

Consider $R' = R/(x)$: we claim that $R/(x)$ is regular of dimension $\dim R - 1$. That it has dimension $\dim R - 1$ is clear by the Hauptidealsatz, and it's regular follows from the fact that if $\mathfrak{n} \subset R/(x)$ is the maximal ideal, then we have:

$$\mathfrak{n}/\mathfrak{n}^2 \cong \mathfrak{m}/\mathfrak{m}^2 + (x)$$

as $R/\mathfrak{m} = R/\mathfrak{n}$-vector spaces. If $x \notin \mathfrak{m}^2$, then $\mathfrak{m}^2 + (x) \neq \mathfrak{m}^2$, and so $\mathfrak{n}/\mathfrak{n}^2$ has dimension at most $\dim R - 1$; but it always has dimension at least that.

So, by induction, $R/(x)$ is an integral domain. This means that $(x) \subset R$ is prime. Since x is not in any minimal prime, we see by (6.1.5) that $\mathrm{ht}(x) = 1$. So there is some minimal prime $P \subset (x)$. Suppose $xa \in P$; since $x \notin P$, we see that $a \in P$. But then $P = xP$, which, by Nakayama's lemma, implies that $P = 0$. This shows that R is also a domain. □

REMARK 6.3.3. We'll show later in Chapter 12 that regular local rings are in fact UFDs. We'll also give a much more powerful homological characterization of regular local rings than the one we have in the following Theorem.

r-local-characterization

THEOREM 6.3.4. *The following are equivalent for a Noetherian local ring* $(R, \mathfrak{m})$*:*

1. R *is regular.*
2. $\mathfrak{m}$ *can be generated by a minimal system of parameters.*
3. *The* $R/\mathfrak{m}$*-vector space* $\mathfrak{m}/\mathfrak{m}^2$ *has dimension* n*.*
4. *The natural map* $(R/\mathfrak{m})[t_1, \ldots, t_n] \longrightarrow \mathrm{gr}_{\mathfrak{m}}(R)$ *is an isomorphism.*
5. $\hat{R}$ *is regular.*

PROOF. We only prove (1) $\Leftrightarrow$ (4) $\Leftrightarrow$. By (2.3.25), we see that (4) holds if and only if $\Delta^n \chi_R^{\mathfrak{m}} = l(R/\mathfrak{m}) = 1$. Assume (1) is true; then, by (6.2.8), we see that $\deg \chi_R^{\mathfrak{m}} = d(R) = n$. From this, it's clear that $\Delta^n \chi_R^{\mathfrak{m}} \geq 1$, since it's integer valued and positive (recall that it's the leading coefficient of $\chi_R^{\mathfrak{m}}$). The other inequality follows from (2.3.25). So we see that (1) $\Rightarrow$ (4).

Now, assume (4) holds; then, in particular, $\dim \mathfrak{m}/\mathfrak{m}^2 = n$, the number of monomials of degree 1. That is, (4) $\Rightarrow$ (3).

For (5) $\Leftrightarrow$ (4), observe that we have a natural isomorphism $\mathrm{gr}_{\mathfrak{m}}(R) \cong \mathrm{gr}_{\hat{\mathfrak{m}}}(\hat{R})$ of graded $R/\mathfrak{m}$-algebras. □

4. Dimension Theory of Graded Modules

The next Theorem contains most of what can be said at this point about the dimension theory of graded modules.

dimension-graded-modules

THEOREM 6.4.1. *Let M be a finitely generated graded module over a graded Noetherian ring R, and let $\mathfrak{p} \subset R$ be a prime in* $\operatorname{Supp} M$.

(1) *If $\mathfrak{p}$ is homogeneous, then we can find a chain of homogeneous primes in* $\operatorname{Supp} M$ *descending from $\mathfrak{p}$ of length d, where $d = \operatorname{ht} \mathfrak{p}$.*
(2) *If $\mathfrak{p}$ is not homogeneous, then* $\dim M_{\mathfrak{p}} = \dim M_{\mathfrak{p}^*} + 1$.

PROOF. First we prove a preliminary fact: for every non-homogeneous prime $\mathfrak{p} \subset R$, $\operatorname{ht} \mathfrak{p}/\mathfrak{p}^* = 1$. Indeed, by quotienting out by $\mathfrak{p}^*$ and taking the graded localization of R at $\mathfrak{p}$, we can assume that R is a graded ring where every homogeneous element is invertible. Therefore, by (1.2.5), we find that $R = k$ or $R = k[t, t^{-1}]$, for some field k. Since $\mathfrak{p} \subset R$ is a non-zero ideal, we must have $R = k[t, t^{-1}]$, and so $\dim R = 1$, which gives us our claim.

Now, since $\dim M = \dim R/\operatorname{ann}(M)$ and $\dim M_{\mathfrak{p}} = \operatorname{ht} \mathfrak{p}/\operatorname{ann}(M)$, for any prime $\mathfrak{p} \in \operatorname{Supp} M$, we can restrict our attention to the case $M = R$.

We will show that, for any prime $\mathfrak{p} \subset R$, with $\operatorname{ht} \mathfrak{p} = d$, there is a chain of length d

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_{d-1} \subsetneq \mathfrak{p}_d = \mathfrak{p},$$

with $\mathfrak{p}_i$ homogeneous for $0 \leq i \leq d-1$. This will prove both (1) and (2).

We'll do this by induction on d. If $d = 1$, then we can take $\mathfrak{p}_0 = \mathfrak{p}^*$. Suppose $d > 1$; then, by induction, we can find a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_{d-2} \subsetneq \mathfrak{p}_{d-1} \subsetneq \mathfrak{p}_d = \mathfrak{p},$$

where $\mathfrak{p}_i$ is homogeneous for $0 \leq i \leq d-2$. If $\mathfrak{p}$ is non-homogeneous, then we can replace $\mathfrak{p}_{d-1}$ by $\mathfrak{p}^*$. So we can assume that $\mathfrak{p}$ is homogeneous. In this case, by quotienting out by $\mathfrak{p}_{d-2}$, we can assume that R is a domain and show that, if $\operatorname{ht} \mathfrak{p} > 1$, then there exists another non-zero homogeneous prime $\mathfrak{q} \subsetneq \mathfrak{p}$. For this, choose any non-zero homogeneous element $a \in \mathfrak{p}$, and consider any prime $\mathfrak{q} \subset \mathfrak{p}$ that's minimal over a. Then, by the Hauptidealsatz, $\operatorname{ht} \mathfrak{q} \leq 1$; moreover, by (1.4.2), $\mathfrak{q}$ is homogeneous. □

dt-positively-graded

COROLLARY 6.4.2. *If R is a positively graded Noetherian ring and M is a finitely generated graded R-module, then*

$$\dim M = \sup\{\dim M_{\mathfrak{p}} : \mathfrak{p} \in \operatorname{Supp} M,\ \mathfrak{p} \text{ homogeneous}\}.$$

In particular, if $(R, \mathfrak{m})$ is a positively graded *local ring, then $\dim R = \dim R_{\mathfrak{m}}$.

PROOF. As in the proof of the Theorem, we can assume that $M = R$. Let $\mathfrak{m} \subset R$ be a maximal homogeneous prime. Since R is positively graded, $R/\mathfrak{m} = k$ (1.2.5). Hence $\mathfrak{m}$ is in fact a maximal ideal of R. Now, let $\mathfrak{p} \subset R$ be a maximal ideal such that $\dim R = \operatorname{ht} \mathfrak{p}$. If $\mathfrak{p}$ is homogeneous, then we're done; otherwise, we find from part (2) of the Theorem that $\operatorname{ht} \mathfrak{p}^* = \operatorname{ht} \mathfrak{p} - 1$. Since $\mathfrak{p}^*$ is not a maximal ideal, there is a homogeneous prime $\mathfrak{m}$ that strictly contains it. Then we see that $\operatorname{ht} \mathfrak{m} \geq \operatorname{ht} \mathfrak{p}^* + 1 = \dim R$. □

gebra-hilbert-polynomial

COROLLARY 6.4.3. *Let R be a positively graded ring finitely generated over $R_0 = k$ by R_1, with k a field. Then* $\dim R = 1 + \deg H(R, n)$, *where $H(R, n)$ is the Hilbert polynomial of R.*

PROOF. Let $\mathfrak{m} = R^+$ be the irrelevant ideal of R; then, by the Corollary above, $\dim R = \dim R_{\mathfrak{m}}$. We claim that $\operatorname{gr}_{\mathfrak{m}}(R) \cong R$; indeed, $\mathfrak{m}^n = \oplus_{m \geq n} R_m$, and so $\mathfrak{m}^n/\mathfrak{m}^{n+1} \cong R_n$. Now, since $\operatorname{gr}_{\mathfrak{m}}(R) \cong \operatorname{gr}_{\mathfrak{m}}(R_{\mathfrak{m}})$, we find that $H^{\mathfrak{m}}_{R_{\mathfrak{m}}}(n) = H(R, n)$. The result now follows from (6.2.8). □

DEFINITION 6.4.4. Let $(R, \mathfrak{m})$ be a local ring. If $\mathfrak{q} = (x_1, \ldots, x_n)$, and $\mathscr{B}(\mathfrak{q}, R)$ is the blow-up algebra associated to the $\mathfrak{q}$-adic filtration on R, then $x_1, \ldots, x_n$ are *analytically independent* if the kernel of the surjection

$$\begin{aligned} \psi_{\mathfrak{q}} : R[T_1, \ldots, T_n] &\to \mathscr{B}(\mathfrak{q}, R) \\ T_i &\to x_i t \end{aligned}$$

is contained in $\mathfrak{m}[T_1, \ldots, T_n]$.

dt-anal-ind-equiv

PROPOSITION 6.4.5. *Let $(R, \mathfrak{m})$ be a local ring, and let $x_1, \ldots, x_n$ be elements in $\mathfrak{m}$. Set $\mathfrak{q} = (x_1, \ldots, x_n)$; then the following are equivalent:*

(1) *$x_1, \ldots, x_n$ are analytically independent.*
(2) *The induced surjection*

$$(R/\mathfrak{m})[T_1, \ldots, T_n] \to \mathscr{B}(\mathfrak{q}, R)/\mathfrak{m}\mathscr{B}(\mathfrak{q}, R)$$

is an isomorphism.
(3) $\dim \mathscr{B}(\mathfrak{q}, R)/\mathfrak{m}\mathscr{B}(\mathfrak{q}, R) = \dim \operatorname{gr}_{\mathfrak{q}}(R)/\mathfrak{m} \operatorname{gr}_{\mathfrak{q}}(R) = n$.
(4) $\deg H\big(\mathscr{B}(\mathfrak{q}, R)/\mathfrak{m}\mathscr{B}(\mathfrak{q}, R), d\big) = \deg H\left(\operatorname{gr}_{\mathfrak{q}}(R)/\mathfrak{m} \operatorname{gr}_{\mathfrak{q}}(R), d\right) = n - 1$

PROOF. We'll show (1) ⇔ (2) ⇔ (3) ⇔ (4).

(1) ⇔ (2)**:** We have the following exact sequence:

$$0 \to \ker \psi_{\mathfrak{q}} \xrightarrow{i} R[T_1, \ldots, T_n] \xrightarrow{\psi_{\mathfrak{q}}} \mathscr{B}(\mathfrak{q}, R) \to 0.$$

Tensor this with $R/\mathfrak{m} = k$ to get an exact sequence

$$\ker \psi_{\mathfrak{q}} \otimes_R k \xrightarrow{i \otimes k} (R/\mathfrak{m})[T_1, \ldots, T_n] \to \mathscr{B}(\mathfrak{q}, R)/\mathfrak{m}\mathscr{B}(\mathfrak{q}, R) \to 0.$$

Now, $\operatorname{im}(i \otimes k) = 0$ if and only if $\operatorname{im} i \subset \mathfrak{m}[T_1, \ldots, T_d]$. From this the equivalence follows.

(2) ⇔ (3)**:** Clear. Use the isomorphism

$$\operatorname{gr}_{\mathfrak{q}}(R)/\mathfrak{m} \operatorname{gr}_{\mathfrak{q}}(R) \cong \mathscr{B}(\mathfrak{q}, R)/\mathfrak{m}\mathscr{B}(\mathfrak{q}, R).$$

(3) ⇔ (4)**:** Follows from (6.4.3).

□

analytically-independent

COROLLARY 6.4.6. *Every system of parameters of minimal length of a local ring $(R, \mathfrak{m})$ is analytically independent.*

PROOF. Let $x_1, \ldots, x_n \in R$ be a minimal system of parameters, so that $\dim R = n$, let $\mathfrak{q} = (x_1, \ldots, x_n)$, and let $\varphi(d)$ be the polynomial $H\left(\operatorname{gr}_{\mathfrak{q}}(R)/\mathfrak{m} \operatorname{gr}_{\mathfrak{q}}(R), d\right)$. We will show that $\deg \varphi = n - 1$. Consider the $R/\mathfrak{m}$-module $\mathfrak{q}^d/\mathfrak{m}\mathfrak{q}^d$: we find that, for d large enough, $\varphi(d) = l(\mathfrak{q}^d/\mathfrak{m}\mathfrak{q}^d)$ is the size of a minimal set of generators for $\mathfrak{q}^d$. We claim that we have the following inequality, for d large enough:

$$H^{\mathfrak{q}}_R(d) = l(\mathfrak{q}^d/\mathfrak{q}^{d+1}) \leq l(R/\mathfrak{q}) \cdot \varphi(d).$$

To prove the inequality, simply observe that we have a surjection $R^{\varphi(d)} \to \mathfrak{q}^d$, which induces a surjection $(R/\mathfrak{q})^{\varphi(d)} \to \mathfrak{q}^d/\mathfrak{q}^{d+1}$. Given this and the trivial observation that $\varphi(d) \leq H^{\mathfrak{q}}_R(d)$, we immediately deduce:

$$\deg \varphi = \deg H^{\mathfrak{q}}_R = n - 1.$$

□

5. Integral Extensions and the Going Up property

dt-secn:going-up
dt-defn-going-up

DEFINITION 6.5.1. We say that a map of rings $f : R \to S$ has the *going up property* when the following condition holds:

Given primes $\mathfrak{q} \subset S$ and $\mathfrak{p} \subset R$ such that $\mathfrak{q}^c = \mathfrak{p}$, and another prime $\mathfrak{p}^* \supsetneq \mathfrak{p}$, there is a prime $\mathfrak{q}^* \supset \mathfrak{q}$ such that $(\mathfrak{q}^*)^c = \mathfrak{p}^*$. In other words, the map $\operatorname{Spec} S/\mathfrak{q} \to \operatorname{Spec} R/\mathfrak{p}$ is surjective.

It has the *lying over* property if the map $\operatorname{Spec} S \to \operatorname{Spec} R/\ker f$ is surjective.

dt-defn-incomp

DEFINITION 6.5.2. We say that two primes $\mathfrak{p}_1, \mathfrak{p}_2 \subset R$ are *incomparable* if they are incomparable in the prime lattice of R.

A map of rings $f : R \to S$ has the *incomparability property* if, given a prime $\mathfrak{p} \subset R$, and two distinct primes $\mathfrak{q}_1, \mathfrak{q}_2 \subset S$ such that $\mathfrak{q}_i^c = \mathfrak{p}$, for $i = 1, 2$, $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are incomparable. In other words, all the primes in $S \otimes k(\mathfrak{p})$ are maximal.

dt-dim-equality-going-up

PROPOSITION 6.5.3. *If $f : R \to S$ is a map of rings with the going up property and the lying over property, then, for every ideal $I \subset S$, we have*

$$\dim S/I \geq \dim R/(I \cap R).$$

If, in addition, f has the incomparability property, then equality holds in the expression above.

PROOF. First, observe that if $f : R \to S$ has the going up property and the lying over property, then so does the map induced map $R/(I \cap R) \to S/I$, for any ideal $I \subset S$. Just note that if $\mathfrak{q} \in V(I)$ is a prime with $\mathfrak{q}^c = \mathfrak{p}$, then $\mathfrak{p} \in V(I \cap R)$.

So it suffices to show that $\dim S \geq \dim R/\ker f$. For this, just observe that the lying over property, along with the going up property, lets us extend any chain of primes in $R/\ker f$ to a chain of primes in S contracting to the same chain of primes in $R/\ker \phi$.

If, in addition, f has the incomparability property, then any strict chain of primes in S contracts to a strict chain of primes in $R/\ker \phi$, thus giving us also the reverse inequality. □

Observe that by (4), integral maps have all three properties. So we find

dt-dim-equality-integral

COROLLARY 6.5.4. *If $f : R \to S$ is an integral map of rings, then, for every ideal $I \subset S$, we have*

$$\dim S/I = \dim R/(I \cap R).$$

6. Dimensions of Fibers

dt-secn:fibers

We specialize further to the case of R a local, Noetherian ring, with maximal ideal $\mathfrak{m}$. Suppose $\phi : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a local homomorphism of local Noetherian rings. Then, the *fiber* over the maximal ideal $\mathfrak{m}$ is the quotient ring $S/\mathfrak{m}S$. It basically contains all the information about primes in S that contract to $\mathfrak{m}$.

dt-fiber-inequality

PROPOSITION 6.6.1. *If M is a finitely generated R-module, and N is a a finitely generated S-module, then:*

$$\dim_S M \otimes_R N \leq \dim_R M + \dim_S N/\mathfrak{m}N.$$

In particular,

$$\dim S \leq \dim R + \dim S/\mathfrak{m}S.$$

PROOF. Observe that for a prime $P \subset S$, $(M \otimes_R N)_P \neq 0$ if and only if $M_{P^c} \neq 0$ and $N_P \neq 0$. So $\operatorname{ann}(M)S + \operatorname{ann}(N) \subset P$, and we see that

$$\dim_S(M \otimes_R N/\operatorname{ann}(M)N) = \dim S'.$$

where $S' = S/(\operatorname{ann}(M)S + \operatorname{ann}(N))$. Also, $(N/\mathfrak{m}N)_P \neq 0$ if and only if $N_P \neq 0$ and $\mathfrak{m} \subset P$. Hence

$$\dim_S(N/\mathfrak{m}N) = \dim S/(\mathfrak{m}S + \operatorname{ann}(N)) = \dim S'/\mathfrak{m}S'.$$

So if we replace S with S' and R with $R/\operatorname{ann}(M)$, then we're reduced to showing the second assertion of the Proposition. Let $\mathfrak{q}$ be an ideal of definition for R, and let $\mathfrak{q}^* \supset \mathfrak{m}S$ be an ideal in S that descends to an ideal of definition for $S/\mathfrak{m}S$. Then, there are $n, m \in \mathbb{N}$ such that $\mathfrak{m}^n \subset \mathfrak{q}$ and $\mathfrak{n}^m \subset \mathfrak{q}^* + \mathfrak{m}S$. But then $\mathfrak{n}^{n+m} \subset \mathfrak{q}^* + \mathfrak{q}$, and so we see that $\mathfrak{q}^* + \mathfrak{q}$ is an ideal of definition for S. This shows that

$$\delta(S) \leq \delta(R) + \delta(S/\mathfrak{m}S),$$

and finishes our proof. □

With this in hand, we will investigate the dimensions of polynomial rings over Noetherian rings in the next series of results.

LEMMA 6.6.2. *If k is a field, then* $\dim k[x] = 1$.

PROOF. Since $k[x]$ is a PID, by Krull's theorem, every prime in $k[x]$ has height at most 1. On the other hand, (x) is a prime of height at least 1. Hence the result. □

dt-polynom-dim

PROPOSITION 6.6.3. *Let R be a Noetherian ring; then*

$$\dim R[x_1, \ldots, x_n] = \dim R + n,$$

where $R[x_1, \ldots, x_n]$ is the polynomial ring in n variables over R.

PROOF. It suffices to show that $\dim R[x] = \dim R + 1$. For any ring R, if we have a chain of primes

$$P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_r$$

in R, then we get a longer chain of primes in $R[x]$ of the form

$$P_0[x] \subsetneq P_1[x] \subsetneq \ldots \subsetneq P_r[x] \subsetneq (x) + P_r[x]$$

So we see that $\dim R[x] \geq \dim R + 1$. We just need to prove the reverse inequality.

First assume that R is local with maximal ideal $\mathfrak{m}$, and let $\mathfrak{q} \subset R[x]$ be any maximal ideal contracting to $\mathfrak{m}$. Then, by (6.6.1), we have

$$\begin{aligned}
\dim R[x]_{\mathfrak{q}} &\leq \dim R + \dim(R[x]_{\mathfrak{q}}/\mathfrak{m}R[x]_{\mathfrak{q}}) \\
&= \dim R + \dim(R/\mathfrak{m}[x])_{\mathfrak{q}} \\
&= \dim R + \dim k[x] \\
&= \dim R + 1,
\end{aligned}$$

where k is the residue field of R.

Now we discard the assumption of locality. If $\mathfrak{p} \subset R$ is any maximal prime, and $\mathfrak{q} \subset R[x]$ is a prime contracting to $\mathfrak{p}$, then by the argument above, we see that

$$\dim R[x]_{\mathfrak{q}} \leq \dim R_{\mathfrak{p}} + 1 \leq \dim R + 1.$$

Since this is true for any such maximal ideal $\mathfrak{q}$, the reverse inequality holds, and so we're done. □

7. The Going Down property

dt-subsecn:flat

If a map between rings has the going down property, then we can be more precise in our study of the dimensions of fibers. See (3.6.7) for the definition of the going down property. We have already encountered examples of families of maps that enjoy going down in (3.6.8) and (4.6.3).

Here's a stronger version of (6.6.1) with this constraint in hand.

oing-down-fiber-equality

PROPOSITION 6.7.1. *If $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a local homomorphism of local Noetherian rings with the going down property, then*

$$\dim S = \dim R + \dim S/\mathfrak{m}S.$$

PROOF. It suffices to show that $\dim S \geq \dim R + \dim S/\mathfrak{m}S$. Let

$$P_0 \subsetneq \ldots \subsetneq P_r = \mathfrak{m}$$

be a maximal chain of primes in R. Then, the going down property implies that we can find a chain

$$Q_0 \subsetneq \ldots \subsetneq Q_r$$

of primes in S with $Q_i^c = P_i$ and such that Q_r is a minimal prime over $\mathfrak{m}S$ with $\dim S/Q_r = \dim S/\mathfrak{m}S$. This gives us the inequality we need. □

dt-flat-fiber-equality

PROPOSITION 6.7.2. *Suppose $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a local homomorphism of local, Noetherian rings, and suppose M is a finitely generated module over R, and N is a finitely generated S-module that's flat over R. Then, we have:*

$$\dim_S M \otimes_R N = \dim_R M + \dim_S N/\mathfrak{m}N.$$

In particular, if f is a flat map, then

$$\dim S = \dim R + \dim S/\mathfrak{m}S.$$

PROOF. Note that N is in fact faithfully flat, since, for any prime $\mathfrak{p} \in \operatorname{Spec} R$, we have $\mathfrak{p}N \subset \mathfrak{m}N \neq N$, by Nakayama's lemma. By the same argument as in the proof of (6.6.1), we end up having to show

$$\dim S' = \dim R' + \dim S'/\mathfrak{m}S',$$

where $S' = S/(\operatorname{ann}(M)S + \operatorname{ann}(N))$ and $R' = R/\operatorname{ann}(M)$. Moreover, $\operatorname{Spec} S' = \operatorname{Supp} N'$, where $N' = N \otimes R'$. Now, N' is a flat R'-module, and it's faithfully flat by (3.6.3). Thus, by (3.6.8), going down holds, and we're done, by Proposition (6.7.1). □

COROLLARY 6.7.3. *For any local ring R, and any finitely generated R-module M, we have*

$$\dim_R M = \dim_{\hat{R}} \hat{M}.$$

PROOF. Follows from the Proposition, the fact that $\hat{R}$ is flat over R with

$$\dim \hat{R}/\mathfrak{m}\hat{R} = \dim R/\mathfrak{m}R = 0,$$

and the other fact that $\hat{M} = M \otimes \hat{R}$. □

Another class of maps that satisfies the Going Down property is the class of integral extensions $f : R \hookrightarrow S$, where both R and S are domains, and R is normal. See (4.6.3).

dt-normal-fiber-equality

PROPOSITION 6.7.4. *If $f : (R, \mathfrak{m}) \hookrightarrow (S, \mathfrak{n})$ is an integral extension of local rings with R, S domains, and R normal, then*

$$\dim S = \dim R + \dim S/\mathfrak{m}S.$$

PROOF. Follows immediately from the comment just above and (6.7.1). □

CHAPTER 7

Invertible Modules and Divisors

chap:im

1. Locally Free Modules

In this section, we'll look at some characterizations of locally free R-modules that are analogous to those of locally free *sheaves* over a locally ringed space (see [RS, 5.1]). We'll see that these modules are the same as projective modules when they're finitely presented.

DEFINITION 7.1.1. A *locally free module* is an R-module M such that for every prime $P \subset R$, $M_P \cong R_P^n$, for some $n \in \mathbb{N}$ (not necessarily the same n for all P!).

The next Proposition gives the first hint of the general philosophy of equivalence between vector bundles and projective modules. See [AG, **??**] for the algebro-geometric situation.

im-proj-iff-locfree

PROPOSITION 7.1.2. *A finitely presented R-module M is projective iff it is locally free.*

We'll actually present two proofs of this. The first proof is based on the following Lemma.

im-fingen-proj-locfree

LEMMA 7.1.3. *Any finitely generated projective R-module M is locally free.*

PROOF. It clearly suffices to show that any finitely generated projective module over a local ring is free. So assume R is local with maximal ideal $\mathfrak{m}$. Choose a minimal generating set $\{m_i : 1 \leq i \leq n\}$ for M (namely, one that induces a basis for $M/\mathfrak{m}M$), and consider the map $\phi : R^n \to M$ that takes the standard ordered basis $\{e_i\}$ of R^n to $\{m_i\}$. Since this map induces an isomorphism $(R/\mathfrak{m})^n \to M/\mathfrak{m}M$, we see that $\ker\phi \subset \mathfrak{m}R^n$. But since M is projective, we have a splitting map $\psi : M \to R^n$ such that

$$M = \operatorname{im}\psi \oplus \ker\phi = \operatorname{im}\psi + \mathfrak{m}M,$$

which, by Nakayama, implies that $\ker\phi = 0$. Thus, ϕ is an isomorphism, and M is free. □

REMARK 7.1.4. It is a theorem of Kaplansky that *any* projective R-module is locally free.

PROOF OF PROPOSITION (7.1.2). Here are the two proofs:

Proof 1: We get one direction from the Lemma above. Suppose now that M is a locally free R-module; then, by (3.1.12), all the localizations of the functor $\operatorname{Hom}_R(M, \_\_)$ are exact, and hence $\operatorname{Hom}_R(M, \_\_)$ is itself exact, telling us precisely that M is projective.

Proof 2: Using (3.3.4), we find that a finitely presented R-module M is flat if and only if it is projective. From (3.3.7), we find that a finitely generated R-module M is flat if and only if it is locally free.

□

There's actually a characterization of projectives, where we'll only have to check *finitely* many localizations. This has a tight connection with [RS, 5.8], where we prove something similar for locally free sheaves (the statements are actually equivalent on the affine scheme Spec R).

Before we do that, we need two lemmas, the first of which is in fact entirely analogous to part (4) of [RS, 4.14].

im-stalkfree-locfree

LEMMA 7.1.5. *Suppose M and N are finitely presented R-modules, with $M_P \cong N_P$, for some prime $P \subset R$. Then, we can find $f \in R \setminus P$ such that $M_f \cong N_f$.*

PROOF. Suppose we have an isomorphism $\phi : M_P \to N_P$. Then, from Lemma (3.1.12), we can find $\psi : M \to N$ and $s \in R \setminus P$ such that $\phi = \psi_P/s$. Let $\{n_i\}$ be a set of generators for N, and let $\{m_j\}$ be a set of generators for M. Then, we can find $a_{ij} \in R$, $b_{ij} \in R \setminus P$, such that

$$s^{-1}\psi_P(\sum_j \frac{a_{ij}}{b_{ij}} m_j) = \phi(\sum_j \frac{a_{ij}}{b_{ij}} m_j) = n_i$$

for all i.

If $g = s\prod_{i,j} b_{ij}$, then we see immediately that $\psi_g : M_g \to N_g$ is surjective. Similarly, we can find $\eta : N \to M$ and $h \in R \setminus P$ such that $\eta_h : N_h \to M_h$ is surjective. Then, if $f = gh$, we see that the maps $(\psi\eta)_f : M_f \to M_f$ and $(\eta\psi)_f : N_f \to N_f$ are both surjective. Since any surjective endomorphism of a finitely generated module is an isomorphism, we see that ψ_f must be in fact an isomorphism. □

loc-criterion-generators

LEMMA 7.1.6. *Suppose $R = (f_1, \ldots, f_n)$. Let P be any R-module and let $\phi : M \to N$ be a map of R-modules. Then the following statements hold:*

1. *$P = 0$ iff $P_{f_i} = 0$, for all i.*
2. *ϕ is injective iff ϕ_{f_i} is injective, for all i.*
3. *ϕ is surjective iff ϕ_{f_i} is surjective, for all i.*
4. *ϕ is an isomorphism iff ϕ_{f_i} is an isomorphism for all i.*

PROOF. It's enough to prove (1), since (2) and (3) follow from applying (1) to the cases where $P = \ker\phi$ and $P = \operatorname{coker}\phi$, respectively, and (4) is just (2) and (3) put together.

So assume $P_{f_i} = 0$, for all i. Then, for any $p \in P$, there is a power f_i^r of f_i such that $f_i^r p = 0$. Since, for any $r \in \mathbb{N}$, we have $R = (f_1^r, \ldots, f_n^r)$, we see that $Rp = 0$, and thus $p = 0$. □

im-loc-free-nbd-free

PROPOSITION 7.1.7. *If M is a finitely presented R-module, then M is projective if and only if there are finitely many elements $f_1, f_2, \ldots, f_n \in R$ that generate R and are such that $M_{f_i} \cong R_{f_i}$, for all i.*

PROOF. First assume that we can find such f_i. In this case, we see by Lemmas (7.1.6) and (3.1.12) that the functor $\mathrm{Hom}_R(M, \_\_)$ is exact iff $\mathrm{Hom}_{R_{f_i}}(M_{f_i}, \_\_)$ is exact, for all i. Since M_{f_i} is free, the latter functors are all exact, and we're done.

Now, for the converse, by Lemma (7.1.5), we see that for every prime $P \subset R$, we can find $f_P \notin R \setminus P$ such that $M_{f_P} \cong R_{f_P}$. Since $(f_P : P \in \operatorname{Spec} R) = R$, we see that there must be finitely many f_P that generate R (Just pick the ones that appear in some expression of 1 in terms of the f_P). □

im-sec-inv-modules

2. Invertible Modules

In this section, we'll study the so-called invertible modules over a Noetherian ring, and show that there's a good reason they are called what they are.

See also [RS, 5.2] for an analogous treatment of invertible modules over coherent rings of sheaves.

All rings in this section will be Noetherian.

im-invertible-module

DEFINITION 7.2.1. An *invertible* module over R is a finitely generated, locally free module of rank 1. In other words, it's a finitely generated R-module M such that, for every prime $P \in \operatorname{Spec} R$, $M_P \cong R_P$.

NOTE ON NOTATION 8. We'll denote the dual of an R-module M, $\operatorname{Hom}_R(M, R)$ by M^*.

Here's a characterization of invertible modules that we'll actually use in this section.

im-dual-is-inverse

PROPOSITION 7.2.2. *An R-module M is invertible if and only if the natural map $\mu : M^* \otimes_R M \to R$, given by $\phi \otimes m \mapsto \phi(m)$, is an isomorphism.*

PROOF. First suppose that M is invertible. Then, for every prime $P \subset R$, we have the following commutative diagram

$$\begin{array}{ccc} M_P^* \otimes M_P & \xrightarrow{\mu_P} & R_P \\ \cong \downarrow & & \| \\ R_P^* \otimes R_P & \xrightarrow{\cong} & R_P \end{array}$$

So we see that μ_P is an isomorphism, for all P, and thus μ is itself an isomorphism.

Conversely, suppose μ is an isomorphism, and suppose

$$1 = \mu(\sum_i \phi_i \otimes m_i) = \phi_i(m_i).$$

Then, for every prime P, we can find an i such that $\phi_i(m_i) \notin P$. This means that $\phi_i(m_i)$ is a unit in R_P, which implies that we can find an element $u \in R \setminus P$ such that $(\phi_i)_P(um_i) = 1 \in R_P$. Set $a_i = um_i$; then we see that

$$M_P = \ker(\phi_i)_P \oplus R_P a_i,$$
$$M_P^* = \ker(a_i)_P \oplus R_P \phi_i$$

where we treat a_i as an element of M_P^{**}. Observe that

$$\mu_P(\ker(a_i)_P \otimes R_P a_i) = 0 = \mu_P(R_P \phi_i \otimes \ker(\phi_i)_P).$$

Since μ_P is an isomorphism, this implies that $\ker(a_i)_P = \ker(\phi_i)_P = 0$, because $R_P a_i \cong R_P \cong R_P \phi_i$. Hence, we see that $M_P = R_P a_i \cong R_P$. Moreover, if $M' = \sum_i R a_i$, then the inclusion $M' \hookrightarrow M$, localizes to an isomorphism at every prime,

and is thus itself an isomorphism. So we can conclude that M is a finitely generated R-module that's locally free of rank 1. In other words, M is invertible. □

Recall the discussion of invertible ideals of Dedekind domains in AM: there, we only talked about R-submodules of the quotient field $K(R)$, and defined the Picard group, etc., using only those. As it turns out, that's in fact sufficient even in our more general situation, since every invertible R-module is isomorphic to such an invertible ideal. Before we show that we need two preliminary lemmas.

im-sum-with-iso-iso

LEMMA 7.2.3. *Let $\phi : M \to N$ and $\psi : M \to N$ be two homomorphisms of finitely generated modules over a local Noetherian ring R with maximal ideal $\mathfrak{m}$. Then, if ϕ is an isomorphism and $\operatorname{im}\psi \subset \mathfrak{m}N$, $\phi + \psi$ is also an isomorphism.*

PROOF. As usual, this is just an application of Nakayama's lemma. We see that the map induced by $\phi + \psi$ from $M/\mathfrak{m}M$ to $N/\mathfrak{m}N$ is the same as the map induced by ϕ (since the map induced by ψ is identically 0) and is thus an isomorphism. This means that $\phi + \psi$ is surjective. But then $\phi^{-1}(\phi + \psi)$ is a surjective map from M to M and is thus an isomorphism (4.1.2). This implies that $\phi + \psi$ has trivial kernel, and is thus an isomorphism. □

im-semiloc-lochom-ext

LEMMA 7.2.4. *Suppose R is a Noetherian* semilocal ring*, a ring with only finitely many maximal ideals, say, $\{P_i : 1 \leq i \leq n\}$, and suppose M and N are finitely generated R-modules with local isomorphisms $M_{P_i} \cong N_{P_i}$, for all i. Then, in fact, $M \cong N$.*

PROOF. Let $\phi_i : M_{P_i} \to N_{P_i}$ be the isomorphism given by hypothesis. Then, by Lemma (3.1.12), there is a $\psi_i : M \to N$, and $a \notin P_i$ such that $(\psi_i)_P/a = \phi_i$. Since $a\phi_i$ is still an isomorphism, we may assume that $(\psi_i)_P = \phi_i$. Now, by Prime Avoidance, for each i, we can choose $r_i \in (\bigcap_{j \neq i} P_j) \setminus P_i$. Let $\psi = \sum_i r_i\psi_i$; then, for each i, $\psi_{P_i} = r_i\phi_i + \eta_i$, where $\operatorname{im}\eta_i \subset P_i N_{P_i}$, and $r_i\phi_i$ is an isomorphism. By the previous Lemma, this means that ψ_{P_i} is an isomorphism. Since this is true for all i, we see that ψ is also an isomorphism. □

DEFINITION 7.2.5. An *invertible fractional ideal* of R is an invertible R-submodule of $K(R)$.

im-invmod-submod-tqr

PROPOSITION 7.2.6. *Every invertible module M is isomorphic to an invertible fractional ideal of R.*

PROOF. First, we will show that $M \otimes K(R) \cong K(R)$. Recall that $K(R)$ is a Noetherian semi-local ring, whose maximal ideals are the the maximal associated primes of R. Thus, by the lemma (7.2.4) above, it suffices to show that $(M \otimes K(R))_{PK(R)} \cong K(R)_{PK(R)}$, for every maximal associated prime P of R. Note that for any homomorphism of rings $R \to S$, and any prime $Q \subset S$, with $Q^c = P$, we have $(M \otimes S)_Q \cong M_P \otimes_{R_P} S_Q$, for any R-module M. So the left hand side is just

$$M_P \otimes_{R_P} K(R)_{PK(R)} \cong R_P \otimes K(R)_{PK(R)} \cong K(R)_{PK(R)}.$$

Now, it suffices to show that the natural map $M \to M \otimes K(R)$ is a monomorphism. This can be checked locally, and here it's the map

$$R_P \to R_P \otimes K(R) \cong K(R)_P.$$

But this map is injective, since the map $R \to K(R)$ is. □

REMARK 7.2.7. The Proposition above says that every invertible R-module is isomorphic to an invertible fractional ideal of R.

rtible-fractional-ideals

PROPOSITION 7.2.8. *Let $I, J \subset K(R)$ be invertible fractional ideals.*

1. *The natural map $I \otimes_R J \to IJ$ is an isomorphism.*
2. *I contains a non-zero divisor of R.*
3. *If $u \in I \cap R$ is a non-zero divisor, and φ, ψ are two R-module maps from I to J such that $\varphi(u) = \psi(u)$, then in fact $\varphi = \psi$.*
4. *The natural map $I^{-1}J \to \mathrm{Hom}_R(I, J)$ taking a to the map $\varphi_a : t \mapsto ta$ is an isomorphism. In particular, $I^{-1} \cong I^*$.*
5. *If $L \subset K(R)$ is any R-module, then L is invertible if and only if $L^{-1}L = R$.*

PROOF. For (1), it suffices to show that for every prime P, the map

$$I_P \otimes J_P \to K(R)_P \to K(R_P)$$

is a monomorphism. So we might as well assume that R is local. Since $I \cong R \cong J$, we have $a \in I$, $b \in J$, both non zero divisors, such that $I = Ra$, $J = Rb$. Then,

$$I \otimes J = Ra \otimes Rb = R(a \otimes b)$$

maps to Rab. Since both a and b are non zero divisors, this is a monomorphism.

Suppose $I \cap R$ consists entirely of zero-divisors; then it's contained in some associated prime of R, and so there is $b \in R$ such that $R \cap I \subset \mathrm{ann}(b)$. Since I is finitely generated, we can find a non-zero divisor $u \in R$ such that $uI \subset R \cap I \subset \mathrm{ann}(b)$. But then I is itself annihilated by ub. Let P be a prime containing $\mathrm{ann}(ub)$; then $0 \neq ub/1 \in R_P$ is a zero-divisor of I_P, which contradicts the fact that $I_P \cong R_P$. Hence $I \cap R$ contains at least one non-zero divisor.

On to statement (3): since u is a non-zero divisor, it remains one on localization at any prime $P \subset R$. Also, to show that $\varphi = \psi$, it suffices, using (3.1.12), to show that they agree modulo every prime $P \subset R$. Thus, we can assume that R is local and that $I \cong R$. Observe that u goes to a non-zero divisor of R under this isomorphism. Hence, we're reduced to showing: if $\varphi, \psi : R \to K(R)$ are two maps that agree on a non-zero divisor u, then $\varphi = \psi$. This is simple: just observe that we have

$$u\varphi(1) = \varphi(u) = \psi(u) = u\psi(1),$$

and since u is a non-zero divisor, this tells us that $\varphi(1) = \psi(1)$, and so $\varphi = \psi$.

First, using (2), pick a non-zero divisor $u \in I \cap R$. If we pick non-zero $a \in I^{-1}J$; then $ua \neq 0$, and so the map φ_a is non-zero, implying that $a \mapsto \varphi_a$ is an injective map. To show that it's surjective, let $\varphi : I \to J$ be any R-module map, and let $w = u^{-1}\varphi(u)$. Then it follows from part (3) that $\varphi = \varphi_w$, since they both agree on u.

Assertion (4): If L is invertible, then (2) combined with (3) says

$$\begin{aligned} L^* \otimes_R L &\cong L^{-1} \otimes_R L \\ &\cong L^{-1}L = R. \end{aligned}$$

Conversely, suppose $L^{-1}L = R$. We may assume that R is local and show that $L \cong R$. But if R is local, then our hypothesis implies that there exist $v \in L^{-1}$ and $u \in L$ such that $vu \in R$ is a unit. Now we see that multiplication by v gives an isomorphism from L to R. □

DEFINITION 7.2.9. The *Picard group* $\mathrm{Pic}(R)$ is the group formed by isomorphism classes of invertible R-modules, with the group operation being given by tensor product. Note that I^* gives us the inverse to I.

The *group of Cartier divisors* $C(R)$ is the group formed by the invertible fraction ideals of R under the operation of multiplication. Note that I^{-1} is the inverse to I. An element of $C(R)$ is called, unsurprisingly enough, a *Cartier divisor*.

ard-grp-cartier-divisors

PROPOSITION 7.2.10. *Let R be a Noetherian ring.*

(1) *The natural map $C(R) \to \mathrm{Pic}(R)$ sending an invertible fractional ideal to its isomorphism class in $\mathrm{Pic}(R)$ is a surjective homomorphism of groups. Its kernel is isomorphic to $K(R)^*/R^*$, so that we have an exact sequence of groups*

$$1 \to R^* \to K(R)^* \to C(R) \to \mathrm{Pic}(R) \to 1.$$

(2) *$C(R)$ is generated by the invertible ideals of R; that is, by the invertible fractional ideals of R* contained *in R.*

PROOF. That the map in (1) is surjective follows from (7.2.6). To see that it is a homomorphism of groups we use (7.2.8) for the isomorphism $IJ \cong I \otimes_R J$, valid for any pair of fractional ideals I and J. Next, suppose we have an isomorphism $\varphi : I \xrightarrow{\cong} R$ from a fractional ideal I to R. We want to show that $I = uR$, for some element $u \in K(R)^*$. For this, note that every map from I to R is given by multiplication by an element $u \in I^{-1}$ (7.2.8), and so $\varphi(a) = ua$, for all $a \in I$. Suppose $\varphi^{-1}(1) = v \in I$; then we have $uv = 1$, and so $u \in K(R)^*$. But now, for all $a \in I^{-1}$, we have $u(va) = a$, and so $I = uR$, which is what we had wanted to show.

For (2), just note that, for every invertible fractional ideal $I \subset K(R)$, we can find $a \in R$ such that $aI \subset R$. Then $I = (a)^{-1}(aI)$ is expressible as a product of invertible ideals of R. □

3. Unique Factorization of Ideals

The aim of this section is to prove unique factorization of height 1 ideals in locally factorial rings.

DEFINITION 7.3.1. A ring R is said to have *unique factorization of height* 1 *ideals* if $C(R)$ is isomorphic to the free abelian group generated by the height 1 primes of R.

REMARK 7.3.2. In other words, R has unique factorization of height 1 ideals if every invertible fractional ideal can be expressed uniquely (up to multiplication by an element of $K(R)^*$) as a finite product of powers of height 1 primes in R. It is of course enough to have unique factorization for the invertible ideals of R.

We first present a useful criterion for a domain to be a UFD.

im-ufd-criterion

PROPOSITION 7.3.3. *A Noetherian domain R is a UFD iff every prime associated to a non zero principal ideal is principal iff every height* 1 *prime is principal.*

PROOF. Suppose R is a UFD, and $a \in R - 0$. Then we can express a uniquely as a product $u \prod_i p_i^{r_i}$, where u is a unit and $p_i \in R$ is irreducible, for each i. It is easy to see that we have the equality

$$(a) = \cap_i (p_i)^{r_i}$$

Now, if $Q \in \operatorname{Spec} R$ is associated to (a), then we can find $b \in R \setminus (a)$ such that $bQ \subset (a) = \cap_i (p_i)^{r_i}$. So $bQ \subset (p_i)^{r_i}$, for all i. This means that either $Q \subset (p_i)$, for some i, in which case $Q = (p_i)$, since $\operatorname{ht} Q \geq 1$ by the Hauptidealsatz. Or: $b \in (p_i)^{r_i}$, for all i, in which case $b \in (a)$, which is a contradiction. Hence, $\operatorname{Ass}(a) = \{(p_i)\}$, and every prime associated to (a) is principal.

Conversely, suppose R is such that every prime associated to a principal ideal is principal. Then, if $a \in R - 0$, any prime minimal over a will be principal, say it's (p), for some prime element p. In that case, since a is irreducible, we must have $a = up$, for some unit u, which means, of course, that (a) is itself prime.

The second equivalence follows from the corollaries to Krull's Theorem, (6.1.8) and (6.1.10). □

im-unique-factorization

THEOREM 7.3.4. *Let R be a Noetherian ring such that, for every maximal ideal $\mathfrak{m} \subset R$, $R_{\mathfrak{m}}$ is a UFD.*

1. *An ideal $I \subset R$ is invertible if and only if all the primes minimal over it have height 1; that is, if it has pure co-dimension 1.*
2. *R has unique factorization of height 1 ideals.*

PROOF. One direction of (1) follows immediately from (7.3.3). For the other, first suppose that $I \subset R$ is a prime of height 1. Then, for any maximal ideal $\mathfrak{m} \subset R$ containing I, $I_{\mathfrak{m}} \subset R_{\mathfrak{m}}$ is a height 1 prime and is thus principal, again, by (7.3.3). This of course immediately implies that I is invertible.

Now, let $I \subset R$ be an arbitrary ideal of pure co-dimension 1. We will show that we can express I as a product of primes of height 1. Since the product of invertible ideals is of course invertible, we will then have shown that I is invertible. To do this, let $I \subset R$ be a maximal ideal of pure co-dimension 1 not expressible as a product of height 1 primes. Pick $P \in \operatorname{Ass}(R/I)$, and consider the ideal $P^{-1}I$; this contains I, but if it were equal to I, then we would find from (4.2.2) that elements of P^{-1} are integral over R. But R is normal, since its localizations are normal (4.3.13), and so we would then have $P^{-1} \subset R$, which is absurd. Therefore $I \neq P^{-1}I$, and by the maximality of I, we can express $P^{-1}I$ as a product of the form $Q_1 \dots Q_r$, where the Q_i are primes of height 1. But then we find $I = PQ_1 \dots Q_r$, which is a contradiction.

We now move on to (2). Suppose we have two expressions of I as the product of height 1 primes:

$$I = \prod_{i=1}^{r} P_i^{k_i} = \prod_{j=1}^{s} Q_j^{l_j}.$$

We will show by induction on $d = \sum_i k_i$ that the two sides must be equal. If $d = 0$, then $I = R$, and we must have $s = 0$ also. If $r > 0$, then we have $P_j \subset Q_1$, for some j, since the product $\prod_j P_j \subset Q_1$. As both P_j and Q_1 are height 1 primes, it follows that $P_j = Q_1$. In this case, we can multiply both expressions by Q_1^{-1} to get

$$Q_1^{-1}I = P_j^{k_j - 1} \prod_{i \neq j} P_i^{k_i} = Q_1^{l_1 - 1} \prod_{m=2}^{s} Q_m^{l_m}.$$

By induction, the two expressions must both rearrangements of the products of the same prime powers, and so we're done. □

DEFINITION 7.3.5. Let R be as in the Theorem above; then, for all maximal ideals $P \subset R$, we will associate a function $v_P : C(R) \to \mathbb{Z}$ that sends every fractional invertible ideal I to the power of P appearing in its unique factorization into maximal ideals. We'll call this map the *valuation at* P.

4. Cartier and Weil Divisors

5. Discrete Valuation Rings and Dedekind Domains

im-serres-criterion

THEOREM 7.5.1 (Serre's Criterion). *A Noetherian ring is normal if and only if it satisfies the following conditions:*

R_1: *For $i \leq 1$, the localization of R at every height i prime is regular.*
S_2: *Every prime associated to* (0) *is minimal, and every prime associated to a non-zero divisor has height* 1.

PROOF. First, assume that R is normal. Then, by Proposition (4.3.20), it's a product of normal domains. Now, any localization of R at a prime is isomorphic to the localization of one of its factors at a prime. Given this, we see that we just have to show that a normal domain S satisfies conditions R_1 and S_2. The only prime $P \subset S$ of height 0 is the prime (0), and the localization at (0) is the fraction field $K(S)$ of S, which is regular. Now let $P \subset S$ be a height 1 prime; then (4.3.19) says that S_P is regular, since it has dimension 1 and its maximal ideal is principal. It remains to show that S2 holds. So let $P \subset S$ be a prime associated to (0); then since S is a domain, $P = (0)$, and $\operatorname{ht} P = 0$. If P is associated to a non-zero divisor, then (4.3.19) says that $\operatorname{ht} P = 1$.

Conversely, assume R satisfies the two conditions. Then it also satisfies R_0 and S_1, and hence by Serre's criterion for reducedness (4.3.4), it's reduced.

Now, observe that any localization of R also satisfies conditions R_1 and S_2, and, for any prime $P \subset R$, R_P is a domain. If it satisfies the two conditions, then it also satisfies the criterion given in Proposition (4.3.19), and hence is normal. Since R_P is normal for every prime $P \subset R$, this implies that R is also normal, by (4.3.13). □

REMARK 7.5.2. As one would expect, we can talk, more generally, about conditions R_n and S_n, for $n \in \mathbb{N}$. The formulation of R_n is obvious, but that of S_n is not quite so evident at this point. We'll define these conditions in Chapter 12 and show that they behave very well under flat extensions. In particular, we will find that normality and reducedness 'descend' down from faithfully flat extensions.

DEFINITION 7.5.3. A regular local ring $(R, \mathfrak{m})$ of dimension 1 is called a *discrete valuation ring* or a *DVR*

A domain R is a *Dedekind domain* if, for all primes $P \subset R$, R_P is a DVR. In particular, every non-zero prime in R is maximal.

im-dvr-characterization

THEOREM 7.5.4. *The following are equivalent for a one dimensional Noetherian local domain $(R, \mathfrak{m})$, with residue field $k = R/\mathfrak{m}$:*

(1) *R is a DVR.*
(2) *$\mathfrak{m}$ is principal.*
(3) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$
(4) $k[t] \cong \operatorname{gr}_{\mathfrak{m}}(R)$.
(5) *R is a principal ideal domain.*

(6) *There exists $\pi \in \mathfrak{m}$ such that every non-zero ideal of R is of the form (π^r), for some $r \in \mathbb{N}$.*
(7) *Every non-zero ideal in R is of the form $\mathfrak{m}^r$, for some $r \in \mathbb{N}$.*
(8) *Every fractional ideal of R is of the form $\mathfrak{m}^r$, for some $r \in \mathbb{Z}$.*
(9) *Every fractional ideal of R is invertible.*
(10) *R is a valuation ring.*
(11) *R is normal.*

PROOF. (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4) follows from (6.3.4). The implications (6) $\Rightarrow$ (7) $\Leftrightarrow$ (8) $\Rightarrow$ (9) are trivial, (10) $\Rightarrow$ (11) follows from (**??**), and (11) $\Leftrightarrow$ (1) follows from (7.5.1).

Now observe that every fractional ideal of R is invertible if and only if every ideal of R is invertible, and, since R is local, every ideal of R is invertible if and only if every ideal is principal. This gives us (5) $\Leftrightarrow$ (9). Also, if R is a PID, then we're in the situation of (7.3.4), from which (6) follows.

Thus we'll be done if we show (2) $\Rightarrow$ (6) and (6) $\Rightarrow$ (10). We'll do the first implication now. Let π be a generator of $\mathfrak{m}$, and let $\mathfrak{a} \subset R$ be a non-zero ideal. We can find $r \in \mathbb{N}$ such that $\pi^r \in \mathfrak{a}$, but $\pi^{r-1} \notin \mathfrak{a}$. We claim that $\mathfrak{a} = (\pi^r)$. Indeed, suppose we have $a \in \mathfrak{a} \setminus (\pi^r)$; then $a = u\pi^k$, for $k < r$, and $u \notin \mathfrak{m}$. But then $\pi^k \in \mathfrak{a}$, which is a contradiction.

Now for (6) $\Rightarrow$ (10): this is easy, since every element $x \in K(R)$ is of the form $u\pi^r$, where $u \in R \setminus \mathfrak{m}$ and $r \in \mathbb{Z}$. Therefore, either $x \in R$ or $x^{-1} \in R$, which shows that R is a valuation ring. □

DEFINITION 7.5.5. A generator π of the maximal ideal $\mathfrak{m}$ in a DVR $(R, \mathfrak{m})$ is called a *uniformizer* for R.

edekind-characterization

THEOREM 7.5.6. *Let R be a one dimensional Noetherian domain. Then the following are equivalent:*

(1) *R is a Dedekind domain.*
(2) *R is normal.*
(3) *Every fractional ideal of R has a unique expression as a product of maximal ideals of R.*
(4) *Every fractional ideal of R is invertible.*

PROOF. Follows immediately from (7.5.4), since all the statements localize nicely. □

im-dedekind-flatness

PROPOSITION 7.5.7. *Let R be a Dedekind domain and let S be an R-algebra. Then the following are equivalent:*

(1) *S is flat over R.*
(2) *For every associated prime $Q \in \operatorname{Ass} S$, $Q \cap R = (0)$.*

PROOF. After localizing, we reduce immediately to the case where $(R, \mathfrak{m})$ is a DVR with uniformizer π. In this case, since R is a PID we have to show that $\pi \notin \mathcal{Z}(S)$ if and only if $Q \cap R = (0)$, for all associated primes $Q \subset S$ (We're using (3.2.2) here). But this is easy, since $\mathcal{Z}(S) = \bigcup_{Q \in \operatorname{Ass}(S)} Q$. □

m-dedekind-dedekind-flat

COROLLARY 7.5.8. *Let $R \subset S$ be an integral extension of Dedekind domains; then S is faithfully flat over R.*

PROOF. Since S is integral over R, for any maximal ideal $Q \subset S$, S/Q is integral over $R/(Q \cap R)$. But then $1 = \dim S/Q = \dim R/(Q \cap R)$, by (6.5.4), and so $Q \cap R \subset R$ is also a maximal ideal. Thus by the Proposition above S is flat over R. By lying over, we clearly have $PS \neq S$, for all primes $P \subset R$, and so S is in fact faithfully flat over R by (3.6.4). □

6. The Krull-Akizuki Theorem

rank-length-quotient-nzd

THEOREM 7.6.1. *Let R be a one dimensional domain, and let $x \in R$ be a non-zero element. For every torsion free R-module M, we have*

$$l(M/xM) \leq \mathrm{rk}(M) l(R/(x)),$$

with equality holding whenever M is finitely generated. Here $\mathrm{rk}(M) = \dim_{K(R)}(K(R) \otimes_R M)$.

PROOF. First assume that M is finitely generated. Let $r = \mathrm{rk}(M)$; if $r = \infty$, then there is nothing to show. Otherwise, we can find elements $m_1, \ldots, m_r \in M$ whose images form a $K(R)$-basis for $K(R) \otimes_R M$. Let $R^r \to M$ be the map induced by these elements; this map is injective, because its kernel is a torsion sub-module of R^r, which is of course torsion free. Let N be the cokernel of this map; then N is also finitely generated, and we have an exact sequence

$$0 \to R^r \to M \to N \to 0,$$

and tensoring with $R/(x)$ gives us another exact sequence

$$\mathrm{Tor}_1^R(M, R/(x)) \to \mathrm{Tor}_1^R(N, R/(x)) \to (R/(x))^r \to M/xM \to N/xN \to 0.$$

Since, for any R-module P, $\mathrm{Tor}_1^R(P, R/(x))$ is just the x-torsion of P, we see that we in fact have an exact sequence

$$0 \to (0 :_N x) \to (R/(x))^r \to M/xM \to N/xN \to 0$$

of $R/(x)$-modules of finite length. Thus we have

$$r \cdot l(R/(x)) + l(0 :_N x) = l(M/xM) + l(N/xN).$$

So to finish the proof in the case where M is finitely generated, we just have to show that $l(0 :_N x) = l(N/xN)$. But this follows from the exact sequence:

$$0 \to (0 :_N x) \to N \xrightarrow{x} N \to N/xN \to 0.$$

Now we can discard the assumption that M is finitely generated. First observe that for every finitely generated R-submodule $M' \subset M$, we have

$$l(M'/xM') \geq l((M' \cap xM)/xM).$$

Next note that we have

$$M/xM = \bigcup_{\substack{M' \subset M \\ M' \text{ finitely generated}}} (M' \cap xM)/xM.$$

Therefore, if $l(M/xM) > r \cdot l(R/(x))$, then it follows that we have some finitely generated R-submodule $M' \subset M$ such that

$$\begin{aligned} l(M'/xM') &\geq l((M' \cap xM)/xM) \\ &> r \cdot l(R/(x)) \\ &\geq \mathrm{rk}(M') l(R/(x)), \end{aligned}$$

which contradicts the paragraph above that dealt with finitely generated R-modules. □

al-intersect-non-trivial

LEMMA 7.6.2. *Let R and S be domains such that $K(S)/K(R)$ is an algebraic extension. Then, for every ideal $J \subset S$, $J \cap R \neq 0$.*

PROOF. It suffices to prove this for principal ideals. Pick $s \in S$ and let $p(t) \in R[t]$ be an irreducible polynomial such that $p(s) = 0$. Then we see that the constant term of $p(t)$ (which is necessarily non-zero) is in the ideal generated by s and lies in R. □

im-krull-akizuki

COROLLARY 7.6.3 (Krull-Akizuki). *Let R be a one dimensional Noetherian domain, let $L/K(R)$ be a finite extension of fields, and let $S \subset L$ be a sub-ring containing R. Then, for any non-zero ideal $J \subset S$, S/J has finite length. In particular, S is Noetherian of dimension at most* 1.

PROOF. Since S is torsion free as an R-module, we see that $K(R) \otimes_R S$ is a $K(R)$-subspace of $K(S)$, and thus has finite dimension over $K(R)$. So we see that $\mathrm{rk}(S)$ is finite. Moreover, if $J \subset S$ is any non-zero ideal, by the lemma above, we can find a non-zero element $x \in J \cap S$. Thus by (7.6.1) we have

$$\begin{aligned} l(S/J) &\leq l(S/xS) \\ &\leq \mathrm{rk}(S) l(R/(x)) < \infty. \end{aligned}$$

Given this, we immediately find that any non-zero ideal must be finitely generated, and also that S has dimension at most 1. □

ntegral-closure-dedekind

COROLLARY 7.6.4. *Let R be a one dimensional Noetherian domain, and let $L/K(R)$ be a finite extension of fields. Then the integral closure of R in L is a Dedekind domain.*

PROOF. Let S be the integral closure of R in L; then, from the above Corollary, we find that S is Noetherian and thus it also has dimension 1 by (6.5.4). The statement now follows from (7.5.6). □

7. Grothendieck Groups

All our rings in this section will be Noetherian.

DEFINITION 7.7.1 (General Grothendieck Construction). Let $\mathscr{C}$ be an abelian category, and let $\mathscr{D}$ be a sub-category of $\mathscr{C}$ with a small skeleton. Let $C(\mathscr{D})$ be the set of isomorphism classes of objects in $\mathscr{D}$, and let $F(\mathscr{D})$ be the free abelian group generated by $C(\mathscr{D})$. We denote by $E(\mathscr{D})$ the sub-group of $F(\mathscr{D})$ generated by elements of the form $[M'] - [M] + [M'']$, where

$$0 \to M' \to M \to M'' \to 0$$

is an exact sequence of objects in $\mathscr{D}$. The *Grothendieck group* $K(\mathscr{D})$ is the quotient $F(\mathscr{D})/E(\mathscr{D})$.

The natural map $C(\mathscr{D}) \to K(\mathscr{D})$ is denoted $\gamma_{\mathscr{D}}$.

ndieck-grp-universal-prp

PROPOSITION 7.7.2. *Let $\mathscr{C}$ be an abelian category and let $\mathscr{D}$ be a sub-category of $\mathscr{C}$ with a small skeleton with Grothendieck group $K(\mathscr{D})$. Then, for every additive function λ from $\mathscr{D}$ to a group G, there exists a unique homomorphism $\widetilde{\lambda} : K(\mathscr{D}) \to G$ such that $\lambda(M) = \widetilde{\lambda}(\gamma_{\mathscr{D}}([M]))$.*

PROOF. Immediate from the definition. □

DEFINITION 7.7.3. A subset $\Gamma \subset C(\mathscr{D})$ is said to be a *generating subset* if it contains 0, and if, for any object A in $\mathscr{D}$, there exists a finite, separated filtration $F^\bullet A$ of A such that, for every $r \in \mathbb{N}$, there exists an element $[A_r]$ in Γ such that $[A_r] = [F^r A/F^{r+1}A]$.

ndieck-generating-subset

PROPOSITION 7.7.4. *With the notation as in the definition above, for any generating subset $\Gamma \subset C(\mathscr{D})$, $K(\mathscr{D})$ is generated by elements of the form $\gamma_{\mathscr{D}}([A])$, for $[A] \in \Gamma$).*

PROOF. Clear. □

7.1. Finitely Generated Modules.

DEFINITION 7.7.5. Let R be a Noetherian ring. If, in the Grothendieck construction, we take $\mathscr{C} = R$-mod and $\mathscr{D}$ to be the sub-category of finitely generated R-modules, then the Grothendieck group $K(\mathscr{D})$ is denoted $K(R)$. The natural map $\gamma_{\mathscr{D}}$ is denoted γ^R.

7.2. Projective Modules.

7.3. Flat Modules.

7.4. Modules of Finite Length over Dedekind Domains.

DEFINITION 7.7.6. Let R be a Noetherian ring. If, in the Grothendieck construction, we take $\mathscr{C} = R$-mod and $\mathscr{D}$ to be the sub-category of R-modules of finite length, then the Grothendieck group $K(\mathscr{D})$ is denoted $K_a(R)$ (the 'a' stand for Artinian). The natural map $\gamma_{\mathscr{D}}$ is denoted γ_a^R.

REMARK 7.7.7. It's easy to see that the set of objects $[R/\mathfrak{m}]$, where $\mathfrak{m}$ is a maximal ideal of R, is a generating subset.

im-euler-characteristic

PROPOSITION 7.7.8. *Let R be a Dedekind domain, and let* $\mathrm{Pic}(R)$ *be its Picard group. There is a unique isomorphism*

$$\chi : K_a(R) \xrightarrow{\cong} \mathrm{Pic}(R)$$

such that $\chi(\gamma_a^R[R/P]) = [P]$, where $[P]$ denotes the isomorphism class of invertible ideals that P belongs to.

PROOF. Let M be an R-module of finite length, and consider any composition series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_{r-1} \supsetneq M_r = 0,$$

where, for $0 \leq i < r$, $M_i/M_{i+1} \cong R/P_i$, for some maximal ideal $P_i \subset R$. By Jordan-Hölder the set $\{P_1, \ldots, P_r\}$ is uniquely determined by the isomorphism class of M, and so we can set $\psi([M]) = \prod_{i=1}^r [P_i]$. To determine if this gives us a well-defined homomorphism, it suffices to check that, for two maximal ideals $P, Q \subset R$, we have

$$\psi([R/P])\psi([R/Q]) = \psi([R/P] \oplus [R/Q]).$$

But this is obvious.

The map ψ is surjective, since $\mathrm{Pic}(R)$ is generated by the maximal ideals of R (7.5.6). Moreover, suppose we have an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of modules of finite length; then, since it's immediate that $\psi([M'])\psi([M'']) = \psi([M])$. Thus ψ is an additive map, and so factors through a unique homomorphism $\chi : K_a(R) \to \mathrm{Pic}(R)$ such that $\psi([M]) = \chi(\gamma_a^R([M]))$.

That χ is in fact injective follows $\square$

CHAPTER 8

Noether Normalization and its Consequences

chap:noeth

1. Noether Normalization

LEMMA 8.1.1. *Suppose k is a field and that $f \in T = k[x_1, \ldots, x_r]$ is a nonconstant polynomial. Then there are elements $y_1, \ldots, y_{r-1} \in T$ such that T is a finitely generated module over $k[y_1, \ldots, y_{r-1}, f]$. Moreover,*

1. *We can choose $y_i = x_i - x_r^{e^i}$, for any sufficiently large integer e.*
2. *If k is infinite, then, there is an open dense set $U \subset \mathbb{A}_k^{r-1}$, such that for all $(a_1, \ldots, a_{r-1}) \in U$, we may choose $y_i = x_i + a_i x_r$.*

PROOF. We'll show that f can be expressed as a polynomial in $y_1, \ldots, y_{r-1}, x_r$ that's monic in x_r. Thus, x_r will be integral over the subring $k[y_1, \ldots, y_{r-1}, f]$, and so T will be finitely generated over it in both cases (1) and (2).

1. Consider a monomial $x_1^{a_1} \ldots x_r^{a_r}$: when written in terms of the y_i, it becomes a polynomial of degree $d = a_r + \sum_{i=1}^{r-1} a_i e^i$ in x_r. If e is bigger than the exponents of any of the x_i appearing in f, then the expression we have for d is its expansion in base e. In particular, the degree of x_r corresponding to each monomial of f is uniquely determined by that monomial. Call this the x_r-weight of the monomial in f. Let $\mathbf{x^a}$ be the monomial in f with highest x_r-weight, say d; then we see that f, when expressed in terms of the y_i and x_r will be monic in x_r of degree d.
2. Let f have degree d, and let f_d be the sum of all the degree d monomials in f. If we write f in terms of the y_i, then we'll see that
$$f_d(y_1, \ldots, y_{r-1}, x_r) = \ldots + f_d(a_1, \ldots, a_{r-1}, 1)x_r^d.$$
So, for any $\mathbf{a} \in U = \{f_d(\mathbf{a}, 1) \neq 0\}$, we'll have an expression monic in x_r.

□

th-noether-normalization

THEOREM 8.1.2 (Noether Normalization). *Let R be an affine ring of dimension d over a field k. If $I_1 \subset \ldots \subset I_m$ is chain of ideals in R with $\dim R/I_j = d_j$ and $d_1 > \ldots > d_m$, then R contains a polynomial ring $S = k[x_1, \ldots, x_d]$ such that R is finite over S, and*
$$I_j \cap S = (x_{d_j+1}, \ldots, x_d).$$
If k is infinite, and $R = k[y_1, \ldots, y_r]$, then, for $j \leq d_m$, the x_j may be chosen to be k-linear combinations of the y_i.

er-normalization-domains

COROLLARY 8.1.3. *Let $R \subset S$ be a tower of domains, with S a finitely generated R-algebra. Then, there exist $a \in R$, and elements $x_1, \ldots, x_d \in S$ algebraically independent over $K(R)$ such that S_a is finite over $T = R_a[x_1, \ldots, x_d]$. If S is a graded R-algebra, then we may choose the x_i from among the homogeneous elements of S.*

PROOF. Suppose $S = R[y_1, \ldots, y_r]$; then

$$S' = K(R) \otimes_R S = K(R)[y_1, \ldots, y_r].$$

So, by Noether Normalization (with $I_m = 0$), we can find $x_1, \ldots, x_d \in S'$ algebraically independent (homogeneous, if S is graded over R) over $K(R)$ such that S' is finite over $T' = K(R)[x_1, \ldots, x_d]$. By multiplying the x_i by a suitable element in R, we can assume that they're in S. Now, suppose y_i satisfies a monic equation

$$y_i^n + p_{i,1}(x_1, \ldots, x_d)y_i^{n-1} + \ldots + p_{i,n} = 0$$

over T'.

Now, just take a to be the product of the denominators of the coefficients of all the $p_{i,k}$, to see that S_a is integral and finitely generated over T, and hence finite over T. □

In the next few sections we'll present some important consequences of Noether Normalization.

2. Generic Freeness

noeth-generic-freeness

THEOREM 8.2.1 (Generic Freeness). *Let R be a Noetherian domain, and let S be a finitely generated R-algebra. If M is a finitely generated S-module, then there exists an element $0 \neq a \in R$ such that M_a is a free R_a-module. If, in addition, S is positively graded, with R acting in degree 0, and if M is a graded S-module, then a may be chosen so that each graded component of M_a is free over R.*

PROOF. We'll do this by induction on $d = \dim K(R) \otimes_R S$. If $K(R) \otimes_R S = 0$, then there is some $0 \neq a \in \operatorname{ann}(S)$. In this case we also have $a \in \operatorname{ann}(M)$, and so $M_a = 0$ is free over $S_a = 0$. Suppose therefore that $d \geq 0$: in this case, by (8.1.3), there exists $0 \neq a \in R$ such that S_a is finite over some polynomial ring $R_a[x_1, \ldots, x_r]$. We also have:

$$d = \dim(K(R) \otimes_R S) = \dim(K(R)[x_1, \ldots, x_r]) = r.$$

So we can replace R with R_a, S with $R_a[x_1, \ldots, x_r]$ and M with M_a, and assume that $S = R[x_1, \ldots, x_d]$, where the x_i may be chosen to be homogeneous, if S is graded.Now, since M is finite over S, we can find a filtration:

$$M = M_n \supset M_{n-1} \supset \ldots \supset M_1 \supset M_0 = 0,$$

such that for all $1 \leq i \leq n$, $M_i/M_{i-1} \cong S'/Q_i$, for some prime $Q_i \subset S'$. If S and M are graded, then by (1.4.3), we may take Q to be homogeneous. If $Q_i \neq 0$, then $\dim K(R) \otimes (S/Q_i) < d$, and so, by the inductive hypothesis, there is $0 \neq a_i \in R$ such that $(S/Q_i)_{a_i}$ is free over R_{a_i} (in the graded case, we can ensure that each graded component is free over R_{a_i}). If $Q_i = 0$, then S is of course already free over R. In sum, we can find $a_1, \ldots, a_n \in R$ such that $M_{a_1 \cdots a_n}$ has a filtration by free $R_{a_1 \cdots a_n}$-modules. But then $M_{a_1 \cdots a_n}$ has to be free over $R_{a_1 \cdots a_n}$. We also get the analogue in the graded case by the same argument. □

3. Finiteness of Integral Closure

Here is an immediate consequence of Noether Normalization

ness-of-integral-closure

THEOREM 8.3.1. *Let R be a normal affine domain, and let $L/K(R)$ be a finite extension. Let $R' \subset L$ be the integral closure of R in L. Then R' is finite over R.*

PROOF. By Noether Normalization, R is finite over a polynomial ring $k[x_1, \dots, x_d]$; so we can assume that $R = k[x_1, \dots, x_d]$. Furthermore, we can replace L by its normal closure, and assume $L/K(R)$ is normal. Hence there is a tower of fields $K(R) \subset L' \subset L$, where $L'/K(R)$ is purely inseparable, and L'/L is Galois. Let S be the integral closure of R in L, and S' the integral closure of R in L'. By (4.3.23), S is finite over S'. So it suffices to show that S' is finite over R. Thus we can assume that L is a purely inseparable extension of $K(R) = k(x_1, \dots, x_d)$.

Now, since L is finite over $K(R)$, there exists $n \in \mathbb{N}$ such that $a^{p^n} \in K(R)$, for all $a \in L$, where $p = \operatorname{char} K(R)$. In particular, if $q = p^n$, then $L \subset k'(x_1^{1/q}, \dots, x_d^{1/q})$, where k' is obtained from k by adjoining the q^{th} roots of the coefficients of the minimal polynomials of the generators of $L/K(R)$. So it suffices to show that the integral closure of $k[x_1, \dots, x_d]$ in $k'(x_1^{1/q}, \dots, x_d^{1/q})$ is finitely generated. But the integral closure is simply $k'[x_1^{1/q}, \dots, x_d^{1/q}]$, which is definitely finite over R. □

The next Corollary uses a whole host of results from Chapter 5.

l-closure-laurent-series

COROLLARY 8.3.2. *Let k be an algebraically closed field of characteristic 0, and let $L = k((x))$ be the field of Laurent series over k. The algebraic closure of L is the field $\bigcup_{n=1}^{\infty} k((x^{1/n}))$, and the integral closure of $k[[x]]$ in $k((x^{1/n}))$ is $k[[x^{1/n}]]$.*

PROOF. We'll show that any finite extension of $k((x))$ is of the form $k((x^{1/n}))$ for some $n \in \mathbb{N}$. To show this, we'll show that the integral closure of $k[[x]]$ in any finite extension L of $k((x))$ is of the form $k[[x^{1/n}]]$, for some $n \in \mathbb{N}$. From this, all our assertions will follow.

Indeed, by the Theorem above, if T is the integral closure of $k[[x]]$ in L, then T is finite over $k[[x]]$ and is thus a Dedekind domain. By (**??**), since $k[[x]]$ is a complete DVR, T must also be one (that it's a DVR follows from (7.5.4)).

Let π be a uniformizer of T, and let $n \in \mathbb{N}$ and $u \in T \setminus (\pi)$ be such that $x = u\pi^n$. Since k is algebraically closed, $T/(\pi) = k$ (since it's finite over k), and the image of u in k has an n^{th}-root in k. Now, because $\operatorname{char} k = 0$, we can apply Hensel's lemma (5.4.6) to lift this root to a root $v \in T$. So $\pi' = v\pi$ is another generator of (π) and we have $\pi'^n = x$. By (5.4.2), there is a unique map $\psi : k[[y]] \to T$ such that $\psi(y) = \pi'$. Since π' generates the maximal ideal of T, the induced map $\operatorname{gr} \psi$ is surjective. Hence, by (5.2.6), ψ is also surjective. But $\dim T = \dim k[[y]] = 1$, and so $\ker \psi = 0$, and thus ψ is in fact an isomorphism. □

noeth-puiseux-series

COROLLARY 8.3.3 (Puiseux series). *Let k be an algebraically closed field of characteristic 0, and let f be a polynomial in $k[x, y]$.*

1. *There exists $n \in \mathbb{N}$ and $p(x^{1/n}) \in k((x^{1/n}))$ such that $f(x, p(x^{1/n})) = 0$.*
2. *If f is monic in y, then p can be chosen to be a power series in $x^{1/n}$.*
3. *If f is monic and $f(0, 0) = 0$, then p can be chosen so that it has no constant term.*

PROOF. By the Corollary above, there exists $n \in \mathbb{N}$ such that

$$f(x, y) = a(x) \prod_{i=1}^{r} (y - p_i(x^{1/n})),$$

for some $a(x) \in k[x]$, and $p_i \in k((x^{1/n}))$. If $f(x, y)$ is monic in y, then each p_i is integral over $k[[x]]$, and thus is contained in $k[[x^{1/n}]]$. If $f(0, 0) = 0$, then there is at least one i such that $p_i(0) = 0$. □

4. Jacobson Rings and the Nullstellensatz

The treatment here is from the exercises after chapter 5 in Atiyah-Macdonald.

DEFINITION 8.4.1. A ring R is *Jacobson* if every prime in R is the intersection of maximal ideals.

noeth-equiv-prps-jacobson

PROPOSITION 8.4.2. *The following statements are equivalent for a ring R:*

1. *R is Jacobson.*
2. *In every homomorphic image of A, the nilradical is equal to the Jacobson radical.*
3. *Every prime ideal in A that is not maximal is equal to the intersection of the prime ideals that contain it strictly.*

PROOF. (1) $\Leftrightarrow$ (2): This is easy. For one implication, note that the intersection of all the primes containing an ideal equals the intersectino of all the maximal ideals containing that ideal. For the other, given a prime $P \subset A$, look at the image A/P.

(1) $\Rightarrow$ (3): Trivial.

(3) $\Rightarrow$ (1): Suppose there (1) is false; then there is some prime $P \subset R$ that's not the intersection of maximal ideals. Quotient out by P, and assume that R is a domain, for which (2) fails. That is, $\operatorname{Jac} R \neq 0$. So let $0 \neq f \in \operatorname{Jac} R$, and consider R_f. Since R is a domain, $R_f \neq 0$, and we can find a maximal ideal $\mathfrak{m} \subset R_f$ such that $Q = \mathfrak{m} \cap R$ is a prime ideal not containing f, and is maximal with respect to this property. But then Q is not maximal, and it's not the intersection of the prime ideals that strictly contain it, since every prime ideal strictly containing it will contain f. □

COROLLARY 8.4.3. *Every homomorphic image of a Jacobson ring is also Jacobson.*

PROOF. Immediate from characterization (2) above. □

Now, we can present the Nullstellensatz for Jacobson rings.

noeth-nullstellensatz

THEOREM 8.4.4 (Nullstellensatz). *The following are equivalent for a ring R:*

1. *R is Jacobson.*
2. *Every finitely generated R-algebra S that's a field is finite over R.*

PROOF. (1) $\Rightarrow$ (2): Since every homomorphic image of R is Jacobson, we can assume $R \subset S$. So R is also a domain.

Then, by (8.1.3), we see that we can find $a \in R$ such that $S = S_a$ is finite over a polynomial ring T over R_a. Since S is, in particular, integral over T, we see that T is a field, by (4.4.1). This implies that $R_a = T$ is a field. If $a \in R$ is not a unit, then a is contained in every non-zero prime of R, implying that (0) is not the intersection of all the primes strictly containing it. This contradicts the fact that R is Jacobson, according to characterization (3) of (8.4.2). So $a \in R$ is a unit, and $R_a = R$, which means that S is finite over R.

(2) $\Rightarrow$ (1): We'll prove that R satisfies condition (3) of (8.4.2). So let $P \subset R$ be a non-maximal prime, and suppose $f \in R \setminus P$ is in the intersection of all the primes strictly containing P. Then, let $S = R/P$, and consider S_f: this has no non-zero primes, since every non-zero prime in S contains f. Hence, it's a field; but since it's a finitely generated R-algebra, it's finite over R, and hence over R/P. But then R/P is a field, and so P is maximal, contradicting the fact that it wasn't! □

h-fin-gen-rings-jacobson

COROLLARY 8.4.5. *Let R be a Jacobson ring. Then every finitely generated R-algebra is Jacobson. In particular, every finitely generated ring and every affine ring is Jacbson.*

PROOF. The first statement follows immediately from characterization (2) above, since every finitely generated algebra over a finitely generated R-algebra S is again a finitely generated R-algebra. So if it's a field, then it's finite over R, and hence over S.

The second statement follows from the fact that $\mathbb{Z}$ is Jacobson: every non-zero prime is maximal, and (0) is the intersection of all the maximal ideals, and also the fact that any field is trivially Jacobson. □

acobson-max-contract-max

COROLLARY 8.4.6. *Let $f : R \to S$ be a map of finite type with R Jacobson. Then, for every maximal ideal $\mathfrak{n} \subset S$, $\mathfrak{m} = f^{-1}(\mathfrak{n})$ is a maximal ideal. Moreover $R/\mathfrak{m} \hookrightarrow S/\mathfrak{n}$ is a finite extension of fields.*

PROOF. Replacing R with its image in S, we can assume $R \subset S$, with S a finitely generated R-algebra. Then, $S/\mathfrak{n}$ is a finitely generated $R/\mathfrak{m}$-algebra that's a field. So the Theorem tells us that it's in fact finite over $R/\mathfrak{m}$, and so $R/\mathfrak{m}$ is also a field, with $S/\mathfrak{n}$ a finite extension over it. □

5. Dimension Theory for Affine Rings

noeth-secn:affine-rings

Here, we present the main theorem in the dimension theory of affine rings. Some of its consequences can also be obtained from the fact that any field is Cohen-Macaulay. But we'll prove them here the classical way.

th-main-thm-affine-rings

THEOREM 8.5.1. *For every affine domain R over a field k, we have*

$$\dim R = \operatorname{tr\,deg}_k R.$$

Moreover, every maximal chain of primes in R has length $\dim R$.

PROOF. By Noether Normalization, R is finite over a polynomial ring $S = k[x_1, \ldots, x_d]$. By (6.5.4), this implies that $\dim R = d$. So it suffices to show that $d = \operatorname{tr\,deg}_k S = \operatorname{tr\,deg}_k R$. But this follows from the fact that $K(R)$ is algebraic over $K(S)$.

Let $P_0 \subset P_1 \subset \ldots P_m$ be a chain of primes in R with $m < d$. We want to show that we can stick a prime in to make it longer. Take $I_j = P_j$, and let S be as in the statement of Noether Normalization corresponding to this chain of ideals. Now, we can assume that $P_0 = 0$, and that P_m is maximal. By the choice of S, if $\dim R/P_j = d_j$, then we see that

$$Q_j = P_j \cap S = (x_{d_j} + 1, \ldots, x_d).$$

Since $P_m \cap S = (x_1, \ldots, x_d)$, and $P_0 \cap S = 0$, we see that there must be a j somewhere such that $d_j + 1 < d_{j-1}$. So we have the prime $Q = (x_{d_{j-1}}, \ldots, x_d)$ lying strictly between Q_{j-1} and Q_j. Let $R' = R/P_{j-1}$ and let $S' = S/Q_{j-1}$; then we still have a tower $S' \subset R'$, with S' a polynomial ring over k.

Now, S' is a normal domain, so we're in a position to apply the going down theorem (4.6.3) to conclude that there is a prime P contained in P_j, and containing P_{j-1} that contracts to Q. □

DEFINITION 8.5.2. A ring R is called *catenary* if, for every pair of primes $Q \subset P \subset R$, any maximal chain of primes from Q to P has the same length.

A ring R is *universally catenary* if every finitely generated R-algebra is catenary.

eld-universally-catenary

COROLLARY 8.5.3. *Any field, or equivalently, any affine ring, is universally catenary.*

PROOF. Let R be any affine ring, and let $Q \subset P \subset R$ be a chain of two primes. By quotienting out by Q, we can assume that R is a domain, and reduce the problem to showing that, in an affine domain, every maximal chain of primes going down from a prime in R has the same length, which is in fact $\operatorname{ht} P$. For, if some maximal chain of primes going down from P has length less than $\operatorname{ht} P$, then that chain can't be extended to a maximal chain of primes in R of length $\dim R$. □

oeth-codim-equals-height

COROLLARY 8.5.4. *If R is an affine domain, and $I \subset R$ is an ideal, then*

$$\operatorname{ht} I = \dim R - \dim R/I.$$

PROOF. Suppose P is a minimal prime over I; then we can find a chain of primes in R that includes P. Hence, we see that $\operatorname{ht} P = \dim R - \dim R/P$, for all primes P minimal over I. Then, we see that

$$\begin{aligned} \operatorname{ht} I &= \min\{\operatorname{ht} P : P \supset I \text{ minimal}\} \\ &= \dim R - \max\{\dim R/P : P \supset I \text{ minimal}\} \\ &= \dim R - \dim R/I. \end{aligned}$$

□

e-dom-reg-elt-dim-by-one

COROLLARY 8.5.5. *If R is an affine domain, and $0 \neq f \in R$, then*

$$\dim R/(f) = \dim R - 1.$$

PROOF. By the Theorem, we can localize at any maximal ideal not containing f, and then use the local version (6.2.12). □

We finish with a result on the dimension of tensor products.

dimension-tensor-product

PROPOSITION 8.5.6. *Let R be an affine ring, and S a Noetherian k-algebra. Then*

$$\dim R \otimes_k S = \dim R + \dim S.$$

PROOF. By Noether Normalization R is finite over the polynomial ring $k[x_1, \ldots, x_n]$, where $n = \dim R$. Now, $R \otimes_k S$ is finite over $S[x_1, \ldots, x_n]$. The result now follows from (6.5.4) and (6.6.3). □

6. Dimension of Fibers

The next Theorem is essential in the study of fibers.

fiber-inequality-domains

THEOREM 8.6.1. *Let $R \subset S$ be a tower of Noetherian domains, with S finitely generated over R. If $\mathfrak{q} \subset S$ is a prime, and $\mathfrak{p} = \mathfrak{q} \cap R$, then:*

$$\dim S_{\mathfrak{q}} + \operatorname{tr\,deg}_{k(\mathfrak{p})}(k(\mathfrak{q})) \leq \dim R_{\mathfrak{p}} + \dim K(R) \otimes_R S.$$

If R is universally catenary, then in fact equality holds in the expression above.

PROOF. Observe first that

$$\dim K(R) \otimes_R S = \operatorname{tr.deg}_{K(R)} K(S),$$

by the main Theorem.

Also note that $k(\mathfrak{q}) = K(S_\mathfrak{p}/\mathfrak{q}_\mathfrak{p})$, and so again by the main Theorem,

$$\operatorname{tr.deg}_{k(\mathfrak{p})}(k(\mathfrak{q})) = \dim S_\mathfrak{p}/\mathfrak{q}_\mathfrak{p} \leq \dim S_\mathfrak{p} - \dim S_\mathfrak{q}$$

with equality holding if R is universally catenary.

Therefore, we see that

$$\dim S_\mathfrak{q} + \operatorname{tr.deg}_{k(\mathfrak{p})} k(\mathfrak{q}) \leq \dim S_\mathfrak{p},$$

with equality holding if R is universally catenary.

So it will suffice to show that

$$\dim S_\mathfrak{p} \leq \dim R_\mathfrak{p} + \operatorname{tr.deg}_{K(R)} K(S),$$

with equality holding whenever R is universally catenary.

The proof is by induction on the number of generators of S over R. We can localize at $\mathfrak{p}$ at the outset and assume that $(R, \mathfrak{p})$ is a local ring.

Suppose $S = R[x]/P$, for some prime $P \subset S$. If $P = (0)$, then

$$\dim K(R) \otimes_R S = \dim K(R)[x] = 1,$$

and

$$\dim S_\mathfrak{p} = \dim R[x] = \dim R + 1,$$

and so this case is taken care of.

Suppose that $P \neq (0)$; then, since $R \subset S$, we must have $P \cap R = 0$, and so, $\operatorname{ht} P = 1$. Moreover, since every element of S is algebraic over R, we have $\operatorname{tr.deg}_{K(R)} K(S) = 0$. Now,

$$\dim S_\mathfrak{p} \leq \dim R[x] - \operatorname{ht} P = \dim R,$$

with equality holding again if R is universally catenary.

Now, suppose S is generated over R by n elements $s_1, \ldots, s_n$, and let S' be the subring of S generated by the first $n-1$ generators. Let $\mathfrak{q}^* = \mathfrak{q} \cap S$; then by the inductive hypothesis, and the previous result for the case of a single generator, we have,

$$\dim S'_{\mathfrak{q}^*} + \operatorname{tr.deg}_{k(\mathfrak{p})}(k(\mathfrak{q}^*)) \leq \dim R + \operatorname{tr.deg}_{K(R)} K(S'),$$
$$\dim S_\mathfrak{q} + \operatorname{tr.deg}_{k(\mathfrak{q}^*)}(k(\mathfrak{q})) \leq \dim S'_{\mathfrak{q}^*} + \operatorname{tr.deg}_{K(S')} K(S),$$

with equality holding in both expressions, if R is universally catenary.

Putting these two expressions together, we find

$$\dim S_\mathfrak{q} + \operatorname{tr.deg}_{k(\mathfrak{p})}(k(\mathfrak{q})) \leq \dim R + \operatorname{tr.deg}_{K(R)} K(S),$$

with equality holding whenever R is universally catenary. □

CHAPTER 9

Quasi-finite Algebras and the Main Theorem of Zariski

chap:zariski

1. Quasi-finite Algebras

-artinian-finite-k-space

LEMMA 9.1.1. *Let k be a field and let S be a finitely generated k-algebra. The following are then equivalent:*

(1) *S is Artinian.*
(2) *$\operatorname{Spec} S$ is discrete.*
(3) *S is finite over k.*
(4) *$\operatorname{Spec} S$ is finite.*

PROOF. By Noether Normalization (8.1.2), we can find a polynomial algebra $T = k[x_1, \ldots, x_r]$ such that S is finite over T, where $r = \dim S$. In particular, S is Artinian if and only if $r = 0$. But, since $\operatorname{Spec} S$ surjects onto $\operatorname{Spec} T$, we also find that $\operatorname{Spec} S$ is finite if and only if $r = 0$, since a non-trivial polynomial ring over k will contain infinitely many primes (it is a UFD). Thus we see that S is Artinian if and only if S is finite over k, if and only if $\operatorname{Spec} S$ is finite. It is also clear that S is Artinian if and only if $\operatorname{Spec} S$ is discrete, since the latter is true if and only if every prime in S is maximal. □

zariski-isolated-prime

PROPOSITION 9.1.2. *Let R be a ring, and let S be an R-algebra of finite type. Suppose $Q \subset S$ is a prime ideal, with $P = Q \cap R$. Then the following are equivalent:*

(1) *Q is an isolated point in $\operatorname{Spec}(S \otimes_R k(P))$.*
(2) *Q is both a maximal and a minimal prime in $S \otimes_R k(P)$.*
(3) *S_Q/PS_Q is finite over $k(P)$.*

PROOF. By replacing R with $k(P)$ and S with $S \otimes_R k(P)$, we reduce immediately to the case where R is a field and S is a finitely generated R-algebra. Now we have to show the equivalence between the following statements:

(1) Q is an isolated point in $\operatorname{Spec} S$.
(2) Q is both open and closed in $\operatorname{Spec} S$.
(3) Q is both a maximal and a minimal prime of S.
(4) S_Q is finite over R.

Note that Q is an isolated point in $\operatorname{Spec} S$ if and only if $\{Q\}$ is an open subset of $\operatorname{Spec} S$. But Q is an open point if and only if $\{Q\} = \operatorname{Spec} S_a$, for some $a \in S$. Since S is Jacobson (8.4.5), and Q_a is a maximal ideal in S_a with S_a finitely generated over S, we find that in this case Q must also be maximal in S (8.4.6). Thus Q is an isolated point in $\operatorname{Spec} S$ if and only if $\{Q\}$ is both open and closed in $\operatorname{Spec} S$ if and only if Q is both maximal and minimal in S. This shows (1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3).

We proceed now to show that (1) is equivalent to (4). Suppose Q is an isolated point in $\operatorname{Spec} S$, and let $a \in S$ be such that $\{Q\} = \operatorname{Spec} S_a$. But this implies that

$S_Q = S_a$, since S_a is already a local ring with maximal ideal Q_a. Therefore, S_Q is finitely generated over R, and we find from the lemma above that S_Q is finite over R.

Conversely, suppose S_Q is finite over R; then, in particular, S_Q is Artinian, and so Q is minimal in S. Moreover, S_Q is also finite over S, and since Q_Q is maximal in S_Q its contraction in S, which is of course Q, is also maximal in S (4.4.2). Thus Q is both maximal and minimal in S, which finishes our proof. □

DEFINITION 9.1.3. Let S be an R-algebra of finite type and let Q be a prime in S. We say that S is *quasi-finite over R at Q* if Q satisfies any of the equivalent conditions in (9.1.2).

We say that S is *quasi-finite over R* if it is quasi-finite over R at Q for all primes $Q \subset S$.

REMARK 9.1.4. Observe that quasi-finiteness at Q is essentially a topological condition. If we define a continuous map $f : X \to Y$ of topological spaces to be *quasi-finite at x*, for some $x \in X$, whenever x is isolated in $f^{-1}(f(x))$, then we see that S is quasi-finite over R at Q if and only if S is of finite type over R and $\operatorname{Spec} S \to \operatorname{Spec} R$ is a quasi-finite at Q.

-quasi-finite-equiv-prps

PROPOSITION 9.1.5. *Let R be a ring and let S be an R-algebra of finite type. Then the following are equivalent:*

1. *S is quasi-finite over R.*
2. *For every prime $P \subset R$, $\operatorname{Spec}(S \otimes_R k(P))$ is a discrete space.*
3. *For every prime $P \subset R$, $S \otimes_R k(P)$ is Artinian.*
4. *For every prime $P \subset R$, $\operatorname{Spec}(S \otimes_R k(P))$ is a finite set.*
5. *For every prime $P \subset R$, $S \otimes_R k(P)$ is finite over k.*

PROOF. The equivalence (1) $\Leftrightarrow$ (2) is an immediate consequence of the definition and (9.1.2). The equivalences of the remaining statements is simply the content of (9.1.1). □

icipal-open-quasi-finite

COROLLARY 9.1.6. *Let S be a finite R-algebra. Then, for $a \in S$, S_a is quasi-finite over R.*

PROOF. Just observe that, for every prime $P \subset R$, $\operatorname{Spec}(S_a \otimes_R k(P))$ is an open subset of $\operatorname{Spec}(S \otimes_R k(P))$. □

The goal of this chapter is the following Theorem which is a sort of converse to the Corollary above. For geometric applications of this Theorem, see [AG, 5].

zariski-main-thm

THEOREM 9.1.7 (Main Theorem of Zariski). *Let R be a ring, S an R-algebra of finite type, R' the integral closure of R in S, and Q a prime in S. If B is quasi-finite over R at Q, then there exists $a \in R' \setminus Q$ such that the natural map $R'_a \to S_a$ is an isomorphism.*

The proof of this Theorem is very involved and will be the content of the whole of the next section.

2. Proof of Zariski's Main Theorem

We will prove a series of lemmas that will culminate in a proof of the Main Theorem.

egrally-closed-monogenic

LEMMA 9.2.1. *Let $(R, \mathfrak{m})$ be a local ring with residue field $k = R/\mathfrak{m}$. Suppose $S = R[\alpha]$ is an R-algebra generated by one element $\alpha \in S$ such that $R \subset S$, and suppose also that R is integrally closed in S. Then S is quasi-finite over R at some prime Q lying over $\mathfrak{m}$ if and only if $S = R$.*

PROOF. One direction is trivial. For the non-trivial one, suppose S is quasi-finite over R at some prime Q lying over $\mathfrak{m}$; then it suffices to show that α is integral over R. For this, first observe that, if $\overline{\alpha}$ is the image of α in $S/\mathfrak{m}S$, then $S/\mathfrak{m}S = k[\overline{\alpha}]$ is quasi-finite over k at $\overline{Q}$, the image of Q in $k[\overline{\alpha}]$. This of course means that $\overline{\alpha}$ is algebraic over k, since the polynomial ring over k contains no primes that are simultaneously maximal and minimal. Given this, we see that $k[\overline{\alpha}]$ is in fact finite over k.

Therefore, there is some monic polynomial $p(t) \in R[t]$ such that $p(\alpha) \in \mathfrak{m}S$ (just pick one whose image in $k[t]$ is the minimal polynomial for $\overline{\alpha}$ over k). Let $\beta = 1 + p(\alpha)$; then, α is clearly integral over $T = R[\beta]$, and so it suffices to show that β is in R.

Next note that the image $\overline{\beta}$ of β in $T/\mathfrak{m}T$ is integral over k. Indeed, the map $\operatorname{Spec} S/\mathfrak{m}S \to \operatorname{Spec} T/\mathfrak{m}T$ is surjective, since S is finite over T, and so $\operatorname{Spec} T/\mathfrak{m}T$ is finite, which, by lemma (9.1.1, means that $T/\mathfrak{m}T$ is finite over k. Moreover, we claim that $\overline{\beta}$ is invertible in $T/\mathfrak{m}T$. Indeed, if $\overline{\beta}$ were contained in some prime ideal P of $T/\mathfrak{m}T$, then we can find a prime ideal P' of $S/\mathfrak{m}S$ lying over P, and so the image of $\overline{\beta}$ in $S/\mathfrak{m}S$ will lie in P'. But the image of $\overline{\beta}$ in $S/\mathfrak{m}S$ is 1, which makes this scenario impossible.

So we see that there is a monic polynomial $q(t) \in R[t]$ such that $q(\beta) \in \mathfrak{m}T$, and also such that the constant term q_0 of $q(t)$ is a unit (take any monic polynomial mapping to the minimal polynomial for $\overline{\beta}$ over k; q_0 must be a unit, since $\overline{\beta}$ is invertible in $T/\mathfrak{m}T$). Therefore, there is a polynomial $r(t) \in \mathfrak{m}R[t]$ such that $q(\beta) = r(\beta)$. But now, $(q - r)(\beta) = 0$, and the constant term $u = q_0 - r_0$ of $(q - r)(t)$ is a unit, since $q_0 \notin \mathfrak{m}$ and $r_0 \in \mathfrak{m}$. In sum, we have a polynomial expression

$$a_m\beta^m + a_{m-1}\beta^{m-1} + \ldots + u = 0,$$

where $a_i \in R$, for $1 \leq i \leq m$, and $u \in R$ is a unit. This implies that β is a unit in S, and also that β^{-1} is integral over R (just multiply the polynomial equation above by $u^{-1}\beta^{-m}$ to find a monic polynomial over R vanishing on β^{-1}).

But now, since R is integrally closed $\beta^{-1} \in R$. It is not possible that $\beta^{-1} \in \mathfrak{m}$, since, in this case, β^{-1} will not be invertible in S. Therefore β^{-1} is a unit in R, and so β lies in R. This completes our proof. □

ntaining-polynomial-ring

LEMMA 9.2.2. *Let $R \subset S$ be a tower of domains, and suppose S contains the polynomial ring $R[t]$, and is integral over $R[t]$. Then S is nowhere quasi-finite over R.*

PROOF. We need to show that there is no prime $Q \subset S$ that is both maximal and minimal in its fiber ring $S \otimes_R k(P)$, where $P = Q \cap R$. So it suffices to show that no prime $Q \subset S$ that is maximal in its corresponding fiber ring is also minimal in it. In this situation, we need to find a prime $Q^* \subsetneq Q$ that also lies over $P = Q \cap R$.

First assume that R and S are normal domains, and let $P_1 = R[t] \cap Q$. Since S is integral over $R[t]$, P_1 is also maximal in the fiber ring $R[t] \otimes_R k(P) = k(P)[t]$, and therefore P_1 strictly contains the prime ideal $P[t] \subset R[t]$. In this case, $R[t]$ is

also normal (4.3.17), and so we are in a situation to apply Going Down (4.6.3) to conclude that there is a prime $Q^* \subsetneq Q$ of S.lying over $P[t]$ and thus over P.

In the general case, let R' and S' be the integral closures of R and S, respectively, in their quotient fields. Let P' be a prime in R' lying over P and let Q' be a prime in S' lying over Q. Then, by the case considered in the paragraph above, there is a prime $Q'^* \subsetneq Q'$ contracting to P', and then taking $Q^* = Q'^* \cap S$ gives us what we want (observe that $Q^* \neq Q$ by incomparability (4.4.7). $\square$

CHAPTER 10

Regular Sequences and Depth

chap:rrrs

NOTE ON NOTATION 9. In this chapter, all rings will be Noetherian and all modules will be finitely generated. As usual, R will denote a (Noetherian) ring, and M an R-module, finitely generated, of course.

1. Regular Sequences

rrrs-defn-reg-seq

DEFINITION 10.1.1. If M is an R-module, and $I \subset R$ is an ideal, then an *M-sequence* in I is an ordered subset $\mathbf{x} = \{x_1, \ldots, x_r\} \subset I$ that satisfies the following conditions:

(1) $M/\mathbf{x}M \neq 0$, where $\mathbf{x}M$ denotes the module $(x_1, \ldots, x_r)M$.
(2) For every $i \in \{1, \ldots, r\}$, $x_i \notin \mathcal{Z}(M/(x_1, \ldots, x_{i-1}))$. By convention, this means that $x_1 \notin \mathcal{Z}(M)$.

If $\mathbf{x}$ only satisfies condition 2, then we say it is a *weak M-sequence*.

REMARK 10.1.2. Observe that $\mathbf{x}$ is an M-sequence in I iff for all $i < r$, $\{x_{i+1}, \ldots, x_r\}$ is an $M/(x_1, \ldots, x_i)M$-sequence in I.

NOTE ON NOTATION 10. If $x \notin \mathcal{Z}(M)$, then we say that x is *M-regular*. For example, one can rephrase the second requirement for an M-sequence as requiring x_i to be $M/(x_1, \ldots, x_{i-1})M$-regular. More generally, if $\mathbf{x}$ is a (weak) M-sequence, then we may also say that $\mathbf{x}$ is (weakly) M-regular.

In some sense, M-sequences act as a co-ordinate system for M: they cut out the right dimension, as the following Proposition illustrates.

rrrs-reg-seq-dim-by-one

PROPOSITION 10.1.3. *If R is a local ring, and $\mathbf{x} \subset I$ is a weak M-sequence in I, then for every $i \in \{1, \ldots, r\}$ we have*

$$\dim M/(x_1, \ldots, x_i) = \dim M - i.$$

PROOF. We'll prove this by induction on r. Observe from (6.2.12) that for any $x \notin \mathcal{Z}(M)$ we have $\dim M/xM = \dim M - 1$. So the base case holds. Now, by the remark after Definition (10.1.1), we see that $\{x_2, \ldots, x_r\}$ is an M'-regular sequence, where $M' = M/x_1M$. By the inductive hypothesis, we have

$$\dim M'/(x_2, \ldots, x_i) = \dim M' - (i-1).$$

But $M'/(x_2, \ldots, x_i) = M/(x_1, \ldots, x_i)$, and so we have the equality we seek. □

rrrs-reg-seq-flat-ext

PROPOSITION 10.1.4. *Suppose $\mathbf{x} \subset I$ is a weak M-sequence in I, $f : R \to S$ is a ring map, and N is an S-module flat over R. Then, $f(\mathbf{x})$ is a weak $(M \otimes N)$-sequence in IS. If $\mathbf{x}(M \otimes N) \neq M \otimes N$, then $\mathbf{x}$ is an M-sequence and $f(\mathbf{x})$ is an $(M \otimes N)$-sequence in IS. If N is faithfully flat over R, then $f(\mathbf{x})$ is an $(M \otimes N)$-sequence if and only if $\mathbf{x}$ is an M-sequence.*

PROOF. Observe that for any ideal $J \subset R$, N/JN is flat over R/J. In particular, if $x \notin \mathcal{Z}(M/JM)$, then $x \notin \mathcal{Z}((M \otimes N)/J(M \otimes N))$, since

$$(M \otimes N)/J(M \otimes N) = M/JM \otimes_{R/J} N/JN,$$

and tensoring with N/JN preserves injections. This means, in particular, that for $i \in \{1, \dots, r\}$, $x_i \notin \mathcal{Z}((M \otimes N)/(x_1, \dots, x_{i-1})(M \otimes N)$. So $\mathbf{x} \in IS$ satisfies condition 2 for being an $(M \otimes N)$-sequence, and is thus a weak $(M \otimes N)$-sequence. The second statement follows immediately from this.

For the last assertion, the 'if' part was taken care of above; so we'll look at the 'only if' part. By induction on the length of $\mathbf{x}$, we reduce this to the case where $\mathbf{x} = \{x\}$, for some $x \in I$. So, we see that the sequence

$$0 \to M \otimes_R N \xrightarrow{x \otimes 1} M \otimes_R N$$

is exact, which, by the definition of faithful flatness (3.6.4), implies that the sequence

$$0 \to M \xrightarrow{x} M$$

is also exact. □

rrrs-reg-seq-loc

COROLLARY 10.1.5. *If $\mathbf{x} \subset I$ is a weak M sequence in I, and $U \subset R$ is a multiplicative set, then $U^{-1}\mathbf{x} \subset U^{-1}I$ is a weak $U^{-1}M$-sequence. If $U = R \setminus P$ for some prime P, and $I \subset P$, then $\mathbf{x}_P \subset I_P$ is in fact an M_P-sequence in I_P.*

PROOF. Most of this follows from the Proposition and the fact that $U^{-1}R$ is a flat extension of R. For the second statement, just note that $\mathbf{x}_P M_P \subset P_P M_P \neq M_P$, unless $M_P = 0$, by Nakayama's lemma. □

rrrs-reg-seq-comp

COROLLARY 10.1.6. *If $(R, \mathfrak{m})$ is a local ring, and $\mathbf{x}$ is an M-sequence in I, then $\mathbf{x} \subset I\hat{R}$ is an $\hat{M}$-sequence in $I\hat{R}$.*

PROOF. It suffices to show that $\mathbf{x}\hat{M} \neq \hat{M}$. But this again follows from Nakayama's lemma, since $\mathbf{x} \subset \hat{\mathfrak{m}}$. □

In general, a re-ordering of an M-sequence need not be regular, but the situation is better when we're in a local ring, or, more generally, when our ideal I lies in the Jacobson radical of M.

rrrs-reg-seq-transpose

LEMMA 10.1.7. *If $I \subset \mathrm{Jac}(R)$, and $\{x_1, x_2\} \subset I$ is an M-regular sequence, then so is $\{x_2, x_1\}$.*

PROOF. There are two things that can go wrong: either $x_2 \in \mathcal{Z}(M)$, or $x_1 \in \mathcal{Z}(M/x_2M)$. Let's take them on one at a time.

Let $N = (0 :_M x_2)$. If $0 \neq m \in N$, then $x_2 m = 0 \in x_1 M$. Since $x_2 \notin \mathcal{Z}(M/x_1M)$, it follows that $m = x_1 n$, for some $n \in M$. But now $x_1(x_2 n) = x_2(x_1 n) = 0$, and so, since $x_1 \notin \mathcal{Z}(M)$, we see that $x_2 n = 0$. Thus, we have $n \in N$, and so $N = x_1 N$. By Nakayama's lemma, we then see that $N = 0$, and so $x_2 \notin \mathcal{Z}(M)$.

Now, suppose $m \in M$ is such that $x_1 m = x_2 n \in x_2 M$. Then, we have $n \in (x_1 M :_M x_2)$, and since $x_2 \notin \mathcal{Z}(M/x_1M)$, we see that $n \in x_1 M$. So we can find $n' \in M$ such that $n = x_1 n'$. But then $x_1(m - x_2 n') = 0$, which, because $x_1 \notin \mathcal{Z}(M)$, implies that $m = x_2 n' \in x_2 M$. Therefore, $x_1 \notin \mathcal{Z}(M/x_2M)$. □

rrrs-reg-seq-permute

PROPOSITION 10.1.8. *If $I \subset \mathrm{Jac}(R)$, and $\mathbf{x} \subset I$ is an M-sequence, then any permutation of $\mathbf{x}$ is also an M-sequence.*

PROOF. Since every permutation is a composition of transpositions of adjacent elements, it's enough to prove that every switch between adjacent elements of an M-sequence still gives an M-sequence. That is, we want to show that if $\{x_1, \ldots, x_r\}$ is an M-sequence, then so is $\{x_1, \ldots, x_i, x_{i-1}, \ldots, x_r\}$. But this follows immediately from the Lemma above, and the remark after Definition (10.1.1). □

2. Flatness

Quotients by regular sequences have striking flatness properties with respect to the modules for which the sequences are regular. We will explore some of these in this section.

rrrs-reg-seq-almost-flat

LEMMA 10.2.1. *If $\mathbf{x}$ is a weak M-sequence, and we have an exact sequence*

$$N_2 \xrightarrow{\phi_2} N_1 \xrightarrow{\phi_1} N_0 \xrightarrow{\phi_0} M \to 0,$$

then the sequence

$$N_2/\mathbf{x}N_2 \to N_1/\mathbf{x}N_2 \to N_0/\mathbf{x}N_0 \to M/\mathbf{x}M \to 0,$$

is also exact.

PROOF. By induction on the length of $\mathbf{x}$ it suffices to show this for the sequence $\{x\}$, where x is M-regular. Since tensoring with $R/(x)$ is right exact, it suffices to show exactness at N_1/xN_1. Let $u \in N_1$ be such that $\phi_1(u) = xn$, for some $m \in N_0$. Then, we see that $x\phi_0(n) = 0$. Since x is M-regular, this implies that $\phi_0(n) = 0$, and so $n = \phi_1(v)$, for some $v \in N_1$. But then $\phi_1(xv - u) = 0$, and so $xv - u = \phi_2(a)$, for some $a \in N_2$. This shows that $\overline{u} = \overline{\phi}(\overline{a}) \in N_1/xN_1$, and so the sequence is indeed exact. □

s-reg-seq-pres-complexes

PROPOSITION 10.2.2. *Suppose we have an exact complex*

$$N_\bullet : \ldots N_i \xrightarrow{\phi_i} N_{i-1} \xrightarrow{\phi_{i-1}} \ldots \xrightarrow{\phi_1} N_0 \xrightarrow{\phi_0} N_{-1} \to 0,$$

and suppose $\mathbf{x} \subset R$ is a weak N_i-sequence, for all $i \geq -1$, then $N_\bullet \otimes R/\mathbf{x}R$ is again exact.

PROOF. Again, we induct on the length of $\mathbf{x}$. For length 1, it's easy, since x is N_i-regular only if it's also $\operatorname{im}\phi_{i+1}$-regular. So we just apply the lemma to all exact sequences of the form:

$$N_i \xrightarrow{\phi_i} N_{i-1} \xrightarrow{\phi_{i-1}} N_{i-2} \xrightarrow{\phi_{i-2}} \operatorname{im}\phi_{i-2} \to 0.$$

□

rs-reg-seq-fiber-reg-all

COROLLARY 10.2.3. *Let $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of local rings. Let P be an R-module, and let N be an S-module that's flat over R. Suppose $\mathbf{y} \subset \mathfrak{n}$ is an $N/\mathfrak{m}N$-regular sequence.*

1. *$\mathbf{y}$ is also $P \otimes_R N$-regular.*
2. *$N/\mathbf{y}N$ is also flat over R.*

PROOF. (1) Using an inductive argument, it suffices to prove this for the case where $\mathbf{y} = \{y\}$ is a one-element sequence. Observe that we have

$$\mathfrak{m}^i(P \otimes N)/\mathfrak{m}^{i+1}(P \otimes N) \cong \left(\mathfrak{m}^i P/\mathfrak{m}^{i+1}P\right) \otimes N \cong k^r \otimes N \cong (N/\mathfrak{m}N)^r,$$

for some $r \in \mathbb{N}$. Now, since y is $N/\mathfrak{m}N$-regular, it follows that it is also $\mathfrak{m}^i(P \otimes N)/\mathfrak{m}^{i+1}(P \otimes N)$-regular, for all integers $i \geq 0$. Suppose y is a

zero divisor of $P \otimes N$, and let $0 \neq z \in P \otimes N$ be such that $yz = 0$. Then, by Krull's Intersection theorem (2.2.9), there is an $i \in \mathbb{N}$ such that $z \in \mathfrak{m}^i(P \otimes N)$, but $z \notin \mathfrak{m}^{i+1}(P \otimes N)$. This implies that y is a zero divisor of $\mathfrak{m}^i(P \otimes N)/\mathfrak{m}^{i+1}(P \otimes N)$, which contradicts what we found above. This shows that y is $P \otimes N$-regular.

(2) By (3.4.2), it suffices to show that the map

$$\mathfrak{m} \otimes_R N/\mathbf{y}N \to N/\mathbf{y}N$$

is a monomorphism. This follows from part (1) and the Proposition.

□

rrrs-req-seq-tor

COROLLARY 10.2.4. *Let M be an R-module, and let $\mathbf{x} \subset R$ be a sequence that is both weakly R-regular and weakly M-regular. Then, for any $R/\mathbf{x}R$-module N, we have an isomorphism of complexes of R-modules:*

$$\operatorname{Tor}_\bullet^{R/\mathbf{x}R}(N, M/\mathbf{x}M) \cong \operatorname{Tor}_\bullet^R(N, M).$$

PROOF. Let $F_\bullet$ be a free resolution of M over R. Then the Proposition tells us that $F_\bullet \otimes_R R/\mathbf{x}R$ is also a free resolution of $M/\mathbf{x}M$ over $R/\mathbf{x}R$. This shows that

$$\begin{aligned}\operatorname{Tor}_\bullet^{R/\mathbf{x}R}(N, M/\mathbf{x}M) &= H_\bullet(N \otimes_{R/\mathbf{x}R} (F_\bullet \otimes_R R/\mathbf{x}R)) \\ &= H_\bullet(N \otimes_R F_\bullet) \\ &= \operatorname{Tor}_\bullet^R(N, M).\end{aligned}$$

□

rrrs-splicing-criterion

COROLLARY 10.2.5 (Splicing Criterion). *Let $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of local Noetherian rings, and let M be a finitely generated S-module. Let $t \in \mathfrak{m}$ be a non-zero divisor for R and M. Then M is flat over R if and only if M/tM is flat over $R/(t)$.*

PROOF. The only if direction, as always, is trivial. Using the Local Criterion for flatness (3.4.2), we see that M is flat if and only if $\operatorname{Tor}_1^R(R/\mathfrak{m}, M) = 0$. But now since M/tM is flat over $R/(t)$, we see that $\operatorname{Tor}_1^{R/(t)}(R/\mathfrak{m}, M/tM) = 0$. Now our result follows from the previous Corollary. □

We finish this section with another result associating certain flatness properties to quotients by regular sequences, and also illustrates a general method for proving statements about regular sequences.

rrrs-reg-seq-m-flat

PROPOSITION 10.2.6. *Let $\mathbf{x} \subset R$ be a weak M-sequence.*

(1) *The map $\mathbf{x}R \otimes_R M \to M$ is a monomorphism.*
(2) $\operatorname{Tor}_1^R(R/\mathbf{x}R, M) = 0$
(3) *If $\mathbf{x}$ is also R-regular, then $\operatorname{Tor}_n^R(R/\mathbf{x}R, M) = 0$, for all $n \in \mathbb{N}$.*

PROOF. Observe that (1) and (2) are equivalent. We'll prove (1) now. Suppose for now that R is local, and that $\mathbf{x}$ is in fact an M-sequence.

Now, by (10.1.8), every permutation of $\mathbf{x}$ is also an M-sequence. Assume that we had a relation in M of the form

$$x_{i_1}m_1 + \ldots + x_{i_s}m_s = 0,$$

with $x_{i_k} \in \mathbf{x}$.

We will prove, by induction on s, that $\sum_{k=1}^{s} x_{i_k} \otimes m_k = 0$. When $s = 1$, this is clear, since x_{i_1} is M-regular. So suppose $s > 1$; we then find that

$$x_{i_1} m_1 \in (x_{i_2}, \ldots, x_{i_s})M.$$

Since x_{i_1} is $M/(x_{i_2}, \ldots, x_{i_s})M$-regular, we find that $m_1 \in (x_{i_2}, \ldots, x_{i_s})M$, and so there exist $n_k \in M$ such that $m_1 = \sum_{k=2}^{s} x_{i_k} n_k$. This gives us the relation:

$$\sum_{k=2}^{s} x_{i_k}(x_{i_1} n_k + m_k) = 0.$$

By the induction hypothesis, this means that we have

$$\begin{aligned} 0 &= \sum_{k=2}^{s} x_{i_k} \otimes (x_{i_1} n_k + m_k) \\ &= \sum_{k=2}^{s} x_{i_1} \otimes x_{i_k} n_k + \sum_{k=2}^{s} x_{i_k} \otimes m_k \\ &= x_{i_1} \otimes (\sum_{k=2}^{s} x_{i_k} n_k) + \sum_{k=2}^{s} x_{i_k} \otimes m_k \\ &= \sum_{k=1}^{s} x_{i_k} \otimes m_k. \end{aligned}$$

Now, we discard the local hypothesis. For any prime $P \subset R$, either $\mathbf{x} \subset P$, in which case, $\mathbf{x}$ is an M_P-sequence, by (10.1.5), and so from our local result, we find that

$$\mathbf{x} R_P \otimes M_P \to M_P$$

is a monomorphism.

If $\mathbf{x} \not\subseteq P$, then $\mathbf{x} R_P = R_P$, in which case the map above is already an isomorphism. So all the localizations of the map $\mathbf{x}R \otimes M \to M$ are injective, which means that the map itself is injective.

Now, we move on to (3). Suppose now that $\mathbf{x}$ is also weakly R-regular. We'll prove the statement by induction on the length r of $\mathbf{x}$. If $r = 1$, since $x_1 \notin \mathcal{Z}(R) \cup \mathcal{Z}(M)$, we know that

$$\operatorname{Tor}_n^R(M, R/(x_1)) = 0, \text{ for } n \geq 1.$$

Note that this assumes knowledge of the simple computation of Tor in this case, using the free resolution

$$0 \to R \xrightarrow{x_1} R \to R/(x_1) \to 0$$

So suppose now that $r > 1$; let $\mathbf{x}' = \{x_1, \ldots, x_{r-1}\}$. Since x_r is $R/\mathbf{x}'R$-regular, we have a short exact sequence:

$$0 \to R/\mathbf{x}'R \xrightarrow{x_r} R/\mathbf{x}'R \to R/\mathbf{x}R \to 0.$$

If we look at the long exact sequence of $\operatorname{Tor}_\bullet^R(M, \_\_)$ corresponding to this short exact sequence, then we find exact sequences of the form

$$\operatorname{Tor}_n^R(M, R/\mathbf{x}'R) \to \operatorname{Tor}_n^R(M, R/\mathbf{x}R) \to \operatorname{Tor}_{n-1}^R(M, R/\mathbf{x}'R).$$

By the induction hypothesis $\operatorname{Tor}_\bullet^R(M, R/\mathbf{x}'R)$ vanishes for $n > 0$. So we see that $\operatorname{Tor}_\bullet^R(M, R/\mathbf{x}R)$ also vanishes for $n > 1$. The $n = 1$ case was dealt with in the last part. $\square$

3. Quasiregular Sequences

We saw in Section 1 of Chapter 2 that whenever we have an ideal $I \subset R$ generated by d elements $x_1, \ldots, x_d \in I$, we can equip the R-module M with the natural I-adic filtration and obtain a surjection

$$(M/IM)[T_1, \ldots, T_d] \to \mathrm{gr}_I(M).$$

The question of when this is an isomorphism, as we noted earlier, is very important, and is tightly connected with the notion of regular sequences.

DEFINITION 10.3.1. A sequence $\mathbf{x} \subset R$ of length d is *M-quasiregular* if $\mathbf{x}M \neq M$, and the natural surjection

$$(M/\mathbf{x}M)[T_1, \ldots, T_d] \to \mathrm{gr}_{\mathbf{x}}(M)$$

is an isomorphism.

Before we prove anything about the existence and properties of such sequences, let's set up the notation. Given an R-module M and a sequence $\mathbf{x} \subset R$ of length d such that $\mathbf{x}M \neq M$, we denote the natural surjection discussed above by $\varphi_M^{\mathbf{x}}$. Also, we have an associated surjection

$$\begin{aligned} \Phi_M^{\mathbf{x}} : M[T_1, \ldots, T_d] &\longrightarrow \mathscr{B}(\mathbf{x}, M) \\ m \cdot p(T_1, \ldots, T_d) &\mapsto p(x_1, \ldots, x_d)m \end{aligned}$$

where $\mathscr{B}(\mathbf{x}, M) = \oplus_{n \geq 0} \mathbf{x}^n M t^n$ denotes the blow-up module associated with the natural $\mathbf{x}$-adic filtration on M. This gives us the following commutative diagram of graded $R[T_1, \ldots, T_d]$-modules, with exact rows and columns.

$$\begin{array}{ccccc} M[T_1, \ldots, T_d] & \xrightarrow{\Phi_M^{\mathbf{x}}} & \mathscr{B}(\mathbf{x}, M) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} & & \\ (M/\mathbf{x}M)[T_1, \ldots, T_d] & \xrightarrow{\varphi_M^{\mathbf{x}}} & \mathrm{gr}_{\mathbf{x}}(M) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \\ 0 & & 0 & & \end{array}$$

From the commutative diagram, we see that $\varphi_M^{\mathbf{x}}$ is injective (and thus an isomorphism) if and only if whenever $\Phi_M^{\mathbf{x}}(F) \in \ker \pi'$, we have $F \in \ker \pi$. Now, observe that $\ker \pi = (\mathbf{x}M)[T_1, \ldots, T_d]$ and $\ker \pi' = \mathbf{x}\mathscr{B}(\mathbf{x}, M)$. So we now give an alternate description of quasiregularity:

DEFINITION 10.3.2 (Quasiregularity Bis). A sequence $\mathbf{x} \subset R$ of length d is *M-quasiregular* if $\mathbf{x}M \neq M$, and if, with the notation as in the discussion above, we have

$$\Phi_M^{\mathbf{x}\,-1}(\mathbf{x}\mathscr{B}(\mathbf{x}, M)) = (\mathbf{x}M)[T_1, \ldots, T_d].$$

In fact, we can do better. Suppose $\Phi_{\mathbf{x}}(F) \in \ker \pi'$ with $\deg F = n$; then we can find $G_i \in M[T_1, \ldots, T_d]$ of degree n such that $\Phi_{\mathbf{x}}(F) = \sum_i x_i \Phi_{\mathbf{x}}(G_i)$. Let $G_i' = x_i G_i$, and set $G = \sum_i G_i'$; then $G \in \ker \pi$, and moreover $\Phi_{\mathbf{x}}(F - G) = 0$. So

to show that $F \in \ker \pi$, it suffices to show that $F - G \in \ker \pi$. This gives us a third characterization of quasiregularity.

DEFINITION 10.3.3 (Quasiregularity Part Trois). A sequence $\mathbf{x} \subset R$ of length d is *M-quasiregular* if $\mathbf{x}M \neq M$, and if, with the notation as above, we have

$$\ker \Phi_M^{\mathbf{x}} \subset (\mathbf{x}M)[T_1, \ldots, T_d].$$

REMARK 10.3.4. We can rephrase this in the following way: a sequence $\mathbf{x}$ is quasiregular if, for every F such that $\Phi_M^{\mathbf{x}}(F) = 0$, F has its coefficients in $\mathbf{x}M$.

rrrs-quasireg-reg-elt

PROPOSITION 10.3.5. *Suppose $\mathbf{x} \subset R$ is an M-quasiregular sequence; then, if $a \in R$ is $M/\mathbf{x}M$ regular, then it is also $M/\mathbf{x}^r M$-regular, for all $r \in \mathbb{N}$.*

PROOF. As always, the answer's induction; this time on r. The case $r = 1$ is our hypothesis; so we can assume $r > 1$. Let $y \in M$ be such that $ay \in \mathbf{x}^r M$. Then, by induction, $y \in \mathbf{x}^{r-1}M$. Now, there is some element $F \in M[T_1, \ldots, T_d]$ (where d is the length of $\mathbf{x}$) of degree $r-1$ such that $\Phi_M^{\mathbf{x}}(F) = yt^{r-1}$. By our assumption, we find that $\Phi_M^{\mathbf{x}}(aF) \in \mathbf{x}\mathscr{B}(\mathbf{x}, M)$. So, since $\mathbf{x}$ is quasiregular, aF must have its coefficients in $\mathbf{x}M$. Since a is $M/\mathbf{x}M$-regular, this means that F must also have its coefficients in $\mathbf{x}M$, which implies that $yt^{r-1} \in \mathbf{x}\mathscr{B}(\mathbf{x}, M)$. But then $y \in \mathbf{x}^r M$, which shows that a is $M/\mathbf{x}^r M$-regular. □

Before we move on to the next (very important) Theorem, let's fix some more notation. Suppose $\mathbf{x} \subset R$ is a sequence of length $d > 1$. Let $\mathbf{z} \subset \mathbf{x}$ be any subsequence indexed by some subset $\{i_1, \ldots, i_k\} \subset \{1, \ldots, d\}$; then we have the following commutative diagram:

$$\begin{array}{ccc} M[T_{i_1}, \ldots, T_{i_k}] & \xrightarrow{\Phi_M^{\mathbf{z}}} & \mathscr{B}(\mathbf{z}, M) \\ \downarrow & & \downarrow \\ M[T_1, \ldots, T_d] & \xrightarrow{\Phi_M^{\mathbf{x}}} & \mathscr{B}(\mathbf{x}, M) \end{array}$$

So, for any element $G \in M[T_{i_1}, \ldots, T_{i_k}]$, we'll speak interchangeably of $\Phi_M^{\mathbf{x}}(G)$ and $\Phi_M^{\mathbf{z}}(G)$.

rrs-regular-quasiregular

THEOREM 10.3.6 (Rees). *Any M-regular sequence $\mathbf{x}$ is also M-quasiregular.*

PROOF. We'll be using both characterizations of quasiregularity that we gave after the original one. Let d be the length of $\mathbf{x}$: we'll do induction on d. Suppose $d = 1$, and suppose $\Phi_M^{\mathbf{x}}(F) = 0$, for some homogeneous element $mT_1^n \in M[T_1]$. This implies that $x_1^n m = 0 \in M$; but then $m = 0$, since x_1 is M-regular. So we see in fact that $M[T_1] \cong \mathscr{B}(x_1, M)$ (we'll have more to say about this later). Thus we can assume $d > 1$. Let $\mathbf{z} = \{x_1, \ldots, x_{d-1}\}$: by induction $\mathbf{z}$ is M-quasiregular.

Now, suppose $F \in \ker \Phi_M^{\mathbf{x}}$: write F in the form $G + T_d H$, where $G \in M[T_1, \ldots, T_{d-1}]$ is of degree n, and $H \in M[T_1, \ldots, T_d]$ is of degree $n-1$.

Let $y \in \mathbf{x}^{n-1}M$ be such that $\Phi_M^{\mathbf{x}}(H) = yt^{n-1}$; then we see that

$$x_d y t^n = x_d \Phi_M^{\mathbf{x}}(H) t = -\Phi_M^{\mathbf{x}}(G) \in \mathbf{z}^n M t^n \subset \mathscr{B}(\mathbf{z}, M).$$

Hence, $x_d y \in \mathbf{z}^n M$; but since x_d is $M/\mathbf{z}M$-regular, and $\mathbf{z}$ is M-quasiregular, by induction, the Lemma above tells us that x_d is also $M/\mathbf{z}^n M$ regular, and so we must have $y \in \mathbf{z}^n M$. But this implies that $\Phi_M^{\mathbf{x}}(H)$ is contained in $\ker \pi'$, and we

can now do an induction on the degree n to conclude that H has its coefficients in $\mathbf{x}M$ (the $n = 0$ case is trivial). Now, it also follows that $\Phi^{\mathbf{z}}_M(G)$ is contained in $\ker \pi'$, and by the induction hypothesis on d, we conclude that G has its coefficients in $\mathbf{z}M$, and hence in $\mathbf{x}M$.

All this combines to assure us that F also has its coefficients in $\mathbf{x}M$. □

Here's a nice consequence of the Theorem.

rrrs-ideal-reg-seq-free

COROLLARY 10.3.7. *Suppose $I \subset R$ is generated by an R-regular sequence of length d. Then I/I^2 is free over R/I of rank d, and for every $n \in \mathbb{N}$, we have* $\mathrm{Sym}^n(I/I^2) \cong I^n/I^{n+1}$.

PROOF. Immediate from the theorem. □

Since quasiregular sequences remain quasiregular under permutations, we cannot expect every quasiregular sequence to be regular. But, as one could have guessed, the local situation is better. First we need a lemma.

s-quasireg-tail-quasireg

LEMMA 10.3.8. *Let $\mathbf{x} \subset R$ be an M-quasiregular sequence of length $d > 1$.*

1. *For any $r \in M$, and any $n \in \mathbb{N}$, $x_1 r \in \mathbf{x}^n M$ if and only if $r \in \mathbf{x}^{n-1}M$.*
2. *Let $\mathbf{y} = \{x_2, \ldots, x_d\}$; then $\mathbf{y}$ is M/x_1M-quasiregular.*

PROOF. (1) We'll prove this by induction n. When $n = 1$, the statement is trivial; so suppose $n > 1$. Then, by the induction step, we see that $r \in \mathbf{x}^{n-2}M$. Hence, we can find a homogeneous element $H \in M[T_1, \ldots, T_d]$ of degree $n-2$ such that $\Phi^{\mathbf{x}}_M(H) = rt^{n-2}$ and such that $\Phi^{\mathbf{x}}_M(T_1H)t = \Phi^{\mathbf{x}}_M(G)$, for some $G \in M[T_1, \ldots, T_d]$ of degree n. Using Euler's formula, we can write $G = \sum_i T_i G_i$, for some G_i of degree $n-1$. Let $G' = \sum_i x_i G_i$; then we find that $\Phi^{\mathbf{x}}_M(T_1H - G') = 0$. Since $\mathbf{x}$ is M-quasiregular, this implies that $T_1H - G'$ has its coefficients in $\mathbf{x}M$. Now, G' already has its coefficients in $\mathbf{x}M$, and therefore so also must T_1H. But then H also has its coefficients in $\mathbf{x}M$, thus implying that $r \in \mathbf{x}^{n-1}M$.

(2) Let $M' = M/x_1M$; first observe that

$$\mathbf{y}M' = (\mathbf{y} + x_1)\, M/x_1M = \mathbf{x}M/x_1M \neq M',$$

since $\mathbf{x}M \neq M$ by hypothesis.

Suppose now that$\Phi^{\mathbf{y}}_{M'}(F) = 0$, for some homogeneous $F \in M'[T_2, \ldots, T_d]$ of degree n. We can find $G \in M[T_2, \ldots, T_d]$ of degree n such that G goes to F under the natural projection from $M[T_2, \ldots, T_d]$ to $M'[T_2, \ldots, T_d]$. To say that $\Phi^{\mathbf{y}}_{M'}(F) = 0$ is equivalent to saying that $\Phi^{\mathbf{x}}_M(G) \in (\mathbf{y}^n M \cap x_1 M)\, t^n$. This follows from the following simple observation:

$$\mathbf{y}^n M' = (\mathbf{y}^n M + x_1 M)\, /x_1 M \cong \mathbf{y}^n M/\,(\mathbf{y}^n M \cap x_1 M)\,.$$

Now, let $r \in M$ be such that $\Phi^{\mathbf{x}}_M(G) = x_1 r t^n$, and let $k \in \mathbb{N}$ be maximal such that $r \in \mathbf{x}^k M$ (set $k = \infty$ if there is no maximal such number). Observe that, by the first part, since $x_1 r \in \mathbf{x}^n M$, we must have $k \geq n-1$. So we can find $H \in M[T_1, \ldots, T_d]$ of degree $n-1$ such that $\Phi^{\mathbf{x}}_M(H) = rt^{n-1}$. Let $H' = T_1 H$; then we find that

$$\Phi^{\mathbf{x}}_M(G - H') = x_1 r t^n - x_1 r t^n = 0.$$

Hence $G - H'$ has its coefficients in $\mathbf{x}M$. But observe that G does not depend on T_1; hence G and H' can have no common monomials, and it

follows that both G and H' separately have their coefficients in $\mathbf{x}M$. In particular, F will have its coefficients in $\mathbf{y}M'$. This finishes the proof. □

i-separated-quasireg-reg

PROPOSITION 10.3.9. *Let $\mathbf{x} \subset R$ be any sequence, and let $I = \mathbf{x}R$. Suppose that for every $1 \leq i \leq d$, $M/(x_1, \ldots, x_i)M$ is separated under the I-adic filtration. Then $\mathbf{x}$ is M-regular if and only if it is M-quasiregular.*

PROOF. One direction was proved in (10.3.6). For the other, we'll use induction on the length d of the sequence. For the base case, suppose x is an M-quasiregular element. Suppose $xm = 0$, for some $0 \neq m \in M$; then we find that $\Phi^x_M(mT_1) = 0$, and so $m \in xM$. Continuing this way, we find that $m \in \cap_{n\geq 1} x^n M = 0$. Therefore, x is M-regular. Now, suppose $d > 1$; then, by the lemma, $\mathbf{y} = \{x_1, \ldots, x_{d-1}\}$ is M/x_1M-quasiregular, and hence, by induction, it is M/x_1M-regular. To finish our proof, it suffices to show that x_1 is M-regular. This follows exactly as in the case for the sequence of length 1. □

rrrs-local-quasireg-reg

COROLLARY 10.3.10. *Suppose $(R, \mathfrak{m})$ is a local ring, and let $\mathbf{x} \subset R$ be any sequence. Then $\mathbf{x}$ is M-regular if and only if it is M-quasiregular.*

PROOF. Follows from the Proposition above and Krull's Intersection theorem (2.2.9). □

With this in hand, we can give some useful characterizations of quasiregular sequences.

rrs-quasireg-iff-loc-reg

THEOREM 10.3.11. *Let $\mathbf{x} \subset R$ be a sequence. The following statements are equivalent:*

1. *$\mathbf{x}$ is M-quasiregular.*
2. *For every prime $P \subset R$ containing $\mathbf{x}$, the image of $\mathbf{x}$ in R_P is M_P-regular.*
3. *For every maximal ideal $\mathfrak{m} \subset R$ containing $\mathbf{x}$, the image of*

PROOF. Note that the map $\varphi^{\mathbf{x}}_M$ is an isomorphism if and only if each of its localizations at the maximal ideals of R is an isomorphism. If a maximal ideal $\mathfrak{m}$ does not contain $\mathbf{x}$, then both the domain and the range of $\varphi^{\mathbf{x}}_{M\mathfrak{m}}$ are 0. If $\mathbf{x} \subset \mathfrak{m}$, then the previous Corollary tells us that the image of $\mathbf{x}$ in $R_\mathfrak{m}$ is $M_\mathfrak{m}$-regular if and only if it is $M_\mathfrak{m}$-quasiregular. From this, we obtain (1) ⇔ (2) ⇔ (3). □

The next Corollary gives yet another characterization of quasiregular sequences.

rrrs-gr-reg-iff-quasireg

COROLLARY 10.3.12. *Let $\mathbf{x} \subset R$ be a sequence, and let ξ be its image in $\mathbf{x}R/\mathbf{x}^2R \subset \mathrm{gr}_\mathbf{x}(R)$. For an R-module N, let $\hat{N}$ denote the completion of N with respect to the $\mathbf{x}$-adic filtration. Then the following statements are equivalent.*

1. *$\mathbf{x}$ is M-quasiregular.*
2. *ξ is $\mathrm{gr}_\mathbf{x}(M)$-regular.*
3. *$\mathbf{x}$ is $\hat{M}$-regular.*

PROOF. (1) ⇔ (2)**:** If $\mathbf{x}$ is M-quasiregular, then ξ acts on $\mathrm{gr}_{\mathbf{x}R}(M)$ like the canonical set of generators of a polynomial algebra, and is thus $\mathrm{gr}_\mathbf{x}(M)$-regular.

For the converse, by the last Theorem, we can assume that $(R, \mathfrak{m})$ is local, and show that ξ being $\mathrm{gr}_\mathbf{x}(M)$-regular implies that $\mathbf{x}$ is M-regular, for any sequence $\mathbf{x} \subset \mathfrak{m}$. For this, we'll use induction on the length d of

$\mathbf{x}$. If $d = 1$, then this is clear; so assume $d > 1$, and let $\mathbf{y} = \{x_2, \dots, x_d\}$. Let $R' = R/(x_1)$, and let $M' = M/x_1M$.

By (2.1.17), we observe that

$$\operatorname{gr}_{\mathbf{y}R'}(R') = \operatorname{gr}_{\mathbf{x}}(R)/(\xi_1), \text{ and}$$
$$\operatorname{gr}_{\mathbf{y}R'}(M') = \operatorname{gr}_{\mathbf{x}}(M)/\xi_1 \operatorname{gr}_{\mathbf{x}}(M).$$

Hence, by induction, we find that the image of $\mathbf{y}$ in R' is M'-regular. So it suffices to show now that x_1 is M-regular. Were this not so, there would be $0 \neq m \in M$ such that $x_1 m = 0$. Since $\mathbf{x} \subset \mathfrak{m}$, the $\mathbf{x}$-adic filtration on M is separated, and so $\operatorname{in}(m) \neq 0$. But then $\xi_1 \operatorname{in}(m) = 0$, contradicting the fact that ξ_1 is a $\operatorname{gr}_{\mathbf{x}}(M)$-regular element.

(2) $\Leftrightarrow$ (3)**:** Observe that, for every R-module N, $\hat{N}$ is separated when equipped with the $\mathbf{x}$-adic filtration. Moreover, for any ideal $I \subset R$, $\hat{M}/I\hat{M} \cong \widehat{M/IM}$ (5.3.3) is again complete and hence separated. In particular, $\hat{M}$ satisfies the hypotheses of (10.3.9) with respect to $\mathbf{x}$, and hence $\mathbf{x}$ is $\hat{M}$-regular if and only if it is $\hat{M}$-quasiregular. Now the equivalence follows from the equivalence (1) $\Leftrightarrow$ (2) shown above and the isomorphism

$$\operatorname{gr}_{\mathbf{x}}(M) \cong \operatorname{gr}_{\mathbf{x}}(\hat{M})$$

shown in (5.1.7).

□

To round off this section, we present several criteria for a system of parameters in a local ring to be a regular sequence.

rrs-sop-reg-seq-criteria

THEOREM 10.3.13. *Let $(R, \mathfrak{m})$ be a local ring, and let $\mathfrak{q} \subset R$ be an ideal of definition for M, generated by a system of parameters $\mathbf{x} \subset \mathfrak{m}$ of length d. Let ξ be the image of $\mathbf{x}$ in $\mathfrak{q}/\mathfrak{q}^2 \subset \operatorname{gr}_{\mathfrak{q}}(R)$, and let $\hat{M}$ be the completion of M along $\mathbf{x}R$. Then the following are equivalent:*

(1) $\mathbf{x}$ *is M-regular.*
(2) $\mathbf{x}$ *is M-quasiregular.*
(3) $\mathbf{x}$ *is $\hat{M}$-regular.*
(4) ξ *is $\operatorname{gr}_{\mathfrak{q}}(M)$-regular.*
(5) $\chi_M^{\mathfrak{q}}(n) = l(M/\mathfrak{q}M)\binom{n+d}{d}$.
(6) $\Delta^d \chi_M^{\mathfrak{q}} = l(M/\mathfrak{q}M)$.

Moreover, if any (hence every one) of these conditions is true, then we have $\dim M = d$, *and* $\mathbf{x}$ *is a minimal system of parameters for M.*

PROOF. (1) $\Leftrightarrow$ (2) follows from (10.3.10), (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4) follows from (10.3.12), and, finally, we get (2) $\Leftrightarrow$ (5) $\Leftrightarrow$ (6) from (2.3.25). For the last couple of assertions, observe that $\dim M = \deg \chi_M^{\mathfrak{q}}$, by (6.2.8); moreover, $\dim M$ is also the minimal length of a system of parameters for M. This gives us the Theorem. □

4. Grade and Depth

In this section, we'll introduce the powerful homological methods discovered, among others, by Auslander-Buchsbaum (that's two different people) and Serre. In the next chapter, we'll look at another homological method of characterizing regular sequences using Koszul complexes, and in Chapter 18, we'll see yet another homological characterization of regular sequences using local cohomology.

DEFINITION 10.4.1. If $IM \neq M$, then an M-sequence $\mathbf{x}$ in I is *maximal* if $I \subset \mathcal{Z}(M/\mathbf{x}M)$. That is, if we cannot extend the sequence any further within I.

It so happens that all maximal M-sequences in an ideal I have the same length. This gives us a very important invariant of ideals and local rings that will be the object of discussion in this section. We need some preliminaries before that.

rrrs-ass-of-hom

LEMMA 10.4.2. *If M and N are finitely generated modules over a Noetherian ring R, then*

$$\operatorname{Ass}\operatorname{Hom}_R(M,N) = \operatorname{Supp} M \cap \operatorname{Ass} N.$$

PROOF. Observe that all the sets involved behave well under localizations. Moreover, by (3.1.12), we have $\operatorname{Hom}_R(M,N)_P = \operatorname{Hom}_{R_P}(M_P, N_P)$, for all primes $P \subset R$. So we can assume that R is local with maximal ideal $\mathfrak{m}$. We just have to show that $\mathfrak{m}$ is in the set on the right hand side iff it's also in the set on the left hand side. Note that $\mathfrak{m} \in \operatorname{Supp} M$ always, unless $M = 0$, in which case the equality follows trivially.

Suppose first that $\mathfrak{m} \in \operatorname{Ass}\operatorname{Hom}_R(M,N)$; then we have $0 \neq \phi : M \to N$ such that $a\phi = 0$, for all $a \in \mathfrak{m}$. Now, just choose any $m \in M$ such that $\phi(m) \neq 0$. Then we'll have $\operatorname{ann}(\phi(m)) = \mathfrak{m}$, and so $\mathfrak{m} \in \operatorname{Ass} N$.

Now, suppose that $\mathfrak{m} \in \operatorname{Ass} N$. Then we have an embedding $R/\mathfrak{m} \hookrightarrow N$. Now, since $M/\mathfrak{m}M \neq 0$, by Nakayama, and it's a module over the field $R/\mathfrak{m}$, we have a surjection $M/\mathfrak{m} \to R/\mathfrak{m}$, which gives us a surjection $M \to R/\mathfrak{m}$. Consider the composition

$$\phi : M \to R/\mathfrak{m} \to N.$$

This is non-zero, yet $\mathfrak{m} \subset \operatorname{ann}(\phi)$. So we see that $\mathfrak{m} \in \operatorname{Ass}\operatorname{Hom}_R(M,N)$. □

The observation that follows is crucial in characterizing maximal sequences invariantly.

rrrs-reg-elt-hom-vanish

COROLLARY 10.4.3. *With M and N as in the Proposition,* $\operatorname{Hom}_R(M,N) = 0$ *iff* $\operatorname{ann}(M)$ *contains an N-regular element.*

PROOF. In one direction, suppose $\operatorname{ann}(N)$ contains an N-regular element x. Then, for all $\phi \in \operatorname{Hom}_R(M,N)$, we have $x\phi = 0$. But x is N-regular; so $\phi = 0$.

For the other direction, assume $\operatorname{ann}(M)$ contains no N-regular elements. This says that $\operatorname{ann}(M) \subset \bigcup_{P \in \operatorname{Ass} N} P$. So there is some $P \in \operatorname{Ass} N$ such that $\operatorname{ann}(M) \subset P$. But then $P \in \operatorname{Supp} M \cap \operatorname{Ass} N$, which, by the Lemma above, implies that $P \in \operatorname{Ass}\operatorname{Hom}_R(M,N)$, and so $\operatorname{Hom}_R(M,N) \neq 0$. □

rrrs-ext-hom-isomorph

LEMMA 10.4.4. *If M and N are finitely generated R-module, and $\mathbf{x} = \{x_1, \ldots, x_r\}$ is a weak M-sequence in* $\operatorname{ann}(N)$*, then*

$$\operatorname{Ext}^r_R(N,M) \cong \operatorname{Hom}_R(N, M/\mathbf{x}M).$$

PROOF. We'll do this by induction on r. For $r = 0$, this is trivial. So assume that $r > 0$. Let $\mathbf{x}_i = \{x_1, \ldots, x_i\}$. We will show by induction on i that

$$\operatorname{Ext}^i_R(N, M/\mathbf{x}_{r-i}M) \cong \operatorname{Hom}_R(N, M/\mathbf{x}M),$$

which will finish our proof. For $i = 0$, this is again trivial. So assume $i > 0$, and consider the short exact sequence

$$0 \to M/\mathbf{x}_{r-i}M \xrightarrow{x_{r-i+1}} M/\mathbf{x}_{r-i}M \to M/\mathbf{x}_{r-i+1}M \to 0.$$

The long exact sequence of $\operatorname{Ext}^\bullet_R(N, \_\_)$ corresponding to this gives us the following exact sequence

$$0 \to \operatorname{Ext}^{i-1}_R(N, M/\mathbf{x}_{r-i+1}M) \to \operatorname{Ext}^i_R(N, M/\mathbf{x}_{r-i}M) \xrightarrow{x_{r-i+1}} \operatorname{Ext}^i_R(N, M/\mathbf{x}_{r-i}M).$$

This needs a little more explanation: the zero on the left hand side corresponds to $\operatorname{Ext}^{i-1}_R(N, M/\mathbf{x}_{r-i}M)$. By the induction hypothesis on r, this is isomorphic to $\operatorname{Hom}_R(N, M/\mathbf{x}_{r-1}M)$, which is 0, by Corollary (10.4.3), since $x_r \in \operatorname{ann}(N)$ is $M/\mathbf{x}_{r-1}M$-regular.

Now, since $x_{r-i+1} \in \operatorname{ann}(N)$, the map on the right is 0, giving us the isomorphism

$$\operatorname{Ext}^i_R(N, M/\mathbf{x}_{r-i}M) \cong \operatorname{Ext}^{i-1}_R(N, M/\mathbf{x}_{r-i+1}M) \cong \operatorname{Hom}_R(N, M/\mathbf{x}M).$$

This finishes our induction, and thus our proof. □

NOTE ON NOTATION 11. We denote by $V(I)$ the set of primes in R containing I.

rrrs-max-seq-same-length

THEOREM 10.4.5 (Definition). *If $IM \neq M$, then all maximal M-sequences have the same length, which is called the* grade *of I with respect to M, and is denoted* $\operatorname{grade}(I, M)$. *We have*

$$\operatorname{grade}(I, M) = \min\{i : \operatorname{Ext}^i_R(R/I, M) \neq 0\}.$$

Moreover, if $IM = M$, then $\operatorname{Ext}^i_R(R/I, M) = 0$, for all i, and in this case we set $\operatorname{grade}(I, M) = \infty$.

PROOF. Assume that $IM \neq M$. Suppose $\mathbf{x} = \{x_1, \ldots, x_r\}$ is a maximal M-sequence in I. Set

$$\mathbf{x}_i = \{x_1, \ldots, x_i\};$$

then, for $i < r$, since $I = \operatorname{ann}(R/I)$ contains the $M/\mathbf{x}_iM$-regular element x_{i+1}, we see by Corollary (10.4.3) that $\operatorname{Hom}_R(R/I, M/\mathbf{x}_iM) = 0$. But then Lemma (10.4.4) says that

$$\operatorname{Ext}^i_R(R/I, M) = \operatorname{Hom}_R(R/I, M/\mathbf{x}_iM) = 0.$$

Also, since $\mathbf{x}$ is maximal, we see that I contains no $M/\mathbf{x}M$-regular elements, and so by the same Corollary, we see that $\operatorname{Hom}_R(R/I, M/\mathbf{x}M) \neq 0$. Now, the Lemma goes to work again to give us

$$\operatorname{Ext}^r_R(R/I, M) = \operatorname{Hom}_R(R/I, M/\mathbf{x}M) \neq 0.$$

This finishes the proof of the first part.

Now, suppose $IM = M$; we claim that this equivalent to saying that $I + \operatorname{ann}(M) = R$. Given this claim, we see that $IM = M$ implies

$$\operatorname{Ext}^i_R(R/I, M) = 0, \text{ for all } i,$$

since Ext is linear in both variables, and both I and $\operatorname{ann}(M)$ annihilate $\operatorname{Ext}^\bullet_R(R/I, M)$.

So it remains to prove the claim. Note that the proof of (6.2.4) tells us that $V(I + \operatorname{ann}(M)) = V(\operatorname{ann}(M/IM))$. Hence

$$I + \operatorname{ann}(M) = R \Leftrightarrow V(\operatorname{ann}(M/IM)) = \emptyset \Leftrightarrow \operatorname{ann}(M/IM) = R \Leftrightarrow M = IM.$$

□

DEFINITION 10.4.6. The *depth* of an ideal $I \subset R$ is just $\operatorname{grade}(I, R)$, and is denoted $\operatorname{depth} I$.

If $(R, \mathfrak{m}, k)$ is a local ring, and M is a finitely generated R-module, then we set

$$\operatorname{depth} M = \operatorname{grade}(\mathfrak{m}, M).$$

The theorem gives us a homological description of $\operatorname{depth} M$.

rrrs-ext-descrip-depth

COROLLARY 10.4.7. *If M is a finitely generated module over a local ring $(R, \mathfrak{m}, k)$, then*

$$\operatorname{depth} M = \min\{i : \operatorname{Ext}^i_R(k, M) \neq 0\}.$$

Given an exact sequence

$$0 \to M' \to M \to M'' \to 0,$$

of R-modules, we get the corresponding long exact sequence for $\operatorname{Ext}^\bullet_R(R/I, \_\_)$. This gives us a number of inequalities between the grade of I with respect to the modules in the sequence. We'll list them in the following Proposition.

rrrs-grade-exct-seq

PROPOSITION 10.4.8. *With the exact sequence as in the paragraph above, we have the following inequalities:*

1. $\operatorname{grade}(I, M') \leq \min\{\operatorname{grade}(I, M), \operatorname{grade}(I, M'') + 1\}$.
2. $\operatorname{grade}(I, M) \leq \min\{\operatorname{grade}(I, M'), \operatorname{grade}(I, M'')\}$.
3. $\operatorname{grade}(I, M'') \leq \min\{\operatorname{grade}(I, M) - 1, \operatorname{grade}(I, M)\}$.

PROOF. We'll make extensive use of (10.4.5).

1. For $k < \min\{\operatorname{grade}(I, M), \operatorname{grade}(I, M'') + 1\}$, we have
$$\operatorname{Ext}^k_R(R/I, M) = \operatorname{Ext}^{k-1}_R(R/I, M'') = 0.$$
So from the long exact sequence of Ext, we find that $\operatorname{Ext}^k_R(R/I, M') = 0$. This implies the statement.
2. For $k < \min\{\operatorname{grade}(I, M'), \operatorname{grade}(I, M'')\}$, we have
$$\operatorname{Ext}^k_R(R/I, M') = \operatorname{Ext}^k_R(R/I, M'') = 0.$$
Again, we get our result from the long exact sequence of Ext.
3. For $k < \min\{\operatorname{grade}(I, M') - 1, \operatorname{grade}(I, M)\}$, we have
$$\operatorname{Ext}^{k+1}_R(R/I, M') = \operatorname{Ext}^k_R(R/I, M) = 0.$$
From this the result follows.

□

The following Proposition tells us that knowing depth tells us everything about grade.

rrrs-grade-min-depth

PROPOSITION 10.4.9. *Suppose $I \subset R$ is an ideal; then we can find $P \in V(I)$ such that $\operatorname{grade}(P, M) = \operatorname{grade}(I, M)$. In particular, we have*

$$\operatorname{grade}(I, M) = \min\{\operatorname{depth} M_P : P \in V(I)\}.$$

PROOF. If $IM = M$, then we see that $\operatorname{grade}(P, M) = \operatorname{grade}(I, M) = \infty$, for all $P \in V(I)$. Assume therefore that $IM \neq M$, and pick a maximal M-sequence $\mathbf{x}$ in I. Since I contains no $M/\mathbf{x}M$-regular element, we know that there is some $P \in \operatorname{Ass} M/\mathbf{x}M$ such that $I \subset P$. In this case, $\mathbf{x}$ is also a maximal M-sequence in P, and so we see that $\operatorname{grade}(I, M) = \operatorname{grade}(P, M)$. For the second statement,

note that, by Proposition (10.1.5), we have that $\operatorname{grade}(P, M) \leq \operatorname{depth} M_P$. But we see that $P_P \in \operatorname{Ass} M_P/\mathbf{x}M_P$, and so $\mathbf{x}$ is in fact a maximal M_P-sequence in P_P. From this it follows that $\operatorname{grade}(I, M) = \operatorname{depth} M_P$, from which the Proposition follows. □

rrrs-grade-is-geometric

COROLLARY 10.4.10. *With all the notation as in the Proposition, we have*

$$\operatorname{grade}(I, M) = \operatorname{grade}(\operatorname{rad}(I), M).$$

Moreover, if $J \subset R$ is another ideal, then

$$\operatorname{grade}(I \cap J, M) = \min\{\operatorname{grade}(I, M), \operatorname{grade}(J, M)\}.$$

PROOF. The statements follow from the Proposition and the following equalities:

$$V(I) = V(\operatorname{rad} I),$$
$$V(I \cap J) = V(I) \cup V(J).$$

Observe that one could also have obtained the first equality from [BHP, 1.10]. □

Depth, like dimension, decreases strictly when one quotients by a regular sequence.

rrrs-reg-seq-dep-by-one

PROPOSITION 10.4.11. *If $\mathbf{x}$ is an M-sequence in I of length r, then*

$$\operatorname{grade}(I/\mathbf{x}, M/\mathbf{x}M) = \operatorname{grade}(I, M/\mathbf{x}M) = \operatorname{grade}(I, M) - r.$$

PROOF. For any R-module N, let $\overline{N} = N/\mathbf{x}N$. Then,

$$I\overline{M} = (IM + \mathbf{x}M)/\mathbf{x}M = \overline{IM} \neq \overline{M}.$$

This tells us that $\overline{I} \cdot \overline{M} = I\overline{M} \neq \overline{M}$. Now, if $\mathbf{x}$ extends to a maximal M-sequence $\{x_1, \ldots, x_r, \ldots, x_n\}$ in I, then $\{x_{r+1}, \ldots, x_n\}$ is a maximal $M/\mathbf{x}M$-sequence in I. From this, the second equality above follows immediately. For the first, we just have to show that $\{\overline{x}_{r+1}, \ldots, \overline{x}_m\}$ is a maximal $M/\mathbf{x}M$-sequence in $\overline{I}$. But this is immediate. □

rrrs-reg-seq-sop

PROPOSITION 10.4.12. *If R is local, and $M \neq 0$, then every M-sequence in R extends to a system of parameters for M. In particular, we have*

$$\operatorname{depth} M \leq \dim M.$$

PROOF. From (10.1.3), we see that for any M-sequence $\mathbf{x} \subset R$ of length r, we have

$$\dim M/\mathbf{x}M = \dim M - r.$$

So given any system of parameters form $M/\mathbf{x}M$, we get one for M, by adjoining $\mathbf{x}$ to it. The inequality then follows immediately from (6.2.8). □

rrrs-grade-less-height

COROLLARY 10.4.13. *For any ideal $I \subset R$, we have*

$$\operatorname{depth} I \leq \operatorname{ht} I.$$

PROOF. We have from Propositions (10.4.9) and (10.4.12) that

$$\begin{aligned}\operatorname{depth} I &= \min\{\operatorname{depth} R_P : P \in V(I)\} \\ &\leq \min\{\dim R_P : P \in V(I)\} = \operatorname{ht} I.\end{aligned}$$

□

rrrs-depth-min-dim-ass

PROPOSITION 10.4.14. *If $(R, \mathfrak{m})$ is local, and $M \neq 0$, then*

$$\operatorname{depth} M \leq \dim R/P,$$

for every $P \in \operatorname{Ass} M$.

PROOF. We prove this by induction on $\operatorname{depth} M$. If $\operatorname{depth} M = 0$, then the statement is trivial. So assume $\operatorname{depth} M > 0$; then we can find some regular element $x \in \mathfrak{m}$. Now, if $Q \in \operatorname{Ass} M/xM$, we see, by Proposition (10.4.11) and the induction hypothesis, we have

$$\dim R/Q \geq \operatorname{depth} M/xM = \operatorname{depth} M - 1.$$

So to finish our proof, it will be enough to find, for every $P \in \operatorname{Ass} M$, a $Q \in \operatorname{Ass} M/xM$ such that $P \subsetneq Q$. Given such a P, let $m \in M$ be such that Rm is the maximal cyclic R-submodule of M annihilated by P. If $m = xn$, then, for $a \in P$, $axn = 0$. But x is M-regular, and so $an = 0$, implying that Rn is annihilated by P. But $Rm \subsetneq Rn$, contradicting the maximality of Rm. Therefore, $m \notin xN$; this means that $P \subset \mathcal{Z}(M/xM)$, and so there is a $Q \in \operatorname{Ass} M/xM$ such that $P \subset Q$. Since $x \notin P$ (x is M-regular), we see that $P \notin \operatorname{Ass} M/xM$, and so $P \subsetneq Q$, which finishes our proof. □

5. Behavior of Depth under Flat Extensions

Just as for dimension (6.7.2), we'd like to know how depth behaves under flat change of rings. For the rest of this section, fix a local homomorphism $f : (R, \mathfrak{m}, k) \to (S, \mathfrak{n}, l)$.

rrs-prod-formula-loc-hom

LEMMA 10.5.1. *If M is a finitely generated R-module and N is a finitely generated S-module that's flat over R, then we have the formula*

$$\dim_l \operatorname{Hom}_S(l, M \otimes N) = \dim_k \operatorname{Hom}_R(k, M) \cdot \dim_l \operatorname{Hom}_S(l, N/\mathfrak{m}N).$$

PROOF. Observe that we have

$$\begin{aligned} \operatorname{Hom}_S(l, \operatorname{Hom}_S(S/\mathfrak{m}S, M \otimes N)) &\cong \operatorname{Hom}_S(l \otimes S/\mathfrak{m}S, M \otimes N) \\ &\cong \operatorname{Hom}_S(l, M \otimes N). \end{aligned}$$

Since M is finitely presented and N is flat, we use (3.1.11) to find:

$$\begin{aligned} \operatorname{Hom}_S(S/\mathfrak{m}S, M \otimes N) &\cong \operatorname{Hom}_S(k \otimes S, M \otimes N) \\ &\cong \operatorname{Hom}_R(k, M) \otimes N \\ &\cong (N/\mathfrak{m}N)^s, \end{aligned}$$

where $s = \dim_k \operatorname{Hom}_R(k, M)$. We get the formula we need from this relation. □

lat-fiber-depth-equality

PROPOSITION 10.5.2. *Let $f : (R, \mathfrak{m}, k) \to (S, \mathfrak{n}, l)$ be a local homomorphism of local rings. If M is a finitely generated R-module, and N is a finitely generated S-module flat over R, then*

$$\operatorname{depth}_S(M \otimes_R N) = \operatorname{depth}_R M + \operatorname{depth}_S N/\mathfrak{m}N.$$

In particular, if f is itself a flat map, then we have

$$\operatorname{depth} S = \operatorname{depth} R + \operatorname{depth} S/\mathfrak{m}S.$$

PROOF. First, let's assume that $\operatorname{depth}_R M = \operatorname{depth}_S N/\mathfrak{m}N = 0$. In this case, we see from (10.4.7), that

$$\operatorname{Hom}_R(k, M) \neq 0; \operatorname{Hom}_S(l, N/\mathfrak{m}N) \neq 0.$$

Then, from Lemma (10.5.1), we see that

$$\operatorname{Hom}_S(l, M \otimes N) \neq 0,$$

and so, again by (10.4.7), we see that $\operatorname{depth}_S(M \otimes N) = 0$, just as we expected.

Now, we can reduce the general case to this situation in the following fashion. Suppose $\mathbf{x}$ is a maximal M-sequence of length r, and $\mathbf{y}$ is a maximal $N/\mathfrak{m}N$-sequence of length s. Then, we have

$$\operatorname{Ext}^r_R(k, M) \cong \operatorname{Hom}_R(k, M/\mathbf{x}M) \neq 0$$
$$\operatorname{Ext}^s_S(l, N/\mathfrak{m}N) \cong \operatorname{Hom}_S(l, N'/\mathfrak{m}N') \neq 0,$$

where $N' = N/\mathbf{y}N$. Observe that both $M' = M/\mathbf{x}M$ and $N'/\mathfrak{m}N'$ have depth 0. Moreover, by (10.2.3), N' is R-flat. So we can use what we found at the beginning of the proof to see that

$$\operatorname{Hom}_S(l, M' \otimes N') \neq 0.$$

But note that

$$M' \otimes N' \cong (M \otimes N)/\mathbf{z}(M \otimes N),$$

where $\mathbf{z} = f(\mathbf{x}) \cup \mathbf{y}$.

So we see, by (10.4.4), that

$$\operatorname{Ext}^{r+s}_S(l, M \otimes N) \cong \operatorname{Hom}_S(l, (M \otimes N)/\mathbf{z}(M \otimes N) \neq 0.$$

Now, to show that $\operatorname{depth}_S(M \otimes N) = r + s$, it suffices to show that $\operatorname{Ext}^k_S(l, M \otimes N) = 0$, for $k < r + s$. For this, it's enough to show that $\mathbf{z}$ is an $(M \otimes N)$-regular sequence. Here, use (10.2.3) again, with P replaced by $M/\mathbf{x}M$ to see that $\mathbf{y}$ is $(M \otimes N)/\mathbf{x}(M \otimes N)$-regular, since

$$(M \otimes N)/\mathbf{x}(M \otimes N) \cong (M/\mathbf{x}M) \otimes N.$$

This finishes our proof. □

CHAPTER 11

The Cohen Macaulay Condition

chap:cmr

1. Basic Definitions and Results

DEFINITION 11.1.1. A finitely generated module M over a local Noetherian ring R is *Cohen-Macaulay* if $\operatorname{depth} M = \dim M$.

A Noetherian ring A is *Cohen-Macaulay* if, for every prime $P \subset A$, A_P is a Cohen-Macaulay module over itself.

For the next few results, we'll fix a local Noetherian ring R and a Cohen-Macaulay module M over R.

cmr-unmixedness

PROPOSITION 11.1.2. *For every $P \in \operatorname{Ass} M$, we have $\dim A/P = \dim M$. Moreover, every prime associated to M is minimal over $\operatorname{ann}(M)$.*

PROOF. The second statement follows immediately from the first. For the first, observe from (10.4.14) that we have for any $P \in \operatorname{Ass} M$:

$$\dim M \geq \dim A/P \geq \operatorname{depth} M = \dim M.$$

□

cmr-ideal-unmixed

COROLLARY 11.1.3. *If A is a Cohen-Macaulay ring, $I \subset A$ is an ideal such that $\operatorname{ht} I = \operatorname{depth} I$; then we have $\operatorname{ht} I + \dim R/I = \dim R$.*

PROOF. □

cmr-dim-dec-iff-reg

LEMMA 11.1.4. *For $x \in R$, we have*

$$\dim M/xM = \dim M - 1$$

iff $x \notin \mathcal{Z}(M)$.

PROOF. In one direction, if $x \notin \mathcal{Z}(M)$, we see that $\dim M/xM = \dim M - 1$ from (10.1.3). For the other, since $\dim M/xM = \dim M - 1$, we see that x is not contained in any minimal prime of $R/\operatorname{ann}(M)$. But from the last Proposition, we see that all the primes associated to M are minimal over $\operatorname{ann}(M)$; so $x \notin \mathcal{Z}(M)$. □

cmr-sop-iff-reg-seq

PROPOSITION 11.1.5. *A sequence $\mathbf{x} \subset R$ is an M-sequence iff it is part of a system of parameters for M. In particular, if $\mathbf{x}$ is a system of parameters for M, then $M/\mathbf{x}M$ is also Cohen-Macaulay.*

PROOF. Note that a sequence $\mathbf{x}$ of length r is part of a system of parameters for M iff

$$\dim M/\mathbf{x}M = \dim M - r.$$

If we use the lemma above inductively, then we'll see that this is also equivalent to $\mathbf{x}$ being an M-sequence.

For the second statement, just use (10.1.3) and (10.4.11). □

The reason Cohen-Macaulay rings are important from a geometric point of view is that they are 'height unmixed'. That is, if we consider a subvariety of a Cohen-Macaulay variety, then all its irreducible components will be of the same dimension.

2. Characterizations of Cohen-Macaulay Modules

CHAPTER 12

Homological Theory of Regular Rings

chap:rloc

1. Regular Local Rings

c-regular-cohen-macaulay

PROPOSITION 12.1.1. *For any regular local ring R, we have $\dim R = \operatorname{depth} R$. That is, every regular local ring is Cohen-Macaulay.*

PROOF. We'll prove this by induction on $\operatorname{depth} R$. When $\operatorname{depth} R = 0$, every element of $\mathfrak{m}$ is a zero-divisor. By the last Proposition R is a domain, and so this means that $\mathfrak{m} = 0$, implying that $\dim R = 0$.

Now, suppose $\operatorname{depth} R > 0$; then pick $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Let $R' = R/(x)$; we then have, by Propositions (10.1.3) and (10.4.11) that

$$\dim R' = \dim R - 1; \operatorname{depth} R' = \operatorname{depth} R - 1.$$

So if we show that R' is regular, then we'll by done by the induction hypothesis. But if $\mathfrak{m}' \subset R'$ is the maximal ideal, then we have

$$\mathfrak{m}'/\mathfrak{m}'^2 \cong \mathfrak{m}/(\mathfrak{m}^2 + (x)) \cong (\mathfrak{m}/\mathfrak{m}^2)/(\mathfrak{m}^2 + (x)/\mathfrak{m}^2),$$

as $R/\mathfrak{m}$-modules. Since $x \notin \mathfrak{m}^2$, we see that $\dim(\mathfrak{m}^2 + (x)/\mathfrak{m}^2) = 1$. Thus,

$$\dim \mathfrak{m}'/\mathfrak{m}'^2 = \dim \mathfrak{m}/\mathfrak{m}^2 - 1,$$

and so, by Nakayama's lemma, $\mathfrak{m}'$ is generated by $\dim R - 1$ elements. This shows that R' is regular and finishes the proof. □

2. Characterization of Regular Rings

Here we give the extremely important homological characterization of regular local rings.

-local-characterizations

THEOREM 12.2.1. *Let $(R, \mathfrak{m})$ be a Noetherian local ring of dimension n. Then the following statements are equivalent*

1. *R is regular.*
2. *$\mathfrak{m}$ can be generated by an R-sequence.*
3. *The $R/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ has dimension n.*
4. *$\operatorname{gl\,dim} R < \infty$, in which case $\operatorname{gl\,dim} R = n$.*
5. *The natural map $(R/\mathfrak{m})[t_1, \ldots, t_n] \longrightarrow \operatorname{gr}_{\mathfrak{m}}(R)$ is an isomorphism.*

PROOF. We'll show (2) ⇒ (4) now. First, assume (2); then let $\mathbf{x}$ be a regular sequence generating $\mathfrak{m}$. By the remark after Proposition (**??**), if we set $F_i = K_R^{n-i}(\mathbf{x})$, then we get a free resolution $F_\bullet$ of $k = R/\mathfrak{m}$ of length n. If we tensor this resolution with k, then we get the Koszul complex $K_k^\bullet(\mathbf{x})$. Since $\operatorname{depth} k = 0$, we see that $H^0(\mathbf{x}, k) \neq 0$ (**??**), implying that $H_n(F \otimes k) \neq 0$. From this, we deduce that $\operatorname{Tor}_n^R(k, k) = k \neq 0$. This establishes that $\operatorname{pd} k = n$, and we see now by Corollary (**??**) that $\operatorname{gl\,dim} R = n < \infty$.

Finally, suppose (4) holds; we'll prove (1) by induction on $\mu(R) = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. If this is 0, then $\mathfrak{m} = 0$, and R is a field, and hence regular. So we can assume $\mu(R) > 0$; we claim that in this case $\mathfrak{m} \notin \operatorname{Ass} R$. For, suppose that were true, with $\mathfrak{m} = \operatorname{ann}_R(a)$; then if we take any minimal free resolution $F_\bullet$ of k of length r, we'd have $F_r \subset \mathfrak{m}F_{r-1}$, and so $aF_r = 0$, which contradicts the fact that F_r is free. Since $\mathfrak{m} \notin \operatorname{Ass} R$, we can pick, by prime avoidance, an $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ such that x is R-regular. Now, consider the ring $R' = R/(x)$. If we take a finite free resolution of $\mathfrak{m}$, and tensor that with R', then, since x is R-regular, we see by Proposition (10.2.2) that we have a finite free resolution of $\mathfrak{m}/x\mathfrak{m}$ over R'. We will show that $\mathfrak{m}/(x)$ is a direct summand of $\mathfrak{m}/x\mathfrak{m}$ and thus also has finite projective dimension. Moreover,

$$\mu(R') = \dim_k \mathfrak{m}/(\mathfrak{m}^2 + (x)) < \dim_(\mathfrak{m}/\mathfrak{m}^2) = \mu(R),$$

since $x \notin \mathfrak{m}^2$. So by the induction hypothesis, R' will be regular of dimension $\dim R - 1$; but if $\mathbf{x}$ is a sequence in R whose image is a regular sequence generating $\mathfrak{m}/(x)$, we see that $\mathbf{x} \cup x$ is a regular sequence of length $\dim R$ generating $\mathfrak{m}$, thus showing that R is regular.

So it remains only to show that $\mathfrak{m}/x\mathfrak{m}$ is a direct summand of $\mathfrak{m}/(x)$. For this, choose any elements $x_2, \dots, x_r \in \mathfrak{m}$ such that the images of $x, x_2, \dots, x_r$ form a basis for $\mathfrak{m}/\mathfrak{m}^2$. Let $J = (x_2 \dots, x_r)$; then, since the generators of J and x are linearly independent over k, we see immediately that $J \cap (x) \subset x\mathfrak{m}$. Given this, we have the following sequence of maps.

$$\mathfrak{m}/(x) = J + (x)/(x) \cong J/(J \cap (x)) \to \mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}/(x).$$

If we follow the residue class of each x_i through these maps, we'll see that it remains unchanged at the end. So the natural quotient map $\mathfrak{m}/x\mathfrak{m} \to \mathfrak{m}(x)$ in fact splits, and $\mathfrak{m}/(x)$ is a direct summand of $\mathfrak{m}/x\mathfrak{m}$. This finishes our proof. □

This has important corollaries. But before we state them, we need a lemma.

loc-pdim-sup-local-pdims

LEMMA 12.2.2. *If R is a Noetherian ring, then we have*

$$\operatorname{gl\,dim} R = \sup\{\operatorname{gl\,dim} R_P : P \in \operatorname{Spec} R\} =: \phi(R).$$

PROOF. Recall from (**??**) that $\operatorname{gl\,dim} R \leq n$ iff $\operatorname{Ext}^k_R(M, N) = 0$, for all $k > n$ and all R-modules M and N.

Every projective resolution of an R-module M gives rise to a projective resolution of the R_P-module M_P when tensored with R_P. So we see that $\operatorname{gl\,dim} R \geq \phi(R)$. If $\phi(R) = \infty$, then there's nothing to prove; so assume that $\phi(R) = n$ is finite. Then we see that for all R-modules M, N and all primes $P \subset R$, we have

$$\operatorname{Ext}^k_{R_P}(M_P, N_P) = 0, \text{ for all } k > n.$$

But, since R is Noetherian, we know that

$$\operatorname{Ext}^k_R(M, N)_P = \operatorname{Ext}^k_{R_P}(M_P, N_P).$$

This follows essentially from (3.1.12). So we see immediately from Auslander's characterization that $\operatorname{gl\,dim} R \leq \phi(R)$, which finishes our proof. □

DEFINITION 12.2.3. A Noetherian ring is *regular* when all its localizations at primes are regular local rings.

rloc-regular-fin-gldim

COROLLARY 12.2.4. *A Noetherian ring R is regular iff it has finite global dimension, and in this case we have*

$$\operatorname{gl\,dim} R = \dim R$$

PROOF. By the Lemma, a Noetherian ring R has finite global dimension iff every localization R_P has finite global dimension. But, by the Theorem, this can only happen iff every R_P is in fact a regular local ring. Moreover, we have

$$\begin{aligned}\operatorname{gl\,dim} R &= \sup\{\operatorname{gl\,dim} R_P : P \in \operatorname{Spec} R\} \\ &= \sup\{\dim R_P : P \in \operatorname{Spec} R\} = \dim R.\end{aligned}$$

□

rloc-loc-reg-regular

COROLLARY 12.2.5. *Every localization of a regular ring is regular.*

PROOF. Suppose R is a regular ring, and S is a multiplicative subset of R; then just as in the Proposition above, we can see that $\operatorname{gl\,dim} S^{-1}R \leq \operatorname{gl\,dim} R < \infty$. This, and the the Corollary above, finish our proof. □

3. Behavior under Flat Extensions

As always, we'd like to see how regularity behaves under flat extensions.

oc-regularity-flat-extns

PROPOSITION 12.3.1. *Suppose $f : (R, \mathfrak{m}, k) \to (S, \mathfrak{n}, l)$ is a flat, local homomorphism of local, Noetherian rings. Then:*

1. *If S is regular, then so is R.*
2. *If R and $S/\mathfrak{m}S$ are regular, then so is S.*

PROOF. (1) Let $F_\bullet$ be a minimal, free resolution of $k = R/\mathfrak{m}$; then $F_\bullet \otimes S$ is a minimal, free resolution of $k \otimes S = S/\mathfrak{m}S$, since

$$\operatorname{im} F_i \otimes S \subset \mathfrak{m}F_{i+1} \otimes S \subset \mathfrak{n}(F_{i+1} \otimes S).$$

This implies that

$$\operatorname{pd} k = \operatorname{pd}_S S/\mathfrak{m}S < \infty,$$

and so R is regular.

(2) Suppose $\{x_1, \ldots, x_r\} \subset R$ is a minimal set of generators for $\mathfrak{m}$, and suppose $\{y_1, \ldots, y_s\} \subset S$ is a minimal set of generators for $\mathfrak{n}/\mathfrak{m}S \subset S/\mathfrak{m}S$. Then $\{x_1, \ldots, x_r, y_1, \ldots, y_s\}$ generate $\mathfrak{n}$.

Now, we have, by (6.7.2), that

$$\dim S = \dim R + \dim S/\mathfrak{m}S = r + s.$$

Hence, the set above is in fact a minimal set of generators for $\mathfrak{n}$, and we see therefore that S is regular.

□

mpletion-regular-regular

COROLLARY 12.3.2. *If $(R, \mathfrak{m})$ is a local ring, then it's regular iff its completion $(\hat{R}, \hat{\mathfrak{m}})$ is regular.*

PROOF. Suppose R is regular; by the Proposition above, we only have to show that $\hat{R}/\mathfrak{m}\hat{R}$ is regular. But this is just $\hat{R}/\hat{m}x$, which is a field.

Now, assume $\hat{R}$ is regular; then that R is also regular follows from part (1) of the Proposition. □

A very important result that follows from a combined application of our main theorem and the Auslander-Buschsbaum formula is a criterion for a ring to be Cohen-Macaulay.

loc-cm-iff-free-over-reg

PROPOSITION 12.3.3. *Suppose $f : (R, \mathfrak{m}) \to (S, \mathfrak{n})$ is a local homomorphism of local rings so that S is finite over R. Then the following statements are true:*

(1) *If R is regular, then S is Cohen-Macaulay iff S is free over R.*
(2) *If S is regular, then R is regular iff S is free over R.*

PROOF. (1) Since R is regular, and S is finite over R, we see that S has finite projective dimension over R. So we can apply the Auslander-Buschsbaum formula to see that

$$\operatorname{pd}_R S = \operatorname{depth} R - \operatorname{depth}_R S = \dim R - \operatorname{depth} S,$$

where the last equality follows from CM-ness of R, and [BHP, 1.26]. But S is CM iff $\operatorname{depth} S = \dim S = \dim R$. From this the statement follows.

(2) First suppose that R is regular; then, since S is regular, and hence CM, it follows from the first part that S is free over R. Conversely, if S is free over R, then in particular it's flat, in which case, (12.3.1) gives us the result.

□

PROPOSITION 12.3.4. *Suppose R is a Noetherian ring. Then, the following statements are equivalent:*

(1) *R is regular.*
(2) *$R[x_1, \ldots, x_n]$ is regular, for some indeterminates $x_1, \ldots, x_n$.*
(3) *$R[[x_1, \ldots, x_n]]$ is regular, for some indeterminates $x_1, \ldots, x_n$.*

PROOF. (1) $\Rightarrow$ (2): It clearly suffices to prove that, if R is regular, then so is $R[x]$, for some indeterminate x. First, assume $R = k$ is a field. Then, $k[x]$ is a Dedekind domain, and $k[x]_{\mathfrak{n}}$ is a DVR, and hence a regular local ring, for any maximal ideal $\mathfrak{n} \subset k[x]$. So we see that $k[x]$ is regular. Now, let R be an arbitrary regular ring, and let $\mathfrak{n} \subset R[x]$ be a maximal ideal. We want to show that $R[x]_{\mathfrak{n}}$ is a regular local ring. Let $\mathfrak{m} = R \cap \mathfrak{n}$; since $R_{\mathfrak{m}}$ is regular, it suffices, by Proposition (12.3.1), to show that $R[x]_{\mathfrak{n}}/\mathfrak{m}R[x]_{\mathfrak{n}}$ is regular. But we have

$$R[x]_{\mathfrak{n}}/\mathfrak{m}R[x]_{\mathfrak{n}} = (R[x]/\mathfrak{m}R[x])_{\mathfrak{n}} = (R/\mathfrak{m})[x]_{\mathfrak{n}} = k[x],$$

where $k = R_{\mathfrak{m}}/\mathfrak{m}_{\mathfrak{m}}$. So, by the first part of the proof, we see that this is regular, which shows that $R[x]_{\mathfrak{n}}$ is regular. Since $\mathfrak{n}$ was arbitrary, we see that $R[x]$ is regular.

(2) $\Rightarrow$ (3): Follows from Corollary (12.3.2).

(3) $\Rightarrow$ (1): Follows from part (1) of Corollary (12.3.1). □

4. Stably Free Modules and Factoriality of Regular Local Rings

rloc-stably-free

DEFINITION 12.4.1. An R-module M is *stably free*, if there exists a free R-module F such that $M \oplus F$ is free.

rloc-finpdim-stably-free

PROPOSITION 12.4.2 (Serre). *Any projective R-module M with a finite free resolution is stably free.*

PROOF. We'll do induction on the minimal length of a finite free resolution of M. If M has a free resolution of length 0, then M is already free; so we can assume that M has a finite free resolution $F_\bullet$ of minimal, non-zero length. If N is the first syzygy of this resolution, then N has a finite free resolution of lower length. Moreover, since $F_0 \cong M \oplus N$ (M is projective), we see that N is also projective. So by induction we can find a free R-module L such that $N \oplus L$ is free, and so $M \oplus (F_0 \oplus L)$ is free. □

rank-one-stablyfree-free

PROPOSITION 12.4.3. *If M is an R-module satisfying $M \oplus R^n \cong R^{n+1}$ for some $n \in Nat$, then $M \cong R$.*

PROOF. The given relation says that $M_P \cong R_P$ for every prime $P \subset R$. In particular, this means that $\bigwedge^i M_P = 0$, for all $i > 1$, for all $P \in \operatorname{Spec} R$. So we see that $\bigwedge^i M = 0$, for all $i > 1$. This means that

$$\begin{aligned} R &\cong \wedge^{n+1} R^{n+1} \\ &\cong \wedge^{n+1}(M \oplus R^n) \\ &\cong \bigoplus_{i=0,1} \wedge^i M \otimes \wedge^{n+1-i} R^n \\ &\cong \wedge^1 M \otimes \wedge^n R^n \\ &\cong M \otimes R \cong M. \end{aligned}$$

□

oc-stablyfree-ideal-free

COROLLARY 12.4.4. *Any non-zero stably free ideal I of a Noetherian ring R is a principal ideal generated by a non zero divisor.*

PROOF. We can assume that $I \neq 0$. Suppose L and F are two free R-modules of rank s and r respectively, such that $I \oplus L \cong F$. Then, let P be any prime such that $I_P \neq 0$. We know by (7.1.2) that I_P is a free R_P-module, and hence has rank 1. To see this, note that if we had two linearly independent basis elements $a, b \in I$, then we'll have $ab \in Ra \cap Rb = 0$, but this violates the torsion freeness of a free module. This immediately tells us that $s = r - 1$, allowing us to apply the previous Proposition. □

-loc-factorial-factorial

LEMMA 12.4.5 (Nagata). *Suppose R is a Noetherian domain and $x \in R$ is a prime element. Then, if R_x is a UFD, so is R.*

PROOF. Recall from the characterization of UFDs (7.3.3) that a Noetherian ring R is a UFD iff every height 1 prime in R is principal.

Now, suppose $P \subset R$ is a height 1 prime not containing x. Then, $P_x \subset R_x$ is principal. Let $(a) \subset P$ be a maximal principal ideal such that $aR_x = P_x$. In particular, this means that $a \notin (x)$, for if $a = sx$ we'll have a bigger principal ideal (s) also localizing to P_x.

If $b \in P$, then there is some minimal $k \in \mathbb{N}$ such that $x^k b \in (a)$. Suppose $k > 0$; then, if $c = x^{k-1}b$, we see that $c \notin (a)$, but $xc \in (a)$. Suppose $xc = ra$, for some $r \in R$; then, since (x) is prime, and $a \notin (x)$, we see that $r \in (x)$. But this means that $c = r'a$, for $r' = r/x$, which contradicts the fact that $c \notin (a)$. Hence $(a) = P$; this shows that any height 1 prime not containing x is principal. The only other height 1 prime in R is (x) itself, which is already principal. So we conclude that R is a UFD. □

rloc-regloc-ufd

THEOREM 12.4.6 (Auslander-Buchsbaum-Serre). *Every regular local ring is a UFD.*

PROOF. Suppose $(R, \mathfrak{m})$ is regular local, and $x \in R$ is a part of a regular sequence generating $\mathfrak{m}$. Then, $R/(x)$ is also regular local, and is thus a domain, by Proposition (??). So x is a prime element, and it suffices, by the lemma above, to show that R_x is a UFD. We'll use the criterion from (7.3.3) again.

Let $Q \subset R_x$ be a height 1 prime. We wish to show that Q is principal. Now, by Proposition (12.2.5), R_x is a regular ring, and so, for every maximal ideal $P \subset R_x$, $(R_x)_P$ is a regular local ring. But observe that $\dim R_x < \dim R$; we lose the maximal ideal $\mathfrak{m}$, since it contains x.

This tells us that induction on dimension might be a good idea. We know already that regular local rings of dimensions 0 and 1 are UFDs (they're fields and DVRs, respectively); so assume that $\dim R > 1$. Then, by induction, $(R_x)_P$ is a UFD, and so Q_P is principal. In particular, Q_P is free of rank 1. By (7.1.2), we see that Q is projective as an R_x-module.

Let $Q' \subset R$ be a prime ideal such that $Q'_x = Q$. Since Q' has finite projective dimension as an R-module (R has finite global dimension), we see that it has a finite free resolution over R. Tensoring this resolution with R_x gives us a finite free resolution of Q over R_x.

Now, by Serre's Lemma (12.4.2), we see that Q is stably free. Then, Corollary (12.4.4) tells us that Q is in fact free, and is thus a principal ideal. □

CHAPTER 13

Formal Smoothness and the Cohen Structure Theorems

chap:smooth

CHAPTER 14

Witt Rings

chap:witt

1. Cohen Structure Theorem: The Equicharacteristic Case

DEFINITION 14.1.1. Let $(R, F^\bullet R)$ be a filtered ring. We say that R is *equicharacteristic* if the residue ring R/F^1R has the same characteristic as the ring R. Otherwise, we say that it has *unequal characteristic*.

DEFINITION 14.1.2. Let $(R, F^\bullet R)$ be a filtered ring, and let $k = R/F^1R$ be its residue ring. A *multiplicative system of representatives* for R is a section $f : k \to R$ of the quotient map $R \to k$ such that the following conditions hold:

(1) For all $a, b \in k$, $f(ab) = f(a)f(b)$.
(2) If k has characteristic $p > 0$, then an element $r \in R$ lies in the image of f if and only if it has $(p^n)^{th}$ roots in R, for all $n \geq 0$.

If R is equicharacteristic, then we require in addition that f be a *ring homomorphism*.

The statement of the next Proposition is longer than its proof.

resentative-power-series

PROPOSITION 14.1.3. *Let R be a ring complete with respect to the I-adic filtration, where $I \subset R$ is an ideal generated by finitely many elements $(g_1, \ldots, g_n)$. Let $f : R/I \to R$ be a multiplicative system of representatives. Define a map*

$$\varphi : (R/I)[[T_1, \ldots, T_n]] \to R$$
$$aT_1^{i_1}T_2^{i_2}\ldots T_n^{i_n} \mapsto f(a)g_1^{i_1}\ldots g_n^{i_n},$$

where we extend the map on the monomials to the entire power series ring linearly, using the completeness of R. Then φ is always surjective, and when (R, I) is equicharacteristic, it is in fact a surjective homomorphism of rings.

PROOF. First observe that the image of φ is clearly closed under the taking of limits of convergent sequences. Now pick $r \in R$, and suppose that, for some $n > 1$, we have constructed an element s_n in the image of φ such that $r - s_n \in I^n$ (for $n = 1$, we can take $s_1 = f(\pi(r))$, where $\pi : R \to R/I$ is the natural map). Then we see that

$$r - s_n \equiv \sum_k f(a_k)\mathbf{g}^{\alpha_k} \pmod{I^{n+1}},$$

for some multi-indices α_k with $|\alpha_k| = n$. Take $s_{n+1} = s_n + \sum_k f(a_k)\mathbf{g}^{\alpha_k}$. In this way we can construct a sequence of elements in the image of φ converging to r.

If R is equicharacteristic, then f is a ring map, and φ is simply the unique ring map that takes T_i to g_i (5.4.2). □

epresentatives-char-zero

PROPOSITION 14.1.4. *Let $(R, F^\bullet R)$ be a complete ring with residue ring $k = R/F^1R$. Suppose R is equicharacteristic of characteristic zero, and suppose that k is in fact a field; then R has a multiplicative system of representatives.*

PROOF. Since R has characteristic zero, we have an inclusion of $\mathbb{Z}$ into R; since R maps onto the characteristic zero field k, we see that in fact $\mathbb{Q}$ must embed into R. Let S be a maximal sub-field of R. We claim that S maps isomorphically onto k under the natural surjection $\pi : R \to k$.

First observe that k is algebraic over $\pi(S)$. If this were not the case, then k would contain a copy of the function field $\pi(S)(t)$. Let $r \in R$ be an element mapping onto t; then $S[r]$ maps injectively into $\pi(S)[t]$, and so is isomorphic to $S[t]$. Moreover, $S[r] \cap F^1R = 0$, and so R must also contain a copy of the function field $S(t)$, which contradicts the maximality of S.

Given that k is algebraic over $\pi(S)$, for any $a \in A$, there is a monic polynomial $f(t) \in S[t]$ such that a is a simple zero of the polynomial $\pi(f(t))$ over $\pi(S)$. By (5.4.7), we can lift a to a zero r of the polynomial $f(t)$. But since S is a maximal sub-field of R, we see that $r \in S$, and so $a \in \pi(S)$, thus showing that S maps isomorphically onto k. The inverse map from k to S gives us the multiplicative system of representatives we were looking for. □

DEFINITION 14.1.5. A ring R is *perfect* if it either has characteristic 0, or if it has characteristic $p > 0$ and the Frobenius map $r \mapsto r^p$ is an automorphism of R.

witt-pth-powers

LEMMA 14.1.6. *Let $(R, F^\bullet R)$ be a complete ring, and suppose it has a residue ring $k = R/F^1R$ of characteristic $p > 0$. For $r, n \in \mathbb{N}$, if $b, b' \in R$ are such that $b \equiv b' \pmod{F^nR}$, then $b^{p^r} \equiv b'^{p^r} \pmod{F^{n+r}R}$.*

PROOF. Clearly it suffices to show that $b^p \equiv b'^p \pmod{F^{n+1}R}$. We can choose $r \in F^nR$ such that $b' = b + r$. Now we have

$$b'^p = b^p + \sum_{i \geq 1} \binom{p}{i} b'^i b^{p-i}.$$

Since p is prime, it divides $\binom{p}{i}$. Moreover, since k has characteristic p, $p \in F^1R$. Hence we see that the sum on the right hand side above is contained in $F^{n+1}R$, which is of course what we wanted to show. □

resentatives-finite-char

PROPOSITION 14.1.7. *With the hypotheses as in the Lemma above, suppose in addition that k is perfect. Then there exists a multiplicative system of representatives for R, which is the unique multiplicative section of the quotient map $R \to k$. Moreover, if R is equicharacteristic, then f is in fact a ring homomorphism*

PROOF. Pick an element $a \in k$. For each $n \in \mathbb{N}$, we can then find a unique residue class $a^{p^{-n}} \in k$ such that $(a^{p^{-n}})^{p^n} = a$. Suppose $r_n, r'_n \in R$ are two representatives of this residue class. Then, by the Lemma above, we have

$$r'^{p^n}_n \equiv r^{p^n}_n \pmod{F^{n+1}R}.$$

That is, there is a unique element $a_{n+1} \in R/F^{n+1}R$ such that $a_{n+1} \equiv a \pmod{F^1R}$ and such that a_{n+1} is a $(p^n)^{th}$ power. Given this, consider the coherent sequence $(a_n : n \geq 0)$ in $\lim R/F^nR$, where $a_1 = a$. Since R is complete, this corresponds to an element in R, which we will denote by $f(a)$. In fact this argument shows that $f(a)$ is the unique element in R such that $f(a) \equiv a \pmod{F^1R}$ and such that, for every $n \in \mathbb{N}$, its residue class in R/F^nR has a $(p^n)^{th}$ root in R.

Now, if a, b are two elements in k, and a_n, b_n are representatives in R/F^nR of the residue classes of a and b, respectively, such that both are $(p^n)^{th}$ powers, then a_nb_n is a representative of the residue class of ab that is also a $(p^n)^{th}$ power.

Therefore, we find that $f(ab) = f(a)f(b)$. If R also has characteristic p, then the same argument, using the fact that $r \mapsto r^p$ is now a ring homomorphism on R, serves to show that f is also a ring homomorphism.

Given this, we see immediately that every element in the image of f has $(p^n)^{th}$ roots, for all $n \geq 0$: for any n, we can just take $r_n = f(a^{p^{-n}})$, and we see that $r_n^{p^n} = f(a)$. Conversely, if $r \in R$ has $(p^n)^{th}$ roots, for all $n \geq 0$, then a representative of the residue class of r in R/F^nR has a $(p^n)^{th}$ root in R, which shows that $r = f(a)$, where $r \equiv a \pmod{F^1R}$.

Thus we have constructed a multiplicative system of representatives for R. For its uniqueness, observe that if $f' : k \to R$ is another multiplicative section of the quotient map, then, for every $a \in k$, $f'(a)$ has $(p^n)^{th}$ roots for all $n \geq 0$, and must therefore equal $f(a)$. □

EXAMPLE 14.1.8. Consider the ring of p-adics $\hat{\mathbb{Z}}_p$ and the the unique multiplicative system of representatives $f : \mathbb{F}_p \to \hat{\mathbb{Z}}_p$. Since f is multiplicative, it follows that every element in the image of f (apart from 0, of course) is a $(p-1)^{th}$ root of unity, and since there are precisely $p-1$ such roots of unity, we see that the multiplicative system of representatives on $\hat{\mathbb{Z}}_p$ also consists precisely of the $(p-1)^{th}$ roots of unity. These are called the *Teichmüller representatives*, and the bijection in (14.1.3) gives a *Teichmuüller representation* of every element in $\hat{\mathbb{Z}}_p$.

Now we're ready for the main result of this section.

rfect-equicharacteristic

THEOREM 14.1.9. *Let $(R, \mathfrak{m})$ be a complete, equicharacteristic, Noetherian local ring with perfect residue field $k = R/\mathfrak{m}$; then R is isomorphic to a quotient $k[[T_1, \ldots, T_n]]/I$ of some power series ring over k.*

PROOF. By (14.1.3), this will follow immediately if we can find a multiplicative system of representatives for R. We can definitely do this: when R has characteristic zero, we use (14.1.4), and when R has finite characteristic, we appeal to (14.1.7) instead. □

DEFINITION 14.1.10. Let $(R, \mathfrak{m})$ be a local ring. A *coefficient field* for R is a sub-field $K \subset R$ mapping isomorphically onto the residue field $k = R/\mathfrak{m}$.

lete-finite-power-series

PROPOSITION 14.1.11. *Let $(R, \mathfrak{m})$ be a complete, Noetherian local ring with residue field k, and suppose that R contains a coefficient field. Then R is finite over the power series ring $k[[t_1, \ldots, t_n]]$, where $n = \dim R$.*

PROOF. Let $\mathbf{x} \subset \mathfrak{m}$ be a system of parameters for R, so that $n = \dim R$ is the length of $\mathbf{x}$. Since R is also a k-algebra, we can consider the natural map $\varphi : k[[t_1, \ldots, t_n]] \to R$ induced by the sequence $\mathbf{x}$ (5.4.2). To check that this is a finite homomorphism, it suffices, by (5.2.8), to show that $R/\mathbf{x}R$ is finite over k. But this is immediate from the definition of a system of parameters. □

witt-coefficient-field

COROLLARY 14.1.12. *Every complete, equicharacteristic, Noetherian local ring $(R, \mathfrak{m})$ with perfect residue field contains a coefficient field. In particular, R is finite over the power series ring $k[[t_1, \ldots, t_n]]$, where $n = \dim R$. If R has finite characteristic, then this coefficient field is in fact unique.*

PROOF. The existence follows trivially from (14.1.9), and the uniqueness in the finite characteristic case follows at once from (14.1.7), since the existence of a coefficient field K is equivalent to the existence of a section $f : k \to R$ with image K. □

2. The Witt Scheme

The aim of this section is in essence to give a formula for multiplication in an I-adically complete ring (R, I) of unequal characteristic in terms of a multiplicative system of representatives. In particular, we will be able to give formulas for multiplication in $\hat{\mathbb{Z}}_p$ in terms of Teichmüller representations. This is a much more natural way of representing the p-adics than the naïve one that uses representatives $\{0, \dots, p-1\}$ of the residue classes, and is of course subsumed in a much more general study.

2.1. Generalities on Ring Schemes.

Definition 14.2.1. Let R be a ring, and let R-alg be the category of R-algebras. A *ring scheme over* R is a functor $F : R\text{-alg} \to \text{Ring}$. A ring scheme F is *representable* if there exists an R-algebra S such that F is isomorphic to the functor $\text{Hom}_{R\text{-alg}}(S, \_\_)$. In this case, we say that F is *represented by* S. Abusing language, we might also call S a ring scheme in this situation. Sometimes, to make the distinction clear, we will refer to S (or $\operatorname{Spec} S$) as the *underlying* R*-scheme* of the ring scheme F. It is possible for two representable ring schemes to have the same underlying R-scheme.

A *homomorphism* between two ring schemes F and G over R is simply a natural transformation from F to G.

Remark 14.2.2. To clarify certain concepts, we will, as above, use some basic terminology and facts from scheme theory. In this setting, a representable ring scheme over R is just a ring object in the category of schemes over R.

Remark 14.2.3. If an R-algebra S represents a ring scheme over R, then it is naturally equipped with a co-ring structure; that is, two maps $a, m : S \to S \otimes_R S$ corresponding to co-addition and co-multiplications, and two maps $o, e : S \to R$ corresponding to the co-zero and the co-unit, and a co-additive co-inverse $i : S \to S$, all satisfying the duals of the usual commutative diagrams in the definition of a ring. In particular, if we forget the co-multiplication and the co-unit on S, we end up with an abelian group scheme over R.

In this setting, a homomorphism between representable ring schemes S and T becomes a homomorphism of R-algebras from T to S that respects the obvious commutative diagrams.

Example 14.2.4. The canonical example of a ring scheme over R is the polynomial ring $R[X]$; this represents the forgetful functor from R-alg to Ring. Co-addition and co-multiplication are given by

$$X \mapsto X \otimes 1 + 1 \otimes X$$
$$X \mapsto X \otimes X.$$

The co-zero is the surjection $R[X] \mapsto R[X]/(X) = R$ and the co-unit is the surjection $R[X] \mapsto R[X](X-1) = R$. The co-additive co-inverse is the map taking X to $-X$.

We will call this ring scheme $\mathbb{A}^1_R$.

Extending this further, we can show more generally that $R[X_1, \dots, X_n]$ represents the ring scheme taking every R-algebra to its n-fold direct product with itself, and that $R[X_i : i \geq 1]$ represents the ring scheme taking every R-algebra S to the

ring of sequences over S with component-wise addition and multiplication. We will call these ring schemes $\mathbb{A}^n_R$ and $\mathbb{A}^\infty_R$, respectively.

EXAMPLE 14.2.5. Another example of a representable ring scheme over R is the power series functor; that is, the functor that assigns to every R-algebra S, the ring of power series $S[[T]]$. It's represented by the ring $R[T_i : i \geq 0]$, where we define co-addition and co-multiplication by

$$T_i \mapsto T_i \otimes 1 + 1 \otimes T_i$$
$$T_i \mapsto \sum_{r+s=i} T_r \otimes T_s.$$

We'll call this ring scheme $\mathbb{T}_R$.

2.2. Ring Scheme Structures on Polynomial Algebras. Let R be a ring. Consider the ring scheme $\mathbb{A}^\infty_R$. For the corresponding operations of co-addition and co-multiplication on $R[X_i : i \geq 1]$, we can find polynomials $\Phi^a(U,V)$ and $\Phi^m(U,V)$ in two variables over $\mathbb{Z}$ such that

$$a(X_i) = \Phi^a(X_i \otimes 1, 1 \otimes X_i)$$
$$m(X_i) = \Phi^m(X_i \otimes 1, 1 \otimes X_i),$$

for all $i \geq 1$. More explicitly, we have $\Phi^a(U,V) = U + V$ and $\Phi^m(U,V) = UV$. Note that the co-zero, the co-unit and the co-additive co-inverse are also given by polynomials in (at most) two variables. In fact, using analogous notation, we have $\Phi^e(U,V) = 1$, $\Phi^o(U,V) = 0$, and $\Phi^i(U,V) = -U$.

In this section, we will investigate more general ring scheme structures that one can equip the polynomial ring $R[X_1, \ldots, X_n]$ with. In particular, we will establish a condition for a morphism of R-schemes from a ring scheme F over R with underlying R-scheme $R[T_1, \ldots, T_n]$ to $\mathbb{A}^\infty$ to be a homomorphism of ring schemes over R.

Now, a ring scheme structure on $R[T_1, \ldots, T_n]$ is given by families of polynomials $\{\gamma^\alpha_r \in R[U_1, \ldots, U_n]^{\otimes 2} : 1 \leq r \leq n\}$, for $\alpha = e, o, i, a, m$, corresponding respectively to the co-unit, the co-zero, the co-additive co-inverse, co-addition and co-multiplication, so that we have

$$\alpha(T_r) = \gamma^\alpha_r(T_1 \otimes 1, \ldots, T_n \otimes 1; 1 \otimes T_1, \ldots, 1 \otimes T_n).$$

Of course, when $\alpha = e, o$, the polynomials γ^α_r are constants, and when $\alpha = i$, they are independent the second set of indeterminates, and the structures provided by these polynomials must be coherent with each other, so that we can put them together to get a ring scheme structure. But for now it doesn't matter what the relationships between these polynomials are. We'll denote such a ring scheme structure on $R[T_1, \ldots, T_n]$ by $\mathbb{P}_\gamma$.

NOTE ON NOTATION 12. From now on, we will use T_i and T'_i to denote the elements $T_i \otimes 1$ and $1 \otimes T_i$ in the tensor product of the polynomial algebra with itself.

Now suppose S is an R-algebra. What do the ring operations on $\mathbb{P}_\gamma(S)$ look like? Suppose $\varphi, \psi : R[T_1, \ldots, T_n] \to S$ are two maps of R-algebras. Then we have

$$\begin{aligned}(\varphi + \psi)(T_r) &= (\varphi \otimes \psi)(\gamma^a_r(T_1, \ldots, T_n; T'_1, \ldots, T'_n)) \\ &= \gamma^a_r(\varphi(T_1), \ldots, \varphi(T_n); \psi(T_1), \ldots, \psi(T_n)). \\ (\varphi\psi)(T_r) &= \gamma^m_r(\varphi(T_1), \ldots, \varphi(T_n); \psi(T_1), \ldots, \psi(T_n)).\end{aligned}$$

ial-ring-scheme-morphism

PROPOSITION 14.2.6. *Let $\mathbb{P}_\gamma$ be a ring scheme over R with underlying R-scheme $R[T_1, \ldots, T_n]$, and let $\chi : \mathbb{P}_\gamma \to \mathbb{A}^\infty$ be a morphism of R-schemes given by polynomials $P_1, \ldots, P_n \in R[T_1, \ldots, T_n]$. Then χ is a homomorphism of ring schemes over R if and only if, for $1 \leq r \leq n$, and for $\alpha = e, o, i, a, m$, the following identity holds:*

$$\Phi^\alpha(P_r(T_1, \ldots, T_n), P_r(T'_1, \ldots, T'_n)) = P_r(\gamma_1^\alpha(T_1, \ldots, T_n; T'_1, \ldots, T'_n), \ldots, \gamma_n^\alpha(T_1, \ldots, T_n; T'_1, \ldots, T'_n)).$$

PROOF. Let $\psi : R[X_1, \ldots, X_n] \to R[T_1, \ldots, T_n]$ be the R-algebra map corresponding to χ. We have $\psi(X_r) = P_r(T_1, \ldots, T_n)$. Then the left hand side is just $(\psi \otimes \psi)(\alpha(X_r))$ and the right hand side is $\alpha(\psi(X_r))$, and χ defines a homomorphism of ring schemes if and only if we have

$$(\psi \otimes \psi)(\alpha(X_r)) = \alpha(\psi(X_r)),$$

for $\alpha = e, o, i, a, m$. □

2.3. The Universal Witt Scheme.

DEFINITION 14.2.7. For each $n \geq 0$, the n^{th} *Witt polynomial* W_n is an element of $\mathbb{Z}[T_1, \ldots, T_n]$ given by

$$W_n(T_1, \ldots, T_n) = \sum_{d|n} dT_d^{n/d}.$$

DEFINITION 14.2.8. We say that a subset $S \subset \mathbb{N}$ is a *sieve* if is is closed under the taking of factors; that is, if, for all $s \in S$ and for all $d \mid s$, $d \in S$. The *set of prime divisors* $p(S)$ of a sieve S is the collection of primes dividing any element in S. A *principal sieve* is a sieve of the form $\{d \in \mathbb{N} : \ d \mid n\}$, for some $n \in \mathbb{N}$, and is denoted by $S(n)$.

REMARK 14.2.9. Clearly, we can express an indeterminate T_n in terms of the W_j using rational coefficients and only such j as divide n. In other words, for all n, $T_n \in \mathbb{Q}[W_j : \ j \in S(n)]$. For example, we have $T_2 = \frac{1}{2}(W_2 - W_1^2)$.

DEFINITION 14.2.10. Let $\mathbb{W}$ be the scheme $\operatorname{Spec} \mathbb{Z}[T_i : \ i \geq 1]$; then the polynomials W_n give us a morphism φ of schemes from $\mathbb{W}$ to $\mathbb{A}^\infty$ (we omit the $\mathbb{Z}$, since it's clear from context) called the *Witt transformation*.

witt-truncated

DEFINITION 14.2.11. Let $S \subset \mathbb{N}$ be a sieve, and let $\mathbb{W}^S = \operatorname{Spec} \mathbb{Z}[T_s : \ s \in S]$, $\mathbb{A}^S = \operatorname{Spec} \mathbb{Z}[X_s : \ s \in S]$; then φ descends to a morphism φ^S from $\mathbb{A}^S$ to $\mathbb{W}^S$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{W} & \xrightarrow{\varphi} & \mathbb{A}^\infty \\ \downarrow & & \downarrow \\ \mathbb{W}^S & \xrightarrow{\varphi_S} & \mathbb{A}^S \end{array}$$

This basically follows from the fact that the polynomials W_s are given entirely in terms of indeterminates T_d, where $d \mid s$. This is called a *truncated Witt transformation associated to the sieve* S, and the natural map from $\mathbb{W}$ to $\mathbb{W}^S$ is called the *S-truncation*.

REMARK 14.2.12. Since we can express the T_i in terms of the W_j using rational coefficients, this gives us a section of φ over $\mathbb{A}^\infty_{\mathbb{Q}} = \mathbb{A}^\infty \times \operatorname{Spec} \mathbb{Q}$. That is, we have a morphism

$$\psi : \mathbb{A}^\infty_{\mathbb{Q}} \to \mathbb{W}_{\mathbb{Q}}$$

that is an inverse to $\varphi_{\mathbb{Q}} : \mathbb{W}_{\mathbb{Q}} \to \mathbb{A}^\infty_{\mathbb{Q}}$. We define a ring structure on $\mathbb{W}_{\mathbb{Q}}$ using this isomorphism on $\mathbb{A}^\infty_{\mathbb{Q}}$, and this makes $\mathbb{W}_{\mathbb{Q}}$ a ring scheme over $\mathbb{Q}$.

Moreover, for any sieve S, the inverse $\psi : \mathbb{A}^\infty_{\mathbb{Q}} \to \mathbb{W}_{\mathbb{Q}}$ descends to an inverse ψ^S to φ^S. Hence, for each such set S, we have a unique ring structure on $\mathbb{W}^S_{\mathbb{Q}}$ that makes $\varphi^S_{\mathbb{Q}}$ an isomorphism of ring schemes over $\mathbb{Q}$.

Observe moreover that, if $p(S)$ is finite (for example, if $S = \{p^i : i \geq 0\}$), then we can in fact find a principal open subscheme $\operatorname{Spec} \mathbb{Z}[1/n]$ inside $\operatorname{Spec} \mathbb{Z}$, where $n = \prod_{p \in p(S)} p$, such that the morphism

$$\varphi^S_{\mathbb{Z}[1/n]} : \mathbb{W}^S \times \operatorname{Spec} \mathbb{Z}[1/n] \to \mathbb{A}^S \times \operatorname{Spec} \mathbb{Z}[1/n]$$

has an inverse. Thus in this case φ^S is a birational morphism.

t-mod-p-witt-polynomials

LEMMA 14.2.13. *For any pair of n-tuples of elements $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ over a ring R, and a prime $p \in \mathbb{Z}$ such that $a_i \equiv b_i \pmod{pR}$, for all i, we have*

$$W_n(a_1, \ldots, a_n) \equiv W_n(b_1, \ldots, b_n) \pmod{p^{r+1}R},$$

where p^r is the greatest power of r dividing n.

PROOF. This is immediate using the definition of the Witt polynomials, and lemma (14.1.6) □

The next result is crucial. Before we dive into it, consider a polynomial $\Phi \in \mathbb{Z}[U, V]$ in two variables; then we claim that there exist uniquely determined polynomials $\gamma_n \in \mathbb{Q}[U_s : s \in S(n)]^{\otimes 2}$ such that

$$\Phi(W_i(T_s : s \in S(i)), W_i(T'_s : s \in S(i)) = W_i(\gamma_1(T_1; T'_1), \ldots, \gamma_i(T_s; T'_s : s \in S(i))).$$

In fact, γ_r will have its coefficients in $\mathbb{Z}[r^{-1}][U_s : s \in S(n)]$. This follows from the observation that we can extract γ_r in the following fashion: if $P_r \in \mathbb{Z}[r^{-1}][U_s : s \in S(r)]$ is the polynomial such that $P_r(W_s : s \in S(r)) = T_r$, then we set

$$\gamma_r = P_r(\Phi(W_s(T_k : k \in S(s)), W_s(T'_k : k \in S(s)) : s \in S(r)).$$

se-integral-coefficients

PROPOSITION 14.2.14. *Let $\Phi \in \mathbb{Z}[U, V]$ be a polynomial in two variables, and let $\gamma_n \in \mathbb{Q}[U_s : s \in S(n)] \otimes \mathbb{Q}[V_s : s \in S(n)]$ be the unique polynomials such that*

$$(*) \qquad \Phi(W_i(T_1, T_2, \ldots, T_i), W_i(T'_1, T'_2, \ldots, T'_i)) = W_i(\gamma_1(T_1; T'_1), \ldots, \gamma_i(T_1, \ldots, T_i; T'_1, \ldots, T'_i)),$$

for all $i \geq 1$. Then the polynomials γ_n in fact have their coefficients in $\mathbb{Z}$.

PROOF. We'll do this by induction on n. We already know that $\gamma_1 = \Phi$ is integral. Now, assume that $n > 1$ and that for all $d \in S(n)$, $d \neq n$, the polynomials γ_d satisfying the corresponding identity (*) are integral. Let p be a prime, and suppose $n = p^r m$, where $(p, m) = 1$. Then we have

$$\begin{aligned} W_n(T_1, \ldots, T_n) &= \sum_{d | p^{r-1} m} d X_d^{n/d} + \sum_{k | m} p^r k X_{p^r k}^{m/k} \\ &= W_{n/p}(T_1^p, \ldots, T_{n/p}^p) + \sum_{k | m} p^r k X_{p^r k}^{m/k} \end{aligned}$$

where $W_{n/p} = 0$ if $r = 0$. Assume that $r \neq 0$; thus we find:

$$\Phi(W_n(T_1, \ldots, T_n), W_n(T'_1, \ldots, T'_n)) = \Phi(W_{n/p}(T_1^p, \ldots, T_{n/p}^p), W_{n/p}(T'^p_1, \ldots, T'^p_{n/p})) + p^r G,$$

where G is a polynomial in T_{kp^r}, for $k \mid m$. We have the identity

$$\begin{aligned} W_n(\gamma_1, \ldots, \gamma_n) &= W_{n/p}(\gamma_1^p, \ldots, \gamma_{n/p}^p) + p^r(\sum_{k|m} \gamma_{p^r k}^{m/k}) \\ &= W_{n/p}(\gamma_1^p, \ldots, \gamma_{n/p}^p) + p^r(m\gamma_n + H(\gamma_{kp^r} : k \neq m). \end{aligned}$$

So we have

$$m\gamma_n - p^r H = \frac{\Phi(W_{n/p}(T_1^p, \ldots, T_{n/p}^p), W_{n/p}(T'^p_1, \ldots, T'^p_{n/p})) - W_{n/p}(\gamma_1^p, \ldots, \gamma_{n/p}^p)}{p^r} - G,$$

By induction, H is already an integral polynomial. We will show that p does not divide the denominators of the coefficients of γ_n, when they're in reduced form. For this it suffices to show

$$\Phi(W_{n/p}(T_1^p, \ldots, T_{n/p}^p), W_{n/p}(T'^p_1, \ldots, T'^p_{n/p})) \equiv W_{n/p}(\gamma_1^p, \ldots, \gamma_{n/p}^p) \pmod{p^r}.$$

This is equivalent to showing

$$W_{n/p}(\gamma_1(T_1^p, T'^p_1), \ldots, \gamma_{n/p}(T_1^p, \ldots, T'^p_{n/p})) \equiv W_{n/p}(\gamma_1^p, \ldots, \gamma_{n/p}^p) \pmod{p^r}.$$

This follows from the Lemma above, using the fact that $a \mapsto a^p$ is a homomorphism in characteristic p.

If p does not divide n, then, since γ_n has its coefficients in $\mathbb{Z}[1/n]$, p cannot divide the denominators of the coefficients of γ_n, when they're in reduced form. In particular, we have shown that no prime p divides the coefficients of the denominators of γ_n, when they're in reduced form. This is equivalent to saying that γ_n is a polynomial over $\mathbb{Z}$, and our proof is done. □

tt-ring-scheme-structure

THEOREM 14.2.15. *There is a unique ring scheme structure on $\mathbb{W}$ such that the Witt transformation $\varphi : \mathbb{W} \to \mathbb{A}^\infty$ is a homomorphism of ring schemes. Moreover, for every sieve $S \subset \mathbb{Z}$, this descends to a unique ring scheme structure on $\mathbb{W}^S$, so that, for any two sieves $S, T \subset \mathbb{Z}$, with $S \subset T$, the following diagram of ring schemes commutes:*

$$\begin{array}{ccc} \mathbb{W}^T & \xrightarrow{\varphi^T} & \mathbb{A}^T \\ \downarrow & & \downarrow \\ \mathbb{W}^S & \xrightarrow{\varphi^S} & \mathbb{A}^S. \end{array}$$

Also, for every sieve $S \subset \mathbb{N}$, if $p(S)$ is the set of prime divisors of S, then the S-truncated Witt transformation φ^S induces an isomorphism of ring schemes over $\mathbb{Z}[p(S)^{-1}]$:

$$\varphi^S_{\mathbb{Z}[p(S)^{-1}]} : \mathbb{W}^S \times \operatorname{Spec} \mathbb{Z}[p(S)^{-1}] \xrightarrow{\cong} \mathbb{A}^S \times \operatorname{Spec} \mathbb{Z}[p(S)^{-1}].$$

DEFINITION 14.2.16. The scheme $\mathbb{W}$ with the ring scheme structure constructed in the Theorem above is called the *Witt scheme*. For a sieve $S \subset \mathbb{N}$, the ring scheme $\mathbb{W}^S$ is called the *S-truncated Witt scheme*.

2.4. Relationship with Power Series Rings.

2.5. The Morphisms V and F.

2.6. The p-adic Witt Scheme.

DEFINITION 14.2.17. For a prime $p \in \mathbb{N}$, the *p-adic Witt scheme* $\mathbb{W}^p$ is the S-truncated Witt scheme $\mathbb{W}^S$, where $S = \{p^n : n \geq 0\}$. For $n \geq 0$, the *n^{th} truncated p-adic Witt scheme* is the $S(p^n)$-truncated Witt scheme $\mathbb{W}^{S(p^n)}$.

3. Cohen Structure Theorem: The Unequal Characteristic Case

4. Finiteness of Integral Closure

As a very important corollary of all our work, we're now ready to prove finiteness of integral closure for complete local rings with perfect residue fields.

l-finiteness-int-closure

THEOREM 14.4.1. *Let $(R, \mathfrak{m})$ be a complete, Noetherian local domain with perfect residue field, and let L/K be a finite extension of the quotient field $K = K(R)$. Then the integral closure S of R in L is a finitely generated R-module and thus also a complete, Noetherian local domain.*

PROOF. If we show that S is a finitely generated R-module, then we know, by (5.5.3), that it's a product of local rings. Since it's a domain, it must be a local ring itself, and will be complete by (5.3.3).

By (5.2.8) it now suffices to show that $S/\mathfrak{m}S$ is finitely generated over $R/\mathfrak{m}$, and by (4.3.23), it's enough to do this for the case where L/K is purely inseparable. In this case, we can find a prime power $q \in \mathbb{N}$ such that, for all $a \in S$, $a^q \in R$. $\square$

CHAPTER 15

Derivations and Differentials

chap:diff

1. Derivations and Infinitesimal Extensions

All our rings in this section will be commutative R-algebras for some ring R.

DEFINITION 15.1.1. Let S be an R-algebra, and let M be an S-module. A *derivation over* R or an R-*derivation* from S to M is a map of R-modules $D : S \to M$ such that, for all $s, t \in S$, we have:

$$D(st) = sD(t) + tD(s).$$

The set of all derivations from S to M is denoted $\mathrm{Der}_R(S, M)$. This has a natural structure of an S-module: addition is quite clear; for $s \in S$ and $D \in \mathrm{Der}_R(S, M)$, define sD by $(sD)(t) = sD(t)$.

We denote $\mathrm{Der}_R(S, S)$ simply by $\mathrm{Der}_R(S)$.

In fact, $\mathrm{Der}_R(S, \_\_)$ is a covariant functor from S-mod to S-mod. If $\varphi : M \to N$ is an S-module map, then we have a natural map

$$\begin{aligned} \mathrm{Der}_R(S, M) &\xrightarrow{\varphi_*} \mathrm{Der}_R(S, N) \\ D &\mapsto \varphi \circ D. \end{aligned}$$

We will show in the next section that this functor is representable.

REMARK 15.1.2. Observe that we have $D(1) = D(1.1) = D(1) + D(1)$, for all derivations D, and so $D(1) = 0$. Moreover, if r is in R, then we have $D(r) = rD(1) = 0$. Hence all R-derivations from S to M act trivially on R.

DEFINITION 15.1.3. Let S be an R-algebra. An *infinitesimal extension* of S is an R-algebra T and a surjection $u : T \twoheadrightarrow S$ such that $N^2 = 0$, where $N := \ker u$. Observe that in this case N is also an S-module. We'll usually say in this situation that (T, N, u) is an infinitesimal extension of S.

An infinitesimal extension (T, N, u) of S is *split* if in the short exact sequence:

$$0 \to N \to T \xrightarrow{u} S \to 0$$

there is a map $i : S \to T$ of R-algebras such that $iu = 1_S$.

Given an S-module M, we can construct a *canonical split infinitesimal extension* $(S * M, M, u)$, where $S * M$ as an R-module is simply $S \oplus M$, with the multiplication given by

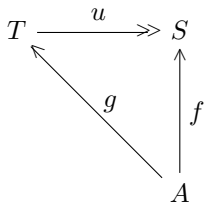
$$(s, m)(s', m') = (ss', sm' + s'm).$$

The map u is the obvious one, and the splitting map is just $s \mapsto (s, 0)$.

The next Proposition relates the two concepts that we have defined so far.

gs-difference-derivation

PROPOSITION 15.1.4. *Let S be an R-algebra, and let (T, N, u) be an infinitesimal extension of S. Suppose $f : A \to S$ is a map of R-algebras, and suppose there is a lift $g : A \to T$ of f so that the following diagram of homomorphisms of R-algebras commutes:*



Then, the assignment $D \mapsto g + D$ induces a bijection from $\mathrm{Der}_R(A, N)$ to lifts of f to T.

PROOF. Implicit in the statement of the Proposition is the assertion that N is an A-module; this follows from the fact that N is an S-module, which is an A-algebra. More explicitly, we have, for $a \in A$ and $n \in N$, $an = f(a)n = tn$, for any $t \in T$ such that $u(t) = f(a)$.

Now suppose $D : S \to N$ is an R-derivation; then we have, for all $a, b \in A$:

$$\begin{aligned}(g + D)(a)(g + D)(b) &= g(a)g(b) + g(a)D(b) + D(a)g(b) \\ &= g(ab) + aD(b) + bD(a) \\ &= (g + D)(ab).\end{aligned}$$

Hence $g + D$ is a map of R-algebras; since u vanishes on the image of D it is clear that it is again a lift of f to T.

Conversely, suppose $g' : A \to T$ is another lift of f to T. Then $g - g'$ maps A into N; we claim that this is a derivation. Indeed, we have, for any $a, b \in A$,

$$\begin{aligned}(g - g')(ab) &= g(a)g(b) - g'(a)g'(b) \\ &= g(a)(g(b) - g'(b)) + g'(b)(g(a) - g'(a)) \\ &= a(g - g')(b) + b(g - g')(a).\end{aligned}$$

This finishes the proof. □

2. Kähler Differentials

DEFINITION 15.2.1. Let S be an R-algebra; then the *module of Kähler differentials* is a pair $(\Omega_{S/R}, \mathrm{d})$–where $\Omega_{S/R}$ is an R-module and $\mathrm{d} : S \to \Omega_{S/R}$ is a derivation–representing the endofunctor $\mathrm{Der}_S(S, \_\_)$ in the following sense: For every S-module M, the natural map

$$\begin{aligned}\mathrm{Hom}_S(\Omega_{S/R}, M) &\to \mathrm{Der}_S(S, M) \\ \varphi &\mapsto \varphi \circ \mathrm{d}\end{aligned}$$

is an isomorphism. Clearly, if it exists, then it's unique up to unique isomorphism; this justifies the use of the definite article.

We prove existence of $\Omega_{S/R}$ in the next Theorem.

diff-existence-kahler

THEOREM 15.2.2. *Let S be an R-algebra; then the module of Kähler differentials $(\Omega_{S/R}, d)$ exists and is generated by the image of d.*

PROOF. Let $m : S \otimes_R S \to S$ be the map $s \otimes t \mapsto st$, and let $I = \ker m$. Let $T = S \otimes_R S/I^2$; then we have a natural surjection $u : T \to S$ with kernel I/I^2. Observe that $(T, I/I^2, u)$ is then an infinitesimal extension of S. We have two lifts of the identity map 1_S to T given by

$$g_1 : s \mapsto s \otimes 1 \pmod{I^2}$$
$$g_2 : s \mapsto 1 \otimes s \pmod{I^2}.$$

By (15.1.4), we see that $\mathrm{d} = g_1 - g_2$ gives a derivation from S to I/I^2. We claim that $(I/I^2, \mathrm{d})$ is the module of Kähler differentials for S over R.

So let M be an S-module, and suppose $D : S \to M$ is a derivation. Define a map of R-modules from $S \otimes_R S$ to $S * M$ by

$$\varphi : s \otimes t \mapsto (st, sDt).$$

But this is in fact a map of R-algebras:

$$\begin{aligned}\varphi(ss' \otimes tt') &= (sts't', ss'tDt' + ss't'Dt) \\ &= (st, sDt)(s't', s'Dt') \\ &= \varphi(s \otimes t)\varphi(s' \otimes t').\end{aligned}$$

Moreover, if $\sum_i (s_i \otimes t_i) \in I$, then we have

$$\varphi(\sum_i (s_i \otimes t_i)) = (0, \sum_i s_i Dt_i) \in M.$$

Hence $\varphi(I^2) \subset M^2 = 0$, and we get a map

$$\psi : I/I^2 \to M$$
$$\sum_i (s_i \otimes t_i) \pmod{I^2} \mapsto \sum_i s_i Dt_i.$$

We claim that ψ is a map of S-modules. Indeed, we have, for any $s \in S$:

$$\begin{aligned}\psi(\sum_i (s_i \otimes st_i) \pmod{I^2}) &= \sum_i s_i D(st_i) \\ &= \sum_i (s_i s D(t_i) + s_i t_i D(s)) \\ &= s(\sum_i s_i D(t_i)) = s\psi(\sum_i (s_i \otimes t_i)),\end{aligned}$$

since $\sum_i s_i t_i = 0$. Now we see:

$$\begin{aligned}\psi(\mathrm{d}(s)) &= \psi((s \otimes 1 - 1 \otimes s) \pmod{I^2}) \\ &= sD(1) + 1 \cdot D(s) = D(s).\end{aligned}$$

This shows that the natural map $\mathrm{Hom}_S(I/I^2, M) \to \mathrm{Der}_R(S, M)$ is a surjection.

If we show that I/I^2 is generated by the image of d, then we'll know that this natural map is in fact an injection, and our proof will be done. Observe that for $s, t \in S$ we can write:

$$s \otimes t = (s \otimes 1)(t \otimes 1 - 1 \otimes t) - st \otimes 1$$

Therefore, for any $\sum_i (s_i \otimes t_i) \in I$, since $\sum_i s_i t_i$, we have

$$\sum_i (s_i \otimes t_i) \pmod{I^2} = \sum_i s_i \mathrm{d}t_i,$$

which shows that I/I^2 is indeed generated over S by the image of d. □

DEFINITION 15.2.3. For $s \in S$, the element $\mathrm{d}s \in \Omega_{S/R}$ is called the *differential* of s.

REMARK 15.2.4. We'll give a more explicit description of the Kähler differentials in the next section.

f-kahler-polynomial-ring

EXAMPLE 15.2.5. Let $R = k$ and let $S = k[t_1, \ldots, t_n]$ be a polynomial algebra in n indeterminates. Then we see from the Theorem that $\Omega_{S/k}$ is generated by $\mathrm{d}t_1, \ldots, \mathrm{d}t_n$. But in fact these differentials are linearly independent over S. Indeed, consider the derivations $D_i : S \to S$ defined by $D_i(t_j) = \delta_{ij}$. It's easy to see that we have

$$D_i(f(t_1, \ldots, t_n)) = \frac{\partial f}{\partial t_i}.$$

We have maps $\varphi_i : \Omega_{S/k} \to S$ such that $\varphi_i \mathrm{d} = D_i$. If $\sum_i a_i \mathrm{d}t_i$ is a dependence relation on the t_i, then we have

$$\begin{aligned} 0 &= \varphi_i(\sum_j a_j \mathrm{d}t_j) \\ &= \sum_j a_j D_i(t_j) = a_i. \end{aligned}$$

This shows the linear independence we claimed. Hence $\Omega_{S/k} \cong S^n$ as an S-module, and the φ_i are the dual basis for $\mathrm{Hom}_S(\Omega_{S/k}, S)$. With this in hand, we can compute $\mathrm{d}f$, for all $f \in S$. We just have to know that $\varphi_i(\mathrm{d}f) = D_i f$ looks like, which we already do. So we find

$$\mathrm{d}f = \sum_i \frac{\partial f}{\partial t_i} \mathrm{d}t_i.$$

3. The Fundamental Exact Sequences

DEFINITION 15.3.1. An R-algebra A is 0-*smooth over* R if, for every infinitesimal extension (T, N, u) of any R-algebra S, and any map $f : A \to S$ of R-algebras, there exists a lift $g : A \to T$ of f to T.

A is instead 0-*unramified over* R if there exists at most one such lift in this situation.

It is 0-*étale over* R if it is both 0-smooth and 0-unramified. In particular, in our situation, there is a *unique* lift of f to T.

ero-unramified-criterion

PROPOSITION 15.3.2. *An R-algebra A is 0-unramified over R if and only if $\Omega_{A/R} = 0$. In particular, if the structure map $R \to A$ is an epimorphism of R-algebras, then $\Omega_{A/R}$.*

PROOF. Observe that if $\Omega_{A/R} = 0$, then $\mathrm{Der}_R(A, N) = 0$, for all A-modules N, and so any lifts of R-algebra maps $A \to S$ to infinitesimal extensions of S is unique by (15.1.4). Conversely, suppose such lifts are unique; then, for any A-module M, we can take $T = A * M$ to be the canonical split extension of A by M. The fact that there is only one lifting of the identity map 1_A to T tells us, via (15.1.4), that $\mathrm{Der}_R(A, M) = 0$, for all A-modules M, and thus $\Omega_{A/R} = 0$.

The second assertion follows easily, since, when $R \to A$ is an epimorphism, for any R-algebra S, there is at most one map of R-algebras from A to S. □

-localization-zero-etale

EXAMPLE 15.3.3. Suppose $U \subset R$ is a multiplicative set; then we claim that $U^{-1}R$ is 0-étale over R. By (15.3.2), since the map $R \to U^{-1}R$ is an epimorphism, we see that $U^{-1}R$ is 0-unramified over R. It remains to show that it's 0-smooth over R. To do this it suffices to show that if elements of U are invertible in an R-algebra S, then they are invertible in every infinitesimal extension of S. For this it's enough to show that in any ring S an element x that's invertible modulo a nilpotent ideal N is in fact invertible in S. Indeed, if $y \in S$ is such that $xy = 1 + n$, with $n \in N$, then since $1 + n$ is invertible, we see that x must also be so.

ndamental-exact-sequence

THEOREM 15.3.4 (First Fundamental Exact Sequence). *Let $R \xrightarrow{f} S \xrightarrow{g} T$ be a sequence of ring homomorphisms. Then we have an exact sequence:*

$$\Omega_{S/R} \otimes_S T \to \Omega_{T/R} \to \Omega_{T/S} \to 0$$

If T is 0-smooth over S, then the sequence

$$0 \to \Omega_{S/R} \otimes_S T \to \Omega_{T/R} \to \Omega_{T/S} \to 0$$

is split exact.

PROOF. By a version of Yoneda's Lemma for abelian categories, it suffices to show that, for all T-modules M, the sequence

$$\mathrm{Hom}_T(\Omega_{S/R} \otimes_S T, M) \leftarrow \mathrm{Hom}_T(\Omega_{T/R}, M) \leftarrow \mathrm{Hom}_T(\Omega_{T/S}, M) \leftarrow 0$$

is exact. By the universal property of the module of differentials, this reduces to showing that the sequence

$$\mathrm{Der}_R(S, M) \leftarrow \mathrm{Der}_R(T, M) \leftarrow \mathrm{Der}_S(T, M) \leftarrow 0$$

is exact. But this is clear, since any R-derivation from T to M vanishing on S is in fact an S-derivation from T to M.

Now suppose T is 0-smooth over S. The statement we have to prove is equivalent to showing that the map

$$\begin{aligned} g^* : \mathrm{Der}_R(T, M) &\to \mathrm{Der}_R(S, M) \\ D &\mapsto Dg \end{aligned}$$

given by restriction is surjective, for every R-module M. Define a map $h : S \to T * M$ by $h(s) = (g(s), Ds)$. This is a map of S-algebras:

$$\begin{aligned} h(st) &= (g(st), g(t)Ds + g(s)Dt) \\ &= (g(s), Ds)(g(t), Dt). \end{aligned}$$

This gives $T * M$ the structure of an S-algebra. Now, since T is 0-smooth over S, the identity map 1_T must lift to a map $v : T \to T * M$ such that $v(t) = (t, D't)$. Since $D' = v - i$, where $i : T \to T * M$ is the splitting map, we see that $D' : T \to M$ is an S-derivation (15.1.4). Moreover, we have

$$\begin{aligned} (g(s), Ds) &= v(g(s)) \\ &= (g(s), D'(g(s))), \end{aligned}$$

which shows that $D = D'g$, and so also the surjectivity of g^*. □

Now suppose the map $g : S \to T$ is surjective with kernel J. If we consider the restriction of $\mathrm{d}_{S/R}$ to J, we get a map from J to $\Omega_{S/R}$ and thence to $\Omega_{S/R} \otimes_S T$.

It is clear the kernel of this map contains J^2, since $g(s) = 0$, for all $s \in J$, and we have, for $s, t \in J$,

$$\mathrm{d}_{S/R}(st) \otimes 1 = \mathrm{d}_{S/R}(s) \otimes g(t) + \mathrm{d}_{S/R}(t) \otimes g(s).$$

So we get a map $\delta : J/J^2 \to \Omega_{S/R} \otimes_S T$ defined by $\delta(s \pmod{J^2}) = \mathrm{d}_{S/R}s \otimes 1$.

ndamental-exact-sequence

THEOREM 15.3.5 (Second Fundamental Exact Sequence). *Let $R \xrightarrow{f} S \xrightarrow{g} T$ be a sequence of ring homomorphisms, and suppose g is surjective with kernel J. Then we have the following exact sequence of T-modules:*

$$J/J^2 \xrightarrow{\delta} \Omega_{S/R} \otimes_S T \to \Omega_{T/R} \to 0.$$

If T is 0-smooth over R, then the sequence

$$0 \to J/J^2 \to \Omega_{S/R} \otimes_S T \to \Omega_{T/R} \to 0$$

is split exact. In fact the map δ is a split injection if and only if the identity 1_T lifts to a map $T \to S/J^2$, where we are considering $(S/J^2, J/J^2, u)$ as an infinitesimal extension of T, with $u : S/J^2 \to T$ the natural surjection.

PROOF. First, observe that from (15.3.2) we have $\Omega_{T/S} = 0$. So the sequence is exact on the right by (15.3.4).

Now, like in the proof of the last theorem, it suffices to show that the following sequence is exact for every T-module M:

$$\mathrm{Hom}_T(J/J^2, M) \xleftarrow{\delta^*} \mathrm{Der}_R(S, M) \leftarrow \mathrm{Der}_R(T, M) \leftarrow 0.$$

But a derivation $D : S \to M$ is in the kernel of δ^* if and only if $D = f\mathrm{d}_{S/R}$, where $f : \Omega_{S/R} \to M$ is such that $(f \otimes 1)\delta = 0$; that is, if and only if, for all $s \in J$, we have $Ds = fd_{S/R}s = 0$, which is equivalent to saying that D is induced by a derivation $D' : T = S/J \to M$.

Suppose now that T is 0-smooth over R, and observe that $(S/J^2, J/J^2, u)$, where $u : S/J^2 \to T$ is the natural surjection, gives an infinitesimal extension of T. By 0-smoothness, there exists a map $i : T \to S/J^2$ of R-algebras lifting the identity map 1_T. Now, consider the map $iu : S/J^2 \to S/J^2$: we have $uiu = 1_T u = u$, and so both $1 = 1_{S/J^2}$ and iu are lifts of the identity map $1_{S/J^2}$. In particular, $D = 1 - iu$ is an R-derivation from S/J^2 to J/J^2 (15.1.4). Moreover, observe that we have $D|_{J/J^2} = 1_{J/J^2}$.

Let $\pi : S \to S/J^2$ be the natural surjection. Given a map $f : J/J^2 \to M$ of T-modules, we get a derivation

$$D_f = fD\pi : S \to M.$$

Now, observe that we have, for $s \in J$,

$$\begin{aligned}(\delta^* D_f)(\pi(s)) &= D_f s \\ &= fD\pi(s) \\ &= f(\pi(s))\end{aligned}$$

and so $f \mapsto D_f$ gives a splitting map for δ^*, and so δ is in fact a split injection.

Conversely, suppose there is a splitting map $i : \Omega_{S/R} \otimes_S T \to J/J^2$ for δ, so that $i\delta = 1_{J/J^2}$. This induces a derivation $D = i(d_{S/R} \otimes 1) : S \to J/J^2$. Suppose

$s \in J$; then we have

$$\begin{aligned} Ds &= i(d_{S/R}s \otimes 1) \\ &= i\delta(\pi(s)) \\ &= \pi(s) \end{aligned}$$

Thus $D|_{J^2} = 0$, and so we have an induced derivation $D : S/J^2 \to J/J^2$. Then, by (15.1.4), $j = 1_{S/J^2} - D$ gives a lifting of the projection $u : S/J^2 \to T$. Now we also have, for $s \in J$:

$$\begin{aligned} j(\pi(s)) &= \pi(s) - D(\pi(s)) \\ &= 0. \end{aligned}$$

Therefore, $j|_{J/J^2} = 0$, and so we have an induced map $k : T \to S/J^2$, so that the following diagram commutes:

$$\begin{array}{ccccc} S/J^2 & \xrightarrow{u} & T & \longrightarrow & 0 \\ \uparrow{\scriptstyle j} & \nwarrow{\scriptstyle k} & \| & & \\ S/J^2 & \xrightarrow{u} & T & \longrightarrow & 0, \end{array}$$

and so we find that $k : T \to S/J^2$ is a splitting map for u. □

The Theorem lets us describe the module of differentials $\Omega_{S/R}$ concretely when S is finitely generated over R.

ation-finitely-generated

COROLLARY 15.3.6. *Let T be a finitely generated R-algebra; then, for any polynomial ring $S = R[t_1, \ldots, t_n]$ such that $T = S/J$, for some ideal $J \subset S$, we have*

$$\Omega_{T/R} \cong \frac{T^n}{(\sum_i \frac{\partial f}{\partial t_i} e_i : \ f \in J)},$$

where $\{e_1, \ldots, e_n\}$ form a basis for the free T-module T^n. We have a natural map $\pi : \Omega_{S/R} \to \Omega_{T/R}$ sending $d_{S/R}f$ to $\sum_i \frac{\partial f}{\partial t_i} e_i$, and the differential $d_{T/R} : T \to \Omega_{T/R}$ is defined by sending t to $\pi(d_{S/R}f)$, where $f \in S$ is any element mapping to t.

In particular, if J is finitely generated over S, then $\Omega_{T/R}$ is finitely presented over T.

PROOF. Immediate from (15.2.5) and the Theorem above. □

4. Functorial Properties of the Module of Differentials

diff-base-change

PROPOSITION 15.4.1 (Base Change). *Suppose S and R' are R-algebras, and let $S' = S \otimes_R R'$. Then we have a natural isomorphism*

$$\Omega_{S'/R'} \cong \Omega_{S/R} \otimes_S S'$$

PROOF. The R-derivation $\mathrm{d}_{S/R} : S \to \Omega_{S/R}$ lifts to an R'-derivation

$$\mathrm{d}' = \mathrm{d}_{S/R} \otimes 1 : S' \to \Omega_{S/R} \otimes_S S'.$$

By the universal property of $\Omega_{S'/R'}$, there is an S'-module map

$$\alpha : \Omega_{S'/R'} \to \Omega_{S/R} \otimes_S S'$$

such that $\mathrm{d}' = \alpha \mathrm{d}_{S'/R'}$. We claim that α is an isomorphism. To do this it suffices to show that, for all S'-modules N, the map

$$\begin{aligned} \mathrm{Hom}_S(\Omega_{S/R}, N) &\xrightarrow{\alpha^*} \mathrm{Hom}_{S'}(\Omega_{S'/R'}, N) \\ f &\mapsto (f \otimes 1)\alpha \end{aligned}$$

is an isomorphism, where $(f \otimes 1)(s \otimes r) = rf(s)$.

From the universal property of the module of differentials, it suffices then to prove the following map is an isomorphism:

$$\begin{aligned} \mathrm{Der}_R(S, N) &\xrightarrow{\psi} \mathrm{Der}_{R'}(S', N) \\ \psi D : (s \otimes r') &\mapsto r' Ds. \end{aligned}$$

Now, given an R-derivation $D' : S' \to N$, we can naturally associate to it the R-derivation $\varphi D' : S \to N$ given by $(\varphi D)(s) = D(s \otimes 1)$. We have

$$\begin{aligned} (\varphi\psi D)(s) = (\psi D)(s \otimes 1) &= D(s), \end{aligned}$$

and

$$\begin{aligned} (\psi\varphi D')(s \otimes r') &= r'(\varphi D')(s) \\ &= r' D'(s \otimes 1) \\ &= D'(s \otimes r'). \end{aligned}$$

This shows that ψ is in fact an isomorphism, and we are done. □

diff-localization

PROPOSITION 15.4.2 (Localization). *Let S be an R-algebra, let $U \subset S$ be a multiplicative set, and let $S' = U^{-1}S$; then we have*

$$\Omega_{S'/R} \cong U^{-1}\Omega_{S/R}.$$

Moreover, under this isomorphism, we have

$$d(1/s) = -s^{-2}\, ds.$$

PROOF. By (15.3.3), we know that S' is 0-étale and thus 0-smooth over S. Moreover, since it's 0-unramified over S, we have $\Omega_{S'/S} = 0$. Now the required isomorphism follows immediately from (15.3.4). For the final assertion, observe that, under the natural map, $-s^{-2}\mathrm{d}s$ goes to

$$\begin{aligned} -s^{-2}\mathrm{d}(s/1) &= -\mathrm{d}(1/s) + (s/1)\mathrm{d}(s^{-2}) \\ &= -\mathrm{d}(1/s) + 2\mathrm{d}(s^{-1}) \\ &= d(1/s). \end{aligned}$$

□

diff-localization-fingen

COROLLARY 15.4.3. *Let S be a finitely generated R-algebra, and let $U \subset S$ be a multiplicative set. Then $\Omega_{U^{-1}S/R}$ is a finitely generated $U^{-1}S$-module.*

PROOF. By (15.3.6), $\Omega_{S/R}$ is a finitely generated S-module. The result now follows from (15.4.2). □

diff-coproducts

PROPOSITION 15.4.4 (Coproducts). *Suppose $T = \bigotimes_{i \in I R} S_i$, for R-algebras S_i. Then the natural map*

$$\bigoplus_{i \in I} \left(\Omega_{S_i/R} \otimes S_i T\right) \to \Omega_{T/R}$$

given, for $s \in S_i$, by $d_{S_i/R}s \otimes 1 \mapsto d_{T/R}(k_i(s))$, where $k_i : S_i \to T$ is the natural map.

PROOF. Again, it suffices to show that, for every T-module M, the natural map

$$\mathrm{Der}_R(T, M) \to \prod_{i \in I} \mathrm{Der}_R(S_i, M)$$

given by restriction onto each co-ordinate is an isomorphism. But it is easy to define an inverse for this map. If $(D_i : i \in I)$ is an element on the right hand side, then it defines an R-derivation D from T to M with $D \circ k_i = D_i$; that there is a unique D satisfying this condition is quite clear. □

diff-coequalizers

PROPOSITION 15.4.5 (Co-equalizers). *Suppose $f, g : S \to T$ are two maps of R-algebras; let $S' = T/J$ be the co-equalizer of the two maps, where J is the ideal generated by elements of the form $f(s) - g(s)$, for $s \in S$. Let Ω' be the co-kernel of the map of T-modules given by*

$$\begin{aligned} \Omega_{S/R} \otimes_S S' &\to \Omega_{T/R} \otimes_S S' \\ d_{S/R}s \otimes 1 &\mapsto d_{T/R}(f(s) - g(s)) \otimes 1. \end{aligned}$$

Then the natural map

$$\Omega' \mapsto \Omega_{S'/R}$$

is an isomorphism.

PROOF. Consider the second fundamental exact sequence (15.3.5)

$$J/J^2 \to \Omega_{T/R} \otimes_T S' \to \Omega_{S'/R} \to 0.$$

Let $\pi : T \to T/J^2$ be the natural surjection; then the map from J/J^2 to $\Omega_{T/R} \otimes_T S'$ is given simply by taking $\pi(s)$ to $\mathrm{d}_{T/R}s \otimes 1$. But we see immediately from the definitions that the image of this map is precisely the kernel of the map from $\Omega_{T/R} \otimes_T S' \to \Omega'$, and so the Proposition follows. □

diff-colimits

THEOREM 15.4.6 (Colimits). *Let I be any category, and let $F : I \to R\text{-alg}$ be a functor. Suppose $T = \operatorname{colim} F$, and let $\mathscr{R}$ be the category whose objects are R-algebra maps $S \to T$, and whose morphisms are the obvious commuting triangles; then F induces a natural functor F' from I to $\mathscr{R}$. Define a functor $\Omega : \mathscr{R} \to T\text{-mod}$ by $S \mapsto \Omega_{S/R} \otimes_S T$. Then we have a natural isomorphism*

$$\operatorname{colim}(\Omega F') \cong \Omega_{T/R}.$$

PROOF. Since every colimit can be expressed as the co-equalizer of two maps between co-products, this follows immediately from (15.4.5) and (15.4.4). □

diff-finite-products

PROPOSITION 15.4.7 (Finite Products). *Let $T = \prod_{i=1}^n S_i$ be a finite product of R-algebras. Then the natural map*

$$\Omega_{T/R} \mapsto \prod_{i=1}^n \Omega_{S_i/R}$$

that maps $d_{T/R}t$ to $(d_{S_i/R}(\pi_i(t)))$, where $\pi_i : T \to S_i$ is the natural projection is an isomorphism.

PROOF. This amounts to showing that the natural map

$$\prod_{i=1}^{n} \mathrm{Der}_R(S_i, M) \to \mathrm{Der}_R(T, M)$$

taking (D_i) to D, where $D\pi_i = D_i$, is an isomorphism. But this is clear. We of course needed the finiteness of the product to be able to pull out the product symbol outside Der. □

5. Applications to Field Theory

6. Ramification and the Different

CHAPTER 16

Étale Algebras

chap:etale

CHAPTER 17

Free Resolutions and Fitting Ideals

chap:frf

CHAPTER 18

Gorenstein Rings and Local Duality

chap:gorn