Commutative Algebra

Lectures by Chris Brookes
Notes by David Mehrle
dfm33@cam.ac.uk

Cambridge University
Mathematical Tripos Part III
Michaelmas 2015

Contents

Last updated May 19, 2016.

Contents by Lecture

1 Introduction

1.1 Course overview

Lecturer Email: brookes@dpmms.cam.ac.uk

For prerequisites, I'm going to assume that you aren't algebraic virgins. You should know about rings and modules and so forth.

The best book to have is Atiyah Macdonald, but it leaves a lot to the exercises and doesn't do homology. A decent book that fills in a bunch of the details is Kaplansky or Sharp (Sharp may not be so nice). Miles Reid wrote a book called *Undergraduate Commutative Algebra* that focuses on it's use in algebraic geometry. Matsumura is a good second book in commutative algebra. Zariski and Samuel is dense; Bourbaki is encyclopediac.

There will be examples classes. I'll probably hand out an examples sheet on Monday.

1.2 A Brief History

Most of what's presented in this course goes back to a series of papers as presented by David Hilbert. He was studying invariant theory and published several papers from 1888 to 1893.

Invariant theory is the study of fixed points of group actions on algebras.

Example 1.1. Let k be a field. Given a polynomial algebra $k[x_1, \ldots, x_n]$ and the symmetric group Σ_n. (There will be lot's of S's in this course so we use sigma for the symmetric group). $\Sigma_n \circlearrowright k[x_1, \ldots, x_n]$ by permuting the variables. The invariants are the polynomials fixed under this action. For example, the elementary symmetric polynomials are fixed:

$$\begin{aligned}
\sigma_1 &= x_1 + \ldots + x_n \\
\sigma_2 &= \sum_{i<j} x_i x_j \\
&\vdots \\
\sigma_n &= x_1 x_2 \cdots x_n
\end{aligned}$$

In fact the ring of invariants is generated by these elementary symmetric polynomials σ_i, and this ring is isomorphic to $k[\sigma_1, \ldots, \sigma_n]$.

David Hilbert considered rings of invariants for various groups acting on $k[x_1, \ldots, x_n]$. Along the way he proved 4 big theorems:

(1) Hilbert's Basis Theorem;

(2) Nullstellensatz;

(3) polynomial nature of a certain function, now known as the **Hilbert Function**;

(4) Syzygy Theorem.

We'll see the Hilbert Basis Theorem shortly, the Nullstellensatz gives the link with geometry, (3) leads to dimension theory and (4) leads to homology.

The next person to come along was Emmy Noether. In 1921 she abstracted from the proof of the Basis Theorem the key property that made it work.

Definition 1.2. A (commutative) ring is **Noetherian** if any ideal is finitely generated. There are many equivalent definitions.

The abstract version of the basis theorem says

Theorem 1.3. If R is Noetherian, then so is $R[x]$.

Corollary 1.4. If k is a field, then $k[x_1, \ldots, x_n]$ is Noetherian.

Noether also developed the ideal theory for Noetherian rings. One has primary decomposition of ideals, which is a generalization of factorization from number theory.

The link between commutative algebra and algebraic geometry is quite strong. For instance, the fundamental theorem of algebra says that any polynomial $f \in \mathbb{C}[x]$ has finitely many roots, and any such polynomial is determined up to scalar by the set of zeros including multiplicity. In n variables, instead consider $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$. Define the **(affine) algebraic set**

$$Z(I) := \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid f(a_1, \ldots, a_n) = 0 \ \forall f \in I\}.$$

These sets form the closed sets in a topology on $\mathbb{C}^n$, known as the Zariski topology.

Given any set I, we can replace it by the ideal generated by the set I without changing $Z(I)$.

For a set $\mathcal{S} \subset \mathbb{C}^n$, we can define the **ideal associated to** $\mathcal{S}$

$$I(S) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in \mathcal{S}\}.$$

This is a special sort of ideal, called a **radical ideal**.

Definition 1.5. An ideal I is **radical** if $f^n \in I$ implies $f \in I$.

One form of the Nullstellensatz says

Theorem 1.6 (Nullstellensatz)**.** There is a bijective correspondence between radical ideals of $\mathbb{C}[x_1, \ldots, x_n]$ and algebraic subsets of $\mathbb{C}^n$.

Most of the course dates from 1920 to 1950. I'll spend quite a lot of time on dimension. Krull's principal ideal theorem and it's generalizations are quite important to this.

For finitely generated rings, there are three different approaches that lead to the same number for the dimension of a ring:

(1) lengths of chains of prime ideals;

(2) by growth rate – Hilbert's function and it's degree;

(3) the transcendence degree of the field of fractions in the case of integral domains.

The rings of dimension zero are called the **Artinian rings**. In dimension 1, special things happen which are important in number theory. This is crucial in the study of algebraic curves.

2 Noetherian Rings and Ideal Theory

Remark 2.1. Convention: all rings are unital and commutative.

Lemma 2.2. Let M be a (left) R-module. Then the following are equivalent:

(i) every submodule of M, including M itself, is finitely generated;

(ii) there does not exist an infinite strictly ascending chain of submodules. This is the **ascending chain condition (ACC)**;

(iii) every nonempty subset of submodules of M contains at least one maximal member.

Definition 2.3. An R-module is **Noetherian** if it satisfies any of the conditions of Lemma 2.2.

Definition 2.4. A ring R is **Noetherian** if it is a Noetherian R-module.

Lemma 2.5. Let N be a submodule of M. Then M is Noetherian if and only if both N and M/N are Noetherian.

Lemma 2.6. Let R be a Noetherian ring. Then any finitely generated R-module M is also Noetherian.

Exercise 2.7. Prove Lemma 2.2, Lemma 2.5, and Lemma 2.6.

Let's have some examples.

Example 2.8.

(1) Fields are Noetherian;

(2) Principal Ideal Domains are Noetherian, e.g. $\mathbb{Z}$, $k[x]$;

(3)
$$\left\{ g \in \mathbb{Q} \mid g = {}^{m}\!/_{n}, m, n \in \mathbb{Z}, p \nmid n \text{ for some fixed prime } p \right\}$$

This is an example of a localization of $\mathbb{Z}$. In general, the localization of a Noetherian ring is Noetherian.

(4) $k[x_1, \ldots, x_n]$, $\mathbb{Z}[x_1, \ldots, x_n]$. This follows from Hilbert's Basis Theorem.

(5) $k[x_1, x_2, \ldots]$ is not Noetherian. This has an infinite, strictly ascending chain of ideals
$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \ldots$$

(6) Finitely generated commutative rings R are Noetherian, because then each ideal is finitely generated. If $a_1, \ldots, a_n$ generated R, then there is a ring homomorphism $\mathbb{Z}[x_1, \ldots, x_n] \twoheadrightarrow \mathbb{R}$, $f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n)$. Then the first isomorphism theorem tells us that R is isomorphic to a quotient of a Noetherian ring, namely $\mathbb{Z}[x_1, \ldots, x_n]$, which is Noetherian.

(7) $k[[x]]$ (the **formal power series ring**) is Noetherian. Elements are power series
$$a_0 + a_1 x^1 + a_2 x^2 + \ldots$$
with the usual multiplication.

Theorem 2.9 (Hilbert's Basis Theorem)**.** Let R be a Noetherian ring. Then $R[x]$ is also Noetherian.

Proof. (A bit sketchy). We prove that every ideal of $R[x]$ is finitely generated. Let I be an ideal. Define $I(n)$ to be those elements of I of degree at most n. Note that $0 \in I(n)$ for each n, so each is nonempty. We have a chain
$$I(0) \subseteq I(1) \subseteq I(2) \subseteq \ldots$$
Define $R(n)$ to be the set of all leading coefficients of x^n appearing in elements of $I(n)$.

Then $R(n)$ is a nonempty ideal of R. Moreover, we have another ascending chain
$$R(0) \subseteq R(1) \subseteq \ldots$$
By assumption R is Noetherian, so the ascending chain terminates. Hence there is some N such that $R(n) = R(N)$ for all $n \geqslant N$. Additionally, we can say that each $R(n)$ is finitely generated, say
$$R(n) = Ra_{n1} + \ldots + R_{a_{nm_n}}.$$
Because the a_{ij} are leading coefficients, there are polynomials
$$f_{nm}(x) = a_{nm}x^n + \text{ lower degree terms } \in I$$
The set
$$\{f_{ij}(x) \colon 0 \leqslant i \leqslant N, 1 \leqslant j \leqslant m_i\}$$
is finite, and we claim that this set generates I as an ideal. This follows from Claim 2.10. □

Claim 2.10.
$$\{f_{ij}(x) \colon 0 \leqslant i \leqslant N, 1 \leqslant j \leqslant m_i\}$$
generates I as an ideal.

Proof. Given $f(x) \in I$, we show by induction on degree $f(x) \in I$ that $f(x)$ is in the ideal generated by this set.

For $\deg f = 0$, $f(x) = a \in I(0) = R(0) = Ra_{01} + \ldots + Ra_{0m_0}$. But $f(x) = a_{0m_0}$.

Now assume for $\deg f = n > 0$, and that the claim is true for terms in I of smaller degree. There are two cases:

(a) If $n \leqslant N$, we have $f(x) = aX^n +$ lower degree terms , with $a \in R(n)$. So there exists $r_n \in R$ such that
$$a = \sum r_m a_{nm}$$
because a lies in the ideal $R(n)$. Define
$$g(x) = \sum r_m f_{nm}(x).$$
Then consider
$$h(x) = f(x) - g(x),$$
which is of lower degree and belongs to I. Hence, by inductive hypothesis we see that $f(x) = g(x) + h(x)$ is of the right form. Thus, $f(x) \in I$.

(b) If $n > N$, the strategy is the same but we have to correct for degree. Let $f(x) = ax^n +$ lower degree terms . Again we write
$$a = \sum r_m a_{Nm} \in R(N) = R(n).$$
Likewise, we conjure up $g(x)$ but this time we have to correct for the degree. Set
$$g(x) = \sum r_m x^{n-N} f_{Nm}(x) \in I(n).$$
Then we just carry on as before. $h(x) = f(x) - g(x) \in I(n-1)$ and so the inductive hypothesis applies. Therefore, $f(x) = h(x) + g(x)$ is of the right form.

□

Exercise 2.11. Fill in the details in Theorem 2.9.

Remark 2.12. In computation, we really want to be able to find the generating set without too much redundancy. The proof of Theorem 2.9 produces a generating set that is hugely redundant. We can do better. Such sets are called **Gröbner Bases**, and are commonly used in computer algebra algorithms.

Theorem 2.13. If R is Noetherian, then so is $R[[X]]$.

Proof. Either directly in a similar fashion by considering trailing coefficients of $f(X) = a_r X^r +$ higher degree terms, *or* use Cohen's Theorem. □

Exercise 2.14. Prove Theorem 2.13 by analogue to the proof of Theorem 2.9.

Theorem 2.15 (Cohen's Theorem)**.** R is Noetherian if and only if all prime ideals of R are finitely generated.

Lemma 2.16. Let P be a prime ideal of $R[[x]]$ and θ be the constant term map $\theta\colon R[[X]] \to R$, $\sum a_i X^i \mapsto a_0$. Then P is finitely generated ideal of $R[[X]]$ if and only if $\theta(P)$ is a finitely generated ideal of R.

Proof of Theorem 2.15. If R is Noetherian, then all of its ideals, and in particular the prime ideals, are finitely generated.

Conversely, suppose R is not Noetherian but all prime ideals are finitely generated. Then there are ideals which are not finitely generated.

By Zorn's Lemma, there is a maximal member I, not necessarily unique, of the set of all non-finitely generated ideals. (One needs to check that in our nonempty, partially ordered set, each chain has an upper bound that lies in the set – however, the union of our chain will suffice).

We claim that I is prime. To prove this, suppose not. So there are a, b with $ab \in I$ such that $a \notin I$, $b \notin I$. Then $I + Ra$ is an ideal strictly containing I. The maximality of I shows that $I + Ra$ is finitely generated by $u_1 + r_1 a, \dots, u_n + r_n a$.

Let $J = \{s \in R \mid sa \in I\}$. Note that J is an ideal containing $I + Rb$. We have inclusions
$$I \subsetneq I + Rb \subseteq J.$$

Again by the maximality of I, we claim that J is finitely generated. Now we prove that
$$I = Ru_1 + \dots + Ru_n + Ja,$$
which shows that I is finitely generated by $u_1, \dots, u_n$, and aJ (which is finitely generated).

Take $t \in I \subseteq I + Ra$. So $t = v_1(u_1 + r_1 a) + \dots + v_n(u_n + r_n a)$ for some coefficients $v_i \in R$. Hence $v_1 r_1 + \dots + v_n r_n \in J$, and so t is of the required form, for any $t \in I$. $\square$

This concludes the proof of Theorem 2.15. Now we can use this to prove Theorem 2.13.

Proof of Theorem 2.13. Let $\theta\colon R[[X]] \to R$ be the homomorphism that takes the constant term. Let P be a prime ideal of $R[[X]]$. If P is finitely generated, then $\theta(P)$ is finitely generated as well.

Conversely, suppose that $\theta(P)$ is a finitely generated ideal of R, say
$$\theta(P) = Ra_1 + \dots + Ra_n.$$

If $X \in P$, then P is generated by X and $a_1, \dots, a_n$.

If $X \notin P$, there's some work to do. Let $f_1, \dots, f_n$ be power series in P, with constant terms $a_1, \dots, a_n$, respectively. We prove that $f_1, \dots, f_n$ generate P. Take $g \in P$, with constant term b. But $b = \sum b_i a_i$ since the constant terms are generated by $a_1, \dots, a_n$. So
$$g - \sum b_i f_i = Xg_1$$
for some power series g_1. Note that $Xg_1 \in P$, but P is prime and $X \notin P$. So $g_1 \in P$. Similarly,
$$g_1 = \sum c_i f_i + g_2 X$$

with $g_2 \in P$. Continuing gives power series $h_1, \dots, h_n \in R[[X]]$ with

$$h_i = b_i + c_i X + d_i X^2 + \dots$$

These power series satisfy

$$g = h_1 f_1 + \dots + h_n f_n,$$

and therefore the f_i generate P. □

2.1 Nilradical and Jacobson Radical

About 50 years ago, there were lots of people writing papers about radicals.

Lemma 2.17. The set $\mathrm{Nil}(R)$ of nilpotent elements of a commutative ring R form an ideal. $R/\mathrm{Nil}(R)$ has no non-zero nilpotent elements.

Proof. If $x \in \mathrm{Nil}(R)$ then $x^m = 0$ for some m, so $(rx)^m = 0$ for any $r \in R$. Thus, $rx \in \mathrm{Nil}(R)$. If $x, y \in \mathrm{Nil}(R)$, then $x^m = y^n = 0$ for some n, m. Then

$$(x+y)^{n+m+1} = \sum_{i=0}^{n+m+1} \binom{n+m+1}{i} x^i y^{n+m+1-i} = 0$$

So $x + y \in \mathrm{Nil}(R)$.

If $\overline{x} \in R/\mathrm{Nil}(R)$ is the image of $x \in R$ in $R/\mathrm{Nil}(R)$ with $\overline{x}^m = 0$, then $x^m \in \mathrm{Nil}(R)$ and so $(x^m)^n = 0 \in R$. So $x \in \mathrm{Nil}(R)$ and hence $\overline{x} = 0$ in $R/\mathrm{Nil}(R)$. □

Definition 2.18. The ideal $\mathrm{Nil}(R)$ is the **nilradical**

Lemma 2.19 (Krull)**.** $\mathrm{Nil}(R)$ is the intersection of all prime ideals of R.

Proof. Let

$$I = \bigcap_{P \text{ prime}} P.$$

If $x \in R$ is nilpotent, then $x^m = 0 \in P$ for any prime ideal P. The primeness of P shows that $x \in P$ for any prime P. Hence, $x \in I$.

Conversely, suppose that x is not nilpotent. We show that it's not in I. Set $\mathcal{S}$ to be the set of ideals J such that for any $n \geqslant 0$, $x^n \notin J$,

$$\mathcal{S} = \{J \lhd R \mid n > 0 \implies x^n \notin J\}.$$

We now want to apply Zorn's lemma. So we check that $\mathcal{S}$ is nonempty, as $0 \in \mathcal{S}$. Furthermore, a union of such ideals is also in $\mathcal{S}$. Let J_1 be this maximal element of $\mathcal{S}$, say.

Now we claim that J_1 is prime, and thus x does not lie in at least one prime ideal. This would finish the proof by showing that $x \notin I$.

To establish that J_1 is prime, proceed by contradiction. Suppose $yz \in J_1$ with $y \notin J_1$, $z \notin J_1$. So ideals $J_1 + Ry$, $J_1 + Rz$ strictly contain J_1. Hence by maximality of J_1 in $\mathcal{S}$, $x^n \in J_1 + Ry$, $x^m \in J_1 + Rz$ for some m, n. So $x^{m+n} \in J_1 + Ryz$, and so $yz \notin J_1$. □

Definition 2.20. For an ideal $I \lhd R$, it's **radical** $\sqrt{I}$ is

$$\sqrt{I} = \{x \mid x^n \in I \text{ for some } n\}.$$

Definition 2.21. The **Jacobson radical** of R is the intersection of all maximal ideals,

$$\mathrm{Jac}(R) = \bigcap_{M \text{ maximal}} M.$$

In general, we have

$$\mathrm{Nil}(R) = \bigcap_{P \text{ prime}} \subseteq \bigcap_{M \text{ maximal}} M = \mathrm{Jac}(R).$$

These need not be equal.

Example 2.22. For example,

$$R = \{{}^{m}/_{n} \in \mathbb{Q} \mid p \nmid n \text{ for some fixed prime } p\}$$

This is a **local ring** with a unique maximal ideal

$$P = \{{}^{m}/_{n} \in \mathbb{Q} \mid p \nmid n, p \mid m\}$$

The only nilpotent element is zero, so $\mathrm{Nil}(R) = 0$ yet $\mathrm{Jac}(R) = P$.

Lemma 2.23 (Nakayama's Lemma)**.** Let M be a finitely generated R-module. Then $\mathrm{Jac}(R)M = M$ if and only if $M = 0$.

Proof. If $M = 0$, then $\mathrm{Jac}(R)M = M = 0$.

Conversely, suppose $M \neq 0$. Consider the set of proper submodules of M. These are the submodules that do not contain the given finite generating set of M. Zorn applies to this set, and so there is a maximal member N, say. This is a maximal, proper submodule of M.

Therefore, M/N is **simple** – it has no submodules other than zero and itself. Take any nonzero element $\overline{m}$ of M/N. It generates M/N, and so M/N is cyclic. This means that $\theta\colon R \to M/N$, $r \mapsto r\overline{m}$ is surjective. By the first isomorphism theorem, then

$$R/_{\ker\theta} \cong M/_{N}.$$

Therefore $\ker\theta$ is a maximal ideal of R (else $R/\ker\theta$ has an ideal and so M/N is not simple). Note that $(\ker\theta)M \leqslant N$, because $(\ker\theta) = \{r \in R \mid rm \in N\}$. Finally, we have that

$$\mathrm{Jac}(R)M \subseteq (\ker\theta)M \subseteq N \subsetneq M,$$

which contradicts our assumption that $\mathrm{Jac}(R)M = M$.

We assumed $M \neq 0$, and showed that equality does not hold. $\square$

Remark 2.24.

(1) This is not the usual proof found in Atiyah-Macdonald, for example. But this one carries over to the non-commutative case!

(2) The same proof shows that $M = 0 \iff PM = M$ for all maximal ideals P of R.

(3) A stronger version of Nakayama's Lemma is recorded below, using a generalized version of the Cayley Hamilton theorem.

Theorem 2.25 (Cayley Hamilton Theorem)**.** Let M be a finitely generated R-module, and let $\phi\colon M \to M$ be an R-module homomorphism. Then if I is an ideal of R such that $\phi(M) \subseteq IM$, then ϕ satisfies a monic polynomial

$$\phi^n + a_1\phi^{n-1} + a_2\phi^{n-2} + \ldots + a_n = 0$$

with $a_k \in I^k$.

Proof. Suppose that $x_1, \ldots, x_n$ generate M as an R-module. Then we have that

$$\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j$$

with $a_{ij} \in I$, because $\phi(M) \subseteq IM$. Then we have that

$$\sum_{j=1}^{n} (\phi\delta_{ij} - a_{ij})x_j = 0.$$

Then let A be the matrix $A = (\phi\delta_{ij} - a_{ij})_{1\leqslant i,j\leqslant n}$. Multiply by the adjugate of the matrix A to see that

$$\det(A) = 0.$$

Hence ϕ satisfies the polynomial $\det(A)$. □

Lemma 2.26 (Strong Nakayama's Lemma)**.** Let I be an ideal of R and let M be a finitely generated R-module. Then if $IM = M$, there is some $r \in R$, $r \equiv 1 \pmod I$, such that $rM = 0$.

Proof. We want to apply the Cayley-Hamilton Theorem. Let $\phi = \mathrm{id}_M$ be the identity on M; we know that $\phi(M) \subseteq IM$ because $M = IM$. Then the identity id_M satisfies a monic polynomial, say

$$\mathrm{id}_M^n + a_1\mathrm{id}_M^{n-1} + \ldots + a_n = 0.$$

for some $a_i \in I$. This implies that

$$\mathrm{id}_M(1 + a_1 + a_2 + \ldots + a_n) = 0$$

Let $r = 1 + a_1 + a_2 + \ldots + a_n$. Then because $a_i \in I$, we have that $r \equiv 1 \pmod I$. Moreover, since $r\mathrm{id}_M = 0$, we have that $rM = 0$. □

To show the normal Nakayama Lemma (Lemma 2.23) from Lemma 2.26, notice that if $r \equiv 1 \pmod{\mathrm{Jac}(R)}$, then $r - 1 \in \mathrm{Jac}(R)$, which means that r is a unit. Hence, $rM = 0 \implies M = 0$.

2.2 Nullstellensätze

The Nullstellensätze, which is a family of results really, that tells us about how the ideals lie inside polynomial algebras. There's several versions, and books tend to state them in many different ways.

Theorem 2.27 (Weak Nullstellensatz)**.** Let k be a field and T be a finitely generated k-algebra. Let Q be a maximal ideal of T. Then the field T/Q is a finite algebraic extension of k.

In particular, if k is algebraically closed and $T = k[X_1, \ldots, X_n]$ is a polynomial algebra, then $Q = (X_1 - a_1, \ldots, X_n - a_n)$ for some $(a_1, \ldots, a_n) \in k^n$.

The proof we're going to present is due to Artin and Tate. We need a couple of Lemmas.

Lemma 2.28. Let $R \subseteq S \subseteq T$ be rings. Suppose R is Noetherian, and T is generated as a ring by R and $t_1, \ldots, t_n$. Suppose moreover that T is a finitely generated S-module. Then S is generated as a ring by R and finitely many elements.

Proof. Since T is finitely generated as an S-module, write $T = Sx_1 + \ldots + Sx_m$ for some $x_1, \ldots, x_m \in T$. Then for each i,

$$t_i = \sum_{j=1}^{m} s_{ij} x_j \tag{1}$$

for some $s_{ij} \in S$. Additionally, products of the x_i are in T, so we can write

$$x_i x_j = \sum_{k=1}^{m} s_{ijk} x_k \tag{2}$$

for some $s_{ijk} \in S$.

Let S_0 be the ring generated by R and all the s_{ij} and s_{ijk}, $S_0 = R\left[\{s_{ij}\}, \{s_{ijk}\}\right]$. Then $R \subseteq S_0 \subseteq S$. The second equation, (2), tells us that powers and products of the x_i can be written using just elements of S_0 and the x_i themselves.

Note that any element of T is a polynomial in the t_i with coefficients in R. Using (1) and (2), we see that each element of T is a linear combination of the x_i with coefficients in S_0. Conversely, we already know that $S_0 \subseteq S \subseteq T$ and $x_i \in T$, so we conclude that

$$T = S_0 x_1 + \ldots + S_0 x_m$$

Therefore, T is a finitely generated S_0-module.

Now R is Noetherian, and $S_0 = R\left[\{s_{ij}\}, \{s_{ijk}\}\right]$ is finitely generated as a ring over R, so by the Hilbert Basis Theorem, S_0 is Noetherian as a ring as well.

Hence, T is a Noetherian S_0-module, because S_0 is Noetherian as a ring and T is finitely generated over S_0. S is an S_0-submodule of T, and hence is a finitely generated S_0-module. But S_0 is generated as a ring by R and finitely many elements, so we conclude that S is generated as a ring by R and finitely many elements. □

Proposition 2.29. Let k be a field, and let R be a finitely-generated k-algebra. If R is a field, then it is a finite algebraic extension of k.

Proof. Suppose R is generated by k and $x_1, \ldots, x_n$, and is a field. Assume for contradiction that R is not algebraic over k. By reordering the x_i if necessary, we may assume that the first m-many variables, $x_1, \ldots, x_m$, are algebraically independent over k, and $x_{m+1}, \ldots, x_n$ are algebraic over $F = k(x_1, \ldots, x_m)$.

R is a finite field extension of F, so $[R\colon F] < \infty$. Therefore, R is a finitely generated F-module / finite dimensional vector space over F.

Apply Lemma 2.28 to $k \subseteq F \subseteq R$. It follows that F is a finitely generated k-algebra. Name the generators $q_1, \ldots, q_t$, with each $q_i = {}^{f_i}/_{g_i}$ for some $f_i, g_i \in k[x_1, \ldots, x_m]$ and $g_i \neq 0$.

There is a polynomial h which is prime to each of the g_i, for example we might take $h = g_1 g_2 \cdots g_t + 1$. The element ${}^{1}/_{h}$ cannot be in the ring generated by k and $q_1, \ldots, q_t$, which contradicts the fact that F is a finitely-generated k-algebra.

Therefore, R must be algebraic over k and so $[R\colon k] < \infty$. $\square$

Proof of Theorem 2.27 (Due to Artin and Tate). Let Q be a maximal ideal of finitely generated k-algebra T. Set $R = T/Q$ and apply Proposition 2.29 to get that T/Q is a finite algebraic field extension of k.

Now if $T = k[X_1, \ldots, X_n]$ a polynomial algebra with k algebraically closed, then $T/Q \cong k$ because k is algebraically closed. Set $\pi\colon T \to k$ with $\ker \pi = Q$. Then $\ker \pi = (X_1 - \pi(X_1), \ldots, X_n - \pi(X_n))$. So Q is of the form we wanted, i.e. $Q = (X_1 - a_1, \ldots, X_n - a_n)$ for some $(a_1, \ldots, a_n) \in k^n$. $\square$

We all have our favorite algebraically closed fields, and yours is probably $\mathbb{C}$. So set $k = \mathbb{C}$. Recall the bijection we talked about in the introduction between radical ideals of $\mathbb{C}[X_1, \ldots, X_n]$ and algebraic subsets of $\mathbb{C}^n$.

Using the Nullstellensatz, we can reformulate this slightly. It tells us that all the maximal ideals of $\mathbb{C}[X_1, \ldots, X_n]$ look like $Q_{(a_1,\ldots,a_n)} = (X - a_1, \ldots, X - a_n)$.

The bijection between radical ideals and algebraic subsets of $\mathbb{C}^n$ can be reformulated as follows:

radical ideals		algebraic subsets
I	$\longrightarrow$	$\{(a_1, \ldots, a_n) \mid I \subseteq Q_{(a_1,\ldots,a_n)}\}$
$\bigcap_{(a_1,\ldots,a_n)\in\mathcal{S}} Q_{(a_1,\ldots,a_n)}$	$\longleftarrow$	$\mathcal{S}$

The Strong Nullstellensatz is saying that this is a bijective correspondence.

Theorem 2.30 (Strong Nullstellensatz)**.** Let k be an algebraically closed field, and let R be a finitely generated k-algebra. Let P be a prime ideal of R. Then

$$P = \bigcap (\text{ maximal ideals } Q \supseteq P\ )$$

Hence,

$$\bigcap_{P \text{ prime in } R} P = \bigcap_{Q \text{ max'l in } R} Q,$$

or more concisely, $\mathrm{Nil}(R) = \mathrm{Jac}(R)$.

Thus, any radical ideal I of $k[X_1, \ldots, X_n]$ is the intersection of the maximal ideals $Q_{(a_1,\ldots,a_n)}$ containing I.

Proof. Let $r \in R \backslash P$ and $\bar{r}$ the image of r in $\mathcal{S} = R/P$. We're going to find a maximal ideal not containing r. Since we're quotienting by a prime ideal, this is an integral domain and since R is a finitely generated k-algebra, then S is finitely generated by k and $s_1, \ldots, s_n$ say.

Invert $\bar{r}$ to get $T = \langle S, \bar{r}^{-1} \rangle$ contained in the fraction field of R/P. Take a maximal ideal Q of T. By the weak Nullstellensatz, $T/Q \cong k$, and so $Q \cap S$ contains elements $s_i - \lambda_i$ with $\lambda_i \in k$. Hence, $Q \cap S$ is a maximal ideal of S not containing $\bar{r}$. Thus, there is a maximal ideal of R containing P but not r, because ideals of R/P are ideals of R containing P.

Therefore
$$\bigcap \{\text{maximal ideals containing } P\} = P.$$
The last part of the theorem follows from the characterization of maximal ideals of $k[x_1, \ldots, x_n]$ being of the form $Q_{(a_1,\ldots,a_n)}$.

Also a radical ideal I is the intersection of the maximal primes containing it because $\mathrm{Nil}(R/I) = 0$, and these primes are the intersection of the maximal ideals containing them. □

2.3 Minimal and associated primes

Throughout this section R is always Noetherian.

Lemma 2.31. If R is Noetherian then every ideal I contains a power of its radical $\sqrt{I}$. In particular, we discover that $\mathrm{Nil}(R)$ is nilpotent if we take $I = 0$ (because $\mathrm{Nil}(R) = \sqrt{0}$).

Proof. Suppose $x_1, \ldots, x_m$ generate $\sqrt{I}$, which is finitely generated because R is Noetherian. Thus $x_i^{n_i} \in I$ for some n_i for each i. Let $n = \sum(n_i - 1) + 1$, and notice that $\left(\sqrt{I}\right)^n$ is generated by products
$$x_1^{r_1} x_2^{r_2} \cdots x_m^{r_m}$$
with $\sum_i r_i = n$, and we must have that $r_i \geqslant n_i$ for some i by the choice of n. Thus, each of these products lies in I. This shows that $\left(\sqrt{I}\right)^n \subseteq I$. □

Definition 2.32 (Alternative definition of prime)**.** A proper ideal I of R is **prime** if, for any two ideals J_1, J_2, $J_1 J_2 \subseteq I \implies J_1 \subseteq I$ or $J_2 \subseteq I$.

Lemma 2.33. If R is Noetherian, a radical ideal is the intersection of finitely many primes.

Proof. Suppose not. Then there are some radical ideals which are not the intersection of finitely many primes. By Zorn, let I be a maximal member of the set of radical ideals that are not the intersection of finitely many primes.

We claim that I must itself be prime, and therefore I is the intersection of a single prime, which is a contradiction.

To see that I is prime, suppose not. Then there are ideals J_1, J_2 with $J_1 J_2 \subseteq I$ but $J_1 \nsubseteq I$, $J_2 \nsubseteq I$ (note: this is an alternative definition of prime). Then notice that $(J_1 + I)(J_2 + I) \subseteq I$, but $I \subsetneq (J_1 + I)$, $I \subsetneq (J_2 + I)$. Let $K_1 = J_1 + I$ and $K_2 = J_2 + I$.

The maximality of I gives that

$$\sqrt{K_1} = Q_1 \cap \ldots \cap Q_s$$

$$\sqrt{K_2} = Q_1' \cap \ldots \cap Q_t'$$

for Q_i, Q_i' prime ideals. Define

$$K = Q_1 \cap Q_2 \cap \ldots \cap Q_s \cap Q_1' \cap \ldots \cap Q_t' = \sqrt{K_1} \cap \sqrt{K_2}.$$

So by Lemma 2.31, we see that

$$K^{m_1} \subseteq K_1,$$

$$K^{m_2} \subseteq K_2,$$

for some m_1, m_2. Hence, $K^{m_1+m_2} \subseteq K_1 K_2 \subseteq I$. But I is a radical ideal and so $K \subseteq I$. However, all the Q_i, Q_j' contain I and so $K \supseteq I$. Therefore, $I = K$, which is a contradiction because I was assumed *not* to be an intersection of finitely many primes. $\square$

Now let I be any ideal of a Noetherian ring R. By Lemma 2.33,

$$\sqrt{I} = P_1 \cap \ldots \cap P_n$$

for finitely many primes P_i. We may remove any P_i from this intersection if it contains one of the others. In doing so, we may assume $P_i \nsubseteq P_j$ for $i \neq j$. Note that if P is prime with $\sqrt{I} \subseteq P$, then

$$P_1 P_2 \cdots P_n \subseteq P_1 \cap \ldots \cap P_n = \sqrt{I} \subseteq P,$$

and so some $P_i \leqslant P$. (This again uses the alternative definition of prime).

Definition 2.34. The **minimal primes** over an ideal I of a Noetherian ring R are those primes P such that if Q is another prime, and $I \subseteq Q \subseteq P$, then $P = Q$.

Lemma 2.35. Let I be an ideal of a Noetherian ring R. Then $\sqrt{I}$ is the intersection of the minimal primes over I and I contains a finite product of the minimal primes over I.

Proof. Each minimal prime over I contains $\sqrt{I}$. The discussion above shows that $\sqrt{I}$ is the intersection of these. Lemma 2.31 now gives that some finite product of these minimal primes lies in I. $\square$

Definition 2.36. Let M be a finitely generated R-module over a Noetherian ring R. A prime ideal P is an **associated prime** for M if it is the **annihilator** of some nonzero element of M.

$$\mathrm{Ann}(m) = \{r \in R \mid rm = 0\}$$

$$\mathrm{Ass}(M) = \{P \mid P \text{ prime}, P = \mathrm{Ann}(m) \text{ for some } m \in M\}.$$

Definition 2.37. A submodule N of M is P-**primary** if $\mathrm{Ass}\left({}^{M}/_{N}\right) = \{P\}$ for some prime ideal P.

Example 2.38. If P is prime, then $\mathrm{Ass}\left({}^{R}/_{P}\right) = \{P\}$. Thus, if P is prime then it is P-primary. In general, an ideal I is P-primary if $\mathrm{Ass}\left({}^{R}/_{I}\right) = \{P\}$.

At the moment, we don't even know that the set of associated primes is nonempty! Let's find some associated primes for a given module.

Lemma 2.39. Let M be a finitely generated module over a Noetherian ring. If $\mathrm{Ann}(M) = \{r \mid rm = 0 \text{ for all } m \in M\} = P$ for a prime ideal P, then $P \in \mathrm{Ass}(M)$.

Proof. Let $m_1, \ldots, m_n$ generate M and let $I_j = \mathrm{Ann}(m_j)$. Then the product $\prod_j I_j$ annihilates each m_j, and so $\prod I_j \subseteq \mathrm{Ann}(M) = P$. Hence, some $I_j \leqslant P$. However, $I_j = \mathrm{Ann}(m_j) \supseteq \mathrm{Ann}(M) = P$. Hence, $I_j = P$ and therefore P is the annihilator of $\mathrm{Ann}(m_j)$, so $P \in \mathrm{Ass}(M)$. □

In fact, we can see that $\mathrm{Ass}(M)$ is nonempty in this case – take the annihilator of the generator m_j.

Lemma 2.40. Let Q be maximal among all annihilators of non-zero elements of M. Then Q is prime and $Q \in \mathrm{Ass}(M)$.

Proof. Suppose $Q = \mathrm{Ann}(m)$ and $r_1 r_2 \in Q$ with $r_2 \notin Q$. We show that $r_1 \in Q$. To that end, $r_1 r_2 \in Q \implies r_1 r_2 m = 0$. Therefore, $r_1 \in \mathrm{Ann}(r_2 m)$. Since $r_2 \notin Q = \mathrm{Ann}(m)$, so $r_2 m \neq 0$. But $Q \subseteq \mathrm{Ann}(r_2 m)$ by commutativity. Therefore, Q and r_1 lie inside $\mathrm{Ann}(r_2 m)$. Maximality among annihilators gives that $Q = \mathrm{Ann}(r_2 m)$ and so $r_1 \in Q$. □

Next, we'll show that $\mathrm{Ass}(M)$ is finite and that all minimal primes over I lie in $\mathrm{Ass}\left({}^{R}/_{I}\right)$.

Since any prime in $\mathrm{Ass}\left({}^{R}/_{I}\right)$ contains I and hence contains a minimal prime over I, we see that minimal primes over I are precisely the minimal members of $\mathrm{Ass}\left({}^{R}/_{I}\right)$. However, there may be non-minimal primes in $\mathrm{Ass}\left({}^{R}/_{I}\right)$.

Example 2.41. Let $R = k[X, Y]$, and let $P = (X, Y)$. P is a prime ideal containing $Q = (X)$. Let $I = PQ = (X^2, XY)$. Then $\mathrm{Ass}\left({}^{R}/_{I}\right) = \{P, Q\}$ but the only minimal prime over I is Q.

Note that I is not primary, but $I = (X^2, XY, Y^2) \cap (X)$, and

$$\mathrm{Ass}\left({}^{R}/_{(X^2, XY, Y^2)}\right) = \{P\}$$

$$\mathrm{Ass}\left({}^{R}/_{(X)}\right) = \{Q\}$$

This example illustrates the following theorem.

Theorem 2.42 (Primary Decomposition)**.** Let M be a finitely generated R-module, for R a Noetherian ring. Let N be a submodule. Then there are $N_1, \ldots, N_t$ with $N = N_1 \cap N_2 \cap \ldots \cap N_t$ with $\mathrm{Ass}\left({}^{M}/_{N_i}\right) = \{P_i\}$ for some distinct primes $P_1, \ldots, P_t$.

We're not going to prove it, because it doesn't come up in practice too often. If you're curious, it's proved in Atiyah-Macdonald. In fact, if one takes a "minimal" such decomposition avoiding redundancy, then the set of primes appearing is unique and is exactly $\mathrm{Ass}\left({}^{M}/_{N}\right)$.

Remark 2.43. Question 17 on the first example sheet shows us that there is an equivalent definition of an ideal I being P-primary, which is more common.

There are two things left to show in our discussion of minimal and associated primes. First, that there are only finitely many associated primes, and second, that the minimal associated primes are exactly the minimal primes.

Lemma 2.44. For a non-zero finitely generated R-module M with R Noetherian, there is a strictly ascending chain of submodules

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_s = M$$

such that each ${}^{M_i}/_{M_{i-1}} \cong {}^{R}/_{P_i}$ for some prime ideal P_i. The P_i need not be distinct.

Proof. By Lemma 2.40, there is $m_1 \in M$ with $\mathrm{Ann}(m_1) = P_1$ a prime. Set $M_1 = Rm_1$ and therefore $M_1 \cong {}^{R}/_{P_1}$. Repeat with ${}^{M}/_{M_1}$ to get ${}^{M_2}/_{M_1} \cong {}^{R}/_{P_2}$. The process terminates since M is Noetherian. □

Lemma 2.45. If $N \leqslant M$, then $\mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}\left({}^{M}/_{N}\right)$.

Proof. Suppose $P \in \mathrm{Ass}(M)$, and so $P = \mathrm{Ann}(m)$ for some $m \in M$. Let $M_1 = Rm \cong {}^{R}/_{P}$. For any nonzero $m_1 \in M_1$, we know that $\mathrm{Ann}(m_1) = P$ since P is prime.

So if $M_1 \cap N \neq 0$, then there is some $m_1 \in M_1 \cap N$ with $\mathrm{Ann}(m_1) = P$. And so $P \in \mathrm{Ass}(N)$.

If $M_1 \cap N = 0$, then the image of M_1 in ${}^{M}/_{N}$ is isomorphic to M_1, and is therefore isomorphic to ${}^{R}/_{P}$, and $\mathrm{Ann}\,(m + N) = \{P\}$ and $P \in \mathrm{Ass}\left({}^{M}/_{N}\right)$. □

Lemma 2.46. $\mathrm{Ass}(M)$ is finite for any finitely generated R-module M, with R Noetherian.

Proof. Use Lemma 2.45 inductively on the chain produced in Lemma 2.44. Therefore, $\mathrm{Ass}(M) \subseteq \{P_1, \ldots, P_s\}$ with P_i as in Lemma 2.44. □

Theorem 2.47. The set of minimal primes over I is a subset of $\mathrm{Ass}\left({}^{R}/_{I}\right)$, for I an ideal of a Noetherian ring R.

Proof. Let $P_1, \ldots, P_n$ be the distinct minimal primes over I. By Lemma 2.33, there is a product of minimal primes over I contained in I.

$$P_1^{s_1} \cdots P_n^{s_n} \subseteq I.$$

Now consider

$$M = {(P_2^{s_2} \cdots P_n^{s_n} + I)}/{I}.$$

Claim that $M \neq 0$. Let $J = \mathrm{Ann}(M)$. It suffices to show that $J \neq R$. We have that $J \geqslant P_1^{s_1}$, so $JP_2^{s_2} \ldots P_n^{s_n} \leqslant I \leqslant P_1$. Since P_1 is primes and not equal to any of $P_2, \ldots, P_n$, we have that $J \leqslant P_1$. Hence, $J \leqslant P_1 \lneq R$, so $M \neq 0$.

So now by Lemma 2.44, there is a chain of submodules

$$0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_t = M$$

with each factor $M_j/M_{j-1} \cong R/Q_j$ for some prime ideal Q_j. Note that $P_1^{s_1} \leqslant \mathrm{Ann}(M)$, so in particular $P_1^{s_1} \leqslant \mathrm{Ann}\left({M_j}/{M_{j-1}}\right) = Q_j$ for all j. Since Q_j is prime, this implies $P_1 \leqslant Q_j$ for all j. Now we also have that $\prod_{i=1}^{t} Q_i \leqslant \mathrm{Ann}(M) = P_1$, so there is some k such that $Q_k \leqslant P_1$ since P_1 is prime. This shows $Q_k = P_1$ for this particular k.

Pick the least j with $Q_j = P_1$. Therefore, $\prod_{k<j} Q_k \nsubseteq P_1$. Now take some nonzero $x \in M_j \backslash M_{j-1}$.

- If $j = 1$, then $\mathrm{Ann}(x) = Q_1 = P_1$, and so $P_1 \in \mathrm{Ass}\,(M)$.
- If $j \neq 1$, pick $r \in \prod_{k<j} Q_k \backslash P_1$. Notice that if $s \in P_1 = Q_j = \mathrm{Ann}(M_j/M_{j-1})$, we have $sx \in M_{j-1}$. Hence, $r(sx) = 0$ because r is a product of things in Q_k for $k < j$, so multiplying by r is multiplying successively by elements of $Q_{j-1}, Q_{j-2}, \ldots$. Multiplying sx by r therefore sends the element sx down the line of factors $M_{j-1}, M_{j-2}, \ldots$, until it hits zero. This was a rather long and convoluted explanation of the fact that $r(sx) = 0$. Now we have that $r(sx) = 0 \implies s(rx) = 0$ for any $s \in P_1$, so $P_1 \leqslant \mathrm{Ann}(rx)$.

  However, $rx \notin M_{j-1}$ since $r \notin P_1$ and $P_1 = \mathrm{Ann}(M_j/M_{j-1})$. So we have that $\mathrm{Ann}(rx + M_{j-1}) = Q_j = P_1$, since $\mathrm{Ass}(M_j/M_{j-1}) = \{Q_j\} = \{P_1\}$. Then $\mathrm{Ann}(rx) \subseteq \mathrm{Ann}(rx + M_{j-1}) = P_1$.

  So $\mathrm{Ann}(rx) \leqslant P_1$. Therefore, $P_1 = \mathrm{Ann}(rx)$, so $P \in \mathrm{Ass}(M)$.

So we have shown that $P_1 \in \mathrm{Ass}(M) \subset \mathrm{Ass}\left({R}/{I}\right)$. We can similarly conclude that any minimal prime P_i is an associated prime of ${R}/{I}$. Therefore,

$$\{\text{minimal primes over } I\} \subseteq \mathrm{Ass}\left({R}/{I}\right). \qquad \square$$

Notice that associated primes need not be minimal, by Example 2.41.

3 Localization

Let R be a commutative ring with identity.

Definition 3.1. S is a **multiplicatively closed set** of R if

(1) S is closed under multiplication;

(2) $1 \in S$.

Define a relation $\equiv$ on $R \times S$ by

$$(r_1, s_1) \equiv (r_2, s_2) \iff (r_1 s_2 - r_2 s_1)x = 0 \text{ for some } x \in S.$$

This is an equivalence relation. Denote the class of (r, s) by ${}^r\!/_s$ and the set of equivalence classes by $S^{-1}R$. This can be made into a ring in the obvious way:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

There is a ring homomorphism $\theta \colon R \to S^{-1}R$ given by $r \mapsto {}^r\!/_1$.

Lemma 3.2. Let $\phi \colon R \to T$ be a ring homomorphism with $\phi(s)$ is a unit in T for all $s \in S$. Then there is a unique ring homomorphism $\alpha \colon S^{-1}R \to T$ such that ϕ factors through θ: $\phi = \alpha \circ \theta$.

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\theta"'] & T \\ S^{-1}R \arrow[ur, "\alpha"'] & \end{tikzcd}$$

Example 3.3. Examples of localization.

(1) The fraction field of an integral domain R with $S = R \backslash \{0\}$.

(2) $S^{-1}R$ is the zero ring if and only if $0 \in S$.

(3) If I is an ideal of R, we can take $S = 1 + I = \{1 + r \mid r \in I\}$.

(4) R_f where $S = \{f^n \mid n \geqslant 0\}$.

(5) If P is a prime ideal of R, set $S = R \backslash P$. We write R_P for $S^{-1}R$ in this case.

The process of passing from R to R_P is called **localization**. Some authors (e.g. Atiyah-Macdonald) restrict the use of the word localization to this case. In the noncommutative setting, "localization" is used more generally.

The elements ${}^r\!/_s$ with $r \in P$ forms an ideal P_P of R_P. This is the unique maximal ideal of R_P.

If ${}^r\!/_s$ is such that $r \notin P$, then $r \in S = R \backslash P$. If ${}^r\!/_s$ is such that $r \notin P$ then $r \in S$ and ${}^r\!/_s$ is a unit in R_P.

Definition 3.4. A ring with a unique maximal ideal is called a **local ring**.

Example 3.5. Examples of local rings.

(1) $R = \mathbb{Z}$, and $P = (p)$ for p a prime. $R_P = \{{}^m/_n \mid p \text{ does not divide } n\} \subseteq \mathbb{Q}$. $P_P = \{{}^m/_n \colon p \mid m, p \nmid n\}$.

(2) $R = k[X_1, \ldots, X_n]$ are the polynomial functions on k^n. $P = (X_1 - a_1, \ldots, X_n - a_n)$ is a maximal ideal by the Nullstellensatz. R_P is the subring of $k(X_1, \ldots, X_n)$, the field of rational functions, consisting of rational functions defined at $(a_1, \ldots, a_n) \in k^n$. The maximal ideal of this local ring consists of such rational functions which are zero at $(a_1, \ldots, a_n)$.

We can also localize modules. Given an R-module M, we may define an equivalence relation $\equiv$ on $M \times S$ for S a multiplicatively closed subset S of R by

$$(m_1, s_1) \equiv (m_2, s_2) \iff \exists x \in S \text{ such that } x(s_1 m_2 - s_2 m_1) = 0.$$

This is an equivalence relation. Denote the set of equivalence classes of (m, s) by ${}^m/_s$. The set of equivalence relations is denoted $S^{-1}M$, and $S^{-1}M$ is an $S^{-1}R$-module via

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}$$
$$\frac{r}{s_1} \cdot \frac{m}{s_2} = \frac{rm}{s_1 s_2}$$

In the case where $S = R \backslash P$ for a prime ideal P, we write M_P for the module $S^{-1}M$.

If $\theta \colon N \to M$ is an R-module homomorphism, then we may define $S^{-1}\theta \colon S^{-1}N \to S^{-1}M$ by ${}^n/_s \mapsto {}^{\theta(n)}/_s$. This is an $S^{-1}R$-module map.

If $\phi \colon M \to L$ is another R-module map, then $S^{-1}(\phi \circ \theta) = S^{-1}\phi \circ S^{-1}\theta$. This means that $S^{-1}(-)$ is a functor from R-**Mod** to $S^{-1}R$-**Mod**.

Definition 3.6. A sequence of R-modules $M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2$ is **exact** at M if $\operatorname{im}\theta = \ker\phi$. A **short exact sequence** is of the form

$$0 \longrightarrow M_1 \xrightarrow{\ \theta\ } M \xrightarrow{\ \phi\ } M_2 \longrightarrow 0$$

with exactness at M_1, M, and M_2.

In a short exact sequence, exactness at M_1 tells us that θ is injective, and exactness at M_2 tells us that ϕ is surjective. Exactness at M tells us that M_2 is isomorphic to ${}^M/_{M_1}$.

Lemma 3.7. If $M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2$ is exact at M, then the sequence

$$S^{-1}M_1 \xrightarrow{S^{-1}\theta} S^{-1}M \xrightarrow{S^{-1}\phi} S^{-1}M_2$$

is exact at $S^{-1}M$. Hence, $S^{-1}(-)$ is an exact functor.

Proof. Since $\ker\phi = \operatorname{im}\theta$, we know that $\phi\circ\theta = 0$. Therefore, $(S^{-1}\phi)\circ(S^{-1}\theta) = S^{-1}(\phi\circ\theta) = 0$. Therefore, $\operatorname{im} S^{-1}\theta \subseteq \ker S^{-1}\theta$.

Now suppose that $m/s \in \ker S^{-1}\phi \subseteq S^{-1}M$. So $\phi(m)/s = 0$ in $S^{-1}M_2$. Hence, by the definition of localization, there is a $t \in S$ with $t(\phi(m)) = 0$ in M_2. So $tm \in \ker\phi = \operatorname{im}\theta$ and $tm = \theta(m')$ for some $m' \in M_1$. So in $S^{-1}M$,

$$\frac{m}{s} = \frac{\theta(m')}{ts} = S^{-1}\theta\left(\frac{m'}{ts}\right) \in \operatorname{im} S^{-1}\theta.$$

Therefore, $\ker S^{-1}\phi \subseteq \operatorname{im} S^{-1}\theta$. □

Lemma 3.8. Let $N \leqslant M$. Then $S^{-1}\left({}^{M}/_{N}\right) \cong {}^{S^{-1}M}/_{S^{-1}N}$ as $S^{-1}R$-modules.

Proof. Apply Lemma 3.7 to the short exact sequence $0 \to N \hookrightarrow M \twoheadrightarrow {}^{M}/_{N} \to 0$, where $N \hookrightarrow M$ is the embedding as a submodule and $M \twoheadrightarrow {}^{M}/_{N}$ is the natural quotient map. We get a short exact sequence

$$0 \to S^{-1}N \to S^{-1}M \to S^{-1}\left({}^{M}/_{N}\right) \to 0$$

and hence $S^{-1}\left({}^{M}/_{N}\right) \cong {}^{S^{-1}M}/_{S^{-1}N}$. □

Remark 3.9. If $N \leqslant M$, then $S^{-1}N \to S^{-1}M$ is injective and we can regard $S^{-1}N$ as a submodule of $S^{-1}M$.

Let R be a ring and let S be a multiplicatively closed subset. What are the ideals of $S^{-1}R$? If I is an ideal of R, then $S^{-1}I$ is an ideal of $S^{-1}R$, by Lemma 3.7.

Lemma 3.10.

(1) Every ideal J of $S^{-1}R$ is of the form $S^{-1}I$ for $I = \{r \in R \mid r/1 \in J\}$, which is an ideal of R.

(2) Prime ideals of $S^{-1}R$ are in bijection with prime ideals of R avoiding S (i.e, have an empty intersection with S).

$$\begin{array}{ccc} \{\text{ prime ideals of } S^{-1}R \} & \longleftrightarrow & \{\text{ prime ideals of } R \text{ which don't meet } S \} \\ S^{-1}P & \longleftarrow & P \\ Q & \longrightarrow & \{r \in R \mid r/1 \in Q\} \end{array}$$

Remark 3.11. Warning! This correspondence in Lemma 3.10(2) doesn't extend to all ideals!

Example 3.12. Consider $R = \mathbb{Z}/6\mathbb{Z}$, with $P = 2\mathbb{Z}/6\mathbb{Z}$ and $S = \{1, 3, 5\}$. We have a short exact sequence

$$0 \to {}^{2\mathbb{Z}}/_{6\mathbb{Z}} \to {}^{\mathbb{Z}}/_{6\mathbb{Z}} \to {}^{\mathbb{Z}}/_{2\mathbb{Z}} \to 0.$$

Localizing at P, we see that

$$0 \to \left({}^{2\mathbb{Z}}/_{6\mathbb{Z}}\right)_P = 0 \to \left({}^{\mathbb{Z}}/_{6\mathbb{Z}}\right)_P \to \left({}^{\mathbb{Z}}/_{2\mathbb{Z}}\right)_P \to 0.$$

Here, $P_P = 0$ and $R_P/P_P \cong \mathbb{Z}/2\mathbb{Z}$. This shows that the correspondence does not extend to arbitrary ideals.

Proof.

(1) Let J be an ideal of $S^{-1}R$, and $r/s \in J$. Then by multiplying by $s/1$, we can see that $r/1 \in J$. Then let $I = \{r \in R \mid r/1 \in J\}$. Then $r \in I$, so clearly $J \subseteq S^{-1}I$.

Conversely, if $r \in I$ then $r/1 \in J$, and so $S^{-1}I \subseteq J$. Hence, $J = S^{-1}I$.

(2) Let Q be a prime of $S^{-1}R$, and set $P = \{r \in R \mid r/1 \in Q\}$. Claim that P is a prime ideal, and $P \cap S = \varnothing$.

If $xy \in P$, then $xy/1 \in Q$, so either $x/1 \in Q$ or $y/1 \in Q$. Hence, either $x \in P$ or $y \in P$.

If $s \in P \cap S$, then $s/1 \cdot 1/s = 1/1 \in Q$. However, this is the unit in $S^{-1}R$, which is a contradiction because prime ideals must be proper.

Now let's do the converse. First, notice that if $r/1 \in S^{-1}P$ then $r/1 = p/s$ for some $p \in P$, and therefore $s_1(rs - p) = 0$ for some $s_1 \in S$, and $rss_1 \in P$. But S is multiplicatively closed so $ss_1 \in S$. Since $P \cap S = \varnothing$, then $ss_1 \notin P$, and so $r \in P$.

So if P is prime with $P \cap S = \varnothing$ and $r_1/s_1 \cdot r_2/s_2 \in S^{-1}P$, then $r_1r_2/s_1s_2 \in S^{-1}P$ and therefore $r_1r_2/1 \in S^{-1}P$. Therefore, $r_1r_2 \in P$ and so either $r_1 \in P$ or $r_2 \in P$. Hence, $r_1/s_1 \in S^{-1}P$ or $r_2/s_2 \in S^{-1}P$ so $S^{-1}P$ is prime. □

Example 3.13. When P is a prime ideal of R and $S = R\backslash P$, then we get a bijective correspondence between prime ideals in R_P and prime ideals of R contained in P.

$$\left\{\begin{matrix}\text{prime ideals}\\ \text{of } R_P\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{prime ideals of } R\\ \text{contained in } P\end{matrix}\right\}$$

For example, if P is a minimal prime of R, R_P has only one prime P_P.

If $R = k[X_1, \ldots, X_n]$ and Q is a maximal ideal of the form $(X_1 - a_1, \ldots, X_n - a_n)$, then the prime ideals of R_Q correspond to the prime ideals contained in $(X_1 - a_1, \ldots, X_n - a_n)$. These ideals consist only of the polynomials vanishing at $(a_1, \ldots, a_n)$.

Lemma 3.14. If R is a Noetherian ring, then $S^{-1}R$ is Noetherian.

Proof. Consider any chain of ideals $J_1 \leqslant J_2 \leqslant \ldots$ in $S^{-1}R$. Set $I_k = \{r \in R \mid r/1 \in J_k\}$. Then $J_k = S^{-1}I_k$ using Lemma 3.10(1), and we have a chain of ideals $I_1 \leqslant I_2 \leqslant \ldots$ in R. R is Noetherian so this chain terminates, say $I_t = I_{t+1} = I_{t+2}$. But $J_k = S^{-1}I_k$ and therefore $J_t = J_{t+1} = \ldots$. The chain terminates in $S^{-1}R$. □

This last lemma is just something that will be useful later, so we'll make a note of it now.

Lemma 3.15. Let P be a prime ideal of R and let S be a multiplicatively closed subset with $S \cap P = \varnothing$. By Lemma 3.10, $S^{-1}P$ is a prime ideal of $S^{-1}R$. Then $(S^{-1}R)_{S^{-1}P} \cong R_P$. In particular, if Q is a prime ideal of R with $P \leqslant Q$, then $S = R\backslash Q$, then $(R_Q)_{P_Q} = R_P$.

Exercise 3.16. Prove Lemma 3.15. This is on example sheet 2.

Remark 3.17. The reason that Lemma 3.15 is introduced now is that we'll need it when we go to prove Krull's principal ideal theorem and its generalizations. When we talk about dimension, we'll be interested in chains of prime ideals. This theorem is so important that the first time Brookes lectured this class, he was told off for not proving it.

3.1 Local Properties

Definition 3.18. A property $\mathcal{P}$ is a property of a ring R (or an R-module M) is said to be **local** if R (or M) has property P precisely when R_P (or M_P) has $\mathcal{P}$ for each prime ideal P of R.

The next lemma says that being zero is a local property.

Lemma 3.19. The following are equivalent for an R-module M.

(1) $M = 0$;

(2) $M_P = 0$ for all prime ideals P of R;

(3) $M_Q = 0$ for all maximal ideals Q of R.

Proof. Clearly (1) $\implies$ (2) $\implies$ (3).

To see (3) $\implies$ (1), suppose that $M \neq 0$, and take a nonzero element $m \in M$. Then $\operatorname{Ann}_R(m) \subsetneq R$ is a proper ideal. Extend this to a maximal ideal Q containing $\operatorname{Ann}_R(m)$. There is a surjective map $\phi\colon M_1 \cong R/\operatorname{Ann}_R(m) \to R/Q$, where $M_1 = Rm$. So we have a short exact sequence

$$0 \to \ker\phi \to M_1 \xrightarrow{\phi} {}^{R}/_{Q} \to 0.$$

By the exactness of localization, Lemma 3.7, we get a short exact sequence

$$0 \to (\ker\phi)_Q \to (M_1)_Q \to \left({}^{R}/_{Q}\right)_Q \to 0$$

But $\left({}^{R}/_{Q}\right)_Q \cong {}^{R_Q}/_{Q_Q} \neq 0$. Therefore, $(M_1)_Q \neq 0$.

But we have a short exact sequence

$$0 \to M_1 \to M \to {}^{M}/_{M_1} \to 0$$

and exactness of localization gives

$$0 \to (M_1)_Q \neq 0 \to M_Q \to \left({}^{M}/_{M_1}\right)_Q \to 0$$

so $M_Q \neq 0$. $\square$

Another proof of Lemma 3.19. Clearly (1) $\implies$ (2) $\implies$ (3).

To see that (3) $\implies$ (1), let $m \in M$. Then for each maximal ideal Q of R, ${}^{m}/_{1} = {}^{0}/_{1}$ in M_Q, so there is some $s_Q \in R \backslash Q$ such that $s_Q m = 0$. There is such an

s for each maximal ideal Q. Let I be the ideal generated by s_Q for all maximal ideals Q. Since $s_Q \notin Q$, I is not contained in any maximal ideal of R. Therefore, $1 \in I$. Hence, 1 is a linear combination of some of these s_Q, and $s_Q m = 0$ for all Q, so $1m = 0$. □

Lemma 3.20. Let $\phi \colon M \to N$ be an R-module homomorphism. Then the following are equivalent:

(1) ϕ is injective;

(2) $\phi_P \colon M_P \to N_P$ is injective for all prime ideals P;

(3) $\phi_P \colon M_Q \to N_Q$ is injective for all maximal ideals Q.

Exercise 3.21. Prove Lemma 3.20, and then prove it with injective replaced by surjective. This is also on Example Sheet 2.

There are other local properties that are more exciting, such as flatness (which we'll meet when we think about homological algebra).

4 Dimension

For this section, we'll assume that all rings are commutative with an identity. There are several different notions of dimension: Krull dimension for rings, transcendence degree over the field for finite-dimensional k-algebras, and length.

I don't think we'll talk about the spectra too much but it's useful to define at least for notation. It's used a lot in algebraic geometry.

Definition 4.1. The **spectrum** of a ring R is the set of prime ideals of R.

$$\operatorname{Spec}(R) = \{P \mid P \text{ prime ideal of } R\}.$$

Definition 4.2. The **length** of a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n$ is n. Note that the numbering starts at zero, so the length is the number of links in the chain.

Definition 4.3. The **(Krull) dimension** of a ring R is the supremum of the length of chains of prime ideals, if it exists, or otherwise infinite.

$$\dim R = \sup\{n \mid \text{ there is a chain of prime ideals of } R \text{ of length } n\}$$

Definition 4.4. The **height** of a prime ideal P is

$$\operatorname{ht}(P) = \sup\{n \mid \text{ there is a chain of primes } P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_n = P\},$$

or infinite if this does not exist.

Now by Lemma 3.10, the correspondence between primes with empty intersection with $R \backslash P$ and primes of R_P, we have that $\operatorname{ht}(P) = \dim R_P$.

Example 4.5.

(1) An Artinian ring has dimension zero, by example sheet 1, since all primes are maximal. Conversely, a Noetherian ring of dimension zero is Artinian (example sheet 2).

(2) $\dim \mathbb{Z} = 1$, because $(0) \subsetneq (p)$ where p is prime is a chain of length 1. Likewise, $\dim k[x] = 1$ where k is a field. These are examples of Dedekind domains (that is, integrally closed dimension 1 integral domains).

(3) $\dim k[X_1, \dots, X_n] \geqslant n$ since there is a chain of prime ideals of length n given by

$$\langle 0 \rangle \subsetneqq \langle X_1 \rangle \subsetneqq \langle X_1, X_2 \rangle \subsetneqq \langle X_1, X_2, X_3 \rangle \subsetneqq \dots \subsetneqq \langle X_1, X_2, \dots, X_n \rangle.$$

In fact, $\dim k[X_1, \dots, X_n] = n$, but this will take some proving.

Lemma 4.6. The height 1 primes of $k[X_1, \dots, X_n]$ are precisely those of the form $\langle f \rangle$ for f prime/irreducible in $k[X_1, \dots, X_n]$.

Proof. (c.f. question 5 on example sheet 1).

Recall $k[X_1, \dots, X_n]$ is a UFD. Certainly such an ideal $\langle f \rangle$ is prime because f is prime, and any nonzero prime ideal P contains such an $\langle f \rangle$ since if $g \in P \backslash \{0\}$, then one of its irreducible factors is in P.

If Q is another prime with $0 \subsetneqq Q \leqslant \langle f \rangle$ for f irreducible, then there is an irreducible h with $0 \subsetneqq \langle h \rangle \leqslant Q \leqslant \langle f \rangle$, so f divides h and irreducibility tells us that $\langle h \rangle = \langle f \rangle$. □

Before proving that $\dim k[X_1, \dots, X_n] = n$, we need to consider the relationship between chains of prime ideals in a subring R and a larger ring T.

$$\begin{array}{ccc} \operatorname{Spec} T & \xrightarrow{\text{restriction}} & \operatorname{Spec} R \\ P & \longmapsto & P \cap R \end{array}$$

But we'll show that if T is integral over R then the restriction map has finite fibers. We need to consider integral extensions for this to make sense.

4.1 Integral Extensions

Definition 4.7. Let $R \subseteq S$ be rings. Then $x \in S$ is **integral** over R if it satisfies a monic polynomial with coefficients in R.

For example, the elements of Q which are integral over $\mathbb{Z}$ are just the integers. This means that the term *integral* is not actually terrible.

Lemma 4.8. The following are equivalent:

(1) $x \in S$ is integral over R;

(2) $R[x]$ (the subring of S generated by R and x) is a finitely generated R-module;

(3) $R[x]$ is contained in a subring T of S with T being a finitely generated R-module.

Proof.

(1) $\implies$ (2). If x satisfies a monic polynomial $x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0$ with $r_i \in R$, then $R[x]$ is generated by $1, x, x^2, \ldots, x^{n-1}$ as an R-module.

(2) $\implies$ (3). Obvious: take $T = R[x]$.

(3) $\implies$ (1). (c.f. Theorem 2.25) Suppose $y_1, \ldots, y_m$ generate T as an R-module. Consider multiplication by x in the ring T.

$$xy_i = \sum_j r_{ij} y_j$$

for each i. Therefore,

$$\sum_j (x\delta_{ij} - r_{ij}) y_j = 0$$

Multiplying on the right by the adjugate of the matrix $(A_{ij}) = (x\delta_{ij} - r_{ij})$, we deduce that $(\det A) y_j = 0$ for all j. But $1 \in S$ is an R-linear combination of the y_j and so $\det A = 0$. But $\det A$ is of the form $x^m + r_{m-1}x^{m-1} + \ldots + r_0 = \det A = 0$, so x is integral over R. □

Lemma 4.9. If $x_1, \ldots, x_n \in S$ are integral over R then $R[x_1, \ldots, x_n]$, the subring of R generated by R and $x_1, \ldots, x_n$, is a finitely generated R-module.

Proof. Easy induction on n. □

Lemma 4.10. Let $R \subseteq S$ be rings. The set $T \subseteq S$ of elements of S integral over R forms a subring containing R.

Proof. Clearly every element of R is integral over R, satisfying $x - r = 0$. If $x, y \in T$, then by Lemma 4.9 $R[x, y]$ is a finitely generated R-module. So by Lemma 4.8(3), $x \pm y$ and xy are integral over R. □

Definition 4.11. Let $R \subseteq S$ be rings. Let $T \subseteq S$ be those elements of S integral over R. Then

(a) T is the **integral closure of** R **in** S;

(b) if $T = R$, then R is **integrally closed in** S;

(c) if $T = S$, then S is **integral over** R;

(d) if R is an integral domain, we say that R is **integrally closed** if it is integrally closed in the fraction field of R.

Example 4.12. $\mathbb{Z}$ is integrally closed (over $\mathbb{Q}$, but per Definition 4.11(d) we won't mention what it's integrally closed over because it's an integral domain.) Likewise, $k[X_1, \ldots, X_n]$ is integrally closed.

In number field K, a finite algebraic extension of $\mathbb{Q}$, the integral closure of $\mathbb{Z}$ is the **ring of integers** of K.

Remark 4.13. Being "integrally closed" is a local property of integral domains (also on example sheet 2).

Remark 4.14. There were a few things that I left unsaid last time because we ran out of time.

(1) We'll prove Noether's normalization lemma for finitely generated k-algebras T to say that they contain a subalgebra R isomorphic to a polynomial algebra over which T is integral.

Furthermore, we'll see that if T is an integral domain, and is a finitely generated k-algebra, then it's integral closure T_1 in its fraction field is a finitely generated T-module.

Considering the prime spectra,

$$\begin{array}{ccccc} \mathrm{Spec}(T_1) & \xrightarrow{\text{restriction}} & \mathrm{Spec}(T) & \xrightarrow{\text{restriction}} & \mathrm{Spec}(R) \\ & & Q & \longmapsto & Q \cap R \end{array}$$

We'll see that the fibers in both maps are finite. The geometric property corresponding to "integrally closed" is "**normal.**"

For curves, normal is the same as "non-singular" or "smooth".

(2) The integral closure of an integral domain R has an alternative characterization as the intersection of all the valuation rings of the fraction field of R containing R.

We need to understand how prime ideals behave under integral extensions. We're going to prove eventually two theorems from the 1940's, the Going Up Theorem and the Going Down Theorem. The Going Up Theorem is easy, but Going Down requires lots more work. To set up the proofs, we need some lemmas and some new terminology about primes in an integral extension laying over others.

Lemma 4.15 (Integrality is transitive)**.** If $R \subseteq T \subseteq S$ and T is integral over R and S is integral over T, then S is integral over R.

Proof. Let $x \in S$. Then x is integral over T, so there are $t_i \in T$ such that

$$x^n + t_{n-1}x^{n-1} + \ldots + t_0 = 0. \tag{3}$$

Each of these t_i is integral over R, so $R[t_0, \ldots, t_{n-1}]$ is a finitely generated R-module. Then (3) shows that $R[t_0, \ldots, t_{n-1}, x]$ is a finitely generated R-module, and this R-module contains $R[x]$. Hence, x is integral over R by Lemma 4.8 □

Lemma 4.16. Let $R \subseteq T$ be rings with T integral over R

(i) If J is an ideal of T then ${}^{T}/_{J}$ is integral over ${}^{R}/_{R \cap J} \cong {}^{R+J}/_{J} \leqslant {}^{T}/_{J}$.

(ii) If S is a multiplicatively closed subset of R, then $S^{-1}T$ is integral over $S^{-1}R$.

Proof.

(i) If $x \in T$, then x satisfies a monic polynomial with coefficients in r, say

$$x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0 \tag{4}$$

for some $r \in R$. Modulo J, let $\bar{r}$ denote the image of r in ${}^{T}/_{J}$. Hence, we have that in T/J,

$$\bar{x}^n + \bar{r}_{n-1}\bar{x}^{n-1} + \ldots + \bar{r}_0 = 0$$

and $\bar{x}$ satisfies a monic equation with coefficients in ${}^{T}/_{J}$.

(ii) Suppose ${}^{x}/_{s} \in S^{-1}T$. Then dividing (4) by s^n gives

$$\left({}^{x}/_{s}\right)^n + \left({}^{r_{n-1}}/_{s}\right)\left({}^{x}/_{s}\right)^{n-1} + \ldots + \left({}^{r_0}/_{s^n}\right) = 0$$

and so ${}^{x}/_{s}$ is integral over $S^{-1}R$.

$\square$

Lemma 4.17. Suppose $R \subseteq T$ are integral domains with T integral over R. Then T is a field if and only if R is a field.

Proof. Suppose R is a field. Let $t \in T \backslash \{0\}$ and choose an equation of least degree of the form

$$t^n + r_{n-1}t^{n-1} + \ldots + r_0 = 0$$

with $r_i \in R$. T is an integral domain and so $r_0 \neq 0$, else we could cancel t on both sides to get another monic equation of smaller degree. So t has inverse given by the formula

$$-r_0^{-1}\left(t^{n-1} + r_{n-1}t^{n-2} + \ldots + r_1\right) \in T$$

and therefore T is a field.

Conversely, suppose T is a field and $x \in R$, $x \neq 0$. Then it has an inverse $x^{-1} \in T$. So x^{-1} satisfies some monic equation

$$x^{-m} + r'_{m-1}x^{-m+1} + \ldots + r'_0 = 0$$

with $r_i \in R$. Multiply by x^m and rearrange to get

$$x^{-1} = -(r'_{m-1} + r'_{m-2} + \ldots + r'_0 x^{m-1}) \in R$$

Therefore, the inverse of x lies inside R, so R is a field. $\square$

This is our last lemma before the important theorem.

Lemma 4.18. Let $R \subseteq T$ be rings with T integral over R. Let Q be a prime ideal of T and set $P = Q \cap R$. Then Q is maximal if and only if P is maximal.

Proof. This is easy once we apply the previous lemmas! By Lemma 4.16(i), ${}^{T}/_{Q}$ is integral over ${}^{R}/_{P}$, and both are integral domains because Q, P are prime ideals. Then by Lemma 4.17, ${}^{T}/_{Q}$ is a field if and only if ${}^{R}/_{P}$ is a field. Hence, Q is maximal if and only if P is maximal. $\square$

Now it's theorem time!

Theorem 4.19 (Incomparability Theorem)**.** Let $R \subseteq T$ be rings with T integral over R. Let $Q \leqslant Q_1$ be prime ideals in T. Suppose $Q \cap R = P = Q_1 \cap R$. Then $Q = Q_1$.

It follows from this theorem that a strict chain in $\operatorname{Spec}(T)$ restricts to a strict chain in $\operatorname{Spec}(R)$. And therefore, $\dim R \geqslant \dim T$.

Proof. Apply Lemma 4.16(ii) with $S = R \backslash P$. Then T_P is integral over R_P. We should note the slight abuse of notation that $T_P = S^{-1}T$ but P is not an ideal of T.

From the last chapter, we know that there is a prime $S^{-1}P = P_P$ in R_P, which is the unique maximal ideal in the local ring R_P. Also there are $S^{-1}Q$ and $S^{-1}Q_1$ in $T_p = S^{-1}T$ which are also prime (note that Q, Q_1 miss S). Moreover, using the fact that $Q \cap R = Q_1 \cap R$, then

$$S^{-1}Q \cap S^{-1}R = S^{-1}P$$

$$S^{-1}Q_1 \cap S^{-1}R = S^{-1}P$$

By Lemma 4.18, since $S^{-1}P$ is the unique maximal ideal of $S^{-1}R$, then $S^{-1}Q$ and $S^{-1}Q_1$ are both maximal. But $S^{-1}Q \leqslant S^{-1}Q_1$ since $Q \leqslant Q_1$, so maximality gives $S^{-1}Q = S^{-1}Q_1$. Finally, using the bijection between prime ideals in $S^{-1}T$ and prime ideals in T that don't meet S gives $S^{-1}Q = S^{-1}Q_1 \implies Q = Q_1$. □

Theorem 4.20 (Lying Over Theorem)**.** Let $R \subseteq T$ be rings, T integral over R. Let P be a prime ideal of R. Then there is a prime Q of T with $Q \cap R = P$, i.e. Q **lies over** P**.** In other words, the restriction map $\operatorname{Spec} T \to \operatorname{Spec} R$ is surjective.

Proof. By Lemma 4.16(ii), $S^{-1}T = T_P$ is integral over $S^{-1}R = R_P$, where $S = R \backslash P$(again we abuse notation with T_P). Take a maximal ideal of T_P. By the bijection between primes of $S^{-1}T$ and primes of T that miss S, this maximal ideal is of the form $S^{-1}Q$ for some prime ideal Q of T with $Q \cap S = \varnothing$.

Then $S^{-1}Q \cap S^{-1}R$ is maximal by Lemma 4.18, but $S^{-1}R = R_P$ has the unique maximal ideal $S^{-1}P = P_P$. So, $S^{-1}Q \cap S^{-1}R = S^{-1}P$.

Hence, we deduce that $Q \cap R = P$ by considering things of the form ${}^{r}/_{1}$ in $S^{-1}Q \cap S^{-1}R$ and $S^{-1}P$. □

Earlier, we talked about the restriction map $\operatorname{Spec} T \to \operatorname{Spec} R$ for rings $R \subseteq T$ with T integral over R. The Lying Over Theorem says that this map is surjective, and the Incomparability Theorem says that if $Q \cap R = Q_1 \cap R$ with $Q \leqslant Q_1$, then $Q = Q_1$ (this is not quite injectivity). Today we'll prove two theorems of Cohen and Seidenberg from 1946 called the Going Up and Going Down theorems. The Going Up theorem is an easy induction from the Lying Over Theorem, but the Going Down theorem requires some field theory.

Theorem 4.21 (Going Up Theorem)**.** Let $R \subseteq T$ be rings with T integral over R. Let $P_1 \leqslant \ldots \leqslant P_n$ be a chain of primes in R, and let $Q_1 \leqslant \ldots \leqslant Q_m$ (with $m \leqslant n$)

be a chain of prime ideals of T wtih $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant m$. Then the chain $Q_1 \leqslant \ldots \leqslant Q_m$ can be extended to a chain $Q_1 \leqslant \ldots \leqslant Q_m \leqslant Q_{m+1} \leqslant \ldots Q_n$ with $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant n$.

Theorem 4.22 (Going Down Theorem)**.** Let $R \subseteq T$ be integral domains with R integrally closed, T integral over R. Let $P_1 \geqslant \ldots \geqslant P_n$ be a chain of prime ideals of R and let $Q_1 \geqslant \ldots \geqslant Q_m$ be a chain of prime ideals of T with $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant m$. Then we can extend the chain $Q_1 \geqslant \ldots \geqslant Q_m$ to a chain $Q_1 \geqslant \ldots \geqslant Q_m \geqslant Q_{m+1} \geqslant \ldots \geqslant Q_m$ with $Q_i \cap R = P_i$ for $1 \leqslant i \leqslant n$.

Note that the Going Down Theorem requires stronger hypotheses than the Going Up Theorem! Specifically, we require that R, T are integral domains and R is integrally closed in its fraction field in addition to the assumptions of the Going Up Theorem.

Before we prove these, let's just see why they're useful. There are several straightforward corollaries.

Corollary 4.23 (Corollary to Going Up (Theorem 4.21))**.** Dimensions stay the same under integral extension. More precisely, let $R \subseteq T$ be rings with T integral over R. Then $\dim R = \dim T$.

Proof. Take a chain $Q_0 \subsetneqq Q_1 \subsetneqq \ldots \subsetneqq Q_n$ of prime ideals of T. By the Incomparability Theorem (Theorem 4.19) we have a chain $P_0 \subsetneqq P_1 \subsetneqq \ldots \subsetneqq P_n$ where $P_i = Q_i \cap R$. Therefore, $\dim R \geqslant \dim T$.

Conversely, if $P_0 \subsetneqq P_1 \subsetneqq \ldots \subsetneqq P_n$ is a chain of primes in R, then the Lying Over Theorem (Theorem 4.20) gives a prime Q_0 lying over P_0, and the Going Up Theorem (Theorem 4.21) gives a chain $Q_0 \subsetneqq Q_1 \subsetneqq \ldots \subsetneqq Q_n$ with $Q_i \cap R = P_i$. Note that we must have strict containment here, because the Q_i lay over the P_i and the P_i have strict inclusion. Therefore, $\dim R \leqslant \dim T$. □

This tells us that dimension is stable under integral extension. There is a similar corollary for the Going down theorem that says that heights of prime ideals are the same under the restriction map $\operatorname{Spec} T \to \operatorname{Spec} R$.

Corollary 4.24 (Corollary to Going Down (Theorem 4.22))**.** Let $R \subseteq T$ be integral domains with R integrally closed, T integral over R. Let Q be a prime of T. Then $\operatorname{ht}(Q \cap R) = \operatorname{ht}(Q)$.

Proof. Again we can apply Incomparability (Theorem 4.19) to see that, given a chain $Q_0 \subsetneqq Q_1 \subsetneqq \ldots \subsetneqq Q_n = Q$, this restricts to a strict chain $P_0 \subsetneqq P_1 \subsetneqq \ldots \subsetneqq P_n = Q \cap R$. Therefore, $\operatorname{ht}(Q \cap R) \geqslant \operatorname{ht}(Q)$.

Conversely, if $P_0 \subsetneqq P_1 \subsetneqq \ldots \subsetneqq P_n = Q \cap R$, then the Going Down Theorem (Corollary 4.23) allows us to extend the chain $Q_n = Q$ to a chain $Q_0 \subsetneqq Q_1 \subsetneqq \ldots \subsetneqq Q_n = Q$ with $Q_i \cap R = P_i$. Therefore, $\operatorname{ht}(Q \cap P) \leqslant \operatorname{ht}(Q)$. □

Now we can prove the theorems.

Proof of Theorem 4.21. By induction.

It's enough to consider the case $m = 1$, $n = 2$. Write $\overline{R} = R/P_1$ and $\overline{T} = T/Q_1$. Then because Q_1 lays over P_1, then $\overline{R} \hookrightarrow \overline{T}$ with $\overline{T}$ integral over $\overline{R}$ by Lemma 4.16(i).

Now by Lying Over (Theorem 4.20), there is a prime $\overline{Q}_2$ of $\overline{T}$ such that $\overline{Q}_2 \cap \overline{R} = \overline{P}_2$, where $\overline{P}_2$ is the image of P_2 in $\overline{R}$.

Lifting back gives a prime ideal $Q_2 \geqslant Q_1$ with $Q_2 \cap R = P_2$. □

That wasn't so hard. Going down is harder than going up, like with many things in life. Proving Going Down requires some additional hypotheses, lemmas, some extension of terminology, and some field theory (Galois Theory).

Definition 4.25. If I is an ideal of R, with $R \subseteq T$, then $x \in T$ is **integral over** I if x satisfies a monic equation

$$x^n + r_{n-1}x^{n-1} + \ldots + r_0 = 0 \tag{5}$$

with $r_i \in I$. The **integral closure of** I **in** T is the set of all such x.

Lemma 4.26. Let $R \subseteq T$ be rings with T integral over R. Let I be an ideal of R. Then the integral closure of I in T is the radical $\sqrt{TI}$, where TI is an ideal of T, and is thus closed under addition and multiplication. In particular, if $R = T$, we get the integral closure of I in R is just $\sqrt{I}$.

Proof. If x is integral over I, then it satisfies a monic equation of the form (5). By this, we see that $x^n \in TI$ by moving x^n to the other side. Therefore, $x \in \sqrt{TI}$.

Conversely, if $x \in \sqrt{TI}$, then $x^n \in TI$. Therefore,

$$x^n = \sum_{i=1}^{\ell} t_i r_i$$

for some $r_i \in I$, $t_i \in T$. But each t_i is integral over R and so by Lemma 4.9 we have that $M = R[t_1, \ldots, t_\ell]$ is a finitely generated R-module. Furthermore, $x^n M \subseteq IM$. Now apply Lemma 2.26, but the details are spelled out below.

We said that M was a finitely generated R-module, so let's give ourselves a generating set. Let $y_1, \ldots, y_s$ generate M as an R-module. Then multiplying by x^n,

$$x^n y_j = \sum_{k=1}^{s} r_{jk} y_k$$

with $r_{jk} \in I$. As in Lemma 4.8, we get

$$\sum_k (x^n \delta_{jk} - r_{jk}) y_k = 0.$$

Let $A_{jk} = x^n \delta_{jk} - r_{jk}$ and let A be the matrix $A = \left(A_{jk}\right)_{j,k=1}^{s}$. We deduce that x^n satisfies a monic equation

$$(x^n)^s + r'_{s-1}(x^n)^{s-1} + \ldots + r'_0 = 0,$$

namely the equation $\det A = 0$. Note that all but the top coefficient is in I. Thus, x is integral over I. □

Lemma 4.27. Let $R \subseteq T$ with T integral over R with R, T integral domains. (Note that it's enough to assume T is an integral domain, because if T is an integral domain then so is R). Let R be integrally closed. Let $x \in T$ be integral over an ideal I of R.

Then x is algebraic over the field of fractions K of R and its minimal polynomial over K

$$X^n + r_{n-1}X^{n-1} + \ldots + r_0 \tag{6}$$

has its coefficients $r_{n-1}, \ldots, r_0 \in \sqrt{I}$.

Proof. Certainly x is algebraic over K, because it satisfies a monic polynomial with coefficients in $R \subseteq K$. Now claim that the coefficients r_i in (6) are integral over I.

To see this claim, take an extension field L of K containing all the conjugates $x_1, \ldots, x_s$ of x, e.g. a splitting field of the minimal polynomial of x over K.

There is a K-automorphism of L sending x to x_i for each i. And so if

$$x^m + a_{m-1}x^{m-1} + \ldots + a_0 = 0$$

with $a_i \in I$, then x_i satisfies the same equation,

$$x_i^m + a_{m-1}x_i^{m-1} + \ldots + a_0 = 0.$$

So each conjugate x_i of x is integral over I, and in particular lies in the integral closure T_1 of R in L. However, the coefficients in (6) are obtained by taking sums and products of roots, that is, sums and products of the x_i.

By Lemma 4.26, such sums and products are also integral over I, which establishes that the coefficients r_i in (6) are integral over I. Note also that $r_i \in K$. Now by Lemma 4.26 (with $T = R$), $r_i \in \sqrt{I}$ since they lie in the integral closure of I in R. ☐

Remark 4.28. I've got soggy toes.

Now we've set the groundwork for proving the Going Down Theorem Theorem 4.22. Instead of talking about being integral over rings, we were talking about being integral over ideals. We established two lemmas that we'll need for the proof. Now we can prove Theorem 4.22.

Proof of Going Down (Theorem 4.22). By induction it's enough to consider the case $m = 1$ and $n = 2$. We're given $P_1 \gneqq P_2$ and Q_1 with $Q_1 \cap R = P_1$. We want to construct Q_2 with $Q_2 \cap R = P_2$ and so $Q_1 \gneqq Q_2$. Let $S_2 = R \backslash P_2$ and let $S_1 = T \backslash Q_1$. Let $S = S_1 S_2 = \{rt \mid r \in S_1, t \in S_2\}$. Note that S is both multiplicatively closed and contains both S_1, S_2.

We'll show that $TP_2 \cap S = \varnothing$. Assuming this, then TP_2 is an ideal of T and $S^{-1}(TP_2)$ is an ideal of $S^{-1}T$. It is proper since $TP_2 \cap S = \varnothing$ (our assumption). So $S^{-1}(TP_2)$ lies in a maximal ideal of $S^{-1}T$, which is necessarily of the form $S^{-1}Q_2$ for some prime ideal Q_2 of T with $Q_2 \cap S = \varnothing$. Notice also that $TP_2 \leqslant Q_2$

since $S^{-1}(TP_2) \leqslant S^{-1}Q_2$. Hence, $P_2 \leqslant TP_2 \cap R \leqslant Q_2 \cap R$. Since $Q_2 \cap S = \varnothing$ and $S_2 = R \backslash P_2 \subseteq S$ we have that $P_2 = Q_2 \cap R$.

Similarly, $S_1 = T \backslash Q_1 \subseteq S$, and so $Q_2 \leqslant Q_1$, as desired. We're finished modulo the assumption that $TP_2 \cap S = \varnothing$.

Let's prove this claim by contradiction. Take $x \in TP_2 \cap S$. By Lemma 4.26, x is in the integral closure of P_2 in T (using Lemma 4.26 with $I = P_2$). So by Lemma 4.27, x is algebraic over the fraction field K of R, and the minimal polynomial of x is

$$X^s + r_{s-1}X^{s-1} + \ldots + r_0$$

with $r_{s-1}, \ldots, r_0 \in \sqrt{P_2} = P_2$. But $x \in S$ and so is of the form rt with $r \in S_2$ and $t \in S_1$. So $t = {}^{x}/_{r}$ has minimal polynomial over K given by

$$X^n + \frac{r_{s-1}}{r} X^{s-1} + \ldots + \frac{r_0}{r^s}$$

with ${}^{r_i}/_{r^{s-i}} \in R$ (using Lemma 4.27 with $I = R$) since $t \in T$ is integral over R. Write these coefficients as $r_i' = {}^{r_i}/_{r^{s-i}}$. But $r_i \in P_2$, $r \notin P_2$, and ${}^{r_i}/_{r^{s-i}} = r_i' \in R \implies r_i = r_i' r^{s-i}$. Therefore, conclude that $r_i' \in P_2$ for all i. Thus, t is integral over P_2. Then by Lemma 4.26, $t \in \sqrt{TP_2}$. This is a contradiction since $t \in S_1 = T \backslash Q_1$ and $TP_2 \leqslant Q_1$ (and hence $\sqrt{TP_2} \leqslant Q_1$ because Q_1 is prime). □

The whole point of Going Up and Going Down is to show things about dimension in the case of finite-dimensional k-algebras. Noether's normalization lemma is the key result for finitely-generated k-algebras that allows us to make use of our knowledge of the behavior of restriction maps $\operatorname{Spec} T \to \operatorname{Spec} R$ where T is integral over R.

Theorem 4.29 (Noether's Normalization Lemma)**.** Let T be a finitely generated k-algebra. Then T is integral over some subring $R = k[x_1, \ldots, x_r]$ with $x_1, \ldots, x_r$ algebraically independent.

Definition 4.30. $x_1, \ldots, x_n$ are **algebraically independent** if the evaluation map $k[X_1, \ldots, X_n] \to k[x_1, \ldots, x_n]$ is an isomorphism. If things are not algebraically independent, they are **algebraically dependent**.

By this definition, we may regard $R = k[x_1, \ldots, x_n]$ in Theorem 4.29 as a polynomial subalgebra of T with T integral over R.

Proof of Theorem 4.29. Let $T = k[a_1, \ldots, a_n]$ because T is finitely generated. Proof by induction on the number n of generators.

If a_i is algebraic over k for all i, then T is a finite dimensional k-vector space and we can set $R = k$. Also note that if $a_1, \ldots, a_n$ are algebraically independent, we set $R = T$ and T is integral over itself T as a polynomial algebra.

Renumbering the a_i if necessary, assume that $a_1, \ldots, a_r$ are algebraically independent over k and $a_{r+1}, \ldots, a_n$ are algebraically dependent over $k[a_1, \ldots, a_r]$. Take a nonzero $f \in k[X_1, \ldots, X_r, X_n]$ with $f(a_1, \ldots, a_r, a_n) = 0$. Thus the polynomial $f(X_1, \ldots, X_r, X_n)$ is a sum of terms

$$f(X_1, \ldots, X_r, X_n) = \sum_{\vec{\ell} = (\ell_1, \ldots, \ell_r, \ell_n)} \lambda_{\vec{\ell}} X_1^{\ell_1} \cdots X_r^{\ell_r} X_n^{\ell_n}$$

Claim 4.31. There are positive integers $m_1, \dots, m_r$ such that $\phi\colon \vec{\ell} \mapsto m_1\ell_1 + \dots + m_r\ell_r + \ell_n$ is one-to-one for those $\vec{\ell}$ with $\lambda_{\vec{\ell}} \neq 0$.

Proof of Claim 4.31. There are finitely many possibilities for differences $\vec{d} = \vec{\ell} - \vec{\ell}'$ with $\lambda_{\vec{\ell}} \neq 0 \neq \lambda_{\vec{\ell}'}$. Write $\vec{d} = (d_1, \dots, d_r, d_n)$ and consider the finitely many non-zero $(d_1, \dots, d_r) \in \mathbb{Z}^r$ obtained. Vectors in $\mathbb{Q}^r$ orthogonal to one of these lie in finitely many $(r-1)$-dimensional subspaces.

Pick $(q_1, \dots, q_r)$ with each $q_i > 0$ such that $\sum_i q_i d_i \neq 0$ for all of the finitely many non-zero $(d_1, \dots, d_r)$. Multiply $(q_1, \dots, q_r)$ by a suitable positive integer N to clear denominators and get an r-tuple of integers $(m_1, \dots, m_r) \in \mathbb{Z}^r$. We may choose N so large that

$$\left| \sum_i m_i d_i \right| > d_n$$

for all of the finitely many $\vec{d}$ with $(d_1, \dots, d_r) \neq 0$. Thus if $\phi(\vec{\ell}) = \phi(\vec{\ell}')$, then $d_1 = \dots = d_r = 0$. Deduce that $\ell_n = \ell_n'$ and $\vec{\ell} = \vec{\ell}'$. This concludes the proof of the claim. □

Now put $g(X_1, \dots, X_r, X_n) = f(X_1 + X_n^{m_1}, \dots, X_r + X_n^{m_n}, X_n)$ where m_i are as in the claim. This is a sum

$$g(X_1, \dots, X_r, X_n) = \sum_{\vec{\ell} \text{ s.t. } \lambda_{\vec{\ell}} \neq 0} \lambda_{\vec{\ell}} (X_1 + X_n^{m_1})^{\ell_1} \cdots (X_r + X_n^{m_n})^{\ell_r} X_n^{\ell_n}$$

By Claim 4.31, different terms in this sum have different powers of X_n because the map $\phi\colon \vec{\ell} \mapsto m_1\ell_1 + \dots + m_r\ell_r + \ell_n$ is injective: for $\ell \neq \ell'$, the power of X_n in the term corresponding to ℓ must be different than the power of X_n in the term corresponding to ℓ'. Moreover, the degree of X_n in any term is higher than the degree of any X_i for $1 \leqslant i \leqslant r$. Hence, there will be a single term with highest power in X_n. As a polynomial in X_n, the leading coefficient is therefore $\lambda_{\vec{\ell}} \neq 0$, and is therefore in k.

If we put $b_i = a_i - a_n^{m_i}$ for $1 \leqslant i \leqslant r$ and $h(X_n) = g(b_1, \dots, b_r, X_n)$, this has a leading coefficient in k and all its coefficients in $k[b_1, \dots, b_r]$. Moreover, $h(a_n) = g(b_1, \dots, b_r, a_n) = f(a_1, \dots, a_r, a_n) = 0$. Dividing through by the leading coefficient shows that a_n is integral over $k[b_1, \dots, b_r]$. So for each i, $1 \leqslant i \leqslant r$, $a_i = b_i + a_n^{m_i}$ is also integral over $k[b_1, \dots, b_r]$. Hence, we have that T is integral over $k[b_1, \dots, b_r, a_{r+1}, \dots, a_{n-1}]$.

Apply the inductive hypothesis as we have a smaller number of generators. □

The proof of Noether's Normalization Lemma is quite complicated so it's worthwhile to review. The idea is to inductively remove the generators that are not algebraically independent over the rest by replacing the algebraically independent generators by other ones. The geometric lemma we used was mostly in service of this idea.

Another idea related to algebraic independence is transcendence degree of a field extension. In Definition 4.30 we defined algebraic independence over k.

As in linear algebra, where we deal with linear independence and define the dimension of a vector space as a maximal linear independent set , we have the analogous theory for algebraic independence considering maximal algebraically independent subsets. Here, there is also an exchange lemma which enables us to prove that all such maximal algebraically independent subsets of L have the same size. Such a set is called a **transcendence basis** of L over k. This cardinality is called the **transcendence degree** of L over k, denoted $\operatorname{trdeg}_k L$. (For a reference, see Stewart Galois Theory pp 151-153).

Theorem 4.32. Let T be a finitely generated k-algebra that is an integral domain with fraction field L. Then $\dim T = \operatorname{trdeg}_k L$.

Proof. Let T be a finitely generated k-algebra that is an integral domain with fraction field L. Apply Noether's normalization lemma (Theorem 4.29) to get $x_1, \dots, x_r$ algebraically independent (so $k[x_1, \dots, x_r]$ is a polynomial algebra) and T is integral over $k[x_1, \dots, x_r]$. By Going Up (Corollary 4.23), $\dim T = \dim k[x_1, \dots, x_r]$. Therefore, any finitely generated k-algebra T has dimension equal to the dimension of a polynomial algebra. Moreover, since T is an integral extension of $k[x_1, \dots, x_r]$, L is algebraic over $k(x_1, \dots, x_r)$. Hence, $\operatorname{trdeg}_k L = \operatorname{trdeg}_k k(x_1, \dots, x_r)$. If this T k-algebra is an integral domain, then the fraction field L of T exists and $\dim T$ is the dimension of a polynomial algebra with r variables, with $r = \operatorname{trdeg}_k L$.

It remains to prove that $\dim k[x_1, \dots x_r] = r = \operatorname{trdeg}_k L$. In Example 4.5 we saw we could produce a chain of primes of length r, and so $\dim k[x_1, \dots, x_r] \geqslant r$.

We prove the other inequality by induction. If $r = 0$, this is trivial.

If $r > 0$, consider a chain of primes $P_0 \subsetneqq P_1 \subsetneqq \dots \subsetneqq P_s$. Since we are working in the integral domain $k[x_1, \dots, x_r]$, we may as well assume $P_0 = 0$ (otherwise add it to the bottom). And since $k[x_1, \dots, x_n]$ is a UFD, then $P_1 \geqslant \langle f \rangle$ with f irreducible (P_1 contains a principal prime ideal; see Lemma 4.6). So we may as well assume that $P_1 = \langle f \rangle$. Let L_1 be the fraction field of $k[x_1, \dots, x_r]/\langle f \rangle$. Without too much thought, we can see that $\operatorname{trdeg}_k L_1 = r - 1$. By Noether normalization (Theorem 4.29), we see that

$$\dim {}^{k[x_1, \dots, x_r]}\!\big/_{\langle f \rangle} = \dim k[Y_1, \dots, Y_t].$$

for some polynomial algebra $k[Y_1, \dots, Y_t]$. Then

$$\operatorname{trdeg}_k k(Y_1, \dots, Y_t) = \operatorname{trdeg}_k L_1 = r - 1$$

so $t = r - 1$. Now by induction, $\dim k[Y_1, \dots, Y_{r-1}] = r - 1$. But $P_1 = \langle f \rangle$, so we can find a strict chain

$${}^{P_1}\!\big/_{P_1} \subsetneqq {}^{P_2}\!\big/_{P_1} \subsetneqq \dots \subsetneqq {}^{P_s}\!\big/_{P_1}$$

of length $s - 1$ in $k[Y_1, \dots, Y_{r-1}]$. Therefore, $s - 1 \leqslant r - 1$, so $s \leqslant r$. Hence, $\dim k[x_1, \dots, x_r] \leqslant r$.

But we already saw that $\dim k[x_1, \dots, x_r] \geqslant r$, so $\dim k[x_1, \dots, x_r] = r$. $\square$

Theorem 4.33. Let R be a Noetherian integrally closed integral domain, let K be the fraction field of R, and let L be a finite separable extension of K. Then if T is the integral closure of R in L, T is a finitely generated R-module.

Note that the separability assumption holds always in characteristic zero. The motivation for this theorem comes from algebraic geometry. We want to get a finite fiber of the following map.

$$\operatorname{Spec} T \xrightarrow{\text{restriction}} \operatorname{Spec} k[x_1, \ldots, x_r]$$

This theorem also has several interesting corollaries, the first of which is exactly the algebraic geometry thing above.

Corollary 4.34. Let S be a finitely generated k-algebra that is an integral domain integral over a polynomial algebra $R = k[x_1, \ldots, x_r]$. Let L be the fraction field of S. We deduce that the integral closure T of R in L is a finitely generated R-module. Thus, T is a finitely generated k-algebra.

Theorem 4.33 is also useful in number theory.

Corollary 4.35. Let $R = \mathbb{Z}$. Then the integral closure of $\mathbb{Z}$ in a finite degree extension of $\mathbb{Q}$ is a finitely generated $\mathbb{Z}$-module.

Definition 4.36. The proof of Theorem 4.33 uses **trace functions**

$$\operatorname{Tr}_{L/K}(x) := -c|L\colon K(x)|,$$

where c is the coefficient of the second highest term in the minimal polynomial for some x over K. Equivalently, if L is Galois over K with Galois group G, then

$$\operatorname{Tr}_{L/K}(x) = \sum_{g \in G} g(x)$$

Remark 4.37. This is a sum of conjugates of x but they may be repeated, and therefore have a multiple of a coefficient of the minimal polynomial.

Fact 4.38. We can define a bilinear form $L \times L \to K$ given by $(x, y) \mapsto \operatorname{Tr}_{L/K}(xy)$. If L is separable, then it is a non-degenerate symmetric K-bilinear form. (See Reid 8.13).

Proof of Theorem 4.33. Pick a basis $y_1, \ldots, y_n$ of L over K. If the minimal polynomial of y_i is

$$X^m + {}^{r_{m-1}}\!/\!_{s_{m-1}} X^{m-1} + \ldots + {}^{r_0}\!/\!_{s_0},$$

with ${}^{r_j}\!/\!_{s_j} \in K$, then the minimal polynomial of $y_i\,(\prod_i s_i)$ has coefficients in R. So by multiplying by suitable elements of K, we may assume $y_i \in T$ for all i.

Since $\operatorname{Tr}(xy)$ yields a non-degenerate symmetric bilinear form (from our separability assumption on L), then there is a basis $x_1, \ldots, x_n$ for L over K so that $\operatorname{Tr}(x_i y_j) = \delta_{ij}$. We'll show that $T \subseteq \sum_i R x_i$.

Let $z \in T$. Then $z = \sum_i \lambda_i x_i$ with $\lambda_i \in K$. So

$$\mathrm{Tr}(zy_j) = \mathrm{Tr}\left(\sum_i \lambda_i x_i y_j\right) = \sum_i \lambda_i \mathrm{Tr}(x_i y_j) = \sum_i \lambda_i \delta_{ij} = \lambda_j$$

But z and y_j are in T and hence $zy_j \in T$.

By Lemma 4.27 with $I = R$ (using R integrally closed) the coefficients of the minimal polynomial of zy_j lie in R, and so $\mathrm{Tr}(zy_j) \in R$. Hence, $\lambda_j = \mathrm{Tr}(zy_j) \in R$ for each j.

Then a general element z of T as a linear combination of things with coefficients in R. By the Hilbert Basis Theorem, $R[x_1, \ldots, x_n]$ is Noetherian since R is Noetherian. T is a submodule of $R[x_1, \ldots, x_n]$, and therefore a finitely generated R-module. □

5 Heights

This chapter concerns itself with Krull's Principal Ideal Theorem and it's generalization, which allows us to say that in any Noetherian ring, every prime ideal has finite height. A consequence of this is that any Noetherian local ring has finite dimension.

Theorem 5.1 (Catenary Property)**.** Let Q be a prime ideal of a finitely generated k-algebra T which is an integral domain, with $\dim T = n$. Then

$$\mathrm{ht}(Q) + \dim\left({}^{T}\!/_{Q}\right) = n.$$

Proof. By induction on n. In the case that $n = 0$, we have an artinian ring and $\mathrm{ht}(Q) = 0$ and T/Q is a field with dimension zero.

Now assume $n > 0$. Let $m = \mathrm{ht}(Q)$ and pick a chain of prime ideals in T,

$$0 = Q_0 \subsetneqq Q_1 \subsetneqq \ldots \subsetneqq Q_m = Q.$$

By Noether normalization (Theorem 4.29), there is a subring R of T with T integral over R, and R is a polynomial algebra. Now by Corollary 4.23, dimension is preserved under integral extension, so $\dim T = \dim R$. Moreover, by Theorem 4.32, $n = \dim T = \dim R = \mathrm{trdeg}_k L$ where L is the fraction field of R. This is also equal to the number of variables in the polynomial algebra R.

Write $P_i = Q_i \cap R$. Observe that $\mathrm{ht}(Q_1) = 1$, as otherwise we could find a longer chain and the height of Q would be greater than m.

Note that R is integrally closed being a polynomial algebra. Therefore by Corollary 4.24, $\mathrm{ht}(P_1) = 1$. So $P_1 = \langle f \rangle$ as a height 1 prime in a polynomial algebra (which is a UFD), where f is irreducible.

Now we can cope with transcendence degrees for polynomial algebras, so

$$\mathrm{trdeg}_k\left(\text{frac.field of } \left({}^{R}\!/_{P_1}\right)\right) = \mathrm{trdeg}_k\left(\text{frac. field of } \left({}^{R}\!/_{\langle f \rangle}\right)\right) = n - 1.$$

Hence, $\dim\left({}^{R}/_{P_1}\right) = n-1$ by Theorem 4.32.

Now we want to apply induction to the prime Q/Q_1 of T/Q_1. Here's all that we know:

(a) $\operatorname{ht}(Q/Q_1) = m-1$

(b) $\dim\left({}^{T}/_{Q_1}\right) = \dim\left({}^{R}/_{P_1}\right) = n-1$, since R/P_1 embeds in T/Q_1 and T/Q_1 is integral over it.

(c) $\dim\left(\frac{{}^{T}/_{Q_1}}{{}^{Q}/_{Q_1}}\right) = \dim\left({}^{T}/_{Q}\right)$

So induction gives that $(m-1) + \dim\left({}^{T}/_{Q}\right) = n-1$ and hence

$$\operatorname{ht} Q + \dim\left({}^{T}/_{Q}\right) = n \qquad \square$$

Theorem 5.2 (Krull's Principal Ideal Theorem)**.** Let R be a Noetherian ring and let $a \in R$ a nonunit. Let P be a minimal prime over $\langle a\rangle$. Then $\operatorname{ht}(P) \leqslant 1$.

This provides the start of an induction argument that proves the following theorem.

Theorem 5.3 (Generalized Principal Ideal Theorem)**.** Let R be a Noetherian ring and let I be a proper ideal. We know that I is finitely generated, so say I is generated by n-elements. Then $\operatorname{ht}(P) \leqslant n$ for each minimal prime P over I.

Proof of Krull's Principal Ideal Theorem (Theorem 5.2). Let P be a minimal prime over $\langle a\rangle$, where $a \in R$ is not a unit and R is a Noetherian ring. First localize at P to get R_P, which has unique maximal ideal $P_P = S^{-1}P$ where $S = R\backslash P$.

Observe that $S^{-1}P$ is a minimal prime over $S^{-1}\langle a\rangle$. This follows from the correspondence between prime ideals of R_P and primes in R disjoint from S (Lemma 3.10). So we may assume R is local with P the unique maximal ideal.

Now we've reduced to the case where R is local and P is the unique maximal ideal. (We will also want to localize again, and for ease of notation, that will again use S.)

Suppose $\operatorname{ht}(P) > 1$ and there is a chain of primes $Q' \subsetneqq Q \subsetneqq P$. Consider $R/\langle a\rangle$. This is a Noetherian ring with a unique prime ideal $P/\langle a\rangle$, so it is Artinian.

Now consider $I_m = \{r \in R \mid r/1 \in S^{-1}Q^m\}$ where $S = R\backslash Q$. Clearly $Q = I_1$ by Lemma 3.10, but we don't know much more.

$$Q = I_1 \geqslant I_1 \geqslant I_2 \geqslant \dots \tag{7}$$

We also know that $I_m \geqslant Q^m$, but we don't have equality because the correspondence in Lemma 3.10 is only for *prime* ideals.

From (7), we get a chain

$$I_1 + {}^{\langle a\rangle}/_{\langle a\rangle} \geqslant I_2 + {}^{\langle a\rangle}/_{\langle a\rangle} \geqslant \dots$$

is a descending chain of ideals in $R/\langle a \rangle$, which is Artinian. So $I_m + \langle a \rangle = I_{m+1} + \langle a \rangle$ for some m. Next we show that the chain (7) terminates.

Let $r \in I_m$. Then $r = t + xa$ for some $t \in I_{m+1}$ and some $x \in R$. So $xa = r - t \in I_m$. But $a \notin Q$ as P is a minimal prime over $\langle a \rangle$, and $Q = I_1 \geqslant I_m \geqslant Q^m$, so $a \notin I_m$. Also, localizing (7) gives a chain in $S^{-1}R$,

$$S^{-1}R \geqslant S^{-1}Q \geqslant S^{-1}Q^2 \geqslant \ldots \geqslant S^{-1}Q^m.$$

If $x/1 \notin S^{-1}Q^m$, then $xa/1 \notin S^{-1}Q^m$. This is a contradiction. So $x \in I_m$ and hence $I_m = I_{m+1} + I_m a$. So we can look at the quotient $I_m/I_{m+1} = P\left(I_m/I_{m+1}\right)$ since $\langle a \rangle \leqslant P$.

Note $P = \mathrm{Jac}(R)$ because R is local with maximal ideal P. Looks like a job for Nakayama! We conclude that $I_m/I_{m+1} = 0$, and therefore $I_m = I_{m+1}$.

We're on the finishing straight now. Note

$$(S^{-1}Q)^m = S^{-1}Q^m = S^{-1}I_m;$$

the last equality comes from Lemma 3.10. Moreover,

$$(S^{-1}Q)^{m+1} = S^{-1}Q^{m+1} = S^{-1}I_{m+1}.$$

So $(S^{-1}Q)^m = (S^{-1}Q)^{m+1}$. Nakayama for the maximal ideal $S^{-1}Q$ of $R_Q = S^{-1}R$ gives that $(S^{-1}Q)^m = 0$ in R_Q.

From the correspondence of prime ideals Lemma 3.10, we see that $0 = (S^{-1}Q)^m \leqslant S^{-1}Q'$, but $S^{-1}Q'$ is prime, so it must contain $S^{-1}Q$ (if a prime contains a product of ideals, it must contain one of the ideals). But we saw that $S^{-1}Q'$ is strictly contained in $S^{-1}Q$, which is a contradiction.

So it must be that $\mathrm{ht}(P) \leqslant 1$. □

We can now use this to prove the General Principal Ideal Theorem (Theorem 5.3).

Proof of the General Principal Ideal Theorem (Theorem 5.3). Let R be Noetherian, and I a proper ideal generated by n elements. We want to show that $\mathrm{ht}\, P \leqslant n$ for each minimal prime P over I.

Proof by induction on n. For $n = 1$, this is Krull's Principal Ideal Theorem (Theorem 5.2).

Now assume $n > 1$. We may assume by passing to R_P that R is local with maximal ideal P. Pick any prime Q maximal subject to $Q \lneqq P$, and thus P is the only prime strictly containing Q.

We'll show that $\mathrm{ht}(Q) \leqslant n - 1$. It's enough to do this for all such Q, and thereby we can deduce that $\mathrm{ht}(P) \leqslant n$. Since P is minimal over I, $Q \not\geqslant I$.

By assumption there are generators $a_1, \ldots, a_n$ for I. Re-numbering if necessary, we may assume that $a_n \notin Q$. P is the only prime containing $Q + \langle a_n \rangle$, so $\mathrm{Nil}\left(R/Q+\langle a_n \rangle\right) = P/Q+\langle a_n \rangle$. The nilradical of a Noetherian ring is nilpotent, and so there is m such that $a_i^m \in Q + \langle a_n \rangle$, and this m works for all i, $1 \leqslant i \leqslant n-1$. In particular, this means that $a_i^m = x_i + r_i a_n$ for some $x_i \in Q$, $r_i \in R$.

Any prime of R containing $x_1, \ldots, x_{n-1}$ and a_n must also contain $a_1, \ldots, a_n$. Note also that $\langle x_1, \ldots, x_{n-1} \rangle \subseteq Q$ since $x_i \in Q$.

Now we claim that Q is a minimal prime over $\langle x_1, \ldots, x_{n-1} \rangle$. To see this, write $\overline{R} = {}^{R}\!/\!_{\langle x_1, \ldots, x_{n-1} \rangle}$, and write bars for the images of things in R. The unique maximal ideal $\overline{P}$ of $\overline{R}$ is a minimal prime over $\overline{\langle a_n \rangle}$. Apply Krull's Principal Ideal Theorem to get $\operatorname{ht}\left(\overline{P}\right) \leqslant 1$, and therefore $\operatorname{ht}\left(\overline{Q}\right) = 0$.

So Q is a minimal prime over an ideal $\langle x_1, \ldots, x_{n-1} \rangle$ with $n-1$ generators, so $\operatorname{ht}(Q) \leqslant n - 1$ by induction. Therefore, $\operatorname{ht}(P) \leqslant n$ since Q was maximal among primes strictly contained in P. □

The hard part of this induction was really the base case. Now that we have this theorem, we have some important corollaries

Corollary 5.4 (Corollary of Theorem 5.3)**.**

(a) Each prime ideal of a Noetherian ring has finite height;

(b) Every Noetherian local ring R has finite dimension, which is at most the minimum number of generators of the maximal ideal P.

(c) Moreover, if R is a Noetherian local ring with maximal ideal P, then the minimum number of generators of P is equal to $\dim_{R/P}\left({}^{P}\!/\!_{P^2}\right)$, where this is a vector space dimension.

Proof.

(a) Any ideal of a Noetherian ring is finitely generated. A prime P is minimal over itself. From Theorem 5.3, we get that $\operatorname{ht}(P)$ is bounded above by the minimum number of generators of P. In particular, this is finite.

(b) For a local ring, $\dim R = \operatorname{ht}(P)$, where P is the maximal ideal. By (a), $\dim(R) = \operatorname{ht}(P)$ is bounded above by the minimum number of generators of P.

(c) This is an application of Nakayama's Lemma. It suffices to show that

Claim: P is generated by $x_1, \ldots, x_s$ if and only if ${}^{P}\!/\!_{P^2}$ is generated by $\overline{x}_1, \ldots, \overline{x}_s$, where $\overline{x}_i = x_i + P^2$.

Proof of Claim. ($\Rightarrow$). In the fashion of Atiyah-Macdonald, we'll just draw a checkmark.

($\Leftarrow$). Suppose $\overline{x}_1, \ldots, \overline{x}_s$ generate ${}^{P}\!/\!_{P^2}$ with $x \in P$. Consider the ideal $I = \langle x_1, \ldots, x_s \rangle \leqslant P$. Clearly $I + P^2 = P$ and so $P\left({}^{P}\!/\!_{I}\right) = {}^{P}\!/\!_{I}$. Nakayama then implies that ${}^{P}\!/\!_{I} = 0$, so $P = I$. □

This concludes the proof of Corollary 5.4. □

Definition 5.5. A **regular local ring** is a ring R in which $\dim R = \dim_{R/P}\left({}^{P}\!/\!_{P^2}\right)$, where P is the unique maximal ideal.

Remark 5.6. Regular local rings are necessarily integral domains. You'll prove this on examples sheet 3.

Remark 5.7. If we consider as in the next section the P-adic filtrations of a local ring R and form it's associated graded ring $\mathrm{gr}(R)$, R is regular if and only if $\mathrm{gr}(R)$ is a polynomial algebra in $\dim(R)$-many variables. In particular, $\mathrm{gr}(R)$ is an integral domain implies that R is an integral domain.

In geometry, regular local rings correspond to localizations at *non-singular* points, and P/P^2 is the cotangent space at this point.

Remark 5.8. Our proof of Theorem 5.3 actually gives a slightly stronger result. We can say in fact that $\mathrm{ht}(P)$ is bounded above by the minimum number of generators of any ideal I for which $\sqrt{I} = P$.

In the case of a local ring, we see that $\dim(R)$ is at most the minimum number of generators for any ideal I for which $\sqrt{I} = P$.

In fact, although we won't prove it, we have that $\dim R$ is the minimum over all I for which $\sqrt{I} = P$ of the minimum number of generators for I.

6 Filtrations and Graded Rings

This section ties in to the last section, about dimension, through the Hilbert polynomial and Hilbert series, which gives another definition of dimension.

Definition 6.1. A $(\mathbb{Z})$-**filtered ring** R **is** one whose additive group is filtered by

$$\ldots \leqslant R_{-1} \leqslant R_0 \leqslant R_1 \leqslant \ldots$$

by subgroups R_i of the additive group of R with $\begin{cases} R_iR_j \leqslant R_{i+j} & \text{for } i,j \in \mathbb{Z} \\ 1 \in R_0 \end{cases}$

Notice that $\bigcup_i R_i$ is a subring; and usually we have an **exhaustive filtration**, wherein $\bigcup_i R_i = R$.

Moreover, R_0 is a subring of R, and $\bigcap_i R_i$ is an ideal of R_0; usually we have a **separated filtration** wherein $\bigcap_i R_i = 0$.

Note R_i for $i \leqslant 0$ is an ideal of R_0.

Example 6.2.

(a) The I-adic filtration where I is an ideal of R is given by $R_i = R$ for $i \geqslant 0$ and $R_{-j} = I^j$ for $j > 0$.

(b) R is the k-algebra generated by $x_1, \ldots, x_n$. Set $R_{-j} = 0$ for $j > 0$, and $R_0 = k1$, $R_1 =$ the k-subspace span of $x_1, \ldots, x_n$, and $R_i =$ the k-subspace span of polynomials in $x_1, \ldots, x_n$ of total degree $\leqslant i$.

Such examples are also important in a non-commuative context. For example, Iwasawa algebras, which are completed group algebras of p-adic Lie groups. This is interesting in representation theory. Sometimes, starting with these non-commutative group algebras and then taking the associated graded ring to a

P-adic filtration might give a commutative ring, whose study is relevant to the study of representation theory of these p-adic Lie groups.

Alternatively, the universal enveloping algebras of finite-dimensional Lie algebras have a natural filtration.

Definition 6.3. If a ring R has a filtration $\ldots R_{-1} \leqslant R_0 \leqslant R_1 \leqslant \ldots$, the **associated graded ring** to this filtration is

$$\operatorname{gr} R = \bigoplus_i {}^{R_i}\!/_{R_{i-1}}$$

as an abelian group with multiplication $(r + R_{i-1})(s + R_{j-1}) = rs + R_{i+j-1}$ for $r \in R_i$, $s \in R_j$, and extend linearly.

Remark 6.4. For notation, books often write $\sigma(r)$ for $r + R_{i-1}$ when $r \in R_i/R_{i-1}$. This is called the **symbol of** r**.**

Example 6.5. For a P-adic filtration of a local ring R with maximal ideal P,

$$\operatorname{gr} R = \bigoplus_j {}^{P^j}\!/_{P^{j+1}},$$

where P^j/P^{j+1} is the j-th component. Write $K = R/P$. Then $\operatorname{gr} R$ is generated as a K algebra by any K-vector space basis of P/P^2. When R is a regular local ring (in which case $\dim R = \dim_{R/P}(P/P^2)$), $\operatorname{gr} R$ is a polynomial algebra taking the basis of P/P^2 as the algebraically independent set of variables. (This will be proved on example sheet 3).

Definition 6.6. A $\mathbb{Z}$**-graded ring** S has a family of additive subgroups S_i such that $S = \bigoplus_i S_i$ with $S_i S_j \subseteq S_{i+j}$ for $i, j \in \mathbb{Z}$. The subgroup S_i is called the i**-th homogeneous component**. We also require that S_0 is a subring, and each S_i is an S_0-module.

A **graded ideal** $I \subseteq S$ is an ideal of the form $I = \bigoplus_i I_i$ with $I_i \subseteq S_i$.

An element $s \in S$ is **homogenous of degree** i if it lies in S_i.

Note that if a graded ideal is finitely generated as an ideal, then there is a finite generating set consisting of homogenous elements. Commutative graded rings arise in connection with projective geometry. In the non-commutative examples from last time (Iwasawa algebras and universal enveloping algebras), we can in both cases filter and may get a commutative associated graded ring.

As we talked about filtrations and graded rings, we can do the same with modules.

Definition 6.7. Let R be a filtered ring with filtration $\{R_i\}$, and let M be an R-module. Then M is a **filtered** R**-module** with filtration $\{M_j\}$ of additive groups

$$\ldots \leqslant M_{-1} \leqslant M_0 \leqslant M_1 \leqslant \ldots$$

if $R_i M_j \subseteq M_{i+j}$.

Definition 6.8. If $S = \bigoplus_i S_i$ is a graded ring, then a **graded S-module** is one of the form $V = \bigoplus V_j$ such that $S_i V_j \subseteq V_{i+j}$.

Definition 6.9. The **associated graded module** of a filtered R-module is

$$\operatorname{gr} M = \bigoplus_j {}^{M_j}\!/_{M_{j-1}}$$

as additive groups with $\operatorname{gr} R$-module structure given by $(r + R_{i-1})(m + M_{j-1}) = rm + M_{i+j-1}$ for $r \in R_i$ and $m \in M_j$. It is a graded $\operatorname{gr} R$-module.

Next we talk about submodules and quotient modules of these objects. Here you have to be an expert at isomorphism theorems.

Given a filtered R-module M with filtration $\{M_i\}$, and N a submodule of M, there are induced filtrations $\{N \cap M_i\}$ of N and $\left\{{}^{(N+M_i)}\!/_N\right\}$ of M/N.

Lemma 6.10. For $N \leqslant M$ a filtered R-module, with N and M/N having the induced filtrations, then

$$0 \longrightarrow \operatorname{gr} N \xrightarrow{\ \phi\ } \operatorname{gr} M \xrightarrow{\ \pi\ } \operatorname{gr}\left({}^{M}\!/_N\right) \longrightarrow 0$$

is a short exact sequence for canonical maps ϕ and π.

Proof. The inclusion $N \subseteq M$ allows the definition of a map

$$\phi_i \colon {}^{(N \cap M_i)}\!/_{(N \cap M_{i-1})} \longrightarrow {}^{M_i}\!/_{M_{i-1}}$$

Putting these together gives a map of additive groups $\phi\colon \operatorname{gr} N \to \operatorname{gr} M$, which is an $\operatorname{gr} R$-module homomorphism.

Now consider ${}^{(N+M_i)}\!/_N \cong {}^{M_i}\!/_{N \cap M_i}$ (this isomorphism by the second isomorphism theorem). Factors in the induced filtration ${}^{M}\!/_N$ are

$$\left({}^{(N+M_i)}\!/_N\right)\Big/\left({}^{(N+M_{i-1})}\!/_N\right) \cong {}^{M_i}\!/_{(M_{i-1} + (N \cap M_i))}$$

There is a canonical quotient map

$$\pi_i \colon {}^{M_i}\!/_{M_{i-1}} \longrightarrow \left({}^{(N+M_i)}\!/_N\right)\Big/\left({}^{(N+M_{i-1})}\!/_N\right)$$

corresponding to

$${}^{M_i}\!/_{M_{i-1}} \longrightarrow {}^{M_i}\!/_{(M_{i-1} + (N \cap M_i))}$$

Putting these together gives $\pi\colon \operatorname{gr} M \to \operatorname{gr} {}^{M}\!/_N$. Notice also that

$$\ker \pi_i = {}^{(M_{i-1} + (N \cap M_i))}\!/_{M_{i-1}} \cong {}^{(N \cap M_i)}\!/_{(N \cap M_{i-1})}$$

So

$$0 \longrightarrow {}^{N \cap M_i}\!/_{N \cap M_{i-1}} \xrightarrow{\ \phi_i\ } {}^{M_i}\!/_{M_{i-1}} \xrightarrow{\ \pi_i\ } \left({}^{(N+M_i)}\!/_N\right)\Big/\left({}^{(N+M_{i-1})}\!/_N\right) \longrightarrow 0$$

is a short exact sequence. Put these together to get the result. □

Exercise 6.11. Fill in the details in the proof of Lemma 6.10.

Definition 6.12. Let R be a filtered ring, with filtration $\{R_i\}$. Then the **Rees ring** for the filtration $\{R_i\}$ is a subring of the Laurent polynomial ring $R[T, T^{-1}]$ given by

$$\mathrm{Rees}(R) = \bigoplus_{i \in \mathbb{Z}} R_i T^i \subseteq R[T, T^{-1}]$$

There is no standard notation for the Rees ring. Sometimes people use E. It was first used by Rees to prove a lemma about I-adic filtrations.

Remark 6.13. Lemma 6.10 holds for $\operatorname{gr} M$ replaced by $\mathrm{Rees}(M)$.

Remark 6.14. The Rees ring is a subring of $R[T, T^{-1}]$ since $R_i R_j \subseteq R_{i+j}$, and moreover $\mathrm{Rees}(R)$ is graded with i-th homogeneous component $R_i T^i$. Observe also that $T \in \mathrm{Rees}(R)$ since $1 \in R_0 \subseteq R_1$, and

(a) ${}^{\mathrm{Rees}(R)}/_{\langle T \rangle} \cong \operatorname{gr} R$;

(b) If we have an exhaustive filtration, ${}^{\mathrm{Rees}(R)}/_{\langle 1-T \rangle} \cong R$ since $\langle 1 - T \rangle$ is the kernel of the map $\mathrm{Rees}(R) \to R$ defined by $\sum_i r_i t^i \mapsto \sum_i r_i$.

Example 6.15. Let R be Noetherian and consider the I-adic filtration $R_{-j} = I^j$ for $j > 0$ and $R_i = R$ for $i \geqslant 0$, for some ideal I of R.

Then I is finitely generated by $x_1, \ldots, x_n$ say, as an ideal. Then the Rees ring $\mathrm{Rees}(R) = \bigoplus_i R_i T^i$ is generated by $R_0 = R$ and $x_1 T^{-1}, \ldots, x_n T^{-1}$. It is therefore a ring image of the polynomial ring $R[Z_0, Z_1, \ldots, Z_n]$ under $Z_0 \mapsto T$ and $Z_i \mapsto x_i T^{-1}$ for $1 \leqslant i \leqslant n$ and is therefore Noetherian.

More about the Rees ring and graded rings.

Example 6.16. Suppose R is a finitely generated k-algebra which is an integral domain. Let I be an ideal and take the I-adic filtration. Then $\mathrm{Rees}(R)$ is a finitely generated k-algebra which is a subring of the Laurent polynomial algebra $R[T, T^{-1}]$, and hence $\mathrm{Rees}(R)$ is an integral domain.

The Principal Ideal Theorem says that the minimal primes over the ideals $\langle T \rangle$ and $\langle 1 - T \rangle$ in $\mathrm{Rees}(R)$ are of height 1, and the Catenary Property (Theorem 5.1) says that

$$\dim \mathrm{Rees}(R) = 1 + \dim \left({}^{\mathrm{Rees}(R)}/_{\langle T \rangle} \right) = 1 + \dim \left({}^{\mathrm{Rees}(R)}/_{\langle 1-T \rangle} \right).$$

Therefore, $\dim(R) = \dim(\operatorname{gr} R)$ in this case.

Remark 6.17. R is a "deformation" of $\operatorname{gr} R$ and as long as $\mathrm{Rees}(R)$ is well-behaved, the properties of $\operatorname{gr} R$ are inherited by R.

Definition 6.18. If M is a filtered R-module with $\{M_j\}$, $\{R_i\}$ the filtrations, then the **associated Rees module** is

$$\mathrm{Rees}(M) := \bigoplus_j T^j M_j.$$

It is a $\mathrm{Rees}(R)$-module via

$$\left(r_i T^i\right)(T^j m_j) = T^{i+j}(r_i m_j).$$

Remark 6.19. For $N \leqslant M$, and given the induced filtrations on N and $M/_N$, Lemma 6.10 implies $\text{Rees}(M/N) \cong \text{Rees}(M)/\text{Rees}(N)$.

Definition 6.20. A filtration is **good** if $\text{Rees}(M)$ is a *finitely generated* $\text{Rees}(R)$-module.

Lemma 6.21. Let $N \leqslant M$ and $\{M_j\}$ be a good filtration of M. If $\text{Rees}(R)$ is Noetherian, then the induced filtrations of N and M/N are also good.

Proof. This is a straightforward consequence of easy properties of Noetherian rings. $\text{Rees}(N)$ is a $\text{Rees}(R)$-submodule of $\text{Rees}(M)$. But $\text{Rees}(M)$ is a finitely generated R-module and hence is Noetherian. Therefore, $\text{Rees}(N)$ is finitely generated and so the induced filtration on N is good. Additionally (by Lemma 6.10) $\text{Rees}\left(M/_N\right) \cong {}^{\text{Rees}(M)}/_{\text{Rees}(N)}$ is also finitely generated and so the induced filtration on $M/_N$ is also good. ☐

Example 6.22. Apply this to the case where R is a Noetherian ring and I is an ideal of R, and the filtration is the I-adic filtration.

Let M be a finitely generated R-module. Then a filtration of M is good exactly when there is J such that M_{-j-J} is $I^j M_{-J}$ for all $j \geqslant 0$.

Such a filtration is said to be **stable**.

Lemma 6.23 (Artin, Rees 1956)**.** Let R be a Noetherian ring and let I be an ideal. Let $N \leqslant M$ be finitely generated R-modules. Then there exists k such that $N \cap I^a M = I^{a-k}(N \cap I^k M)$ for all $a \geqslant k$.

Proof. Use the I-adic filtration $M_{-j} = I^j M$. This is a good filtration. Then the induced filtration $\{N \cap M_{-j}\}$ is good by Lemma 6.21. In other words, $N \cap I^{j+J} M = I^j(N \cap I^J M)$ for some $J, j \geqslant 0$. Set $k = J$ and $a = j + J$. ☐

The original proof of this lemma is where the Rees ring comes from. Hence the name. The next lemma was proved by Krull in the 1930's, but the standard proof nowadays is to use Artin & Rees's lemma from 1956 to prove it.

Corollary 6.24 (Krull's Intersection Theorem)**.** Let R be a Noetherian ring, I an ideal contained in the Jacobson radical. Then $\bigcap_j I^j = 0$, so the I-adic filtration is separated. In particular, in a Noetherian local ring, $\bigcap_j I^j = 0$ for any proper ideal I.

Proof. Let $M = R$ and $N = \bigcap_j I^j$. So $N \cap I^k M = N$ for all k. Then Artin Rees (Lemma 6.23) says that $N = IN$. But N is a finitely generated R-module, so Nakayama's Lemma shows that $N = 0$.

For the local ring case, observe that any proper ideal $I \subseteq \text{Jac}(R)$, because the Jacobson radical is equal to the unique maximal ideal. ☐

Remark 6.25.

(1) For a finitely generated k-algebra, we know that $\text{Jac}(R) = \text{Nil}(R)$ by the Strong Nullstellensatz (Theorem 2.30). $\text{Jac}(R) = \text{Nil}(R)$ is nilpotent and so for $I \leqslant \text{Jac}(R)$, $I^n = 0$ for some n.

(2) There is a formulation of Corollary 6.24 in terms of modules rather than ideals.

(3) There is also a more general version of Corollary 6.24 in which I is not contained in the Jacobson radical. One can describe $\bigcap I^j$ for more general ideals I.

Consider now positively graded rings $S = \bigoplus_{i=0}^{\infty} S_i$ and a finitely generated graded S-module $V = \bigoplus_{i=0}^{\infty} V_i$. Suppose S is Noetherian, generated by S_0 and a finite set of homogeneous generators $x_1, \ldots x_m$ of degrees $k_1, \ldots, k_m$, respectively.

Remark 6.26. This all applies to negatively graded rings arising as associated graded rings of I-adic filtrations. After one has formed the associated graded ring, one can re-number to change the indexing so that it is positive.

Definition 6.27. Given finitely generated S_0-modules U_1, U_2, U_3 an **additive function** λ is one such that for any short exact sequence

$$0 \longrightarrow U_1 \longrightarrow U \longrightarrow U_2 \longrightarrow 0,$$

we have that $\lambda(U) = \lambda(U_1) + \lambda(U_2)$.

Example 6.28. For example, if $S_0 = k$ is a field, then we can take λ to be the dimension as a k-vector space.

Alternatively, if S_0 is local and Artinian, with maximal ideal P, then each finitely generated S_0-module U has a chain $U \geqslant U_1 \geqslant \ldots \geqslant U_t = 0$, with each factor isomorphic to S_0/P. The number of factors is called the **composition length** and can be taken for λ. This is also independent of the choice of chain (exercise).

Definition 6.29. The **Poincaré series** of $V = \bigoplus V_i$ with respect to an additive function λ is a power series contained in $\mathbb{Z}[[t]]$ defined to be the generating function for $\lambda(V_i)$.

$$P(V, t) = \sum_{i=0}^{\infty} \lambda(V_i) t^i.$$

Theorem 6.30 (Hilbert-Serre)**.** $P(V, t)$ is a rational function in t of the form

$$P(V, t) = \frac{f(t)}{\prod_{i=1}^{m}(1 - t^{k_i})} \tag{8}$$

where $f(t) \in \mathbb{Z}[t]$, and k_i is the degree of the homogenous generator x_i.

Remark 6.31. Normally I come into CMS and look at my lecture notes before the lecture, but today I couldn't find them! So I went back to college to look and couldn't find them there either. Turns out they were with me the whole time. Anyway, I got lots of exercise this morning but haven't had too much time to prepare the lecture.

Corollary 6.32 (Corollary of Theorem 6.30)**.** If each $k_1, \dots, k_m = 1$ in (8), then for large enough i, $\lambda(V_i) = \phi(i)$ for some polynomial $\phi(t) \in \mathbb{Q}[t]$, of degree $d-1$ where d is the order of the pole of $P(V,t)$ at $t=1$.

Moreover,

$$\sum_{j=0}^{i} \lambda(V_j) = \chi(i)$$

where $\chi(t) \in \mathbb{Q}[t]$ is a polynomial of degree d.

Definition 6.33. The polynomial $\phi(t)$ in Corollary 6.32 is the **Hilbert Polynomial**. The polynomial $\chi(t)$ in Corollary 6.32 is the **Samuel Polynomial**.

Our aim is to apply this to the associated graded rings arising from I-adic filtrations. The d given by Hilbert-Serre (Theorem 6.30) gives us another number associated with a ring or module, which is another notion of dimension. The last result in this chapter will be to show that for finitely generated k-algebras, and I any maximal ideal, then this is equal to the dimension of R, $d = \dim R$.

Proof of Theorem 6.30. By induction on the number m of generators x_i.

If $m = 0$, then $S = S_0$ and V is a finitely generated S_0-module. So for large enough i, $V_i = 0$, and therefore $P(V,t)$ is a polynomial.

For $m > 0$, assume this is true for the case when S has $m-1$ generators. Multiplication by x_m is a map $V_i \to V_{i+k_m}$. We have an exact sequence

$$0 \longrightarrow K_i \longrightarrow V_i \xrightarrow{\cdot x_m} V_{i+k_m} \longrightarrow L_{i+k_m} \to 0, \tag{9}$$

where $K_i = \ker\left(V_i \xrightarrow{\cdot x_m} V_{i+k_m}\right)$ and $L_i = \operatorname{coker}\left(V_i \xrightarrow{\cdot x_m} V_{i+k_m}\right)$.

Let $K = \bigoplus_i K_i$ and let $L = \bigoplus_i L_i$. K is a graded submodule of $V = \bigoplus_i V_i$ and hence a finitely generated S-module because S is Noetherian. Similarly, L is a finitely generated S-module because $L = V/x_m V$.

Both K and L are annihilated by x_m and so may be regarded as $S_0[x_1, \dots, x_{m-1}]$-modules. Apply λ to (9) to see that

$$\lambda(K_i) - \lambda(V_i) + \lambda(V_{i+k_m}) - \lambda(L_{i+k_m}) = 0$$

Multiply by t^{i+k_m} and sum from $i = 0$ to ∞, to see that

$$t^{k_m} P(K,t) - t^{k_m} P(V,t) + P(V,t) - P(L,t) = g(t) \tag{10}$$

with $g(t) \in \mathbb{Z}[t]$ arising from the first few terms in $P(V,t)$ and $P(L,t)$ that were not hit by the summation. Apply the inductive hypothesis to $P(K,t)$ and $P(L,t)$ and this yields the result. ☐

Proof of Corollary 6.32. Here $k_1 = \dots = k_m = 1$, and so we may rewrite Equation 8 as

$$P(V,t) = \frac{f(t)}{(1-t)^d}$$

for some d, f with $f(1) \neq 0$, $f(t) \in \mathbb{Z}[t]$. Since

$$(1-t)^{-1} = 1 + t + t^2 + \dots$$

repeated differentiation yields

$$(1-t)^{-d} = \sum_i \binom{d+i-1}{d-1} t^i$$

If $f(t) = a_0 + a_1 t + \dots + a_s t^s$, then

$$\lambda(V_i) = a_0 \binom{d+i-1}{d-1} + a_1 \binom{d+i-2}{d-1} + \dots + a_s \binom{d+i-s-1}{d-1} \tag{11}$$

setting $\binom{r}{d-1} = 0$ for $r < d-1$.

The right hand side can be rearranged to give $\phi(i)$ for a polynomial $\phi(t)$ with rational coefficients valid for $d+i-s-1 \geqslant d-1$.

$$\phi(t) = \frac{f(1)}{(d-1)!} t^{d-1} + \text{(lower degree terms)}$$

So the degree of $\phi(t)$ is $d-1$, since $f(1) \neq 0$.

Using (11), we can produce an expression for $\sum_{j=0}^{i} \lambda_i(V_j)$. Using the identity

$$\sum_{j=0}^{i} \binom{d+j-1}{d-1} = \binom{d+i}{d},$$

(derived from $\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}$), we see that

$$\sum_{j=0}^{i} \lambda(V_j) = a_0 \binom{d+i}{d} + a_1 \binom{d+i-1}{d} + \dots + a_s \binom{d+i-s}{d} \tag{12}$$

for $i \geqslant s$, and this is equal to $\chi(i)$ for a rational polynomial $\chi(t) \in \mathbb{Q}[t]$. $\square$

Example 6.34. Let $S = k[x_1, \dots, x_m]$ and grade by total degree of monomials, $S = \bigoplus_{k=0}^{\infty} S_k$ where

$$S_k = \operatorname{span}\left\{ x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} \;\middle|\; \textstyle\sum_{j=1}^{m} a_j = k \right\}.$$

Let λ be the dimension as a k-vector space.

Then $\dim S_k$ is the number of monomials of degree k, which is $\binom{k+m-1}{m-1}$ for all $k > 0$. Thus

$$\phi(t) = \frac{1}{(m-1)!}(t+m-1)(t+m-2)\cdots(t+1)$$

is the Hilbert polynomial of S, which has degree $m-1$. Thus, $d = m$, and this is also equal to $\dim S$.

Example 6.35. Now we return to the case where R is a finitely generated k-algebra negatively filtered (e.g. the I-adic filtration). If M is a finitely generated R-module with good filtration $\{M_i\}$, form $V = \operatorname{gr} M$ and $S = \operatorname{gr} R$. Recall that the grading can be rearranged to be positive. We can apply the Hilbert-Serre Theorem (Theorem 6.30) with $\lambda = \dim_k$ is the k-vector space dimension if $\dim_k \left({}^{R}\!/_{I} \right) < \infty$.

By Corollary 6.32 there are Hilbert and Samuel polynomials $\phi(t), \chi(t) \in \mathbb{Q}[t]$ where for large enough i, (the sum telescopes)

$$\chi(i) = \sum_{j=-i}^{0} \dim_k \left({}^{M_j}\!/_{M_{j-1}} \right) = \dim_k \left({}^{M_0}\!/_{M_{-i-1}} \right)$$

Alternatively if $\sqrt{I} = P$ is maximal, then we might choose $\lambda = \dim_{R/P}$ is the $\left({}^{R}\!/_{P} \right)$-vector space dimension.

Definition 6.36. $d(M) =$ degree of $\chi(t)$.

Remark 6.37.

(1) In fact, Definition 6.36 is independent of the choice of good filtration.

(2) If R is a Noetherian local ring with maximal ideal P, and $\sqrt{I} = P = \sqrt{J}$ for ideals I and J, then the two Samuel polynomials arising from I-adic and J-adic filtrations have the same degree, where $\lambda(V) = \dim_{R/P}(V)$.

(3) A theorem not proved here says that for a Noetherian local domain R (e.g. a regular local ring), $d(R) = \dim R =$ least number of generators of some ideal I with $\sqrt{I} = P$.

(4) If $0 \to M_1 \to M_2 \to M_3 \to 0$ is a short exact sequence, then we have $d(M_2) = \max\{d(M_1), d(M_3)\}$ (exercise).

Lemma 6.38. If x is not a zerodivisor, then x is not in any minimal prime.

Proof. If there is only one minimal prime P and it's zero, then we're done because there are no zerodivisors.

If there is only one minimal prime $P \neq 0$, then $P = \operatorname{Nil}(R)$, and if $y \in P$ is nonzero, then $y^n = 0$ for some $n \geqslant 2$, so $yy^{n-1} = 0$ and y is a zerodivisor.

Now assume we have more than one minimal prime, say $P_1, \ldots, P_n$, and $y \in P_1$. We want to show that it's a zerodivisor. Set $N = \operatorname{Nil}(R) = \bigcap_{i=1}^n P_i$.

Then $Q = \bigcap_{i=2}^n P_i \supsetneqq N$. Pick $z \in Q \backslash N$. Thus $z \neq 0$, and is not nilpotent. So $yz \in \bigcap_{i=1}^n P_i = N$, and therefore $(yz)^n = 0$ for some n. Since $z^n \neq 0$, there is an r such that $yy^r z = 0$ yet $y^r z \neq 0$. Hence, y is a zerodivisor. ☐

Theorem 6.39. For a finitely generated k-algebra R that is an integral domain, let K be its field of fractions. Then

$$\dim R = \operatorname{trdeg}_k K = d(R)$$

using the P-adic filtration for any maximal ideal P.

Proof Sketch. We've already seen that $\operatorname{trdeg}_k K = \dim R$ in Theorem 4.32. We also saw that $\dim R = \dim \operatorname{gr} R$ with respect to the P-adic filtration. So it remains to show that for finitely generated graded k-algebras S, $\dim S = d(S)$.

This is proved by induction; using the Principal Ideal Theorem (Theorem 5.2) and the Catenary Property (Theorem 5.1). We want to apply the Catenary property, but S need not be an integral domain. But observe that $\dim S = \dim \left({}^{S}/_{P}\right)$ for some minimal prime P. Write $\overline{S} = {}^{S}/_{P}$. Let x be a homogenous non-unit non-zerodivisor (this means that $x \notin P$ by Lemma 6.38). Then

$$\dim \left({}^{S}/_{xS}\right) = \dim \left({}^{\overline{S}}/_{x\overline{S}}\right) = \dim \overline{S} - 1 = \dim S - 1$$

We also observe that

$$d\left({}^{S}/_{xS}\right) = d(S) - 1$$

for such an x. To see this consider the proof of Hilbert-Serre (Theorem 6.30), replacing x_m by x. Then the kernel of multiplication by x is zero, since x is not a zerodivisor. We deduce from equation (10) that $d(L) = d(M) - 1$ where $L = {}^{S}/_{xS}$ and $M = S$.

Clearly $\dim S = d(S)$ when these are zero – this is just the case of finite-dimensional k-vector spaces. This just checks the base case of the induction. $\square$

Remark 6.40. Note that this works for any maximal ideal P and so we have also established that $d(R)$ is independent of the choice of P.

7 Homological Algebra

Initially, we will assume R is a commutative ring with identity, but some things chapter also work for noncommutative rings.

Definition 7.1. Let L, M, N be R-modules. A map $\phi\colon M \times N \to L$ is R**-bilinear** if

(i) $\phi(r_1 m_1 + r_2 m_2, n) = r_1\phi(m_1, n) + r_2\phi(m_2, n)$

(ii) $\phi(m, r_1 n_1 + r_2 n_2) = r_1\phi(m, n_1) + r_2\phi(m, n_2)$

for $r_1, r_2 \in M$, $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$.

The idea of tensor products is to talk about multilinear maps by just talking about linear maps. If $\phi\colon M \times N \to T$ is R-bilinear, and $\theta\colon T \to L$ is R-linear, then $\theta \circ \phi$ is bilinear, and we get a map

$$\phi^*\colon \{R\text{-module maps } L \to T\} \longrightarrow \{\text{bilinear maps } M \times N \to T\}$$

We say that ϕ is **universal** if ϕ^* is a 1-1 correspondence for all L.

Lemma 7.2.

(a) Given M, N, there is an R-module T and a universal map $\phi\colon M \times N \to T$.

(b) Given two such $\phi_1 \colon M \times N \to T_1$ and $\phi_2 \colon M \times N \to T_2$, there is a unique isomorphism $\beta \colon T_2 \to T_1$ with $\beta \circ \phi_1 = \phi_2$.

Proof. (a) We have to construct a T-module and a universal map. Let F be the free R-module on the generating set $e_{(m,n)}$ indexed by pairs $(m,n) \in M \times N$. Let X be the R-submodule generated by all elements of the form

$$e_{(r_1 m_2 + r_2 m_2, n)} - r_1 e_{(m_1,n)} - r_2 e_{(m_2,n)}$$

$$e_{(m, r_1 n_1 + r_2 n_2)} - r_1 e_{(m,n_1)} - r_2 e_{(m,n_2)}$$

Set $T = F/X$ and write $m \otimes n$ for the image of $e_{(m,n)}$ in this quotient. We have a map

$$\begin{aligned} \phi \colon M \times N &\longrightarrow T \\ (m,n) &\longmapsto m \otimes n \end{aligned}$$

Note that T is generated by elements $m \otimes n$ and ϕ is bilinear. Furthermore, any map $\alpha \colon M \times N \to L$ extends to an R-module map

$$\begin{aligned} \overline{\alpha} \colon F &\longrightarrow L \\ e_{(m,n)} &\longmapsto \alpha(m,n) \end{aligned}$$

If α is bilinear, then $\overline{\alpha}$ vanishes on X and so $\overline{\alpha}$ induces a map $\alpha' \colon T \to L$ with $\alpha'(m \otimes n) = \alpha(m,n)$, and α' is uniquely defined by this equation.

(b) Follows quickly from universality (exercise). □

Remark 7.3 (Warning!)**.** Not all elements of $M \otimes N$ are of the form $m \otimes n$; a general element is of the form $\sum_{i=1}^{s} m_i \otimes n_i$.

Definition 7.4. T is the **tensor product of** M **and** N **over** R, written $M \otimes_R N$. If R is unambiguous, we can write $M \otimes N$.

For example, if $R = k$ is a field, then M, N are finite-dimensional k-vector spaces. Then $M \otimes_k N$ is a vector space of dimension $(\dim_k M)(\dim_k N)$.

Remark 7.5. For noncommutative R, one may take the tensor product $M \otimes_R N$ for a right R-module M and a left R-module N. One would then have F the free $\mathbb{Z}$-module on $e_{(m,n)}$ and X generated by all elements of the form.

$$e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}$$

$$e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}$$

$$e_{(mr,n)} - e_{(m,rn)}$$

In this situation, this is an additive group that doesn't necessarily have the structure of an R-module. However, if M is an R-S bimodule (that is, a left R-module and a right S-module) and N is a S-T bimodule, then $M \otimes_S N$ is an R-T bimodule.

Lemma 7.6. There are unique isomorphisms

(a) $M \otimes N \to N \otimes M$ given by $m \otimes n \mapsto n \otimes m$;

(b) $(M \otimes N) \otimes L \to M \otimes (N \otimes L)$ given by $(m \otimes n) \otimes \ell \mapsto m \otimes (n \otimes \ell)$;

(c) $(M \oplus N) \otimes L \to (M \otimes L) \oplus (N \otimes L)$ with $(m+n) \otimes \ell \mapsto (m \otimes \ell) + (n \otimes \ell)$;

(d) $R \otimes_R M \to M$ given by $r \otimes m \mapsto rm$.

Remark 7.7. I'm a bit low on caffeine this morning. **Interrupts lecture to drink coffee**

Definition 7.8. If $\phi \colon R \to T$ is a ring homomorphism and N is a T-module, then N may be regarded as an R-module via $r \cdot n = \phi(r)n$. This is called **restriction of scalars**.

Definition 7.9. Given an R-module M we can form $T \otimes_R M$, which can be viewed as a T-module via $t_1(t_2 \otimes m) = t_1t_2 \otimes m$ and extend linearly. This is called **extension of scalars**.

Example 7.10. Localization. Given an R-module M and a multiplicatively closed subset S of R, there is a unique isomorphism $S^{-1}R \otimes_R M \cong S^{-1}M$. Certainly, there is an R-bilinear map $S^{-1}R \times M \to S^{-1}M$ defined by $({}^{r}/_{s}, m) \mapsto {}^{rm}/_{s}$, and universality yields an R-module map $S^{-1}R \otimes M \to S^{-1}M$.

Exercise 7.11. Check that the map $S^{-1}R \otimes_R M \to S^{-1}M$ in Example 7.10 is an isomorphism.

Definition 7.12. Given $\theta \colon M_1 \to M_2$ and $\phi \colon N_1 \otimes N_2$, the **tensor product of** θ **and** ϕ is the map given by

$$\begin{array}{rcl} \theta \otimes \phi \colon M_1 \otimes N_1 & \longrightarrow & M_2 \otimes N_2 \\ m \otimes n & \longmapsto & \theta(m) \otimes \phi(n) \end{array}$$

Remark 7.13. Note that the map $M_1 \times N_1 \to M_2 \otimes N_2$ given by $(m, n) \mapsto \theta(m) \otimes \phi(n)$ is bilinear, and universality gives the map in Definition 7.12.

Lemma 7.14. Given R-modules M, N, L, $\operatorname{Hom}(M \otimes N, L) \cong \operatorname{Hom}(M, \operatorname{Hom}(N, L))$.

Proof. Given a bilinear map $\phi \colon M \times N \to L$, we have

$$\begin{array}{rcl} \theta \colon M & \longrightarrow & \operatorname{Hom}(N, L) \\ m & \longmapsto & \left(\begin{array}{rcl} \theta_m \colon N & \to & L \\ n & \mapsto & \phi(m, n) \end{array} \right) \end{array}$$

Conversely, given $\theta \colon M \to \operatorname{Hom}(N, L)$, we have a bilinear map

$$\begin{array}{rcl} M \times N & \longrightarrow & L \\ (m, n) & \longmapsto & \theta(m)(n) \end{array}$$

Thus there is an isomorphism

$$\{\text{bilinear maps } M \times N \to L\} \longrightarrow \{\text{linear maps } M \to \operatorname{Hom}(N, L)\}$$

But the left hand side is in bijection with the linear maps $M \otimes N \to L$. $\square$

Definition 7.15. Given $\phi_1 \colon R \to T_1$ a ring homomorphism, (and so T_1 is an R-module via restriction of scalars $r \cdot t = \phi(r)t$), we say that T_1 is an R**-algebra**.

Remark 7.16. Given $\phi_2 \colon R \to T_2$, we can form the **tensor product of two R-algebras** T_1 and T_2, which is an R-module $T_1 \otimes_R T_2$ with a product

$$(t_1 \otimes t_2)(t_1' \otimes t_2') = t_1 t_1' \otimes t_2 t_2'$$

Note that $1 \otimes 1$ is the multiplicative identity.

We should check that this map $(T_1 \otimes T_2) \times (T_1 \otimes T_2) \to T_1 \otimes T_2$ is well-defined.

The map

$$\begin{aligned} R &\longrightarrow T_1 \otimes T_2 \\ r &\longmapsto \phi_1(r) \otimes 1 = 1 \otimes \phi_2(r) \end{aligned}$$

is a ring homomorphism, and so $T_1 \otimes_R T_2$ is an R-algebra.

Exercise 7.17. Go home and check all the details in Remark 7.16.

Example 7.18. Examples of R-algebras.

(1) k a field, $k[X] \otimes k[Y] \cong k[X, Y]$.

(2) $\mathbb{Q}[X]/\langle X^2+1 \rangle \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}[X]/\langle X^2+1 \rangle$.

(3) $k[X]/\langle f(X) \rangle \otimes k[Y]/\langle g(Y) \rangle \cong k[X,Y]/\langle f(X), g(Y) \rangle$.

7.1 Projective and Injective Modules

Example 7.19. Observe that in general for a short exact sequence of R-modules,

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0,$$

we don't necessarily have exactness for

$$0 \longrightarrow \mathrm{Hom}(N, M_1) \longrightarrow \mathrm{Hom}(N, M) \longrightarrow \mathrm{Hom}(N, M_2) \longrightarrow 0$$

as not all maps $N \to M_2$ lift to maps $N \to M$. For example, given the short exact sequence

$$0 \longrightarrow 2\mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \xrightarrow{\ \pi\ } \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

take $N = \mathbb{Z}/2\mathbb{Z}$. Any map $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ has image in $2\mathbb{Z}/4\mathbb{Z}$ and so composition with π must be zero.

Similarly, we don't necessarily get exactness in

$$0 \longrightarrow \mathrm{Hom}(M_2, N) \longrightarrow \mathrm{Hom}(M, N) \longrightarrow \mathrm{Hom}(M_1, N) \longrightarrow 0$$

using the same example, the restriction of any map $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ must be zero on $M_1 = 2\mathbb{Z}/4\mathbb{Z}$.

The property that $\mathrm{Hom}(N, -)$ is exact is characterized by N being a projective module.

Definition 7.20. An R-module P is **projective** if given a map $\phi\colon P \to M_2$ and a surjection $\psi\colon M_1 \twoheadrightarrow M_2$, then ϕ may be lifted to a map $\widehat{\phi}\colon P \to M_1$ such that $\psi \circ \widehat{\phi} = \phi$.

$$\begin{tikzcd} & P \arrow[d, "\phi"] \arrow[dl, dashed, "\widehat{\phi}"'] & \\ M_1 \arrow[r, "\psi"'] & M_2 \arrow[r] & 0 \end{tikzcd}$$

In other words,

$$\mathrm{Hom}(P, M_1) \longrightarrow \mathrm{Hom}(P, M_2) \longrightarrow 0$$

is exact.

There is also a dual definition of injective modules.

Definition 7.21. An R-module E is **injective** if given a map $\sigma\colon M_1 \to E$ and an injection $\rho\colon M_1 \hookrightarrow M_2$, then σ is the restriction of some map $\widehat{\sigma}\colon M_2 \to E$ such that $\sigma = \widehat{\sigma} \circ \rho$.

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\rho"] \arrow[d, "\sigma"'] & M_2 \arrow[dl, dashed, "\widehat{\sigma}"] \\ & E & \end{tikzcd}$$

In other words,

$$\mathrm{Hom}(M_2, E) \longrightarrow \mathrm{Hom}(M_1, E) \longrightarrow 0$$

is exact.

Example 7.22.

(1) Free modules are projective.

(2) The fraction field K over an integral domain R is an injective R-module.

Lemma 7.23. For an R-module P, the following are equivalent.

(1) P is projective.

(2) for every short exact sequence $0 \to M_1 \to M \to M_2 \to 0$, the induced sequence $0 \to \mathrm{Hom}(P, M_1) \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M_2) \to 0$ is exact.

(3) If $\varepsilon\colon M \to P$ is surjective, then there is a homomorphism $\beta\colon P \to M$ such that $\varepsilon\beta = \mathrm{id}_P$.

(4) P is a direct summand of every module of which it is a quotient.

(5) P is a direct summand of a free module.

Proof of Lemma 7.23.

(1) $\implies$ (2) Definition.

(2) $\implies$ (3). Choose an exact sequence $0 \to \ker \varepsilon \to M \to P \to 0$. Then by condition (2), $0 \to \mathrm{Hom}(P, \ker \varepsilon) \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, P) \to 0$ is exact, and so there is a $\beta \colon P \to M$ such that $\varepsilon\beta = \mathrm{id}$.

(3) $\implies$ (4). Let $P = M/M_1$, and we have $0 \to M_1 \to M \to P \to 0$ by (3) there is $\beta \colon P \to M$ such that $\varepsilon\beta = \mathrm{id}$, and hence P is a direct summand of M.

(4) $\implies$ (5). P is a quotient of a free module: take a generating set S of P and form F, the free R-module with basis $\{e_x \mid x \in S\}$. Then we have a map $\theta \colon F \to P$ given by $e_x \mapsto x$. By (4), P is a direct summand of F. (Aside: $\ker \theta$, the module of relations between the generators, is called the **first syzygy module**).

(5) $\implies$ (1). By (5), we know that $F = P \oplus Q$ where F is a free R-module, and since free modules are projective and Hom behaves well with direct sums, we deduce P is projective. □

Remark 7.24. If R is a PID, then every submodule of a finitely generated free module is free, and so direct summands of finitely generated free modules are free. Thus finitely generated projective modules are free.

Lemma 7.25. For an R-module E, the following are equivalent.

(1) E is injective.

(2) for every short exact sequence $0 \to M_1 \to M \to M_2 \to 0$, the induced sequence $0 \to \mathrm{Hom}(M_2, E) \to \mathrm{Hom}(M, E) \to \mathrm{Hom}(M_1, E) \to 0$ is exact.

(3) If $\mu \colon E \to M$ is injective (a monomorphism) then there is some $\beta \colon M \to E$ with $\beta\mu = \mathrm{id}$.

(4) E is a direct summand in every module which contains E as a submodule.

Exercise 7.26. Prove Lemma 7.25. (Look up the definition of **injective hull**).

Now let us consider $- \otimes_R N$ for an R-module N.

Lemma 7.27. If $M_1 \to M \to M_2 \to 0$ is an exact sequence of R-modules, and N is an R-module, then the induced sequence $M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$ is exact.

Remark 7.28. However, considering the short exact sequence of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\ 2\ } \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

and $N = \mathbb{Z}/2\mathbb{Z}$, we see that $\mathbb{Z} \otimes N \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \otimes N \cong \mathbb{Z}/2\mathbb{Z}$. Tensoring with N gives

$$\mathbb{Z}/2\mathbb{Z} \xrightarrow{\ 0\ } \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

and the zero map is not injective. Thus, in this case tensoring with N need not preserve exactness of short exact sequences.

Lemma 7.27 is saying that $- \otimes_R N$ is **right exact**.

To prove Lemma 7.27, we make use of Lemma 7.14 $\mathrm{Hom}(M \otimes N, L) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, L))$, and the following lemma:

Lemma 7.29.

(a) The sequence $M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2 \to 0$ is exact if and only if there is an exact sequence $0 \to \mathrm{Hom}(M_2, L) \xrightarrow{\phi^*} \mathrm{Hom}(M, L) \xrightarrow{\theta^*} \mathrm{Hom}(M_1, L)$ for all R-modules L.

(b) The sequence $0 \to M_1 \to M \to M_2$ is exact if and only if there is an exact sequence $0 \to \mathrm{Hom}(L, M_1) \to \mathrm{Hom}(L, M) \to \mathrm{Hom}(L, M_2)$ for all R-modules L.

Proof. The only part we consider is the backwards implication for (a). The rest is left as an exercise.

So assume $0 \to \mathrm{Hom}(M_2, L) \to \mathrm{Hom}(M, L) \to \mathrm{Hom}(M_1, L)$ is exact for all L. Then $\mathrm{Hom}(M_2, L) \to \mathrm{Hom}(M, L)$ is injective for all L, so the map $M \to M_2$ is surjective (exercise). Hence, the sequence $M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2 \to 0$ is exact at M_2.

Next we check that $\operatorname{im}\theta \leqslant \ker\phi$. Take $L = M_2$, $f = \mathrm{id}_{M_2}$ the identity map $M_2 \to M_2$. Then $\theta^*(\phi^*(f)) = 0$. Hence, $f \circ \phi \circ \theta = 0$ and $\phi \circ \theta = 0$ since $f = \mathrm{id}_{M_2}$. Therefore, $\operatorname{im}\theta \leqslant \ker\phi$.

Finally we need to check that $\ker\phi \leqslant \operatorname{im}\theta$. Take $L = M/\operatorname{im}\theta$ and let $\pi \colon M \to L$ be the projection. Then $\pi \in \ker\theta^*$, and hence by exactness there is $\psi \in \mathrm{Hom}(M_2, L)$ such that $\pi = \phi^*(\psi)$. So $\ker\pi \geqslant \ker\phi$. But $\ker\pi = \operatorname{im}\theta$, so we have that $\operatorname{im}\theta \geqslant \ker\phi$.

Therefore, $\operatorname{im}\theta = \ker\phi$, so $M_1 \xrightarrow{\theta} M \xrightarrow{\phi} M_2 \to 0$ is exact at M. □

This gives us everything we need to prove Lemma 7.27.

Proof of Lemma 7.27. Given an exact sequence $M_1 \to M \to M_2 \to 0$, we want to show that $M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$ is exact.

Let L be any R-module. The sequence

$$0 \to \mathrm{Hom}(M_2, \mathrm{Hom}(N, L)) \to \mathrm{Hom}(M, \mathrm{Hom}(N, L)) \to \mathrm{Hom}(M_1, \mathrm{Hom}(N, L))$$

is exact, using Lemma 7.29(a) replacing L by $\mathrm{Hom}(N, L)$. Hence by Lemma 7.14,

$$0 \to \mathrm{Hom}(M_2 \otimes N, L) \to \mathrm{Hom}(M \otimes N, L) \to \mathrm{Hom}(M_1 \otimes N, L)$$

is exact for all L. Finally, using Lemma 7.29(a) again, we see that

$$M_1 \otimes N \to M \otimes N \to M_2 \otimes N \to 0$$

is exact. □

Definition 7.30. N is a **flat** R-module if given any short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0,$$

then

$$0 \longrightarrow M_1 \otimes N \longrightarrow M \otimes N \longrightarrow M_2 \otimes N \longrightarrow 0$$

is exact. That is, $- \otimes_R N$ is **exact**.

Example 7.31.

(1) R is a flat R-module, since $R \otimes_R M \cong M$.

(2) Free modules are flat.

(3) Direct summands of free modules are flat, since $\otimes$ behaves well with respect to $\oplus$. Thus, projective modules are flat.

(4) If $R = \mathbb{Z}$, then $\mathbb{Q}$ is a flat Z-module.

Now we'll get to grips with Ext and Tor.

Remark 7.32. Given an R-module M, we can pick a generating set and produce a short exact sequence $0 \to K \to F \to M \to 0$ where F is free, and K is the relations among generators in M. The map $F \to M$ is given by sending a basis element to the corresponding generator in M.

Definition 7.33. By a **projective presentation** of M we mean a short exact sequence $0 \to K \to P \to M \to 0$ with P projective. It is a **free presentation** if P is free.

Definition 7.34. K is called the **first syzygy module** of M.

Definition 7.35 (Ext & Tor)**.** Given a projective presentation $0 \to K \to P \to M \to 0$ of M, then apply $- \otimes_R N$ to get a sequence

$$K \otimes N \longrightarrow P \otimes N \longrightarrow M \otimes N \longrightarrow 0.$$

Define $\mathrm{Tor}^R(M, N) = \mathrm{Tor}_1^R(M, N) := \ker(K \otimes N \to P \otimes N)$.

If instead we apply $\mathrm{Hom}(-, N)$ to this projective presentation, we get

$$0 \longrightarrow \mathrm{Hom}(M, N) \longrightarrow \mathrm{Hom}(P, N) \longrightarrow \mathrm{Hom}(K, N).$$

Define $\mathrm{Ext}_R(M, N) = \mathrm{Ext}_R^1(M, N) := \mathrm{coker}\,(\mathrm{Hom}(P, N) \to \mathrm{Hom}(K, N))$

Remark 7.36. Thus, if N is flat, then $\mathrm{Tor}^R(M, N) = 0$ for all M, since tensoring with N preserves short exact sequences when N is flat. If E is injective, then $\mathrm{Ext}_R(M, E) = 0$ for all M, since $\mathrm{Hom}(-, E)$ is an injective functor. Furthermore, if P is projective and we have $0 \to K \to P_1 \to P \to 0$, then Lemma 7.23 tells us that P is a direct summand of P_1, and since we know Hom behaves well with respect to direct sums, we note that $\mathrm{Ext}(P, N) = 0$ for all N if P is projective.

Remark 7.37.

(1) Often, the R is omitted from Tor^R and Ext_R unless it's needed. Usually it's clear from the context.

(2) Our definitions appear dependent on the choice of projective presentation. However, $\mathrm{Tor}(M, N)$ and $\mathrm{Ext}(M, N)$ are actually *independent* of the choice of projective presentation for M.

(3) One may also take a projective presentation for N and apply $M \otimes -$ to it. The analogous kernel is isomorphic to $\mathrm{Tor}(M, N)$ as defined above. We also see that $\mathrm{Tor}(M, N) \cong \mathrm{Tor}(N, M)$.

(4) Similarly, one may also take a short exact sequence $0 \to N \to E \to L \to 0$ with E injective, and apply $\mathrm{Hom}(M, -)$ and consider the cokernel of the map $\mathrm{Hom}(M, E) \to \mathrm{Hom}(M, L)$. This is isomorphic to $\mathrm{Ext}(M, N)$ as defined above.

(5) Given any R module, it does indeed embed in an injective one. In fact, there is a smallest such injective module (by Zorn), unique up to isomorphism, called the **injective hull** $E(M)$.

(6) The name Ext comes from an alternative description where $\mathrm{Ext}(M, N)$ consists of equivalence classes of extensions of M by N, meaning a short exact sequence $0 \to N \to X \to M \to 0$. The zero element is the equivalence class of the direct sum $0 \to N \to M \oplus N \to M \to 0$.

(7) The name Tor is more obscure. If $R = \mathbb{Z}$, it relates to torsion.

Example 7.38. Take the free presentation of the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \tag{13}$$

Apply $- \otimes \mathbb{Z}/2\mathbb{Z}$ and we get

$$\mathrm{Tor}\left(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\right) = \ker\left(\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}\right) \cong \mathbb{Z}/2\mathbb{Z}$$

Instead apply $\mathrm{Hom}(-, N)$ to (13), to see

$$\mathrm{Ext}\left(\mathbb{Z}/2\mathbb{Z}, N\right) = \mathrm{coker}\left(\mathrm{Hom}(\mathbb{Z}, N) \longrightarrow \mathrm{Hom}(\mathbb{Z}, N)\right)$$

The map $\mathrm{Hom}(\mathbb{Z}, N) \to \mathrm{Hom}(\mathbb{Z}, N)$ is induced by multiplication by 2, and given by $\phi \mapsto 2\phi$. Notice that for a $\mathbb{Z}$-module N, $\mathrm{Hom}(\mathbb{Z}, N) \cong N$, so we see that

$$\mathrm{Ext}\left(\mathbb{Z}/2\mathbb{Z}, N\right) = \mathrm{coker}\left(\mathrm{Hom}(\mathbb{Z}, N) \longrightarrow \mathrm{Hom}(\mathbb{Z}, N)\right) \cong N/2N$$

Remark 7.39. "I hope you like my zed's."

Example 7.40 (**Koszul Complex**)**.** Let $R = k[X]$. We have a free presentation of the trivial R-module k with X acting like zero,

$$0 \longrightarrow \langle X \rangle \longrightarrow k[X] \longrightarrow k \longrightarrow 0$$

Notice that $\langle X \rangle \cong k[X]$ as a $k[X]$-module. Hence, we can write this short exact sequence as

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k[X] & \xrightarrow{\text{mult. by } X} & k[X] & \longrightarrow & k & \longrightarrow & 0 \\ & & g(X) & \longmapsto & Xg(X) & & & & \\ & & & & f(X) & \longmapsto & f(0) & & \end{array} \tag{14}$$

If instead $R = k[X_1, X_2]$, then we have a short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \langle X_1, X_2\rangle & \longrightarrow & k[X_1, X_2] & \longrightarrow & k & \longrightarrow & 0 \\ & & & & f(X_1, X_2) & \longmapsto & f(0,0) & & \end{array}$$

Notice that $k[X_1, X_2]$ is isomorphic to the submodule of $k[X_1, X_2] \oplus k[X_1, X_2]$ generated by $(X_2, -X_1)$, so we can rewrite the above as

$$\begin{array}{ccccccccc} 0 & \to & k[X_1, X_2] & \to & k[X_1, X_2] \oplus k[X_1, X_2] & \longrightarrow & (X_1, X_2) & \longrightarrow & 0 \\ & & & & (g_1, g_2) & \longmapsto & X_1 g_1 + X_2 g_2 & & \\ & & f & \longmapsto & (X_2 f, -X_1 f) & & & & \end{array} \tag{15}$$

If we put together (14) and (15), we can get an exact sequence

$$0 \longrightarrow F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \longrightarrow k \longrightarrow 0$$

with $F_2 \cong k[X_1, X_2]$, $F_1 \cong k[X_1, X_2] \oplus k[X_1, X_2]$ and $F_0 \cong k[X_1, X_2]$. This is a **free resolution** of the trivial module.

Definition 7.41. Let M be an R-module. A **projective resolution of** M is an exact sequence

$$\cdots \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$$

with P_i projective for all i. It is a **free resolution** if all P_i are free.

Remark 7.42. If R is Noetherian and M is a finitely generated R-module then there is a free presentation $0 \to K \to F \to M \to 0$ with F finitely generated and free and so K is finitely generated. Repeating shows that M has a free resolution where all the free modules are finitely generated.

Definition 7.43. The **Koszul complex** gives a free resolution of the trivial module for $k[X_1, \ldots, X_n]$. Define F_i to be free on basis $\{e_{j_1,\ldots,j_i}\}$ indexed by subsets $\{j_1, \ldots, j_i\} \subseteq \{1, \ldots, n\}$. Further define the boundary maps $d\colon F_i \to F_{i-1}$

$$d\left(e_{j_1,\ldots,j_i}\right) = \sum_{\ell=1}^{i} (-1)^{\ell-1} X_{j_\ell} e_{j_1,\ldots,j_{\ell-1},j_{\ell+1},\ldots,j_i} \in F_{i-1}$$

Remark 7.44. Quite a few authors would write a projective resolution without the final term. We write

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0,$$

with each P_i projective and the whole thing exact, but many authors would write

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \xrightarrow{\phi} P_0$$

and M would be $\operatorname{coker} \phi$.

Definition 7.45. Applying $-\otimes N$ to a projective resolution for M, we have

$$\cdots \longrightarrow P_2 \otimes N \xrightarrow{\theta_1} P_1 \otimes N \xrightarrow{\theta_0} P_0 \otimes N \longrightarrow 0$$

If $\operatorname{im}\theta_i \subseteq \ker\theta_{i-1}$, then this is called a **chain complex**, and ${}^{\ker\theta_{i-1}}\!/_{\operatorname{im}\theta_i}$ are called the **homology groups** of the chain complex. These are R-modules.

Definition 7.46. $\operatorname{Tor}_i^R(M,N)$ is the homology group at $P_i \otimes N$. Thus $\operatorname{Tor}_0(M,N) = M \otimes N$ and $\operatorname{Tor}_1(M,N) = \operatorname{Tor}(M,N)$ as defined in Definition 7.35.

Example 7.47. If K_1 is the first syzygy module associated with the resolution

$$0 \longrightarrow K_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

then $\operatorname{Tor}_{i-1}(K_1,N) = \operatorname{Tor}_i(M,N)$. This process is called **dimension shifting**.

We can do a similar thing for Ext.

Definition 7.48. Given a projective resolution for M, one can apply $\operatorname{Hom}(-,N)$, and consider the homology groups in the **cochain complex**

$$0 \longrightarrow \operatorname{Hom}(P_0,N) \longrightarrow \operatorname{Hom}(P_1,N) \longrightarrow \cdots . \tag{16}$$

We define $\operatorname{Ext}_R^i(M,N)$ to be the homology group at $\operatorname{Hom}(P_i,N)$. Thus $\operatorname{Ext}^0(M,N) = \operatorname{Hom}(M,N)$ and $\operatorname{Ext}^1(M,N) = \operatorname{Ext}(M,N)$ as defined in Definition 7.35.

Note that the sequence (16) may not be exact at $\operatorname{Hom}(P_0,N)$, but it's still a cochain complex so we get homology.

Example 7.49. Let K_1 be the first syzygy module associated with the resolution

$$0 \longrightarrow K_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

then $\operatorname{Ext}^i(M,N) = \operatorname{Ext}^{i-1}(K,N)$. Another form of **dimension shifting.**

Remark 7.50. These definitions are independent of the choice of projective resolution. Moreover, one can obtain $\operatorname{Ext}^i(M,N)$ by applying $\operatorname{Hom}(M,-)$ to an **injective resolution** of N. Such an injective resolution is an exact sequence

$$0 \longrightarrow N \longrightarrow E_1 \longrightarrow E_1 \longrightarrow \cdots$$

with E_i injective. Considering then the homology groups in

$$0 \longrightarrow \operatorname{Hom}(M,E_1) \longrightarrow \operatorname{Hom}(M,E_2) \longrightarrow \cdots$$

gives us the same thing.

Lemma 7.51. The following are equivalent

(1) $\operatorname{Ext}^{n+1}(M,N) = 0$ for all R-modules N;

(2) M has a projective resolution of length n

$$0 \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0.$$

Exercise 7.52. Prove Lemma 7.51.

Definition 7.53. The **projective dimension** of M is n if $\mathrm{Ext}^{n+1}(M,N) = 0$ for all R-modules N, but there is some L with $\mathrm{Ext}^n(M,L) \neq 0$.

There is an analogous definition of **injective dimension**, which uses Tor instead of Ext.

Remark 7.54 (Offhand comment)**.** If you have a bound on the projective dimension, then you also have a bound on the injective dimension.

Definition 7.55. The **global dimension** of R is the supremum of all the projective dimensions of R-modules.

Example 7.56.
(1) If k is a field, then all k-modules are free and the global dimension is zero.
(2) The global dimension of any PID that is not a field, such as $\mathbb{Z}$ or $k[X]$ is 1.
(3) The condition that the global dimension of R is zero is equivalent to saying that all submodules of R are direct summands. In other words, R is semisimple – c.f. complex representation theory of finite groups, where the group algebra has global dimension zero.

Theorem 7.57 (Hilbert's Syzygy Theorem)**.** Let k be a field and $S = k[X_1, \dots, X_n]$, considered as a graded module with respect to the total degree of polynomials. Let M be any finitely generated graded S-module.

Then there is a free resolution of M of length at most n.

Remark 7.58. The Koszul complex (Example 7.40) gives a free resolution of the trivial module k of length n.

Proof Sketch of Hilbert's Syzygy Theorem (Theorem 7.57). Consider $\mathrm{Tor}_i(k,M)$ obtained in two different ways. Either

(a) apply $- \otimes M$ to the Koszul complex and consider the homology groups;

(b) apply $k \otimes -$ to a free resolution for M and consider the homology groups.

(Remember that $\mathrm{Tor}_i(M,N) = \mathrm{Tor}_i(N,M)$).

We may assume that the free resolution for M is a minimal free resolution, that is, at each stage we take a minimal number of generators. Write the free resolution as

$$\cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

with each F_i free. The minimality means that when we tensor with the trivial module,

$$\cdots \longrightarrow k \otimes F_1 \longrightarrow k \otimes F_0 \longrightarrow k \otimes M \longrightarrow 0$$

all the maps apart from the last one are zero. So the homology groups are finite dimensional k-vector spaces of dimension equal to the rank of the corresponding free module (apart from at the end).

However, from the description using $- \otimes M$ on the Koszul complex, we know that $\mathrm{Tor}_i(k,M) = 0$ for large enough i. Thus, the free modules in the minimal free resolution for M must be eventually zero. $\square$

Remark 7.59. There is a proof of Theorem 7.57 without using Tor_i in Zariski and Samuel.

Proposition 7.60. Given a short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0,$$

there are long exact sequences

$$\cdots \to \mathrm{Tor}_1(M,N) \to \mathrm{Tor}_1(M_2,N) \to \mathrm{Tor}_0(M_1,N) \to \mathrm{Tor}_0(M,N) \to \mathrm{Tor}_0(M_2,N) \to 0$$

and

$$0 \to \mathrm{Ext}^0(M_2,N) \to \mathrm{Ext}^0(M,N) \to \mathrm{Ext}^0(M_1,N) \to \mathrm{Ext}^1(M_2,N) \to \mathrm{Ext}^1(M,N) \to \cdots$$

7.2 Hochschild (co)Homology

This is the cohomological theory of bimodules. Consider R to be a k-algebra, not necessarily commutative.

Definition 7.61. An $R - S$ **bimodule** M is simultaneously a left R-module and a right S-module such that the two actions of R and S commute.

Definition 7.62. For a k-algebra R, the **opposite algebra** R^{op} has the same elements as R but $x \cdot y = yx$, where $\cdot$ is multiplication in R^{op} and juxtaposition yx is multiplication in R. This is sometimes (but uncommonly) called the **enveloping algebra** of R, denoted R^e.

Remark 7.63. One can reformulate an R-R bimodule as a right module for $R \otimes_k R^{\mathrm{op}}$, where R^{op} is the k-algebra R but with backwards multiplication. One can reformulate an $R - R$ bimodule as a right module for $R \otimes_k R^{\mathrm{op}}$, with $m \cdot r \otimes s = smr$, where smr is multiplication of m on the left by s and on the right by r as an R-R bimodule.

Example 7.64.
(a) R itself is an $R - R$ bimodule via left/right multiplication.
(b) $R \otimes_k R$ is also an $R - R$ bimodule, generated by $1 \otimes 1$. It corresponds to the free $R \otimes R^{\mathrm{op}}$-module of rank 1.

Definition 7.65. Given an $R - R$ bimodule M, the i-th **Hochschild Homology** of M is

$$\mathrm{HH}_i(R,M) = \mathrm{Tor}_i^{(R\text{-}R)}(R,M) = \mathrm{Tor}_i^{R\otimes R^{\mathrm{op}}}(R,M)$$

where we take Tor_i of M as an R-bimodule.

Similarly, we have the i-th **Hochschild Cohomology**

$$\mathrm{HH}^i(R,M) = \mathrm{Ext}^i_{R\text{-}R}(R,M) = \mathrm{Ext}^i_{R\otimes R^{\mathrm{op}}}(R,M)$$

Remark 7.66. Notice that in particular

$$\mathrm{HH}^0(R,M) = \mathrm{Hom}_{R\text{-}R}(R,M) \cong \{m \in M \mid rm = mr \forall r \in R\}.$$

So we can say that $\mathrm{HH}^0(R,R) = Z(R)$, the center of R. Similarly,

$$\mathrm{HH}_0(R,M) \cong M/\langle rm - mr \mid m \in M, r \in R\rangle$$

Remark 7.67. Given the $R-R$ bimodule R, there is a short exact sequence

$$0 \longrightarrow \ker\mu \longrightarrow R\otimes_k R \xrightarrow{\mu} R \longrightarrow 0$$

where $\mu(r\otimes s) = rs$ is the multiplication map (an $R-R$ bimodule map). It is a free presentation for R.

$\ker\mu$ is spanned by elements of the form $r\otimes 1 - 1\otimes r$, and if we take a k-basis of R then the corresponding elements $r\otimes 1 - 1\otimes r$ would be a k-basis for $\ker\mu$.

If $\theta \in \mathrm{Hom}_{R\text{-}R}(R\otimes_k R, M)$, it is determined by the image m of $1\otimes 1$ and the restriction to $\ker\mu$ is the map $r\otimes 1 - 1\otimes r \mapsto rm - mr$.

Now consider $\phi \in \mathrm{Hom}_{R\text{-}R}(\ker\mu, M)$. Denote by d the map

$$\begin{aligned} d\colon R &\longrightarrow M \\ r &\longmapsto \phi(r\otimes 1 - 1\otimes r) \end{aligned}$$

and observe that

$$\begin{aligned} rs \mapsto \phi(rs\otimes 1 - 1\otimes rs) &= \phi(r(s\otimes 1 - 1\otimes s) + (r\otimes 1 - 1\otimes r)s) \\ &= r\phi(s\otimes 1 - 1\otimes s) + \phi(r\otimes 1 - 1\otimes r)s \\ &= rd(s) + d(r)s \end{aligned}$$

Definition 7.68. A map $d\colon R\to M$ satisfying $d(rs) = rd(s) + d(r)s$ is called a **derivation**. The set of derivations from R to M is $\mathrm{Der}(R,M)$.

The derivations of the form $d(r) = rm - mr$ for some fixed $m\in M$ are called the **inner derivations**. The set of inner derivations from R to M is $\mathrm{InnDer}(R,M)$.

Lemma 7.69.

$$\begin{aligned} \mathrm{HH}^1(R,M) &= \mathrm{coker}\left(\mathrm{Hom}_{R\text{-}R}(R\otimes_k R, M) \to \mathrm{Hom}_{R\text{-}R}(\ker\mu, M)\right) \\ &\cong \mathrm{Der}(R,M)/\mathrm{InnDer}(R,M) \end{aligned}$$

In particular,

$$\mathrm{HH}^1(R,R) = \mathrm{Der}(R,R)/\mathrm{InnDer}(R,R)$$

If R is commutative then $\mathrm{InnDer}(R,R) = 0$, so $\mathrm{HH}^1(R,R) \cong \mathrm{Der}(R,R)$.

Remark 7.70. $\mathrm{HH}_1(R,R)$ is obtained from tensoring our free presentation of R (as a bimodule) with the R-R bimodule R. This gives the Kähler differentials (see example sheet 4).

Remark 7.71. We can use this bimodule theory to define yet another dimension for a k-algebra R via global dimension. Note that the R-R bimodule R is projective as an bimodule precisely if R embeds as a bimodule in $R\otimes_k R$ as a direct summand. If this is the case then the k-algebra is said to be **separable**. Separable field extensions may be defined in this way, which coincides with the usual definition. Separable k-algebras are necessarily finite dimensional as k-vector spaces. These separable k-algebras are precisely those of dimension zero as bimodules.