University of Cambridge

Mathematics Tripos

Part III

Algebra

Michaelmas, 2019

Lectures by
C. Brookes

Notes by
Qiangru Kuang

Contents

0 Brief history & Introduction

David Hilbert published a series of papers in 1980s about invariant theory. The primary example is as follow. let k be a field and consider the polynomial $k[x_1, \dots, x_n]$ over k. The symmetric group Σ_n acts on the variables and this induces an action on $k[x_1, \dots, x_n]$: if $g \in \Sigma_n$ then

$$g(f)(x_1, \dots, x_n) = f(x_{g(1)}, \dots, x_{g(n)}).$$

These are ring automorphisms.

Consider the polynomials fixed under this action, which are called *symmetric polynomials*. We have elemetary symmetric polynomials

$$\begin{aligned} f_1(x_1, \dots, x_n) &= x_1 + \dots x_n \\ f_2(x_1, \dots, x_n) &= \sum_{i<j} x_i x_j \\ &\cdots \\ f_n(x_1, \dots, x_n) &= x_1 x_2 \cdots x_n \end{aligned}$$

The ring of symmetric polynomials is generated by $f_1, \dots, f_n$ and is in fact isomorphic to the polynomial algebra $k[Y_1, \dots, Y_n]$ where f_i corresponds to Y_i.

Hilbert considered a lot of other groups, such as the alternating group. Along the way, he proved four big theorems:

1. basis theorem,
2. Nullstellensatz,
3. polynomial nature of a certain function, which is called nowadays Hilbert function,
4. syzygy theorem.

If you are taking this course you should be familiar with 1. 2 is a famous result in algebraic geometry. 3 marks the beginning of dimension theory and 4 starts the subject of homological algebra.

Emmy Noether (1921) abstracted from Hilbert's work the crucial property behind the basis theorem: a commutative ring R is *Noetherian* if all its ideals are finitely generated. In this language,

Theorem 0.1 (basis theorem). *If R is Noetherian then so is $R[X]$.*

As a corollary, $R[X_1, \dots, X_n]$ is also Noetherian.

Noether went on to develop the theory of ideals in Noetherian rings. One has primary decomposition of ideals, which is a weak version of prime factorisation.

Most content of the course is from 1920 to 1950.

A word on the link between commutative algebra and algebraic geometry. The fundamental theorem of algebra says that a polynomial $f \in \mathbb{C}[x]$ is determined up to scalars by its zeros up to multiplicity. More generally, for a subset I of polynomials in $\mathbb{C}[x_1, \dots, x_n]$, we define the set of common zeros

$$Z(I) = \{(a_1, \dots, a_n) \in \mathbb{C}^n : f(a_1, \dots, a_n) = 0 \text{ for all } f \in I\}.$$

$Z(I)$'s are called *(affine) algebraic sets* and form the closed subsets of $\mathbb{C}^n$ under Zariski topology. Note that one can replace I by the ideal generated by I without changing $Z(I)$.

On the other hand, if we have $\mathcal{S} \subseteq \mathbb{C}^n$ then we define

$$I(\mathcal{S}) = \{f \in \mathbb{C}[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in \mathcal{S}\}.$$

It is easy to see that it is an ideal of $\mathbb{C}[x_1, \dots, x_n]$ and in fact a *radical* one.

One form of Nullstellensatz says that there is a bijective correspondence

$$\begin{aligned} \{\text{radical ideals of } \mathbb{C}[x_1, \dots, x_n]\} &\longleftrightarrow \{\text{algebraic subsets of } \mathbb{C}^n\} \\ I &\mapsto Z(I) \\ I(\mathcal{S}) &\mapsfrom \mathcal{S} \end{aligned}$$

As for the third major theorem proved by Hilbert, we'll spend quite a bit of time talking about dimension. In commutative algebra there are at least three approaches

1. by lengths of chains of prime ideals (Krull dimension),
2. by growth rate – degree of the Hilbert function,
3. by transcendence degree of the field of fraction of integral domains.

For finitely generated commutative algebra they all give the same answer.

Dimension 0 rings are important and dimension 0 Noetherian rings are called *Artinian rings*. For example, fields or rings that are finitely dimensional as vector spaces. In this case we talk about the non-commutative rings.

Dimesion 1 rings also have special properties. They arise naturally in number theory and algebraic curves. See III Algebraic Number Theory.

At the end of the course, we will learn differential operators which lead into Hochschild cohomology, the cohomology theory for associative algebras.

Course convention: we use upper case letters such as X and Y for polynomial algebras, e.g. $k[X]$, and use lower case letters for the subalgebra generated by such elements, e.g. if R is a k-algebra and $x_1, \dots, x_n \in R$ then $k[x_1, \dots, x_n] \subseteq R$ is the subalgebra generated by x_i's.

1 Examples, Localisation & Tensor products

Throughout this chapter R is a commutative ring with a unit.

1.1 Noetherianness

> **Lemma 1.1.** *Let M be a (left) R-module. Then TFAE:*
>
> 1. *every submodule of M (including itself) is finitely generated.*
> 2. *there does not exist an infinite strictly ascending chain of submodules (ascending chain condition).*
> 3. *every non-empty set of submodules of M contains at least one maximal member.*

Proof. Exercise. □

> **Definition** (Noetherian module)**.** An R-module M is *Noetherian* if it satisfies any of the conditions above.

> **Definition** (Noetherian ring)**.** A commutative ring is *Noetherian* if it is Noetherian as a (left) module.

Remark. Submodules of a ring are the ideals.

> **Lemma 1.2.** *Let N be a submodule of M. Then M is Noetherian if and only if N and M/N are Noetherian.*

Proof. Exercise. □

Remark.

1. Images of Noetherian modules are Noetherian.
2. Ring images of Noetherian rings are Noetherian.

> **Lemma 1.3.** *Let R be a Noetherian ring. Then finitely generated R-modules are Noetherian.*

Proof. Exercise. □

Example.

1. Fields are Noetherian.
2. Principal ideal domains, e.g. $\mathbb{Z}, k[X]$ and fields, are Noetherian.
3. $\{q \in \mathbb{Q} : q \text{ of the form } \frac{m}{n}, m, n \in \mathbb{Z}, n \neq 0 \, p \nmid n\}$ is Noetherian. This is an example of a localisation of $\mathbb{Z}$. In general, localisations of Noetherian rings are Noetherian.

4. $k[X_1, \ldots, X_n], \mathbb{Z}[X_1, \ldots, X_n]$ are Noetherian from basis theorem.

5. $k[X_1, X_2, \ldots]$ with infinitely many variables is not Noetherian as

$$(X_1) \subseteq (X_1, X_2) \subseteq \cdots$$

is an infinite strictly ascending chain of ideals.

6. A finitely generated commutative ring R (there exists a set $\{a_1, \ldots, a_n\}$ such that there is a surjective ring homomorphism $\mathbb{Z}[X_1, \ldots, X_n] \to R, X_i \mapsto a_i$) is Noetherian.

7. $k[[X]]$, formal power series ring, is Noetherian. We wil prove this shortly.

> **Theorem 1.4** (basis theorem). *Let R be a Noetherian ring then $R[x]$ is Noetherian.*

Sketch proof. We prove every ideal I of $R[x]$ is finitely generated. Define $I(n)$ to be elements of I of degree $\leq n$. $I(n) \neq \emptyset$ as $0 \in I(n)$ and we have

$$I(0) \subseteq I(1) \subseteq I(2) \subseteq \cdots$$

Define $R(n)$ to be the set of all (leading) coefficients of X^n for all elements of I of degree $\leq n$. Then $R(n)$ is an ideal of R and

$$R(0) \subseteq R(1) \subseteq R(2) \subseteq \cdots$$

As R is Noetherian, we must have $R(n) = R(N)$ for all $n \geq N$ for some N. Each $R(n) = Ra_{n1} + \cdots + Ra_{nm_n}$ say. There are polynomials $f_{nj}(X) = a_{nj}X^n +$ lower terms $\in I$. The set

$$\{f_{ij}(X) : 1 \leq i \leq N, 1 \leq j \leq m_i\}$$

is finite. Claim that they generate I as an ideal, which is left as an exercise. □

Remark. In computation it's usually important to be dealing with generating sets without too much redundancy. Such set are Gröbner basis and underlie a lot of algorithms in computer algebra and computational algebraic geometry.

> **Theorem 1.5.** *If R is Noetherian then $R[[X]]$ is Noetherian.*

We can either use a proof similar to that of the basis theorem but using trailing coefficients instead of leading coefficients, which is left as an exercise, or we can use a more interesting prooof. We use the following two results

> **Theorem 1.6** (Cohn). *A ring is Noetherian if and only if all its prime ideals are finitely generated.*

> **Lemma 1.7.** *Let P be a prime ideal of $R[[X]]$ and $\theta : R[[X]] \to R$ be the ring homomorphism taking a formal power series to its constant term. Then P is a finitely generated ideal if and only if $\theta(P)$ is.*

Proof of Theorem 1.6. Suppose R is not Notherian and so there are non-finitely generated ideals. Consider the set of all such ideals. It is non-empty by supposition. We can partially order the set by inclusion. The union of a chain of such ideals is also non-finitely generated. By Zorn's lemma, this set has maximal members. Let P be one such (note it is proper). Claim P is prime:

Proof. Suppose P is not prime, so there exist a, b with $ab \in P, a \notin P, b \notin P$. Then $P + Ra$ is an ideal strictly containing P so by maximality of P, $P + Ra$ is finitely generated, say by $p_1 + r_1a, \dots, p_n + r_na$. Set

$$J = \{r \in R : ra \in P\} \supseteq P + Rb \supsetneq P$$

so J is a finitely generated ideal. We show $P = Rp_1 + \dots Rp_n + Ja$ and so P is finitely generated, a contradiction: take $t \in P \subseteq P + Ra$. Then

$$t = u_1(p_1 + r_1a) + \dots + u_n(p_n + r_na)$$

for some $u_i \in R$. Hence

$$u_1r_1 + \dots + u_nr_n \in J$$

and so P is of the required form. □

□

Proof of Lemma 1.7. If P is finitely generated then $\theta(P)$ certainly is. Conversely, suppose $\alpha_1, \dots, \alpha_n$ generate $\theta(P)$. There are two cases:

1. if $X \in P$ then P is generated by $x, \alpha_1, \dots, \alpha_n$.
2. If $X \notin P$, let $f_1, \dots, f_n$ be power series in P with constant terms $\alpha_1, \dots, \alpha_n$. Claim $f_1, \dots, f_n$ generate P:

   Proof. Take $g \in P$. Then $g = a +$ higher terms where $a = \sum a_i\alpha_i$. Then $g - \sum a_if_i = Xg_1 \in P$ for some power series g_1. But $X \notin P$ so $g_1 \in P$ since P is prime. Similarly $g_1 = \sum b_if_i + Xg_2$ where $g_2 \in P$. Continuing gives

   $$h_i = a_i + b_iX + c_iX^2 + \dots \in R[[X]]$$

   for $1 \le i \le n$ satisfying

   $$g = h_1f_1 + \dots + h_nf_n.$$

   □

□

Example. $\mathbb{Z}[[X]]/(X - p)$ for some $p \in \mathbb{Z}$ is Noetherian. This is the ring of *p-adic integers.*

1.2 Localisation

Definition (multiplicatively closed subset)**.** S is a *multiplicatively closed subset* of R is

1. S is closed under multiplication,

2. $1 \in S$.

Define a relation $\equiv$ on $R \times S$ where $(r_1, s_1) \equiv (r_2, s_2)$ if and only if $(r_1 s_2 - r_2 s_1)x = 0$ for some $x \in S$. Check this is an equivalence relation. The class of (r, s) is written as $\frac{r}{s}$. The set of classes $S^{-1}R$ can be made into a ring via

$$\begin{aligned}\frac{r_1}{s_1} + \frac{r_2}{s_2} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_1} \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &= \frac{r_1 r_2}{s_1 s_2}\end{aligned}$$

There is a ring homomorphism

$$\begin{aligned}\theta : R &\to S^{-1}R \\ r &\mapsto \frac{r}{1}\end{aligned}$$

$S^{-1}R$ has the universal property

Lemma 1.8. *Let $\phi : R \to T$ be a ring homomorphism with $\phi(s)$ a unit in T for all $s \in S$. Then there is a unique ring homomorphism $\alpha : S^{-1}R \to T$ such that $\phi = \alpha \circ \theta$.*

Proof. For uniqueness, if $\alpha : S^{-1}R \to T$ with $\phi = \alpha \circ \theta$ then

$$\alpha(\frac{r}{s}) = \phi(r)\phi(s)^{-1}$$

is uniquely determined. For existence check this is well-defined. □

Example.

1. Field of fractions of an integral domain R: take $S = R \setminus \{0\}$ then $S^{-1}R$ is the fraction field of R.
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
$$S = 1 + I = \{1 + r : r \in I\}.$$
4. R_f where $S = \{1, f, f^2, \dots\}$.
5. If P is a prime ideal of R then take $S = R \setminus P$. Write R_P for $S^{-1}P$ in this case. The process of going from R to R_P is called *localisation.* The elements $\frac{r}{s} \in R_P$ with $r \in P$ form an ideal P_P of R_P. This is the unique maximal ideal of R_P: if $r \notin P$ then $r \in S$ so $\frac{r}{s}$ is a unit.

Definition (local ring)**.** A ring is *local* if it has a unique maximal ideal.

Example.

1. Let $R = \mathbb{Z}, P = (p)$ where p prime. Then $R_P = \{\frac{m}{n} : p \nmid n\} \subseteq \mathbb{Q}$, $P_P = \{\frac{m}{n} : p \nmid n, p | m\}$.

2. Let $R = k[X_1, \dots, X_n]$ which can be regarded as functions on k^n, $P = (X_1 - a_1, \dots, X_n - a_n)$. Then R_P is the subring of the rational functions that are defined at $(a_1, \dots, a_n) \in k^n$. The unique maximal ideals P_P consists of the rational functions that are zero at $(a_1, \dots a_n)$.

Similarly, given an R-module M, we can define an equivalence relation $\equiv$ on $M \times S$ for a multiplicatively closed subset $S \subseteq R$ where $(m_1, s_1) \equiv (m_2, s_2)$ if and only if $x(s_1 m_2 - s_2 m_1) = 0$ for some $x \in S$. This is an equivalence relation. The set of equivalence classes is denoted $S^{-1}M$.

$S^{-1}M$ can be regarded as an $S^{-1}R$-module via

$$\begin{aligned} \frac{m_1}{s_1} + \frac{m_2}{s_2} &= \frac{s_1 m_2 + s_2 m_1}{s_1 s_2} \\ \frac{r_1}{s_1} \cdot \frac{m_2}{s_2} &= \frac{r_1 m_2}{s_1 s_2} \end{aligned}$$

Write M_P where $S = R \setminus P$ for prime ideal P.

If $\theta : M_1 \to M$ is an R-module map. Then

$$\begin{aligned} S^{-1}\theta : S^{-1}M_1 &\to S^{-1}M \\ \frac{m_1}{s} &\mapsto \frac{\theta(m_1)}{s} \end{aligned}$$

is an $S^{-1}R$-module map and if $\phi : M \to M_2$ is an R-module map then

$$S^{-1}(\phi \circ \theta) = S^{-1}\phi \circ S^{-1}\theta.$$

Definition ((short) exact sequence)**.** A sequence of R-modules

$$\begin{tikzcd} M_1 \arrow[r, "\theta"] & M \arrow[r, "\phi"] & M_2 \end{tikzcd}$$

is *exact* at M if $\operatorname{im}\theta = \ker\phi$.

A *short exact sequence* is a sequence of the form

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\theta"] & M \arrow[r, "\phi"] & M_2 \arrow[r] & 0 \end{tikzcd}$$

which is exact at M_1, M, M_2.

Lemma 1.9 (localisation is exact)**.** *If*

$$\begin{tikzcd} M_1 \arrow[r, "\theta"] & M \arrow[r, "\phi"] & M_2 \end{tikzcd}$$

is exact at M then

$$\begin{tikzcd} S^{-1}M_1 \arrow[r, "S^{-1}\theta"] & S^{-1}M \arrow[r, "S^{-1}\phi"] & S^{-1}M_2 \end{tikzcd}$$

is exact at $S^{-1}M$, so we have an exact functor from the category of R-modules to the category of $S^{-1}R$-modules.

Proof. Since $\ker\phi = \operatorname{im}\theta$ we know $\phi\circ\theta = 0$ so

$$S^{-1}\phi \circ S^{-1}\theta = S^{-1}(0) = 0$$

and hence $\operatorname{im} S^{-1}\theta \subseteq \ker S^{-1}\phi$.

Now suppose $\frac{m}{s} \in \ker S^{-1}\phi$ so $\frac{\phi(m)}{s} = 0 \in S^{-1}M_2$ and hence there is $t \in S$ with $0 = t\phi(m) = \phi(tm)$ in M_2. So $tm \in \ker\phi = \operatorname{im}\theta$ so $tm = \theta(m_1)$ for some $m_1 \in M_1$. Hence in $S^{-1}M$,

$$\frac{m}{s} = \frac{tm}{ts} = \frac{\theta(m_1)}{ts} = S^{-1}\theta(\frac{m_1}{ts}) \in \operatorname{im} S^{-1}\theta.$$

□

Corollary 1.10. *Let $N \leq M$ then*

$$S^{-1}(M/N) = S^{-1}M/S^{-1}N.$$

Proof. Apply the exact functor S^{-1} to the short exact sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

to get

$$0 \longrightarrow S^{-1}N \longrightarrow S^{-1}M \longrightarrow S^{-1}(M/N) \longrightarrow 0$$

□

Remark. We can regard $S^{-1}N$ as a submodule of $S^{-1}M$.

Recall that we have a map $\theta : R \to S^{-1}R$. If I is an ideal then $S^{-1}I$ is an ideal of $S^{-1}R$.

Lemma 1.11.

1. *Every ideal $J \subseteq S^{-1}R$ is of the form $S^{-1}I$ for some ideal I of R.*
2. *There is a bijective correspondence*

$$\{\textit{prime ideals of } S^{-1}R\} \longleftrightarrow \{\textit{prime ideals disjoint from } S\}$$
$$S^{-1}P \hookleftarrow P$$
$$Q \mapsto \{r \in R : \frac{r}{1} \in Q\}$$

Example.

1. Let P be a prime ideal, $S = R\backslash P$. Then there is a correspondence between prime ideals of R_P and prime ideals of R contained in P. For example if $R = k[X_1,\dots,X_n]$ and P is a maximal ideal of the form $(X_1-a_1,\dots,X_n-a_n)$ for $(a_1,\dots,a_n) \in k^n$ then the prime ideals of R_P correspond to prime ideals R consisting only of elements which are 0 at $(a_1,\dots,a_n)$.

2. Let $R = \mathbb{Z}/6\mathbb{Z}, P = 2\mathbb{Z}/6\mathbb{Z}, S = \{1,3,5\}$ then $(2\mathbb{Z}/6\mathbb{Z})_P = 0$ since $2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$ and $3 \in S$. Thus $P_P = 0$. The short exact sequence
$$\begin{tikzcd} 0 \arrow[r] & 2\mathbb{Z}/6\mathbb{Z} \arrow[r] & \mathbb{Z}/6\mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$
becomes
$$\begin{tikzcd} 0 \arrow[r] & 0 \arrow[r] & R_P \arrow[r] & (\mathbb{Z}/2\mathbb{Z})_P \arrow[r] & 0 \end{tikzcd}$$
on localisation. So $R_P \cong (\mathbb{Z}/2\mathbb{Z})_P \cong \mathbb{Z}/2\mathbb{Z}$. Note that the bijective correspondence in part 2 of the lemma does not extend to all ideals, as 0 and P are distinct but 0_P and P_P are both zero.

Proof.

1. Let J be an ideal in $S^{-1}R$ and $\frac{r}{s} \in J$. Then $\frac{r}{1} \in J$. Let $I = \{r \in R : \frac{r}{1} \in J\}$. Then $r \in I$ and clearly $J \subseteq S^{-1}I$. If $r \in I$ then $\frac{r}{1} \in J$ and hence $\frac{r}{s} \in J$ for any $s \in S$. So $S^{-1}I \subseteq J$.

2. Let Q be a prime ideal of $S^{-1}R$ and let $P = \{r \in R : \frac{r}{1} \in Q\}$. Claim P is prime and does not meet S:

   Proof. Q is proper and hence P is proper. If $xy \in P$ then $\frac{xy}{1} \in Q$ and so either $\frac{x}{1} \in Q$ or $\frac{y}{1} \in Q$. Hence $x \in P$ or $y \in P$.
   If $s \in P \cap S$ then
   $$\frac{s}{1} \cdot \frac{1}{s} = \frac{1}{1} \in Q,$$
   contradicting properness of Q. □

   Conversely, suppose P is a prime ideal of R with $P \cap S = \emptyset$. Let $\frac{r_1}{s_1}, \frac{r_2}{s_2} \in S^{-1}R$ with $\frac{r_1 r_2}{s_1 s_2} \in S^{-1}P$. So $(r_1 r_2)s \in P$ for some $s \in S$. But since $S \cap P = \emptyset$, $s \notin P$ so $r_1 r_2 \in P$ and hence either $r_1 \in P$ or $r_2 \in P$. Thus $\frac{r_1}{s_1} \in S^{-1}P$ or $\frac{r_2}{s_2} \in S^{-1}P$. $S^{-1}P$ is also proper so it is prime.

   Furthermore $\frac{r}{1} \in S^{-1}P$ implies $s_1(rs - p) = 0$ for some $p \in P, s, s_1 \in S$, so $rss_1 \in P$. But $ss_1 \in S$ and hence $ss_1 \notin P$ so $r \in P$. Thus we have established the bijection.

□

Lemma 1.12. *If R is a Noetherian ring then $S^{-1}R$ is a Noetherian ring.*

Proof. Consider any chain of ideals
$$J_1 \subseteq J_2 \subseteq \cdots$$
of $S^{-1}R$. Set $I_k = \{r \in R : \frac{r}{1} \in J_k\}$ so $J_k = S^{-1}I_k$. So we get
$$I_1 \subseteq I_2 \subseteq \cdots$$
is a chain of ideals in R. R is Noetherian so $I_n = I_N$ for all $n \geq N$ for some N. Thus $J_n = S^{-1}I_n = S^{-1}I_N = J_N$ for all $n \geq N$. □

Exercise. Let P be a prime ideal and S a multiplicatively closed subset with $S \cap P = \emptyset$. Then $S^{-1}P$ is a prime ideal of $S^{-1}R$. Show

$$(S^{-1}R)_{S^{-1}P} \cong R_P.$$

In particular if Q is a prime ideal of R with $P \subseteq Q$, then taking $S = R \setminus Q$, we have

$$(R_Q)_{P_Q} \cong R_P.$$

We'll need this when dealing with chains of prime ideals, in particular when proving Krull's principal ideal theorem and generalisations.

Local properties

> **Definition** (local property)**.** A property $\mathcal{P}$ of a ring R (or an R-module M) is *local* if R (or M) has property $\mathcal{P}$ if and only if R_P (or M_P) has property $\mathcal{P}$ for all prime ideals of R.

> **Lemma 1.13.** *For an R-module M, TFAE:*
>
> 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.
>
> *Therefore being zero is a local property.*

Proof. $1 \implies 2 \implies 3$ easily. Suppose $M \neq 0$. We'll show there exists maximal ideal Q with $M_Q \neq 0$. Take $m \in M$ nonzero. Consider the annihilator

$$\operatorname{Ann}_R(m) = \{r \in R : rm = 0\}$$

which is a proper ideal and we have $R/\operatorname{Ann}_R(m) \cong Rm \leq M$. Take maximal ideal Q containing $\operatorname{Ann}_R(m)$ and we have a surjective map $\phi : M_1 \cong R/\operatorname{Ann}_R(m) \to R/Q$ so we have a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker\phi \arrow[r] & M_1 \arrow[r, "\phi"] & R/Q \arrow[r] & 0 \end{tikzcd}$$

Localise at Q,

$$\begin{tikzcd} 0 \arrow[r] & (\ker\phi)_Q \arrow[r] & M_{1Q} \arrow[r] & (R/Q)_Q \arrow[r] & 0 \end{tikzcd}$$

is exact. But $(R/Q)_Q \cong R_Q/Q_Q \neq 0$ and we deduce $M_{1Q} \neq 0$. However we observed we could regard M_{1Q} as a submodule of M_Q and so $M_Q \neq 0$ for this choice of maximal ideal Q. □

Example sheet 1 question 7 uses this to prove that

> **Proposition 1.14.** *Let $\phi : M \to N$ be an R-module map. Then TFAE*
>
> 1. ϕ *is injective.*
> 2. $\phi_P : M_P \to N_P$ *is injective for all prime ideals* P *of* R.

> *3. $\phi_Q : M_Q \to N_Q$ is injective for all maximal ideals Q of R.*

Similarly for surjectivity.

1.3 Tensor products

The whole point is to study multilinear maps via a consideration of linear maps.

> **Definition** (bilinear map)**.** Let L, M, N be R-modules. $\phi : M \times N \to L$ is *R-bilinear* if
>
> 1. $\phi(r_1 m_1 + r_2 m_2, n) = r_1\phi(m, n) + r_2\phi(m, n)$.
> 2. $\phi(m, r_1 n_1 + r_2 n_2) = r_1\phi(m, n_1) + r_2\phi(m, n_2)$.

If $\phi : M \times N \to T$ is R-bilinear and $\theta : T \to L$ is R-linear then $\theta \circ \phi$ is R-bilinear and we get

$$\phi^* : \mathrm{Hom}_R(T, L) \to \mathrm{Bilin}_R(M \times N, L).$$

ϕ is *universal* if ϕ^* is a one-to-one correspondence.

> **Lemma 1.15.**
>
> 1. *Given M, N there is an R-module T and a universal map $\phi : M \times N \to T$.*
> 2. *Given two such $\phi_1 : M \times N \to T_1, \phi_2 : M \times N \to T_2$, there is a unique isomorphism $\beta : T_1 \to T_2$ with $\beta \circ \phi_1 = \phi_2$.*

> **Definition** (tensor product)**.** T is the *tensor product* over R of M and N, written $M \otimes N$.

Proof. Let F be the free R-module on generators $e_{(m,n)}$ labelled by pairs $(m, n) \in M \times N$. Let X be the R-submodule of F generated by all elements of the form

$$e_{(r_1 m_1 + r_2 m_2, n)} - r_1 e_{(m_1, n)} - r_2 e_{(m_2, n)}$$
$$e_{(m, r_1 n_1 + r_2 n_2)} - r_1 e_{(m, n_1)} - r_2 e_{(m, n_2)}$$

Set $T = F/X$ and write $m \otimes n$ for the image of the element $e_{(m,n)}$. Set

$$\begin{aligned}\phi : M \times N &\to T \\ (m, n) &\mapsto m \otimes n\end{aligned}$$

Note T is generated as an R-module by $m \otimes n$ and ϕ is bilinear. Any map $\alpha : M \times N \to L$ extends to an R-module map

$$\begin{aligned}\overline{\alpha} : F &\to L \\ e_{(m,n)} &\mapsto \alpha(m, n)\end{aligned}$$

If α is bilinear then $\overline{\alpha}$ is zero on X and so $\overline{\alpha}$ induces a map $\alpha' : T \to L$. α' is uniquely defined by this.

Uniqueness follows from universality. □

Warning: not all elements of $M \otimes N$ are of the form $m \otimes n$. In general, an element of $M \otimes N$ is of the form $\sum_{i=1}^{s} m_i \otimes n_i$.

Usually if R is unambiguous one writes $M \otimes N$. If not then write $M \otimes_R N$.

Example. If $R = k$ a field and M, N are vector spaces of dimension m and n then $M \otimes_k N$ is a vector space of dimension mn.

Remark. One may also define tensor products over non-commutative rings but in this case M needs to be a right R-module and N a left R-module in order to define $M \otimes_R N$. $M \otimes_R N$ is an additive group but there may not be any R-module structure. For the construction one takes a free $\mathbb{Z}$-module on $e_{(m,n)}$ and X is generated by

$$\begin{gathered} e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)} \\ e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)} \\ e_{(mr,n)} - e_{(m,rn)} \end{gathered}$$

If M is an (R, S)-bimodule (i.e. it is a left R-module and a right S-module and the two actions commute) and N is an (S, T)-bimodule for rings R, S, T not necessarily commutative, then $M \otimes_S N$ is an (R, T)-bimodule.

Lemma 1.16. *There exist unqiue R-module isomorphisms*

1.

$$\begin{aligned} M \otimes N &\to N \otimes M \\ m \otimes n &\mapsto n \otimes m \end{aligned}$$

2.

$$\begin{aligned} (M \otimes N) \otimes L &\to M \otimes (N \otimes L) \\ (m \otimes n) \otimes \ell &\mapsto m \otimes (n \otimes \ell) \end{aligned}$$

3.

$$\begin{aligned} (M \oplus N) \otimes L &\to (M \otimes L) \oplus (N \otimes L) \\ (m + n) \otimes L &\mapsto m \otimes \ell + n \otimes \ell \end{aligned}$$

4.

$$\begin{aligned} R \otimes M &\to M \\ r \otimes m &\mapsto rm \end{aligned}$$

Proof. Exercises. □

Restriction of scalars If $\phi : R \to T$ is a ring homomorphism and N is a T-module, we can regard it as an R-module via

$$rn = \phi(r)n$$

for $r \in R, n \in N$. In particular T itself can be regarded as an R-module.

Extension of scalars Given an R-module M, we can form $T \otimes_R M$ which can be regarded as a T-module via

$$t_1(t_2 \otimes m) = (t_1 t_2) \otimes m.$$

Example. Localisation is an example of extension of scalars. Given an R-module M and multiplicatively closed subset S of R, there is a unique isomorphism $f : S^{-1}R \otimes_R M \to S^{-1}M$ since there is a bilinear map $S^{-1}R \times M \to S^{-1}M, (\frac{r}{s}, m) \mapsto \frac{rm}{s}$ and universality yields the map f. Check this is an isomorphism.

Tensor products of maps Given R-module maps $\theta : M_1 \to M_2, \phi : N_1 \to N_2$, then we can define an R-module

$$\begin{aligned}\theta \otimes \phi : M_1 \otimes N_1 &\to M_2 \otimes N_2 \\ m_1 \otimes n_1 &\mapsto \theta(m_1) \otimes \phi(n_1)\end{aligned}$$

This is induced by the bilinear map

$$\begin{aligned}M_1 \times N_1 &\to M_2 \otimes N_2 \\ (m_1, n_1) &\mapsto \theta(m_1) \otimes \phi(n_1)\end{aligned}$$

Given a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\theta"] & M \arrow[r, "\phi"] & M_2 \arrow[r] & 0 \end{tikzcd}$$

by tensoring with N we can form a sequence

$$\begin{tikzcd} 0 \arrow[r] & N \otimes M_1 \arrow[r, "\mathrm{id} \otimes \theta"] & N \otimes M \arrow[r, "\mathrm{id} \otimes \phi"] & N \otimes M_2 \arrow[r] & 0 \end{tikzcd}$$

where $\mathrm{id} : N \to N$ is the identity.

We saw that when $N = S^{-1}R$ then localisation is exact so we have a short exact sequence. However, in general it is not exact.

Example. Let $R = \mathbb{Z}$ and a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "2"] & \mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

set $N = \mathbb{Z}/2\mathbb{Z}$, we observe that

$$N \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$$

so we have a sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r, "\mathrm{id} \otimes 2"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

with $\mathrm{id} \otimes 2 = 0$ so we do not have exactness on the left hand side. So $N \otimes_{\mathbb{Z}} -$ does not preserve exactness. However, it is indeed right exact. This is the starting point of homology theory.

> **Definition** (flat module)**.** N is a *flat* R-module if $N \otimes_R -$ preserves exactness of all short exact sequences.

Example. $S^{-1}R$ is a flat R-module for all multiplicatively closed subsets S of R. In particular R itself is a flat R-module. Moreoever R^n is flat.

> **Definition** (algebra)**.** Given $\phi : R \to T$ a ring homomorphism, we say T is an *R-algebra*.

> **Definition** (tensor product of algebras)**.** Given R-algebras $\phi_i : R \to T_i$ for $i = 1, 2$, we can define the *tensor product over* R by endowing $T_1 \otimes_R T_2$ with a product
>
> $$(t_1 \otimes t_2)(t_1' \otimes t_2') = t_1 t_1' \otimes t_2 t_2'$$
>
> and
>
> $$\begin{aligned} R &\to T_1 \otimes_R T_2 \\ r &\mapsto \phi_1(r) \otimes 1 = 1 \otimes \phi_2(r) = r(1 \otimes 1) \end{aligned}$$
>
> This is well-defined and $1 \otimes 1$ is the multiplicative identity.

Example.

1. Let $R = k$ be a field. Then $k[X_1] \otimes_k k[X_2] \cong k[X_1, X_2]$.
2. $\mathbb{Q}[X]/(X^2 + 1) \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}[X]/(X^2 + 1)$.
3. $k[X_1]/(f(X_1)) \otimes_k k[X_2]/(g(X_2)) \cong k[X_1, X_2]/(f(X_1), g(X_2))$.

2 Ideal structure

Throughout this chapter R is commutative with a 1.

2.1 Nilradical & Jacobson radical

> **Lemma 2.1.** *The set of nilpotent elements of a commutative ring R form an ideal $\mathcal{N}(R)$ and $R/\mathcal{N}(R)$ has no nilpotent elements.*

Proof. Exercise. □

> **Definition** (nilradical)**.** The ideal $\mathcal{N}(R)$ is the *nilradical* of R.

> **Lemma 2.2** (Krull)**.** *$\mathcal{N}(R)$ is the intersection of all the 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 some m. P prime implies that $x \in P$ so $x \in I$. If x is not nilpotent then consider $S = \{1, x, x^2, \dots\}$ which does not contain 0. Localise to get $S^{-1}R = R_x$ which is not zero. Take a maximal ideal of R_x. By prime ideal correspondence this maximal ideal of R_x corresponds to a prime ideal P with $P \cap S = \emptyset$. In particular $x \notin P$ so $x \notin I$. Thus $I = \mathcal{N}(R)$. □

> **Definition** (radical)**.** For an ideal I of R its *radical* is
> $$\sqrt{I} = \{x : x^m \in I \text{ for some } m\}.$$

Note that $\sqrt{I}/I = \mathcal{N}(R/I)$.

> **Definition** (Jacobson radical)**.** The *Jacobson radical* of R is the intersection of all the maximal ideals of R, written $\operatorname{Jac} R$.

Thus
$$\mathcal{N}(R) = \bigcap_{\text{prime}} P \subseteq \bigcap_{\text{maximal}} P = \operatorname{Jac} R.$$

In general we don't have equality. For example if R is a local ring with unique maximal ideal P then $\operatorname{Jac} R = P$. But if $R = \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ which is an integral domain then it does not have nonzero nilpotent elements so $\mathcal{N}(R) = (0)$.

> **Proposition 2.3** (Nakayama's lemma)**.** *Let M be a finitely generated R-module. Then $M = 0$ if and only if $\operatorname{Jac}(R)M = M$.*

Proof. Only if is trivial. Suppose $M \neq 0$. We consider the family of proper submodules. If $m_1, \dots, m_n$ is a generating set for M, these are the submodules that do not contain all of $m_1, \dots, m_n$. Zorn's lemma applies to this family and so we have a maximal member, a maximal submodule M_1. Thus M/M_1 is a simple (or irreducible) module (i.e. any non-zero element generates M/M_1). Take $\overline{m}$ to be nonzero in M/M_1, then $R\overline{m} \cong R/\operatorname{Ann}_R(\overline{m})$ and $Q = \operatorname{Ann}_R(\overline{m})$

is a maximal ideal of R. Thus $QM \leq M_1 \lneq M$ but $\operatorname{Jac} R$ is the intersection of all maximal ideals so

$$\operatorname{Jac}(R)M \leq QM \lneq M$$

so $\operatorname{Jac}(R)M \neq M$. □

Remark.

1. This is not the normal proof you find in A-M, but it generalises to non-commutative rings.

2. For finitely generated R-modules, $M = 0$ if and only if $QM = M$ for all maximal ideal Q.

Exercise. Find a ring R and a non-zero R-module M such that $QM = M$ for all maximal ideals Q.

The name *Nullstellensatz* is attached to a family of results.

Theorem 2.4 (weak Nullstellensatz). *Let k be a field and T a finitely generated k-algebra. Let Q be a maximal ideal. Then T/Q is a finite field extension of k. In particular if k is algebraically closed and $T = k[X_1, \dots, X_n]$ the polynomial algebra then Q is of the form $(X_1 - a_1, \dots, X_n - a_n)$ for some $(a_1, \dots, a_n) \in k^n$.*

We need two results.

Lemma 2.5 (Artin, Tate). *Let $R \subseteq S \subseteq T$ be rings. Suppose R is Noetherian and T is generated as a ring by R and $t_1, \dots, t_n$, say. Suppose moreover T is a finitely generated S-module. Then S is generated as a ring by finitely many elements.*

Proof. Let T be generated by $x_1, \dots, x_m$ as an S-module. For each t_i we may write $t_i = \sum s_{ij} x_j$ for $s_{ij} \in S$ and $x_i x_j = \sum s_{ijk} x_k$ for $s_{ijk} \in S$. Let S_0 be the subring of S generated by R and all the s_{ij}, s_{ijk}. Then $R \subseteq S_0 \subseteq S$. Any element of T is a "polynomial" in the t_i's with coefficients in R. Thus each element of T is a linear combination of the x_j's with coefficients in S_0. Thus T is a finitely generated S_0-module.

S_0 is Noetherian as it is a finitely generated R-algebra and R is Noetherian. Hence T is a Noetherian S_0-module. But 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 S is generated as a ring by R and finitely many elements. □

Proposition 2.6. *Let k be a field and R be a finitely generated k-algebra. If R is a field then it is a finite field extension of k.*

Proof. Suppose R is generated by k and $x_1, \dots, x_n$ and is a field. If R is algebraic over k then it is a finite field extension. Suppose for contradiction it is not. We reorder the x_i's so that $x_1, \dots, x_m$ are algebraically independent and $x_{m+1}, \dots, x_n$ are algebraically dependent of $F = k(x_1, \dots, x_n)$. Hence R is a finite field extension of F and thus a finitely generated F-module (i.e. an

F-vector space). Apply the lemma to $k \subseteq F \subseteq R$ and it follows that F is a finitely generated k-algebra.

Suppose F is generated by k and $q_1, \dots, q_t$ where $q_i = \frac{f_i}{g_i}$ where $f_i, g_i \in k[x_1, \dots, x_n], g_i \neq 0$. There is a polynomial h which is prime to $g_1, \dots, g_t$, for example $g_1 \cdots g_t + 1$, then $\frac{1}{h}$ is not in the ring generated by k and the q_i's, absurd. Thus $m = 0$. □

Proof of weak Nullstellensatz. Let Q be a maximal ideal of T, a finitely generated k-algebra. Set $R = T/Q$ and apply the proposition to get R a finite field extension of k.

Now if $T = k[X_1, \dots, X_n]$ and k is algebraically closed then $T/Q \cong k$. Let $\pi : T \to k$ with $\ker \pi = Q$. But $\ker \pi = (X_1 - \pi(X_1), \dots, X_n - \pi(X_n))$. Hence Q is of the form required. □

Now let $k = \mathbb{C}$. In the introduction we get a bijection

$$\{\text{radical ideals of } \mathbb{C}[x_1, \dots, x_n]\} \longleftrightarrow \{\text{algebraic subsets of } \mathbb{C}^n\}$$

The weak Nullstellensatz says that all the maximal ideals of the complex polynomial algebra are of the form $Q_{(a_1, \dots, a_n)} = (x_1 - a_1, \dots, x_n - a_n)$. We can restate the bijection:

$$\begin{aligned}
\{\text{radical ideals of } \mathbb{C}[x_1, \dots, x_n]\} &\longleftrightarrow \{\text{algebraic subsets of } \mathbb{C}^n\} \\
I &\mapsto \{(a_1, \dots, a_n) \in k^n : Q_{(a_1, \dots, a_n)} \supseteq I\} \\
\bigcap_{(a_1, \dots, a_n) \in \mathcal{S}} Q_{(a_1, \dots, a_n)} &\mapsfrom \mathcal{S}
\end{aligned}$$

Theorem 2.7. *Let k be a field and R a finitely generated k-algebra. Then $\mathcal{N}(R) = \operatorname{Jac} R$. Thus if I is a radical ideal of $k[X_1, \dots, X_n]$ and $R = k[X_1, \dots, X_n]/I$ then the intersection of the maximal ideals of R is zero, and thus the intersection of the maximal ideals of $k[X_1, \dots, X_n]$ containing I is equal to I.*

We'll need the following for the proof.

Lemma 2.8. *Let k be a field, R be an integral domain which is finite-dimensional as a k-vector space. Then R is a field.*

Proof. Take $r \in R$ nonzero. Then $\phi_r : R \to R, x \mapsto rx$ is k-linear and is injective because R is an integral domain. By rank-nullity θ_r is surjective so $1 \in \operatorname{im} \theta_z$. Thus there is an $x \in R$ such that $rx = 1$, so r has an inverse and thus R is a field. □

Proof of Theorem 2.7. Let P be a prime ideal of R, $s \in R \setminus P$. Let $S = \{1, s, s^2, \dots\}$. Localise with respect to S so we have a canonical map $\theta : R \to S^{-1}R$. $S^{-1}R$ is a finitely generated as a k-algebra since it is generated by $\theta(R)$ and $\frac{1}{s}$.

Take a maximal ideal Q of $S^{-1}R$ containing $S^{-1}P$. By Proposition 2.6, $S^{-1}R/Q$ is a finite field extension of k. Q corresponds to a prime ideal $P_1 = \theta^{-1}(Q) = \{r \in R : \frac{r}{1} \in Q\}$ of R containing P and not intersecting S. θ

induces an embedding $R/P_1 \to S^{-1}R/Q$ and as $S^{-1}R/Q$ is a finite-dimensional k-vector space, so is R/P_1. Thus R/P_1 is a field and thus P_1 is a maximal ideal containing P but not intersecting S, so $\bigcap_{P' \subseteq P \text{ maximal}} P' = P$. It follows that $\mathcal{N}(R) = \operatorname{Jac} R$. □

2.2 Minimal and associated primes

Lemma 2.9. *If R is Noetherian then every ideal I contains a power of its radical $\sqrt{I}$. In particular $\mathcal{N}(R)$ is nilpotent, i.e. $\mathcal{N}(R)^k = 0$ for some k.*

Proof. Suppose $x_1, \dots, x_n$ generate $\sqrt{I}$ as an ideal. Then $x_i^{m_i} \in I$ for some m_i for each i. Let $m = \sum (m_i - 1) + 1$, then $(\sqrt{I})^m \subseteq I$ since $(\sqrt{I})^m$ is generated by elements of the form $\prod x_i^{r_i}$ where $\sum r_i = m$, and at least one of the r_i has to be $\geq m_i$ so all these products are in I. □

Lemma 2.10. *If R is Noetherian then a radical ideal is the intersection of finitely many primes.*

Proof. Suppose not then let I be a maximal member of the set of radical ideals which aren't an intersection of finitely many primes. Claim that I is itself prime, therefore contradiction.

Proof. Suppose not, then there are ideals J_1, J_2 with $J_1 J_2 \subseteq I$ but $J_1 \nsubseteq I, J_2 \nsubseteq I$. By taking $J_i = J_i + I$, wlog $I \subsetneq J_i$. Maximality of I forces $\sqrt{J_1}, \sqrt{J_2}$ to be intersections of finitely may primes, say $\sqrt{J_1} = Q_1 \cap \dots \cap Q_s$, $\sqrt{J_2} = Q_1' \cap \dots \cap Q_t'$ where Q_i, Q_j' are primes. Set

$$J = Q_1 \cap \dots \cap Q_s \cap Q_1' \cap \dots \cap Q_t' = \sqrt{J_1} \cap \sqrt{J_2}$$

and $J^{m_1} \subseteq J_1, J^{m_2} \subseteq J_2$ for some m_1, m_2. Hence $J^{m_1 + m_2} \subseteq J_1 J_2 \subseteq I$. But I is radical so $J \subseteq I$. However all the Q_i, Q_j' contain I so $I \subseteq J$, so equality. Absurd. □

□

Now suppose I is an ideal of a Noetherian ring R. By the lemma $\sqrt{I} = P_1 \cap \dots \cap P_n$ for some primes P_i. We may remove any P_i if it contains some of the others so we may assume $P_i \nsubseteq P_j$ for $i \neq j$. Moreover if P is any prime ideal containing I then

$$P_1 \cdots P_n \subseteq P_1 \cap \dots \cap P_n = \sqrt{I} \subseteq P$$

so $P_i \subseteq P$ for some P.

Definition (minimal prime)**.** The *minimal primes* over I are the minimal members of primes containing I.

Lemma 2.11. *Let I be an ideal of a Noetherian ring R. Then the set of minimal primes over I is finite. Moreover their intersection is $\sqrt{I}$ and I contains some finite product of the minimal primes (perhaps with repetition).*

Definition (associated prime)**.** Let R be a Noetherian ring and let M be a finitely generated R-module. A prime ideal P is an *associated prime* of M if $P = \mathrm{Ann}_R(m)$ for some $m \in M$. We write $\mathrm{Ass}(M)$ for the set of associated primes of M.

Definition (primary submodule)**.** A submodule N of M is *P-primary* if $\mathrm{Ass}(M/N) = \{P\}$.

Remark.

1. If P is obvious from the context then we just say it is primary.
2. There is an alternative definition of P-primary submodules, which is on example sheet 2.

Our aim is to show that for R Noetherian, non-zero finitely generated R-module M, $\mathrm{Ass}(M)$ is non-empty and finite, and in the case of $M = R/I$, $\mathrm{Ann}(R/I) \supseteq \{\text{minimal primes over } I\}$. However we don't necessarily have equality here.

Example. Let $R = k[x, y], Q = (x, y) \supsetneq P = (x)$ and $I = PQ$. Then $\mathrm{Ass}(R/I) = \{P, Q\}$ but the only prime over I is P. Note that I is not primary. But $I = (x^2, xy, y^2) \cap (x)$, with $(x^2, xy, y^2) = Q^2$ is Q-primary, (x) is P-primary. This is an example of primary decomposition.

Theorem 2.12 (primary decomposition)**.** *Suppose R is Noetherian, M a finitely generated R-module and N a submodule of M. Then there exist $N_1, \dots, N_s$ with $N_1 \cap \dots \cap N_s = N$ and $\mathrm{Ass}(M/N_i) = \{P_i\}$ for prime ideal P_i all distinct.*

In particular given an ideal $I \subsetneq R$ then $I = J_1 \cap \dots \cap J_s$for some P_i-primary ideal J_i. If one takes a minimal decomposition like this then the P_i's appearing are precisely the associated primes of I.

Proof. Atiyah and MacDonald. □

In practice, one needs to know $\mathrm{Ass}(M)$ or $\mathrm{Ass}(R/I)$ rather than the primary decomposition. Instead you tend to consider localisations.

Lemma 2.13. *If $\mathrm{Ann}(M) = \{r : rm = 0 \text{ for all } m \in M\} = \bigcap_{m \in M} \mathrm{Ann}(m)$ for a finitely generated M is a prime ideal P, then $P \in \mathrm{Ass}(M)$.*

Proof. Let $m_1, \dots, m_s$ be a generating set for M and $I_i = \mathrm{Ann}(m_i)$. Then $\prod I_j$ annhilates each m_j so $\prod I_j \subseteq \mathrm{Ann}(M) = P$ by supposition. Hence some $I_j \subseteq P$ since P is prime. However $I_j = \mathrm{Ann}(m_j) \supseteq \mathrm{Ann}(M) = P$ so $P = I_j$ for some j so $P = \mathrm{Ann}(m_j) \in \mathrm{Ass}(M)$. □

Lemma 2.14. *Suppose M is a non-zero module over a Noetherian ring R and Q is maximal among all annihilators of non-zero elements of M. Then Q is prime and so $Q \in \operatorname{Ass}(M)$.*

So $\operatorname{Ass}(M)$ for non-zero M is non-empty.

Proof. Take such a Q and suppose $Q = \operatorname{Ann}(m)$ with $r_1r_2 \in Q, r_2 \notin Q$. We are going to show $r_1 \in Q$. $r_1r_2m = 0$ so $r_1 \in \operatorname{Ann}(r_2m)$. As $r_2 \notin Q$, $r_2m \neq 0$. But $Q \subseteq \operatorname{Ann}(r_2m)$. Hence Q and r_1 lie in $\operatorname{Ann}(r_2m)$ so by maximality of Q, $r_1 \in Q$. □

Lemma 2.15. *For a non-zero finitely generated R-module M with R Noetherian, there is a chain of submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_s = M$$

with each factor $M_j/M_{j-1} \cong R/P_j$ for some prime P_j not necessarily distinct.

Proof. There is $m_1 \in M$ non-zero with $\operatorname{Ann}(m_1) = P_1$ for some P_1. Set $M_1 = Rm_1$ and thus $M_1 \cong R/P_1$. Repeat for M/M_1 to find M_2 with $M_2/M_1 \cong R/P_2$. M is Noetherian and so the process terminates. □

Lemma 2.16. *If $N \leq M$ then $\operatorname{Ass}(M) \subseteq \operatorname{Ass}(N) \cup \operatorname{Ass}(M/N)$.*

Proof. Suppose $P = \operatorname{Ann}(m)$ for some $m \in M$ and P is prime. Let $M_1 = Rm \cong R/P$. Note that for any $m_1 \in M_1$ nonzero, $\operatorname{Ann}(m_1) = P$. If $M_1 \cap N \neq 0$ then there exists $m_1 \in M_1 \cap N$ non-zero with $\operatorname{Ann}(m_1) = P$ so $P \in \operatorname{Ass}(N)$. If $M_1 \cap N = 0$ then the image of M_1 in M/N is isomorphic to $M_1 \cong R/P$ and $\operatorname{Ann}(m + N) = P$. Thus $P \in \operatorname{Ass}(M/N)$. □

Lemma 2.17. *Suppose M is a finitely generated module over a Noetherian ring R then $\operatorname{Ass}(M)$ is finite.*

Proof. Use Lemma 2.16 inductively on the chain obtained in Lemma 2.15 $\operatorname{Ass}(M) \subseteq \{P_1, \dots, P_s\}$ for the P_i's. □

Lemma 2.18. *Minimal primes over I are in $\operatorname{Ass}(R/I)$.*

Proof. Recall that there is a product of minimal primes over I, perhaps with repetition, contained in I, so $P_1^{s_1} \cdots P_n^{s_n} \subseteq I$ with $P_i \nsubseteq P_j$ for $i \neq j$. Let $M = (P_2^{s_2} \cdots P_n^{s_n} + I)/I$ and consider $J = \operatorname{Ann}(M)$. Clearly $J \supseteq P_1^{s_1}$. Also $JP_2^{s_2} \cdots P_n^{s_n} \subseteq I \subseteq P_1$ and since P_1 is a minimal prime over I and it is distinct from $P_2, \dots, P_n$, so must have $J \subseteq P_1$.

Note that $M \neq 0$ since $J \subseteq P_1 \subsetneq R$ so we have a chain of submodules of M

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_t = M$$

with each factor $M_j/M_{j-1} \cong R/Q_j$ with Q_j prime. But $P_1^{s_1}$ annihilates M and hence each factor M_j/M_{j-1}, so primality of Q_j ensures $P_1 \subseteq Q_j$ for all j. Since $\prod Q_j \subseteq J \subseteq P_1$, have $Q_j \subseteq P_1$ for some j and hence $Q_j = P_1$. Now pick least j with $Q_j = P_1$ and thus $\prod_{k<j} Q_k \nsubseteq P_1$. Take $x \in M_j \setminus M_{j-1}$. If $j = 1$ then $\mathrm{Ann}(x) = Q_1 = P_1$ and so $P_1 \in \mathrm{Ass}(R/I)$. If $j > 1$ then pick $r \in (\prod_{k<j} Q_k)\backslash P_1$. Note $r(sx) = 0$ for any $s \in P_1 = Q_j$ so $s(rx) = 0$ and $P_1 \subseteq \mathrm{Ann}(rx)$. However $rx \notin M_{j-1}$ since $r \notin P_1$ and $\mathrm{Ann}(rx + M_{j-1}) = P_1$. Hence $\mathrm{Ann}(rx) \subseteq P_1$ so equality. This shows that $P_1 \in \mathrm{Ass}(M) \subseteq \mathrm{Ass}(R/I)$. □

3 Dimension

3.1 Krull dimension

In this chapter all rings are commutative with a 1.

Definition (prime spectrum)**.** The *prime spectrum* of R is

$$\operatorname{Spec} R = \{P : P \text{ prime ideal of } R\}.$$

Definition (length)**.** The *length* of a chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

is n. Note the numbering starts at 0.

Definition (Krull dimension)**.** The *(Krull) dimension* $\dim R$ of R is defined as the supremum of n where there is a chain of prime ideals of length n, if this exists, and ∞ otherwise.

Definition (height)**.** Then *height* $\operatorname{ht}(P)$ of $P \in \operatorname{Spec} R$ is the supremum of n where there is a strict chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P$$

if this exists.

Note. The correspondence between primes of R_P and the prime ideals of R contained in P tells us that $\operatorname{ht}(P) = \dim R_P$.

Example.

1. We'll see later that being Artinian (i.e. satisfying DCC) is equivalent to being Noetherian of dimension 0.
2. $\dim \mathbb{Z} = 1$ and $\dim k[X] = 1$. These are examples of *Dedekind domains*, i.e. integrally closed dimension 1 Noetherian integral domains.
3. $\dim k[X_1, \dots, X_n] \geq n$ since we can write down a chain of prime ideals

$$0 \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \cdots, X_n)$$

In fact, we'll prove it has dimension n.

Lemma 3.1. *The height one primes of $k[X_1, \dots, X_n]$ are precisely those of the form (f) for prime element f.*

Proof. Recall Kaplansky from example sheet 1: $k[X_1, \dots, X_n]$ is a UFD and so each non-zero prime contains a non-zero principal prime ideal, so a height one prime is principal. Conversely if (f) is a principal prime ideal and $0 \subsetneq P \subseteq (f)$ for prime ideal P then there exists principal prime (g) such that $0 \subsetneq (g) \subseteq P \subseteq (f)$. Since f, g are prime elements we have equality. □

Remark. In general for a Noetherian R the height 1 primes are precisely the minimal primes over principal ideal. This is Krull's principal ideal theorem. A generalisation of this theorem shows that any prime ideal has finite height. Thus the dimension of any Noetherian local ring is finite.

3.2 Integral extensions

Definition (integral element)**.** Suppose $R \subseteq T$ are rings. $x \in T$ is *integral over* R if it satisfies a monic polynomial with coefficients in R.

T is *integral over* R if x is integral over R for all $x \in T$.

Our next aim is to discuss the relationship between $\operatorname{Spec} R$ and $\operatorname{Spec} T$ when T is integral over R.

Lemma 3.2. *TFAE:*

1. *$x \in T$ is integral over R.*
2. *$R[x]$, the subring of T generated by R and x, is a finitely generated R-module.*
3. *$R[x]$ is contained in a subring T_1 of T where T_1 is a finitely generated R-module.*

Proof. Left to show $3 \implies 1$. Consider multiplication by x in T_1. Take $y_1, \dots, y_m \in T_1$, an R-module generating set for T_1. Suppose $xy_i = \sum r_{ij} y_j$ so $\sum (x\delta_{ij} - r_{ij}) y_j = 0$. Multiply by the adjugate of the matrix $(A_{ij}) = (x\delta_{ij} - r_{ij})$ to deduce $(\det A) y_j = 0$ for all j. But 1 is a linear combination of the y_j and so we deduce $\det A = 0$. But this gives a monic polynomial with coefficients in R and satisfied by x. □

Lemma 3.3. *If $x_1, \dots, x_n \in T$ are integral over R then $R[x_1, \dots, x_n]$, the subring of T generated by R and $x_1, \dots, x_m$, is a finitely generated R-module.*

Proof. Induction. □

Lemma 3.4. *The set $T_1 \subseteq T$ of elements integral over R form a subring containing R.*

Proof. Clearly if $x \in R$ it is integral over R. If $x, y \in T_1$ then $x \pm y, xy$ lie in $R[x, y]$ which is finitely generated as an R-module so are in T_1. □

Definition (integral closure)**.** T_1 is the *integral closure* of R in T. If $T_1 = R$ we say R is *integrally closed* in T. If $T_1 = T$ then T is integral over R. If R is an integral domain then we say R is integrally closed if it is closed in its fractional field.

Example. $\mathbb{Z}$ and $k[X_1, \dots, X_n]$ are integrally closed. In a number field the ring of integers is the integral closure of $\mathbb{Z}$ in the number field.

Remark.

1. Being integrally closed is a local property of integral domains. See example sheet.
2. We'll prove Noether's normalisation lemma for a finitely generated k-algebra T, which says that T has a subalgebra R isomorphic to a polynomial algebra and T is integral over R. Furthermore we'll see that if T is a finitely generated algebra which is an integral domain then its integral closure T' of T in its fractional field is a finitely generated T-module. Then we have maps of prime spectrums

   $$\operatorname{Spec} T' \to \operatorname{Spec} T \to \operatorname{Spec} R$$

   given by restrictions. The geometric property equivalent to integrally closed is normality. We'll see that those restriction maps are surjective and their fibres are finite.
3. Integral closure of an integral domain has an alternative characterisation as the intersection of all valuation rings containing R.

Now suppose $R \subseteq T$ then we have a map $\operatorname{Spec} T \to \operatorname{Spec} R, Q \mapsto Q \cap R$. Our aim is to understand the behaviour of chains in $\operatorname{Spec} T$ under this restriction.

Lemma 3.5. *If $R \subseteq T \subseteq T'$ with T integral over R, T' integral over T then T' is integral over R.*

Proof. Exercise. □

Lemma 3.6. *Let $R \subseteq T$ with T integral over R then*

1. *if $J \subseteq T$ then T/J is integral over $R/(J \cap R)$ (by identifying $R/(J \cap R)$ with $(R+J)/J \subseteq T/J$).*
2. *if S is a multiplicatively closed subset of R then $S^{-1}T$ is integral over $S^{-1}R$.*

Proof.

1. If $x \in T$ then $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$ for some $r_i \in R$. Modulo J, $\overline{x}^n + \overline{r}_{n-1}\overline{x}^{n-1} + \cdots + \overline{r}_0 = 0$ so $\overline{x}$ satisfies a monic equation.
2. Suppose $\frac{x}{s} \in S^{-1}T$ then

   $$\left(\frac{x}{s}\right)^n + \frac{r_{n-1}}{s}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{r_0}{s^n} = 0$$

   so $\frac{x}{s}$ satisfies a monic expression.

□

Lemma 3.7. *Suppose $R \subseteq T$ are integral domains with T integral over R. Then T is a field if and only if R is.*

Proof. Suppose R is a field and $t \in T$ nonzero. Choose $r_i \in R$ such that

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

has minimal degree, T is an integral domain so $r_0 \neq 0$ so t has inverse

$$-r_0^{-1}(t^{n-1} + \cdots + r_1) \in T.$$

Conversely suppose T is a field and let $x \in R$ nonzero. Then it has an inverse $x^{-1} \in T$ which satisfies a monic equation

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

for some $r'_i \in R$. Multiply by x^{-m+1} to get

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

so R is a field. □

Corollary 3.8. *Let $R \subseteq T$ with T integral over R. Let $Q \in \operatorname{Spec} T$ with $P = Q \cap R$. Then Q is maximal if and only if P is maximal.*

Proof. T/Q is integral over R/P. Thus T/Q is a field if and only if R/P is a field. □

Theorem 3.9 (incomparability theorem)**.** *Let $R \subseteq T$ be rings with T integral over R. Let $Q \subseteq Q_1$ be prime ideals of T. Suppose $Q \cap R = Q_1 \cap R$. Then $Q = Q_1$. Hence a strict chain in* $\operatorname{Spec} T$ *maps to a strict chain in* $\operatorname{Spec} R$ *under the restriction map. In particular* $\dim R \geq \dim T$.

Proof. Let $P = Q \cap R$ and $S = R \setminus P$. We have T_P is integral over R_P where we're writing T_P for $S^{-1}T$. We have the unique maximal ideal $P_P = S^{-1}P$ in R_P. Also $S^{-1}Q$ and $S^{-1}Q_1$ are prime and $S^{-1}Q \cap S^{-1}R = S^{-1}P = P_P$ and same for $S^{-1}Q_1$ (since $S^{-1}Q \cap S^{-1}R$ is proper and contains $S^{-1}P$). Then $S^{-1}Q, S^{-1}Q_1$ are maximal. But since $S^{-1}Q \subseteq S^{-1}Q'$, we have equality. Finally prime ideal correspondence for localisation forces $Q = Q_1$. □

Theorem 3.10 (lying over)**.** *Let $R \subseteq T$ be rings with T integral over R. Take $P \in \operatorname{Spec} R$. Then there exists $Q \in \operatorname{Spec} T$ with $Q \cap R = P$. In this case we say Q* lies above *P. In other words, the restriction map* $\operatorname{Spec} T \to \operatorname{Spec} R$ *is surjective.*

Proof. Take $S = R \setminus P$ and then T_P is integral over R_P. Take a maximal ideal of T_P. It is of the form $S^{-1}Q$ for some $Q \in \operatorname{Spec} T$. Then $S^{-1}Q \cap S^{-1}R$ is maximal. But R_P is local with a unique maximal ideal P_P, so $S^{-1}Q \cap S^{-1}R = P_P$. Hence $Q \cap R = P$. □

We next have two theorems due to Cohen and Seidenberg (1946) that explain how to relate chains of primes in $\operatorname{Spec} R$ and $\operatorname{Spec} T$.

Theorem 3.11 (going up theorem)**.** *Let $R \subseteq T$ with T integral over R. Let $P_1 \subseteq \cdots \subseteq P_n$ be a chain in $\operatorname{Spec} R$ and $Q_1 \subseteq \cdots \subseteq Q_m$ with $m < n$ be a chain in $\operatorname{Spec} T$ with $Q_i \cap R = P_i$ for $i \leq m$. Then we can extend the chain of Q_i's to give $Q_1 \subseteq \cdots \subseteq Q_n$ with $Q_i \in \operatorname{Spec} T$ with $Q_i \cap R = P$ for $1 \leq i \leq n$.*

Theorem 3.12 (going down theorem)**.** *Let $R \subseteq T$ be integral domains, R integrally closed and T integral over R. Let $P_1 \supseteq \cdots \supseteq P_n$ be a chain in $\operatorname{Spec} R$, $Q_1 \supseteq \cdots \supseteq Q_m$ with $m < n$ be a chain in $\operatorname{Spec} T$ with $Q_i \cap R = P_i$ for all $i \leq m$. Then we can extend the chain of Q_i's to give $Q_1 \supseteq \cdots \supseteq Q_n$ with $Q_i \cap R = P_i$ for $1 \leq i \leq n$, $Q_i \in \operatorname{Spec} T$.*

Corollary 3.13. *Let $R \subseteq T$ with T integral over R. Then $\dim R = \dim T$.*

Proof. Incomparability says $\dim R \geq \dim T$: take a chain $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ of T, then $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ where $P_i = Q_i \cap R$.

Conversely if $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$ is a chain in $\operatorname{Spec} R$. Then by lying over there is a prime Q_0 of T with $Q_0 \cap R = P_0$. Going up gives chain $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ in $\operatorname{Spec} T$ with $Q_i \cap R = P_i$ so $\dim T \geq \dim R$. □

Corollary 3.14. *Let $R \subseteq T$ be integral domains with R integrally closed and T integral over R. Let $Q \in \operatorname{Spec} T$. Then $\operatorname{ht}(Q) = \operatorname{ht}(Q \cap R)$.*

Proof. Take a chain $Q_0 \subsetneq \cdots \subsetneq Q_n = Q$. By incomparability $P_0 \subsetneq \cdots \subsetneq P_n = Q \cap R$ where $P_i = Q \cap R$. Thus $\operatorname{ht}(Q \cap R) \geq \operatorname{ht}(Q)$.

Conversely, if $P_0 \subsetneq \cdots \subsetneq P_n = Q \cap R$ then going down gives us $Q_0 \subsetneq \cdots \subsetneq Q_n = Q$ with $Q_i \cap R = P_i$. Thus $\operatorname{ht}(Q \cap R) \leq \operatorname{ht}(Q)$. Equality. □

Proof of going up theorem. By induction it's enough to consider the case $n = 2, m = 1$. Write $\overline{R}$ for R/P_1, $\overline{T} = T/Q_1$. Then $\overline{R} \to \overline{T}$ with $\overline{T}$ integral over $\overline{R}$. By lying over there is a prime $\overline{Q}_2$ of $\overline{T}$ such that $\overline{Q}_2 \cap \overline{R} = \overline{P}_2$. Lift back to a prime Q_2 of T such that $Q_2 \cap R = P_2$. □

The proof of going down is harder — we need to extend our terminology about integrality, two lemmas of a bit of Galois theory.

Definition (integral over an ideal)**.** If I is an ideal of R and $R \subseteq T$ then $x \in T$ is *integral over I* if it satisfies a monic equation $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$ with $r_i \in I$.

The *integral closure of I in T* is the set of all such x's.

Lemma 3.15. *Let $R \subseteq T$ be rings with T integral over R, I an ideal of R. Then the integral closure of I in T is the radical $\sqrt{TI}$, which is closed under addition and multiplication. In particular if $R = T$ then the integral closure of I in R is $\sqrt{I}$.*

Proof. If x is integral over I then $x^n + r_{n-1}x^{n-1} + \cdots + r_0 = 0$ implies $x^n \in TI$ so $x \in \sqrt{TI}$. Conversely if $x \in \sqrt{TI}$ then $x^n = \sum t_i r_i$ for some $r_i \in I, t_i \in T$. But each t_i is integral over r so $M = R[t_1, \dots, t_m]$ is a finitely generated R-module. Let $y_1, \dots, y_s$ be a generating set for M as an R-module. Then we have $x^n y_j = \sum r_{jk} y_k$ with $r_{jk} \in I$. Rearrange to get $\sum (x^n \delta_{jk} - r_{jk}) y_k = 0$ so x^n satisfies a monic equation with all but the top coefficient in I. Thus x is integral over I. □

> **Lemma 3.16.** *Let $R \subseteq T$ be integral domains with R integrally closed and T integral over R and let $x \in T$ be integral over I. Then x is algebraic over the fraction field K of R and its minimal polynomial over K*
>
> $$X^n + r_{n-1}X^{n-1} + \cdots + r_0 \tag{†}$$
>
> *has coefficients $r_{n-1}, \dots, r_0 \in \sqrt{I}$.*

Proof. Certainly x is algebraic over K from its integral dependence equation. Claim the coefficients r_i in (†) are integral over I.

Proof. Take an extension field L of K containing all the conjugates $x_1, \dots, x_s$ of x, e.g. taking a splitting field of the minimal polynomial. By Galois theory for each i there is a K-automorphism of L sending x to x_i. If x satisfies $x^m + r'_{m-1}x^{m-1} + \cdots + r'_0 = 0$, $r'_j \in I$ then so does x_i. Thus each conjugate of x is integral over I, and so sums and products of them are also integral over I. However the coefficients in (†) by the usual theory of roots of polynomials are obtained by taking sums and products of the roots, namely the conjugates of x. So the coefficients are integral over I. □

They are in K and R by supposition is integrally closed in K, so those coefficients are in R, so lie in $\sqrt{I}$. □

Proof of going down theorem. By induction it's enough to consider the case $n = 2, m = 1$, i.e. we have $P_1 \supseteq P_2$ and $Q_1 \cap R = P_1$. We want to construct Q_2 such that $Q_1 \supseteq Q_2$ and $Q_2 \cap R = P_2$. Let $S_1 = T \setminus Q_1, S_2 = R \setminus P_2$ and $S = S_1 S_2 = \{tr : t \in S_1, r \in S_2\}$. This is multiplicatively closed and contains both S_1 and S_2. We claim $TP_2 \cap S = \emptyset$. Assuming this, $S^{-1}(TP_2)$ is a proper ideal of $S^{-1}T$ an is contained in a maximal ideal of $S^{-1}T$, necessarily of the form $S^{-1}Q_2$ for some prime ideal Q_2 of T with $Q_2 \cap S = \emptyset$. This implies $Q_2 \subseteq Q_1$. As $S^{-1}(TP_2) \subseteq S^{-1}Q_2$, $TP_2 \subseteq Q_2$ so $P_2 \subseteq TP_2 \cap R \subseteq Q_2 \cap R$. Together with $Q_2 \cap S = \emptyset$ we have equality. Thus Q_2 is a sought after prime ideal.

Proof of claim. Suppose for contradiction exists $x \in TP_2 \cap S$. Then x is in the integral closure of P_2 in T. x is algebraic over the field of fractions of R and its minimal polynomial is $X^n + r_{n-1}X^{n-1} + \cdots + r_0$ with $r_i \in \sqrt{P_2} = P_2$. But $x \in S$ is of the form tr for $t \in S_1, r \in S_2$. So $t = \frac{x}{r}$ has minimal polynomial

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

Since t is integral over R, apply the lemma to $I = R$ to conclude that $r_i = \frac{r_i}{r^{n-i}} \in R$. But $r \notin P_2$ so $r'_i \in P_2$. Thus t is integral over P_2, and so $t \in \sqrt{TP_2}$. But this is a contradiction: $t \in S_1 = T \setminus Q_1$, but $TP_2 \subseteq Q_1$ and Q_1 is prime, so $\sqrt{TP_2} \subseteq Q_1$. □

□

The key result allowing us to use integral extension is

> **Lemma 3.17** (Noether's normalisation lemma)**.** *Let T be a finitely generated k-algebra. Then T is integral over a subalgebra $k[x_1, \dots, x_n]$ with $x_1, \dots, x_n$ algebraically independent over k.*

> **Definition** (algebraically independent)**.** $x_1, \dots, x_n$ are *algebraically independent over k* if the map $k[X_1, \dots, X_n] \to k[x_1, \dots, x_n], X_i \mapsto x_i$ is a ring isomorphism.

Proof. Suppose $T = k[a_1, \dots, a_n]$. Induction on n, the number of generators. If all the a_i's are algebraic over k then we can take our subalgebra to be k. Otherwise relabel them so $a_1, \dots, a_r$ are algebraically independent over k and $a_{r+1}, \dots, a_n$ are algebraically dependent over $a_1, \dots, a_r$. Take non-zero $f \in k[X_1, \dots, X_r, X_n]$ such that $f(a_1, \dots, a_r, a_n) = 0$. Then $f(X_1, \dots, X_r, X_n)$ is a sum of terms

$$\lambda_\ell X_1^{\ell_1} \cdots X_r^{\ell_r} X_n^{\ell_n}$$

where $\lambda_\ell \in k$. Claim that there exist integers $m_1, \dots, m_r$ such that $\phi : \ell \mapsto m_1\ell_1 + \cdots + m_r\ell_r$ is injective for those ℓ for which $\lambda_\ell \neq 0$.

Proof. There are finitely many possibilities for differences $d = \ell - \ell'$ with $\lambda_\ell \neq 0 \neq \lambda_{\ell'}$. Write $d = (d_1, \dots, d_r, d_n)$ and consider the finitely many $(d_1, \dots, d_r) \in \mathbb{Z}^r$ obtained. Vectors orthogonal to the finitely many r-tuples lie in finitely many $(r-1)$-dimensional vector subspaces of $\mathbb{Q}^r$. Pick $(q_1, \dots, q_r)$ with each $q_i > 0$ such that $\sum q_i d_i \neq 0$ for all the finitely many non-zero $(d_1, \dots, d_r)$. Multiply by a positive integers to get $(m_1, \dots, m_r)$ so that $|\sum m_i \ell_i| > |d_n|$ for all the finitely many $d = (d_1, \dots, d_r, d_n) \neq 0$. Then if $\phi(\ell) = \phi(\ell')$ then $d_1 = \cdots = d_r = 0$ and so $\ell_n = \ell'_n$ and $\ell = \ell'$. □

Now put

$$\begin{aligned} g(X_1, \dots, X_r, X_n) &= f(X_1 + X_n^{m_1}, \dots, X_r + X_n^{m_r}, X_n) \\ &= \sum_\ell \lambda_\ell (X_1 + X_n^{m_1})^{\ell_1} \cdots (X_r + X_n^{m_r})^{\ell_r} X_n^{\ell_n}. \end{aligned}$$

Now different terms have different powers of X_n and there will be a single term of highest power in X_n. As a polynomial in X_n the leading coefficient is one of the $\lambda_\ell \in k$. Put $b_i = a_i - a_n^{m_i}$ for $1 \leq i \leq r$ and $h(X_n) = g(b_1, \dots, b_r, X_n)$. Thus the leading coefficient of h is in k and all coefficients are in $k[b_1, \dots, b_r]$. Moreover

$$h(a_n) = g(b_a, \dots, b_r, a_n) = f(a_1, \dots, a_r, a_n) = 0.$$

Dividing through by the top coefficient shows that a_n is integral over $k[b_1, \dots, b_r]$ so for each $1 \leq i \leq r$, $a_i = b_i + a_n^{m_i}$ is also integral over $k[b_1, \dots, b_r]$. Hence T is integral over $k[b_1, \dots, b_r, a_{r+1}, \dots, a_{n-1}]$, which has $n-1$ generators so by induction is integral over some polynomial subalgebra. Thus T is integral over the polynomial algebra. □

Remark. There are other proofs, not using the little result from linear algebra: using $X_i + X_n^{m_i}$ with m_i being the power of some integers α (Nagata).

We now show that this dimension agrees with transcendence degree from field theory.

As in linear algebra, in a field K with subfield k we can consider maximal algebraically indepedent subsets over k. They exist by Zorn's lemma and all have the same cardinality — we can use a version of the exchange lemma. A maximal algebraically independent subset over k is a *transcendence basis* of K over k, written $\operatorname{trdeg}_k K$.

The *algebraic closure of a set* S over k is the set of elements which are algebraically dependent over the subfield generated by k and S.

Theorem 3.18. *Let T be a finitely generated k-algebra that is an integral domain. Let L be its field of fraction. Then* $\dim T = \operatorname{trdeg}_k L$. *In particular* $\dim k[X_1, \dots, X_n] = \operatorname{trdeg}_k k(X_1, \dots, X_n) = n$.

Proof. Apply Noether normalisation to get T is integral over $k[x_1, \dots, x_r]$ with $x_1, \dots, x_r$ algebraically independent. Then by Corollary 3.13 $\dim T = \dim k[X_1, \dots, X_r]$. Thus any finitely generated k-algebra has the same dimension as the dimension of a polynomial algebra with r variables where $r = \operatorname{trdeg}_k(L)$.

It's left to prove that the dimension of such a polynomial algebra is r. Recall that we observed $\dim k[X_1, \dots, X_r] \geq r$. When $r = 0$ equality holds. For general r, suppose

$$P_0 \subsetneq \cdots \subsetneq P_s$$

is a chain of prime ideals, and we may assume $P_0 = \{0\}, P_1 = (f)$. But

$$\operatorname{trdeg} \operatorname{Frac} k[X_1, \dots, X_r]/(f) = r - 1.$$

However by Noether normalisation, $\dim k[X_1, \dots, X_n]/(f) = \dim k[\overline{Y}_1, \dots, \overline{Y}_t]$ where $\overline{Y}_1, \dots, \overline{Y}_t$ algebraically independent in $k[X_1, \dots, X_r]/(f)$ and $k[X_1, \dots, X_r]/(f)$ integral over $k[\overline{Y}_1, \dots, \overline{Y}_t]$. However

$$\operatorname{trdeg} k(\overline{Y}_1, \dots, \overline{Y}_t) = \operatorname{trdeg}(\operatorname{Frac} k[X_1, \dots, X_r]/(f)) = r - 1$$

so $r = t - 1$. By induction $\dim k[\overline{Y}_1, \dots, \overline{Y}_t] = r - 1$. But $P_1 = (f)$ so modulo P_1 we get

$$\overline{P}_1 \subsetneq \overline{P}_1 \subsetneq \cdots \subsetneq \overline{P}_s$$

is a chain of primes of length $s - 1$, so $s - 1 \leq r - 1$ and $s \leq r$. Thus $\dim k[X_1, \dots, X_r] \leq r$ so equality. □

Theorem 3.19. *Let R be a Noetherian integral domain that is integrally closed with field of fractions K and L a finite separable field extension of K. Let T be the integral closure of R in L. Then T is a finitely generated R-module.*

Corollary 3.20. *The integral closure of $\mathbb{Z}$ in a number field L, i.e. a finite field extension of $\mathbb{Q}$, is a finitely generated $\mathbb{Z}$-module.*

Corollary 3.21. *Suppose* $\operatorname{char} k = 0$ *and let* T *be a finitely generated* k*-algebra which is an integral domain and is integral over the polynomial algebra* $R = k[x_1, \dots, x_n]$*. Let* L *be the field of fractions of* T*. Then the integral closure* T_1 *of* R *in* L *is a finitely generated* R*-module. Thus* T_1 *is integrally closed and in the chain of maps*

$$\operatorname{Spec} T_1 \to \operatorname{Spec} T \to \operatorname{Spec} R$$

all the fibres are finite.

Proof. Immediate from Theorem 3.19 apart from finiteness of fibre, which is example sheet 2 question 15, 16. □

The proof of Theorem 3.19 uses the *trace function*

$$\operatorname{tr}_{L/K}(x) = -[L : K(x)] \cdot \text{next to top coefficient of min poly of } x \text{ over } K$$

for $x \in L$, for any finite field extension L/K. If L is Galois over K then

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

The next to top coefficient of the minimal polynomial is minus the sum of all the conjugates of x, and then we may have repetitions so the factor $[L : K(\alpha)]$.

Recall the following fact from Galois theory: if L is separable over K then

$$\begin{aligned} L \times L &\to K \\ (x, y) &\mapsto \operatorname{tr}_{L/K}(xy) \end{aligned}$$

is a non-degenerate symmetric K-bilinear form on L.

Proof of Theorem 3.19. Pick a K-vector space basis $y_1, \dots, y_n$ of L. By multiplying by suitable elements of K we may assume each y_i lies in T. Since $\operatorname{tr}_{L/K}(xy)$ yields a non-degenerate symmetric bilinear form we can find a dual basis $x_1, \dots, x_n$. We'll show that $T \subseteq \sum Rx_i$, and then since R is Noetherian, T is a finitely generated R-module.

Proof. Let $z \in T$. Then $z = \sum \lambda_i x_i$ with $\lambda_i \in K$. Thus

$$\operatorname{tr}_{L/K}(zy_j) = \operatorname{tr}_{L/K}(\sum \lambda_i x_j y_j) = \sum \lambda_i \operatorname{tr}_{L/K}(x_i y_j) = \lambda_j.$$

But z and y_j are in T and hence $zy_j \in T$. Then by Lemma 3.16 with $I = R$ the coefficients of the minimal polynomial of zy_j lie in R, in particular the next to top coefficient is in R. Thus $\lambda_j = \operatorname{tr}_{L/K}(zy_j) \in R$. □

□

4 Heights

Let R be a commutative ring with 1, but note we're going to talk about general Noetherian rings, not just finitely generated k-algebras.

Recall that for UFDs the height 1 primes are precisely those of the form (f) with f irreducible. The principal ideal theorem gives us a recipe for finding height 1 primes in general.

Theorem 4.1 (principal ideal theorem)**.** *Let R be a Noetherian ring and a be a non-unit. Let P be a minimal prime over (a). Then* $\operatorname{ht} P \leq 1$.

This starts an inductive argument and appears in the proof of the inductive step proving

Theorem 4.2 (generalised principal ideal theorem)**.** *Let R be a Noetherian ring and I be a proper ideal generated by n elements. Let P be a minimal prime over I. Then* $\operatorname{ht} P \leq n$.

Corollary 4.3.

1. *Every prime ideal P of a Noetherian ring R has finite height, less than or equal to the minimum number of generators of P.*
2. *Every Noetherian local ring R has finite dimension, less than or equal to minimum number of generators of the unique maximal ideal P, which equal to* $\dim_{R/P} P/P^2$.

Proof.

1. Any ideal of a Noetherian ring is finitely generated and a prime ideal is a minimal prime over itself. Thus $\operatorname{ht} P \leq$ minimum number of generators of P.
2. By 1 $\dim R = \operatorname{ht} P \leq$ minimum number of generators of P. The final equality follows from Nakayama's lemma: claim P is generated by $x_1, \dots, x_r$ if and only if P/P^2 is generated by $\overline{x}_1, \dots, \overline{x}_r$.

   Proof. For the nontrivial direction, suppose $\overline{x}_1, \dots, \overline{x}_n$ generate P/P^2 with $x_i \in R$. Consider $I = (x_1, \dots, x_r) \subseteq P$. Clearly $I + P^2 = P$ and so $P(P/I) = P/I$. As $P = \operatorname{Jac} R$, by Nakayama's lemma $P/I = 0$ so P is generated by $x_1, \dots, x_r$. □

□

Definition (regular local ring)**.** A *regular local ring R* is one where $\dim R = \dim_{R/P} P/P^2$.

In algebraic geometry this correponds to localisation at a non-singular point, and P/P^2 is the cotangent space at P.

Remark. Using generalised principal ideal theorem we can get a better bound for a local ring R: $\dim R = \operatorname{ht} P \leq$ minimum number of generators of I with $\sqrt{I} = P$. In fact (we will not prove here), $\dim R = \operatorname{ht} P =$ minimum number of generators of some I with $\sqrt{I} = P$.

Proof of principal ideal theorem. Take a non-unit $a \in P$ and P a minimal prime over (a). First localise at P so R_P has unique prime ideal $P_P = S^{-1}P$ where $S = R \setminus P$. Observe that P_P is minimal over $S^{-1}(a)$ by ideal correspondence. As $\operatorname{ht} S^{-1}P = \operatorname{ht} P$, we may assume that R is local with unique maximal ideal P.

Suppose for contradiction $\operatorname{ht} P > 1$ and we have a chain of primes $Q' \subsetneq Q \subsetneq P$. Consider $R/(a)$ which has unique maximal ideal $P/(a)$ which is also a minimal prime, so it is the only prime of $R/(a)$. Thus $\mathcal{N}(R/(a)) = P/(a)$, and it is Noetherian as $R/(a)$ is Noetherian. Thus $P^n \subseteq (a)$ for some n. Now consider

$$R \supsetneq P \supseteq P^2 \supseteq \cdots \supseteq P^n$$

and each factor is a finite dimensional R/P-vector space. Each factor satisfies the descending chain condition on subspaces and so R/P^n satisfies DCC on submodules, i.e. ideals. Thus R/P^n is Artinian and so is $R/(a)$.

Now consider localisation at Q with $S = R \setminus Q$.

$$S^{-1}R \supsetneq S^{-1}Q \supseteq (S^{-1}Q)^2 \supseteq \cdots$$

is a chain of ideals in $S^{-1}R$. Set $I_m = \{r : \frac{r}{1} \in (S^{-1}Q)^m\}$ so $S^{-1}I_m = (S^{-1}Q)^m$. Clearly

$$Q = I_1 \supseteq I_2 \supseteq \cdots$$

and its image in $R/(a)$

$$(I_1 + (a))/(a) \supseteq (I_2 + (a))/(a) \supseteq \dots$$

is a descending chain so must terminate and $I_m + (a) = I_{m+1} + (a)$ for some m. Now we show $I_1 \supseteq I_2 \supseteq \cdots$ terminates. Take $r \in I_m$. Then $r = t + xa$ for some $t \in I_{m+1}, r \in R$. Thus $xa = r - t \in I_m$. However $a \notin Q$ as P is minimal over (a) and so $a \in S$. Thus $\frac{a}{1}$ is a unit in $S^{-1}R$. Then $xa \in I_m$ if and only if $\frac{xa}{1} \in (S^{-1}Q)^m$, if and only if $\frac{x}{1} \in (S^{-1}Q)^m$, if and only if $x \in I_m$. So $I_m = I_{m+1} + I_m a$ and $I_m/I_{m+1} = P(I_m/I_{m+1})$ since $a \in P$. Thus by Nakayama $I_m/I_{m+1} = 0$ and hence $I_m = I_{m+1}$, so

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

Now $S^{-1}Q = \operatorname{Jac} S^{-1}R$ so by Nakayama $(S^{-1}Q)^m = 0$. However when we localise the chain $Q' \subsetneq Q$ we get $S^{-1}Q' \subsetneq S^{-1}Q$, contradiction. □

Proof of generalised principal ideal theorem. Induction on n. For $n = 1$ this is principal ideal theorem. Assume $n > 1$. By passing to R_P we can assume R is local with unique maximal ideal P. Pick any prime maximal subject to $Q \subsetneq P$. Then P is the only prime ideal strictly containing Q. Claim that $\operatorname{ht} Q \leq n - 1$, and then it follows that $\operatorname{ht} P \leq n$.

Proof. Since P is minimal over I we must have $I \not\subseteq Q$. By assumption $I = (a_1, \dots, a_n)$ and we may assume $a_n \notin Q$. P is the only prime containing $Q + (a_n)$, so $\mathcal{N}(R/(Q+(a_n))) = P/(Q+(a_n))$. It is nilpotent so there is m such that $a_i^m \in Q+(a_n)$ for all $i \leq n-1$, say $a_i^m = t_i + x_i a_n$ for some $t_i \in Q, x_i \in R$. Any prime of R containing $t_1, \dots, t_{n-1}$ and a_n contains a_i^m and thus contains $a_1, \dots, a_n$. Note that $(t_1, \dots, t_{n-1}) \subseteq Q$. Claim that Q is minimal over $(t_1, \dots, t_{n-1})$, and then we are done by induction hypothesis.

Write $\overline{R} = R/(t_1, \dots, t_{n-1})$ and use bar to denote image in $\overline{R}$. The unique maximal ideal $\overline{P}$ of $\overline{R}$ is minimal over $\overline{(a_n)}$. Then by principal ideal theorem $\operatorname{ht} \overline{P} \leq 1$. But $\overline{Q} \subsetneq \overline{P}$ so must have height 0. Thus Q is minimal over $(t_1, \dots, t_{n-1})$. □

□

5 Artinian rings

In this chapter R is not necessarily commutative.

> **Definition** ((right) Artinian ring). R is *right Artinian* if it satisfies the descending chain condition on right ideals. Left Artinian rings are defined analogously.

We can similarly define left/right Artinian modules.

Example.

1. Let k be a field. Any k-algebra R that is finite dimensional as k-vector space is right and left Artinian as right and left ideals are vector subspaces.

2. $M_n(k)$, the ring of $n \times n$ matrices, is Artinian.

3. $R = \{ \left(\begin{smallmatrix} q & r \\ 0 & s \end{smallmatrix}\right) : q \in \mathbb{Q}, r, s \in \mathbb{R} \}$ is not left Artinian but is right Artinian.

4. The group algebra kG for a finite group G. This is the k-space with bases labelled by $g \in G$ and multiplication
$$(\sum_g \lambda_g \cdot g) \cdot (\sum_h \mu_h \cdot h) = \sum_{k \in G} \nu_k \cdot k$$
where $\nu_k = \sum_{gh=k} \lambda_g \mu_h$.

5. Any division ring is Artinian. For example quaternions $\mathbb{H} = \mathbb{R} + \mathbb{R}j + \mathbb{R}i + \mathbb{R}k$.

6. $R = M_n(D)$ for a division ring D. A right ideal generated by a matrix A is
$$AR = \{B : \text{columns of } B \subseteq \text{right span of columns of A}\}.$$
Thus right ideals are of the form $\{B : \text{columns of } B \subseteq \text{right subspace of } D^n\}$. Similarly the left ideal generated by A is
$$RA = \{B : \text{rows of } B \subseteq \text{left span of rows of A}\}$$
so left ideals are of the form $\{B : \text{rows of } B \subseteq \text{left subspace of } D^n\}$. Note that the only two-sided ideals are 0 and R.

> **Definition** (simple ring). R is a *simple ring* if the only two-sided ideals are 0 and R.

For a noncommutative ring R, we define its Jacobson radical $\operatorname{Jac} R$ to be the intersection of all maximal right ideals.

Remark. This is actually a two-sided ideal: I is a maximal right ideal if and only if R/I is a simple right R-module.

Definition (simple module)**.** A module M is *simple* if the only submodules are 0 and M.

Let M be a simple right R-module and $0 \neq m \in M$. Then

$$\operatorname{Ann}_R(m) = \{r : mr = 0\}$$

is a maximal right ideal of R. Note that annihilator of an element is a right ideal, but $\operatorname{Ann}_R M = \bigcap_{m \in M} \operatorname{Ann}_R(m)$ is a two-sided ideal, since for any $m \in \operatorname{Ann} M, x \in R$, $m(xr) = (mx)r = 0$ so $xr \in \operatorname{Ann}(m)$ for all m.

We see $\operatorname{Jac} R = \bigcap_{M \text{ simple right } R\text{-module}} \operatorname{Ann}(M)$ and so a two-sided ideal.

Proposition 5.1 (Nakayama's lemma)**.** *For a right ideal I, TFAE:*

1. $I \subseteq \operatorname{Jac} R$.
2. *If M is a finitely generated R-module with submodule N such that $N + MI = M$ then $N = M$.*
3. $\{1 + x : x \in I\}$ *is a subgroup of the unit group of R.*

Proof. Example sheet 3. □

From this we can see that $\operatorname{Jac} R$ is characterised as the largest two-sided ideal I such that $\{1 + x : x \in I\}$ forms a subgroup of the unit group. This characterisation is insensitive to right/left so if we developed the definition of $\operatorname{Jac} R$ using left ideals we would get the same result.

Definition (semisimple ring)**.** R is *semisimple* if $\operatorname{Jac} R = 0$.

Example.

1. $M_n(D)$ for D a division ring is semisimple.
2. Let G be the cyclic group of order p and let $\mathbb{F}_p$ be the field with p elements. Then $\mathbb{F}_p G \cong \mathbb{F}_p[x]/(x^p - 1)$ is not semisimple since $x^p - 1 = (x - 1)^p$.
3. Let G be a finite group, $\operatorname{char} k = 0$. Then kG is semisimple by Maschke's theorem from representation theory.

The main goal of this chapter is to prove Artin-Wedderburn theorem which says that a right Artinian semisimple ring is a direct sum of matrix algebras over division rings. Before that we prove some properties about Artinian rings, which generalises the commutative results on example sheet 2.

Theorem 5.2. *Let R be right Artinian. Then*

1. $\operatorname{Jac} R$ *is nilpotent.*
2. *R is right Noetherian.*

To prove this we need some lemmas and terminology.

Lemma 5.3. *Let R be a semisimple right Artinian ring. Then R is a finite direct sum of simple right R-modules.*

Proof. Consider maximal right ideals M_i and the chain

$$R \supsetneq M_1 \cap M_2 \supseteq \cdots$$

The DCC on right ideals forces this to terminate so $\operatorname{Jac} R = M_1 \cap \cdots \cap M_n$, say, and we may assume n is minimal. Consider the module map

$$\begin{aligned} \theta : R &\to \bigoplus_{i=1}^{n} R/M_i \\ r &\mapsto (r + M_1, \dots, r + M_n) \end{aligned}$$

Note R/M_i are simple modules. Consider the restriction of $R \to R/M_i$ to $\bigcap_{j \neq i} M_j$. This is injective since the kernel is $\bigcap M_j = \operatorname{Jac} R = (0)$ and is surjective since the image is a non-zero submodule of a simple module M/M_i. The image of $\bigcap_{j \neq i} M_j$ under θ is $(0, \dots, R/M_i, \dots, 0)$ so the image is $\bigoplus_{i=1}^{n} R/M_i$. θ is injective since $\ker \theta = \bigcap M_i = (0)$. □

Lemma 5.4. *Let R be a semisimple right Artinian ring and M a right Artinian R-module. Then M is a finite direct sum of simple R-modules.*

Proof. Example sheet 3. □

Definition (socle)**.** The *socle* of a non-zero Artinian module M is the sum of all the simple submodules of M.

Note that since M is non-zero Artinian, it does have minimal non-zero submodules, which are necessarily simple. Then $\operatorname{soc} M \neq 0$.

Lemma 5.5. $\operatorname{soc} M = \{m \in M : mJ = 0\}$ *where* $J = \operatorname{Jac} R$.

Proof. Each minimal submodule M' of M is simple and thus of the form $R/\operatorname{Ann}(m)$ for each $m \in M'$. Thus $J \subseteq \bigcap_{m \in M'} \operatorname{Ann}(m)$ and so $\operatorname{Jac} R$ annihilates M' and hence annihilates $\operatorname{soc} M$.

Conversely if $mJ = 0$ then mR can be regarded as a R/J-module. But mR inherits the Artinian property and so we have an Artinian module over a semisimple ring R/J. Thus mR is a finite direct sum of simple modules, so $mR \subseteq \operatorname{soc} M$. □

Definition. We define the *socle series* of M inductively by

$$\operatorname{soc}_0 M = 0, \operatorname{soc}_1 M = \operatorname{soc} M, \frac{\operatorname{soc}_i M}{\operatorname{soc}_{i-1} M} = \operatorname{soc}(M/\operatorname{soc}_{i-1} M).$$

Note that we have strict inequalities

$$0 = \operatorname{soc}_0 M \subsetneq \operatorname{soc}_1 M \subsetneq \cdots$$

until we reach $\operatorname{soc}_n M = M$. We do reach M since we have descending chain

$$R \supseteq J \supseteq J^2 \supseteq \cdots$$

which must terminate, say $J^n = J^{n+1}$, and so

$$\operatorname{soc}_n M = \{m \in M : mJ^n = 0\} = \operatorname{soc}_{n+1} M = \{m \in M : mJ^{n+1} = 0\}.$$

Proof of Theorem 5.2. Let $M = R$. We have seen that the socle series terminates

$$0 = \operatorname{soc}_0 M \subseteq \operatorname{soc}_1 M \subseteq \cdots \subseteq \operatorname{soc}_n M = M.$$

Each factor $\operatorname{soc}_i M / \operatorname{soc}_{i-1} M$ is annihilated by J and so can be viewed as an R/J-module. Thus it is a finite direct sum of simple modules. Such a finite direct sum satisfies both ACC and DCC so $\operatorname{soc}_i M / \operatorname{soc}_{i-1} M$ is a right Noetherian module. Hence $M = \operatorname{soc}_n M$ is right Noetherian.

$\operatorname{soc}_n R = R$ implies R is annihilated by J^n, in particular 1 is annihilated by J^n. Thus $J^n = (0)$. □

To prove Artin-Wedderburn we need to think about endormorphim rings of modules.

> **Lemma 5.6** (Schur's lemma)**.** *Let S be a simple right R-module. Then $\operatorname{End}_R(S)$ is a division ring. If S_1 and S_2 are non-isomorphic simple modules then $\operatorname{Hom}_R(S_1, S_2) = \{0\}$.*

Note that S is a left $\operatorname{End}_R(S)$-module and thus S is an $(\operatorname{End}_R(S), R)$-bimodule.

Proof. Let $\phi : S \to S$ be an R-module map. Then either $\phi(S) = 0$ so $\phi = 0$, or $\phi(S) = S$. Furthermore $\ker \phi$ is a submodule of S so either $\ker \phi = 0$ or $\ker \phi = S$, in which case $\phi = 0$. Thus if $\phi \neq 0$ then it must be bijective and have a right and left inverse. Thus $\operatorname{End}_R(S)$ is a division ring.

If S_1, S_2 are non-isomorphic simple and $\phi : S_1 \to S_2$ a similar argument about $\ker \phi$ and $\operatorname{im} \theta$ shows $\theta = 0$. □

> **Lemma 5.7.** *Regard R as a right R-module, which we write R_R for emphasis, then $\operatorname{End}_R(R_R) \cong R$.*

Proof. Observe that multiplication on the left by $r \in R$ gives an R-module endomorphism of R_R. Observe that $\phi \in \operatorname{End}_R(R_R)$ is uniquely determined by $\phi(1)$ and so $\operatorname{End}_R(R) \to R, \phi \mapsto \phi(1)$ is the sought after isomorphism. □

> **Theorem 5.8** (Artin-Wedderburn)**.** *Let R be a semisimple right Artinian ring. Then $R = \bigoplus_{i=1}^r R_i$ where $R_i = M_{n_i}(D_i)$ for some division ring D_i and the R_i's are uniquely determined. R has exactly r isomorphism classes of simple modules S_i and $\operatorname{End}_R(S_i) = D_i$ and $\dim_{D_i} S_i = n_i$ when viewed as a left D_i-vector space.*
>
> *Futhermore if R is finite dimensional as a k-vector space for a field k then D_i has finite dimension as k-vector spaces. If k is algebraically closed*

> *then $D_i \cong k$.*

For example for a finite group G, $\mathbb{C}G = \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C})$ where r is the number of simple modules of dimension n_i up to isomorphism.

> **Corollary 5.9.** *Let G be a finite group. Then $Z(\mathbb{C}G)$ is an r-dimensional $\mathbb{C}$-vector space where r is the number of isomorphism class of simple $\mathbb{C}G$-modules, equivalently the number of conjugacy classes in G.*

Proof. Any class sum $\sum_{g' \in \mathrm{ccl}(g)} g'$ is in $Z(\mathbb{C}G)$ and any element of $Z(\mathbb{C}G)$ is a linear combination of such class sums. These class sums are also linearly independent over $\mathbb{C}$ so $\dim_{\mathbb{C}}(Z(\mathbb{C}G))$ is the number of conjugacy classes. But $\mathbb{C}G$ is semisimple and right Artinian so Artin-Wedderburn applies. $\mathbb{C}$ is algebraically closed so $\mathbb{C}G = \bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C})$. But $Z(M_{n_i}(\mathbb{C})) = \{\lambda I : \lambda \in \mathbb{C}\}$ which is 1-dimensional. Thus $Z(\bigoplus_{i=1}^{r} M_{n_i}(\mathbb{C}))$ is r-dimensional, and from Artin-Wedderburn r is the number of isomorphism class of simple $\mathbb{C}G$-modules. □

Proof of Artin-Wedderburn. R_R is a finite direct sum of simple modules. Group them by isomorphism classes to get

$$R_R = \underbrace{(S_{11} \oplus \cdots \oplus S_{1n_1})}_{R_1} \oplus \underbrace{(S_{11} \oplus \cdots \oplus S_{2n_2})}_{R_2} \oplus \cdots$$

so that $S_{im} \cong S_{i\ell}$ for $1 \le m, \ell \le n_i$, $S_{im} \ncong S_{j\ell}$ for $i \ne j$.

Let S be a simple submodule of R_R and consider the projections $\pi_{ik} : R \to S_{ik}$ restricted to S. By Schur's lemma $\pi_{ik}|_S$ are 0 or isomorphism. But at least one of the restrictions must be non-zero and the non-zero restrictions must all be into the same R_i. Thus $S \le R_i$ for some i and is isomorphic to all the R_{ik}. If $S_{ik} \cong S_i$, say, then R_i is the sum of all simple submodules of $R - R$ that are isomorphic to S_i and this is uniquely determined.

Consider $\mathrm{End}_R(R_R)$. We know that it is isomorphic to R.

$$\mathrm{End}_R(R_R) = \mathrm{End}_R((S_{11} \oplus \cdots \oplus S_{1n_1}) \oplus (S_{21} \oplus \cdots \oplus S_{2n_2}) \oplus \cdots).$$

Consider $\mathrm{End}_R(S_{11} \oplus \cdots \oplus S_{1n_1})$ where $S_{1k} \cong S_1$ for all k. This is $M_{n_1}(D_1)$ where $D_1 = \mathrm{End}_R(S_1)$ which is a division ring from Schur's lemma. $\phi \in \mathrm{End}_R(S_{11} \oplus \cdots \oplus S_{1n_1})$ is represented by a matrix $(\phi_{m\ell})$ where $\phi_{m\ell} \in \mathrm{Hom}_R(S_{im}, S_{i\ell})$. So

$$R = \mathrm{End}_R(R_R) = \begin{pmatrix} M_{n_1}(D_1) & & \\ & M_{n_2}(D_2) & \\ & & \ddots \end{pmatrix}$$

which is block diagonal.

Recall our example about $M_n(D)$ for a division ring D. We know a minimal right ideals consist of matrices B whose columns are all of the form $\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \lambda$ for a column $\begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$ and $\lambda \in D$. These are all of dimension n as a D-vector space and so $\dim_{D_i} S_i = n_i$. □

U_1	trivial	1-dim	g, h acts trivially
U_2	signature	1-dim	g acts by multiplication by -1, h acts by multiplication by $+1$
U_3		2-dim	k^2 row vectors with g acting by multiplication on right by $\left(\begin{smallmatrix} -1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$ and h acts by $\left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$

Example. Consider the group ring kS_3 where k is a field. Let $g = (12), h = (123)$. When $\operatorname{char} k = 0$ we know kG is semisimple. There are 3 conjugacy classes, with corresponding simple modules

Now suppose $\operatorname{char} k = 3$. Modulo 3 we get $\overline{U}_1, \overline{U}_2$ two simple 1-dimensional modules. Note that $\overline{U}_3$ in characteristic 3 has $(2, 1)$ as a common eigenvector of both g and h and so there is a 1-dimensional submodule. In fact there are only 2 isomorphism classes of simple modules. $\operatorname{Jac} kS_3 = \ker(kS_3 \to kC_2)$, the map induced by the group map $S_3 \to C_2$. This is 4-dimensional over k. We have semisimple quotient

$$kS_3 / \operatorname{Jac} kS_3 \cong M_1(k) \oplus M_1(k)$$

where $M_1(k)$ corresponds to a simple 1-dimensional modules. $(h-1)^3 = h^3 - 1 = 0$ since h has order 3. One can show $\operatorname{Jac} kS_3$ is nilpotent. $\operatorname{soc}(kS_3)$ is the right ideal generated by $(h-1)^2 = h^2 + h + 1$. It is 2-dimensional and has a copy of $\overline{U}_1$ and $\overline{U}_2$.

Some final words on noncommutative rings:

1. they are related to modular representation theory;
2. when considering rational representation (of say, Galois groups) we need to consider division rings.

6 Filtrations and Graded rings

We end our short interlude to noncommutative rings and assume R is commutative with 1.

> **Definition** (filtered ring). A *($\mathbb{Z}$-)filtered ring* R is one with additive subgroups R_i
>
> $$\cdots \subseteq R_{-1} \subseteq R_0 \subseteq R_1 \subseteq \cdots$$
>
> with $R_i R_j \subseteq R_{ij}$ for $i, j \in \mathbb{Z}$ and $1 \in R_0$.

Note.

1. $\bigcup R_i$ is a subring — usually we have $\bigcup R_i = R$, in which case it is called a *exhaustive filtration.*
2. R_0 is a subring.
3. $\bigcap_{i\in\mathbb{Z}} R_i$ is an ideal of R_0. We usually have $\bigcap R_i = \{0\}$, in which case it is called a *separated filtration.*

Example.

1. I-adic filtration: given an ideal $I \subseteq R$, we set

$$R_i = \begin{cases} R & i \geq 0 \\ I^{-i} & i < 0 \end{cases}$$

   If R is a local ring we're particularly interested in the P-adic filtration where P is the maximal ideal.

2. If R is a k-algebra generated by $x_1, \dots, x_n$ say, set $R_i = 0$ for $i < 0$, $R_0 = k \cdot 1$ and R_i to be the k-subspace of polynomial expressions in the generators of total degree $\leq i$.

> **Definition** (associated graded ring). The *associated graded ring* is
>
> $$\operatorname{gr} R = \bigoplus R_i / R_{i-1}$$
>
> as an additive group with multiplication
>
> $$(r + R_{i-1})(s + R_{j-1}) = rs + R_{i+j-1}$$
>
> where $r \in R_i, s \in R_j$.

Example. For P-adic filtration of a local ring, the associated graded ring is

$$\operatorname{gr} R = \bigoplus P^i / P^{i+1}.$$

Write $K = R/P$, then $\operatorname{gr} R$ is generated as a K-algebra by any K-vector space basis of P/P^2.

Remark.

1. On example sheet 3 we'll see that the regular case is when $\operatorname{gr} R$ is a polynomial algebra in n variables where $n = \dim_K P/P^2$.
2. Filtrations and associated graded rings are also of use for non-commutative R, for example when R is the universal emveloping algebra of a finite dimensional Lie algebra. $\operatorname{gr} R$ is commutative when R is filtered as in example 2 above.

Definition (filtered module)**.** 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 respect to filtration R_i of R if there are additive subgroups M_i of M such that $R_j M_i \subseteq M_{i+j}$.

The *associated graded module* is defined as the additive group

$$\operatorname{gr} M = \bigoplus M_i/M_{i-1}$$

with multiplication

$$(r + R_{j-1})(m + M_{i-1}) = rm + M_{i+j-1}$$

for $r \in R_j, m \in M_i$, making it a $\operatorname{gr} R$-module.

Lemma 6.1. *If*

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] & M \arrow[r] & M/N \arrow[r] & 0 \end{tikzcd}$$

is exact then

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{gr} N \arrow[r] & \operatorname{gr} M \arrow[r] & \operatorname{gr}(M/N) \arrow[r] & 0 \end{tikzcd}$$

is exact, using the filtration $N \cap M_i$ for N, $(M_i + N)/N$ for M/N.

Proof. Example sheet 3 question $9\frac{3}{4}$. □

Definition (Rees ring)**.** The *Rees ring* of the filtration $\{R_i\}$ of R is a subring of $R[T, T^{-1}]$

$$\operatorname{Rees}(R) = \bigoplus_{j \in \mathbb{Z}} R_j T^j \subseteq R[T, T^{-1}].$$

Note that $1 \in R_0 \subseteq R_1$ and so $T \in \operatorname{Rees}(R)$. Observe also that

$$R = \operatorname{Rees}(R)/(T-1)$$
$$\operatorname{gr} R = \operatorname{Rees}(R)/(T)$$

Definition (Rees module)**.** Given an R-module M with a filtration M_j with respect to filtration $\{R_i\}$ of R, we define the *Rees R-module* to be

$$\operatorname{Rees}(M) = \bigoplus M_i T^i$$

which is a $\operatorname{Rees}(R)$-module.

Similarly we have $\operatorname{gr}(M) = \operatorname{Rees}(M)/T\operatorname{Rees}(M)$.

Definition (graded ring, graded ideal, graded module)**.** A *($\mathbb{Z}$-)graded ring* S is $S = \bigoplus_{i\in\mathbb{Z}} S_i$ where S_i's are additive subgroups such that $S_iS_j \subseteq S_{ij}$. S_0 is a subring and each S_i is an S_0-module. S_i is the *ith component* and $s \in S$ is *homogeneous of degree i* if $s \in S_i$.

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

A *graded S-module V* is of the form $\bigoplus V_j$ such that $S_iV_j \subseteq V_{i+j}$.

Similarly for positive/negative graded rings/ideals.

Note that if a graded ideal is finitely generated as an ideal then there is a finite generating set of homogeneous elements.

Note that a negative graded ring may after renumbering be treated as a positive graded ring. For example the associated graded ring of an I-adic filtration may be treated after renumbering as a positive graded ring.

6.1 Poincaré-Serre theorem

Suppose $S = \bigoplus_{i\geq 0} S_i$ is a commutative Noetherian ring generated by S_0 and generators $x_1, \dots, x_m$ of degree $k_1, \dots, k_m$ respectively. Let λ be an *additive* integer valued function on finitely generated S_0-modules, i.e. if we have a short exact sequence

$$0 \longrightarrow U_1 \longrightarrow U_2 \longrightarrow U_3 \longrightarrow 0$$

then $\lambda(U_2) = \lambda(U_1) + \lambda(U_3)$.

Example.

1. $S_0 = k$, can take λ to be k-vector space dimension.
2. S_0 is local Artinian with unique maximal ideal P then for any finitely generately S_0-module U we have a chain

   $$0 = U_0 \subsetneq U_1 \subsetneq U_2 \subsetneq \cdots \subsetneq U_n = U$$

   with $U_i/U_{i-1} \cong S_0/P$ for each i. The number of factors is the *composition length* of U. Set $\lambda(U)$ to be composition length of U and it is an additive function. Check this is independent of the choice of the chain.

Definition (Poincaré series)**.** The *Poincaré series* of a graded finitely generated S-module $V = \bigoplus_{i\geq 0} V_i$, is the power series

$$P(V,t) = \sum_{i\geq 0} \lambda(V_i)t^i \in \mathbb{Z}[[t]].$$

Theorem 6.2 (Hilbert-Serre)**.** *$P(V,t)$ is a rational function of the form*

$$\frac{f(t)}{\prod_{j=1}^m (1 - t^{k_j})}$$

where $f(t) \in \mathbb{Z}[t]$ is a polynomial and k_j is the degree of the generator x_j.

Corollary 6.3. *If each $k_j = 1$ then for large enough i*

$$\lambda(V_i) = \phi(i)$$

for some rational polynomial $\phi(t) \in \mathbb{Q}[t]$ of degree $d-1$ where d is the degree of 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 of degree d.

Definition (Hilbert polynomial, Samuel polynomial)**.** $\phi(t)$ is the *Hilbert polynomial* and $\chi(t)$ is the *Samuel polynomial.*

Note that the degree of χ gives us another dimension.

Definition. We define $d(V) = \deg \chi(t)$. For a ring S we define $d(S)$ by taking $V = S$.

Proof of Hilbert-Serre. Induction on m, the number of generators. If $m = 0$ then $S = R_0$ and V is a finitely generated S_0-module so $V_j = 0$ for large enough j so in fact $P(V,t)$ is a polynomial.

For $m > 0$, multiplication by x_m gives maps $x_m : V_i \to V_{i+k_m}$ and so we get an exact sequence

$$\begin{tikzcd} 0 \arrow[r] & K_i \arrow[r] & V_i \arrow[r, "x_m"] & V_{i+k_m} \arrow[r] & L_{i+k_m} \arrow[r] & 0 \end{tikzcd}$$

where K_i and L_{i+k_m} are the kernel and cokernel of multiplication by x_m respectively. Let $K = \bigoplus K_i, L = \bigoplus L_i$. K is a graded submodule of V and hence a finitely generated S-module. $L = V/x_mV$ is also a finitely generated S-module. Note that x_m acts by 0 on K and L and so they may be viewed as fintely-generated $S_0[x_1, \dots, x_{m-1}]$-modules.

Apply λ to the exact sequence to get

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

Multiply by t^{i+k_m} and sum over i,

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

where $g(t) \in \mathbb{Z}[t]$ arising from the first few terms. Apply the induction hypothesis to $P(K,t)$ and $P(L,t)$ □

Proof of Corollary 6.3. Have $k_1 = \cdots = k_m = 1$ so

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

where $f(t) \in \mathbb{Z}[t], f(1) \neq 0$. Since

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

repeated differentiation gives

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

Let $f(t) = a_0 + a_1 t + \cdots + a_s t^s$ say, then

$$\lambda(V_i) = a_0 \binom{d+i-1}{d-1} + a_1 \binom{d+i-2}{d-1} + \cdots + a_s \binom{d+i-s-1}{d-1} \qquad (\dagger)$$

with $\binom{r}{d-1} = 0$ for $r < d-1$. RHS can be rearranged to give $\phi(i)$ for $\phi(t) \in \mathbb{Q}[t]$ valid for $d+i-s-1 \geq d-1$.

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

Note $f(1) \neq 0$ and so degree of $\phi(t)$ is $d-1$.

Using ($\dagger$) we can produce an expression for $\sum_{j \leq i} \lambda(V_j)$,

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

using $\binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n}$ and so

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

This is $\chi(t)$ for $\chi(t) \in \mathbb{Q}[t]$ of degree d. □

Example. Let $S = k[X_1, \dots, X_m]$ be a polynomial algebra over a field k, graded by total degree. The number of monomials of total degree i is $\binom{i+m-1}{m-1}$ for all $i \geq 0$. Thus the Hilbert polynomial is

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

of degree $m-1$. Then $d(S) = m$ with respect to this grading.

Our aim is to apply the theorem to P-adic filtrations of a Noetherian ring R where P is a maximal ideal. The filtration is P^j for $-j$th term of filtration and R for positive terms. The associated graded ring is

$$\operatorname{gr} R = \bigoplus_{i \in \mathbb{Z}} R_i / R_{i-1} = \bigoplus P^j / P^{j+1}.$$

Renumber so that this is positively graded and we can apply Hilbert-Serre. Note that $S_0 = R/P$ is a field since P is maximal. If $S_1 = P/P^2$ then S_0 and S_1 generate $S = \operatorname{gr} R$. Then can take $\lambda = \dim_K$ since P^i/P^{i+1} is a R/P-vector space. The corollary applies and we have Hilbert and Samuel polynomials

$$\phi(i) = \dim_K(P^i/P^{i+1}) \text{ for large enough } i$$

$$\chi(i) = \sum_{j=0}^{i} \dim_K(P^j/P^{i+1}) = \text{ composition length of } R/P^{i+1}$$

Definition. For a Noetherian ring R with a maximal ideal P, define $d_P(R) = d(\operatorname{gr} R)$.

This equals to $\deg \chi(t) = 1 + \deg \phi(t)$. Note that this depends on the choice of maximal ideal P.

Remark. We state without proof some facts about dimensions.

1. For a Noetherian local ring we have a unique maximal ideal P, and so can suppress P. In fact $d(R) = \dim R$ when R is an integral domain.
2. For general Noetherian R, $d_P(R) = d(R_P)$ and so for integral domains $d_P(R) = d(R_P) = \dim R_P = \operatorname{ht} P$.
3. From example sheet 3 for a finitely generaetd k-algebra R which is an integral domain, all maximal ideals are of height $\dim R$ and so we deduce $d_P(R) = \dim R$ for all maximal ideal P.
4. For a finitely generated R-module M and maximal ideal P of R, we can consider the P-adic filtration of M (P^iM). Define $d(M) = d(\operatorname{gr} M)$ so we have a dimension for M. If $N \leq M$ is a submodule then there is a filtration induced on N from P-adic filtration on M $(N \cap P^iM)$ and we can again form the associated graded module. Reassuringly the value of $d(N)$ obtained from this filtration and obtained from the P-adic filtration on N are the same. The proof relies on Artin-Rees lemma, which is on example sheet 3.

7 Homological algebra

R is a commutative ring with a 1, but most of time doesn't need to be.

We've already seen that if we apply $N \otimes_R -$ to a short exact sequence it may not remain exact. We defined flat modules N to be those where exactness is preserved for all short exact sequences. We also considered $\mathrm{Hom}_R(N, -)$ and $\mathrm{Hom}_R(-, N)$. If $0 \longrightarrow M_1 \longrightarrow M \longrightarrow M_2 \longrightarrow 0$ then we get

$$0 \longrightarrow \mathrm{Hom}(N, M_1) \longrightarrow \mathrm{Hom}(N, M) \longrightarrow \mathrm{Hom}(N, M_2) \longrightarrow 0$$

$$0 \longrightarrow \mathrm{Hom}(M_2, N) \longrightarrow \mathrm{Hom}(M, N) \longrightarrow \mathrm{Hom}(M_1, N) \longrightarrow 0$$

but these need not be exact. We do have exactness at left and middle terms but not necessarily on right. For example if $R = \mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z}$ then

$$0 \longrightarrow 2\mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

we get non-exactness.

> **Definition** (projective module)**.** A module P is *projective* if for any map $\phi : P \to M_2$ there is a map $P \to M$ which composes with $M \to M_2$ to give ϕ.
>
> $$\begin{tikzcd} & P \arrow[dl, dotted] \arrow[d, "\phi"] & \\ M \arrow[r] & M_2 \arrow[r] & 0 \end{tikzcd}$$
>
> Equivalently, $\mathrm{Hom}(P, -)$ preserves exactness of short exact sequences.

Dually

> **Definition** (injective module)**.** A module E is *injective* if $\mathrm{Hom}(-, E)$ preserves exactness of short exact sequences.
>
> $$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r] \arrow[d, "\phi"] & M \arrow[dl, dotted] \\ & E & \end{tikzcd}$$

Example.

1. Free modules are projective.
2. The fraction field of an integral domain R is an injective R-module.

> **Lemma 7.1.** *For an R-module P, TFAE:*
>
> 1. *P is projective.*
> 2. $\mathrm{Hom}(P, -)$ *preserves exactness of short exact sequences.*
> 3. *If $\epsilon : M \to P$ is surjective then there exists $\beta : P \to M$ with $\epsilon\beta = \mathrm{id}$.*

> 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.

- $1 \implies 2$: by definition.
- $2 \implies 3$: we have a short exact sequence

  $$0 \longrightarrow \ker \epsilon \longrightarrow M \xrightarrow{\epsilon} P \longrightarrow 0$$

  then

  $$0 \longrightarrow \mathrm{Hom}(P, \ker \epsilon) \longrightarrow \mathrm{Hom}(P, M) \longrightarrow \mathrm{Hom}(P, P) \longrightarrow 0$$

  is also exact and so exists $\beta : P \to M$ such that $\varepsilon\beta = \mathrm{id}$.
- $3 \implies 4$: suppose $P = M/M_1$ and so we have a short exact sequence

  $$0 \longrightarrow M_1 \longrightarrow M \xrightarrow{\alpha} P \longrightarrow 0$$

  so there exists $\beta : P \to M$ such that $\alpha\beta = \mathrm{id}$. Thus P is a direct summand of M.
- $4 \implies 5$: given P we can define a free module F on e_{x_λ} where $\{x_\lambda\}$ is a generating set of P. $F \to P, e_{x_\lambda} \mapsto x_\lambda$ gives an R-module map so P is a direct summand of F.
- $5 \implies 1$: there exists F free such that $F = P \oplus Q$. Free modules are projective and Hom behaves well with respect to direct summand and so P is projective.

□

Remark.

1. Given a PID, every finitely generated projective module is free (using structure theorem of finitely generated modules over PID).
2. There is a similar result giving equivalent statements for injective modules. See example sheet 4.
3. Projective modules, being direct summands of free modules, are flat.

> **Definition** (projective/free presentation)**.** A *projective presentation* of M is a short exact sequence
>
> $$0 \longrightarrow K \longrightarrow P \longrightarrow M \longrightarrow 0$$
>
> with P projective. K is called the *syzygy module.* It is a *free presentation* if P is free.

Remark. The proof of $4 \implies 5$ shows how to produce a free presentation of a module.

> **Definition** (Tor, Ext)**.** Given a projective presentation of M, apply $N \otimes -$ to get
>
> $$N \otimes K \longrightarrow N \otimes P \longrightarrow N \otimes M \longrightarrow 0$$
>
> Define $\operatorname{Tor}^R(N, M) = \ker(N \otimes K \to N \otimes P)$.
>
> Apply $\operatorname{Hom}_R(-, N)$ to get
>
> $$0 \longrightarrow \operatorname{Hom}(M, N) \longrightarrow \operatorname{Hom}(P, N) \longrightarrow \operatorname{Hom}(K, N)$$
>
> Define $\operatorname{Ext}_R(M, N) = \operatorname{coker}(\operatorname{Hom}(P, N) \to \operatorname{Hom}(K, N))$.

Thus if N is flat $\operatorname{Tor}^R(N, M) = 0$ for all M and if E is injective $\operatorname{Ext}_R(M, E) = 0$ for all M. If P is projective then $\operatorname{Ext}_R(P, N) = 0$ for all N (if we have a projective presentation of P

$$0 \longrightarrow K \longrightarrow P' \longrightarrow P \longrightarrow 0$$

but P is a direct summand of P' and so if we apply $\operatorname{Hom}(-, N)$ we still have a short exact sequence and so we get $\operatorname{Ext}_R(P, N) = 0$).

Remark.

1. Tor and Ext are independent of choice of projective presentation. See example sheet 4.
2. One may take a projective presentation of N and apply $- \otimes_R M$ to it. The analogous kernel is isomorphic to $\operatorname{Tor}(N, M)$.
3. Similarly we could have taken a short exact sequence

   $$0 \longrightarrow N \longrightarrow E \longrightarrow L \longrightarrow 0$$

   with E injective and consider $\operatorname{coker}(\operatorname{Hom}(M, E) \to \operatorname{Hom}(M, L))$. This is isomorphic to $\operatorname{Ext}(M, N)$.

Example. The $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ has free presentation

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Apply $\mathbb{Z}/2\mathbb{Z} \otimes -$ to get

$$\operatorname{Tor}^{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) = \ker(\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Apply $\operatorname{Hom}_{\mathbb{Z}}(-, N)$ for N a $\mathbb{Z}$-module,

$$\operatorname{Ext}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, N) = \operatorname{coker}(\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \xrightarrow{\cdot 2} \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, N)) = \operatorname{coker}(N \xrightarrow{\cdot 2} N) \cong N/2N.$$

Remark.

1. The name Ext is derived from the alternative characterisation that $\operatorname{Ext}(M, N)$ is the equivalence classes of *extensions* of M by N, namely short exact sequences of the form

   $$0 \longrightarrow N \longrightarrow X \longrightarrow M \longrightarrow 0$$

and two extensions are equivalent if exists an R-module map θ such that the following diagram commmutes:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r] \arrow[d, "\mathrm{id}"] & X_1 \arrow[r] \arrow[d, "\theta"] & M \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & N \arrow[r] & X_2 \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Note θ is necessarily an isomorphism. On example sheet 4 we will show $\mathrm{Ext}(M, N)$ is isomorphic to equivalence of classes of extensions of M by N (one can define a sum of extensions, the *Baer sum*, and the zero element is direct sum).

For example if $R = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z}, N = \mathbb{Z}/2\mathbb{Z}$ then $\mathrm{Ext}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, corresponding to the two equivalence classes of extensions $\mathbb{Z}/2 \oplus \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$.

2. The name Tor is a bit less clear. It is ultimately derived from $R = \mathbb{Z}$. If A is an abelian group, then the torsion subgroup is isomorphic to $\mathrm{Tor}(\mathbb{Q}/\mathbb{Z}, A)$.

3. When R is commutative, $N \otimes_R M$ and $\mathrm{Hom}_R(M, N)$ are R-modules, and so $\mathrm{Tor}(N, M)$ and $\mathrm{Ext}(M, N)$ are R-modules. In general they are additive groups but not necessarily R-modules.

Example.

1. Let $R = k[X]$. Then k is a trivial $k[X]$-module where X acts trivially. Then we have projective presentation

$$\begin{tikzcd}
0 \arrow[r] & k[X] \arrow[r] & k[X] \arrow[r] & k \arrow[r] & 0 \\
& g(X) \arrow[r, mapsto] & Xg(X) & &
\end{tikzcd}$$

2. Let $R = k[X, Y]$. Then

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] & k[X,Y] \arrow[r] & k \arrow[r] & 0 \\
& & f(X,Y) \arrow[r, mapsto] & f(0,0) &
\end{tikzcd}$$

where K is the ideal generated by X and Y.

K has projective presentation

$$\begin{tikzcd}
0 \arrow[r] & k[X,Y] \arrow[r] & k[X,Y] \oplus k[X,Y] \arrow[r] & K \arrow[r] & 0 \\
& & (g,h) \arrow[r, mapsto] & Xg + Yh & \\
& f \arrow[r, mapsto] & (Yf, -Xf) & &
\end{tikzcd}$$

We can take $F_0 = F_2 = k[X, Y], F_1 = k[X, Y] \oplus k[X, Y]$ and put everything together to get an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & F_2 \arrow[r] & F_1 \arrow[r] & F_0 \arrow[r] & k \arrow[r] & 0
\end{tikzcd}$$

Definition (projective/free resolution). A *projective resolution* of an R-module M is an exact sequence of the form

$$\cdots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

with P_i's projective. It is a *free presentation* if all P_i's are free.

Remark.

1. We just constructed a free resolution of the $k[X,Y]$-module k.
2. If R is Noetherian and M is a finitely generated R-module, then we saw how to construct a free presentation of M using a generating set. This can be taken to be finite and the syzygy module K is then a finitely generated R-module. Repeating for K etc gives a free resolution for M where all P_i's are free of finite rank.

Definition (Koszul complex). The *Koszul complex* gives a free resolution of the trivial R-module k where $R = k[X_1, \dots, X_n]$. Define F_i to be free R-module on a basis $e_{j_1,\dots,j_i}$ where $\{j_1, \dots, j_i\}$ is a subset of $\{1, \dots, n\}$ of size i. We define an R-module map

$$\begin{aligned} F_i &\to F_{i-1} \\ e_{j_1,\dots,j_i} &\mapsto \sum_{\ell=1}^{i} (-1)^{\ell-1} X_{j_\ell} e_{j_1,\dots,\hat{j}_\ell,\dots,j_i} \end{aligned}$$

Note that this is what we did in the case of $k[X]$ and $k[X,Y]$. It is an exercise to check this this complex is exact and therefore gives a free resolution.

Now we go on to define higher Ext and Tor. There are two approaches. The first is by iternation the previous definition.

Definition (Tor, Ext). We define

$$\operatorname{Tor}_i(N,M) = \begin{cases} N \otimes M & i = 0 \\ \operatorname{Tor}(N,M) & i = 1 \\ \operatorname{Tor}_{i-1}(N,K) & i \geq 2 \end{cases}$$

where K is the syzygy module in a projective presentation for M. Similarly we define

$$\operatorname{Ext}^i(M,N) = \begin{cases} \operatorname{Hom}(M,N) & i = 0 \\ \operatorname{Ext}(M,N) & i = 1 \\ \operatorname{Ext}^{i-1}(K,N) & i \geq 2 \end{cases}$$

The alternative way is to put the presentations for syzygy module K_i together to get a projective resolution for M

$$\cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

Apply $N \otimes -$ to get

$$\cdots \longrightarrow N \otimes P_i \xrightarrow{\theta_i} \cdots \longrightarrow N \otimes P_1 \longrightarrow N \otimes P_0 \longrightarrow N \otimes M \longrightarrow 0$$

which need not be exact but $\operatorname{im}\theta_i \subseteq \ker\theta_{i-1}$ and we can consider the homology groups $\ker\theta_{i-1}/\operatorname{im}\theta_i$ and these are the $\operatorname{Tor}_i(N, M)$ for $i \geq 1$.

Similarly applying $\operatorname{Hom}(-, N)$ to our projective resolution of M gives

$$0 \longrightarrow \operatorname{Hom}(M, N) \longrightarrow \operatorname{Hom}(P_0, N) \longrightarrow \cdots$$

and $\operatorname{Ext}^i(M, N)$ arises as the cohomology group of the complex.

Remark. These are independent of the choice of presentations/resolutions.

Lemma 7.2. *TFAE:*

1. $\operatorname{Ext}^{n+1}(M, N) = 0$ *for all R-modules N.*
2. *M has a projective resolution of length n, i.e. it has a projective resolution of the form*

$$0 \longrightarrow P_n \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

Proof. Induction on n. For $n = 1$, $\operatorname{Ext}^2(M, N) = 0$ for all N if and only if $\operatorname{Ext}(K, N) = 0$ for N where N is the syzygy module in a projective resolution for M, if and only if K is projective, if and only if M has a projective resolution of length 1.

For general n, $\operatorname{Ext}^{n+1}(M, N) = 0$ for all N if and only if $\operatorname{Ext}^n(K, N) = 0$ for all N, if and only if K has a projective resolution of length $n - 1$, if and only if M has a projective resolution of length n. □

Definition (projective dimension)**.** The *projective dimension* of M is n if $\operatorname{Ext}^{n+1}(M, N) = 0$ for all N but exists N such that $\operatorname{Ext}^n(M, N) \neq 0$.

Example. Koszul complex gives a free resolution of the trivial $k[X_1, \dots, X_n]$-module k and we can deduce $\operatorname{projdim}(k) = n$.

Definition (global dimension)**.** The *global dimension* of R is the supremum of projective dimensions for all finitely generated R-modules M.

Example.

1. $\operatorname{gldim} k = 0$ since all finitely generated k-modules are free.
2. $\operatorname{gldim} R = 1$ if R is a PID which isn't a field: consider free presentation of a finitely generated R-module then the syzygy module must be free.
3. $\operatorname{gldim} k[X_1, \dots, X_n] = n$. We will not prove this.

> **Theorem 7.3** (Hilbert syzygy theorem). *Let k be a field and $R = k[X_1, \dots, X_n]$ considered as a graded k-algebra using by degree. Let M be a finitely generated graded R-module. Then there is a free resolution of M of length $\leq n$.*

Proof. The proof relies on some properties of Tor that we take on trust. The Koszul complex gives a free resolution of the trivial module k of length n. We'll consider $\mathrm{Tor}_i(k, M)$ in two different ways by either taking a resolution for k (the Koszul complex) or taking a resolution for M. Either apply $- \otimes M$ to the Koszul complex and consider homology groups, or apply $k \otimes -$ to a projective resolution for M.

We can take a free resolution of M

$$\cdots \longrightarrow F_i \longrightarrow F_{i-1} \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M$$

with each F_i of finite rank. Moreover, we may assume it is minimal in the sense that the rank is minimal at each stage, for example $\mathrm{rk}(F_0)$ equals to the minimal number of generators of M. This is called a *minimal free resolution* for M. The crucial point is that if we consider

$$0 \longrightarrow K \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

where K is the first syzygy module, then after applying $k \otimes -$ the map $k \otimes K \to k \otimes F_0$ is the zero map. Indeed if we take a homogeneous element of K and it is mapped to $(p_1, \dots, p_n) \in F_0$. Each p_i is a homogeneous polynomial. Since K is the syzygy module, if say p_n is constant then since k is a field we can write the nth generator of M in terms of other generators, contradicting minimality of F_0.

Hence after tensoring with the trivial module

$$\cdots \longrightarrow k \otimes F_i \longrightarrow k \otimes F_{i-1} \longrightarrow \cdots \longrightarrow k \otimes F_0 \longrightarrow k \otimes M$$

we get a zero complex except the last map. Thus the homology groups are $k \otimes F_i$, which is a k-vector space of dimension equal to the rank of F_i.

However we know $\mathrm{Tor}_i(k, M) = 0$ for $i \geq n+1$ by tensor the Koszul complex with M. Thus we conclude in our minimal resolution F_i is of rank 0 for $i \geq n+1$, so it has length $\leq n$. □

7.1 Hochschild (co)homology

Hochschild (co)homology is the (co)homology theory for (R, R)-bimodules where R is a k-algebra. An (R, R)-bimodule M (R acting on left and right and the two actions commute) may be viewed as a right $R \otimes_k R^{\mathrm{op}}$-module. R^{op} is the k-algebra with the same elements as R but

$$r \cdot_{R^{\mathrm{op}}} s = s \cdot_R r.$$

Therefore a (R, R)-bimodule is a right $R \otimes R^{\mathrm{op}}$-module via

$$rms = m(s \otimes r).$$

Simiarly M can be regarded as a left $R \otimes R^{\mathrm{op}}$-module.

Example.

1. If R is commutative then $R^{\mathrm{op}} = R$.
2. If $R = kG$ then $R^{\mathrm{op}} \cong R$ via $\sum \lambda_g g \mapsto \sum \lambda_g g^{-1}$.

Note.

1. R itself is an (R, R)-bimodule.
2. $R \otimes_k R$ is an (R, R)-bimodule. Regard it as a right $R \otimes R^{\mathrm{op}}$-module then it is freely generated by $1 \otimes 1$. Thus we regard $R \otimes_k R$ as the free (R, R)-bimodule of rank 1.
3. There is a free presentation of R as a bimodule

   $$0 \longrightarrow \ker \mu \longrightarrow R \otimes_k R \xrightarrow{\mu} R \longrightarrow 0$$

   where μ is the multiplication $r \otimes s \to rs$.

Definition (separable algebra)**.** R is a *separable k-algebra* if R is a projective (R, R)-bimodule (or equivalently projective right $R \otimes R^{\mathrm{op}}$-module). Thus R can be regarded as a direct summand of $R \otimes_k R$.

Note that a finite field extension K of k is k-separable if and only if it is a separable field extension of k. See example sheet 4.

Remark. Hochschild (co)homology has the advantage that it applies to any k-algebra R, not just to ones where there is a canonical map $R \to k$. Also note the multiplication in the algebra R is encoded clearly in the resolution of R.

Definition (Hochschild chain complex)**.** The *Hochschild chain complex* gives a free resolution for the bimodule R

$$\longrightarrow R \otimes R \otimes R \otimes R \xrightarrow{d} R \otimes R \otimes R \xrightarrow{d} R \otimes R \xrightarrow{\mu} R \longrightarrow 0$$

where

$$\begin{aligned} d : R^{\otimes n+2} &\to R^{\otimes n+1} \\ r_0 \otimes \cdots \otimes r_{n+1} &\mapsto \sum_{i=0}^{n} (-1)^i r_0 \otimes \cdots \otimes r_{i-1} \otimes r_i r_{i+1} \otimes \cdots \otimes r_{n+1} \end{aligned}$$

Definition (Hochschild (co)homology)**.** Given an (R, R)-bimodule M, define *Hochschild homology* to be

$$\mathrm{HH}_i(R, M) = \mathrm{Tor}_i^{R,R}(R, M) = \mathrm{Tor}_i^{R \otimes R^{\mathrm{op}}}(R, M)$$

and *Hochschild chomology* to be

$$\mathrm{HH}^i(R, M) = \mathrm{Ext}^i_{R,R}(R, M) = \mathrm{Ext}^i_{R \otimes R^{\mathrm{op}}}(R, M)$$

Observe that we need to regard R and its resolution as right $R \otimes R^{\mathrm{op}}$-modules and M as a left $R \otimes R^{\mathrm{op}}$-module so that we can form the tensor product $R \otimes_{R \otimes R^{\mathrm{op}}} M$.

In particular

$$\begin{aligned}
\mathrm{HH}^0(R, M) &= \mathrm{Hom}_{R,R}(R, M) = \{m \in M : rm = mr \text{ for all } r \in R\} \\
\mathrm{HH}^0(R, R) &= \{s \in R : rs = sr \text{ for all } r \in R\} = Z(R) \\
\mathrm{HH}_0(R, M) &= R \otimes_{R \otimes R^{\mathrm{op}}} M \cong M/\langle rm - mr : m \in M, r \in R\rangle \\
\mathrm{HH}_0(R, R) &= R/[R, R]
\end{aligned}$$

where $[r, s] = rs - sr$ is the *Lie bracket* on R.

> **Definition** (Hochschild cohomological dimension)**.** The (Hochschild cohomological) *dimension* $\dim R$ of R is
>
> $$\dim R = \sup\{n : \mathrm{HH}^n(R, M) \neq 0 \text{ for some bimodule } M\}.$$

Remark. A separable k-algebra R is equivalently a k-algebra R such that $\mathrm{HH}^i(R, M) = 0$ for $i \geq 1$ and all M.

Example.

1. $M_n(k)$, the matrix algebra over k, is k-separable. In general given a section $\nu : R \to R \otimes R$, the image of 1 is called a *separating idempotent*. For $M_n(k)$ a separating idempotent is obtained as follow: let E_{ij} be the elementary matrix which has 1 at ijth entry and 0 otherwise. Fix j and consider $\sum_i E_{ij} \otimes E_{ji}$. This is a separating idempotent. Note that the image of the under μ is the identity matrix.

2. For G a finite group, $\mathbb{C}G$ is $\mathbb{C}$-separable:

   $$\mathbb{C}G \otimes \mathbb{C}G^{\mathrm{op}} \cong \mathbb{C}G \otimes \mathbb{C}G \cong \mathbb{C}(G \times G)$$

   which is semisimple (or completely reducible), so all submodules are direct summands. In particular we get $\mathbb{C}G$ as a direct summand of $\mathbb{C}(G \times G)$. Thus $\dim(\mathbb{C}G) = 0$.

Now consider higher dimensions. Note that

$$\mathrm{Hom}_{R \otimes R}(R \otimes R, M) \cong \mathrm{Hom}_k(k, M).$$

On LHS a map is determined by the image of $1 \otimes 1$, and on RHS it is determined by 1. More generally

$$\mathrm{Hom}_{R \otimes R}(\underbrace{R \otimes \cdots \otimes R}_{n+2}, M) \cong \mathrm{Hom}_k(\underbrace{R \otimes \cdots \otimes R}_{n}, M).$$

> **Definition** (Hochschild cochain complex)**.** The *Hochschild cochain complex* is
>
> $$M \cong \mathrm{Hom}_k(k, M) \xrightarrow{\delta_0} \mathrm{Hom}_k(R, M) \xrightarrow{\delta_1} \mathrm{Hom}_k(R \otimes R, M) \longrightarrow \cdots$$

where

$$\begin{aligned}(\delta_0 f)(r) &= rf(1) - f(1)r\\ (\delta_1 f)(r_1 \otimes r_2) &= r_1 f(r_2) - f(r_1 r_2) + f(r_1)r_2\\ (\delta_2 f)(r_1 \otimes r_2 \otimes r_3) &= r_1 f(r_2 \otimes r_3) - f(r_1 r_2 \otimes r_3) + f(r_1 \otimes r_2 r_3) - f(r_1 \otimes r_2)r_3\end{aligned}$$

and so on.

Definition (derivation, inner derivation)**.**

$$\ker \delta_1 = \{f \in \operatorname{Hom}_k(R, M) : f(r_1 r_2) = r_1 f(r_2) + f(r_1) r_2\}$$

is called the *derivations* from R to M and is denoted $\operatorname{Der}(R, M)$.

$$\operatorname{im} \delta_0 = \{f \in \operatorname{Hom}_k(R, M) \text{ of the form } r \mapsto rm - mr \text{ for some } m \in M\}$$

is called the *inner derivations* and is denoted $\operatorname{Innder}(R, M)$.

Thus

$$\operatorname{HH}^1(R, M) = \frac{\operatorname{Der}(R, M)}{\operatorname{Innder}(R, M)}.$$

If $M = R$ we get

$$\operatorname{HH}^1(R, R) = \frac{\operatorname{Der}(R)}{\operatorname{Innder}(R)}.$$

If R is commutative then $\operatorname{Innder} R = 0$ and so $\operatorname{HH}^1(R, R) = \operatorname{Der} R$.

In general, $\operatorname{Der} R$ forms a Lie algebra: if D_1, D_2 are derivations $R \to R$ then so is $D_1 D_2 - D_2 D_1 \in \operatorname{End}_k R$.

Definition (semidirect product)**.** Given an (R, R)-bimodule M, we can form a *semidirect product* $R \ltimes M$ as follow: the underlying set is $R \times M$, addition is pairwise addition, multiplication is

$$(r_1, m_1) \cdot (r_2, m_2) = (r_1 r_2, r_1 m_2 + m_1 r_2).$$

Alternatively you can think of this as $R + M\varepsilon$ where $\varepsilon^2 = 0$ and ε commutes with everything. The ideal $M\varepsilon$ in $R + M\varepsilon$ satisfies $(M\varepsilon)^2 = 0$.

Lemma 7.4.

$$\operatorname{Der}(R, M) \cong \{\textit{algebra complements to } M \textit{ in } R \ltimes M\}.$$

Proof. A complement to M is an embedded copy of R in $R \ltimes M$ with some embedding

$$\begin{aligned}R &\hookrightarrow R \ltimes M\\ r &\mapsto (r, D(r))\end{aligned}$$

The map $D : R \to M$ is a derivation. Conversely a derivation $D : R \to M$ gives an emedding of R in $R \ltimes M$. □

Corollary 7.5. *Identify*

$$\begin{aligned}\mathrm{Der}(R,M) &= \{\textit{automorphism of } R \ltimes M \textit{ sending } r \mapsto (r, D(r)), m \mapsto (0,m)\}\\ &= \{\textit{automorphism of } R + M\varepsilon \textit{ sending } r \mapsto r + D(r)\varepsilon, m\varepsilon \mapsto m\varepsilon\}\end{aligned}$$

where we make a choice of isomorphism $R \ltimes M \to R + M\varepsilon, r \mapsto r, m \mapsto m\varepsilon$. Then Innder$(R,M)$ *is the set of automorphisms of $R + M\varepsilon$ of obtained by conjugation by $1 + m\varepsilon$.*

Example. $R = k[X]$ with $\operatorname{char} k = 0$. Then

$$\operatorname{Der} R = \{p(X)\frac{d}{dX} : p(X) \in k[X]\}.$$

For a commutative k-algebra R, we define the differential operators inductively

$$\begin{aligned}\mathcal{D}^0(R) &= \{D \in \mathrm{End}_k(R) : [r, D] = 0 \text{ for all } r \in R\}\\ \mathcal{D}^{i+1}(R) &= \{D \in \mathrm{End}_k(R) : [r, D] \in \mathcal{D}^i \text{ for all } r \in R\}\end{aligned}$$

and define

$$\mathcal{D}(R) = \bigcup_i \mathcal{D}^i(R).$$

In geometry we have D-modules, which are modules of differential operators.

Example. Let $R = k[X]$. Then

$$\mathcal{D}(R) = k[X, \frac{d}{dX}] \subseteq \mathrm{End}_k(R).$$

If $R = k[X_1, \dots, X_n]$ then

$$\mathcal{D}(R) = k[X_1, \frac{\partial}{\partial X_1}, \dots, X_n, \frac{\partial}{\partial X_n}]$$

by a messy induction.

Exercise. Work out $\mathcal{D}(k[X])$ when $\operatorname{char} k = p > 0$.

Theorem 7.6 (Hochschild-Kostant-Rosenberg)**.** *Let $R = k[X_1, \dots, X_n]$, $\operatorname{char} k = 0$. Then* $\mathrm{HH}^*(R,R) \cong \Lambda \operatorname{Der}(R)$*, the exterior algebra of* $\operatorname{Der}(R)$*.*

Index