Commutative Algebra

Shing Tak Lam

Michaelmas 2023*

Contents

Lecture 1

In this course, a ring is a commutative unital ring R. One non-commutative exception is the ring $\mathrm{End}(M)$, where M is an abelian group. This is a ring with pointwise addition, and composition as multiplication.

*Based on lectures by Oren Becker. Last updated December 22, 2023.

Definition 0.0.1 (module)
An R-*module* M is an abelian group M with an fixed ring homomorphism $\rho : R \to \text{End}(M)$. We will write $r \cdot m := \rho(r)(m)$.

Remark 0.0.2. By definition, this implies that $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$, $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$ and $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$.

Example 0.0.3 (Examples of modules)

- Let k be a field. Then a k-module is the same as a k-vector space.
- Every abelian group is a $\mathbb{Z}$-module in a unique way, since we must have that $\rho(1) = \text{id}_M$. Therefore, abelian groups and $\mathbb{Z}$-modules are the same thing.
- Every ring R is (trivially) an R-module.
- More generally, $R^{\oplus \mathbb{N}}$ (direct sum) and $R^{\mathbb{N}}$ (direct product) are R-modules.

Another useful example to keep in mind is that if I is an ideal in R, then R/I is an R-module.

1 Chain conditions

Definition 1.0.1 (Noetherian, Artinian module)
An R-module M is *Noetherian* if one of the following (equivalent) conditions hold:

1. Every ascending chain of submodules $M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots$ stabilises. That is, it is eventually constant.
2. Every non-empty set Σ of submodules of M has a maximal element.

M is *Artinian* if we replace in the above: ascending with descending, maximal with minimal.

Lemma 1.0.2. An R-module M is Noetherian if and only if every submodule of M is finitely generated.

In particular, every Noetherian module is finitely generated. If $R = \mathbb{Z}[T_1, T_2, \dots]$, with $M = R$ as an R-module. Then M is finitely generated. On the other hand, $M' = \langle T_1, T_2, T_3, \dots \rangle$, is not finitely generated.

Definition 1.0.3 (Noetherian, Artinian ring)
A ring R is Noetherian (resp. Artinian) if it is Noetherian (resp. Artinian) as an R-module.

Example 1.0.4

1. $\mathbb{Z}$ is Noetherian (as it is a PID), but not Artinian (e.g. $\langle 2 \rangle \supseteq \langle 4 \rangle \supseteq \langle 8 \rangle \supseteq \cdots$).
2. $\mathbb{Z}[1/2]/\mathbb{Z}$ is Artinian, but not Noetherian as a $\mathbb{Z}$-module.
3. A ring R is Artinian if and only if R is Noetherian and R has Krull dimension 0.

Definition 1.0.5 (Exact sequence)

A sequence

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

of R-modules and R-module homomorphisms is *exact* if $\mathrm{im}(f_i) = \ker(f_{i+1})$ for all i.

Definition 1.0.6 (Short exact sequence)
A *short exact sequence* (SES) is an exact sequence of the form

$$0 \longrightarrow N \overset{\iota}{\hookrightarrow} M \twoheadrightarrow L \longrightarrow 0$$

That is, we have an embedding $\iota : N \hookrightarrow M$, and an isomorphism $L \cong M/\iota(N)$.

Lemma 1.0.7. Let

$$0 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 0$$

be an SES of R-modules. Then M is Noetherian (resp. Artinian) if and only if N and L are Noetherian (resp. Artinian).

Proof. We may assume without loss of generality that N is a submodule of M. Let $P_1 \subseteq P_2 \subseteq \ldots$ be an increasing (resp. decreasing) sequence of submodules of M. In this case,

$$N \cap P_1 \subseteq N \cap P_2 \subseteq \cdots$$

is an increasing (resp. decreasing) sequence of submodules of N, hence eventually constant. Similarly,

$$\frac{N + P_1}{N} \subseteq \frac{N + P_2}{N} \subseteq \cdots$$

is an increasing (resp. decreasing) sequence of submodules of $L = M/N$, hence eventually constant. For large n, we will have

$$P_n \subseteq P_{n+1} \quad N \cap P_n = N \cap P_{n+1} \quad N + P_n = N + P_{n+1}$$

Hence $P_n = P_{n+1}$ for large enough n. □

Corollary 1.0.8. If $M_1, \ldots, M_n$ are Noetherian (resp. Artinian) R-modules, then $M_1 \oplus \cdots \oplus M_n$ is Noetherian (resp. Artinian).

Proof. By the lemma and induction. □

Recall a module homomorphism

$$\varphi : M_1 \oplus \cdots \oplus M_n \to L$$

is the same as a collection of module homomorphism $\varphi_i : M_i \to L$. This is also true for infinite direct sums (but not products!).

Proposition 1.0.9. For a Noetherian (resp. Artinian) ring R, every finitely generated R-module is Noetherian (resp. Artinian).

Proof. M is finitely generated if and only if there exists a surjection $R^n \twoheadrightarrow M$ for some $n \in \mathbb{N}$. The fact that R^n is Noetherian (resp. Artinian) implies that M is Noetherian (resp. Artinian), as quotients of Noetherian (resp. Artinian) modules are Noetherian (resp. Artinian). This follows by the correspondence theorem. □

Definition 1.0.10 (algebra)
An R-*algebra* A is a ring A with a fixed ring homomorphism $\rho : R \to A$. We will write $r \cdot a := \rho(r)a$.

Definition 1.0.11 (noetherian algebra)
An R-algebra A is *Noetherian* if it is Noetherian as a ring.

Remark 1.0.12. Every R-algebra is an R-module.

Example 1.0.13
The polynomial ring $k[T_1, \ldots, T_n]$ is a k-algebra. Do note however that it is a finitely generated by $T_1, \ldots, T_n$ as a k-algebra, but it is infinite dimensional as a k-vector space.

Definition 1.0.14 (algebra homomorphism)
$\varphi : A \to B$ is an R-*algebra homomorphism* if φ is a ring homomorphism and $\varphi(r \cdot 1_A) = r \cdot 1_B$.

Equivalently, it is a ring homomorphisms which is also an R-linear map.

Definition 1.0.15 (finitely generated algebra)
An R-algebra A is *finitely generated* if there exists a surjective R-algebra homomorphism $R[T_1, \ldots, T_n] \twoheadrightarrow A$ for some $n \in \mathbb{N}$.

Lecture 2

Theorem 1.0.16 (Hilbert basis theorem)**.** Every finitely generated algebra A over a Noetherian ring R is Noetherian (as a ring).

For example, if k is a field, then $k[T_1, \ldots, T_n]$ is Noetherian.

Proof. It suffices to prove for $A = R[T_1, \ldots, T_n]$, since every finitely generated algebra is a quotient of $R[T_1, \ldots, T_n]$. Moreover, by induction, suffices to prove the result for $A = R[T]$.

Let $\mathfrak{a}$ be an ideal of $A = R[T]$. For every $i \geq 0$, define

$$\mathfrak{a}(i) = \left\{ c_0 \mid c_0 t^i + \cdots + c_i t^0 \in \mathfrak{a} \right\}$$

for the set of all leading coeffients of elements of degree i in $\mathfrak{a}$ (and containing 0). In this case, $\mathfrak{a}(i) \subseteq R$ is an ideal, and we have an ascending chain of ideals

$$\mathfrak{a}(i) \subseteq \mathfrak{a}(i+1) \subseteq \cdots$$

Since R is Noetherian, each $\mathfrak{a}$ is finitely generated (as an ideal), and the ascending sequence of ideal stabilises. That is,

$$\mathfrak{a}(m') = \mathfrak{a}(m)$$

for all $m' \geq m$. We write $\mathfrak{a}(i) = \langle b_{i,1}, \ldots, b_{i,m_i} \rangle$, where $b_{i,j} \in R$. Let $f_{i,j} \in \mathfrak{a}$ be a polynomial of degree i, with leading coefficient $b_{i,j}$. Define the new ideal

$$\mathfrak{b} = \left\langle f_{i,j} \mid i \leq m, 1 \leq j \leq m_i \right\rangle \trianglelefteq R[T]$$

In this case, $\mathfrak{b}(i) = \mathfrak{a}(i)$ for all i. By construction, $\mathfrak{b} \subseteq \mathfrak{a}$.

Suppose for contradiction that $\mathfrak{a} \nsubseteq \mathfrak{b}$. Take $f \in \mathfrak{a} \setminus \mathfrak{b}$ of minimal degree i. But $\mathfrak{b}(i) = \mathfrak{a}(i)$, and so there exists $g \in \mathfrak{b}$, of degree i, and with the same leading coefficient as f. That is, $\deg(f - g) < i$. By minimality, $f - g \in \mathfrak{b}$, and so $f = (f - g) + g \in \mathfrak{b}$. Contradiction. $\square$

Therefore, if we have a subset $S \subseteq R[T_1, \ldots, T_n]/I$, then $\langle S \rangle = \langle S_0 \rangle$, where $S_0 \subseteq S$ is finite.

2 Tensor products

Let M, N be R-modules. An informal definition of their tensor product is

$$M \otimes_R N = \left\{ \sum_{i=1}^{\ell} m_i \otimes n_i \;\middle|\; m_i \in M, n_i \in N \right\}$$

where we have the relations $(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n$, $m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2$, and that for $r \in R$, $(rm) \otimes n = r(m \otimes n) = m \otimes (rn)$.

For example, consider $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3$. Then

$$x \otimes y = (3x) \otimes y = x \otimes (3y) = x \otimes 0 = 0$$

and so, $\mathbb{Z}/2 \otimes_{\mathbb{Z}} \mathbb{Z}/3 = 0$. On the other hand, if we have vector spaces, then

$$\mathbb{R}^m \otimes_{\mathbb{R}} \mathbb{R}^\ell \cong \mathbb{R}^{m\ell}$$

Recall $f : M \times N \to L$ is R-*bilinear* if $n \mapsto f(m_0, n)$ and $m \mapsto f(m, n_0)$ are R-linear for all $m_0 \in M, n_0 \in N$.

Definition 2.0.1 (tensor product of modules)
Let M, N be R-modules, let

$$\mathcal{F} = R^{\oplus(M\times N)} = \operatorname{span}_R \left\{ e_{(m,n)} \mid m \in m, n \in N \right\}$$

be the free module indexed by $m \times n$, and define $\mathcal{K} \subseteq \mathcal{F}$ for the submodule generated by the relations (where we write (m, n) for $e_{(m,n)}$)

$$\begin{aligned} (m, n_1) + (m, n_2) &= (m, n_1 + n_2) \\ (m_1, n) + (m_2, n) &= (m_1 + m_2, n) \\ r(m, n) &= (rm, n) \\ r(m, n) &= (m, rn) \end{aligned}$$

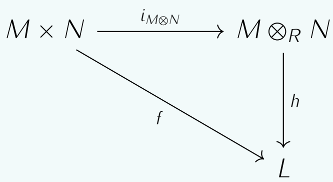
The *tensor product* is

$$M \otimes_R N := \frac{\mathcal{F}}{\mathcal{K}}$$

We have an R-bilinear map

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

Proposition 2.0.2 (universal property of tensor product)**.** For every R-module L and any R-bilinear map $f : M \times N \to L$, there exists a unique R-linear $h : M \otimes N \to L$, making the diagram



commute.

Proof. Uniqueness is clear, since we must have that

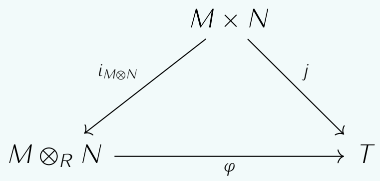
$$h(m \otimes n) = f(m, n)$$

since the pure tensors generate, h must be unique, if it exists. Therefore, suffices to show the above extends to an R-linear map $M \otimes_R N \to L$. This follows from the map

$$\begin{aligned} R^{\oplus(M\times N)} &\to L \\ e_{(m,n)} &\mapsto f(m,n) \end{aligned}$$

extending to a linear map (by the universal property of the direct sum), and that this map vanishes on $\mathcal{K}$. Therefore, h extends to $M \otimes_R N$ from the pure tensors. □

Proposition 2.0.3. Let M, N be R-modules, T an R-module, $j : M \times N \to T$ an R-bilinear map, (T, j) satisfying the universal property of tensors. Then there exists a unique R-linear isomorphism $\varphi : M \otimes N \to T$, such that



commutes.

Proof. By the universal property of tensor product, such a map φ exists, with $\varphi(m \otimes n) = j(m, n)$. Similarly, we have a homomorphism $\psi : T \to M \otimes_R N$. In particular,

$$\psi \circ \varphi \circ i_{M\otimes N} = i_{M\otimes N} = \mathrm{id}_{M\otimes N} \circ i_{M\otimes N}$$

In particular, by uniqueness in the universal property, we must have that $\psi \circ \varphi = \mathrm{id}_{M\otimes N}$. □

Lecture 3

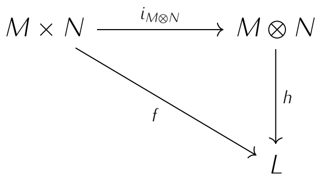
Proposition 2.0.4. Suppose M, N are R-modules, then

$$\sum_i m_i \otimes n_i = 0 \in M \otimes_R N$$

if and only if for all R-modules L, and every R-bilinear map $f : M \times N \to L$ has

$$\sum_i f(m_i, n_i) = 0$$

Proof. Suppose $\sum m_i \otimes n_i = 0$, let $f : M \times N \to L$ be bilinear. Then f factors through $M \times N \to M \otimes_R N$, and we can write



In this case, we have that

$$\sum_i f(m_i, n_i) = \sum_i h(i(m,n)) = \sum_i h(m_i \otimes n_i) = h\left(\sum_i m_i \otimes n_i\right) = h(0) = 0$$

Conversly, if

$$\sum_i m_i \otimes n_i \neq 0$$

then by definition,

$$\sum_i i_{m\otimes n}(m_i, n_i) \neq 0$$

□

Example 2.0.5

Let k be a field, and consider the tensor product

$$k^m \otimes k^\ell$$

Suppose k^m has basis $\{e_1, \dots, e_m\}$, and k^ℓ has basis $\{f_1, \dots, f_\ell\}$, then

$$k^m \otimes k^\ell = \operatorname{span}_k\{v \otimes w \mid v \in k^m, w \in k^\ell\} = \operatorname{span}_k \{e_i \otimes f_j\}$$

Claim 2.0.6. $\{e_i \otimes f_j\}$ is a basis.

Proof. Suppose we have

$$\sum_{ij} \alpha_{ij}(e_i \otimes f_j) = 0$$

For every $1 \leq a \leq m, 1 \leq b \leq \ell$, define a bilinear map

$$T_{ab} : k^m \times k^\ell \to k$$
$$T_{ab}((v_i), (w_j)) = v_a w_b$$

This is a k-bilinear map. By proposition 2.0.4,

$$0 = \sum_{i,j} \alpha_{ij} T_{ab}(e_i, f_j) = \sum_{i,j} \alpha_{ij}\delta_{ia}\delta_{jb} = \alpha_{ab}$$

□

Example 2.0.7

More concretely, let us consider $\mathbb{R}^2 \otimes \mathbb{R}^2$. We have a basis of size 4, given by

$$e_1 \otimes f_1, e_1 \otimes f_2, e_2 \otimes f_1, e_2 \otimes f_2$$

What do pure tensors look like?

$$(\alpha e_1 + \beta e_2) \otimes (\gamma f_1 + \delta f_2) = \alpha\gamma(e_1 \otimes f_1) + \alpha\delta(e_1 \otimes f_2) + \beta\gamma(e_2 \otimes f_1) + \beta\delta(e_2 \otimes f_2)$$

These are not generic elements of $\mathbb{R}^2 \otimes \mathbb{R}^2$, since the vectors

$$(\alpha\gamma, \alpha\delta) \quad \text{and} \quad (\beta\gamma, \beta\delta)$$

are linearly dependent. In particular,

$$e_1 \otimes f_1 + 2e_1 \otimes f_2 + 3e_2 \otimes f_1 + 4e_2 \otimes f_2$$

is *not* a pure tensor.

Example 2.0.8 (warning)

First consider

$$\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2$$

In this case,

$$2 \otimes 1 = 1 \otimes 2 = 1 \otimes 0 = 0$$

Now consider

$$2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2$$

But in this case,

$$2 \otimes 1 \neq 0$$

since we can define a bilinear map

$$B : 2\mathbb{Z} \times \mathbb{Z}/2 \to \mathbb{Z}/2$$
$$B(2m, x) = mx$$

In this case,

$$B(2, 1) = 1 \cdot 1 = 1 \neq 0$$

However, if $M' \leq M, N' \leq N$ are submodules, and

$$\sum_i m_i \otimes n_i = 0$$

in $M' \otimes N'$, then

$$\sum_i m_i \otimes n_i = 0$$

in $M \otimes N$.

Proposition 2.0.9. If

$$\sum m_i \otimes n_i = 0 \in M \otimes_R N$$

then there are finitely generated R-submodules $M' \leq M, N' \leq N$, such that

$$\sum m_i \otimes n_i = 0 \in M' \otimes_R N'$$

Intuitively, a proof that the sum is zero is finite, and so it can only involve finitely many expressions. We can take them to be the generators.

Proof.

$$\sum m_i \otimes n_i = 0 \in M \otimes N = \frac{R^{\oplus(M \times N)}}{\mathcal{K}}$$

then

$$\sum_i e_{(m_i, n_i)} = 0 \in \mathcal{K}$$

This means that we can write the left hand side as a finite sum of the generators of $\mathcal{K}$. Taking all the elements of M and N which appear, gives the result. □

Corollary 2.0.10. Let A, B be torsion-free abelian groups, then $A \otimes_{\mathbb{Z}} B$ is torsion free.

Proof. Suppose

$$n \cdot \left(\sum_i a_i \otimes b_i \right) = 0 \in A \otimes B$$

for some $n \geq 1$. By proposition 2.0.9, there exists finitely generated subgroups $A' \leq A, B' \leq B$, such that

$$n \cdot \left(\sum_i a_i \otimes b_i \right) = 0 \in A' \otimes B'$$

By the structure theorem of finitely generated abelian groups, $A' \cong \mathbb{Z}^r, B' \cong \mathbb{Z}^s$, and so we have that

$$A' \otimes B' \cong \mathbb{Z}^{rs}$$

which is torsion free. Contradiction. □

Example 2.0.11

$$\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^3 \cong \mathbb{C}^6$$

as $\mathbb{C}$-vector spaces, and we also have that $\mathbb{C}^6 \cong \mathbb{R}^{12}$ as $\mathbb{R}$-vector spaces. On the other hand,

$$\mathbb{C}^2 \otimes_{\mathbb{R}} \mathbb{C}^3 \cong \mathbb{R}^4 \otimes_{\mathbb{R}} \mathbb{R}^6 \cong \mathbb{R}^{24}$$

Proposition 2.0.12.
1. $M \otimes N \cong N \otimes N$
2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$, where we define $M \otimes N \otimes P$ using trilinear maps.
3. $\left(\bigoplus_i M_i\right) \otimes P \cong \bigoplus_i (M_i \otimes P)$
4. $R \otimes_R M \cong M$,

Proof. See examples sheet 1. □

Example 2.0.13

Using proposition 2.0.12, we can compute

$$\begin{aligned} R^m \otimes R^\ell &\cong \left(\oplus_{i=1}^m R\right) \otimes \left(\oplus_{j=1}^\ell R\right) \\ &\cong \oplus_{i,j} R \\ &\cong R^{m\ell} \end{aligned}$$

2.1 Tensor product of R-linear maps

Proposition 2.1.1. For R-linear maps $f : M \to M', g : N \to N'$, then there exists a unique R-linear map

$$f \otimes g : M \otimes N \to M' \otimes N'$$

with

$$(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$$

Proof. Uniqueness is clear since the pure tensors generate. For existence, we can use the universal property on the R-bilinear map

$$\begin{aligned} T : M \times N &\to M' \otimes N' \\ T(m,n) &= f(m) \otimes g(n) \end{aligned}$$

□

Lecture 4

Exercise: $(f \otimes g) \circ (h \otimes i) = (f \circ h) \otimes (h \circ i)$. We can check this in pure tensors, since they generate. But the statement is clear in that case.

Example 2.1.2

Let $T : k^a \to k^c$ and $S : k^b \to k^d$ be linear. Then

$$(T \otimes S)(e_i \otimes e_j) = T(e_i) \otimes S(e_j) = \sum_{\ell,t} [T]_{\ell i}[S]_{tj}(f_\ell \otimes f_t)$$

where $[T]$ is the matrix representation of T. If we order the basis of $k^a \otimes k^b$ by

$$e_1 \otimes e_1, \dots, e_1 \otimes e_c, e_2 \otimes e_1, \dots, e_2 \otimes e_c, \dots, e_a \otimes e_c$$

and a similar ordering for the range, then

$$[T \otimes S] = \begin{pmatrix} [T]_{11}S & \cdots & [T]_{1a}S \\ \vdots & \ddots & \vdots \\ [T]_{c1}S & \cdots & [T]_{ca}S \end{pmatrix}$$

is the *Kronecker product* of $[T]$ and $[S]$.

Proposition 2.1.3. Let $f : M \to M'$, $g : N \to N'$ be $\mathbb{R}$-linear.

(i) If f, g are isomorphisms, then so is $f \otimes g$,

(ii) if f and g are surjective, so is $f \otimes g$.

Proof. For (i), $(f^{-1} \otimes g^{-1}) = (f \otimes g)^{-1}$, since we have that $(f \otimes g) \circ (h \otimes i) = (f \circ h) \otimes (h \circ i)$.

For (ii), notice that $\operatorname{im}(f \otimes g)$ contains all pure tensors in $M' \otimes N'$. □

Example 2.1.4

If $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = pn$, then we have

$$(f \otimes \mathrm{id}) : \mathbb{Z} \otimes \mathbb{Z}/p \to \mathbb{Z} \otimes \mathbb{Z}/p$$

is the zero map, as

$$(f \otimes \mathrm{id})(a \otimes b) = (pa) \otimes b = a \otimes (pb) = a \otimes 0 = 0$$

But $\mathbb{Z} \otimes \mathbb{Z}/p \cong \mathbb{Z}/p$ which is nonzero.

2.2 Tensor product of algebras

Let B, C be R-algebras. Then we have $B \otimes_R C$ as an R-module. We would like to define the multiplication by

$$(b \otimes c)(b' \otimes c') = (bb') \otimes (cc')$$

This is well-defined. Fix $(b, c) \in B \times \mathbb{C}$, then we have a bilinear map

$$\begin{aligned} B \times C &\to B \otimes C \\ (b', c') &\mapsto (bb') \otimes (cc') \end{aligned}$$

which gives us a map $B \otimes C \to B' \otimes C'$, with

$$b' \otimes c' \mapsto (bb') \otimes (cc')$$

It is easy to show that this then satisfies the ring axioms. Hence $B \otimes C$ is a ring. The R-algebra structure will be given by

$$\begin{aligned} R &\to B \otimes C \\ r &\mapsto (r1_B) \otimes 1_C = r(1_B \otimes 1_C) = 1_B \otimes (r1_C) \end{aligned}$$

Example 2.2.1

There is an isomorphism

$$\varphi : R[x_1, \dots, x_n] \otimes_R R[t_1, \dots, t_r] \cong R[x_1, \dots, x_n, t_1, \dots, t_r]$$

Proof. We have an R-basis for the left hand side, which is

$$x^k \otimes t^\ell$$

and we also have a R-basis for the right hand side,

$$x^k t^\ell$$

Define

$$\varphi(x^k \otimes t^\ell) = x^k t^\ell$$

which gives us a R-module isomorphism. Moreover,

$$\varphi(r \otimes 1) = r1 = 1$$

and by distributivity, suffices to show

$$\varphi((x^k \otimes t^\ell)(x^m \otimes t^n)) = x^k t^\ell x^m t^n$$

which is clear by definition. □

More generally,

$$\frac{R[x_1, \dots, x_n]}{I} \otimes \frac{R[t_1, \dots, t_r]}{J} \cong \frac{R[x_1, \dots, x_n, t_1, \dots, t_r]}{L} \cong \frac{R[x_1, \dots, x_n, t_1, \dots, t_r]}{I^e + J^e}$$

where $I^e = \langle I \rangle \trianglelefteq R[x_1, \dots, x_n, t_1, \dots, t_r]$ denotes the extension of I.

Example 2.2.2

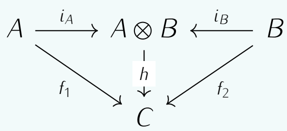
$\frac{\mathbb{C}[x,y,z]}{\langle f,g \rangle} \otimes \frac{\mathbb{C}[w,u]}{h}$ is isomorphic as $\mathbb{C}$-algebras to

$$\frac{\mathbb{C}[x, y, z, w, u]}{\langle f, g, h \rangle}$$

Proposition 2.2.3 (universal property of tensor product of algebras)**.** Let A, B be R-algebras, for every R-algebra C, and R-algebra homomorphisms $f_1 : A \to C$ and $f_2 : B \to C$, there exists a unique R-algebra map

$$h : A \otimes B \to C$$

such that



commutes, where $i_A(a) = a \otimes 1$, $i_B(b) = 1 \otimes b$. Moreover, this characterises $(A \otimes B, i_A, i_B)$ uniquely (up to isomorphism).

Proof. $A \otimes B$ is generated, as an R-algebra, by

$$\{a \otimes 1 \mid a \in A\} \cup \{1 \otimes b \mid b \in B\}$$

This then implies the uniqueness of h, as it defines h on the generators. For the existence, define the bilinear map $A \times B \to C$, given by

$$f(a, b) = f_1(a) f_2(b)$$

Using the universal property of tensor product of modules, there exists $h : A \otimes B \to C$ which is R-linear, with

$$h(a \otimes b) = f_1(a) f_2(b)$$

It is then easy to show that h is an algebra homomorphism. □

Consider $R[x_1, \dots, x_n, t_1, \dots, t_r]$ from above. We have natural embeddings from $R[x_1, \dots, x_n]$ and $R[t_1, \dots, t_n]$. Given f_1, f_2 as above, we see that the image of the x_i is determined by f_1, and the image of t_i is determined by f_2. Therefore,

$$R[x_1, \dots, x_n, t_1, \dots, t_r] \cong \mathbb{R}[x_1, \dots, x_n] \otimes R[t_1, \dots, t_r]$$

as it satisfies the universal property.

Lecture 5

If we have $f : A \to A', g : B \to B'$ which are algebra homomorphisms, then the tensor product of R-linear maps,

$$f \otimes g : A \otimes B \to A' \otimes B'$$

is an R-algebra homomorphism. Moreover, we have R-algebra isomorphisms

- $(R/I) \otimes (R/J) \cong R/(I + J)$
- $A \otimes B \cong B \otimes A$,
- $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$,
- $A \otimes B^n \cong (A \otimes B)^n$,

2.3 Restriction and extension of scalars

Restriction of scalars

We will have a ring homomorphisms $f : R \to S$, let M be an S-module, so M is also an R-module,

$$r \cdot m := f(r)m$$

for $r \in R, m \in M$. The fact that this is a module is clear by our definition, since it is just the composition

$$R \xrightarrow{\ f\ } S \longrightarrow \mathrm{End}(M)$$

Example 2.3.1
If we consider the embedding $\mathbb{R} \hookrightarrow \mathbb{C}$, then $\mathbb{C}^n$ is a C-vector space, but also an $\mathbb{R}$-vector space, of dimension $2n$.

Extension of scalars

Let $f : R \to S$ be a ring homomorphism, M be an S-module (thus an R-module by restriction of scalars), N is an R-module. From this, we can form

$$M \otimes_R N$$

which is an R-module. In fact, $M \otimes_R N$ is also an S-module, with

$$s \cdot (m \otimes n) := (sm) \otimes n$$

Is this well defined? We have an R-bilinear map

$$\begin{aligned} M \times N &\to M \otimes_R N \\ (m, n) &\mapsto (sm) \otimes n \end{aligned}$$

By the universal property, we have a map

$$h_s : M \otimes_R N \to M \otimes_R N$$

which is R-linear, and $h_s(m \otimes n) = (sm) \otimes n$. Now define

$$\begin{aligned} \varphi : S &\to \mathrm{End}(M \otimes_R N) \\ \varphi(s) &= h_s \end{aligned}$$

Which is a ring homomorphism, and so, we have an S-module structure on $M \otimes_R N$.

Example 2.3.2

We know from before that $S \otimes_R R \cong S$ as R-module, with

$$s \otimes r \mapsto s \cdot f(r)$$

But in fact, this is also S-linear, since

$$s' \cdot (s \otimes r) = (s's) \otimes r \mapsto s's \cdot f(r)$$

For example, this implies that

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R} \cong \mathbb{C}$$

as $\mathbb{C}$-vector spaces.

Example 2.3.3

If M is an S-module, N_i are R-modules, then

$$M \otimes_R \left(\bigoplus_i N_i \right) \cong \bigoplus_i (M \otimes_R N_i)$$

as S-modules.

In this case,

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \cong \mathbb{C}^n$$

as $\mathbb{C}$-vector spaces.

Example 2.3.4

Consider $\mathbb{C}^n$ as a $\mathbb{C}$-module. Restricting to $\mathbb{R}$,

$$\mathbb{C}^n \cong \mathbb{R}^{2n}$$

as $\mathbb{R}$-vector spaces. Now extending scalars,

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^{2n} \cong \mathbb{C}^{2n}$$

as $\mathbb{C}$-vector spaces.

Example 2.3.5

Now consider $\mathbb{R}^n$ as an $\mathbb{R}$-vector space. Extending scalars,

$$\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C}^n$$

over $\mathbb{C}$. Restricting to $\mathbb{R}$,

$$\mathbb{C}^n \cong \mathbb{R}^{2n}$$

Example 2.3.6

Consider $\mathbb{Z}^n$ as an $\mathbb{Z}$-module, and let $f : \mathbb{Z} \to \mathbb{Z}/2$ be the quotient map. Extending scalars,

$$(\mathbb{Z}/2) \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong (\mathbb{Z}/2)^n$$

Example 2.3.7
Consider
$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell$$
One way to compute this:
$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \cong_{\mathbb{R}} \mathbb{R}^{2n} \otimes \mathbb{R}^\ell \cong_{\mathbb{R}} \mathbb{R}^{2n\ell} \cong_{\mathbb{R}} \mathbb{C}^{n\ell}$$
where $\cong_{\mathbb{R}}$ denotes isomorphism as $\mathbb{R}$-vector spaces. Another way to do this:
$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \cong_{\mathbb{C}} \mathbb{C}^n \otimes_{\mathbb{C}} \left(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^\ell\right) \cong_{\mathbb{C}} \mathbb{C}^n \otimes \mathbb{C}^\ell \cong_{\mathbb{C}} \mathbb{C}^{n\ell}$$
The first isomorphism is given by
$$v \otimes u \mapsto v \otimes (1 \otimes u)$$
Combining these, the isomorphism $\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \to \mathbb{C}^n \otimes \mathbb{C}^\ell$ sends
$$v \otimes u \mapsto v \otimes u$$
where we use the inclusion $\mathbb{R}^\ell \hookrightarrow \mathbb{C}^\ell$.

Proposition 2.3.8. Let M be an S-module, N be an R-module, then
$$M \otimes_R N \cong M \otimes_S (S \otimes_R N)$$
as S-modules. In particular, the isomorphism is given by
$$\begin{aligned} m \otimes n &\mapsto m \otimes (1 \otimes n) \\ (sm) \otimes n &\leftarrow m \otimes (s \otimes n) \end{aligned}$$

Intuitively, what this is saying is that we only need to consider the special case of extension by scalars, which is $N \otimes_R S$.

Proposition 2.3.9. Let M, M' be S-modules, N, N' be R-modules, then we have S-module isomorphisms

(i) $M \otimes_R N \cong N \otimes_R M$, via $m \otimes n \to n \otimes m$

(ii) $(M \otimes_R N) \otimes_R N' \cong M \otimes_R (N \otimes_R N')$

(iii) $(M \otimes_R N) \otimes_S M' \cong M \otimes_S (N \otimes_R M')$

(iv) $M \otimes_R (\bigoplus_i N_i) \cong \bigoplus_i (M \otimes_R N_i)$

Proof. We will prove (iii). Using proposition 2.3.8, we have
$$\begin{aligned} (M \otimes_R N) \otimes_S M' &\cong (M \otimes_S (N \otimes_R S)) \otimes_S M' \\ &\cong M \otimes_S \left((N \otimes_R S) \otimes_S M'\right) \\ &\cong M \otimes_S (N \otimes_R M') \end{aligned}$$
□

Example 2.3.10
As $\mathbb{C}$-vector spaces,
$$\mathbb{C} \otimes_{\mathbb{R}} (\mathbb{R}^\ell \otimes_{\mathbb{R}} \mathbb{R}^k) \cong (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^\ell) \otimes_{\mathbb{C}} (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^k) \cong \mathbb{C}^\ell \otimes \mathbb{C}^k \cong \mathbb{C}^{\ell k}$$

Corollary 2.3.11. If N, N' are R-modules, then

$$S \otimes_R (N \otimes N') \cong_S (S \otimes_R N) \otimes_S (S \otimes N')$$

Proof. By proposition 2.3.8 and proposition 2.3.9 (ii):

$$S \otimes_R (N \otimes_{\mathbb{R}} N') \cong (S \otimes_R N) \otimes_R N' \cong (S \otimes_R N) \otimes_S (S \otimes_R N')$$

□

Lecture 6

By induction, we have that

$$S \otimes_R (N_1 \otimes_R \cdots \otimes_R N_\ell) \cong (S \otimes_R N_1) \otimes_S \cdots \otimes_S (S \otimes_R N_1)$$

Extension of scalars for morphisms

Let $f : N \to N'$ be R-linear, where N, N' are R-modules, M is an S-module. Then we have a map

$$\mathrm{id} \otimes f : M \otimes_R N \to M \otimes_R N'$$

In particular, it is S-linear, as

$$(\mathrm{id} \otimes f)(s(m \otimes n)) = (\mathrm{id} \otimes f)((sm) \otimes n) = (sm) \otimes f(n) = s(m \otimes f(n)) = s(\mathrm{id} \otimes f)(m \otimes n)$$

Given $T : \mathbb{R}^n \to \mathbb{R}^\ell$ which is an $\mathbb{R}$-linear map, $\mathbb{R}^n$ with basis $e_1, \ldots, e_n$ and $\mathbb{R}^\ell$ with basis $f_1, \ldots, f_\ell$. In this case, consider

$$\mathrm{id} \otimes T : \mathbb{C} \otimes \mathbb{R}^n \to \mathbb{C} \otimes \mathbb{R}^\ell$$

Note that $\mathbb{C} \otimes \mathbb{R}^n$ has basis $1 \otimes e_1, \ldots, 1 \otimes e_n$. In particular,

$$(\mathrm{id} \otimes T)(1 \otimes e_i) = 1 \otimes T(e_i) = 1 \otimes \sum_{j=1}^{\ell} T_{ji} f_j = \sum_{j=1}^{\ell} T_{ji}(1 \otimes f_j)$$

Thus, T and $\mathrm{id} \otimes T$ have the same matrix representation.

Extension of scalars of algebras

Let A, B be R-algebras. Recall that in this case, $A \otimes_R B$ is also an R-algebra. In fact, $A \otimes_R B$ is an A-algebra (and by symmetry a B-algebra). For example, we have

$$\begin{aligned} A &\to A \otimes_R B \\ a &\mapsto a \otimes 1 \end{aligned}$$

Example 2.3.12

$S \otimes_R R[x_1, \ldots, x_n] \cong_S S[x_1, \ldots, x_n]$ (where $\cong_S$ denotes isomorphism of S-algebras).

Proof. We already have an S-module isomorphism

$$\varphi : S \otimes_R R[x_1, \ldots, x_n] \to S[x_1, \ldots, x_n]$$

with $\varphi(s \otimes f) = sf$. It is easy to show that

$$\varphi(s \otimes 1) = s$$

and that φ preserves multiplication. □

More generally, we have that

$$S \otimes \left(\frac{R[x_1, \ldots, x_n]}{I} \right) \cong \frac{S[x_1, \ldots, x_n]}{I^e}$$

where $I^e = \langle f(I) \rangle$ is the ideal generated by I under the ring homomorphism $f : R \to S$.

Proposition 2.3.13. Suppose A is an R-algebra, B is an S-algebra, then $A \otimes_R B$ is an S-algebra. Moreover,

$$A \otimes_R B \cong_{S\text{-alg}} (A \otimes_R S) \otimes B$$

Proof. $A \otimes_R B$ is a B-algebra, and we can then restrict scalats to S. The isomorphism is clear from the module case, as all we need to check is it preserves multiplication. □

Proposition 2.3.14. Suppose A, B are R-algebras, then

$$S \otimes_R (A \otimes_R B) \cong_{S\text{-alg}} (S \otimes_R A) \otimes_S (S \otimes_R B)$$

2.4 Exactness properties of the tensor product

Let M be a fixed R-module. Define

$$\mathrm{T}_M(N) = M \otimes_R N$$

where N is an R-module. If $f : N \to N'$ is R-linear, then we have an induced map

$$\mathrm{T}_M(f) = \mathrm{id}_M \otimes f : \mathrm{T}_M(N) \to \mathrm{T}_M(N')$$

Suppose we have an exact sequence

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

of R-modules. We will show that we have an exact sequence

$$\mathrm{T}_M(A) \xrightarrow{\mathrm{T}_M(f)} \mathrm{T}_M(B) \xrightarrow{\mathrm{T}_M(g)} \mathrm{T}_M(C) \longrightarrow 0$$

That is, T_M is a *right exact functor* from R-modules to R-modules.

Definition 2.4.1 (Hom)
Suppose Q, P are R-modules, then we can define

$$\mathrm{Hom}_R(Q, P) = \{f : Q \to P \mid f \text{ is } R\text{-linear}\}$$

This is an R-module itself, with

$$(r \cdot \varphi)(q) = r \cdot \varphi(q)$$

Definition 2.4.2 (Hom functors)
We have two functors,

1. $\mathrm{Hom}_R(Q, \cdot)$, where Q is a fixed R-module,
2. $\mathrm{Hom}_R(\cdot, P)$, where P is a fixed R-module.

Suppose we have $f : N \to N'$ which is R-linear, then the action on morphisms are

$$\begin{aligned} \mathrm{Hom}_R(Q, f) : \mathrm{Hom}_R(Q, N) &\to \mathrm{Hom}_R(Q, N') \\ \varphi &\mapsto f \circ \varphi =: f_*(\varphi) \end{aligned}$$

On the other hand, $\mathrm{Hom}_R(\cdot, P)$ is contravariant. That is,

$$\begin{aligned}\mathrm{Hom}_R(f, P) : \mathrm{Hom}_R(N', P) &\to \mathrm{Hom}_R(N, P)\\ \varphi &\mapsto \varphi \circ f =: f^*(\varphi)\end{aligned}$$

Proposition 2.4.3 (left exactness of the Hom-functors)**.**

1. If
$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$$
is exact, then so is
$$0 \longrightarrow \mathrm{Hom}_R(Q, A) \xrightarrow{\mathrm{Hom}_R(Q,f)} \mathrm{Hom}_R(Q, B) \xrightarrow{\mathrm{Hom}_R(Q,g)} \mathrm{Hom}_R(Q, C)$$

2. If
$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$
is exact, then so is
$$0 \longrightarrow \mathrm{Hom}_R(C, P) \xrightarrow{\mathrm{Hom}_R(g,P)} \mathrm{Hom}_R(B, P) \xrightarrow{\mathrm{Hom}_R(f,P)} \mathrm{Hom}_R(A, P)$$

In both cases, we say that the respective Hom functor is *left exact*.

Proof. Omitted. □

Lemma 2.4.4. Consider a (not necessarily exact) sequence

$$A \xrightarrow{f} B \xrightarrow{g} C$$

and suppose for all R-module P, the sequence

$$\mathrm{Hom}_R(C, P) \longrightarrow \mathrm{Hom}_R(B, P) \longrightarrow \mathrm{Hom}_R(A, P)$$

is exact, then the original sequence is exact.

Proof. **Step 1:** let $P = C$. Then we get the sequence

$$\mathrm{Hom}_R(C, C) \longrightarrow \mathrm{Hom}_R(B, C) \longrightarrow \mathrm{Hom}_R(A, C)$$

which is exact by assumption. Under this,

$$\mathrm{id}_C \mapsto \mathrm{id}_C \circ g = g \mapsto g \circ f$$

Thus, we have that $g \circ f = 0$, and so $\mathrm{im}(f) \subseteq \ker(g)$.

Step 2: Let $P = \mathrm{coker}\, f = \frac{B}{\mathrm{im}(f)}$. In this case, we have

$$\mathrm{Hom}(C, \mathrm{coker}(f)) \longrightarrow \mathrm{Hom}(B, \mathrm{coker}(f)) \longrightarrow \mathrm{Hom}(A, \mathrm{coker}(f))$$

Let $h : B \to \mathrm{coker}(f)$ denote the quotient map. Then $h \circ f = 0$, and so by exactness, there exists $e : C \to \mathrm{coker}(f)$, with

$$\mathrm{Hom}(g, \mathrm{coker}(f))(e) = e \circ g = h$$

In particular, $\ker(g) \subseteq \ker(h) = \mathrm{im}(f)$. □

Recall that we have a bijection $\mathrm{Hom}_R(M \otimes_R N, L) \cong \mathrm{Bil}(M \times N, L)$ from the universal property of the tensor product. But

$$\mathrm{Bil}(M \times N, L) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, L))$$

and so we have an isomorphism

$$\mathrm{Hom}_R(M \otimes N, L) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, L))$$

sending φ to $n \mapsto (m \mapsto \varphi(m \otimes n))$

Lecture 7

Proposition 2.4.5. Let M be an R-module. Then T_M is a right exact functor.

Proof. Given an exact sequence

$$A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Fix an R-module P. We will apply the functors $\mathrm{Hom}_R(\cdot, P)$, then the functor $\mathrm{Hom}_R(M, \cdot)$, to get the sequence

$$0 \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(C, P)) \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(B, P)) \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(A, P))$$

which is exact as the Hom functors are left exact. Using the isomorphism above, and noting that the square

$$\begin{array}{ccc} \mathrm{Hom}_R(M, \mathrm{Hom}_R(C, P)) & \longrightarrow & \mathrm{Hom}_R(M, \mathrm{Hom}_R(B, P)) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_R(M \otimes C, P) & \longrightarrow & \mathrm{Hom}_R(M \otimes B, P) \end{array}$$

commutes, we have an exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(M \otimes C, P) \longrightarrow \mathrm{Hom}(M \otimes B, P) \longrightarrow \mathrm{Hom}(M \otimes A, P)$$

Since P is arbitrary, using lemma 2.4.4, we see that

$$\mathrm{T}_M(A) \longrightarrow \mathrm{T}_M(B) \longrightarrow \mathrm{T}_M(C) \longrightarrow 0$$

is exact, as required. □

Remark 2.4.6. Note on the other hand that

$$A \longrightarrow B \longrightarrow C$$

being exact does not imply that

$$\mathrm{T}_M(A) \longrightarrow \mathrm{T}_M(B) \longrightarrow \mathrm{T}_M(C)$$

is exact.

For example, consider the exact sequence

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

This is exact, but

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

is not.

2.5 Flat modules – a first encounter

Definition 2.5.1 (flat module)
An R-module M is *flat* if for any injective R-module homomorphism $N \to N'$, the map $\mathrm{T}_M(f) : \mathrm{T}_M(N) \to \mathrm{T}_M(N')$ is injective.

Example 2.5.2

$\mathbb{Z}/2$ is not a flat $\mathbb{Z}$-module, as seen in the remark above.

Example 2.5.3

Free modules are flat. To see this, suppose $f : N \to N'$ is an injective R-linear map. Then we have the commuting square

$$\begin{array}{ccc} R^{\oplus I} \otimes N & \xrightarrow{\mathrm{id} \otimes f} & R^{\oplus I} \otimes N' \\ \updownarrow & & \updownarrow \\ (R \otimes N)^{\oplus I} & & (R \otimes N')^{\oplus I} \\ \updownarrow & & \updownarrow \\ N^{\oplus I} & \xrightarrow{f^{\oplus I}} & (N')^{\oplus I} \end{array}$$

where the vertical maps are isomorphisms, and

$$f^{\oplus I}((n_i)_{i \in I}) = (f(n_i))_{i \in I}$$

It is clear that $f^{\oplus I}$ is injective.

Remark 2.5.4. With this, we see that the base ring matters. $\mathbb{Z}/2$ is not a flat $\mathbb{Z}$-module, but it is a flat $\mathbb{Z}/2$-module as it is free.

Definition 2.5.5 (torsion free)

An R-module is *torsion free* if for any $r \in R, m \in M$, $rm = 0$ implies that $m = 0$ or r is a zero divisor.

Proposition 2.5.6. Flat modules are torsion free.

Proof. Suppose M was not torsion free. Then there exists $r_0 \in R, m_0 \in M$ with r_0 not a zero divisor, $m_0 \neq 0$, such that $r_0 m_0 = 0$. We can define a map

$$f : R \to R$$
$$f(x) = r_0 x$$

f is injective as r_0 is not a zero divisor. Thus, we have the square

$$\begin{array}{ccc} M \otimes R & \xrightarrow{\mathrm{id} \otimes f} & M \otimes R \\ \updownarrow & & \updownarrow \\ M & \xrightarrow[r_0 \cdot]{} & M \end{array}$$

But the bottom map is not injective, as it sends m_0 to zero. □

For a specical case of the above:

Proposition 2.5.7. Let R be an integral domain, I a non-zero, non-unit ideal. Then R/I is not flat.

Proof. Since $I \neq R$, R/I is non-zero. Choose $x \in I \setminus 0$, and consider the map

$$f : R \to R$$
$$f(r) = xr$$

This is an injective map. But the induced map on $R \otimes (R/I) \cong R/I$ is multiplication by x, which is the zero map. □

Proposition 2.5.8 (criterion for flatness). Let M be an R-module. Then teh following are equivalent:

(i) T_M preserves exactness of all exact sequences,

(ii) T_M preserves exactness of short exact sequences,

(iii) T_M is flat,

(iv) if $f : N \to N'$ is R-linear and injective, N, N' are finitely generated R-modules, then $\mathrm{id}_M \otimes f$ is injective.

Proof. (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) is clear.

For (ii) $\implies$ (i), suppose

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is exact, then we have a short exact sequence

$$0 \longrightarrow \frac{A}{\ker(f)} \xrightarrow{\bar{f}} B \xrightarrow{g} \mathrm{im}(g) \longrightarrow 0$$

Thus, we have a short exact sequence

$$0 \longrightarrow M \otimes \frac{A}{\ker(f)} \longrightarrow M \otimes B \longrightarrow M \otimes \mathrm{im}(g) \longrightarrow 0$$

That is, $\ker(\mathrm{id}_M \otimes g) = \mathrm{im}(\mathrm{id}_M \otimes \bar{f}) = \mathrm{im}(\mathrm{id}_M \otimes f)$. Thus the sequence

$$M \otimes A \longrightarrow M \otimes B \longrightarrow M \otimes C$$

is exact.

We will omit the proof of (iv) $\implies$ (iii), it can be found in the lecturer's notes.

For (iii) $\implies$ (ii), we note that this follows from T_M being right exact. □

Proposition 2.5.9. Let $f : R \to S$ be a ring homomorphism, M is a flat R-module. Then $S \otimes_R M$ is a flat S-module.

Proof. Let $g : N \to N'$ be an injective S-linear map. Then the square

$$\begin{array}{ccc} (S \otimes_R M) \otimes_S N & \longrightarrow & (S \otimes_R M) \otimes_S N' \\ \updownarrow & & \updownarrow \\ M \otimes_R N & \longrightarrow & M \otimes_R N' \end{array}$$

commutes. But the bottom map is injective as M is flat. □

Lecture 8

2.6 Further examples of tensor products

Example 2.6.1

First consider $x \otimes y \in \mathbb{Q} \otimes_Z (\mathbb{Z}/n)$. We can write

$$x \otimes y = n\frac{x}{n} \otimes y = \frac{x}{n} \otimes ny = 0$$

and so, $\mathbb{Q} \otimes_{\mathbb{Z}} (\mathbb{Z}/n) = 0$. We used the fact that $\mathbb{Q}$ is a *divisible group*, that is, for all $x \in \mathbb{Q}, n \in \mathbb{N}$, there exists $y \in \mathbb{Q}$ such that $ny = x$. Moreover, we also used the fact that $\mathbb{Z}/n$ is torsion.

More generally,

$$\text{divisible} \otimes \text{torsion} = 0$$

and so

$$(\mathbb{Q}/\mathbb{Z}) \otimes_Z (\mathbb{Q}/\mathbb{Z})$$

But for an R-module M which is non-zero, if M is finitely generated, then $M \otimes_R M \neq 0$.

Example 2.6.2

Let V be a $\mathbb{Q}$ vector space, then

$$\mathbb{Q} \otimes_{\mathbb{Q}} V = V$$

But in this case, we also have that

$$\mathbb{Q} \otimes_{\mathbb{Z}} V = V$$

with $x \otimes v \mapsto xv$.

Proof. Every tensor in $\mathbb{Q} \otimes_{\mathbb{Z}} V$ is pure, since we can write

$$\sum \frac{a_i}{b_i} \otimes v_i = \sum \frac{1}{b_i} \otimes (a_i v_i) = \sum \frac{1}{b_i} \otimes \frac{a_i}{b_i} v_i = \sum 1 \otimes \frac{a_i}{b_i} v_i = 1 \otimes \sum \frac{a_i}{b_i}$$

Clearly this map is surjective, and it is easy to see that if $xv = 0$ then either $x = 0$ or $v = 0$. □

Example 2.6.3

Recall that

$$M \otimes_R \left(\bigoplus_{i \in I} N_i \right) \cong \bigoplus_{i \in I} (M \otimes N_i)$$

On the other hand, if we consider the direct product, we have a map

$$M \otimes \prod_i N_i \to \prod_i (M \otimes N_i)$$
$$m \otimes (n_i) \mapsto (m \otimes n_i)$$

which is in general, not an isomorphism. For example, consider

$$\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{n \geq 1} \frac{\mathbb{Z}}{2^n} \to \prod_{n \geq 1} \mathbb{Q} \otimes \frac{\mathbb{Z}}{2^n}$$

But from above, $\mathbb{Q} \otimes (\mathbb{Z}/2^n) = 0$, and so the right hand side is zero. For the left hand side, take

$$g = (1, 1, \ldots) \in \prod_{n \geq 1} \frac{\mathbb{Z}}{2^n}$$

Note that g has infinite order, and so it generates a subgroup isomorphic to Z. But recall that

$$\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z} = \mathbb{Q}$$

With this, we have an injective map

$$\mathbb{Q} \otimes \langle g \rangle \hookrightarrow \mathbb{Q} \otimes \prod_{n \geq 1} \frac{\mathbb{Z}}{2^n}$$

We will see later that $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

Example 2.6.4

Consider $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ as an $\mathbb{C}$-algebra, where we first restrict scalars on the right copy of $\mathbb{C}$, and extend scalars using the left copy.

Recall that as a $\mathbb{C}$-vector space,

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^2 \cong \mathbb{C}^2$$

and we have a basis $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, which is $1 \otimes 1, 1 \otimes i$ as a $\mathbb{C}$-vector space.

To consider this as a $\mathbb{C}$-algebra, then

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \otimes_{\mathbb{R}} \frac{\mathbb{R}[t]}{\langle t^2+1\rangle} \cong \frac{\mathbb{C}[t]}{\langle t^2+1\rangle} = \frac{\mathbb{C}[t]}{\langle t-i\rangle\langle t+i\rangle} \cong \frac{\mathbb{C}[t]}{\langle t-i\rangle} \times \frac{\mathbb{C}[t]}{\langle t+i\rangle} \cong \mathbb{C} \times \mathbb{C}$$

where we used the Chinese remainder theorem. On a pure tensor, we have

$$(a+bi) \otimes (c+di) \mapsto (a+bi) \otimes \underbrace{[c+dt]}_{\text{coset of } c+dt} \mapsto (a+bi)[c+dt]$$

We can compute this, to get

$$P = (ac + bdit) + (ibc + tad)$$

and we then have

$$P \mapsto (ac - bd + i(bc+ad), ac + bd + i(bc - ad))$$

If we set $x = a+bi, y = c+di$, then the result is just $(xy, x\overline{y})$.

3 Localisation

Definition 3.0.1 (multiplicative subset)

A *multiplicative(ly closed) subset* $S \subseteq \mathbb{R}$ such that

1. $1 \in S$,
2. if $a, b \in S$, then $ab \in S$.

If $U \subseteq R$ is any set, then the *multiplicative closure* S of U is the set of

$$\prod_{i=1}^{n} u_i$$

where $u_i \in U$, $n \geq 0$.

Example 3.0.2

If R is an integral domain, then $S = R \setminus \{0\}$ is multiplicative. More generally, if $\mathfrak{p} \trianglelefteq R$ is a prime ideal (of any ring R), then $S = R \setminus \mathfrak{p}$ is multiplicative.

Example 3.0.3

If $x \in R$, then $S = \{1, x, x^2, \ldots\}$ is multiplicative.

Example 3.0.4

$\mathbb{Q}$ is obtained from $\mathbb{Z}$ by adding inverses for the elements of the multiplicative subset $\mathbb{Z} \setminus \{0\}$, and we have a ring homomorphism $\mathbb{Z} \hookrightarrow \mathbb{Q}$.

We will generalise this example to general rings R, and with arbitrary multiplicative subsets $S \subseteq R$. But in general, we will lose injectivity.

Lecture 9

3.1 Construction

Definition 3.1.1 (localisation)
Let $S \subseteq R$ be a multiplicative set, M is an R-module. Consider the set $M \times S$, with the relation $(m_1, s_1) \sim (m_2, s_2)$ if there exists $u \in S$, such that

$$u(s_2m_1 - s_1m_2) = 0$$

This is an equivalence relation, and we $S^{-1}M$ for the set of equivalence classes. We write

$$\frac{m}{s} = [(m, s)]$$

for the equivalence class. Finally, we write

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{m_1s_2 + m_2s_1}{s_1s_2}$$

and

$$r \cdot \frac{m}{s} = \frac{rm}{s}$$

The above makes $S^{-1}M$ into an R-module. We call $S^{-1}M$ the *localisation of M at S*.

If $M = R$, we can make $S^{-1}R$ into a ring by

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

Next, we note that we have an $S^{-1}R$-module structure on $S^{-1}M$, via

$$\frac{r}{s} \cdot \frac{m}{t} = \frac{rm}{st}$$

We have localisation maps:

$$R \to S^{-1}R$$
$$r \mapsto \frac{r}{1}$$

which is a ring homomorphism, and

$$M \to S^[- 1]M$$
$$m \mapsto \frac{m}{1}$$

which is an R-linear map.

We check that $\sim$ above defines an equivalence relation: Reflexivity and symmetry are clear. Say $(m_1, s_1) \sim (m_2, s_2)$ and $(m_2, s_2) \sim (m_3, s_3)$. That is, there exists $u, v \in S$ such that

$$u(s_2m_1 - s_1m_2) = v(s_3m_2 - s_2m_3) = 0$$

Multiplying the first term by vs_3 and the second by us_1, we get

$$uvs_2s_3m_1 = uvs_3s_1m_2$$
$$uvs_1s_3m_2 = uvs_1s_2m_3$$

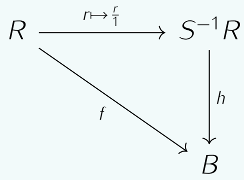
and so, we have that

$$uvs_2(s_3m_1 - s_1m_3) = 0$$

Since S is multiplicatively closed, we are done.

Proposition 3.1.2 (universal property of $S^{-1}R$). Let $U \subseteq R$ be any subset, and let $S \subseteq R$ be the multiplicative closure of U. Let $f : R \to B$ be a ring homomorphism, such that $f(u)$ is a unit for all $u \in U$.

Then there exists a unique ring homomorphism $h : S^{-1}R \to B$, such that the diagram



commutes. That is,

$$f(r) = h\left(\frac{r}{1}\right)$$

Another way of thinking about this is that we have a bijection

$$\mathrm{Hom}_{\mathrm{Ring}}(S^{-1}R, B) \leftrightarrow \{\varphi : R \to B \text{ ring hom., with } \varphi(U) \subseteq B^\times\}$$

given by sending f to $r \mapsto f\left(\frac{r}{1}\right)$.

Proof. Let $f : R \to B$ be a ring homomorphism, with $f(U) \subseteq B^\times$. In this case, $f(S) \subseteq B^\times$ as well. We want $h : S^{-1}R \to B$, with

$$f(r) = h\left(\frac{r}{1}\right)$$

First, such h must satisfy:

$$1 = h(1) = h\left(\frac{1}{s} \cdot \frac{s}{1}\right) = h\left(\frac{1}{s}\right) f(s)$$

Thus, we must have that $h(1/s) = f(s)^{-1}$. With this, we have

$$h\left(\frac{r}{s}\right) = h\left(\frac{r}{1}\right) h\left(\frac{1}{s}\right) = f(r)f(s)^{-1}$$

But we need to check if h is well defined. That is, if $r_1/s_1 = r_2/s_2$, then there exists $t \in S$ such that $t(s_2r_1 - s_1r_2) = 0$, or equivalently,

$$ts_2r_1 = ts_1r_2$$

Applying f, we get

$$f(t)f(s_2)f(r_1) = f(t)f(s_1)f(r_2)$$

But every element in the above equality are in $B^\times$, and so we are done. It is easy to check that h is a ring homomorphism. □

Proposition 3.1.3. If (A, j) satisfies the same universal property of $(S^{-1}R, \iota)$, where $\iota(r) = r/1$, then there exists an isomorphism $S^{-1}R \to A$, sending

$$\frac{r}{s} \mapsto j(r)j(s)^{-1}$$

Facts

1. Take $r/s \in S^{-1}R$, then
$$\frac{r}{s} = \frac{0}{1} \iff \text{there exists } u \in S \text{ with } ur = 0$$
2. $S^{-1}R = 0$ if and only if $0 \in S$.
3. $$\ker(\iota : R \to S^{-1}R) = \{r \in R \mid \text{ there exists } u \in S \text{ with } ur = 0\}$$
4. In particular, ι is injective if and only if S does not contain any zero divisors.
5. ι is always an epimorphism[1], but usually not surjective. For example, $\iota : \mathbb{Z} \to \mathbb{Q}$ is an epimorphism. If we have $f, g : \mathbb{Q} \to A$ ring homomorphisms, with $f \circ \iota = g \circ \iota$, then $f = g$.

[1]A morphism $f : X \to Y$ (in some category) is called an *epimorphism* if for all $g_1, g_2 : Y \to Z$, with $g_1 \circ f = g_2 \circ f$, we have $g_1 = g_2$.

Example 3.1.4

For $f \in R$, let $S = \{f^n \mid n \geq 0\}$. Then we define $R_f = S^{-1}R$.

If $R = \mathbb{Z}$, $f = 2$, then

$$R_f = \left\{ \frac{a}{2^n} \mid a \in \mathbb{Z}, n \geq 0 \right\} = \mathbb{Z}\left[\frac{1}{2}\right]$$

Notation 3.1.5. In this course, we will write:

- $\mathbb{Z}/n$ for the finite ring,
- $\mathbb{Z}_2$ for the 2-adic integers,
- $\mathbb{Z}[1/2]$ for the above ring.

Example 3.1.6

For a ring R, let $\operatorname{Spec}(R)$ denote its prime spectrum. For $\mathfrak{p} \in \operatorname{Spec}(R)$, we can let $S = R \setminus \mathfrak{p}$, and we write $R_{\mathfrak{p}} = (R \setminus \mathfrak{p})^{-1}R$.

If $R = \mathbb{Z}$, $p = \langle 3 \rangle$, then

$$\mathbb{Z}_{\langle 3 \rangle} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, 3 \nmid b \right\}$$

Proposition 3.1.7. If M is an R-module, $S \subseteq R$ a multiplicative subset, then we have an isomorphism:

$$\begin{aligned} S^{-1}R \otimes_R M &\to S^{-1}M \\ \frac{r}{s} \otimes m &\mapsto \frac{rm}{s} \end{aligned}$$

Proof. We can define a bilinear map

$$\begin{aligned} S^{-1}R \times M &\to S^{-1}M \\ \left(\frac{r}{s}, m\right) &\mapsto \frac{rm}{s} \end{aligned}$$

and thus, by the universal property we haev $\varphi : S^{-1}R \otimes_R M \to S^{-1}M$. This is R-linear, and it is easy to see that φ is also $S^{-1}R$-linear. It is clear that φ is surjective, since

$$\varphi\left(\frac{1}{s} \otimes m\right) = \frac{m}{s}$$

We want to show that every tensor

$$t = \sum_i \frac{r_i}{s_i} \otimes m_i \in S^{-1}R \otimes_R M$$

is prime. Define $s = \prod_i s_i$, and $t_j = \prod_{i \neq j} s_i$. In this case,

$$\begin{aligned} \sum \frac{r_i}{s_i} \otimes m_i &= \sum \frac{1}{s_i} \otimes (r_i m_i) \\ &= \sum \frac{t_i}{s} \otimes (r_i m_i) \\ &= \frac{1}{s} \otimes \left(\sum_i r_i t_i m_i\right) \end{aligned}$$

Using this, if

$$\varphi\left(\frac{1}{s} \otimes m\right) = \frac{m}{s} = 0 = \frac{0}{1}$$

That is, there exists $u \in S$, such that $um = 0$. In this case,

$$\frac{1}{s} \otimes m = \frac{u}{us} \otimes m = \frac{1}{us} \otimes (um) = 0$$

$\square$

With this, $S^{-1}R \otimes (\cdots)$ acts on R-modules. But in fact, it also acts on R-linear maps.

Lecture 10

Proposition 3.1.8 (localisation is a functor)**.** Let M be an R-module, $S \subseteq R$ a multiplicative subset. Let $f : N \to N'$ be an R-linear map. Then the following square commutes:

$$\begin{array}{ccc} S^{-1}R \otimes N & \xrightarrow{\mathrm{id}_{S^{-1}R} \otimes f} & S^{-1}R \otimes N' \\ \downarrow \sim & & \downarrow \sim \\ S^{-1}N & \xrightarrow[S^{-1}(f)]{} & S^{-1}N' \end{array}$$

In particular,

$$(S^{-1}f)\left(\frac{n}{s}\right) = \frac{f(n)}{s}$$

With this, the functors $S^{-1}R \otimes (\cdot)$ and $S^{-1}(\cdot)$ are naturally isomorphic.

Remark 3.1.9. Let A be an R-algebra, $S^{-1}R \otimes A \to S^{-1}A$ is $S^{-1}R$-linear, and also an isomorphism of $S^{-1}R$-algebras.

Lemma 3.1.10. If M is an $S^{-1}R$-module, then, we can restrict scalars on M from $S^{-1}R$ to R, then apply $S^{-1}(\cdot)$. Then

$$S^{-1}M \cong M$$

as $S^{-1}R$-modules. Equivalently,

$$M \cong S^{-1}R \otimes M$$

as $S^{-1}R$-modules.

Proof. We can see that the map

$$\begin{aligned} M &\to S^{-1}M \\ m &\mapsto \frac{m}{1} \end{aligned}$$

is $S^{-1}R$-linear. Surjectivity and injectivity are clear. $\square$

Proposition 3.1.11. Let M be an R-module, L an $S^{-1}R$-module, $f : M \to L$ is R-linear. Then there exists a unique $h : S^{-1}M \to L$ which is $S^{-1}R$-linear, such that

$$f(m) = h\left(\frac{m}{1}\right)$$

Proof. We know that $S^{-1}(\cdot) \otimes S^{-1}R \otimes (\cdot)$, and so it suffices to prove the result for the tensor product. With this, the localisation map is

$$\begin{aligned} \iota : M &\to S^{-1}R \otimes M \\ m &\mapsto \frac{1}{1} \otimes m \end{aligned}$$

Let $f : M \to L$ be R-linear. We then have that

$$h : \mathrm{id}_{S^{-1}R} \otimes f : S^{-1}R \otimes_R M \to S^{-1}R \otimes_R L$$

But the previous lemma shows that $S^{-1}R \otimes_R L \cong L$ as $S^{-1}R$-modules. In particular,

$$h\left(\frac{r}{s} \otimes m\right) = \frac{r}{s} f(m)$$

For the uniqueness of h, it follows from the fact that elements of the form $\frac{1}{1} \otimes m$ generate $S^{-1}R \otimes_R M$ as an $S^{-1}R$-module. □

Proposition 3.1.12 (the functor $S^{-1}R$ is exact)**.** If

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is an exact sequence of R-modules, then

$$S^{-1}A \xrightarrow{S^{-1}f} S^{-1}B \xrightarrow{S^{-1}g} S^{-1}C$$

is an exact sequence of $S^{-1}R$-modules.

Proof.

$$(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = S^{-1}(0) = 0$$

and so $\mathrm{im}(S^{-1}f) \subseteq \ker(S^{-1}g)$. Let

$$\frac{b}{s} \in \ker(S^{-1}g)$$

Then

$$\frac{g(b)}{s} = \frac{0}{1}$$

That is, there exists $u \in S$, such that $u \cdot g(b) = 0$. But g is R-linear, $u \in R$, and so $g(ub) = 0$, which means that $ub \in \ker(g) = \mathrm{im}(f)$. Thus, there exists $a \in A$ such that $f(a) = ub$. Now

$$\frac{b}{s} = \frac{ub}{us} = \frac{f(a)}{us} = S^{-1}f\left(\frac{a}{us}\right) \in \mathrm{im}(S^{-1}f)$$

□

Equivalently, $S^{-1}R$ is a flat R-module. Suppose $\iota : N \to M$ is the inclusion map, then

$$S^{-1}\iota : S^{-1}N \to S^{-1}M$$

is injective, and so the expression

$$\frac{n}{s}$$

makes sense in $S^{-1}N$ *and* $S^{-1}(M)$.

Proposition 3.1.13. Let M be an R-module, N, P submodules of M. Then

(i) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$.

(ii) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$,

(iii) $(S^{-1}M)/(S^{-1}N) \cong S^{-1}(M/N)$ as $S^{-1}R$ modules via

$$\frac{m}{s} + S^{-1}N \leftrightarrow \frac{m + N}{s}$$

Proof. For (i), the left hand side consists of elements of the form $\frac{n+p}{s}$, and the right hand side consists of elements of the form $\frac{n}{s_1} + \frac{p}{s_2}$. The result is then clear.

For (ii), $\subseteq$ is clear. Given $x \in S^{-1}N \cap S^{-1}P$, that is,

$$x = \frac{n}{s_1} = \frac{p}{s_2}$$

for $n \in N, p \in P, s_1, s_2 \in S$. But then there exists $u \in S$, such that $us_2n = us_1p =: w \in N \cap P$. With this,

$$x - \frac{n}{s_1} = \frac{us_2n}{us_1s_2} = \frac{w}{us_1s_2} \in S^{-1}(N \cap P)$$

For (iii), consider the exact sequence

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

Applying the exact functor S^{-1},

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

But this immediately gives that

$$S^{-1}(M/N) \cong \frac{S^{-1}M}{S^{-1}N}$$

as $S^{-1}R$-modules. Computing the respective maps gives the result. □

Proposition 3.1.14. If M, N are R-modules, then

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \cong S^{-1}(M \otimes_R N)$$

Proof. We have the isomorphism from extension of scalars:

$$(S^{-1}R \otimes_R M) \otimes_{S^{-1}R} (S^{-1}R \otimes_R N) \cong S^{-1}R \otimes_R (M \otimes_R N)$$

□

A special case of this is that if $\mathfrak{p}$ is a prime ideal of R, then

$$M_\mathfrak{p} \otimes_{R_\mathfrak{p}} N_\mathfrak{p} = (M \otimes_R N)_\mathfrak{p}$$

3.2 Extension and contraction of ideals

Recall if $f : A \to B$ is a ring homomorphism, we define the *contraction of* $\mathfrak{b} \trianglelefteq B$ as

$$\mathfrak{b}^c = f^{-1}(\mathfrak{b}) \trianglelefteq A$$

and the *extension of* $\mathfrak{a} \trianglelefteq A$ as

$$\mathfrak{a}^e = \langle f(\mathfrak{a}) \rangle \trianglelefteq B$$

In examples sheet 1, we have a bijection

$$\{\text{contracted ideals of } A\} \leftrightarrow \{\text{extended ideals of } B\}$$

To see this, we have that an ideal $\mathfrak{a}$ is contracted if and only if $\mathfrak{a} = \mathfrak{a}^{ec}$, and an ideal $\mathfrak{b}$ is extended if and only if $\mathfrak{b} = \mathfrak{b}^{ce}$, and so the bijection is given by extension/contraction.

Let S be a multiplicative subset of R, and we will consider the ring homomorphism $R \to S^{-1}R$, given by $r \mapsto r/1$. For an ideal $\mathfrak{a}$ of R, we have the *extension*

$$\mathfrak{a}^e = S^{-1}\mathfrak{a} \trianglelefteq S^{-1}R$$

and for an ideal $\mathfrak{b}$ of $S^{-1}R$, we have the contraction $\mathfrak{b}^c \trianglelefteq R$.

Proposition 3.2.1.
$$\mathfrak{a}^e = S^{-1}\mathfrak{a} = \left\{ \frac{a}{s} \;\middle|\; a \in \mathfrak{a}, s \in S \right\}$$

Lecture 11

Proof. $\mathfrak{a}^e$ is the ideal generated by $a/1$ for $a \in \mathfrak{a}$, and so $\supseteq$ holds. But the right hand side is already an ideal, and so by minimality, equality holds. □

Proposition 3.2.2. $\mathfrak{a}^{ec} = \bigcup_{s \in S}(\mathfrak{a} : s)$ where $(\mathfrak{a} : s) = \{r \in R \mid rs \in \mathfrak{a}\}$.

Proof. Take $r \in \bigcup_{s\in S}(\mathfrak{a} : s)$. That is, $rs = a \in \mathfrak{a}$, and so in $S^{-1}R$,
$$\frac{rs}{1} = \frac{a}{1} \implies \frac{r}{1} = \frac{a}{s} \in \mathfrak{a}^e$$
and so $r \in \mathfrak{a}^{ec}$. Conversly, if $r \in \mathfrak{a}^{ec}$, then
$$\frac{r}{1} = \frac{a}{s}$$
for some $a \in \mathfrak{a}, s \in S$. But this means that there exists $u \in S$, such that $urs = ua$. With this, $r \in (\mathfrak{a} : us)$, $us \in S$ as S is multiplicative. □

Now suppose $\mathfrak{b}$ is an ideal of $S^{-1}R$. Then
$$\mathfrak{b}^c = \left\{ r \in R \;\middle|\; \frac{r}{1} \in \mathfrak{b} \right\}$$

Proposition 3.2.3. $\mathfrak{b}^{ce} = \mathfrak{b}$.

Proof. $\subseteq$ always holds. Take $r/s \in \mathfrak{b}$, then $r/1 \in \mathfrak{b}$. Thus, $r \in \mathfrak{b}^c$, and so $r/1 \in \mathfrak{b}^{ce}$, which means that $r/s \in \mathfrak{b}^{ce}$. □

Proposition 3.2.4. Consider the localisation map $R \to S^{-1}R$, then

(i) Every ideal of $S^{-1}R$ is extended.

(ii) An ideal $\mathfrak{a}$ of R is contracted if and only if the image of S in $R/\mathfrak{a}$ contains no zero divisors of $R/\mathfrak{a}$.

(iii) $\mathfrak{a}^e = S^{-1}R$ if and only if $\mathfrak{a} \cap S \neq \varnothing$.

(iv) We have a bijection:
$$\begin{aligned} \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \varnothing\} &\leftrightarrow \operatorname{Spec}(S^{-1}R) \\ \mathfrak{p} &\mapsto \mathfrak{p}^e \\ \mathfrak{q}^c &\leftarrow\!\shortmid \mathfrak{q} \end{aligned}$$

Proof. (i) Follows from proposition 3.2.3. For (ii), $\mathfrak{a}$ is contracted if and only if $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$. But
$$\mathfrak{a}^{ec} = \bigcup_{s \in S}(\mathfrak{a} : s)$$
Thus, $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$ if and only if: for all $r \in R$, if $Sr \cap \mathfrak{a} \neq \varnothing$, then $r \in \mathfrak{a}$. But $Sr \cap \mathfrak{a} \neq$ is true if and only if $0 + \mathfrak{a}$ is in the image of S, and $r \in \mathfrak{a}$ is the same as $r + \mathfrak{a} = 0$. Thus, $\mathfrak{a}$ is contracted if and only if the image of S in $R/\mathfrak{a}$ contains no zero divisors.

For (iii), suppose $\mathfrak{a} \cap S \neq \varnothing$. Choose $x \in \mathfrak{a} \cap S$, then

$$1 = \frac{x}{x} \in \mathfrak{a}^e$$

Conversely, if $\mathfrak{a}^e = S^{-1}R$. Then $1 \in \mathfrak{a}^e$, and so

$$\frac{1}{1} = \frac{a}{s}$$

for some $a \in \mathfrak{a}, s \in S$, and so there exists $u \in S$ such that $us = ua$. But $us \in S$ as it is multiplicative, $ua \in \mathfrak{a}$ as it is an ideal.

For (iv), first consider the contraction map $\operatorname{Spec}(S^{-1}R) \to \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \cap S = \varnothing\}$. This makes sense as the contraction of a prime ideal is prime, and if $\mathfrak{p} \in \operatorname{Spec}(R)$ is contracted, by (ii), we see that $S \cap \mathfrak{p}$ is empty, since $R/\mathfrak{p}$ is an integral domain, and so the only zero divisor is zero.

Moreover, this map is injective, since it has a left inverse, as all ideals in $S^{-1}R$ are extended ideals, and so $\mathfrak{q}^{ce} = \mathfrak{q}$. In the other direction, for a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$, with $\mathfrak{p} \cap S = \varnothing$, we have seen that $\mathfrak{p}$ is contracted, and so $\mathfrak{p}^{ec} = \mathfrak{p}$. With this, all we need to show is that $\mathfrak{p}^e$ is prime.

We would like to show that $(S^{-1}R)/\mathfrak{p}^e$ is an integral domain. We know that $\mathfrak{p}^e$ is not all of $S^{-1}R$, and so $(S^{-1}R)/\mathfrak{p}^e$ is not the zero ring. So we need to show that $(S^{-1}R)/\mathfrak{p}^e$ has no zero divisors. We will do this by embedding $(S^{-1}R)/\mathfrak{p}^e$ into $\operatorname{Frac}(R/\mathfrak{p})$.

Now consider the composition map

$$R \longrightarrow R/\mathfrak{p} \longrightarrow \operatorname{Frac}(R/\mathfrak{p})$$

This has the property that the elements of S are sent to units, since $S \cap \mathfrak{p} = \varnothing$. Using the universal property of $S^{-1}R$, we hava an induced map

$$\begin{array}{ccccc} R & \longrightarrow & R/\mathfrak{p} & \longrightarrow & \operatorname{Frac}(R/\mathfrak{p}) \\ \downarrow & & & \nearrow_{\varphi} & \\ S^{-1}R & & & & \end{array}$$

In particular,

$$\varphi\left(\frac{r}{s}\right) = \frac{r + \mathfrak{p}}{s + \mathfrak{p}}$$

It suffices to show that $\ker(\varphi) = \mathfrak{p}^e$. First, we see that $\operatorname{im}(\varphi) \subseteq \overline{S}^{-1}(R/\mathfrak{p})$, where $\overline{S}$ is the image of S in $S^{-1}R$. With this, we cam consider $\varphi : S^{-1}R \to \overline{S}^{-1}(R/\mathfrak{p})$. Take $r/s \in \ker(\varphi)$. That is,

$$\frac{r + \mathfrak{p}}{s + \mathfrak{p}} = \frac{0}{1} \in \overline{S}^{-1}(R/\mathfrak{p})$$

Then there exists $u + \mathfrak{p} \in \overline{S}$, such that

$$(u + \mathfrak{p})(r + \mathfrak{p}) = (ur) + \mathfrak{p} = 0$$

That is, $ur \in \mathfrak{p}$. Then we have that

$$\frac{r}{s} = \frac{ur}{us} \in \mathfrak{p}^e$$

Conversely, take $x \in \mathfrak{p}^e$. Then $x = p/s$, and

$$\varphi(x) = \frac{p + \mathfrak{p}}{s + \mathfrak{p}} = 0$$

and so $x \in \ker(\varphi)$. $\square$

In the special case where $S = \{1, f, \cdots\}$, we can view this in terms of algebraic geometry. There, we have a natural identification of $\operatorname{Spec}(R_f)$ with $D(f)$, which is the complement of the zero set of f. The left hand side is precisely $D(f)$, essentially by definition.

An application

If $I \trianglelefteq R$ is an ideal, then the *radical of* I is

$$\sqrt{I} = \{r \in R \mid \exists m \geq 1 \text{ such that } r^m \in I\}$$

Proposition 3.2.5.

$$\sqrt{I} = \bigcap_{I \leq \mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}$$

Proof. Take $x \in \sqrt{I}$, then $x^n \in I$, and so for every $\mathfrak{p} \in \operatorname{Spec}(R)$, if $I \subseteq \mathfrak{p}$, then $x^n \in \mathfrak{p}$, and so $x \in \mathfrak{p}$. That is, $\subseteq$ holds. For the other inclusion, take $x \in R$, $x \notin \sqrt{I}$. We know that $I \neq R$, and R/I is not the zero ring. Let $\overline{x} \in R/I$ be the image of x. Consider

$$(R/I)_{\overline{x}} = \{\overline{x}^n\}^{-1}(R/I)$$

This is not the zero ring, since we did not invert zero. Therefore, $(R/I)_{\overline{x}}$ has a prime ideal, which corresponds to a prime ideal of R/I which avoids $\overline{x}$, which in turn, corresponds to a prime ideal of R, which contains I, and avoids x. □

Lecture 12

3.3 Local properties

Definition 3.3.1 (local ring)

A ring R is *local* if it has a unique maximal ideal. We write $(R, \mathfrak{m})$ for the local ring R with maximal ideal $\mathfrak{m}$.

Example 3.3.2

Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then recall that we have a bijection

$$\{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\} \leftrightarrow \operatorname{Spec}(R_\mathfrak{p})$$

given by extension and contraction. With this, all prime ideals of $R_\mathfrak{p}$ are contained in $\mathfrak{p}R_\mathfrak{p}$. Thus, $(R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p})$ is a local ring.

In particular, $\mathbb{Z}_{\langle 2 \rangle}$ is a local ring, and the unique maximal ideal is

$$\langle 2 \rangle \mathbb{Z}_{\langle 2 \rangle} = \left\{ \frac{2a}{b} \,\middle|\, a, b \in \mathbb{Z}, 2 \nmid b \right\}$$

Proposition 3.3.3. Let M be an R-module. Then the following are equivalent:

(i) $M = 0$,

(ii) $M_\mathfrak{p} = 0$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$,

(iii) $M_\mathfrak{m} = 0$ for all $\mathfrak{m} \in \operatorname{maxSpec}(R)$.

That is, being zero is a local property (i.e. it is localisable and local to global).

Proof. The implications $(i) \implies (ii) \implies (iii)$ is clear. Suppose (iii) holds, and suppose for contradiction there exists $m \in M$ non-zero. Consider

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

Since $m \neq 0$, $1 \notin \operatorname{Ann}_R(m)$. Take a maximal ideal $\mathfrak{m}$ containing $\operatorname{Ann}_R(m)$. In this case,

$$\frac{m}{1} = 0 \in M_{\mathfrak{m}}$$

That is, $um = 0$ for some $u \in R \setminus \mathfrak{m}$. But in this case, $u \notin \operatorname{Ann}_R(m)$. Contradiction. $\square$

Proposition 3.3.4. Lte $f : M \to N$ be an R-linear map. Then the following are equivalent:

(i) f is injective,

(ii) $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ is injective for every $\mathfrak{p} \in \operatorname{Spec}(R)$,

(iii) $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is injective for every $\mathfrak{m} \in \operatorname{maxSpec}(R)$,

The same statements holds for surjectivity.

Recall

$$f_{\mathfrak{p}}\left(\frac{m}{s}\right) = \frac{f(m)}{s}$$

Proof. Suppose (i) holds. Since localising at $\mathfrak{p}$ is an exact functor, (ii) follows. (ii) implies (iii) is by definition.

Suppose (iii) holds. We have the exact sequence

$$0 \longrightarrow \ker(f) \hookrightarrow M \xrightarrow{f} N$$

Localising at $\mathfrak{m}$, we get

$$0 \longrightarrow \ker(f)_{\mathfrak{m}} \longrightarrow M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \qquad (*)$$

which is exact as localisation is an exact functor. But $(*)$ shows that

$$\ker(f_{\mathfrak{m}}) = \ker(f)_{\mathfrak{m}}$$

But we assumed $\ker(f_{\mathfrak{m}}) = 0$, and so $\ker(f)_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$. Thus, by proposition 3.3.3, $\ker(f) = 0$. $\square$

Proposition 3.3.5. Let M be an R-module. Then the following are equivalent:

(i) M is a flat R-module,

(ii) $M_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$-module for all $\mathfrak{p} \in \operatorname{Spec}(R)$,

(iii) $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module for all $\mathfrak{m} \in \operatorname{maxSpec}(R)$.

Proof. For (i) $\implies$ (ii), since $M_{\mathfrak{p}} \cong R_{\mathfrak{p}} \otimes_R M$ as $R_{\mathfrak{p}}$-modules, and we have shown that extension of scalars preserves flatness. As usual, (ii) $\implies$ (iii) is trivial.

Suppose (iii) holds. Suppose $f : N \to P$ is R-linear and injective. Fix a maximal ideal $\mathfrak{m} \in \operatorname{maxSpec}(R)$. Then $f_{\mathfrak{m}} : N_{\mathfrak{m}} \to P_{\mathfrak{m}}$ is injective by proposition 3.3.4. Then

$$N_{\mathfrak{m}} \otimes M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}} \otimes \mathrm{id}} P_{\mathfrak{m}} \otimes M_{\mathfrak{m}}$$

is injective by (iii). But we have isomorphisms $(N \otimes_R M)_{\mathfrak{m}} \cong N_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}}$, and using this,

$$\begin{array}{ccc} N_{\mathfrak{m}} \otimes M_{\mathfrak{m}} & \xrightarrow{f_{\mathfrak{m}} \otimes \mathrm{id}} & P_{\mathfrak{m}} \otimes M_{\mathfrak{m}} \\ \Big| \wr & & \Big| \wr \\ (N \otimes_R M)_{\mathfrak{m}} & \xrightarrow{(f \otimes \mathrm{id})_{\mathfrak{m}}} & (P \otimes_R M)_{\mathfrak{m}} \end{array}$$

the bottom map must be injective. But then $(f \otimes \mathrm{id})_{\mathfrak{m}}$ is injective for all $\mathfrak{m}$, and so $f \otimes \mathrm{id}$ is injective by proposition 3.3.4. $\square$

Example 3.3.6

An R-module M is *locally free* if $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ module for every $\mathfrak{p} \in \operatorname{Spec}(R)$.

Take $R = \mathbb{C} \times \mathbb{C}$. The set of prime ideals of R is just

$$\{\mathbb{C} \times 0, 0 \times \mathbb{C}\}$$

But then we have a ring homomorphism

$$\begin{aligned} \mathbb{C} \times \mathbb{C} &\to \mathbb{C} \\ (a, b) &= b \end{aligned}$$

This sends $\mathbb{C} \times \mathbb{C} \setminus \mathbb{C} \times 0$ to units, and so we have a ring homomorphism

$$\begin{aligned} (\mathbb{C} \times \mathbb{C})_{\mathbb{C} \times 0} &\to \mathbb{C} \\ \frac{(a, b)}{(c, d)} &\mapsto \frac{b}{d} \end{aligned}$$

This is a bijection. With this, $(\mathbb{C} \times \mathbb{C})_{\mathbb{C} \times 0} \cong (\mathbb{C} \times \mathbb{C})_{0 \times \mathbb{C}}$ are fields, and so every $\mathbb{C} \times \mathbb{C}$-module M is locally free.

Now consider $M = \mathbb{C} \times \{0\}$ as an $\mathbb{C} \times \mathbb{C}$-module. This is not free (it is not zero, and it is not free of rank ≥ 1). Thus, M is locally free but not free.

3.4 Localisation as a quotient

Let $U \subseteq R$ be a subset, $S \subseteq R$ be its multiplicative closure. Define

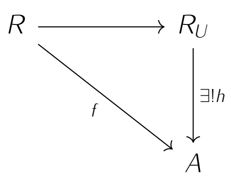
$$R_U = \frac{R[\{T_u : u \in U\}]}{\langle u T_u \mid u \in U \rangle}$$

Denote the ideal $I_U = \langle u T_u \mid u \in U \rangle$. Let $\overline{u}, \overline{T_u}$ denote the images of u, T_u respectively.

Claim 3.4.1. R_U is isomorphic to $S^{-1}R$ as rings, and also as R-algebras. The isomorphism is given by

$$\begin{aligned} R_U &\leftrightarrow S^{-1}R \\ \overline{T_u} &\mapsto \frac{1}{u} \\ \overline{r}\,\overline{T_{u_1}} \cdots \overline{T_{u_n}} &\leftarrow\!\shortmid \frac{r}{u_1 \cdots u_n} \end{aligned}$$

Proof. We will show that R_U satisfies the universal property of localisation. Let A be any ring, $f : R \to A$ any ring homomorphism, sending U to units.



Since A is an R-algebra via f, the diagram commutes if and only if h is an R-algebra as well. But we have the bijection

$$\operatorname{Hom}_{R-\mathrm{alg}}(R_U, A) \leftrightarrow \{\varphi : U \to A \mid f(u)\varphi(u) = 1\}$$

But the set on the right hand side has one elmeent. □

Example 3.4.2
For $x \in R$, we can invert x, and we have that

$$R_x \cong \frac{R[t]}{\langle tx - 1\rangle}$$

The intuition here is that $T_u = 1/u$.

Lecture 13

4 Nakayama's lemma

Proposition 4.0.1 (Cayley-Hamilton). Let M be a finitely generated R-module, $f : M \to M$ an R-linear map, $\mathfrak{a} \trianglelefteq R$ an ideal, with $f(M) \subseteq \mathfrak{a}M$. Then

$$f^n + a_1 f^{n-1} + a_n \operatorname{id} = 0$$

where $a_i \in \mathfrak{a}$.

Proof. Say $M = \operatorname{span}_R\{m_1, \dots, m_n\}$, then $\mathfrak{a}M = \operatorname{span}_{\mathfrak{a}}\{m_1, \dots, m_n\}$. Therefore,

$$\begin{pmatrix} f(m_1) \\ \vdots \\ f(m_n) \end{pmatrix} = P \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

where $P \in \operatorname{Mat}_n(\mathfrak{a})$. Take $\rho : R \to \operatorname{End}(M)$ to be the structure ring homomorphism of M as an R-module, then we can define

$$\begin{aligned} R[t] &\to \operatorname{End}_R(M) \\ t &\mapsto f \end{aligned}$$

which makes M into an $R[t]$-module. Using this,

$$t \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = P \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}$$

and so

$$Q \begin{pmatrix} m_1 \\ \vdots \\ m_n = 0 \end{pmatrix}$$

where $Q = t \cdot I_n - P = 0$. Multiplying by $\operatorname{adj}(Q)$, we get that

$$\det(Q) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

Hence $\det(Q)m = 0$ for all $m \in M$, and so $m \mapsto \det(Q)m$ is the zero map. But then $\det(Q)$ gives the polynomial as required. □

Corollary 4.0.2. Let M be a finitely generated R-module. $\mathfrak{a} \trianglelefteq R$ an ideal, if $\mathfrak{a}M = M$, then there exists $a \in \mathfrak{a}$ such that $am = m$ for every $m \in M$.

Proof. Apply Cayley-Hamilton with $f = \operatorname{id}_M$, we get that

$$(1 + a_1 + \cdots + a_n) \operatorname{id}_M = 0$$

and so we can take $a = -(a_1 + \cdots + a_n)$. □

Definition 4.0.3 (Jacobson radical)
The *Jacobson radical* of a ring R is

$$J(R) = \bigcap_{\mathfrak{m} \trianglelefteq R \text{ maximal}} \mathfrak{m}$$

Example 4.0.4
If $(R, \mathfrak{m})$ is a local ring, then $J(R) = \mathfrak{m}$. On the other hand, $J(\mathbb{Z}) = 0$.

Proposition 4.0.5. For $x \in R$, $x \in J(R)$ if and only if $1 - xy$ is a unit in R for every $y \in R$.

Proof. Suppose that $x \in J(R)$, and suppose for contradiction that $1 - xy$ is not a unit, for some $y \in R$. With this, $1 - xy$ is contained in a maximal ideal $\mathfrak{m}$. Since $x \in J(R)$, $x \in \mathfrak{m}$. Thus,

$$1 = (1 - xy) + xy \in \mathfrak{m}$$

Contradiction. On the other hand, if $x \notin J(R)$, then there exists a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$. Then $\mathfrak{m} + \langle x \rangle = R$. In particular, there exists $t \in \mathfrak{m}, y \in R$ such that $t + xy = 1$. In this case, $1 - xy = t \in \mathfrak{m}$, and so it is not a unit. □

Proposition 4.0.6 (Nakayama's lemma)**.** Let M be a finitely generated R-module, $\mathfrak{a} \leq J(R)$ is an ideal of R, with $\mathfrak{a}M = M$. Then $M = 0$.

Proof. By corollary 4.0.2, there exists $a \in \mathfrak{a}$ such that $am = m$ for all $m \in M$. By proposition 4.0.5, $1 = a$ is a unit, and so we can multiply by $(1 - a)^{-1}$, to get that

$$m = (1 - a)^{-1}(1 - a)m = (1 - a)^{-1} \cdot 0 = 0$$

□

Corollary 4.0.7. Let M be a finitely generated R-module, $N \leq M$ an R-submodule, $\mathfrak{a} \leq J(R)$ an ideal, such that

$$N + \mathfrak{a}M = M$$

then $N = M$.

Proof.

$$\mathfrak{a} \cdot \left(\frac{M}{N}\right) = \frac{\mathfrak{a}M + N}{N} = \frac{M}{N}$$

Therefore, by Nakayama, $M/N = 0$, and so $N = M$. □

5 Integral and finite extensions

Definition 5.0.1 (integral)
Let A be an R-algebra, $x \in A$ is *integral over* R if there exists $f \in R[t]$ monic, such that $f(x) = 0$.

Example 5.0.2
If K is a field, A is a K-algebra, $x \in A$, then x is integral over K if and only if it is algebraic over K.

Example 5.0.3
We will see later

1. the elements of $\mathbb{Q}$ which are integral over $\mathbb{Z}$ is just $\mathbb{Z}$,
2. the $\mathbb{Z}$ integral elements of $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$,
3. the $\mathbb{Z}$ integral elements of $\mathbb{Q}(\sqrt{5})$ is $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

To see this, we can also recall Part II Number Fields and the ring of integers of a number field.

Definition 5.0.4 (faithful)
An R-module M is *faithful* if the structure ring homomorphism $R \to \mathrm{End}_R(M)$ is injective.
That is, for every non-zero $r \in R$, there exists $m \in M$ such that $rm \neq 0$.

Example 5.0.5
Let $R \subseteq A$ be rings, and so A is an R-module in a natural way. It must be faithful, since we have $r1 = r$.

Proposition 5.0.6. Let $R \subseteq A$ be rings, $x \in A$. Then $R[x] \subseteq A$ is a subring, which makes A into an $R[x]$-algebra (and thus an $R[x]$-module). Then x is $R[x]$-integral if and only if there exists $M \subseteq A$ such that

1. M is a faithful $R[x]$-module, that is, M is an R-submodule of A, $xM \subseteq M$, and $R[x] \to \mathrm{End}_{R[x]}(M)$ is injective,
2. M is finitely generated as an R-module.

Proof. Suppose such an M exists. With this, we have an R-linear map $f : M \to M$,

$$f(m) = xm$$

Since M is a finitely generated R-module, we can apply Cayley-Hamilton (proposition 4.0.1), to get

$$f^n + r_1 f^{n-1} + \cdots + r_n = 0$$

where $r_i \in R$. Evaluating at $m \in M$, we get that

$$(x^n + r_1 x^{n-1} + \cdots + r_n)(m) = 0$$

Since M is a faithful $R[x]$-module, $x^n + f_1 x^{n-1} + \cdots + r_n = 0$ That is, x is integral over R. Now suppose x is integral over R. Then

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0$$

for some $r_i \in R$. Take

$$M = \mathrm{span}_R\{1, x, \cdots, x^{n-1}\}$$

satisfies $xM = M$, and as $1 \in M$, it is faithful. The fact that it is finitely generated is clear by definition. □

Lecture 14

Definition 5.0.7 (integral)
Let A be an R-algebra. Then A is *integral over* R if every $x \in A$ is integral over R.

Definition 5.0.8 (finite over)
Let A be an R-algebra, then A is *finite over* A if it is finitely generated as an R-module.

Proposition 5.0.9. Let A be an R-algebra. Then the following are equivalent:

(i) A is a finitely generated integral R-algebra,

(ii) A is generated as an R-algebra by a finite set of integral elements,

(iii) A is finite over R,

Proof. (i) $\implies$ (ii) is trivial. Suppose (ii) holds. Then A is generated by $\alpha_1, \ldots, \alpha_m$ as an R-algebra. But α_i being integral implies that

$$\alpha_i^{n_i} + r_{i,1}\alpha_i^{n_i-1} + \cdots + r_{i,n_i} = 0$$

That is,

$$\alpha_i^{n_i} \in \operatorname{span}_R\{1, \alpha_i, \ldots, \alpha_i^{n_i-1}\}$$

But this means that for all $e_1, \ldots e_n \geq 0$,

$$\alpha_1^{e_1} \cdots \alpha_m^{e_m} \in \operatorname{span}_R\{\alpha_1^{f_1} \cdots \alpha_m^{f_m} \mid 0 \leq f_i \leq n_i - 1\}$$

Hence A is a finitely generated R-module.

Finally, suppose (iii) holds. If A is finitely generated as an R-module, then it is necessarily finitely generated as an R-algebra. Choose $\alpha \in A$, we would like to show that α is integral over R. Let $\rho; R \to A$ be the structure ring homomorphism of A as an R-algebra. Then $\rho(R)$ is a subring of A. With this, it then makes sense to consider $\rho(R)[\alpha]$ as a subring of A.

Next, A is a $\rho(R)[\alpha]$-module, and it must be faithful as $1 \in A$. Using this, and the fact that A is a finitely generated $\rho(R)[\alpha]$-module, so by proposition 5.0.6, α is integral over $\rho(R)$. Equivalently, α is integral over R. □

Proposition 5.0.10. If A is an R-algebra, $\mathcal{O}$ is the integral elements of A, then $\mathcal{O}$ is an R-subalgebra of A.

Proof. Take $x, y \in \mathcal{O}$. Then this is a finite set of R-integral elements, and so must generate an integral R-subalgebra of A. But this contains $x \pm y, xy$, which must then be integral. Hence $\mathcal{O}$ is a ring. The fact that it is an R-subalgebra is clear. □

Proposition 5.0.11. If $A \subseteq B \subseteq C$ are rings,

(i) if C is finite over B, and B is finite over A, then C is finite over A.

(ii) if C is integral over B, B is integral over A, then C is integral over A.

Proof. For (i), if $C = \operatorname{span}_B\{\gamma_1, \ldots, \gamma_n\}$, $B = \operatorname{span}_A\{\beta_1, \ldots, \beta_\ell\}$, then $C = \operatorname{span}_A\{\beta_i\gamma_j\}$.

For (ii), let $c \in C$. We would like to show that c is A-integral. We know that c is B-integral, and so $f(c) = 0$ for some

$$f(T) = T^n + b_1T^{n-1} + \cdots + b_n \in B[T]$$

Hence $f \in A[b_1, \ldots, b_n][T]$. Set $A' = A[b_1, \ldots, b_n]$. Then we have inclusions

$$A \subseteq A' \subseteq A'[c]$$

Both inclusions are integral, as they are generated by finitely many integral elements. But this tells us that both extensions are finite by proposition 5.0.9. By (i), $A \subseteq A'[c]$ is finite, and so $A \subseteq A'[c]$ is integral, and so c is integral over A. □

Definition 5.0.12
Let $A \subseteq B$ be rings. The *integral closure* of A in B is

$$\overline{A} = \{b \in B \mid b \text{ integral over } A\}$$

We say that A is *integrally closed* if $A = \overline{A}$.

If A is an integral domain, then its *integral closure* is its integral closure in $\mathrm{Frac}(A)$, and it is *integrally closed* if it is integrally closed in $\mathrm{Frac}(A)$.

Example 5.0.13
Consider $A = \mathbb{Z}[\sqrt{5}]$. This is not integrally closed, since $\mathrm{Frac}(A) = \mathbb{Q}(\sqrt{5})$. In this case,

$$\alpha = \frac{1+\sqrt{5}}{2} \in \mathrm{Frac}(A) \setminus A$$

But α is integral over A, since $\alpha^2 - \alpha - 1 = 0$.

Example 5.0.14
$\mathbb{Z}$ and $k[t_1, \cdots, t_n]$ are integrally closed.

Proposition 5.0.15. If A is a UFD, then A is integrally closed.

Proof. Take $x \in \mathrm{Frac}(A) \setminus A$, say $x = a/b$, $a, b \in A$, with some $p \in A$ prime, $p \mid b$ but $p \nmid a$. If x is A-integral, then

$$\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0$$

Multiply through by b^n, we get

$$a^n = -b(a_1 + a_2 b + \cdots + a_n b^{n-1})$$

Since $p \mid b$, p divides the right hand side, and so $p \in a^n$. Thus, $p \mid a$. □

Lemma 5.0.16. If $A \subseteq B$ are rings, $\overline{A}$ the integral closure of A in B, then $\overline{A}$ is integrally closed over A.

Proof. If $x \in B$ is integral over $\overline{A}$, then we have integral extensions

$$A \subseteq \overline{A} \subseteq \overline{A}[x]$$

By transitivity, $A \subseteq \overline{A}[x]$ is integral, and so x is integral over A, that is, $x \in \overline{A}$. □

Proposition 5.0.17. Let $A \subseteq B$ be rings,

(i) If B is integral over A,

(a) for every ideal $\mathfrak{b}$ of B,

$$\frac{B}{\mathfrak{b}} \text{ is integral over } \frac{A}{\mathfrak{b} \cap A}$$

(b) if $S \subseteq A$ is a multiplicative set, then $S^{-1}B$ is integral over $S^{-1}A$,

(ii) If $\overline{A}$ is the integral closure of A in B, then then $S^{-1}\overline{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$. That is, $\overline{S^{-1}A} = S^{-1}\overline{A}$

Proof. See notes. □

Lemma 5.0.18. Suppose $A \subseteq B$ is an integral extension of rings,

(i) $A \cap B^\times = A^\times$,

(ii) if A, B are domains, then A is a field if and only if B is a field.

Proof. For (i), $\supseteq$ is clear. Conversely, take $a \in A \cap B^\times$. Then there exists $b \in B$ such that $ab = 1$. We need to show that $b \in A$. We know that b is integral over A, that is,

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

Multiply this by a^{n-1}, we get

$$b + a_1 + a_2 a + \cdots + a_n a^{n-1} = 0$$

But $a_1 + a_2 a + \cdots + a_n a^{n-1} \in A$, and so $b \in A$.

For (ii), suppose that B is a field. Then

$$A^\times = A \cap B^\times = A \cap (B \setminus \{0\}) = A \setminus \{0\}$$

and so A is a field. Now suppose A is a field. Let $b \in B$ be non-zero. Since b is integral over A,

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

where n is *minimal*. With this,

$$b\underbrace{(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1})}_{=\delta} = -a_n$$

By minimality, $\delta \neq 0$. Therefore, $a_n \neq 0$ as it is a domain. But $a_n \in A$ is a unit, so

Lecture 15

$$b(a_n^{-1}\delta) = 1$$

and so b is a unit. □

Corollary 5.0.19. Let $A \subseteq B$ be an integral extension of rings, $\mathfrak{q}$ a prime ideal of B. Then $\mathfrak{q}$ is a maximal ideal of B if and only if $\mathfrak{q} \cap A$ is a maximal ideal of A.

Proof. We have a ring embedding

$$\frac{A}{\mathfrak{q} \cap A} \hookrightarrow \frac{B}{\mathfrak{q}}$$

and these are integral domains as $\mathfrak{q}$ is prime. Moreover, this is an integral extension, and so we are done. □

6 Noether normalisation and Hilbert's Nullstellensatz

6.1 Noether normalisation

Throughout, let k be a field.

Definition 6.1.1 (algebraically independent)

If A is a k-algebra, and $x_1, \ldots, x_n \in A$, then $x_1, \ldots, x_n$ are *k-algebraically independent* if for every $p \in k[T_1, \ldots, T_n]$ non-zero, $p(x_1, \ldots, x_n) \neq 0$. That is, the k-algebra homomorphism $k[T_1, \ldots, T_n] \to A$ given by sending T_i to x_i is injective.

Theorem 6.1.2 (Noether normalisation)**.** If $A \neq 0$ is a finitely generated k-algebra, then there exists $x_1, \ldots, x_n \in A$, which are k-algebraically independent, such that A is finite over

$$A' = k[x_1, \ldots, x_n]$$

Example 6.1.3 (of the method of proof)
Let $A = k[t, t^{-1}]$. First of all, note that $k[t] \subseteq k[t, t^{-1}]$ is not a finite extension. To see this, suppose it was, then t^{-1} is integral over $k[t]$. That is,

$$t^{-n} \in \operatorname{span}_{k[t]}\{1, t^{-1}, \ldots, t^{-(n-1)}\}$$

Multiply through by t^n, we get

$$1 \in \operatorname{span}_{k[t]}\{t^n, t^{n-1}, \ldots, t\}$$

which is a contradiction. However, let $c \in k$ (which we will choose later). Then

$$A = k[t, t^{-1}] = k[t, t^{-1} - ct]$$

Claim 6.1.4. $k[T^{-1} - cT] \subseteq A$ is a finite extension for "most" c.

Proof. Since $tt^{-1} - 1 = 0$, we have that

$$((t^{-1} - ct) + ct)t - 1 = 0$$

Expanding,

$$ct^2 + (t^{-1} - ct)t - 1 = 0$$

Thus, if $c \neq 0$, then we can divide by c to show that t is integral over $k[t - ct^{-1}]$. □

Proof of theorem 6.1.2 assuming k is infinite. We will induct on the minimal number m of generators of A as an k-algebra.

Base case: $m = 0$ is trivial since $A = k$. We can take $A' = A$.

Inducive step: Suppose A is generated by $x_1, \ldots, x_m \in A$ as an k-algebra. If $x_1, \ldots, x_m$ are algebraically independent, then we can take $A = A'$. Otherwise,

Claim 6.1.5. There exists $c_1, \ldots, c_{m-1} \in k$ such that x_m is integral over

$$B = k[x_1 - c_1 x_m, \ldots, x_{m-1} - c_{m-1} x_m]$$

Assuming the claim, then $A = B[x_n]$, and so A is finite over B. But B is generated by $m - 1$ elements, and so by induction, B contains $z_1, \ldots, z_n \in B$, with B finite over $A' = k[z_1, \ldots, z_n]$. Then A is finite over A' by transitivity.

Proof of claim 6.1.5. Since $x_1, \ldots, x_n$ are not algebraically independent over k, there exists a non-zero $f \in k[t_1, \ldots, t_m]$, with

$$f(x_1, \ldots, x_m) = 0$$

We would like to prove that x_m is integral over B, where $c_i \in k$ we will choose later. Write

$$f = \sum_{i=0}^{r} f_{[i]}$$

as a sum of homogeneous parts. Set $F = f_{[r]}$ for the highest order part. For $c_1, \ldots, c_{m-1} \in k$, set

$$g(t_1, \ldots, t_m) = f(t_1 + c_1 t_m, \ldots, t_{m-1} + c_{m-1} t_m, t_m) = F(c_1, \ldots, c_{m-1}, 1)t_m^r + h(t_1, \ldots, t_m)$$

where each term in h has degree of t_m less than r. Note

$$g(x_1 - c_1x_m, \cdots, x_{m-1} - c_{m-1}x_m, x_m) = f(x_1, \ldots, x_m) = 0$$

and that g as a polynomial in t_m over $k[t_1, \ldots, t_{m-1}]$ has degree at most r, and the coefficient of t_m^r is $F(c_1, \ldots, c_{m-1}, 1)$, Since $F(t_1, \ldots, t_m)$ is a non-zero homogeneous polynomial, and so $F(t_1, \ldots, t_{m-1}, 1)$ is not zero. Therefore, there are $c_1, \ldots, c_{m-1}$, with

$$F(c_1, \ldots, c_{m-1}) \neq 0$$

since we are working over an infinite field (Schwartz-Zippel). □

□

Remark 6.1.6. Noether normalisation is true for any field.

From the example

$$k[t, t^{-1}] \cong \frac{k[x, y]}{\langle xy - 1 \rangle}$$

Geometrically, $xy - 1$ is a hyperbola. The projection onto the x-axis is not surjective, but the projection onto $y = cx$ is surjective for $c \neq 0$.

6.2 Hilbert Nullstellensatz

Proposition 6.2.1 (Zariski's lemma)**.** Let $k \subseteq L$ be fields, with L finitely generated as a k-algebra. Then $\dim_k(L) < \infty$.

Proof. By Noether normalisation, we have a finite extension $k[x_1, \ldots, x_\ell] \leq L$ where the x_i are algebraically independent. Moreover, this is an integral extension, and so $k[x_1, \ldots, x_\ell]$ is a field. So $\ell = 0$. Hence $k \leq L$ is a finite extension. □

Lecture 16

From now on, fix a field extension Ω/k, where Ω is algebraically closed.

Definition 6.2.2 (vanishing locus, algebraic set)

For $S \subseteq k[T_1, \ldots, T_n]$, define

$$\mathbb{V}(S) = \{x \in \Omega^n \mid f(x) = 0 \text{ for all } f \in S\}$$

we call such sets *k-algebraic sets*

Definition 6.2.3 (ideal of a subset)

For $X \subseteq \Omega^n$, define

$$I(X) = \{f \in k[T_1, \ldots, T_n] \mid f(x) = 0 \text{ for all } x \in X\} \trianglelefteq k[T_1, \ldots, T_n]$$

Remark 6.2.4. Note $\mathbb{V}(S) = \mathbb{V}(\langle S \rangle)$.

Recall from field theory that if L/k is a finite field extension, then there exists a k-homomorphism $L \to \Omega$.

Theorem 6.2.5. Let $\mathfrak{a} \trianglelefteq k[T_1, \ldots, T_n]$ be an ideal. Then

(i) (Weak Nullstellensatz) $\mathbb{V}(\mathfrak{a}) = \varnothing$ if and only if $1 \in \mathfrak{a}$,

(ii) (Strong Nullstellensatz) $I(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Proof. For (i), $\Longleftarrow$ is clear. Now suppose $1 \notin \mathfrak{a}$. Hence there exists a maximal ideal $\mathfrak{m}$ of $k[T_1, \dots, T_n]$ containing $\mathfrak{a}$, and so $L = k[T_1, \dots, T_n]/\mathfrak{m}$ is a field, and it is also finitely generated as a k-algebra. By Zariski's lemma, $\dim_k(L) < \infty$. Hence there exists a k-homomorphism $L \to \Omega$.

Consider the composition $\varphi : k[T_1, \dots, T_n] \to L \to \Omega$. In this case, $\ker(\varphi) = \mathfrak{m}$. Define

$$x = (\varphi(T_1), \dots, \varphi(T_n)) \in \Omega^n$$

Then for $f \in k[T_1, \dots, T_n]$,

$$\varphi(f) = f(\overline{x})$$

Hence for all $f \in \mathfrak{a} \subseteq \mathfrak{m}$,

$$f(\overline{x}) = \varphi(f) = 0$$

For (ii), let $f \in \sqrt{\mathfrak{a}}$. Then then $f^\ell \in \mathfrak{a}$ for some ℓ, and thus $f^\ell(x) = 0$ for all $x \in \mathbb{V}(\mathfrak{a})$. But we are working in a field, and so $f(x) = 0$ for all $x \in \mathbb{V}(\mathfrak{a})$, i.e. $f \in I(\mathbb{V}(\mathfrak{a}))$.

Conversely, take $f \in I(\mathbb{V}(\mathfrak{a}))$. We want to show that $f \in \sqrt{\mathfrak{a}}$. Equivalently, $\overline{f}$ is nilpotent in $R = k[T_1, \dots, T_n]/\mathfrak{a}$. In turn, this is equivalent to

$$R_{\overline{f}} = 0$$

But recall that

$$R_{\overline{f}} = \frac{R[T_1, \dots, T_n, U]}{\mathfrak{a}^e + \langle Uf - 1 \rangle}$$

Let $\mathfrak{b} = \mathfrak{a}^e + \langle UF - 1 \rangle$. Hence we need to show that $1 \in \mathfrak{b}$. By the Weak Nullstellensatz, it suffices to show $\mathbb{V}\mathfrak{b} = \varnothing$.

Take $x = (x_1, \dots, x_n, u) \in \mathbb{V}(\mathfrak{b}) \subseteq \Omega^{n+1}$. Let $x' = (x_1, \dots, x_n)$, then

$$x' \in \mathbb{V}(\mathfrak{a})$$

Hence $f(x')$, since $f \in I(\mathbb{V}(\mathfrak{a}))$. Considering the canonical embedding $k[T_1, \dots, T_n] \hookrightarrow k[T_1, \dots, T_n, U]$, $f(x') = 0$. Now $(Uf - 1)(x) = -1 \neq 0$, contradiction, as $Uf - 1 \in \mathfrak{b}$. □

Recall $\sqrt{\sqrt{I}} = \sqrt{I}$, and we have that

1. if $X \subseteq Y \subseteq \Omega^n$, then $I(Y) \subseteq I(X)$,
2. if $S \subseteq T \subseteq k[T_1, \dots, T_n]$, then $\mathbb{V}(T) \subseteq \mathbb{V}(S)$,
3. if $S \subseteq k[T_1, \dots, T_n]$, then $S = I(\mathbb{V}(S))$,
4. if $X \subseteq \Omega^n$, then $X \subseteq \mathbb{V}(I(X))$.
5. if $X \subseteq \Omega^n$ is an algebraic set, then $X = \mathbb{V}(I(X))$. This follows from writing $X = \mathbb{V}(\mathfrak{a})$.
6. if $X \subseteq \Omega^n$, then $I(X)$ is a radical ideal.

Proposition 6.2.6. We have a bijection

$$\begin{aligned} \{k\text{-alg. subsets of } \Omega^n\} &\leftrightarrow \{\text{radical ideals in } k[T_1, \dots, T_n]\} \\ X &\mapsto I(X) \\ \mathbb{V}(\mathfrak{a}) &\leftarrow\!\shortmid \mathfrak{a} \end{aligned}$$

Proof. We know $I(X)$ is radical, and $X = \mathbb{V}(I(X))$. Now take $\mathfrak{a} \in k[T_1, \dots, T_n]$ a radical ideal, then by the strong Nullstellensatz

$$I(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$$

□

Remark 6.2.7. Note that we defined algebraic subsets with respect to $k \subseteq \Omega$.

Corollary 6.2.8. Under the above correspondence, maximal ideals correspond to minimal non-empty algebraic sets. In particular, let $k = \Omega$ be an algebraically closed field. Then we have a bijection

$$\Omega^n \leftrightarrow \{\text{maximal ideals of } \Omega[T_1, \ldots, T_n]\}$$
$$x = (x_1, \ldots, x_n) \mapsto \mathfrak{m}_x = (T_1 - x_1, \ldots, T_n - x_n)$$

Proof. The first part is just the fact that $\mathbb{V}$ and I are order reversing.

Since $\Omega[T_1, \ldots, T_n]/\mathfrak{m}_x = \Omega$, $\mathfrak{m}_x$ is a maximal ideal. Moreover, $\mathfrak{m}_x$ is the ideal of polynomials which vanish on x. To see this,

$$\mathfrak{m}_x \subseteq I(\{x\})$$

But $\mathfrak{m}_x$ is maximal, and $I(\{x\})$ is a proper ideal, and so equality holds. Moreover, $\mathbb{V}(\mathfrak{m}_x) = \{x\}$. The claim follows from the inclusion reversing bijection from before. □

Note that the requirement that $k = \Omega$ above is necessary. Consider the field extension $\mathbb{C}/\mathbb{R}$. In $\mathbb{R}[t]$, $\langle t^2 + 1 \rangle$ is a maximal ideal, but it corresponds to the points $\{i, -i\} \subseteq \mathbb{C}$. In general, for Ω/k as above, each point $x \in k^n$ is a minimal k-algebraic subsets of Ω^n, but there can be more. If $\text{char}(k) = 0$, then $x \in \Omega^n$ is k-algebraic if and only if the coordinates are in k. More generally, if Ω/k is separable.

On the other hand, if $k = \mathbb{F}_p(x)$ is the field of rational functions over $\mathbb{F}_p$, $\Omega = \overline{k}$, $n = 1$. Consider the polynomial

$$T^p - x \in k[T]$$

By Frobenius and that k is algebraically closed, $T^p - x = (T - x^{1/p})^p$ over Ω. Hence

$$\mathbb{V}(T^p - x) = \{x^{1/p}\}$$

Finally, note that every prime ideal is radical.

Definition 6.2.9 (irreducible)
$X \subseteq \Omega^n$ is *irreducible* if X is not the union $X = X_1 \cup X_2$, X_1, X_2 algebraic and $X \neq X_1, X_2$.

Proposition 6.2.10. Let $X \subseteq \Omega^n$ be an algebraic set. Then X is irreducible if and only if $I(X)$ is prime.

Proof. See notes, or Part II Algebraic Geometry. □

7 Integral and finite extensions again

Definition 7.0.1 (integral over an ideal)
If $A \subseteq B$, $\mathfrak{a} \trianglelefteq A$, $x \in B$ is *integral over* $\mathfrak{a}$ if

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

where $a_i \in \mathfrak{a}$.

Lecture 17

Definition 7.0.2 (integral closure over an ideal)
If $A \subseteq B$ rings, $\mathfrak{a} \trianglelefteq A$, then the *integral closure of* $\mathfrak{a}$ *in* B is

$$\{x \in B \mid x \text{ is } \mathfrak{a}\text{-integral}\}$$

Proposition 7.0.3. If $A \subseteq B$ are rings, $\overline{A}$ the integral closure of $A \subseteq B$, $\mathfrak{a} \subseteq A$ is an ideal. Then the integral closure of $\mathfrak{a}$ in B is

$$\sqrt{\mathfrak{a}\overline{A}}$$

where we take the radical in $\overline{A}$.

Proof. Suppose $b \in B$ is $\mathfrak{a}$-integral, then

$$b^n + a_1 b^{n-1} + a_n = 0$$

with $a_i \in \mathfrak{a}$. In particular, $\mathfrak{b}$ is integral over A, and therefore, $b_0, \dots, b_{n-1} \in \overline{A}$. Using the above,

$$b^n \in \mathfrak{a}\overline{A}$$

and so $b \in \sqrt{\mathfrak{a}\overline{A}}$.

Now suppose $b \in \sqrt{\mathfrak{a}\overline{A}}$. Then $b^n \in \mathfrak{a}\overline{A}$ for some n, and so

$$b^n = \sum_{i=1}^{m} a_i x_i \tag{$*$}$$

where $a_i \in \mathfrak{a}$, $x_i \in \overline{A}$. Define the algebra

$$M := A[x_1, \dots, x_m]$$

Since each x_i is integral over A, M is a finite A-algebra. Moreover, from $(*)$, $b^n M \subseteq \mathfrak{a}M$. Now define $f : M \to M$,

$$f(m) = b^n m$$

This satisfies $f(M) \subseteq \mathfrak{a}M$, and f is A-linear. Therefore, by Cayley-Hamilton,

$$f^\ell + \alpha_1 f^{\ell-1} + \cdots + \alpha_\ell = 0 \in \mathrm{End}_R(M)$$

where each $\alpha_i \in \mathfrak{a}$. Evaluating this at $1 \in A$, we get that

$$b^{n\ell} + \alpha_1 b^{n(\ell-1)} + \cdots + \alpha_\ell = 0 \in B$$

and so b is $\mathfrak{a}$-integral. □

Corollary 7.0.4. Suppose $A \subseteq B$ are rings, $\mathfrak{a} \trianglelefteq A$, $b \in B$, then b is $\mathfrak{a}$-integral if and only if b is $\sqrt{\mathfrak{a}}$-integral.

Proof. By the proposition, it suffices to show

$$\sqrt{\mathfrak{a}\overline{A}} = \sqrt{\sqrt{\mathfrak{a}}\,\overline{A}}$$

$\subseteq$ is clear. For $\supseteq$, note that in general, $\sqrt{I}^e \subseteq \sqrt{I^e}$. Applying this to the above, we have that

$$\sqrt{\mathfrak{a}}\,\overline{A} \subseteq \sqrt{\mathfrak{a}\overline{A}}$$

and so

$$\sqrt{\sqrt{\mathfrak{a}}\,\overline{A}} \subseteq \sqrt{\mathfrak{a}\overline{A}}$$

□

Proposition 7.0.5. Let A be an integrally closed[a] integral domain, and $A \subseteq B$ rings, B is an integral domain, and an ideal $\mathfrak{a} \trianglelefteq A$. Let $b \in B$, We have a field extension $\operatorname{Frac}(B)/\operatorname{Frac}(A)$, and the following are equivalent:

(i) b is integral over $\mathfrak{a}$

(ii) b is algebraic over $\operatorname{Frac}(A)$, with minimal polynomial over $\operatorname{Frac}(A)$ of the form

$$T^n + a_1 T^{n-1} + \cdots + a_0$$

where $a_i \in \sqrt{\mathfrak{a}}$.

[a] in $\operatorname{Frac}(A)$

Proof. Suppose (ii) holds, then b is integral over $\sqrt{\mathfrak{a}}$ by definition. By the corollary, b is integral over $\mathfrak{a}$.

Now suppose (i) holds. Let $F = \operatorname{Frac}(A)$. Then we have that

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

where $a_i \in \mathfrak{a}$. Set

$$h(T) = T^n + a_1 T^{n-1} + \cdots + a_n \in F[T]$$

Then $h(b) = 0$, and so b is algebraic over $\operatorname{Frac}(A)$. Now let f be the minimial polynomial of b over F. Let Ω/F be an algebraically closed field. In this case,

$$f = \prod_{i=1}^{\ell} (T - \alpha_i) \tag{$*$}$$

where each $\alpha_i \in \Omega$. We would like to show that the coefficient of f are in $\sqrt{\mathfrak{a}}$. Since A is integrally closed, the integral closure of $\mathfrak{a}$ in F is $\sqrt{\mathfrak{a}} \trianglelefteq A$. Thus, it suffices to show that the coefficients of f are $\mathfrak{a}$-integral. Note that by definition, the coefficient of f are in F.

Expanding $(*)$, we see the coefficients of f are sums of products of the α_i. By the proposition, the integral closure of $\mathfrak{a}$ in Ω is closed under sums and products (as it is an ideal). Therefore, we need to show that each α_i is integral over A.

In this case, α_i and b have the same minimal polynomial over $\operatorname{Frac}(A)$, and therefore, there exists $\varphi_i : F(b) \to F(\alpha_i)$, which is a F-homomorphism, with $\varphi_i(b) = \alpha_i$. Since h has coefficients in F,

$$h(\alpha_i) = h(\varphi_i(b)) = \varphi(h_i(b)) = 0$$

□

7.1 Cohen-Seidenberg theorems

Let $\iota : A \hookrightarrow B$ be the inclusion map. Then we have a pullback

$$\begin{aligned} i^* : \operatorname{Spec}(B) &\to \operatorname{Spec}(A) \\ \mathfrak{q} &\mapsto \mathfrak{q} \cap A \end{aligned}$$

We are interested in studying i^*, in particular its fibres.

Proposition 7.1.1 (incomparability)**.** If $A \subseteq B$ is an integral extension, $\mathfrak{q}, \mathfrak{q}' \in \operatorname{Spec}(B)$, $\mathfrak{q} \subseteq \mathfrak{q}'$, and $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Then $\mathfrak{q} = \mathfrak{q}'$.

That is, the elements of the fibres are pairwise incomparable.

Proof. Let $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$, and $S = A \setminus \mathfrak{p}$. $\mathfrak{q}$ and $\mathfrak{q}'$ are prime ideals of B not intersecting S, So

$$\mathfrak{q} = (S^{-1}\mathfrak{q})^c$$

where by $S^{-1}\mathfrak{q}$, we mean the extension of $\mathfrak{q}$ to $S^{-1}B$. Note this is not the localisation of B at $\mathfrak{p}$, since $\mathfrak{p}$ need not be a prime in B. Similarly, $\mathfrak{q}' = (S^{-1}\mathfrak{q}')^c$. We would like to show that

$$S^{-1}\mathfrak{q} = S^{-1}\mathfrak{q}'$$

To see this,

$$S^{-1}\mathfrak{q} \cap A_\mathfrak{p} = S^{-1}\mathfrak{q} \cap S^{-1}A = S^{-1}(\mathfrak{q} \cap A) = S^{-1}\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$$

Similarly, $S^{-1}\mathfrak{q}' \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$, which is the unique maximal ideal of $A_\mathfrak{p}$.

Since $A \subseteq B$ is an integral extension, so is $A_\mathfrak{p} \subseteq S^{-1}B$. Therefore, the contractions $S^{-1}\mathfrak{q}, S^{-1}\mathfrak{q}'$ are maximal ideals of $S^{-1}B$. But $\mathfrak{q} \subseteq \mathfrak{q}'$, and so they are equal. □

Lecture 18

Proposition 7.1.2 (lying over)**.** Let $A \subseteq B$ be an integral extension, $\mathfrak{p} \in \operatorname{Spec}(A)$. Then there exists $\mathfrak{q} \in \operatorname{Spec}(B)$ with $\mathfrak{q} \cap A = \mathfrak{p}$.

Equivalently, the natural map $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is surjective.

We can think about this geometrically, if $p : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ denotes the natural map, then we can think of $\operatorname{Spec}(B)$ as a "bundle" over $\operatorname{Spec}(A)$. Surjectivity means that each fibre is non-empty.

Proof. Let $S = A \setminus \mathfrak{p}$, then we have the commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \beta \\ A_\mathfrak{p} = S^{-1}A & \longrightarrow & S^{-1}B \end{array}$$

Take $\mathfrak{m} \in \operatorname{maxSpec}(S^{-1}B)$. Since $S^{-1}A \subseteq S^{-1}B$ is an integral extension, and so $\mathfrak{m} \cap S^{-1}A \in \operatorname{maxSpec}(S^{-1}A) = \{\mathfrak{p}A_\mathfrak{p}\}$. Hence $\mathfrak{m} \cap S^{-1}A = \mathfrak{p}A_\mathfrak{p}$. Under the localisation map, $\mathfrak{p}A_\mathfrak{p}$ contracts to $\mathfrak{p}$. Thus, $\mathfrak{m}$ contracts to $\mathfrak{p}$, and so $\mathfrak{q} = \beta^{-1}(\mathfrak{m})$ has $\mathfrak{q} \cap A = \mathfrak{p}$. □

Proposition 7.1.3 (going up)**.** Let $A \subseteq B$ be an integral extension of rings, let $\mathfrak{p}_1, \mathfrak{p}_2 \in \operatorname{Spec}(A)$, $\mathfrak{q}_1 \in \operatorname{Spec}(B)$, with $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$, $\mathfrak{q}_1^c = \mathfrak{p}_1$. That is,

$$\begin{array}{ccc} \mathfrak{q}_1 & & \\ | & & \\ \mathfrak{p}_1 & \hookrightarrow & \mathfrak{p}_2 \end{array}$$

there exists $\mathfrak{q}_2 \in \operatorname{Spec}(B)$, with $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, and $\mathfrak{q}_2^c = \mathfrak{p}_2$. Note that in the diagram we use vertical line with no arrows to denote contraction.

Proof. $\mathfrak{p}_1 = \mathfrak{q}_1 \cap A$, and so we have an injective map $A/\mathfrak{p}_1 \to B/\mathfrak{q}_1$. This is an integral extension. From lying over, there exists a prime ideal $\mathfrak{q}_2/\mathfrak{q}_1 \in \operatorname{Spec}(B/\mathfrak{q}_1)$, with $\mathfrak{q}_2 \in \operatorname{Spec}(B)$, which contracts to $\mathfrak{p}_2/\mathfrak{p}_1 \in \operatorname{Spec}(A/\mathfrak{p}_1)$.

Claim 7.1.4. $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

For this, consider the diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A/\mathfrak{p}_1 & \longrightarrow & B/\mathfrak{q}_1 \end{array}$$

Contracting along the bottom left we get $\mathfrak{p}_2$, and contracting along thr right gives $\mathfrak{q}_2$. □

Proposition 7.1.5 (going down)**.** Let $A \subseteq B$ be an integral extension of integral domains, and assume A is integrally closed. Consider the diagram

$$\begin{array}{ccc} \mathfrak{q}_1 & & \\ \Big| & & \\ \mathfrak{p}_1 & \hookleftarrow & \mathfrak{p}_2 \end{array}$$

Then there exists a prime $\mathfrak{q}_2 \in \mathrm{Spec}(B)$ with $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

Proof. Consider the map

$$A \hookrightarrow B \hookrightarrow B_{\mathfrak{q}_1}$$

Claim 7.1.6. There exists $\mathfrak{n} \in \mathrm{Spec}(B_{\mathfrak{q}_1})$ such that $\mathfrak{n} \cap A = \mathfrak{p}_2$.

Assuming the claim, $(\mathfrak{n} \cap B) \cap A = \mathfrak{p}_2$, and $\mathfrak{n} \cap B$ is a prime ideal of B contained in $\mathfrak{q}_1$.

To prove the claim, it suffices to show that

$$(\mathfrak{p}_2 B)B_{\mathfrak{q}_1} = \mathfrak{p}_2 B_{\mathfrak{q}_1} \cap A \subseteq \mathfrak{p}_2$$

Take $y/s \in (\mathfrak{p}_2 B)B_{\mathfrak{q}_1} \cap A$, with $y \in \mathfrak{p}_2 B$, $s \in B \setminus \mathfrak{q}_1$. Now $A \subseteq B$ is an integral extension, therefore the integral closure of $\mathfrak{p}_2$ in B is $\sqrt{\mathfrak{p}_2 B}$. Thus, y is integral over $\mathfrak{p}_2$. Since A is integrally closed, by proposition 7.0.5, $y \in \mathrm{Frac}(A)$ is algebraic over $\mathrm{Frac}(A)$, and the minimal polynomial has the form

$$y^r + u_1 y^{r-1} + \cdots + u_r = 0$$

where $u_i \in \mathfrak{p}_2$ (note any prime ideal is radical). We can then write

$$y = \frac{y}{s} s$$

$y, s \in B \subseteq \mathrm{Frac}(B)$, $y/s \in A \subseteq \mathrm{Frac}(A)$, and so we have

$$\left(\frac{y}{s} s\right)^r + u_1 \left(\frac{y}{s} s\right)^{r-1} + \cdots + u_r = 0$$

Multiply through by $(s/y)^r$,

$$s^r + \frac{s}{y} u_1 s^{r-1} + \cdots + \left(\frac{s}{y}\right)^r u_r = 0 \tag{$*$}$$

This is the minimal polynomial of s over $\mathrm{Frac}(A)$, since the process above is reversible. But $s \in B$, and so s is integral over A. Therefore, the coefficients of $(*)$ must all be in A, again by proposition 7.0.5.

Suppose for contradiction $y/s \notin \mathfrak{p}_2$. Then

$$u_i = \left(\frac{y}{s}\right)^i \left(\frac{s}{y}\right)^i u_i$$

Then $(y/s)^i \in A \setminus \mathfrak{p}_2$, and we know that $(s/y)^i u_i \in A$. Since $u_i \in \mathfrak{p}_2$, we must have that $(s/y)^i u_i \in \mathfrak{p}_2$. With this, by $(*)$,

$$s^r \in \mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B = (\mathfrak{q}_1 \cap A)B \subseteq \mathfrak{q}_1$$

Hence $s \in \mathfrak{q}_1$. Contradiction. □

With the geometric picture as above, going up and going down allows us to move between the fibres in a "nice" way. One way to think about this would be constructing a section of a bundle.

In terms of algebraic geometry, going up says that the natural map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a closed map. Similarly, going down says that the map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is open. Some assumptions might be needed to make this analogy rigorous.

8 Primary decomposition

Definition 8.0.1 (primary ideal)
Let I be an ideal of R, then I is *primary* if R/I is non-zero, and every zero divisor in R/I is nilpotent.

Remark 8.0.2. Contrast this with I being prime if R/I is an integral domain, and I is radical if R/I has no non-zero nilpotent elements.

In particular, any prime ideal is radical and primary. Note R is radical, but not prime nor primary.

Lecture 19

Example 8.0.3
In $\mathbb{Z}$, $\langle 6\rangle$ is radical, but not primary, since in $\mathbb{R}/6$, there are no non-zero nilpotent elements, but $2 \times 3 = 6$. But $\langle 9\rangle$ is primary, but not radical.

More generally, for $x \neq 0$,

- $\langle x\rangle$ if and only if x is prime,
- $\langle x\rangle$ is radical if and only if x is square free,
- $\langle x\rangle$ is primary if and only if $x = p^n$ for some prime p.

Proposition 8.0.4. Let $I \trianglelefteq R$ be a proper ideal.

(i) if I is primary, then $\mathfrak{p} = \langle I\rangle$ is prime, and we say that I is $\mathfrak{p}$-primary,

(ii) if $\sqrt{I}$ is maximal, then I is primary,

(iii) if $\mathfrak{q}_1, \dots, \mathfrak{q}_n$ are all $\mathfrak{p}$-primary, then so is $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$,

(iv) if I has a *primary decomposition*, i.e.

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \qquad (*)$$

where $\mathfrak{q}_i$ is primary, then I has a *minimal primary decomposition*, i.e. like $(*)$, but $\sqrt{\mathfrak{q}_1}, \dots, \sqrt{\mathfrak{q}_n}$ are distinct, and none of the $\mathfrak{q}_i$ can be dropped,

(v) if R is Noetherian, then every ideal I has a primary decomposition

Proof. Examples sheet. □

Example 8.0.5
In $\mathbb{Z}$,

$$\langle 90\rangle = \langle 2\rangle \cap \langle 3^2\rangle \cap \langle 5\rangle$$

Example 8.0.6
For a prime ideal $\mathfrak{p}$ of R, if $\mathfrak{p}^n$ is primary, then $\mathfrak{p}^n$ is $\mathfrak{p}$-primary, as $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$.

1. **Not every primary ideal is a power of a prime**. Let $R = k[x, y]$, $\mathfrak{q} = \langle x, y^2\rangle$. To see that $\mathfrak{q}$ is primary, $\sqrt{\mathfrak{q}} = \langle x, y\rangle$, which is a maximal ideal, and so $\mathfrak{q}$ is $\langle x, y\rangle$-primary. Alternatively, $k[x, y]/\mathfrak{q} = k[y]/\langle y^2\rangle$. If $f \in k[y]$ and $f + \langle y^2\rangle$ is a zero divisor, then y divides f, and so $f + \langle y^2\rangle$ is nilpotent.

   On the other hand, if $\mathfrak{q} = \mathfrak{p}^n$, then $\sqrt{\mathfrak{q}} = \mathfrak{p}$, but $\sqrt{\mathfrak{q}} = \langle x, y\rangle$. But we have that

   $$\langle x, y\rangle^2 \subset \langle x, y^2\rangle \subset \langle x, y\rangle$$

2. **Power of a prime does not have to be primary.** Let $R = k[x,y,z]/\langle xy - z^2 \rangle = k[\overline{x}, \overline{y}, \overline{z}]$. Let $\mathfrak{p} = \langle \overline{x}, \overline{z} \rangle$. We will show that $\mathfrak{p}$ is prime, but $\mathfrak{p}^2$ is not primary. In this case,

$$R/\mathfrak{p} = k[y]$$

which is an integral domain, and so $\mathfrak{p}$ is prime. On the other hand,

$$\mathfrak{p}^2 = \langle \overline{x}^2, \overline{xz}, \overline{z}^2 \rangle$$

With this,

$$\overline{xy} = \overline{z}^2 \in \mathfrak{p}^2$$

so the image of $\overline{xy}$ in $R/\mathfrak{p}^2$ is zero. But $\overline{x} + \mathfrak{p}^2 \neq 0$, and so $\overline{y} + \mathfrak{p}^2$ is a zero divisor in $R/\mathfrak{p}^2$. But

$$R/\mathfrak{p}^2 = k[x,y,z]/\langle xy - z^2, x^2, xz, z^2 \rangle$$

and no power of y is in $\langle xy - z^2, x^2, xz, z^2 \rangle$.

Theorem 8.0.7. Let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be a minimal primary decomposition. Let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, then

(i) (*associated primes of* I) $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are determined only by I,

(ii) (*isolated primes of* I) the minimal elements amongst the $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are exactly the minimal primes of R containing I,

(iii) if $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are the isolated primes of I, then $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ are determined only by I.

Proof. Examples sheet. □

Definition 8.0.8 (embedded primes)
The *embedded primes* of I are the associated primes which are not isolated.

Example 8.0.9
Let $R = k[x,y]$, $I = \langle x^2, xy \rangle$. Then we have primary decompositions

$$I = \langle x \rangle \cap \langle x, y \rangle^2 = \langle x \rangle \cap \langle x^2, y \rangle$$

In this case, $\sqrt{\langle x \rangle} = \langle x \rangle$, $\sqrt{\langle x, y \rangle^2} = \langle x, y \rangle$, and $\sqrt{\langle x^2, y \rangle} = \langle x, y \rangle$.

In this case, the associated primes are $\langle x \rangle, \langle x, y \rangle$, which don't depend on the decomposition. In particular, $\langle x \rangle$ is isolated and $\langle x, y \rangle$ is embedded.

Thining about this geometrically, $\mathbb{V}(\langle x, y \rangle) \subseteq \mathbb{V}\langle x \rangle$, which is why we call them *embedded*.

If $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is a minimal primary decomposition, $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Say $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are the isolated primes. Then

$$\sqrt{I} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_t} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$$

which is a (minimal) primary decomposition of $\sqrt{I}$, and all associated primes are isolated. Thus, going from I ot $\sqrt{I}$ is the same as forgetting the embedded primes of I.

Geometrically, in $k[t_1, \ldots, t_n]$, where $k \subseteq \mathbb{C}$ is a subfield, then

$$\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$$

and $I(\mathbb{V}(I)) = \sqrt{I}$, thus $\mathbb{V}(I)$ only sees $\sqrt{I}$, or equivalently, it forgets about the embedded primes.

9 Direct and inverse limits

Lecture 20

Let $\mathscr{C}$ be a category.

Definition 9.0.1 (directed set)
A *directed set* $(I, \leq)$ is a poset, such that for all $a, b \in I$, there exists $c \in I$ such that $a \leq c, b \leq c$.

Definition 9.0.2 (directed system)
A *direct system* on I is objects $(X_i)_{i \in I}$ of $\mathscr{C}$, and for every $i \leq j$, a morphism $f_{ij} : X_i \to X_j$, such that

1. $f_{ii} = \mathrm{id}_{X_i}$ for all i,
2. $f_{ik} = f_{jk} f_{ij}$ for all $i \leq j \leq k$.

Definition 9.0.3 (inverse system)
An *inverse system* on I is objects $(Y_i)_{i \in I}$ of $\mathscr{C}$, and for every $i \leq j$, a morphism $h_{ij} : X_j \to X_i$, such that

1. $h_{ii} = \mathrm{id}_{Y_i}$ for all i,
2. $f_{ik} = f_{ij} f_{jk}$ for all $i \leq j \leq k$.

Example 9.0.4
Let $I = (\mathbb{N}, \leq)$, fix a prime $\mathfrak{p}$, consider the direct system

$$X_i = \mathbb{F}_{p^{i!}}$$

and f_{ij} being field embeddings. Recall if $a \mid b$, then there exists an embedding $\mathbb{F}_{p^a} \hookrightarrow \mathbb{F}_{p^b}$, and that the set of all embeddings are given by

$$x \mapsto \varphi(x)^{p^c}$$

for $0 \leq c \leq a - 1$. But we can just define $f_{i,i+1}$, and the other maps are defined by composition.

Example 9.0.5
Let $I = (\mathbb{N}, \leq)$, fix a prime p, and consider

$$Y_i = \mathbb{Z}/p^i$$

and

$$\begin{aligned} h_{ij} : \mathbb{Z}/p^j &\to \mathbb{Z}/p^i \\ x &\mapsto p^{i-j} x \end{aligned}$$

the natural projection map.

Definition 9.0.6 (direct limit)
Let $(I, \leq)$ be a directed set. If $D = ((X_i), (f_{ij}))$ forms a direct system, then the *direct limit* of D is

$$\varinjlim X_i = \frac{\bigsqcup_i X_i}{\sim}$$

where for $x_i \in X_i, x_j \in X_j$, $x_i \sim x_j$ if and only if there exists k such that $f_{ik}(x_i) = f_{jk}(x_j)$. Equivalently, take the equivalence relation generated by $x_i \sim f_{ij}(x_i)$ for all $i \leq j$.

Remark 9.0.7. If $\mathcal{D}$ is a direct system in $\mathscr{C}$, then the direct limit is in $\mathscr{C}$ as well.

Definition 9.0.8 (inverse limit)

Let $(I, \leq)$ be a direct set. If $E = ((Y_i), (h_{ij}))$ forms an inverse system, then the *inverse limit* of E is

$$\varprojlim Y_i = \left\{ y \in \prod_i Y_i \mid y_i = f_{ij}(y_j) \text{ for all } i \leq j \right\}$$

Example 9.0.9

We claim that $\mathbb{F}_p^{\text{alg}} = \varinjlim \mathbb{F}_{p^{i!}}$ is an algebraic closure of $\mathbb{F}_p$.

First we check that $\mathbb{F}_p^{\text{alg}}$ is algebraic over $\mathbb{F}_p$. Choose $[x] \in \mathbb{F}_p^{\text{alg}}$, say $x \in \mathbb{F}_{p^{i!}}$, then $x^{p^{i!}} - x = 0$, and so $[x]^{p^{i!}} - [x] = 0$.

Next we check that it is algebraically closed. Let $[h] \in \mathbb{F}_p^{\text{alg}}[t]$. Since $[h]$ has finitely many coefficients, we have that $h \in \mathbb{F}_{p^{i!}}[t]$. Considering a splitting field for h, which is $\mathbb{F}_{p^{\ell}}$, which in turn embeds into $\mathbb{F}_{p^{\ell!}}$. Hence h splits over $\mathbb{F}_{p^{\ell!}}$, and so h splits under the embdedding $f_{i\ell} : \mathbb{F}_{p^{i!}} \to \mathbb{F}_{p^{\ell!}}$. This means that $[h]$ splits over the direct limit.

Example 9.0.10

Let

$$\mathbb{Z}_p = \varprojlim \frac{\mathbb{Z}}{p^i}$$

be the ring of p-adic integers. For example, $1 = (1, 1, 1, \ldots)$ and

$$-1 = (p-1, p^2-1, p^3-1, \ldots)$$

Definition 9.0.11 ($\mathfrak{a}$-adic completion)

Let R be a ring, $\mathfrak{a} \trianglelefteq R$ an ideal, then the $\mathfrak{a}$*-adic completion* of R is

$$\widehat{R} = \varprojlim \frac{R}{\mathfrak{a}^i}$$

Example 9.0.12

If $R = \mathbb{Z}$, $\mathfrak{a} = \langle p \rangle$, then $\widehat{R} = \mathbb{Z}_p$.

Example 9.0.13

If $R = k[T]$, $\mathfrak{a} = \langle T \rangle$, then

$$\widehat{R} = \varprojlim \frac{R}{\langle T^i \rangle} = k[\![T]\!]$$

Definition 9.0.14 ($\mathfrak{a}$-adic completion of a module)
Let R be a ring, $\mathfrak{a} \trianglelefteq R$ be an ideal, M an R-module, then $\mathfrak{a}$-*adic completion* of M is

$$\widehat{M} = \varprojlim \frac{M}{\mathfrak{a}^i M}$$

which is naturally a $\widehat{M}$-module.

Definition 9.0.15 (filtration, completion with respect to a filtration)
A *filtration* of an R-module M is a sequence (M_n) of submodules of M, with $M_n \supseteq M_{n+1} \supseteq \cdots$, and $M_0 = M$.

The *completion of* M *with respect to the filtration* is the inverse limit

$$\varprojlim \frac{M}{M_n}$$

Theorem 9.0.16. Let R be a Noetherian ring, and let $\mathfrak{a} \trianglelefteq R$ be an ideal. Let $\widehat{R}$ denote the $\mathfrak{a}$-adic completion of R.

(i) $\widehat{R}$ is Noetherian,

(ii) the functor $\widehat{R} \otimes_R (\cdot)$ is exact.

(iii) if M is a finitely generated R-module, then the natural map

$$\widehat{R} \otimes M \to \widehat{M}$$

is an $\widehat{R}$-linear isomorphism.

Corollary 9.0.17. If R is a Noetherian ring, $R[[T_1, \ldots, T_n]]$ is Noetherian.

Proof. It is the $\mathfrak{m}$-adic completion of $R[T_1, \ldots, T_n]$ at $\mathfrak{m} = \langle T_1, \ldots, T_n \rangle$. □

Lecture 21

10 Filtration and graded rings

10.1 Graded rings and modules

Definition 10.1.1 (graded ring)
A *graded ring* A is a ring

$$A = \bigoplus_{n=0}^{\infty} A_n$$

where each A_i is an additive subgroup of A, and $A_n A_m \subseteq A_{n+m}$.

Lemma 10.1.2. A_0 is a subring of A.

Proof. The only thing we need to show is that $1 \in A_0$. If $A = A_0$ then we are done. Otherwise, choose $z \in A_n$, and say

$$1 = \sum_i y_i$$

where $y_i \in A_i$. Then $y_i z \in A_{n+i}$. But $z = 1z$, and so we must have that $y_0 = 1, y_i = 0$ for $i > 0$. □

Example 10.1.3

$A_d = k[T_1, \ldots, T_n]$ is a graded ring, and in this case A_d is the degree d homogeneous polynomials.

Definition 10.1.4 (irrelevant ideal)

We call

$$A_+ = \bigoplus_{n \geq 1} A_n$$

the *irrelevant ideal*.

A_+ is the kernel of the projection map $A \to A_0$, and so $A/A_+ \cong A_0$.

Definition 10.1.5 (graded module)

Let A be a graded ring. A *graded A-module* is an A-module M, with

$$M = \bigoplus_n M_n$$

each M_i an additive subgroup, and $A_n M_m \subseteq M_{n+m}$.

Proposition 10.1.6. Let A be a graded ring. Then A is Noetherian if and only if A_0 is Noetherian and A is a finitely generated A_0-algebra.

Proof. From Hilbert's basis theorem, if A_0 is Noetherian and A is a finitely generated A_0-algebra, then A is Noetherian.

Now suppose A is Noetherian. Then $A_0 = A/A_+$ is the quotient of a Noetherian ring, and so Noetherian. Next, A_+ is generated by the set of homogeneous elements of positive degree. Now A_+ is finitely generated, as A is Noetherian. That is,

$$A_+ = \langle x_1, \ldots, x_s \rangle$$

where $x_i \in A_{k_i}, k_i > 0$. Let A' be the A_0-subalgebra of A, defined by

$$A' = A_0[x_1, \ldots, x_s]$$

We would like to show $A = A'$. It suffices to show that $A_n \subseteq A'$ for every A. We will prove this by induction on n. $n = 0$ is clear.

Now take $y \in A_n$, $n > 0$. Now $y \in A_+$, and so we can write

$$y = \sum_{i=1}^{s} r_i x_i$$

where $r_i \in A$. Apply the projection $A \to A_n$, we get

$$y = \sum_{i=1}^{s} a_i x_i$$

where $a_i \in A_{n-k_i}$. But as $k_i > 0$, the induction hypothesis implies that each a_i is in A', and so $y \in A'$. □

10.2 Associated graded ring

Definition 10.2.1 ($\mathfrak{a}$-filtration)
Let $\mathfrak{a} \trianglelefteq R$ be an ideal, M an R-module. A filtration (M_n) is an $\mathfrak{a}$-*filtration* if $\mathfrak{a}M_n \subseteq M_{n+1}$ for all n.
An $\mathfrak{a}$-filtration is *stable* if $\mathfrak{a}M_n = M_{n+1}$ for all sufficiently large n.

Example 10.2.2
$(\mathfrak{a}^n M)_{n \geq 0}$ is a stable $\mathfrak{a}$-filtration of M.

Definition 10.2.3 (associated graded ring)
If $\mathfrak{a} \trianglelefteq R$ is an ideal, then we have an *associated graded ring*

$$\mathrm{G}_{\mathfrak{a}}(R) = \bigoplus_{n \geq 0} \frac{\mathfrak{a}^n}{\mathfrak{a}^{n+1}}$$

We make this into a ring, by

$$(x + \mathfrak{a}^{n+1})(y + \mathfrak{a}^{\ell+1}) = xy + \mathfrak{a}^{n+\ell+1}$$

for $x \in \mathfrak{a}^n$, $y \in \mathfrak{a}^\ell$.

Definition 10.2.4 (associated graded module)
If $\mathfrak{a} \trianglelefteq R$ an ideal, M an R-module, $(M_n)_{n \geq 0}$ an $\mathfrak{a}$-filtration of M, then we have an *associated graded module*

$$\mathrm{G}(M) = \bigoplus_{n \geq 0} \frac{M_n}{M_{n+1}}$$

which is an $\mathrm{G}_{\mathfrak{a}}(R)$-module, with module structure given by

$$(x + \mathfrak{a}^{n+1})(m + M_{\ell+1}) = xm + M_{n+\ell+1}$$

Proposition 10.2.5. Let R be a Noetherian ring, $\mathfrak{a} \trianglelefteq R$ an ideal. Then

(i) $\mathrm{G}_{\mathfrak{a}}(R)$ is Noetherian,

(ii) if M is a finitely generated R-module, (M_n) is a stable $\mathfrak{a}$-filtration of M, then $\mathrm{G}(M)$ is a finitely generated $\mathrm{G}_{\mathfrak{a}}(R)$-module.

Proof. For (i), since R is Noetherian, $\mathfrak{a}$ is finitely generated, say

$$\mathfrak{a} = \langle x_1, \dots, x_s \rangle$$

Set $\overline{x_i} = x_i + \mathfrak{a}^2 \in \mathfrak{a}/\mathfrak{a}^2$. Then $\mathrm{G}_{\mathfrak{a}}(R)$ is generated as an $R/\mathfrak{a}$-algebra by $\overline{x_1}, \dots, \overline{x_n}$. But $R/\mathfrak{a}$ is a Noetherian ring, and so $\mathrm{G}_{\mathfrak{a}}(R)$ by the Hilbert Basis Theorem.

For (ii), since (M_n) is stable, so there exists N such that

$$M_{N+r} = \mathfrak{a}^r M_N$$

Then $\mathrm{G}(M)$ is generated by

$$\bigoplus_{n \leq N} \frac{M_n}{M_{n+1}}$$

as a $\mathrm{G}_{\mathfrak{a}}(R)$-module. But each M_n/M_{n+1} is a Noetherian R-module, annihilated by $\mathfrak{a}$. In particular, each M_n/M_{n+1} is a finitely generated $R/\mathfrak{a}$-module. So

$$\bigoplus_{n \leq N} \frac{M_n}{M_{n+1}}$$

is a finitely genertaed $R/\mathfrak{a}$-module, and so it is a finitely generated $\mathrm{G}_{\mathfrak{a}}(R)$-module. □

10.3 Filtrations

Definition 10.3.1 (equivalent)
Let M be an R-module. Then filtrations $(M_n), (M'_n)$ of M are *equivalent* if there exists n_0 such that

$$M_{n+n_0} \subseteq M'_n \quad \text{and} \quad M'_{n+n_0} \subseteq M_n$$

for all $n \geq 0$.

Lecture 22

Lemma 10.3.2. Let $\mathfrak{a} \trianglelefteq R$ be an ideal, M an R-module, (M_n) is a stable $\mathfrak{a}$-filtration on M. Then (M_n) is equivalent to $(\mathfrak{a}^n M)$.

Proof. We have that

$$M_n \supseteq \mathfrak{a}M_{n-1} \supseteq \cdots \supseteq \mathfrak{a}^n M \supseteq \mathfrak{a}^{n+n_0} M$$

for all $n_0 \geq 0$. In the other direction, there exist $n_0 \geq 0$ such that $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$. Hence

$$M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subseteq \mathfrak{a}^n M$$

□

Let $\mathfrak{a} \trianglelefteq R$ be an ideal, M an R-module, (M_n) an $\mathfrak{a}$-filtration of M. Let

$$R^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$$

and

$$M^* = \bigoplus_{n=0}^{\infty} M_n$$

Then R^* is a graded ring, and M^* is a graded R^*-module with the natural actions.

If R is Noetherian, then $\mathfrak{a} = \langle x_1, \ldots, x_r \rangle$, and R^* is generated as an R-algebra by

$$x_1, \ldots, x_n \in \mathfrak{a}$$

Hence by the Hilbert basis theorem, R^* is Noetherian.

Lemma 10.3.3. Let R be a Noetherian ring, M a finitely generated R-module, (M_n) an $\mathfrak{a}$-filtration. Then M^* is a finitely generated R^*-module if and only if the $\mathfrak{a}$-filtration (M_n) is stable.

Proof. First of all, note that

1. Each (M_n) is a finitely generated R-module. Since R is Noetherian, and M is finitely generated, M is Noetherian, and so every submodule is finitely generated.

2. Consider the submodule
$$M_n^* = M_0 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots$$
of M^*, then the ascending chain (M_n^*) stabilises, if and only if (M_n) is a stable $\mathfrak{a}$-filtration.

Suppose M^* is finitely generated. We know that R is Noetherian, and so R^* is Noetherian, and therefore, M^* is Noetherian. But then the ascending chain (M_n^*) stabilises, and so (M_n) is a stable $\mathfrak{a}$-filtration by 2.

Now suppose the filtration (M_n) is stable. Then the sequence (M_n^*) stabilises at some n_0. Now note that

$$M^* = \bigcup_n M_n^*$$

Hence $M^* = M^*_{n_0}$. But we know that

$$M_0 \oplus \cdots \oplus M_{n_0}$$

generates M^*_n as an R^*-module. But each M_n is a finitely generated R-module, and so $M_0 \oplus \cdots \oplus M_{n_0}$ is a finitely generated R-module. Thus, M^*_n is a finitely generated R^*-module. □

Proposition 10.3.4 (Artin-Rees)**.** Let R be a Noetherian ring, $\mathfrak{a} \trianglelefteq R$ an ideal, M a finitely generated R-module, (M_ℓ) a stable $\mathfrak{a}$-filtration of M, and $N \subseteq M$ a submodule.

Then $(N \cap M_\ell)$ is a stable $\mathfrak{a}$-filtration of N.

Proof. First of all,

$$\mathfrak{a}(N \cap M_\ell) \subseteq N \cap \mathfrak{a}M_\ell \subseteq N \cap M_{\ell+1}$$

and so $(N \cap M_\ell)$ is an $\mathfrak{a}$-filtration. Define

$$N^* = \bigoplus_{\ell=0}^{\infty}(N \cap M_\ell)$$

This is an R^*-submodule of M^*. Recall R is Noetherian, and so R^* is Noetherian. Since (M_ℓ) is stable, M^* is finitely generated, and so M^* is a Noetherian R^*-module. Hence N^* is a finitely generated R^*-module, and so $(N \cap M_\ell)$ is stable. □

11 Dimension theory

Definition 11.0.1 (height)

Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be a prime. Then the *height* of $\mathfrak{p}$ is

$$\mathrm{ht}(\mathfrak{p}) = \sup\{d \mid \mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{p}\}$$

Geometrically, irreducible closed subsets of $\mathrm{Spec}(R)$ are precisely $\mathbb{V}(\mathfrak{p})$ for a prime ideal $\mathfrak{p}$> Thus, if we take $\mathbb{V}$ in the definition of height, we instead obtain

$$Z_0 \supsetneq \cdots \supseteq Z_d = \mathbb{V}(\mathfrak{p})$$

which matches the definition of dimension.

Definition 11.0.2 ((Krull) dimension)

The *(Krull) dimension of a ring* is

$$\dim(R) = \sup\{\mathrm{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \mathrm{Spec}(R)\} = \sup\{\mathrm{ht}(\mathfrak{m}) \mid \mathfrak{m} \in \mathrm{maxSpec}(R)\}$$

Using the above, we can see that the dimension of R makes sense geometrically.

We can see that $\dim(R_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$, and so

$$\dim(R) = \sup\{\dim(R_\mathfrak{m}) \mid \mathfrak{m} \in \mathrm{maxSpec}(R)\}$$

Definition 11.0.3

For an ideal I of R,

$$\mathrm{ht}(I) = \inf\{\mathrm{ht}(\mathfrak{p}) \mid I \subseteq \mathfrak{p} \in \mathrm{Spec}(R)\}$$

Proposition 11.0.4. If $A \subseteq B$ is an integral extension of rings, then

(i) $\dim(A) = \dim(B)$,

(ii) if A, B are integral domains and k-algebras, where k is a field, then $\operatorname{trdeg}_k(A) = \operatorname{trdeg}_k(B)$.

Proof. First, we show that $\dim(A) \leq \dim(B)$. Given a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d$$

By lying over and going up, we have

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_d$$

with $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, and so $\mathfrak{q}_i \neq \mathfrak{q}_{i+1}$. Thus, $\dim(A) \leq \dim(B)$.

Next, we show $\dim(A) \geq \dim(B)$. Let

$$\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_d$$

be a chain in $\operatorname{Spec}(B)$, then

$$\mathfrak{q}_0 \cap A \subsetneq \cdots \subsetneq \mathfrak{q}_d \cap A$$

is a chain in $\operatorname{Spec}(A)$. By incomparability, $\mathfrak{q}_i \cap A \neq \mathfrak{q}_{i+1} \cap A$, and so $\dim(A) \geq \dim(B)$.

(ii) is left as an exercise. □

Now if k is a field, A a finitely generated k-algebra, then by the Noether normalisation theorem, we had a k-algebra embedding

$$k[T_!, \dots, T_d] \hookrightarrow A$$

which is an integral extension. Hence by the proposition,

$$\dim(A) = \dim(k[T_1, \dots, T_d]) = d$$

by examples sheet 3 question 10.

Lecture 23

11.1 Hilbert polynomials and functions

Let A be a Noetherian graded ring. That is, A_0 is Noetherian and A is a finitely generated A_0-algebra. Let M be a finitely generated graded A-module. Then each M_n is an A_0-module.

Claim 11.1.1. M_n is a finitely generated A_0-module.

Proof. Say $M = \operatorname{span}_A\{m_1, \dots, m_t\}$, each $m_i \in M_{r_i}$ homogeneous. Therefore,

$$M_n = \{a_1 m_1 + \cdots + a_t m_t \mid a_i \in A_{n-r_i}\}$$

We have that $A = A_0[x_1, \dots, x_s]$, each $x_i \in A_{k_i}$, $k_i > 0$. Then

$$M_n = \operatorname{span}_{A_0}\left\{x_1^{e_1} \cdots x_s^{e_s} m_i \;\middle|\; e_i \geq 0, \sum k_i e_i = n - r_i\right\}$$

□

Now we will assume in addition that A_0 is also Artinian. Therefore, each M_n is an Artinian and Noetherian module. Hence $\ell(M_n) < \infty$[2].

Definition 11.1.2 (Poincaré series)
Let A, M be as above. The *Poincaré series* of M is

$$P(M, T) = \sum_{n=0}^{\infty} \ell(M_n) T^n \in \mathbb{Z}[\![T]\!]$$

[2]That is, it has finite length. Equivalently, it has a composition series of finite length.

Theorem 11.1.3 (Hilbert-Serre)**.** $P(M,T)$ is a rational function of the form

$$\frac{f(T)}{\prod_{i=1}^{s}(1-T^{k_i})}$$

for $f \in \mathbb{Z}[T]$, s, k_i as above.

Proof. For the base case, $s = 0$, then $A = A_0$, and so $M = \operatorname{span}_{A_0} S$, where S is a finite set. Hence it must belong to a finite direct sum, and so $M_n = 0$ for $n > n_0$. Thus, $P(M,T)$ is a polynomial.

Now write

$$M = \bigoplus_{n\in\mathbb{Z}} M_n$$

where $M_\ell = 0$ for $\ell < 0$. We have an exact sequence of the form

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{m\mapsto x_s m} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0$$

where K_n, L_{n+k_s} are the kernel and cokernel respectively. Set

$$K = \bigoplus_n K_n$$

$$L = \bigoplus_n L_n$$

These are graded A-modules[3]. Now note that K, L are annihilated by x_s,

Apply ℓ to the exact sequence, we get

$$\ell(K_n) - \ell(M_n) + \ell(M_{n+k_s}) - \ell(L_{n+k_s}) = 0$$

since ℓ is additive. Hence

$$\ell(K_n)T^{n+k_s} - \ell(M_n)T^{n+k_s} + \ell(M_{n+k_s})T^{n+k_s} - \ell(L_{n+k_s})^{n+k_s} = 0$$

Rearranging,

$$\ell(M_{n+k_s})T^{n+k_s} - T^{k_s}\ell(M_n)T^n = \ell(L_{n+k_s})T^{n+k_s} - T^{k_s}\ell(K_n)T^n$$

Summing this over the integers, we get

$$(1-T^{k_s})P(M,T) = P(M,T) - T^{k_s}P(M,T) = P(L,T) - T^{k_s}P(K,T)$$

But we can write the right hand side as

$$\frac{f_1}{\prod_{i=1}^{s-1}(1-T^{k_i})} - \frac{T^{k_s}f_2}{\prod_{i=1}^{s-1}(1-T^{k_i})}$$

by induction. Rearranging gives the result. □

Let $d(M)$ be the order of the pole of $P(M,T)$ at $t = 1$. Then if $M \neq 0$, $d \geq 0$. See notes for details.

Example 11.1.4

Let $A = k[T_1, \ldots, T_s]$, A_n the homogeneous parts. Then

1. A is generated as an $A_0 = k$-algebra by $T_1, \ldots, T_s$. In each case, $k_i = 1$.
2. $\ell(A_n) = \dim_k(A_n) = \binom{n+s-1}{s}$, which is a polynomial of degree $s-1$ in n over $\mathbb{Q}$. In this case,
3. $$P(A,T) = \sum \binom{n+s-1}{n} T^n = \frac{1}{(1-T)^s}$$

[3] If we defined homomorphisms of graded modules, then K, L are the kernel and cokernel respectively.

Proposition 11.1.5. If $k_1 = \cdots = k_s = 1$, then there exists a polynomial $\mathrm{HP}_M \in \mathbb{Q}[T]$, and $n_0 \geq 1$, such that

$$\ell(M_n) = \mathrm{HP}_M(n)$$

for all $n \geq N_0$. Moreover,

$$\deg(\mathrm{HP}_M) = d(M) - 1$$

This is called the *Hilbert polynomial*.

Proof. Let $d = d(M) \geq 0$. Then we can write

$$\sum_{n\geq 0} \ell(M_n)T^n = \frac{f(T)}{(1-T)^d}$$

where $f \in \mathbb{Z}[T]$, with $f(1) \neq 0$. Write

$$f = \sum_{k=0}^{\deg(f)} a_k T^k$$

for $a_k \in \mathbb{Z}$. Next,

$$\frac{1}{(1-T)^d} = \sum_{j=0}^{\infty} b_j T^j$$

where $b_j = \binom{j+d-1}{j}$. Then

$$\ell(M_n) = \sum_{i=0}^{\deg(f)} a_{n-i} b_i$$

for $n \geq \deg(f)$. Since $a_i \in \mathbb{Z}$, b_j is a polynomial in j over $\mathbb{Q}$ of degree $d-1$. Moreover, the leading coefficient of b_i is

$$\frac{1}{(d-1)!}$$

Hence $\ell(M_n) = p(n)$, where $p \in \mathbb{Q}[T]$. All we need to show is that $\deg(p) = d-1$. The coefficient of T^{d-1} in p is

$$\sum_{i=0}^{\deg(f)} a_i \frac{1}{(d-1)!} = \frac{f(1)}{(d-1)!}$$

which is non-zero, as $f(1) \neq 0$ by assumption. □

11.2 Dimension of local Noetherian rings

Lemma 11.2.1. Let $(A, \mathfrak{m})$ be a Noetherian local ring, then

(i) an ideal $\mathfrak{q}$ of A is $\mathfrak{m}$-primary if and only if there exists $t \geq 1$ such that $\mathfrak{m}^t \subseteq \mathfrak{q} \subseteq \mathfrak{m}$.

(ii) If $\mathfrak{q}$ is $\mathfrak{m}$-primary, then $A/\mathfrak{q}$ is Artinian.

Lecture 24

Proof. See notes. □

Theorem 11.2.2 (dimension)**.** If $(A, \mathfrak{m})$ is a Noetherian local ring, then

$$\dim(A) = \delta(A) = d(G_{\mathfrak{m}}(A))$$

where

$$\delta(A) = \min\{\delta(\mathfrak{q}) \mid \mathfrak{q} \subseteq A \ \mathfrak{m}\text{-primary}\}$$
$$\delta(\mathfrak{q}) = \text{minimal number of generators for } \mathfrak{q}$$

and $d(G_{\mathfrak{m}}(A))$ is the order of the pole at $T = 1$ of the rational function associated to the Poincaré series of $G_{\mathfrak{m}}(A)$. That is, the order of the pole at 1 of

$$\sum_{n\geq 0} \ell\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) T^n$$

Corollary 11.2.3 (Krull's height theorem)**.** Let A be a Noetherian ring, $\mathfrak{a} = (x_1, \ldots, x_r) \subseteq A$ an ideal. Let $\mathfrak{a} \leq \mathfrak{p}$ be a minimal prime of $\mathfrak{a}$. Then

$$\operatorname{ht}(\mathfrak{p}) \leq r$$

Proof. First of all, we claim that

$$\sqrt{\mathfrak{a}A_{\mathfrak{p}}} = \mathfrak{p}A_{\mathfrak{p}}$$

To see this, let $\mathfrak{n} \in \operatorname{Spec}(A)$ be such that $\mathfrak{a}A_{\mathfrak{p}} \subseteq \mathfrak{n}$, then

$$\mathfrak{a} \subseteq (\mathfrak{a}A_{\mathfrak{p}})^c \subseteq \mathfrak{n}^c \subseteq \mathfrak{p}$$

Then by minimality, $\mathfrak{n}^c = \mathfrak{p}$. Hence $\mathfrak{n}^{ce} = \mathfrak{p}^e$, and the result follows. Thus, $\mathfrak{a}A_{\mathfrak{p}}$ is $\mathfrak{p}A_{\mathfrak{p}}$-primary. On the other hand,

$$\mathfrak{a}A_{\mathfrak{p}} = \left\langle \frac{x_1}{1}, \ldots, \frac{x_r}{1} \right\rangle$$

Then

$$\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}}) = \delta(A_{\mathfrak{p}}) \leq \delta(\mathfrak{a}A_{\mathfrak{p}}) \leq r$$

□

Geometrically, the height of $\mathfrak{p}$ should be interpreted as the *co*domension of $\mathbb{V}(\mathfrak{p})$ in $\operatorname{Spec}(A)$. Therefore, if $\mathfrak{a}$ is generated by r elements, we are imposing r-equations, and so the codimension should be at most r.

Let $(A, \mathfrak{m})$ be a Noetherian local ring, $\mathfrak{q} \trianglelefteq A$ an $\mathfrak{m}$-primary ideal. Say $\delta(\mathfrak{q}) = s$, and $\mathfrak{q} = \langle x_1, \ldots, x_s \rangle$. Then

$$G_{\mathfrak{q}}(A) = \frac{A}{\mathfrak{q}} \oplus \frac{\mathfrak{q}}{\mathfrak{q}^2} \oplus \bigoplus_{n\geq 2} \frac{\mathfrak{q}^n}{\mathfrak{q}^{n+1}}$$

In this case, $A/\mathfrak{q}$ is Artinian, and the images of $x_1, \ldots, x_s$ generate $\mathfrak{q}/\mathfrak{q}^2$ as an $A/\mathfrak{q}$ algebra, the x_i are of degree 1. Here, we have that

$$\ell\left(\frac{\mathfrak{q}^n}{\mathfrak{q}^{n+1}}\right) < \infty$$

From the Hilbert polynomial, $\ell\left(\frac{\mathfrak{q}^n}{\mathfrak{q}^{n+1}}\right)$ is eventually a polynomial, of degree $\leq s - 1 = \delta(\mathfrak{q}) - 1$.

Fix $\mathfrak{q}_0 \subseteq A$ $\mathfrak{m}$-primary, with $\delta(\mathfrak{q}_0) = \delta(A)$. With this, we have two special cases. We will write $\deg(\ell(\mathfrak{q}^n/\mathfrak{q}^{n+1}))$ for the degree of the corresponding Hilbert polynomial.

First of all,

$$\deg(\ell(\mathfrak{q}_0^n/\mathfrak{q}_0^{n+1})) \leq \delta(A) - 1$$

and

$$\deg(\ell(A/\mathfrak{q}_0^n)) = \sum_{i=0}^{n-1} \ell(\mathfrak{q}_0^i/\mathfrak{q}_0^{i+1}) \leq \delta(A)$$

Next,

$$\deg(\ell(\mathfrak{m}^n/\mathfrak{m}^{n+1})) = d(G_{\mathfrak{m}}(A)) - 1$$

and

$$\deg(\ell(A/\mathfrak{m}^n)) = d(G_{\mathfrak{m}}(A))$$

Moreover, there exists $t \geq 1$ such that

$$\mathfrak{m}^t \subseteq \mathfrak{q} \subseteq \mathfrak{m}$$

and so

$$\ell(A/\mathfrak{m}^n) \leq \ell(A/\mathfrak{q}_0^n) \leq \ell(A/\mathfrak{m}^{tn})$$

Thus, we must have that $\deg(\ell(A/\mathfrak{m}^n)) = \deg(\ell(A/\mathfrak{q}_0^n))$.

Proposition 11.2.4. $\delta(A) \geq d(\mathrm{G}_{\mathfrak{m}}(A))$

Proof.

$$\begin{aligned}\delta(A) &= \delta(\mathfrak{q}_0)\\ &\geq \deg(\ell(A/\mathfrak{q}_0^n))\\ &= \deg(\ell(A/\mathfrak{m}^n))\\ &= d(\mathrm{G}_{\mathfrak{m}}(A))\end{aligned}$$

□

Proposition 11.2.5. If $x \in \mathfrak{m}$ is not a zero divisor, then

$$d\left(\mathrm{G}_{\mathfrak{m}/xA}(A/xA)\right) \leq d(\mathrm{G}_{\mathfrak{m}}(A)) - 1$$

Proof. We know that $(A/xA, \mathfrak{m}/xA)$ is still a local ring. In this case,

$$d(\mathrm{G}_{\mathfrak{m}}(A)) = \deg(\ell(A/\mathfrak{m}^n))$$

and

$$d(\mathrm{G}_{\mathfrak{m}/xA}(A/xA)) = \deg(\ell((\mathfrak{m}^n + xA)/xA))$$

We want to show that

$$\deg(\ell(A/(\mathfrak{m} + xA))) \leq \deg(\ell(A/\mathfrak{m}^n)) - 1$$

We have a short exact sequence

$$0 \longrightarrow \frac{\mathfrak{m}^n + xA}{\mathfrak{m}^n} = \frac{xA}{\mathfrak{m}^n \cap xA} \longrightarrow \frac{A}{\mathfrak{m}^n} \longrightarrow \frac{A}{\mathfrak{m}^n + xA} \longrightarrow 0$$

Hence by additivity,

$$\ell(A/(\mathfrak{m}^n + xA)) = \ell(A/\mathfrak{m}^m) - \ell(xA/(\mathfrak{m}^n \cap xA))$$

We know the terms on the right hand side have the same degree, and so it suffices to show they have the same leading coefficient.

But $(\mathfrak{m}^n)$ is a stable $\mathfrak{m}$-filtration of A, and so by Artin-Rees, $(\mathfrak{m}^n \cap xA)$ is a stable $\mathfrak{m}$ filtration of xA. Hence this is equivalent to $(\mathfrak{m}^n xA)$. Hence we have that

$$\ell(xA/(\mathfrak{m}^n \cap xA)) \leq \ell(xA/\mathfrak{m}^{n+n_0} xA)$$

and

$$\ell(xA/\mathfrak{m}^n xA) \leq \ell(xA/(\mathfrak{m}^n \cap xA))$$

Thus, by elemenrary facts about polynomials, they ahev the same degree. □

Proposition 11.2.6.

$$d(\mathrm{G}_{\mathfrak{m}}(A)) \geq \dim(A)$$

Proof. See notes. □

Proposition 11.2.7. $\dim(A) \geq \delta(A)$. That is, there exists $\mathfrak{q} \trianglelefteq A$ $\mathfrak{m}$-primary, generated by $\dim(A)$ elements.

Proof. The height of $\mathfrak{m}$ is exactly $\dim(A)$. Thus, for any other prime $\mathfrak{p} \in \operatorname{Spec}(A)$, $\operatorname{ht}(\mathfrak{p}) < \dim(A)$. So what we want is to form an ideal $\mathfrak{q} = \langle x_1, \ldots, x_d \rangle$, with $\operatorname{ht}(\mathfrak{q}) = \dim(A)$, since then for any minimal prime containing $\mathfrak{q}$, we must have that the height of the prime is $\dim(A)$, and so $\sqrt{\mathfrak{q}} = \mathfrak{m}$, and so $\mathfrak{q}$ is $\mathfrak{m}$-primary.

We construct $\langle x_1, \ldots, x_d \rangle$ inductively, such that if

$$\mathfrak{q}_i = \langle x_1, \ldots, x_i \rangle$$

then

$$\operatorname{ht}(\mathfrak{q}_i) \geq i$$

For the base case $i = 0$, we can just use $\mathfrak{q}_0 = 0$. For the inductive step, assume $\mathfrak{q}_{i-1}$ has $\operatorname{ht}(\mathfrak{q}_i) \geq i - 1$. We claim that there are only finitely many $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ prime ideals, such that $\mathfrak{q}_{i-1} \subseteq \mathfrak{p}_j$, and $\operatorname{ht}(\mathfrak{p}_j) = i - 1$. If not, since $\operatorname{ht} \mathfrak{q}_{i-1} \geq i - 1$, each $\mathfrak{p}_j$ is a minimal prime of $\mathfrak{q}_i$. But in a Noetherian ring, every ideal has finitely many minimal primes.

Now $i - 1 < \dim(A) = \operatorname{ht}(\mathfrak{m})$, and so $\mathfrak{m}$ is not contained in $\mathfrak{p}_j$ for all j, and so $\mathfrak{m}$ is not contained in their union, by prime avoidance. So we can take $x_i \in \mathfrak{m}$, with $x_i \notin \mathfrak{p}_j$ for any j. Define

$$\mathfrak{q}_i = \langle x_1, \ldots, x_i \rangle$$

Then if $\mathfrak{p}$ is prime, which contains $\mathfrak{q}_i$, then it contains $\mathfrak{q}_{i-1}$ and x_i. Hence it cannot be any of the $\mathfrak{p}_j$ above. Thus, $\operatorname{ht}(\mathfrak{p}) \geq i$ as required. □

Index