

Commutative Algebra

Cambridge University Mathematical Tripos: Part III

12th June 2024

Contents

1	Chain conditions	3
1.1	Modules	3
1.2	Noetherian and Artinian modules	3
1.3	Exact sequences	5
1.4	Algebras	6
2	Tensor products	7
2.1	Introduction	7
2.2	Definition and universal property	7
2.3	Zero tensors	9
2.4	Monoidal structure	11
2.5	Tensor products of maps	16
2.6	Tensor products of algebras	17
2.7	Restriction and extension of scalars	19
2.8	Extension of scalars on morphisms	22
2.9	Extension of scalars in algebras	22
2.10	Exactness properties of the tensor product	23
2.11	Flat modules	26
3	Localisation	30
3.1	Definitions	30
3.2	Universal property for rings	32
3.3	Functoriality	33
3.4	Universal property for modules	34
3.5	Exactness	35
3.6	Extension and contraction of ideals	37
3.7	Local properties	39
3.8	Localisations as quotients	41
4	Integrality, finiteness, and finite generation	41
4.1	Nakayama's lemma	41
4.2	Integral and finite extensions	43
4.3	Integral closure	46
4.4	Noether normalisation	47
4.5	Hilbert's Nullstellensatz	49

4.6	Integrality over ideals	51
4.7	Cohen–Seidenberg theorems	53
5	Primary decomposition	56
6	Direct and inverse limits	58
6.1	Limits and completions	58
6.2	Graded rings and modules	60
6.3	Artin–Rees lemma	62
7	Dimension theory	63
7.1	???.	63
7.2	Hilbert polynomials	64
7.3	Dimension theory of local Noetherian rings	66

1 Chain conditions

1.1 Modules

In this course, a *ring* is taken to mean a commutative unital ring R . We do however allow for one noncommutative exception, the endomorphism ring $\text{End}(M)$ of an abelian group M . This is a ring where composition is the multiplication operation.

Definition. An R -module is an abelian group M with a fixed ring homomorphism $\rho : R \rightarrow \text{End}(M)$. If $r \in R$ and $m \in M$, we define $r \cdot m = \rho(r)(m)$.

Remark. Note that as $\rho(r)$ is a group homomorphism,

$$r(m_1 + m_2) = \rho(r)(m_1 + m_2) = \rho(r)(m_1) + \rho(r)(m_2) = r \cdot m_1 + r \cdot m_2$$

Also, as ρ is a ring homomorphism,

$$(r_1 + r_2)m = \rho(r_1 + r_2)(m) = (\rho(r_1) + \rho(r_2))m = r_1 \cdot m + r_2 \cdot m$$

Example. (i) Let k be a field. Then a k -module is a k -vector space.

(ii) Every abelian group M is a \mathbb{Z} -module in a unique way, because the morphism $\mathbb{Z} \rightarrow \text{End } M$ must map 1 to id.

(iii) Every ring R is an R -module, by taking $\rho(r) = r_0 \mapsto r_0 r$.

Definition. The *direct product* of abelian groups $(M_i)_{i \in I}$ is the set of I -tuples $(a_i)_{i \in I}$ where $a_i \in M_i$, with elementwise addition as the group operation.

Definition. The *direct sum* of abelian groups $(M_i)_{i \in I}$ is the set of I -tuples $(a_i)_{i \in I}$ where $a_i \in M_i$ and all but finitely many of the a_i are zero, again with elementwise addition as the group operation.

Direct products are written $\prod_{i \in I} M_i$, and direct sums are written $\bigoplus_{i \in I} M_i$. These constructions coincide if the index set I is finite. Direct products and direct sums of R -modules are also R -modules.

The universal property of the direct sum states that each collection of module homomorphisms $\varphi_i : M_i \rightarrow R$ can be combined into a unique homomorphism $\varphi : \bigoplus_{i \in I} M_i \rightarrow R$. Similarly, the universal property of the direct product states that each collection of module homomorphisms $\varphi_i : R \rightarrow M_i$ can be combined into a unique homomorphism $\varphi : R \rightarrow \prod_{i \in I} M_i$.

1.2 Noetherian and Artinian modules

Definition. An R -module M is *Noetherian* if one of the following conditions holds.

- (i) Every ascending chain of submodules $M_0 \subseteq M_1 \subseteq \dots$ inside M stabilises. That is, for some k , every $j \in \mathbb{N}$ has $M_{k+j} = M_k$.
- (ii) Every nonempty set Σ of submodules of M has a maximal element.

Lemma. The two conditions above are equivalent.

Proof. (i) implies (ii). Let Σ be a nonempty set of submodules of M . If it has no maximal element, then for each $M' \in \Sigma$ there exists $M'' \in \Sigma$ with $M' \subsetneq M''$. We can then use the axiom of choice to pick a sequence $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \dots$ of elements in Σ . This contradicts (i).

(ii) implies (i). Let $M_0 \subseteq M_1 \subseteq \dots$ be an ascending chain of submodules in M . Then let $\Sigma = \{M_0, M_1, \dots\}$. This has a maximal element M_k by (ii). Then for all $j \in \mathbb{N}$, $M_{k+j} = M_k$ as required. \square

Definition. M is *Artinian* if one of the following conditions holds.

- (i) Every descending chain of submodules $M_0 \supseteq M_1 \supseteq \dots$ inside M stabilises.
- (ii) Every nonempty set Σ of submodules of M has a minimal element.

Again, both conditions are equivalent.

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

Proof. Suppose M is Noetherian, and let $N \subseteq M$ be a submodule. Pick $m_1 \in N$, and consider the submodule $M_1 \subseteq N$ generated by m_1 . If $M_1 = N$, then we are done. Otherwise, pick $m_2 \in M_1 \setminus N$, and consider $M_2 \subseteq N$ generated by m_2 . This construction will always terminate, as if it did not, we would have constructed an infinite strictly ascending chain of submodules of M , contradicting that M is Noetherian.

Now suppose every submodule of M is finitely generated, and let $M_0 \subseteq M_1 \subseteq \dots$ be an ascending chain of submodules of M . Let $N = \bigcup_{i=0}^{\infty} M_i$; this is a submodule of M as the M_i form a chain. Then N is finitely generated, say, by generators $m_1, \dots, m_k \in N$. As the M_i form a chain increasing to N , there exists n such that $m_1, \dots, m_k \in M_n$. In particular, $N \subseteq M_n \subseteq N$, so $M_n = N$. Thus the chain stabilises. \square

Note that every Noetherian module is finitely generated. Let $R = \mathbb{Z}[T_1, T_2, \dots]$, and let $M = R$ as an R -module. M is generated by 1_R , so in particular it is finitely generated. But it has a \mathbb{Z} -submodule $\langle T_1, T_2, \dots \rangle$ that is not finitely generated. So in the above lemma we indeed must check every submodule.

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

Example. (i) \mathbb{Z} over itself is a Noetherian module as it is a principal ideal domain, but it is not an Artinian module because we can take the chain $(2) \supsetneq (4) \supsetneq (8) \supsetneq \dots$.

(ii) \mathbb{Z} is similarly a Noetherian ring but not an Artinian ring by unfolding the definition and using (i).

(iii) $\mathbb{Z}\left[\frac{1}{2}\right]_{/\mathbb{Z}}$ is an Artinian \mathbb{Z} -module but not a Noetherian \mathbb{Z} -module. This can be seen from the fact that the only submodules are of the form $\left(\frac{1}{2^k} + \mathbb{Z}\right)$ for $k \in \mathbb{N}$.

(iv) In fact, a ring R is Artinian if and only if R is Noetherian and R has *Krull dimension 0*.

1.3 Exact sequences

Definition. A sequence

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

is *exact* if the image of f_i is equal to the kernel of f_{i+1} for each i , where the M_i are modules and the f_i are module homomorphisms.

Definition. A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow M' \xrightarrow{\text{injective}} M \xrightarrow{\text{surjective}} M'' \longrightarrow 0$$

In this situation, $M'' \simeq M/i(M')$. This is a way to encode M'' as a quotient by a submodule.

Lemma. Let

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\varphi} L \longrightarrow 0$$

be a short exact sequence of R -modules. Then M is Noetherian (resp. Artinian) if and only if both N and L are Noetherian (resp. Artinian).

Proof. We show the statement for Noetherian modules.

Suppose M is Noetherian. If $N_0 \subseteq N_1 \subseteq \cdots$ is an ascending chain of submodules inside N , then by taking images,

$$\iota(N_0) \subseteq \iota(N_1) \subseteq \cdots$$

is also naturally an ascending chain of submodules inside M , so it stabilises. As ι is injective, the original sequence also stabilises. Hence N is Noetherian.

If $L_0 \subseteq L_1 \subseteq \cdots$ is an ascending chain of submodules inside L , then by taking preimages,

$$\varphi^{-1}(L_0) \subseteq \varphi^{-1}(L_1) \subseteq \cdots$$

is an ascending chain of submodules inside M , where

$$\varphi^{-1}(L_i) = \{m \in M \mid \varphi(m) \in L_i\}$$

So this chain stabilises at $\varphi^{-1}(L_k)$. But as φ is surjective, $\varphi(\varphi^{-1}(L_i)) = L_i$, so the original sequence must stabilise at L_k .

Now suppose N and L are Noetherian, and let $M_0 \subseteq M_1 \subseteq \cdots$ be an ascending chain of submodules in M . Then

$$\iota^{-1}(M_0) \subseteq \iota^{-1}(M_1) \subseteq \cdots$$

is an ascending chain of submodules in N , so stabilises at $\iota^{-1}(M_{k_N})$ for some k_N . Similarly,

$$\varphi(M_0) \subseteq \varphi(M_1) \subseteq \cdots$$

is an ascending chain of submodules in L , so stabilises at $\varphi^{-1}(M_{k_L})$ for some k_L . Take $k \geq k_N, k_L$, and let $j \geq 0$. We show $M_{k+j} \subseteq M_k$, proving that the sequence stabilises.

Let $m \in M_{k+j}$. As $\varphi(M_{k+j}) = \varphi(M_k)$, there exists $m' \in M_k$ such that $\varphi(m) = \varphi(m')$. Then $\varphi(m - m') = 0$, so by exactness, $m - m'$ is in the image of ι , say, $\iota(x) = m - m'$. Since $m - m' \in M_{k+j}$, we must have $x \in \iota^{-1}(M_{k+j})$. But then $x \in \iota^{-1}(M_k)$, so $\iota(x) = m - m' \in M_k$. Hence $m \in M_k$. \square

Corollary. If M_1, \dots, M_n are Noetherian (resp. Artinian) modules, then so is $M_1 \oplus \dots \oplus M_n$.

Proof. Consider the sequence

$$0 \longrightarrow M_1 \xrightarrow{\iota} M_1 \oplus M_2 \xrightarrow{\pi} M_2 \longrightarrow 0$$

where $\iota(x) = (x, 0)$ and $\pi(x, y) = y$. This is exact, so $M_1 \oplus M_2$ is Noetherian. We then proceed by induction on n . \square

Proposition. 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 is a surjective module homomorphism $\varphi : R^n \rightarrow M$ for some $n \geq 0$. That is, M is a quotient of R^n . The fact that R^n is Noetherian (or Artinian) passes through to its quotients. \square

1.4 Algebras

Definition. An R -algebra is a ring A together with a fixed ring homomorphism $\rho : R \rightarrow A$.

Example. The map $k \rightarrow k[T_1, \dots, T_n]$ makes the polynomial ring $k[T_1, \dots, T_n]$ a k -algebra.

We will write $ra = \rho(r)a$. Note that $\rho(r) = \rho(r) \cdot 1_A = r \cdot 1_A$, so we can write $r \cdot 1_A$ for $\rho(r)$.

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

Example. As a k -module, $k[T_1, \dots, T_n]$ is infinite-dimensional. As a k -algebra, $k[T_1, \dots, T_n]$ is generated by the n elements T_1, \dots, T_n .

Definition. $\varphi : A \rightarrow B$ is an R -algebra homomorphism if φ is a ring homomorphism and preserves all elements of R . That is, $\varphi(r \cdot 1_A) = r \cdot 1_B$.

An R -algebra A is finitely generated if and only if there is some $n \geq 0$ and a surjective algebra homomorphism $R[T_1, \dots, T_n] \rightarrow A$.

Theorem (Hilbert's basis theorem). Every finitely generated algebra A over a Noetherian ring R is Noetherian.

For example, the polynomial algebra over a field is Noetherian.

Proof. It suffices to prove this for a polynomial ring, as every finitely generated algebra is a quotient of a polynomial ring. It further suffices to prove this for a univariate polynomial ring $A = R[T]$ by induction. Let \mathfrak{a} be an ideal of $R[T]$; we need to show that \mathfrak{a} is finitely generated. For each $i \geq 0$, define

$$\mathfrak{a}(i) = \{c_0 \mid c_0 T^i + \dots + c_i T^0 \in \mathfrak{a}\}$$

Thus $\mathfrak{a}(i)$ is the set of leading coefficients of polynomials of degree i that lie in \mathfrak{a} . Each $\mathfrak{a}(i)$ is an ideal in R , and $\mathfrak{a}(i) \subseteq \mathfrak{a}(i+1)$ by multiplying by T . As R is Noetherian, each $\mathfrak{a}(i)$ is a finitely generated ideal, and this ascending chain stabilises at $\mathfrak{a}(m)$, say. Let

$$\mathfrak{a}(i) = (b_{i,1}, \dots, b_{i,n_i})$$

We can choose $f_{i,j}$ of degree i with leading coefficient $b_{i,j}$. Define the ideal

$$\mathfrak{b} = (f_{i,j})_{i \leq m, j \leq n_i}$$

Note that \mathfrak{b} is finitely generated. Defining $\mathfrak{b}(i)$ in the same way as $\mathfrak{a}(i)$, we have

$$\forall i, \mathfrak{a}(i) = \mathfrak{b}(i)$$

By construction, $\mathfrak{b} \subseteq \mathfrak{a}$; we claim that the reverse inclusion holds, then the proof will be complete. Suppose that $\mathfrak{a} \not\subseteq \mathfrak{b}$, and take $f \in \mathfrak{a} \setminus \mathfrak{b}$ of minimal degree i . As $\mathfrak{a}(i) = \mathfrak{b}(i)$, there is a polynomial g in \mathfrak{b} of degree i that has the same leading coefficient. Then $f - g$ has degree less than i , and lies in \mathfrak{a} . But then by minimality, $f - g \in \mathfrak{b}$, giving $f \in \mathfrak{b}$. \square

Therefore, if $S \subseteq R[T_1, \dots, T_n]_I$ where R is Noetherian, then $(S) = (S_0)$ where $S_0 \subseteq S$ is finite.

2 Tensor products

2.1 Introduction

Let M and N be R -modules. Informally, the tensor product of M and N over R is the set $M \otimes_R N$ of all sums

$$\sum_{i=1}^{\ell} m_i \otimes n_i; \quad m_i \in M, n_i \in N$$

subject to the relations

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

This is a module that abstracts the notion of bilinearity between two modules.

Example. Consider $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$. In this \mathbb{Z} -module,

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

Hence $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z} = 0$.

Example. Now consider $\mathbb{R}^n \otimes_{\mathbb{R}} \mathbb{R}^{\ell}$. We will show later that this is isomorphic to $\mathbb{R}^{n\ell}$.

2.2 Definition and universal property

Definition. A map of R -modules $f : M \times N \rightarrow L$ is R -bilinear if for each $m_0 \in M$ and $n_0 \in N$, the maps $n \mapsto f(m_0, n)$ and $m \mapsto f(m, n_0)$ are R -linear (or equivalently, a homomorphism of R -modules).

Definition. Let M, N be R -modules. Let $\mathcal{F} = R^{\oplus(M \times N)}$ be the free R -module with coordinates indexed by $M \times N$. Define $K \subseteq \mathcal{F}$ to be the submodule generated by the following set of relations:

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

The tensor product $M \otimes_R N$ is \mathcal{F}/K . We further define the R -bilinear map

$$i_{M \otimes N} : M \times N \rightarrow M \otimes N; \quad i_{M \otimes N}(m, n) = e_{(m,n)} = m \otimes n$$

Proposition (universal property of the tensor product). The pair $(M \otimes_R N, i_{M \otimes R N})$ satisfies the following universal property. For every R -module L and every R -bilinear map $f : M \times N \rightarrow L$, there exists a unique homomorphism $h : M \otimes_R N \rightarrow L$ such that the following diagram commutes.

$$\begin{array}{ccc} M \times N & \xrightarrow{i_{M \otimes R N}} & M \otimes_R N \\ & \searrow f & \downarrow h \\ & & L \end{array}$$

Equivalently, $h \circ i_{M \otimes R N} = f$.

Proof. The conclusion $h \circ i_{M \otimes R N} = f$ holds if and only if for all m, n , we have

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

Note that the elements $\{m \otimes n\}$ generate $M \otimes N$ as an R -module, so there is at most one h . We now show that the definition of h on the pure tensors $m \otimes n$ extends to an R -linear map $M \otimes N \rightarrow L$. The map $R^{\oplus(M \times N)} \rightarrow L$ given by $(m, n) \mapsto f(m, n)$ exists by the universal property of the direct sum. However, this map vanishes on the generators of K , so it factors through the quotient \mathcal{F}/K as required. \square

The universal property given above characterises the tensor product up to isomorphism.

Proposition. Let M, N be R -modules, and (T, j) be an R -module and an R -bilinear map $M \times N \rightarrow T$. Suppose that (T, j) satisfies the same universal property as $M \otimes N$. Then there is a unique isomorphism of R -modules $\varphi : M \otimes N \xrightarrow{\sim} T$ such that $\varphi \circ i_{M \otimes N} = j$.

Proof. By using the universal property of $M \otimes N$ and T , we obtain φ and ψ as follows.

$$\begin{array}{ccc}
 M \otimes N & \xleftarrow{\varphi} & T \\
 & \psi & \\
 & \swarrow & \searrow \\
 & M \times N & \\
 & \nwarrow & \nearrow \\
 & i_{M \otimes N} & \\
 & & j
 \end{array}$$

The universal property states that $\varphi \circ i_{M \otimes N} = j$ and $\psi \circ j = i_{M \otimes N}$. Hence, $\psi \circ \varphi \circ i_{M \otimes N} = i_{M \otimes N}$. This means that the following diagram commutes.

$$\begin{array}{ccc}
 M \times N & \xrightarrow{i_{M \otimes N}} & M \otimes N \\
 & \searrow i_{M \otimes N} & \downarrow \text{id} \\
 & & M \otimes N
 \end{array}
 \quad
 \begin{array}{ccc}
 & & \downarrow \psi \circ \varphi \\
 & & M \otimes N
 \end{array}$$

By the uniqueness condition of the universal property, $\text{id} = \psi \circ \varphi$. Similarly, $\text{id} = \varphi \circ \psi$. Hence, φ is an isomorphism $M \otimes N \rightarrow T$ with $\varphi \circ i_{M \otimes N} = j$. Uniqueness of φ is guaranteed by the universal property: it is the only solution to $\varphi \circ i_{M \otimes N} = j$. \square

In particular, we have

$$\text{Bilin}_R(M \times N, L) \simeq \text{Hom}(M \otimes_R N, L)$$

given by the universal property, and the inverse is given by $h \mapsto h \circ i_{M \otimes N}$.

2.3 Zero tensors

Proposition. Let M, N be R -modules. Then

$$\sum m_i \otimes n_i = 0$$

if and only if for every R -module L and every R -bilinear map $f : M \times N \rightarrow L$, we have

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

To show an element of $M \otimes N$ is nonzero, it suffices to find a single R -module L and bilinear map $M \times N \rightarrow L$ with mapping the required sum to a nonzero value.

Proof. Assume $\sum m_i \otimes n_i = 0$. f factors through the map $i_{M \otimes N}$, giving

$$\begin{array}{ccc}
 M \times N & \xrightarrow{i_{M \otimes N}} & M \otimes N \\
 & \searrow f & \downarrow h \\
 & & L
 \end{array}$$

So

$$\sum f(m_i, n_i) = \sum h(i_{M \otimes N}(m_i, n_i)) = h\left(\sum i_{M \otimes N}(m_i, n_i)\right) = h(0) = 0$$

In the other direction, suppose $\sum m_i \otimes n_i \neq 0$. Then, taking $f = i_{M \otimes N}$, we obtain $\sum i_{M \otimes N}(m_i, n_i) \neq 0$ as required. \square

Example. Let k be a field, and consider $k^m \otimes k^\ell$. Let k^m have basis $\{e_1, \dots, e_m\}$ and k^ℓ have basis f_1, \dots, f_ℓ . Then

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

This is in fact a basis. Suppose $\sum_{i,j} \alpha_{i,j} e_i \otimes f_j = 0$. For each $a \leq m, b \leq \ell$, define $T_{a,b} : k^m \times k^\ell \rightarrow k$ by

$$T_{a,b}((v_i)_{i=1}^m, (w_j)_{j=1}^\ell) = v_a w_b$$

By the above proposition,

$$0 = \sum_{i,j} \alpha_{i,j} T_{a,b}(e_i, f_j) = \alpha_{a,b}$$

So $k^m \otimes k^\ell \simeq k^{m\ell}$. Note that this construction only relied on the existence of a free basis, not on k being a field.

Example. Consider $\mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2$. There are infinitely many pure tensors, but there is a basis consisting of the four pure vectors

$$e_1 \otimes f_1; \quad e_1 \otimes f_2; \quad e_2 \otimes f_1; \quad e_2 \otimes f_2$$

A pure tensor in $\mathbb{R}^2 \otimes_{\mathbb{R}} \mathbb{R}^2$ is of the form

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

which expands to

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

Note that there is a linear dependence relation between the coefficients $\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta$, so in some sense ‘most’ tensors are not pure. For example,

$$1(e_1 \otimes f_1) + 2(e_1 \otimes f_2) + 3(e_2 \otimes f_1) + 4(e_2 \otimes f_2)$$

is not pure.

Example. Consider $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. In this module,

$$2 \otimes (1 + 2\mathbb{Z}) = 1 \otimes (2 + 2\mathbb{Z}) = 1 \otimes 0 = 0$$

Note that \mathbb{Z} has a \mathbb{Z} -submodule $2\mathbb{Z}$. In $2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, the element also denoted with $2 \otimes (1 + 2\mathbb{Z})$ is nonzero. For example, we can define a bilinear map to $\mathbb{Z}/2\mathbb{Z}$ given by

$$b(2n, x + 2\mathbb{Z}) = nx + 2\mathbb{Z}$$

Then $b(2, 1 + 2\mathbb{Z}) = 1 \neq 0$. So it is not the case that tensor products of submodules are submodules of tensor products.

However, if $M' \subseteq M$ and $N' \subseteq N$ and $\sum m_i \otimes n_i = 0$ in $M' \otimes N'$, then $\sum m_i \otimes n_i = 0$ in $M \otimes N$.

Proposition. If $\sum m_i \otimes n_i = 0$ in $M \otimes_R N$, then there are finitely generated R -submodules $M' \subseteq M$ and $N' \subseteq N$ such that the expression $\sum m_i \otimes n_i$ also evaluates to zero in $M' \otimes_R N'$.

This is the last proof that will use the direct construction of the tensor product instead of the universal property directly.

Proof. We know that $\sum m_i \otimes n_i = 0$ in $M \otimes_R N = R^{\oplus(M \times N)} / K$, so in particular $\sum e_{(m_i, n_i)} \in K$, where e_x maps $x \in M \times N$ to its basis element in $R^{\oplus(M \times N)}$. So this is a finite sum of $\alpha_i k_i$ with $\alpha_i \in R, k_i \in K$, and so we can take the m'_1, \dots, m'_a that appear on the left-hand sides of the k_i as the generators for M' , and similarly for N' . \square

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

Proof. Suppose $n(\sum a_i \otimes b_i) = 0$ with $n \geq 1$. By the previous proposition, there are finitely generated subgroups $A' \leq A$ and $B' \leq B$ such that $n(\sum a_i \otimes b_i) = 0$ in $A' \otimes_{\mathbb{Z}} B'$. But as A' and B' are finitely generated abelian groups, the structure theorem shows that $A' = \mathbb{Z}^m$ and $B' = \mathbb{Z}^\ell$, showing that $A' \otimes_{\mathbb{Z}} B' \simeq \mathbb{Z}^{m\ell}$ is torsion-free. Thus $\sum a_i \otimes b_i = 0$ in $A' \otimes_{\mathbb{Z}} B'$, so also $\sum a_i \otimes b_i = 0$ in $A \otimes_{\mathbb{Z}} B$. \square

Example.

$$\mathbb{C}^2 \otimes_{\mathbb{C}} \mathbb{C}^3 \simeq \mathbb{C}^6 \simeq \mathbb{R}^{12}$$

However,

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

This is to be expected: tensoring over a larger ring introduces more relations, so the amount of distinguishable elements should shrink.

2.4 Monoidal structure

We will prove a number of elementary propositions in detail to show how tensor products are used in practice.

Proposition (commutativity). There is an isomorphism $M \otimes N \simeq N \otimes M$ mapping a pure tensor $m \otimes n$ to $n \otimes m$.

Proof. Define $f : M \times N \rightarrow N \otimes M$ by $f(m, n) = n \otimes m$; this is bilinear. The universal property yields

$$\begin{array}{ccc} M \times N & \xrightarrow{i_{M \otimes N}} & M \otimes N \\ & \searrow f & \downarrow h \\ & & N \otimes M \end{array}$$

such that $h(m \otimes n) = n \otimes m$. Similarly, we obtain $h' : N \otimes M \rightarrow M \otimes N$ with $h'(n \otimes m) = m \otimes n$. Hence, the following diagram commutes.

$$\begin{array}{ccc} M \times N & \xrightarrow{i_{M \otimes N}} & M \otimes N \\ & \searrow i_{M \otimes N} & \downarrow \text{id} \\ & & M \otimes N \end{array} \quad \begin{array}{ccc} & & \downarrow h' \circ h \\ & & M \otimes N \end{array}$$

So by the uniqueness condition in the universal property, $h' \circ h$ is the identity. Similarly, $h \circ h'$ is the identity, thus h is an isomorphism. \square

Proposition (associativity). There is an isomorphism $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P)$ mapping $(m \otimes n) \otimes p$ to $m \otimes (n \otimes p)$.

Proof. For each $p \in P$, define the bilinear map $f_p : M \times N \rightarrow M \otimes (N \otimes P)$ by

$$f_p(m, n) = m \otimes (n \otimes p)$$

Thus, each f_p factors through $h_p : M \otimes N \rightarrow M \otimes (N \otimes P)$. Then, define the bilinear map $f : (M \otimes N) \times P \rightarrow M \otimes (N \otimes P)$ by

$$f(x, p) = h_p(x)$$

We show this is bilinear in p . Note that

$$\begin{aligned} h_{p_1+p_2}(m \otimes n) &= f_{p_1+p_2}(m, n) \\ &= m \otimes (n \otimes (p_1 + p_2)) \\ &= m \otimes (n \otimes p_1) + m \otimes (n \otimes p_2) \\ &= f_{p_1}(m, n) + f_{p_2}(m, n) \\ &= h_{p_1}(m \otimes n) + h_{p_2}(m \otimes n) \end{aligned}$$

So $h_{p_1+p_2}$ coincides with $h_{p_1} + h_{p_2}$ on the pure tensors, so by the universal property they coincide everywhere. Similarly,

$$\begin{aligned} h_{rp}(m \otimes n) &= f_{rp}(m, n) \\ &= m \otimes (n \otimes rp) \\ &= r(m \otimes (n \otimes p)) \\ &= rf_p(m, n) \\ &= rh_p(m \otimes n) \end{aligned}$$

so $h_{rp} = rh_p$. Then, by the universal property, f factors through $h : (M \otimes N) \otimes P \rightarrow M \otimes (N \otimes P)$, so

$$h((m \otimes n) \otimes p) = m \otimes (n \otimes p)$$

We can similarly construct $h' : M \otimes (N \otimes P) \rightarrow (M \otimes N) \otimes P$ with

$$h'(m \otimes (n \otimes p)) = (m \otimes n) \otimes p$$

Since $h \circ h'$ and $h' \circ h$ are the identity on pure vectors, they are the identity everywhere, and hence are inverse isomorphisms. \square

Proposition (identity). There is an isomorphism $R \otimes M \simeq M$ mapping $r \otimes m$ to rm .

Proof. The map $f : R \times M \rightarrow M$ given by $f(r, m) = rm$ factors through some $h : R \otimes M \rightarrow M$.

$$\begin{array}{ccc} R \times M & \xrightarrow{i_{R \otimes M}} & R \otimes M \\ & \searrow f & \downarrow h \\ & & M \end{array}$$

Now define the R -module homomorphism $h' : M \rightarrow R \otimes M$ by $h'(m) = 1 \otimes m = i_{R \otimes M}(1, m)$. Then

$$(h \circ h')(m) = h(i_{R \otimes M}(1, m)) = f(1, m) = m$$

giving $h \circ h' = \text{id}$. Further,

$$(h' \circ h)(r \otimes m) = 1 \otimes h(r \otimes m) = 1 \otimes f(r, m) = 1 \otimes rm = r \otimes m$$

So by the uniqueness condition in the universal property, $h' \circ h$ is the identity, and hence h is an isomorphism. \square

These operations, together with coherence conditions, make the category of R -modules into a *braided monoidal category*, where the monoid operation is \otimes and the unit is R .

Proposition (distributivity). There is an isomorphism $(\bigoplus_i M_i) \otimes P \simeq \bigoplus_i (M_i \otimes P)$ mapping $(m_i)_i \otimes p$ to $(m_i \otimes p)_i$.

Proof. Define f by

$$f((m_i)_i, p) = (m_i \otimes p)_i$$

Then there is a unique h such that the following diagram commutes.

$$\begin{array}{ccc} (\bigoplus_i M_i) \times P & \xrightarrow{i_{(\bigoplus_i M_i) \otimes P}} & (\bigoplus_i M_i) \otimes P \\ & \searrow f & \downarrow h \\ & & \bigoplus_i (M_i \otimes P) \end{array}$$

For each i , define the map $f'_i : M_i \times P \rightarrow (\bigoplus_i M_i) \otimes P$ by

$$f'_i(m_i, p) = m_i \otimes p$$

By the universal property of the tensor product, this factors through a unique h'_i .

$$\begin{array}{ccc} M_i \times P & \xrightarrow{i_{M_i \otimes P}} & M_i \otimes P \\ & \searrow f'_i & \downarrow h'_i \\ & & (\bigoplus_i M_i) \otimes P \end{array}$$

Then, by the universal property of the direct sum, the h'_i can be combined into a single h' , so this diagram commutes for each i .

$$\begin{array}{ccc} M_i \otimes P & \longrightarrow & \bigoplus_i (M_i \otimes P) \\ & \searrow h'_i & \downarrow h' \\ & & (\bigoplus_i M_i) \otimes P \end{array}$$

It remains to show that h and h' are inverses. To show $h \circ h' = \text{id}_{\bigoplus_i (M_i \otimes P)}$, it suffices by the universal property of the direct sum to show that $(h \circ h')(x) = x$ for all $x \in M_i \otimes P$, for each i . Then, by the universal property of the tensor product, it further suffices to show this result only for pure tensors.

$$\begin{aligned}
(h \circ h')(m_i \otimes p) &= h(h'(m_i \otimes p)) \\
&= h(h'_i(m_i \otimes p)) \\
&= h(f'_i(m_i, p)) \\
&= h(m_i \otimes p) \\
&= f(m_i, p) \\
&= m_i \otimes p
\end{aligned}$$

To show $h' \circ h = \text{id}_{\bigoplus_i M_i \otimes P}$, it suffices by the universal property of the tensor product to show that $(h' \circ h)((m_i)_i \otimes p) = (m_i)_i \otimes p$. By linearity of h and h' , we can reduce to the case where $(m_i)_i$ has a single non-zero element m_i .

$$\begin{aligned}
(h' \circ h)(m_i \otimes p) &= h'(h(m_i \otimes p)) \\
&= h'(f(m_i, p)) \\
&= h'(m_i \otimes p) \\
&= h'_i(m_i \otimes p) \\
&= f'_i(m_i \otimes p) \\
&= f'_i(m_i, p) \\
&= m_i \otimes p
\end{aligned}$$

□

Example.

$$R^m \otimes_R R^\ell = \left(\bigoplus_{i=1}^m R \right) \otimes_R \left(\bigoplus_{j=1}^\ell R \right) \simeq \bigoplus_{i=1}^m \bigoplus_{j=1}^\ell (R \otimes R) \simeq \bigoplus_{i=1}^m \bigoplus_{j=1}^\ell R \simeq R^{m\ell}$$

Proposition (quotients). Let $M' \subseteq M$ and $N' \subseteq N$ be R -modules. Then there is an isomorphism

$$M/M' \otimes N/N' \simeq (M \otimes N)/L$$

where L is the submodule of $M \otimes N$ generated by

$$\{m' \otimes n \mid (m', n) \in M' \times N\} \cup \{m \otimes n' \mid (m, n') \in M \times N'\}$$

and mapping

$$(m + M') \otimes (n + N') \mapsto m \otimes n + L$$

Proof. Define

$$f : M/M' \times N/N' \rightarrow (M \otimes N)/L$$

by

$$f(m + M', n + N') = m \otimes n + L$$

This is well-defined: if $m \in M'$ or $n \in N'$, then $m \otimes n \in L$. By the universal property of the tensor product, f factors through some h .

$$\begin{array}{ccc} M/M' \times N/N' & \xrightarrow{i_{M/M' \otimes N/N'}} & M/M' \otimes N/N' \\ & \searrow f & \downarrow h \\ & & (M \otimes N)/L \end{array}$$

Now define

$$f' : M \times N \rightarrow M/M' \otimes N/N'$$

by

$$f'(m, n) = (m + M') \otimes (n + N')$$

This is clearly bilinear. Thus, we have

$$\begin{array}{ccc} M \times N & \xrightarrow{i_{M \otimes N}} & M \otimes N \\ & \searrow f' & \downarrow h' \\ & & M/M' \otimes N/N' \end{array}$$

We show that if $x \in L$, then $h'(x) = 0$. By linearity it suffices to show this for the generators.

$$h'(m' \otimes n) = f'(m', n) = 0 \otimes (n + N') = 0; \quad h'(m \otimes n') = f'(m, n') = (m + M') \otimes 0 = 0$$

Thus h' factors through the quotient.

$$\begin{array}{ccc} M \otimes N & \xrightarrow{\pi} & (M \otimes N)/L \\ & \searrow h' & \downarrow h'' \\ & & M/M' \otimes N/N' \end{array}$$

We show h and h'' are inverses. To show $h \circ h'' = \text{id}_{(M \otimes N)/L}$, it suffices by the universal properties of the quotient and the tensor product to consider the images of pure tensors under the quotient map π .

$$\begin{aligned} (h \circ h'')(m \otimes n + L) &= h(h''(\pi(m \otimes n))) \\ &= h(h'(m \otimes n)) \\ &= h(f'(m, n)) \\ &= h((m + M') \otimes (n + N')) \\ &= f(m + M', n + N') \\ &= m \otimes n + L \end{aligned}$$

To show $h'' \circ h = \text{id}_{M/M' \otimes N/N'}$, it suffices to show the result for expressions of the form $(m + M') \otimes$

$(n + N')$.

$$\begin{aligned}
 (h'' \circ h)((m + M') \otimes (n + N')) &= h''(h((m + M') \otimes (n + N'))) \\
 &= h''(f(m + M', n + N')) \\
 &= h''(m \otimes n + L) \\
 &= h'(m \otimes n) \\
 &= f'(m + M', n + N') \\
 &= (m + M') \otimes (n + N')
 \end{aligned}$$

□

2.5 Tensor products of maps

Proposition. Let $f : M \rightarrow M'$ and $g : N \rightarrow N'$ be R -module homomorphisms. There is a unique R -module homomorphism $f \otimes g : M \otimes N \rightarrow M' \otimes N'$ such that

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

Proof. We apply the universal property to the map $T : M \times N \rightarrow M \otimes N'$ given by

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

which can be checked to be R -bilinear. □

Example. We can show

$$(f \otimes g) \circ (h \otimes i) = (f \circ h) \otimes (g \circ i)$$

For example, if $T : k^a \rightarrow k^b$ and $S : k^c \rightarrow k^d$,

$$T \otimes S : k^a \otimes_k k^c \rightarrow k^b \otimes_k k^d$$

is given by

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

where $[T]$ denotes T in the standard basis. Ordering the basis elements of $k^a \otimes k^c$ as

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

and similarly for $k^b \otimes k^d$,

$$[T \otimes S] = \begin{pmatrix} [T]_{11} \cdot [S] & \cdots & [T]_{1a} \cdot [S] \\ \vdots & \ddots & \vdots \\ [T]_{b1} \cdot [S] & \cdots & [T]_{ba} \cdot [S] \end{pmatrix}$$

This is known as the *Kronecker product* of matrices.

Proposition. Let $f : M \rightarrow M', g : N \rightarrow N'$ be R -module homomorphisms. Then,
 (i) if f, g are isomorphisms, then so is $f \otimes g$;

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

Proof. Part (i). $f^{-1} \otimes g^{-1}$ is a two-sided inverse for $f \otimes g$, as

$$(f^{-1} \otimes g^{-1}) \circ (f \otimes g) = (f^{-1} \circ f) \otimes (g^{-1} \circ g) = \text{id}$$

and similarly for the other side.

Part (ii). The image of $f \otimes g$ contains all pure tensors of $M' \otimes N'$, so it must be surjective. \square

The analogous result for injectivity does not hold in the general case. Consider $f : \mathbb{Z} \rightarrow \mathbb{Z}$ given by multiplication by p , and $g : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ given by the identity. Here,

$$(f \otimes g)(a \otimes b) = (pa) \otimes b = a \otimes (pb) = a \otimes 0 = 0$$

So $f \otimes g$ is the zero map, but $\mathbb{Z} \otimes \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}$ is not the zero ring.

2.6 Tensor products of algebras

Let B, C be R -algebras. The usual tensor product of modules $B \otimes_R C$ can be made into a ring and then an R -algebra. This allows us to define the tensor product of algebras in a natural way. We want the ring structure to satisfy

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

This extends to a well-defined map on all of $B \otimes C$. Indeed, for a fixed $(b, c) \in B \times C$, there is an R -bilinear map $B \times C \rightarrow B \otimes C$ given by

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

so we can use the universal property to extend this to a map $B \otimes C \rightarrow B \otimes C$ that acts on pure tensors in the obvious way. One can show that the ring axioms are satisfied. To define the R -algebra structure, we define the ring homomorphism $R \rightarrow B \otimes C$ by

$$r \mapsto (r \cdot 1_B) \otimes 1_C = 1_B \otimes (r \cdot 1_C)$$

Example. There is an isomorphism of R -algebras

$$\varphi : R[X_1, \dots, X_n] \otimes_R R[T_1, \dots, T_r] \simeq R[X_1, \dots, X_n, T_1, \dots, T_r]$$

An R -basis for the left-hand side as an R -module is given by elements of the form $a \otimes b$ where a and b are monomials. The right hand side has a basis of elements of the form ab , where $a \in R[X_1, \dots, X_n]$ and $b \in R[T_1, \dots, T_r]$ are monomials as above. Mapping $\varphi(a \otimes b) = ab$, we obtain an R -module isomorphism. To check this is an R -algebra isomorphism, we verify multiplication and its action on scalars.

$$\varphi(r \otimes 1) = r \cdot 1; \quad \varphi(1 \otimes 1)$$

and for monomials p_i, q_i, h_i, g_i ,

$$\begin{aligned}
\varphi\left(\left(\sum_i p_i \otimes q_i\right)\left(\sum_j h_j \otimes g_j\right)\right) &= \sum_{i,j} (p_i h_j)(q_i g_j) \\
&= \sum_{i,j} (p_i q_i)(h_j g_j) \\
&= \sum_{i,j} \varphi(p_i \otimes q_i) \varphi(h_j \otimes g_j) \\
&= \left(\sum_i \varphi(p_i \otimes q_i)\right) \left(\sum_j \varphi(h_j \otimes g_j)\right) \\
&= \varphi\left(\sum_i p_i \otimes q_i\right) \varphi\left(\sum_j h_j \otimes g_j\right)
\end{aligned}$$

More generally,

$$R[X_1, \dots, X_n]_I \otimes R[T_1, \dots, T_r]_J \simeq R[X_1, \dots, X_n] \otimes R[T_1, \dots, T_r]_L \simeq R[X_1, \dots, X_n, T_1, \dots, T_r]_{I^e + J^e}$$

where L is constructed as above when quotients were discussed, and I^e is the extension of I in the larger ring $R[X_1, \dots, X_n, T_1, \dots, T_r]$. For example,

$$\mathbb{C}[X, Y, Z]_{(f, g)} \otimes_{\mathbb{C}} \mathbb{C}[W, U]_{(h)} \simeq \mathbb{C}[X, Y, Z, W, U]_{(f, g, h)}$$

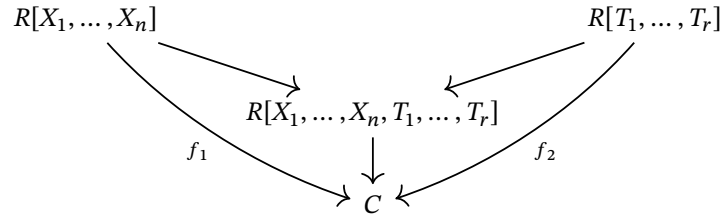
Proposition (universal property of tensor product of algebras). Let A, B be R -algebras. For every algebra C and R -algebra homomorphisms $f_1 : A \rightarrow C$ and $f_2 : B \rightarrow C$, there is a unique R -algebra homomorphism $h : A \otimes_R B \rightarrow C$ such that the following diagram commutes:

$$\begin{array}{ccc}
A & & B \\
& \searrow^{i_A} & \swarrow_{i_B} \\
& A \otimes B & \\
& \searrow_{f_1} & \swarrow_{f_2} \\
& C & \\
& \uparrow h & \\
& A \otimes B & \\
& \swarrow_{i_A} & \searrow_{i_B} \\
A & & B
\end{array}$$

where $i_A(a) = a \otimes 1$ and $i_B(b) = 1 \otimes b$. Furthermore, this characterises the triple $(A \otimes_R B, i_A, i_B)$ uniquely up to unique isomorphism.

Proof. $A \otimes_R B$ is generated as an R -algebra by $\{a \otimes 1 \mid a \in A\} \cup \{1 \otimes b \mid b \in B\}$. This implies the uniqueness of h . For existence, we can define an R -bilinear map $A \times B \rightarrow C$ by $(a, b) \mapsto f_1(a)f_2(b)$, then apply the universal property of the tensor product of modules. This produces an R -linear map $h : A \otimes B \rightarrow C$. It remains to show that this is a homomorphism of algebras. \square

Example.



An algebra homomorphism from a polynomial ring is defined uniquely by giving its action on its variables, thus

$$R[X_1, \dots, X_n] \otimes R[T_1, \dots, T_r] \simeq R[X_1, \dots, X_n, T_1, \dots, T_r]$$

as was shown above.

Remark. (i) If $f : A \rightarrow A', g : B \rightarrow B'$ are R -algebra homomorphisms, then $f \otimes g : A \otimes B \rightarrow A' \otimes B'$ is not only an R -module homomorphism but is also an R -algebra homomorphism.

(ii) There are R -algebra homomorphisms

- (a) $R/I \otimes R/J \simeq R/I + J$;
- (b) $A \otimes B \simeq B \otimes A$;
- (c) $A \otimes (B \times C) \simeq (A \otimes B) \times (A \otimes C)$;
- (d) $A \otimes B^n \simeq (A \otimes B)^n$;
- (e) $(A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$.

2.7 Restriction and extension of scalars

Let $f : R \rightarrow S$ be a ring homomorphism. Let M be an S -module. Then we can *restrict scalars* to make M into an R -module by

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

The composition $R \rightarrow S \rightarrow \text{End } M$ is a ring homomorphism, so this makes M into an R -module automatically without needing to check axioms.

Example. Let $f : \mathbb{R} \rightarrow \mathbb{C}$ be the inclusion. Then any \mathbb{C} -module is an \mathbb{R} -module.

Now suppose $f : R \rightarrow S$ is a ring homomorphism, M is an S -module, and N is an R -module. We can form the R -module $M \otimes_R N$, as M is an R -module by restriction of scalars. *Extension of scalars* shows that $M \otimes_R N$ is also an S -module. The action of $s \in S$ on pure tensors is

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

We have an R -bilinear map $M \times N \rightarrow M \otimes_R N$ by

$$(m, n) \mapsto sm \otimes n$$

so by the universal property this gives rise to a map $h_s : M \otimes_R N \rightarrow M \otimes_R N$ with the desired action on pure tensors. h_s is R -linear by the universal property. Defining $\varphi : S \rightarrow \text{End}(M \otimes_R N)$ by $\varphi(s) = h_s$, one can check that h_s is a well-defined endomorphism and that φ is a ring homomorphism.

Example. $S \otimes_R R \simeq S$ as R -modules, by $s \otimes r \mapsto s \cdot f(r)$. This is also S -linear, since

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

For example, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R} \simeq \mathbb{C}$ as \mathbb{C} -modules.

Example. Let M be an S -module and $(N_i)_{i \in I}$ are R -modules. Then

$$M \otimes \left(\bigoplus_i N_i \right) \simeq \bigoplus_i (M \otimes N_i)$$

as S -modules. So $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \simeq \mathbb{C}^n$ as \mathbb{C} -modules.

Example. Restrict the \mathbb{C} -module \mathbb{C}^n to an \mathbb{R} -module to obtain \mathbb{R}^{2n} . Then, extending to \mathbb{C} ,

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

Similarly, extending \mathbb{R}^n to \mathbb{C} , we find $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \simeq \mathbb{C}^n$ over \mathbb{C} . Restricting to \mathbb{R} , $\mathbb{C}^n \simeq \mathbb{R}^{2n}$. So the operations of restriction and extension of scalars are not inverses in either direction.

Example. Consider \mathbb{Z}^n as a \mathbb{Z} -module. Consider the quotient map $f : \mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$. Extending scalars to $\mathbb{Z}/2\mathbb{Z}$,

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

Example. Consider $\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell$ as a \mathbb{C} -module. As \mathbb{R} -modules,

$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \simeq \mathbb{R}^{2n} \otimes_{\mathbb{R}} \mathbb{R}^\ell \simeq \mathbb{R}^{2n\ell} \simeq \mathbb{C}^{n\ell}$$

We would like to make this into an isomorphism of \mathbb{C} -modules. We will show that in fact

$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \simeq \mathbb{C}^n \otimes_{\mathbb{C}} (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^\ell)$$

where

$$v \otimes u \mapsto v \otimes (1 \otimes u)$$

giving

$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \simeq \mathbb{C}^n \otimes_{\mathbb{C}} \mathbb{C}^\ell \simeq \mathbb{C}^{n\ell}$$

as \mathbb{C} -modules. The isomorphism

$$\mathbb{C}^n \otimes_{\mathbb{R}} \mathbb{R}^\ell \simeq \mathbb{C}^n \otimes_{\mathbb{C}} \mathbb{C}^\ell$$

maps a pure tensor $v \otimes u$ to $v \otimes u$.

Proposition. Let M be an S -module and N be an R -module. Then

$$M \otimes_R N \simeq M \otimes_S (S \otimes_R N)$$

as S -modules, where

$$m \otimes n \mapsto m \otimes (1 \otimes n); \quad sm \otimes n \mapsto m \otimes (s \otimes n)$$

Proof. The map $(m, n) \mapsto m \otimes (1 \otimes n)$ is R -bilinear, so the map f mapping $m \otimes n$ to $m \otimes (1 \otimes n)$ is well-defined as a map of R -modules. We show it is S -linear on pure tensors.

$$f(s(m \otimes n)) = f(sm \otimes n) = sm \otimes (1 \otimes n) = s(m \otimes (1 \otimes n)) = sf(m \otimes n)$$

For a fixed $m \in M$, the map $s \otimes n \mapsto sm \otimes n$ is well-defined and S -linear. This collection of maps is S -linear in its parameter m , so we obtain an S -bilinear map $(m, s \otimes n) \mapsto sm \otimes n$. Hence, we obtain a map g mapping $m \otimes (s \otimes n)$ to $sm \otimes n$, as desired. One can easily check that f and g are inverses on pure tensors. \square

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

$$\begin{aligned} M \otimes_R N &\simeq N \otimes_R M \\ (M \otimes_R N) \otimes_R N' &\simeq M \otimes_R (N \otimes_R N') \\ (M \otimes_R N) \otimes_S M' &\simeq M \otimes_S (N \otimes_R M') \\ M \otimes_R \left(\bigoplus_i N_i \right) &\simeq \bigoplus_i (M \otimes_R N_i) \end{aligned}$$

Heuristically, the tensor products in the above isomorphisms always operate over the largest possible ring: S if both operands are S -modules, else R . We prove only the third result.

Proof. By the previous proposition,

$$\begin{aligned} (M \otimes_R N) \otimes_S M' &\simeq (M \otimes_S (N \otimes_R S)) \otimes_S M' \\ &\simeq M \otimes_S ((N \otimes_R S) \otimes_S M') \\ &\simeq M \otimes_S (N \otimes_R M') \end{aligned}$$

\square

Corollary. Let N, N' be R -modules. Then

$$S \otimes_R (N \otimes_R N') \simeq (S \otimes_R N) \otimes_S (S \otimes_R N')$$

as S -modules.

Proof.

$$S \otimes_R (N \otimes_R N') \simeq (S \otimes_R N) \otimes_R N' \simeq (S \otimes_R N) \otimes_S (S \otimes_R N')$$

\square

Example.

$$\mathbb{C} \otimes_{\mathbb{R}} (\mathbb{R}^\ell \otimes_{\mathbb{R}} \mathbb{R}^k) \simeq (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^\ell) \otimes_{\mathbb{C}} (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^k) \simeq \mathbb{C}^\ell \otimes_{\mathbb{C}} \mathbb{C}^k \simeq \mathbb{C}^{\ell k}$$

By induction, one can see that

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

2.8 Extension of scalars on morphisms

Let $f : N \rightarrow N'$ be an R -linear map, and M be an S -module. Then the map

$$\text{id}_M \otimes f : M \otimes_R N \rightarrow M \otimes_R N'$$

is S -linear. Indeed,

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

Example. Let $T : \mathbb{R}^n \rightarrow \mathbb{R}^\ell$ be R -linear, and use bases e_1, \dots, e_n and f_1, \dots, f_ℓ . Then

$$\text{id}_{\mathbb{C}} \otimes T : \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^n \rightarrow \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^\ell$$

is given by

$$(\text{id}_{\mathbb{C}} \otimes T)(1 \otimes e_i) = 1 \otimes T(e_i) = 1 \otimes \sum_{j=1}^{\ell} [T]_{ji} \cdot f_j = \sum_{j=1}^{\ell} [T]_{ji} (1 \otimes f_j)$$

This shows that the matrix $[\text{id}_{\mathbb{C}} \otimes T]$ has all real elements, and is the same as the matrix $[T]$.

2.9 Extension of scalars in algebras

Let A, B be R -algebras. Then the module $A \otimes_R B$ is also an R -algebra. Furthermore, can see that $A \otimes_R B$ is an A -algebra and a B -algebra by the maps $a \mapsto a \otimes 1$ and $b \mapsto 1 \otimes b$.

Example. Consider $R[X_1, \dots, X_n]$ and $f : R \rightarrow S$. Then

$$\varphi : S \otimes_R R[X_1, \dots, X_n] \simeq S[X_1, \dots, X_n]$$

as S -algebras. Indeed, φ already exists as an isomorphism of S -modules given by

$$\varphi(s \otimes p) = sp$$

and one can verify that unity and multiplication are preserved. Further,

$$S \otimes (R[X_1, \dots, X_n]_I) \simeq S[X_1, \dots, X_n]_{I^e}$$

Proposition. Let A be an R -algebra and B be an S -algebra. Then

$$A \otimes_R B \simeq (A \otimes_R S) \otimes_S B$$

as S -algebras.

Proposition. Let A, B be R -algebras. Then

$$S \otimes_R (A \otimes_R B) \simeq (S \otimes_R A) \otimes_S (S \otimes_R B)$$

as S -algebras.

The proofs are omitted, but trivial.

2.10 Exactness properties of the tensor product

Let M be an R -module. There is a functor

$$T_M : \mathbf{Mod}_R \rightarrow \mathbf{Mod}_R$$

from the category of R -modules to itself given by

$$T_M(N) = M \otimes_R N; \quad T_M(N \xrightarrow{f} N') = \text{id}_M \otimes f$$

We intend to show that if

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

is an exact sequence of R -modules, then

$$M \otimes_R A \xrightarrow{T_M(f)} M \otimes_R B \xrightarrow{T_M(g)} M \otimes_R C \longrightarrow 0$$

is also an exact sequence. This shows that T_M is a *right exact* functor.

Definition. Let Q, P be R -modules. Then

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

This is also an R -module: if $\varphi \in \text{Hom}_R(Q, P)$,

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

Definition. Let Q, P be R -modules. Then

$$\text{Hom}_R(Q, -) : \mathbf{Mod}_R \rightarrow \mathbf{Mod}_R$$

and

$$\text{Hom}_R(-, P) : \mathbf{Mod}_R^{\text{op}} \rightarrow \mathbf{Mod}_R$$

are functors, with action on morphisms $f : N' \rightarrow N$ given by

$$\text{Hom}_R(Q, f)(\varphi) = f \circ \varphi = f_*(\varphi) : \text{Hom}_R(Q, N') \rightarrow \text{Hom}_R(Q, N)$$

and

$$\text{Hom}_R(f, P)(\varphi) = \varphi \circ f = f^*(\varphi) : \text{Hom}_R(N, Q) \rightarrow \text{Hom}_R(N', Q)$$

Proposition. Suppose

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

is exact. Then, so is

$$0 \longrightarrow \text{Hom}_R(Q, A) \xrightarrow{f_*} \text{Hom}_R(Q, B) \xrightarrow{g_*} \text{Hom}_R(Q, C)$$

Thus, the covariant hom-functor is *left exact*.

Proof. First, we show f_* is injective. Suppose $f_*(\varphi) = 0$, so $f \circ \varphi = 0$. Then as f is injective, $f(\varphi(x)) = 0$ implies $\varphi(x) = 0$, giving $\varphi = 0$ as required.

Now consider $\varphi : Q \rightarrow A$. Then

$$g_*(f_*(\varphi)) = g \circ (f \circ \varphi) = (g \circ f) \circ \varphi = 0 \circ \varphi = 0$$

so $\text{im } f_* \subseteq \ker g_*$. Now suppose $\varphi : Q \rightarrow B$ has $g_*(\varphi) = g \circ \varphi = 0$. So for all $x \in Q$, $g(\varphi(x)) = 0$. By exactness of the original sequence, $\varphi(x) \in \text{im } f$. As f is injective, $\varphi(x)$ has a unique preimage $\psi(x)$ under f . As f is R -linear, so is $\psi : Q \rightarrow A$. Hence $f_*(\psi) = \varphi$ as required. \square

Proposition. Suppose

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

is exact. Then, so is

$$0 \longrightarrow \text{Hom}_R(C, P) \xrightarrow{g^*} \text{Hom}_R(B, P) \xrightarrow{f^*} \text{Hom}_R(A, P)$$

Thus, the contravariant hom-functor is also left-exact.

Proof. First, we show g^* is injective. Suppose $g^*(\varphi) = 0$, so $\varphi \circ g = 0$. As g is surjective, we must have $\varphi = 0$.

Now consider $\varphi : C \rightarrow P$. Then

$$f^*(g^*(\varphi)) = (\varphi \circ g) \circ f = \varphi \circ (g \circ f) = \varphi \circ 0 = 0$$

so $\text{im } g^* \subseteq \ker f^*$. Now suppose $\varphi : B \rightarrow P$ has $f^*(\varphi) = \varphi \circ f = 0$. So for all $x \in A$, $\varphi(f(x)) = 0$. Define $\psi : C \rightarrow P$ by

$$\psi(g(x)) = \varphi(x)$$

We show this is well-defined. If $g(x) = g(y)$, then $g(x - y) = 0$, so $x - y = f(a)$ for some $a \in A$. But then $\varphi(f(a)) = 0$, so $\varphi(x) = \varphi(y)$. As φ and g are R -linear, so is ψ . Hence $g^*(\psi) = \varphi$ as required. \square

Lemma. Consider a sequence of R -modules

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

Suppose that for each R -module P ,

$$\text{Hom}_R(C, P) \xrightarrow{g^*} \text{Hom}_R(B, P) \xrightarrow{f^*} \text{Hom}_R(A, P)$$

is exact. Then the original sequence

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

is exact.

Proof. First, take $P = C$. By hypothesis, the following sequence is exact.

$$\mathrm{Hom}_R(C, C) \xrightarrow{g^*} \mathrm{Hom}_R(B, C) \xrightarrow{f^*} \mathrm{Hom}_R(A, C)$$

Consider

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

By exactness, id_C must be mapped to zero under $f^* \circ g^*$, so $g \circ f = 0$. Hence $\mathrm{im} f \subseteq \ker g$.

Now, take $P = B/\mathrm{im} f = \mathrm{coker} f$.

$$\mathrm{Hom}_R(C, B/\mathrm{im} f) \xrightarrow{g^*} \mathrm{Hom}_R(B, B/\mathrm{im} f) \xrightarrow{f^*} \mathrm{Hom}_R(A, B/\mathrm{im} f)$$

Let $h : B \rightarrow B/\mathrm{im} f$ be the quotient map. Then,

$$f^*(h) = h \circ f; \quad h(f(x)) = 0$$

Thus by exactness, h has a preimage $e : C \rightarrow B/\mathrm{im} f$. Then $g^*(e) = e \circ g = h$, so $\ker g \subseteq \ker h = \mathrm{im} f$, giving the reverse inclusion. \square

By the universal property of the tensor product,

$$\mathrm{Hom}_R(M \otimes_R N, L) \simeq \mathrm{Bilin}_R(M \times N, L) \simeq \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, L))$$

given by

$$\varphi \mapsto (n \mapsto m \mapsto \varphi(m \otimes n)); \quad (m \otimes n \mapsto \varphi(m)(n)) \leftarrow \varphi$$

This bijection is *natural*, in the sense that many commutative diagrams involving them will commute.

Proposition. Let M be an R -module. Then the functor $T_M = M \otimes_R (-)$ is right exact.

Proof. Consider an exact sequence of R -modules

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

We must show that

$$M \otimes_R A \xrightarrow{\mathrm{id}_M \otimes f} M \otimes_R B \xrightarrow{\mathrm{id}_M \otimes g} M \otimes_R C \longrightarrow 0$$

is exact. Let P be an R -module, and consider apply the functor $\mathrm{Hom}(-, P)$ to this sequence. As this is left exact, the resulting sequence will be exact.

$$0 \longrightarrow \mathrm{Hom}_R(C, P) \xrightarrow{g^*} \mathrm{Hom}_R(B, P) \xrightarrow{f^*} \mathrm{Hom}_R(A, P)$$

Then, apply the functor $\mathrm{Hom}(M, -)$, which is also left exact.

$$0 \longrightarrow \mathrm{Hom}_R(M, \mathrm{Hom}_R(C, P)) \xrightarrow{(g^*)^*} \mathrm{Hom}_R(M, \mathrm{Hom}_R(B, P)) \xrightarrow{(f^*)^*} \mathrm{Hom}_R(M, \mathrm{Hom}_R(A, P))$$

We thus obtain

$$\begin{array}{ccccccc}
 0 & \longrightarrow & \text{Hom}_R(M, \text{Hom}_R(C, P)) & \longrightarrow & \text{Hom}_R(M, \text{Hom}_R(B, P)) & \longrightarrow & \text{Hom}_R(M, \text{Hom}_R(A, P)) \\
 \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\
 0 & \longrightarrow & \text{Hom}_R(M \otimes_R C, P) & \longrightarrow & \text{Hom}_R(M \otimes_R B, P) & \longrightarrow & \text{Hom}_R(M \otimes_R A, P)
 \end{array}$$

As this diagram commutes, the bottom sequence is exact. Since this holds for all P , by the previous lemma, we can cancel P to give exact sequences

$$0 \longrightarrow M \otimes_R C \longrightarrow M \otimes_R B \longrightarrow M \otimes_R A$$

which combine into the longer sequence as required. \square

Remark. It is not the case that if

$$A \longrightarrow B \longrightarrow C$$

is exact, then

$$M \otimes_R A \longrightarrow M \otimes_R B \longrightarrow M \otimes_R C$$

is also exact; the fact that the sequence has a zero on the right is important. Consider the exact sequence

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

and tensor with $\mathbb{Z}/2\mathbb{Z}$. We would then obtain

$$\begin{array}{ccccc}
 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z} \\
 \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\
 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\times 2} & \mathbb{Z}/2\mathbb{Z}
 \end{array}$$

but this sequence is not exact.

2.11 Flat modules

Definition. An R -module M is *flat* if whenever $f : N \rightarrow N'$ is R -linear and injective, the map

$$\text{id}_M \otimes f : M \otimes_R N \rightarrow M \otimes_R N'$$

is injective.

Example. (i) $\mathbb{Z}/2\mathbb{Z}$ is not a flat \mathbb{Z} -module.

(ii) Free modules are flat. Suppose $f : N \rightarrow N'$ is an injective R -linear map. Then

$$\begin{array}{ccc}
 R^{\oplus I} \otimes_R N & \xrightarrow{\text{id}_{R^{\oplus I}} \otimes f} & R^{\oplus I} \otimes_R N' \\
 \cong \downarrow & & \downarrow \cong \\
 N^{\oplus I} & \xrightarrow{g} & (N')^{\oplus I}
 \end{array}$$

commutes, where

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

But g is injective, so $\text{id}_{R \oplus I} \otimes f$ must also be injective.

(iii) The base ring matters. One can see that $\mathbb{Z}/2\mathbb{Z}$ is not a flat \mathbb{Z} -module but it is a flat $\mathbb{Z}/2\mathbb{Z}$ -module as it is a free $\mathbb{Z}/2\mathbb{Z}$ -module.

Definition. An R -module M is *torsion-free* if $rm \neq 0$ whenever r is not a zero divisor in R and $m \neq 0$.

Proposition. Flat modules are torsion-free.

Proof. Suppose M is not torsion-free. Then there is $r_0 \in R$ not a zero divisor and $m_0 \neq 0$, such that $r_0 m_0 = 0$. Consider the R -linear map $f : R \rightarrow R$ given by multiplication by r_0 . Its kernel is zero, as r_0 is not a zero divisor. So f is injective. The following diagram commutes.

$$\begin{array}{ccc} M \otimes_R R & \xrightarrow{\text{id}_M \otimes f} & M \otimes_R R \\ \cong \downarrow & & \downarrow \cong \\ M & \xrightarrow{m \mapsto r_0 m} & M \end{array}$$

If M were flat, $\text{id}_M \otimes f$ would be injective, but then the map $m \mapsto r_0 m$ would also be injective, which is a contradiction. \square

Example. Let R be an integral domain, and let I be a nonzero ideal of R . Then R/I is not flat. Indeed, if $I = R$ then $R/I = 0$ is not flat. Instead, suppose $I \subsetneq R$, and let $0 \neq x \in I$. Tensoring with R/I , the map $R/I \rightarrow R/I$ given by multiplication by x is the zero map, but R/I is not the zero module, so R/I is not torsion-free.

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

- (i) T_M preserves exactness of all exact sequences;
- (ii) T_M preserves exactness of short exact sequences;
- (iii) M is flat;
- (iv) if $f : N \rightarrow N'$ is R -linear and injective, and N, N' are finitely generated R -modules, then $\text{id}_M \otimes f$ is injective.

Note that a map $f : M \rightarrow N$ is injective exactly when the sequence

$$0 \longrightarrow M \xrightarrow{f} N$$

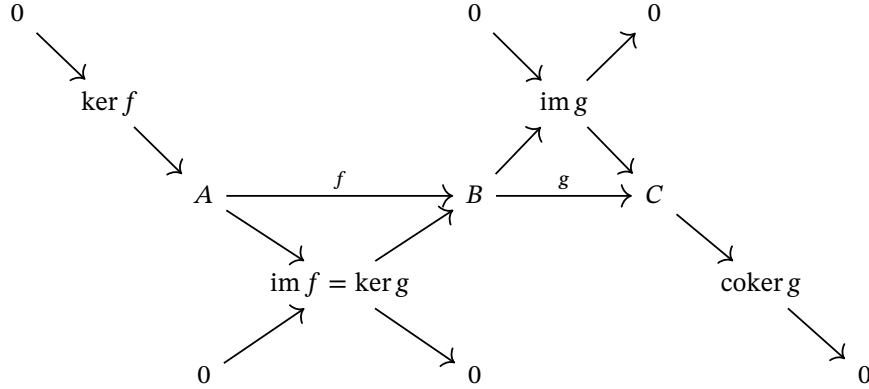
is exact, so all of these conditions relate exact sequences.

Proof. Note that (i) implies (ii) which implies (iii) which implies (iv).

(ii) implies (i). Suppose the sequence

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

is exact. Then, the following diagram is exact.



After applying $T = T_M$, the diagram still commutes, and the diagonal lines remain exact.

$$\begin{aligned}
 \text{im}(TA \rightarrow TB) &= \text{im}(TA \rightarrow T(\text{im } f) \rightarrow TB) \\
 &= \text{im}(T(\text{im } f) \rightarrow TB) \\
 &= \text{ker}(TB \rightarrow T(\text{im } g)) \\
 &= \text{ker}(TB \rightarrow T(\text{im } g) \rightarrow TC) \\
 &= \text{ker}(TB \rightarrow TC)
 \end{aligned}$$

(iii) implies (ii). Suppose the sequence

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

is exact. As T_M is right exact, we obtain the exact sequence

$$M \otimes_R A \xrightarrow{\text{id}_M \otimes f} M \otimes_R B \xrightarrow{\text{id}_M \otimes g} M \otimes_R C \longrightarrow 0$$

It suffices to show that $\text{id}_M \otimes f$ is injective, but this is precisely the hypothesis of (iii).

(iv) implies (iii). Let $f : N \rightarrow N'$ be R -linear and injective. Let $\sum m_i \otimes n_i \in M \otimes_R N$ be such that

$$0 = (\text{id}_M \otimes f)\left(\sum m_i \otimes n_i\right) \in M \otimes N'$$

Then there are finitely generated submodules L, L' of N, N' such that the n_i are elements of L and

$$0 = (\text{id}_M \otimes f)\left(\sum m_i \otimes n_i\right) \in M \otimes L'$$

By (iv), we obtain

$$0 = \sum m_i \otimes n_i \in M \otimes L$$

But L is a submodule of N , so

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

Hence $\text{id}_M \otimes f : M \otimes_R N \rightarrow M \otimes_R N'$ is injective. \square

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

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

$$\begin{array}{ccc} (S \otimes_R M) \otimes_S N & \xrightarrow{\text{id}_{S \otimes_R M} \otimes g} & (S \otimes_R M) \otimes_S N' \\ \simeq \downarrow & & \downarrow \simeq \\ M \otimes_R N & \xrightarrow{\text{id}_M \otimes g} & M \otimes_R N' \end{array}$$

commutes. The map $\text{id}_M \otimes g$ is injective as M is flat, so the map $\text{id}_{S \otimes_R M} \otimes g$ is also injective. Thus $S \otimes_R M$ is a flat S -module. \square

We now explore some further examples of tensor products.

Example. Consider $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$. In this ring,

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

So this ring is trivial. To prove this, we used the fact that for all $x \in \mathbb{Q}$ and $n \geq 1$, there is an element $y \in \mathbb{Q}$ such that $ny = x$. We say that \mathbb{Q} is a *divisible group*. We also needed the fact that $\mathbb{Z}/n\mathbb{Z}$ is a *torsion group*: all elements are of finite order. Hence the tensor product of a divisible group with a torsion group is zero. In particular, it follows that

$$\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$$

However, for an R -module $M \neq 0$, if M is finitely generated then $M \otimes_R M \neq 0$.

Example. Let V be a vector space over \mathbb{Q} . Then $\mathbb{Q} \otimes_{\mathbb{Q}} V \simeq V$ as \mathbb{Q} -modules, given by the map $x \otimes v \mapsto xv$. However, $\mathbb{Q} \otimes_{\mathbb{Z}} V$ is also isomorphic to V , given by the same map. First, note that every tensor in $\mathbb{Q} \otimes_{\mathbb{Z}} V$ is pure.

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

Surjectivity of the map is clear as $1 \otimes v \rightarrow v$. We check injectivity on pure tensors. If $xv = 0$, then $x = 0$ or $v = 0$, and in any case, $x \otimes v = 0$.

Example. Consider

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

given by $m \otimes (n_i)_{i \in I} \mapsto (m \otimes n_i)_{i \in I}$. This is not true with the direct product. However, we do have a map

$$M \otimes_R \left(\prod_{i \in I} N_i \right) \rightarrow \prod_{i \in I} (M \otimes_R N_i)$$

given by the same formula, but this is in general not an isomorphism. Consider

$$\mathbb{Q} \otimes_{\mathbb{Z}} \prod_{n=1}^{\infty} \mathbb{Z}/2^n \mathbb{Z} \rightarrow \prod_{n=1}^{\infty} (\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2^n \mathbb{Z})$$

The right-hand side is zero, as each factor is a tensor product of a divisible group by a torsion group. However, the left-hand side is nonzero. Let

$$g = (1, 1, 1, \dots) \in \prod_{n=1}^{\infty} \mathbb{Z}/2^n\mathbb{Z}$$

This is an element of infinite order, so $\langle g \rangle \simeq \mathbb{Z}$ as a subgroup of $\prod_{n=1}^{\infty} \mathbb{Z}/2^n\mathbb{Z}$. Thus

$$\mathbb{Q} \otimes_{\mathbb{Z}} \langle g \rangle \simeq \mathbb{Q}$$

as \mathbb{Z} -modules. But we have an injective inclusion map

$$\langle g \rangle \rightarrow \prod_{n=1}^{\infty} \mathbb{Z}/2^n\mathbb{Z}$$

We will later show that \mathbb{Q} is a flat \mathbb{Z} -module. This justifies the fact that there is an inclusion

$$\mathbb{Q} \otimes_{\mathbb{Z}} \langle g \rangle \rightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \prod_{n=1}^{\infty} \mathbb{Z}/2^n\mathbb{Z}$$

showing that in particular the module in question is nonzero.

Example. Consider $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$. We will choose to extend scalars on the left, treating the right-hand copy of \mathbb{C} as an \mathbb{R} -module isomorphic to \mathbb{R}^2 . As a module, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}^2$ is isomorphic to \mathbb{C}^2 . The basis for \mathbb{C}^2 is given by $1 \otimes 1, 1 \otimes i$.

As a \mathbb{C} -algebra, we again choose to extend scalars on the left, considering the right-hand copy of \mathbb{C} as an \mathbb{R} -algebra.

$$\begin{aligned} \mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} &\simeq \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[T]/(T^2 + 1) \\ &\simeq \mathbb{C}[T]/(T^2 + 1) \\ &\simeq \mathbb{C}[T]/(T - i)(T + i) \\ &\simeq \mathbb{C}[T]/(T - i) \times \mathbb{C}[T]/(T + i) \\ &\simeq \mathbb{C} \times \mathbb{C} \end{aligned}$$

using the Chinese remainder theorem, which will be explored later. The action of this isomorphism on a pure tensor is

$$\begin{aligned} x \otimes y = (a + bi) \otimes (c + di) &\mapsto (a + bi) \otimes (c + dT + (T^2 + 1)\mathbb{R}[T]) \\ &\mapsto (a + bi)(c + dT) + (T^2 + 1)\mathbb{C}[T] \\ &= \underbrace{(ac + bdiT) + (ibc + adT)}_P + (T^2 + 1)\mathbb{C}[T] \\ &\mapsto (P + (T - i)\mathbb{C}[T], P + (T + i)\mathbb{C}[T]) \\ &\mapsto ((ac - bd) + i(bc + ad), (ac + bd) + i(bc - ad)) = (xy, x\bar{y}) \end{aligned}$$

3 Localisation

3.1 Definitions

Definition. A *multiplicative set* or *multiplicatively closed set* $S \subseteq R$ is a subset such that $1 \in S$ and if $a, b \in S$, then $ab \in S$. If $U \subseteq R$ is any set, its *multiplicative closure* S is the set

$$\left\{ \prod_{i=1}^n u_i \mid n \geq 0, u_i \in U \right\}$$

which is the smallest multiplicatively closed set containing U .

Example. (i) If R is an integral domain, then $S = R \setminus \{0\}$ is multiplicative.

(ii) More generally, if \mathfrak{p} is a prime ideal in R , then $S = R \setminus \mathfrak{p}$ is multiplicative.

(iii) If $x \in R$, then the set $\{x^n \mid n \geq 0\}$ is multiplicative.

Remark. \mathbb{Q} is obtained from \mathbb{Z} by adding inverses for the elements of the multiplicative subset $\mathbb{Z} \setminus \{0\}$. We have a ring homomorphism $\mathbb{Z} \rightarrow \mathbb{Q}$. We generalise this construction to arbitrary rings and multiplicative sets. In general, injectivity of the ring homomorphism in question may fail.

Definition. Let $S \subseteq R$ be a multiplicative set, and let M be an R -module. Then the *localisation* of M by S is the set $S^{-1}M = M \times S / \sim$ where $(m_1, s_1) \sim (m_2, s_2)$ if and only if there exists $u \in S$ such that $u(s_2m_1 - s_1m_2) = 0$. We write $\frac{m}{s}$ for the equivalence class corresponding to (m, s) . We make $S^{-1}M$ into an R -module by defining

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{m_1s_2 + m_2s_1}{s_1s_2}; \quad r \cdot \frac{m}{s} = \frac{rm}{s}$$

We can make $S^{-1}R$ into a ring by defining

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$$

Then $S^{-1}M$ is an $S^{-1}R$ -module by

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

We have the localisation map $R \rightarrow S^{-1}R$ given by $r \mapsto \frac{r}{1}$, which is a ring homomorphism. We also have the localisation map $M \rightarrow S^{-1}M$ given by $m \mapsto \frac{m}{1}$, which is a homomorphism of R -modules.

We must show that \sim is an equivalence relation. The only nontrivial thing to prove is transitivity. Let

$$u(s_2m_1 - s_1m_2) = 0 = v(s_3m_2 - s_2m_3); \quad u, v \in S$$

Then

$$0 = uv(s_2s_3m_1 - s_1s_3m_2) + uv(s_1s_3m_2 - s_1s_2m_3) = uv s_2(s_3m_1 - s_1m_3); \quad uv s_2 \in S$$

as required. All other operations mentioned are well-defined; the proofs are not enlightening so are omitted.

3.2 Universal property for rings

Proposition. Let $U \subseteq R$, and let $S \subseteq R$ be its multiplicative closure. Let $f : R \rightarrow B$ be a ring homomorphism such that $f(u)$ is a unit for all $u \in U$. Then there is a unique ring homomorphism $h : S^{-1}R \rightarrow B$ such that the following diagram commutes.

$$\begin{array}{ccc} R & \xrightarrow{\iota_{S^{-1}R}} & S^{-1}R \\ & \searrow f & \downarrow h \\ & & B \end{array}$$

where $\iota_{S^{-1}R}(r) = \frac{r}{1}$, so in particular, $f(r) = h\left(\frac{r}{1}\right)$.

Thus

$$\text{Hom}_{\text{Ring}}(S^{-1}R, B) \simeq \{\varphi \in \text{Hom}_{\text{Ring}}(R, B) \mid \varphi(U) \subseteq B^\times\}$$

mapping

$$f \mapsto \left(r \mapsto \frac{r}{1}\right); \quad \left(\frac{r}{s} \mapsto \frac{\varphi(r)}{\varphi(s)}\right) \leftrightarrow \varphi$$

Proof. Let $f : R \rightarrow B$ be a ring homomorphism such that $f(u)$ is a unit for all $u \in U$. Then $f(s)$ is a unit for all $s \in S$. We want to construct a ring homomorphism $h : S^{-1}R \rightarrow B$ such that $f(r) = h\left(\frac{r}{1}\right)$ for all $r \in R$. Such an h must satisfy the following condition.

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

Thus $h\left(\frac{1}{s}\right) = f(s)^{-1}$. Hence, we must have

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

It thus suffices to show that this h is well-defined; it is then a ring homomorphism satisfying the correct property. If $\frac{r_1}{s_1} = \frac{r_2}{s_2}$, then there is $t \in S$ such that $ts_2r_1 = ts_1r_2$. Applying f ,

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

As $f(t), f(s_1), f(s_2)$ are invertible,

$$\frac{f(r_1)}{f(s_1)} = \frac{f(r_2)}{f(s_2)}$$

so h is well-defined. □

Proposition. Suppose (A, j) has the same universal property of $(S^{-1}R, \iota_{S^{-1}R})$ where $\iota_{S^{-1}R}(r) = \frac{r}{1}$, then there is a unique ring isomorphism $S^{-1}R \rightarrow A$ mapping $\frac{r}{s}$ to $j(s)^{-1}j(r)$.

Remark. (i) Let $\frac{r}{s} \in S^{-1}R$. Then $\frac{r}{s} = \frac{0}{1}$ if and only if there exists $u \in S$ such that $ur = 0$.

(ii) In particular, $S^{-1}R = 0$ when $\frac{1}{1} = \frac{0}{1}$, which occurs precisely when $0 \in S$.

- (iii) $\ker \iota_{S^{-1}R} = \{r \in R \mid \exists u \in S, ur = 0\}$.
- (iv) $\iota_{S^{-1}R}$ is injective if and only if S contains no zero divisors.
- (v) $\iota_{S^{-1}R}$ is always an epimorphism, but usually not surjective. For example, the map $\iota : \mathbb{Z} \rightarrow \mathbb{Q}$ is epic. Indeed, for $f, g : \mathbb{Q} \rightarrow A$ are such that $f \circ \iota = g \circ \iota$, then

$$f\left(\frac{p}{q}\right) = \frac{f(\iota(p))}{f(\iota(q))} = \frac{g(\iota(p))}{g(\iota(q))} = g\left(\frac{p}{q}\right)$$

Example. (i) Let $f \in R$ and define $S = \{f^n \mid n \geq 0\}$. Define $R_f = S^{-1}R$. Taking for instance $R = \mathbb{Z}$ and $f = 2$,

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

producing the ring of dyadic rational numbers. Since we write $\mathbb{Z}/n\mathbb{Z}$ for the finite quotient ring and \mathbb{Z}_2 for the 2-adic integers, we must use the notation $\mathbb{Z}\left[\frac{1}{2}\right]$ for this particular construction instead. Thus R_f is the zero ring if and only if f is nilpotent.

- (ii) Let $\mathfrak{p} \in \text{Spec } R$, where $\text{Spec } R$ is the set of prime ideals in R . Then $S = R \setminus \mathfrak{p}$ is a multiplicative set. Consider $(R \setminus \mathfrak{p})^{-1}R = R_{\mathfrak{p}}$. For example,

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

3.3 Functoriality

Proposition. Let M be an R -module and $S \subseteq R$ be a multiplicative set. Then there is an isomorphism of $S^{-1}R$ -modules

$$S^{-1}R \otimes_R M \rightarrow S^{-1}M$$

given by $\frac{r}{s} \otimes m \mapsto \frac{rm}{s}$.

Thus the localisation of any module can be reduced to a tensor product with the localisation of a ring.

Proof. Define the map $S^{-1}R \times M \rightarrow S^{-1}M$ mapping $\left(\frac{r}{s}, m\right) \mapsto \frac{rm}{s}$; this is bilinear and thus gives rise to an R -linear map $\varphi : S^{-1}R \otimes_R M \rightarrow S^{-1}M$ with the desired action on pure tensors. One can check that this is in fact $S^{-1}R$ -linear. Clearly φ is surjective by $\frac{1}{s} \otimes m \mapsto \frac{m}{s}$. For injectivity, we first show that every tensor

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

is pure. We define

$$s = \prod_i s_i; \quad t_j = \prod_{j \neq i} s_j$$

hence

$$\sum_i \frac{r_i}{s_i} \otimes m_i = \sum_i \frac{1}{s_i} \otimes r_i m_i = \sum_i \frac{t_i}{s} \otimes r_i m_i = \sum_i \frac{1}{s} \otimes t_i r_i m_i = \frac{1}{s} \otimes \sum_i t_i r_i m_i$$

as required. Now, it suffices to prove injectivity on pure tensors. If $\varphi\left(\frac{1}{s} \otimes m\right) = \frac{0}{1}$, then there exists $u \in S$ such that

$$u(1m - 0s) = 0 \implies um = 0$$

Thus

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

as required. \square

The map $S^{-1}R \otimes (-)$ acts on modules and on morphisms. The map $S^{-1}(-)$ acts on modules, and can be extended to act on morphisms in the following way. If $f : N \rightarrow N'$ is R -linear, we produce the commutative diagram

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

with action

$$\begin{array}{ccc} \frac{1}{s} \otimes n & \longmapsto & \frac{1}{s} \otimes f(n) \\ \uparrow & & \downarrow \\ \frac{n}{s} & \longmapsto & \frac{f(n)}{s} \end{array}$$

Then the functor $S^{-1}R \otimes_R (-)$ is naturally isomorphic to the functor $S^{-1}(-)$.

Remark. If A is an R -algebra, then we have an $S^{-1}R$ -linear isomorphism $S^{-1}R \otimes_R A \simeq S^{-1}A$; this is also an isomorphism of $S^{-1}R$ -algebras.

Lemma. Let M be an $S^{-1}R$ -module. Treating M as an R -module, we can define $S^{-1}M$. Then,

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

as $S^{-1}R$ -modules, mapping $\frac{m}{s} \mapsto \frac{1}{s}m$.

Equivalently, $M \simeq S^{-1}R \otimes_R M$ as $S^{-1}R$ -modules, mapping $m \mapsto \frac{1}{1} \otimes m$.

Proof. The localisation map $M \rightarrow S^{-1}M$ maps $m \mapsto \frac{m}{1}$. This is $S^{-1}R$ -linear, and surjective as $\frac{1}{s} \cdot m \mapsto \frac{m}{s}$. To show injectivity, note that $\frac{m}{1} = \frac{0}{1}$ implies there exists $u \in S$ with $um = 0$. Multiplying by $\frac{1}{u}$ as M is an $S^{-1}R$ -module we obtain $m = 0$ as required. \square

3.4 Universal property for modules

Recall that if U has multiplicative closure S ,

$$\text{Hom}_{\text{Ring}}(S^{-1}R, B) \simeq \{\varphi \in \text{Hom}_{\text{Ring}}(R, B) \mid \varphi(U) \subseteq B^\times\}$$

If M is a fixed R -module and L is an $S^{-1}R$ -module, we have

$$\mathrm{Hom}_R(M, L) \simeq \mathrm{Hom}_{S^{-1}R}(S^{-1}M, L)$$

Proposition. Let M be an R -module and L be an $S^{-1}R$ -module. Let $f : M \rightarrow L$ be R -linear. Then there exists a unique $S^{-1}R$ -linear map $h : S^{-1}M \rightarrow L$ such that $f = h \circ i_{S^{-1}M}$.

$$\begin{array}{ccc} M & \xrightarrow{i_{S^{-1}M}} & S^{-1}M \\ & \searrow f & \downarrow h \\ & & L \end{array}$$

As usual with universal properties, this characterises $S^{-1}M$ uniquely up to unique isomorphism.

Proof. We use the natural isomorphism between $S^{-1}(-)$ and $S^{-1}R \otimes_R (-)$. After applying this, we have a map

$$\iota : M \rightarrow S^{-1}R \otimes_R M; \quad m \mapsto \frac{1}{1} \otimes m$$

Let $f : M \rightarrow L$ be R -linear, and define

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

Note that $S^{-1}R \otimes_R L \simeq L$, so we can consider h as mapping to L , with action

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

Uniqueness of h follows from the fact that $\{1 \otimes m\}_{m \in M}$ generate $S^{-1}R \otimes_R M$ as an $S^{-1}R$ -module. \square

3.5 Exactness

Proposition. The functor $S^{-1}(-)$ is exact. More explicitly, 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. First,

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

so $\mathrm{im} S^{-1}f \subseteq \ker S^{-1}g$. Now suppose $\frac{b}{s} \in \ker S^{-1}g$, so $\frac{g(b)}{s} = \frac{0}{1}$. Hence there exists $u \in S$ such that $ug(b) = 0$. As g is R -linear and $u \in R$, we have $g(ub) = 0$. By exactness, $ub \in \ker g = \mathrm{im} f$. Thus there exists $a \in A$ such that $f(a) = ub$. Hence,

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

□

In particular, $S^{-1}R$ is a flat R -module, so for example \mathbb{Q} is a flat \mathbb{Z} -module.

Remark. Suppose $N \subseteq M$ are R -modules, and $\iota : N \rightarrow M$ is the inclusion map. Then applying the localisation, the map $S^{-1}\iota : S^{-1}N \rightarrow S^{-1}M$ given by $\frac{n}{s} \mapsto \frac{n}{s}$ is still injective. Note that the similar result for tensor products fails.

Proposition. Let M be an R -module and N, P be 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) $S^{-1}M/S^{-1}N \simeq S^{-1}(M/N)$ given by $\frac{m}{s} + S^{-1}N \mapsto \frac{m+N}{s}$.

Parts (i) and (ii) rely on a slight abuse of notation, thinking of $S^{-1}N$ as a submodule of $S^{-1}M$. Due to the above remark, this should not cause confusion.

Proof. *Part (i).* Note that

$$\frac{n+p}{s} = \frac{n}{s} + \frac{p}{s} \in S^{-1}N + S^{-1}P$$

and

$$\frac{n}{s_1} + \frac{p}{s_2} = \frac{s_2n + s_1p}{s_1s_2} \in S^{-1}(N + P)$$

Part (ii). The forward inclusion is clear. Conversely, suppose $x \in S^{-1}N \cap S^{-1}P$, so $x = \frac{n}{s_1} = \frac{p}{s_2}$. Hence, there exists $u \in S$ such that $us_2n = us_1p = w$. Note $us_2n \in N$ and $us_1p \in P$, so $w \in N \cap P$. Now,

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

Part (iii). Consider the short exact sequence

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

Applying the exact functor $S^{-1}(-)$, we obtain the short exact sequence

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

Thus

$$(S^{-1}\iota)(S^{-1}N) = S^{-1}N \subseteq S^{-1}M$$

and

$$(S^{-1}\pi)\left(\frac{m}{s}\right) = \frac{m+N}{s}$$

giving the isomorphism as required. □

Proposition. Let M, N be R -modules. Then

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

Proof. We have already proven that

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

giving the result as required. \square

Example. Let \mathfrak{p} be a prime ideal in R . Then by setting $S = R \setminus \mathfrak{p}$,

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

3.6 Extension and contraction of ideals

If $f : A \rightarrow B$ is a ring homomorphism and \mathfrak{b} is an ideal in B , the preimage $f^{-1}(\mathfrak{b}) = \mathfrak{b}^c$ is an ideal in A , called its *contraction*. If \mathfrak{a} is an ideal in A , we can generate an ideal $(f(\mathfrak{a})) = \mathfrak{a}^e$ in B , called its *extension*. We show on the first example sheet that for any ring homomorphism $f : A \rightarrow B$, there is a bijection

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

noting that the contracted ideals are those ideals with $\mathfrak{a} = \mathfrak{a}^{ec}$, and the extended ideals are those ideals with $\mathfrak{b} = \mathfrak{b}^{ce}$, where the bijection maps $\mathfrak{a} \mapsto \mathfrak{a}^e$ and $\mathfrak{b}^c \mapsto \mathfrak{b}$.

We now study the special case where $f : R \rightarrow S^{-1}R$ is the localisation map of a ring, given by $r \mapsto \frac{r}{1}$. In this case, the extension of an ideal is written $S^{-1}\mathfrak{a} = \mathfrak{a}^e$. We claim that

$$\mathfrak{a}^e = \left\{ \frac{a}{s} \mid a \in \mathfrak{a}, s \in S \right\}$$

Indeed, \mathfrak{a}^e is generated by $\left\{ \frac{a}{1} \mid a \in \mathfrak{a} \right\}$, so \mathfrak{a}^e must contain $\left\{ \frac{a}{s} \mid a \in \mathfrak{a}, s \in S \right\}$, but this is already an ideal. We also claim that

$$\mathfrak{a}^{ec} = \bigcup_{s \in S} (\mathfrak{a} : s); \quad (\mathfrak{a} : s) = \{r \in R \mid rs \in \mathfrak{a}\}$$

Indeed, for $r \in \bigcup_{s \in S} (\mathfrak{a} : s)$, we have $rs = a$ in R for some $s \in S$ and $a \in \mathfrak{a}$, so $\frac{rs}{1} = \frac{a}{1}$, giving $\frac{r}{1} = \frac{a}{s}$, so $r \in \mathfrak{a}^e$ as required. In the other direction, if $r \in \mathfrak{a}^e$, then $\frac{r}{1} = \frac{a}{s}$ for some $s \in S$ and $a \in \mathfrak{a}$, so there exists $u \in S$ such that $rus = ua \in \mathfrak{a}$, so $r \in (\mathfrak{a} : us)$ as required.

Now, let \mathfrak{b} be an ideal of $S^{-1}R$. Then

$$\mathfrak{b}^c = \left\{ r \in R \mid \frac{r}{1} \in \mathfrak{b} \right\}$$

We claim that $\mathfrak{b}^{ce} = \mathfrak{b}$, so all ideals in $S^{-1}R$ are extended. Note that the inclusion $\mathfrak{b}^{ce} \subseteq \mathfrak{b}$ holds for any pair of rings. For the reverse inclusion, consider $\frac{r}{s} \in \mathfrak{b}$, so $\frac{r}{1} \in \mathfrak{b}$. Hence $r \in \mathfrak{b}^c$, so $\frac{r}{1} \in \mathfrak{b}^{ce}$, thus $\frac{r}{s} \in \mathfrak{b}^{ce}$ as \mathfrak{b}^{ce} is an ideal in $S^{-1}R$.

Proposition. Consider the localisation map $R \rightarrow S^{-1}R$ given by $r \mapsto \frac{r}{1}$.

- (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.
- (iii) $\mathfrak{a}^e = S^{-1}\mathfrak{a}$ if and only if $\mathfrak{a} \cap S \neq \emptyset$.
- (iv) There is a bijection

$$\{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \cap S = \emptyset\} \leftrightarrow \text{Spec } S^{-1}R$$

given by $\mathfrak{p} \mapsto \mathfrak{p}^e, \mathfrak{q}^c \leftarrow \mathfrak{q}$.

Proof. Part (i). Follows from the fact that $\mathfrak{b}^{ce} = \mathfrak{b}$ for all ideals \mathfrak{b} in $S^{-1}R$.

Part (ii). \mathfrak{a} is contracted if and only if $\mathfrak{a}^{ec} \subseteq \mathfrak{a}$, because the reverse inclusion always holds. This happens if and only if

$$\bigcup_{s \in S} (\mathfrak{a} : s) \subseteq \mathfrak{a}$$

which occurs if and only if

$$\forall r \in R, (Sr \cap \mathfrak{a} \neq \emptyset \implies r \in \mathfrak{a})$$

$$\forall r \in R, (0 + \mathfrak{a} \in S(r + \mathfrak{a}) \implies r + \mathfrak{a} = 0 + \mathfrak{a})$$

which in turn occurs if and only if the image of S in R/\mathfrak{a} contains no zero divisors.

Part (iii). Suppose $\mathfrak{a} \cap S \neq \emptyset$, so let $x \in \mathfrak{a} \cap S$. Then $\frac{x}{x} \in \mathfrak{a}^e$, so $\mathfrak{a}^e = (1) = S^{-1}R$. Conversely, if $\mathfrak{a}^e = S^{-1}R$, then $\frac{1}{1} \in \mathfrak{a}^e$, so $\frac{1}{1} = \frac{a}{s}$ for some $a \in \mathfrak{a}, s \in S$. Therefore there exists $u \in S$ such that $us = ua \in S \cap \mathfrak{a}$.

Part (iv). Consider the contraction map $\text{Spec } S^{-1}R \rightarrow \{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \cap S = \emptyset\}$ given by $\mathfrak{q} \mapsto \mathfrak{q}^c$. We show this is well-defined. In general, a contraction of a prime ideal is always prime. Further, $\mathfrak{p} \in \text{Spec } R$ is contracted if and only if the image of S in R/\mathfrak{p} contains no zero divisors, but R/\mathfrak{p} is an integral domain, so its only zero divisor is zero itself. So this condition is equivalent to the condition $\mathfrak{p} \cap S = \emptyset$. In particular, $\{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \cap S = \emptyset\}$ is precisely the set of contracted prime ideals of R . The map is injective, since if $\mathfrak{q} \in \text{Spec } S^{-1}R$, then $\mathfrak{q}^{ce} = \mathfrak{q}$.

In the other direction, for $\mathfrak{p} \in \text{Spec } R$ such that $\mathfrak{p} \cap S = \emptyset$, it must be contracted, so $\mathfrak{p}^{ec} = \mathfrak{p}$. It therefore remains to show that \mathfrak{p}^e is a prime ideal. We want to show that $S^{-1}R/\mathfrak{p}^e$ is an integral domain. We have that $\mathfrak{p}^e \neq S^{-1}R$ by (iii), so $S^{-1}R/\mathfrak{p}^e$ is not the zero ring, so it suffices to show that this quotient has no zero divisors. To show this, we embed $S^{-1}R/\mathfrak{p}^e$ in the field $FF(R/\mathfrak{p})$.

Consider the composite map

$$R \rightarrow R/\mathfrak{p} \rightarrow FF(R/\mathfrak{p})$$

which is a surjection followed by an injection. This has the property that all elements of S are mapped to units, because $S \cap \mathfrak{p} = \emptyset$. By the universal property of the localisation, we have a map

$$\varphi : S^{-1}R \rightarrow FF(R/\mathfrak{p}); \quad \frac{r}{s} \mapsto \frac{r + \mathfrak{p}}{s + \mathfrak{p}}$$

It suffices to show that $\ker \varphi = \mathfrak{p}^e$, then the result holds by the isomorphism theorem. Let $\frac{r}{s} \in \ker \varphi$, so $\frac{r + \mathfrak{p}}{s + \mathfrak{p}} = \frac{0}{1}$ in $FF(R/\mathfrak{p})$. Observe that $\text{im } \varphi \subseteq \overline{S}^{-1}(R/\mathfrak{p})$, where \overline{S} is the image of S in R/\mathfrak{p} . Restricting the range, we can consider φ as a map from $S^{-1}R$ to $\overline{S}^{-1}(R/\mathfrak{p})$. So $\varphi\left(\frac{r}{s}\right) = \frac{0}{1}$ implies that there exists $u + \mathfrak{p} \in \overline{S}$ such that $(u + \mathfrak{p})(r + \mathfrak{p}) = 0$, so $ur + \mathfrak{p} = 0$. In particular, $u \in S$ and $ur \in \mathfrak{p}$. Hence $\frac{r}{s} = \frac{ur}{us}$ where $ur \in \mathfrak{p}$ and $us \in S$, so $\frac{r}{s} \in \mathfrak{p}^e$.

For the other direction, take $x \in \mathfrak{p}^e$, so $x = \frac{p}{s}$ for $p \in \mathfrak{p}, s \in S$. Then $\varphi(x) = \frac{p + \mathfrak{p}}{s + \mathfrak{p}} = 0$, so $x \in \ker \varphi$. \square

It is not true in general that the extensions of prime ideals are prime.

Definition. If I is an ideal in R , the *radical* of I is the ideal

$$\sqrt{I} = \{r \in R \mid \exists n \geq 1, r^n \in I\}$$

Proposition. Let I be an ideal in a ring R . Then

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p} \in \text{Spec } R} \mathfrak{p}$$

Proof. Let $x \in \sqrt{I}$. Then $x^n \in I$ for some $n \geq 1$. For every $\mathfrak{p} \in \text{Spec } R$, if $I \subseteq \mathfrak{p}$, then $x^n \in \mathfrak{p}$, so $x \in \mathfrak{p}$. Conversely, suppose $x^n \notin I$ for all $n \geq 1$. As $I \neq R$, we have $R/I \neq 0$. Let \bar{x} be the image of x in R/I , and consider

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

This is not the zero ring, because $x^n \notin I$ for all $n \geq 1$. Therefore, $(R/I)_{\bar{x}}$ has a prime ideal, as it contains a maximal ideal. By the bijection described in part (iv) of the previous result, this prime ideal corresponds to a prime ideal of R/I that avoids \bar{x} . This in turn corresponds to a prime ideal $\mathfrak{p} \in \text{Spec } R$ that contains I and avoids x . Hence $x \notin \bigcap_{I \subseteq \mathfrak{p} \in \text{Spec } R} \mathfrak{p}$. \square

3.7 Local properties

Definition. A ring R is *local* if it has exactly one maximal ideal.

We write $\text{mSpec } R$ for the set of maximal ideals of R .

Example. Let $\mathfrak{p} \in \text{Spec } R$. Then there is a bijection between the prime ideals of R contained within \mathfrak{p} to $\text{Spec } R_{\mathfrak{p}}$, mapping $\mathfrak{n} \mapsto \mathfrak{n}R_{\mathfrak{p}}$ and $\mathfrak{q}^c \mapsto \mathfrak{q}$. Hence, all prime ideals of $R_{\mathfrak{p}}$ are contained in $\mathfrak{p}^e = \mathfrak{p}R_{\mathfrak{p}}$. Thus $(R_{\mathfrak{p}}, \mathfrak{p}R_{\mathfrak{p}})$ is a local ring.

Example. Recall that

$$\mathbb{Z}_{(2)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, 2 \nmid b \right\}$$

This ring is local, and the unique maximal ideal is

$$(2)\mathbb{Z}_{(2)} = \left\{ \frac{2a}{b} \mid a, b \in \mathbb{Z}, 2 \nmid b \right\}$$

Proposition. Let M be an R -module. The following are equivalent.

- (i) M is the zero module;
- (ii) $M_{\mathfrak{p}}$ is the zero module for all prime ideals $\mathfrak{p} \in \text{Spec } R$;
- (iii) $M_{\mathfrak{m}}$ is the zero module for all maximal ideals $\mathfrak{m} \in \text{mSpec } R$.

Informally, for modules, being zero is a local property.

Proof. First, note that (i) implies (ii) and (ii) implies (iii). We show that (iii) implies (i). Suppose that M is not the zero module, so let $m \in M$ be a nonzero element. Consider $\text{Ann}_R(m) = \{r \in R \mid rm = 0\}$. This is an ideal of R , but is a proper ideal because $1 \notin \text{Ann}_R(m)$. Let \mathfrak{m} be a maximal ideal of R containing $\text{Ann}_R(m)$. Now, $\frac{m}{1} \in M_{\mathfrak{m}} = 0$. Thus, $\frac{m}{1} = \frac{0}{1}$, so $um = 0$ for some $u \in R \setminus \mathfrak{m}$. But then $u \notin \text{Ann}_R(m)$, giving a contradiction. \square

Proposition. Let $f : M \rightarrow N$ be an R -linear map. The following are equivalent.

- (i) f is injective;
- (ii) $f_{\mathfrak{p}} : M_{\mathfrak{p}} \rightarrow N_{\mathfrak{p}}$ is injective for every prime ideal $\mathfrak{p} \in \text{Spec } R$;
- (iii) $f_{\mathfrak{m}} : M_{\mathfrak{m}} \rightarrow N_{\mathfrak{m}}$ is injective for every maximal ideal $\mathfrak{m} \in \text{mSpec } R$.

The same result holds for surjectivity.

Proof. The fact that (i) implies (ii) follows directly from the fact that localisation at \mathfrak{p} is an exact functor. Clearly (ii) implies (iii). Suppose that $f_{\mathfrak{m}}$ is injective for each $\mathfrak{m} \in \text{mSpec } R$. We have the following exact sequence.

$$0 \longrightarrow \ker f \longrightarrow M \xrightarrow{f} N$$

As $(-)_{\mathfrak{p}}$ is exact, the sequence

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

is exact. But by assumption, $(\ker f)_{\mathfrak{m}} = \ker(f_{\mathfrak{m}}) = 0$. So $(\ker f)_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \in \text{mSpec } R$, so $\ker f = 0$. \square

Proposition. Let M be an R -module. The following are equivalent.

- (i) M is a flat R -module;
- (ii) $M_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$ -module for every prime ideal $\mathfrak{p} \in \text{Spec } R$;
- (iii) $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$ -module for every maximal ideal $\mathfrak{m} \in \text{mSpec } R$.

Proof. (i) implies (ii). Note that $M_{\mathfrak{p}} \simeq R_{\mathfrak{p}} \otimes_R M$ as $R_{\mathfrak{p}}$ -modules, by extension of scalars. Since extension of scalars preserves flatness, $M_{\mathfrak{p}}$ is flat.

Clearly (ii) implies (iii).

(iii) implies (i). Let $f : N \rightarrow P$ be an R -linear injective map. Let $\mathfrak{m} \in \text{mSpec } R$. Then $f_{\mathfrak{m}} : N_{\mathfrak{m}} \rightarrow P_{\mathfrak{m}}$ is injective by the previous proposition. Note that the following diagram commutes.

$$\begin{array}{ccc} N_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} & \xrightarrow{f_{\mathfrak{m}} \otimes \text{id}_{M_{\mathfrak{m}}}} & P_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} \\ \sim \downarrow & & \downarrow \sim \\ (N \otimes_R M)_{\mathfrak{m}} & \xrightarrow{(f \otimes \text{id}_M)_{\mathfrak{m}}} & (P \otimes_R M)_{\mathfrak{m}} \end{array}$$

Hence $(f \otimes \text{id}_M)_{\mathfrak{m}}$ is injective. Since this holds for each $\mathfrak{m} \in \text{mSpec } R$, the map $f \otimes \text{id}_M$ must be injective, as required. \square

Example. An R -module M is *locally free* if $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ -module for every prime ideal $\mathfrak{p} \in \text{Spec } R$. Consider $R = \mathbb{C} \otimes \mathbb{C}$. Then

$$\text{Spec } R = \{\mathfrak{p} \times \mathbb{C} \mid \mathfrak{p} \in \text{Spec } \mathbb{C}\} \cup \{\mathbb{C} \times \mathfrak{p} \mid \mathfrak{p} \in \text{Spec } \mathbb{C}\} = \{\mathbb{C} \times (0), (0) \times \mathbb{C}\}$$

The map $\mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$ given by $(a, b) \mapsto b$ sends $(\mathbb{C} \times \mathbb{C}) \setminus \mathbb{C} \times (0)$ to units. Thus, by the universal property of the localisation, we have a map

$$(\mathbb{C} \times \mathbb{C})_{\mathbb{C} \times (0)} \rightarrow \mathbb{C}; \quad \frac{(a, b)}{(c, d)} \mapsto \frac{b}{d}$$

This is clearly surjective, and one can check that this is also injective. Thus $(\mathbb{C} \times \mathbb{C})_{\mathbb{C} \times (0)} \simeq \mathbb{C}$ is a field. Similarly, $(\mathbb{C} \times \mathbb{C})_{(0) \times \mathbb{C}}$ is a field. So for every $\mathbb{C} \times \mathbb{C}$ -module M and prime ideal $\mathfrak{p} \in \text{Spec}(\mathbb{C} \times \mathbb{C})$, the module $M_{\mathfrak{p}}$ is a \mathbb{C} -vector space, so is free. Thus every module over $\mathbb{C} \times \mathbb{C}$ is locally free, but not every module over $\mathbb{C} \times \mathbb{C}$ is free. For example, take $M = \mathbb{C} \times \{0\}$ as a $\mathbb{C} \times \mathbb{C}$ -module. One can show that M is not the zero module, and not free of rank at least 1, so cannot be free.

3.8 Localisations as quotients

Let $U \subseteq R$, and let $S \subseteq R$ be its multiplicative closure. We can define

$$R_U = R[\{T_u\}_{u \in U}] / I_U; \quad I_U = (\{uT_u - 1\}_{u \in U})$$

We claim that $R_U = S^{-1}R$ as rings, and also as R -algebras. Writing \bar{u} and \bar{T}_u to be the images of these elements in R_U , the isomorphism maps

$$\bar{T}_u \mapsto \frac{1}{u}; \quad rT_{u_1} \dots T_{u_\ell} + I_U \mapsto \frac{r}{u_1 \dots u_\ell}$$

This is because R_U has the universal property of $S^{-1}R$. Indeed, for any $f : R \rightarrow A$ mapping U to units, there is a unique h making the following diagram commute.

$$\begin{array}{ccc} R & \longrightarrow & R_U \\ & \searrow f & \downarrow h \\ & & A \end{array}$$

Note that A is an R -algebra via f , so the diagram commutes if and only if h is an R -algebra homomorphism. We have

$$\text{Hom}_{R\text{-algebra}}(R_U, A) \simeq \{\varphi : U \rightarrow A \mid f(u)\varphi(u) = 1\}$$

But the the right hand side is a singleton.

Example. Let $x \in R$, and consider $R_x = R_{\{1, x, x^2, \dots\}}$. Here,

$$R_x \simeq R[T] / (xT - 1)$$

4 Integrality, finiteness, and finite generation

4.1 Nakayama's lemma

Proposition (Cayley–Hamilton theorem). Let M be a finitely generated R -module, and let $f : M \rightarrow M$ be an R -linear endomorphism. Let \mathfrak{a} be an ideal in R such that $f(M) \subseteq \mathfrak{a}M$. Then, we have an equality in $\text{End}_R M$

$$f^n + a_1 f^{n-1} + \cdots + a_n f^0 = 0; \quad f^r = \underbrace{f \circ \cdots \circ f}_{r \text{ times}}$$

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

Proof. Let $M = \text{span}_R \{m_1, \dots, m_n\}$, so $\mathfrak{a}M = \text{span}_{\mathfrak{a}} \{m_1, \dots, m_n\}$. Then

$$\begin{pmatrix} f(m_1) \\ \vdots \\ f(m_n) \end{pmatrix} = P \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix}; \quad P \in M_{n \times n}(\mathfrak{a})$$

Let $\rho : R \rightarrow \text{End } M$ be the structure ring homomorphism of M as an R -module. Then we can define $R[T] \rightarrow \text{End } M$ by $T \mapsto f$, making M into an $R[T]$ -module. Hence,

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

Thus

$$Q \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0; \quad Q = TI_n - P$$

Multiplying by the adjugate matrix $\text{adj } Q$ on the left on both sides,

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

In particular, $(\det Q)m = 0$ for all $m \in M$, as the m_i generate M . Hence, $m \mapsto (\det Q)m = (\det Q)|_{T=f}$ is 0 in $\text{End}_R M$. Finally, note that $\det Q$ is a monic polynomial, and all other coefficients lie in \mathfrak{a} . \square

Corollary. Let M be a finitely generated R -module, and let \mathfrak{a} be an ideal in R . If $\mathfrak{a}M = M$, then there exists $a \in \mathfrak{a}$ such that $am = m$ for all $m \in M$.

Proof. Apply the Cayley–Hamilton theorem with $f = \text{id}_M$. We obtain a polynomial

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

Take $a = -(a_1 + \cdots + a_n)$. \square

Definition. The *Jacobson radical* of a ring R , denoted $J(R)$, is the intersection of all maximal ideals of R .

Example. (i) If (R, \mathfrak{m}) is a local ring, then $J(R) = \mathfrak{m}$.

(ii) $J(\mathbb{Z}) = \{0\}$.

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

Proof. First, let $x \in J(R)$, and suppose $y \in R$ is such that $1 - xy$ is not a unit. Then $(1 - xy)$ is a proper ideal, so it is contained in a maximal ideal \mathfrak{m} . But as $x \in J(R)$, we must have $x \in \mathfrak{m}$, giving $1 = 1 - xy + xy \in \mathfrak{m}$, contradicting that \mathfrak{m} is a maximal ideal.

Now suppose $x \notin J(R)$, so there is a maximal ideal \mathfrak{m} such that $x \notin \mathfrak{m}$. Then $\mathfrak{m} + (x) = R$ as \mathfrak{m} is maximal. In particular, there exists $t \in \mathfrak{m}$ and $y \in R$ such that $t + xy = 1$, or equivalently, $1 - xy = t \in \mathfrak{m}$. Note that t cannot be a unit, because it is contained in a proper ideal. \square

Proposition (Nakayama's lemma). Let M be a finitely generated R -module, and let $\mathfrak{a} \subseteq J(R)$ be an ideal of R such that $\mathfrak{a}M = M$. Then $M = 0$.

This lemma is more useful when $J(R)$ is large, so is particularly useful when applied to local rings.

Proof. By the above corollary, there exists $a \in \mathfrak{a}$ such that $am = m$ for all $m \in M$, or equivalently, $(1 - a)m = 0$. By assumption, $a \in J(R)$, so $1 - a$ is a unit in R . Hence $m = 0$. \square

Corollary. Let M be a finitely generated R -module, and let $N \subseteq M$ be a submodule. Let $\mathfrak{a} \subseteq J(R)$ be an ideal in R such that $N + \mathfrak{a}M = M$. Then $N = M$.

This can be applied to find generating sets for M .

Proof. Note that

$$\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N = M/N$$

so $M/N = 0$ by Nakayama's lemma. \square

4.2 Integral and finite extensions

Definition. Let A be an R -algebra, and let $x \in A$. Then x is *integral over R* if there exists a monic polynomial $f \in R[T]$ such that $f(x) = 0$.

Example. (i) If $R = k$ is a field, then x is integral over k if and only if x is algebraic over k .

(ii) We will prove later that

- (a) the \mathbb{Z} -integral elements of \mathbb{Q} are \mathbb{Z} ;
- (b) the \mathbb{Z} -integral elements of $\mathbb{Q}[\sqrt{2}]$ are $\mathbb{Z}[\sqrt{2}]$;
- (c) the \mathbb{Z} -integral elements of $\mathbb{Q}[\sqrt{5}]$ are $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right] \not\cong \mathbb{Z}[\sqrt{5}]$.

Definition. Let M be an R -module. We say that M is *faithful* if the structure homomorphism $\rho : R \rightarrow \text{End } M$ is injective. Equivalently, for every nonzero ring element r , there exists

$m \in M$ such that $rm \neq 0$.

Example. Let $R \subseteq A$ be rings, and let A be an R -module in the natural way. Then A is a faithful R -module, as if $r \neq 0$, then $r1_A = r \neq 0$.

Proposition. Let $R \subseteq A$ be rings and $x \in A$, and consider A as an $R[x]$ -module. Then x is integral over R if and only if there exists $M \subseteq A$ such that

- (i) M is a faithful $R[x]$ -module; and
- (ii) M is finitely generated as an R -module.

Condition (i) is that M is an R -submodule of A , $xM \subseteq M$, and M is faithful over $R[x]$.

Proof. First, assume conditions (i) and (ii) hold. We have an R -linear map $f : M \rightarrow M$ given by multiplication by x , as $xM \subseteq M$. As M is a finitely generated R -module, we can apply the Cayley-Hamilton theorem to find

$$f^n + r_1 f^{n-1} + \dots + r_n f^0 = 0; \quad r_i \in R$$

in $\text{End}_R M$. Then, evaluating at $m \in M$,

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

As this holds for all m , and M is a faithful $R[x]$ -module, we must have

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

Thus x is integral over R .

Now suppose x is integral over R . Then

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

for some $r_1, \dots, r_n \in R$. We define

$$M = \text{span}_R \{x^0, \dots, x^{n-1}\}$$

This is finitely generated, and satisfies $xM \subseteq M$. M is faithful over $R[x]$ as it contains $x^0 = 1$. □

Definition. Let A be an R -algebra. Then A is

- (i) *integral* over R , if all of its elements are integral over R ;
- (ii) *finite* over R , if A is finitely generated as an R -module.

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

- (i) A is a finitely generated R -algebra and is integral over R ;
- (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). The generators for A are integral.

(ii) implies (iii). Suppose A is generated by $\alpha_1, \dots, \alpha_m$ as an R -algebra, and the α_i are integral over R . As α_i is integral,

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

Hence $\alpha_i^{n_i}$ lies in the R -linear span of $\{\alpha_i^0, \dots, \alpha_i^{n_i-1}\}$. Thus, every element is an R -linear combination of products of the form $\alpha_1^{e_1} \dots \alpha_n^{e_n}$, which in turn lies in the R -linear span of products of the same form where all e_i are less than the corresponding n_i . This is a finite set, so A is finitely generated as an R -module.

(iii) implies (i). As A is finitely generated as an R -module, it must be finitely generated as an R -algebra. Let $\alpha \in A$; we show α is integral over R . Let $\rho : R \rightarrow A$ be the structure homomorphism of A as an R -algebra. Then $\rho(R) \subseteq A$, and consider $(\rho(R))[\alpha] \subseteq A$. Now, A is a $(\rho(R))[\alpha]$ -module, and is faithful because $1_A \in A$. As A is a finitely generated $\rho(R)$ -module, the previous proposition shows that α is $\rho(R)$ -integral. Equivalently, α is R -integral. \square

Proposition. Let A be an R -algebra and let \mathcal{O} be the set of elements of A that are integral over R . Then \mathcal{O} is an R -subalgebra of A .

Proof. Let $x, y \in \mathcal{O}$. Then $\{x, y\}$ is a finite set of R -integral elements, so the set generates an integral R -subalgebra of A . Hence $x + y, xy$ lie in this subalgebra, and so they are integral. \square

Proposition. Let $A \subseteq B \subseteq C$ be rings. Then,

- (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 and B is integral over A , then C is integral over A .

Proof. Part (i). Suppose that

$$C = \text{span}_B \{\gamma_1, \dots, \gamma_n\}; \quad B = \text{span}_A \{\beta_1, \dots, \beta_\ell\}$$

Then

$$C = \text{span}_A \{\gamma_i \beta_j \mid i \leq n, j \leq \ell\}$$

Part (ii). Let $c \in C$, so $f(c) = 0$ for

$$f(T) = T^n + b_1 T^{n-1} + \dots + b_n T^0 \in B[T]$$

Then $f \in A'[T]$, where $A' = A[b_1, \dots, b_n]$. The inclusion $A \subseteq A'$ is generated as an A -algebra by finitely many integral elements. Similarly, $A' \subseteq A'[c]$ is generated as an A -algebra by c , which is integral over A' as $f \in A'[T]$. By the previous result, both extensions are finite. Then, by part (i), $A \subseteq A'[c]$ is finite, so c is integral over A . \square

4.3 Integral closure

Definition. Let $A \subseteq B$ be rings. The *integral closure* of A in B is the set \bar{A} of elements of B that are integral over A , which is an A -algebra. We say that A is *integrally closed* in B if $\bar{A} = A$.

Definition. Let A be an integral domain. In this case, the *integral closure* of A is the integral closure of A in its field of fractions $FF(A)$. We say that A is *integrally closed* if it is integrally closed in its field of fractions.

Example. (i) $\mathbb{Z}[\sqrt{5}]$ is not integrally closed, because $\alpha = \frac{1+\sqrt{5}}{2} \in FF(\mathbb{Z}[\sqrt{5}]) = \mathbb{Q}[\sqrt{5}]$, and $\alpha^2 - \alpha - 1 = 0$ so it is $\mathbb{Z}[\sqrt{5}]$ -integral.

(ii) \mathbb{Z} is integrally closed.

(iii) If k is a field, $k[T_1, \dots, T_n]$ is integrally closed.

Examples (ii) and (iii) are special cases of the following result.

Proposition. Let A be a unique factorisation domain. Then A is integrally closed.

Proof. Let $x \in FF(A) \setminus A$, and write $x = \frac{a}{b}$ with $a \in A, b \in A \setminus \{0\}$. As A is a unique factorisation domain, we can assume there is a prime p such that $p \mid b$ and $p \nmid a$. If x is integral over A , then

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

Multiplying by b^n ,

$$a^n = -b(a_1b_0a^{n-1} + \dots + a_nb^{n-1}a^0)$$

But as $p \mid b$, we must have $p \mid a^n$, so $p \mid a$, which is a contradiction. \square

Lemma. Let $A \subseteq B$ be rings, and let \bar{A} be the integral closure of A in B . Then \bar{A} is integrally closed in B .

Taking the integral closure is an idempotent operation.

Proof. Let $x \in B$ be integral over \bar{A} . Then, we have

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

The first extension is integral by definition, and the second is integral by the above proposition, as x is integral over \bar{A} . By transitivity of integrality, $\bar{A}[x]$ is integral over A , so in particular, x is integral over A . Thus $x \in \bar{A}$. \square

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

(i) if B is integral over A and \mathfrak{b} is an ideal in B , then B/\mathfrak{b} is integral over $A/\mathfrak{b}c$;

- (ii) if B is integral over A and $S \subseteq A$ is a multiplicative set, then $S^{-1}B$ is integral over $S^{-1}A$;
- (iii) if \bar{A} is the integral closure of A in B and $S \subseteq A$ is a multiplicative set, then $S^{-1}\bar{A}$ is the integral closure of $S^{-1}A$ in $S^{-1}B$, so $\overline{S^{-1}A} = S^{-1}\bar{A}$.

The proofs follow directly from the definitions.

Lemma. Let $A \subseteq B$ be an integral extension of rings. Then

- (i) $A \cap B^\times = A^\times$;
- (ii) if A, B are integral domains, then A is a field if and only if B is a field.

Proof. Part (i). One inclusion is clear: $A^\times \subseteq A \cap B^\times$. Suppose $a \in A$ and a is a unit in B with inverse $b \in B$; we show that $b \in A$. As b is integral over A ,

$$b^n + a_1 b^{n-1} + \dots + a_n b^0 = 0; \quad a_i \in A$$

Multiplying by a^{n-1} ,

$$b + \underbrace{a_1 + a_2 a^1 + \dots + a_n a^{n-1}}_{\in A} = 0$$

Hence b must lie in A .

Part (ii). Suppose B is a field. Then

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

Hence A is a field. Conversely, suppose A is a field. Let $b \in B$ be a nonzero element; we want to show that b is a unit in B . As b is integral over A ,

$$b^n + a_1 b^{n-1} + \dots + a_n b^0 = 0; \quad a_i \in A$$

Let n be minimal with this property. Then

$$b \underbrace{(b^{n-1} + a_1 b^{n-2} + \dots + a_{n-1} b^0)}_{\Delta} = -a_n$$

Note that $b \neq 0$ by assumption, and $\Delta \neq 0$ by minimality. As B is an integral domain, $a_n \neq 0$. Because A is a field, a_n is invertible. Thus

$$b(-a_n^{-1}\Delta) = 1 \implies b \in B^\times$$

□

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

Proof. We have an embedding of rings

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

which is an integral extension of integral domains. By the previous result, one is a field if and only if the other is, so $\mathfrak{q} \cap A$ is maximal in A if and only if \mathfrak{q} is maximal in B . □

4.4 Noether normalisation

Definition. Let A be a k -algebra, and let $x_1, \dots, x_n \in A$. We say that x_1, \dots, x_n are *k -algebraically independent* if for every nonzero polynomial $p \in k[T_1, \dots, T_n]$, we have $p(x_1, \dots, x_n) \neq 0$. Equivalently, the k -algebra homomorphism $k[T_1, \dots, T_n] \rightarrow A$ given by $T_i \mapsto x_i$ is injective.

Theorem (Noether's normalisation theorem). Let k be a field, and let $A \neq 0$ be a finitely generated k -algebra. Then there exist $x_1, \dots, x_n \in A$ which are k -algebraically independent and A is finite over $A' = k[x_1, \dots, x_n]$.

We first present an example of the method used in the proof.

Example. Let $A = k[T, T^{-1}] \simeq k[X, Y]_{(XY-1)}$. We claim that $k[T] \subseteq k[T, T^{-1}]$ is not a finite extension. Indeed, suppose it were finite. Then T^{-1} would be integral over $k[T]$, so

$$(T^{-1})^n \in \text{span}_{k[T]} \{(T^{-1})^0, \dots, (T^{-1})^{n-1}\}$$

Multiplying by T^n , we have

$$1 \in \text{span}_{k[T]}(T^n, \dots, T)$$

which is false. However, if $c \in k$ is a scalar which we will choose later,

$$A = k[T, T^{-1}] = k[T, T^{-1} - cT]$$

We claim that $k[T^{-1} - cT] \subseteq A$ is a finite extension for most values of c , and in particular, for at least one. First, note $T^{-1}T - 1 = 0$, and then change variables to

$$((T^{-1} - cT) + cT)T - 1 = 0 \implies \underbrace{c}_{\in k} T^2 + \underbrace{(T^{-1} - cT)}_{\in k[T^{-1} - cT]} T - \underbrace{1}_{\in k[T^{-1} - cT]} = 0$$

Hence if $c \neq 0$, T is integral over $k[T^{-1} - cT]$.

Proof. In this proof, we will assume k is infinite, although the theorem is true even if k is finite. We will proceed by induction on the minimal number of generators of A as a k -algebra, which we will denote m . For the case $m = 0$, we have $A = k$, so we can take $A' = k$.

Suppose that A is generated as a k -algebra by $x_1, \dots, x_m \in A$. If x_1, \dots, x_m are algebraically independent, then we can take $A' = A$. Otherwise, we claim that there are $c_1, \dots, c_{m-1} \in k$ such that x_m is integral over

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

Assuming that this holds, we have $A = B[x_m]$, so $B \subseteq A$ is a finite extension. But B is generated by $m - 1$ elements, so by induction B contains $z_1, \dots, z_n \in B$ which are k -algebraically independent, and B is finite over $A' = k[z_1, \dots, z_n]$. Then A is finite over A' by transitivity of finiteness.

We now prove the claim. As x_1, \dots, x_m are not algebraically independent over k , there is a nonzero polynomial $f \in k[T_1, \dots, T_m]$ such that $f(x_1, \dots, x_m) = 0$. We want to show that x_m is integral over B . Write f as the sum of its homogeneous parts, and let F be the part of highest degree $\deg f = r$. For scalars $c_1, \dots, c_{m-1} \in k$ which will be chosen later, we define

$$\begin{aligned} g(T_1, \dots, T_m) &= f(T_1 + c_1 T_m, \dots, T_{m-1} + c_{m-1} T_m, T_m) \\ &= \underbrace{F(c_1, \dots, c_{m-1}, 1)}_{\in k} T_m^r + \text{terms of lower degree in } T_m \text{ with coefficients in } k[T_1, \dots, T_{m-1}] \end{aligned}$$

Note that

$$g(x_1 - c_1 x_m, \dots, x_{m-1} - c_{m-1} x_m, x_m) = f(x_1, \dots, x_m) = 0$$

but as a polynomial in T_m over $k[T_1, \dots, T_{m-1}]$, it has degree at most r , and the coefficient of T_m^r is $F(c_1, \dots, c_m, 1)$. As $F(T_1, \dots, T_m)$ is a nonzero homogeneous polynomial, $F(T_1, \dots, T_{m-1}, 1)$ is not the zero polynomial. Thus there are c_1, \dots, c_{m-1} such that $F(c_1, \dots, c_{m-1}, 1) \neq 0$ as k is an infinite field. \square

4.5 Hilbert's Nullstellensatz

Proposition (Zariski's lemma). Let $k \subseteq L$ be fields where L is finitely generated as a k -algebra. Then $\dim_k L$ is finite.

Proof. By Noether normalisation, we have

$$k \subseteq k[x_1, \dots, x_n] \subseteq L$$

where x_1, \dots, x_n are algebraically independent over k , and L is finite over $k[x_1, \dots, x_n]$. As this is an integral extension of integral domains and L is a field, $k[x_1, \dots, x_n]$ must be a field. But as $k[x_1, \dots, x_n]$ is a polynomial algebra over k , the x_i cannot be invertible. Hence $n = 0$, so $k \subseteq L$ is finite as required. \square

Definition. Let $k \subseteq \Omega$ be an extension of fields, where Ω is algebraically closed.

(i) Let $S \subseteq k[T_1, \dots, T_n]$. We define

$$\mathbb{V}(S) = \{\mathbf{x} \in \Omega^n \mid \forall f \in S, f(\mathbf{x}) = 0\}$$

Sets of this form are called k -algebraic subsets of Ω^n .

(ii) Let $X \subseteq \Omega^n$. We define

$$I(X) = \{f \in k[T_1, \dots, T_n] \mid \forall \mathbf{x} \in X, f(\mathbf{x}) = 0\}$$

Note that $\mathbb{V}(S) = \mathbb{V}(I)$, where I is the ideal generated by S . Recall that for every finite field extension $k \subseteq L$, there is a k -algebra embedding $L \rightarrow \Omega$, because Ω is algebraically closed.

Theorem. Let $\mathfrak{a} \subseteq k[T_1, \dots, T_n]$ be an ideal. Then

(i) (weak Nullstellensatz) $\mathbb{V}(\mathfrak{a}) = \emptyset$ if and only if $1 \in \mathfrak{a}$;

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

Proof. Weak Nullstellensatz. Clearly if $1 \in \mathfrak{a}$ then $\mathbb{V}(\mathfrak{a}) = \emptyset$, as $1 \neq 0$. Now suppose $1 \notin \mathfrak{a}$. There is a maximal ideal $\mathfrak{m} \in \text{mSpec } k[T_1, \dots, T_n]$ such that $\mathfrak{a} \subseteq \mathfrak{m}$. Then $L = k[T_1, \dots, T_n]_{\mathfrak{m}}$ is a field, which is finitely generated over k as an algebra. By Zariski's lemma, this extension is finitely generated as a module. Hence, there is an injective k -algebra homomorphism $L \rightarrow \Omega$. Composing with the quotient map, we obtain a k -algebra homomorphism $\varphi : k[T_1, \dots, T_n] \rightarrow \Omega$ with kernel \mathfrak{m} . Now, let

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

We claim that this is a common solution to all polynomials in \mathfrak{a} . Note that for $f \in k[T_1, \dots, T_n]$, we have $\varphi(f) = f(\mathbf{x})$. Therefore, for all $f \in \mathfrak{a}$, we have $f \in \ker \varphi$ so $f(\mathbf{x}) = \varphi(f) = 0$.

Strong Nullstellensatz. Let $f \in \sqrt{\mathfrak{a}}$. Then $f^\ell \in \mathfrak{a}$ for some $\ell \geq 1$, and therefore, $f^\ell(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{V}(\mathfrak{a})$. As Ω is an integral domain, $f(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{V}(\mathfrak{a})$. Hence $f \in I(\mathbb{V}(\mathfrak{a}))$.

Conversely, suppose $f \in I(\mathbb{V}(\mathfrak{a}))$, so for all $\mathbf{x} \in \mathbb{V}(\mathfrak{a})$, we have $f(\mathbf{x}) = 0$. We want to show that $f \in \sqrt{\mathfrak{a}}$. To do this, we show that \bar{f} is nilpotent in $k[T_1, \dots, T_n]_{\bar{\mathfrak{a}}}$. It suffices to show that

$$(k[T_1, \dots, T_n]_{\bar{\mathfrak{a}}})_{\bar{f}} = 0$$

Note that

$$(k[T_1, \dots, T_n]_{\bar{\mathfrak{a}}})_{\bar{f}} \simeq k[T_1, \dots, T_n, T_{n+1}]_{\bar{\mathfrak{b}}}; \quad \bar{\mathfrak{b}} = \mathfrak{a}^e + (T_{n+1}f - 1)$$

We will show that $1 \in \bar{\mathfrak{b}}$, or equivalently by the weak Nullstellensatz, $\mathbb{V}(\bar{\mathfrak{b}}) = \emptyset$.

Suppose $\mathbf{x} = (x_1, \dots, x_{n+1}) \in \mathbb{V}(\bar{\mathfrak{b}}) \subseteq \Omega^{n+1}$. Define $\mathbf{x}_0 = (x_1, \dots, x_n)$, so $\mathbf{x}_0 \in \mathbb{V}(\mathfrak{a})$. In particular, $f(\mathbf{x}_0) = 0$, as $f \in I(\mathbb{V}(\mathfrak{a}))$. Thus $f(\mathbf{x}) = 0$. Now, $(T_{n+1}f - 1)(\mathbf{x}) = -1 \neq 0$, but $(T_{n+1}f - 1) \in \bar{\mathfrak{b}}$, so \mathbf{x} is not a common solution to all polynomials in $\bar{\mathfrak{b}}$, which is a contradiction. \square

One can easily derive the weak Nullstellensatz from the strong Nullstellensatz.

Note that

(i) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.

(ii) If $X \subseteq Y \subseteq \Omega^n$, then $I(X) \supseteq I(Y)$.

(iii) If $S \subseteq T \subseteq k[T_1, \dots, T_n]$, then $\mathbb{V}(S) \supseteq \mathbb{V}(T)$.

(iv) If $S \subseteq k[T_1, \dots, T_n]$, then $S \subseteq I(\mathbb{V}(S))$.

(v) If $X \subseteq \Omega^n$, then $X \subseteq \mathbb{V}(I(X))$.

(vi) If $X \subseteq \Omega^n$ is an algebraic set, then $X = \mathbb{V}(I(X))$, as $X = \mathbb{V}(\mathfrak{a})$ gives

$$\mathbb{V}(\mathfrak{a}) \subseteq \mathbb{V}(I(\mathbb{V}(\mathfrak{a}))) \subseteq \mathbb{V}(\mathfrak{a})$$

(vii) If $X \subseteq \Omega^n$, then $I(X)$ is a radical ideal.

Proposition. Let $k = \Omega$ be an algebraically closed field, and let $n \geq 0$. Then we have an inclusion-reversing bijection

$$\{k\text{-algebraic subsets of } \Omega^n\} \leftrightarrow \{\text{radical ideals of } k[T_1, \dots, T_n]\}$$

given by $X \mapsto I(X)$ and $\mathfrak{a} \mapsto \mathbb{V}(\mathfrak{a})$.

Proof. We have already shown that $I(X)$ is radical, and $X = \mathbb{V}(I(X))$ if X is an algebraic set. For the converse, let $\mathfrak{a} \subseteq k[T_1, \dots, T_n]$ be a radical ideal. Then $I(\mathbb{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}} = \mathfrak{a}$ by the strong Nullstellensatz. \square

Remark. Every prime ideal \mathfrak{p} is radical, as $x^n \in \mathfrak{p}$ implies $x \in \mathfrak{p}$. In particular, every maximal ideal is radical.

Corollary. Let $k = \Omega$ be an algebraically closed field. Then we have a bijection

$$\Omega^n \leftrightarrow \text{mSpec } k[T_1, \dots, T_n]$$

given by $\mathbf{x} = (x_1, \dots, x_n) \mapsto (T_1 - x_1, \dots, T_n - x_n) = \mathfrak{m}_{\mathbf{x}}$.

Proof. First, note that $\mathfrak{m}_{\mathbf{x}}$ is a maximal ideal for every \mathbf{x} , since it is the kernel of the map $k[T_1, \dots, T_n] \rightarrow \Omega$ given by $T_i \mapsto x_i$. Also, $\mathfrak{m}_{\mathbf{x}} = I(\{\mathbf{x}\})$. Indeed, the inclusion $\mathfrak{m}_{\mathbf{x}} \subseteq I(\{\mathbf{x}\})$ is clear, and $I(\{\mathbf{x}\})$ is a proper ideal of $k[T_1, \dots, T_n]$, so they must be equal by maximality. Note that $\mathbb{V}(\mathfrak{m}_{\mathbf{x}}) = \{\mathbf{x}\}$. Hence the claim follows from the inclusion-reversing bijection, as maximal ideals correspond to minimal nonempty algebraic sets. \square

Definition. We say that $X \subseteq \Omega^n$ is *irreducible* if X cannot be expressed as the union of two strictly smaller algebraic subsets.

Proposition. $X \subseteq \Omega^n$ is irreducible if and only if $I(X)$ is prime.

4.6 Integrality over ideals

Definition. Let $A \subseteq B$ be an extension of rings, and let $\mathfrak{a} \subseteq A$ be an ideal. We say that $x \in B$ is integral over \mathfrak{a} if

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

for some $a_1, \dots, a_n \in \mathfrak{a}$. The *integral closure* of \mathfrak{a} in B is the set of elements of B that are integral over \mathfrak{a} .

Proposition. Let $A \subseteq B$ be an extension of rings, and let \overline{A} be the integral closure of A in B . Let \mathfrak{a} be an ideal of A . Then the integral closure of \mathfrak{a} in B is $\sqrt{\mathfrak{a}\overline{A}}$, the radical in \overline{A} of the extension of \mathfrak{a} to \overline{A} .

Proof. If $b \in B$ is integral over \mathfrak{a} , then

$$b^n + a_1 b^{n-1} + \dots + a_n b^0 = 0; \quad a_i \in \mathfrak{a}$$

In particular, b lies in \overline{A} , and so all of its powers lie in \overline{A} as \overline{A} is a ring. Using the integrality equation for b , we observe that $b^n \in \mathfrak{a}\overline{A}$, hence $b \in \sqrt{\mathfrak{a}\overline{A}}$.

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

$$b^n = \sum_{i=1}^m a_i x_i; \quad a_i \in \mathfrak{a}, x_i \in \overline{A}$$

Define $M = A[x_1, \dots, x_m]$. The generators lie in \bar{A} , so M is an A -algebra generated by finitely many integral elements over A . Hence M is a finite A -algebra. Note that $b^n M \subseteq \mathfrak{a}M$ by the equation for b^n , thought of as an extension of A -modules.

Now define $f : M \rightarrow M$ by multiplication by b^n . This satisfies $f(M) \subseteq \mathfrak{a}M$, and f is A -linear. Thus by the Cayley–Hamilton theorem,

$$f^\ell + \alpha_1 f^{\ell-1} + \dots + \alpha_\ell f^0 = 0 \in \text{End}_R M; \quad \alpha_i \in \mathfrak{a}$$

Evaluating this at $1_A \in M$,

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

This is an integrality relation for b is \mathfrak{a} -integral. □

Hence, the integral closure of an ideal is closed under sums and products.

Corollary. Let $A \subseteq B$ be an extension of rings, and let \mathfrak{a} be an ideal of A . Then $b \in B$ is \mathfrak{a} -integral if and only if b is $\sqrt{\mathfrak{a}}$ -integral.

Proof. By the previous proposition, it suffices to show that

$$\sqrt{\mathfrak{a}\bar{A}} = \sqrt{\sqrt{\mathfrak{a}}\bar{A}}$$

The forwards inclusion is clear. For the other direction, it is a general fact that $\sqrt{\sqrt{I}^e} \subseteq \sqrt{I^e}$, so

$$\sqrt{\mathfrak{a}\bar{A}} \subseteq \sqrt{\sqrt{\mathfrak{a}}\bar{A}}$$

Taking radicals on both sides,

$$\sqrt{\sqrt{\mathfrak{a}\bar{A}}} \subseteq \sqrt{\sqrt{\sqrt{\mathfrak{a}}\bar{A}}} = \sqrt{\mathfrak{a}\bar{A}}$$

□

Proposition. Let A be an integrally closed integral domain (in its field of fractions). Let $A \subseteq B$ be an extension of rings, let \mathfrak{a} be an ideal in A , and let $b \in B$. The following are equivalent:

- (i) b is integral over \mathfrak{a} ;
- (ii) b is algebraic over $FF(A)$ with minimal polynomial over $FF(A)$ of the form

$$T^n + a_1 T^{n-1} + \dots + a_n T^0 = 0; \quad a_i \in \sqrt{\mathfrak{a}}$$

Note that there is an embedding $FF(A) \subseteq FF(B)$.

Proof. Suppose (ii) holds. Then b is integral over $\sqrt{\mathfrak{a}}$ by definition. Thus, by the above corollary, b is integral over \mathfrak{a} .

Now suppose (i) holds. We have an integrality equation

$$b^n + a_1 b^{n-1} + \dots + a_n b^0 = 0; \quad a_i \in \mathfrak{a}$$

Define

$$h = T^n + a_1 T^{n-1} + \cdots + a_n T^0 \in (FF(A))[T]$$

so $h(b) = 0$, so certainly b is algebraic over $FF(A)$. Let $f \in (FF(A))[T]$ be the minimal polynomial of b over $FF(A)$. Let $FF(A) \subseteq \Omega$ where Ω is an algebraically closed field, so

$$f = \prod_{i=1}^{\ell} (T - \alpha_i); \quad \alpha_1 = b, \alpha_i \in \Omega$$

We want to show that the coefficients of f are in $\sqrt{\mathfrak{a}}$. By the previous proposition, together with the fact that A is integrally closed, the integral closure of \mathfrak{a} in $FF(A)$ is $\sqrt{\mathfrak{a}} \subseteq A$. So it suffices to show that the coefficients of f lie in $FF(A)$ and are integral over \mathfrak{a} . As f is the minimal polynomial over $FF(A)$, the first part holds by definition.

Expanding brackets in the equation for f , the coefficients of f are sums of products of the α_i . The proposition above implies that the integral closure of \mathfrak{a} in Ω is closed under sums and products, so it suffices to show that the α_i are all integral over \mathfrak{a} . As the α_i and b have the same minimal polynomial f over $FF(A)$, there is an isomorphism of $FF(A)$ -algebras $\varphi_i : FF(A)[b] \rightarrow FF(A)[\alpha_i]$ that maps b to α_i . Then as $h(b) = 0$ and $h \in (FF(A))[T]$, we must have $h(\alpha_i) = h(\varphi_i(b)) = \varphi_i(h(b)) = \varphi_i(0) = 0$. \square

4.7 Cohen–Seidenberg theorems

If $A \subseteq B$ is an extension of rings, the inclusion $\iota : A \rightarrow B$ gives rise to $\iota^* : \text{Spec } B \rightarrow \text{Spec } A$ given by $\iota^*(\mathfrak{q}) = \mathfrak{q} \cap A$. We will study the fibres of this induced map on spectra.

Proposition (incomparability). Let $A \subseteq B$ be an integral extension, and let $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of B . Suppose that \mathfrak{q} and \mathfrak{q}' contract to the same prime ideal $\mathfrak{p} = \mathfrak{q} \cap A = \mathfrak{q}' \cap A$ of A , and that $\mathfrak{q} \subseteq \mathfrak{q}'$. Then $\mathfrak{q} = \mathfrak{q}'$.

In this section, we will write $B_{\mathfrak{p}}$ to abbreviate $(A \setminus \mathfrak{p})^{-1}B$.

Proof. Define $S = A \setminus \mathfrak{p}$. Then \mathfrak{q} and \mathfrak{q}' are prime ideals of B not intersecting S . Hence $\mathfrak{q} = (S^{-1}\mathfrak{q})^c$, where $S^{-1}\mathfrak{q} = \mathfrak{q}B_{\mathfrak{p}}$ is the extension of \mathfrak{q} to $S^{-1}B$, due to the bijection

$$\{\mathfrak{p} \in \text{Spec } R \mid \mathfrak{p} \cap S = \emptyset\} \leftrightarrow \text{Spec } S^{-1}R$$

It suffices to show that $\mathfrak{q}B_{\mathfrak{p}} = \mathfrak{q}'B_{\mathfrak{p}}$, as then they are the contractions of the same ideal. Note that

$$\mathfrak{q}B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = S^{-1}\mathfrak{q} \cap S^{-1}A = S^{-1}(\mathfrak{q} \cap A) = S^{-1}\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}}$$

Similarly, $\mathfrak{q}'B_{\mathfrak{p}} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$, which is a maximal ideal of $A_{\mathfrak{p}}$. As $A \subseteq B$ is an integral extension, $A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}$ is also an integral extension. Recall that if the contraction of a prime ideal is maximal in an integral extension, the prime ideal was maximal. Thus, $\mathfrak{q}B_{\mathfrak{p}} \subseteq \mathfrak{q}'B_{\mathfrak{p}}$ are maximal ideals of $B_{\mathfrak{p}}$, so they must coincide. \square

Proposition (lying over). Let $A \subseteq B$ be an integral extension of rings, and let $\mathfrak{p} \in \text{Spec } A$. Then there is a prime ideal $\mathfrak{q} \in \text{Spec } B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$. In other words, $\iota^* : \text{Spec } B \rightarrow \text{Spec } A$ is surjective.

Proof. We have a commutative diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \beta \\ A_{\mathfrak{p}} & \longrightarrow & B_{\mathfrak{p}} = (A \setminus \mathfrak{p})^{-1}B \end{array}$$

Let \mathfrak{m} be a maximal ideal of $B_{\mathfrak{p}}$. Then $A_{\mathfrak{p}} \subseteq B_{\mathfrak{p}}$ is an integral extension, so \mathfrak{m} contracts to a maximal ideal $\mathfrak{m} \cap A_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$. But there is exactly one maximal ideal in $A_{\mathfrak{p}}$, namely $\mathfrak{p}A_{\mathfrak{p}}$. Note that $\mathfrak{p}A_{\mathfrak{p}}$ contracts to \mathfrak{p} under the map $A \rightarrow A_{\mathfrak{p}}$.

We have that \mathfrak{m} contracts to \mathfrak{p} under the map $A \rightarrow A_{\mathfrak{p}} \rightarrow B_{\mathfrak{p}}$, but this is the same as the map $A \rightarrow B \rightarrow B_{\mathfrak{p}}$, so $\beta^{-1}(\mathfrak{m}) \cap A = \mathfrak{p}$. Note that $\beta^{-1}(\mathfrak{m})$ is a prime ideal, as required. \square

Theorem (going up). Let $A \subseteq B$ be an integral extension of rings. Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$ be prime ideals in A , and let $\mathfrak{q}_1 \in \text{Spec } B$ be a prime ideal such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there is a prime ideal $\mathfrak{q}_2 \in \text{Spec } B$ such that $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, and $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

$$\begin{array}{ccc} \mathfrak{q}_1 & \xrightarrow{\subseteq} & \mathfrak{q}_2 \\ \cap A \downarrow & & \downarrow \cap A \\ \mathfrak{p}_1 & \xrightarrow{\subseteq} & \mathfrak{p}_2 \end{array}$$

Proof. We have an injection $A/\mathfrak{p}_1 \rightarrow B/\mathfrak{q}_1$ given by $a + \mathfrak{p}_1 \mapsto a + \mathfrak{q}_1$. This is an integral extension, so by lying over, there is a prime ideal $\mathfrak{q}_2/\mathfrak{q}_1$ of B/\mathfrak{q}_1 that contracts to $\mathfrak{p}_2/\mathfrak{p}_1$ in A/\mathfrak{p}_1 . We claim that $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. In the diagram

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A/\mathfrak{p}_1 & \longrightarrow & B/\mathfrak{q}_1 \end{array}$$

we obtain contractions of prime ideals

$$\begin{array}{ccc} \mathfrak{p}_2 & & \mathfrak{q}_2 \\ \uparrow & & \uparrow \\ \mathfrak{p}_2/\mathfrak{p}_1 & \longleftarrow & \mathfrak{q}_2/\mathfrak{q}_1 \end{array}$$

hence \mathfrak{q}_2 contracts to \mathfrak{p}_2 , as required. \square

Theorem (going down). Let $A \subseteq B$ be an integral extension of integral domains, and suppose that A is integrally closed (in its field of fractions). Let $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$ be prime ideals in A , and let $\mathfrak{q}_1 \in \text{Spec } B$ be a prime ideal such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there is a prime ideal $\mathfrak{q}_2 \in \text{Spec } B$

such that $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$, and $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$.

$$\begin{array}{ccc} \mathfrak{q}_1 & \xleftarrow{\supseteq} & \mathfrak{q}_2 \\ \downarrow \cap A & & \downarrow \cap A \\ \mathfrak{p}_1 & \xleftarrow{\supseteq} & \mathfrak{p}_2 \end{array}$$

Proof. Consider the map $A \rightarrow B \rightarrow B_{\mathfrak{q}_1}$. These maps are injective as B is an integral domain, so we can think of these as inclusions of rings. We want to prove that there is a prime ideal $\mathfrak{n} \in \text{Spec } B_{\mathfrak{q}_1}$ such that $\mathfrak{n} \cap A = \mathfrak{p}_2$. This suffices, as $(\mathfrak{n} \cap B) \cap A = \mathfrak{p}_2$ is a contraction of a prime ideal $\mathfrak{q}_2 = \mathfrak{n} \cap B$ of B contained in \mathfrak{q}_1 to $\mathfrak{p}_2 \in \text{Spec } A$. In other words, we want to show that \mathfrak{p}_2 is a contracted ideal under the map $A \rightarrow B_{\mathfrak{q}_1}$. As contracted ideals are contracted from their own extension, it suffices to show that $(\mathfrak{p}_2 B_{\mathfrak{q}_1}) \cap A \subseteq \mathfrak{p}_2$, noting that the converse inclusion always holds.

Note that $\mathfrak{p}_2 B_{\mathfrak{q}_1} = (\mathfrak{p}_2 B) B_{\mathfrak{q}_1}$. Let $\frac{y}{s} \in (\mathfrak{p}_2 B) B_{\mathfrak{q}_1} \cap A$, where $y \in \mathfrak{p}_2 B$ and $s \in B \setminus \mathfrak{q}_1$. As $A \subseteq B$ is an integral extension, the integral closure of \mathfrak{p}_2 in B is $\sqrt{\mathfrak{p}_2 B}$. In particular, y is integral over \mathfrak{p}_2 . Since A is integrally closed and y is integral over \mathfrak{p}_2 , the minimal polynomial of $y \in FF(B)$ over $FF(A)$ has the form

$$y^r + u_1 y^{r-1} + \cdots + u_r y^0 = 0; \quad u_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$$

We can write $y = \frac{y}{s} \cdot s$, where $y, s \in FF(B)$ and $\frac{y}{s} \in FF(A)$. Hence,

$$\left(\frac{y}{s} \cdot s\right)^r + u_1 \left(\frac{y}{s} \cdot s\right)^{r-1} + \cdots + u_r \left(\frac{y}{s} \cdot s\right)^0 = 0$$

Multiplying by $\left(\frac{s}{y}\right)^r$,

$$s^r + \left(\frac{s}{y}\right)^1 u_1 s^{r-1} + \cdots + \left(\frac{s}{y}\right)^r u_r s^0 = 0; \quad u_i \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$$

This must be the same minimal polynomial of s as an element of $FF(B)$ over $FF(A)$. As $s \in B$, s is integral over A , so the coefficients in this polynomial must lie in A .

$$\left(\frac{s}{y}\right)^1 u_1, \dots, \left(\frac{s}{y}\right)^r u_r \in A$$

Suppose $\frac{y}{s} \notin \mathfrak{p}_2$. Then

$$u_i = \left(\frac{y}{s}\right)^i \cdot \left(\frac{s}{y}\right)^i u_i$$

But

$$u_i \in \mathfrak{p}_2; \quad \left(\frac{y}{s}\right)^i \in A \setminus \mathfrak{p}_2; \quad \left(\frac{s}{y}\right)^i u_i \in A$$

By primality, $\left(\frac{s}{y}\right)^i u_i \in \mathfrak{p}_2$. As this holds for all i , the coefficients in the equation for s lie in \mathfrak{p}_2 , so

$$s^r \in \mathfrak{p}_2 B \subseteq \mathfrak{p}_1 B = (\mathfrak{q}_1 \cap A) B \subseteq \mathfrak{q}_1$$

Hence $s \in \mathfrak{q}_1$ by primality, giving a contradiction. \square

5 Primary decomposition

Definition. Let I be an ideal of R . I is

- (i) *prime* if $R/I \neq 0$ and 0 is the only zero divisor of R/I ;
- (ii) *radical* if the only nilpotent element of R/I is zero;
- (iii) *primary* if $R/I \neq 0$ and every zero divisor in R/I is nilpotent.

The prime ideals precisely those ideals that are both radical and primary. R is radical but not prime or primary.

Example. (i) Let $R = \mathbb{Z}$. The ideal (6) is radical but not primary, as $R/(6)$ contains zero divisors $2, 3$ which are not nilpotent. The ideal (9) is primary but not radical.

- (ii) More generally, let $R = \mathbb{Z}$ and $x \neq 0$. Then (x) is prime if and only if $x = 0$ or $|x|$ is prime, and (x) is radical if and only if x is squarefree. (x) is primary if and only if $x = p^n$ for some prime p and $n \geq 1$.

Proposition. Let I be a proper ideal in R . Then

- (i) If I is primary, then $\mathfrak{p} = \sqrt{I}$ is prime. We say 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 \mathfrak{p} -primary, then $\bigcap_{i=1}^n \mathfrak{q}_i$ is also \mathfrak{p} -primary.
- (iv) If I has a *primary decomposition* $I = \bigcap_{i=1}^n \mathfrak{q}_i$ where the \mathfrak{q}_i are primary, then I has a minimal primary decomposition $\bigcap_{j=1}^m \mathfrak{r}_j$ where the $\sqrt{\mathfrak{r}_j}$ are distinct and no \mathfrak{r}_j can be dropped.
- (v) If R is Noetherian, then every proper ideal has a primary decomposition.

In \mathbb{Z} ,

$$(90) = (2) \cap (3^2) \cap (5)$$

Primary decomposition therefore generalises prime factorisation. Note that for a prime ideal \mathfrak{p} , if \mathfrak{p}^n is primary, then \mathfrak{p}^n is \mathfrak{p} -primary, because $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$.

Example. (i) Not every primary ideal is a power of a prime ideal. For instance, consider $R = k[X, Y]$ and $\mathfrak{q} = (X, Y^2)$. We claim that this is primary. For instance, $\sqrt{\mathfrak{q}} = (X, Y)$ is maximal, so \mathfrak{q} is (X, Y) -primary. Alternatively,

$$k[X, Y]_{(X, Y^2)} \simeq k[Y]_{(Y^2)}$$

If $f \in k[Y]$ satisfies $f \in (Y^2)$ so it is a zero divisor, then $Y \mid f$, so $f + (Y^2)$ is nilpotent. Now, if $\mathfrak{q} = \mathfrak{p}^n$, then

$$(X, Y) = \sqrt{\mathfrak{q}} = \sqrt{\mathfrak{p}^n} = \mathfrak{p}$$

But

$$(X, Y) \supsetneq (X, Y^2) \supsetneq (X, Y)^2$$

So \mathfrak{q} is not a power of $\mathfrak{p} = (X, Y)$.

- (ii) If \mathfrak{p} is prime, \mathfrak{p}^n need not be primary. Let

$$R = k[X, Y, Z]_{(XY - Z^2)} = k[\bar{X}, \bar{Y}, \bar{Z}]; \quad \mathfrak{p} = (\bar{X}, \bar{Z})$$

where $\bar{X}, \bar{Y}, \bar{Z}$ are the images of X, Y, Z under the quotient map. We claim that \mathfrak{p} is prime, but \mathfrak{p}^2 is not primary. Indeed,

$$R/\mathfrak{p} \simeq k[X, Y, Z]/(X, Z, XY - Z^2) \simeq k[X, Y, Z]/(X, Z) \simeq k[Y]$$

which is an integral domain, so \mathfrak{p} is prime. For the second part,

$$\mathfrak{p}^2 = (\bar{X}^2, \bar{X} \cdot \bar{Z}, \bar{Z}^2)$$

Then $\bar{X} \cdot \bar{Y} = \bar{Z}^2 \in \mathfrak{p}^2$, that is,

$$(\bar{X} + \mathfrak{p}^2)(\bar{Y} + \mathfrak{p}^2) = 0 + \mathfrak{p}^2$$

But $\bar{X} + \mathfrak{p}^2 \neq 0$ and $\bar{Y} + \mathfrak{p}^2 \neq 0$. Hence $\bar{Y} + \mathfrak{p}^2$ is a zero divisor in R/\mathfrak{p}^2 . Note that

$$R/\mathfrak{p}^2 \simeq k[X, Y, Z]/(XY - Z^2, X^2, XZ, Z^2) \simeq k[X, Y, Z]/(XY, X^2, Z^2)$$

so $Y + \mathfrak{p}^2$ is not nilpotent.

Theorem. Let $\bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition for an ideal I of R , and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ for each i . Then

- (i) (*associated prime ideals of I*) The prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are determined only by I , even though there may not be a unique minimal primary decomposition.
- (ii) (*isolated prime ideals of I*) The minimal elements of $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$, ordered by inclusion, are exactly the minimal prime ideals of R that contain I . An associated prime ideal that is not isolated is called *embedded*.
- (iii) (*isolated primary components of I*) If $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ are the isolated prime ideals of I for $t \leq n$, then $\mathfrak{q}_1, \dots, \mathfrak{q}_t$ are determined only by I .

Example. Let $R = k[X, Y]$ and $I = (X^2, XY)$. We have primary decompositions

$$I = (X) \cap (X, Y)^2 = (X) \cap (X^2, Y)$$

Note that

$$\sqrt{(X)} = (X); \quad \sqrt{(X, Y)^2} = (X, Y); \quad \sqrt{(X^2, Y)} = (X, Y)$$

The associated primes of I are (X) and (X, Y) . The isolated prime is (X) and the embedded prime is (X, Y) .

Remark. Let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a minimal primary decomposition with $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Suppose $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ are the isolated primes. Then

$$\sqrt{I} = \sqrt{\bigcap_{i=1}^n \mathfrak{q}_i} = \bigcap_{i=1}^n \sqrt{\mathfrak{q}_i} = \bigcap_{i=1}^n \mathfrak{p}_i = \bigcap_{i=1}^t \mathfrak{p}_i$$

This is a primary decomposition of \sqrt{I} , and one can check that this is minimal. All associated primes in this decomposition are isolated. Going from I to \sqrt{I} , we only ‘remember’ the isolated primes.

Analogously, let $R = k[T_1, \dots, T_n]$, where $k \subseteq \mathbb{C}$. Then $\mathbb{V}(I) = \mathbb{V}(\sqrt{I})$ and $I(\mathbb{V}(I)) = \sqrt{I}$. Hence, taking the algebraic set of I ‘remembers’ the radical of I and nothing else.

6 Direct and inverse limits

6.1 Limits and completions

Definition. Let \mathcal{C} be a category.

- (i) A *directed set* (I, \leq) is a partially ordered set such that for all $a, b \in I$, there exists $c \in I$ such that $a, b \leq c$.
- (ii) A *direct system* on a directed set (I, \leq) is a pair $((X_i)_{i \in I}, (f_{ij})_{i \leq j})$ where $X_i \in \text{ob } \mathcal{C}$ and $f_{ij} : X_i \rightarrow X_j$, such that $f_{ii} = 1_{X_i}$ and $f_{ik} = f_{jk} \circ f_{ij}$.
- (iii) An *inverse system* on (I, \leq) is a pair $((Y_i)_{i \in I}, (h_{ij})_{i \leq j})$ where $Y_i \in \text{ob } \mathcal{C}$ and $h_{ij} : Y_j \rightarrow Y_i$, such that $h_{ii} = 1_{Y_i}$ and $h_{ik} = h_{ij} \circ h_{jk}$.

Remark. An inverse system in \mathcal{C} is the same as a direct system in \mathcal{C}^{op} .

Example. Let $I = (\mathbb{N}, \leq)$.

- (i) Let p be a prime, and let $X_i = \mathbb{F}_{p^{i!}}$. Recall that if $a \mid b$, then there is an embedding $\varphi : \mathbb{F}_{p^a} \rightarrow \mathbb{F}_{p^b}$. The collection of embeddings $\mathbb{F}_{p^a} \rightarrow \mathbb{F}_{p^b}$ is then given by $x \mapsto (\varphi(x))^{p^c}$ where $0 \leq c < a - 1$. The map $f_{i(i+1)} : \mathbb{F}_{p^{i!}} \rightarrow \mathbb{F}_{p^{(i+1)!}}$ is defined to be one such embedding. A general embedding f_{ij} is given by the composite $f_{(j-1)j} \circ \cdots \circ f_{i(i+1)}$. This creates a direct system on I .
- (ii) Let $Y_i = \mathbb{Z}/p^i\mathbb{Z}$, and let $h_{ij} : \mathbb{Z}/p^j\mathbb{Z} \rightarrow \mathbb{Z}/p^i\mathbb{Z}$ be the natural projection. This is an inverse system on I .

Definition. Let (I, \leq) be a directed set.

- (i) Let $D = ((X_i)_{i \in I}, (f_{ij})_{i \leq j})$ be a direct system on I . Then the *direct limit* of D is

$$\varinjlim X_i = \left(\prod_{i \in I} X_i \right) / \sim$$

where for $x_i \in X_i$ and $x_j \in X_j$,

$$x_i \sim x_j \iff \exists k \geq i, j, f_{ik}(x_i) = f_{jk}(x_j)$$

Equivalently, one can define \sim to be the smallest equivalence relation containing $x_i \sim f_{ij}(x_i)$.

- (ii) Let $E = ((Y_i)_{i \in I}, (h_{ij})_{i \leq j})$ be an inverse system on I . Then the *inverse limit* of E is

$$\varprojlim Y_i = \left\{ \mathbf{y} \in \prod_{X_i} \mid \forall i \leq j, y_i = h_{ij}(y_j) \right\}$$

Example. (i) $\mathbb{F}_p^{\text{alg}} = \varinjlim \mathbb{F}_{p^{i!}}$ is an algebraic closure of \mathbb{F}_p . First, $\mathbb{F}_p^{\text{alg}}$ is algebraic over \mathbb{F}_p . Indeed, for $[x] \in \mathbb{F}_p^{\text{alg}}$, we have $x \in \mathbb{F}_{p^{i!}}$ for some $i \geq 1$. Then $x^{p^{i!}} - x = 0$. Hence

$$[x]^{p^{i!}} - [x] = [x^{p^{i!}} - x] = [0]$$

Further, $\mathbb{F}_p^{\text{alg}}$ is algebraically closed. Any polynomial $h \in \mathbb{F}_p^{\text{alg}}[T]$ has coefficients in $\mathbb{F}_{p^{i!}}$, so in particular h arises from an element of $\mathbb{F}_{p^{i!}}[T]$ for some i . This element splits under some

$\mathbb{F}_{p^i} \rightarrow \mathbb{F}_{p^e}$, so it splits under some $\mathbb{F}_{p^i} \rightarrow \mathbb{F}_{p^e}$. Hence it splits under $h_{ij} : \mathbb{F}_{p^i} \rightarrow \mathbb{F}_{p^j}$, so h splits in the direct limit $\mathbb{F}_p^{\text{alg}}$.

- (ii) Define $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}$. This is the ring of *p-adic integers*. For example, writing numbers in base $p = 5$,

$$\begin{aligned} 1 &= (1 + 5^1\mathbb{Z}, 1 + 5^2\mathbb{Z}, 1 + 5^3\mathbb{Z}, \dots) \\ -1 &= (4 + 5^1\mathbb{Z}, 44 + 5^2\mathbb{Z}, 444 + 5^3\mathbb{Z}, \dots) \end{aligned}$$

In every position in such an expansion, we ‘expose’ another digit of the p -adic integer to the left.

Definition. Let R be a ring, and let \mathfrak{a} be an ideal of R . Then the \mathfrak{a} -adic completion of R is

$$\hat{R} = \varprojlim R/\mathfrak{a}^i$$

where the inverse limit is taken over the directed system (\mathbb{N}, \leq) with morphisms given by the natural projections.

Example. (i) If $R = \mathbb{Z}$ and $\mathfrak{a} = (p)$, then $\hat{R} = \mathbb{Z}_p$.

- (ii) If $R = k[T]$ and $\mathfrak{a} = (T)$, then

$$\hat{R} = \varprojlim k[T]/(T^i) = k[[t]]$$

Definition. Let M be an R -module, and let \mathfrak{a} be an ideal of R . Then the \mathfrak{a} -adic completion of M is

$$\hat{M} = \varprojlim M/\mathfrak{a}^i M$$

which is naturally an \hat{R} -module.

We can make the following more general definition.

Definition. Let M be an R -module.

- (i) A *filtration* of M is a sequence $(M_n)_{n \geq 1}$ of submodules of M such that $M_0 = M$ and $M_n \supseteq M_{n+1}$ for each n .
(ii) The *completion* of M with respect to a filtration $(M_n)_{n \geq 1}$ is $\varprojlim M/M_n$.

Theorem. Let R be a Noetherian ring, and let \mathfrak{a} be an ideal of R . Then,

- (i) the \mathfrak{a} -adic completion \hat{R} is Noetherian;
(ii) the functor $\hat{R} \otimes_R (-)$ is exact;
(iii) if M is a finitely generated R -module, then the natural map $\hat{R} \otimes_R M \rightarrow \hat{M}$ is an \hat{R} -linear isomorphism.

Thus \mathfrak{a} -adic completion is an exact functor from the category of finitely generated R -modules if R is Noetherian.

6.2 Graded rings and modules

Definition. A *graded ring* is a ring $A = \bigoplus_{n=0}^{\infty} A_n$, where each A_n is an additive subgroup of A , such that $A_m A_n \subseteq A_{m+n}$.

Proposition. A_0 is a subring of A .

Proof. It is clearly a subgroup closed under multiplication, so it suffices to check that it contains the identity element of A . We have

$$1_A = \sum_{i=0}^m y_i; \quad y_i \in A_i$$

For $z_n \in A_n$,

$$z_n = \sum_{i=0}^m y_i z_n$$

z_n is an element of A_n , and each term $y_i z_n$ is an element of A_{n+i} . But since the sum is direct, we must have $z_n = y_0 z_n$, so $z = y_0 z$ for all $z \in A$. Hence $y_0 \in A_0$ is the identity element. \square

Remark. Each A_n is an A_0 -module as $A_0 A_n \subseteq A_n$.

Example. The polynomial ring in finitely many variables has a grading: $k[T_1, \dots, T_m] = \bigoplus_{n=0}^{\infty} A_n$ where A_n is the set of homogeneous polynomials of degree n .

Definition. Let $A = \bigoplus_{n=0}^{\infty} A_n$ be a graded ring. A *graded A -module* is an A -module $M = \bigoplus_{n=0}^{\infty} M_n$ such that $A_m M_n \subseteq M_{m+n}$.

For a graded ring A , we define $A_+ = \bigoplus_{n=1}^{\infty} A_n = \ker(A \rightarrow A_0)$. This is an ideal of A , and $A/A_+ \simeq A_0$.

Proposition. Let $A = \bigoplus_{i=0}^{\infty} A_i$ be a graded ring. Then the following are equivalent:

- (i) A is Noetherian;
- (ii) A_0 is Noetherian and A is finitely generated as an A_0 -algebra.

Proof. Hilbert's basis theorem shows that (ii) implies (i). For the converse, A_0 is Noetherian as it is isomorphic to a quotient of the Noetherian ring A . Note that A_+ is generated by the set of homogeneous elements of positive degree. By (i), A_+ is an ideal in a Noetherian ring so is generated by a finite set $\{x_1, \dots, x_s\}$, and we can take each x_i to be homogeneous, say, $x_i \in A_{k_i}$ where $k_i > 0$. Let A' be the A_0 -subalgebra of A generated by $\{x_1, \dots, x_s\}$; we want to show $A' = A$. It suffices to show that $A_n \subseteq A'$ for every $n \geq 0$, which we will show by induction. The case $n = 0$ is clear.

Let $n > 0$, and let $y \in A_n$. Note that $y \in A_+$, so

$$y = \sum_{i=1}^s r_i x_i$$

where $r_i \in A$ and $x_i \in A_{k_i}$. Applying the projection to A_n ,

$$y = \sum_{i=1}^s a_i x_i; \quad a_i \in A_{n-k_i}$$

where a_i is the $(n - k_i)$ homogeneous part of r_i . As k_i is positive, the inductive hypothesis implies that each a_i can be written as a polynomial in x_1, \dots, x_s with coefficients in A_0 , giving $y \in A'$ as required. \square

Definition. Let \mathfrak{a} be an ideal of R , and let M be an R -module. Then a filtration $(M_n)_{n \geq 0}$ is an \mathfrak{a} -filtration if $\mathfrak{a}M_n \subseteq M_{n+1}$ for each $n \geq 0$. An \mathfrak{a} -filtration $(M_n)_{n \geq 0}$ is *stable* if there exists $n_0 \geq 0$ such that $\mathfrak{a}M_n = M_{n+1}$ for all $n \geq n_0$.

Example. $(\mathfrak{a}^n M)_{n \geq 0}$ is a stable \mathfrak{a} -filtration of M .

Definition. Let \mathfrak{a} be an ideal in R . The *associated graded ring* is

$$G_{\mathfrak{a}}(R) = \bigoplus_{n \geq 0} \mathfrak{a}^n / \mathfrak{a}^{n+1}; \quad \mathfrak{a}^0 = R$$

This is a ring by defining

$$(x + \mathfrak{a}^{n+1})(y + \mathfrak{a}^{m+1}) = xy + \mathfrak{a}^{n+m+1}; \quad x \in \mathfrak{a}^n, y \in \mathfrak{a}^m$$

Definition. Let M be an R -module, and let \mathfrak{a} be an ideal of R . Let $(M_n)_{n \geq 0}$ be an \mathfrak{a} -filtration of M . The *associated graded module* is

$$G(M) = \bigoplus_{n \geq 0} M_n / M_{n+1}$$

This is a module over $G_{\mathfrak{a}}(R)$ by defining

$$(x + \mathfrak{a}^{n+1})(m + M_{\ell+1}) = xm + M_{n+\ell+1}$$

Proposition. Let R be a Noetherian ring, and let \mathfrak{a} be an ideal of R . Then

- (i) the associated graded ring $G_{\mathfrak{a}}(R)$ is Noetherian; and
- (ii) if M is a finitely generated R -module and $(M_n)_{n \geq 0}$ is a stable \mathfrak{a} -filtration of M , then the associated graded module $G(M)$ is a finitely generated $G_{\mathfrak{a}}(R)$ -module.

Proof. Part (i). Let R be Noetherian. Then let $\mathfrak{a} = (x_1, \dots, x_s)$, and write \bar{x}_i for the image of x_i in $\mathfrak{a}/\mathfrak{a}^2$. Note that

$$G_{\mathfrak{a}}(R) = R/\mathfrak{a} \oplus \mathfrak{a}/\mathfrak{a}^2 \oplus \mathfrak{a}^2/\mathfrak{a}^3 \oplus \dots$$

$G_{\mathfrak{a}}(R)$ is generated as an R/\mathfrak{a} -algebra by $\bar{x}_1, \dots, \bar{x}_s$, by taking sums and products. Note that R/\mathfrak{a} is Noetherian, so $G_{\mathfrak{a}}(R)$ is Noetherian by Hilbert's basis theorem.

Part (ii). Let $(M_n)_{n \geq 0}$ be a stable \mathfrak{a} -filtration of M . Then there exists n_0 such that for all $n \geq n_0$, we have $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$. Thus $G(M)$ is generated as a $G_{\mathfrak{a}}(R)$ -module by

$$M_0/M_1 \oplus M_1/M_2 \oplus \cdots \oplus M_{n_0}/M_{n_0+1}$$

Each factor M_i/M_{i+1} is a Noetherian R -module, as they are quotients of Noetherian modules, and are annihilated by \mathfrak{a} . In particular, $G(M)$ is a finitely generated $G_{\mathfrak{a}}(R)$ -module, say by x_1, \dots, x_s . \square

Definition. Let M be an R -module. We say that filtrations $(M_n), (M'_n)$ of M are *equivalent* if there exists n_0 such that for all $n \geq 0$, we have $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$.

Lemma. Let \mathfrak{a} be an ideal of R . Let M be an R -module, and let $(M_n)_{n \geq 0}$ be a stable \mathfrak{a} -filtration of M . Then $(M_n)_{n \geq 0}$ is equivalent to $(\mathfrak{a}^n M)_{n \geq 0}$.

Proof. As $(M_n)_{n \geq 0}$ is an \mathfrak{a} -filtration, for all $n \geq 0$, we have

$$M_n \supseteq \mathfrak{a}M_{n-1} \supseteq \mathfrak{a}^2 M_{n-2} \supseteq \cdots \supseteq \mathfrak{a}^n M \supseteq \mathfrak{a}^{n+n_0} M$$

For the other direction, as the filtration is stable, there exists n_0 such that for each $n \geq n_0$, we have $\mathfrak{a}M_n = M_{n+1}$. Then $M_{m+n_0} = \mathfrak{a}^n M_{n_0} \subseteq \mathfrak{a}^n M$ as required. \square

6.3 Artin–Rees lemma

Definition. Let \mathfrak{a} be an ideal of R . Let M be an R -module, and let $(M_n)_{n \geq 0}$ be an \mathfrak{a} -filtration of M . Then we define

$$R^* = \bigoplus_{n \geq 0} \mathfrak{a}^n; \quad M^* = \bigoplus_{n \geq 0} M_n$$

Note that R^* is a graded ring, as for $x \in \mathfrak{a}^n, y \in \mathfrak{a}^\ell$, we have $xy \in \mathfrak{a}^{n+\ell}$. As $(M_n)_{n \geq 0}$ is an \mathfrak{a} -filtration, M^* is a graded R^* -module. Indeed, for $x \in \mathfrak{a}^n$ and $m \in M_\ell$, we have $xm \in M_{n+\ell}$ as required.

If R is Noetherian, the ideal \mathfrak{a} is finitely generated, say by x_1, \dots, x_r . Then R^* is generated as an R -algebra by x_1, \dots, x_r by taking sums and products. By Hilbert's basis theorem, R^* is a Noetherian ring.

Lemma. Let R be a Noetherian ring, and let \mathfrak{a} be an ideal of R . Let M be a finitely generated R -module, and let $(M_n)_{n \geq 0}$ be an \mathfrak{a} -filtration of M . Then, the following are equivalent:

- (i) M^* is finitely generated as an R^* -module;
- (ii) the \mathfrak{a} -filtration $(M_n)_{n \geq 0}$ is stable.

Proof. First, note that each M_n is a finitely generated R -module. Indeed, R is a Noetherian ring and M is finitely generated, so M is a Noetherian module, or equivalently, every submodule is finitely generated. Now, consider

$$M_n^* = M_0 \oplus \cdots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \cdots$$

This is an R^* -submodule of M^* . Note that $(M_n^*)_{n \geq 0}$ is an ascending chain of R^* -submodules of M^* , and this chain stabilises if and only if the \mathfrak{a} -filtration $(M_n)_{n \geq 0}$ is stable.

(i) *implies* (ii). As R is Noetherian, so is R^* by the discussion above. By assumption, M^* is finitely generated as a module over a Noetherian ring, so it is Noetherian. Hence the ascending chain $(M_n^*)_{n \geq 0}$ stabilises, giving the result.

(ii) *implies* (i). Suppose $(M_n)_{n \geq 0}$ is stable. Then $(M_n^*)_{n \geq 0}$ stabilises at some $n_0 \geq 0$, so

$$M^* = \bigcup_{n \geq 0} M_n^* = M_{n_0}^*$$

Now, note that $M_0 \oplus \cdots \oplus M_{n_0}$ generates $M_{n_0}^*$ as an R^* -module. Each M_n is a finitely generated R -module, so $M_0 \oplus \cdots \oplus M_{n_0}$ is also finitely generated as an R -module. So these generators span $M_{n_0}^* = M^*$ as an R^* -module, as required. \square

Proposition (Artin–Rees). Let R be a Noetherian ring, and let \mathfrak{a} be an ideal of R . Let M be a finitely generated R -module, and let $(M_n)_{n \geq 0}$ be a stable \mathfrak{a} -filtration of M . Then for any submodule $N \leq M$, $(N \cap M_n)_{n \geq 0}$ is a stable \mathfrak{a} -filtration of N .

Thus, stable filtrations pass to submodules.

Proof. First, we show that $(N \cap M_n)_{n \geq 0}$ is indeed an \mathfrak{a} -filtration.

$$\mathfrak{a}(N \cap M_n) \subseteq N \cap \mathfrak{a}M_n \subseteq N \cap M_{n+1}$$

Now, define

$$M^* = \bigoplus_{n \geq 0} M_n; \quad N^* = \bigoplus_{n \geq 0} (N \cap M_n)$$

Note that M^* is an R^* -submodule of N^* . As R is Noetherian, so is R^* . Then as $(M_n)_{n \geq 0}$ is stable, M^* is a finitely generated R^* -module by the previous lemma. Thus M^* is a Noetherian R^* -module. Its submodule N^* is then finitely generated, so $(N \cap M_n)_{n \geq 0}$ is stable. \square

7 Dimension theory

7.1 ???

Definition. Let \mathfrak{p} be a prime ideal of R . The *height* of \mathfrak{p} , denoted $\text{ht}(\mathfrak{p})$, is

$$\text{ht}(\mathfrak{p}) = \sup \{d \mid \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_d = \mathfrak{p}; \mathfrak{p}_i \in \text{Spec } R\}$$

The (*Krull*) *dimension* of R is

$$\dim R = \sup \{\text{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \text{Spec } R\} = \sup \{\text{ht}(\mathfrak{m}) \mid \mathfrak{m} \in \text{mSpec } R\}$$

Remark. The height of a prime ideal \mathfrak{p} is the Krull dimension of the localisation $R_{\mathfrak{p}}$. In particular,

$$\dim R = \sup \{\dim R_{\mathfrak{p}} \mid \mathfrak{p} \in \text{Spec } R\} = \sup \{\dim R_{\mathfrak{m}} \mid \mathfrak{m} \in \text{mSpec } R\}$$

So the problem of computing dimension can be reduced to computing dimension of local rings.

Definition. Let I be a proper ideal of R . Then the *height* of I is

$$\text{ht}(I) = \inf\{\text{ht}(\mathfrak{p}) \mid I \subseteq \mathfrak{p}\}$$

Proposition. Let $A \subseteq B$ be an integral extension of rings. Then,

- (i) $\dim A = \dim B$; and
- (ii) if A, B are integral domains and k -algebras for some field k , they have the same transcendence degree over k .

We prove part (i); the second part is not particularly relevant for this course.

Proof. First, we show that $\dim A \leq \dim B$. Consider a chain of prime ideals $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_d$ in $\text{Spec } A$. By the lying over theorem and the going up theorem, we obtain a chain of prime ideals $\mathfrak{q}_0 \subseteq \cdots \subseteq \mathfrak{q}_d$ in $\text{Spec } B$. As $\mathfrak{p}_i = \mathfrak{q}_i \cap A$ and $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$, we must have $\mathfrak{q}_i \neq \mathfrak{q}_{i+1}$. So this produces a chain of length d in B , as required.

Now consider a chain $\mathfrak{q}_0 \subsetneq \cdots \subsetneq \mathfrak{q}_d$ in $\text{Spec } B$. Contracting each ideal, we produce a chain $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_d$ in $\text{Spec } A$. Suppose that \mathfrak{q}_i and \mathfrak{q}_{i+1} contract to the same prime ideal \mathfrak{p}_i in $\text{Spec } A$. Note that $\mathfrak{q}_i \subseteq \mathfrak{q}_{i+1}$, so by incomparability, they must be equal, but this is a contradiction. \square

Remark. If A is a finitely generated k -algebra for some field k , then by Noether normalisation, we obtain a k -algebra embedding $k[T_1, \dots, T_d] \rightarrow A$, and the extension is integral. Thus $\dim A = \dim k[T_1, \dots, T_d]$. One can show that $\dim k[T_1, \dots, T_d] = d$, and hence that the integer d obtained by Noether normalisation is uniquely determined by A and k .

7.2 Hilbert polynomials

Let $A = \bigoplus_{n \geq 0} A_n$ be a Noetherian graded ring, so A_0 is Noetherian and A is finitely generated as an A_0 -algebra. Now let $M = \bigoplus_{n \geq 0} M_n$ be a finitely generated graded A -module. Then each M_n is an A_0 -module.

We claim that M_n is finitely generated as an A_0 -module. Indeed, $M = \text{span}_A \{m_1, \dots, m_t\}$, and the m_i can be taken to be homogeneous, say, $m_i \in M_{r_i}$. Then

$$M_n = \{a_1 m_1 + \cdots + a_t m_t \mid a_i \in A_{n-r_i}\}$$

Let x_1, \dots, x_s generate A as an A_0 -algebra, where $x_i \in A_{k_i}, k_i > 0$. Then

$$M_n = \text{span}_{A_0} \left\{ x_1^{e_1} \cdots x_t^{e_t} m_i \mid 1 \leq i \leq t, e_i \geq 0, \sum_{i=1}^s k_i e_i = n - r_i \right\}$$

and the right-hand side is a finite set.

We will make the further assumption that A_0 is Artinian. Hence, each M_n is a finitely generated module over a ring that is both Noetherian and Artinian, so each M_n is Noetherian and Artinian as an A_0 -module. Further, each M_n is of finite length $\ell(M_n) < \infty$; it has a *composition series* of finite length. Note that if $A_0 = k$ is a field, then $\ell(M_n) = \dim_k M_n$.

Definition. Let A, M be as above. Then the *Poincaré series* of M is

$$P(M, T) = \sum_{n=0}^{\infty} \ell(M_n) T^n \in \mathbb{Z}[[T]]$$

Theorem (Hilbert–Serre theorem). Let A be generated by x_1, \dots, x_s as an A_0 -module with $x_i \in A_{k_i}$ for $k_i > 0$. The Poincaré series $P(M, T)$ is a rational function of the form

$$\frac{f(T)}{\prod_{i=1}^s (1 - T^{k_i})}; \quad f \in \mathbb{Z}[T]$$

Proof. For the base case $s = 0$, we must have $A = A_0$, so M is a finitely generated A_0 -module, say, $M = \text{span}_{A_0} S$ where S is a finite subset of $M_0 \oplus \dots \oplus M_n$. Thus there exists n_0 such that $M_m = 0$ for all $m > n_0$. In particular, $P(M, T)$ is a polynomial.

For the inductive step, let

$$M = \bigoplus_{n \in \mathbb{Z}} M_n; \quad M_\ell = 0 \text{ if } \ell < 0$$

Let $f : M_n \rightarrow M_{n+k_s}$ be the homomorphism given by multiplication by x_s . We obtain the exact sequence

$$0 \longrightarrow K_n \longrightarrow M_n \xrightarrow{f} M_{n+k_s} \longrightarrow L_{n+k_s} \longrightarrow 0$$

where $K_n = \ker f$ and $L_{n+k_s} = \text{coker } f$. Then let $K = \bigoplus_{n \in \mathbb{Z}} K_n$ and $L = \bigoplus_{n \in \mathbb{Z}} L_n$. These are graded A -modules, and K is a submodule of M . Note that K and L are annihilated by x_s . Applying the length function to the exact sequence, we obtain

$$\ell(K_n) - \ell(M_n) + \ell(M_{n+k_s}) - \ell(L_{n+k_s}) = 0$$

Multiplying by T^{n+k_s} ,

$$\ell(M_{n+k_s}) T^{n+k_s} - T^{k_s} \ell(M_n) T^n = \ell(L_{n+k_s}) T^{n+k_s} - T^{k_s} \ell(K_n) T^n$$

Then, taking the sum over all integers,

$$P(M, T) - T^{k_s} P(M, T) = (1 - T^{k_s}) P(M, T) = P(L, T) - T^{k_s} P(K, T)$$

By the inductive hypothesis,

$$(1 - T^{k_s}) P(M, T) = \frac{f_1(T)}{\prod_{i=1}^{s-1} (1 - T^{k_i})} + \frac{f_2(T)}{\prod_{i=1}^{s-1} (1 - T^{k_i})}$$

as required. □

In particular, this rational function is holomorphic almost everywhere, with potentially a pole of some order at 1. Let $d(M)$ be the order of the pole of $P(M, T)$ at $T = 1$. One can show that if $M \neq 0$, then $d(M) \geq 0$.

Example. Let $A = k[T_1, \dots, T_s] = \bigoplus_{n \geq 0} A_n$ where A_n is the set of homogeneous polynomials of degree n . Then A is generated as an $A_0 = k$ -algebra by $\{T_1, \dots, T_s\}$. For this choice of generators, $k_1 = \dots = k_s = 1$. The length of A_n is $\dim_k A_n = \binom{n+s-1}{n}$, which is a polynomial of degree $s-1$ in n over \mathbb{Q} . The Poincaré series of A over itself is

$$P(A, T) = \sum_{n \geq 0} \binom{n+s-1}{n} T^n = \frac{1}{(1-T)^s}$$

Proposition. If $k_1 = \dots = k_s = 1$, then there exists a *Hilbert polynomial* $HP_M \in \mathbb{Q}[T]$ and $n_0 \geq 0$ such that

$$\ell(M_n) = HP_M(n)$$

for all $n \geq n_0$. In addition, $\deg HP_M = d(M) - 1$ where $d(M)$ is the order of the pole of $P(M, T)$ at $T = 1$.

Proof. Let $d = d(M) \geq 0$. Then,

$$P(M, T) = \sum_{n \geq 0} \ell(M_n) T^n = \frac{f(T)}{(1-T)^d}; \quad f \in \mathbb{Z}[T], f(1) \neq 0$$

Let

$$f = \sum_{k=0}^{\deg f} a_k T^k; \quad a_k \in \mathbb{Z}$$

Note that

$$\frac{1}{(1-T)^d} = \sum_{j=0}^{\infty} \underbrace{\binom{j+d-1}{j}}_{b_j} T^j$$

Thus, for $n \geq \deg f$,

$$\ell(M_n) = \sum_{i=0}^{\deg f} a_i b_{n-i}$$

Note that b_j is a polynomial in j over \mathbb{Q} of degree $d-1$ with leading coefficient $\frac{1}{(d-1)!}$. Then $\ell(M_n)$ is a polynomial p in n over \mathbb{Q} for $n \geq \deg f$. Then $\deg p \leq d-1$, and the coefficient of T^{d-1} in p is

$$\sum_{i=0}^{\deg f} a_i \cdot \frac{1}{(d-1)!} = \frac{f(1)}{(d-1)!} \neq 0$$

so the degree is exactly $d-1$. □

7.3 Dimension theory of local Noetherian rings

Lemma. 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.

Proof. Part (i). Given an ideal \mathfrak{q} between \mathfrak{m}^t and \mathfrak{m} , taking radicals we obtain

$$\sqrt{\mathfrak{m}^t} \subseteq \sqrt{\mathfrak{q}} \subseteq \sqrt{\mathfrak{m}}$$

Hence $\sqrt{\mathfrak{q}} = \mathfrak{m}$ and thus \mathfrak{q} is \mathfrak{m} -primary. Conversely, if \mathfrak{q} is \mathfrak{m} -primary, $(\sqrt{\mathfrak{q}})^t \subseteq \mathfrak{q}$ for some t as A is Noetherian, so $\mathfrak{m}^t \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ as required.

Part (ii). $(A/\mathfrak{q}, \mathfrak{m}/\mathfrak{q})$ is a Noetherian local ring. If $\mathfrak{q} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$, then taking radicals,

$$\mathfrak{m} = \sqrt{\mathfrak{q}} \subseteq \mathfrak{p} \subseteq \mathfrak{m}$$

Hence $\mathfrak{p} = \mathfrak{m}$. In particular, the spectrum of A/\mathfrak{q} is the single ideal $\mathfrak{m}/\mathfrak{q}$. Thus its dimension is zero, and so the quotient is Artinian. \square

Theorem (dimension theorem). If A is a Noetherian local ring, then

$$\dim A = \delta(A) = d(G_{\mathfrak{m}}(A))$$

where $\delta(A) = \min \{\delta(\mathfrak{q}) \mid \mathfrak{q} \subseteq A \text{ is } \mathfrak{m}\text{-primary}\}$ and $\delta(\mathfrak{q})$ is the minimal number of generators of \mathfrak{q} , and where the right-hand side is the order of the pole at $T = 1$ of the rational function equal to the Poincaré series

$$\sum_{n \geq 0} \ell\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) T^n$$

of the associated graded ring.

Proof. We will show that $\delta \geq d \geq \dim \geq \delta$.

Let \mathfrak{q} be an \mathfrak{m} -primary ideal of A , generated by x_1, \dots, x_s where $s = \delta(\mathfrak{q})$. Then

$$G_{\mathfrak{q}}(A) = A/\mathfrak{q} \oplus \mathfrak{q}/\mathfrak{q}^2 \oplus \bigoplus_{n \geq 2} \mathfrak{q}^n/\mathfrak{q}^{n+1}$$

The first factor A/\mathfrak{q} is Artinian, and the images of x_1, \dots, x_s generate $G_{\mathfrak{q}}(A)$ as an A/\mathfrak{q} -algebra, where the x_i are of degree 1. Then $\ell(\mathfrak{q}^n/\mathfrak{q}^{n+1}) < \infty$. From the theorem on Hilbert polynomials, $\ell(\mathfrak{q}^n/\mathfrak{q}^{n+1})$ is a polynomial in n of degree at most $\delta(\mathfrak{q}) - 1$, for sufficiently large n .

Fix some \mathfrak{m} -primary ideal \mathfrak{q}_0 such that $\delta(\mathfrak{q}_0) = \delta(A)$. We consider two special cases: $\mathfrak{q} = \mathfrak{q}_0$ and $\mathfrak{q} = \mathfrak{m}$. For \mathfrak{q}_0 , we have

$$\deg \ell\left(\frac{\mathfrak{q}_0^n}{\mathfrak{q}_0^{n+1}}\right) \leq \delta(A) - 1$$

As

$$\ell\left(\frac{A}{\mathfrak{q}_0^n}\right) = \sum_{i=0}^{n-1} \ell\left(\frac{\mathfrak{q}_0^i}{\mathfrak{q}_0^{i+1}}\right)$$

we have

$$\deg \ell\left(\frac{A}{\mathfrak{q}_0^n}\right) \leq \delta(A)$$

For \mathfrak{m} ,

$$\deg \ell\left(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}\right) = d(G_{\mathfrak{m}}(A)) - 1$$

and hence

$$\deg \ell(A/\mathfrak{m}^n) = d(G_{\mathfrak{m}}(A))$$

Now, there exists $t \geq 1$ such that $\mathfrak{m}^t \subseteq \mathfrak{q}_0 \subseteq \mathfrak{m}$. Then

$$\ell(A/\mathfrak{m}^n) \leq \ell(A/\mathfrak{q}_0^n) \leq \ell(A/\mathfrak{m}^{tn})$$

But all of these terms are eventually polynomial, and the degrees of the left-hand and right-hand sides are the same, so we must have $\ell(A/\mathfrak{q}_0^n) = \ell(A/\mathfrak{m}^n)$.

Proposition. $\delta(A) \geq d(G_{\mathfrak{m}}(A))$.

Proof.

$$\delta(A) = \delta(\mathfrak{q}_0) \geq \deg \ell(A/\mathfrak{q}_0^n) = \deg \ell(A/\mathfrak{m}^n) = d(G_{\mathfrak{m}}(A))$$

□

Proposition. If $x \in \mathfrak{m}$ is not a zero divisor, then

$$d(G_{(\mathfrak{m}/xA)}(A/xA)) \leq d(G_{\mathfrak{m}}(A)) - 1$$

This proposition allows us to prove results by induction on d .

Proof. We have a local ring $(A/xA, \mathfrak{m}/xA)$. Then

$$d(G_{\mathfrak{m}}(A)) = \deg \ell(A/\mathfrak{m}^n)$$

and

$$d(G_{(\mathfrak{m}/xA)}(A/xA)) = \deg \ell(A/xA/(\mathfrak{m}/xA)^n) = \deg \ell((\mathfrak{m}^n + xA)/xA)$$

We want to show that

$$\deg \ell((\mathfrak{m}^n + xA)/xA) \leq \deg \ell(A/\mathfrak{m}^n) - 1$$

We have the short exact sequence

$$0 \longrightarrow (\mathfrak{m}^n + xA)/\mathfrak{m}^n \longrightarrow A/\mathfrak{m}^n \longrightarrow A/(\mathfrak{m}^n + xA) \longrightarrow 0$$

By the second isomorphism theorem,

$$(\mathfrak{m}^n + xA)/\mathfrak{m}^n \cong xA/(\mathfrak{m}^n \cap xA)$$

Thus, by additivity of length,

$$\ell(A/\mathfrak{m}^n + xA) = \ell(A/\mathfrak{m}^n) - \ell(xA/(\mathfrak{m}^n \cap xA))$$

Note that $(\mathfrak{m}^n)_{n \geq 0}$ is a stable \mathfrak{m} -filtration of A , so $(\mathfrak{m}^n \cap xA)_{n \geq 0}$ is a stable \mathfrak{m} -filtration of the submodule xA by the Artin–Rees lemma. Then $(\mathfrak{m}^n \cap xA)_{n \geq 0}$ is equivalent to the \mathfrak{m} -filtration $(\mathfrak{m}^n xA)_{n \geq 0}$. This equivalence implies that there exists n_0 such that

$$\ell(xA/(\mathfrak{m}^n xA)) \leq \ell(xA/(\mathfrak{m}^{n+n_0} \cap xA)); \quad \ell(xA/(\mathfrak{m}^n \cap xA)) \leq \ell(xA/(\mathfrak{m}^{n+n_0} xA))$$

Hence the polynomials have the same leading term, and so the degree of $\ell(A/\mathfrak{m}^n)$ must decrease. □

Proposition. $d(G_{\mathfrak{m}}(A)) \geq \dim A$.

Proof. We can prove this by induction using the previous proposition. □

Proposition. $\dim A \leq \delta(A)$. That is, there exists an \mathfrak{m} -primary ideal \mathfrak{q} that is generated by $d = \dim A$ elements.

Proof. As \mathfrak{m} is the unique maximal ideal, we must have $\text{ht}(\mathfrak{m}) = d$. Also, $\text{ht}(\mathfrak{p}) < d$ for any prime $\mathfrak{p} \neq \mathfrak{m}$. We will form an ideal \mathfrak{q} generated by d elements such that $\text{ht}(\mathfrak{q}) \geq d$. This suffices, as then for every minimal prime ideal \mathfrak{p} of \mathfrak{q} , we must have $\text{ht}(\mathfrak{p}) = d$ and thus $\mathfrak{p} = \mathfrak{m}$, giving $\sqrt{\mathfrak{q}} = \mathfrak{m}$ so \mathfrak{p} is \mathfrak{m} -primary as required.

Construct x_1, \dots, x_d inductively such that $\text{ht}(\mathfrak{q}_i) \geq i$ where $\mathfrak{q}_i = (x_1, \dots, x_i)$. For the base case, we take $\mathfrak{q}_0 = (0)$. For the inductive step, we assume that $\mathfrak{q}_{i-1} = (x_1, \dots, x_{i-1})$ has already been constructed, with $i-1 < d$ and $\text{ht}(\mathfrak{q}_{i-1}) \geq i-1$. We claim that there are only finitely many prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_t$ that contain \mathfrak{q}_{i-1} and have height exactly $i-1$. Indeed, $\text{ht}(\mathfrak{q}_{i-1}) \geq i-1$, so each \mathfrak{p}_j is a minimal prime ideal of \mathfrak{q}_{i-1} , and in a Noetherian ring, every ideal has only finitely many minimal primes. We know that $i-1 < d = \text{ht}(\mathfrak{m})$, so $\mathfrak{m} \not\subseteq \mathfrak{p}_j$ for all j . Therefore, $\mathfrak{m} \not\subseteq \bigcup_j \mathfrak{p}_j$ by the prime avoidance lemma. Take $x_i \in \mathfrak{m} \setminus \bigcup_j \mathfrak{p}_j$, and define $\mathfrak{q}_i = (x_1, \dots, x_{i-1}, x_i)$. Now, if \mathfrak{p} is a prime ideal that contains \mathfrak{q}_i , as $\mathfrak{p} \not\subseteq \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$, we must have $\text{ht}(\mathfrak{p}) \geq i$ as required. □

Corollary (Krull's height theorem). Let A be a Noetherian ring, and let $\mathfrak{a} = (x_1, \dots, x_r)$ be an ideal of A . Let \mathfrak{p} be a minimal prime ideal of \mathfrak{a} . Then $\text{ht}(\mathfrak{p}) \leq r$.

Proof. First, we claim that $\sqrt{\mathfrak{a}A_{\mathfrak{p}}}$ is the unique maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ of the localisation. Indeed, suppose $\mathfrak{a}A_{\mathfrak{p}} \subseteq \mathfrak{n} \in \text{Spec} A_{\mathfrak{p}}$. Contracting, we obtain $\mathfrak{a} \subseteq (\mathfrak{a}A_{\mathfrak{p}})^c \subseteq \mathfrak{n}^c \subseteq \mathfrak{p}$. But as \mathfrak{p} is a minimal prime ideal of \mathfrak{a} , we must have $\mathfrak{n}^c = \mathfrak{p}$. Extending, $\mathfrak{n}^{ce} = \mathfrak{p}^e = \mathfrak{p}A_{\mathfrak{p}}$, but $\mathfrak{n}^{ce} = \mathfrak{n}$ as required. Hence, $\sqrt{\mathfrak{a}A_{\mathfrak{p}}}$ is the intersection of the primes containing it, which is just $\mathfrak{p}A_{\mathfrak{p}}$.

As the radical is maximal, the ideal $\mathfrak{a}A_{\mathfrak{p}}$ is $\mathfrak{p}A_{\mathfrak{p}}$ -primary. Note that $\mathfrak{a}A_{\mathfrak{p}} = \left(\frac{x_1}{1}, \dots, \frac{x_r}{1}\right)$, so by applying the dimension theorem,

$$\text{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}} = \delta(A_{\mathfrak{p}}) \leq \delta(\mathfrak{a}A_{\mathfrak{p}}) \leq r$$

□