

Commutative Algebra

Amy Needham

October 2025

Contents

1	Introduction	2
1.1	Rings and Ideals	2
1.2	Radicals	2
2	Extension, Contraction and Spectra	3
3	Modules	4
3.1	Constructions and Universal Properties	5
3.2	Generation of Modules	6
4	Localisation	7
4.1	Local Rings and Local Properties	11
4.2	Extension and Contraction under Localisation	13
5	Tensor Products	14
5.1	Restriction and Extension of Scalars	16
5.2	Exactness properties of Hom and $\otimes$	19
6	Chain Conditions	23
6.1	Noetherian Rings and Modules	25
6.2	Artinian Rings	26
7	Primary Decomposition	27
8	Integrality	30
9	Dedekind Domains and Discrete Valuation Rings	35
9.1	Discrete Valuation Rings	35
9.2	Dedekind Domains	38
10	Completions	38
10.1	Graded Rings and Modules	40

11 Dimension Theory	43
11.1 Hilbert Functions	43
11.2 Dimension Theory of Noetherian Local Rings	46

1 Introduction

1.1 Rings and Ideals

In this course, unless otherwise stated, rings are commutative and unital, with homomorphisms sending the identity to the identity. R is usually a ring, and K a field. I, J are ideals, however prime ideals may be $\mathfrak{p}, \mathfrak{q}$ and maximal ideals may be $\mathfrak{m}$.

Theorem 1.1. *For every proper ideal $I \triangleleft R$ there is a maximal ideal $\mathfrak{m} \triangleleft R$ such that $I \subseteq \mathfrak{m}$.*

We recall the following needed definitions and theorem before the proof

Definition 1.1. Let $(P, \leq)$ be a poset (ie $\leq$ is reflexive, transitive, and if $x \leq y, y \leq x$ then $x = y$). We say $x \in P$ is an *upper bound* for $A \subseteq P$ if $a \leq x$ for all $a \in A$. For $A \subseteq P$, it is a *chain* if it is linearly ordered by $\leq$. $x \in P$ is *maximal* if for all $y \in P$, $x \leq y$ implies $x = y$.

Proposition 1.1. *(Zorn's lemma) If $P \neq \emptyset$ is a poset such that every non-empty chain has an upper bound, then P has a maximal element.*

Proof. See your favourite logic course. □

Proof. (Of Theorem 1.1) Consider the set of proper ideals containing I ordered by inclusion. This is non-empty (as I is in it), and every chain has an upper bound (the union, which is proper as being proper is equivalent to not containing 1), so by Zorn's lemma, the result follows. □

1.2 Radicals

Definition 1.2. Let $I \subseteq R$. The *radical* of I , denoted $\sqrt{I}$, is the ideal given by $\{r \in R \mid r^n \in I, n \geq 1\}$. This is an ideal as if $r \in \sqrt{I}, s \in \sqrt{I}$ and $r^n \in I, s^m \in I$, then $(r + s)^{n+m-1} \in I$.

Remark. $I(V(I)) = \sqrt{I}$ (Hilbert's nullstellensatz)

Proposition 1.2. *Let $I \triangleleft R$. Then $\sqrt{I} = \bigcap_{\mathfrak{p} \subseteq I \text{ prime}} \mathfrak{p}$*

Proof. Let J be the right hand side of the claimed equality. We claim $\sqrt{I} \subseteq J$. Let $r^n \in I$. Then $r^n \in \mathfrak{p}$ for any $\mathfrak{p} \supseteq I$, so $r \in \mathfrak{p}$ by primality, so $r \in J$ as $\mathfrak{p}$ was arbitrary.

For the opposite direction, suppose $r \notin \sqrt{I}$. Let Σ be ideals containing I and not containing any r^n . This set is non-empty as it contains I , and is clearly

closed under upwards unions, so has a maximal element $\mathfrak{p}$. Let $s, t \notin \mathfrak{p}$ (exists as $\mathfrak{p}$ is proper, as it doesn't contain r). Then $\mathfrak{p} + (s), \mathfrak{p} + (t) \supset \mathfrak{p}$. Hence they are not elements of Σ , so there are $r^n \in \mathfrak{p} + (s)$ and $r^m \in \mathfrak{p} + (t)$. But then $r^{n+m} \in \mathfrak{p} + (st)$, so $st \notin \mathfrak{p}$, so $\mathfrak{p}$ is prime, and so $r \notin J$. Hence the proposition is proven. $\square$

Definition 1.3. $r \in R$ is *nilpotent* if $r^n = 0$ for some $n \geq 1$. The *nilradical*, $\text{nil}(R)$ is the set of nilpotents

Remark. $\text{nil}(R) = \sqrt{(0)}$

Corollary 1.1.1. *The nilradical of R is the intersection of all the prime ideals of R*

Proof. Trivial $\square$

Definition 1.4. We define the *Jacobson radical* $\mathcal{J}(R)$ is the intersection of all maximal ideals. This contains the nilradical.

Proposition 1.3. $r \in \mathcal{J}(R)$ if and only if $1 - rs$ is a unit for all $s \in R$

Proof. If $1 - rs$ is not a unit for some s , it is contained in some maximal ideal $\mathfrak{m}$. Hence if $r \in \mathcal{J}(R)$ then $1 - rs, rs \in \mathfrak{m}$, so $1 \in \mathfrak{m}$ contradiction.

If $r \notin \mathcal{J}(R)$, take maximal $\mathfrak{m}$ such that $r \notin \mathfrak{m}$. Then $(\mathfrak{m}, r) = (1)$, so $1 = m + sr$ for some $m \in \mathfrak{m}, s \in R$. Hence $1 - sr = m \in \mathfrak{m}$ is not a unit, so we are done. $\square$

2 Extension, Contraction and Spectra

Definition 2.1. If $j: A \rightarrow B$ is a ring homomorphism,

1. If $J \trianglelefteq B$, the *contracted ideal* of J is $J^c = j^{-1}(J) \trianglelefteq A$
2. $I \trianglelefteq A$, I is *contracted* if $I = J^c$ for some $J \trianglelefteq B$
3. Given $I \trianglelefteq A$, the *extended ideal* of I is $I^e = (j(I))$
4. $J \trianglelefteq B$ is *extended* if $J = I^e$ for some $I \trianglelefteq A$

Proposition 2.1. *Let $j: A \rightarrow B$ be a ring homomorphism*

1. *For any $I \trianglelefteq A$, $I \subseteq I^{ec}$ and $I^e = I^{ece}$*
2. *I is contracted if and only if $I = I^{ec}$*
3. *For any $J \trianglelefteq B$, $J \subseteq J^{ce}$ and $J^c = J^{cec}$*
4. *J is extended if and only if $J = J^{ce}$*

We therefore have a bijection between contracted ideals of A and extended ideals of B via extension and contraction.

Proof. On example sheet 1 $\square$

Lemma 2.1. *If $\mathfrak{p} \leq B$ is prime, then so is $\mathfrak{p}^c \leq A$*

Proof. Let $r, s \in A \setminus \mathfrak{p}^c$. Then $f(r), f(s) \notin \mathfrak{p}$, so $f(rs) \notin \mathfrak{p}$, so $rs \notin \mathfrak{p}^c$. $\square$

Remark. It is not necessarily true that $\mathfrak{p}^c$ is prime even if $\mathfrak{p}$ is, eg see all of algebraic number theory.

Definition 2.2. The *spectrum* of the ring R is the set of prime ideals of R , and is denoted $\text{Spec}(R)$.

Definition 2.3. If $E \subseteq R$, we can define $V(E) = \{\mathfrak{p} \in \text{Spec } R \mid R \subseteq \mathfrak{p}\}$

Remark. The sets $V(E)$ form the closed subsets of a topology, called the *Zariski topology* (see algebraic geometry for proof)

Corollary 2.1.1. *If $f: A \rightarrow B$ is a ring homomorphism, then there is an induced set-map $f^{-1}: \text{Spec } B \rightarrow \text{Spec } A$.*

Proof. Trivial $\square$

Remark. In fact, this is Zariski continuous (see algebraic geometry)

Definition 2.4. The *maximal spectrum*, denoted $\text{mSpec}(R)$, is the set of maximal ideals of R .

Remark. If $\mathfrak{m} \subseteq B$ is a maximal ideal, its contraction is not necessarily maximal in A (take $A = \mathbb{Z}, B = \mathbb{Q}$ and f the inclusion)

3 Modules

Definition 3.1. An *R -module* M is an abelian group on which R acts linearly. An *R -module homomorphism* is a group homomorphism $f: M \rightarrow N$ such that $f(rm) = rf(m)$ for all $r \in R, m \in M$.

]

Remark. If M, N are R modules, then $\text{Hom}_R(M, N)$ (the set of all R -module homomorphisms from M to N) is an R -module, with addition given pointwise, and $(r \cdot f)(m) = r \cdot f(m)$. We denote $\text{End}_R(M) = \text{Hom}_R(M, M)$ for the *R -endomorphisms* of M . This is also a not-necessarily-commutative ring

Example 3.1.

1. $\mathbb{Z}$ -modules are exactly abelian groups
2. $k[t]$ -modules are exactly vector spaces over k equipped with a k -linear map $t: V \rightarrow V$

3.1 Constructions and Universal Properties

Definition 3.2. Given a set I and a family of R -modules indexed by I , called $\{M_i\}_{i \in I}$, the *direct product* of this family is

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i\}$$

with pointwise operation and R -action. The *direct sum* of this family is

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} \mid m_i \in M_i, \text{ only finitely many non-zero}\}$$

with pointwise operation and R -action.

Proposition 3.1. (*Universal Property of Direct Products*) Let I be a set, $\{M_i\}_{i \in I}$ an I -indexed family of R modules, and p_j the projection of the direct product onto the j th coordinate. If N is an R -module with homomorphisms $f: N \rightarrow M_i$, then there is a unique R -module homomorphism $f: N \rightarrow \prod_{i \in I} M_i$ such that $f_j = p_j \circ f$ for all $j \in I$. In diagram form,

$$\begin{array}{ccc} N & & \\ \downarrow f & \searrow f_j & \\ \prod_{i \in I} M_i & \xrightarrow{p_j} & M_j \end{array}$$

commutes. N is furthermore unique up to unique isomorphism with these properties.

Proof. We define $f: N \rightarrow \prod_{i \in I} M_i$ via $f(n) = (f_i(n))_{i \in I}$. This satisfies the properties, and determines f uniquely. If M also has the property, then we get f, g in the diagram $M \xrightarrow{f} N \xrightarrow{g} M$ by the universal property. Now $g \circ f$ and id_M satisfy the universal property condition, so are the same. Similarly, the same holds for $f \circ g$, so we are done. $\square$

Proposition 3.2. (*Universal Property of Direct Products*) Let I be a set, $\{M_i\}_{i \in I}$ an I -indexed family of R modules, and l_j the inclusion of the j th coordinate direct sum. If N is an R -module with homomorphisms $f: M_i \rightarrow N$, then there is a unique R -module homomorphism $f: \bigoplus_{i \in I} M_i \rightarrow N$ such that $f_j = f \circ l_j$ for all $j \in I$. In diagram form,

$$\begin{array}{ccc} M_j & \xrightarrow{l_j} & \bigoplus_{i \in I} M_i \\ & \searrow f_j & \downarrow f \\ & & N \end{array}$$

commutes. N is furthermore unique up to unique isomorphism with these properties.

Proof. Basically the same as for direct products. $\square$

3.2 Generation of Modules

Definition 3.3. Let $\{N_i \mid i \in I\}$ be a family of submodules of an R -module M . We define

$$\sum_{i \in I} N_i = \left\{ \sum_{i \in I} m_i \mid m_i \in N_i, m_i = 0 \text{ for all but finitely many } i \right\}$$

. Given $m \in M$ we write $Rm = \{rm \mid r \in R\}$.

If $M = \sum_{i \in I} Rm_i$ for some set $\{m_i\} \subseteq M$ then we call $\{m_i\}$ a *set of generators* of M , or the set *generates* M .

M is *finitely generated* if it has a finite set of generators.

Definition 3.4. A *free* R -module M is a module such that $M \cong \bigoplus_i M_i$ where $M_i \cong R$ for all $i \in I$. A *finitely generated free* R -module is a finite direct sum of copies of R .

Proposition 3.3. An R -module M is finitely generated if and only if there is a surjective R -module homomorphism $R^n \rightarrow M$ for some $n \geq 0$.

Proof. In the forwards direction, let $m_1, \dots, m_n$ is a finite generating set of M . We can define $R^n \rightarrow M$ by $f(r_1, \dots, r_n) = \sum_{i \in I} r_i m_i$, which is surjective as $\{m_1, \dots, m_n\}$ generates M .

In the other direction, suppose $f: R^n \rightarrow M$ is surjective and denote by $e_i = (0, \dots, 1, \dots, 0)$ with the 1 in the i th position. As $e_1, \dots, e_n$ generates R^n , $f(e_1), \dots, f(e_n)$ generates M so we are done. $\square$

Theorem 3.1. (Cayley-Hamilton theorem) If M is a finitely generated R -module, $I \trianglelefteq R$, $f: M \rightarrow M$ is an R -homomorphism such that $f(M) \subseteq IM$. Then $f^n + i_{n-1}f^{n-1} + \dots + i_0 = 0$ in $\text{End}_R(M)$ for some $i_{n-1}, \dots, i_0 \in I$

Proof. Let $\{m_1, \dots, m_n\}$ be a set of generators of M . We know $f(m_i) \in IM$, so we can write $f(m_i) = \sum_{j=1}^n r_{ij} m_j$ with $r_{ij} \in I$, ie

$$\sum_{k=1}^n (\delta_{jk} f - r_{jk}) m_j = 0$$

If we package this into a matrix, we get $(If - (r_{ij}))(m_k)_{1 \leq k \leq n} = 0$. Applying the adjugate matrix to both sides, we get $\det(If - (r_{ij}))(m_k)_{1 \leq k \leq n} = 0$, so $\det(If - (r_{ij}))(m_k) = 0$ for all $1 \leq k \leq n$, so $\det(If - (r_{ij}))$ acts as 0 multiplication on M , so expanding the determinant via the usual expansion, the result follows. $\square$

Corollary 3.1.1. Let M be a finitely generated R module and let $I \trianglelefteq R$ such that $IM = M$. Then there is $r \in R$ such that $r + I = 1 + I$ and $rM = 0$. Hence $1 - r \in I$ and $(1 - r)M = M$

Proof. Apply the Cayley Hamilton theorem with $f = \text{id}$ and let $r = 1 + i_{n-1} + \dots + i_0$. This acts as 0 on M , and $r + I = 1 + I$. $\square$

Corollary 3.1.2. (*Nakayama's lemma*) Let M be a finitely generated R -module and let $I \trianglelefteq R$ be a subset of $\mathcal{J}(R)$. Then $IM = M$ implies $M = 0$

Proof. By the corollary, $rM = 0$ for some $r \in 1 + I$, but then r is a unit, as $r = 1 - i$ for some $i \in I \subseteq \mathcal{J}(R)$, so $M = 0$. $\square$

Remark. Restating this, $M \neq 0$ implies $IM \subsetneq M$ for $I \subseteq \mathcal{J}(R)$

Example 3.2. 1. If $R = k[t]$, $k = \bar{k}$, then $\text{mSpec}(R) = \{(t - \lambda) \mid \lambda \in k\}$ so $\mathcal{J}(R) = \{0\}$ as k is infinite.

2. If $R = k[[t]]$, then $\text{mSpec}(R) = \{(t)\}$ as every other element is a unit. Therefore $\mathcal{J}(R) = (t)$

Definition 3.5. A non-zero R -module M is *simple* (or *irreducible*) if it has no submodules other than $0, M$

Remark. The 0 module is considered to be non-simple.

Proposition 3.4. The set of simple R -modules is in bijection with the set of quotients of R by maximal ideals

Proof. Every quotient of R by a maximal ideal is simple as their submodules correspond to ideals lying between $\mathfrak{m}$ and R , so there is only the 0 module (corresponding to $\mathfrak{m}$), and R/I (corresponding to R).

Suppose $M \neq 0$ is a simple R module. If $0 \neq m \in M$, then $Rm \leq M$ is a submodule, so $Rm = M$. Hence there is a surjection $R \rightarrow M$, so $M \cong R/I$ for some ideal I and by the first half, I is maximal. $\square$

Proposition 3.5. $\mathcal{J}(R) = \{r \in R \mid rM = 0 \text{ for all simple } M\}$

Proof. $\subseteq$ as $M = R/\mathfrak{m}$ for some maximal $\mathfrak{m}$, so $\mathcal{J}(R) \subseteq \mathfrak{m}$ acts trivially on M . $\supseteq$ We know r acts as 0 on every $R/\mathfrak{m}$ if $r \in \mathfrak{m}$ (as in particular, $r + \mathfrak{m} = r(1 + \mathfrak{m}) = \mathfrak{m}$) for all maximal $\mathfrak{m}$, so $r \in \mathcal{J}(R)$ $\square$

Lemma 3.2. (*Schur's lemma*) If M, N are simple R -modules, then if $f: M \rightarrow N$ is an R -module homomorphism, then it is 0 or an isomorphism

Proof. $\ker f$ is a submodule of M , so it is 0 or M . If it is M then $f = 0$, if it is 0 , then f is injective. The $\text{im } f$ is similarly either 0 (then $f = 0$) or N , so it is surjective. Therefore f is either 0 or bijective, so we are done. $\square$

4 Localisation

Definition 4.1. Let R be an integral domain. The *field of fractions* of R is $\text{Frac } R$ with elements equivalence classes of pairs (r, s) where $r \in R, s \in R \setminus 0$ modulo $(r, s) \sim (r', s')$ if $rs' - sr' = 0$, with addition $(r, s) + (r', s') = (rs' + sr', ss')$ and multiplication $(r, s)(r', s') = (rr', ss')$

Localisation generalises this

Definition 4.2. Let R be a ring and $S \subseteq R$. We say S is *multiplicatively closed* if $1 \in S$ and if $ab \in S$ whenever $a, b \in S$.

From now on, S will be a multiplicatively closed subset of R . We define $\sim$ on $R \times S$ via $(r, s) \sim (r', s')$ if $(rs' - sr')t = 0$ for some $t \in S$.

Lemma 4.1. $\sim$ as defined above is an equivalence relation

Proof. Reflexive and symmetric are immediate.

For transitivity, suppose $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$ so there are $t, t' \in S$ so that $(r_1s_2 - r_2s_1)t = 0$ and $(r_2s_3 - r_3s_2)t' = 0$. Then $(r_1s_2s_3 - r_2s_1s_3)tt' = 0$ and $(r_2s_3s_1 - r_3s_2s_1)t't = 0$, so $(r_1s_2s_3 - r_3s_1s_2)tt' = 0$, so $(r_1s_3 - r_3s_1)tt's_2 = 0$, hence as $tt's_2 \in S$ by multiplicative closure, $(r_1, s_1) \sim (r_3, s_3)$ $\square$

Definition 4.3. We denote by r/s the $\sim$ equivalence class of (r, s) . The *localisation of R at S* is $S^{-1}R = \{r/s \mid r \in R, s \in S\}$. We define $r_1/s_1 + r_2/s_2 = (r_1s_2 + r_2s_1)/(s_1s_2)$ and $(r_1/s_1) \cdot (r_2/s_2) = r_1r_2/s_1s_2$.

Lemma 4.2.

1. Addition and multiplication are well defined in $S^{-1}R$
2. $S^{-1}R$ is a commutative unital ring
3. $f: R \rightarrow S^{-1}R$ by $r \mapsto r/1$ is a ring homomorphism, which we call the *localisation homomorphism*

Proof. Exercise. $\square$

Proposition 4.1. (Universal property of localisation) With R a ring and S a multiplicatively closed subset, if $g: R \rightarrow R'$ is a ring homomorphism such that $g(s)$ is a unit of R' for all $s \in S$, then there is a unique ring homomorphism $h: S^{-1}R \rightarrow R'$ such that $g = h \circ f$, where f is the localisation homomorphism

$$\begin{array}{ccc} R & \xrightarrow{g} & R' \\ & \searrow f & \uparrow h \\ & & S^{-1}R \end{array}$$

Proof. We first show h is unique if it exists. Note that for any $r \in R$, $h(r/1) = h(f(r)) = g(r)$ and moreover if $s \in S$, $h(1/s) = h((s/1)^{-1}) = h(s/1)^{-1} = g(s)^{-1}$, so that we must have $h(r/s) = g(r)g(s)^{-1}$.

We now show that h exists. We define $h(r/s) = g(r)g(s)^{-1}$, and need to show this is a well defined ring homomorphism. Suppose $(r, s) \sim (r', s')$. Then

$$\begin{aligned} g(r)g(s^{-1}) - g(r')g(s')^{-1} &= g(s^{-1}s'^{-1})(g(rs') - g(r's)) \\ &= g(s^{-1}s'^{-1}t^{-1})(g((rs' - r's)t)) \\ &= 0 \end{aligned}$$

for t witnessing the equivalence of the pairs. It is easy to show that h is a ring homomorphism, so we are done. $\square$

Proposition 4.2. $\ker(f: R \rightarrow S^{-1}R) = 0$ if and only if S contains no zero divisors

Proof. $r/1 = 0 = 0/1$ if and only if there is $s \in S$ such that $sr = 0$, so there is something in the kernel of f if and only if some $s \in S$ is a zero divisor, and further $\ker f = \{r \in R \mid tr = 0, t \in S\}$ $\square$

Remark. If $I \subseteq R$, then $R \setminus I$ is multiplicatively closed if and only if I is prime.

Example 4.1.

1. If $f \in R$ and $S = \{1, f, f^2, \dots\}$ we write A_f for $S^{-1}R$ and say that R_f is A localised at f .
2. If $\mathfrak{p} \subseteq R$ is prime, then $S = R \setminus \mathfrak{p}$ is multiplicatively closed, and we write $R_{\mathfrak{p}}$ for $S^{-1}R$.
3. If $R = \mathbb{Z}$ and $\mathfrak{p} = (p)$ for p a prime number. Then $R_{\mathfrak{p}} = \{\frac{m}{n} \in \mathbb{Q} \mid p \nmid n\}$.
4. If $f \in k[t_1, \dots, t_n] = R$ and $k = \bar{k}$, then $R_f = \{g/h \in k(t_1, \dots, t_n) \mid h = f^n, n \in \mathbb{Z}_{\geq 0}\}$. These are rational functions which are well defined (regular) on $k^n \setminus V(f)$.
5. If $\mathfrak{p} \subseteq R = k[t_1, \dots, t_n]$ is prime, then $R_{\mathfrak{p}} = \{f/g \in k(t_1, \dots, t_n) \mid g \notin \mathfrak{p}\}$. This is the set of rational functions which are well defined almost everywhere on a variety $V(\mathfrak{p})$.

Definition 4.4. If M is an R -module, define $\sim$ on $M \times S$ by $(m, s) \sim (m', s')$ if $t(ms' - m's) = 0$ for some $t \in S$. We define m/s to be the $\sim$ equivalence class of (m, s) and we define $m_1/s_1 + m_2/s_2 = (m_1s_2 + m_2s_1)/(s_1s_2)$ and an $S^{-1}R$ action on the set of such equivalence classes by $(r/s) \cdot (m/t) = rm/st$. We denote the resulting $S^{-1}R$ module by $S^{-1}M$.

Lemma 4.3. The above definition is well defined

Proof. Exercise. $\square$

Definition 4.5. Given $u: M \rightarrow N$ an R -module homomorphism, we get an $S^{-1}R$ -module homomorphism $S^{-1}u: m/s \mapsto u(m)/s$

Lemma 4.4. The above homomorphism is a well defined $S^{-1}R$ -homomorphism

Proof. exercise $\square$

Lemma 4.5. Given R -module homomorphisms $v: M \rightarrow N$ and $u: L \rightarrow M$ then $S^{-1}(vu) = S^{-1}v \circ S^{-1}u$

Proof. $S^{-1}(vu)(l/s) = (vu(l))/s = S^{-1}v(u(l)/s) = (S^{-1}v \circ S^{-1}u)(l/s)$ $\square$

Definition 4.6. (Inexact definition) A *functor* is an operation which acts on both R -modules and R -module homomorphisms which respects composition

Corollary 4.5.1. *Localisation is a functor*

Proof. Trivial □

Definition 4.7. Homomorphisms $A \xrightarrow{f} B \xrightarrow{g} C$ are *exact at B* if $\text{Im}(f) = \ker(g)$. We say a longer sequence

$$\dots \xrightarrow{f_{i+3}} A_{i+2} \xrightarrow{f_{i+2}} A_{i+1} \xrightarrow{f_{i+1}} A_i \xrightarrow{f_i} A_{i-1} \xrightarrow{f_{i-1}} \dots$$

is *exact* if it is exact at each A_i .

Example 4.2. 1. $0 \rightarrow L \xrightarrow{f} M$ is exact if and only if f is injective

2. $L \xrightarrow{f} M \rightarrow 0$ is exact if and only if f is surjective

3.

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

is exact if and only if $N \cong M/L$ induced by the surjection. These are called *short exact sequences*

Definition 4.8. A functor F is called *exact* if whenever $L \xrightarrow{f} M \xrightarrow{g} N$ is exact, then so is $FL \xrightarrow{Ff} FM \xrightarrow{Fg} FN$

Proposition 4.3. *Localisation is an exact functor*

Proof. Suppose $L \xrightarrow{f} M \xrightarrow{g} N$ is exact. We want to show $S^{-1}L \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}N$ is exact. Now $S^{-1}g \circ S^{-1}f = S^{-1}(gf) = S^{-1}0 = 0$, so it suffices to show $\ker S^{-1}g \subseteq \text{im } S^{-1}f$. Let $m/s \in \ker S^{-1}g$. Then $g(m)/s = 0$ so there is $t \in S$ with $tg(m) = 0$. So $g(tm) = 0$ and hence $tm \in \ker g = \text{im } f$, so there is $l \in L$ with $f(l) = tm$. In $S^{-1}M$, we have $m/s = tm/ts = f(l)/ts = S^{-1}f(l/st)$, so we are done. □

Corollary 4.5.2. *Let M be an R -module with submodules L, N . Then*

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

$$2. S^{-1}(L \cap N) = S^{-1}L \cap S^{-1}N$$

$$3. S^{-1}(M/L) = S^{-1}M/S^{-1}L$$

Proof. 1. Trivial.

2. $S^{-1}(L \cap N) \subseteq S^{-1}L \cap S^{-1}N$ is immediate. Let $x \in S^{-1}L \cap S^{-1}N$. Then $x = l/s = n/t$ with $l \in L, n \in N, s, t \in S$. Then there is $u \in S$ such that $(tl - sn)u = 0$, so if we set $m = utl = usn$, then $m/uts = l/s = n/t \in S^{-1}(L \cap N)$.

3. We have a short exact sequence

$$0 \longrightarrow L \longrightarrow M \longrightarrow M/L \longrightarrow 0$$

, so by exactness we get a short exact sequence

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

so the result follows. $\square$

Definition 4.9. If $f: M \rightarrow N$ is an R -module homomorphism, the *cokernel* of f is $\text{coker } f = N/f(M)$

Corollary 4.5.3. If $f: M \rightarrow N$ is an R -module homomorphism, then

1. $\ker S^{-1}f = S^{-1}\ker f$
2. $\text{coker } S^{-1}f = S^{-1}\text{coker } f$
3. $\text{im } S^{-1}f = S^{-1}\text{im } f$

Proof. We have an exact sequence

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

so we get an exact sequence

$$0 \longrightarrow S^{-1}\ker f \longrightarrow S^{-1}M \xrightarrow{f} S^{-1}N \longrightarrow S^{-1}\text{coker } f \longrightarrow 0$$

so the first two follow. For (3), $S^{-1}f(m/s) = f(m)/s$, so we are done. $\square$

4.1 Local Rings and Local Properties

Definition 4.10. A ring R is *local* if it has a unique maximal ideal $\mathfrak{m}$. We frequently may write $(R, \mathfrak{m})$ is a local ring. In this case, $R/\mathfrak{m}$ is a field which we call the *residue field* of $(R, \mathfrak{m})$

Proposition 4.4. If $\mathfrak{p} \trianglelefteq R$ is prime, then $R_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{m} = \{p/s \mid p \in \mathfrak{p}\}$

Proof. It is easy to check that $\mathfrak{m}$ is an ideal. For $\mathfrak{m}$ to be a unique maximal ideal, it suffices to prove that if $I \trianglelefteq R_{\mathfrak{p}}$ with $I \not\subseteq \mathfrak{m}$, then $I = R_{\mathfrak{p}}$. Let $I \trianglelefteq R_{\mathfrak{p}}$ with $I \not\subseteq \mathfrak{m}$. Then there is $r/s \in I$ with $r \notin \mathfrak{p}$. But then $s/r \in R_{\mathfrak{p}}$, so $1 = (s/r)(r/s) \in I$, so $I = R$ $\square$

Example 4.3. $R = k[[t]]$ is a local ring with $\mathfrak{m} = (t)$

Definition 4.11. A property P of a ring R is *local* if $P(R)$ is equivalent to “ $P(R_{\mathfrak{p}})$ for all prime ideals $\mathfrak{p}$ ”. A property P of an R -module M is *local* if $P(M)$ is equivalent to “ $P(M_{\mathfrak{p}})$ for all prime ideals $\mathfrak{p}$ ”

Definition 4.12. Let M be an R -module. We define the *annihilator* of M to be $\text{Ann } M = \{r \in R \mid rM = 0\}$. If $N = Rn$ for some $n \in M$, then we write $\text{Ann}(n) = \text{Ann}(N)$

Proposition 4.5. *Being 0 is a local property, ie if M is an R -module, the following are equivalent*

1. $M = 0$
2. $M_{\mathfrak{p}} = 0$ for all prime ideals $\mathfrak{p} \leq R$
3. $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \leq R$

Proof. (1) implies (2) implies (3) are immediate. Suppose (3) holds and $M \neq 0$. Take $0 \neq m \in M$ and let $I = \text{Ann}(m)$. I is a proper ideal since $m \neq 0$, so $1 \notin I$. So there is a maximal ideal $\mathfrak{m}$ with $I \subseteq \mathfrak{m}$. By (3), $M_{\mathfrak{m}} = 0$, so $m/1 = 0/1$ in $M_{\mathfrak{m}}$. So there is $r \in R \setminus \mathfrak{m}$ such that $rm = 0$, contradiction, as then $r \in \text{Ann}(m) \setminus \mathfrak{m} = \emptyset$ $\square$

Proposition 4.6. *Exactness is a local property: If $L \xrightarrow{f} M \xrightarrow{g} N$ is a sequence of R -module homomorphisms, the following are equivalent*

1. $L \xrightarrow{f} M \xrightarrow{g} N$ is exact.
2. $L_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} M_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} N_{\mathfrak{p}}$ is exact for all prime ideals $\mathfrak{p}$.
3. $L_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} M_{\mathfrak{m}} \xrightarrow{g_{\mathfrak{m}}} N_{\mathfrak{m}}$ is exact for all maximal ideals $\mathfrak{m}$.

Proof. (1) implies (2) as localisation is exact, and (3) is a special case of (2). Assume (3). Then $(\text{im}(gf))_{\mathfrak{m}} = \text{im}((gf)_{\mathfrak{m}}) = 0$, and hence $\text{im}(gf) = 0$ as being 0 is a local property, so $g \circ f = 0$ and $\text{im } f \subseteq \ker g$. Therefore we consider $(\ker g)/(\text{im } f)_{\mathfrak{m}}$. By an identical argument this is 0, so (1) follows and we are done. $\square$

Remark. In particular injectivity and surjectivity are local.

Definition 4.13. An R -module M is *locally free* if $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$ module for all prime $\mathfrak{p} \leq R$

Example 4.4. Locally free modules are not always free. Let $R = \mathbb{C} \times \mathbb{C}$. This has two prime ideals $\mathfrak{p}_1 = \mathbb{C} \times \{0\}$ and $\mathfrak{p}_2 = \{0\} \times \mathbb{C}$. We compute the localisation $R_{\mathfrak{p}_1}$. There is a map $R \rightarrow \mathbb{C}$ by projection on the second coordinate. This sends $R \setminus \mathfrak{p}_1$ to units, so there is a map $R_{\mathfrak{p}_1} \rightarrow \mathbb{C}$ which has kernel all elements of the form $(x, 0)/(a, b)$. But these are equal to 0 in $R_{\mathfrak{p}_1}$ as $(x, 0)(0, 1) = (0, 0)$ and $(0, 1) \notin \mathfrak{p}_1$, so R is locally a field and R -modules are locally vector spaces, hence locally free. If we take $M = \mathfrak{p}_1$, then M is not free, but it is locally free.

4.2 Extension and Contraction under Localisation

Definition 4.14. If $I, J \trianglelefteq R$, the *ideal quotient* is $(I : J) = \{r \in R \mid rJ \subseteq I\} \trianglelefteq R$. If $J = (j)$, we write $(I : j)$.

Proposition 4.7. Let $f: R \rightarrow S^{-1}R$ be the localisation homomorphism.

1. Every ideal of $S^{-1}R$ is extended
2. If $I \trianglelefteq R$, then $I^{ec} = \bigcup_{s \in S} (I : s)$
3. $I \trianglelefteq R$ is a contracted ideal if and only if the image of S in R/I has no zero divisors
4. $I^e = S^{-1}R$ if and only if $S \cap I \neq \emptyset$
5. There is a bijection between prime ideals of R not intersecting S and $\text{Spec } S^{-1}R$ by extension and contraction.

Proof. 1. Let $J \trianglelefteq S^{-1}R$, $r/s \in J$. Then $r/1 \in J$, so $r \in R^c$ and $r/s \in J^{ce}$ so $J \subseteq J^{ce} \subseteq J$ and we are done.

2. Let $I \trianglelefteq R$. Now $r \in I^{ec} = (S^{-1}I)^c$ if and only if $r/1 = i/t$ for $i \in I, t \in S$, if and only if $(rt - i)u = 0$ for some $i \in I, t, u \in S$ if and only if $rv \in I$ for some $v \in S$ so we are done.

3. I is contracted if and only if $I \supseteq I^{ec}$ and note that the image of S in R/I contains no zero divisors if and only if $sr \in I$ for $s \in S$ implies $r \in I$. Assume $I \supseteq I^{ec}$ and suppose $sr \in I$. Then $r/1 \in I^e$, so $r \in I^{ec} \subseteq I$. In the other direction assume $sr \in I$ for $s \in S$ implies $r \in I$ and let $r \in I^{ec}$. Then $r/1 \in I^e$, so $sr/1 \in f(I)$ for some $s \in S$, so $sr \in I$ so $r \in I$. (Note this is also immediate from (2))

4. In the backwards direction, suppose $I \cap S \neq \emptyset$ and let $s \in I \cap S$. Then $1 = s/s \in I^e$ so $I^e = S^{-1}R$. In the forwards direction if $I^e = S^{-1}R$ then $1/1 \in I^e$ so $1/1 = r/s$ for $r \in I, s \in S$, so there is $t \in S$ such that $tr = ts \in I \cap S$

5. If $\mathfrak{q} \in \text{Spec } S^{-1}R$ then $\mathfrak{q}^c \in \text{Spec } R$ as we've already proven, and $\mathfrak{q}^c \cap S$ is empty as otherwise $\mathfrak{q} = \mathfrak{q}^{ce} = S^{-1}R$ contradiction (by 1, 4). Conversely suppose $\mathfrak{p} \in \text{Spec } R$. Then $R/\mathfrak{p}$ is an integral domain and (exercise) $S^{-1}R/S^{-1}\mathfrak{p} \cong \bar{S}^{-1}(R/\mathfrak{p})$ where $\bar{S}$ is the image of S in $R/\mathfrak{p}$, so $\bar{S}^{-1}(R/\mathfrak{p}) \subseteq \text{Frac } R/\mathfrak{p}$, so it is 0 or an integral domain, so either $S^{-1}\mathfrak{p} = S^{-1}R$, or it is prime, with the former case if and only if $\mathfrak{p} \cap S \neq \emptyset$. $\square$

Corollary 4.5.4. Let $\mathfrak{p} \trianglelefteq R$. There is a bijection between prime ideals contained in $\mathfrak{p}$ and $\text{Spec } R_{\mathfrak{p}}$

Proof. Trivial $\square$

Proposition 4.8. *If $g: A \rightarrow B$ is a ring homomorphism and $\mathfrak{p} \in \text{Spec } A$, then $\mathfrak{p} = \mathfrak{q}^c$ for $\mathfrak{q} \in \text{Spec } B$ if and only if $\mathfrak{p}^{ec} = \mathfrak{p}$*

Proof. The forward direction is immediate. In the backwards direction, suppose $\mathfrak{p}^{ec} = \mathfrak{p}$ and let $S = g(A \setminus \mathfrak{p})$. Then $\mathfrak{p}^e \cap S = \emptyset$ otherwise $\mathfrak{p} \subsetneq \mathfrak{p}^{ec}$, so $S^{-1}(\mathfrak{p}^e)$ is proper and $S^{-1}(\mathfrak{p}^e) \subseteq \mathfrak{m}$ for a maximal ideal $\mathfrak{m} \trianglelefteq S^{-1}B$. Let $\mathfrak{q} = f^{-1}(\mathfrak{m})$. This is prime. $\mathfrak{q} \supseteq \mathfrak{p}^e$ and $\mathfrak{q} \cap S = \emptyset$ by Proposition 4.7(5), so $\mathfrak{q}^c \supseteq \mathfrak{p}^{ec} = \mathfrak{p}$ but $\mathfrak{q}^c$ is not a proper superset of $\mathfrak{p}$ as it doesn't intersect S , so $\mathfrak{q}^c = \mathfrak{p}$ $\square$

5 Tensor Products

Definition 5.1. Let M, N be R -modules and set $C = R^{M \times N}$ a free R -module. Let $e(m, n)$ be the element of C with 1 in the (m, n) -place, for $m \in M, n \in N$. Elements of C are formal finite R -linear sums of elements of this form. Let D be the submodule of C generated by $\{e(m + m', n) - e(m, n) - e(m', n), e(m, n + n') - e(m, n) - e(m, n'), e(rm, n) - re(m, n), e(m, rn) - re(m, n)\}$ for all $m, m' \in M, n, n' \in N, r \in R$. We define $M \otimes_R N = C/D$. We write $m \otimes n$ for $e(m, n)$. These are called *pure tensors* and they generate (but are not all of) the module.

Definition 5.2. Let L, M, N be R -modules. A map $f: M \times N \rightarrow L$ is *R -bilinear* if $f_n: M \rightarrow L$ by $m \mapsto f(m, n)$ is R linear (and the same holds in the other argument)

Proposition 5.1. (*Universal Product of the Tensor Product*) *There is an R -bilinear map $f: M \times N \rightarrow M \otimes N$ such that for any R -bilinear map $g: M \times N \rightarrow L$ there is a unique $h: M \otimes N \rightarrow L$ such that $g = h \circ f$*

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

Proof. We define $f(m, n) = m \otimes n$. This is R -bilinear by definition of the quotient. To get the h , there is a map $g': C \rightarrow L$ by $e(m, n) \mapsto g(m, n)$. Let $q: C \rightarrow C/D$ be the quotient homomorphism. Since g is R -bilinear, $g'(D) = 0$, so there is a well defined map $h: C/D \rightarrow L$, and g is equal to $h \circ f$. We must always have $h(m \otimes n) = g(m, n)$ by commutativity, so h is determined uniquely $\square$

Remark. We can analogously define R -multilinear maps and multitensor products

Example 5.1.

1. Let $\{e_1, \dots, e_n\}$ and $\{f_1, \dots, f_m\}$ be a K -basis of K -vector spaces E, F . Then $\{e_i \otimes e_j\}$ is an nm -size basis of $E \otimes F$.
2. Consider $\sum_{i=1}^k m_i \otimes n_i, m_i \in \mathbb{Z}, n_i \in \mathbb{Z}/2\mathbb{Z}$. This is equal to $\sum_{i=1}^k 1 \otimes m_i n_i = 1 \otimes \sum_{i=1}^k m_i n_i$, so if $x \in \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ then $x = 1 \otimes n, n \in \mathbb{Z}/2\mathbb{Z}$ and in fact $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$

3. Consider $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ and suppose $m \in \mathbb{Z}/3\mathbb{Z}, n \in \mathbb{Z}/2\mathbb{Z}$. Then $m \otimes n = m \otimes 3n = 3m \otimes n = 0 \otimes n = 0$ so $\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = 0$

Lemma 5.1. *Let $m_1, \dots, m_k \in M$ and $n_1, \dots, n_k \in N$ such that $\sum m_i \otimes n_i = 0$ in the tensor product. Then there are finitely generated submodules $M' \leq M, N' \leq N$ which contain all the m_i, n_i respectively and such that $\sum m_i \otimes n_i = 0$ in $M' \otimes N'$*

Proof. As $\sum m_i \otimes n_i = 0$ in $M \otimes N$, $\sum e(m_i, n_i) \in D$, so can be written as a finite sum of some generators of D . Let M' be the submodule generated by the m_i and the m -factors in the generators of D used, and similarly for N' . Then in $M' \otimes N'$, $\sum e(m_i, n_i) =$ same sum of generators but now the generators are in D' (as all of the factors of them are in M', N' , and the generators of D' are all those of the same form as D), so $\sum m_i \otimes n_i = 0$ in $M' \otimes N'$ $\square$

Proposition 5.2. *If L, M, N are R -modules, then $(L \oplus M) \otimes N \cong (L \oplus N) \otimes (M \oplus N)$ by $(l, m) \otimes n \mapsto (l \otimes n, m \otimes n)$*

Proof. Define a R -bilinear map $(L \oplus M) \times N \rightarrow (L \otimes N) \oplus (M \otimes N)$ by $((l, m), n) \mapsto (l \otimes n, m \otimes n)$ which descends by the universal property. We can define an inverse by $L \times N \rightarrow (L \oplus M) \otimes N$ by $(l, n) \mapsto (l, 0) \otimes n$ (and similar for M), use the universal property of the direct sum to combine them, and then check the two maps we've defined are mutually inverse. $\square$

Proposition 5.3. *If L, M, N are R modules, then*

1. $M \otimes N \cong N \otimes M$
2. $(L \otimes M) \otimes N \cong L \otimes (M \otimes N) \cong L \otimes M \otimes N$
3. $R \otimes M \cong M$
4. $(L \oplus M) \otimes N \cong (L \oplus N) \otimes (M \oplus N)$

Proof. (4) is above, (1)-(3) are on example sheet 2. $\square$

Definition 5.3. If $f: M \rightarrow M'$ and $g: N \rightarrow N'$ are R -module homomorphisms, we define $h: M \times N \rightarrow M' \otimes N'$ by $(m, n) \mapsto f(m) \otimes g(n)$. This is R -bilinear as f, g are R -linear, so we get a map $f \otimes g: M \otimes N \rightarrow M' \otimes N'$ by $m \otimes n \mapsto f(m) \otimes g(n)$.

Lemma 5.2. *If $f: M' \rightarrow M'', g': N' \rightarrow N''$ are additional R -module homomorphisms, then $(f' \otimes g')(f \otimes g) = (f'f \otimes g'g)$*

Proof. They trivially agree on pure tensors, and pure tensors generate the tensor product. $\square$

Example 5.2. If k is a field and $S: k^m \rightarrow k^r, T: k^n \rightarrow k^s$ are k -linear with the four vector spaces having bases $\{e_i\}, \{f_i\}, \{e'_i\}, \{f'_j\}$ respectively. We write $[S], [T]$ for the matrices of S, T in these bases and $[S]_{ki}$ for their entries. $\{e_i \otimes e'_j\}$ is a basis of $k^m \otimes k^n$ and $\{f_i \otimes f'_j\}$ is a basis of $k^r \otimes k^s$. In this basis, the matrix of $S \otimes T$ is $[S \otimes T]_{ij,kl} = [S]_{ki}[T]_{lj}$

Proposition 5.4. *If $S \subseteq R$ is a multiplicatively closed subset and M is an R -module, then there is an isomorphism $f_M: S^{-1}R \otimes_R M \rightarrow S^{-1}M$ via $r/s \otimes m \mapsto rm/s$ and this isomorphism is natural, ie given $h: M \rightarrow N$ an R -module homomorphism, the following commutes*

$$\begin{array}{ccc} S^{-1}R \otimes M & \xrightarrow{1_{S^{-1}R} \otimes h} & S^{-1}R \otimes N \\ \downarrow f_M & & \downarrow f_N \\ S^{-1}M & \xrightarrow{S^{-1}h} & S^{-1}N \end{array}$$

Proof. We define $S^{-1}R \otimes M \rightarrow S^{-1}M$ by $(r/s, m) \mapsto (rm/s)$ so by the universal property of the tensor product we get f_M . This map is clearly surjective. We want to show the map is injective. We first show every element of $S^{-1}R \otimes_R M$ is of the form $1/s \otimes m$. Let $m' = \sum_i (r_i/s_i) \otimes m_i$ be an element of the tensor product and let $s = \prod_i s_i$ and let $t_i = \prod_{j \neq i} s_j$. Then

$$\begin{aligned} m' &= \sum_i (r_i t_i / s) \otimes m_i \\ &= \sum_i (1/s) \otimes r_i t_i m_i \\ &= 1/s \otimes \sum_i r_i t_i m_i \end{aligned}$$

so every element of $S^{-1}R \otimes_R M$ is of the form $1/s \otimes m$. Now let $1/s \otimes m \in S^{-1}R \otimes_R M$ and suppose $f_M(1/s \otimes m) = 0$. Then $m/s = 0 \in S^{-1}M$, so there is $t \in S$ with $tm = 0$ in M , so $1/s \otimes m = 1/st \otimes tm = 0$ and so f_M is injective and hence an isomorphism. To show naturality, we need only show the square commutes on pure tensors, which is clear. $\square$

Lemma 5.3. *If M, N are R -modules, there is an isomorphism of $S^{-1}R$ -modules $f: S^{-1}M \otimes_{S^{-1}R} S^{-1}N \rightarrow S^{-1}(M \otimes_R N)$ by $(m/s) \otimes (n/t) \mapsto (m \otimes n)/(st)$*

Proof.

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

and tracing the isomorphisms given gives the result on elements. $\square$

5.1 Restriction and Extension of Scalars

Let $f: A \rightarrow B$ be a ring homomorphism

Definition 5.4. (Restriction of Scalars) Let M be a B -module. Then M is an A -module via $a \cdot m = f(a)m$ where $a \in A, m \in M$

Definition 5.5. (Extension of Scalars) Let N be an A -module. Note that B is an A module by restriction of scalars. We define the extension of scalars on N as $B \otimes_A N$, which is a B -module by acting on the B component.

Remark. Localising an R -module M is the same as extending scalars to $S^{-1}R$

Proposition 5.5. Let $f: A \rightarrow B$ be a ring homomorphism making B a finitely generated A -module. Let M be a finitely generated B -module. Then M is a finitely generated A -module.

Proof. Let $\{b_1, \dots, b_k\}$ generate B as an A module and let $\{m_1, \dots, m_l\}$ generate M as a B module. Then $\{b_i m_j \mid 1 \leq i \leq k, 1 \leq j \leq l\}$ generates M as an A -module $\square$

Proposition 5.6. If $f: A \rightarrow B$ is a ring homomorphism and N is a finitely generated A module, then $B \otimes_A N$ is a finitely generated B -module

Proof. If $\{n_1, \dots, n_l\}$ generate n as an A module, then $\{1 \otimes n_1, \dots, 1 \otimes n_l\}$ generate $B \otimes_A N$ as a B module as if $a \in A$, $f(a)(1 \otimes n_i) = f(a) \otimes n_i = (a \cdot 1) \otimes n_i = 1 \otimes an_i$, so $1 \otimes N$ is generated by them, and then multiplying by B gives the result $\square$

Definition 5.6. Given a ring R , an R -algebra A is an R -module which is also a ring such that for all $r \in R, a_1, a_2 \in A$, $r(a_1 a_2) = (ra_1)a_2 = a_1(ra_2)$

Proposition 5.7. R -algebras are equivalent to rings A with a ring homomorphism $f: R \rightarrow A$

Proof. Let A be an R -algebra. Define $f: R \rightarrow A$ by $r \mapsto r \cdot 1$. This is a ring homomorphism as $(r_1 r_2) \cdot 1 = r_1 \cdot (r_2 \cdot 1) = (r_1 \cdot 1) \cdot (r_2 \cdot 1)$.

Let A be a ring with a homomorphism $f: R \rightarrow A$. A is an R module by restriction of scalars, and the condition to be an algebra is just associativity in A . $\square$

Definition 5.7. Let A, B be R -algebras. Then an R -algebra homomorphism $h: A \rightarrow B$ is a module homomorphism which is also a ring homomorphism

Proposition 5.8. Suppose $f: R \rightarrow A, g: R \rightarrow B$ be the ring homomorphisms making A, B into R -algebras. Then $h: A \rightarrow B$ is an R -algebra homomorphism if and only if h is a ring homomorphism and $h \circ f = g$

Proof. Let $a \in A, r \in R$. Then $h(rm) = h(f(r)m) = hf(r)h(m) = g(r)h(m) = rh(m)$ gives one direction, and splitting it in the middle and equating the ends and setting $m = 1$ gives the other. $\square$

Example 5.3.

1. If k is a field, then $k[x_1, \dots, x_n]$ is a k -algebra, with the homomorphism being inclusion

2. Rings are equivalent to $\mathbb{Z}$ -algebras as there is always exactly one homomorphism $\mathbb{Z} \rightarrow R$ by $1 \mapsto 1$.

Let $f: R \rightarrow A$ be a ring homomorphism. Recall A is finitely generated as an R -module if there are $a_1, \dots, a_n$ such that for all $a \in A$, a can be written in the form $\sum_{i=1}^n a_i r_i$ with $r_i \in R$.

Definition 5.8. A is *finitely generated as an R -algebra* if there are $\{a_1, \dots, a_n\} \subseteq A$ such that for any $a \in A$ there are $r_{i_1, \dots, i_n}$ with $a = \sum_{i_1, \dots, i_n \geq 0} r_{i_1, \dots, i_n} a_1^{i_1} \dots a_n^{i_n}$.

Remark. If A is finitely generated as an R -module, then it is finitely generated as an R -algebra.

Proposition 5.9. A is a finitely generated R -algebra if there is a surjective R -algebra homomorphism $R[t_1, \dots, t_n] \rightarrow A$.

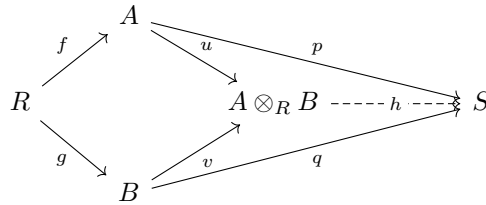
Proof. Exercise. □

Definition 5.9. Let $f: R \rightarrow A, g: R \rightarrow B$ be ring homomorphisms. We define the R -module $C = A \otimes_R B$ and give it an R -algebra structure by $A \times B \times A \times B \rightarrow C$ via $(a, b, a', b') \mapsto aa' \otimes bb'$, so we get a map $A \otimes B \otimes A \otimes B \rightarrow C$, and hence a map $C \otimes C \rightarrow C$ given on pure tensors in the obvious way, so we get an R -bilinear map $\mu: C \times C \rightarrow C$ by $\mu(a \otimes b, a' \otimes b') = (aa' \otimes bb')$.

Remark. We know $r(a \otimes b) = f(r)a \otimes b = a \otimes g(r)b$ and hence we get a ring homomorphism $R \rightarrow C$ by $r \mapsto r(1 \otimes 1) = f(r) \otimes 1 = 1 \otimes g(r)$.

Example 5.4. If we have $k[x_1] \otimes_k k[x_2]$, this is isomorphic to $k[t_1, t_2]$.

Proposition 5.10. (*Universal property of Tensor Products of Algebras*) Let $f: R \rightarrow A, g: R \rightarrow B$ be ring homomorphisms. Then there are ring homomorphisms $u: A \rightarrow A \otimes_R B$ and $v: B \rightarrow A \otimes_R B$ such that $u \circ f = v \circ g$, and for any ring S with ring homomorphisms $p: A \rightarrow S, q: B \rightarrow S$ such that $p \circ f = q \circ g$, there is a unique map $h: A \otimes_R B \rightarrow S$ such that $p = h \circ u, q = h \circ v$.



Proof. We define $u(a) = a \otimes 1, v(b) = 1 \otimes b$. Then $u(f(r)) = f(r) \otimes 1 = 1 \otimes g(r) = v(g(r))$, so $u \circ f = v \circ g$.

We define $A \times B \rightarrow S$ by $(a, b) \mapsto p(a)q(b)$ which is R -bilinear, so we get a map $h: A \otimes_R B \rightarrow S$ via $h(a \otimes b) = p(a)q(b)$. Now $h(u(a)) = p(a)$ by definition and similar for $h \circ v$. We need to show h is a ring homomorphism. $h((a \otimes b)(a' \otimes b')) = h(aa' \otimes bb') = p(aa')q(bb') = p(a)q(b)p(a')q(b') = h(a \otimes b)h(a' \otimes b')$. h is unique as we must have $h(a \otimes 1) = p(a), h(1 \otimes b) = q(b)$. These immediately force $h(a \otimes b) = p(a)q(b)$, so h is unique on pure tensors, hence unique. So we are done. □

Remark. The tensor product of algebras is the pushout of rings.

5.2 Exactness properties of Hom and $\otimes$

Fix an R -module P . Then $\cdot \otimes P$ is a functor, where $f: L \rightarrow M$, an R -module homomorphism, maps to $f \otimes 1_P$. This functor is not always exact, eg

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

(with the first map being multiplication by 2). If we apply $\cdot \otimes \mathbb{Z}/2\mathbb{Z}$ we get

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

which is just

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{1} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

which is not exact. However,

$$\mathbb{Z}/2\mathbb{Z} \xrightarrow{0} \mathbb{Z}/2\mathbb{Z} \xrightarrow{1} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

is exact.

Definition 5.10. A functor F is *right exact* if given an exact sequence

$$L \xrightarrow{f} M \xrightarrow{g} N \rightarrow 0$$

the sequence

$$F(L) \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(N) \rightarrow 0$$

is exact. A functor is *left exact* if exact sequences

$$0 \rightarrow L \xrightarrow{f} M \xrightarrow{g} N$$

map to exact sequences

$$0 \rightarrow F(L) \xrightarrow{F(f)} F(M) \xrightarrow{F(g)} F(N)$$

Lemma 5.4. A functor F is exact if and only if it is left and right exact

Proof. The forwards direction is immediate.

For the backwards direction, note that if F is left and right exact, then F sends short exact sequences to short exact sequences. Suppose we have an exact sequence $L \xrightarrow{f} M \xrightarrow{g} N$ of R -module homomorphisms. Then there are short exact sequences

$$0 \longrightarrow \ker f \longrightarrow L \longrightarrow \operatorname{im} f \longrightarrow 0$$

$$0 \longrightarrow \operatorname{im} f \longrightarrow M \longrightarrow \operatorname{im} g \longrightarrow 0$$

$$0 \longrightarrow \operatorname{im} g \longrightarrow N \longrightarrow N/\operatorname{im} g \longrightarrow 0$$

Applying F , we get short exact sequences

$$0 \longrightarrow F(\ker f) \longrightarrow F(L) \longrightarrow F(\operatorname{im} f) \longrightarrow 0$$

$$0 \longrightarrow F(\operatorname{im} f) \longrightarrow F(M) \longrightarrow F(\operatorname{im} g) \longrightarrow 0$$

$$0 \longrightarrow F(\operatorname{im} g) \longrightarrow F(N) \longrightarrow F(N/\operatorname{im} g) \longrightarrow 0$$

We want to show $F(L) \rightarrow F(M) \rightarrow F(N)$ is exact. Now

$$\begin{aligned} \operatorname{im} F(f) &= \operatorname{im} F(L \rightarrow \operatorname{im} f \rightarrow M) \\ &= \operatorname{im} F(\operatorname{im} f \rightarrow M) \\ &= \ker F(M \rightarrow \operatorname{im} g) \\ &= \ker F(M \rightarrow \operatorname{im} g \rightarrow N) \\ &= \ker F(g) \end{aligned}$$

so we are done $\square$

Definition 5.11. Let M be an R -module and let $g: N \rightarrow N'$ be an R -module homomorphism. We define $g_*: \operatorname{Hom}_R(M, N) \rightarrow \operatorname{Hom}_R(M, N')$ by $\phi \mapsto g \circ \phi$. Similarly if $f: M \rightarrow M'$ is an R -module homomorphism, then we define $f^*: \operatorname{Hom}_R(M', N) \rightarrow \operatorname{Hom}_R(M, N)$ by $\phi \mapsto \phi \circ f$.

Remark. f^*, g_* are both R -module homomorphisms.

Lemma 5.5. This makes $\operatorname{Hom}_R(M, \cdot)$ and $\operatorname{Hom}_R(\cdot, M)$ into functors.

Proof. Trivial $\square$

Remark. Functors like $\operatorname{Hom}_R(\cdot, N)$ which reverse direction are called *contravariant* (normal functors are *covariant*)

Proposition 5.11. Hom functors are left exact and even

1. A sequence of R -module homomorphisms $L \rightarrow M \rightarrow N \rightarrow 0$ is exact if and only if $0 \rightarrow \operatorname{Hom}_R(N, P) \rightarrow \operatorname{Hom}_R(M, P) \rightarrow \operatorname{Hom}_R(L, P)$ is exact for all R -modules P
2. A sequence of R -module homomorphisms $0 \rightarrow L \rightarrow M \rightarrow N$ is exact if and only if $0 \rightarrow \operatorname{Hom}_R(P, L) \rightarrow \operatorname{Hom}_R(P, M) \rightarrow \operatorname{Hom}_R(P, N)$ is exact for all R -modules P

Proof. See example sheet 2. $\square$

Proposition 5.12. (Tensor-Hom Adjunction) Let L, M, N be R -modules. Then there is an isomorphism of R -modules

$$\operatorname{Hom}_R(L \otimes_R M, N) \rightarrow \operatorname{Hom}_R(L, \operatorname{Hom}_R(M, N))$$

Proof. First we exhibit a bijection between the two sets. Given an R -linear map f , we get by the universal property an R -bilinear map $\tilde{f}: L \times M \rightarrow N$, we define $\phi(f): L \rightarrow \text{Hom}_R(M, N)$ by $l \mapsto (m \mapsto \tilde{f}(l, m))$. Conversely given $g: L \rightarrow \text{Hom}_R(M, N)$ we define $\tilde{\psi}(g): L \times M \rightarrow N$ by $(l, m) \mapsto g(l)(m)$. This is R -bilinear so this descends to a map $\psi(g): L \otimes_R M \rightarrow N$. Then $\phi \circ \psi(g)(l) = (m \mapsto \psi(g)(l \otimes m)) = (m \mapsto g(l)(m)) = g(l)$ so $\phi \circ \psi = 1$, and the reverse is similar.

We verify ϕ is an R module homomorphism. If $r \in R$, then

$$\begin{aligned}\phi(rf)(l) &= (m \mapsto rf(l, m)) \\ &= r(m \mapsto f(l, m)) \\ &= r \cdot \phi(f)(l)\end{aligned}$$

and ψ is similar so we are done. $\square$

Proposition 5.13. *The tensor-hom adjunction is natural in L, N . Naturality in L (N is similar) means that given an R -module homomorphism $f: L \rightarrow L'$, the following diagram commutes*

$$\begin{array}{ccc}\text{Hom}_R(L' \otimes_R M, N) & \xrightarrow{\phi_{L'}} & \text{Hom}_R(L', \text{Hom}_R(M, N)) \\ \downarrow (f \otimes 1_M)^* & & \downarrow f^* \\ \text{Hom}_R(L \otimes_R M, N) & \xrightarrow{\phi_L} & \text{Hom}_R(L, \text{Hom}_R(M, N))\end{array}$$

Proof. Let $g \in \text{Hom}_R(L' \otimes_R M, N)$ and let $l \in L$. We want to show that $(\phi_L \circ (f \otimes 1_M)^*)(g)(l) = (f^* \circ \phi_{L'})(g)(l)$. We have

$$\begin{aligned}(\phi_L \circ (f \otimes 1_M)^*)(g)(l) &= (\phi_L \circ (g \circ (f \otimes 1_M)))(l) \\ &= (m \mapsto (g \circ (f \otimes 1_M))(l \otimes m)) \\ &= (m \mapsto g(f(l) \otimes m)) \\ &= \phi_{L'}(g)(f(l)) \\ &= (\phi_{L'}(g) \circ f)(l) \\ &= (f^* \circ \phi_{L'})(g)(l)\end{aligned}$$

$\square$

Definition 5.12. Two sequences are *isomorphic* if there is a commutative diagram

$$\begin{array}{ccccccc}\dots & \longrightarrow & M_{i-1} & \longrightarrow & M_i & \longrightarrow & M_{i+1} \longrightarrow \dots \\ & & \downarrow & & \downarrow & & \downarrow \\ \dots & \longrightarrow & N_{i-1} & \longrightarrow & N_i & \longrightarrow & N_{i+1} \longrightarrow \dots\end{array}$$

with all vertical maps isomorphisms

Lemma 5.6. *If two sequences*

$$\begin{array}{ccccccc}\dots & \longrightarrow & M_{i-1} & \longrightarrow & M_i & \longrightarrow & M_{i+1} \longrightarrow \dots \\ & & \downarrow & & \downarrow & & \downarrow \\ \dots & \longrightarrow & N_{i-1} & \longrightarrow & N_i & \longrightarrow & N_{i+1} \longrightarrow \dots\end{array}$$

are exact with an isomorphism between them, and the top sequence is exact, then the bottom sequence is exact

Proof. Trivial □

Proposition 5.14. *Given an R -module P , $\cdot \otimes_R P$ is a right exact functor*

Proof. Let $L \rightarrow M \rightarrow N \rightarrow 0$ be an exact sequence of R -modules. For any R -module Q , we have

$$0 \rightarrow \text{Hom}_R(N, \text{Hom}_R(P, Q)) \rightarrow \text{Hom}_R(M, \text{Hom}_R(P, Q)) \rightarrow \text{Hom}_R(L, \text{Hom}_R(P, Q))$$

is exact by left exactness of $\text{Hom}_R(\cdot, \text{Hom}_R(P, Q))$. We have an isomorphism of exact sequences

$$\begin{array}{ccccccc} 0 & \rightarrow & \text{Hom}_R(N, \text{Hom}_R(P, Q)) & \rightarrow & \text{Hom}_R(M, \text{Hom}_R(P, Q)) & \rightarrow & \text{Hom}_R(L, \text{Hom}_R(P, Q)) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Hom}_R(N \otimes_R P, Q) & \longrightarrow & \text{Hom}_R(M \otimes_R P, Q) & \longrightarrow & \text{Hom}_R(L \otimes_R P, Q) \end{array}$$

so the lower sequence is exact. So as Hom_R ‘reflects’ left exactness, we deduce that

$$L \otimes_R P \rightarrow M \otimes_R P \rightarrow N \otimes_R P \rightarrow 0$$

is exact so we are done. □

Lemma 5.7. *Given a multiplicatively closed subset $S \subseteq R$, $S^{-1}R \otimes_R \cdot$ is an exact functor*

Proof. By Lemma 5.6 as $S^{-1}M \cong S^{-1}R \otimes_R M$, and the exactness of localisation □

Definition 5.13. M is a *flat* R -module if $\cdot \otimes_R M$ is an exact functor

Example 5.5.

1. R is a flat R -module as $M \cong M \otimes_R R$ for all R -modules M
2. $\mathbb{Q}$ is a flat $\mathbb{Z}$ module as it is a localisation of $\mathbb{Z}$
3. $\mathbb{Z}/2\mathbb{Z}$ is not a flat $\mathbb{Z}$ -module

Proposition 5.15. *Let N be an R -module. The following are equivalent*

1. N is flat
2. If $f: L \rightarrow M$ is injective, then so is $f \otimes 1_N: L \otimes N \rightarrow M \otimes N$
3. If $f: L \rightarrow M$ is injective and L, M are finitely generated, then $f \otimes 1_N: L \otimes N \rightarrow M \otimes N$ is injective

Proof. (1) is equivalent to (2) immediately as tensoring with N is right exact, so exactness follows from preserving injections.

(3) is a special case of (2) so (2) implies (3)

(3) implies (2): Let $f: L \rightarrow M$ be an injective R -module homomorphism and let $u = \sum l_i \otimes m_i \in \ker(f \otimes 1_N)$, ie $\sum f(l_i) \otimes m_i = 0$. let $L' = \sum Rl_i \subseteq L$ be the submodule generated by the l_i . We define $u' = \sum l_i \otimes n_i \in L' \otimes N$. There is a finitely generated submodule $M' \leq M$ such that $\sum f(l_i) \otimes n_i = 0$ in $M' \otimes N$ by Lemma 5.1. Since L' is finitely generated, so is its image under f . Hence we can further assume $M' \supseteq f(L')$ (otherwise let $M'' = M' + f(L')$). Let $f|_{L'} = f': L' \rightarrow M'$. This is injective, so as $(f' \otimes 1_N)(u') = 0$, we get $u' = 0$ by (3), and hence $u = 0$, so $f \otimes 1_N$ is injective. $\square$

Proposition 5.16. *Flatness is a local property, ie for any R -module N the following are equivalent*

1. N is flat as an R -module
2. $N_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$ module for all prime ideals $\mathfrak{p} \trianglelefteq R$
3. $N_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$ module for all maximal ideals $\mathfrak{m} \trianglelefteq R$

Proof. (1) implies (2): Let N be flat and suppose $L \rightarrow M$ is an injective R -module homomorphism. Then $R_{\mathfrak{p}}$ is a flat R -module, so $R_{\mathfrak{p}} \otimes_R L \rightarrow R_{\mathfrak{p}} \otimes_R M$ is injective, and hence so is $N \otimes_R R_{\mathfrak{p}} \otimes_R L \rightarrow N \otimes_R R_{\mathfrak{p}} \otimes_R M$ by (1), and we know $N \otimes_R R_{\mathfrak{p}} \otimes_R M \cong N_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} M$, so we are done.

(3) is a special case of (2)

(3) implies (1): Suppose $N_{\mathfrak{m}}$ is flat for all $\mathfrak{m} \in \text{mSpec } R$ and $L \rightarrow M$ is an injective R -module homomorphism. Then $L_{\mathfrak{m}} \rightarrow M_{\mathfrak{m}}$ is injective as localisation is exact, and $L_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} N_{\mathfrak{m}} \cong (L \otimes N)_{\mathfrak{m}}$, so we get injectivity of $(L \otimes N)_{\mathfrak{m}} \rightarrow (M \otimes N)_{\mathfrak{m}}$, and hence $L \otimes N \rightarrow M \otimes N$ is injective as injectivity is local $\square$

Proposition 5.17. *Let $f: A \rightarrow B$ be a ring homomorphism and let N be a flat A module. Then $B \otimes_A N$ is a flat B -module*

Proof. Let $L \rightarrow M$ be an injective map of B -modules. Then by example sheet 2 and naturality, we have a commutative diagram

$$\begin{array}{ccc} (B \otimes_A N) \otimes_B L & \longrightarrow & (B \otimes_A N) \otimes_B M \\ \downarrow & & \downarrow \\ N \otimes_A L & \longrightarrow & N \otimes_A M \end{array}$$

where the vertical maps are isomorphisms, so N is a flat A module implies $N \otimes_A L \rightarrow N \otimes_A M$ is injective, implies $(B \otimes_A N) \otimes_B L \rightarrow (B \otimes_A N) \otimes_B M$ is injective, which is exactly what we want $\square$

6 Chain Conditions

Definition 6.1. Let M be an R -module.

1. M is *Noetherian* if every ascending chain of submodules stabilises, ie if

$$M_0 \subseteq M_1 \subseteq M_2 \subseteq \dots$$

are submodules of M , there is some n such that for all $m \geq n$, $M_m = M_n$

2. M is *Artinian* if every descending chain of submodules stabilises, ie if

$$M_0 \supseteq M_1 \supseteq M_2 \supseteq \dots$$

are submodules of M , there is some n such that for all $m \geq n$, $M_m = M_n$

Example 6.1.

1. Finite (in the sense of being a finite set) $\mathbb{Z}$ -modules are both Noetherian and Artinian (as we have finitely many submodules)
2. $\mathbb{Z}$ is Noetherian but not Artinian
3. $G = \{x \in \mathbb{Q}/\mathbb{Z} \mid rx = 0 \text{ for } r = 2^n, n \geq 0\}$ is Artinian but not Noetherian as the subgroups are the p^n -torsion subgroups of $\mathbb{Q}/\mathbb{Z}$.
4. $R = k[t_1, \dots, t_n, \dots]$ is neither Noetherian nor Artinian as $(t_1), (t_1, t_2), \dots$ is ascending and doesn't stabilise, and neither does $(t_1), (t_1^2), \dots$

Proposition 6.1. *An R -module M is Noetherian (Artinian) if and only if every non-empty subset of R modules of M has a maximal (minimal) element with respect to inclusion*

Proof. If M is Noetherian then any non-empty subset of submodules of M must have a maximal element, otherwise we can construct an infinite strictly increasing chain by always just taking a larger module than the current largest in our partial chain.

In the other direction let $\{M_0, M_1, \dots\}$ be a set of submodules forming an ascending chain. By assumption this has a maximal element M_n , so then for $m \geq n$, $M_m = M_n$ and so M is Noetherian. $\square$

Proposition 6.2. *Let*

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

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

Proof. Forwards direction: An ascending chain of submodules of L, N gives an ascending chain of submodules of M (by the inclusion, or the correspondence theorem), and so ascending chains of submodules in L, N must stabilise so they are Noetherian

Backwards direction: Let $(M_n)_{n \geq 0}$ be an ascending chain of submodules of M . The preimage under the inclusion gives an ascending chain of submodules of L , and the images under the quotient give an ascending chain of submodules of

N , so for some $m \geq 0$, the image under the quotient and the preimage under the inclusion of M_n stabilise past m . Suppose that $x \in M_n$ for some $n > m$. Then the image of x under the quotient is in the image of M_m , let $y \in M_m$ have the same image as x in the quotient. Then $y \in M_n \supseteq M_m$ and $x - y$ is in the image of the inclusion, so there is $z \in L$ whose image is $x - y$. We know z is in the preimage of M_n , and hence in the preimage of M_m , so $x - y \in M_m$ and so $x \in M_m$, so $M_n = M_m$. $\square$

Corollary 6.0.1. *If M_i are Noetherian (Artinian) for $1 \leq i \leq n$, then $\bigoplus M_i$ is too*

Proof. By induction with the previous result. $\square$

Definition 6.2. A ring R is *Noetherian (Artinian)* if it is Noetherian (Artinian) as an R -module

Proposition 6.3. *R is Noetherian (Artinian) if and only if every finitely generated R -module is Noetherian (Artinian)*

Proof. In the forwards direction, every finitely generated module is a quotient of the Noetherian (Artinian) ring R^n .

In the backwards direction R is finitely generated by 1 as an R -module. $\square$

Proposition 6.4. *If R is Noetherian (Artinian) and $I \trianglelefteq R$, then R/I is Noetherian (Artinian)*

Proof. There is a short exact sequence of R modules

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

and so R/I is Noetherian as an R -module. This proves R/I is Noetherian as an R/I module, as R/I submodules are the same as R submodules for R/I as I acts as 0 on R/I . $\square$

6.1 Noetherian Rings and Modules

Proposition 6.5. *M is Noetherian as an R -module if and only if every submodule of M is finitely generated*

Proof. In the forwards direction, let N be a submodule of M and let Σ be the set of its finitely generated submodules, which is non-empty as it contains 0, so it has a maximal element N_0 by Noetherianity of M . If $N_0 \neq N$, let $x \in N \setminus N_0$. Then $N_0 + Rx$ is finitely generated and larger than N_0 , contradiction so $N_0 = N$. In the backwards direction, let $(M_n)_{n \geq 0}$ be an ascending chain. The union of the M_n , called M' , is a submodule of M , so is finitely generated by $m_1, \dots, m_n$. Let M_{n_i} be such that $m_i \in M_{n_i}$ and let $k = \max n_i$. Then every $m_1, \dots, m_n \in M_k$, so $M' = M_k$, so every module M_n for $n \geq k$ is equal to M' , so the chain stabilises. $\square$

Remark. M being finitely generated doesn't imply every submodule is finitely generated. If $R = k[x_1, \dots, x_n, \dots]$ then R is finitely generated as an R -module, but $(x_1, \dots, x_n, \dots)$ isn't.

Corollary 6.0.2. R is Noetherian if and only if every ideal is finitely generated

Proof. As submodules of R are exactly the ideals. $\square$

Proposition 6.6. If A is a subring of a ring B and A is Noetherian, B is a finitely generated A -module, then B is Noetherian.

Proof. B is a Noetherian A module, so for any ideal $I \trianglelefteq B$, there is a finite A -generating set as it is an A -submodule. But this generating set is also a B -generating set, and hence I is finitely generated as a B -module, so B is Noetherian. $\square$

Theorem 6.1. (Hilbert's Basis Theorem) If R is Noetherian, then so is $R[t]$.

Proof. Let $I \trianglelefteq R[t]$. Define $J = \{r_n t^n + \dots + r_0 \in I\}$. Then $J \trianglelefteq R$ so J is finitely generated, say by $j_1, \dots, j_l$. We take $f_i \in I$ with leading coefficient j_i and we let $n = \max \deg f_i$. Define $I' = (f_1, \dots, f_l) \trianglelefteq R[t]$, which is a subset of I . Now let $f \in I$ with leading coefficient r . Then $r \in J$, so if $m \geq n$, write $r = \sum_{i=1}^l u_i j_i$ for $u_i \in R$. Then $f - \sum_{i=1}^l u_i f_i t^{m-\deg f_i} \in I$ has degree less than m . We continue subtracting elements of I' from f until we get a polynomial g of degree less than n , with $f = g + h$ and $h \in I'$. We let M be the R -submodule of $R[t]$ generated by $\{1, t, \dots, t^{n-1}\}$. By the above $I = (I \cap M) + I'$. Now $I \cap M \leq R\{1, \dots, t^{n-1}\}$, so it is finitely generated as an R -module (hence as a $R[t]$ -module) as M is Noetherian, so we are done. $\square$

Corollary 6.1.1. If R is a Noetherian ring, then so is $R[t_1, \dots, t_n]$

Proof. Induction $\square$

Corollary 6.1.2. If A is a finitely generated R -algebra and R is Noetherian, then A is Noetherian

Proof. As there is a surjection from some $R[t_1, \dots, t_n]$ $\square$

6.2 Artinian Rings

Theorem 6.2. Let R be an Artinian ring

1. Every prime ideal of R is maximal
2. $\text{nil}(R) = \mathcal{J}(R)$
3. R only has finitely many maximal ideals
4. The nilradical is a nilpotent ideal, ie $(\text{nil } R)^n = 0$ for some $n \geq 1$

Proof. Example sheet 3 $\square$

Theorem 6.3. A ring R is Artinian if and only if it is Noetherian, and every prime ideal is maximal.

Proof. Example sheet 3 □

Proposition 6.7. Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then exactly one of the following is true

1. $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all $n \geq 0$ and R is not Artinian
2. $\mathfrak{m}^n = 0$ for some n and R is Artinian

Proof. Example sheet 4 □

Theorem 6.4. If R is an Artinian ring, then $R \cong \prod_{i=1}^n R_i$ where each R_i is Artinian local, and if we have $R \cong \prod_{j=1}^m R'_j$ for R'_j Artinian local, then $m = n$ and $R_i = R'_i$ up to reordering.

Proof. Example sheet 4 □

Example 6.2. For k a field and $n \geq 1$, $k[t]/(t^n)$ is a local Artinian ring, and so is a product of such.

7 Primary Decomposition

Definition 7.1. Let $I \leq R$ (the first two are rephrasings of definitions previously given in order to motivate (3))

1. I is *prime* if $R/I \neq 0$ and the only zero divisor in R/I is 0
2. I is *radical* if the only nilpotent element of R/I is 0
3. I is *primary* if $R/I \neq 0$ and all zero divisors in R/I are nilpotent

Remark. I is prime if and only if it is radical and primary

Example 7.1. Let $R = \mathbb{Z}$ and $x \in \mathbb{Z} \setminus \{0\}$

1. (x) is prime if and only if $|x|$ is prime
2. (x) is radical if and only if $|x|$ is squarefree
3. (x) is primary if and only if $|x|$ is a prime power

Lemma 7.1. If I is primary, then $\sqrt{I}$ is the smallest prime ideal containing I .

Proof. ES3 □

Example 7.2. Not every primary ideal is a power of a prime ideal. Let $R = k[x, y]$ and $I = (x, y^2)$. Then $R/I = k[y]/(y^2)$ has only the zero divisors the multiples of y , and hence nilpotent. Now $\sqrt{I} = (x, y)$ and so as (x, y) is maximal, it is the only prime containing I , but I is not a power of (x, y) as no power of (x, y) contains x .

Example 7.3. Not every power of a prime ideal is primary. Let $R = k[x, y, z]/(xy - z^2)$ and let $\bar{x}, \bar{y}, \bar{z}$ be the images of x, y, z in R . Consider $\mathfrak{p} = (\bar{x}, \bar{z})$. Now $R/\mathfrak{p} = k[y]$ so $\mathfrak{p}$ is prime. Also $\mathfrak{p}^2 \ni \bar{z}^2 = \bar{x}\bar{y}$, but $\bar{x} \notin \mathfrak{p}^2, \bar{y} \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p}$, so the image of $\bar{y} \in R/\mathfrak{p}^2$ is a non-nilpotent zero divisor, so $\mathfrak{p}^2$ is not primary.

Definition 7.2. Given $\mathfrak{p} \in \text{Spec } R$, a primary ideal I with $\mathfrak{p} = \sqrt{I}$ is called a $\mathfrak{p}$ -primary ideal

Proposition 7.1. If $I \trianglelefteq R$ is an ideal with $\sqrt{I}$ maximal, then I is primary. In particular, the powers of a maximal ideal are always primary.

Proof. ES3 (This entire course is an exercise on ES3.) □

Proposition 7.2. If $I_1, \dots, I_n$ are $\mathfrak{p}$ -primary ideals for some $\mathfrak{p} \in \text{Spec } R$, then $I_1 \cap \dots \cap I_n$ is also $\mathfrak{p}$ -primary

Proof. ES3 (What did I tell you?) □

Definition 7.3. Given an ideal I , a *primary decomposition* of I is an expression $I = J_1 \cap \dots \cap J_n$ where J_i are primary ideals. This primary decomposition is *minimal* if all the $\sqrt{J_i}$ are distinct and $J_i \not\supseteq \bigcap_{i \neq j} J_j$

Example 7.4. In $\mathbb{Z}$, $(90) = (2) \cap (3^2) \cap (5)$ is a minimal primary decomposition

Proposition 7.3. If an ideal has a primary decomposition, then it has a minimal primary decomposition

Proof. ES3 (Ok this one is fair) □

Proposition 7.4. In a Noetherian ring, every proper ideal has a primary decomposition

Proof. ES3 (But at some point we have to actually give a proof of something right?) □

Definition 7.4. Let $I = J_1 \cap \dots \cap J_n$ be a minimal primary decomposition of $I \trianglelefteq R$. Let $\mathfrak{p}_i = \sqrt{J_i}$. Then $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are called the *associated primes* of I

Example 7.5. The associated primes of (90) are $(2), (3), (5)$

Theorem 7.2. (*First Uniqueness Theorem of Primary Decomposition*) Let I be an ideal with minimal primary decomposition $J_1 \cap \dots \cap J_n$ and let $\mathfrak{p}_i = \sqrt{J_i}$. Then $\mathfrak{p}_1, \dots, \mathfrak{p}_n = \{\sqrt{(I : r)} \mid r \in R\} \cap \text{Spec } R$, so the associated primes of I depend only on I , and not the choice of primary decomposition

Proof. ES3 (He claims we're going to prove something soon) □

Lemma 7.3. The contraction of a primary ideal is primary

Proof. (A proof!) Let $f: A \rightarrow B$ be a ring homomorphism and $I \trianglelefteq B$ primary. Let $I^c = f^{-1}(I)$. Then f defines a ring homomorphism $\bar{f}: A/I^c \rightarrow B/I$ which is injective, and hence every zero divisor of A/I^c must be a nilpotent, as it is a subring of B/I in which that holds. □

Proposition 7.5. *If $S \subseteq R$ is multiplicatively closed and $I \trianglelefteq R$ is $\mathfrak{p}$ -primary, then*

1. *If $S \cap \mathfrak{p}$ is non-empty then $S^{-1}I = S^{-1}R$*
2. *If $S \cap \mathfrak{p} = \emptyset$ then $S^{-1}I$ is $S^{-1}\mathfrak{p}$ -primary and $(S^{-1}I)^c = I$*

Hence primary ideals correspond to primary ideals in the bijection between ideals of $S^{-1}R$ and contracted ideals in R .

Proof.

1. If $s \in S^{-1}\mathfrak{p}$, then $s^n \in S \cap I$ for some n , and so $s^n/1 \in S^{-1}I$ is a unit, so $S^{-1}I = S^{-1}R$
2. Suppose $S \cap \mathfrak{p} = \emptyset$. Then if $s \in S$ and $rs \in I$ for $r \in R$ then $r \in I$, as otherwise s would be a non-nilpotent zero divisor in R/I , so $(I : s) = I$ for all $s \in S$, so $I^{ec} = \bigcup_{s \in S} (I : s) = I$ and so $I = (S^{-1}I)^c$. Then $\sqrt{S^{-1}I} = S^{-1}\sqrt{I} = S^{-1}\mathfrak{p}$. That $S^{-1}I$ is primary is an exercise.

□

Proposition 7.6. *Let $S \subseteq R$ be multiplicatively closed and let $I \trianglelefteq R$ have minimal primary decomposition $\bigcap_{i=1}^n J_i$. Let $\mathfrak{p}_i = \sqrt{J_i}$ and suppose the J_i are numbered so that $S \cap J_i \neq \emptyset$ for $i > m$ and $S \cap \mathfrak{p}_i = \emptyset$ for $i \leq m$. Then $S^{-1}I = \bigcap_{i=1}^m S^{-1}J_i$ and $(S^{-1}I)^c = \bigcap_{i=1}^m S^{-1}J_i$ are minimal primary decompositions*

Proof.

$$\begin{aligned} S^{-1}I &= \bigcap_{i=1}^n S^{-1}J_i \\ &= \bigcap_{i=1}^m S^{-1}J_i \end{aligned}$$

This is a primary decomposition, and is minimal as $\sqrt{S^{-1}J_i} = S^{-1}\mathfrak{p}_i$ are distinct as extension and contraction is a bijection. If $S^{-1}J_j \supseteq \bigcap_{i \neq j} S^{-1}J_i$, then contracting $J_j \supseteq \bigcap_{i \neq j} J_i$, so it is minimal. We find the contraction of $S^{-1}I$ by contracting the decomposition, and this is minimal just as above □

Definition 7.5. Let $I = J_1 \cap \cdots \cap J_n$ be a minimal primary decomposition, $\mathfrak{p}_i = \sqrt{J_i}$. Then the *isolated* prime ideals of I are the minimal elements of the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. If $\mathfrak{p}_i$ is isolated, J_i is an *isolated primary component*. Otherwise $\mathfrak{p}_i$ is *embedded* and J_i is an *embedded primary component*

Theorem 7.4. *(Second uniqueness theorem of primary decomposition) If $I \trianglelefteq R$ has a primary decomposition, the isolated primary components depend only on I , and not on the choice of decomposition*

Proof. Let $I = J_1 \cap \dots \cap J_n$ be a minimal primary decomposition with $\mathfrak{p}_i = \sqrt{J_i}$. Suppose the first k are isolated. Let $J'_1 \cap \dots \cap J'_n$ be another minimal primary decomposition. By the first uniqueness theorem, the associated primes are the same so $n = n'$. We can therefore assume $\mathfrak{p}_i = \mathfrak{p}_{i'}$, so the first k of the J'_i are the isolated ones. Let $S = R \setminus \mathfrak{p}_l$ for $l \in \{1, \dots, k\}$. By isolatedness, $S \cap \mathfrak{p}_j \neq \emptyset$ for $j \neq l$, and therefore $J_l = (S^{-1}I)^c = J'_l$. $\square$

Example 7.6. If $I = (x^2, xy) \in k[x, y]$ we have $I = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$ being minimal primary decomposition, so only (x) is isolated, and the embedded ones change, but the associated primes are $(x), (x, y)$

Proposition 7.7. *If I is a radical ideal with a primary decomposition then the minimal primary decomposition is unique, and is given by $I = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$ where $\mathfrak{p}_i$ are the associated (and isolated) primes.*

Proof. Let $I = J_1 \cap \dots \cap J_n$ be a minimal primary decomposition. Then $J_1 \cap \dots \cap J_n = I = \sqrt{I} = \sqrt{J_1} \cap \dots \cap \sqrt{J_n}$. Call these $\mathfrak{p}_i$. If $\mathfrak{p}_i$ are isolated primes, then $I = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_n$, which is minimal primary as $\mathfrak{p}_i$ are distinct and by ES1. By the first uniqueness theorem, these are the associated primes, and as they are all isolated we are done. $\square$

8 Integrality

Definition 8.1. Let A be an R -algebra. Then $a \in A$ is *integral* over R if there is a monic polynomial $f \in R[x]$ such that $f(a) = 0$ in A . f is an *equation of integral dependence*

Definition 8.2. An R -module M is *faithful* if for any $0 \neq r \in R$, there is $m \in M$ with $rm \neq 0$

Proposition 8.1. *The following are equivalent for A an R -algebra*

1. $a \in A$ is integral over R
2. $R[a]$ is a finitely generated R module
3. $R[a] \subseteq B$ where B is a subring of A finitely generated as an R -module
4. There is a faithful $R[a]$ module M which is finitely generated over R

Proof. (1) implies (2): There are $r_0, \dots, r_{n-1}$ with $a^{n+k} = -(r_{n-1}a^{n+k-1} + \dots + r_0a^k)$, so $1, \dots, a^{n-1}$ generate $R[a]$ as an R module.

(2) implies (3) is trivial

(3) implies (4): Take $M = B$. We claim this is faithful. This is because if $x \in R[a]$, then $x \cdot 1 = x \neq 0$ for $1 \in B$.

(4) implies (1): We use Cayley Hamilton on $f: M \rightarrow M$ via $m \mapsto am$, which is an R -module homomorphism. This gives us a monic polynomial which a satisfies, when applied to m , so we are done using faithfulness. $\square$

Corollary 8.0.1. *If $a_1, \dots, a_n \in A$ are integral over R , then $R[a_1, \dots, a_n]$ is finitely generated as an R -module*

Proof. Trivial $\square$

Corollary 8.0.2. *The set of elements of A which are integral over R is a subring of A*

Proof. $B \supseteq R$ is easy. If $b_1, b_2 \in B$ then $R[b_1, b_2]$ is finitely generated over R , and so as this contains $b_1 \pm b_2, b_1 b_2$, these are integral. $\square$

Definition 8.3. Let A be an R -algebra. If every element of A is integral over R , we say A is an *integral R -algebra* or *A is integral over R* . If R is a subring of A , we say A is an *integral extension* of R if it is integral. The set of elements of A which are integral over R is the *integral closure* of R in A , and if $B = R$, then R is *integrally closed*

Example 8.1.

1. If K is a number field and $\mathcal{O}_K$ its ring of integers, then $\mathcal{O}_K$ is the integral closure of $\mathbb{Z}$ in K
2. Consider $\mathbb{C}[x^n] \leq \mathbb{C}[x]$. Then $\mathbb{C}[x]$ is an integral extension of $\mathbb{C}[x^n]$ as x satisfies $t^n - x^n = 0$

Proposition 8.2. *Let A be an R -algebra. The following are equivalent*

1. *A is an integral R -algebra and is finitely generated as an R -algebra*
2. *A is finitely generated as an R -algebra by a finite set of integral elements*
3. *A is finitely generated as an R -module*

Proof. (1) implies (2) is immediate, and (2) implies (3) by Corollary 8.0.1. (3) implies (1) follows from Proposition 8.1. $\square$

Proposition 8.3. *(Transitivity of Integrality) Let $R \subseteq A \subseteq B$ be rings such that A is integral over R and B is integral over A , then B is integral over R*

Proof. Given $b \in B$, there is a monic polynomial in A that it satisfies with coefficients $a_0, \dots, a_{n-1} \in A$. Then if $A' = R[a_1, \dots, a_{n-1}]$, it is a finitely generated R -module, so A' is integral over R . $A'[b]$ is a finitely generated A' module, hence a finitely generated R -module, so b is integral over R $\square$

Corollary 8.0.3. *Let $R \subseteq A$ be rings with C the integral closure of R in A . Then C is integrally closed in A*

Proof. If $a \in A$ is integral over C , then by above it is integral over R , so it is in C . $\square$

Proposition 8.4. *Let $R \subseteq A$ be rings and let S be a multiplicatively closed subset of R*

1. Let $I \subseteq A$ and $J = I^c = I \cap R$. If A is integral over R , then A/I is integral over R/J .
2. If A is integral over R , $S^{-1}A$ is integral over $S^{-1}R$.
3. If B is the integral closure of R in A then $S^{-1}B$ is the integral closure of $S^{-1}R$ in $S^{-1}A$.

Proof.

1. For $a \in A$, there is $f \in R[t]$ with $f(a) = 0$. Taking the image of this setup in A/I , we get the result.
2. Consider $a/s \in S^{-1}R$, with $f \in R[t]$ such that $f(a) = 0$. Then multiplying by $1/s^n$, we get that if the coefficients of f are a_i , then g with coefficients $s^{n-i}a_i$ has $g(a/s) = (1/s^n)f(a) = 0$. So a/s is integral over $S^{-1}R$.
3. Suppose a/s is integral over $S^{-1}R$, and $(a/s)^n + (r_{n-1}/s_{n-1})(a/s)^{n-1} + \dots + r_0/s_0 = 0$. If $t = s_1 \dots s_n$, we get an equation of integral dependence for at over R by multiplying by $(st)^n$, so $at \in B$ and hence $at/st = a/s \in S^{-1}B$.

□

Proposition 8.5. *Let $R \subseteq A$ be integral domains with A an integral extension of R . Then A is a field if and only if R is*

Proof. In the backwards direction, let $a \in A \setminus \{0\}$ and suppose $a^n + r^{n-1}a_{n-1} + \dots + r_0 = 0$ of minimal degree with $r_i \in R$. Suppose $r_0 = 0$, then we can factor out a to get either $a = 0$, or a satisfies an equation of lower degree, contradiction, so r_0 is a unit. Therefore $a(-r_0^{-1}(a^{n-1} + \dots + r_1)) = 1$, so a is a unit.

In the backwards direction, we need only prove that if $r \in R$, then $r^{-1} \in A$ is in fact in R , but multiplying the equation of integral dependence by $-r^{-1}r_0^{-1}$, we see the result we wish.

□

Corollary 8.0.4. *If $R \subseteq A$ is an integral extension, $\mathfrak{p} \in \text{Spec } A$ and $\mathfrak{q} = \mathfrak{p}^c = \mathfrak{p} \cap R$, then $\mathfrak{q}$ is a maximal ideal if and only if $\mathfrak{p}$ is*

Proof. Quotient to get $R/\mathfrak{q}, A/\mathfrak{p}$ and use Proposition 8.4(1) and Proposition 8.5.

□

If $R \subseteq A$ and $\mathfrak{p} \in \text{Spec } R$, then $R \setminus \mathfrak{p}$ is multiplicatively closed in A , we write $A_{\mathfrak{p}} = (R/\mathfrak{p})^{-1}A$.

Corollary 8.0.5. *If $R \subseteq A$ is an integral extension, $\mathfrak{p}, \mathfrak{p}' \in \text{Spec } A$ with $\mathfrak{p} \subseteq \mathfrak{p}'$, and $\mathfrak{p} \cap R = \mathfrak{p}' \cap R$ then $\mathfrak{p} = \mathfrak{p}'$.*

Proof. Let $\mathfrak{q}$ be $\mathfrak{p} \cap R = \mathfrak{p}' \cap R$. Then $A_{\mathfrak{q}}$ is still integral over $R_{\mathfrak{q}}$. Let $\mathfrak{n} = (R \setminus \mathfrak{q})^{-1}\mathfrak{p}$, $\mathfrak{n}' = (R \setminus \mathfrak{q})^{-1}\mathfrak{p}'$ so $\mathfrak{n} \subseteq \mathfrak{n}'$. Let $\mathfrak{m} = (R \setminus \mathfrak{q})^{-1}\mathfrak{q}$, the unique maximal ideal of $R_{\mathfrak{q}}$. Now

$$\begin{aligned}\mathfrak{n} \cap R_{\mathfrak{q}} &= (R \setminus \mathfrak{q})^{-1}\mathfrak{p} \cap (R \setminus \mathfrak{q})^{-1}R \\ &= (R \setminus \mathfrak{q})^{-1}(\mathfrak{p} \cap R) \\ &= (R \setminus \mathfrak{q})^{-1}\mathfrak{q} \\ &= \mathfrak{m}\end{aligned}$$

Similarly $\mathfrak{n}' \cap R_{\mathfrak{q}} = \mathfrak{m}$ since $\mathfrak{p}' \cap R = \mathfrak{q}$, so $\mathfrak{n}, \mathfrak{n}'$ are maximal, so they are equal as $\mathfrak{n} \subseteq \mathfrak{n}'$, so $\mathfrak{p} = \mathfrak{p}'$ by contraction as $\mathfrak{p} \cap (R \setminus \mathfrak{q}) = \emptyset = \mathfrak{p}' \cap (R \setminus \mathfrak{q})$ $\square$

Theorem 8.1. (*Lying over*) Let $R \subseteq A$ be an integral extension. If $\mathfrak{p} \in \text{Spec } R$ then there is $\mathfrak{q} \in \text{Spec } A$ such that $\mathfrak{q} \cap R = \mathfrak{p}$, so $\text{Spec } A \rightarrow \text{Spec } R$ is surjective

Proof. $A_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$. We denote the localisation by $\mathfrak{p}$ map as $f_A: A \rightarrow A_{\mathfrak{p}}$ and $f_R: R \rightarrow R_{\mathfrak{p}}$. The diagram

$$\begin{array}{ccc} R & \hookrightarrow & A \\ \downarrow & & \downarrow \\ R_{\mathfrak{p}} & \hookrightarrow & A_{\mathfrak{p}} \end{array}$$

commutes. Let $\mathfrak{n}$ be a maximal ideal in $A_{\mathfrak{p}}$. Then $\mathfrak{m} = R_{\mathfrak{p}} \cap \mathfrak{n}$ is maximal, but the maximal ideal of $R_{\mathfrak{p}}$ is unique, so $f_R^{-1}(\mathfrak{m}) = \mathfrak{p}$. However,

$$\begin{aligned}f_R^{-1}(\mathfrak{m}) &= f_R^{-1}(R_{\mathfrak{p}} \cap \mathfrak{n}) \\ &= f_R^{-1}(\iota_{\mathfrak{p}}^{-1}(\mathfrak{n})) \\ &= \iota^{-1}(f_A^{-1}(\mathfrak{n})) \\ &= R \cap f_A^{-1}(\mathfrak{n})\end{aligned}$$

so if $\mathfrak{q} = f_A^{-1}(\mathfrak{n})$, then $\mathfrak{q} \cap R = \mathfrak{p}$ as desired. $\square$

Theorem 8.2. (*Going Up Theorem*) If $R \subseteq A$ is an integral extension, and $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_m$ is a chain of prime ideals of R , and $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ is a chain of prime ideals of A with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all $1 \leq i \leq n$, where $n < m$, then the chain in A can be extended to a chain $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all $1 \leq i \leq m$.

Proof. By induction, we reduce to $n = 1, m = 2$. Let $\bar{R} = R/\mathfrak{p}_1$ and $\bar{A} = A/\mathfrak{q}_1$. We know by Proposition 8.4 that $\bar{R} \subseteq \bar{A}$ is integral. Let $\bar{\mathfrak{p}}_2$ be the image of $\mathfrak{p}_2$ in $\bar{R}$. By lying over, there is $\bar{\mathfrak{q}}_2 \in \text{Spec } \bar{A}$ such that $\bar{\mathfrak{p}}_2 = \bar{R} \cap \bar{\mathfrak{q}}_2$. Let $\mathfrak{q}_2$ be the preimage of $\bar{\mathfrak{q}}_2$ in A . We have $\mathfrak{q}_2 \supseteq \mathfrak{q}_1$ and $\mathfrak{q}_2 \cap R = \mathfrak{p}_2$ so we are done. $\square$

Definition 8.4. Let R be an integral domain. The *integral closure* of R is the integral closure of R in $\text{Frac } R$. R is *integrally closed* if it is integrally closed in $\text{Frac } R$

Proposition 8.6. *If R is a UFD, it is integrally closed.*

Proof. Let $a/b \in \text{Frac } R$ be integral over R . We know that

$$(a/b)^n + r_{n-1}(a/b)^{n-1} + \cdots + r_1(a/b) + r_0 = 0$$

In particular, multiplying by b^n ,

$$a^n = -b(r_{n-1}a^{n-1} + \cdots + r_1ab^{n-2} + r_0b^{n-1})$$

so any prime factor of b is a prime factor of a to at least as large a power, and so b divides a , and $a/b \in R$. $\square$

Example 8.2. $R = k[x, y]/(y^2 - x^3)$ is not integrally closed. $\text{Frac } R = K(y/x)$, and $y/x \notin R$, but y/x is integral over R since it satisfies $t^2 - x = 0$

Lemma 8.3. *Let $R \subseteq A$ with $f \in R[t]$ is monic. Suppose that $f = gh$ with $g, h \in A[t]$ and g is monic.*

1. *There is $B \supseteq A$ such that $f(t)$ splits into linear factors in $B[t]$.*
2. *The coefficients of g, h are integral over R .*

Proof.

1. Let $A' = A[t]/(f)$ and let b_1 be the image of t in A' . Then $f(b_1) = 0$, so $f(t) = (t - b_1)f_1(t)$ in $A'[t]$. We are done by induction on the degree.
2. Apply (1) to g to get a ring B' in which $g(t) = \prod (t - b_i)$. Then the b_i are integral over R as they are roots of f , and so the coefficients of g are integral as they are polynomials in the b_i (and similar for h , which must be monic as g is)

$\square$

Definition 8.5. Given a field extension $L \supseteq K$, the *minimal polynomial* of $a \in L$ over K is the unique non-zero monic polynomial such that $f(a) = 0$ and such that if $0 \neq g \in K[t]$, then $f \mid g$

Proposition 8.7. *Let R be an integrally closed integral domain and $K = \text{Frac } R \subseteq L$ fields. Let $a \in L$ which is integral over R with minimal polynomial $g \in K[t]$. Then $g \in R[t]$*

Proof. Since a is integral over R , there is monic $f \in R[t]$ with $f(a) = 0$ such that $f = gh$ for $h \in K[t]$, but then the coefficients of g must be integral over R , so g is a polynomial over R as R is integrally closed. $\square$

Theorem 8.4. (*Going Down Theorem*) *Let $R \subseteq A$ be integral domains with R integrally closed and A integral over R . Let $\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_m$ be a chain of prime ideals of R , and for $n < m$, let $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$ be a chain of prime ideals of A such that $\mathfrak{p}_i = R \cap \mathfrak{q}_i$ for $i \in \{1, \dots, n\}$. Then the chain of primes in A can be extended to a chain $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ such that $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ for $i \in \{1, \dots, m\}$*

Proof. As in the Going Up Theorem, we may assume $n = 1, m = 2$ by induction. We want to show that given $\mathfrak{q}_2 \in \text{Spec } A$ with $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$ and $\mathfrak{p}_2 = R \cap \mathfrak{q}_2$. This happens if and only if there is some $\mathfrak{q}'_2 \in \text{Spec } A_{\mathfrak{q}_1}$ such that $(\mathfrak{q}'_2)^c = \mathfrak{p}_2$ which happens if and only if $\mathfrak{p}_2 = \mathfrak{p}_2^{ec} = (A_{\mathfrak{q}_1} \mathfrak{p}_2) \cap R$. Note that $\mathfrak{p}_2 \subseteq (A_{\mathfrak{q}_1} \mathfrak{p}_2) \cap R$. Every $x \in A_{\mathfrak{q}_1} \mathfrak{p}_2$ is of the form y/s for $y \in A \mathfrak{p}_2$ and $s \in A \setminus \mathfrak{q}_1$. We write $y = \sum_{i=1}^k p_i y_i$ for $p_i \in \mathfrak{p}_2$ and $y_i \in A$. We let $A' = R[y_1, \dots, y_k]$, which is a finitely generated R -module since $y_i \in A$ and A is integral over R . Moreover $yA' \subseteq \mathfrak{p}_2 A'$. Applying Cayley-Hamilton to multiplication by y , we get some monic $f \in A'[t]$ with $f(y) = 0$ and all non-leading coefficients in $\mathfrak{p}_2$. We claim the same holds for the minimal polynomial of y . Suppose $f = gh$ for $g, h \in K[t]$. Then $g, h \in R[t]$ by Lemma 8.3, but $f = t^r \pmod{\mathfrak{p}_2}$, so g, h are also congruent to powers of $t \pmod{\mathfrak{p}_2}$ by unique factorisation in $\text{Frac}(R/\mathfrak{p}_2)[t]$, so the claim holds. Now suppose $x = r/s \in R$. Then $s = yx^{-1} \in \text{Frac}(A)$, and so the minimal polynomial for s over $\text{Frac}(R)$ is $g(t) = x^r f(x^{-1}t)$, so if u_i (resp v_i) is the i th coefficient of f (resp g) then $x^{r-i}v_i = u_i \in \mathfrak{p}_2$. Now $s \in A$, so it is integral over R , and so $v_i \in R$. If $x \notin \mathfrak{p}_2$, then $s^r \in A \mathfrak{p}_2$ as $g(s) = 0$ and all the lower coefficients are in $\mathfrak{p}_2$, so $s^r \in \mathfrak{q}_1$, contradiction. So $x \in \mathfrak{p}_2$, so $A_{\mathfrak{q}_1} \mathfrak{p}_2 \cap R = \mathfrak{p}_2$, so we are done. $\square$

9 Dedekind Domains and Discrete Valuation Rings

Exercise 9.1.

1. If $I, J \trianglelefteq R$ have coprime radicals, then I, J are coprime.
2. If $I_1, \dots, I_n$ are pairwise coprime, then $\prod I_j = \bigcap I_j$

Proposition 9.1. *Let R be a Noetherian integral domain where every non-zero prime ideal is maximal. Then every non-zero $I \trianglelefteq R$ can be uniquely expressed as a product of primary ideals with distinct radicals.*

Proof. Since R is Noetherian, I has a minimal primary decomposition $I = \bigcap_{i=1}^j J_i$. Let $\mathfrak{p}_i = \sqrt{J_i}$. This is maximal by assumption, so they are pairwise coprime. From the exercises before, we deduce that the J_i are pairwise coprime, and so that $\prod_{i=1}^n J_i = \bigcap_{i=1}^n J_i$.

For uniqueness, suppose we have another decomposition as a product, then again we get another primary decomposition, which is minimal as follows: If $J'_i \supseteq \bigcap_{i \neq j} J'_j$, then $\mathfrak{p}'_i \supseteq J'_i \supseteq \bigcap_{i \neq j} J'_j = \prod_{i \neq j} J'_j$, but this is a contradiction as we have distinct radicals, which are all maximal. As every radical is maximal, every prime in the primary decomposition is isolated, so we get full uniqueness. $\square$

9.1 Discrete Valuation Rings

Definition 9.1. Let K be a field and $K^\times$ be its unit group. A *discrete valuation* on K is a surjection $\nu: K^\times \rightarrow \mathbb{Z}$ such that

1. $\nu(xy) = \nu(x) + \nu(y)$

$$2. \nu(x + y) \geq \min\{\nu(x), \nu(y)\}$$

We set $\nu(0) = \infty$. The *valuation ring* of ν is $\{x \in K \mid \nu(x) \geq 0\}$. An integral domain is a *discrete valuation ring* if it is the valuation ring of a valuation on $\text{Frac } R$

Example 9.1. If $K = \mathbb{Q}$ and $p \in \mathbb{Z}$ is a prime, we define the valuation (where the numerator and denominator of y are coprime to p) $p^r y = x \in \mathbb{Q} \mapsto r$, the valuation ring is $\mathbb{Z}_{(p)}$

Proposition 9.2. Let $\nu: K \rightarrow \mathbb{Z}$ be a discrete valuation with valuation ring R .

1. $r \in R^\times$ if and only if $\nu(r) = 0$
2. R is a local ring with maximal ideal $\mathfrak{m} = \{\nu(r) \geq 1\}$
3. R is an integral domain
4. R is Noetherian
5. $\text{Spec } R = \{0, \mathfrak{m}\}$

Proof.

1. Note that 0 is not a unit and $\nu(0) \neq 0$. For $r \in R \setminus \{0\}$, $r^{-1} \in R$ if and only if $\nu(r^{-1}) = -\nu(r) \geq 0$. But also $\nu(r) \geq 0$, so this happens if and only if $\nu(r) = 0$.
2. Obviously $\mathfrak{m} \subseteq R$. It is maximal as it contains every non-unit by (1).
3. As R is a subring of a field.
4. Let $I \trianglelefteq R$ be non-zero. Then there is a least $k \in \mathbb{Z}$ such that $\nu(i) = k$ for some $i \in I$. Suppose $r \in R$ has valuation at least k . Then $\nu(ri^{-1}) \geq 0$, so $ri^{-1} \in R$, so $r \in I$. So the ideals are exactly $\nu^{-1}([n, \infty)) = I_n$, so the set of ideals has ordertype $\mathbb{N} \cup \{\infty\}$, and we are done.
5. Let $r \in R$ be such that $\nu(r) = 1$ by surjectivity. Then $\mathfrak{m}_n = (r^n)$, so only 0 and $\mathfrak{m}_1$ are prime.

□

Proposition 9.3. Let $(R, \mathfrak{m})$ be a Noetherian local integral domain with $K = R/\mathfrak{m}$. Suppose $\text{Spec } R = \{0, \mathfrak{m}\}$. The following are equivalent

1. R is a DVR
2. R is integrally closed
3. $\mathfrak{m}$ is principal
4. $\dim_K \mathfrak{m}/\mathfrak{m}^2 = 1$

5. Every non-zero ideal is a power of $\mathfrak{m}$
6. There is $m \in R$ such that every non-zero ideal has $I = (m^k)$ for some $k \geq 0$

Proof. We have some key properties from the setup (see ES3): If $0 \neq I \leq R$, then I is $\mathfrak{m}$ -primary and moreover $I \supseteq \mathfrak{m}^n$ for some n . $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$, if $\mathfrak{m}^n \neq 0$ for all n .

1. (1) implies (2): Let $x \in \text{Frac } R$ be integral over R . Then there is some monic $f \in R[t]$ with $f(x) = 0$. We are done if $x \in R$, otherwise $x^{-1} \in R$ as R is a DVR. But then we can use f to find x in terms of x^{-1} , contradiction.
2. (2) implies (3): Let $r \in \mathfrak{m} \setminus \{0\}$. If $\mathfrak{m} \neq (r)$, then the first key property implies there is some n with $\mathfrak{m}^n \subseteq (r)$ and $\mathfrak{m}^{n-1} \not\subseteq (r)$. Let $s \in \mathfrak{m}^{n-1} \setminus (r)$ and let $x = r/s \in \text{Frac } R$. Then $x^{-1} \notin R$ as $s \notin (r)$, so x^{-1} is not integral over R , so $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ as otherwise $\mathfrak{m}$ is a faithful finitely R -generated $R[x^{-1}]$ -module. But $x^{-1}\mathfrak{m} \subseteq R$. Since $s\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (r) = rR$, we get $x^{-1}\mathfrak{m} = R$, so $\mathfrak{m} = Rx = (x)$
3. (3) implies (4): If $\mathfrak{m} = (r)$ for some $r \in R$, then r spans $\mathfrak{m}/\mathfrak{m}^2$ as a K -vector space. We know $\mathfrak{m} \neq \mathfrak{m}^2$ by the second fact at the top, so $\dim_K \mathfrak{m}/\mathfrak{m}^2 = 1$.
4. (4) implies (3): Let $r \in \mathfrak{m}$ be such that $r \in \mathfrak{m}/\mathfrak{m}^2$ is spanning. Let $I = (r) \subseteq \mathfrak{m}$. Then we get

$$I \rightarrow \mathfrak{m} \rightarrow \mathfrak{m}/\mathfrak{m}^2$$

which is a surjection, so $I + \mathfrak{m}^2 = \mathfrak{m}$. Now $\mathfrak{m}(\mathfrak{m}/I) = \mathfrak{m}^2/I = (\mathfrak{m}^2 + I)/I = \mathfrak{m}/I$, so $\mathfrak{m} = I$ by Nakayama.

5. (3) implies (5): Let $\mathfrak{m} = (m)$ and let $0 \neq I \leq R$, so $I \subseteq \mathfrak{m}$. By the statements before the proof, there is a k with $(m^k) = \mathfrak{m}^k \supseteq I$ and $\mathfrak{m}^{k+1} \not\supseteq I$, so there is $i \in I \setminus \mathfrak{m}^{k+1}$. But $i = rm^k$ for some $r \in R$. $r \notin \mathfrak{m}$ so it is a unit, so $m^k \in I$, so $I = \mathfrak{m}^k$.
6. (5) implies (6): By the second fact above, we have some $m \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then by (5), $\mathfrak{m}^k = (m)$ for some $k \geq 0$, so $\mathfrak{m} = (m)$, so every non-zero ideal is of the form (m^k) by (5)
7. (6) implies (1): $\mathfrak{m}^k = (m^k) \neq (m^{k+1})$ by the second fact. If $r \in R \setminus \{0\}$, then $(r) = (m^k)$ for exactly one k . Set $\nu(r) = k$ and extend to $\text{Frac } R$ in the natural way. Check this is a well defined discrete valuation and we are done.

□

9.2 Dedekind Domains

Theorem 9.1. *Let R be a Noetherian integral domain where every non-zero prime is maximal. The following are equivalent*

1. R is integrally closed
2. Every primary ideal is a power of a prime
3. For all $\mathfrak{p} \in \text{Spec } R$, $R_{\mathfrak{p}}$ is a DVR

Proof. $R_{\mathfrak{p}}$ is a Noetherian integral domain since this is preserved by localisation. Non-zero prime ideals of $R_{\mathfrak{p}}$ are maximal since they correspond to prime ideals contained in $\mathfrak{p}$, so they must all be $\mathfrak{p}$.

For (1) is equivalent to (3), we observe $R_{\mathfrak{p}}$ is a DVR is equivalent to $R_{\mathfrak{p}}$ being integrally closed by the previous proposition, and integral closedness is a local property.

(3) implies (2): Let $I \trianglelefteq R$ be $\mathfrak{p}$ -primary for some $\mathfrak{p} \in \text{Spec } R$. Then $IR_{\mathfrak{p}} \trianglelefteq R_{\mathfrak{p}}$ since $I \subseteq \mathfrak{p}$, so $IR_{\mathfrak{p}} = (\mathfrak{p}R_{\mathfrak{p}})^n$ by the previous proposition, and this is equal to $\mathfrak{p}^n R_{\mathfrak{p}}$. $I = (IR_{\mathfrak{p}})^c$, but this is exactly $\mathfrak{p}^n$.

(2) implies (3): Let $0 \neq \mathfrak{p} \in \text{Spec } R$ and let $J \trianglelefteq R_{\mathfrak{p}}$. Then J is $\mathfrak{p}R_{\mathfrak{p}}$ -primary by the lede, so J^c is $\mathfrak{p}$ -primary, and hence $J^c = \mathfrak{p}^n$, so $J = (\mathfrak{p}R_{\mathfrak{p}})^n$ hence $R_{\mathfrak{p}}$ is a DVR. $\square$

Definition 9.2. A ring satisfying any of the equivalent characterisations of the above theorem is a *Dedekind domain*.

Corollary 9.1.1. *In a Dedekind domain, every non-zero proper ideal has a unique factorisation into prime ideals*

Proof. Trivial $\square$

Example 9.2. $\mathcal{O}_K$ for K a number field, $\mathbb{C}[t]$, $\mathbb{C}[x, y]/(y - x^2)$ are all Dedekind domains

10 Completions

Definition 10.1. A *directed set* is a partially ordered set $(I, \leq)$ such that for all $a, b \in I$ there is $c \in I$ with $a, b \leq c$. A *direct system* of R -modules is a set of R -modules $\{G_a\}_{a \in I}$ and homomorphisms $\rho_{ab}: G_a \rightarrow G_b$ for $a \leq b$ such that $\rho_{aa} = 1_{G_a}$ and $\rho_{ac} = \rho_{bc} \circ \rho_{ab}$ for $a \leq b \leq c$.

An *inverse system* of R -modules is a set of R -modules $\{G_a\}_{a \in I}$ and homomorphisms $\rho_{ab}: G_b \rightarrow G_a$ for $a \leq b$ such that $\rho_{aa} = 1_{G_a}$ and $\rho_{ac} = \rho_{ab} \circ \rho_{bc}$ for $a \leq b \leq c$.

Example 10.1. $I = \mathbb{N} \setminus \{0\}$ under the usual order is a direct system, and for p a prime number, $N_i = \mathbb{Z}/p_i\mathbb{Z}$ with g_{ij} given by reduction mod p^i is an inverse system.

Definition 10.2. The *direct limit* of a direct system is

$$\varinjlim_I G_a = \bigoplus_{a \in I} G_a / \langle x - \rho_{ab}(x) \mid x \in G_a, b \geq a \rangle$$

Proposition 10.1. $\varinjlim M_i$ is an R -module

Proof. If $m_i \in M_i, m_j \in M_j$ then take $i, j \leq k$. Then $[m_i] + [m_j] = [\phi_{ik}(m_i) + \phi_{jk}(m_j)]$. Verify that this with the obvious R -action is an R -module. $\square$

Definition 10.3. The *inverse limit* of an inverse system is

$$\varprojlim_I G_a = \{(a_i) \in \prod G_i \mid a_i = g_{ij}(a_j), i \leq j\}$$

Remark. It is easy to show this is an R -module. It is also possible to define direct/inverse limits of R -algebras

Example 10.2. $\varprojlim \mathbb{Z}/p^n \mathbb{Z}$ for p a prime number is the p -adic integers $\mathbb{Z}_p$ (you can take this as a definition if you don't know about them)

Proposition 10.2. (*Universal property of direct limit*) Let I be a directed set and $(\{M_i\}, \{f_{ij}\})$ a direct system. For any R -module with R -module homomorphisms $f_i: M_i \rightarrow M$ such that $f_i = f_j f_{ij}$ there is a unique R -module homomorphism $f: \varinjlim M_i \rightarrow M$ such that $f_i = f f'_i$ where f_j are the structure morphisms for the direct limit.

Proof. Trivial $\square$

Remark. The universal property of the inverse limit is the dual

Definition 10.4. Let $I \trianglelefteq R$. Then we get an inverse system

$$\cdots \rightarrow R/I^3 \rightarrow R/I^2 \rightarrow R/I$$

The inverse limit of this system is the I -adic completion of R

Example 10.3.

1. $\mathbb{Z}_p$ is the (p) -adic completion of $\mathbb{Z}$
2. The (t) -adic completion of $k[t]$ is $k[[t]]$

Definition 10.5. Let M be an R -module.

1. A *filtration* of M is a sequence of submodules $(M_n)_{n \geq 0}$ such that $M_0 = M, M_n \supseteq M_{n+1}$
2. The *completion* of M with respect to $(M_n)_{n \geq 0}$ is $\varprojlim M/M_n$
3. Given $I \trianglelefteq R$, the I -adic completion of M is the completion with respect to $(I^n M)_{n \geq 0}$

Theorem 10.1. *Let R be Noetherian with $I \subseteq R$ and $\hat{R}$ the I -adic completion.*

1. $\hat{R}$ is Noetherian
2. $\hat{R}$ is a flat R -module
3. If M is a finitely generated R -module with $\hat{M}$ its I -adic completion, then $\hat{M}$ is a $\hat{R}$ module and $\hat{M} \cong \hat{R} \otimes_R M$

Proof. No proof □

Corollary 10.1.1. *If R is Noetherian, then so is $R[[t_1, \dots, t_n]]$*

Proof. Hilbert basis theorem, and the preceding theorem □

10.1 Graded Rings and Modules

Definition 10.6. A *graded ring* is a ring R with a family $(R_n)_{n \geq 0}$ of additive subgroups of R such that $R = \bigoplus_{i=0}^{\infty} R_i$ and $R_m R_n \subseteq R_{m+n}$

Example 10.4. $R = k[x_1, \dots, x_l]$ is graded with R_n consisting of 0 and the degree n homogeneous polynomials.

Remark. If R is a graded ring, then R_0 is a subring of R and each R_n is an R_0 -module. (The hard part is $1 \in R_0$: suppose $1 = \sum_{n=0}^{\infty} 1_n$ with $1_n \in R_n$. Given $r_m \in R_m$, then $\sum_{n=0}^{\infty} 1_n r_m \in R_m$, so $1_n = 0$ if $n > 0$, so we are done.)

Definition 10.7. Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a graded ring.

1. A *graded R -module* is an R -module M with $M = \sum_{i=0}^{\infty} M_i$ where M_n is an additive subgroup of M and $R_m M_n \subseteq M_{m+n}$.
2. A *homomorphism of graded R -modules* is a homomorphism sending the n -graded component of the domain into the n -graded component of the codomain
3. $m \in M$ is *homogeneous of degree n* if $m \in M_n$. Any $m \in M$ can be written as $m = \sum_{n=0}^{\infty} m_n$ with all but finitely many m_n zero. The non-zero m_n are *homogeneous components* of m .

Proposition 10.3. *Let $R = \bigoplus_{i=0}^{\infty} R_i$ be a graded ring. The following are equivalent*

1. R is Noetherian
2. R_0 is Noetherian and R is a finitely generated R_0 algebra

Proof. (2) implies (1) is immediate from Hilbert basis theorem.

(1) implies (2): Let $R_+ = \bigoplus_{i=1}^{\infty} R_i$. This is an ideal as it is the kernel of the projection to R_0 . Then R_0 is Noetherian as it is a quotient of R , and R_+ is finitely generated as it is an ideal of R . We may assume each generator r_i of R_+ is homogeneous, and in R_{k_i} . Let $R' = R_0[r_1, \dots, r_l]$. We want to show $R_n \subseteq R'$

for every n . We induct on n , the result being immediate for R_0 . Let $r \in R_n$ with $n \geq 1$. Since $r \in R_+$, we express it as $r = \sum_{i=1}^l t_i r_i$ with $t_i \in R$. We apply the projection $\pi_n: R \rightarrow R_n$. Now $\pi_n(r) = r$, and $\pi(t_i r_i) = s_i r_i$ for some $s_i \in R_{n-k_i}$, so $r = \sum_{i=1}^l s_i r_i$. By induction, $s_i \in R'$ and so $r \in R'$. $\square$

Definition 10.8. Let $I \trianglelefteq R$, and M an R -module.

1. A filtration $(M_n)_{n=0}^\infty$ of M is an *I-filtration* if $IM_n \subseteq M_{n+1}$ for all $n \geq 0$
2. An *I-filtration* $(M_n)_{n=0}^\infty$ is *stable* if there is some n_0 such that $IM_n = M_{n+1}$ for $n \geq n_0$.

Example 10.5. $(I^n M)_{n=0}^\infty$ is a stable *I-filtration*

Definition 10.9. Let $I \trianglelefteq R$. The *associated graded ring* of R with respect to I is

$$G_I(R) = \bigoplus_{n=0}^{\infty} I^n / I^{n+1}$$

where $I^0 = R$ and for $x \in I^m, y \in I^n$, we define $\bar{x}\bar{y} = \overline{xy} \in I^{m+n}/I^{m+n+1}$ being the image. This is well defined

Definition 10.10. Let M be an R -module with $(M_n)_{n=0}^\infty$ an *I* filtration. We define

$$G(M) = \bigoplus_{n=0}^{\infty} M_n / M_{n+1}$$

and $G_n(M) = M_n / M_{n+1}$

Remark. This is a graded $G_I(R)$ module. For $r \in I^n, m \in M_k$ we define $\bar{r}\bar{m} = \overline{rm} \in M_{k+n}/M_{k+n+1}$. Check that this is well defined.

Proposition 10.4. Let R be Noetherian and $I \trianglelefteq R$

1. $G_I(R)$ is Noetherian
2. If M is a finitely generated R module with a stable *I* filtration, then $G(M)$ is a finitely generated $G_I(R)$ -module

Proof.

1. As R is Noetherian, $I = (r_1, \dots, r_l)$ for some $r_i \in R$. Let $\bar{r}_i$ be their images in I/I^2 . Now $G_I(R) = R/I \oplus \bigoplus_{n=1}^{\infty} I^n / I^{n+1}$, which is generated as an R/I algebra by $\bar{r}_1, \dots, \bar{r}_l$, but R/I is Noetherian, so $G_I(R)$ is Noetherian by Proposition 10.3.
2. Let $(M_n)_{n=0}^\infty$ be stable, so there is n_0 with $M_{n_0+k} = I^k M_{n_0}$ for all $k \geq 0$. So $G(M)$ is generated by $\bigoplus_{n=0}^{n_0} M_n / M_{n+1}$ as a $G_I(R)$ module. We know M is a Noetherian R -module as it is finitely generated, so M_{n_0} is Noetherian and hence so is M_{n_0} / M_{n_0+1} . We know $I(M_{n_0} / M_{n_0+1}) = 0$, so M_{n_0} / M_{n_0+1} is a finitely generated R/I module, and hence so is $\bigoplus_{n=0}^{n_0} M_n / M_{n+1}$, so $G(M)$ is finitely generated as a $G_I(R)$ module and we are done.

□

Definition 10.11. Two filtrations $(M_n)_{n=0}^\infty$ and $(M'_n)_{n=0}^\infty$ of an R -module M are *equivalent* if there is n_0 such that $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$ for all $n \geq 0$

Lemma 10.2. Given $I \trianglelefteq R$, every stable I -filtration $(M_n)_{n=0}^\infty$ of an R -module M is equivalent to $(I^n M)_{n=0}^\infty$

Proof. $(M_n)_{n=0}^\infty$ is an I filtration, so $M_n \supseteq IM_{n-1} \cdots \supseteq I^n M$, so for all $k \geq 0$, $M_n \supseteq I^{n+k} M$. For the other inclusion, there is some $n_0 \geq 0$ such that $IM_n = M_{n+1}$ for $n \geq n_0$. Then $M_{n+n_0} = I^n M_{n_0} \subseteq I^n M$ so we are done □

Let $I \trianglelefteq R$, M an R -module and $(M_n)_{n=0}^\infty$ an I -filtration of M . We define a graded ring $R_* = \bigoplus_{n=0}^\infty I^n / I^{n+1}$ with the usual multiplication. We define a graded module $M_* = \bigoplus_{n=0}^\infty M_n$. This is an R^* module in the obvious way.

Lemma 10.3. If R is Noetherian, then R^* is Noetherian

Proof. Since R is Noetherian, I is finitely generated, and so R^* is generated as an algebra by their reductions, and so it is Noetherian. □

Lemma 10.4. If R is a Noetherian ring and M is a finitely generated R -module with $(M_n)_{n=0}^\infty$ an I filtration. Then the following are equivalent

1. M_* is a finitely generated R_* module
2. $(M_n)_{n=0}^\infty$ is stable

Proof. Note that M being finitely generated implies M is Noetherian so each M_n is finitely generated. We consider the R_* submodule of M_* of the form $M_*^{(n)} = M_0 \oplus \cdots \oplus M_n \oplus \bigoplus_{i=1}^\infty I^i M_n$. Then $M_*^{(0)} \subseteq M_*^{(1)} \subseteq \dots$ since $(M_n)_{n=0}^\infty$ is an I filtration. The chain stabilises if and only if the filtration is stable.

(1) implies (2) is now immediate.

For (2) implies (1), we need to prove that if the chain stabilises, then M_* is finitely generated. We know $M_* = \bigcup_{n=0}^\infty M_*^{(n)} = M_*^{(n_0)}$, so M_* is generated by $\bigoplus_{i=0}^{n_0} M_i$ which is finitely generated as each M_i is finitely generated, so we are done □

Theorem 10.5. (Artin-Rees lemma) Let R be a Noetherian ring with $I \trianglelefteq R$ and M a finitely generated R module. If $(M_n)_{n=0}^\infty$ is a stable I -filtration of M and N is a submodule of M , then $(N \cap M_n)_{n=0}^\infty$ is a stable I -filtration of N .

Proof. Now $I(N \cap M_n) \subseteq N \cap IM_n \subseteq N \cap M_{n+1}$, so our filtration on N is an I -filtration. We use $N_n = N \cap M_n$. We have a module N_* which is graded R_* submodule of M_* . By assumption, $(M_n)_{n=0}^\infty$ is stable, so by the lemma above, M_* is a finitely generated R_* module. R_* is Noetherian, so M_* is and hence N_* is. So N_* is finitely generated, so $(N_n)_{n=0}^\infty$ is stable and we are done. □

11 Dimension Theory

Definition 11.1.

1. The *height*, $\text{ht } \mathfrak{p}$ of a prime ideal $\mathfrak{p} \subseteq R$ is the supremum of lengths of chains of prime ideals $\mathfrak{p}_0 \subseteq \cdots \subseteq \mathfrak{p}_d = \mathfrak{p}$ ending in $\mathfrak{p}$.
2. The *krull dimension* of R , denoted $\dim R$, is the supremum of the heights of all prime ideals

Remark. $\dim R_{\mathfrak{p}} = \text{ht } \mathfrak{p}$ for all $\mathfrak{p} \in \text{Spec } R$, so $\dim R = \sup \dim R_{\mathfrak{m}}$ where $\mathfrak{m} \in \text{mSpec } R$

Example 11.1. If $R = k[x, y]$ then $(0) \subseteq (x) \subseteq (x, y)$. It is a fact we will prove later that $\dim R = 2$

We list some corollaries of things we have proven before

Corollary 11.0.1.

1. R is Artinian if and only if it is Noetherian of dimension 0
2. DVRs are integrally closed Noetherian local integral domains of krull dimension 1
3. Dedekind domains are integrally closed Noetherian integral domains of krull dimension 1

11.1 Hilbert Functions

Lemma 11.1. Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a Noetherian graded ring with $M = \bigoplus_{n=0}^{\infty} M_n$ a finitely generated graded R -module. Then each M_n is a finitely generated R_0 module.

Proof. As R is Noetherian, so R_0 , and R is a finitely generated R_0 algebra. Suppose $R = R[r_1, \dots, r_k]$. By taking homogeneous components, each r_i is homogeneous. As M is a finitely generated R -module, let $m_1, \dots, m_l$ be homogeneous generators with m_i having degree k_i . We can write $m \in M_n$ as $m = \sum_{i=1}^l f_i(r_1, \dots, r_k)m_i$ where f_i is a homogeneous polynomial of degree $n - k_i$ if it is non-zero. Therefore M_n is generated by $\{g(r_1, \dots, r_k)m_i \mid g(r_1, \dots, r_k) \text{ monomial of degree } n - k_i\}$, which is finite. $\square$

Definition 11.2. Let $R = \bigoplus_{n=0}^{\infty} R_n$ be a Noetherian graded ring with $M = \bigoplus_{n=0}^{\infty} M_n$ a finitely generated R -module. Let λ be an additive function on finitely generated R_0 modules with values in $\mathbb{Z}$, where *additive* means that if $0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$ is exact, then $\lambda(M) = \lambda(L) + \lambda(N)$. The *Poincaré series* of M with respect to λ is the generating function of $\lambda(M_n)$, ie

$$P_M(t) = \sum_{n=0}^{\infty} \lambda(M_n)t^n \in \mathbb{Z}[[t]]$$

Theorem 11.2. (Hilbert-Serre Theorem) $P_M(t)$ is a rational function of the form

$$P_M(t) = \frac{f(t)}{\prod_{i=1}^s (1 - t^{k_i})}$$

where $f(t) \in \mathbb{Z}[t]$

Proof. We induct on s , the number of generators of R over R_0 . For $s = 0$, we have $R = R_0$, and M is a finitely generated R_0 -module, so $M_n = 0$ for sufficiently large n , and so $P_M(t) \in \mathbb{Z}[t]$

Suppose $s \geq 1$ and the result holds for $s - 1$. Let $r_1, \dots, r_s$ be generators of R over R_0 . Multiplication by r_s gives an R -module homomorphism $M_n \rightarrow M_{n+k_s}$. Taking the kernel and cokernel as K_n, L_{n+k_s} , we get

$$0 \rightarrow K_n \rightarrow M_n \rightarrow M_{n+k_s} \rightarrow L_{n+k_s}$$

Summing over all n , we get $K = \bigoplus_{n=0}^{\infty} K_n, L = \bigoplus_{n=0}^{\infty} L_n$. These are finitely generated as they are a submodule resp. quotient of M and R is Noetherian. Both are annihilated by r_s , so they are finitely generated over $R_0[r_1, \dots, r_{s-1}]$. By ES3,

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0$$

Multiplying by t^{n+k_s} ,

$$t^{n+k_s} \lambda(M_{n+k_s}) - t^{k_s} \lambda(M_n) t^n = t^{n+k_s} \lambda(L_{n+k_s}) - t^{k_s} \lambda(K_n) t^n$$

Then

$$P_M(t) - \sum_{n=0}^{k_s-1} \lambda(M_n) t^n - t^{k_s} P_M(t) = P_L(t) - \sum_{n=0}^{k_s-1} \lambda(L_n) t^n - t^{k_s} P_K(t)$$

Rearranging for $P_M(t)$ and applying the inductive hypothesis to L, K gives the result. $\square$

Example 11.2. If $R = k[x_1, \dots, x_s] = \bigoplus_{n=0}^{\infty} R_n$ where R_n are the homogeneous polynomials of degree n (and 0). Let λ be the length of the module over $R_0 = k$. $t_1, \dots, t_s$ are generators all of degree 1. There are $\binom{n+s-1}{n}$ monomials of degree n in R , which form a k -basis for R_n . Then

$$\begin{aligned} P_R(t) &= \sum_{n=0}^{\infty} \binom{n+s-1}{n} t^n \\ &= \left(\sum_{k=0}^{\infty} t^k \right)^s \\ &= \frac{1}{(1-t)^s} \end{aligned}$$

Definition 11.3. We write $d(M)$ for the order of the pole of $P_M(t)$ at $t = 1$

Lemma 11.3. $d(M) \geq 0$ if $M \neq 0$ and $\lambda = l$ is the length

Proof. If $d(M) < 0$, then $\sum \dim M_i = P_M(1) = 0$, so every $\dim M_i = 0$. $\square$

Corollary 11.3.1. *If each $k_i = 1$, then for sufficiently large n , we have that $\lambda(M_n)$ is a polynomial in n of degree $d - 1$ with rational coefficients where $d = d(M)$*

Proof. Convention: $\deg 0 = -1$.

By Hilbert-Serre, $\lambda(M_n)$ is the coefficient of t^n in $f(t)(1-t)^{-s}$. By cancelling powers of $(1-t)$, we can assume $s = d$ and $f(1) \neq 0$. Let $f(t) = \sum_{i=0}^l a_i t^i$. So we get for $n \geq l$

$$\lambda(M_n) = \sum_{i=0}^l a_i \binom{d+n-i-1}{d-1}$$

The right hand side is a polynomial in n with leading term $\frac{n^{d-1}}{(d-1)!} \sum_{i=0}^l a_i$ which is non-zero. $\square$

Definition 11.4. The function $n \mapsto \lambda(M_n)$ is called the *Hilbert function* of M with respect to λ . The polynomial of the corollary is called the *Hilbert polynomial*

Definition 11.5. $r \in R \setminus \{0\}$ is a *zero divisor* in M if there is $m \in M \setminus \{0\}$ such that $rm = 0$

Proposition 11.1. *If $r \in R_k$ is not a zero divisor in M , then $d(M/rM) = d(M) - 1$*

Proof. Consider the exact sequence

$$0 \rightarrow K_n \rightarrow M_n \xrightarrow{r} M_{n+k} \rightarrow L_{n+k} \rightarrow 0$$

as in the Hilbert Serre Theorem, and let $K = \bigoplus_{n=0}^{\infty} K_n$ and $L = \bigoplus_{n=0}^{\infty} L_n$. We know $K = 0$ as r is not a zero divisor in M , and $L = M/rM$. Repeating the proof of the Hilbert-Serre theorem,

$$(1-t^k)P_M(t) = P_{M/rM}(t) + g(t)$$

for some polynomial $g(t)$, so the result follows. $\square$

From now on, we make the following assumptions: λ is the length function, R_0 is Artinian (we already knew it is Noetherian) so finitely generated R_0 -modules M_n are Noetherian and Artinian, so have finite length

Proposition 11.2. *Let $(R, \mathfrak{m})$ be a Noetherian local ring, and $I \trianglelefteq R$ be $\mathfrak{m}$ -primary. Let M be a finitely generated R -module with stable I -filtration $(M_n)_{n=0}^{\infty}$. Then*

1. $l(M/M_n) < \infty$ for all $n > 0$

2. For sufficiently large n , $l(M/M_n) = g(n)$ where g is a polynomial of degree s , where s is the minimal number of generators of I
3. The degree and leading coefficient of $g(n)$ depend only on M and I , and not on the choice of filtration

Proof. $G(R) = G_I(R)$ is Noetherian, so $G_0(R) = R/I$ is a Noetherian local ring with sole prime ideal $\mathfrak{m}$, so every prime is maximal and hence $G_0(R)$ is Artinian and local. $G(M)$ is a finitely generated $G(R)$ module since the I -filtration is stable, so $G_n(M) = M_n/M_{n+1}$ is a Noetherian R -module annihilated by I , hence is a Noetherian $G_0(R)$ module (and so is Artinian). Therefore $l(G_n(M)) < \infty$. We deduce that $l(M/M_n) < \infty$ as it is equal to $\sum_{i=1}^n l(G_i(M))$, so (1) is proven. As R is Noetherian, we can write $I = (r_1, \dots, r_s)$ with s minimal. The images $\bar{r}_i \in I/I^2$ generate $G(R)$ as a $G_0(R)$ -algebra, and $\deg \bar{r}_i = 1$. Therefore $l(M_n/M_{n+1}) = f(n)$, the Hilbert polynomial, for sufficiently large n , where $\deg f = s - 1$. We have $f(n) = l(G_{n+1}(M)) - l(G_n(M))$, so l_n is a polynomial of degree s for sufficiently large n , so (2) is done.

Let $(\tilde{M}_n)_{n=0}^\infty$ be another stable I -filtration and $\tilde{g}(n) = l(\tilde{M}_n/\tilde{M}_{n+1})$. By equivalence, there is some n_0 with $M_{n+n_0} \subseteq \tilde{M}_n$ (and the reverse holds). Then $g(n + n_0) = l(M/M_{n+n_0}) \geq l(M/\tilde{M}_n) = \tilde{g}(n)$, so $\deg g \leq \deg \tilde{g}$ (and the same inequality for leading coefficient if we have equality), and swapping the roles gives the reverse, so we are done. $\square$

Definition 11.6. We denote by $\chi_I^M(n)$, $g(n)$ for $(I^n M)_{n=0}^\infty$, ie $\chi_I^M(n) = l(M/I^n M)$ for sufficiently large n . If $M = R$, we write $\chi_I(n)$ instead and call this the *characteristic polynomial* of the $\mathfrak{m}$ -primary ideal I

Proposition 11.3. $\deg \chi_I(n) = \deg \chi_{\mathfrak{m}}(n)$ under the same assumptions of the preceding proposition.

Proof. We know $\mathfrak{m} \supseteq I \supseteq \mathfrak{m}^k$ for some k , so $l(R/\mathfrak{m}^n) \leq l(R/I^n) \leq l(R/\mathfrak{m}^{kn})$, so $\chi_{\mathfrak{m}}(n) \leq \chi_I(n) \leq \chi_{\mathfrak{m}}(kn)$ for sufficiently large n . Letting $n \rightarrow \infty$, we are done. $\square$

Corollary 11.3.2. $\deg \chi_{\mathfrak{m}}(n) = d(G_{\mathfrak{m}}(R))$

Proof. $l(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ is a polynomial $f(n)$ of degree $d(G_{\mathfrak{m}}(R)) - 1$. If $l_n = l(M/M_n)$, then $l_{n+1} - l_n = f(n)$, so l_n is a polynomial of degree $d(G_{\mathfrak{m}}(R))$, so the result follows. $\square$

11.2 Dimension Theory of Noetherian Local Rings

Let $(R, \mathfrak{m})$ be a Noetherian local ring. We denote by $\delta(R)$ the minimal number of generators of an $\mathfrak{m}$ -primary ideal of R . We denote $D(R) = d(G_{\mathfrak{m}}(R)) = \deg \chi_{\mathfrak{m}}(n)$. We aim to show these are equal, and equal to $\dim R$

Proposition 11.4. $\delta(R) \geq D(R)$

Proof. This was Proposition 11.2(2) $\square$

We will now show $D(R) \geq \dim R \geq \delta(R)$.

Proposition 11.5. *Let I be $\mathfrak{m}$ -primary, and let M be a finitely generated R -module, and $r \in R$ not a zero divisor in M . If we write $M' = M/rM$, then $\deg \chi_I^{M'} \leq \deg \chi_I^M - 1$*

Proof. Let $N = rM$, so $N \cong M$ as r is not a zero divisor in M . Let $N_n = I^n M \cap N$. There is a short exact sequence

$$0 \rightarrow N/N_n \rightarrow M/I^n M \rightarrow M'/I^n M' \rightarrow 0$$

So if $g(n) = l(N/N_n)$, then $g(n) - \chi_I^M(n) + \chi_I^{M'}(n) = 0$. By the Artin-Rees lemma, $(N_n)_{n=0}^\infty$ is a stable I -filtration. Since $M \cong N$, $g(n)$ and $\chi_I^M(n)$ have the same leading term by Proposition 11.2(3), so $\deg \chi_I^{M'} \leq \deg \chi_I^M - 1$ as desired $\square$

Corollary 11.3.3. *If R is Noetherian local and $r \in R$ is not a zero divisor, then $D(R/(r)) \leq D(R) - 1$*

Proof. Trivial $\square$

Proposition 11.6. $D(R) \geq \dim R$

Proof. We proceed by induction on $d = D(R)$.

If $d = 0$, then $l(R/\mathfrak{m}^n)$ is eventually constant, so $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ for some $n > 0$, hence R is Artinian, so is dimension 0. Now let $d \geq 1$, and $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_k$ with $\mathfrak{p}_i \in \text{Spec } R$. Let $r \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$, $R' = R/\mathfrak{p}_0$, and $r' = \bar{r}$. Then $r' \neq 0$ and R' is an integral domain, so $D(R/(r')) \leq D(R') - 1$. Let $\mathfrak{m}'$ be the maximal ideal of R' . We get a commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{a} & R' \\ c \downarrow & & \downarrow b \\ R/\mathfrak{m}^n & \xrightarrow{u} & R'/(\mathfrak{m}')^n \end{array}$$

u is surjective since $b \circ a$ is, so $l(R/\mathfrak{m}^n) \geq l(R'/(\mathfrak{m}')^n)$ and so $D(R) \geq D(R')$. Then $D(R/(r')) \leq D(R') - 1 \leq D(R) - 1 = d - 1$. By induction, $\dim R'/(r') \leq d - 1$. The images of $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ in $R'/(r')$ form a chain of prime ideals, so $k - 1 \leq d - 1$, ie $k \leq d$. $\square$