Elementary commutative algebra

Will Troiani

August 2020

Contents

1 Linear Algebra

1.1 Orthogonal matrices

Throughout, k is an algebraically closed field.

Definition 1.1.1. A square matrix $X \in M_n(k)$ is **orthogonal** if $X^T = X^{-1}$.

These come up when dealing with orthonormal bases:

Lemma 1.1.2. *A square matrix $X \in M_n(k)$ is orthonormal if and only if its columns form an orthogonal basis for k^n.*

Proof. Write $X = [v_1, ..., v_n]$ for vectors $v_i \in k^n$. Then $v_i \cdot v_j = \delta_{ij}$ if and only if $XX^T = I$. □

Lemma 1.1.3. *For every symmetric matrix $X \in M_n(k)$ there exists an orthogonal matrix U such that U^TXU is diagonal.*

Proof. We proceed by induction on n, the base case is trivial. Say $n > 1$. Since k is algebraically closed we can find an eigenvector $v_1 \in k^n$ of X with eigenvalue $\lambda \in k$ and by replacing v_1 with $v_1/||v_1||$ if necessary we may assume v_1 is of unit length too. We extend v_1 to an orthonormal basis $\{v_1, ..., v_n\}$ of k^n and set $Q = [v_1, ..., v_n]$, that is, Q is the matrix with i^{th} column is the vector v_i. We then have

$$Q^TXQ = \begin{pmatrix} \lambda & u \\ 0 & X' \end{pmatrix}$$

for some $u \in M_{1\times n-1}(k)$ and $X' \in M_{n-1}(k)$. Taking the transpose of each side we have:

$$Q^TX^TQ = \begin{pmatrix} \lambda & 0 \\ u & X'^T \end{pmatrix}$$

Since X is symmetric we have $X = X^T$ and so $Q^TXQ = Q^TX^TQ$ which implies $u = 0$ and X' is symmetric. We can apply the inductive hypothesis to X' to get an orthogonal matrix $V \in M_{n-1}(k)$ such that $V^TX'V = D$ is diagonal. We thus have

$$Q^TXQ = \begin{pmatrix} \lambda & 0 \\ 0 & VDV^T \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & D \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & V^T \end{pmatrix}$$

The result then follows as $Q \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix}$ is orthogonal. □

1.2 Partial trace

Throughout, V, W are finite dimensional vector spaces. First we make an observation, let $\{v_1, ..., v_n\}$ and $\{w_1, ..., w_m\}$ be bases for V, W respectively. Let $\gamma : V \otimes W \longrightarrow V \otimes W$ be a linear map. We write

$$\begin{aligned}\gamma(v_i \otimes w_j) = \alpha_{11,ij} v_1 \otimes w_1 + \ldots + \alpha_{1m,ij} v_1 \otimes w_m \\ + \ldots \\ + \alpha_{n1,ij} v_n \otimes w_1 + \ldots + \alpha_{nm,ij} v_n \otimes w_m\end{aligned}$$

so that if we make the following definitions:

$$\begin{aligned} E_{ij} : V &\longrightarrow V & \qquad F_{ij} : W &\longrightarrow W \\ v_i &\longmapsto \delta_{ij} v_j & \qquad w_i &\longmapsto \delta_{ij} w_j \end{aligned}$$

where $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j$, we have:

$$\begin{aligned}\gamma = \sum_{i=1}^{n} \sum_{j=1}^{m} \Big(\alpha_{11,ij} E_{i1} \otimes F_{j1} + \ldots + \alpha_{1m,ij} E_{i1} \otimes F_{jw} \\ + \ldots \\ + \alpha_{n1,ij} E_{in} \otimes F_{j1} + \ldots + \alpha_{nm,ij} E_{in} \otimes F_{jm} \Big)\end{aligned}$$

We arrive at:

Observation 1.2.1. The set

$$\{E_{ik} \otimes F_{jl}\}_{i,k=1,...,n}^{j,l=1,...,m} \tag{1}$$

forms a basis for $\operatorname{Hom} V \otimes W$. More sophisticatedly, an easy extension of what we have shown yields:

Lemma 1.2.2. *For arbitrary vector spaces X, Y, X', Y' there exists a natural injection*

$$\operatorname{Hom}(X, X') \otimes \operatorname{Hom}(Y, Y') \rightarrowtail \operatorname{Hom}(X \otimes Y, X' \otimes Y') \tag{2}$$

which is an isomorphism if X, Y, X', Y' are finite dimensional.

Remark 1.2.3. The map described in Lemma 1.2.2 sends a formal tensor element $f \otimes g$ to the tensor product of the two maps f and g, which is also denoted $f \otimes g$. Hence we clearly have an injection, and the argument above shows surjectivity in the finite dimensional case.

It follows easily from this presentation that this map is natural in all arguments.

Corollary 1.2.4. *There is a natural isomorphism (recall that V, W are finite dimensional).*

$$\operatorname{Hom}(V, W) \longrightarrow V^* \otimes W \tag{3}$$

$$f \longmapsto \sum_{i=1}^{n} v_i^* \otimes f(v_i) \tag{4}$$

where $\{v_1, ..., v_n\}$ is ar arbitrary basis for V.

Proof. By Lemma 1.2.2 we have:

$$\mathrm{Hom}(V \otimes k, k \otimes W) \cong \mathrm{Hom}(V, k) \otimes \mathrm{Hom}(k, W) \tag{5}$$

hence we can perform the following calculation, where $s : V \otimes k \longrightarrow k \otimes V$ is the swap map, for $i = 1, ..., n$ we denote by $E_i : V \longrightarrow k$ is the linear map sending $v_i \longmapsto 1$ and $F_j : k \longrightarrow V$ the linear map sending $1 \longmapsto v_i$.

$$f \longmapsto 1 \otimes f \circ s = \sum_{i=1}^{n} E_i \otimes fF_i \longmapsto \sum_{i=1}^{n} v_i^* \otimes f(v_i) \tag{6}$$

□

We will generalise the definition of the trace operator to the definition of a *partial* trace operator, to do this we use the natural isomorphism of Corollary 1.2.4 and combine it with the following adjunction, the **tensor-hom** adjunction.

Fact 1.2.5. *There is an adjunction*

$$\mathrm{Hom}(V \otimes W, U) \cong \mathrm{Hom}(W, \mathrm{Hom}(V, U)) \tag{7}$$

$$f \longmapsto \big(w \mapsto (v \mapsto f(v \otimes w))\big) \tag{8}$$

$$\big(v \otimes w \mapsto g(v)(w)\big) \longleftarrow\!\shortmid\ g \tag{9}$$

with counit given by the evaluation map (we simply write h for Hom*)*

$$\begin{aligned} V \otimes h(V, U) &\longrightarrow U \\ v \otimes f &\longmapsto f(v) \end{aligned}$$

and unit given by tensor:

$$\begin{aligned} U &\longrightarrow h(V, V \otimes U) \\ u &\longmapsto (v \mapsto v \otimes u) \end{aligned}$$

Corollary 1.2.6. *For finite dimensional vector spaces, there is an adjunction:*

$$\mathrm{Hom}(V \otimes W, U) \longrightarrow \mathrm{Hom}(W, U \otimes V^*) \tag{10}$$

$$f \longmapsto \big(w \mapsto \sum_{i=1}^{n} v_i^* \otimes f(u_i \otimes w)\big) \tag{11}$$

where $\{u_1, ..., u_n\}$ is an arbitrary choice of basis for V.

The counit of this adjunction is given by

$$\begin{aligned} V \otimes U \otimes V^* &\longrightarrow U \\ x \otimes u \otimes y^* &\longmapsto y^*(x)u \end{aligned}$$

and unit given by (where $v_1, ..., v_n$ is an arbitrary basis for V)

$$\begin{aligned} W &\longrightarrow W \otimes V \otimes V^* \\ w &\longmapsto w \otimes (\sum_{i=1}^{n} v_i \otimes v_i^*) \end{aligned}$$

Proof. For existence of the adjunction, we observe the following algebra.

$$\begin{aligned} \mathrm{Hom}(V \otimes W, U) &\cong \mathrm{Hom}(W, \mathrm{Hom}(V, U)) && (12) \\ &\cong \mathrm{Hom}(W, V^* \otimes U) && (13) \end{aligned}$$

Now we unwind definitions and find the unit and counit. Writing simply h for Hom the map:

$$h(V,V) \longrightarrow h(V \otimes k, k \otimes V) \longrightarrow h(V,k) \otimes h(k,V) \longrightarrow V^* \otimes V \tag{14}$$

acts on id_V in the following way, where s denotes the *swap map* and $v_1, ..., v_n$ is an arbitrary basis for V,

$$\mathrm{id}_V \longmapsto s \longmapsto \sum_{i=1}^{n} v_i^* \otimes (1 \mapsto v_i) \longmapsto \sum_{i=1}^{n} v_i^* \otimes v_i \tag{15}$$

which describes the unit. The counit is calculated similarly. □

With this language, we come up with a description of the trace operator.

Observation 1.2.7. Let $f : V \longrightarrow V$ be a linear map. Then the map $k \longrightarrow k$ given by $1 \longmapsto \mathrm{Trace}\, f$ is given by the following composite, where η, ϵ are respectively the unit and counit of the adjunction (10) and $v_1, ..., v_n$ is an arbitrary basis for V:

$$\begin{array}{ccccccc} k & \xrightarrow{\eta} & V \otimes V^* & \xrightarrow{f \otimes 1} & V \otimes V^* & \xrightarrow{\qquad\qquad \epsilon \qquad\qquad} & k \\ 1 & \longmapsto & \sum_{i=1}^n v_i \otimes v_i^* & \longmapsto & \sum_{i=1}^n f(v_i) \otimes v_i^* & \longmapsto & \sum_{i=1}^n v_i^*(f(v_i)) = \mathrm{Trace}\, f \end{array} \tag{16}$$

We use this observation to make a definition:

Definition 1.2.8. Let $f : W \otimes V \longrightarrow W \otimes V$ be a linear map. We define the **partial trace operator** $\mathrm{Trace}_V f$ as the following composite:

$$\begin{array}{ccccccc} W & \xrightarrow{\qquad 1 \otimes \eta \qquad} & W \otimes V \otimes V^* & \xrightarrow{\qquad\qquad f \otimes 1 \qquad\qquad} & W \otimes V \otimes V^* & \xrightarrow{1 \otimes \epsilon} & W \\ w & \longmapsto & w \otimes (\sum_{i=1}^n v_i \otimes v_i^*) = \sum_{i=1}^n (w \otimes v_i) \otimes v_i^* & \longmapsto & \sum_{i=1}^n f(w \otimes v_i) \otimes v_i^* & \longmapsto & \dots \end{array} \tag{17}$$

the final formula is a bit difficult to write out, in the special case where $f = f_1 \otimes f_2$ for $f_1 : W \longrightarrow W, f_2 : V \longrightarrow V$ we obtain

$$(\mathrm{Trace}_V\, f)(w) = \sum_{i=1}^{n} f_1(w) v_i^*\big(f_2(v_i)\big) = (\mathrm{Trace}\, f_2) f_1(w) \tag{18}$$

In fact we can write out a formula for (17) if we use Dirac notation. Let $|1\rangle, ..., |n\rangle$ be a basis for V, we think of these as operators $k \longrightarrow V$. We write $\mathrm{id} \otimes |i\rangle$ for the composite $W \longrightarrow W \otimes k \longrightarrow W \otimes V$. Also, we denote the multiplication map $W \otimes k \longrightarrow W$ defined by $w \otimes x \longmapsto xw$ by Mult. We have

$$\begin{aligned} \mathrm{Trace}_V\, f &= \epsilon\Big(\sum_{i=1}^{n} f(\mathrm{id} \otimes |i\rangle) \otimes \langle i| \Big) \\ &= \mathrm{Mult}\Big(\sum_{i=1}^{n} (\mathrm{id} \otimes \langle i|) f (\mathrm{id} \otimes |i\rangle) \Big) \end{aligned}$$

2 Rings and modules

Definition 2.0.1. Let A be a ring, the **Jacobson radical** $\mathfrak{R}$ is the intersection of all maximal ideals of A.

Lemma 2.0.2. *Let A be a ring. $x \in \mathfrak{R}$ if and only if $1 - xy$ is a unit for all $y \in A$.*

Proof. Say $1-xy$ is not a unit. Then it is contained inside some maximal ideal $\mathfrak{m}$, but so is xy as $x \in \mathfrak{m}$, thus $1 \in \mathfrak{m}$ which is a contradiction.

Conversely, if x is not contained in some maximal ideal $\mathfrak{m}$ then $\mathfrak{m}$ and x generated (1) (by maximality). Thus $1 = yx + u$ for some $u \in \mathfrak{m}$, that is, $1 - xy \in \mathfrak{m}$, and is therefore not a unit. □

Definition 2.0.3. Let A be a ring, the **nilradical** is the ideal of nilpotents.

Lemma 2.0.4. *The nilradical is equal to the intersection of all prime ideals (in a commutative ring).*

Proof. Clearly all nilradicals are contained in all prime ideals.

Conversely, if a is not nilpotent then A_a is not the zero ring and thus contains a prime. □

2.1 Localisation (Nakayama's Lemma)

Lemma 2.1.1. *Let M be an R-module such that for all maximal ideals $\mathfrak{m}$ of R we have $M_{\mathfrak{m}} = 0$. Then $M = 0$.*

Proof. Let $x \in M$ be such that $x/1 = 0$ in $M_{\mathfrak{m}}$. Then there exists $a \notin \mathfrak{m}$ such that $ax = 0$, which is to say $\operatorname{ann}(x) \not\subseteq \mathfrak{m}$. Since this is true for all maximal ideals $\mathfrak{m}$ we have that $\operatorname{ann}(x) = A$ which implies $x = 0$. □

We use the above to give a slick proof that a ring map being an isomorphism is a local property:

Corollary 2.1.2. *A ring homomorphism $\psi : A \longrightarrow B$ is an isomorphism if and only if its localisation at all maximal ideals is.*

Proof. It's easy to show $\ker \psi_{\mathfrak{m}} \cong (\ker \psi)_{\mathfrak{m}}$ and $\operatorname{coker} \psi_{\mathfrak{m}} \cong (\operatorname{coker} \psi)_{\mathfrak{m}}$. Thus the Lemma follows from Lemma 2.1.1 □

Lemma 2.1.3 (Nakayama's Lemma)**.** *Let R be a ring and M a finitely generated R-module. If $I \subseteq R$ is an ideal contained in the jacobson radical such that $IM = M$ then $M = 0$.*

We reduce to the local case and then make a simple observation.

Proof. We use Lemma 2.1.1.

Let $\mathfrak{m}$ be a maximal ideal such that $I \subseteq \mathfrak{m}$ which necessarily exists as I is contained in the jacobson radical. Then $\mathfrak{m}M = M$ and $(\mathfrak{m}A_{\mathfrak{m}})M_{\mathfrak{m}} = M_{\mathfrak{m}}$, so it suffices to assume A is local and I is maximal. Let $\mathfrak{m}$ denote the unique maximal ideal.

Let $m_1, ..., m_n$ be a set of generators for M. Then $m_1 = i_1 m_1 + \ldots + i_n m_n$ for some elements i_j contained in the maximal ideal of R. Thus $(1 - i_1)m_1 = i_2 m_2 + \ldots + i_n m_n$. In fact $1 - i_1$ is a unit because $i_1 \in \mathfrak{m}$ and $1 \notin \mathfrak{m}$, thus $m_2, ..., m_n$ form a generating set. Applying this logic finitely many times we see that M is generated by m_n, but then $m_n = i m_n$ for some $i \in \mathfrak{m}$ so $(1 - i)m_n = 0$ which by the same logic as above implies $m_n = 0$. □

2.2 Chain conditions

Lemma 2.2.1. *Given a short exact sequence of A-modules*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

M is Noetherian if and only if M', M'' are.

Proof. Every sub and quotient module of a neotherian module is Noetherian which establishes one direction.

Conversely, let $N \subseteq M$ be a submodule and let $x \in N$. Then consider $[x] \in M/\ker\psi$ where we can write $[x] = \sum_{i=0}^{n} \alpha_i [x_i]$ where $\{[x_i]\}_{i=0}^{n}$ is a finitely generating set of $\psi(N)$. Choosing representatives we have $x - \sum_{i=0}^{n} \alpha_i x_i \in \ker\psi$. We have a short exact sequence so $\ker\psi = M'$ which is finitely generated so there exists $y_1, ..., y_m$ such that $x - \sum_{i=0}^{n} \alpha_i x_i = \sum_{j=0}^{m} \beta_j y_j$. Thus N is finitely generated. □

Remark 2.2.2. There is a better proof which can be used here. The obvious idea working directly with the ascending chain condition works and gives a proof idea which also works for Artinian. The above proof does not work for Artinian rings because there is no analogue in the setting of Artinian rings to the statement that a ring a module is Noetherian if and only if all its submodules are finitely generated.

Corollary 2.2.3. *If R is a Noetherian ring then so is R^n.*

Proof. Obvious inductive argument. □

Corollary 2.2.4. *If R is Noetherian then every finitely generated R-module M is Noetherian.*

Proof. Write $M = R^n/I$. □

2.2.1 Artinian rings/modules

Definition 2.2.5. A ring A is **Artinian** if every *descending* chain of ideals

$$I_1 \supseteq I_2 \supseteq \dots$$

terminates. That is, there exists $N > 0$ where for all $n > N$ we have $I_n = I_{n+1}$.

Lemma 2.2.6. *Every Artinian ring A has finitely many maximal ideals.*

Proof. Say A has infinitely many maximal ideals $\{\mathfrak{m}_1, \mathfrak{m}_2, \dots\}$. Then consider the chain

$$\mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \dots$$

we claim this is an infinite descending chain. Consider the link $\mathfrak{m}_1 \dots \mathfrak{m}_n \supseteq \mathfrak{m}_1 \dots \mathfrak{m}_n\mathfrak{m}_{n+1}$ for any n. If this was equality then we would have

$$\mathfrak{m}_1 \dots \mathfrak{m}_n \subseteq \mathfrak{m}_1 \dots \mathfrak{m}_n\mathfrak{m}_{n+1} \subseteq \mathfrak{m}_{n+1}$$

so by primality, $\mathfrak{m}_i \subseteq \mathfrak{m}_{n+1}$ for some $i \leq n$. By maximality it follows that $\mathfrak{m}_i = \mathfrak{m}_{n+1}$ contradicting that these are distinct maximal ideals. □

Lemma 2.2.7. *Let A be Artinian, by Lemma 2.2.1 there is a finite set of maximal ideals $\{\mathfrak{m}_1, \dots, \mathfrak{m}_n\}$, denote by I the product $\mathfrak{m}_1 \dots \mathfrak{m}_n$. Then there exists $n > 0$ such that $I^n = (0)$.*

Proof. Suppose for a contradiction that $I^n \neq (0)$ for any n. Let n be such that $I^n = I^m$ for all $m > n$, which exists as A is Artinian. Let $\mathcal{S}$ be the set of ideals of A which do not annihilate I^n, then $A \in \mathcal{S}$ and so $\mathcal{S}$ is non-empty. Let J be a minimal element of $\mathcal{S}$, which exists as A is Artinian. We have that $JI^n \subseteq J$ and $(JI^n)I^n = JI^2n = JI^n \neq (0)$. so by minimality we have $JI^n = J$. There exists $j \in J$ such that $jI^n \neq 0$ and so again by minimality we have $(j) = J$. Thus there exists $i \in I^n$ such that $ji = j$, that is, $j(i-1) = 0$. We then have that $i \in \mathfrak{m}_k$ for all k and so $i - 1$ must not be in any $\mathfrak{m}_k$, which implies $i - 1$ is a unit and that $j = 0$, contradicting that J does not annihilate I^n. □

Proposition 2.2.8. *All Artinian rings are Noetherian.*

Proof. Let A be Artinian and $\{\mathfrak{m}_1, ..., \mathfrak{m}_m\}$ be the set of maximal ideals of A and let n be such that $(\mathfrak{m}_1 \dots \mathfrak{m}_m)^n = (0)$. Consider the chain

$$A \supseteq \mathfrak{m}_1 \supseteq \dots \supseteq \mathfrak{m}_1^n \supseteq \mathfrak{m}_1^n\mathfrak{m}_2 \supseteq \dots \supseteq \mathfrak{m}_1^n\mathfrak{m}_2^n \supseteq \dots \supseteq \mathfrak{m}_1^n \dots \mathfrak{m}_m^n = 0$$

each subquotient is an $A/\mathfrak{m}_i$-vector space for some i, and in fact is finite dimensional as these subquotients are Artinian modules. We thus have a decomposition series with Noetherian quotients and thus A is Noetherian. □

Corollary 2.2.9. *All finitely generated modules over Artinian rings are both Artinian and Noetherian.*

Proof. Let M be finitely generated over Artinian A. Then $M \cong A^n/I$ for some integer n and ideal $I \subseteq A$, and hence is Artinian. Since A is Artinian, it is thus Noetherian, and so M is Noetherian. □

Definition 2.2.10. A **composition series** of a module M is a finite sequence of submodules

$$0 = M_0 \subseteq M_1 \subseteq \dots \subseteq M_n = M$$

such that M_{i+1}/M_i is simple (admits no non-trivial submodules) for all $i \geq 0$. Such a series is denoted (M_i) and the length is denoted $l(M_i)$ (we will see shortly that this integer is independent of choice of decomposition series where the notation $l(M)$ will be adopted).

If N is a proper submodule of M and (M_i) is a decomposition series for M then we have a chain of submodules of N given by $(N_i := N \cap M_i)$. These are such that $N_{i+1}/N_i \rightarrowtail M_{i+1}/M_i$ so since the latter is simple we either have $N_{i+1}/N_i = M_{i+1}/M_i$ or $N_{i+1} = N_i$. We can remove equal terms so that the latter case is ruled out, and then we have a decomposition series for N satisfying $l(N_i) \leq l(M_i)$. If we had equality we would then have $N_{i+1}/N_i = M_{i+1}/M_i$ for all i form which we deduce that $N_1 = M_1$ which implies $N_2 = M_2$ and so on until $M = N$. Thus $l(N_i) < l(M_i)$.

Remark 2.2.11. An application of this is the following: let (N_i) be any ascending chain, say of length k. Then $N_0 \subseteq \dots \subseteq N_k = M$ implies $l(N_0) < \dots < l(N_k)$ and so $k \leq l(M)$. Thus all ascending chains have length less than or equal to that of the minimal decomposition series, in particular, all decomposition series have the same length. We denote this integer $l(M)$:

Proposition 2.2.12. *For any module M:*

1. *all decomposition series of M have the same length,*
2. *if $N \subsetneq M$ is a proper submodule, then $l(N) < l(M)$,*
3. *if M admits a decomposition series then any ascending chain can be extended to a decomposition series.*

Proof. The first two dotpoints have already been proved. For the last, if an ascending chain is not a decomposition series, then there exist intermediate modules which can be added to the chain. Do so finitely many times until a decomposition series is obtained. □

Remark 2.2.13. One might suspect that since there is no finite chain condition imposed on M in Proposition 2.2.12 that there may be an issue with part 3, for instance, maybe M admits infinite length chains as well as finite decomposition series. However this is impossible, as the length of any chain in M is bounded by the length of the decomposition series assumed to exist as per Remark 2.2.11.

The proof of the next Corollary shows that any finitely generated module over an Artinian ring admits a decomposition series:

Corollary 2.2.14. *Any finitely generated module over an Artinian ring has finite length.*

Proof. Let M be such a module. Then M is also Noetherian and so admits a maximal proper submodule M_1. M_1 itself is Noetherian and so also admits a maximal proper submodule. Continuing in this way we obtain a descending chain which terminates by the Artinian property. Thus we have a composition series and so all composition series are of this length, moreover any chain must have length less than this. ([6, §6]) □

Theorem 2.2.15. *A ring A is Artinian if and only if it is Noetherian and has dimension 0.*

2.3 Associated primes/primary decomposition

Definition 2.3.1. An ideal $I \subseteq R$ of a ring R is **primary** if it satisfies the following property:
if $ab \in I$ then either $a \in I$ or $b \in \sqrt{I}$.
If I is primary and $\sqrt{I}$ is a known prime $\mathfrak{p}$ then I is **$\mathfrak{p}$-primary**.

Definition 2.3.2. We refer to $\sqrt{(0)}$ as the **nilradical**. (Notice this agrees with Definition 2.0.3).

Lemma 2.3.3. *The nilradical is equal to the intersection of all prime ideals, in symbols:*

$$\sqrt{(0)} = \bigcap_{\mathfrak{p} \text{ prime}} \mathfrak{p}$$

Proof. See Lemma 2.0.4. □

Corollary 2.3.4. *For an ideal I the radical $\sqrt{I}$ is equal to the intersection of all prime ideals containing I,* $\bigcap_{\mathfrak{p} \supseteq I,\ \mathfrak{p} \text{ prime}} \mathfrak{p}$

Proof. By the correspondence Theorem the only check to make is that the image of $\sqrt{I}$ under the projection $A \longrightarrow A/I$ is equal to $\sqrt{(0)}$ but this is clear. □

Definition 2.3.5. Let $I \subseteq R$ be an ideal of a ring R. The **vanishing set** $V(I)$ is the set of prime ideals containing I,

$$V(I) := \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq I\}$$

Corollary 2.3.6. *If I, J are ideals and $V(I) \subseteq V(J)$, then $\sqrt{J} \subseteq \sqrt{I}$.*

Proof. Follows from Corollary 2.3.4. □

Remark 2.3.7. Clearly, if I is primary then $\sqrt{I}$ is prime however the converse does not hold: let $R = k[x, y, z]/(xy - z^2)$ and let $P = (x, z)$ which is prime, then P^2 is not primary. This is because $xy = z^2 \in P^2$ but $x \notin P^2$ and $y^n \notin P^2$ for any $n \geq 0$. This also shows that a power of a prime need not be primary.

Lemma 2.3.8. *If $\sqrt{I}$ is maximal, then I is primary. In particular, for a maximal ideal $\mathfrak{m}$ we have that $\mathfrak{m}^n$ for any $n > 0$ is $\mathfrak{m}$-primary.*

Proof. Let $\sqrt{I} = \mathfrak{m}$. Then the image of $\mathfrak{m}$ in A/I is the nilradical of A/I. Since the nilradical is the intersection of all primes, it follows that the A/I has only one prime. Thus every element of A/I is either a nilpotent or a unit, which means every zero divisor of A/I is nilpotent. □

Lemma 2.3.9. *Let R be a Noetherian ring and $I \subseteq R$ and ideal. There exists $n > 0$ such that $(\sqrt{I})^n \subseteq I$.*

Proof. Let $\sqrt{I}$ be generated by $a_1, ..., a_m$. For any n, the ideal $(\sqrt{I})^n$ is generated by elements of the form $a_1^{k_1}...a_m^{k_m}$ where $k_1 + \ldots + k_m = n$. Now let $r_i > 0$ be such that $a_i^{r_i} \in I$ and fix $n = r_1 + \ldots + r_m$. For each generating element $a_1^{k_1}...a_m^{k_m}$ of $(\sqrt{I})^n$ we must have for some j that $k_j \geq r_j$, and so $a_1^{k_1}...a_m^{k_m} \in I$ which completes the proof. Notice this proof works for any finitely generated ideal, be R Noetherian or not. □

Corollary 2.3.10. *Let A be a Noetherian local ring with maximal ideal $\mathfrak{m}$. Then for some $n \geq 0$, an ideal I is $\mathfrak{m}$-primary if and only if $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$.*

Proof. If I is $\mathfrak{m}$-primary then $\sqrt{I} = \mathfrak{m}$ and so by Lemma 2.3.9 we have $\mathfrak{m}^n = \sqrt{I}^n \subseteq I$. Also since A is local we have $I \subseteq \mathfrak{m}$.

Conversely, if $\mathfrak{m}^n \subseteq I \subseteq \mathfrak{m}$ for some n, $ab \in I$ implies $ab \in \mathfrak{m}$, say $a \notin \mathfrak{m}$. Then $b \in \mathfrak{m}$ and so $b^n \in \mathfrak{m}^n \subseteq I^n$, thus I is primary. Moreover,

$$\mathfrak{m} \subseteq \sqrt{\mathfrak{m}^n} \subseteq \sqrt{I} \subseteq \sqrt{\mathfrak{m}} \subseteq \mathfrak{m}$$

and so I is $\mathfrak{m}$-primary. □

We know that the prime ideals of $\mathbb{Z}$ are given by (p) where p is prime. The *primary ideals* of $\mathbb{Z}$ are given by (p^n). This follows from the fact that $\mathbb{Z}$ is a PID and that an ideal I is primary implies $\sqrt{I}$ is prime. Consider for example (p^n) for $n > 0$, then there exist zero divisors (as a $\mathbb{Z}$-module) $p, p^2, ..., p^{n-1} \in \mathbb{Z}$ of $\mathbb{Z}/p^n$ and all of these are such that $p^j \in \sqrt{\mathrm{ann}_{\mathbb{Z}}(\mathbb{Z}/p^n)} = (p)$.

Definition 2.3.11. A submodule $N \subseteq M$ of an R-module M is **primary** if it satisfies the following condition:

if $a \in R$ is a zero-divisor of M/N then $a \in \sqrt{\mathrm{ann}_R(M/N)}$.

Fact 2.3.12. *If M is a primary submodule then $\mathrm{ann}_R(M/N)$ is primary.*

Proof. Let $ab \in \mathrm{ann}_R(M/N)$ and say $a \notin \mathrm{ann}_R(M/N)$. Then $ab(M/N) = 0$ but $a(M/N) \neq 0$. This implies $b(ax) = 0$ for some $x \in M/N$ which is to say that b is a zero-divisor of M/N. Since N is primary, this implies $b \in \sqrt{\mathrm{ann}_R(M/N)}$. □

Definition 2.3.13. Let M be an R-module, then the set of **associated primes** is

$$\mathrm{Ass}_R M := \{\mathfrak{p} \mid \exists x \in M, \mathrm{ann}_R(x) = \mathfrak{p}\}$$

We say that $\mathfrak{p} = \mathrm{ann}_R M$ is **associated**.

How do we think about associated primes? They have surprisingly useful properties which we go through now.

Lemma 2.3.14. *If R is Noetherian and M a non-zero R-module, then*

1. $\mathrm{Ass}_R M \neq \varnothing$,

2. the set of zero divisors of M is the union of all associated primes of M.

Proof. (1): as R is Noetherian the set $\{\mathrm{ann}_R(x) \mid x \in M\}$ contains a maximal element.
(2) Any zero divisor a is contained in $\mathrm{ann}_R(x)$ for some x and so by the first part is contained in some associated prime. □

The next Theorem shows how associated primes interact with localisation:

Theorem 2.3.15. *Let S be a multiplicative subset of R and consider* $\operatorname{Spec} A_S$ *as a subset of* $\operatorname{Spec} A$*,*

1. Let M an R_S-module (and hence also an A-module). Then $\operatorname{Ass}_R M = \operatorname{Ass}_{R_S} M$*.*

2. Let M be an R-module, if R is Noetherian then $\operatorname{Ass}_R M \cap \operatorname{Spec} R_S = \operatorname{Ass}_{R_S} M_S$*.*

Proof. (1) We already know there is a bijection between primes of R_S and primes of R disjoint from S given by $\mathfrak{p} \mapsto \mathfrak{p} \cap R$. In fact, any associated prime $\mathfrak{p}$ of R must be disjoint from S as elements of S act invertably on M, thus it remains to show that associated primes are mapped to associated primes under this bijection. We have

$$\begin{aligned} a(x/1) = 0 &\Leftrightarrow \exists s \in S, sax = 0 \\ &\Leftrightarrow ax = 0 \end{aligned}$$

because M is an R_S module and thus elements of S act invertibly on M. Thus $\mathrm{ann}_{R_S}(x) \cap R = \mathrm{ann}_R(x)$, for any $x \in M$.

(2) Let $\mathfrak{p} = \mathrm{ann}_R(x) \in \operatorname{Ass}_R M \cap \operatorname{Spec} R_S$ and consider the prime ideal $\mathfrak{p}R_S$, we claim this is equal to $\mathrm{ann}_{R_S}(x/1)$. Say $(a/s)(x/1) = 0$, then there exists $t \in S$ such that $tax = 0$, but $t \notin \mathrm{ann}_R(x)$ (as $\mathfrak{p} \cap S = \varnothing$) and so $ax = 0$, which is to say $a \in \mathfrak{p}$ and so $a/1$ and thus $a/s \in \mathfrak{p}R_S$. Also, if $a/1 \in \mathfrak{p}R_S$ then $ax = 0$ and thus $(a/1)(x/1) = 0$. Notice that we did not use the assumption that R is Noetherian here.

Conversely, let $\mathfrak{p} = \mathrm{ann}_{R_S}(x/s) \in \operatorname{Ass}_{R_S} M_S$ and consider the prime $P := \mathfrak{p} \cap R$. Let $a_1, ..., a_n$ generate P. The image of these under the localisation map $P \longrightarrow \mathfrak{p}$ are such that $(a_i/1)(x/s) = 0$, so there exists $t_i \in S$ such that $t_i a_i x = 0$. We claim $P = \mathrm{ann}_R(t_1 ... t_n x)$. If $y \in P$ then $y = \sum_{i=1}^n \alpha_i a_i$ which annihilates $t_1 ... t_n x$, and if $y \in \mathrm{ann}_R(t_1, ..., t_n x)$ then $yx/1 = 0$ in R_S so $y/1 \in \mathfrak{p}$ which implies $y \in P$. □

Corollary 2.3.16. *For a Noetherian ring R and R-module M we have*

$$\mathfrak{p} \in \operatorname{Ass}_R M \Longleftrightarrow \mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}_{R_{\mathfrak{p}}} M_{\mathfrak{p}}$$

Proof. This follows from (2) and the simple observation $\mathfrak{p} \in \operatorname{Spec} R_{\mathfrak{p}}$. □

Theorem 2.3.17. *Let R be a ring and let the following be a short exact sequence of M modules:*

$$0 \longrightarrow M' \xrightarrow{\varphi} M \xrightarrow{\psi} M'' \longrightarrow 0$$

then $\operatorname{Ass}_R M \subseteq \operatorname{Ass}_R M' \cup \operatorname{Ass}_R M''$*.*

Proof. Let $\mathfrak{p} = \mathrm{ann}_R x \in \operatorname{Ass}_R M$, the map $R \longrightarrow M$ given by $a \mapsto ax$ gives rise to a submodule N of M which is isomorphic to $R/\mathfrak{p}$. If $y \neq 0 \in N$ then $\mathrm{ann}_A(y) = \mathfrak{p}$ as $\mathfrak{p}$ is prime. Thus if $N \cap M' \neq \varnothing$ we have that $\mathfrak{p} \in \operatorname{Ass}_R M'$. On the other hand, if $N \cap M' = \varnothing$ then the image of N under ψ is also isomorphic to $A/\mathfrak{p}$ and so $\psi(N) = \mathrm{ann}_A(y)$ for any $y \in \psi(N)$. □

Theorem 2.3.18. *Let R be Noetherian and M a finitely generated R-module. Then there exists a sequence of submodules*

$$0 = M_0 \subseteq ... \subseteq M_n = M$$

along with a sequence of prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_n$ of R such that for $i > 0$, $M_i/M_{i-1} \cong A/\mathfrak{p}_i$.

Proof. Choose any $\mathfrak{p}_1 \in \operatorname{Ass}_R M$ which gives rise to a submodule M_1 of M which is isomorphic to $A/\mathfrak{p}_1$. Then either $M_1 = M$ or not. If not, then consider M/M_1 and perform the same process to obtain a submodule $M_2' \subseteq M/M_1$, then set M_2 to be the preimage of M_2' under $M \longrightarrow M/M_1$. M is Noetherian by Lemma 2.2.1 so this process eventually terminates. □

Remark 2.3.19. The statement of Theorem 2.3.18 provides a statement of some structure of finitely generated modules over a Noetherian ring and is *completely free of any mention of associated primes.* However, the existence of a submodule isomorphic to an integral domain is crucially used in the proof presented here, so this gives a good justification for the existence of associated primes.

Definition 2.3.20. The **support** of an R-module M is $\operatorname{Supp} M := \{\mathfrak{p} \subseteq R \mid M_\mathfrak{p} \neq 0\}$.

Theorem 2.3.21. *Let R be Noetherian and M a finitely generated R-module. Then*

1. *$\operatorname{Ass}_R M$ is a finite set,*
2. *$\operatorname{Ass}_R M \subseteq \operatorname{Supp} M$,*
3. *The minimal elements of $\operatorname{Ass}_R M$ and $\operatorname{Supp} M$ coincide.*

Proof. (1) Follows from Theorems 2.3.17 and 2.3.18.
(2) By Corollary 2.3.16 we have $\mathfrak{p} \in \operatorname{Ass}_R M \Rightarrow \mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}$ which in particular means $\mathfrak{p}R_\mathfrak{p}$ is prime and thus not equal to $R_\mathfrak{p}$ so $M_\mathfrak{p} \neq 0$.
(3) By (2) it suffices to show that minimal elements of $\operatorname{Supp} M$ are associated. Let $\mathfrak{p}$ be such. Then $M_\mathfrak{p} \neq 0$ which means there exists an associated prime in $\operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}$. Thus there is an element of $\operatorname{Ass}_R M \cap \operatorname{Spec} R_\mathfrak{p}$ by Corollary 2.3.16. We use that $M_\mathfrak{p}$ is non-zero, (2), and (2) of Theorem 2.3.15 to obtain:

$$\varnothing \neq \operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p} = \operatorname{Ass}_R M \cap \operatorname{Spec} R_\mathfrak{p} \subseteq \operatorname{Supp} M \cap \operatorname{Spec} R_\mathfrak{p} = \{\mathfrak{p}\}$$

which shows $\mathfrak{p} \subseteq \operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}$. □

We will make use of the following:

Lemma 2.3.22. *Let I, J be ideals of a ring R and $\mathfrak{p}$ a prime ideal. Then $IJ \subseteq \mathfrak{p}$ implies $I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$.*

Proof. The proof reduces to showing if R is an integral domain and $IJ = 0$ then either $I = 0$ or $J = 0$. If neither I nor J were zero then there exists $i \neq 0 \in I$ and $j \neq 0 \in J$ such that $ij \neq 0 \in IJ$. □

The following provides another way of thinking about support of a finitely generated module over a neotherian ring:

Lemma 2.3.23. *If M is a finitely generated R-module then*

$$\operatorname{Supp} M = V(\operatorname{ann}_R(M))$$

where $V(\operatorname{ann}_R(M))$ is the vanishing set (Definition 2.3.5).

Proof. Let $x_1, ..., x_n$ be a set of generators for M. We have

$$\begin{aligned} M_\mathfrak{p} \neq 0 &\iff \exists i,\ x_i/1 \neq 0 \\ &\iff \exists i,\ \operatorname{ann}_R(x_i) \subseteq \mathfrak{p} \\ &\iff \operatorname{ann}_R(M) = \bigcap_{i=1}^{n} \operatorname{ann}_R(x_i) \subseteq \mathfrak{p} \end{aligned}$$

The ($\Longleftarrow$) direction of the final implication uses that M is finitely generated. Indeed,

$$\prod_{i=1}^{n} \operatorname{ann}_R(x_i) \subseteq \bigcap_{i=1}^{n} \operatorname{ann}_R(x_i) \subseteq \mathfrak{p} \Longrightarrow \exists i,\ \operatorname{ann}_R(x_i) \subseteq \mathfrak{p}$$

using Lemma 2.3.22. □

Theorem 2.3.24. *Let R be Noetherian and M a finitely generated R-module. A submodule $N \subseteq M$ is primary if and only if $\operatorname{Ass}_R(M/N)$ consists of a single element. In this case, $\sqrt{\operatorname{ann}_R(M/N)}$ is associated, and thus is the single element of $\operatorname{Ass}_R(M/N)$.*

Proof. First say $\operatorname{Ass}_R(M/N) = \{\mathfrak{p}\}$. Denote $\operatorname{ann}_R(M/N)$ by I. By (3) of Theorem 2.3.21 we have that $\operatorname{Supp}(M/N) = V(\mathfrak{p})$, which by Lemma 2.3.23 implies $V(\mathfrak{p}) = V(I)$, and thus by Corollary 2.3.6, $\mathfrak{p} = \sqrt{I}$. Using this, if $a \in R$ is a zero divisor, and so by 2 of Lemma 2.3.14, $a \in \mathfrak{p}$, then $a \in \sqrt{I}$. That is, N is primary.

Conversely, say N is primary and let $\mathfrak{p}$ be associated. For any $a \in \mathfrak{p}$ we have that a is a zero divisor, and thus $a \in \sqrt{I}$. This shows that $\mathfrak{p} \subseteq \sqrt{I}$, and by the definition of associated prime we clearly have the reverse inclusion. □

Remark 2.3.25. *Recall that an ideal I with the property that $\sqrt{I}$ is prime need not be such that I is primary (Remark 2.3.7). So we do not obtain from Theorem 2.3.24 for free that in the context given there, $\operatorname{ann}_R(M/N)$ is primary. This however is true (we continue to denote $\operatorname{ann}_R(M/N)$ by I): say $ab \in I$ and $a \notin I$, then $ab(M/N) = 0$ and $a(M/N) \neq 0$, which means b is a zero-divisor of M/N and so $b \in \sqrt{I}$ as N is primary.*

Definition 2.3.26. If M is a finitely generated R module with R Noetherian, $N \subseteq M$ is primary, and $\operatorname{Ass}_R(M) = \{\mathfrak{p}\}$ then M is **$\mathfrak{p}$-primary**.

Definition 2.3.27. Let M be an R-module, M finitely generated and R Noetherian.

- The module M is **reducible** if there exists submodules $N_1, N_2 \subseteq M$ such that $N_1 \cap N_2 = M$ with $N_1 \neq M$ and $N_2 \neq M$. If M is not reducible it is **irreducible**,
- An **irreducible decomposition** of M is a finite set of modules $N_1, ..., N_n \subseteq M$ such that $N_1 \cap \ldots \cap N_n = M$,
- A **primary decomposition** of M is a set of primary modules $N_1, ..., N_n$ such that $N_1 \cap \ldots \cap N_n = M$,
- If $N_1 \cap ... \cap N_n$ is either type of decomposition and moreover for all j satisfies: $N_1 \cap ... \cap \hat{N}_j \cap ... \cap N_n \neq M$ (where $\hat{N}_j$ means to omit N_j) then the decomposition is **irredundant**.

Lemma 2.3.28. *Let M be a finitely generated R module with R Noetherian. If $N = N_1 \cap ... \cap N_n$ is an irredundant, primary decomposition of a proper submodule $N \subseteq M$ where N_i is $\mathfrak{p}_i$-primary then $\operatorname{Ass}_R(M/N) = \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$.*

Proof of Lemma 2.3.28. By replacing M with M/N we can assume that $N = 0$. The module M is isomorphic to a submodule of $\bigoplus_{i=1}^{n} M/N_i$ and so

$$\operatorname{Ass}_R(M) = \operatorname{Ass}_R\Big(\bigoplus_{i=1}^{n} M/N_i\Big) \subseteq \bigcup_{i=1}^{n} \operatorname{Ass}_R M/N_i = \{\mathfrak{p}_1, ..., \mathfrak{p}_n\}$$

where the inclusion is by Theorem 2.3.17.

For the reverse inclusion, pick an arbitrary $\mathfrak{p}_i$, we will construct explicitly an element $y \in M$ such that $\operatorname{ann}_R(y) = \mathfrak{p}_i$. By irredundancy, $N_1 \cap ... \cap \hat{N}_i \cap ... \cap N_n \neq 0$, so choose some element $x \neq 0$ of this module. We claim there exists $\nu > 0$ such that $\mathfrak{p}_i^\nu x = 0$. We know that N_i is $\mathfrak{p}_i$ primary which means $\mathfrak{p}_i = \sqrt{\operatorname{ann}_R(M/N_i)}$. By Lemma 2.3.9 there exists $\nu > 0$ such that $\mathfrak{p}_i^\nu M \subseteq N_i$, and so $\mathfrak{p}_i^\nu x = 0$, establishing the claim.

Assume that ν is such that $\mathfrak{p}_i^{\nu-1} x \neq 0$ and pick any non-zero element of this module, we take this to be y. We have that $\mathfrak{p}_i y = 0$ and so $\mathfrak{p}_i \subseteq \operatorname{ann}_R(y)$, it remains to show this is an equality.

Since N_i is primary and $\mathfrak{p}_i = \sqrt{\operatorname{ann}_R(M/N_i)}$ it suffices to show that every element of $\mathfrak{p}_i$ is a zero-divisor of M/N_i. We know that $\mathfrak{p}_i y = 0$ so this reduces to showing $y \notin N_i$. Say $y \in N_i$. As y is a scalar multiple of x, and $x \in N_j$ for all $i \neq j$, we have $y \in N_1$ iff $y = 0$, thus $y \neq 0$. □

Fact 2.3.29. *Every finitely generated module over a Noetherian ring admits an irreducible decomposition.*

Proof. If the module is reducible, reduce it. This terminates as the module is Noetherian. □

Lemma 2.3.30. *All irreducible modules are primary.*

Proof. Let $N \subseteq M$ be a submodule which is not primary. By replacing M by M/N we can assume that $N = 0$. Moreover, assume $N_1 \cap N_2 = 0$. By Theorem 2.3.24 we have that $\operatorname{Ass}_R(M)$ has at least two elements $\mathfrak{p}_1, \mathfrak{p}_2$. Thus there are two submodules of $K_1, K_2 \subseteq M$ such that $K_i \cong A/\mathfrak{p}_i$. For any non-zero element $x \in K_i$ we have $\operatorname{ann}_R(x) = \mathfrak{p}_i$ and so $K_1 \cap K_2 = 0$, that is, 0 is reducible. □

Fact 2.3.29 and Lemma 2.3.30 together show that every module admits a primary decomposition, in fact, more can be said, see [, §2.6 Thm 6.8]

3 Polynomial rings

3.1 The quotient of a polynomial ring by a maximal ideal

Given a field F and maximal ideal $\mathfrak{m}$ of the polynomial ring $F[x_1, ..., x_n]$ we obtain a field extension $F[x_1, ..., x_n]/\mathfrak{m}$ of F. The following shows that this is always an *algebraic* extension:

Lemma 3.1.1. *Let $\mathfrak{m}$ be a maximal ideal of $F[x_1, ..., x_n]$, then $F[x_1, ..., x_n]/\mathfrak{m}$ is an algebraic extension of F.*

This Lemma is a special case of the following more general result:

Lemma 3.1.2. *Let K/F be some field extension, and say $k_1, ..., k_n \in K$ are such that $F[k_1, ..., k_n]$ is an integral domain. If $F[k_1, ..., k_n]$ is a field, then it is an algebraic extension of F.*

Notice that once this is established, Lemma 7.1.3 follows by simply making the observation that

$$F[x_1, ..., x_n]/\mathfrak{m} = F[[x_1]_\mathfrak{m}, ..., [x_n]_\mathfrak{m}]$$

We will need the following lemmas:

Lemma 3.1.3. *Let k be a field and l an algebraic extension. Then for any finite sequence of elements in l, $(l_1, ..., l_n)$:*

- *$k[l_1, ..., l_n] = k(l_1, ..., l_n)$, and*
- *there exists polynomials $f_i \in k[x_1, ..., x_i]$ for $i = 1, ..., n$ such that $\ker \varphi_n = (f_1, ..., f_n)$ where $\varphi_n : k[x_1, ..., x_n] \to k(l_1, ..., l_n)$ is the map defined by $x_i \mapsto l_i$.*

Proof. The first claim is proved by induction on n. First notice that the ideal generated by the minimal polynomial f_1 of (l_1) is contained within the kernel of the surjective map $\varphi_1 : k[x_1] \to k[l_1]$ defined by $\varphi_1(x_1) = l_1$. Moreoever, if $p \in k[x_1]$ is such that $\varphi_1(p) = 0$, ie, $p(l_1) = 0$, then we can divide by f_1 to obtain $p = f_1 q + r$. Notice that $r(l_1) = 0$. To avoid contradicting minimality of f_1, it must be that $r = 0$, that is, $p \in (f_1)$. Thus $(f_1) = \ker \varphi_1$. As f_1 is minimal, (f_1) is maximal, thus $k[x_1]/\ker \varphi_1 = k[x_1]/(f_1) \cong k[l_1]$ is a field, that is, $k[l_1] = k(l_1)$.

The inductive step is similar; first notice that $k[l_1, ..., l_r] = (k[l_1, ..., l_{r-1}])[l_r]$ which by the inductive hypothesis is equal to $k(l_1, ..., l_{r-1})[l_r]$. As proven in the base case, the map

$$k(l_1, ..., l_{r-1})[x_r] \twoheadrightarrow k(l_1, ..., l_{r-1})[l_r]$$

has kernel given by the ideal generated by the minimal polynomial $g_r \in k(l_1, ..., l_{r-1})[x_r]$ of l_r. Again, since g_r is minimal, (g_r) is maximal, thus $k(l_1, ..., l_{r-1})[l_r] = k(l_1, ..., l_{r-1})(l_r) = k(l_1, ..., l_r)$.

For the second claim, for all $r = 1, ..., n$, since $k(l_1, ..., l_{r-1}) = k[l_1, ..., l_{r-1}]$ there exists a polynomial $f_r \in k[x_1, ..., x_{r-1}]$ such that $f(l_1, ..., l_{r-1}, x_r) = g_r$. So if $p \in \ker \varphi_n$, ie, if p is such that $p(l_1, ..., l_n) = 0$, we can divide p as a polynomial in x_n by f_n to obtain $p = f_n q_n + r_n$ for some q_n and $r_n(l_1, ..., l_{n-1}, x_n)$ either equal to 0 or such that $\deg(r_n(l_1, ..., l_{n-1}, x_n)) < \deg(f_n)$. By minimality of g_n, it follows that $r_n(l_1, ..., l_{n-1}, x_n) = 0$. We can thus divide r_n by f_{n-1} to obtain $r_n = f_{n-1}q_{n-1} + r_{n-2}$. Repeating this process finitely many times yields

$$p = \sum_{i=1}^{n} \left(f_n q_n + r_{n-1} \right)$$

where $r_0 = 0$. Thus $p \in (f_1, ..., f_n)$. □

The first dotpoint of Lemma 3.1.3 can be extended to the case where infinitely many elements of l are taken, this is a useful result and so we include it here, but only the finite version will be used to prove the Nullstellensatz.

Lemma 3.1.4. *Let F/k be an algebraic extension and $L \subseteq F$ a subfield. Then $k[L] = k(L)$.*

Proof. We prove that every non-zero element x of $k[L]$ is a unit. Write $x = \alpha_1 x_1 + ... + \alpha_n x_n$ for elements $\alpha_i \in k, x_i \in L$. By the finite case we have $k(x_1, ..., x_n) = k[x_1, ..., x_n] \subseteq k[L]$. □

Proof of Lemma 3.1.2. We will prove the contrapositive. It can be assumed that $k_1, ..., k_n$ are ordered such that $k_1, ..., k_r$ form a transcendence basis of $F(k_1, ..., k_n)$ so that $F(k_1, ..., k_n)$ is an algebraic extension of $F(k_1, ..., k_r)$. By Lemma 3.1.3 there exists $f_{r+i} \in F(k_1, ..., k_r)[x_{r+1}, ..., x_i]$ such that the kernel of the map $F(k_1, ..., k_r)[x_{r+1}, ..., x_n] \to F(k_1, ..., k_n)$ which maps x_{r+i} to k_{r+i} is given by $(f_{r+1}, ..., f_n)$. Since the coefficients of each f_{r+i} are in $F(k_1, ..., k_r)$, by clearing denominators, there exists $g \in F[k_1, ..., k_r]$ such that for all i, $gf_{r+i} \in F[k_1, ..., k_r, x_{r+1}, ..., x_n]$. In other words, for all i,

$$f_{r+i} \in (F[k_1, ..., k_r, x_{r+1}, ..., x_n])_g$$

Now, $(F[k_1, ..., k_r])_g$ is not a field, as $F[k_1, ..., k_r]$ is isomorphic to a polynomial ring with infinitely many irreducible elements, so we can pick an irreducible element which is not in the unique factorisation of g, this element will not be a unit in $(F[k_1, ..., k_r])_g$. Thus there exists a non-trivial ideal I of $(F[k_1, ..., k_r])_g$. The module $(F[k_1, ..., k_n])_g$ is free over $(F[k_1, ..., k_r])_g$, a fact we leave as an exercise, and so $I(F[k_1, ..., k_n])_g$ is a non-trivial ideal of $(F[k_1, ..., k_n])_g$. Lastly, notice that if $F[k_1, ..., k_n]$ were a field, then so would be $(F[k_1, ..., k_n])_g$, thus $F[k_1, .., k_n]$ is not a field. □

3.2 Hilbert's Nullstellensatz

The goal of this section is to prove Hilbert's Nullstellensatz, for part 2 of Theorem 3.2.2 we will need the content of Section 3.1. Throughout, F is a field:

Definition 3.2.1. An **algebraic zero** of a subset $\Phi \subseteq F[x_1, ..., x_n]$ is a sequence $(\alpha_1, ..., \alpha_n)$ of elements in an algebraic closure $\bar{F}$ such that $f(\alpha_1, ..., \alpha_n) = 0$ for all $f \in \Phi$.

Notice that if a root exists in any algebraic closure it exists in them all, so it makes sense to talk about an algebraic zero in absence of a particular algebraic closure.

Theorem 3.2.2. *Let $\Phi \subseteq F[x_1, ..., x_n]$, and write (Φ) for the ideal generated by Φ,*

1. *if Φ admits no algebraic zeros, then $(\Phi) = F[x_1, ..., x_n]$.*
2. *let $f \in F[x_1, ..., x_n]$ be such that $f(\alpha_1, ..., \alpha_n) = 0$ for all algebraic zeros $(\alpha_1, ..., \alpha_n)$ of Φ, then there exists $r > 0$ such that $f^r \in (\Phi)$.*

First we show how 1 proves 2.

Proof of part 1 of Theorem 3.2.2. Consider the set $\Phi \cup \{1 - fy\} \subseteq F[x_1, ..., x_n, y]$. Then by the assumption of f, this set has no algebraic zeros. Thus by 1 $(\Phi \cup \{1 - fy\}) = f[x_1, ..., x_n, y]$, so there exists sets of polynomials $\{h_i\}_{i \in I} \subseteq \Phi$, $\{p_i\}_{i \in I} \subseteq F[x_1, ..., x_n, y]$ and polynomial $q \in F[x_1, ..., x_n, y]$ such that

$$1 = \sum_{i \in I} p_i(x, y) h_i(x) + q(1 - f(x)y)$$

Thus the image of both sides of the equation are equal under the map $F[x_1, ..., x_n, y] \to (F[x_1, ..., x_n])_f$ given by substituting $1/f$ for y are equal, ie,

$$1 = \sum_{i \in I} p_i(x, 1/f(x)) h_i(x) \in (F[x_1, ..., x_n])_f$$

clearing denominators then gives the result. □

Proof of part 2 of Theorem 3.2.2. Assume that $(\Phi) \neq F[x_1, ..., x_n]$ and let $\mathfrak{m}$ be a maximal ideal containing (Φ). $F[x_1, ..., x_n]/\mathfrak{m}$ over F being algebraic (7.1.3) admits an embedding θ into $\bar{F}$. For any $f \in \Phi$, $f(\alpha_1, ..., \alpha_m) = f(\theta([x_1]), ..., \theta([x_n])) \in \ker(\theta)$, and so $(\theta([x_1]), ..., \theta([x_n]))$ is an algebraic zero of Φ. □

3.3 Hilbert's Basis Theorem

Theorem 3.3.1 (Hilbert's Basis Theorem)**.** *If R is Noetherian then so is $R[x]$.*

Proof. Say $I \subseteq R[x]$ is an ideal which is not finitely generated. Let $f_0 \in I$ be of minimal degree, and $f_r \in I \setminus (f_0, ..., f_{r-1})$ be of minimal degree (note $\setminus$ here is set exclusion, not modulus). Denote by a_i the coefficient of the leading term of f_i. The sequence $(a_0) \subseteq (a_0, a_1) \subseteq (a_0, a_1, a_2) \subseteq \ldots$ eventually stabilises and so that $(a_0, ..., a_{N-1}) = (a_0, ..., a_n)$ for any $n \geq N$. Thus we can write

$$a_N = \sum_{i=0}^{N-1} u_i a_i$$

for some $u_i \in R$. Consider the following polynomial:

$$g = \sum_{i=0}^{N-1} u_i x^{\deg f_N - \deg f_i} f_i$$

which has the same leading term as f_N and is in $(f_0, ..., f_{N-1})$. f_N itself is not in $(f_0, ..., f_{N-1})$ and so neither is $g - f_N$, which has smaller degree than f_N, contradicting minimality. □

Corollary 3.3.2. *Every finitely generated algebra over a Noetherian ring is Noetherian.*

Proof. Using that quotients of Noetherian rings are Noetherian. □

3.4 Noether normalisation

There is a great note by Hochster `http://www.math.lsa.umich.edu/~hochster/615W10/supNoeth.pdf`. We extend the notion of *algebraic independence* (Definition 4.2.2) to make sense over any k-algebra (not just over a field):

Definition 3.4.1. Let A be a k-algebra. A set of elements $\{\alpha_1, ..., \alpha_n\} \subseteq A$ are **algebraically independent** if the ring morphism $k[x_1, ..., x_n] \longrightarrow A$ which maps $x_i \mapsto \alpha_i$ is injective.

Lemma 3.4.2. *Let k be a field and $A \cong k[\alpha_1, ..., \alpha_n]$ a finitely generated k-algebra. Then there exists algebraically independent elements $\{\beta_1, ..., \beta_r\} \subseteq A$ such that A is a finite $k[\beta_1, ..., \beta_r]$-module. In other words, every finitely generated k-algebra is a finite module over a polynomial ring.*

Proof. We proceed by induction on n. k is a finite k-module so the case when $n = 0$ is trivial. Say $n > 0$ and the result holds for k-algebras finitely generated by $n-1$ elements. If $n = r$ then we can take $\beta_i = \alpha_i$ and then A is finitely generated by 1 over A. So, assume there exists a non-zero polynomial $f \in k[x_1, ..., x_n]$ such that $f(\alpha_1, ..., \alpha_n) = 0$. Take N to be any integer which is greater than every exponent of every x_i in f. Consider the following set of generators of A:

$$\{\alpha_i' := \alpha_i - \alpha_n^{N^i}, \text{ for } i < n \text{ and } \alpha_n\}$$

These satisfy the polynomial $g(x_1, ..., x_n) := f(x_1 + x_1^N, x_2 + x_2^{N^2}, ..., x_{n-1} + x_{n-1}^{N^{n-1}}, x_n)$, moreover, for every monomial $x_1^{d_1} ... x_{n-1}^{d_{n-1}} x_n^{d_n}$ in f we have $(x_1 + x_n^N)^{d_1} ... (x_{n-1} + x_n^{N^{n-1}})^{d_{n-1}} x_n^{d_n}$ whose highest degree monomial is given by $x_n^{d_n + d_1 N + ... + d_{n-1} N^{n-1}}$ whose exponent, by the uniqueness of representations of integers base N, is uniquely determined by $d_1, ..., d_n$. This means that in g none of these terms cancel out, and so there exists a highest degree power of x_n in g and it is of the form cx_n^m for some $c \in k$ and integer m.

We can divide through by c to replace g with a monic polynomial h in x_n with coefficients in $k[x_1, ..., x_{n-1}]$ such that $h(\alpha_1', ..., \alpha_{n-1}', \alpha_n) = 0$. This shows that α_n is integral over $k[\alpha_1', ..., \alpha_{n-1}']$ and thus $k[\alpha_1', ..., \alpha_{n-1}', \alpha_n]$ is a finite $k[\alpha_1', ..., \alpha_{n-1}']$-module (Lemma 6.1.9). Since $k[\alpha_1', ..., \alpha_{n-1}']$ is generated by $n-1$ elements, the inductive hypothesis implies there is algebraically independent elements $\beta_1, ..., \beta_l$ of the ring $k[\alpha_1', ..., \alpha_{n-1}']$ such that $k[\alpha_1', ..., \alpha_{n-1}']$ is a finite $k[\beta_1, ..., \beta_l]$ module. The result follows by transitivity of finiteness of modules. □

If A is a k-integral domain, then $l = \text{tr. deg}_k A$. This is because $k[\beta_1, ..., \beta_l] \longrightarrow A$ is finite and thus integral, which in turn implies $k(\beta_1, ..., \beta_l) \longrightarrow \text{Frac}\, A$ is algebraic (Lemma 6.1.11). Thus $\text{tr. deg}_k A = \text{tr. deg}_k k(\beta_1, ..., \beta_l) = l$.

Example 3.4.3. Let A be the finitely generated k-algebra $k[x_1, x_2, x_3, x_4]/(x_1x_2 - x_3x_4)$ which we write as $k[\alpha_1, ..., \alpha_4]$. Then $f(X_1, X_2, X_3, X_4) := X_1X_2 - X_3X_4$ is such that $f(\alpha_1, ..., \alpha_4) = 0$, so consider the polynomial

$$f(X_1 + X_4^2, X_1 + X_4^4, X_1 + X_4^8, X_4) = (X_1 + X_3^2)(X_2 + X_4^4) - (X_3 + X_4^8)X_4 = \ldots + X_4^9$$

which is a monic polynomial such that $f(\alpha_1 - \alpha_4^2, \alpha_2 - \alpha_4^4, \alpha_3 - \alpha_4^8, \alpha_4) = 0$. This shows that α_4 is integral over $k[\alpha_1, \alpha_2, \alpha_3]$ and thus $k[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ is a finite $k[\alpha_1, \alpha_2, \alpha_3]$-module with generating set $\{1, \alpha_4, ..., \alpha_4^l\}$ for some l. Moreover, $\{\alpha_1, \alpha_2, \alpha_3\}$ is an algebraically independent set, and so A is a finitely generated $k[\alpha_1, \alpha_2, \alpha_3]$-module.

4 Fields

4.1 Algebraic closure

Every integral domain R can canonically be embedded within a field in the following way:

Definition 4.1.1. Let $\mathrm{Frac}(R)$ be the **field of fractions** of R, the construction of which mimics that of the rational numbers from the integers: The underlying set of $\mathrm{Frac}(R)$ consists of equivalence classes of pairs $(x, y) \in R \times R \setminus \{0\}$ where two pairs $(x, y), (x', y')$ are equivalent if $xy' - x'y = 0$. Addition is defined by $(x, y) + (x', y') = (xy' + x'y, yy')$ and multiplication $(x, y) \cdot (x', y') = (x \cdot x', y \cdot y')$. The canonical injection φ_R is given by $x \mapsto (x, 1)$.

This field is minimal as made precise by the following Lemma:

Lemma 4.1.2. *Say R is an ID and let $\psi : R \to F$ is a ring homomorphism where F is a field. Then there exists a unique morphism $\gamma : \mathrm{Frac}(R) \to F$ such that the following diagram commutes*

$$\begin{array}{ccc} R & \xrightarrow{\varphi_R} & \mathrm{Frac}(R) \\ & \searrow^{\psi} & \downarrow{\scriptstyle \gamma} \\ & & F \end{array}$$

Proof. The map $\gamma(x, y) = \psi(x) \cdot \psi(y)^{-1}$ is the unique map. □

If a field F is such that for every polynomial $p \in F[x]$ there exists $f \in F$ which is a root of p, then F is said to be **algebraically closed**.

Lemma 4.1.3. *Every field F can be embedded into an algebraically closed field $\bar{F}$.*

Proof. Let Λ be the collection of monic, irreducible polynomials with coefficients in F. For each $f \in F$, let $u_{f,0}, ..., u_{f,d}$ be formal indeterminants, where d is the degree of f. Let $F[\{U\}]$ be the polynomial ring over F where U is the collection of all $u_{f,i}$. Write

$$f - \prod_{i=0}^{d}(x - u_{f,i}) = \sum_{i=0}^{d-1} \alpha_{f,i} x^i \in F[\{U\}][x]$$

Let I be the ideal generated by $\alpha_{f,i}$. I is not all of $F[\{U\}]$ so there exists a maximal ideal M containing I. Let $F_1 = F[\{U\}]/M$. Repeat this process to define f_i for all $i > 0$. Then $\cup_{i=1}^{\infty} F_i$ is algebraically closed which F embeds into, and moreover is an algebraic extension of F. □

This constructed field will be denoted $\bar{F}$ and it along with the embedding $F \rightarrowtail \bar{F}$ is called the **algebraic closure** of F and is denoted $\bar{F}$. It is essentially unique in a way made precise by the following Lemma:

Lemma 4.1.4. *Let F be a field and $\varphi : F \to L$ a ring homomorphism such that L is algebraic over F. Then if L is algebraically closed, $L \cong \bar{F}$.*

Proof. The collection of pairs (K, σ) where K is an algebraic extension of F and $\sigma : K \to L$ is a ring homomorphism, with partial order $(K, \sigma) < (K', \sigma')$ defined by $K \rightarrowtail K'$ and $\sigma' \restriction_K = \sigma$ defines a non-empty poset closed under ascending chains. By zorn's Lemma, there thus exists a maximal element which can be shown to be $\bar{F}$. Since L is algebraic over F it then follows that $\sigma : K \to L$ is surjective, thus this is an isomorphism. □

Notation 4.1.5. Given a field extension K/F, and elements $k_1, ..., k_n \in K$ we denote

- the smallest subring of K containing F and $k_1, ..., k_n$ by $F[k_1, ..., k_n]$,
- the smallest subfield of K containing F and $k_1, ..., k_n$ by $F(k_1, ..., k_n)$.

Notice that $F(k_1, ..., k_n) \cong \text{Frac}(F[k_1, ..., k_n])$. So we can define these notions without the presence of a field extension:

Notation 4.1.6. Given a field k we denote

- $k[x_1, ..., x_n]/I$ by $k[\alpha_1, ..., \alpha_n]$,
- $\text{Frac}\left(k[x_1, ..., x_n]/I\right) = \text{Frac}\, k[\alpha_1, ..., \alpha_n]$ by $k(\alpha_1, ..., \alpha_n)$.

4.2 Transcendence degree

Throughout, let K/F be a field extension.

Definition 4.2.1. An element f of a field F is **transcendental** if whenever $p \in F[x]$ admits f as a root, p is the zero polynomial.

Similarly, there are *algebraically independent sets*:

Definition 4.2.2. A subset $S \subseteq F$ is **algebraically independent** if the map

$$K[x_s \mid s \in S] \to F$$

which maps $x_s \mapsto s$ is injective.

Definition 4.2.3. An algebraically independent subset S of F is a **transcendence basis** of K/F if F is an algebraic extension of $K(S)$.

Lemma 4.2.4. *A transcendence basis always exists, and the cardinality of any two such bases are always equal.*

Proof. That a transcendence basis always exists can be shown using a similar method to how a basis for a vector space always exists; apply Zorn's Lemma to the poset of algebraically independent sets S of K to yield a maximal element B (note: if this poset is empty, then the empty set can be taken as a basis for K/F). It can then be shown that K is an algebraic extension of $F(B)$ [2, §9.26].

Next we prove the following statement by induction on n: if E/J is any field extension, and $B = \{b_1, ..., b_n\}, B' = \{b'_1, ..., b'_m\}$ for some $m \leq n$ are bases for E/J then $m = n$. This establishes the case of the claim when the cardinality of the two bases are finite.

If $n = 0$ then E/J is an algebraic extension, which means $n = m = 0$.

Now say $n > 0$. Since B' is a basis, there exists a polynomial $f \in J[x, y_1, ..., y_m]$ such that $f(b_1, b'_1, ..., b'_m) = 0$. This polynomial f must involve x and some y_i, lest either B' not be a basis, or b_1 be algebraic over J. Without loss of generality, assume $i = 1$.

Let $B^* = \{b_1, b'_2, ..., b'_m\}$. Our next claim is that B^* is algebraically independent over J. Indeed, if $g \in J[x_1, ..., x_m]$ were such that $g(b_1, b'_2, ..., b'_m) = 0$, where g necessarily involves x_1, then b_1 is algebraic over $J(b'_2, ..., b'_m)$. This in turn implies b'_1 is algebraic over $J(b'_2, ..., b'_m)$, due to the existence of f.

Thus $\{b_2, ..., b_n\}$ and $\{b'_2, ..., b'_m\}$ are bases for $E/J(b_1)$, which by the inductive hypothesis implies $n = m$.

Now say B, B' are such that $|B'| \leq |B|$ and $|B|$ is infinite, it will be shown throughout the course of this part of the argument that it is necessarily the case that $|B'|$ is also infinite, so this is the last case to consider.

For each $b \in B'$ choose a polynomial $p[x_1, ..., x_n]$ and elements $b_2, ..., b_n$ of B such that $p(b, b_2, ..., b_n) = 0$. Let B^* be the set containing all such b_i for all such p. Then $B^* \subseteq B$ and we claim moreover that $B^* = B$. To see this, say $\beta \in B \setminus B^*$. Then β is algebraic over $F(B')$ and so is algebraic over $F(B^*)$, a contradiction. Thus $|B| = |B^*|$ which since $|B|$ is infinite implies that $|B'|$ is infinite. It now follows from $|B'|$ being infinite that $|B^*| = |B'|$. □

Lemma 4.2.5. *Any generating set contains a transcendence basis.*

Proof. Similar to the corresponding statement about bases of vector spaces (we are working with fields here). □

4.3 Perfect fields and separable elements

Throughout, k is a completely arbitrary field, possibly not algebraically closed, possibly of positive characteristic. Say k has characteristic p, denote by k^p the image of the **Frobenius Endomorphism** on k which maps $x \mapsto x^p$. This is indeed a homomorphism, with additivity following from the important relation $(x + y)^p = x^p + y^p$. Since k is a field we have that $x^p = 0$ implies $x = 0$ so indeed this map is injective. Of particular interest is the case when this endomorphism is also surjective:

Definition 4.3.1. A field is **perfect** if the characteristic is 0, or it is not 0 and the Frobenius Endomorphism is an isomorphism.

Example 4.3.2. Examples and a non-example of perfection:

- If k is finite then the Frobenius Endomorphism is an injective map between two sets with equal cardinality, and thus is an isomorphism. So every finite field is perfect.
- If k is algebraically closed then it is perfect.
- Let $\mathbb{F}_p$ be the finite field of characteristic $p > 0$. The field $\mathbb{F}_p(t)$ is not perfect, see Example 4.3.9.

Lemma 4.3.3. *Let A be a UFD. If $f \in A$ is an irreducible polynomial of positive degree then its image in* Frac A *is also irreducible.*

Proof. Write $f = f_1 f_2$ for polynomials $f_1, f_2 \in \operatorname{Frac} A$, we can write $f_i = \frac{f'_i}{a_i}$ with $a_i \in A$. We now have that f divides $f'_1 f'_2$ and since f is irreducible and A is a UFD we thus have f is prime and so f divides either f'_1 or f'_2, say f divides f'_1. This implies $\deg f \leq \deg f'_1$. As A is an integral domain we also have $\deg f'_1 + \deg f'_2 = \deg f$. It follows that $\deg f'_2 = 0$ and so f_2 is a unit. Since $\deg f > 0$ it follows that f_1 is not a unit, thus f is irreducible in Frac A. □

Definition 4.3.4. An element a of a field k **admits an l^{th} root** if there exists $b \in k$ such that $b^l = a$.

An alternative condition for a field being perfect will involve its *formal derivative*:

Definition 4.3.5. The **formal derivative** (often abbreviated to **derivative**) of a polynomial $f = \sum_{i=0}^{n} a_i x^i \in k[x]$ is $f' := \sum_{i=1}^{n-1} i a_i x^{i-1}$.

Lemma 4.3.6. *Let k be a field of characteristic p and let $a \in k$ be an element which does not admit a p^{th} root. For any $e \geq 0$, the polynomial $x^{p^e} - a$ is irreducible in $k[x]$.*

Proof. We proceed by induction on e, the result holds trivially if $e = 0$. Assume $e > 0$ and the result holds for $e - 1$. Let $f \in k[x]$ be a monic, irreducible polynomial which divides $x^{p^e} - a$. Let $d \geq 0$ be the greatest integer such that f^d divides $x^{p^e} - a$ and let $g \in k[x]$ be such that

$$f^h g = x^{p^e} - a \tag{19}$$

Taking derivatives of both sides and dividing by f^{d-1} we obtain:

$$0 = df'g + fg' \tag{20}$$

This equation implies g divides fg'. Since $\gcd(f, g) = 1$ it follows that g divides g', which means $g' = 0$. Thus $g \in k[x^p]$. Moreover, (20) now reads $0 = df'g$ which implies $df' = 0$, that is, $f^d \in k[x^p]$. Equation (19) now can be written as $f_1(x)g_1(x) = x^{p^{e-1}} - a$ where $f_1(x^p) = f(x)^d$ and $g_1(x^p) = g(x)$. By the inductive hypothesis, this is irreducible, and so g_1 is a uni. In fact, $g_1 = 1$ as both $x^{p^{e-1}} - a$ and f_1 are monic. We now have

$$f_1(x) = x^{p^{e-1}} - a, \qquad f(x)^d = x^{p^e} - a$$

We finish the proof by proving $d = 1$, first we show p does not divide d. Say it did, then $f(x)^d$ would be a power of $f(x)^p$ which would imply all the coefficients of $f(x)^d$ have a d^{th} root, which would mean all the coefficients of $x^{p^e} - a$ would have a d^{th} root (as such elements form a subring), but this contradicts the assumption that a does not have a p^{th} root. Since p does not divide d, the equation $df' = 0$ implies $f' = 0$ which means $f \in k[x^p]$, so we can write $f(x^p) - f_2(x)$. Thus the equation $f_1(x^p) = f(x)^d$ implies $f_1(x) = f_2^d$ and so to avoid contradicting irreducibility of $x^{p^{e-1}} - a$ we must have that $d = 1$. □

Definition 4.3.7. An irreducible polynomial $f \in k[x]$ is **separable** if $f' \neq 0$ and **inseperable** if $f' = 0$. An arbitrary polynomial $f \in k[x]$ of positive degree is is **separable** if its irreducible components are. Otherwise it is **inseparable**.

We now give an alternate characterisation of a field being *perfect*:

Lemma 4.3.8. *A field k is perfect if and only if every irreducible polynomial $f \in k[x]$ is separable.*

Proof. Assume k is perfect. Let f be an arbitrary polynomial with zero derivative. Then $f \in k[x^p]$ so we can write $f = \sum_{i=0}^{n} \alpha_i x^i$ where $\alpha_i \in k$. Since k is perfect there exists α_i' such that $(\alpha_i')^n = \alpha_i$. Thus we have $\sum_{i=0}^{n} \alpha_i x^i = \left(\sum_{i=0}^{n} \alpha_i' x\right)^n$. That is, f is reducible.

Conversely, say k is imperfect and let $a \in k$ admit no n^{th} root for some $n > 1$. Consider the polynomial $x^p - a$, this has zero-derivative so it remains to show that this is irreducible. This follows from Lemma 4.3.6. □

Example 4.3.9. The field $\mathbb{F}_p(t)$ is imperfect. It admits at least one irreducible, separable polynomial.

Definition 4.3.10. Given a field extension K/k, an element $a \in K$ which is algebraic over k is **separable over** k if its minimal polynomial is. Otherwise it is **inseparable**.

The following gives a reduction to the problem of separability of an element.

Lemma 4.3.11. *An element $a \in F$ of a field extension F/k is separable if and only if $f'(a) \neq 0$ where f is the minimal polynomial of a.*

Proof. We should that a is *inseparable* if and only if $f'(a) = 0$. If $f'(a) = 0$ then by minimality of f we have that $f' = 0$. Conversely $f' = 0$ implies $f'(a) = 0$. □

The following lemma show that the derivative of a polynomial which vanishes at a separable element also vanishes at that separable element, thus extending Lemma 4.3.11:

Lemma 4.3.12. *Let $a \in k$ be an inseparable element of a field extension F/k and let $g \in k[x]$ be a polynomial such that $g(a) = 0$, then $g'(a) = 0$.*

Proof. Let $f \in k[x]$ be the minimal polynomial of a. That $g(a) = 0$ implies f divides g and so $fh = g$ for some h, taking derivatives gives the result. □

5 Field extensions

Extensions of algebraic objects can be studied at various levels of generality, we may have an extension of *groups*, or an extension of *rings*, etc. A bottom up approach would be to consider extensions of decreasingly "bare" algebraic objects, perhaps starting at group extensions. However, the nature of the theory changes. For example, when considering an extension of fields K/k in the special situation where K is a finite dimensional vector space over k, one may ask "what does the dimension of this vector space mean for the extension"? This is a question which in the more general setting of an extension of rings A/B where A is a finitely generated B-module cannot be asked.

We thus consider the theory of field extensions in this Section, and the theory of extensions of rings (*integral extensions*) separately in Section 6.

Definition 5.0.1. Given a field extension K/k, an element $\alpha \in K$ is:

- **algebraic** if there exists a polynomial $f \in k[x]$ such that $f(\alpha) = 0$. Since $k[x]$ is a UFD for any algebraic α there exists a unique, monic, irreducible polynomial $\hat{f} \in k[x]$ such that $\hat{f}(\alpha) = 0$ which we call the **minimal polynomial of** α,
- **purely inseparable over** k in the case where k has characteristic $p \neq 0$ and there exists $e \geq 0$ such that $\alpha^{p^e} \in k$,

Recall also Definition 4.3.10 that given a field extension K/k and an element $\alpha \in K$ is *separable* if its minimal polynomial admits a nonzero formal derivative.

Definition 5.0.2. A field extension K/k is:

- **algebraic** if every element of K is,
- **finitely generated** if there exists $\alpha_1, ..., \alpha_n \in K$ such that $K = k(\alpha_1, ..., \alpha_n)$,
- **finite** if the dimension of K as a k-vector space is finite,
- **separable** if every element of K is, otherwise the extension is **inseparable**,
- **purely inseparable** if every element of K is,
- **separably generated** if K/k is finitely generated, and there exists a transcendence basis $\{\alpha_1, ..., \alpha_m\} \subseteq K$ such that $K/k(\alpha_1, ..., \alpha_m)$ is a separable. Such a set of elements $\{\alpha_1, ..., \alpha_m\}$ is a **separating transcendence basis**.

Proposition 5.0.3. *Let K/k be a field extension, then:*

- *if K/k is finite then it is algebraic,*
- *if K/k is finitely generated and algebraic, then it is finite,*

Proof. The respective arguments are:

- if K/k is a finite field extension and say the dimension of K as a k-vector space is d, then for any $\alpha \in K$, the set $\{1, \alpha, \ldots, \alpha^d\}$ is linearly dependent, and so α is algebraic.
- if $\alpha \in K$ is such that $K = k(\alpha)$ and moreover, α is algebraic over k, then the extension K/k is finite, this is because there exists a polynomial $p(x) \in k[x]$ such that $p(\alpha) = 0$, which implies α^r for some r can be written as a linear combination of $1, ..., \alpha^{r-1}$. Continuing inductively, the result follows.

□

5.1 Separable extensions

We want to introduce the terminology of a root's *multiplicity* but we need to show this is well defined:

Lemma 5.1.1. *Let F_1/k and F_2/k be two field extensions and $a \in k$ a root of a polynomial $g \in k[x]$. Write $g(x) = (x-a)^{r_1} f_1(x)$ and $g(x) = (x-a)^{r_2} f_2(x)$ where $f_i \in F_i[x]$ and $f_i(a) \neq 0$. Then $r_1 = r_2$. This integer is the **multiplicity** of the root a.*

Proof. Assume without loss of generality that $r_1 \geq r_2$. Let $\bar{k}$ be an algebraically closed field and consider F_1 and F_2 as subfields of $\bar{k}$. Then inside $\bar{k}[x]$ we have $f_2(x) = (x-a)^{r_1 - r_2} f_1(x)$, but $f_2(a) \neq 0$ and so $r_1 = r_2$. □

Lemma 5.1.2. *If K/F is a separable extension and L is any field such that $F \subseteq L \subseteq K$ then K/L is a separable extension.*

Proof. Let $a \in K$ be separable over F. The minimal polynomial $f \in F[x]$ of a admits a as a *simple root* (a root of multiplicity 1). The image of f in $L[x]$ must also have a as a simple root otherwise f in $K[x]$ would have a multiple root, which by Lemma 4.3.11 would contradict a being separable (over F). Thus by Lemma 4.3.12 we have the result. □

From here on, assume k has characteristic $p \neq 0$.

Lemma 5.1.3. *If an element $\alpha \in F$ is separable over k and is purely inseparable, then $\alpha \in k$.*

Proof. Let e be the least integer such that $\alpha^{p^e} \in k$. Suppose for a contradiction that $e \neq 0$, then α^{p^e} does not have a root in k and so the polynomial $p(x) := x^{p^e} - \alpha^{p^e}$ is irreducible (Lemma 4.3.6). This is also monic, and thus is the irreducible polynomial of α. By separability, $p' \neq 0$, but this is a contradiction, so $e = 0$. □

Definition 5.1.4. Given a polynomial $f \in k[x]$, the greatest integer e such that $f \in k[x^{p^e}]$ is the **reduced degree** of f.

Recall the notation k^p for the subfield of k given by p^{th} powers of elements of k.

Lemma 5.1.5. *Say F/k is a separable extension, then $k = k[F^p]$. Conversely, if $k = k[F^p]$ and F/k is finite, then F/k is separable.*

Proof. By Lemma 3.1.4 we have that $k[F^p]$ is a field. We have $k \subseteq k[F^p] \subseteq F$ so since F/k is separable, by Lemma 5.1.2 we have $F/k[F^p]$ is separable. Moreover, since $F \subseteq k[F^p]$ we have that every element of F is purely inseparable over $k[F^p]$. By Lemma 5.1.3 we have $F = k[F^p]$.

For the converse, we first prove the following claim: let $\alpha_1, ..., \alpha_n$ be a linearly independent set of F as a k-vector space, then $\alpha_1^p, ..., \alpha_n^p$ is also linearly independent. We know the Frobenius endomorphism

is an isomorphism onto its image, so $\alpha_1^p, ..., \alpha_n^p$ form a linearly independent set in F^p as a k-vector space. By assumption though, $k[F^p] = F$ and so this set is linearly independent in F.

Let $a \in F$ be an element not in k and let $f \in k[x]$ be the minimal polynomial of a, say $\deg f = n$. Say a is inseparable and let $e < n$ be the reduced degree of f. To avoid contradicting minimality of n we must have $1, a, a^2, ..., a^e$ is linearly independent, but $1, a^{p^e}, a^{2p^e}, ..., a^{ep^e}$ we claim is linearly independent. Since $f \in k[x^{p^e}]$ we can write $f(x) = f_1(x^{p^e})$ where $f_1 \in k[x^{p^e}]$. We have $0 = f(a) = f_1(a^{p^e})$. □

Corollary 5.1.6. *If x is separable over k then $k(x) = k(x^p)$. Conversely if $k(x) = k(x^p)$ then x is separable over k.*

Lemma 5.1.7. *If $\alpha_1, ..., \alpha_n \in F$ are separable over k then $F/k(\alpha_1, ..., \alpha_n)$ is separable.*

Proof. By induction, apply Corollary 5.1.6. □

Lemma 5.1.8. *If $k \subseteq L \subseteq K$ are fields with L/K separable and K/L separable then K/k is separable.*

Proof. See [5, II §5, 9]. □

5.2 Theorem of a Primitive element

In this Section, k is an arbitrary field of infinite cardinality (not necessarily algebraically closed).

Lemma 5.2.1. *If $p \in k[x]$ is irreducible, then $p \in (k[x])(\{x_i\}_{i\in I})$ is irreducible for any collection of indeterminants $\{x_i\}_{i\in I}$.*

Proof. Write

$$p(x) = p_1(x, x_{i_1}, ..., x_{i_{n_1}})p_2(x, x_{j_1}, ..., x_{j_{n_2}}) \in (k[x])[\{x_i\}_{i\in I}] \tag{21}$$

for some elements $i_1, ..., i_{n_1}, j_1, ..., j_{n_2} \in I$. Then (21) still holds if we set $x_{i_k} = x_{j_l} = 0$ for all $k = i_1, ..., i_{n_1}, l = j_1, ..., j_{n_2}$. We obtain $p(x) = p_1(x, 0, ..., 0)p_2(x, 0, ..., 0)$ which we consider as an equation in the ring $k[x]$, by irreducibility of p we have $\deg p(x) = \deg p_1(x)$, say. Thus $\deg p_1 \geq \deg p$ and so p_2 has degree 0 in x. Hence, p_1 considered as an element of $(k[x])(\{x_i\}_{i\in I})$ is a unit. □

Notation 5.2.2. Given a polynomial $f \in k[x_1, ..., x_n]$ we denote $(\partial/\partial x_i)f$ by f_x.

Theorem 5.2.3 (Theorem of a primitive element)**.** *Let F/k be a finite, separable extension. Then there exists $\alpha \in F$ such that $F = k(\alpha)$.*

If $\alpha_1, ..., \alpha_n \in F$ are such that $F = k(\alpha_1, ..., \alpha_n)$ (which exists as F/k is finite, hence finitely generated) then α can be taken to be a linear combination of $\alpha_1, ..., \alpha_n$ which coefficients in k.

Proof. Since F/k is finite, there exists $\alpha_1, ..., \alpha_n \in F$ such that $F = k(\alpha_1, ..., \alpha_n)$. We let $k^* := k(x_1, ..., x_n)$ and $F^* := F(x_1, ..., x_n)$. Notice that $F^* = k^*(\alpha_1, ..., \alpha_n)$ and since α_i is separable over k we have that α_i, when considered in F^*, is separable over k^* for all i, by Lemma 5.2.1. It then follows from Lemma 5.1.7 that F^* is a finite, separable extension of k^*. Consider the element $\beta(x_1, ..., x_n) := \alpha_1 x_1 + ... + \alpha_n x_n$ of F^* and let f be the minimal polynomial of $\beta(x_1, ..., x_n)$ in $k^*[x]$. By clearing denominators, there exists $h \in k[x_1, ..., x_n], g \in k[x, x_1, ..., x_n]$ such that

$$h(x_1, ..., x_n)f(x, x_1, ..., x_n) = g(x, x_1, ..., x_n) \in k[x, x_1, ..., x_n] \tag{22}$$

subject to

$$g(\beta(x_1, ..., x_n), x_1, ..., x_n) = 0 \tag{23}$$

By (22) we have

$$g_x(x, x_1, ..., x_n) = h(x_1, ..., x_n)f_x(x, x_1, ..., x_n) \tag{24}$$

and since $\beta(x_1, ..., x_n)$ is separable over k^* we have

$$g_x(\beta(x_1, ..., x_n), x_1, ..., x_n) = h(x_1, ..., x_n) f_x(\beta(x_1, ..., x_n), x_1, ..., x_n) \neq 0 \tag{25}$$

Since k is infinite we can find elements $c_1, ..., c_n \in k$ such that $g_x(\beta(c_1, ..., c_n), c_1, ..., c_n) \neq 0$.

On the other hand, by (23) and the chain rule we have

$$g_{x_i} = \alpha_i g_x(\beta(x_1, ..., x_n), x_1, ..., x_n) + g_{x_i}(\beta(x_1, ..., x_n), x_1, ..., x_n) = 0 \tag{26}$$

So, setting $\alpha = \alpha_1 c_1 + ... + \alpha_n c_n$ we have:

$$0 = \alpha_i g_x(\alpha, c_1, ..., c_n) + g_{x_i}(\alpha, c_1, ..., c_n) \tag{27}$$

which implies $\alpha_i \in k(\alpha)$, thus $k(\alpha) = F$. □

Remark 5.2.4. In the proof of Theorem 5.2.3 we only used the fact that F/k is finitely generated and separable, however, if F/k is separable then it is in particular algebraic. Hence also being finitely generated, we have by Proposition 5.0.3 that F/k is finite. So this hypothesis is equivalent to what was taken here.

5.3 Separating transcendence bases

Remark 5.3.1. Considering the definition of *separably generated* one might think that a field extension K/k is finitely generated if there exists $\alpha_1, ..., \alpha_n \in K$ such that $K/k(\alpha_1, ..., \alpha_n)$ is a finite extension. Notice however, that $K/k(\alpha_1, ..., \alpha_n)$ being finite implies it is algebraic, and so every element $x \in K$ is a root of a monic polynomial $p(x)$ with coefficients in $k(\alpha_1, ..., \alpha_n)$, that is, there exists $\beta_1, ..., \beta_n \in k(\alpha_1, ..., \alpha_n)$ such that

$$x^n + \beta_1 x^{n-1} + \ldots + \beta_{n-1} x + \beta_n = 0$$

so since K is a field, we have

$$x = \beta_1 + (x^{-1})\beta_2 + \ldots + (x^{-1})^{n-2}\beta_{n-1} + (x^{-1})^{n-1}$$

which is to say $K = k(\alpha_1, ..., \alpha_n)$, so these definitions are equivalent.

Theorem 5.3.2. *Let K/k be an extension which is finitely generated and separably generated. Then any transcendence basis is a separating transcendence basis.*

Proof. We proceed by induction on $\text{tr. deg}_k K := r$. Say $r = 1$ and let $\{\alpha\}$ be a separating transcendence basis, in other words, $\alpha \in K$ is transcendental over k and $K/k(\alpha)$ is separable. Let $\beta \in K$ be any element transcendental over k. We need to show that $K/k(\beta)$ is separable. First, extend β to a generating set $\{\beta, \beta_1, ..., \beta_n\}$ (which is necessarily finite by hypothesis of K/k), and notice that each β_i and β are separable over $k(\alpha)$ (as $K = k(\beta, \beta_1, ..., \beta_n)$ and $K/k(\alpha)$ is separable). We have $k(\alpha) \subseteq k(\alpha, \beta) \subseteq K$ and thus (Lemma 5.1.2) $K/k(\alpha, \beta)$ is separable. By Lemma 5.1.8 it thus remains to show that $k(\alpha, \beta)/k(\beta)$ is separable, that is, α is separable over $k(\beta)$.

Since $\text{tr. deg}_k K = 1$ and both α, β are transcendental, there exists a polynomial $f(x, y) \in k[x, y]$ such that $f(\alpha, \beta) = 0$. Moreover, as $k[x, y]$ is a UFD we may assume that f is irreducible. Assume for a contradiction that α is inseparable over $k(\beta)$. Then by Lemma 4.3.12 we have $f'(x, \beta) = 0$ and thus $f(x, \beta) \in k(\beta)[x^p]$, write $f(x, \beta) = g(x^p, \beta)$. We know that β is separable over $k(\alpha)$ (as $K/k(\alpha)$ is separable) and so for any irreducible polynomial $j(y) \in k(\alpha)[y]$ we have $j'(\beta) \neq 0$. The polynomial $g(\alpha^p, y)$ is irreducible, to see this, notice α and hence α^p is transcendental over k, so $g(\alpha^p, y)$ reducible implies $g(x^p, y)$ and hence $f(x, y)$ reducible. Thus, $\frac{\partial}{\partial \beta} g(\beta, \alpha^p) \neq 0$. This implies by Lemma 4.3.12 that β is separable over $k(\alpha^p)$.

On the other hand, α is transcendental and so $\alpha \notin k(\alpha^p)$ which means $x^p - \alpha^p \in k(\alpha^p)[x]$ is the minimal polynomial of α over $k(\alpha^p)$ which shows α is inseparable over $k(\alpha^p)$. Thus $K/k(\alpha^p)$ cannot possibly be separable. and noting that $K = k(\beta, \beta_1, ..., \beta_n)$, we have that β is inseparable over $k(\alpha^p)$ (Lemma 5.1.7). Thus we have a contradiction.

For the inductive step, let $\{\alpha_1, ..., \alpha_r\}$ be a separating transcendence basis for K/k and let $\{\beta_1, ..., \beta_r\}$ be a transcendence basis. We extend $\{\beta_1, ..., \beta_r\}$ to a set of generators $\{\beta_1, ..., \beta_r, \gamma_1, ..., \gamma_l\}$ of K. Now, $\{\alpha_2, ..., \alpha_r\}$ form a separating transcendence basis for $k(\beta_1)(\beta_2, ..., \beta_r, \gamma_1, ..., \gamma_l)$ and so by the inductive hypothesis there is a subset of $\{\beta_1, ..., \beta_r\}$ consisting of $r-1$ elements which is a separating transcendence basis, say this set is $\{\beta_1, ..., \beta_{r-1}\}$. Extend $\{\alpha_1, ..., \alpha_r\}$ to a generating set $\{\alpha_1, ..., \alpha_r, \delta_{r+1}, ..., \delta_n\}$, then $K = k(\alpha_1, ..., \alpha_{r-1})(\alpha_r, \delta_{r+1}, ..., \delta_n)$ and via this decomposition we have that K is a finitely generated and separably generated by the single variable α_r. This must be separating by the inductive hypothesis again and so the result follows. □

Lemma 5.3.3. *Let K be a finitely generated k-field with $\operatorname{tr.deg}_k K = r$, and $\{\alpha_1, ..., \alpha_n\}$ a set of generators. If K/k is not separably generated then there exists $i_1, ..., i_{r+1}$ such that $k(\alpha_{i_1}, ..., \alpha_{r+1})/k$ is not separably generated.*

Proof. We proceed by induction on n, if $n = r + 1$ then there is nothing to show. Assume $n > r + 1$ and assume the result holds for the $n - 1$ case. Assume wlog that α_1 is algebraically dependent on $\alpha_2, ..., \alpha_n$. If $k(\alpha_2, ..., \alpha_n)/k$ is not separably generated then the result holds by the inductive step. Assume $k(\alpha_2, ..., \alpha_n)/k$ is separably generated. Then by Theorem 5.3.2 there exists $i_2, ..., i_{r+1}$ such that $\alpha_2, ..., \alpha_{i_{r+1}}$ is a separating transcendence basis of $k(\alpha_2, ..., \alpha_n)$. Since α_1 is algebraically dependent on $\alpha_2, ..., \alpha_n$ we have that $k(\alpha_2, ..., \alpha_n) = k(\alpha_1, ..., \alpha_n) = K$, and thus $K/k(\alpha_1, \alpha_{i_2}, ..., \alpha_{i_{r+1}})$ is separable, so since K/k is not, it follows from Lemma 5.1.2 that $k(\alpha_1, \alpha_{i_2}, ..., \alpha_{i_{r+1}})/k$ is not. □

Theorem 5.3.4. *Let k be perfect. Every algebraic extension of k is separable.*

Proof. Let $\alpha \in K$ and let $f(x) \in k[x]$ be the minimal polynomial of α. Write $f(x) = g(x^{p^d})$ for some $d \geq 0$ with g separable. Then $g(x^{p^d}) = h(x)^{p^d}$ for some h (as k is perfect). Since f is irreducible, we have that $d = 0$ so that $f(x) = g(x)$ and thus f is separable. □

Corollary 5.3.5. *If k is a perfect field then any finitely generated extension of k is separably generated.*

6 Integral extensions and jacobson rings

6.1 Cayley-Hamilton Theorem, finite modules, and integrality

Definition 6.1.1. A morphism $f : A \to B$ is a **finitely generated A-algebra** or **is of finite type** if B is an A-algebra and there exists a surjective algebra homomorphism $A[x_1, ..., x_n] \to B$. In such a setting we often denote the subring $f(A)$ by A, even though f need not be injective.

Definition 6.1.2. Let B be an A algebra. An element $b \in B$ of B is **integral over** A if there exists a monic polyonomial $f(x) \in A[x]$ such that $f(b) = 0$. The ring B is **integral over** A if every element $b \in B$ is integral over A. A homomorphism of finite type $f : A \to B$ is **integral** if B is an integral extension of A.

Theorem 6.1.3 (Cayley-Hamilton Theorem)**.** *Let M be a finitely generated A-module (note: module, not algebra) and $\varphi : M \to M$ an endomorphism. Then φ satisfies its own characteristic equation.*

Throught, we denote the $n \times n$ identity matrix by $\mathbf{1}_n$. Recall that for an $n \times n$ matrix X, the **adjugate** of X, $\operatorname{Adj} X$ is given by the trasnpose of the matrix of cofactors. The adjugate matrix has the important property that $\operatorname{Adj} X \cdot X = \det X \cdot \mathbf{1}_n$.

Proof of Theorem 6.1.3. Let $\{m_1, ..., m_n\}$ be a set of generators of M and let $\underline{m}$ denote the column vector $(m_1, ..., m_n)^T$. For each i, write $\varphi(m_i) = \sum_{j=1}^{n} a_{ij}m_j$ and let A denote the matrix with ij^{th} entry a_{ij}. Notice that

$$\varphi\mathbf{1}_n \cdot \underline{m} = A \cdot \underline{m} \tag{28}$$

and so

$$(\varphi\mathbf{1}_n - A)\underline{m} = 0 \tag{29}$$

Left multiplying both sides of (29) by the adjugate of $\varphi\mathbf{1} - A$ gives:

$$\begin{aligned} 0 &= \mathrm{Adj}(\varphi\mathbf{1}_n - A) \cdot \big(\varphi\mathbf{1}_n - A)\underline{m}\big) \\ &= \big(\mathrm{Adj}(\varphi\mathbf{1}_n - A) \cdot \big(\varphi\mathbf{1}_n - A)\big)\underline{m} \\ &= \det(\varphi\mathbf{1}_n - A)\mathbf{1}_n \cdot \underline{m} \end{aligned}$$

and since $\underline{m}$ is a set of generators, this implies that $\det(\varphi\mathbf{1}_n - A) = 0$. □

Remark 6.1.4. An important further observation is that $\det(\varphi\mathbf{1}_n - A)$ is a monic polynomial $x^n + c_1x^{n-1} + ... + c_{n-1}x + c_n$, and if there is an ideal I such that $\varphi(M) \subseteq IM$ we have that $c_i \in I^i$.

Corollary 6.1.5. *If M is a finitely generated R-module and there is an ideal $I \subseteq R$ such that $IM = M$ then there exists $c_1, ..., c_n \in I$ with $c_i \in I^i$ such that $(1 + c_1 + ... + c_n)M = 0$. In particular, there exists $c \in I$ such that $(1 + c)M = 0$.*

Proof. Apply Theorem 6.1.3 to the identity function and take note of Remark 6.1.4. □

So Theorem 6.1.3 gives a powerful way of creating integral elements.

Definition 6.1.6. If $f : A \to B$ is a finitely generated A-module, then f is **finite**. Also, for an element $b \in B$ we denote by $f(A)[b]$ the A-algebra $\{f(b) \in B \mid f(x) \in A[x]\}$ (in other words, $f(A)[b]$ is the A-subalgebra of B generated by b).

Lemma 6.1.7. *An element $b \in B$ is integral if and only if $f(A)[b]$ is finite.*

Proof. If b is integral then there exists monic $g(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1} + x^n \in A[x]$ such that $g(b) = 0$. Thus $b^n \in A + Ab + \ldots + Ab^{n-1}$. That $\{1, b, \ldots, b^{n-1}\}$ generate $f(A)[b]$ follows from an obvious inductive argument.

If $f(A)[b]$ is a finitely generated A-module, then multiplication by b gives an endomorphism. The result then follows by Cayley-Hamilton. □

Lemma 6.1.8. *The integral elements of B over A form a subalgebra.*

Proof. $A \cdot 1$ is integral, thus it suffices to show the integral elements are closed under multiplication and subtraction. Let b_1, b_2 be integral. Let $i_1 : A \to A[b_1]$ and $i_2 : A[b_1] \to (A[b_1])[b_2]$ be inclusion maps. By 6.1.7 we have that $i_1(A)[b_1]$ and $i_2(A[b_1])[b_2]$ are finitely generated modules, and by the previous exercise, this implies $A[b_1, b_2]$ is a finitely generated A-module. Multiplication by $b_1 - b_2$ and multiplication by b_1b_2 give endomorphisms so the result follows from Cayley-Hamilton. □

In light of Lemma 6.1.8 we define the **integral closure** of A in B, denoted $\bar{A}$, to be the subalgebra of B given by the integral elements.

The following establishes a strong relationship between integrality and finitality:

Lemma 6.1.9. *A morphism $f : A \to B$ is finite if and only if $B = f(A)[b_1, ..., b_n]$ with b_i integral. In other words, $f : A \to B$ is finite if and only if B is a finitely generated and integral over A.*

Proof of ($\Rightarrow$) *direction.* If f is finite, then $f(A)[b]$ for all $b \in B$ is a finitely generated A-module, and thus b is integral by Lemma 6.1.7.

The converse is proved by induction on n and using the fact that the composition of finite morphisms is finite. □

The following results show that integrality is preserved by quotients, and is a local property:

Lemma 6.1.10. *Let $f : A \longrightarrow B$ be a ring homomorphism and let $I \subseteq B$ be an ideal. Then $A/(A \cap I) \longrightarrow B/I$ is integral.*

Proof. This really just comes down to realising what the induced $A/(A\cap I)$-algebra structure on B/I is: let $\bar{b} \in B/I$ and consider a representative $b \in B$. Then since $f : A \longrightarrow B$ is integral there exists a monic polynomial $p(x) \in A[x]$ with coefficients in A such that $p(b) = 0$. This polynomial with coefficients reduced modulo $A/(A \cap I)$ evaluates $\bar{b}$ to 0. □

Lemma 6.1.11. *Let $A \longrightarrow B$ be integral where A, B are k-algebras. Then* $\operatorname{Frac} A \longrightarrow \operatorname{Frac} B$ *is algebraic.*

Proof. Let $a/b \in \operatorname{Frac} A$ and $f = x^n + \sum_{j=0}^{n-1} \alpha_j x^j \in k[x]$ such that $f(a) = 0$. Then

$$0 = (1/b^n)(a^n/1) + (1/b^n)\sum_{j=0}^{n-1} \alpha_j (a^j/1) = (a/b)^n + \sum_{j=0}^{n-1} \alpha_j / b^{n-j} (a/b)^j$$

□

Remark 6.1.12. The above proof uses nothing special about the fact that we localised at (0). In fact if $A \longrightarrow B$ is integral and S is any multiplicative subset of A then $A_S \longrightarrow B_S$ is also integral.

6.2 Jacobson rings

We need the following fact about jacobson rings:

Lemma 6.2.1. *A is jacobson if and only if it satisfies the following property: for any prime $\mathfrak{p} \in A$ and element $a \in A/\mathfrak{p}$, if $(A/\mathfrak{p})_a$ is a field, then $A/\mathfrak{p}$ is a field.*

We prove the following special case of Lemma 6.2.3 as a warm up:

Lemma 6.2.2. *Let A be a jacobson domain and $B = A[s]$ an A-algebra generated by a single element. Then if B is a field, so is A.*

Proof. In light of Lemma 6.2.1 we see that it is sufficient to find an element $a \in A$ such that A_a is a field. Let $K = \operatorname{Frac} A$ be the field of fractions of A, we argue first that B is a finite field extension of K.

Write $B \cong A[x]/\mathfrak{q}$ for some ideal $\mathfrak{q}$. There is an obvious map $\varphi : A[x] \to K[x]/\mathfrak{q}K[x]$ with kernel equal to $\mathfrak{q}$. The induced map $\psi : A[x]/\mathfrak{q} \to K[x]/\mathfrak{q}K[x]$ is injective, we show this is an isomorphism.Let $\sum_{i=0}^{n} \left[\frac{a_i}{a_i'} x^i\right]$ be an arbitrary element of $K[x]/\mathfrak{q}K[x]$. In general, if $\gamma : Y \to X$ is a ring homomorphism with both $y \in Y$ and $\gamma(y) \in Y$ units, then $\gamma(y)^{-1} = \gamma(y^{-1})$. Thus

$$\sum_{i=0}^{n} \left[\frac{a_0}{a_0'} x^i\right] = \psi\Big(\sum_{i=0}^{n} [a_i][a_i']^{-1} x^i\Big)$$

proving surjectivity.

Since B is a finite field extension of K, it is algebraic. Thus there exists a (not necessarily monic) polynomial $p(x) = \sum_{i=0}^{n} \frac{a_i}{a_i'} x^i$ with coefficients in K such that $p(s) = 0$. By clearing denominators we obtain an expression $\sum_{i=0}^{n} a_i s^i = 0$, that is, s is integral over A. By inverting the leading coefficient a_n and dividing through, we see that s is integral over A_{a_n}. Since A_{a_n} is an integral extension of the field B, it follows from Corollary **??** that A_{a_n} is a field, which finishes the proof. □

With that warm up out of the way, we show the result we really want:

Lemma 6.2.3. *Let A be a jacobson domain and $B = A[s]$ an A-algebra generated by a single element. If B is a domain and there exists $b \in B$ such that B_b is a field, then both A and B are fields.*

Proof. In light of Lemma 6.2.1 we see that to show that A is a field, it is sufficient to find an element $a \in A$ such that A_a is a field, which similarly to the proof of Lemma 6.2.2, we do by finding an element $a \in A$ so that B_b is an integral extension of A_a. Once this is done, we will use the same lemma to show that B is a field by proving that B_b and hence B is an integral extension of A.

Let $K = \operatorname{Frac} A$ be the field of fractions of A, we argue that B_b is a finite field extension of K.

Write $B \cong A[x]/\mathfrak{q}$. There is an obvious map $\varphi : A[x] \to K[x]/\mathfrak{q}K[x]$ with kernel equal to $\mathfrak{q}$. The induced map $\big(A[x]/\mathfrak{q}\big)_b \to K[x]/\mathfrak{q}K$ is an isomorphism. Thus B_b is a finite field extension of K and so is algebraic; so there exists a polynomial $p(x) \in A[x]$ with coefficients in A such that $p(s) = 0$. Inverting the leading term p_n shows that s is integral over A_{a_n}, however, this is not the A_{a_n} that we will end up taking, as we still need b^{-1} to be integral over A_a.

Since $b \in B \subseteq K[x]/\mathfrak{q}K[x]$, there exists a polynomial $q(x) \in A[x]$ with coefficients in A such that $q(b) = q_m b^m + \ldots + q_0 = 0$. Since B is an domain we can cancel powers of b to assume that the Let q_m be the leading term of this polynomial. We can invert $q_0 b^m$ and divide through show that b^{-1} is integral in A_{q_0}. We now have that s and b^{-1} are integral in $A_{q_0 p_n}$ and so B_b is an integral extension of the field $A_{q_0 p_n}$.

Thus, B_b is an integral extension of the field $A_{q_0 p_n}$ and thus $A_{q_0 p_n}$ is a field. Since A is jacobson, it follows that A is a field, in fact, $A = A_{q_0 p_n}$. This shows that B_b and hence B is an integral extension of A, and so B is also a field. □

We use Lemma 6.2.3 to prove two important properties of jacobson rings.

Theorem 6.2.4. *If A is a jacobson ring and B a finitely generated A-algebra, then B is jacobson.*

Proof. Consider the case where B is generated by a single element $s \in B$. Let $\mathfrak{p} \subseteq B$ be a prime and $b \in B/\mathfrak{p}$ be such that $(B/\mathfrak{p})_b$ is a field. In light of Lemma 6.2.3 it suffices to show that $B/\mathfrak{p}$ is generated by a single element as an algebra over some jacobson ring. $B/\mathfrak{p}$ is generated by $[s]$ over $A/(A \cap \mathfrak{p})$, and indeed this is a jacobson ring as the quotient of any jacobson ring by any ideal is jacobson by the correspondence Theorem. The general case then follows by an obvious induction argument. □

Theorem 6.2.5. *If $f : A \to B$ is a ring homomorphism with A jacobson and B a finitely generated A-algebra, then $A \cap \mathfrak{m}$ is maximal for any maximal ideal $\mathfrak{m} \in B$.*

Proof. First consider the case where B is generated by a single element s. Let $\mathfrak{m} \in B$ be maximal. By the Correspondence Theorem, $A/f^{-1}(\mathfrak{m})$ is jacobson. Moreover, $B/\mathfrak{m}$ is generated by a single element as an algebra over $A/f^{-1}(\mathfrak{m})$. Thus by Lemma 6.2.2 we have that $A/f^{-1}(\mathfrak{m})$ is a field, that is, $f^{-1}(\mathfrak{m})$ is maximal. For the general case we proceed by induction. Say $B = A[b_1, ..., b_n]$. Let $\mathfrak{m}' \subseteq A[b_1, ..., b_{n-1}]$ be the preimage of $\mathfrak{m}$ in $A[b_1, ..., b_{n-1}]$. Since $A[b_1, ..., b_n] = \big(A[b_1, ..., b_{n-1}]\big)[b_n]$, and $A[b_1, ..., b_{n-1}]$ being a finitely generated A-algebra is jacobson (Theorem 6.2.4), it follows that $\mathfrak{m}'$ is maximal from the base case. The final observation to make is $\mathfrak{m}' = \mathfrak{m}$. □

Lemma 6.2.6. *For a jacobson ring A, the nilradical is equal to the jacobson radical.*

Proof. The nilradical is equal to the intersection of all primes, since all primes are the intersection of a family of maximals, the result follows. □

6.3 Going Up and Lying over Theorems

Loosely speaking, an integral extension $A \subseteq B$ occurs when every element of B is algebraically related to 0 usingonly using elements scalars from A. If A, B are integral domains then any polynomial relating an element of B to 0 can be "divided through" by the powers of x so that the constant term is non-zero. Another way of stating this is that if A, B are integral domains then an integral extension $A \subseteq B$ occurs when every element of B is algebraically related to an element of A only using elements of A:

Lemma 6.3.1. *Let $A \subseteq B$ be an integral extension with A, B integral domains. Then A is a field if and only if B is.*

Proof. First assume that A is a field. Let $b \neq 0 \in B$ and consider an expression

$$b^n + a_1 b^{n-1} + \ldots a_{n-1} b + a_0 = 0$$

where we may assume $a_0 \neq 0$ as B is an integral domain. We then ahve

$$a_0^{-1}(-b^{n-1} - a_1 b^{n-2} - \ldots - a_{n-1})b = 1$$

and so b is a unit.

Conversely, let $a \neq 0 \in A$ and consider a as an element of B. Since B is a field we have that a^{-1} exists in B and so there is

$$(a^{-1})^n + a_1(a^{-1})^{n-1} + \ldots + a_{n-1}(a^{-1}) + a_n = 0$$

which yields:

$$a^{-1} = a_1 a + \ldots + a_{n-1} a^{n-2} + a_n a^{n-1}$$

where the expression on the right is an element of A. □

A corollary of this is a sufficient condition for maximal ideals to be pulled back to maximal ideals:

Corollary 6.3.2. *Let $A \subseteq B$ an integral extension and $\mathfrak{p} \subseteq B$ an ideal of B. Then $\mathfrak{p}$ is maximal if and only if $A \cap \mathfrak{p}$ is.*

Proof. Integrality is preserved by taking quotients (Lemma 6.1.10) so $A/(A \cap \mathfrak{p}) \longrightarrow B/\mathfrak{p}$ is integral. We now have an integral extension of integral domains so we can apply Lemma 6.3.1. □

In turn, an application of this is for integral extensions $A \subseteq B$ the chains of primes of B lying over a prime in A are of length 0:

Corollary 6.3.3. *Let $A \subseteq B$ be integral and $\mathfrak{q} \subseteq \mathfrak{q}' \subseteq B$ primes in B such that $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof. Denote $\mathfrak{q} \cap A$ by $\mathfrak{p}$. Integrality is preserved by localisation (Lemma 6.1.11) so $A_\mathfrak{p} \longrightarrow B_{A \setminus \mathfrak{p}}$ is integral (warning: $\mathfrak{p} \subseteq B$ need not even be an ideal, let alone prime. However, $A \setminus \mathfrak{p}$ is multiplicative, so this localisation still makes sense). Consider $\mathfrak{q}B_{A\setminus\mathfrak{p}}$ and $\mathfrak{q}'B_{A\setminus\mathfrak{p}}$ which both intersect with $A_\mathfrak{p}$ to give $\mathfrak{p}A_\mathfrak{p}$. The result then follows from Corollary 6.3.2 and that primes in $B_{A\setminus\mathfrak{p}}$ are in bijection with primes in B disjoint from $A \setminus \mathfrak{p}$ (notice that $A \setminus \mathfrak{p} = A \setminus (\mathfrak{q} \cap A)$ so and ideal $I \subseteq B$ such that $I \cap (A \setminus (\mathfrak{q} \cap A)) = \varnothing$ is just an ideal I such that $I \cap A = \mathfrak{p}$). □

We have the lying over Theorem:

Theorem 6.3.4. *Let $A \subseteq B$ be integral. Then* $\operatorname{Spec} B \longrightarrow \operatorname{Spec} A$ *is surjective.*

Proof. Let $\mathfrak{p} \subseteq A$ be a prime. The localisation of integral extensions in integral, and so $A_{\mathfrak{p}} \longrightarrow B_{A\setminus\mathfrak{p}}$ is integral. We have the following commutative diagram:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow{\scriptstyle \beta} \\ A_{\mathfrak{p}} & \longrightarrow & B_{A\setminus\mathfrak{p}} \end{array}$$

Since $A_{\mathfrak{p}} \longrightarrow B_{A\setminus\mathfrak{p}}$ is integral, any maximal ideal $\mathfrak{m}$ of $B_{A\setminus\mathfrak{p}}$ is such that $\mathfrak{m} \cap A_{\mathfrak{p}} = \mathfrak{p}A_{\mathfrak{p}}$. So by commutativity we have $\beta^{-1}(\mathfrak{m})$ is a prime such that $\beta^{-1}(\mathfrak{m}) \cap A = \mathfrak{p}$. □

an easy Corollary of which is the going up Theorem:

Theorem 6.3.5. *Let $A \subseteq B$ be integral and consider say $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq A$ are prime ideals, and $\mathfrak{q}_1 \subseteq B$ is prime such that $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$. Then there exists prime $\mathfrak{q}_2 \subseteq B$ containing $\mathfrak{q}_1$ such that $\mathfrak{q}_2 \cap A = \mathfrak{p}_1$.*

Proof. Apply Theorem 6.3.4 to the integral extension $A/\mathfrak{p}_1 \subseteq B/\mathfrak{q}_1$. □

7 Dimension Theory

7.1 Transcendence degree of finitely generated k-domains

We prove:

Theorem 7.1.1. *Let A be a finitely generated k-integral domain, with k a field. Then*

1. $\text{tr.deg}_k A = \dim A$,
2. *if $\mathfrak{p}$ is any prime of A then* $\text{ht.}\,\mathfrak{p} + \dim A/\mathfrak{p} = \dim A$

We first establish some lemmas, we denote $k[x_1, ..., x_n]$ by $k[\underline{x}]$

Lemma 7.1.2. *Let $\mathfrak{p} \subseteq k[\underline{x}]$ be prime ideal, and consider $S = k[x_1, ..., x_m] \setminus \{0\}$ as a multiplicative subset of $k[\underline{x}]$. Then writing $k[\underline{x}]/\mathfrak{p} = k[\alpha_1, ..., \alpha_n]$ we have*

$$k[\underline{x}]_S/\mathfrak{p}k[\underline{x}]_S \cong k(\alpha_1, ..., \alpha_r)[\alpha_{r+1}, ..., \alpha_n]$$

Proof. Writing $\overline{S}$ for the image of S under $k[\underline{x}] \to k[\underline{x}]/\mathfrak{p}$ we have,

$$k[\underline{x}]_S/\mathfrak{p}k[\underline{x}]_S \cong (k[\underline{x}]/\mathfrak{p})_{\overline{S}} \cong k(\alpha_1, ..., \alpha_r)[\alpha_{r+1}, ..., \alpha_n]$$

□

The following Lemma was established in [**?**] as a required Lemma for proving Hilbert's Nullstellensatz, but we also use it here to prove Theorem 7.1.1:

Lemma 7.1.3. *Let $\mathfrak{m}$ be a maximal ideal of $F[x_1, ..., x_n]$, then $F[x_1, ..., x_n]/\mathfrak{m}$ is an algebraic extension of F.*

Proof. See [**?**, §2.1] □

Proof of Theorem 1. First we show $\text{tr. deg}_k A \geq \dim A$, we claim it suffices to show for any pair of prime ideals $\mathfrak{q} \subsetneqq \mathfrak{r}$ of $k[\underline{x}]$ that

$$\text{tr. deg}_k k[\underline{x}]/\mathfrak{r} < \text{tr. deg}_k k[\underline{x}]/\mathfrak{q} \tag{30}$$

Write $A \cong k[\underline{x}]/\mathfrak{p}$, any chain of primes in A corresponds to a chain $\mathfrak{x}_\mathfrak{o} \subsetneqq \ldots \subsetneqq \mathfrak{x}_\mathfrak{m}$ of primes in $k[\underline{x}]$ containing $\mathfrak{p}$. So given Equation 30 holds, we find

$$n - 1 < \text{tr. deg}_k A$$

establishing the claim.

There is a surjective map $k[\underline{x}]/\mathfrak{q} \to k[\underline{x}]/\mathfrak{r}$ so $\text{tr. deg}_k k[\underline{x}]/\mathfrak{r} \leq \text{tr. deg}_k k[\underline{x}]/\mathfrak{q}$ is clear. Say equality held. Let $\beta_1, ..., \beta_n$ denote the image of $x_1, ..., x_n$ under $k[\underline{x}] \to \text{Frac}\, k[\underline{x}]/\mathfrak{r}$ and by rearranging the order of $\underline{x}$ if necessary, assume that $\beta_1, ..., \beta_r$ be algebraically independent where $r := \text{tr. deg}_k k[\underline{x}]/\mathfrak{r}$. We denote by $\alpha_1, ..., \alpha_n$ elements of $k[\underline{x}]/\mathfrak{q}$ such that under $k[\underline{x}]/\mathfrak{q} \to k[\underline{x}]/\mathfrak{p}$ α_i maps to β_i. Notice that $\alpha_1, ..., \alpha_r$ are algebraically independent.

Consider $S := k[x_1, ..., x_r] \setminus \{0\}$ as a subset of $k[\underline{x}]$. $\alpha_1, ..., \alpha_r$ are algebraically independent, so $k[x_1, ..., x_r] \to k[\underline{x}]/\mathfrak{q}$ is injective and so $\mathfrak{q} \cap S = \varnothing$. Similarly, $\mathfrak{r} \cap S = \varnothing$. Writing $k[\underline{x}] = R$, it follows from Lemma 7.1.2 that

$$R_S/\mathfrak{q}R_S \cong k(\alpha_1, ..., \alpha_r)[\alpha_{r+1}, ..., \alpha_n]$$

where we think of the right hand side as a subring of $k(\alpha_1, ..., \alpha_n)$. By Lemma 3.1.3 this is a field, and so $\mathfrak{q}R_S$ is maximal. That is $\mathfrak{q}R_S = \mathfrak{r}R_S$ and so $\mathfrak{q} = \mathfrak{r}$, a contradiction.

Now we show $\text{tr. deg}_k A \leq \dim A$, we proceed by induction on $r := \text{tr. deg}_k A$. Write $A \cong k[\underline{x}]/\mathfrak{p}$, if $r = 0$ then A is a field and so $\dim A = 0$. Say $r > 0$, write $k[\underline{x}]/\mathfrak{p} = k[\alpha_1, ..., \alpha_n]$ and assume that α_1 is transcendental. Write $R := k[\underline{x}]$ and consider $S := k[x_1] \setminus \{0\}$ as a subset of R. Then $R_S \cong k(x_1)[x_2, ..., x_n]$ and $R_S/\mathfrak{p}R_S = k(\alpha_1)[\alpha_2, ..., \alpha_n]$, by Lemma 7.1.2. Now, $\text{tr. deg}_k R_S/\mathfrak{p}R_S < r$ so by the inductive hypothesis there exists a chain of primes $\mathfrak{x}_0 \subsetneqq ... \subsetneqq \mathfrak{x}_{r-1}$ of R_S all containing $\mathfrak{p}R_S$. We set $\mathfrak{r}_i := \mathfrak{x}_i \cap \mathfrak{p} \subset R$ and notice that in particular $x_1 \notin \mathfrak{r}_{r-1}$, and hence the residue class $[x_1] \in R/\mathfrak{r}_{r-1}$ is transcendental over k, which is to say that $\mathfrak{r}_{r-1}$ is not maximal (Lemma 7.1.3). Thus it is contained in a maximal ideal so we obtain a chain $\mathfrak{r}_0 \subsetneq \ldots \subsetneqq \mathfrak{r}_n$ in R all containing $\mathfrak{p}$. Thus $\dim A \geq \text{tr. deg}_k A$. □

We move onto the proof of Theorem 2, we start with the following special case:

Lemma 7.1.4. *Denote $k[\underline{x}]$ by R. Let $\mathfrak{p} \subseteq R$ be prime, then* $\text{ht.}\,\mathfrak{p} + \dim R/\mathfrak{p} = n$.

Proof. We proceed by induction on n. If $n = 0$ then $\mathfrak{p} = (0)$ and $\text{ht.}(0) = \dim R/(0) = 0$. Say $n > 0$. Let $r := \text{tr. deg}_k R/\mathfrak{p}$ and write $R/\mathfrak{p} = k[\alpha_1, ..., \alpha_n]$ where $\alpha_1, ..., \alpha_r$ are algebraically independent. Consider $S := k[x_1, ..., x_r] \setminus \{0\}$ as a subset of R. Then $R_S \cong k(x_1, ..., x_r)[x_{r+1}, ..., x_n]$. By the inductive hypothesis we have

$$\text{ht.}\,\mathfrak{p}R_S + \dim_k R_S/\mathfrak{p}R_S = n - r$$

By Lemma 3.1.3 we have $\dim_k R_S/\mathfrak{p}R_S = 0$. Furthermore, $\mathfrak{p} \cap S = \varnothing$ so $\text{ht.}\,\mathfrak{p}R_S = \text{ht.}\,\mathfrak{p}$. We thus have $\text{ht.}\,\mathfrak{p} + r = n$, the result then follows from Theorem 1 as $r = \text{tr. deg}_k R/\mathfrak{p} = \dim R/\mathfrak{p}$. □

We now generalise this:

Proof of Theorem 2. Write $A \cong k[\underline{x}]/\mathfrak{p}$ and let $\mathfrak{q} \subseteq A$ be prime. Then there is prime $\mathfrak{q}'$ in $k[\underline{x}]$ containing $\mathfrak{p}$ such that $A/\mathfrak{q} \cong k[\underline{x}]/\mathfrak{q}'$. From Lemma 7.1.4 we thus have

$$\text{ht.}\,\mathfrak{q}' + \dim k[\underline{x}]/\mathfrak{q}' = n = \text{ht.}\,\mathfrak{p} + \dim k[\underline{x}]/\mathfrak{p}$$

We thus have $\text{ht.}\,\mathfrak{q}' - \text{ht.}\,\mathfrak{p} + \dim A/\mathfrak{q}' = \dim A/\mathfrak{p}$. Clearly, $\text{ht.}\,\mathfrak{q}' - \text{ht.}\,\mathfrak{p} = \text{ht.}\,\mathfrak{q}$, and $\dim k[\underline{x}]/\mathfrak{q}' = \dim A/\mathfrak{q}$, thus

$$\text{ht.}\,\mathfrak{q} + \dim A/\mathfrak{q} = \dim A$$

as required. □

Next we prove:

Theorem 7.1.5. *A Noetherian integral domain A is a UFD if and only if every prime ideal of height 1 is principal.*

Proof. Let $\mathfrak{p}$ be of height 1 and $f \in \mathfrak{p} \setminus \{0\}$. $\mathfrak{p}$ by assumption is principal so write $\mathfrak{p} = (g_1)$. Let $h_1 \in A$ be such that $f = h_1 g_1$. Say h_1 is not a unit, then similarly there exists a prime ideal $\mathfrak{p}_1$ of height 1 containing h_1. Let $h_2 \in A$ be such that $(h_2) = \mathfrak{p}_2$ and $r_2 \in A$ be such that $h_1 = r_2 h_2$. Repeating this process we obtain a sequence $g_1, g_2, ...$ such that $(g_1) \subsetneqq (g_2) \subsetneqq \dots$ which by the Noetherian assumption is finite, of length n say. We have $f = r_n g_1 \dots g_n$.

Conversely, let $f \in A$ be a non-unit and not zero. Let $\mathfrak{p}$ be a minimal primes lying over f and write $f = r f_1 ... f_n$ for irreducibles f_i and unit r. Fix some $i \leq n$, we claim $\mathfrak{p} = (f_i)$. It suffices to show f_i is prime, but A is a UFD and so all irreducibles are prime. □

7.2 The Poincare Series and the length of a module

7.2.1 The length polynomial

Sometimes the notation of a geometric series is used for convenience sake, for instance, we have that in $\widehat{k[x]}$:

$$(1-x, 1-x, 1-x, \dots)(1, 1+x, 1+x+x^2, \dots) = (1, 1, 1, \dots) - (x, x^2, x^3, \dots)$$

and that $(x, x^2, x^3, ...)$ is equivalent to zero, this is often written as:

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

where both sides of the equality are thought of as elements of $\widehat{k[x]}$. This notation will be used in the statement involving the *Poincare series* (Definition 7.2.3) of a module with respect to an *additive function*:

Definition 7.2.1. Let A be a ring and $\mathcal{M}_A$ the class of all A-modules. A funcion:

$$\lambda : \mathcal{M}_A \longrightarrow \mathbb{Z}$$

is **additive** if for every short exact sequence

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

we have that $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Eventually we will specialise to the case where λ is the *length* of a module:

Definition 7.2.2. Let M be an A-module. The **length** of M is the supremum of the lengths of all ascending chains of submodules

$$M_0 \subsetneqq \dots \subsetneqq M_n$$

A chain consisting of $n+1$ modules has length n.

Definition 7.2.3. Let $A = \bigoplus_{i=0}^{\infty} A_i$ be a Noetherian graded ring and $M = \bigoplus_{i=0}^{\infty} M_i$ a graded A-module. The **Poincare series** is the element of $\mathbb{Z}[\![t]\!]$ given by

$$P(M, t) = \sum_{i=0}^{\infty} \lambda(M_i) t^i$$

What happens in the case where M is finitely generated? Being Noetherian, A is finitely generated as an A_0-module (see [**?**]). In the case where where M is finitely generated as an A_0-module, we have $M_n = 0$ for large n, and so $P(M,t)$ is just a polynomial in t. Now consider the case where A admits elements $a_1, ..., a_m$ with respective degrees $k_1, ..., k_m$ such that M is a finitely generated $A_0[a_1, ..., a_m]$-module. Multiplication by a_m yields an exact sequence for any n:

$$0 \longrightarrow \ker^n a_m \longrightarrow M_n \xrightarrow{a_m} M_{n+k_m} \longrightarrow \operatorname{Coker}^n a_m \longrightarrow 0 \tag{31}$$

where the n in $\ker^n a_m$ is a label signifying this is the kernel which is a submodule of M_n, similarly for $\operatorname{Coker}^n a_m$. Since λ is additive, by multiplying by t^{n+k_m} we obtain:

$$\lambda(\ker^n a_m)t^{n+k_m} - \lambda(M_n)t^{n+k_m} + \lambda(M_{n+k_m})t^{n+k_m} - \lambda(\operatorname{Coker}^{n+k_m} a_m)t^{n+k_m} = 0$$

summing over all n yields:

$$(1-t^{k_m})P(M,t) - \sum_{n=0}^{k_m} \lambda(M_n)t^n = \sum_{n=0}^{\infty} \lambda(\operatorname{Coker}^{n+k_m} a_m)t^{n+k_m} - t^{k_m} P(\ker a_m, t) \tag{32}$$

where $\ker a_m = \bigoplus_{n=0}^{\infty} \ker^n a_m$. Now, by defining

$$\operatorname{Coker} a_m := M_0 \oplus \ldots \oplus M_n \oplus \bigoplus_{n=0}^{\infty} \operatorname{Coker}^{n+k_m} a_m$$

we have

$$\sum_{n=0}^{\infty} \lambda(\operatorname{Coker}^{n+k_m} a_m)t^{n+k_m} = P(\operatorname{Coker} a_m, t) - \sum_{n=0}^{k_m} \lambda(M_n)t^n$$

and so (32) becomes:

$$(1-t^{k_m})P(M,t) = P(\operatorname{Coker} a_m, t) - t^{k_m} P(\ker a_m, t) \tag{33}$$

Noticing now that $\operatorname{Coker} a_m$ and $\ker a_m$ are both finitely generated $A_0[a_1, ..., a_m]$-modules and are annihilated by a_m so in fact are finitely generated $A_0[a_1, ..., a_{m-1}]$-modules, we have proved:

Theorem 7.2.4. *Let $A = \bigoplus_{i=0}^{\infty} A_i$ be a Noetherian graded ring and $M = \bigoplus_{i=0}^{\infty} M_i$ a finitely generated graded A-module. Let $a_1, ..., a_m$ be generators of A as an A_0-module with degrees $k_1, ..., k_m$ respectively. The Poincare series can be written as:*

$$P(M,t) = \frac{f(t)}{\prod_{i=1}^{m}(1-t^{k_m})} \tag{34}$$

where $f(t)$ is a polynomial.

We obtain different representations (34) by taking different sets of generators of A, however the *pole at $t = 1$* is invariant:

Definition 7.2.5. The **pole** of $\frac{f(t)}{\prod_{i=1}^{m}(1-t^{k_m})}$ at $t = 1$, denoted $d(M)$, is the pole in the ordinary sense when considered as a meromorphic function $\mathbb{C} \longrightarrow \mathbb{C}$.

That this pole is an invariant follows from the fact that each representation (34) is equal to $P(M,t)$ which does not depend on a choice of generators.

A further special case of Theorem 7.2.4 is when all the generators $a_1, ..., a_m$ have degree 1, in such a situation we can make a statement about the restriction of λ to the modules M_n for large n:

Corollary 7.2.6. *Let A be a Noetherian graded ring and M a finitely generated A-module. We know A is finitely generated as an A_0-module, assume further that generators of A all of degree 1 can be chosen. Then the function $n \mapsto \lambda(M_n)$ is given by a polynomial (in $\mathbb{Q}[t]$) for sufficiently large n. The degree of this polynomial is independent of the choice of generators and is equal to $d(M) - 1$.*

Proof. By definition of the Poincare series, the coefficient next to t^n is equal to $\lambda(M_n)$ (for all n). First, we calculate the coefficient next to t^n in $\prod_{i=1}^{m}(1-t)^{-m}$. Recall that $(1-t)^{-1} = 1 + t + t^2 + \ldots$ and so we wish to calculate the coefficient in front of t^n of

$$(1 + t + t^2 + \ldots)(1 + t + t^2 + \ldots)\ldots(1 + t + t^2 + \ldots)$$

where there are m factors. This has a combinatorial answer; this coefficient counts the number of multisubsets of the set $\{t_1, ..., t_m\}$ of size n, where t_i represents t chosen from the i^{th} factor. This coefficient is thus $\binom{n+m-1}{m-1}$.

Consider the representation of the Poincare series given by Theorem 7.2.4, we have that $f(t)$ is a polynomial so write $f(t) = \sum_{i=0}^{N} \alpha_i t^i$, by cancelling factors of $(1-t)$ we may assume $m = d(M)$ and $f(1) \neq 0$. We then have that the coefficient in front of t^n in $P(M,t)$ is the coefficient in front of t^n of

$$(\alpha_0 + \alpha_1 t + \alpha_2 t^2 + \ldots)(1 + t + t^2 + \ldots)(1 + t + t^2 + \ldots)\ldots(1 + t + t^2 + \ldots)$$

which by the previous calculation is

$$\sum_{k=0}^{N} \alpha_k \binom{n + d - k - 1}{d - 1} \tag{35}$$

notice that:

$$\binom{n + d - k - 1}{d - 1} = \frac{(n + d + k - 1)!}{(d-1)!(n+k)!} = \frac{(n + d + k - 1)\ldots(n + d - k - (d-1))}{(d-1)!} \tag{36}$$

which is a polynomial in n, and hence so is (35). Equation (35) holds true for all n, and is always a polynomial, but for $n < N$ this polynomial changes as n increases. On the other hand, for all $n \geq N$ this polynomial remains exactly the same. Thus for all $n \geq N$ we have that $\lambda(M_n)$ is equal as a function to a fixed polynomial. Lastly, notice that the numberator of (36) has $d-1$ factors, and so the leading term of (35) is

$$\frac{\left(\sum_{k=0}^{N} \alpha_k\right) n^{d-1}}{(d-1)!} = \frac{f(1) n^{d-1}}{(d-1)!}$$

which is non-zero. □

From now on, $\lambda : \mathcal{M}_A \longrightarrow \mathbb{Z}$ is taken to be the *length* function (Definition 7.2.1).

Assume M is an A-module (with no assumptions on either M nor A) and there is a filtration

$$\ldots \subseteq M_1 \subseteq M_0 = M$$

of M. If $n \geq 0$ is such that M/M_n admits a decomposition series (see the section on Artin Rings/modules of [**?**]) then since any chain of submodules can be extended to a decomposition series we have:

$$\lambda(M/M_n) = \sum_{i=0}^{n} \lambda(M_i/M_{i+1}) \tag{37}$$

Lemma 7.2.7. *Let $f : \mathbb{Z} \longrightarrow \mathbb{R}$ be a polynomial function of degree d. Then the function*

$$h_f : \mathbb{Z} \longrightarrow \mathbb{R}$$
$$n \mapsto \sum_{i=0}^{n} f(i)$$

is a polynomial of degree $d+1$.

Proof. Write $f(n) = \sum_{j=0}^{d} \alpha_j n^j$ so that

$$\begin{aligned} h_f(n) &= \sum_{i=0}^{n} \sum_{j=0}^{d} \alpha_j i^j \\ &= \sum_{j=0}^{d} \alpha_j \sum_{i=0}^{n} i^j \end{aligned}$$

so it remains to show for all $j \geq 0$ that $\sum_{i=0}^{n} i^j$ is a polynomial in n and that $\sum_{i=0}^{n} i^d$ has degree $d+1$. This can be done in many different ways, one of which is by using *Bernoulli numbers* and *Faulhaber's formula*, we omit the details. □

We have:

Proposition 7.2.8. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal, M a finitely-generated A-module, (M_n) a stable $\mathfrak{q}$-filtration of M. Then,*

1. *M/M_n is of finite length for each $n \geq 0$,*
2. *for sufficiently large n, this length is a polynomial $g(n)$ of degree less than or equal to s where s is the least number of generators of $\mathfrak{q}$,*
3. *the degree and leading coefficient of $g(n)$ is independent of the choice of stable $\mathfrak{q}$-filtration.*

Proof. 1: If A is a Noetherian local ring with maximal ideal $\mathfrak{m}$, let $\mathfrak{q} \subseteq A$ be a $\mathfrak{m}$-primary ideal, and assume M is finitely generated. The only prime ideal containing $\mathfrak{q}$ is $\mathfrak{m}$ and so $A/\mathfrak{q}$ is a Noetherian ring of dimension 0, and thus is Artinian. So, each M_i/M_{i+1} is a finitely generated module over an Artinian ring thus has finite length. It follows from (37) that $\lambda(M/M_n)$ is finite.

2: If $a_1, ..., a_s$ is a minimal set of generators of $\mathfrak{q}$ then the images $\bar{a}_1, ..., \bar{a}_m$ in $\mathfrak{q}/\mathfrak{q}^2$ generate $G(A) := \bigoplus_{i=0}^{\infty} \mathfrak{q}^i/\mathfrak{q}^{i+1}$. All of these have degree 1 and so by Corollary 7.2.6 there exists $N > 0$ such that the function $n \mapsto \lambda(M_{N+n}/M_{N+n+1})$ is given by a polynomial $p \in \mathbb{Q}[n]$ such that $\deg p \leq d(G(M))$. By the shape of (34) we have that $d(M) \leq s$. Equality holds when $f(t)$ does not admit 1 as a root.

3: Say (M_n) and (M'_n) are two stable $\mathfrak{q}$ filtrations of M. Let $N > 0$ be such that for all $n > N$ we have $\mathfrak{q}M_n = M_{n+1}$, make a similar definition for N'. We have

$$M_{n+N} = \mathfrak{q}^n M_N \subseteq \mathfrak{q}^n M = \mathfrak{q}^n M'_0 \subseteq M'_n$$

and

$$M'_{n+N} = \mathfrak{q}^n M'_{N'} \subseteq \mathfrak{q}^n M = \mathfrak{q}^n M_0 \subseteq M_n$$

and so if $g(n)$ is the polynomial corresponding to (M_n) and $g'(n)$ is the polynomial corresponding to (M'_n) then

$$g(n + N') \leq g'(n)$$

and

$$g(n) \leq g'(n + N)$$

since these are both polynomials we get $\lim_{n \longrightarrow \infty} g(n)/g'(n) \longrightarrow 1$ and so these have the same degree and leading coefficient. □

In the context of Proposition 7.2.8 where the stable $\mathfrak{q}$-filtration given by $(\mathfrak{q}^n M)$ is taken, we denote the polynomial $g(n)$ by $\chi_{\mathfrak{q}}^M(n)$. In the case where $M = A$ we denote this polynomial by $\chi_{\mathfrak{q}}(n)$. In fact, in this case, the degree of this polynomial is invariant under choice of $\mathfrak{m}$-primary ideal $\mathfrak{q}$, astonishingly, we will see later that this invariant degree is equal to the dimension of A.

Lemma 7.2.9. *The degree of $\chi_{\mathfrak{q}}(n)$ is invariant under choice of $\mathfrak{m}$-primary ideal $\mathfrak{q}$.*

Proof. Since A is Noetherian and $\mathfrak{q}$ is $\mathfrak{m}$-primary, there exists $r > 0$ such that $\mathfrak{m}^r \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, so for all n we have $\mathfrak{m}^{nr} \subseteq \mathfrak{q}^n \subseteq \mathfrak{m}^n$ and so for all n:

$$\lambda(A/\mathfrak{m}^{rn}) \leq \lambda(A/\mathfrak{q}^n) \leq \lambda(A/\mathfrak{m}^n)$$

and so

$$1 = \frac{\chi_{\mathfrak{m}}(rn)}{\chi_{\mathfrak{m}}(rn)} \leq \frac{\chi_{\mathfrak{q}}(n)}{\chi_{\mathfrak{m}}(rn)} \leq \frac{\chi_{\mathfrak{m}}(n)}{\chi_{\mathfrak{m}}(rn)} \overset{n\to\infty}{\longrightarrow} < \infty$$

the result follows. □

Definition 7.2.10. In light of Lemma 7.2.9, we denote the degree of $\chi_{\mathfrak{q}}(n)$ by $d(A)$.

Remark 7.2.11. Lemma 7.2.9 shows that the degree of $\chi_{\mathfrak{q}}(n)$ is independent of the choice of $\mathfrak{q}$, and Proposition 7.2.8 shows that this degree is equal to the size of the least number of generators of $\mathfrak{q}$, a corollary of this is that the size of the least number of generators of all $\mathfrak{m}$-primary ideals are equal.

7.3 The Dimension Theorem

Given a Noetherian, local ring A with maximal ideal $\mathfrak{m}$ we denote the least number of elements required to generate $\mathfrak{m}$ by $\delta(A)$. The amazing fact that we prove in this Section is that this integer and $d(A)$ (Definition 7.2.10) are both equal to $\dim A$. We do this by proving the following sequence of inequalities:

$$\delta(A) \geq d(A) \geq \dim A \geq \delta(A)$$

The first inequality is already proved by part 2 of Proposition 7.2.8. To prove the second inequality, we need the following general Lemmas:

Lemma 7.3.1. *Let A be Noetherian, local, and M a finitely generated A-module. Given any non-zero-divisor $x \in A$ of M we have*

$$d(M/xM) \leq d(M) - 1 \tag{38}$$

Proof. Since x is a non-zero-divisor, the map $M \longmapsto xM$ is injective and thus an isomorphism. It can be shown using the Nine Lemma that in general, if

$$0 \longrightarrow N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \longrightarrow 0$$

is a short exact sequence of modules and $J \subseteq N$ is a submodule, then the sequence

$$0 \longrightarrow N'/\alpha^{-1}J \longrightarrow N/J \longrightarrow N''/\beta(J)N''$$

is also a short exact sequence. Applying this to the submodule $\mathfrak{m}^n M \subseteq M$ we have for all $n \geq 0$ a short exact sequence:

$$0 \longrightarrow xM/(xM \cap \mathfrak{m}^n M) \longrightarrow M/\mathfrak{m}^n M \longrightarrow M'/\mathfrak{m}^n M' \longrightarrow 0$$

where $M' := M/xM$. If we let $g(n)$ denote the polynomial $xM/(xM \cap \mathfrak{m}^n M)$ (taking n sufficiently large) we have:

$$g(n) - \chi_{\mathfrak{m}}^M(n) + \chi_{\mathfrak{m}}^{M'}(n) = 0$$

Now, by the Artin-Rees Lemma (see [**?**]) we have that $xM \cap \mathfrak{m}^n M$ is a stable $\mathfrak{m}$-filtration of xM, and so by part 3 of Proposition 7.2.8 the leading term of $g(n)$ and $\chi_{\mathfrak{m}}^M(n)$ cancel out. The result follows. □

Applying Lemma 7.3.1 to the special case where $M = A$ we get:

Corollary 7.3.2. *If x is a non-zero-divisor of a Noetherian, local ring A, then*

$$d(A/(x)) \leq d(A) - 1$$

We can now prove:

Lemma 7.3.3.

$$d(A) \geq \dim A$$

Proof. We proceed by induction on $d(A)$. If $d(A) = 0$ then for sufficiently large n we have $\lambda(A/\mathfrak{m}^n) = \lambda(A/\mathfrak{m}^{n+1})$ which means $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ which by Nakayama's Lemma implies $\mathfrak{m}^n = 0$. Thus, if $\mathfrak{p}$ is a prime ideal of A we have $\mathfrak{m}^n = 0 \subseteq \mathfrak{p}$ which implies $\mathfrak{m} \subseteq \mathfrak{p}$, in other words, $\dim A = 0$.

Now say that $d(M) > 0$. Consider a chain of ascending prime ideals:

$$\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_r$$

in A. Let $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$, denote $A/\mathfrak{p}_0$ by A' and consider the image x' of x in A'. Then A' is an integral domain and $x' \neq 0$, so by Corollary 7.3.2 we have $d(A'/(x')) \leq d(A') - 1$. Our next claim is that $d(A') \leq d(A)$. There are many ways of showing this so we leave it as an exercise.

Thus $d(A'/(x')) \leq d(A) - 1$ and so the inductive hypothesis applies. However, the image of $\mathfrak{p}_1 \subsetneq \ldots \mathfrak{p}_r$ is an ascending chain in $A'/(x')$ and so $r - 1 \leq d(A) - 1$ which implies $r \leq d(A)$, proving the result. □

The remaining inequality, that $\dim A \leq \delta(A)$ follows from a *Krull's Principal Ideal Theorem*:

Theorem 7.3.4 (Krull's Principal Ideal Theorem)**.** *Let A be a Noetherian ring, $a_1, ..., a_r \in A$ elements of A and $\mathfrak{p}$ a prime, minimal among those containing $(a_1, ..., a_r)$, then* $\operatorname{ht}.\mathfrak{p} \leq r$.

Proof. We proceed by induction on r. Say $\mathfrak{p}$ is minimal over (a) and let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime not equal to $\mathfrak{p}$, we show $\operatorname{ht}.\mathfrak{q} = 0$. Let $l : A \longrightarrow A_\mathfrak{q}$ denote the localisation map and let $\mathscr{X}^n := l^{-1}\big((\mathfrak{q}A_\mathfrak{q})^n A_\mathfrak{q}\big)$. We claim $\mathscr{X}^n = (a)\mathscr{X}^n + \mathscr{X}^{n+1}$.

Since A is Noetherian the chain

$$(a) \subseteq (a) + \mathscr{X} \subseteq (a) + \mathscr{X}^2 \subseteq \ldots$$

eventually stablises, say $(a) + \mathscr{X}^n = (a) + \mathscr{X}^{n+1}$. In particular this means $\mathscr{X}^n \subseteq (a) + \mathscr{X}^{n+1}$ and so for any $f \in \mathscr{X}^n$ we have $f = ba + g$ for some $b \in A$ and $g \in \mathscr{X}^{n+1}$. Thus $f - ba \in \mathscr{X}^{n+1} \subseteq \mathscr{X}^n$, so since $f \in \mathscr{X}^n$ it follows that $ba \in \mathscr{X}^n$. Now, $\mathfrak{p}$ is minimal over (a) and $\mathfrak{q} \subseteq \mathfrak{p}$ so $a \notin \mathfrak{q}$, this means $b \in \mathscr{X}^n$ by definition of $\mathscr{X}$, establishing the claim.

By Nakayama's Lemma, we thus have $\mathscr{X}^n = \mathscr{X}^{n+1}$. Localising at $\mathfrak{q}$ we have $\mathscr{X}^n A_\mathfrak{q} = \mathscr{X}^{n+1} A_\mathfrak{q}$, ie, $(\mathscr{X} A_\mathfrak{q})^n = (\mathscr{X} A_\mathfrak{q})^{n+1}$. Applying Nakayama's Lemma again we have $(\mathscr{X} A_\mathfrak{q})^n = 0$. Thus if $\mathfrak{r} \subseteq A_\mathfrak{q}$ was any prime then $\mathfrak{r} \supseteq (0) = (\mathscr{X} A_\mathfrak{q})^n$ and thus $\mathfrak{r} \supseteq \mathscr{X} A_\mathfrak{q} = \mathfrak{q} A_\mathfrak{q}$ so by maximality $\mathfrak{r} = \mathfrak{q} A_\mathfrak{q}$. Thus $\dim A_\mathfrak{q} = 0$.

We now prove the inductive step. Let $\mathfrak{p} \subseteq A$ be minimal over $x_1, ..., x_n$ and by replacing A by $A_\mathfrak{p}$ if necessary, assume that A is local and $\mathfrak{p}$ maximal. Let $\mathfrak{q} \subseteq \mathfrak{p}$ be a prime with no other primes strictly sitting between. We will show that $\operatorname{ht}.\mathfrak{q} \leq n - 1$ by finding elements $y_1, ..., y_{n-1}$ such that $\mathfrak{q}$ is minimal over $(y_1, ..., y_{n-1})$.

Since $\mathfrak{p}$ is minimal over $(x_1, ..., x_n)$ and $\mathfrak{q} \subsetneq \mathfrak{p}$ we have $\{x_1, ..., x_n\} \not\subseteq \mathfrak{q}$, say $x_1 \notin \mathfrak{q}$. $\mathfrak{p}$ is minimal over $(\mathfrak{q}, x_1)$ and so $\sqrt{(\mathfrak{q}, x_1)} = \mathfrak{p}$, thus for $i = 2, ..., n$ there exists $r_i > 0$, $a_i \in A$, and $y_i \in \mathfrak{q}$ such that $x_i^{r_i} = a_i x_1 + y_i$. We claim $\mathfrak{q}$ is minimal over $y_2, ..., y_n$.

Denote the image of $\mathfrak{p}$ in the quotient ring $A/(y_2, ..., y_n)$ by $\bar{\mathfrak{p}}$, similarly for $\mathfrak{q}$. Then $\bar{\mathfrak{p}}$ is minimal over $\bar{x_1}$ and so $\bar{\mathfrak{q}}$ is minimal over 0. That is, $\mathfrak{q}$ is minimal over $(y_2, ..., y_n)$. □

The inductive step also proves a converse:

Corollary 7.3.5. *If a prime ideal $\mathfrak{p}$ has height n, then there exists $a_1, ..., a_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is minimal amongst all prime ideals containing $(a_1, ..., a_n)$.*

Application: If A is a Noetherian, local ring with maximal ideal $\mathfrak{m}$ and $a_1, ..., a_n$ are elements of A whose images under $A \longrightarrow \mathfrak{m}/\mathfrak{m}^2$ form a basis for this vector space, then if we denote by N the submodule of A generated by $a_1, ..., a_n$ we have

$$N + \mathfrak{m}^2 = \mathfrak{m}$$

so by Nakayama's Lemma, $N = \mathfrak{m}$. This shows:

Corollary 7.3.6. *Let A be Noetherian, local with maximal ideal $\mathfrak{m}$. Then*

$$\dim_k \mathfrak{m}/\mathfrak{m}^2 \geq \dim A$$

Remark 7.3.7. In the above discussion we have used that the vector space dimension agrees with Krull dimension, and the Dimension Theorem.

Corollary 7.3.8. *Let A be Noetherian, local with maximal ideal $\mathfrak{m}$, and $\hat{A}$ the $\mathfrak{m}$-adic completion. Then*

$$\dim A = \dim \hat{A}$$

Proof. $A/\mathfrak{m}^n \cong \hat{A}/\hat{\mathfrak{m}}^n$, so $d(A) = d(\hat{A})$. □

8 Discrete valuation rings

What *is* the integral closure? An answer can be provided once a theory of *valuation rings* has been developed:

Theorem 8.0.1. *Let B be a subring of a field K. Then the integral closure $\bar{B}$ of B in K is the intersection of all subrings of* Frac B *containing B which are* discrete valuation rings.

Definition 8.0.2. A **valuation ring** B is an integral domain satisfying: for all $x \neq 0 \in \operatorname{Frac} B$ either $x \in B$ or $x^{-1} \in B$ (or both).

A valuation ring is **discrete** if the quotient group $(\operatorname{Frac} B)^\times / B^\times$ is isomorphic to $\mathbb{Z}$, here, the superscript $\times$ denotes the group of units (the intuition behind this Definition comes from Lemma **??**)

It is clear that discrete valuation rings exist, any field provides an example, but there are more interesting examples involving homomorphisms into algebraically closed fields. First we provide some properties:

Lemma 8.0.3. *If B is a valuation ring, then*

1. *B is a local ring,*
2. *if B' is a ring such that $B \subseteq B' \subseteq \operatorname{Frac} B$ then B' is also a discrete valuation ring,*
3. *B is integrally closed.*

Proof. 1: Let $\mathfrak{m}$ be the set of all non-units of B, we show that this is an ideal. Let $b, x \in B$. If bx is a unit then $\exists r \in B, rbx = 1$ which implies x is a unit. Thus if $x \in \mathfrak{m}$ then $bx \in \mathfrak{m}$. If $x, y \in \mathfrak{m}$ then since B is a discrete valuation ring, either $x^{-1}y \in B$ or $xy^{-1} \in B$. In the first case we have $x + y = (1 + x^{-1}y)x \in B\mathfrak{m} \subseteq \mathfrak{m}$.

2: Let $x \in \operatorname{Frac} B$ and say $x \notin B'$. Then $x \notin B$ and so $x^{-1} \in B$ which implies $x^{-1} \in B'$.

3: Let $\alpha \in \operatorname{Frac} B$ be integral over B, write

$$\alpha^n + b_1\alpha^{n-1} + \ldots + b_{n-1}\alpha + b_n = 0$$

We have that $\alpha \in B$ or $\alpha^{-1} \in B$, in the first case we are done, in the second we have

$$\alpha = b_n\alpha^{1-n} - b_{n-1}\alpha^{2-n} - \ldots - b_2\alpha^{-1} - b_1$$

where the expression on the right is an element of B. Thus in either case we have $\alpha \in B$. □

Our next goal is to prove:

Proposition 8.0.4. *Let K be a field and Ω an algebraically closed field. Define Σ_K^Ω to be the set of pairs (C, f) where $C \subseteq K$ is a subring and $f : C \longrightarrow \Omega$ a homomorphism;*

$$\Sigma_K^\Omega := \{(C, f) \mid C \subseteq K, f : C \longrightarrow \Omega \text{ a homomorphism}\}$$

We endow Σ_K^Ω with the following partial order: $(C, f) \prec (C', f')$ if $C \subseteq C'$ and $f' \restriction_C = f$, then Σ_K^Ω satisfies the ascending chain condition and so by zorn's Lemma admits at least one maximal element (B, g). This ring B is a discrete valuation ring.

Remark 8.0.5. Note: we do not exclude the possibility that Ω is taken to be the trivial field (0). In this case, the unique maximal element given (B, g) is $(K, 0)$, where 0 denotes the zero map. In this situation, it is clear that K is a valuation ring. In what follows, we consider the case where $K \neq B$.

First we prove a simpler result:

Lemma 8.0.6. *B is a local ring, and if $K \neq B$ then the unique maximal ideal is $\mathfrak{m} := \ker g$.*

Proof. Notice first that $\mathfrak{m}$ is at least prime. As B is a subring of a field it is an integral domain, thus there is an injection $B \longrightarrow B_{\mathfrak{m}}$. We have that for all $x \notin \mathfrak{m}$ that $g(x) \neq 0$ (by definition of $\mathfrak{m}$) so by the universal property of localisation we obtain a homomorphism $B_{\mathfrak{m}} \longrightarrow \Omega$ which extends B. By maximality of B we obtain $B = B_{\mathfrak{m}}$ which implies the statement. □

Remark 8.0.7. Some authors (for example, Hartshorne) do not consider the set Σ_K^Ω but instead consider the set

$$\Gamma := \{R \subseteq K \mid R \text{ is local}\} \tag{39}$$

and endow this set with a partial order given by **domination**, $R \prec S$ if $S \subseteq R$ and $\mathfrak{m}_R \cap S = \mathfrak{m}_S$, with $\mathfrak{m}_T$ denoting the unique maximal ideal of T.

This is equivalent to our presentation as since (B, g) is local, it suffices to consider only local rings in Σ_K^Ω, and all such local rings have unique maximal element given by the inverse of $\{0\}$ which renders the condition on the preorder given to Σ_K^Ω equivalent to the domination condition.

Before proving Proposition 8.0.4 we need the following narky lemma:

Lemma 8.0.8. *Let $x \neq 0 \in K$, then either $\mathfrak{m}B[x] \neq B[x]$ or $\mathfrak{m}B[x^{-1}] \neq B[x^{-1}]$.*

Proof. Say both $\mathfrak{m}B[x] = B[x]$ and $\mathfrak{m}B[x^{-1}] = B[x^{-1}]$. Then we have equations:

$$1 = m_n x^n + \ldots m_1 x + m_0 \tag{40}$$

$$1 = m'_k x^{-k} + \ldots m'_1 x^{-1} + m'_0 \tag{41}$$

with $m_j, m'_j \in \mathfrak{m}$. We assume that these expressions are such that n is minimal. Say $k < n$ and multiply (41) by x^k we get:

$$(1 - m'_0)x^k = m'_k + m'_{k-1}x^1 + \ldots + m'_1 x^{k-1} \tag{42}$$

Since $m'_0 \in \mathfrak{m}$ we have $1 - m'_0$ is a unit and so we can divide through and multiply by x^{n-k} to write (40) with a smaller power of n, contradicting minimality. □

Proof of Proposition 8.0.4. Let $x \neq 0 \in \operatorname{Frac} B$ and assume $\mathfrak{m}B[x] \neq B[x]$ (if in fact $\mathfrak{m}B[x] = B[x]$ then replace x by x^{-1} in the following argument). Let $\mathfrak{n}$ be a maximal ideal containing $\mathfrak{m}B[x]$ in $B[x]$. Then $\mathfrak{n} \cap B$ contains $\mathfrak{m}$ and $\mathfrak{m}$ is maximal, thus $\mathfrak{n} \cap B = \mathfrak{m}$, we thus have a homomorphism $B/\mathfrak{m} \longrightarrow B[x]/\mathfrak{n}$. Also, the homomorphism $g : B \longrightarrow \Omega$ induces $B/\mathfrak{m} \longrightarrow \Omega$. We thus have the following commutative diagram of solid arrows

$$\begin{array}{ccccc} B & \longrightarrow & B/\mathfrak{m} & \longrightarrow & \Omega \\ \downarrow & & \downarrow & \nearrow & \\ B[x] & \longrightarrow & B[x]/\mathfrak{n} & & \end{array} \tag{43}$$

We have that $B[x]/\mathfrak{n} \cong B/\mathfrak{m}[\bar{x}]$ where $\bar{x}$ is the image of x under $B/\mathfrak{m} \longrightarrow B[x]/\mathfrak{n}$ and so $B/\mathfrak{m} \longrightarrow B[x]/\mathfrak{n}$ is a finite and thus algebraic field extension. Thus we have the dashed arrow in (43) (here we crucially use that Ω is algebraically closed). By maximality, it then follows that $B = B[x]$, that is, $x \in B$. □

Theorem 8.0.1 now follows as a Corollary:

Proof of Theorem 8.0.1. Let D denote the intersection of all discrete valuation rings of K. Since all discrete valuation rings are integrally closed it follows that $\bar{B} \subseteq D$.

Conversely, say $x \in K$ and is not integral over B. Then x is not contained in the ring $B[x^{-1}]$. Thus x^{-1} is a non-unit inside $B[x^{-1}]$ and so is contained inside a maximal ideal $\mathfrak{m}$. Let Ω be an algebraic closure of the field $B[x^{-1}]/\mathfrak{m}$, we then have a homomorphism

$$B \longrightarrow B[x^{-1}] \longrightarrow B[x^{-1}]/\mathfrak{m} \longrightarrow \Omega$$

and so by Proposition 8.0.4 extends to a discrete valuation ring not containing x. □

We give an alternative Definition of a valuation ring, which explains the name:

Definition 8.0.9. Let K be a field. and G a totally ordered abelian group. A **valuation** is a function $v : K \setminus \{0\} \longrightarrow G$ satisfying:

1. $v(xy) = v(x) + v(y)$,
2. $v(x + y) \geq \min\{v(x), v(y)\}$

Given a valuation v, the set $R_{K,v} := \{x \in K \mid v(x) \geq 0\}$ is a local ring with maximal ideal $\{x \in K \mid v(x) > 0\}$. We call this local ring the **valuation ring of** v.

A **valuation ring** is an integral domain which is the valuation ring of v for some valuation $v : K \longrightarrow G$.

9 Completion

9.1 Topological bases and neighbourhood bases

We will use extensively the notion of a *neighbourhood* which in some texts are taken to be open, here however we do not require this:

Definition 9.1.1. A **neighbourhood** of a point x in a topological space X is a subset $V \subseteq X$ of X containing an open set U such that $x \in U \subseteq V$.

Remark 9.1.2. Neighbourhoods which are not necessarily open occur in situations where the topological space has extra structure. For instance, a non-open subgroup A' of a topological abelian group A may contain an open subset U containing 0 where U is not a subgroup. The terminology "the subgroup A' is a neighbourhood of 0" is simpler language.

When defining topologies, it is often easier to define a *topology basis*:

Definition 9.1.3. Let X be a set. A **topology basis** $\mathscr{B}$ of X is a collection of subsets of X such that

1. The $\mathscr{B}$ cover X,
2. if $U, V \in \mathscr{B}$ then for every $x \in U \cap V$ there exists $W \in \mathscr{B}$ containing x such that $W \subseteq U \cap V$.

If X is a topological space, then a collection of open subsets $\mathscr{B}$ is a **topological basis** if every open set $U \subseteq X$ can be written as a union of elements in $\mathscr{B}$.

Any topological basis in the second sense is a topological basis in the first sense, and conversely, every topological basis $\mathscr{B}$ in the first sense gives rise to a unique topology such that $\mathscr{B}$ is a topological basis in the second sense.

Lemma 9.1.4. *Given a set X and topology basis $\mathscr{B}$, there is a unique topology $\mathscr{T}$ on X such that $\mathscr{B}$ becomes a topology basis for X as a topological space.*

Proof. Let $\mathcal{T}$ be the topology given by unions of elements of $\mathscr{B}$. Clearly we have that $\mathscr{B}$ is a topology basis for X with respect to this topology.

If $U \in \mathcal{T}'$ where $\mathcal{T}'$ is any topology on X such that $\mathscr{B}$ is a topology basis then U can be written as the union of elements of $\mathscr{B}$ and so $U \in \mathcal{T}$.

Conversely, if $U \in \mathcal{T}$ then since $\mathscr{B}$ is a topology basis for $\mathcal{T}'$ we have that every element of $\mathscr{B}$ is open (in $\mathcal{T}'$), and thus $U \in \mathscr{T}'$. □

It is sometimes more convenient to define a topology by considering particular sets containing each point individually:

Definition 9.1.5. Let X be a set, a **system of neighbourhoods** is a collection of sets of subsets $\{\mathscr{B}(x)\}_{x \in X}$ of X subject to:

1. $\mathscr{B}(x) \neq \varnothing$.
2. if $U \in \mathscr{B}(x)$ then $x \in U$,
3. if $U, V \in \mathscr{B}(x)$ then there exists $W \in \mathscr{B}(x)$ such that $W \subseteq U \cap V$,
4. if $U \in \mathscr{B}(x)$ then there exists a non-empty subset $V \subseteq U$ containing x such that for all $y \in V$, there is $W \in \mathscr{B}(y)$ such that $W \subseteq V$.

Definition 9.1.6. Let X be a topological space and $x \in X$ a point. A **neighbourhood filter** (**neighbourhood system**) of x is a collection of neighbourhoods $\mathcal{U}$ of x such that for any arbitrary neighbourhood $V \subseteq X$ of x there exists $U \in \mathcal{U}$ such that $U \subseteq V$.

Lemma 9.1.7. *Let X be a set and $\{\mathscr{B}(x)\}_{x\in X}$ a system of neighbourhoods. There exists a unique topology on X such that for all x, the set $\mathscr{B}(x)$ is a neighbourhood filter of x.*

Proof. Define a subset of $A \subseteq X$ to be **$\mathscr{B}$-open** if for every $x \in A$ there exists $U \in \mathscr{B}(x)$ such that $U \subseteq A$. Then let $\mathscr{T}$ be the collection of $\mathscr{B}$-open subsets of X.

Let U be a neighbourhood of a point $x \in X$. Then there exists a $\mathscr{B}$-open subset $A \subseteq U$ containing x. By definition of $\mathscr{B}$-open, there exists an element of $\mathscr{B}(x)$ contained inside A. Thus $\mathscr{B}(x)$ forms a neighbourhood filter for x.

Let $\mathscr{T}'$ be any other such topology and let $U \in \mathscr{T}'$. Then for every $x \in U$ there exists an element of $V \subseteq \mathscr{B}(x)$ such that $V \subseteq U$. Moreover, there exists $W \subseteq V$ which is $\mathscr{B}$-open (by (4)), and so $V \in \mathscr{T}$.

Convesely, if $U \in \mathscr{T}$ then $U \in \mathscr{T}'$ follows from (3). □

We conclude by describing the relationship between a topological basis and a system of neighbourhoods.

Proposition 9.1.8. *Let $\mathscr{B}$ be a topological basis for a set X. Then for each x the collection of all sets $\mathscr{B}(x) := \{U \in \mathscr{B} \mid x \in U\}$ is a system of neighbourhoods.*

Conversely, if $\{\mathscr{B}(x)\}_{x\in X}$ is a system of neighbourhoods then $\mathscr{B} := \bigcup_{x\in X} \mathscr{B}(x)$ is a topological basis.

Moreover, if $\mathscr{B}$ is a topology basis, then the topology induced by $\mathscr{B}$ is equal to the topology induced by the system of neighbourhoods $\{\mathscr{B}(x)\}_{x\in X}$. If $\{\mathscr{B}(x)\}_{x\in X}$ is a system of neighbourhoods, then the topology induced by this system of neighbourhoods is equal to the topology induced by the topology basis $\mathscr{B}$.

Proof. Since $\mathscr{B}$ covers X we have that $\mathscr{B}(x) \neq \varnothing$ for each $x \in X$. Next, it is clear that $U \in \mathscr{B}(x)$ implies $x \in U$, by the definition of $\mathscr{B}(x)$. Thirdly, if $U, V \in \mathscr{B}(x)$ then for all $y \in U \cap V$ ther exists $W \ni y$ such that $W \subseteq U \cap V$, so apply this to $y = x$. Lastly, let $U \in \mathscr{B}(x)$ and let $y \in U$. Consider an arbitrary $V \in \mathscr{B}(y)$. There then exists $W \subseteq U \cap V$ such that $y \in W \subseteq U \cap V$. This shows that for every element $y \in U$ there exists $W \in \mathscr{B}(y)$ such that $y \in W \subseteq U$.

Conversely, let $U, V \in \mathscr{B}$. Say $U \in \mathscr{B}(x)$ and $V \in \mathscr{B}(y)$ with $U \cap V \neq \varnothing$. Let $z \in U \cap V$ so that $x, z \in U$ and $z, y \in V$. There exists $W_x \in \mathscr{B}(z)$ such that $W_x \subseteq U$ and $W_y \in \mathscr{B}(z)$ such that $W_y \subseteq V$ by axiom 4. Thus there exists $W_{xy} \subseteq W_x \cap W_y$ such that $W_{xy} \subseteq W_x \cap W_y$ and thus $W_{xy} \subseteq U \cap V$.

Assume we are given a topological basis $\mathscr{B}$. Let $\mathscr{T}_{\mathscr{B}}$ be the topology generated by the topological bass, and $\mathscr{T}_{\mathscr{B}(x)_x}$ the topology generated by the system of neighbourhoods. First we show $\mathscr{T}_{\mathscr{B}} \subseteq \mathscr{T}_{\mathscr{B}(x)_x}$: by Lemma 9.1.7 it suffices to show for all $x \in X$ that $\mathscr{B}(x)$ is a neighbourhood filter of x. Let $U \in \mathscr{B}$ be a neighbourhood of x. Then by definition of $\mathscr{B}(x)$ we have $U \in \mathscr{B}(x)$.

Now we show $\mathscr{T}_{\mathscr{B}(x)_x} \subseteq \mathscr{T}_{\mathscr{B}}$: by Lemma 9.1.4 it suffices to show that $\mathscr{B}$ is a topological basis. Let U be $\mathscr{B}$-open and $u \in U$. By definition of $\mathscr{B}$-open there exists $V \in \mathscr{B}(u)$ such that $V \subseteq U$. Thus $\mathscr{T}_{\mathscr{B}(x)_x} = \mathscr{T}_{\mathscr{B}}$.

The remainder of the proof is similar. □

Remark 9.1.9. In essence, a system of neighbourhoods $\{\mathscr{B}(x)\}$ of X is just a topological basis $\mathscr{B}$ of X parametrised by the elements $x \in U \in \mathscr{B}$, ranging over all x and all U. The axioms for a system of neighbourhoods is then just the translation of the axioms for a topological basis to this new setting:

- Axioms 1,2 together are equivalent to the condition that $\mathscr{B}$ covers X,
- Axioms 3, 4 together are equivalent to the statement then if $U, V \in \mathscr{B}$ then there exists $W \in \mathscr{B}$ such that $W \subseteq U \cap V$.

9.2 Completion of topological abelian groups

Lemma 9.2.1. *Let G be a topological abelian group and H the intersection of all neighbourhoods of 0 in G. Then*

1. *H is a subgroup,*
2. *H is the closure of $\{0\}$,*
3. *G/H is hausdorff,*
4. *G is hausdorff if and only if $H = 0$.*

Proof. (1) Let $a \in H$. We need to first show that $-a \in V$ where V is an arbitrary open neighbourhood of 0. The map ρ is its own inverse and so ρ is a homeomorphism. It follows that $\rho(V)$ is itself an open neighbourhood of 0 and so $a \in \rho(V)$ which implies $-a \in V$.

Similarly, let $a, b \in H$ and consider the homeomorphism $T_a : G \longrightarrow G, g \mapsto a + g$. This is also a homeomorphism so it suffices to show $a + b$ is in every set of the form $T_g^{-1}(V)$ for some $g \in G$ and open neighbourhood V of 0. We take $g = -a$ and this is now obvious.

(2) First we prove that if $x \in H$ then x and 0 have the same set of open neighbourhoods. Since $x \in H$ it is clear that every open neighbourhood of 0 is an open neighbourhood of x, we now show the converse. Let V be an open neighbourhood of x. Then

$$\begin{aligned} x \in V &\implies -x \in -V \\ &\implies 0 \in x - V \\ &\implies x \in x - V, \text{ as every open nbhd of 0 is such of } x, \\ &\implies 0 \in -V \\ &\implies 0 \in V \end{aligned}$$

Now say Z is a closed set containing $\{0\}$, then Z^c is open and does not containing 0 and hence does not contain any element of H, from what we just calculated. Thus $H \subseteq Z$ and so $H \subseteq \overline{\{0\}}$. Conversely, let $x \in \overline{\{0\}}$. Consider an open neighbourhood V of 0. We have

$$\begin{aligned} 0 \in V &\implies x \in x + V \\ &\implies 0 \in x + V, \text{ as every open nbhd of } x \text{ is such of 0}, \\ &\implies -x \in V \\ &\implies -x \in H \\ &\implies x \in H \end{aligned}$$

(3) The diagonal Δ is the inverse image of $\{0\}$ under subtraction. The set $\{0\}$ under the subspace topology is closed by (2).

(4) Follows from (3). □

Definition 9.2.2. Let G be a topological abelian group. A **cauchy sequence in** G is a sequence $(x_1, x_2, ...)$ of elements in G such that for all neighbourhoods U of 0 there exists $N > 0$ such that for $n, m \geq N$ we have $x_n - x_m \in U$. A sequence of elements $(x_1, x_2, ...)$ **converges** to 0 if for all open neighbourhoods U of 0, there exists $N > 0$ such that $\forall n > N$ we have $x_n \in U$. We write $(x_n) \longrightarrow 0$ in this case (even though there may be more elements than just 0 in H).

Lemma 9.2.3. *The relation $\sim$ on the set of all cauchy sequences in G about 0 given by $(x_n)_n \sim (y_n)_n$ if $(x_n - y_n)_n \longrightarrow 0$ is an equivalence relation.*

Proof. Reflexivity is clear. For symmetry it suffices to show that if $(x_n)_n$ is cauchy then so is $(-x_n)_n$. If an element $x \in X$ is contained in every open neighbourhood V of 0 then $-x \in -V$. The result follows as all neighbourhoods W of 0 are given by $-W'$ for some neighbourhood W' (take $W' = -W$). For transitivity it suffices to show the sum of cauchy sequences $(x_n)_n$ and $(y_n)_n$ (given by the sequence $(x_n + y_n)_n$) is cauchy. Let V be an open neighbourhood of 0. Consider $+^{-1}(V)$, by the definition of the product topology there exists open neighbourhoods of 0; U, U' such that $U \times U' \subseteq +^{-1}(V)$. Now let $N_1, N_2 > 0$ be such that $x_n - x_m \in U$ and $y_n - y_m \in U'$ for $n, m > \max N_1, N_2$. Then $x_n + y_n - x_m - y_m \in V$. □

There is a topology on the set of equivalence classes of cauchy sequences on a topological group G, it is defined as follows:

Definition 9.2.4. Let G be a topological abelian group and let G denote the set of cauchy sequences in G. The **induced topology** is given as follows: for every neighbourhood V of 0 in G let $\hat{V}$ be the set containing all cauchy sequences $(x_n)_n$ which are eventually in V, that is, there exists $N > 0$ such that $\forall n > N$ we have $x_m \in N$. The set $\{(x_n)_n + \hat{V} \mid V \subseteq G \text{ neighbourhood}, (x_n)_n \in \text{Cauchy}(G)\}$ forms a system of neighbourhoods in Cauchy(G).

Exercise 9.2.5. Check if the following is true: let (M, d_M) be a metric space and $(\hat{M}, d_{\hat{M}})$ its completion. Then the topology $\mathcal{T}$ induced by the metric $d_{\hat{M}}$ is equivalent to the topology $\mathcal{T}'$ consisting of subsets $\hat{U} \subseteq \hat{M}$ of equivalence classes of cauchy sequences all of which are eventually in U, ranging over all U in the topology on M induced by the metric d_M.

Definition 9.2.6. The **completion** $\hat{G}$ (sometimes denoted Cplt(G)) of a topological abelian group G is the topological abelian group of equivalence classes of cauchy sequences with the quotient space topology of the induced topology (Definition 9.2.4). Addition is given pointwise.

There is a canonical map $\phi : G \longrightarrow \hat{G}$ defined by $g \mapsto (g)_n$ and this map has kernel $\ker \phi = H$.

Lemma 9.2.7. *Completion is a functor* $\underline{\text{TopAbGp}} \longrightarrow \underline{\text{CompleteTopAbGp}}$.

Proof. Let $f : G \longrightarrow G'$ be a continuous homomorphism and let $(x_n)_n$ be a cauchy sequence in G. Let V be an open neighbourhood of 0 in G', and consider $f^{-1}(V)$ which is open in G. There exists N such that $\forall n, m \geq N$ we have $x_n - x_m \in f^{-1}(V)$ thus $\forall n, m \geq N$ we have $f(x_n) - f(x_m) \in V$. Thus $(f(x_n))_n$ is cauchy and thus we have defined $\hat{f} : \hat{G} \longrightarrow \hat{G}'$. Clearly, $\text{Cplt}\, \text{id}_G = \text{id}_{\text{Cplt}\, G'}$ and

$$\text{Cplt}\, gf(x_n)_n = (gf(x_n))_n = \text{Cplt}\, g(f(x_n))_n = \text{Cplt}\, g\, \text{Cplt}\, f(x_n)_n$$

so we get functoriality. That the completion of a topological abelian group is complete is Lemma 9.2.25 below. □

We now come up with another way of arriving at completions in a more general context:

Definition 9.2.8. A **filtration** (G_n) of an abelian group G is a countably infinite chain of subgroups $(\ldots G_2 \subseteq G_1 \subseteq G_0 = G)$. A **filtered abelian group** is an abelian group G along with a filtration (G_n) of G. A **homomorphism of filtered abelian groups** $\phi : G \longrightarrow H$ is a homomorphism such that $\phi(G_n) \subseteq H_n$.

Lemma 9.2.9. *Let G be an abelian group and (G_n) a filtration. Then $\{g + G_n\}_{n \geq 0, g \in G}$ is a system of neighbourhoods.*

Proof. First, any $g + G_n$ in this collection we have that $g = g + 0 \in g + G_n$ and so $g + G_n \neq \varnothing$. Notice that this also shows that $g \in g + G_n$. Next, $g + G_n \cap h + G_m \supseteq g + h + G_{\max\{n,m\}}$. Lastly, if $h \in g + G_n$ then $h - g \in G_n$ which implies $h - g + G_n \subseteq G_n$ which in turn implies $h + G_n \subseteq g + G_n$. □

Definition 9.2.10. Let G be an abelian group and (G_n) a filtration. The topology induced by this filtration is the **topology induced by the filtration** (G_n). Notice by Proposition 9.1.8 this corresponds to the topology induced by the topology base corresponding to this system of neighbourhoods.

Remark 9.2.11. The topology given in Definition 9.2.4 only exists in a setting where we have a *topological* abelian group. That of Definition 9.2.10 exists whenever we have a filtration. Later, we will work with a ring R along with an ideal I and generated a filtration $\ldots \subseteq I^2 \subseteq I \subseteq R$. Since this is a filtration, this topology exists for *any* ring R and ideal I, not just topological rings.

Lemma 9.2.12. *Let G be a abelian group and (G_n) a filtration. The abelian group G when endowed with the topology induced by the filtration is a* topological *abelian group.*

Proof. Let $\rho : G \longrightarrow G, \rho(g) = -g$ denote the inverse map. For all n we have $\rho^{-1}(g+G_n) = -g+\rho^{-1}(G_n)$ so it suffices to show for all G_n that $\rho^{-1}(G_n)$ is open, which is true as $\rho^{-1}(G_n) = -G_n = G_n$ as G_n is a group.

To see the addition map $+ : G \times G \longrightarrow G, +(a, b) = a + b$ is continuous, let $(a, b) \in g + G_n$ then $(a, b) \in (a + G_n) \times (b + G_n) \subseteq +^{-1}(g + G_n)$. □

Definition 9.2.13. Let G be a topological abelian group. A **countable fundamental system** is a filtration (G_n) which forms a neighbourhood filter (Definition 9.1.6) of 0.

Lemma 9.2.14. *If G is a topological abelian group which admits a countable fundamental system (G_n), then each G_i is both open and closed.*

Proof. Let $g \in G_i$, then $g+G_i$ is a neighbourhood of g and $g+G_i \subseteq G_i$ as G_i is a subgroup. Thus there is an open subset U such that $g \in U \subseteq G_i$ and so G_i is open. In fact, this also shows $\bigcup_{g \notin G_n}(g + G_n)$ is open, which indeed is the complement of G_i. □

If G is an abelian group with a countable fundamental system, we can define the completion as an *inverse limit*:

Definition 9.2.15. Let G be an abelian group along with a family of subgroups $\{G_n\}_{n=0}^{\infty}$. Say we have a family of homomorphisms $\{\theta_n : G_n \longrightarrow G_{n-1}\}_{n>0}$. We call the data of the triple $(G, \{G_n\}_{n=0}^{\infty}, \{\theta_n\}_{n>0})$ an **inverse system**. The inverse system is **surjective** if all the maps θ_n are.

The **inverse limit of abelian groups** corresponding to an inverse system is the abelian group $\varprojlim G_n$ whose underlying set is:

$$\varprojlim G_n := \{\text{sequences } (x_n)_n \mid x_i \in G_i,\, \theta_n(x_n) = x_{n-1}\}$$

with addition defined pointwise. The topology is the subspace topology of the product topology.

Definition 9.2.16. Given a countable fundamental system (G_n) the **completion of** G, denoted $\hat{G}$ is the inverse limit of topological abelian groups:

$$\varprojlim G/G_n$$

Remark 9.2.17. We can also define this using the language of limits of a category: for each $n > 0$ there is a morphism $G \longrightarrow G/G_{n-1}$ such that G_n maps to 0. Thus we obtain a homomorphism $\theta_n : G/G_n \longrightarrow G/G$. Let $\mathscr{J}$ be the diagram consisting of all objects G/G_n and morphisms φ_{n-1}, then consider the limit through the inclusion functor $J : \mathscr{J} \longrightarrow \underline{\text{AbGp}} : \varprojlim_{\leftarrow \mathscr{J}} J$, then $\varprojlim_{\leftarrow} G/G_n$ is such a limit. Diagramatically, this is the limit of

$$\ldots \xrightarrow{\theta_3} G/G_2 \xrightarrow{\theta_2} G/G_1 \xrightarrow{\theta_1} G/G_0$$

Lemma 9.2.18. *If G is an abelian topological group whose topology is given by a filtration, then the two notions of* completion *(Definition 9.2.15 and Definition 9.2.6) give isomorphic topological abelian groups.*

Proof. Let G be a topological group and $(G_n)_n$ a countable fundamental system of subgroup neighbourhoods. Let $\hat{G}_T$ denote the completion a la Definition 9.2.6 and let $\hat{G}_A$ denote the completion a la Definition 9.2.15. We define an explicit isomorphism $\Phi : \hat{G}_T \longrightarrow \hat{G}_A$ and inverse:

Let $(x_n)_n \in \hat{G}_T$ and denote by $\pi_n : G \longrightarrow G/G_n$ the projection. The image of $(x_n)_n$ under $\hat{\pi}_n$ is eventually constant, that is, if N is such that $\forall n, m > N$, $x_n - x_m \in G_N$, then for all $n > N$ we have $\pi(x_n) = \pi(x_{N+1})$. Denote this constant by ξ_N. Our next claim is that $(\xi_n)_n$ is an element of $\hat{G}_A$.

For each $n > 0$ the map π_n descends to a map $\theta_n : G/G_n \longrightarrow G/G_{n-1}$ which is such that $\xi_n \mapsto \xi_{n-1}$. To see this, we pick representatives $x_n, x_{n-1} \in G$ of ξ_n, ξ_{n-1} respectively and notice: $x_n - x_{n-1} \in G_n \subseteq G_{n-1}$ thus,

$$\theta_n(\xi_n) = \pi_{n-1}(x_n) = \pi_{n-1}(x_{n-1}) = \xi_{n-1}$$

Addition modulo G_n is well defined, thus we have a homomorphism from cauchy sequences to elements of $\hat{G}_A$, we now show this descends to a map from $\hat{G}_T$.

Let $(x_n)_n$ and $(y_n)_n$ be equivalent cauchy sequences and fix n, we show $\xi_n^x - \xi_n^y = 0$. Since we have a homomorphism it suffices to show $\xi_n^{x-y} = 0$. This follows immediately from the definition of two cauchy sequences being equivalent.

We define an inverse map $\hat{G}_A \longrightarrow \hat{G}_T$ by taking representatives: let $(\xi_n)_n \in \hat{G}_A$ and pick $x_n \in G$ whose image in G/G_n is ξ_n. Then we have $\theta_{n-1}(\xi_n) = \xi_{n-1}$, in other words, $x_n - x_{n-1} \in G_{n-1}$. So we have a cauchy sequence. These maps are clearly inverse to each other. □

Exercise 9.2.19. Finish the proof of Lemma 9.2.18 by proving bicontinuity of the given maps.

Notice also that we have two canonical maps $\phi_A : G \longrightarrow \hat{G}_A$ and $\phi_T : G \longrightarrow \hat{G}_T$. These fit into the follow commuting diagram:

$$\begin{array}{ccc} G & \xrightarrow{\phi_T} & \hat{G}_T \\ & \searrow^{\phi_A} & \downarrow \Phi \\ & & \hat{G}_A \end{array} \tag{44}$$

Remark 9.2.20. The definition of $\hat{G}_A$ presupposes a fixed choice of subgroups $\{G_n\}_n$ which is a drawback of this definition. One could invent a notion of *equivalent sequences of subgroups* but this is cumbersome considering the fact that the topological definition already has such a notion built into it. For instance, there may be multiple different sequences which give the same topology on G, and thus topology theory does not distinguish them.

Proposition 9.2.21. *Given three inverse systems $\{A_n\}, \{B_n\}, \{C_n\}$. If*

$$0 \longrightarrow \{A_n\} \longrightarrow \{B_n\} \longrightarrow \{C_n\} \longrightarrow 0$$

is a short exact sequence of inverse systems, then

$$0 \longrightarrow \varprojlim A_n \longrightarrow \varprojlim B_n \longrightarrow \varprojlim C_n$$

is a short exact sequence. Moreover, if $\{A_n\}$ is a surjective inverse system, then

$$0 \longrightarrow \varprojlim A_n \longrightarrow \varprojlim B_n \longrightarrow \varprojlim C_n \longrightarrow 0$$

is exact.

Proof. Let A denote $\prod_{n=0}^{\infty} A_n$ and define a map $d^A : A \longrightarrow A$ which maps $\xi_n \longrightarrow \xi_n - \theta_{n+1}(\xi_{n+1})$. Then $\ker d^A = \varprojlim A_n$. Then we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

□

so by the *snake Lemma* (see [7]) we have an exact sequence:

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to \operatorname{Coker} d^A \to \operatorname{Coker} d^B \to \operatorname{Coker} d^C \to 0$$

so it remains to show that if $\{A_n\}$ is a surjective inverse system, then $\operatorname{Coker} d^A = 0$, that is, d^A is surjective. Given $(a_n)_n \in A$ we can solve inductively $x_i - \theta_{i+1}(x_{i+1}) = a_n$.

Corollary 9.2.22. *Let $(G, \{G_n\}, \{\theta_n\})$ be an inverse system and let*

$$0 \longrightarrow G' \longrightarrow G \xrightarrow{p} G'' \longrightarrow 0$$

be a short exact sequence of groups. Then the induced sequence

$$0 \longrightarrow \hat{G}' \longrightarrow \hat{G} \longrightarrow \hat{G}'' \longrightarrow 0$$

is exact where $\hat{G}' = \varprojlim G'/(G' \cap G_n)$ and $\hat{G}'' = \varprojlim G''/p(G_n)$.

Proof. Apply Proposition 9.2.21 to the exact sequence of inverse systems

$$0 \longrightarrow \{G'/(G' \cap G_n)\} \longrightarrow \{G/G_n\} \longrightarrow \{G/p(G_n)\} \longrightarrow 0$$

□

Corollary 9.2.23. *Finite direct sum of abelian groups commutes with completion.*

Proof. By Corollary 9.2.22 we have that

$$0 \longrightarrow \operatorname{Cplt}(G') \longrightarrow \operatorname{Cplt}(G' \oplus G'') \longrightarrow \operatorname{Cplt}(G'') \longrightarrow 0$$

and

$$0 \longrightarrow \operatorname{Cplt}(G') \longrightarrow \operatorname{Cplt}(G') \oplus \operatorname{Cplt}(G'') \longrightarrow \operatorname{Cplt}(G'') \longrightarrow 0$$

are both short exact sequences, hence the two middle groups are isomorphic. □

Let G be a group and consider a filtration

$$\ldots \subseteq G_2 \subseteq G_1 \subseteq G_0 = G$$

Denote by $p : G \longrightarrow G/G_n$ be the projection, and fix a particular G_n. Then there is a finite family of subgroups of G/G_n given by

$$0 = p(G_n) \subseteq p(G_{n-1}) \subseteq \ldots \subseteq p(G_1) \subseteq p(G_0) = G/G_n$$

Thus, if $G'' := G/G_n$, elements of $\hat{G}''$ are uniquely determined by finite sequences $(x_0, ..., x_n)$ where if $j < i$, $x_i \bmod j = x_j$, that is, $(x_0, ..., x_n) = (x_n, ..., x_n)$ it follows that $\hat{G}'' \cong G''$. Moreover, $G'' \cong G/G'$ and $\hat{G}'' \cong \hat{G}/\hat{G}'$ (by Corollary 9.2.22) and so we have proven:

Lemma 9.2.24. *If G is a topological abelian group whose topology is given by a filtration $\{G_n\}_n$, then*

$$\hat{G}/\hat{G}_n \cong G/G_n$$

Taking inverse limits we have:

Lemma 9.2.25. $\hat{\hat{G}} \cong \hat{G}$

That is, $\hat{G}$ is *complete*:

Definition 9.2.26. If the canonical morphism $\phi : G \longrightarrow \hat{G}, \phi(g) = (g)_n$ is an isomorphism, then G is **complete**.

Remark 9.2.27. Notice that $\phi : G \longrightarrow \hat{G}$ need not be injective.

Remark 9.2.28. Notice by Lemma 9.2.1 that ϕ has kernel given by

$$\ker \phi = \bigcap_{n=0}^{\infty} G_n$$

9.3 I-adic completion of a ring/module

Lemma 9.3.1. *If A is a ring and $I \subseteq A$ is an ideal, then there is a filtration of the underlying abelian group of A:*

$$\ldots \subseteq I^2 \subseteq I \subseteq I^0 = A$$

and so we obtain a topological abealian group $\hat{A}$ which indeed is a topological ring.

Proof. Denote the multiplication map by $\times : A \times A \longrightarrow A, \times(a, b) = ab$. Let $ab \in x + I^n$, then $(a, b) \in (a + I^n) \times (b + I^n) \subseteq \times^{-1}(x + I^n)$. □

Definition 9.3.2. For a ring A with ideal I, the **I-adic completion** is the topological ring $\hat{A}$.

Proposition 9.3.3. *The canonical map $\phi : A \longrightarrow \hat{A}$ is continuous.*

Proof. Since for each $a \in A$ the map $T_a : A \longrightarrow A$ is a homeomorphism it suffices to prove $\phi^{-1}(\hat{I}^n)$ is open for all n, but this set is just I^n. □

For modules we have:

Definition 9.3.4. If $G = M$ is an A-module, with A a topological ring, let $I \subseteq A$ be an ideal. Take $G_n = I^n M$ and we obtain the **I-topology**. Indeed this endows M with the structure of a topological $\hat{A}$-*module* (where $\hat{A}$ is the I-adic completion). If $f : M \longrightarrow N$ is an A-module homomorphism, then $I^n f(M) \subseteq I^n N$ and so there is an induced continuous function $\hat{f} : \hat{M} \longrightarrow \hat{N}$.

There are other ways of defining the same topology on M:

Definition 9.3.5. Let (M_n) be a filtration of submodules (ie, a filtration of the underlying abelian group). If the filtration satisfies $IM_i \subseteq M_{i+1}$ then we have an **I-filtration** and if there exists $N \geq 0$ so that if $n > N$ we have $IM_n = M_{n+1}$ we have a **stable I-filtration**.

Lemma 9.3.6. *The topology given by any stable I-filtration agrees with the I-topology.*

Proof. For arbitrary n we have $M_{n+N+1} = I^n M_{N+1} \subseteq I^n M$. Conversely, for arbitrary m we have $I^m M = I^m M_0 \subseteq M_m$. □

A rational number $q \in \mathbb{Q}$ is uniquely determined by its base 10 representation, where we allow for negative powers, $q = \sum_{j=0}^{n} a_j 10^{-j}$ for some $n \in \mathbb{Z}$. This representation generalises to the real numbers by allowing j to be arbitrarily small:

$$\mathbb{R} = \Big\{ \sum_{j=0}^{\infty} a_j 10^{-j} \mid a_j \in \mathbb{Z} \Big\}$$

Another formulation of the real numbers is given by equivalence classes of Cauchy sequences. Both these means of constructing the real numbers from the rational numbers can be generalised.

Consider the polynomial ring $k[x]$ where k is a field. Let $\mathfrak{m}$ denote the maximal ideal $(x) \subseteq k[x]$ and consider the completion $\widehat{k[x]}$ of $k[x]$ with respect to (x). An element of this is an equivalence class of a cauchy sequences of elements in $k[x]$ represented by $(a_0, a_1, ...)$ say. For each i, reducing a_i modulo (x^i) yields an element $\hat{a}_i \in k[x]$, doing this for all i yields an element $\hat{a}_0 + \hat{a}_1 x + \hat{a}_2 x^2 + \ldots \in k[\![x]\!]$. Moreover, this element is independent of choice of representative $(a_0, a_1, ...)$, for if $(b_0, b_1, ...)$ was another representative we would have for all $i > 0$ that $b_i - a_i = 0 \bmod (x)^i$. Thus we have a well defined map $\widehat{k[x]} \longrightarrow k[\![x]\!]$. It is easy to see this is an isomorphism:

Lemma 9.3.7. *The completion of $k[x]$ at the ideal (x) is isomorphic to $k[\![x]\!]$.*

9.4 The Artin-Rees Lemma

Definition 9.4.1. A **graded ring** is a ring A together with a countably infinite family of subgroups $\{A_n\}_{n\geq 0}$ of the underlying group of A such that $A = \bigoplus_{n\geq 0} A_n$ and $A_n A_m \subseteq A_{n+m}$ for all $n, m \geq 0$. Thus A_0 is a ring and each A_n is an A-module.

If A is a graded ring then a **graded A-module** is an A-module along with with a countably infinite family of submodules $\{M_n\}_{n\geq 0}$ such that $M = \bigoplus_{n\geq 0} M_n$ and $A_n M_m \subseteq M_{m+n}$, thus each M_n is an A_0-module.

We denote $\bigoplus_{n>0} A_n$ by A_+.

Definition 9.4.2. Let M, N be graded A-modules, a **homomorphism of graded A-modules** $f : M \longrightarrow N$ is a homomorphism of modules such that $f(M_n) \subseteq N_n$ for all $n \geq 0$.

Lemma 9.4.3. *For a graded ring A, the following are equivalent:*

- *A is Noetherian,*

- *A_0 is Noetherian and A is a finitely generated as an A_0-algebra.*

Proof. Let A be Noetherian. Then $A_0 \cong A/A_+$ and so is Noetherian. Let A_+ be generated as an ideal by $\alpha_1, ..., \alpha_m$ which we may assume to be homogeneous and of degrees $k_1, ..., k_m$ respectively (notice each $k_i > 0$). Denote by A' the A_0-subalgebra of A generated by $\alpha_1, ..., \alpha_m$. We proceed with the second claim by showing $A_n \subseteq A'$ by induction on n. Clearly, $A_0 \subseteq A'$. Now say $n > 0$. Let $a \in A_n \setminus A_0$ so that $a \in A_+$. We can write $a = \sum_{i=0}^{m} a_i \alpha_i$. We have that $\deg(a_i) = n - k_i$ (where we take $a_i = 0$ if $n - k_i < 0$). The result then follows by the inductive hypothesis.

The other implication follows from Hilbert's Basis Theorem. □

Notation 9.4.4. Given a (not necessarily graded) ring A and an ideal I we denote the graded ring $\bigoplus_{n\geq 0} I^n$ by I^*. If M is an A-module and M_n is an I-filtration then $M^* = \bigoplus_{n\geq 0} M_n$ is a graded I^*-module.

If A is Noetherian and $\alpha_1, ..., \alpha_n$ are generators for I then $I^* = A[\alpha_1, ..., \alpha_n]$ and is Noetherian (by Lemma 9.4.3). The next main result we are heading towards is:

Proposition 9.4.5. *Given a short exact sequence of finitely generated A-modules, with A Noetherian:*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

the following sequence is also exact:

$$0 \longrightarrow \hat{M'} \longrightarrow \hat{M} \longrightarrow \hat{M''} \longrightarrow 0$$

To prove this, we want to lean on Corollary 9.2.22, however, that Corollary used a fixed choice of filtration, and the definitions of $\hat{M'}, \hat{M''}$ also used a different fixed choice, do these different choices give isomorphic modules?

The topology used to construct $\hat{M''}$ is induced by the filtration $(I^n M'')_n$ which is equal to $(p(I^n M))_n$ (by definition of module homomorphism) but the topology used to construct $\hat{M'}$ is that induced by the filtration $(I^n M)_n$ and Corollary 9.2.22 uses the sequence $(M' \cap I^n M)_n$ instead. The proof of Proposition 9.4.5 thus reduces to showing these two topologies are equivalent, which is an application of the following Theorem (the fact that $M'/I^n M'$ is a surjective inverse system is clear, and considering the equivalence we are about to prove, this is sufficient):

Theorem 9.4.6. *Let A be a Noetherian ring, $I \subseteq A$ an ideal, M a finitely-generated A-module and M' a submodule of M. Then the filtrations $(I^n M')_n$ and $\left((I^n M) \cap M'\right)_n$ induce equivalent topologies.*

To prove Theorem 9.4.6 we will need:

Lemma 9.4.7 (Artin-Rees Lemma)**.** *Let A be a Noetherian ring, $I \subseteq A$ an ideal, M a finitely generated A module, and $(M_n)_n$ a stable I-filtration of M. If M' is a submodule of M, then $(M' \cap M_n)_n$ is a stable I-filtration of M'.*

for which we need:

Lemma 9.4.8. *Let A be Noetherian, and M a finitely generated A-module with an I-filtration $(M_n)_n$. Then the following are equivalent:*

1. *M^* is a finitely generated A^*-module (Notation 9.4.4),*
2. *the filtration $(M_n)_n$ is I-stable.*

Proof of Lemma 9.4.8. Each M_n is a finitely generated module over a Noetherian ring and is therefore itself Noetherian, and thus finitely generated. It follows that $Q_n := \bigoplus_{j=0}^{n} M_j$ is finitely generated. The A^*-submodule generated by Q_n can be explicitly written as

$$Q_n \oplus \bigoplus_{j=1}^{\infty} I^j M_n$$

which we denote by M_n^*. This is a finitely generated I^*-module (as M_n is a finitely generated A-module) and so we have an ascending chain

$$M_1^* \subseteq M_2^* \subseteq \dots$$

which eventually stabilises if and only if there exists N such that for all $m > N$, we have $IM_m = M_{m+1}$, which is another way of stating the result.

Converse? □

Proof of Lemma 9.4.7. We have $I(M' \cap M_n) \subseteq IM' \cap IM_n \subseteq M' \cap M_{n+1}$ and hence $(M' \cap M_n)_n$ is an I-filtration. Hence it defines a graded I^*-module which is a submodule of M'^* and therefore finitely generated (as I^* is Noetherian). The result follows from Lemma 9.4.8. □

Proof of Theorem 9.4.6. By Lemma 9.3.6 we have that any two stable I-filtrations induce equivalent topologies. The result then follows by Lemma 9.4.7. □

9.5 Krull's Theorem

Since there is a homomorphism $\phi : A \longrightarrow \hat{A}$, we can consider $\hat{M}$ as an A-module and thus form $\hat{A} \otimes_A M$. In the case that M is a finitely generated module over a noetherian ring, this agrees with the completion:

Proposition 9.5.1. *For any ring A, if M is finitely-generated then $\hat{A} \otimes_A M \longrightarrow \hat{M}$ is injective. Moreover, this is an isomorphism if A is Noetherian.*

Proof. Since M is finitely generated there is a short exact sequence

$$0 \longrightarrow N \longrightarrow F \longrightarrow M \longrightarrow 0$$

We construct the commutative diagram

$$\begin{array}{ccccccccc} & & \hat{A} \otimes N & \longrightarrow & \hat{A} \otimes F & \longrightarrow & \hat{A} \otimes M & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & \hat{N} & \longrightarrow & \hat{F} & \xrightarrow{\delta} & \hat{M} & \longrightarrow & 0 \end{array}$$

By Corollary 9.2.23 we have that β is an isomorphism. Since the bottom row is exact, δ is surjective, it follows from these two facts that γ is injective. If A is noetherian, then N is also finitely generated, thus α is surjective. It then follows from the four Lemma that γ is injective. □

Notation 9.5.2. Let $I, J \subseteq A$ be ideals and let $\hat{A}$ be the I-completion. We denote by $\hat{J}$ the ideal generated by the image of $A \longrightarrow \hat{A}$.

Lemma 9.5.3. *Let A be a ring and $I \subseteq A$ an ideal, and $n > 0$, denote the homomorphism $A/I^n \longrightarrow \hat{A}/\hat{I}^n$ by ψ. Let $J \subseteq A/I^n$ be an ideal. Then the image of J under ψ is equal to $\hat{J}$.*

Proof. Consider elements of the completion as equivalence classes of cauchy sequences. Let $(b_n)_n$ be a cauchy sequence representing an element of $\hat{J}$. Elements of $\hat{J}$ are given by linear combinations of elements in $\psi(J)$ with scalars given by elements in $\hat{A}/\hat{I}$, thus we can assume that each $b_i \in J$. There exists N such that for all $m > N$ we have $b_N - b_m \in I^n$. Consider the sequence $(b_N, b_N, ...)$, we claim this is equivalent to $(b_n)_n$. Indeed, $(b_N - b_n)_n$ eventually consists of elements in I^n and so is eventually 0, establishing the claim. □

Proposition 9.5.4. *If A is Noetherian, $\hat{A}$ its I-adic completion, then*

1. $\hat{I} \cong \hat{A} \otimes_A I$,
2. $(I^n)\hat{} = (\hat{I})^n$,
3. $I^n/I^{n+1} \cong \hat{I}^n/\hat{I}^{n+1}$,
4. $\hat{I}$ *is contained in the Jacobson radical of* $\hat{A}$.

Proof. (1): Apply Proposition 9.5.1.

(2): Using (1) applied to I and that tensor product commutes with finite products:

$$(I^n)\hat{} \cong \hat{A} \otimes I^n \cong (\hat{A} \otimes I)^n \cong (\hat{I})^n$$

(3): By Lemma 9.2.24 we have $A/I^{n+1} \cong \hat{A}/\hat{I}^{n+1}$. Lemma 9.5.3 then implies $I^n/I^{n+1} \cong \hat{I}^n/\hat{I}^{n+1}$.

(4): $\hat{A}$ is complete in its $\hat{I}$-adic topology (using (2)). So, for $x \in \hat{I}$ we have

$$(1-x, 1-x, 1-x, ...)(1, 1+x, 1+x+x^2, ...) = (1-x, 1-x^2, 1-x^3, ...) = (1,1,1,...) - (x, x^2, x^3, ...)$$

and $(x, x^2, x^3, ...)$ is equivalent to 0, so $1 - x$ in $\hat{A}$ is a unit. That is, x is an element of the Jacobson radical of $\hat{A}$. □

Remark 9.5.5. In the proof of part (4) of 9.5.4 we have used the statement that for any ring R and any element $x \in R$ we have that x is in the jacobson radical if and only if $1 - xy$ is a unit for all $y \in R$. The reason why we only consider $1 - x$ is because we claim that $\hat{I}$ is contained within the jacobson radical and we know that $\hat{I}$ is itself an ideal, so it suffices to show $1 - x$ is a unit for all $x \in \hat{I}$.

Remark 9.5.6. The proof that $I^n/I^{n+1} \cong \hat{I}^n/\hat{I}^{n+1}$ leaves this map implicit and uses the limit definition of completion. In the special case where $(A, \mathfrak{m})$ is a local ring we can show that $A/\mathfrak{m}^n \cong \hat{A}/\hat{\mathfrak{m}}^n$ using the cauchy sequence definition of completion directly: indeed the composition $A \longrightarrow \hat{A} \longrightarrow \hat{A}/\hat{\mathfrak{m}}^n$ is surjective with kernel $\mathfrak{m}^n$, and so descends to an isomoprhism $A/\mathfrak{m}^n \longrightarrow \hat{A}/\hat{\mathfrak{m}}^n$.

Proposition 9.5.7. *Let A be a Noetherian local ring and $\mathfrak{m}$ its maximal ideal. Then the $\mathfrak{m}$-adic completion of A at $\mathfrak{m}$ is a local ring with maximal ideal $\hat{\mathfrak{m}}$.*

Proof. We have that $\hat{A}/\hat{\mathfrak{m}} \cong A/\mathfrak{m}$ is a field and thus $\hat{\mathfrak{m}}$ is maximal. It follows from (4) of Proposition 9.5.4 that $\hat{\mathfrak{m}}$ is contained within the jacobson radical $\mathfrak{J}$ which itself is the intersection of all prime ideals of $\hat{A}$ and so is contained in $\mathfrak{m}$. Thus $\hat{\mathfrak{m}} = \mathfrak{J}$, which implies $\hat{\mathfrak{m}}$ is the unique maximal ideal of $\hat{A}$. □

We classify the kernel of the canonical map $M \longrightarrow \hat{M}$, this will be another application of Theorem 9.4.6.

Theorem 9.5.8 (Krull's Theorem)**.** *Let A be a Noetherian ring, $I \subseteq A$ an ideal, M a finitely generated A-module, and $\hat{M}$ the I-completion of M. Then the kernel $E = \bigcap_{n=0}^{\infty} I^n M$ of the group homomorphism $\phi : M \longrightarrow \hat{M}$ consists of those $x \in M$ annihilated by some element of the set $1 + I$.*

Proof. Consider the space E with topology given by the sequence $((I^nM) \cap E)_n$ (which are all equal to E). This is a space where the only neighbourhood of 0 is all of E itself. By Theorem 9.4.6 we have that this topology coincides with the topology given by $(I^nE)_n$. We thus have $IE = E$. Since M is finitely generated and A is noetherian, E is also finitely generated and so it follows from the Cayley-Hamilton Theorem (see [**?**]) and the fact that $IE = E$ that $(1 + \alpha)E = 0$ for some $\alpha \in I$.

Conversely, if $(1 + \alpha)x = 0$ then

$$x = -\alpha x = \alpha^2 x = ... \in \bigcap_{n=1}^{\infty} I^n M = E$$

□

Corollary 9.5.9. *Let A be a Noetherian domain, I a proper ideal of A. Then $\bigcap_{n\geq 0} I^n = 0$.*

Proof. $1 + I$ contains no zero divisors nor the element 0. □

Corollary 9.5.10. *Let A be a Noetherian ring, I an ideal of A contained in the Jacobson radical and let M be a finitely generated A-module. Then the I-topology of M is Hausdorff, ie, $\bigcap_{n\geq 0} I^n M = 0$.*

Proof. Since I is contained in the jacobson radical, every element of $1 + I$ is a unit. □

As an important special case:

Corollary 9.5.11. *Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, M a finitely generated A-module. Then the $\mathfrak{m}$-topology of M is Hausdorff. In particular, the $\mathfrak{m}$-topology of A is Hausdorff.*

Corollary 9.5.12. *Let A be a Noetherian ring, $\mathfrak{p}$ a prime ideal of A. Then the intersection of all $\mathfrak{p}$-primary (Definition 2.3.1) ideals of A is the kernel of $A \longrightarrow A_{\mathfrak{p}}$.*

Proof. Let $\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$ be the maximal ideal of $A_{\mathfrak{p}}$. By Corollary 2.3.10 we have that all the $\mathfrak{m}$-primary ideals of $A_{\mathfrak{p}}$ are contained between $\mathfrak{m}^n$ and $\mathfrak{m}$ for some n. Thus by Corollary 9.5.11 the intersection of all the $\mathfrak{m}$-primary ideals of the $A_{\mathfrak{p}}$ is 0. These ideals lift to the $\mathfrak{p}$-primary ideals of A. Let $l : A \longrightarrow A_{\mathfrak{p}}$ denote the localisation map, we compute $\ker l$ where by Corollary 9.5.11 we have $0 = \bigcap_{n\geq 0} \mathfrak{m}^n$:

$$\ker l = l^{-1}(0) = l^{-1}(\bigcap_{n\geq 0} \mathfrak{m}^n) = l^{-1}(\bigcap_{\mathfrak{m}\text{-primary}} I) = \bigcap_{\mathfrak{p}\text{-primary}} I$$

where the equality labelled $*$ follows from . □

9.6 The completion of a Noetherian ring is Noetherian

We aim to prove:

Theorem 9.6.1. *Let A be a Noetherian ring and I an ideal of A. The I-completion $\hat{A}$ of A is Noetherian.*

The important objects working behind the scenes are:

Definition 9.6.2. Let A be a ring and I an ideal of A. Define:

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

This is a graded ring, multiplication is defined as $[x]_n[y]_m = [xy]_{n+m}$.

Similarly, if M is an A-module and $\{M_n\}_n$ an I-filtration of M, define:

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

which is a graded $G_I(A)$-module. Let $G_n(M)$ denote M_n/M_{n+1}.

Theorem 9.6.1 will follow from the following Proposition:

Proposition 9.6.3. *Let A be a ring, I an ideal of A, M an A-module, $\{M_n\}_n$ an I-filtration of M. Suppose that A is complete in the I-topology and that M is Hausdorff in its filtration topology (ie, that $\bigcap_{n\geq 0} M_n = 0$). Suppose also that $G(M)$ is a finitely generated $G(A)$-module. Then M is a finitely generated A-module.*

We will need the following two lemmas:

Lemma 9.6.4. *Let A be a Noetherian ring, I an ideal of A. Then*

1. *$G_I(A)$ is Noetherian,*
2. *$G_I(A)$ and $G_{\hat{I}}(\hat{A})$ are isomorphic as graded rings,*
3. *if M is a finitely generated A-module and $\{M_n\}_n$ is a stable I-filtration of M, then $G_I(M)$ is a finitely generated graded $G_I(A)$-module.*

Proof. (1) Since A is Noetherian, I is finitely generated, say by $x_1, ..., x_n$. Let $\bar{x}_i$ be the image of x_i in I/I^2. Then $G_I(A) = (A/I)[\bar{x}_1, ..., \bar{x}_n]$. To see this, consider an element of $I^n/I^{n+1} \subseteq G_I(A)$ which can be written as $\sum_{|\Lambda|=m} \alpha_\Lambda \bar{x}^\Lambda$ where $\Lambda = (\lambda_1, ..., \lambda_n)$, where $\bar{x}_\Lambda = \bar{x}_1^{\lambda_1} ... \bar{x}_n^{\lambda_n}$. Since $\lambda_1 + \ldots + \lambda_n = m$ we have that each $\bar{x}_i$ has degree 1, that is, $\bar{x}_i \in I/I^2$ by the definition of multiplication in this ring.

(2) Follows from Proposition 9.5.4.

(3) There exists $N \geq 0$ such that $M_{N+n} = I^n M_N$ for all $n \geq 0$, hence $G(M)$ is generated as an A-module by $\bigoplus_{n\leq N} G_n(M)$. Each $G_n(M) = M_n/M_{n+1}$ is Noetherian (being finitely generated modules over a Noetherian ring) and annihilated by I, hence this is finitely generated as an A/I-module. Hence $G(M)$ is finitely generated as a $G(A)$-module. □

Lemma 9.6.5. *Let $\phi : A \longrightarrow B$ be a homomorphism of filtered groups (Definition 9.2.8) and let $G(\phi) : G(A) \longrightarrow G(B)$, $\hat{\phi} : \hat{A} \longrightarrow \hat{B}$ be the induced homomorphism of the associated graded and completed groups respectively. Then*

1. *if $G(\phi)$ is injective then so is $\hat{\phi}$,*
2. *if $G(\phi)$ is surjective then so is $\hat{\phi}$.*

Proof. Let $\alpha_m : A/A_m \longrightarrow B/B_m$ be the homomorphism induced by ϕ. Consider the commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n/A_{n+1} & \longrightarrow & A/A_{n+1} & \longrightarrow & A/A_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle G_n(\phi)} & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} & & \\ 0 & \longrightarrow & B_n/B_{n+1} & \longrightarrow & B/B_{n+1} & \longrightarrow & B/B_n & \longrightarrow & 0 \end{array}$$

which by the snake Lemma induces the exact sequence

$$0 \to \ker G_n(\phi) \to \ker \alpha_{n+1} \to \ker \alpha_n \to \operatorname{coker} G_n(\phi) \to \operatorname{coker} \alpha_{n+1} \to \operatorname{coker} \alpha_n \to 0 \tag{45}$$

It's easy to see that $G(\phi)$ injective implies that $G_n(\phi)$ is injective for all n, so in this case, $\ker G_n(\phi) = 0$, and $G_0(\phi) : A/A_1$ is the same morphism as α_1, so $\ker \alpha_1 = 0$. The exact sequence then implies $\ker \alpha_2 = 0$, proceeding by induction we have $\ker \alpha_n = 0$ for all n. Inverse limits is a left exact functor (Proposition 9.2.21) and so the first result follows.

A drawing of $G(\phi)$ might look like:

$$\begin{array}{ccccccccc} \ldots & \bigoplus & A_3/A_4 & \bigoplus & A_2/A_3 & \bigoplus & A_1/A_2 & \bigoplus & A_0/A_1 \\ & & \downarrow{\scriptstyle G_4(\phi)} & & \downarrow{\scriptstyle G_3(\phi)} & & \downarrow{\scriptstyle G_2(\phi)} & & \downarrow{\scriptstyle G_1(\phi)} \\ \ldots & \bigoplus & B_3/B_4 & \bigoplus & B_2/B_3 & \bigoplus & B_1/B_2 & \bigoplus & B_0/B_1 \end{array}$$

and so $G(\phi)$ surjective implies each $G_n(\phi)$ is surjective. Thus $\operatorname{coker} G_n(\phi) = 0$. Using (45) it then follows that each α_n is surjective, and thus $\hat{\phi}$ is surjective. □

We now move to the proof of Proposition 9.5.7, the essence of the proof will be to begin with generators of $G(M)$ as a $G(A)$-module and then pick representatives of these which lie inside M, in fact these representatives generate M as an A-module. We will construct a finitely generated free A-module F and homomorphism $\phi : F \longrightarrow M$ which fits into the commutative diagram (of abelian groups):

$$\begin{array}{ccc} F & \xrightarrow{\phi} & M \\ \downarrow & & \downarrow \\ \hat{F} & \xrightarrow{\hat{\phi}} & \hat{M} \end{array}$$

the proof will be completed by showing ϕ is surjective.

Proof of Proposition 9.5.7. Pick a finite set of generators $\{\xi_1, ..., \xi_r\}$ of $G(M)$ and assume these have been split into their homogeneous components (that is, assume each ξ_i is homogeneous). Denote the degree of ξ_i by $n(i)$ and pick a representative $x_i \in M_{n(i)}$ of each ξ_i. Consider the I-filtration on A given by $(I^{k-n(i)})_k$ for each $n(i)$ (where $I^{k-n(i)} = A$ if $k - n(i) \leq 0$) and consider $F := \bigoplus_{i=1}^r A$. Let m be the least integer such that there exists $1 \leq i \leq r$ such that $m - n(i) \geq 0$ then F admits an I-filtration

$$\bigoplus_{i=1}^r A = \bigoplus_{i=1}^r I^{m-n(i)} \subseteq \bigoplus_{i=1}^r I^{m+1-n(i)} \subseteq \bigoplus_{i=1}^r I^{m+2-n(i)} \subseteq \ldots$$

We now construct a surjective homomorphism of $G(A)$-modules $G(F) \longrightarrow G(M)$. Let $\phi : F \longrightarrow M$ be the homomorphism which maps the i^{th} copy of 1 to x_i. This is a homomorphism of filtered groups as:

$$\begin{aligned} \phi\Big(\bigoplus_{i=1}^r I^{m+k-n(i)}\Big) &= I^{m+k-n(1)}x_1 + \ldots + I^{m+k-n(r)}x_r \\ &\subseteq I^{m+k-n(1)}M_{n(1)} + \ldots + I^{m+k-n(r)}M_{n(r)} \\ &\subseteq M_{m+k} \subseteq M_k \end{aligned}$$

Furthermore, ϕ is surjective: if $m \in G(M)$ then $m = \alpha_1\xi_1 + \ldots \alpha_r\xi_r$ where each $\alpha_i \in G(A)$ is of degree $k - n(i)$ (with $\alpha_i = 0$ if $k - n(i) < 0$). So for each non-zero α_i we have

$$\phi(\alpha_i) = \alpha_i\xi_i$$

and so the image of the sum of the non-zero α_i map to m. We now apply Lemma 9.6.5 to deduce that $\hat{\phi}$ is surjective, we consider the commuting diagram of group homomorphisms

$$\begin{array}{ccc} F & \xrightarrow{\phi} & M \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\beta} \\ \hat{F} & \xrightarrow{\hat{\phi}} & \hat{M} \end{array}$$

Now, F is a free A-module and A is complete, it follows that F is complete (by commuting finite direct sum with completion, Lemma 9.2.23), thus α is an isomorphism. Moreover, M Hausdorff and so β is injective. It then follows that ϕ is surjective. □

Corollary 9.6.6. *With the hypotheses of Proposition 9.6.3, if $G(M)$ is a Noetherian $G(A)$-module, then M is a Noetherian A-module.*

Proof. Let $M' \subseteq M$ be a submodule, we show M' is finitely generated. Let $M'_n = M' \cap M_n$, then (M'_n) is an I-filtration of M', and the embedding $M'_n \longrightarrow M_n$ gives rise to an injective homomorphism $M'_n/M'_{n+1} \longrightarrow M_n/M_{n+1}$, hence an embedding $G(M') \longrightarrow G(M)$. Since $G(M)$ is Noetherian, $G(M')$ is finitely generated, also M' is Hausdorff, since $\bigcap_{n\geq 0} M'_n \subseteq \bigcap_{n\geq 0} M_n = 0$, hence by Proposition 9.5.7 we have that M' is finitely generated as an A-module. □

At long last, we can prove the main result of this Section:

Theorem 9.6.7. *If A is a Noetherian ring, I an ideal of A, then the I-completion $\hat{A}$ of A is Noetherian.*

Proof. We know that $G_I(A) \cong G_{\hat{I}}(\hat{A})$ is Noetherian. Now apply Corollary 9.6.6 to the complete ring $\hat{A}$, taking $M = \hat{A}$. □

Corollary 9.6.8. *If A is a Noetherian ring, the power series ring $A[[x_1, ..., x_n]]$ in n variables is Noetherian. In particular, $k[[x_1, ..., x_n]]$ (k a field) is Noetherian.*

9.7 Hensel's Lemma

The goal of this Section is to prove Hensel's Lemma (Lemma 9.7.4). We begin with an observation concerning the division algorithm for polynomials in one variable:

Lemma 9.7.1. *Let A be an arbitrary ring, $f, g \in A[x]$, with $\deg g > \deg f$, and assume f is monic. Then the division algorithm g/f can still be performed yielding $g = \alpha f + \beta$ with $\deg \beta < \deg = f$, moreover, the polynomials α, β are unique in the sense that if α', β' are such that $\deg \beta' < \deg f$ and $g = \alpha' f + \beta'$ then $\alpha = \alpha', \beta = \beta'$.*

Proof. That the division algorithm can still be performed is simply the observation that the only divisions which occur in the algorithm are with 1 in the denominator as f is monic.

Now we prove the uniqueness claim. We have

$$g = \alpha f + \beta, \qquad \text{and} \qquad g = \alpha' f + \beta' \tag{46}$$

and so $0 = (\alpha - \alpha')f + \beta - \beta'$. This implies that $\beta - \beta'$, which satisfies $\deg(\beta - \beta') < \deg f$, is a multiple of monic f. Thus $\beta - \beta' = 0$.

Now $0 = (\alpha - \alpha')f$. The leading coefficinet of $(\alpha - \alpha')f$ is 0 and also is $\alpha - \alpha'$ by monotonicity of f. □

We make another observation: say $(f_1, f_2, ...)$ is a Cauchy sequence in A (with respect to the $\mathfrak{m}$-adic topology), then since A is complete, there exists $a \in A$ such that $(f_n)_n$ and $(a)_n$ belong to the same equivalence class, which is to say $(f_n - a)_n \longrightarrow 0$. Say $b \in A$ was also such that $(f_n - b)_n \longrightarrow 0$, then for all $i \geq 0$ we have $f_n - a, f_n - b \in \mathfrak{m}^i \Longrightarrow b - a \in \mathfrak{m}^i$, in other words:

$$(f_n - a)_n - (f_n - b)_n = (b - a)_n \longrightarrow 0 \tag{47}$$

This means that $b - a \in \bigcap_{i=0}^{\infty} \mathfrak{m}$ which, if A is Noetherian, is 0. Thus:

Lemma 9.7.2. *In a complete, Noetherian ring, Cauchy sequences have admit limits which are unique.*

Notation 9.7.3. If $f \in A[x]$ is a polynomial and $(A, \mathfrak{m})$ a local ring, we denote by $\bar{f}$ the image of f in $(A/\mathfrak{m})[x]$.

We are now ready to prove:

Lemma 9.7.4 (Hensel's Lemma)**.** *Let $(A, \mathfrak{m})$ be a Noetherian, local, complete ring, and $f \in A[x]$ a monic polynomial of degree n and $G, H \in (A/\mathfrak{m})$ monic, coprime, polynomials of respective degrees $r, n-r$ such that $\bar{f} = GH$. Then there exists monic polynomials $g, h \in A[x]$ respectively of degree $r, n-r$ such that $f = gh$.*

Proof. We lean on the completeness of A: say we have two sequences $(g_1, g_2, ...), (h_1, h_2, ...)$ of monic polynomials $g_i, h_i \in A[x]$ satisfying:

1. For all $i > 0 : \deg g_i = r, \deg h_i = n - r$,
2. for all $i > 0 : f \equiv g_i h_i (\mathrm{mod}\, \mathfrak{m}^i)$,
3. for all $i < j : g_i \equiv g_j (\mathrm{mod}\, \mathfrak{m}^i), h_i \equiv h_j (\mathrm{mod}\, \mathfrak{m}^i)$.

For a general polynomial $q \in A[x]$ we will denote the i^{th} coefficient of q by q_i. Condition (1) implies the existence of sequences $(g_{1k}, g_{2k}, ...), (h_{1k,2k}, ...)$ of coefficients of g, h respectively. Moreover, (3) implies these sequences are Cauchy sequences, so since A is a complete and Noetherian, by Lemma 9.7.2 we have limits $a_k, b_k \in A$ of $(g_{1k}, g_{2k}, ...), (h_{1k,2k}, ...)$ respectively.

We then define

$$g = a_0 + a_1 x + \ldots + a_{r-1} x^{r-1} + x^r \qquad \text{and} \qquad h = b_0 + b_1 x + \ldots + b_{n-r-1} x^{n-r-1} + x^{n-r} \tag{48}$$

which we claim is such that $f = gh$. Let $\phi : A \longrightarrow \hat{A}$ denote the canonical map from a ring to its completion. To show $f = gh$ it suffices to show the coefficients $(f - gh)_i$ for $0 \leq i \leq n$ are all 0, and to show this, it suffices to show $\phi\big((f-gh)_i\big) = 0$ as A is Noetherian (and so ϕ has trivial kernel).

We make a calculation:

$$\begin{aligned}
\phi\big((f-gh)_i\big) &= \phi\big((f)_i\big) - \phi\big((gh)_i\big) \\
&= \phi\big(f_i\big) - \sum_{j=0}^{i} \phi(a_j)\phi(b_{i-j})\big) \\
&= (f_i - \sum_{j=0}^{i} g_{1j} h_{1,i-j}, f_i - \sum_{j=0}^{i} g_{2j} h_{2i-j}, ...), \text{ by construction of } a_j, b_{i-j}
\end{aligned}$$

and so $\phi\big((f-gh)_i\big) = 0$ by (2).

We now move onto constructing $(g_1, g_2, ...), (h_1, h_2, ...)$ satisfying (1), (2), (3).

We construct g_k, h_k satisfying (1), (2) inductively and show they satisfy the following uniqueness claim: if g'_k, h'_k are such that $\overline{g'_k} = G, \overline{h'_k} = H$ and $f \equiv g'_k h'_k (\mathrm{mod}\, \mathfrak{m}^k)$ then $g'_k \equiv g_k, h'_k = h'_k (\mathrm{mod}\, \mathfrak{m}^k)$. This uniqueness claim implies (3).

For the base case, just pick arbitrary representatives for the coefficients of F, G in A (making sure to pick 1 for $1 + \mathfrak{m}$) and build g_1, h_1 from these choices. These clearly satisfy the required properties.

Now assume we have g_k, h_k for some fixed $k \geq 1$ and assume these polynomials satisfy all the requirements. Set $\Delta = f - g_k h_k$, which by the inductive hypothesis is an element of $\mathfrak{m}^k[x]$. We notice that

$$f \equiv \Delta + g_k h_k (\mathrm{mod}\, \mathfrak{m}^{k+1}) \tag{49}$$

and so the goal is to write $\Delta + g_k h_k (\mathrm{mod}\, \mathfrak{m}^{k+1})$ as a product $g_{k+1} h_{k+1}$. Since F, G are coprime, there exists polynomials $\alpha, \beta \in A[x]$ such that

$$1 \equiv \alpha g_k + \beta h_k (\mathrm{mod}\, \mathfrak{m}[x]) \tag{50}$$

Multiplying both sides by Δ we have

$$\Delta \equiv \Delta\alpha g_k + \Delta\beta h_k (\mathrm{mod}\, \mathfrak{m}^{k+1}[x]) \tag{51}$$

For pedagogical reasons we make the following observation, however this next paragraph can be skipped entirely and the proof still holds: since $\Delta \in \mathfrak{m}^k$ we have that $\Delta^2 \in \mathfrak{m}^{2k} \subseteq \mathfrak{m}^{k+1}$ and so we can now write

$$\begin{aligned} f &\equiv \Delta + \Delta\alpha g_k + \Delta\beta h_k + \Delta\alpha\Delta\beta \\ &\equiv (g_k + \Delta\alpha)(h_k + \Delta\beta)(\mathrm{mod}\, \mathfrak{m}^{k+1}[x]) \end{aligned}$$

which makes it look like we have achieved our goal. However we do not have a handle on the degree of $g_k + \Delta\alpha$ nor $h_k + \Delta\beta$ and so we use the division algorithm to replace $\Delta\alpha, \Delta\beta$ by polynomails of degree $< r, n - r$.

We know that g_k, h_k are monic, so we divide $\Delta\alpha$ by h_k to produce $\gamma, \epsilon \in A[x]$ such that

$$\Delta\alpha = \gamma h_k + \epsilon \tag{52}$$

We can now write

$$\Delta \equiv (\gamma h_k + \epsilon) g_k + \Delta\beta h_k \tag{53}$$

$$\equiv \epsilon g_k + (\gamma g_k + \Delta\beta) h_k (\mathrm{mod}\, \mathfrak{m}^{k+1}[x]) \tag{54}$$

We set $h_{k+1} := h_k + \epsilon$ and $g_{k+1} := g_k + \gamma g_k + \Delta\beta$. Thus, calculating $\mathrm{mod}\, \mathfrak{m}^{k+1}$, we have:

$$g_{k+1} h_{k+1} \equiv (g_k + \gamma g_k + \Delta\beta)(h_k + \epsilon) \tag{55}$$

$$\equiv g_k h_k + \epsilon g_k + (\gamma g_k + \Delta\beta) h_k + (\gamma g_k + \Delta\beta)\epsilon \tag{56}$$

$$\equiv \big(g_k + (\gamma g_k + \Delta\beta)\big)\big(h_k + \epsilon\big) + (\gamma g_k + \Delta\beta)\epsilon \tag{57}$$

We now make a few final observations and we have reduced to proving the uniqueness claim. First, since $\Delta \in \mathfrak{m}^k[x]$ it follows from (52) that $0 \equiv \gamma h_k + \epsilon (\mathrm{mod}\, \mathfrak{m}^k[x])$ and so by the uniqueness part of the division algorithm (Lemma 9.7.1) we have that $\gamma, \epsilon \in \mathfrak{m}^k[x]$. Thus $\gamma g_k \in \mathfrak{m}^k[x]$ and so $\gamma g_k + \Delta\beta \in \mathfrak{m}^k[x]$ and so $(\gamma g_k + \Delta\beta)\epsilon \in \mathfrak{m}^{2k}[x] \subseteq \mathfrak{m}^{k+1}[x]$. Combining this with (57) we have

$$g_{k+1} h_{k+1} \equiv \big(g_k + (\gamma g_k + \Delta\beta)\big)\big(h_k + \epsilon\big) \pmod{\mathfrak{m}^{k+1}[x]} \tag{58}$$

Moreover, by the division algorithm we have $\deg \epsilon < n - r$ which implies $\deg(\epsilon g_k) < n$. Also, f, g_k, h_k are all monic and so Δ (which equals $f - g_k h_k$) has degree $< n$. We have from (53) that

$$\Delta - \epsilon g_k \equiv (\gamma g_k + \Delta\beta) h_k \pmod{\mathfrak{m}^{k+1}[x]} \tag{59}$$

where the left hand side is a degree $< n$ polynomial. Thus $\deg(\gamma g_k + \Delta\beta) < r$. Considering this, we now have that g_{k+1}, h_{k+1} are monic and of respective degrees $r, n - r$. It now remains to show uniqueness.

This is the easiest part of the proof. We would truly be re-writing verbatim what is in [9] so we do not reproduce it here. □

10 Kähler Differentials

Let k be a field and let A, B, C be k-algebras. Assume we had morphisms $f : A \longrightarrow B, g : C \longrightarrow B$ along with a pair of **lifts along** g: $h_1, h_2 : C \longrightarrow A$ of f, that is, assume the following diagram commutes for $i = 1, 2$.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \overset{h_i}{\nwarrow} & \uparrow g \\ & & C \end{array} \tag{60}$$

Then $h_1 - h_2$ is a morphism which factors through $\ker f$. Moveover, notice that if $a, a' \in A$ are such that $f(a) = f(a')$ then for any $x \in \ker f$ we have $ax - a'x = (a - a')x$, thus, if $(\ker f)^2 = 0$ then $(a - a')x = 0$ and so $\ker f$ becomes an $f(A)$-module and in fact a C-module by commutativity of (60) (as $g(C) \subseteq f(A)$).

Set $H = h - h'$, let $c, d \in C$ and consider the following calculation.

$$\begin{aligned} H(cd) &= (h - h')(cd) \\ &= h(cd) - h'(cd) \\ &= h(c)h(d) - h'(c)h'(d) \end{aligned}$$

also,

$$\begin{aligned} cH(d) + dH(c) &= c(h - h')(d) + d(h - h')(c) \\ &= c\big(h(d) - h'(d)\big) + b\big(h(c) - h'(c)\big) \\ &= ch(d) - ch'(d) + dh(c) - dh'(c) \end{aligned}$$

Now, $\ker f$ is a C-module and so for any $e, e' \in C$ we have $eh(e') = g(e)h(e') = h(e)h(e') = h'(e)h(e')$. Thus we can continue our calculation,

$$\begin{aligned} ch(d) - ch'(d) + dh(c) - dh'(c) &= h(c)h(d) - h(c)h'(d) + h'(c)h(c) - h'(d)h'(c) \\ &= h(c)h(d) - h'(c)h'(d) \end{aligned}$$

and so the two calculations agree. What we have shown is that $H = h - h'$ is a *k-derivation of C to* $\ker f$.

Definition 10.0.1. A **derivation of A to M** (where A is a ring and M is an A-module) is a function $D : A \longrightarrow M$ satisfying

- $\forall a_1, a_2 \in A, D(a_1 + a_2) = D(a_1) + D(a_2)$, that is D is additive,
- $\forall a_1, a_2 \in A, D(a_1 a_2) = a_1 D(a_2) + a_2 D(a_1)$, that is D satisfies the **Leibniz rule**.

If moreover A is a k-algebra via a morphism $f : k \longrightarrow A$ and $D \circ f = 0$ then D is a k-derivation.

Earlier we proved the first half of the following.

Lemma 10.0.2. *Let $f : A \longrightarrow B$ be a morphism of k-algebras with $(\ker f)^2 = 0$ and assume there exist k-algebra morphisms $h_1, h_2 : C \longrightarrow A, g : C \longrightarrow B$ such that the following diagram commutes.*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \overset{h_i}{\nwarrow} & \uparrow{\scriptstyle g} \\ & & C \end{array} \tag{61}$$

Then $h - h'$ is a k-derivation. Moreover, if h is a lift of f along g then so is $f + D$ for any k-derivation D.

Definition 10.0.3. Denote the set of derivations from A to M by $\mathrm{Der}(A, M)$ and the set of k-derivations by $\mathrm{Def}_k(A, M)$.

Let A be a k-algebra and consider the morphism $\mu : A \otimes_k A \longrightarrow A$ given by $\mu(x \otimes y) = xy$. Let $I = \ker \mu$ denote the kernel of μ and notice that we have a short exact sequence

$$0 \longrightarrow I/I^2 \longrightarrow (A \otimes_k A)/I \xrightarrow{\mu'} A \longrightarrow 0 \tag{62}$$

where μ' is the map on the quotient induced by μ. We introduce some notation, let $\Omega_{A/k}$ denote I/I^2 and B denote $(A \otimes_k A)/I$. So we have a short exact sequence

$$0 \longrightarrow \Omega_{A/k} \longrightarrow B \xrightarrow{\mu'} A \longrightarrow 0 \tag{63}$$

In fact, this sequence is split; the morphisms

$$\begin{aligned} \lambda_1 : A &\longrightarrow B & \qquad \lambda_2 : A &\longrightarrow B \\ a &\longmapsto a \otimes 1 & \qquad a &\longmapsto 1 \otimes a \end{aligned}$$

are such that $\mu'\lambda_i = \mathrm{id}_A$. In fact, $\Omega^2_{A/k} = 0$ and λ_1, λ_2 are lifts of μ' along id_A:

$$\begin{array}{ccc} B & \xrightarrow{\mu'} & A \\ & \overset{\lambda_i}{\nwarrow} & \uparrow{\scriptstyle \mathrm{id}_A} \\ & & A \end{array} \tag{64}$$

and so $\lambda_1 - \lambda_2$ is a k-derivation of A into $\Omega_{A/k}$.

Now we introduce an A-module M. Say we had a k-derivation $D : A \longrightarrow M$. Define the following k-algebra $A * M$:

Definition 10.0.4. The underlying set of $A * M$ is $A \oplus M$, but the multiplication is defined by

$$\begin{aligned} A * M \otimes A * M &\longrightarrow A * M \\ (a, m) \otimes (a', m') &\longmapsto (aa', am' + a'm) \end{aligned}$$

Notice that considering M as a subalgebra of $A * M$ we have $M^2 = 0$. Next, define the morphism of k-algebras:

$$\begin{aligned} \varphi : A \otimes_k A &\longrightarrow A * M \\ a \otimes a' &\longmapsto (aa', aDa') \end{aligned}$$

Notice that if $x \otimes y \in I$ then $\varphi(x \otimes y) = (xy, xDy) = (0, xDy)$ and so φ maps I into M. Lastly, since $M^2 = 0$ we the map φ decends to a map $f : I/I^2 \longrightarrow M$. This map is important because for any $a \in A$ we have

$$\begin{aligned} f((\lambda_1 - \lambda_2)(a)) &= f(a \otimes 1 - 1 \otimes a) \\ &= aD(1) + D(a) \\ &= D(a) \end{aligned}$$

(The last line uses the general fact that for any k-derivation $D(1) = D(1) + D(1)$) which implies $D(1) = 0$).

Lastly, we have for any $a, a' \in A$ that $a \otimes a' = (a \otimes 1)(1 \otimes a - a \otimes 1) + aa' \otimes 1$ and so $a \otimes a' - a(\lambda_1 - \lambda_2)(a') \mod I^2$. That is to say, $\{\lambda_1 - \lambda_2)(a) \mid a \in A\}$ generates $\Omega_{A/k}$. It follows that the above f is the unique morphism such that $D = f(\lambda_1 - \lambda_2)$. We have proven everything except for naturality of the following.

Proposition 10.0.5. *There is a natural (in M) bijection*

$$\mathrm{Hom}_A(\Omega_{A/k}, M) \cong \mathrm{Der}_k(A, M) \tag{65}$$

References

[1] Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag New York 1977

[2] Stacks Project `https://stacks.math.columbia.edu/`

[3] Commutative ring theory *Cambridge University Press Online publication date:June 2012 Print publication year:1987*

[4] Hensel's Lemma `http://therisingsea.org/notes/HenselsLemma.pdf`

[5] Commutative Algebra, *O. Zariski, P. Samuel* D. Van Nostrand Company (Canada), LTD 1958

[6] Commutative Algebra, *Atiyah, MacDonald* Addison-Wesley Publishing Company 1969

[7] W. Troiani, *Introduction to Homological Algebra (note).*

[8] T. Friedrich, *Dirac Operations in Riemannian Geometry* Friedrich

[9] D. Murfet, *Hensel's Lemma* `http://therisingsea.org/notes/HenselsLemma.pdf`