Y3 Revision - Rings!

Apiros3

First Version : Mar 11, 2025
Last Update : Jan 29, 2025

Contents

1 Introduction

1.1 Basic Definitions

In this note we assume rings are associative, commutative, and unitary. Ring homomorphisms are also unitary (sending 0_R to 0_S).

Definitions to cover : TODO - ring - product of rings - subring - integral domain - field - homomorphism of rings - module over a ring - finitely generated module over a ring - ideal - ideal generated by a set - product of ideals - intersection of a family of ideals - sum of a family of ideals - coprime ideals - submodule - intersection of a family of submodules - sum of a family of submodiules - submodule generated by a set - quotient module - direct sum of modules over a rings - homomorphisms of modules over a ring - prime ideal - maximal ideal - ring of polynomials over a ring - zero divisor - unit - chinese remainder theorem - euclidian division - fraction field over a domain

Definition 1.1.1. *Let R be a ring. Let $I \subseteq R$ is an ideal in R. I is **proper** if $I \neq R$ and I is **principal** if it can be generated by a single element.*

Definition 1.1.2. *An element $r \in R$ is **nilpotent** if there exists an integer $n \geq 1$ such that $r^n = 0$.*

Definition 1.1.3. *A ring R is **local** if it has a single maximal ideal $\mathfrak{m}$. In this case, every element in $R \backslash \mathfrak{m}$ is a unit.*

Definition 1.1.4. *The **prime ring** of a ring R is the image of the unique (unitary) homomorphism $\mathbb{Z} \to R$.*

Definition 1.1.5. *The **zero divisor** of a ring R is an element $r \in R$ such that there exists a $r' \in R\backslash\{0\}$ with $r \cdot r' = 0$. If R is not the zero-ring, 0 is always a zero divisor of R.*

Definition 1.1.6. *A **domain** is a ring R with the property that the set of zero divisors consists only of 0. (In the case it is commutative, we call it an **integral domain**).*

Definition 1.1.7. *A **Unique Factorization Domain** (UFD) or a factorial ring is a domain R which has a unique factorization of non-zero elements with irreducible elements up to permutation and multiplication by units.*

Definition 1.1.8. *Given rings R and T, T is said to be an R-algebra if there is a homomorphism of rings $R \to T$.*

Note that an R-algebra T carries the structure of an R-module using the map provided by the homomorphism.

Definition 1.1.9. *Given $\phi_1 : R \to T_1$ and $\phi_2 : R \to T_2$ to be two R-algebras, a homomorphism of R-algebras is a homomorphism of rings $\lambda : T_1 \to T_2$ such that $\lambda \circ \phi_1 = \phi_2$.*

Definition 1.1.10. *An R-algebra $\phi : R \to T$ is said to be **finitely generated** if there exists an integer $k \geq 0$ and a surjective homomorphism of R-algebras $R[x_1, \ldots, x_k] \to T$ (evaluation of variables) where the polynomial is R if $k = 0$.*

Proposition 1.1.11. *Given that $R \to T$ is a finitely generated R-algebra and $T \to W$ is also a finitely generated T-algebra, the composed map from $R \to W$ is a finitely generated R-algebra.*

Proof. TODO!! □

Definition 1.1.12. *Let M be a R-module and $S \subseteq M$. Then,*

$$\operatorname{Ann}_M(S) = \{r \in R \mid rm = 0 \forall m \in S\}$$

The set $\operatorname{Ann}_M(S)$ is an ideal of R and is called the ***annihilator*** *of S.*

Definition 1.1.13. *A* ***poset (partially ordered set)*** *is a set equipped with an operator $\leq$ which is reflexive, transitive and antisymmetric. It is called a* ***total order*** *if it is also connex. We call the operator a* ***partial order****.*

Definition 1.1.14. *Let $T \subseteq S$. An element $s \in S$ is an* ***upper bound*** *of T if for any $t \in T$, $t \leq s$. An element $s \in S$ is a* ***maximal element*** *of S if for any $t \in S$, $s \leq t$ if and only if $s = t$. Similarly, $s \in S$ is a* ***minimal element*** *if $t \leq s$ if and only if $t = s$.*

Remark 1.1.15. Given a poset S and $T \subseteq S$, the relation $\leq$ on S restricted to elements of T gives a poset on T.

Proposition 1.1.16 (Zorn's Lemma (Equivalently, AC))**.** *Let S be a poset. If every $T \subseteq S$ that is totally ordered (with restriction of $\leq$ on T) has an upper bound in S, then there exists a maximal element in S.*

Proof. TODO!! (set theory stuff, ask cs phil) □

Proposition 1.1.17. *Let R be a ring and $I \subseteq R$ be a proper ideal. Then, at least one of the maximal ideals of R contains I.*

Proof. Let S be the set of all proper ideals containing I. Give a partial order on S by inclusion. For any $T \subseteq S$ with T totally ordered, then T has an upper bound $\bigcup_{J \in T} J$ is a proper ideal containing I. It is proper as otherwise we have $1 \in J$ for some $J \in T$. Thus, by Zorn's Lemma, there exists a maximal element $\mathfrak{m}$ in S.

By definition, whenever $\mathfrak{m} \subseteq J$ and J is a proper ideal containing I, we have $\mathfrak{m} = J$. If J does not contain I, as $\mathfrak{m}$ contains I, $\mathfrak{m} \not\subseteq J$. Hence, $\mathfrak{m}$ is maximal and contains I. □

1.2 Helper Theorems (To be Omitted in Main Notes)

Theorem 1.2.1 (Chinese Remainder Theorem)**.** *Let R be a ring and $I_1, \ldots, I_k$ be ideals of R. Let*

$$\phi : R \to \prod_{i=1}^{k} R/I_i$$

be the ring homomorphism such that $\phi(r) = \prod_{i=1}^{k}(r + I_i)$ for all $r \in R$. Then, $\ker(\phi) = \bigcap_{i=1}^{k} I_i$.

The map ϕ is surjective if and only if $I_i + I_j = R$ for every $i, j \in \{1, \ldots, k\}$ with $i \neq j$. In such case, $\bigcap_{i=1}^{k} I_i = \prod_{i=1}^{k} I_i$

Proposition 1.2.2 (Euclidian Division for Polynomial Rings)**.** *The usual.*

Theorem 1.2.3. *Let A be a ring. Then we have a bijection*

$$\{P \subseteq A \mid P \text{ is a prime ideal}\} \simeq \{\phi : A \to K \mid K \text{ is a field}\}/\simeq$$

where the quotient on the right side equates two fields K_1, K_2 if there are ring homomorphisms between the following arrows. Note this is an equivalence class, transitivity comes by taking intersections.

$$\begin{tikzcd} & & K_1 \\ A \arrow[r] & K \arrow[ur] \arrow[dr] & \\ & & K_2 \end{tikzcd}$$

Proof. Consider the map $P \mapsto [\mathrm{Frac} \circ q_P]$ where q_P is the quotient map by P. Also consider the map which takes $[\phi] \mapsto \mathrm{Ker}(\phi)$. We claim these maps are inverses of another, thus is a bijection. Note the latter map is well defined as the kernel of a map from A into a field is preserved by composition of homomorphisms between fields (as such maps are uniquely induced by maps from 1) and is a prime ideal.

For the first direction, the map takes P to $\mathrm{Ker}(\mathrm{Frac} \circ q_P) = P$. For the other direction, we take $[\phi]$ to $[\mathrm{Frac} \circ q_{\mathrm{Ker}(\phi)}]$. The map below using first isomorphism theorem and extension of maps into Frac shows equivalence.

$$\begin{tikzcd} A \arrow[rr, "\phi"] \arrow[d, "q_{\mathrm{Ker}(\phi)}"'] & & K \\ A/\mathrm{Ker}(\phi) \arrow[rr] \arrow[urr, dashed] & & \mathrm{Frac}(A/\mathrm{Ker}(\phi)) \arrow[u, dashed] \end{tikzcd}$$

$\square$

2 Localisation

2.1 Localisation of Rings

Definition 2.1.1. *A subset S of R is said to be **multiplicative** or a **multiplicative set** if $1 \in S$ and $xy \in S$ whenever $x \in S$ and $y \in S$.*

Equivalently, it is a submonoid of the multiplicative monoid $(R, \times)$. For instance, the set $\{1, f, f^2, \dots\}$ for a fixed $f \in R$ is a multiplicative set.

Definition 2.1.2. *Let $S \subseteq R$. Consider the set $R \times S$ and define a relation $\sim$ on it, where $(a, s) \sim (b, t)$ if and only if there exists a $u \in S$ such that $u(ta - sb) = 0$. One can check this is an equivalence relation.*

*Define the **localisation** of R at S, denoted R_S or RS^{-1} to be $(R \times S)/\sim$. Given $a \in R$ and $s \in S$, write a/s for the image of (a, s) in RS^{-1}.*

Define

$$+ : RS^{-1} \times RS^{-1} \to RS^{-1}, (a/s, b/t) \mapsto (at + bs)/(st)$$

and

$$\cdot : RS^{-1} \times RS^{-1} \to RS^{-1}, (a/s, b/t) \mapsto (ab)/(st)$$

These are both well defined with any choice of representative.

The set RS^{-1} with the operations above give a structure of a ring with identity element $1/1$, 0-element $0/1$ and a natural map from R to RS^{-1} via $r \mapsto r/1$. By construction, for any $r \in S$, $r/1$ is invertible with $1/r$.

Note the fact that if R is a domain, the fraction field of R is the ring $R(R\backslash 0)^{-1}$.

Proposition 2.1.3. *If R is a domain, for any $S \subseteq R$, RS^{-1} is also a domain.*

Proof. Suppose $0 \notin S$ and $(a/s)(b/t) = 0$ where $a, b \in R$ and $s, t \in S$. Then, we have $u(ab) = 0$ for some $u \in S$. As R is a domain, $ab = 0$, giving $a = 0$ or $b = 0$. Specifically, $a/s = 0/1$ or $b/t = 0/1$.

If $0 \in S$, the equivalence relation equates all elements, making the localisation a zero-ring. This is a domain. $\square$

Definition 2.1.4. *Let M be a R-module. Let $S \subseteq R$ be multiplicative. Define a relation $\sim$ on $M \times S$ by $(a, s) \sim (b, t)$ if and only if there exists a $u \in S$ such that $u(ta - sb) = 0$. We define **localised module** MS^{-1} or M_S to be $(M \times S)/\sim$ with*

$$+ : MS^{-1} \times MS^{-1} \to MS^{-1}, (a/s, b/t) \mapsto (ta + sb)/(st)$$

and

$$\cdot : RS^{-1} \times MS^{-1} \to MS^{-1}, (a/s, b/t) \mapsto (ab)/(st)$$

which give MS^{-1} the structure of a RS^{-1} module. The 0 element is $0/1$ and carries the structure of a natural map $R \to RS^{-1}$ and a natural map of R-modules $M \to MS^{-1}$ given by $m \mapsto m/1$

Lemma 2.1.5. *Let $\phi : R \to R'$ be a ring homomorphism and $S \subseteq R$ be a multiplicative set. Suppose $\phi(S)$ consists of units in R'. Then, there is a unique ring homomorphism ϕ_S such that $\phi_S(r/1) = \phi(r)$ for all $r \in R$*

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d] & R' \\
RS^{-1} \arrow[ur, dashed, "\phi_S"'] &
\end{tikzcd}$$

Proof. Define the map $\phi_S : R_S \to R'$ by $\phi_S(a/s) = \phi(a)(\phi(s))^{-1}$ for all $a \in R$ and $s \in S$. We first show it is well defined. Suppose $(a, s) \sim (b, t)$. Then,

$$\phi_S(b/t) = \phi(b)(\phi(t))^{-1}$$

and noting that $u(ta - sb) = 0$ for some $u \in S$,

$$\phi(u)(\phi(t)\phi(a) - \phi(s)\phi(b)) = 0$$

As $\phi(u)$ is a unit, multiplying it away we have $\phi(t)\phi(a) - \phi(s)\phi(b) = 0$, or $\phi(t)\phi(a) = \phi(s)\phi(b)$. Consequently, $\phi_S(a/s) = \phi(a)(\phi(s)^{-1}) = \phi(b)(\phi(t)^{-1}) = \phi_S(b/t)$. Noting that ϕ_S is also a homomorphism, we also confirm $\phi_S(r/1) = \phi(r)$ for all $r \in R$.

For uniqueness, if $\phi'_S : R_S \to R'$ is another such map, for every $r \in R$ and $t \in S$,

$$\begin{aligned}
\phi'_S(r/t) &= \phi'_S((r/1)(t/1)^{-1}) \\
&= \phi'_S(r/1)\phi'_S(t/1)^{-1} \\
&= \phi_S(r)\phi_S(t)^{-1} \\
&= \phi_S(r/t)
\end{aligned}$$

□

Lemma 2.1.6. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let M be an R-module, and for all $s \in S$ the map*

$$[s]_M : M \to M, m \mapsto sm$$

is an isomorphism. Then there is a unique structure of an R_S module on M such that $(r/1)m = rm$ for all $m \in M$ and $r \in R$.

Proof. Follows a similar structure to above. The left-multiplication operator being an isomorphism lets us define suitable inverses for elements of S. Specifically, we define $(r/s)m$ to be $[s]_M^{-1}(r/m)$ and extend from here. □

Lemma 2.1.7. *Let R be a ring and $f \in R$. Define $S = \{1, f, f^2, \dots\}$. Then R_S is finitely generated as an R-algebra.*

Proof. Consider the R-algebra $T = R[x]/(fx - 1)$. Note that T is generated as an R-algebra by $1 + (fx - 1)$ and $x + (fx - 1)$. Define $\phi : R[x] \to R_S$ by the homomorphism of R-algebras extneded from $\phi(x) = 1/f$. Then $\phi(fx - 1) = 0$ and thus ϕ induces a homomorphism of R-algebras $\psi : T \to R_S$ by $g + (fx - 1) \mapsto \phi(g)$.

As the image of f in T is invertible by construction, by 2.1.5 there is a unique homomorphism of R-algebras $\lambda : R_S \to T$ that extends from

$$R \to T, 1 \mapsto 1 + (fx - 1)$$

The map $\psi \circ \lambda : R_S \to R_S$ with elements of the form $r/1$ is the identity, thus the entire map is the identity by uniqueness. Specifically, λ is injective. λ is also surjective, as it maps to the generators of T. Consequently, T and R_S are isomorphisms.

$$\begin{tikzcd}
R[x] \arrow[rr, "\phi"] \arrow[d, "q_{(fx-1)}"'] & & R_S \arrow[dll, dashed, bend left=10, "\lambda"] \\
T = R[x]/(fx-1) \arrow[urr, dashed, bend left=10, "\psi"] & &
\end{tikzcd}$$

□

Proposition 2.1.8. *If R is a ring and $\phi : N \to M$ is a homomorphism of R-modules, there is a unique homomorphism of R_S modules $\phi_S : N_S \to M_S$ such that $\phi_S(n/1) = \phi(n)/1$ for all $n \in N$. If $\psi : M \to T$ is another homomorphism of R-modules, then $(\psi \circ \phi)_S = \psi_S \circ \phi_S$.*

Proof. The second part is straightforward. For the first, note that the map is given by $\phi_S(n/m) = \phi(n)/m$, and uniqueness follows. $\square$

Proposition 2.1.9. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let I be an ideal in R. Then,*

$$R_S/I_S \simeq (R/I)_S$$

Given an R-module M and a submodule $N \subseteq M$,

$$M_S/N_S \simeq (M/N)_S$$

Proof. Consider the map $\phi : R_S \to (R/I)_S$ by $(r/s) \mapsto (q(r)/s)$ where q is the quotient map. This is a well defined and surjective map with kernel I_S. The proof follows by the first isomorphism theorem. The case for modules is similar. $\square$

Definition 2.1.10. *Let*

$$\cdots \to M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

*be a sequence of R-modules with homomorphisms mapping between them such that $d_{i-1} \circ d_i = 0$ for all $i \in \mathbb{Z}$. We call such a sequence a **chain complex** of R-modules. We say that the complex is **exact** if $\mathrm{Ker}(d_{i-1}) = \mathrm{Im}(d_i)$ for all $i \in \mathbb{Z}$.*

Lemma 2.1.11. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let*

$$\cdots \to M_i \xrightarrow{d_i} M_{i-1} \xrightarrow{d_{i-1}} \cdots$$

be an chain complex of R-modules. If this is exact, the chain

$$\cdots \to (M_i)_S \xrightarrow{(d_i)_S} (M_{i-1})_S \xrightarrow{(d_{i-1})_S} \cdots$$

is also exact. If the second chain is exact for every maximal ideal $\mathfrak{m}$ of R, the first chain is exact.

Proof. We show the first statement first. Let $m/s \in (M_i)_S$. Suppose that $(d_i)_S(m/s) = 0$. Then, $(d_i)_S(m/1) = d_i(m)/1 = 0$. Thus $u \cdot d_i(m) = 0$. Then $um \in \mathrm{Im}(d_{i+1})$ as the first sequence is exact. Thus, there exists a $p \in M_{i+1}$ such that $d_{i+1}(p) = um$, thus $(d_{i+1})_S(p/us) = m/s$.

For the latter, we show the contrapositive. Suppose the first chain complex is not exact. Then, there exists a $i \in \mathbb{Z}$ such that

$$\mathrm{Ker}(d_i)/\mathrm{Im}(d_{i+1}) \neq 0$$

Take a non-zero element a from this set. Let $\mathfrak{m}$ be a maximal ideal containing $\mathrm{Ann}(a)$, which exists as $1 \notin \mathrm{Ann}(a)$ (a is non-zero). Then, $\mathrm{Ker}(d_i)/\mathrm{Im}(d_{i+1}) \neq 0$ as else there is a $u \in R\backslash\mathfrak{m} \subseteq R\backslash\mathrm{Ann}(a)$ with $u \cdot a = 0$ which is a contradiction. By the first isomorphism theorem, there is a natural isomorphism

$$\mathrm{Ker}(d_i)_\mathfrak{m}/\mathrm{Im}(d_{i+1})_\mathfrak{m} \simeq (\mathrm{Ker}(d_i)/\mathrm{Im}(d_{i+1}))_\mathfrak{m} \not\simeq 0$$

$\square$

Lemma 2.1.12. *Let $\phi : R \to T$ be a ring homomorphism. Let $S \subseteq R$ be a multiplicative set. By Lemma 2.1.5 there is a unique homomorphism of rings $\phi' : R_S \to T_{\phi(S)}$ with $\phi'(r/1) = \phi(r)/1$. Viewning $T_{\phi(S)}$ as an R_S module and T as an R-module, there is a unique isomorphism of R_S modules $\mu : T_S \simeq T_{\phi(S)}$ such that $\mu(a/1) = a/1$ for all $a \in T$ and $\mu \circ \phi_S = \phi'$.*

$$\begin{tikzcd}
R \arrow[r] \arrow[d, "\phi"'] & R_S \arrow[d, dashed, "\phi'"] \arrow[dr, "\phi_S"] & \\
T \arrow[r] & T_{\phi(S)} & T_S \arrow[l, dashed, "\mu"]
\end{tikzcd}$$

Proof. Define $\mu(a/s) = a/\phi(s)$ for every $a \in T$ and $s \in S$. Given $a/s = b/t$, there is a $u \in S$ such that

$$u \cdot (t \cdot a - s \cdot b) = 0$$

The action by R onto T is defined by ϕ, so equivalently,

$$\phi(u)(\phi(t)a - \phi(s)b) = 0$$

meaning $a/\phi(s) = b/\phi(t)$ by definition, meaning μ is well-defined. By construction, μ is a map of R_S modules and is also surjective. To see μ is injective, if $\mu(a/s) = 0/1$ for some $a \in T$ and $s \in S$, there is a $u \in S$ such that $\phi(u)a = 0$. Thus, $u \cdot a = 0$ in T, giving $a/1 = 0$ in T_S, implying $a/s = 0$. Thus μ is bijective.

The identity $\mu \circ \phi_S = \phi'$ follows by noting that composition of homomorphisms are homomorphisms and $\mu \circ \phi_S(1/1) = \phi'(1/1)$. ☐

Remark 2.1.13. Taking the identity map from R to R, we see that localisation of a ring R as viewed as a ring or a module over itself, we get the same R_S-module.

Proposition 2.1.14. *Let R be a ring and $\mathfrak{p}$ be a prime ideal in R. Then $R\backslash\mathfrak{p}$ is a multiplicative set.*

Proof. $1 \notin \mathfrak{p}$ as $\mathfrak{p}$ is prime, and if $x, y \notin \mathfrak{p}$ then $xy \notin \mathfrak{p}$ as it is prime. ☐

Notation 2.1.15. Write $R_\mathfrak{p}$ to denote $R_{R\backslash\mathfrak{p}}$ and if M is an $R-$module, write $M_\mathfrak{p}$ to mean $M_{R\backslash\mathfrak{p}}$. Note that the notation in unambiguous as prime ideals never contain 1.

Simiarly, if $\phi : M \to N$ is a homomorphism of R-modules, write $\phi_\mathfrak{p}$ for $\phi_{R\backslash\mathfrak{p}} : M_\mathfrak{p} \to N_\mathfrak{p}$

Proposition 2.1.16. *If $\phi : U \to R$ is a homomorphism of rings and $\mathfrak{p}$ is a prime ideal of R, then ϕ naturally induced a homomorphism of rings $U_{\phi^{-1}(\mathfrak{p})} \to R_\mathfrak{p}$*

Proof. Noting that $\phi(U\backslash\phi^{-1}(\mathfrak{p})) \subseteq R\backslash\mathfrak{p}$, we can give a map $(a/s) \mapsto (\phi(a)/\phi(s))$. ☐

Notation 2.1.17. The above map is often written as $\phi_\mathfrak{p}$.

Lemma 2.1.18. *Let R be a ring and $S \subseteq R$ be a multiplicative set. Let $\lambda : R \to R_S$ be the natural ring homomorphism. Then, there is a bijective correspondence with the prime ideals of R_S and $\mathfrak{p}$ of R such that $\mathfrak{p} \cap S = \emptyset$.*

The corresponding prime ideal of R_S is $\iota_{\mathfrak{p},S}(\mathfrak{p}_S) \subseteq R_S$ where $\iota_\mathfrak{p} : \mathfrak{p} \to R$ is the inclusion map (which is a homomorphism of R-modules).

Furthermore, $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S

Proof. We first prove that given any ideal I, $\iota_{I,S}(I_S)$ is the ideal generated by $\lambda(I)$ in R_S. Note that by definition, $\iota_{I,S}(I_S)$ consists of all elements $a/s \in R_S$ for $a \in I$ and $s \in S$. Thus this is an ideal of R_S which contains $\lambda(I)$. As $a/s = (a/1)(1/s)$ every element is contained in the ideal generated by $\lambda(I)$.

We show next bijective correspondence. First, we claim that if J is a proper ideal of R_S, then $\lambda^{-1}(J) \cap S = \emptyset$. Otherwise, choose $s \in \lambda^{-1}(J)$ such that $s \in S$. Then, $\lambda(s) = s/1 \in J$, which is a unit, contradicting with J being a proper ideal. As preimages of prime ideals are prime, λ^{-1} maps prime ideals J of R_S into prime ideals of R such that $\lambda^{-1}(J) \cap S = \emptyset$. To show injectivity of λ^{-1} when restricted to prime ideals, we claim that if J is an ideal of R_S, the ideal generated by $\lambda(\lambda^{-1}(J))$ in R_S is J. Inclusion is obvious. If $a/s \in J$, $a/1 \in J$, meaning $a \in \lambda^{-1}(J)$. As $a/s = (a/1)(1/s)$ is in the ideal generated by $\lambda(\lambda^{-1}(J))$.

For the other direction, we first show that if $\mathfrak{p}$ is a prime ideal of R such that $\mathfrak{p} \cap S = \emptyset$, $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is a prime ideal of R_S. For this, consider the exact sequence of R-modules

$$0 \to \mathfrak{p} \to R \xrightarrow{q} R/\mathfrak{p} \to 0$$

where q is the quotient map. By Lemma 2.1.11, the sequence of R_S modules

$$0 \to \mathfrak{p}_S \to R_S \xrightarrow{q_S} (R/\mathfrak{p})_S \to 0$$

is also exact. By Lemma 2.1.12, $(R/\mathfrak{p})_S$ is isomorphic as an R_S module to $(R/\mathfrak{p})_{q(S)}$. By the First isomorphism theorem, $(R/\mathfrak{p})_S \simeq (R_S)/(\mathfrak{p}_S)$, giving $(R_S)/(\mathfrak{p}_S) \simeq (R/\mathfrak{p})_{q(S)}$. By assumption, $R/\mathfrak{p}$ is a domain, and noting $0 \notin q(S)$ as $S \cap \mathfrak{p} = \emptyset$, $(R/\mathfrak{p})_{q(S)}$ is a domain. Consequently, $\mathfrak{p}_S$ is a prime ideal. Finally, to show that $\iota_{p,S}(\cdot_S)$ is injective when restricted to prime ideals $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$, we show $\lambda^{-1}(\iota_{p,S}(\mathfrak{p}_S)) = \mathfrak{p}$ if $\mathfrak{p} \cap S = \emptyset$. Noting that $\iota_{\mathfrak{p},S}(\mathfrak{p}_S)$ is the ideal generated by $\lambda(\mathfrak{p})$ in R_S, we have $\lambda^{-1}(\iota_{\mathfrak{p},S}(\mathfrak{p}_S)) \supseteq \mathfrak{p}$. Taking $a \in \lambda^{-1}(\iota_{\mathfrak{p},S}(\mathfrak{p}_S))$, $a/1 = b/s$ for some $b \in \mathfrak{p}$ and $s \in S$. So, for some $u \in S$, $u(sa - b) = 0$, or $usa = ub$. As $ub \in \mathfrak{p}$ and $us \notin \mathfrak{p}$, it follows $a \in \mathfrak{p}$ from the fact $\mathfrak{p}$ is a prime ideal. $\square$

Remark 2.1.19. As a consequence of Lemma 2.1.18, $\operatorname{Spec}(\lambda)(\operatorname{Spec}(R_S))$ consists of prime ideals in $\operatorname{Spec}(R)$ that do not meet S. Given that $S = \{1, f, f^2, \dots\}$, we have

$$\operatorname{Spec}(\lambda)(\operatorname{Spec}(R_S)) = D_f(R)$$

Corollary 2.1.20. *Given that $\mathfrak{p} \in \operatorname{Spec}(R_S)$ then λ induces a natural homomorphism of rings $R_{\lambda^{-1}(\mathfrak{p})} \to (R_S)_{\mathfrak{p}}$. This homomorphism is an isomorphism.*

Proof. Define the map ϕ with $\phi(r/s) = ((r/1)/(s/1))$. It is straightforward that this map is both injective and surjective. $\square$

Corollary 2.1.21. *The nilradical of R is the intersection of every prime ideal.*

Proof. Following the same proof as before, if we have a nilpotent element, it is part of every prime ideal (by quotienting by the prime). Let R be a ring and $r \in R$ is an element that is not nilpotent. Let $S = \{1, r, r^2, \dots\}$. R_S is non-zero as $r/1 \neq 0/1$ by nilpotence. Let $\mathfrak{q}$ be a prime ideal of R_S. By Lemma 2.1.18, this ideal corresponds to a prime ideal $\mathfrak{p}$ of R such that $r \notin \mathfrak{p}$ (doesn't intersect with S). $\square$

Corollary 2.1.22. *Let R be a ring and $\mathfrak{p} \subseteq R$ be a prime ideal. The ring $R_{\mathfrak{p}}$ is local. If $\mathfrak{m}$ is the maximal ideal of $R_{\mathfrak{p}}$ and $\lambda : R \to R_{\mathfrak{p}}$ is the natural homomorphism of rings, $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$.*

Proof. By Lemma 2.1.18, prime ideals of $R_{\mathfrak{p}}$ correspond to prime ideals of R that don't meet $R \backslash \mathfrak{p}$. Noting that this correspondence is given by monotonic maps on inclusion, every prime ideal of $R_{\mathfrak{p}}$ is contained in the prime ideal corresponding to $\mathfrak{p}$. Let I be a maximal ideal of $R_{\mathfrak{p}}$. As I is contained in the prime ideal contained in the prime ideal corresponding to $\mathfrak{p}$, it must concide by maximality. Thus the prime ideal $\mathfrak{m}$ corresponding to $\mathfrak{p}$ is maximal and is the only maximal ideal. By the correspondence map, $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$. $\square$

3 Prime Ideals

3.1 Nilradical

Definition 3.1.1. *Let R be a ring. The* ***nilradical*** *of R is the set of nilpotent elements of R. We say that R is* ***reduced*** *if its nilradical is $\{0\}$.*

Proposition 3.1.2. *Let R be a ring. The nilradical of R is the intersection of all the prime ideals of R.*

Proof. Let $f \in R$ be a nilpotent element. Let $I \subseteq R$ be a prime ideal. Some power of f is zero, which is an element of I. Specifically, $f + I \in R/I$ is a zero-divisor. As I is prime, R/I is a domain, meaning $f + I = I$. Thus, $f \in I$, meaning f is in the intersection of all the prime ideals of R.

Conversely, suppose $f \in R$ is not nilpotent. Let S be the set of proper ideals I of R such that for all $n \geq 1$, $f^n \notin I$. Note that $(0) \in S$. Giving a partial order on S by inclusion, every total ordered subset in S has an upper bound by union. By Zorn's Lemma, S has a maximal element $\mathfrak{m}$.

We claim $\mathfrak{m}$ is a prime ideal. Then, as $\mathfrak{m} \in S$, $f^n \notin \mathfrak{m}$ for any $n \geq 1$. Specifically, as $f \notin \mathfrak{m}$, f does not lie in the intersection of the prime ideals of R.

To show that $\mathfrak{m}$ is prime, suppose we take $x, y \in R$ and $x, y \notin \mathfrak{m}$. It suffices to show that $xy \notin \mathfrak{m}$. Note first that both $(x) + \mathfrak{m}$ and $(y) + \mathfrak{m}$ are ideals which do not lie in S by maximality. Thus, there exists $n_x, n_y \geq 1$ such that $f^{n_x} \in (x) + \mathfrak{m}$ and $f^{n_y} \in (y) + \mathfrak{m}$ (Note the existence follows as if I is not proper, $I = R$ and $f \in R$). Thus, $f^{n_x} = a_1 x + m_1$ and $f^{n_y} = a_2 y + m_2$ for $a_1, a_2 \in R$ and $m_1, m_2 \in \mathfrak{m}$. Specifically,

$$f^{n_x + n_y} = a_1 a_2 xy + m_3$$

for some $m_3 \in \mathfrak{m}$, using that $\mathfrak{m}$ is an ideal. Thus, $xy \notin \mathfrak{m}$, as else $f^{n_x + n_y} \in \mathfrak{m}$. $\square$

Corollary 3.1.3. *Let R be a ring. The nilradical of R is an ideal.*

Proof. Follows from the fact that the intersection of an arbitrarily set of ideals is an ideal. $\square$

We can prove the above corollary without relying on the previous proposition, by simply showing that the set of nilpotent elements are closed under addition and multiplication by elements of R.

Example 3.1.4. The nilradical of $\mathbb{C}[x]/(x^n)$ for $n \geq 1$ is (x).

3.2 Radical

Definition 3.2.1. *Let $I \subseteq R$ be an ideal. Let $q : R \to R/I$ be the quotient map, and $\mathcal{N}$ be the nilradical of R/I. The* ***radical*** *$\mathfrak{r}(I)$ of I is $q^{-1}(\mathcal{N})$.*

The nilradical of R coincides with the radical $\mathfrak{r}((0))$. As notation, we sometimes write $\mathfrak{r}(R)$ for the nilradical of R. By Proposition 3.1.2, the radical of I has two equivalent definitions :

1. It is the set of elements $f \in R$ such that there exists an integer $n \geq 1$ such that $f^n \in I$.
2. It is the intesection of prime ideals of R which contain I.

Example 3.2.2. Consider $\mathbb{Z}/12\mathbb{Z}$. $\mathfrak{r}(R) = (6)$ is not a prime ideal, so radicals need not be prime.

Proposition 3.2.3. *Let I be an ideal in R. Then, $\mathfrak{r}(\mathfrak{r}(I)) = \mathfrak{r}(I)$.*

Proof. Note that $\mathfrak{r}(I) = \{f \in R \mid f^n \in I,\ n \geq 0\}$. So, $\mathfrak{r}(\mathfrak{r}(I)) = \{f \in R \mid f^{mn} \in I,\ n, m \geq 0\} = \mathfrak{r}(I)$. $\square$

Proposition 3.2.4. *Let I, J be ideals in R. Then, $\mathfrak{r}(I \cap J) = \mathfrak{r}(I) \cap \mathfrak{r}(J)$.*

Proof. Follows from the first equivalent definition. □

Definition 3.2.5. *An ideal that coincides with it's own radical is called a **radical ideal**.*

A trivial radical ideal is the (0) when working with domains.

3.3 Jacobson Radical

Definition 3.3.1. *Let R be a ring. The **Jacobson radical** of R is the intersection of all the maximal ideals of R.*

Note that by definition, the Jacobson radical of R contains the nilradical of R. Also note that if a ring is local, then the Jacobson radical is the maximal ideal of R.

Definition 3.3.2. *Let $I \subsetneq R$ be a non-trivial ideal. Let $q : R \to R/I$ be the quotient map and $\mathcal{J}$ be the Jacobson radical of R/I. The **Jacobson Radical of** I is $q^{-1}(\mathcal{J})$. Equivalently, it is the intersection of all the maximal ideals containing I (by taking a larger ideal and showing it is actually the entire set).*

Note that by definition, the Jacobson radical of I contains the radical of I.

Proposition 3.3.3 (Nakayama's Lemma)**.** *Let R be a ring. Let M be a finitely generated R-module. Let I be an ideal of R contained by the Jacobson radical of R. Suppose further that $IM = M$ (where product is the finite sum). Then $M \simeq 0$.*

Proof. Suppose $M \not\simeq 0$. Let $x_1, \dots, x_s$ be the set of generators of M such that s is minimal, where $s \geq 1$ as M is nonzero. By assumption, there exists $a_1, \dots, a_s \in I$ such that

$$x_s = a_1x_1 + \cdots + a_sx_s$$

Rewriting,

$$(1 - a_s)x_s = a_1x_1 + \cdots + a_{s-1}x_{s-1}$$

If $1 - a_s$ is not a unit, it would be contained in some maximal ideal $\mathfrak{m}$ by Proposition 1.1.17. As $a_s \in I$ which is inside the Jacobson radical which is inside any maximal ideal, we have $a_s \in \mathfrak{m}$, giving $1 \in \mathfrak{m}$, a contradiction. Thus, $1 - a_s$ is a unit. Rewriting,

$$x_s = (1 - a_s)^{-1}a_1x_1 + \cdots + (1 - a_s)^{-1}a_{s-1}x_{s-1}$$

contradicting the minimality of s. Thus, $M \simeq 0$. □

Corollary 3.3.4. *let R be a local ring with maximal ideal $\mathfrak{m}$. Let M be a finitely generated R-module. Let $x_1, \dots, x_s \in M$ be elements of M and $x_1 + \mathfrak{m}M, \dots, x_s + \mathfrak{m}M \in M/\mathfrak{m}M$ generate the $R/\mathfrak{m}$-module $M/\mathfrak{m}M$. Then the elements $x_1, \dots, x_s$ generate M.*

Proof. Let $M' \subseteq M$ be the submodule generated by $x_1, \dots, x_s$. By assumption, $M' + \mathfrak{m}M = M$, thus, $\mathfrak{m}(M/M') = M/M'$. By Nakayama's lemma, we have $M/M' \simeq (0)$, giving $M = M'$. □

Corollary 3.3.5. *Let R be a local ring with maximal ideal $\mathfrak{m}$. Let M, N be finitely generated R-modules and $\phi : M \to N$ be a homomorphism of R-modules. Suppose the induced homomorphism*

$$M/\mathfrak{m}M \to N/\mathfrak{m}N$$

is surjective. Then ϕ is surjective.

Proof. Let $x_1, \dots, x_s$ be generators of M. By assumption, $\phi(x_1) + \mathfrak{m}, \dots, \phi(x_s) + \mathfrak{m}$ generate $N/\mathfrak{m}$. Thus, by Corollary 3.3.4, $\phi(x_1), \dots, \phi(x_s)$ generate N. In particular, ϕ is surjective. ☐

Definition 3.3.6. *A ring R is called a* ***Jacobson ring*** *if for all the proper ideals I of R, the Jacobson radical of I coincides with the radical of I.*

Proposition 3.3.7. *A ring R is a Jacobson ring if and only if every prime ideal I is the intersection of maximal ideals containing I.*

Proof. If R is Jacobson, every Jacobson radical of I coincides with the radical of I. Thus, for any prime I, the intersection of maximal ideals containing I is equal to the intersection of prime ideals containing I, which is just I.

Conversely, let every prime ideal be the intersection of maximal ideals containg itself. Then, for any ideal I, the radical of I is the intersection of maximal ideals containing a prime ideal which contains I. As any maximal ideal is prime, this is just the intersection of maximal ideals containing I, which is the Jacobson radical of I. ☐

Proposition 3.3.8. *Any quotient of a Jacobson ring is also Jacobson.*

Proof. Let R be a Jacobson ring. Let R/I be the quotient ring with some ideal I. It suffices to show every prime ideal of R/I is the intersection of maximal ideals containing it. For any prime ideal J containing I, as R is a Jacobson ring,

$$J = \bigcap_{J \subseteq \mathfrak{m}} \mathfrak{m}$$

for maximal ideals $\mathfrak{m}$. By correspondence, takig quotients,

$$J/I = \bigcap_{J \subseteq \mathfrak{m}} \mathfrak{m}/I$$

writes any prime ideal of R/I as the intersection of maximal ideals containing it. ☐

Example 3.3.9. The following are examples of Jacobson rings.

1. The ring $\mathbb{Z}$
2. Any field
3. Given a field K, the polynomial ring $K[x]$
4. Any finitely generated algebra over a Jacobson ring

Contrary to this, a local domain is never Jacobson unless it is a field. This follows as (0) is prime, which equals the intersection of maximal ideals, which is just $\mathfrak{m}$. As this is (0), it is a field. As a corollary, the ring of p-adic integers $\mathbb{Z}_p$ for prime p is not Jacobson.

3.4 Spectrum

Definition 3.4.1. *Let R be a ring. The* ***spectrum*** *of R written* $\mathrm{Spec}(R)$ *is the set of prime ideals of R.*

Furthermore, given an ideal I of R, define

$$V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \subseteq \mathfrak{p}\}$$

which is the set of prime ideals containing I.

Proposition 3.4.2. *The function $V(\cdot)$ has the following properties*

1. $V(I) \cup V(J) = V(I \cdot J)$
2. $\cap_{I \in \mathcal{I}} V(I) = V(\sum_{I \in \mathcal{I}} I)$
3. $V(R) = \emptyset$
4. $V((0)) = \mathrm{Spec}(R)$

Proof. (1) Double inclusion. One direction is clear, as $IJ \subseteq I$ and $IJ \subseteq J$. If $K \in V(IJ)$, $IJ \subseteq K$ where K is prime. Suppose for a contradiction $I \not\subseteq K$ and $J \not\subseteq K$. Take elements $i \in I \backslash K$ and $j \in J \backslash K$. As $ij \in K$, $i \in K$ or $j \in K$, which contradicts choice.

(2) Double inclusion. One direction is clear, as $J \subseteq \sum_{I \in \mathcal{I}} I$ for any $J \in \mathcal{I}$. For the other direction, suppose we have a prime K such that $I \subseteq K$ for every $I \in \mathcal{I}$. Then we note $\sum_{I \in \mathcal{I}} I \subseteq K$, as for any element in the sum decomposed to elements from I, they are in K, whose sum is also in K.

(3), (4) are immediate. $\square$

Definition 3.4.3. *The topology induced by setting $V(I)$ to be closed sets form a topology called the* ***Zariski Topology****. In this topology, the closed points (in* $\mathrm{Spec}(R)$*) are exactly the maximal ideals of R.*

If R is a Jacobson ring, any nonempty closed set contains a maximal ideal of R. As every prime ideal is also the limit (intersection) of maximal ideals, it follows that the set of closed points is a dense subset of $\mathrm{Spec}(R)$. (MOVE LATER!!!!)

Suppose we have a homomorphism $\phi : R \to T$. This induces a homomorphism

$$\mathrm{Spec}(\phi) : \mathrm{Spec}(T) \to \mathrm{Spec}(R)$$

by the map $\mathfrak{p} \mapsto \phi^{-1}(\mathfrak{p})$. Note this is well-defined as preimages of prime ideals are prime.

If I is an ideal in R and $J = (\phi(I))$ is an ideal in T, we have $\mathrm{Spec}(\phi)^{-1}(V(I)) = V(J)$. Consequently, $\mathrm{Spec}(\phi)$ is a continuous map for the Zariski topologies on source and target. Note also that by definition, $\mathrm{Spec}(\phi) \circ \mathrm{Spec}(\psi) = \mathrm{Spec}(\psi \circ \phi)$.

Lemma 3.4.4. *Let $\phi : R \to T$ be a surjective homomorphism of rings. Then* $\mathrm{Spec}(\phi)$ *is injective and* $\mathrm{Im}(\mathrm{Spec}(\phi)) = V(\mathrm{Ker}(\phi))$.

Proof. To show that $\mathrm{Spec}(\phi)$ is injective, note that for any $\mathfrak{p} \in \mathrm{Spec}(T), \mathfrak{p} = \phi(\phi^{-1}(\mathfrak{p}))$ by surjectivity. In particular, distinct elements of $\mathrm{Spec}(T)$ get sent to distinct elements in $\mathrm{Spec}(R)$.

We show the second by double inclusion. Note first that the image of $\mathrm{Spec}(\phi)$ is contained in $V(\mathrm{Ker}(\phi))$ as the preimage of a prime ideal by ϕ always contains the kernel (equivalently, any prime ideal contains 0).

On the other hand, fixing a $\mathfrak{p}$ to be a prime ideal containing $\mathrm{Ker}(\phi)$, it suffices to show $\mathrm{Spec}(\phi)(\phi(\mathfrak{p})) = \mathfrak{p}$. To do this, we show that $\phi(\mathfrak{p})$ is prime, and $\phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}$. First, we clearly have $\mathfrak{p} \subseteq \phi^{-1}(\phi(\mathfrak{p}))$. Taking any $r \in \phi^{-1}(\phi(\mathfrak{p}))$, there exists $r' \in \mathfrak{p}$ such that $\phi(r) = \phi(r')$. As $\mathfrak{p}$ contains the kernel of ϕ, it follows $r \in \mathfrak{p}$, thus equality. To show that $\phi(\mathfrak{p})$ is a prime ideal, taking $x, y \in T$ such that $xy \in \phi(\mathfrak{p})$, choosing x', y' such that $\phi(x') = x$ and $\phi(y') = y$, $x'y' \in \phi^{-1}(\phi(\mathfrak{p})) = \mathfrak{p}$. Thus $x' \in \mathfrak{p}$ or $y' \in \mathfrak{p}$. The proof follows.

□

Proposition 3.4.5. *Fix $f \in R$. Define*

$$D_f(R) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \notin \mathfrak{p}\}$$

These form open sets in $\mathrm{Spec}(R)$ *and is a basis for the Zariski Topology.*

Proof. First note that

$$\mathrm{Spec}(R) \backslash D_f(R) = V((f))$$

Noting every closed set in $\mathrm{Spec}(R)$ can be expressed as $V(I)$ for some I,

$$\bigcup_{f \in I} D_f(R) = \{p \in \mathrm{Spec}(R) \mid I \not\subseteq \mathfrak{p}\} = \mathrm{Spec}(R) \backslash V(I)$$

So is a basis. □

Lemma 3.4.6. *Given a ring R,* $\mathrm{Spec}(R)$ *is compact.*

Proof. We use the notion that $\mathrm{Spec}(R)$ is compact if every open cover by basis elements has a finite subcover. Note that for any $S \subseteq R$,

$$\begin{aligned} \mathrm{Spec}(R) \backslash \bigcup_{f \in S} D_f &= \bigcap_{f \in S} (\mathrm{Spec}(R) \backslash D_f) \\ &= \bigcap_{f \in S} V((f)) \\ &= V(\sum_{f \in S} (f)) \end{aligned}$$

For any cover $\mathcal{F}$, taking $S = \mathcal{F}$, $V(\sum_{f \in \mathcal{F}} ((f))) = \emptyset$. Thus, $\sum_{f \in \mathcal{F}} ((f))$ is not contained in any prime ideal. By Proposition 1.1.17, every proper ideal has a maximal ideal (which is prime) containing it, meaning $\sum_{f \in \mathcal{F}} ((f)) = R$. Then, we can write 1_R as a finite linear sum of elements of $\mathcal{F}$. These elements form a fintie subset $\mathcal{F}_0$ that generate R, and $\mathrm{Spec}(R) \backslash \bigcup_{f \in \mathcal{F}_0} D_f = V(R) = \emptyset$ □

Lemma 3.4.7. *Let I and J be ideals in R. Then, $V(I) = V(J)$ if and only if $\mathfrak{r}(I) = \mathfrak{r}(J)$.*

Proof. ($\Rightarrow$) Suppose that for every prime ideal $\mathfrak{p}$, $I \subseteq \mathfrak{p}$ if and only if $J \subseteq \mathfrak{p}$. Then, as radicals are intersections of prime ideals containing it, equality follows.

($\Leftarrow$) Suppose for a contradiction that $V(I) \neq V(J)$. Without loss of generality, there exists $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$ and $J \not\subseteq \mathfrak{p}$. Then, $J \not\subseteq \mathfrak{r}(J)$, which contradicts definition. □

Consequently, there is a bijective correspondence between radical ideals in R and closed subsets of $\mathrm{Spec}(R)$. The closed subsets corresponding to prime ideals are called **irreducible**.

Proposition 3.4.8. *If I and J are radical ideals, $I \subseteq J$ if and only if $V(J) \subseteq V(I)$*

Proof. ($\Rightarrow$) is immediate. For ($\Leftarrow$), we have $J \subseteq \mathfrak{p}$ implies $I \subseteq \mathfrak{p}$. As I and J are radical ideals, they are intersections of prime ideals containing it. The proof follows. $\square$

Corollary 3.4.9. *The quotient map from R into $R/\mathfrak{r}((0))$ is a homeomorphism. Thus, closed sets are determied by radical ideals and are unchanged by quotients with the nilradical.*

Remark 3.4.10. Given two ideals I, J of a ring R, we have

$$(I \cap J) \cdot (I \cap J) \subseteq I \cdot J \subseteq I \cap J$$

Thus $\mathfrak{r}(I \cdot J) = \mathfrak{r}(I \cap J)$ which follows from the fact $V(I \cdot J) = V(I \cap J)$, supported by the identity $V(I) \cup V(J) = V(I \cdot J)$.

Also, given that I and J are radical ideals, $I \cap J$ is a radical ideal, whereas $I \cdot J$ need not be.

Lemma 3.4.11. *Let R be a ring and $I \triangleleft R$. Then $V(I)$ has a minimal element up to inclusion. Moreover, if $\mathfrak{p} \supseteq I$ is prime, $\mathfrak{p}$ contains such an ideal.*

Proof. Define $\leq$ on prime ideals containing I but is contained by $\mathfrak{p}$ by $\supseteq$. Take any chain T. Then we claim $\mathcal{T}$ has a maximal element $\bigcap_{\mathfrak{p} \in \mathcal{T}} \mathfrak{p}$. Note first this clearly contains I, is maximal, and is an ideal. To show it is prime, suppose $xy \in \bigcap_{\mathfrak{p} \in \mathcal{T}} \mathfrak{p}$ but $x, y \notin \bigcap_{\mathfrak{p} \in \mathcal{T}} \mathfrak{p}$. Then we can find $\mathfrak{p}_i, \mathfrak{p}_j$ such that $x \notin \mathfrak{p}_i$ and $y \notin \mathfrak{p}_j$. Without loss of generality, as $\mathcal{T}$ is a chain, suppose $\mathfrak{p}_i \leq \mathfrak{p}_j$. Then as $xy \in \mathfrak{p}_j$, $x \in \mathfrak{p}_j$. This contradicts the $\leq$ condition. Thus by Zorn's Lemma, there is a maximal element $\mathfrak{m}$ up to the relation $\leq$. This corresponds to a minimal prime containing I that is contained in $\mathfrak{p}$. $\square$

3.5 Primary Decomposition

Proposition 3.5.1. *Let $\mathfrak{p}_1, \dots \mathfrak{p}_k$ be prime ideals of R. Let I be an ideal of R. If $I \subseteq \bigcup_{i=1}^{k} \mathfrak{p}_i$, then there is some $i_0 \in \{1, \dots, k\}$ such that $I \subseteq \mathfrak{p}_{i_0}$.*

Proof. By induction on k. The case for $k = 1$ holds tautologically. For a general k, if $I \subseteq \bigcup_{i \neq j}^{k} \mathfrak{p}_i$, we are done by the inductive hypothesis. Otherwise, we can find $x_1, \dots, x_k \in I$ such that for all $i \in \{1, \dots, k\}$, $x_i \in \mathfrak{p}_i$ but $x_i \notin \mathfrak{p}_j$ for any $i \neq j$. Consider

$$y = \sum_{j=0}^{k} x_1 x_2 \cdots x_{j-1} x_{j+1} \cdots x_k$$

where $x_0 = x_{k+1} = 1$. Note that by construction $x_1 x_2 \cdots x_{j-1} x_{j+1} \cdots x_k \in \mathfrak{p}_i$ if $i \neq j$. As $y \in I$, $y \in \mathfrak{p}_i$ for some $i \in \{1, \dots, k\}$. Then,

$$y - \sum_{j \neq i}^{k} x_1 x_2 \cdots x_{j-1} x_{j+1} \cdots x_k \in \mathfrak{p}_i$$

So $x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_k \in \mathfrak{p}_i$, which contradicts construction as $\mathfrak{p}_i$ is a prime ideal. $\square$

Proposition 3.5.2. *Let $I_1, \dots, I_k$ be ideals of R and $\mathfrak{p}$ be a prime ideal of R. Suppose that $\mathfrak{p} \supseteq \bigcap_{i=1}^{k} I_i$. Then, there exists a $i_0 \in \{1, \dots, k\}$ such that $p \supseteq I_{i_0}$. If $\mathfrak{p} = \bigcap_{i=1}^{k} I_i$, there is a i_0 such that $p = I_{i_0}$.*

Proof. For the first case, suppose for a contradiction that for every $i \in \{1, \dots, k\}$ there is an element $x_i \in I_i$ such that $x_i \notin \mathfrak{p}$. But $x_1 x_2 \cdots x_k \in \bigcap_{i=1}^{k} I_i \subseteq \mathfrak{p}$ and as $\mathfrak{p}$ is prime, one of x_i lies in $\mathfrak{p}$, a contradiction. The second case follows immediately as a consequence, noting $\bigcap_{i=1}^{k} I_i \subseteq I_{i_0}$. $\square$

Remark 3.5.3. Noting the proof in Proposition 3.5.1, any cover of an ideal by two ideals is covered by a single ideal.

Definition 3.5.4. *An ideal I of R is called* ***primary*** *if it is proper and all the zero-divisors of R/I are nilpotent.*

In other words, if $xy \in I$ and $x, y \notin I$, there exists $l, n > 1$ such that $x^l \in I$ and $y^n \in I$. Consequently, every prime ideal is primary. The converse need not be true. Ideals $(p^n) \in \mathbb{Z}$ are primary if p is prime and $n > 0$ but for $n > 1$ is not a prime ideal.

Lemma 3.5.5. *Suppose that I is a primary ideal of R. Then $\mathfrak{r}(I)$ is a prime ideal.*

Proof. Let $x, y \in R$ and suppose $xy \in \mathfrak{r}(I)$. Then, there is a $n > 0$ with $x^n y^n \in I$. By primarity, $x^n \in I$, or $y^n \in I$, or $x^{ln} \in I$ and $y^{nk} \in I$ for some $l, k > 1$. In any case, $x \in I$ or $y \in I$. □

Definition 3.5.6. *Following the previous lemma, given a prime ideal $\mathfrak{p}$ and ideal I, we say that I is* ***$\mathfrak{p}$-primary*** *if $\mathfrak{r}(I) = \mathfrak{p}$.*

$\mathfrak{p}$-primary ideals I have the property that if $ab \in I$, without loss of generality, if $a \notin I$, then $b \in \mathfrak{p}$.

Example 3.5.7. Consider $\mathbb{Z}[x, y]$ and the ideal (xy). Now, $\mathfrak{r}((xy)) = (x, y)$ who is clearly prime. However (xy) is not primary. Specifically, the radical of an ideal being prime does not imply the original ideal is primary.

However, we have the following.

Lemma 3.5.8. *Let J be a (proper) ideal of R. Suppose that $\mathfrak{r}(J)$ is a maximal ideal. Then J is primary.*

Proof. By assumption, the nilradical of R/J is a maximal ideal (by correspondence). Thus, R/J is local, as any maximal ideal of R/J contains $\mathfrak{r}(R/J)$. Hence every element of R/J is either a unit or is nilpotent. Specifically, J is primary. □

Definition 3.5.9. *If $I, J \subseteq R$ are ideals in R, we write*

$$(I : J) = \{r \in R \mid rJ \subseteq I\}$$

Note that $(I : J)$ is also an ideal and $((0) : J) = \mathrm{Ann}(J)$. When it is clear, we write x to mean (x) for some $x \in R$ (e.g. $(x : I)$ to mean $((x) : I)$).

Note the identity $I \subseteq (I : J)$.

Proposition 3.5.10. *Given ideals I, J, M of R, we have*

$$(I : M) \cap (J : M) = (I \cap J : M)$$

Proof. By double inclusion. □

Lemma 3.5.11. *Let $\mathfrak{p}$ be a prime ideal and I be a $\mathfrak{p}$-primary ideal. Fix any $x \in R$. Then,*

1. *If $x \in I$, $(I : x) = R$*
2. *If $x \notin I$, $\mathfrak{r}(I : x) = \mathfrak{p}$*

3. *If $x \notin \mathfrak{p}$, $(I : x) = I$*

Proof. The first and third cases follow immediately. For the second case, suppose $y \in \mathfrak{r}(I : x)$. By definition, there exists some $n > 0$ such that $xy^n \in I$. As $x \notin I$, $y^n \in \mathfrak{p} = \mathfrak{r}(I)$, so $y^{ln} \in I$ for some $l > 0$. Thus, $y \in \mathfrak{r}(I)$. Thus $\mathfrak{r}(I : x) \subseteq \mathfrak{p}$. Now clearly $I \subseteq \mathfrak{r}(I : x) \subseteq \mathfrak{p}$. As $\mathfrak{r}$ is monotonic, $\mathfrak{r}(I) = \mathfrak{p} \subseteq \mathfrak{r}(\mathfrak{r}(I : x)) = \mathfrak{r}(I : x) \subseteq \mathfrak{r}(\mathfrak{p}) = \mathfrak{p}$, giving $\mathfrak{r}(I : x) = \mathfrak{p}$. □

Lemma 3.5.12. *Let $\mathfrak{p}$ be a prime ideal and $J_1, \dots, J_k$ be $\mathfrak{p}$-primary ideals. Then $J = \bigcap_{i=1}^k J_i$ is also $\mathfrak{p}$-primary.*

Proof. Applying $\mathfrak{r}$,

$$\mathfrak{r}(J) = \mathfrak{r}(\bigcap_{i=1}^k J_i) = \bigcap_{i=1}^k \mathfrak{r}(J_i) = \mathfrak{p}$$

Thus, it remains to check that J is primary. Suppose $xy \in J$ with $x, y \notin J$. Then we can find $i, j \in \{1, \dots, k\}$ such that $x \notin J_i$ and $y \notin J_j$. Hence there exists $l, t > 0$ such that $y^l \in J_i$ and $x^t \in J_j$ (as $xy \in J_i$ and $xy \in J_j$). Thus, $x \in \mathfrak{r}(J_j) = \mathfrak{r}(J) = \mathfrak{r}(J_i) \ni y$, yielding that J is primary. □

Definition 3.5.13. *An ideal $I \triangleleft R$ is **decomposable** if there exists a finite collection $J_1, \dots, J_k$ of primary ideals in R such that $I = \bigcap_{i=1}^k J_i$. The sequence is called a **primary decomposition** of I. A primary decomposition is called **minimal** if*

1. *The radicals $\mathfrak{r}(J_i)$ are distinct*
2. *For all $i \in \{1, \dots, k\}$, $J_i \not\supseteq \bigcap_{j \neq i} J_i$*

Note that any primary decomposition can be reduced to a minimal primarity decomposition by

1. Using Lemma 3.5.12 and replacing all primary ideals with the same radical with their intersection to achieve (1)
2. Remove any primary ideal that covers the entire set

Theorem 3.5.14. *Let I be a decomposable ideal. Let $J_1, \dots, J_k$ be primary ideals and $I = \cap_{i=1}^k J_i$ be a minimal primary decomposition of I. Define $\mathfrak{p}_i = \mathfrak{r}(J_i)$ (such that $\mathfrak{p}_i$ are prime). Then,*

$$\{p_i \mid i \in \{1, \dots, k\}\} = \{prime\ \mathfrak{r}(I : x) \mid x \in R\}$$

Proof. Take $x \in R$. Note that $(I : x) = \bigcap_{i=1}^k (J_i : x)$ and $\mathfrak{r}(I : x) = \bigcap_{i=1}^k \mathfrak{r}(J_i : x)$ by preservation of $\mathfrak{r}$ under intersection. Thus, by Lemma 3.5.11, $\mathfrak{r}(I : x) = \bigcap_{i, x \notin J_i} \mathfrak{p}_i$. If $\mathfrak{r}(I : x)$ is prime, by Proposition 3.5.2, $\mathfrak{r}(I : x) = \mathfrak{p}_{i_0}$ for some $i_0 \in \{1, \dots, k\}$.

Conversely, taking any $i_0 \in \{1, \dots, k\}$, we can find a $x \in J_{i_0}$ such that $x \notin J_i$ for $i \neq i_0$ by minimality of decomposition. Given such x, $\mathfrak{r}(I : x) = \bigcap_{i, x \notin J_i} \mathfrak{p}_i = \mathfrak{p}_{i_0}$ by above. □

Remark 3.5.15. By Theorem 3.5.14, we can associate any decomposable ideal I in R with a unique set of prime ideals. Specifically, this set is fixed for any primary decomposition. We then say that these prime ideals are **associated** with I. Also note that the intersection of these primes give $\mathfrak{r}(I)$ (by choosing x to be a unit and taking $(I : x) = I = \bigcap_i \mathfrak{p}_i$).

Given an ideal that is decomposable into radical ideals, it has a minimal primary decomposition by prime ideals, and these prime ideals are the associated primes. Noting Proposition 3.5.2, any two minimality primary decomposition by prime ideals of a radical ideal coincide.

While out of scope, any minimal primary decomposition of a radical consists only of prime ideals. Specifically, a decomposable radical ideal has a unique primary decomposition by prime ideals.

Example 3.5.16. If $n = \pm p_1^{n_1} \cdots p_k^{n_k} \in \mathbb{Z}$ where p_i are distinct prime numbers and $n_i > 0$, a parimary decomposition of (n) is given by $(n) = \bigcap_{i=1}^{k} (p^{n_i})$ by the Chinese Remainder Theorem. The set of prime ideals associated with this is given by $\{p_1, \ldots, p_k\}$.

Example 3.5.17. Consider the ideal $(x^2, xy) \subseteq \mathbb{C}[x, y]$. Now,

$$(x^2, xy) = (x) \cap (x, y)^2$$

so the associated set of prime ideals is $\{(x), (x, y)\}$. To see equality, note that elements of $(x, y)^2$ are pf tje form $x^2 P(x, y) + xyQ(x, y) + y^2 T(x, y)$, thus the right side consists of polynomials of such form where $T(x, y)$ is divisible by x. Double inclusion follows. To see that these are both primary, we note $\mathbb{C}[x, y]/(x) \simeq \mathbb{C}[y]$ meaning (x) is prime (thus primary), and from $\mathbb{C}[x, y]/(x, y) \simeq \mathbb{C}$, using Lemma 3.5.8, $(x, y)^2$ is also primary.

Lemma 3.5.18. *Let I be a decomposable ideal. Let $\mathcal{S}$ be the set of prime ideals associated with some minimal primary decomposition of I. View $\mathcal{S}$ as a poset by inclusion. Then, the minimal elements of $\mathcal{S}$ coincide with the minimal elements of $V(I)$.*

Proof. The minimal elements of $V(I)$ denoted $V(I)_{\min}$ are minimal elements of $\mathcal{S}$ denoted $\mathcal{S}_{\min}$ by definition (by considering any primary decomposition, we can throw in any element of $\mathcal{I}_{\min}$ into the decomposition to make a decomposition containing this element).

To show the other direction, note that $\mathfrak{r}(I) = \bigcap_{\mathfrak{p} \in \mathcal{S}} \mathfrak{p}$, thus $\mathfrak{r}(I) = \bigcap_{\mathfrak{p} \in \mathcal{S}_{\min}} \mathfrak{p}$. Suppose that $\mathfrak{p}_0 \in \mathcal{S}_{\min}$ and that $\mathfrak{p}_0 \notin V(I)_{\min}$. Then, we can find a $\mathfrak{p}_0' \in V(I)$ such that $I \subseteq \mathfrak{p}_0' \subsetneq \mathfrak{p}_0$. By Proposition 3.5.2, we can find a $\mathfrak{p} \in \mathcal{S}_{\min}$ such that $\mathfrak{p} \subseteq \mathfrak{p}_0'$. This contradicts minimality of $\mathfrak{p}_0$, giving $\mathcal{S}_{\min} = V(I)_{\min}$. $\square$

Definition 3.5.19. *Elements of $\mathcal{S}_{\min}$ are called **isolated** or **minimal** prime ideals associated with I. The elements $\mathcal{S} \backslash \mathcal{S}_{\min}$ are called **embedded** prime ideals.*

Remark 3.5.20. If I is a decomposable radical ideal, the associated primes of I are isolated. This follows immediately from the fact that I has a minimal primary decomposition by prime ideals.

If I is a decomposable ideal, then $V(I)_{\min}$ is a finite set. By the previous lemma, this is exactly the isolated ideals associated with I.

3.6 Noetherian Rings

Definition 3.6.1. *Let R be a ring. We say that R is **noetherian** if every ideal of R is finitely generated. That is, for any $I \lhd R$, $I = (r_1, \ldots, r_k)$ for some $r_i \in R$.*

Example 3.6.2. Fields and PIDs are noetherian, as every ideal is generated by a single element. For instance, $\mathbb{Z}$, $\mathbb{C}$ are noetherian. Given any field K, $K[x]$ is also noetherian as a polynomial over a field is an ED (which is a PID).

Lemma 3.6.3. *The ring R is noetherian if and only if for any chain $I_1 \subseteq I_2 \subseteq \cdots$ is a chain of ideals, there exists a $k \geq 1$ such that $I_k = I_{k+i} = \bigcup_{t=1}^{\infty} I_t$ for all $i \geq 0$.*

Proof. $(\Rightarrow)$ Suppose R is noetherian. Let $I_1 \subseteq I_2 \subseteq \cdots$. The set $\bigcup_{t=1}^{\infty} I_t$ is an ideal, who is finitely generated by assumption. Given such a finite set, it must lie in I_k for some $k \geq 1$. The conclusion follows.

$(\Leftarrow)$ Suppose whenever $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals, $k \geq 1$ such that $I_k = I_{k+i} = \bigcup_{t=1}^{\infty} I_t$ for all $i \geq 0$. Let $J \subseteq R$ be an ideal. Suppose for a contradiction J is not finitely generated. Then we can inductively produce a chain of strictly increasing ideals (by choosing elements not yet in the ideal produced by the prefix set), which contradicts our assumption. $\square$

Lemma 3.6.4. *Let R be a noetherian ring and $I \triangleleft R$. Then R/I is noetherian.*

Proof. Let $q : R \to R/I$ be the quotient map. Let J be any ideal of R/I. The ideal $q^{-1}(J)$ is finitely generated by assumption, and the image of these generators generate J. $\square$

Lemma 3.6.5. *Let R be a noetherian ring and $S \subseteq R$ be a multiplicative set. Then R_S is noetherian.*

Proof. Let $\lambda : R \to R_S$ be the natural ring homomorphism. By Lemma 2.1.18 the ideal generated by $\lambda(\lambda^{-1}(I)) = I$. Thus, the image of any finite set of generators of $\lambda^{-1}(I)$ under λ generates I. $\square$

Lemma 3.6.6. *Let R be a noetherian ring and M be a finitely generated R-module. Then any submodule of M is also finitely generated.*

Proof. By assumption we have a surjective map of R-modules $q : R^n \to M$ for some $n \geq 0$. To show that $N \subseteq M$ is finitely generated, it is enough to show that $q^{-1}(N)$ is finitely generated. As this lies in R^n, we may assume that $M = R^n$.

We now do induction on n. The case $n = 1$ is immediate as submodules of R correspond to ideals and R is noetherian. Suppose $\phi : R^n \to R$ be the projection on the last factor. Let $N \subseteq R^n$ be a submodule. We have the exact sequence

$$0 \to N \cap R^{n-1} \to N \to \phi(N) \to 0$$

where R^{n-1} is viewed as a submodule of R^n via the map $(r_1, \ldots, r_{n-1}) \mapsto (r_1, \ldots, r_{n-1}, 0)$. $\phi(N)$ is finitely generated as it is an ideal in R, and $N \cap R^{n-1}$ is finitely generated by the inductive hypothesis.

Let $a_1, \ldots, a_k \in N \cap R^{n-1}$ generate $N \cap R^{n-1}$ and $b_1, \ldots, b_l \in \phi(N)$ generate $\phi(N)$. Let $b'_1, \ldots, b'_l \in R^n$ be such that $\phi(b'_i) = b_i$ for all $i \in \{1, \ldots, l\}$. Then, $\{a_1, \ldots, a_k, b'_1, \ldots, b'_k\}$ generate N, noting $(N \cap R^{n-1}) \times \phi(N) \simeq N$. $\square$

Lemma 3.6.7. *Let R be a noetherian ring. If $I \triangleleft R$, there is a $t \geq 1$ such that $\mathfrak{r}(I)^t \subseteq I$. Consequently, some power of the nilradical of R is the 0-ideal.*

Proof. Noting $\mathfrak{r}(I)$ is an ideal, it is finitely generated, say $\mathfrak{r}(I) = (a_1, \ldots, a_k)$ for some $a_i \in R$. By definition of the radical, there exists an $n \geq 1$ such that $a_i^n \in I$ for all $i \in \{1, \ldots, k\}$. Define $t = k(n-1)+1$. Then, $\mathfrak{r}(I)^t \subseteq (a_1^n, \ldots, a_k^n) \subseteq I$ where the first inclusion comes from the pigenhole principle. $\square$

Theorem 3.6.8 (Hilbert Basis Theorem)**.** *Let R be noetherian. Then, the polynomial ring $R[x]$ is also noetherian.*

Proof. Let $I \subseteq R[x]$ be an ideal. The leading coefficients of the non-zero polynomials in I (with 0) form an ideal J of R. As R is noetherian, J has a finite set of generators, say $a_1, \ldots, a_k$. For each $i \in \{1, \ldots, k\}$ choose $f_i \in I$ such that $f_i(x) - a_i x^{n_i}$ has degree lower than n_i. Define $n = \max_i n_i$. Let $I' = (f_1(x), \ldots, f_k(x)) \subseteq I$ be the ideal generated by $f_i(x)$. Define M to be the polynomials in I with degree less than n.

Suppose we choose $f(x) \in I \backslash (I' + M)$ of smallest possible degree m. Pick $a \in R$ such that $f - ax^m$ has degree lower than m. As $a \in J$, we have $a = r_1 a_1 + \cdots + r_k a_k$ for some $r_1, \ldots, r_k \in R$. Suppose $m \geq n$. Then,

$$f(x) - r_1 f_1(x) x^{m-n_1} - \cdots - r_k f_k(x) x^{m-n_k}$$

is degree less than m (by cancelling leading term) and lies in I by construction. By minimality of m, this lies in $I' + M$, so $f(x) \in I' + M$, which is a contradiction. If $m < n$, $f(x) \in M$, another contradiction. Consequently, $I = I' + M$.

R is an R-submodule (ideal) of the R-module consisting of polynomials of degree less than n, which is clearly finitely generated as an R-module. Thus, by Lemma 3.6.6, M is finitely generated as an R-module by $g_1(x), \dots, g_t(x) \in M$. Then, $g_1(x), \dots, g_t(x), f_1(x), \dots, f_k(x)$ is a set of generators of I as an ideal. $\square$

Remark 3.6.9. As a consequence of the Hilbert Basis theorem, we see that $R[x_1, \dots, x_k]$ is noetherian for any $k \geq 0$. By noting Lemma 3.6.4, we see that every finitely generated algebra over a noetherian ring is noetherian.

Theorem 3.6.10 (Artin-Tate)**.** *Let T be a ring and $R, S \subseteq T$ be subrings. Suppose $R \subseteq S$ and R is noetherian. Suppose further that T is finitely generated as an R-algebra and that T is finitely generated as an S-module. Then, S is finitely generated as an R-algebra.*

Proof. Let $r_1, \dots, r_k$ be generators of T as an R-algebra. Let $t_1, \dots, t_l$ be generators of T as an S-module. By assumption, for any $a \in \{1, \dots, k\}$ we can write

$$r_a = \sum_{j=1}^{l} s_{ja} t_j$$

where $s_{ja} \in S$. Similarly, for any $b, d \in \{1, \dots, k\}$ we have,

$$t_b t_d = \sum_{j=1}^{l} s_{jbd} t_j$$

where $s_{jbd} \in S$, both of which we use the fact the left side in an element of T.

Define S_0 to be the R-subalgebra generated by all s_{ja} and s_{jbd}. As every element of T can be written as an R-linear combination of products of r_a, we see that T is finitely generated as an S_0-module with $t_1, \dots, t_l$. Note also that S_0 is a finitely generated R-algebra by construction.

The R-algebra S is naturally an S_0 algebra (by inclusion), specifically an S_0 module, and a S_0 submodule of T. As R is noetherian, S_0 is noetherian (as it is finitely generated by R). As S is a submodule of a finitely generated S_0-module (T), S is also finitely generated as a S_0 submodule by Lemma 3.6.6. Specifically, S is finitely generated as an S_0-algebra, and as S_0 is finitely generated over R, so is S.

$$\begin{tikzcd}
R \arrow[d] & S_0 \arrow[d, dashed] \arrow[dr, hook, "\iota"] \arrow[dr, dashed, shift left=2] & \\
R[x_1, \dots, x_k] \arrow[ur, two heads] \arrow[r, two heads] & T & S \arrow[l, hook', "\supseteq"']
\end{tikzcd}$$

Simple illustration above with abuse of notation, where dotted arrows are induced S_0 modules. $\square$

Definition 3.6.11. *Let $I \triangleleft R$. We say that I is **irreducible** if whenever I_1 and I_2 are ideals of R and $I = I_1 \cap I_2$, $I = I_1$ or $I = I_2$. We say that an ideal is **decomposable by irreducible ideals** or dic if it has a finite intersection of irreducible ideals.*

Proposition 3.6.12. *Given $I \triangleleft R$, and R is noetherian, there exists irreducible ideals $I_1, \dots, I_k$ such that $I = \bigcap_{i=1}^{k} I_i$*

Proof. Suppose J is not dic. Specifically, J is not irreducible, and there exists ideals M, N such that $J = M \cap N$ and $J \subsetneq M$ and $J \subsetneq N$. As J is not dic, either N or M is not dic. Without loss of generality, suppose M is not dic. Repeating this produces a strictly increasing chain of non-dic ideals, contradicting the fact R is noetherian. $\square$

Proposition 3.6.13. *Irreducible ideals are primary.*

Proof. Let J be an irreducible ideal and suppose that J is not primary. Then, there exists $x \in R/J$ who is a zero-divisor but not nilpotent. Let $q : R \to R/J$ be the quotient map. Now, consider the sequence

$$\operatorname{Ann}(x) \subseteq \operatorname{Ann}(x^2) \subseteq \operatorname{Ann}(x^3) \subseteq \cdots$$

Noting R/J is noetherian, the sequence must stop at some k such that

$$\operatorname{Ann}(x^k) = \operatorname{Ann}(x^{k+1}) = \operatorname{Ann}(x^{k+2}) = \cdots$$

for some $k \geq 1$.

Consider the ideal $(x^k) \cap \operatorname{Ann}(x^k)$. If $\lambda x^k \in (x^k) \cap \operatorname{Ann}(x^k)$ for some $\lambda \in R/J$, $\lambda x^{2k} = 0$, thus $\lambda \in \operatorname{Ann}(x^{2k})$. As $\operatorname{Ann}(x^{2k}) = \operatorname{Ann}(x^k)$, $\lambda x^k = 0$. Thus, $(x^k) \cap \operatorname{Ann}(x^k) = (0)$. That is, $q^{-1}(x^k) \cap q^{-1}(\operatorname{Ann}(x^k)) = J$. On the other hand, $(x^k) \neq (0)$ by nilpotence and $\operatorname{Ann}(x^k) \neq 0$ by construction. Hence, $q^{-1}(x^k) \neq J$ and $q^{-1}(\operatorname{Ann}(x^k)) \neq J$. This contradicts irreducibility. Thus, J is primary. $\square$

Example 3.6.14. Primary ideals are not necessarily irreducible. Consider the ideal $(x, y)^2 \subseteq \mathbb{Q}[x, y]$. This is primary as $\mathfrak{r}((x, y)^2) = (x, y)$ is a maximal ideal by Lemma 3.5.8. However, this is the intersection of ideals (x, y^2) and (x^2, y).

Proposition 3.6.15 (Lasker-Noether)**.** *Let R be a noetherian ring. Then every ideal of R is decomposable.*

Proof. Follows from Propositions 3.6.12 and 3.6.13. $\square$

Let R be a noetherian ring and $I \subseteq R$ be a radical ideal. As a consequence of Lasker-Noether and the remark after primary decomposition, we have a unique set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ of distinct prime ideals in R such that

- $I = \bigcap_{i=1}^k \mathfrak{q}_i$
- for all $i \in \{1, \ldots, k\}$, $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$

Moreover, the set $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_k\}$ is the set of prime ideals that are minimal among the prime ideals containing I. In other words, $V(I)$ is the union of the closed sets $V(\mathfrak{q}_i)$.

If $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ is the set of minimal prime ideals of R, then there is a natural injective homomorphism of rings

$$R/\mathfrak{r}((0)) \hookrightarrow \prod_{i=1}^{l} R/\mathfrak{p}_i$$

4 Extensions

4.1 Integral Extensions

Definition 4.1.1. *Let B be a ring and $A \subseteq B$ be a subring. Let $b \in B$. We say that b is* ***integral*** *over A if there is a monic polynomial in $A[x]$ that annihalates b. Concretely, we have a $P(x) = x^n + a_{n-1}x^{n-1} + \ldots a_0 \in A[x]$ such that $P(b) = 0$.*

We say that b is **algebraic** *over A if there is a $Q(x) \in A[x]$ such that $Q(b) = 0$.*

Note that if A is a field, b is algebraic over A if and only if it is integral over A.

Definition 4.1.2. *Let $S \subseteq B$ be a subset, $A \subseteq B$ be a subring. Write $A[S]$ for the intersection of all the subrings of B which contain A and S. Note that $A[S]$ is naturally an A-algebra.*

As usual notation, we omit the set notation when it is clear (e.g., we write $A[b]$ for $A[\{b\}]$). If S is finite, we have

$$A[b_1, \ldots, b_k] = \{Q(b_1, \ldots, b_k) \mid Q(x_1, \ldots, x_k) \in A[x_1, \ldots, x_k]\}$$

which is the set of polynomials in A evaluated at $\{b_1, \ldots, b_k\}$. Also Consequently, we have

$$A[b_1, \ldots, b_k] = A[b_1] \cdots [b_k]$$

Proposition 4.1.3. *Let R be a ring and M be a finitely generated R-module. Let $\phi : M \to M$ be a homomorphism of R-modules. Then there exists a monic polynomial $Q(x) \in R[x]$ such that $Q(\phi) = 0$.*

Proof. By assumption, there is a surjective homomorphism of R-modules $\lambda : R^n \to M$ for some $n \geq 0$. Let $b_1, \ldots, b_n$ be the natural basis for R^n. For each b_i, choose an element $v_i \in R^n$ such that $\lambda(v_i) = \phi(\lambda(b_i))$. Define a homomorphism of R-modules $\tilde{\phi} : R^n \to R^n$ by $\tilde{\phi}(b_i) = v_i$. By construction, we have $\lambda \circ \tilde{\phi} = \phi \circ \lambda$, thus $\lambda \circ \tilde{\phi}^n = \phi^n \circ \lambda$ for all $n \geq 0$. Hence, it is sufficient to find a monic polynomial $Q(x) \in R[x]$ such that $Q(\tilde{\phi}) = 0$. We may therefore assume that $M = R^n$.

Now, ϕ is described by an $n \times n$ matrix $C \in \mathrm{Mat}_{n\times n}(R)$. We thus need to find a monic polynomial $Q(x) \in R[x]$ such that $Q(C) = 0$.

Let $h : \mathbb{Z}[x_{11}, x_{12}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}] \to R$ be a ring homomorphism sending x_{ij} to c_{ij}. Let D be a matrix whose image under h is C. If there is a monic polynomial $T(x) \in (\mathbb{Z}[x_{11}, x_{12}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}])[x]$ such that $T(D) = 0$, then the monic polynomial $Q(x)$ whose coefficients are images of the coefficients of $T(x)$ under h has the property that $Q(C) = 0$. Thus it is sufficient to show for $R = \mathbb{Z}[x_{11}, x_{12}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}]$.

Let K be the fraction field of R. The natural homomorphism of rings $R \to K$ is injective as $R = \mathbb{Z}[x_{11}, x_{12}, \ldots, x_{21}, x_{22}, \ldots, x_{nn}]$ is a domain. We may thus view R as a subring of K.

By Cayley-Hamilton, the polynomial $Q(x) = \det(xI - C) \in K[x]$ is monic and $Q(C) = 0$ when C is viewed as an element of $\mathrm{Mat}_{n\times n}(K)$. Since $Q(x)$ is a polynomial with coefficients of C, it has coefficients in R. $\square$

Proposition 4.1.4. *Let A be a subring of the ring B. Let $b \in B$ and let C be a sunbring of B containing A and b. Then,*

1. *If the element $b \in B$ is integral over A, then the A-algebra $A[b]$ is finitely generated as an A-module*

2. *If C is finitely generated as an A-module, then b is integral.*

Proof. (i) If b is integral over A, we have

$$b^n = -a_{n-1}b^{n-1} - \cdots - a_1 b - a_0$$

for some $a_i \in A$. Thus b^{n+k} is in the A-submodule of B generated by $1, b, \ldots, b^{n-1}$ for all $k \geq 0$. In particular, $A[b]$ is generated by $1, b, \ldots, b^{n-1}$ as an A-module.

(ii) Let $[b] : C \to C$ be the homomorphism of A-modules such that $[b](v) = b \cdot v$ for all $v \in C$. By Proposition 4.1.3, there is a monic polynomial $Q(x) \in A[x]$ such that $Q([b]) = 0$. In particular, taking $Q([b])(1)$ shows b is integral over A. ☐

Lemma 4.1.5 (Generalization of Tower Law). *let $\phi : R \to T$ be a homomorphism of rings and let N be a T-module. If T is finitely generated as an R-module and N is finitely generated as an T-module, N is finitely generated as an R-module.*

Proof. Suppose $t_1, \ldots, t_k \in T$ are generators of T as an R-module and $l_1, \ldots, l_s$ are generators of N as a T-module. Then, $t_i l_j$ are generators of N as an R-module. ☐

Corollary 4.1.6. *Let A be a subring of B. Let $b_1, \ldots, b_k \in B$ be integral over A. Then, $A[b_1, \ldots, b_k]$ is finitely generated as an A-module.*

Proof. By Proposition 4.1.4, $A[b_1]$ is finitely generated as an A-module, and $A[b_1, b_2] = A[b_1][b_2]$ is finitely generated as an $A[b_1]$-module, thus is finitely generated as an A-module. The proof follows by induction. ☐

Corollary 4.1.7. *Let A be a subring of B. The subset of elements of B which are integral over A form a subring of B.*

Proof. Let $b, c \in B$ be integral. Then, $b + c, bc \in A[b, c]$ and is finitely generated as an A-module. Thus by Proposition 4.1.4, $b + c$ and bc are integral over A. ☐

Definition 4.1.8. *Let $\phi : A \to B$ be a ring homomorphism. We say that B is **integral** over A if all the elements of B are integral over $\phi(A)$.*

*B is **finite** over A, or a **finite A-algebra** if B is a finitely generated $\phi(A)$-module.*

Note the identity that B is a finite A-algebra if and only if B is a finitely generated integral A-algebra.

Definition 4.1.9. *If A is a subring of a ring B, the set of elements of B which are integral over A is called the **integral closure** of A in B.*

*If A is a domain and K is the fraction field of A, A is said to be **integrally closed** if the integral closure of A in K is A.*

Example 4.1.10. $\mathbb{Z}$ is integrally closed, and if K is a field, so is $K[x]$. The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}(i)$.

Lemma 4.1.11. *Let $A \subseteq B \subseteq C$, wehere A is a subring of B and B is a subring of C. If B is integral over A and C is integral over B, then C is integral over A. Let $c \in C$. We have by assumption,*

$$c^n + b_{n-1}c^{n-1} + \cdots + b_0 = 0$$

for some $b_i \in B$. Define $B' = A[b_0, \ldots, b_{n-1}]$. We use Proposition 4.1.4. Now, c is integral over B' and so $B'[c]$ is finitely generated as a B'-module. Thus $B'[c]$ is finitely generated as an A-module. Thus c is integral over A.

Consequently, the integral closure in C of the integral closure of A in B is the integral closure of A in C.

Lemma 4.1.12. *Let A be a subring of B. Let S be a multiplicative subset of A. Suppose that B is integral (respectively finite) over A. Then the natural ring homomorphism $A_S \to B_S$ makes B_S into an integral (respectively finite) A_S-algebra.*

Proof. We first prove the integrality case. Suppose that B is integral over A. We use the natural ring homomorphism from $A_S \to B_S$. Note first that this map is injective.

Let $b/s \in B_S$ where $b \in B$ and $s \in S$. By assumption, we have

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

for some $a_i \in A$. Thus,

$$(b/s)^n + (a_{n-1}/s)(b/s)^{n-1} + \cdots + a_0/s^n = (1/s^n)(b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0) = 0/1$$

Thus, b/s is integral over A_S.

For the finiteness, suppose that $a_1, \ldots, a_k$ are generators for B as an A-module. Then $a_1/1, \ldots, a_k/1 \in B_S$ are generators of B_S as an A_S module, so B_S is also finite over A_S. □

Lemma 4.1.13. *Suppose that C is a subring of a ring D. Suppose that D is a domain and that D is integral over C. Then D is a field if and only if C is a field.*

Proof. If either of the rings is 0, then both are the 0 ring, and the proof follows. We now suppose that C and D are not the zero ring.

($\Rightarrow$) Suppose that D is a field. Let $c \in C \backslash \{0\}$. We want to show that $c^{-1} \in D$ lies in C. By assumption, D is integral over C, so there is a polynomial $P(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in C[t]$ such that $P(c^{-1}) = 0$ Thus, $c^{n-1}P(c^{-1}) = 0$. That is,

$$c^{-1} + a_{n-1} + \cdots + a_0 c^{n-1} = 0$$

implying that $c^{-1} \in C$.

($\Leftarrow$) Suppose that C is a field. Take $d \in D \backslash \{0\}$. We want to show that d has an inverse in D. Let $C[t] \to D$ be the C-algebra sending t to d. The kernel of this map is a prime ideal as D is a domain, and is non-zero as d is integral over C. Prime ideals are maximal in $C[t]$ as it is a PID, so the image of ϕ is a field, meaning d has an inverse in D. □

Corollary 4.1.14. *Let A be a subring of B and $\phi : A \to B$ be the inclusion map. Suppose that B is integral over A. Let $\mathfrak{q}$ be a prime ideal of B. Then $\mathfrak{q} \cap A$ is a maximal ideal of A if and only if $\mathfrak{q}$ is a maximal ideal of B.*

Proof. The induced map $A/(\mathfrak{q} \cap A) \to B/\mathfrak{q}$ is injective as the natural map from A to $B/\mathfrak{q}$ has kernel $\mathfrak{q} \cap A$. This makes $B/\mathfrak{q}$ into an integral $A/(\mathfrak{q} \cap A)$ algebra, by considering the same monic polynomial in $(A/(\mathfrak{p} \cap A)[x])$. Note that these are both domains, so the proof follows by Lemma 4.1.13. □

Theorem 4.1.15 (Going Up Theorem (Partial))**.** *Let A be a subring of B and let $\phi : A \to B$ be the inclusion map. Suppose that B is integral over A. Then* $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *is surjective.*

Proof. Write $B_\mathfrak{p}$ for the localisation $B_{\phi(A/\mathfrak{p})}$ of the ring B at the multiplicative set $\phi(A/\mathfrak{p})$. By lemma 2.1.12, B is isomorphic to the localisation of B at $\mathfrak{p}$ when B is viewed as an A-module. We thus have a unique ring homomorphism $\phi_\mathfrak{p} : A_\mathfrak{p} \to B_\mathfrak{p}$ such that $\phi_\mathfrak{p}(a/1) = \phi(a)/1$. Write $\lambda_A : A \to A_\mathfrak{p}$ and $\lambda_B : B \to B_\mathfrak{p}$ for the natural ring homomorphisms. Then, we have $\lambda_B \circ \phi = \phi_\mathfrak{p} \circ \lambda_A$. This induces a commutative diagram

$$\begin{tikzcd}
\mathrm{Spec}(B_\mathfrak{p}) \arrow[r, "\mathrm{Spec}(\lambda_B)"] \arrow[d, "\mathrm{Spec}(\phi_\mathfrak{p})"] & \mathrm{Spec}(B) \arrow[d, "\mathrm{Spec}(\phi)"] \\
\mathrm{Spec}(A_\mathfrak{p}) \arrow[r, "\mathrm{Spec}(\lambda_A)"] & \mathrm{Spec}(A)
\end{tikzcd}$$

By Lemma 2.1.22, $\mathfrak{p}$ is the image of the maximal ideal $\mathfrak{m}$ of $A_\mathfrak{p}$ under the map $\mathrm{Spec}(\lambda_A)$. Thus it suffices to show that there is a prime ideal $\mathfrak{q}$ in $B_\mathfrak{p}$ such that $\phi_\mathfrak{p}^{-1}(\mathfrak{q}) = \mathrm{Spec}(\phi_\mathfrak{p})(\mathfrak{q}) = \mathfrak{m}$. By Lemma 4.1.12, $B_\mathfrak{p}$ is integral over $A_\mathfrak{p}$. By Corollary 4.1.14, choosing any maximal ideal $\mathfrak{q}$ of $B_\mathfrak{p}$, $\phi_\mathfrak{p}^{-1}(\mathfrak{q})$ is also a maximal ideal. As $A_\mathfrak{p}$ is local, $m = \phi_\mathfrak{p}^{-1}(\mathfrak{q})$. □

Corollary 4.1.16. *Let $\phi : A \to B$ be a homomorphism of rings. Suppose that B is integral over A. Then the map* $\mathrm{Spec}(\phi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ *is closed.*

Proof. Let $\mathfrak{p}$ be an ideal of B. We want to show that $\mathrm{Spec}(\phi)(V(\mathfrak{p}))$ is closed in $\mathrm{Spec}(A)$. Let $q_\mathfrak{p} : B \to B/\mathfrak{p}$ be the quotient map, and define $\mu := q_\mathfrak{p} \circ \phi : A \to B_\mathfrak{p}$. Also let $q_\mu : A \to A/\ker(\mu)$ be the quotient map, and $\psi : A/\ker(\mu) \to B$ be the ring homomorphism induced by μ Then, we have the following commutative diagram :

$$\begin{tikzcd}
A \arrow[r, "\phi"] \arrow[d, "q_\mu"] \arrow[dr, "\mu"] & B \arrow[d, "q_\mathfrak{p}"] \\
A/\ker(\mu) \arrow[r, "\psi"] & B/\mathfrak{p}
\end{tikzcd}$$

As B is integral over A, $B/\mathfrak{p}$ is integral over $A/\ker(\mu)$. Also, ψ is injective by construction. By Theorem 4.1.15, we have $\mathrm{Spec}(\psi)(\mathrm{Spec}(B/\mathfrak{p})) = \mathrm{Spec}(A/\ker(\mu))$. By Lemma 3.4.4, we have

$$\mathrm{Spec}(q_\mathfrak{p})(\mathrm{Spec}(B/\mathfrak{p})) = V(\ker(q_\mathfrak{p})) = V(\mathfrak{p})$$

and

$$\mathrm{Spec}(q_\mu)(\mathrm{Spec}(A/\ker(\mu))) = V(\ker(\mu))$$

Thus, $\mathrm{Spec}(\phi)(V(\mathfrak{p})) = V(\ker(\mu))$, which is closed. □

Consequently, if ϕ is surjective, then $\mathrm{Spec}(\phi)$ is a closed map. Specifically, $\mathrm{Spec}(\phi)$ is injective and continuous, thus is a homeomorphism onto its image.

Proposition 4.1.17. *Let $\phi : A \to B$ be a ring homomorphism and suppose that B is finite over A. Then the map* $\mathrm{Spec}(\phi)$ *has finite fibres (for any $\mathfrak{p} \in \mathrm{Spec}(A)$, $\mathrm{Spec}(\phi)^{-1}(\{\mathfrak{p}\})$ is finite).*

Proof. Let $q : A \to A/\ker(\phi)$ be the quotient map. The map $\mathrm{Spec}(q)$ has finite fibres (by bijective correspondence between primes). We can therefore consider $A/\ker(\phi) \simeq \mathrm{im}(\phi)$ instead of A, and view it as a subring of B.

Now let $\mathfrak{p}$ be a prime ideal of A. We want to show that there are finitely many prime ideals $\mathfrak{q}$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ ($\mathfrak{q} \cap A$ is the preimage of $\mathfrak{q}$ under inclusion).

Let $\overline{\mathfrak{p}}$ be the ideal of B generated by $\mathfrak{p}$. Let ψ be the ring homomorphism induced by ϕ.

$$\begin{tikzcd}
\mathrm{Spec}(B/\overline{\mathfrak{p}}) \arrow[r, "\mathrm{Spec}(\overline{q})"'] \arrow[d, "\mathrm{Spec}(\psi)"'] & \mathrm{Spec}(B) \arrow[d, "\mathrm{Spec}(\phi)"] \arrow[dl] \\
\mathrm{Spec}(A/\mathfrak{p}) \arrow[r, "\mathrm{Spec}(q)"'] & \mathrm{Spec}(A)
\end{tikzcd}$$

Any prime ideal $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ has the property that $\mathfrak{q} \supseteq \overline{\mathfrak{p}}$, we see any such prime ideal lies in the image of $\mathrm{Spec}(\overline{q})$. The corresponding prime ideals of $\mathrm{Spec}(B/\overline{\mathfrak{p}})$ are prime ideals I such that $\psi^{-1}(I) = (0)$. Thus, it suffices to show that $\mathrm{Spec}(\psi)^{-1}((0))$ is a finite set.

Let $S = (A/\mathfrak{p})\backslash\{0\}$. Define $\lambda_{A/\mathfrak{p}} \to A/\mathfrak{p} \to (A/\mathfrak{p})_S$ and $\lambda_B/\overline{\mathfrak{p}} : B/\overline{\mathfrak{p}} \to (B/\overline{\mathfrak{p}})_{\psi(S)}$ be the natural ring homomorphisms. There is a natural ring homomorphism ψ_S that is compatible with these morphisms to obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{Spec}((B/\overline{\mathfrak{p}})_{\psi(S)}) \arrow[r, "\mathrm{Spec}(\lambda_{B/\overline{\mathfrak{p}}})"] \arrow[d, "\mathrm{Spec}(\psi_S)"] & \mathrm{Spec}(B/\overline{\mathfrak{p}}) \arrow[d, "\mathrm{Spec}(\psi)"] \\
\mathrm{Spec}((A/\mathfrak{p})_{\psi(S)}) \arrow[r, "\mathrm{Spec}(\lambda_{A/\mathfrak{p}})"] & \mathrm{Spec}(A/\mathfrak{p})
\end{tikzcd}$$

If $q \in \mathrm{Spec}(B/\overline{\mathfrak{p}})$, then $\psi^{-1}(\mathfrak{q}) = (0)$ if and only if $\mathfrak{q} \cap \psi(S) = \emptyset$.

□

5 Noether Normalization + Hilbert's Nullstellensatz

Theorem 5.0.1 (Noether's Normalization Lemma)**.** *Let K be a field and R be a non-zero finitely generated K-algebra. Then, there exists an injective homomorphism of K-algebras $K[y_1, \ldots, y_t] \to R$ for some $t \geq 0$ such that R is finite as a $K[y_1, \ldots, y_t]$ module.*

Proof. We only prove the case for when K is infinite.

Let $r_1, \ldots, r_n \in R$ be the generators of minimal size of R as a K-algebra. We prove by induction on n. If $n = 1$, then $R \simeq K[x]$ or $R \simeq K[x]/I$ for some proper ideal I in $K[x]$. In the first case, the proof follows by setting $t = 1$. In the second case, we set $t = 0$, noting that the K-dimension of $K[x]/I$ is bounded above by the degree of any non-zero polynomial in I. So this is true for $n = 1$.

Up to relabelling, we may assume there is a $k \in \{1, \ldots, n\}$ such that for all $i \in \{1, \ldots, k\}$, r_i is not algebraic over $K[r_1, \ldots, r_{i-1}]$ and that r_{k+i} is algebraic over $K[r_1, \ldots, r_k]$. We do this by repeatedly choosing elements that are not algebraic over $K[r_1, \ldots, r_k]$ from $k = 0$. In the case that every generator is algebraic over K, they are integral over K. Then setting $t = 0$, it follows $R = K[r_1, \ldots, r_n]$ is finite over K.

Now we may also assume that $k < n$, as else we may set $t = k = n$, sending x_i to the generators. Thus, r_n is algebraic over $K[r_1, \ldots, r_{n-1}]$. Let $P_1(x) \in K[r_1, \ldots, r_{n-1}][x]$ be a non-zero polynomial such that $P_1(r_n) = 0$. Since $K[r_1, \ldots, r_{n-1}]$ is the image of $K[x_1, \ldots, x_{n-1}]$ sending x_i to r_i, there is a non-zero polynomial

$$P(x_1, \ldots, x_n) \in K[x_1, \ldots, x_{n-1}][x_n] = K[x_1, \ldots, x_n]$$

such that $P(r_1, \ldots, r_n) = 0$.

Now let $F(x_1, \ldots, x_n)$ be the sum of monomials of degree $d = \deg(P)$ which appear in P, such that $\deg(P - F) < d$. Choose $\lambda_i \in K$ such that

$$F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$$

To see why such set exists, as F is a homogenous polynomial, the polynomial $F(x_1, \ldots, x_{n-1}, 1)$ is a sum of homogenous polynomials of distinct degrees and thus is non-zero (else by grouping we see the original polynomial is zero). This has some set that evaluates to a nonzero value, as K is infinite. To see this, we use the fact polynomials in $K[x]$ can only have finitely many roots, so it cannot vanish on every $F(x, \lambda_2, \ldots, \lambda_{n-1}, 1) \in K[x]$.

Setting $u_i = r_i - \lambda_i r_n$, we have

$$\begin{aligned} 0 &= P(r_1, \ldots, r_n) \\ &= P(u_1 + \lambda_1 r_n, \ldots, u_{n-1} + \lambda_{n-1} r_n, r_n) \\ &= F(\lambda_1, \ldots, \lambda_{n-1}, 1) r_n^d + O(r_n^{d-1}) \end{aligned}$$

In particular, r_n is integral over $K[u_1, \ldots, u_{n-1}]$. By the inductive hypothesis, there is an injective homomorphism of K-algebras

$$K[y_1, \ldots, y_t] \to K[u_1, \ldots, u_{n-1}]$$

for some $t \geq 0$ such that $K[u_1, \ldots, u_{n-1}]$ is integral over $K[y_1, \ldots, y_t]$. Thus, $R = K[r_1, \ldots, r_n] = K[u_1, \ldots, u_n - 1][r_n]$ is integral over $K[y_1, \ldots, y_t]$ (transitivity of integrality, algebraicity follows immediately). $\square$

Corollary 5.0.2 (Weak Nullstellensatz)**.** *Let K be a field and R be a finitely generated K-algebra. Suppose that R is a field. Then R is finite over K.*

Proof. Let $K[y_1, \ldots, y_t] \to R$ as in Noether's Normalization Lemma. By Theorem 4.1.15, $\mathrm{Spec}(R) \to \mathrm{Spec}(K[y_1, \ldots, y_t])$ is surjective. As R is a field, $\mathrm{Spec}(R)$ has one element, so $\mathrm{Spec}(K[y_1, \ldots, y_t])$ has one element. Thus $t = 0$ (else, consider the ideal (y_1), and note it is contained in some maximal ideal). Consequently, R is integral over K. As R is finitely generated over K, it must be finite over K. $\square$

Corollary 5.0.3. *Let K be an algebraically closed field. Let $t \geq 1$. The ideal of $K[x_1, \ldots, x_t]$ is maximal if and only if it has the form $(x_1 - a_1, \ldots, x_t - a_t)$ for some $a_1, \ldots, a_t \in K$. A polynomial Q lies in this ideal if and only if $Q(a_1, \ldots, a_t) = 0$.*

Proof. We start with the first statement. ($\Leftarrow$) The ideal $(x_1 - a_1, \ldots, x_t - a_t)$ is the kernel of the evaluation map

$$K[x_1, \ldots, x_t] \to K \qquad p(x_1, \ldots, x_t) \mapsto p(a_1, \ldots, a_t)$$

which is a surjective morphism onto a field, thus the kernel is a maximal ideal. ($\Rightarrow$) Suppose that I is maximal. $K[x_1, \ldots, x_t]/I$ is a field, which is also a finitely generated K-algebra. Thus, by Corollary 5.0.2, $K[x_1, \ldots, x_t]/I$ is finite, thus algebraic over K. As K is algebraically closed, $K[x_1, \ldots, x_t]/I \simeq K$.

$$\begin{tikzcd} K[x_1, \ldots, x_t] \arrow[d, "q_I"'] \arrow[dr, dashed, "\phi"] & \\ K[x_1, \ldots, x_t]/I \arrow[r, "\psi"'] & K \end{tikzcd}$$

Consider ϕ as the induced homomorphism of K-algebras. By construction, I contains the ideal $(x_1 - \phi(x_1), \ldots, x_t - \phi(x_t))$ (by isomorphism, as ϕ takes this to 0, q_I also takes this to 0). Ideals of this form are maximal, so in particular this coincides with I.

For the second part, note the homomorphism of K-algebras $\psi : K[x_1, \ldots, x_t] \to K$ such that $\psi(P(x_1, \ldots, x_t)) = P(a_1, \ldots, a_t)$ is surjective and the $\ker(\psi) \supseteq (x_1 - a_1, \ldots, x_t - a_t)$. As ψ is nonzero, $\ker(\psi)$ is maximal, and $\ker(\psi) = (x_1 - a_1, \ldots, x_t - a_t)$. □

Corollary 5.0.4. *Let K be a field. Let R be a finitely generated K-algebra. Then R is a Jacobson ring.*

Proof. Let $I \subseteq R$ be an ideal. We want to show that the Jacobson radical of I coincides with the radical of I. So, we want to show that the nilradical of R/I coincides with the Jacobson radical of (0) in R/I. Thus we may replace R with R/I and suppose that $I = (0)$.

Let $f \in R$ and suppose that f is not nilpotent. It is sufficient by showing that there exists a maximal ideal $\mathfrak{m}$ in R such that $f \notin \mathfrak{m}$. Let $S = \{1, f, f^2, \ldots\}$. As f is not nilpotent, the localisation is non-zero. Let $\mathfrak{q}$ be a maximal ideal of R_S. Since R_S is a finitely generated K-algebra, the quotient ring is also finitely generated over K. By weak Nullstellensatz, the canonical homomorphism of rings $K \to R_S/\mathfrak{q}$ makes $R_S/\mathfrak{q}$ into a finite field extension of K. Define ϕ to be the natural homomorphism that composes the homomorphisms from $R \to R_S$ and $R_S \to R_S/\mathfrak{q}$. Then $\mathrm{im}(\phi)$ is a domain, which is integral over K. By Lemma 4.1.13, this is a field. Thus $\ker(\phi)$ is maximal ideal of R.

By construction, $\ker(\phi)$ is the inverse image of $\mathfrak{q}$ by the natural homomorphism $R \to R_S$. As $f/1$ is a unit in R_S, $f/1 \notin \mathfrak{q}$, thus $f \notin \ker(\phi)$. We set $\mathfrak{m} = \ker(\phi)$ and are done. □

Corollary 5.0.5 (Strong Nullstellensatz)**.** *Let K be an algebraically closed field. Let $t \geq 1$ and $I \subseteq K[x_1, \ldots, x_t]$ be an ideal. Define*

$$Z(I) = \{(c_1, \ldots, c_t) \in K^n \mid P(c_1, \ldots, c_n) = 0 \text{ for all } P \in I\}$$

Let $Q(x_1, \ldots, x_t) \in K[x_1, \ldots, x_t]$. Then $Q \in \mathfrak{r}(I)$ if and only if $Q(c_1, \ldots, c_t) = 0$ for all $(c_1, \ldots, c_t) \in Z(I)$.

Proof. Let $R = K[x_1, \ldots, x_t]$.

($\Rightarrow$) Take any $Q \in \mathfrak{r}(I)$ and $(c_1, \ldots, c_t) \in Z(I)$. We want to show $Q(c_1, \ldots, c_t) = 0$. If $Q \in \mathfrak{r}(I)$, there exists some m such that $Q^m \in I$. Thus, $Q^m(c_1, \ldots, c_t) = 0$. As we are in a field, this shows $Q(c_1, \ldots, c_t) = 0$.

($\Leftarrow$) Let $Q(x_1, \ldots, x_t) \in K[x_1, \ldots, x_t]$ and suppose that $Q(c_1, \ldots, c_t) = 0$ for all $(c_1, \ldots, c_t) \in Z(I)$. Suppose for contradiction that $Q \notin \mathfrak{r}(I)$. By Corollary 5.0.4, R is a Jacobson ring, thus there exists a maximal ideal $\mathfrak{m} \supseteq I$ and $Q \notin \mathfrak{m}$.

By Corollary 5.0.3, we have $\mathfrak{m} = (x_1 - a_1, \ldots, x_t - a_t)$ for some a_i. By construction, $P(a_1, \ldots, a_t) = 0$ for all $P \in I \subseteq \mathfrak{m}$. Thus $(a_1, \ldots, a_t) \in Z(I)$. By Corollary 5.0.3 again, $Q(a_1, \ldots, a_t) \neq 0$ as $Q \notin \mathfrak{m}$, which is a contradiction. Thus $Q \in \mathfrak{r}(I)$. □

Lemma 5.0.6. *Let K be a field. Let $t \geq 1$ and let $P(x_1, \ldots, x_t)$ and let $P(x_1, \ldots, x_t) \in K[x_1, \ldots, x_t]$. Then there exists a non-zero prime ideal in $K[x_1, \ldots, x_t]$ which does not contain $P(x_1, \ldots x_t)$.*

Proof. Let $L = K(x_1, \ldots, x_{t-1})$ be the quotient field of $K[x_1, \ldots, x_{t-1}]$ where $L = K$ if $t = 1$. Let

$$\iota : K[x_1, \ldots, x_t] = K[x_1, \ldots, x_{t-1}][x_t] \to L[x_t]$$

be the natural injective map. If there is a prime ideal $\mathfrak{p}$ in $L[x_t]$ such that $\iota(P) \notin \mathfrak{p}$, the prime ideal $\iota^{-1}(\mathfrak{p})$ will not contain P, so we may assume that $t = 1$.

Write $x_t = x_1 = x$ so $K[x_1, \dots, x_t] = K[x]$. Assume without loss of generality that $P(x)$ is monic. Also assume that $P(x)$ is not constant (else any maximal ideal suffices).

Let Q be an irreducible factor of $1 + P$. The ideal (Q) does not contain P as else $(Q) = K[x]$, but (Q) is prime. □

Lemma 5.0.7 (Alternative Proof for Weak Nullstellensatz)**.** *Let K be a field and R be a finitely generated K-algebra. Suppose that R is a field. Then R is finite over K.*

Proof. Let $r_1, \dots, r_k$ be generators of R over K. Suppose that r_i are numbered in a way that $r_1, \dots, r_l$ are algebraically independent over K and that r_{k+l} are algebraic over $K(r_1, \dots, r_l)$.

We may also take $l \geq 1$ as else R is a finite field extension of K (as R is integral and finitely generated K-algebra), thus we are done.

As R is a field, the quotient field $L \simeq K(x_1, \dots, x_l)$ of $K[x_1, \dots, x_l] \simeq K[r_1, \dots, r_l]$ (by first isomorphism) can be viewed as a subfield of R. Now R is generated by $r_{l+1}, \dots, r_k$ as an L-algebra and generators are algebraic over L as they are algebraic over $K(r_1, \dots, r_l)$. As L is a field, they are integral over L, and thus R is a finite field extension of L.

By the Artin-Tate Lemma, L is finitely generated as an K-algebra. In particular $K(x_1, \dots, x_l) \simeq L$ is finitely generated as a $K[x_1, \dots, x_l]$ algebra. Let $P_1(x)/Q_1(x), \dots, P_a(x)/Q_a(x)$ be the generators of $K(x_1, \dots, x_l)$ as an $K[x_1, \dots, x_l]$-algebra. Let $Q(x) = \prod_{i=1}^{a} Q_i(x)$ and $S = \{1, Q(x), Q^2(x), \dots\}$. As $K[x_1, \dots, x_l]$ is a domain, the localisation $K[x_1, \dots, x_l]_S$ can be viewed as a subring of $K(x_1, \dots, x_l)$. As every element can be written as a quotient $R(x)/Q^b(x)$ for some $b \geq 0$, $K[x_1, \dots, x_l]_S = K(x_1, \dots, x_l)$. As the field has one prime ideal, we know that any non-zero prime ideal contains $Q(x)$.

This contradicts Lemma 5.0.6, thus $l = 0$, meaning R is a finite field extension of K. □

Lemma 5.0.8. *Let R ba a Jacobson ring. Suppose that R is a domain. Let $b \in R$ and $S = \{1, b, b^2, \dots\}$. Suppose that R_S is a field. Then R is a field.*

Proof. We know by Lemma 2.1.18, there is a bijective correspondence with prime ideals of R that don't meet b with the prime ideals of R_S. As R_S is a field, we only have the (0) ideal. Hence every non-zero prime ideal of R meets b.

Suppose for a contradiction that (0) is not the maximal ideal of R. The radical of (0) is just (0) as R is a domain, but as R is Jacobson, (0) is the intersection of maximal ideals of R, all of which should contain b, a contradiction. Thus (0) is a maximal ideal. R is thus a field. □

Corollary 5.0.9. *Let T be a field and $R \subseteq T$ be a subring. Suppose that R is Jacobson. Suppose also that T is finitely generated over R. Then R is a field. Consequently, T is finite over R.*

Proof. Let $K \subseteq T$ be the fraction field of R. By Weak Nullstellensatz, T is a finite extension of K. Let $t_1, \dots, t_k \in T$ be the generators of T as an R-algebra. Take the set of monic polynomial over K that annihalate t_i. Let b be the product of every denominator that appears as coefficients in thesep polynomials, and set $S = \{1, b, b^2, \dots\}$. Then there is a natural injective homomorphism of R-algebras from R_S into K as R is a domain, and we may view R_S as a sub-R-algebra of K. By construction T is generated by t_i as an R_S algebra and the elements are integral over R_S. Thus T is finite over R_S. By Lemma 4.1.13, R_S is a field. By 5.0.8, R is a field. □

Corollary 5.0.10. *Let T be a field and $R \subseteq T$ be a subring. Suppose that R is noetherian. Suppose also that T is finitely generated over R. Then R is a field. Again, thus, T is finite over R.*

Proof. Let $K \subseteq T$ be the fraction field of R. By Weak Nullstellensatz T is a finite extension of K. Then K is finitely generated over R by Artin Tate. By taking the generators and multiplying the denominators together, we can form a multiplicative set generated by a single element of R such that $K = R_S$. Thus R is a field by Lemma 5.0.8. ☐

Corollary 5.0.11. *Let $\psi : R \to T$ be a homomorphism of rings. Suppose that R is Jacobson and that T is a finitely generated R algebra. Let $\mathfrak{m}$ be a maximal ideal of T. Then $\psi^{-1}(\mathfrak{m})$ is a maximal ideal of R and the induced map $R/\psi^{-1}(\mathfrak{m}) \to T/\mathfrak{m}$ makes $T/\mathfrak{m}$ into a finite field extension of $R/\psi^{-1}(\mathfrak{m})$.*

Proof. Note that $T/\mathfrak{m}$ is a field that is finitely generated over $R/\psi^{-1}(\mathfrak{m})$

$$\begin{tikzcd}
 & R \arrow[rr, "q_{\psi^{-1}(\mathfrak{m})}"] \arrow[dl, "\iota"'] \arrow[dd, "\psi"] & & R/\psi^{-1}(\mathfrak{m}) \arrow[dl] \arrow[dd, dashed] \\
R[x_1, \dots, x_n] \arrow[rr, dashed] \arrow[dr, two heads] & & R/\psi^{-1}(\mathfrak{m})[x_1, \dots, x_n] \arrow[dr, dashed] & \\
 & T \arrow[rr, "q_{\mathfrak{m}}"] & & T/\mathfrak{m}
\end{tikzcd}$$

Quotients of Jacobson ring are Jacobson, so it follows by Corollary 5.0.9. ☐

Theorem 5.0.12. *A finitely generated algebra over a Jacobson ring is Jacobson.*

Proof. Let R be a Jacobson ring and T be a finitely generated R-algebra. Let $I \subseteq T$ be an ideal. We want to show that the Jacobson radical of I of T coincides with the radical of I. Thus, we want to show that the nilradical of T/I coincides with the Jacobson radical of the zero ideal in T/I. As T/I is also finitely generated over R, we may replace T by T/I and suppose that $I = 0$.

Suppose that $f \in T$ and that f is not nilpotent. We want to show that there exists a maximal ideal $\mathfrak{m}$ in T such that $f \notin \mathfrak{m}$. Let $S = \{1, f, f^2, \dots\}$. By non-nilpotence, the localisation is not the zero-ring. Let $\mathfrak{q}$ be a maximal ideal of T_S. T_S is a finitely generated R-algebra as T is a finitely generated R-algebra, thus $T_S/\mathfrak{q}$ is finitely generated over R.

Let ϕ be the canonical ring homomorphism. From Corollary 5.0.11, noting that the kernel of ϕ is just the preimage of $\mathfrak{q}$ in R, we see that $\ker(\phi)$ is a maximal ideal and $T_S/\mathfrak{q}$ is a finite field extension of $R/\ker(\phi)$.

$$\begin{tikzcd}
R \arrow[r] \arrow[d] \arrow[dr, "\phi"] & R/\ker(\phi) \arrow[d, hook, dashed] \\
T_S \arrow[r] & T_S/\mathfrak{q}
\end{tikzcd}$$

Considering the natural map $\Phi : T \to T_S/\mathfrak{q}$, the image $\mathrm{im}(\Phi)$ is an R-subalgebra, thus a $R/\ker(\phi)$-subalgebra of $T_S/\mathfrak{q}$. As $T_S/\mathfrak{q}$ is integral over $R/\ker(\phi)$, $\mathrm{im}(\Phi)$ is integral over $R/\ker(\phi)$, by Lemma 4.1.13, is a field. Thus, $\ker(\Phi)$ is a maximal ideal of T. By construction, $\ker(\Phi)$ is the inverse image of $\mathfrak{q}$ by the natural homomorphism $T \to T_S$ and $f/1 \notin \mathfrak{q}$ as f is a unit in T_S. Thus $f \notin \ker(\Phi)$. The proof concludes by choosing $\mathfrak{m} = \ker(\Phi)$. ☐

Remark 5.0.13. Noting that $\mathbb{Z}$ is Jacobson, any finitely generated algebra over $\mathbb{Z}$ is a Jacobson ring.

6 Dimension

Definition 6.0.1. *Let R be a ring. The* ***dimension*** *of R is*

$$\dim(R) = \sup\{n \mid \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n, \mathfrak{p}_0, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(R)\}$$

If $\mathfrak{p}$ is a prime ideal of R, the ***codimension*** *(or* ***height****) of $\mathfrak{p}$ is*

$$\operatorname{ht}(\mathfrak{p}) = \sup\{n \mid \mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n, \mathfrak{p}_0, \ldots, \mathfrak{p}_n \in \operatorname{Spec}(R)\}$$

Note that dimension need not be finite. Note that if $\mathfrak{q}$ is a prime ideal and $\mathfrak{q} \subsetneq \mathfrak{p}$, then $\operatorname{ht}(\mathfrak{p}) > \operatorname{ht}(\mathfrak{q})$ given that $\operatorname{ht}(\mathfrak{p})$ is finite. If N is the nilradical of R, then it is contained in every prime ideal of R, thus

$$\dim(R) = \dim(R/N)$$

where $\operatorname{ht}(\mathfrak{p} \bmod N) = \operatorname{ht}(\mathfrak{p})$. Finally,

$$\dim(R) = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R)\}$$

Notably, for any ideal $I \subseteq R$, $\dim(R) \geq \dim(R/I)$ by bijective correspondence of ideals.

Lemma 6.0.2. *Let R be a ring and $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $\operatorname{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}})$. Also,*

$$\dim(R) = \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \textit{ is a maximal ideal of } R\}$$

Proof. By Lemma 2.1.18, the primes in $R_{\mathfrak{p}}$ are in one to one correspondence with the prime ideals contained in $\mathfrak{p}$. The correspondence preserves inclusion. Thus the first case follows immediately.

For the second case, note that

$$\dim(R) \geq \sup\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \text{ is a maximal ideal of } R\}$$

so we only need the reverse inequality. For this, suppose $\mathfrak{p}$ is a prime ideal which is not maximal. Consider a chain of prime ideals

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

and let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. Then we have a chain

$$\mathfrak{m} \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

thus $\operatorname{ht}(\mathfrak{m}) \geq \operatorname{ht}(\mathfrak{p})$, and hence follows. □

Remark 6.0.3. We record a consequence of the previous lemma. If R is a ring and S is a multiplicative subset of R. Let $\mathfrak{p}$ be a prime ideal of R_S and $\lambda : R \to R_S$ be the natural ring homomorphism. Then $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\lambda^{-1}(\mathfrak{p}))$ by Lemma 2.1.18.

Definition 6.0.4. *Let R be a ring and $I \subseteq R$ be an ideal. Define the* ***codimension*** *or* ***height*** *$\operatorname{ht}(I)$ of I as*

$$\operatorname{ht}(I) = \min\{\operatorname{ht}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(R), \mathfrak{p} \supseteq I\}$$

This is a generalization of the definition from prime ideals to ideals. By definition, if J is another ideal such that $J \subseteq I$, then $\operatorname{ht}(J) \leq \operatorname{ht}(I)$. Also, by definition, given $\operatorname{ht}(I) < \infty$, there is some prime ideal $\mathfrak{p}$ which is minimal among the prime ideals containing I such that $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(I)$.

Definition 6.0.5. *Let k be a field and K be a field containing k. If $S \subseteq K$ is a finite subset of K, write $k(S)$ for the smallest subfield of K containing k and S. By construction, this is isomorphic to the field of fractions of the k-algebra $k[S] \subseteq K$. As usual, we write $k(\alpha_1, \ldots, \alpha_n)$ for $k(\{\alpha_1, \ldots, \alpha_n\})$.*

Note the identity, $k(S_1 \cup S_2) = k(S_1)(S_2)$ (by definition).

Lemma 6.0.6. *If the elements of a finite S are algebraic over k, then $k(S) = k[S]$.*

Proof. It suffices to show the case for one element and use the identity above for induction. We now have a homomorphism $k[t] \to K$ that sends t to s. As the image of this map is a domain, the kernel is a prime ideal, and is non-zero as s is algebraic over k. As $k[t]$ is a PID, non-zero prime ideals are maximal. Thus, $k[s]$ is a field. $\square$

Also note that if all the elements of S are algebraic over k, then it is integral over k, $k(S)$ is a finite extension of k.

If there is a finite subset S of K such that $K = k(S)$, we say that K is finitely generated over k as a field. This is strictly weaker than a finitely generated k-algebra (consider $k(x)$), but coincides when all the elements of S are algebraic over k.

Definition 6.0.7. *Let S be subset of K. Then S is a* ***finite transcendence basis*** *of K over k if*

- *S is finite*
- *the elements of S are algebraically independent over k*
- *K is algebraic over the field $k(S)$*

Lemma 6.0.8. *If K is finitely generated over k as a field, then K has a transcendence basis over k.*

Proof. Start with a finite set S such that $K = k(S)$. Take a subset S' that is algebraically independent with maximal cardinality. Then, the elements of $S \backslash S'$ are algebraic over $k(S')$ and thus K is algebraic over $k(S')$. This gives a transcendence basis over k. $\square$

Proposition 6.0.9. *Let K be a field and $k \subseteq K$ be a subfield. Suppose that K is finitely generated over k as a field. Let S and T be two transcendence bases of K over k. Then $|S| = |T|$.*

Proof. Write $S = \{\gamma_1, \ldots, \gamma_n\}$ and $T = \{\rho_1, \ldots, \rho_m\}$ such that $n = |S|$ and $m = |T|$. We will show $m = n$ by induction on $\min(m, n)$.

In the case $\min(m, n) = 0$, either S or T is empty, so K is algebraic over k, meaning both S and T must be empty.

Without loss of generality, we may assume that $S \cap T = \emptyset$. To see this, suppose that $S \cap T = U$ and $U \neq \emptyset$. Then, $S \backslash U$ and $T \backslash U$ are transcendence bases for K over $k(U)$. Also,

$$\min(|S \backslash U|, |T \backslash U|) = \min(m, n) - |U|$$

Thus by induction, $|S \backslash U| = |T \backslash U|$, so $|S| = |T|$.

We also claim that m or n is minimal among the cardinalities of all possible transcendence bases of K over k. To see this, suppose that without loss of generality that $m \leq n$ such that $m = \min(m, n)$. Suppose that $m = |T|$ is not minimal. Choose a transcendence basis T' of K over k such that $|T'| < m$ that is minimal. Then, $\min(|T|, |T'|) < \min(m, n)$, thus by induction $|T'| = |T| = m$, a contradiction. Consequently, m is minimal.

Suppose without loss of generality that m is minimal among the cardinalities of all possible transcendence bases of K over k, swapping S and T if necessary. By assumption, there is a non-zero polynomial

$$P(x_0, \ldots, x_m) \in k[x_0, \ldots, x_m]$$

such that $P(\gamma_1, \rho_1, \ldots, \rho_m) = 0$. To see this, note that γ_1 is algebraic over $k(\rho_1, \ldots, \rho_m) \simeq \mathrm{Frac}(k[x_1, \ldots, x_m])$, thus there is a non-zero annihalating polynomial for γ_1. We can thus make a polynomial over $k[x_1, \ldots, x_m]$ that annihalates γ_1. Take P to be of minimal degree with such property.

By assumption, $P(x_0, \ldots, x_m)$ contains monomials with positive powers of x_k for some $k \geq 1$, as else γ_1 is algebraic over k. By reordering, suppose this is x_1. Thus,

$$P(x_0, \ldots, x_m) = \sum_j P_j(x_0, x_2, \ldots, x_m) x_1^j$$

As P contains monomials with positive powers of x_1, there is some $j_0 > 0$ such that $P_{j_0}(x_0, x_2, \ldots, x_m) \neq 0$. Take a maximal such j_0. Also, $P_{j_0}(\gamma_1, \ldots, \rho_2, \ldots, \rho_m) \neq 0$ by the minimality of the degree of P. Then, as

$$P(\gamma_1, \rho_1, \ldots, \rho_m) = \sum_j P_j(\gamma_1, \rho_2, \ldots, \rho_m) \rho_1^j = 0$$

we see that ρ_1 is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$.

Hence, $k(\gamma_1, \rho_1, \ldots, \rho_m)$ is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$ and thus K is algebraic over $k(\gamma_1, \rho_2, \ldots, \rho_m)$ (by using Proposition 4.1.4 and Corollary 4.1.6).

As m is minimal, γ_1 is algebraically independent with $\rho_2, \ldots, \rho_m$, thus $\{\gamma_1, \rho_2, \ldots, \rho_m\}$ is a transcendence basis of K. In particular, $\{\gamma_2, \ldots, \gamma_n\}$ and $\{\rho_2, \ldots, \rho_m\}$ are transcendence bases of K over $k(\gamma_1)$. By induction, $m - 1 = n - 1$, so the proof follows. $\square$

Definition 6.0.10. *Let k be a subfield of K and suppose that K is finitely generated over k as a field. Following the previous Proposition, define the **transcendence degree** $\mathrm{tr}(K|k)$ of k over K as the cardinality of any transcendence basis of K over k.*

For example, $\mathrm{tr}(k(x_1, \ldots, x_n)|k) = n$ for any field k.

Definition 6.0.11. *A **ring grading** on R is the datum of a sequence $R_0, R_1, \ldots$ of additive subgroups of R such that $R = \bigoplus_{i \geq 0} R_i$ and $R_i \cdot R_j \subseteq R_{i+j}$.*

*If $r \in R$, write $[r]_i$ for the projection of r to R_i and is called the i**-th graded component** of r.*

By definition, R_0 is a subring of R and for any i_0, $\bigoplus_{i \geq i_0} R_i$ is an ideal of R. Each R_i naturally carries a structure of an R_0-module.

Finally, the natural map $R_0 \to R/(\bigoplus_{i \geq 1} R_i)$ is an isomorphism of rings (as the natural map from $R \to R_0$ has kernel $\bigoplus_{i \geq 1} R_i$). In general, there is a natural isomorphism of R_0 modules $R_{i_0} \simeq (\bigoplus_{i \geq i_0} R_i)/(\bigoplus_{i \geq i_0+1} R_i)$ for any $i_0 \geq 0$, by first isomorphism theorem by considering it's natural map.

If k is a field, then the ring $k[x]$ has a natural grading given by $(k[x])_i = \{a \cdot x^i \mid a \in k\}$. Any ring carries a trivial grading such that $R_0 = R$ and $R_i = 0$ for all $i \geq 0$.

Definition 6.0.12. *Suppose that R is a graded ring. Suppose further that M is an R-module. A grading on M (relative to the grading on R) is the datum of a sequence $M_0, M_1, \ldots$ of additive subgroups of M such that $M = \bigoplus_{i \geq 0} M_i$ and $R_i \cdot M_j \subseteq M_{i+j}$. Then, we say that M is **graded as a R-module** (but the underlying grading of R is important).*

Lemma 6.0.13. *Let R be a graded ring with grading $R_i, (i \geq 0)$. The following are equivalent*

1. *The ring R is noetherian*

2. *The ring R_0 is noetherian and R is finitely generated as an R_0-algebra*

Proof. The implication $(ii) \implies (i)$ is a consequence of the Hilbert's basis theorem and Lemma 3.6.4.

We show the implication $(i) \implies (ii)$. Note first the ring R_0 is noetherian as it is a quotient of a noetherian ring. We now want to show that R is finitely generated as an R_0-algebra.

Let $a_1, \ldots, a_k$ be the generators of $\bigoplus_{i>0} R_i$ viewed as an ideal of R (as R is noetherian). We claim that the component of a_i generate R as an R_0-algebra, noting that each a_i has finitely many graded components.

We proceed by induction on $i \geq 0$ that R_i lies inside the R_0-subalgebra generated by the graded components of $a_1, \ldots, a_k$. As R is generated by all the R_i, this proves the claim. The claim is immediate for $i = 0$. Suppose that $i > 0$ and $R_0, \ldots, R_{i-1}$ all lie inside the R_0-subalgebra generated by the graded components of $a_1, \ldots, a_k$.

Let $r \in R_i$. By assumption, there are elements $t_i, \ldots, t_k \in R$ such that $r = t_1 a_1 + \cdots + t_k a_k$ (as they generate $\bigoplus_{i>0} R_i$). Now,

$$r = [r]_i = \sum_{j=1}^{k} \sum_{u=1}^{i} [t_j]_{i-u} [a_j]_u$$

Noting that $[t_j]_{i-u} \in R_0 \oplus R_1 \oplus \cdots \oplus R_{i-1}$, $[t_j]_{i-u}$ lies in the R_0-subalgebra generated by the graded components of $a_1, \ldots, a_k$ by the inducitve hypothesis. Now r lies in the R_0-subalgebra also, thus completes the proof. $\square$

Definition 6.0.14. *Let R be a ring and M be an R-module. A **descending filtration** $M_\bullet$ of M is a sequence of R-submodules*

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

*of M. If I is an ideal of R, then $M_\bullet$ is said to be an I-**filtration** if $IM_i \subseteq M_{i+1}$ for all $i \geq 0$. An I-filtration $M_\bullet$ is said to be **stable** if $IM_i = M_{i+1}$ for all i larger than some fixed natural number.*

Definition 6.0.15. *Suppose we have a ring R and an ideal I of R, an R-module M and an I-filtration $M_\bullet$ on M. The directed sum of R-modules $R^\# = \bigoplus_{i \geq 0} I^i$ as an external sum (where $I^0 = R$) carries a natural structure of a graded ring, with the grading given as follows.*

*If $\alpha \in I^i$ and $\beta \in I^j$, then the product of α and β in $R^\#$ is given by the product of α and β in R, viewed as an element of I^{i+j}. The ring $R^\#$ is often called the **blow-up algebra** associated with R and I.*

The directed sum $M^\# = \bigoplus_{i \geq 0} M_i$ of R-modules carries a natural structure of graded $R^\#$ module, where if $a \in I^i$ and $\beta \in M_j$, the multiplication is of β by α in M viewed as an element in M_{i+j}, which it lies in as $M_\bullet$ is an I-filtration.

We can view $R^\#$ as an R-algebra by the natural injective map from $r \in R$ to the corresponding element of degree 0. The R-module structure on $M^\#$ is given by $M^\#$ viewed as a direct sum of R-modules.

Lemma 6.0.16. *Let R be a ring and $I \subseteq R$ be an ideal. Suppose that R is noetherian. Then the ring $R^\#$ associated with R and I is also noetherian.*

Proof. Let $r_1, \ldots, r_k \in I$ be generators of I (which exists as R is noetherian). There is a homomorphism of rings $\phi : R[x_1, \ldots, x_k] \to R^\#$ by $P(x_1, \ldots, x_k) \mapsto P(r_1, \ldots, r_k)$ where $r_1, \ldots, r_k$ are viewed as elements of degree 1 in $R^\#$ and the coefficients of the polynomial are viewed as elements of degree 0, such that ϕ is a homomorphism of R-algebras.

By construction, ϕ is surjective, thus $R^\#$ is surjective, thus finitely generated R-algebra, thus noetherian by Hilbert basis and Lemma 3.6.4. $\square$

Lemma 6.0.17. *Let R be a ring. Let $I \subseteq R$ be an ideal. Let $M_\bullet$ be an I-filtration on M. Suppose that M_j is finitely generated as an R-module for all $j \geq 0$. Let $R^\#$ be the corresponding graded ring and $M^\#$ be the corresponding graded $R^\#$ module. The following are equivalent*

1. *The $R^\#$ module $M^\#$ is fintiely generated*
2. *The filtration $M_\bullet$ is stable*

Proof. Let $n \geq 0$ and consider the graded subgroup

$$M^\#_{(n)} = (\bigoplus_{j=0}^{n} M_j) \bigoplus (\bigoplus_{k=1}^{\infty} I^k M_n)$$

of $M^\#$ (where the left side is the n-head of $M^\#$ and the right is the subgroup tails of M_{n+k}). Note that each $M^\#_{(n)}$ is a $R^\#$-submodule of $M^\#$ by construction. Also, each M_j with $j \in \{0, \ldots, n\}$ is finitely generated as an R-module by assumption, and thus $M^\#_{(n)}$ is finitely generated as an $R^\#$-module (generated by $\bigoplus_{j=0}^n M_j$). We also have the inclusions

$$M^\#_{(0)} \subseteq M^\#_{(1)} \subseteq M^\#_{(2)} \subseteq \cdots$$

and $M^\# = \bigcup_{i=0}^\infty M^\#_{(i)}$.

Also, saying that the I-filtration $M_\bullet$ is stable is equivalent to saying that $M^\#_{(n_0+k)} = M^\#_{(n_0)}$ for all $k \geq 0$ and some $n_0 \geq 0$. We claim this is the case if and only if $M^\#$ is finitely generated as an $R^\#$ module.

If $M^\#$ is finitely generated as an $R^\#$-module, then as there exists some n_0 such that $M^\#_{(n_0)}$ contains all generators, the proof follows. On the other hand, if $M^\#_{(n_0+k)} = M^\#_{(n_0)}$ for all $k \geq 0$, then $M^\# = M^\#_{(n_0)}$, which we know is finitely generated. $\square$

Proposition 6.0.18 (Artin-Rees Lemma)**.** *Let R be a noetherian ring. Let $I \subseteq R$ be an ideal. Let M be a finitely generated R-module and let $M_\bullet$ be a stable I-filtration on M. Let $N \subseteq M$ be a submodule. Then the filtration $N \cap M_\bullet$ is a stable I-filtration of N.*

Proof. By construction, there is a natural inclusion of $R^\#$-modules $N^\# \subseteq M^\#$. By Lemma 6.0.17, the $R^\#$ module is finitely generated. By Lemma 3.6.6, noting $R^\#$ is noetherian by Lemma 6.0.16, submodules of finitely generated modules are finitely generated, thus $N^\#$ is finitely generated. Thus the filtration $N \cap M_\bullet = N_\bullet$ is a stable I-filtration of N. $\square$

Corollary 6.0.19. *Let R be a noetherian ring. Let $I \subseteq R$ be an ideal and let M be a finitely generated R-module. Let $N \subseteq M$ be a submodule. Then, there is a natural number $n_0 \geq 0$ such that*

$$I^n(I^{n_0}M \cap N) = I^{n_0+n}M \cap N$$

for all $n \geq 0$.

Proof. Apply Artin-Rees to the filtration $I^\bullet M = \bigoplus_{i\geq 0} I^i M$ of M. $\square$

Corollary 6.0.20 (Krull's Theorem)**.** *Let R be a noetherian ring. Let $I \subseteq R$ be an ideal and let M be a finitely generated R-module. Then,*

$$\bigcap_{n\geq 0} I^n M = \bigcup_{r\in 1+I} \ker([r])$$

where $[r] : M \to M$ is defined by $m \mapsto r \cdot m$.

Proof. Let $N = \bigcap_{n\geq 0} I^n M$. By Corollary 6.0.19, there is a natural number $n_0 \geq 0$ such that

$$I(I^{n_0} M \cap N) = IN = I^{n_0+1} M \cap N = N$$

By using the general form of Nakayama's Lemma, there exists some $r \in 1 + I$ such that $rN = 0$. Hence $N = \bigcap_{n\geq 0} I^n M \subseteq \bigcup_{r\in 1+I} \ker(r_M)$.

On the other hand, if $r \in 1 + I$, $y \in M$ and $ry = 0$, $(1 + a)y = y + ay = 0$ for some $a \in I$, thus $y \in IM$. By the same logic, $y \in I^2 M$ and so on, giving $y \in N$. $\square$

Corollary 6.0.21 (of Krull's Theorem)**.** *Let R be a noetherian domain. Let I be a proper ideal of R. Then $\bigcap_{n\geq 0} I^n = 0$.*

Proof. Apply Krull's Theorem with $M = R$ and notice that for a nonzero r, $[r]$ always has 0 kernel in a domain. Clearly $0 \notin 1 + I$ as I is proper. $\square$

Corollary 6.0.22 (of Krull's Theorem)**.** *Let R be a noetherian ring and I be an ideal of R. Let M be a finitely generated R-module. Suppose that I is contained in the Jacobson radical of R. Then $\bigcap_{n\geq 0} I^n M = 0$.*

Proof. If $r \in 1+I$, then r is a unit. Else, r is contained in some maximal ideal $\mathfrak{m}$. As I is contained in the Jacobson radical of R, it is contained in $\mathfrak{m}$. But now 1 is contained in $\mathfrak{m}$, a contradiction. Thus $\ker(r_M) = 0$, and the result follows by Krull's Theorem. $\square$

The final corollary is especially useful when R is local, as then any proper ideal I is always contained in the Jacobson radical.

Definition 6.0.23. *We say that a ring is **Artinian** if whenever we have a descending sequence of ideals*

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

in R, then there exists an $n \geq 1$ such that $I_{n+k} = I_n$ for all $k \geq 0$. Then, we say that the sequence $I_\bullet$ stabilises.

Lemma 6.0.24. *Let R be a noetherian local ring with maximal ideal $\mathfrak{m}$. The following are equivalent*

1. $\dim(R) = 0$
2. *$\mathfrak{m}$ is the nilradical of R*
3. *$\mathfrak{m}^n = 0$ for some $n \geq 1$*
4. *R is Artinian*

Proof. $(i) \implies (ii)$ If $\dim(R) = 0$, then every prime ideal of R coincides with $\mathfrak{m}$. Thus $\mathfrak{m}$ is the nilradical of R.

$(ii) \implies (iii)$ Is a consequence of Lemma 3.6.7.

$(iii) \implies (iv)$ Let $I_1 \supseteq I_2 \supseteq \cdots$ be a descending chain of ideals in R. Let $k \geq 0$ be the minimal natural number such that the sequence

$$\mathfrak{m}^k I_1 \supseteq m^k I_2 \supseteq \cdots$$

stabilises. Note that such k exists as $\mathfrak{m}^k = 0$ for some $k \geq 0$. Suppose for a contradiction that $k > 0$. Let $n_0 \geq 1$ be such that $\mathfrak{m}^k I_n = \mathfrak{m}^k I_{n_0}$ for all $n \geq n_0$. Consider the descending sequence

$$\mathfrak{m}^{k-1} I_1 \supseteq \mathfrak{m}^{k-1} I_2 \supseteq \cdots$$

By construction, $\mathfrak{m}^{k-1} I_n \supseteq \mathfrak{m}^k I_{n_0}$ for all $n \geq 1$. Thus, we have the natural inclusions

$$\mathfrak{m}^{k-1} I_1 / \mathfrak{m}^k I_{n_0} \supseteq m^{k-1} I_2 / \mathfrak{m}^k I_{n_0} \supseteq \cdots$$

and for $n \geq n_0$, $\mathfrak{m}(\mathfrak{m}^{k-1} I_n / \mathfrak{m}^k I_{n_0}) = 0$. Thus $(\mathfrak{m}^{k-1} I_n / \mathfrak{m}^k I_{n_0})$ has a natural structure of a $R/\mathfrak{m}$-module if $n \geq n_0$. In particular,

$$\mathfrak{m}^{k-1} I_{n_0} / \mathfrak{m}^k I_{n_0} \supseteq m^{k-1} I_{n_0+1} / \mathfrak{m}^k I_{n_0} \supseteq \cdots$$

is a decreasing sequence of $R/\mathfrak{m}$-modules. These modules (ideals) are finitely generated as R is a noetherian ring.

As $R/\mathfrak{m}$ is a field, we therefore have a descreasing sequence of finite dimensional vector spaces, which must stabilise. Let $n_1 \geq n_0$ be such that

$$\mathfrak{m}^{k-1} I_n / \mathfrak{m}^k I_{n_0} = m^{k-1} I_{n_1} / \mathfrak{m}^k I_{n_0}$$

for all $n \geq n_1$. Then, $\mathfrak{m}^{k-1} I_{n_1} = \mathfrak{m}^{k-1} I_n$. In particular, the sequence $\mathfrak{m}^{k-1} I_n$ also stabilises. This contradicts the minimality of k, thus $k = 0$.

$(iv) \implies (i)$ Suppose that R is Artinian but $\dim(R) \neq 0$. In particular, we can find a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \subsetneq \mathfrak{m}$. Then $\mathfrak{m}$ is not the nilradical of R as it is contained in $\mathfrak{p}$.

As R is Artinian, we know there is a natural number $n_0 \geq 0$ such that $\mathfrak{m}^{n_0} = \bigcap_{i=0}^{\infty} \mathfrak{m}^i$. By Corollary 6.0.22, this equals 0. In particular, $\mathfrak{m}$ is the nilradical of R, a contradiction. ☐

Theorem 6.0.25 (Krull's principal ideal theorem)**.** *Let R be a noetherian ring. Let $f \in R$ be an element which is not a unit. Let $\mathfrak{p}$ be minimal among the prime ideals containing f. Then* $\mathrm{ht}(\mathfrak{p}) \leq 1$*.*

Proof. Note that the maximal ideal of $R_{\mathfrak{p}}$ is minimal among the prime ideals of $R_{\mathfrak{p}}$ containing $f/1 \in R_{\mathfrak{p}}$ (by bijective correspondence). Furthermore, the height of $\mathfrak{p}$ is the same as the height of the maximal ideal of $R_{\mathfrak{p}}$. As $R_{\mathfrak{p}}$ is also noetherian, we may suppose that R is local and that $\mathfrak{p}$ is a maximal ideal.

Now let $\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_{k_0}$ be a chain ideals starting with $\mathfrak{p}$. We wish to show that $k_0 \leq 1$. We may suppose that $k_0 > 0$ as else there is nothing to prove.

Write $\mathfrak{q} = \mathfrak{p}_1$. By assumption, $f \notin \mathfrak{q}$. Write $\lambda : R \to R_{\mathfrak{q}}$ for the natural map. For $n \geq 1$, write $\overline{\lambda(\mathfrak{q}^n)}$ for the ideal of $R_{\mathfrak{q}}$ generated by $\lambda(\mathfrak{q}^n)$. We know that $\overline{\lambda(\mathfrak{q}^n)}$ consists of elements of the form r/t where $r \in \mathfrak{q}^n$ and $t \in R \backslash \mathfrak{q}$. Note also the identity $\overline{\lambda(\mathfrak{q}^n)} = \overline{\lambda(\mathfrak{q})}^n$.

Now consider the ideal $I_n = \lambda^{-1}(\overline{\lambda(\mathfrak{q}^n)})$. By construction, we have $I_n \supseteq \mathfrak{q}^n$. Also, by bijective correspondence, $I_1 = \mathfrak{q}$. Note the difference in property is that if $fr \in I_n$ for any $r \in R$, then $r \in I_n$

as $\lambda(fr)(1/f) = \lambda(r) \in \overline{\lambda(\mathfrak{q}^n)}$. Consider the ring $R/(f)$. This is local as R is local. It is a quotient ring of a noetherian ring, so it is also noetherian. The ring $R/(f)$ has dimension 0 as the maximal ideal ($\mathfrak{p}$ mod (f)) is a minimal prime ideal of $R/(f)$ by construction. We now have a descending sequence of ideals $I_1 \supseteq I_2 \supseteq \cdots$. By Lemma 6.0.24, the image of this sequence in $R/(f)$ must stabilise. Thus, there is some $n_0 \geq 1$ such that for any $n \geq n_0$, $I_n \subseteq I_{n+1} + (f)$. Also, if $r \in I_n$, for any $t \in I_{n+1}$ and $h \in R$ such that $r = t + hf$, as $r - t \in I_n$, and $hf \in I_n$ so $h \in I_n$, shows that $I_n \subseteq I_{n+1} + (f)I_n \subseteq I_{n+1} + \mathfrak{p}I_n$. In particular, the natural map $I_{n+1}/\mathfrak{p}I_{n+1} \to I_n/\mathfrak{p}I_n$ is surjective. By Corollary 3.3.5, $I_{n+1} \to I_n$ is surjective, so $I_{n+1} = I_n$. Thus the sequence I_n stabilises at n_0.

Now noting that $I_n \supseteq q^n$ and $\overline{\lambda(I_n)} = \overline{\lambda(\mathfrak{q})^n} = \overline{\lambda(\mathfrak{q})}^n$, we have the descending sequence of ideals of $R_\mathfrak{q}$

$$\overline{\lambda(\mathfrak{q})} \supseteq (\overline{\lambda(\mathfrak{q})})^2 \supseteq (\overline{\lambda(\mathfrak{q})})^3 \supseteq \cdots$$

also stabilises at n_0. Now, by Corollary 6.0.22, $\bigcap_{i \geq 0} (\overline{\lambda(\mathfrak{q})})^i = 0$. Thus, we have $\overline{\lambda(\mathfrak{q})}^{n_0}$. Now, as $\lambda(\mathfrak{q})$ is the maximal ideal of R_q, by Lemma 6.0.24, $R_\mathfrak{q}$ has dimension 0. In particular, $\mathrm{ht}(\mathfrak{q}) = 0$. Thus q cannot contain any prime ideal other than itself. This gives $k = 1$.

□

Lemma 6.0.26. *Let R be a noetherian ring. Let $\mathfrak{p}$ and $\mathfrak{p}'$ be prime ideals of R and suppose that $\mathfrak{p} \subsetneq \mathfrak{p}'$. Then, there exists a prime ideal $\mathfrak{q}$ such that $\mathfrak{p} \subseteq \mathfrak{q} \subsetneq \mathfrak{p}'$ and $\mathfrak{q}$ is maximal among prime ideals with such property.*

Proof. Suppose not. Let $\mathfrak{q}_1$ be any prime that satisfies the inequality. Then, we can continuously find larger primes from this which are strictly smaller than $\mathfrak{p}$. This contradicts the Noetherian condition on R. □

Corollary 6.0.27. *Let R be a noetherian ring. Let $f_1, \ldots, f_k \in R$. Let $\mathfrak{p}$ be a prime ideal minimal among those containing $(f_1, \ldots, f_k)$. Then $\mathrm{ht}(\mathfrak{p}) \leq k$.*

Proof. By induction on k. The case $k = 1$ is Krull's principal ideal theorem. Using a similar logic to the start of Krull's principal ideal theorem (by localising at $\mathfrak{p}$), we may suppose that R is a local ring with maximal ideal $\mathfrak{p}$.

Let $\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots$ be a possibly infinite chain of prime ideals beginning with $\mathfrak{p}$ and of length $\mathrm{ht}(\mathfrak{p})$. We can also assume that there are no prime ideals between $\mathfrak{p}$ and $\mathfrak{p}_1$, extending the chain by such prime ideal if necessary. Also note this condition is automatic if $\mathrm{ht}(\mathfrak{p}) < \infty$.

We wish to show that $\mathrm{ht}(\mathfrak{p}) \leq k$. Suppose that $\mathrm{ht}(\mathfrak{p}) > 0$ as else there is nothing to prove. Let $\mathfrak{q} = \mathfrak{p}_1$. We claim that $\mathrm{ht}(\mathfrak{q}) \leq k - 1$.

From assumptions, there is an f_i such that $f_i \neq \mathfrak{q}$, as else $\mathfrak{p}$ is not the minimal prime. Up to reordering, assume $f_1 \neq \mathfrak{p}$. As there are no prime ideals between $\mathfrak{p}$ and $\mathfrak{q}$, we see that $\mathfrak{p}$ is minimal among prime ideals containing $(\mathfrak{q}, f_1)$. Hence, the ring $R/(\mathfrak{q}, f_1)$ has dimension 0. Thus, by Lemma 6.0.24, the image of all f_i are nilpotent in $R/(\mathfrak{q}, f_1)$. That is, there exists $b_i \in \mathfrak{q}$ and $a_i \in R$ with $n_i \geq 2$ such that

$$f_i^{n_i} = a_i f_1 + b_i$$

Note also that

$$\mathfrak{p} \supseteq (f_1, f_2^{n_2}, \ldots, f_k^{n_k}) = (f_1, b_2, \ldots, b_k)$$

and that $\mathfrak{p}$ is minimal among the prime ideals containing $f_1, b_2, \ldots, b_k$ since

$$\mathfrak{r}((f_1, f_2^{n_2}, \ldots, f_k^{n_k})) = \mathfrak{r}((f_1, f_2, \ldots, f_k))$$

by definition. Write $J = (b_2, \ldots, b_k)$. Note first that $J \subseteq \mathfrak{q}$. Since $\mathfrak{p}$ is minimal among the prime ideals containing f_1 and J, we see that $\mathfrak{p}$ mod J is minimal among the prime ideals of R/J

containing $f_1 \bmod J$. Hence, $\mathrm{ht}(\mathfrak{p} \bmod J) \leq 1$ by Krull's principal ideal theorem. On the other hand, we have

$$\mathfrak{p} \bmod J \supsetneq \mathfrak{q} \bmod J$$

In particular, $\mathrm{ht}(\mathfrak{q} \bmod J) = 0$. Thus $\mathfrak{q}$ is minimal among the prime ideals containing J. By the inductive hypothesis, $\mathrm{ht}(\mathfrak{q}) \leq k-1$. This completes the proof. $\square$

Remark 6.0.28. As any ideal is generated by finitely many elements, any prime ideal has finite height. Thus, the dimension of a noetherian local ring is finite.

Note that this is not true if we take the local assumption away. TODO: example??

The above also implies that $\mathrm{ht}((f_1, \ldots, f_k)) \leq k$. If we have equality, then any minimal prime ideal associated with $(f_1, \ldots, f_k)$ has any height k (as height $\geq k$ by assumption, and $\leq k$ by proof).

Corollary 6.0.29. *Let R be a noetherian ring. Let $\mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots$ be a descending chain of prime ideals of R. Then there is a $i_0 \geq 0$ such that $\mathfrak{p}_{i_0+i} = \mathfrak{p}_{i_0}$ for all $i \geq 0$. Moreover, if $\mathfrak{p}_0$ is generated by c elements, and the inequality is strict until it stabilises, then $i_0 \leq c$.*

Proof. Is a direct consequence of Corollary 6.0.27. $\square$

Corollary 6.0.30. *Let R be a noetherian ring. Let $\mathfrak{p}$ be a prime ideal of height c. Suppose that $0 \leq k \leq c$ and that we have elements $t_1, \ldots, t_k \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k)) = k$. Then there are elements $t_{k+1}, \ldots, t_c \in \mathfrak{p}$ such that $\mathrm{ht}(t_1, \ldots, t_c) = c$.*

Proof. Note that by assumption, we have $k \leq c$. Note we set the ideal to 0 if $k = 0$. Also, if $\mathrm{ht}(t_1, \ldots, t_c) = c$, then $\mathfrak{p}$ is a minimal prime ideal associated with the ideal $(t_1, \ldots, t_c)$.

If $c = 0$, then $\mathfrak{p}$ is a minimal prime ideal of R, and $\mathrm{ht}((0)) = c = 0$, so we are done. We proceed by induction. Suppose that $c > 0$. We can also take $k < c$.

By induction on k, it is sufficient to construct an element $t \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k, t)) = k+1$. By Corollary 6.0.27 we know the height of this is at most k, so it suffices to find a $t \in \mathfrak{p}$ such that $\mathrm{ht}((t_1, \ldots, t_k, t)) > k$.

Suppose for a contradiction such an element does not exist. Then, we have $\mathrm{ht}((t_1, \ldots, t_k, t)) = k$ for all $t \in \mathfrak{p}$. Specifically, for any $t \in \mathfrak{p}$, there is a prime ideal $\mathfrak{q}$ that contains $(t_1, \ldots, t_k, t)$ and is of height k. Now $\mathfrak{q}$ contains a minimal prime q_1 associated with $(t_1, \ldots, t_k)$ with height k. Note that the height of this it at least k, giving $\mathfrak{q} = \mathfrak{q}_1$. Thus, for all $t \in \mathfrak{p}$, t is contained in a minimal prime ideal of height k associated with $(t_1, \ldots, t_k)$. Consequently, $\mathfrak{p}$ is contained in the union of minimal prime ideals of height k associated with $(t_1, \ldots, t_k)$. Thus $\mathfrak{p}$ is contained in, thus equal to one of these minimal prime ideals. As $\mathrm{ht}(\mathfrak{p}) = c > k$, this contradicts Corollary 6.0.27. $\square$

Lemma 6.0.31. *Let K be a field and let $\mathfrak{p}$ be a non-zero prime ideal of $K[x]$. Then $\mathrm{ht}(\mathfrak{p}) = 1$. In particular, $\dim(K[x]) = 1$.*

Proof. Note that in $K[x]$, non-zero prime ideals are maximal. As the zero-ideal is prime (noting that $K[x]$ is a domain), we must have that the dimension of any non-zero ideal is 1. $\square$

Definition 6.0.32. *Let R be a ring and $\mathfrak{p}$ is an ideal of R, we write $\mathfrak{p}[x]$ for the ideal generated by $\mathfrak{p}$ in $R[x]$. We can note this consists of polynomials with coefficients in $\mathfrak{p}$. If the ideal $\mathfrak{p}$ is prime, so is $\mathfrak{p}[x]$, as*

$$R[x]/\mathfrak{p}[x] \simeq (R/\mathfrak{p})[x]$$

and $(R/\mathfrak{p})[x]$ is a domain, noting that $R/\mathfrak{p}$ is a domain.

Lemma 6.0.33. *Let $\phi : R \to T$ be a ring homomorphism. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ and let I be the ideal generated by $\phi(\mathfrak{p})$ in T. Write $\psi : R/\mathfrak{p} \to T/I$ be the ring homomorphism induced by ϕ, and let $S = (R/\mathfrak{p})\backslash\{0\}$.*

Write $\psi_S : \operatorname{Frac}(R/\mathfrak{p}) \to (T/I)_{\psi(S)}$ for the induced ring homomorphism. Let $\rho : T \to (T/I)_{\psi(T/I)_{\psi(S)}}$ Then, $\operatorname{Spec}(\rho)(\operatorname{Spec}((T/I)_{\psi(S)}))$ consists precisely of the prime ideals $\mathfrak{q}$ of T such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Proof. We have the following commutative diagram of rings.

$$\begin{tikzcd}
T \arrow[r] \arrow[rr, bend left, "\rho"] & T/I \arrow[r] & (T/I)_{\psi(S)} \\
R \arrow[u, "\phi"] \arrow[r] & R/\mathfrak{p} \arrow[u, "\psi"] \arrow[r] & \operatorname{Frac}(R/\mathfrak{p}) \arrow[u, "\psi_S"']
\end{tikzcd}$$

This leads to a commutative diagram of spectra,

$$\begin{tikzcd}
\operatorname{Spec}(T) \arrow[d, "\operatorname{Spec}(\phi)"'] & \operatorname{Spec}(T/I) \arrow[l] \arrow[d, "\operatorname{Spec}(\psi)"'] & \operatorname{Spec}((T/I)_{\psi(S)}) \arrow[l] \arrow[d, "\operatorname{Spec}(\psi_S)"] \arrow[ll, bend right, "\operatorname{Spec}(\rho)"'] \\
\operatorname{Spec}(R) & \operatorname{Spec}(R/\mathfrak{p}) \arrow[l] & \operatorname{Spec}(\operatorname{Frac}(R/\mathfrak{p})) \arrow[l]
\end{tikzcd}$$

Thus, we wish to show that the fibre of $\operatorname{Spec}(\phi)$ above $\mathfrak{p}$ is the image of $\operatorname{Spec}(\rho)$: TODO!! WHAT????

Note first that $\operatorname{Spec}(\operatorname{Frac}(R/\mathfrak{p}))$ consists of one point as it is a field. The image of this point in $\operatorname{Spec}(R/\mathfrak{p})$ is the ideal $(0) \subseteq R/\mathfrak{p}$, and the preimage of this in R is $\mathfrak{p}$. So the image of $\operatorname{Spec}(\rho)$ is contained in the fibre of $\operatorname{Spec}(\phi)$ above $\mathfrak{p}$, noting the diagram is commutative.

Now suppose that $\mathfrak{q} \in \operatorname{Spec}(T)$ with $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ ($\mathfrak{q}$ lies inside the fibre of $\operatorname{Spec}(\phi)$ above $\mathfrak{p}$). Then, $\mathfrak{q} \supseteq I$, so there is an ideal $q' \in \operatorname{Spec}(T/I)$ such that $\mathfrak{q}$ is the image of $\mathfrak{q}'$ in $\operatorname{Spec}(T)$. On the other hand, we know that $\psi^{-1}(\mathfrak{q}')$ is the 0 ideal, as $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$ and the diagram is commutative. Thus, $\mathfrak{q}' \cap \psi(S) = \emptyset$. Consequently, by Lemma 2.1.18, $\mathfrak{q}'$ lies in the image of $\operatorname{Spec}((T/I)_{\psi(S)}) \to \operatorname{Spec}(T/I)$. This completes the proof.

□

Remark 6.0.34. Note that with the correspondence between

- prime ideals $\mathfrak{q}$ such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$
- prime ideals of $(T/I)_{\psi(S)}$

given above, as this is given by $\operatorname{Spec}(\rho)$, respects inclusion in both directions.

Applying the previous lemma with $T = R[x]$, we have

$$(T/I)_{\psi(S)} = (R[x]/\mathfrak{p}[x])_{\psi}(S) \simeq (R/\mathfrak{p})[x]_{(R/\mathfrak{p})^*} \simeq \operatorname{Frac}(R/\mathfrak{p})[x]$$

Note the $A^* = A\backslash\{0\}$ gives the multiplicative structure, noting $R/\mathfrak{p}$ is a domain. Note the final equality comes from the fact

$$(A[x])_S = (A_S)[x]$$

given A is a domain (by considering the map $\sum a_i x^i/s \mapsto \sum (a_i/s)x^i$).

Lemma 6.0.35. *We keep the notation of Lemma 6.0.33. Suppose we have the chain of prime ideals*

$$\mathfrak{q}_0 \supseteq \mathfrak{q}_1 \supseteq \cdots \supsetneq \mathfrak{q}_k$$

in T such that $\phi^{-1}(q_i) = \mathfrak{p}$ for all $i \in \{0, \dots, k\}$. Then, $k \leq \dim((T/I)_{\psi(S)})$.

Proof. By Lemma 6.0.33 and noting that the bijective correspondence respects inclusion. $\square$

Lemma 6.0.36. *Let R be a ring and let N be the nilradical of R. Then the nilradical of $R[x]$ is $N[x]$.*

Proof. Any element of $N[x]$ is a polynomial with nilpotent coefficients and thus is nilpotent (as the nilradical is an ideal, closed under adding nilpotent elements). Suppose $P(x) = a_0 + a_1x + \cdots + a_dx^d$ is an element of the nilradical of $R[x]$. Suppose for a contradiction that a_i is not nilpotent. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ be such that $a_i \notin \mathfrak{p}$ (exists, as a_i is not nilpotent). Then $P(x) \bmod \mathfrak{p} \in (R/\mathfrak{p})[x]$ is a non zero nilpotent polynomial. This is a contradiction as $(R/\mathfrak{p})[x]$ is a domain. $\square$

Lemma 6.0.37. *Let R be a noetherian ring and let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be the minimal prime ideals of R. Then the minimal prime ideals of $R[x]$ are the ideals $\mathfrak{p}_1[x], \dots, \mathfrak{p}_k[x]$. More generally, if I is an ideal of R and $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ are minimal prime ideals associated with I, then the ideals $\mathfrak{p}_1[x], \dots, \mathfrak{p}_k[x]$ are the minimal primes associated with $I[x]$.*

Proof. For the first, note that $\bigcap_i \mathfrak{p}_i = \mathfrak{r}((0))$, because the nilradical of R is decomposable by the Lasker-Noether Theorem. Consequently, $\mathfrak{r}((0))[x] = (\bigcap_i p_i)[x] = \bigcap_i p_i[x]$ is a minimal primary decomposition of $\mathfrak{r}((0))[x]$ by Proposition 3.5.2. By Lemma 6.0.36, this is the nilradical of $R[x]$ and correspond to the minimal primes by Theorem 3.5.14 and correspondence.

For the second statement, apply the first to $p_i \bmod I$, noting that $(R/I)[x] \simeq R[x]/I[x]$. $\square$

Lemma 6.0.38. *Let R be noetherian and let I be an ideal of R. Then $\mathrm{ht}(I) = \mathrm{ht}(I[x])$.*

Proof. We first prove the case if I is prime, writing $I = \mathfrak{p} \in \mathrm{Spec}(R)$. Let $c = \mathrm{ht}(\mathfrak{p})$ and let $a_1, \dots, a_c \in \mathfrak{p}$ be such that $\mathrm{ht}((a_1, \dots, a_c)) = c$, such that $\mathfrak{p}$ is a minimal prime associated with $(a_1, \dots, a_c)$. This exists by Corollary 6.0.30. Let $J = (a_1, \dots, a_c)$. By the previous lemma, $\mathfrak{p}[x]$ is a minimal prime ideal associated with $J[x]$. By Corollary 6.0.27, $\mathrm{ht}(\mathfrak{p}[x]) \leq c$ (as $a_1, \dots, a_c$ generate $J[x]$). Also, if

$$\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq p_c$$

then,

$$\mathfrak{p}[x] \supsetneq \mathfrak{p}_1[x] \supsetneq \mathfrak{p}_2[x] \supsetneq \cdots \supsetneq p_c[x]$$

is also a descending chain of prime ideals in $R[x]$, so $\mathrm{ht}(\mathfrak{p}[x]) \geq c$. Thus we have shown equality.

For the general case, note that there is a minimal prime $\mathfrak{p}$ associated with I such that $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(I)$. Thus, $\mathrm{ht}(I[x]) \leq \mathrm{ht}(\mathfrak{p}[x]) = \mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(I)$. On the other hand, there is a minimal prime ideal associated with $I[x]$ such that $\mathrm{ht}(\mathfrak{q}) = \mathrm{ht}(I[x])$. By Lemma 6.0.37, we have $\mathfrak{q} = (\mathfrak{q} \cap R)[x]$, so

$$\mathrm{ht}(I[x]) = \mathrm{ht}(\mathfrak{q}) = \mathrm{ht}((\mathfrak{q} \cap R)[x]) = \mathrm{ht}(\mathfrak{q} \cap R) \geq \mathrm{ht}(I[x] \cap R) = \mathrm{ht}(I)$$

$\square$

Lemma 6.0.39. *Let $\mathfrak{q}$ be a prime ideal of $R[x]$ and let I be an ideal of R such that $I \subseteq \mathfrak{q} \cap R$. Suppose that $\mathfrak{q} \cap R$ is a minimal prime ideal associated with I. Let $\mathfrak{q}' \subseteq \mathfrak{q}$ be a prime ideal of $R[x]$ which is a minimal prime ideal associated with $I[x]$. Then $\mathfrak{q}' = (\mathfrak{q} \cap R)[x]$.*

Proof. We have,

$$\mathfrak{q}' \cap R \supseteq I[x] \cap R = I$$

and note with this that,

$$\mathfrak{q}' \supseteq (\mathfrak{q}' \cap R)[x] \supseteq I[x]$$

By minimality of $\mathfrak{q}'$, we have $\mathfrak{q}' = (\mathfrak{q}' \cap R)[x]$. Now, $\mathfrak{q}' \subseteq \mathfrak{q}$, so

$$\mathfrak{q}' = (\mathfrak{q}' \cap R)[x] \subseteq (\mathfrak{q} \cap R)[x]$$

By Lemma 6.0.37, we know that $(\mathfrak{q} \cap R)[x]$ is a minimal prime associated with $I[x]$, thus $\mathfrak{q}' = (\mathfrak{q} \cap R)[x]$. □

Proposition 6.0.40. *Let R be a noetherian ring and $\mathfrak{p}$ be a prime ideal of $R[x]$. Then,*

$$\mathrm{ht}(\mathfrak{p}) \leq 1 + \mathrm{ht}(\mathfrak{p} \cap R)$$

If $\mathfrak{p}$ is maximal, we have

$$\mathrm{ht}(\mathfrak{p}) = 1 + \mathrm{ht}(\mathfrak{p} \cap R)$$

Proof. Let $\delta = \mathrm{ht}(\mathfrak{p} \cap R)$ and $c = \mathrm{ht}(\mathfrak{p})$. Note that since $(\mathfrak{p} \cap R)[x] \subseteq \mathfrak{p}$, we have $\delta \leq c$ by Lemma 6.0.38.

Let $a_1, \ldots, a_c \in \mathfrak{p}$ be such that $\mathrm{ht}((a_1, \ldots, a_i)) = i$ for $i \in \{1, \ldots, c\}$. This exists by Corollary 6.0.30. By the same corollary, suppose that $a_1, \ldots, a_\delta \in \mathfrak{p} \cap R$. In particular, $(\mathfrak{p} \cap R)[x]$ is a minimal prime ideal associated with $(a_1, \ldots, a_\delta)$.

Now, inductively define a chain of prime ideals

$$\mathfrak{p} = \mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_c$$

such that $\mathfrak{q}_i$ is a minimal prime associated with $(a_1, \ldots, a_{c-i})$. To construct this, we first let $\mathfrak{q}_0 = \mathfrak{p}$ and suppose that for $i > 0$, the ideals $\mathfrak{q}_0, \ldots, \mathfrak{q}_{i-1}$ are given. Let $\mathfrak{q}_i$ be any minimal prime ideal associated with $(a_1, \ldots, a_{c-i})$, which is contained in $\mathfrak{q}_{i-1}$. This is strict, as the construction gives $\mathrm{ht}(\mathfrak{q}_i) = c - i$ (Corollary 6.0.27).

Now, $\mathfrak{q}_{c-\delta}$ and $(\mathfrak{p} \cap R)[x]$ are minimal prime ideals associated with $(a_1, \ldots, a_\delta)$. By Lemma 6.0.39, we have equality. Thus, for all $i \in \{0, \ldots, c - \delta\}$ we have

$$\mathfrak{p} \supseteq \mathfrak{q}_i \supseteq (\mathfrak{p} \cap R)[x]$$

So,

$$\mathfrak{p} \cap R \supseteq \mathfrak{q}_i \cap R \supseteq \mathfrak{p} \cap R$$

Giving $\mathfrak{q}_i \cap R = \mathfrak{p} \cap R$.

By Lemma 6.0.35,

$$c - \delta \leq \dim((R[x]/(\mathfrak{p} \cap R)[x])_{(R/(\mathfrak{p} \cap R)^*)}) = \dim(\mathrm{Frac}(R/(\mathfrak{p} \cap R))[x])$$

By Lemma 6.0.31, this has dimension at most 1, so the first claim has been shown.

If $\mathfrak{p}$ is maximal, then $\mathfrak{p} \neq (\mathfrak{p} \cap R)[x] = \mathfrak{q}_{c-\delta}$ as $(\mathfrak{p} \cap R)[x]$ is not maximal (by adding (x)), so $c - \delta \geq 1$. In particular, $c = \delta + 1$. □

Theorem 6.0.41. *Let R be a noetherian ring. Suppose that* $\dim(R) < \infty$. *Then* $\dim(R[x]) = \dim(R) + 1$.

Proof. Let $\mathfrak{m}$ be a maximal ideal of $R[x]$ such that $\mathrm{ht}(\mathfrak{m}) = \dim(R[x])$. This exists as the dimension is finite. By the previous proposition, we have $\mathrm{ht}(\mathfrak{m}) = 1 + \mathrm{ht}(\mathfrak{m} \cap R)$. We now claim that $\mathrm{ht}(\mathfrak{m} \cap R) = \dim(R)$. Suppose for a contradiction that $\mathrm{ht}(\mathfrak{m} \cap R) < \dim(R)$. Then, there is a maximal ideal $\mathfrak{p}$ in R such that $\mathrm{ht}(\mathfrak{p}) > \mathrm{ht}(\mathfrak{m} \cap R)$. Let $\mathfrak{n}$ be a maximal ideal of $R[x]$ which contains $\mathfrak{p}[x]$. By maximality, $\mathfrak{n} \cap R = \mathfrak{p}$, giving

$$\mathrm{ht}(\mathfrak{n}) = 1 + \mathrm{ht}(\mathfrak{p}) > 1 + \mathrm{ht}(\mathfrak{m} \cap R) = \mathrm{ht}(\mathfrak{m})$$

which is a contradiction. Thus, $\mathrm{ht}(\mathfrak{m}) = \dim(R[x]) = \dim(R) + 1$. $\square$

Remark 6.0.42. Let R be a noetherian ring and $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals of R. Then, we have

$$\mathrm{ht}(\mathfrak{p}) + \mathrm{ht}(\mathfrak{q} \bmod \mathfrak{p}) \leq \mathrm{ht}(\mathfrak{q})$$

but equality does not hold in general. Rings where this holds are called **catenary** domains. Note further that finitely generated algebras over fields are catenary. So equality holds if R is a domain, as they are always finitely generated over some field. (Both results not shown here)

We note that however $\mathrm{ht}((\mathfrak{m} \cap R)[x]) + \mathrm{ht}(\mathfrak{m}/(\mathfrak{m} \cap R)[x]) = \mathrm{ht}(\mathfrak{m})$.

Corollary 6.0.43. *Let R be a noetherian ring. Suppose that $\dim(R) < \infty$. Then we have that $\dim(R[x_1, \ldots, x_t]) = \dim(R) + t$.*

Proof. This follows from Theorem 6.0.41 and Hilbert's basis theorem. $\square$

Lemma 6.0.44. *Let R be a subring of T. Let T be integral over R. Let $\mathfrak{q}_1, \mathfrak{q}_2$ be prime ideals of T such that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R = \mathfrak{p}$ for some prime $\mathfrak{p}$ in R. If $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$, $\mathfrak{q}_1 = \mathfrak{q}_2$.*

Proof. The ring $R/\mathfrak{p}$ can be viewed as a subring of $T/\mathfrak{q}_1$ (by considering the map from R into $T/\mathfrak{q}_1$ induced by the quotient map). By assumption, we also have $(\mathfrak{q}_2 \bmod \mathfrak{q}_1) \cap R/\mathfrak{p} = (0)$. Without loss of generality, we may therefore view R and T to be domains and $\mathfrak{q}_1$ and $\mathfrak{p}$ are zero ideals.

Take $e \in \mathfrak{q}_2 \backslash \{0\}$ and let $P(x) \in R[x]$ be a non-zero monic polynomial such that $P(e) = 0$. As T is a domain, the constant coefficient of $P(x)$ is non-zero. But the constant term $P(0)$ is a linear combination of positive powers of e, so $P(0) \in R \cap \mathfrak{q}_2 = (0)$, a contradiction. $\square$

Lemma 6.0.45. *Let R be a subring of T. Suppose that T is integral over R. Then $\dim(T) = \dim(R)$. This holds if R or T has infinite dimension (then the other has infinite dimension).*

Proof. Suppose first that $\dim(R), \dim(T) < \infty$. Let

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_{\dim(R)}$$

be a descending chain of prime ideals in R of maximal length. By Theorem 4.1.15, we can find a prime ideal $\mathfrak{q}_i$ in T such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ and

$$\mathfrak{q}_0 \supsetneq \mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_{\dim(R)}$$

Hence $\dim(T) \geq \dim(R)$. We have

$$\mathfrak{q}_0 \cap R \supsetneq \mathfrak{q}_1 \cap R \supsetneq \cdots \supsetneq \mathfrak{q}_{\dim(T)} \cap R$$

by Lemma 6.0.44. Thus $\dim(T) \leq \dim(R)$. The proof uses adjacent logic for the infinite case. $\square$

Corollary 6.0.46. *Let k be a field and let R be a finitely generated k-algebra. Suppose that R is a domain and let $K = \mathrm{Frac}(R)$. Then $\dim(R)$ and $\mathrm{tr}(K|k)$ are both finite and equal.*

Proof. By Noether's Normalization Lemma, there is an injection of rings $k[x_1, \dots, x_d] \hookrightarrow R$ which makes R into an integral $k[x_1, \dots, x_d]$-algebra. From the previous lemma, we have $\dim(R) = \dim(k[x_1, \dots, x_d]) = d$. Also, the fraction field $k(x_1, \dots, x_d) = \mathrm{Frac}(k[x_1, \dots, x_d])$ is naturally a subfield of K, and as every element of R is integral over $k[x_1, \dots, x_d]$, every element of K is algebraic over $k(x_1, \dots, x_d)$. Thus,

$$\mathrm{tr}(K|k) = \mathrm{tr}(k(x_1, \dots, x_d)|k) = d = \dim(R)$$

$\square$

7 Other