Notes on Commutative Algebra

Apiros3

First Version : Mar 19, 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,*

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

*The set $\mathrm{Ann}_M(S)$ 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, $\ker(\phi) = \bigcap_{i=1}^{k} I_i$.

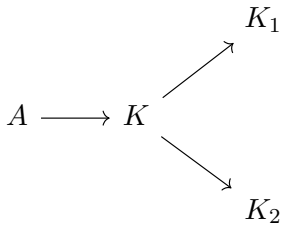
The map ϕ is surjective if and only if $I_i + I_j = R$ for every $i, j \in \{1, \ldots, k\}$ with $i \neq j$. In such case, $\bigcap_{i=1}^{k} I_i = \prod_{i=1}^{k} I_i$

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*

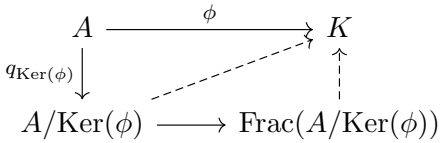
$$\{P \subseteq A \mid P \text{ is a prime ideal}\} \simeq \{\phi : A \to K \mid K \text{ is a field}\}/\simeq$$

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.



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.



□

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. □

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*

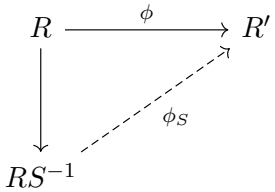
$$+ : MS^{-1} \times MS^{-1} \to MS^{-1}, (a/s, b/t) \mapsto (ta + sb)/(st)$$

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 $r \in R$*



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. □

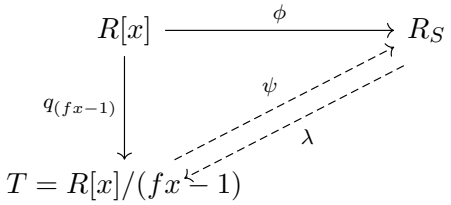
Lemma 2.1.7. *Let R be a ring and $f \in R$. Define $S = \{1, f, f^2, \dots\}$. Then R_S is finitely generated as an R-algebra.*

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.



□

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. □

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. □

Definition 2.1.10. *Let*

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

*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*

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

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

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

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

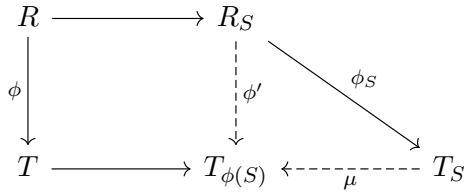
$$\mathrm{Ker}(d_i)/\mathrm{Im}(d_{i+1}) \neq 0$$

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

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

□

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 $\mu \circ \phi_S = \phi'$.*



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. □

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

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

Corollary 2.1.20. *Given that* $\mathfrak{p} \in \mathrm{Spec}(R_S)$ *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. □

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). □

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, $\lambda^{-1}(\mathfrak{m}) = \mathfrak{p}$. □

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 $f^{n_x+n_y} \in \mathfrak{m}$. □

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. □

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, $\mathfrak{r}(\mathfrak{r}(I)) = \{f \in R \mid f^{mn} \in I,\ n, m \geq 0\} = \mathfrak{r}(I)$. □

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 $I \subseteq R$ 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 $x_1, \ldots, x_s$ be the set of generators of M such that s is minimal, where $s \geq 1$ as M is nonzero. By assumption, there exists $a_1, \ldots, a_s \in I$ such that

$$x_s = a_1 x_1 + \cdots + a_s x_s$$

Rewriting,

$$(1 - a_s)x_s = a_1 x_1 + \cdots + a_{s-1} x_{s-1}$$

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,

$$x_s = (1 - a_s)^{-1} a_1 x_1 + \cdots + (1 - a_s)^{-1} a_{s-1} x_{s-1}$$

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 $x_1, \ldots, x_s \in M$ be elements of M and $x_1 + \mathfrak{m}M, \ldots, x_s + \mathfrak{m}M \in M/\mathfrak{m}M$ generate the $R/\mathfrak{m}$-module $M/\mathfrak{m}M$. Then the elements $x_1, \ldots, x_s$ generate M.*

Proof. Let $M' \subseteq M$ be the submodule generated by $x_1, \ldots, x_s$. 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 $x_1, \ldots, x_s$ be generators of M. By assumption, $\phi(x_1) + \mathfrak{m}, \ldots, \phi(x_s) + \mathfrak{m}$ generate $N/\mathfrak{m}$. Thus, by Corollary 3.3.4, $\phi(x_1), \ldots, \phi(x_s)$ 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. □

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. □

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 $I \lhd R$. 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 $\mathfrak{p}$. □

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. □

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 $\bigcap_{i=1}^k I_i \subseteq I_{i_0}$. □

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 $J_1, \ldots, J_k$ 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 $i, j \in \{1, \ldots, k\}$ 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 $J_1, \ldots, J_k$ 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 $i \in \{1, \ldots, k\}$, $J_i \not\supseteq \bigcap_{j \neq i} J_i$*

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 $J_1, \ldots, J_k$ 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,*

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

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 $i_0 \in \{1, \ldots, k\}$.

Conversely, taking any $i_0 \in \{1, \ldots, k\}$, 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 $\mathcal{S}_{\min} = V(I)_{\min}$. □

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 $I \triangleleft R$, $I = (r_1, \ldots, r_k)$ 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. □

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. □

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. □

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 $(N \cap R^{n-1}) \times \phi(N) \simeq N$. □

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. □

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. □

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

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

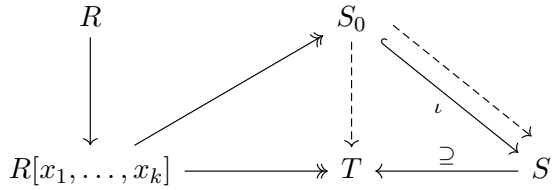
where $s_{ja} \in S$. Similarly, for any $b, d \in \{1, \dots, k\}$ we have,

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

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.



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

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. □

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

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

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

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

for some $k \geq 1$.

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

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. □

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 $P(x) = x^n + a_{n-1}x^{n-1} + \dots a_0 \in A[x]$ 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

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

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

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

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 $b_1, \dots, b_n$ 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 $h : \mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}] \to R$ 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 $T(x) \in (\mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}])[x]$ 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 $R = \mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}]$.

Let K be the fraction field of R. The natural homomorphism of rings $R \to K$ is injective as $R = \mathbb{Z}[x_{11}, x_{12}, \dots, x_{21}, x_{22}, \dots, x_{nn}]$ 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. □

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

$$\begin{array}{ccc} \mathrm{Spec}(B_\mathfrak{p}) & \xrightarrow{\mathrm{Spec}(\lambda_B)} & \mathrm{Spec}(B) \\ \downarrow{\scriptstyle \mathrm{Spec}(\phi_\mathfrak{p})} & & \downarrow{\scriptstyle \mathrm{Spec}(\phi)} \\ \mathrm{Spec}(A_\mathfrak{p}) & \xrightarrow{\mathrm{Spec}(\lambda_A)} & \mathrm{Spec}(A) \end{array}$$

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 :

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow{\scriptstyle q_\mu} & \searrow^{\mu} & \downarrow{\scriptstyle q_\mathfrak{p}} \\ A/\ker(\mu) & \xrightarrow{\psi} & B/\mathfrak{p} \end{array}$$

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

$$\begin{array}{ccc} \mathrm{Spec}(B/\bar{\mathfrak{p}}) & \xrightarrow[\mathrm{Spec}(\bar{q})]{} & \mathrm{Spec}(B) \\ \downarrow{\scriptstyle \mathrm{Spec}(\psi)} & \swarrow & \downarrow{\scriptstyle \mathrm{Spec}(\phi)} \\ \mathrm{Spec}(A/\mathfrak{p}) & \xrightarrow[\mathrm{Spec}(q)]{} & \mathrm{Spec}(A) \end{array}$$

Any prime ideal $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \cap A = \mathfrak{p}$ has the property that $\mathfrak{q} \supseteq \bar{\mathfrak{p}}$, we see any such prime ideal lies in the image of $\mathrm{Spec}(\bar{q})$. The corresponding prime ideals of $\mathrm{Spec}(B/\bar{\mathfrak{p}})$ 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 $\lambda_B/\bar{\mathfrak{p}} : B/\bar{\mathfrak{p}} \to (B/\bar{\mathfrak{p}})_{\psi(S)}$ be the natural ring homomorphisms. There is a natural ring homomorphism ψ_S that is compatible with these morphisms to obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}((B/\bar{\mathfrak{p}})_{\psi(S)}) & \xrightarrow{\mathrm{Spec}(\lambda_{B/\bar{\mathfrak{p}}})} & \mathrm{Spec}(B/\bar{\mathfrak{p}}) \\ \downarrow{\scriptstyle \mathrm{Spec}(\psi_S)} & & \downarrow{\scriptstyle \mathrm{Spec}(\psi)} \\ \mathrm{Spec}((A/\mathfrak{p})_{\psi(S)}) & \xrightarrow{\mathrm{Spec}(\lambda_{A/\mathfrak{p}})} & \mathrm{Spec}(A/\mathfrak{p}) \end{array}$$

If $q \in \mathrm{Spec}(B/\bar{\mathfrak{p}})$, 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. *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). □

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.*

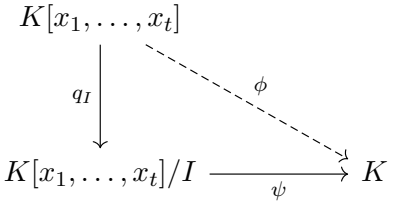
Proof. Let $K[y_1, \ldots, y_t] \to R$ as in Noether's Normalization Lemma. By Theorem 4.1.15, $\mathrm{Spec}(R) \to \mathrm{Spec}(K[y_1, \ldots, y_t])$ is surjective. As R is a field, $\mathrm{Spec}(R)$ has one element, so $\mathrm{Spec}(K[y_1, \ldots, y_t])$ has one element. Thus $t = 0$ (else, consider 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. □

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, $K[x_1, \ldots, x_t]/I \simeq K$.



Consider ϕ as the induced homomorphism of K-algebras. By construction, I contains the ideal $(x_1 - \phi(x_1), \dots, x_t - \phi(x_t))$ (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 $\psi : K[x_1, \dots, x_t] \to K$ such that $\psi(P(x_1, \dots, x_t)) = P(a_1, \dots, a_t)$ is surjective and the $\ker(\psi) \supseteq (x_1 - a_1, \dots, x_t - a_t)$. As ψ is nonzero, $\ker(\psi)$ is maximal, and $\ker(\psi) = (x_1 - a_1, \dots, x_t - a_t)$. □

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 $S = \{1, f, f^2, \dots\}$. 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)**.**

6 Other

Lemma 6.0.1 (Bijective Correspondence between Ideals)**.** *Let $\phi : R \to S$ be a surjective ring homomorphism. Then, we have a correspondence between ideals in R containing* $\mathrm{Ker}(\phi)$ *and ideals in S. The correspondence holds if we change 'ideals' to 'prime ideals', 'maximal ideals', or 'radical ideals'.*

Proof. The main idea is that

1. If $J \lhd S$, $\phi(\phi^{-1}(J)) = J$
2. If $I \lhd R$, $\phi^{-1}(\phi(I)) = I + \mathrm{Ker}(\phi)$

For the first case, note that $\phi(\phi^{-1}(J)) = J \cap \mathrm{Im}(\phi) = J$. The second follows by double inclusion. Then, the maps $J \mapsto \phi^{-1}(J)$ and $I \mapsto \phi(I)$ induce bijections.

For prime ideals, let $J \lhd S$ be prime. Then there exists a $I \lhd R$ with $\mathrm{Ker}(\phi) \subseteq I$ with $\phi(I) = J$. Taking $x, y \in R$ with $xy \in I$. Then, $\phi(xy) = \phi(x)\phi(y) \in J$, so without loss of generality, take $\phi(x) \in J$. By correspondence (taking inverses), $x \in I$. Now let $I \lhd R$ be prime with $\mathrm{Ker}(\phi) \subseteq I$. Take $x, y \in S$ such that $xy \in \phi(I)$. By surjectivity of ϕ, there exists $x', y' \in R$ such that $\phi(x') = x$ and $\phi(y') = y$. Thus, $\phi(x'y') \in \phi(I)$. By correspondence, $x'y' \in I$. The proof follows. □

7 Picture

Often when we talk about $\phi : A \to B$ and B being a $\phi(A)$-module, we implictly make A a subring of B by considering $\text{im}(\phi)$ and talk about A as a subring of B, with ϕ becoming inclusion.

Idea : B is a finite A-algebra (B is finite over A, B is a $\phi(A)$-module) if and only if B is finitely generated integral A-algebra. Follows from:

- if $b_1, \ldots, b_k$ are integral, $A[b_1, \ldots, b_k]$ is finitely generated as an A module (Pf. transitivity of finite generation and using integrality to find finite generators of $A[b_1]$)
- Any element inside a finitely generated module is integral (Pf. consider the map $[b]$ that premultiplies by b, and note that any endomorphism of finitely generated modules over R can be annihalated by some monic polynomial in R, general Cayley-Hamilton)
- finitely generated module implies finitely generated algebra (clear)

8 Big Ideas

8.1 Useful Ideas

Proposition 1.1.17

8.2 Big Ideas

Lemma 2.1.11 Lemma 2.1.12 Lemma 2.1.18