Those are the notes I took when taking a course on **Commutative Rings and Schemes** taught by Professor Ngo Bao Chau at the University of Chicago during Winter 2022.

Contents

Convention: All rings are commutative

1 Rings and Modules

1.1 Basic Notions

Theorem 1.1 (Chinese remainder theorem)**.** *Let R be a ring and $I_1, \cdots, I_n$ ideals of R. There is an injective canonical map $\varphi : A/(I_1 \cap \cdots \cap I_n) \to A/I_1 \times \cdots \times I_n$. If $I_1, \cdots, I_n$ are mutually coprime ($I_j + I_k = R$ for all $j \neq k$), then $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$ and φ is an isomorphism.*

Theorem 1.2 (Prime avoidance)**.** *f*

The **nilradical** $\mathrm{nil}(R)$ of a ring R is the radical of zero ideal. It is the set of all nilpotent elements of R. Alternatively, it is the intersection of prime ideals of R.

A ring R is **reduced** if $\mathrm{nil}(R) = 0$. Every ring R can be thought of as the ring of a certain kind of functions over $\mathrm{Spec}(R)$ taking values in $\kappa(\mathfrak{p}) = \mathrm{Fr}(R/\mathfrak{p})$ for $\mathfrak{p} \in \mathrm{Spec}(R)$. For every $a \in R$, let $a : \mathrm{Spec}(R) \to \kappa(\mathfrak{p})$ be the function such that $a(\mathfrak{p})$ is the class of a modulo $\mathfrak{p}$. Hence we have a ring homomorphism $R \to \prod_{\mathfrak{p} \in \mathrm{Spec}(R)} \kappa(\mathfrak{p})$ which has kernel $\mathrm{nil}(R)$. When R is reduced, this map is injective, and R embeds into the space of all theoretical functions.

The **Jacobson radical** $\mathrm{rad}(R)$ of a ring R is the intersection of all maximal ideals of R. An element $a \in \mathrm{rad}(R)$ if and only if $1 + aR \subset R^\times$.

1.2 Tensor Product and Localization

The most important thing about tensor product $- \otimes_R N$ is its right-exactness:

Proposition 1.3. *Let R be a ring and N an R-module. Let $f : M \to M'$ be a surjective linear map between R-modules. Then the induced map $f \otimes_R \mathrm{id}_N : M \otimes_R N \to M' \otimes_R N$ is also surjective.*

However, $- \otimes_R N$ is not in general left-exact. For instance, consider $R = M = M' = \mathbf{Z}$ with an injective map $\times p : \mathbf{Z} \to \mathbf{Z}$. Let $N = \mathbf{Z}/pZ$. Then the induced map $\mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ is the zero map, which is not injective. The reason for this discrepancy is that elements of $M \otimes_R N$ are finite sums $m_1 \otimes n_1 + \cdots + m_k \otimes n_k$, instead of "pure tensors" $m \otimes n$.

An important case of tensor product is the change of scalars: if R' is an R-algebra, then for an R-module M, $M \otimes_R R'$ has an R'-module structure.

Another important case of tensor product is localization.

Proposition 1.4. *Let R be a ring, M an R-module, and S a multiplicative closed set. Then $M[S^{-1}] \cong M \otimes_R R[S^{-1}]$ as $R[S^{-1}]$-modules.*

Proof. See [Mat] Theorem 4.4. □

In the case of localization, tensor product $\otimes_R R[S^{-1}]$ is *left-exact*. This is because elements of $M \otimes_R R[S^{-1}]$ are "pure tensors":

$$m_1 \otimes \frac{a_1}{b_1} + m_2 \otimes \frac{a_2}{b_2} = b_2 m_1 a_1 \otimes \frac{1}{b_1 b_2} + b_1 m_2 a_2 \otimes \frac{1}{b_1 b_2} = (a_1 m_1 b_2 + a_2 m_1 b_1) \otimes \frac{1}{b_1 b_2}.$$

In that case, injectivity is easily verified. In fact, localization is an exact functor.

Now let us consider the special case of localization $R[S^{-1}]$ of rings. There is an easy but important structural correspondence of ideals:

$$\{\text{ideals } I \text{ of } R\} \longleftrightarrow \{\text{ideals } IR[S^{-1}] \text{ of } R[S^{-1}]\};$$

$$\{\text{prime ideals } \mathfrak{p} \text{ of } R \text{ disjoint from } S\} \longleftrightarrow \{\text{ideals } \mathfrak{p}R[S^{-1}] \text{ of } R[S^{-1}]\}.$$

In particular, prime ideals of $R_{\mathfrak{p}}$ are prime ideals of R contained in $\mathfrak{p}$. For the opposite direction, prime ideals of $R/\mathfrak{p}$ are prime ideals of R containing $\mathfrak{p}$.

Localization commutes with passing to quotient: $R[S^{-1}]/IR[S^{-1}] \cong (R/I)[\bar{S}^{-1}]$ where $\bar{S}$ is the image of S in R/I. This is easily deduced from the uniqueness of universal property.

2 Zariski Topology

Let R be a ring. For an ideal I of R, let $V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \supset I\}$. Then

(i) $V(I) \cup V(I') = V(II') = V(I \cap I')$ for I and I' ideals of R;

(ii) $\bigcap_\lambda V(I_\lambda) = V\left(\sum_\lambda I_\lambda\right)$ for any family of ideals $\{I_\lambda\}_{\lambda\in\Lambda}$ of R.

Let $V(I)$ be the closed sets. It defines a topology on $\mathrm{Spec}(R)$ called the **Zariski topology**. Open sets are of the form $U_I = \mathrm{Spec}(R) \setminus V(I) = \{\mathfrak{p} \in \mathrm{Spec}(R) : \mathfrak{p} \not\supset I\} = \bigcup_{a\in I} U_a$ where $U_a = U_{(a)}$. Sets of the form U_a are called **principal open sets**. They form a basis of the Zariski topology. Also note that $V(I) = V(\sqrt{I})$, and that $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

Recall that a topological space is **quasi-compact** if every open has a finite subcover. It is **compact** if it is quasi-compact and Hausdorff.

Proposition 2.1. *Principal open sets are quasi-compact. In particular,* $\mathrm{Spec}(R)$ *is quasi-compact.*

However, $\mathrm{Spec}(R)$ is not compact in general for it fails to be Hausdorff: if R is a domain, then (0) is a prime ideal that belongs to every nonempty open subset of $\mathrm{Spec}(R)$.

Let $\varphi : A \to B$ be a ring homomorphism. There is an induced map $\mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ by $\mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$ on the prime spectra that is continuous since $\mathrm{Spec}(\varphi)^{-1}(V(I)) = V((\varphi(I)))$.

Proposition 2.2. *The fiber* $\mathrm{Spec}(\varphi)^{-1}(\mathfrak{p})$ *of* $\mathrm{Spec}(\varphi)$ *over* $\mathfrak{p} \in \mathrm{Spec}(A)$ *is* $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p}))$.

Proof. Define $\psi : B \to B \otimes_A \kappa(\mathfrak{p})$ by $b \mapsto b \otimes 1$. Then since $\kappa(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = (A/\mathfrak{p}) \otimes_A A_\mathfrak{p}$, we have

$$B \otimes_A \kappa(\mathfrak{p}) = B \otimes_A (A/\mathfrak{p}) \otimes_A A_\mathfrak{p} = (B/\mathfrak{p}B) \otimes_A A_\mathfrak{p} = (B/\mathfrak{p}B)_{\mathfrak{p}B}.$$

Hence the image of $\mathrm{Spec}(\psi)$ consists of those $\mathfrak{q} \in \mathrm{Spec}(B)$ such that $\mathfrak{q} \supset \mathfrak{p}B$ and $\mathfrak{q} \subset \mathfrak{p}B$. Hence $\mathrm{Spec}(B \otimes_A \kappa(\mathfrak{p})) = \mathrm{Spec}(\psi) = \varphi(\mathfrak{p}) = \mathrm{Spec}(\varphi)^{-1}(\mathfrak{p})$. □

2.1 Linear maps and Nakayama's lemma

Theorem 2.3 (Nakayama's lemma)**.** *Let M be a finitely generate R-module. Let $\mathfrak{m}$ be an ideal of R contained in the Jacobson radical* $\mathrm{rad}(R)$*. If $\mathfrak{m}M = M$, then $M = 0$.*

Proof. Suppose M is generated by $\{a_1, \cdots, a_n\}$ where $n \geq 1$ is chosen to be minimal. Since $\mathfrak{m}M = M$, put $a_1 = \sum_{i=1}^n m_i a_i$ where $m_i \in \mathfrak{m}$, so that $(1 - m_1)a_1 = \sum_{i=2}^n m_i a_i$. But $(1 - m_1)$ is a unit, since $\mathfrak{m} \in \mathrm{rad}(R)$. Hence a_1 is a linear combination of $\{a_2, \cdots, a_n\}$, contradicting the minimality assumption. □

We give some applications of Nakayama's lemma.

Corollary 2.4. *Let M be a finitely generated R-module. If $\varphi : M \to M$ is a surjective R-linear map, then φ is bijective.*

Proof. d □

Corollary 2.5. *Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module. If $N \subset M$ is a submodule with $N + \mathfrak{m}M = M$, then $N = M$.*

Corollary 2.6. *Let $(R, \mathfrak{m})$ be a local ring. Let M be a finitely generated R-module. If $\{m_1, \cdots, m_n\}$ generates $M/\mathfrak{m}M$, then it generates M.*

Proof. d ☐

Remark. Cor. is not true if the finiteness condition is dropped. Indeed, if $R = \mathbf{Z}_{(2)}$ and $M = \mathbf{Q}$, then $M/(2)M = 0$.

Corollary 2.7. *If ring S is integral over ring A, then* $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ *is onto.*

3 Noetherian and Artinian rings

Simple module. An ideal I is maximal if and only if R/I is a simple R-module. All simple modules are of this form.

length
Artinian but not Noetherian https://planetmath.org/exampleofanartinianmodulewhichisnotnoetherian

Proposition 3.1. *Let A be a Noetherian domain with $K = \mathrm{Fr}(A)$. Let L/K be a finite separable extension and B the integral closure of A in L. Then B is a finitely generated A-module, and in particular, B is Noetherian.*

Proof. https://math.stackexchange.com/questions/50332/the-integral-closure-of-a-finite-separable-field-extension-of-the-fraction-field □

Noetherian ring can have infinite Krull dimension! Nagata

4 Associated Primes and Primary Decomposition

4.1 Associated Primes

Let R be a ring and M an R-module. A prime ideal $\mathfrak{p}$ of R is an **associated prime ideal** of M if $R/\mathfrak{p} \subset M$ is a submodule, or equivalently, if $\mathfrak{p}$ is the annihilator $\mathrm{Ann}_R(x)$ of some $x \in M$. Write $\mathrm{Ass}_R(M)$ for the set of associated primes of M. For $M = R$, associated primes are just prime ideals.

Proposition 4.1. *Let R be a Noetherian ring and $M \neq 0$ an R-module. Then*

(i) if $I \in \mathrm{Div}(M) = \{\mathrm{Ann}_R(x) : 0 \neq x \in M\}$ is maximal, then $I \in \mathrm{Ass}(M)$;

(ii) $\mathrm{Ass}(M)$ is nonempty;

(iii) the set of zero-divisors of M is the union of its associated primes

Proposition 4.2. *Let R be a ring and $S \subset R$ a multiplicative subset. Let M be an R-module and N an $R[S^{-1}]$-module. Then*

(i) there is a bijection between $\mathrm{Ass}_R(N)$ and $\mathrm{Ass}_{R[S^{-1}]}(N)$;

(ii) if R is Noetherian, then there is a bijection between $\mathrm{Ass}(M[S^{-1}])$ and $\mathrm{Ass}(M) \cap \mathrm{Spec}(A[S^{-1}])$.

Proposition 4.3. *Let R be a ring and $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ an exact sequence of R-modules. Then $\mathrm{Ass}(M') \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$.*

Proposition 4.4. *Let R be a Noetherian ring and $M \neq 0$ a finitely generated R-module. Then there exists a filtration $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ of R-submodules such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for $\mathfrak{p}_i \in \mathrm{Spec}(R)$ for each i.*

Proposition 4.5. *Let R be a Noetherian ring and M a finitely generated R-module. Then*

1. *$\mathrm{Ass}(M)$ is a finite set;*
2. *$\mathrm{Ass}(M) \subset \mathrm{Supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}(R) : M_\mathfrak{p} \neq 0\}$;*
3. *the set of minimal elements of $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ coincide.*

Minimal elements $\mathfrak{p}_i$ of $\mathrm{Ass}(M)$ are called **isolated primes** of M, and the remaining ones are called **embedded primes** of M. Geometrically, closed set $\mathrm{Supp}(M)$ is the union of irreducible components $V(\mathfrak{p}_i)$. For instance, consider the ring $R = k[x, y, z]$ where k is a field, with its prime ideals $\mathfrak{p} = (x, y)$, $\mathfrak{q} = (x, z)$, and $\mathfrak{m} = (x, y, z)$. For ideal $I = \mathfrak{p}\mathfrak{q} = \mathfrak{p} \cap \mathfrak{q} \cap \mathfrak{m}^2$, $\mathfrak{p}$ and $\mathfrak{q}$ are isolated primes of A/I (minimal prime ideals containing I), while $\mathfrak{m}^2$ is an embedded prime. Geometrically, $\mathfrak{p}$ and $\mathfrak{q}$ are isolated components z-axis and y-axis respectively, while $\mathfrak{m}^2$ is the first-order neighborhood at the origin, embedded inside $\mathfrak{p}$ and $\mathfrak{q}$. As we shall see, the existence of embedded primes prevents primary decomposition to be unique.

Proposition 4.6. *If R is a reduced ring, then R does not have embedded primes.*

4.2 Primary Decomposition

Let R be a ring and M an R-module. A submodule $N \subset M$ is **primary** if for any zero divisor $a \in R$ of M/N, $a \in \sqrt{\mathrm{Ann}(M/N)}$. Taking $M = R$, primary submodules are just primary ideals.

Proposition 4.7. *Let R be a Noetherian ring and M a finitely generated R-module. Then a submodule $N \subset M$ is primary if and only if $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$ with $\mathfrak{p} = \sqrt{\mathrm{Ann}(M/N)}$.*

Therefore, we say N is $\mathfrak{p}$-primary or M/N is $\mathfrak{p}$-coprimary if $\mathrm{Ass}(M/N) = \{\mathfrak{p}\}$.

Proposition 4.8. *If N and N' are $\mathfrak{p}$-primary submodules of M, then so is $N \cap N'$.*

Irreducible modules

Theorem 4.9. *Let R be a Noetherian ring and M a finitely generated R-module. Then*

(i) every proper submodule $N \subset M$ has a primary decomposition $N = N_1 \cap \cdots \cap N_r$;

(ii) if the decomposition is irredundant, then $\mathrm{Ass}(M) = \{\mathfrak{p}_1 \cdots, \mathfrak{p}_r\}$ where $\mathrm{Ass}(M/N_i) = \{\mathfrak{p}_i\}$;

(iii) if $\mathfrak{p}_i \in \mathrm{Ass}(M)$ is minimal, then the $\mathfrak{p}$-primary component $N_i = \ker(M \to M_{\mathfrak{p}_i})$.

Remark. Spec perspective

Non-uniqueness of embedded primes

4.3 Factorization

Let R be a ring. An element $a \in R$ is **irreducible** if $a = bc$ implies that either b or c is invertible. An element $a \in R$ is **prime** if the principal ideal (a) is a prime ideal. In general prime elements are irreducible, but the converse is false: in $R = \mathbf{Q} + x\mathbf{R}[x]$ the element x is irreducible but not prime, since $\sqrt{2}x \cdot \sqrt{2}x = 2x^2 \in (x)$ but $\sqrt{2}x \notin (x)$.

A domain R is a **Unique Factorization Domain** (UFD) if every element $a \in R$ can be factored into a product of prime elements that is unique up to multiplication by a unit.

Proposition 4.10. *If R is a UFD, then $R[x_1, \cdots, x_n]$ is a UFD.*

If R is a Noetherian ring, then every element can be factored into irreducible elements. But R does not always admit a prime factorization: in $k[X,Y]$ the ideal (X^2, Y^2) cannot be factored into primes. There is a primary decomposition, but it is not always unique: $(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^2)$. When does R admit a unique prime factorization?

Proposition 4.11. *Let R be a Noetherian domain. If $a \in R$ admits a prime factorization $a = u\prod_{i=1}^n p_i^{m_i}$ with $u \in R^\times$, then $\mathrm{Ass}(R/(a)) = \{(p_i) : 1 \le i \le n\}$ and m_i are the greatest integers for which $a \in (p_i^{m_i})$. Moreover, the factorization is unique, and $(a) = \bigcap_{i=1}^n (p_i^{m_i})$ is a minimal primary decomposition of (a).*

Proposition 4.12. *A Noetherian domain is a UFD if and only if every prime ideal which is minimal among those containing a principal ideal is principal.*

4.4 Symbolic powers

Symbolic powers can be used to prove the following important theorem.

Theorem 4.13 (Krull's principal ideal theorem)**.** *fff*

Another less tricky and more intrinsic proof is given in Corollary 8.3.

5 Discrete Valuation Rings and Dedekind Domains

5.1 Discrete Valuation Ring

For a field K, a **discrete valuation** on K is a surjective group homomorphism $v : K^\times \to \mathbf{Z}$ that satisfies $v(x+y) \geq \min\{v(x), v(y)\}$. An integral domain R is a **discrete valuation ring** if there exists a discrete valuation on $K = \mathrm{Fr}(R)$ and $R = \{x \in K : v(x) \geq 0\}$.

Ideals I of a discrete valuation ring R are of the form $I = \{x \in k : v(x) \geq n\}$ for some $n \geq 0$. It follows that R is local with maximal ideal $\mathfrak{m} = \{x \in K : v(x) > 0\}$. Every ideal is generated by a single element of minimal valuation, so R is a principal ideal domain and in particular R is Noetherian. The generator of $\mathfrak{m}$ is called the **uniformizer**, and it is unique up to units.

Common examples of discrete valuation rings include $\mathbf{Z}_{(p)}$ and $K[[X]]$ with K being a field. For $\mathbf{Z}_{(p)}$, the valuation v on $\mathbf{Q} = \mathrm{Fr}(\mathbf{Z}_{(p)})$ is given by $v(r) = k$ for $r = p^k(z/n)$ the unique factorization in $\mathbf{Q}$. The uniformizer is p. For $K[[X]]$, the valuation v on $\mathrm{Fr}(K[[X]]) = K((X))$ assigns each formal Laurent series to the degree of its first nonzero term. The uniformizer is X.

Proposition 5.1. *A Noetherian local domain with maximal ideal principal is a DVR.*

Proof. Let $(R, \mathfrak{m})$ be a Noetherian local domain with $\mathfrak{m} = (t)$. We will prove the decomposition $R \setminus \{0\} = \coprod_{n \geq 0} R^\times t^n$. Given this, the valuation $v(at^k) = k \in \mathbf{Z}$ on $K^\times = \mathrm{Fr}(R) = \coprod_{n \in \mathbf{Z}} R^\times t^n$ admits R as a discrete valuation ring.

Since R is Noetherian, by Krull's intersection theorem $\cap_{n \geq 0} \mathfrak{m}^n = 0$. It suffices to prove that $\mathfrak{m}^n \setminus \mathfrak{m}^{n+1} = A^\times t^n$ for any n, that is, any $x \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$ can be written *uniquely* as $x = ut^n$ for $u \in R^\times$. Since t^n generates $\mathfrak{m}^n$, $x = rt^n$ for $r \in R$, and uniquely so, since R is a domain. Since $x \notin \mathfrak{m}^{n+1}$, $r \notin \mathfrak{m}$. Since R is local, $r \in A^\times$. $\square$

A discrete valuation ring R is integrally closed, that is, there is no finitely generated R-algebra contained in $K = \mathrm{Fr}(R)$ but R itself. Indeed, if $A \neq R$ is a finitely generated R-algebra contained in K, then the valuation restricted to A is bounded from below; yet for $a \in A \setminus R$ with $v(a) < 0$, $v(a^n) = nv(a)$ is not bounded from below.

Proposition 5.2. *An integrally closed Noetherian domain with exactly two prime ideals is a DVR.*

Proof. Let $(R, \mathfrak{m})$ be an integrally closed local Noetherian domain such that there exists $a \in \mathfrak{m}$ such that $\mathfrak{m} \in \mathrm{Ass}(R/(a))$. We will show that R is a discrete valuation ring. By Proposition 5.1 it suffices to show that $\mathfrak{m}$ is principal.

Let $K = \mathrm{Fr}(R)$ and Let $A = \{x \in K : x\mathfrak{m} \subset R\}$ be an R-submodule of K containing R. We will show that $\mathfrak{m} \subsetneq \mathfrak{m}A$. Given this, since R is local, there exists $x \in A$ and $y \in \mathfrak{m}$ such that $xy \in R^\times$. Replacing x up to some unit, we may assume that $xy = 1$. Then for any $z \in \mathfrak{m}$, $z = z(xy) = (zx)y \in Ry$, which implies that $\mathfrak{m} = (y)$.

Assume for contradiction that $\mathfrak{m}A \subset \mathfrak{m}$. Since R is Noetherian, $\mathfrak{m}$ is finitely generated. Since $A \subset x^{-1}R$ for any $x \in \mathfrak{m}$, A is finitely generated over R. But since R is integrally closed, $A = R$. Since $\mathfrak{m} \in \mathrm{Ass}(R/(a))$, there exists $b \in R/(a)$ such that $\mathfrak{m}b \subset (a)$, which implies that $\mathfrak{m}(b/a) \subset R$. Then $b/a \in A \setminus R$, contradicting $A = R$. Hence $\mathfrak{m} \subsetneq \mathfrak{m}A$.

If R is an integrally closed Noetherian domain with exactly two prime ideals 0 and $\mathfrak{m}$, then R is local, and for any $a \in \mathfrak{m}$, since $R/(a) \neq 0$, $\mathrm{Ass}(R/(a)) \neq \emptyset$. Since $0 \notin \mathrm{Ass}(R/(a))$, the only possibility is that $\mathfrak{m} \in \mathrm{Ass}(R/(a))$. Hence by previous analysis R is a discrete valuation ring. $\square$

5.2 Complete Discrete Valuation Ring

Proposition 5.3. *A local Noetherian domain $(R, \mathfrak{m})$ is a DVR if and only if $\hat{R}_{\mathfrak{m}}$ is a DVR.*

A **complete** discrete valuation ring $(R, \mathfrak{m})$ is a discrete valuation ring that is complete with respect to $\mathfrak{m}$-adic topology.

Proposition 5.4. *Let $(R, \mathfrak{m}, k)$ be a complete DVR. Then for every prime element $p \in R$ there is an isomorphism $k[[t]] \to R$ of k-algebras given by $t \mapsto p$.*

Lemma 5.5. *Let $(R, \mathfrak{m})$ be a local ring and M a finitely generated R-module. Then there is a bijection between* $\mathrm{SpecMax}(M)$ *and prime ideals of $R/\mathfrak{m}B = B \otimes_A A/\mathfrak{m}$.*

Proof. We first show that every maximal ideal in B contains $\mathfrak{m}B$. Suppose $\mathfrak{n} \in \mathrm{SpecMax}(B)$ is otherwise. Then by Nakayama's lemma $\mathfrak{n} + \mathfrak{m}B =$ □

Theorem 5.6. *Let $(A, \mathfrak{m})$ be a complete DVR and $K = \mathrm{Fr}(A)$. Let L/K be a finite separable extension. Let B be the integral closure of A in L. Then B is a complete DVR.*

Proof. We will show that B is an integrally closed Noetherian domain with two prime ideals. By Proposition 3.4, B is Noetherian. Since $B \otimes_A K$ is a field, the fiber of $(0) \in \mathrm{Spec}(A)$ is $(0) \in \mathrm{Spec}(B)$, which implies that B is a domain. It remains to show that B is local, that is, $\overline{B} = B/\mathfrak{m}B$ has only one prime ideal. Since $\overline{B}$ is Artinian, being finite over a field $A/\mathfrak{m}$, it suffices to show that $\overline{B}$ is local. To do that, we show that $\overline{B}$ does not have proper idempotent.

Being a finitely generated module over an $\mathfrak{m}$-adically complete Noetherian ring A, B is also $\mathfrak{m}$-adically complete. Lifting idempotents, we get $\mathrm{Idem}(B) = \mathrm{Idem}(B/\mathfrak{m}B)$. Since $\overline{B}$ is a domain, it has no proper idempotents, so neither does $B/\mathfrak{m}B$. □

Remark. If R is not complete, then Theorem 5.5 fails to be true. Indeed, consider

$$\begin{array}{ccc} \mathbf{Z}_{(p)} & \text{———} & \mathbf{Q} \\ | & & | \\ \mathbf{Q}_{(p)} & \text{———} & \mathbf{Q}[i] \end{array} .$$

The integral closure $\mathbf{Q}_{(p)}$ of $\mathbf{Z}_{(p)}$ in $\mathbf{Q}[i]$ fails to be local, as (p) is not prime in $\mathbf{Q}$.

Proposition 5.7. *All finite extensions of the field of Laurent formal series $\mathbf{C}((X))$ are of the form $\mathbf{C}((X^{1/n}))$, the field of Puiseux series.*

Then there is a canonical isomorphism $A/\mathfrak{m}^n \to \hat{A}/\hat{\mathfrak{m}}^n$. Indeed, since $\mathfrak{m}^n = A \cap \hat{\mathfrak{m}}^n$, it is an injection; since A is dense in $\hat{A}$ and $\hat{\mathfrak{m}}^n$ is an open set in the $\mathfrak{m}$-adic topology, $(x + \hat{\mathfrak{m}}^n) \cap A \neq \emptyset$ for any $x \in A$, and thus it is a surjection.

Lemma 5.8. *Let R be a DVR and A a complete R-algebra. If e is an idempotent element in $A/\pi A$, (π being the uniformizer of R) then there exists idempotent elements E in A such that $e = E + \pi A$.*

Proof. Idempotent lifting lemma. Completion preserves Noetherian, completion of a pid is a domain. We show that B is local. Then since it is a Dedekind ring, it is a DVR (all nonzero primes are maximal, but only one maximal ideal, so only two ideals)

Suppose B has A-basis $x_1, \cdots, x_m$. Let $\{a_n\}$ be a Cauchy sequence in B, with $a_n = a_{n,1}x_1 + \cdots + a_{n,m}x_m$ with $a_{n,i} \in A$. Then since $\lim_{n\to\infty}\{a_{n,i}\}$ exists in A for each i, $\{a_n\}$ has a limit in B, proving that B is complete.

Let $\mathfrak{m}$ be the maximal ideal of of A. Then $\mathfrak{m}B$ has factorization $\mathfrak{p}_1^{k_1} \cdots p_g^{k_g}$. By Chinese Remainder Theorem $B/\mathfrak{m}B \cong B/\mathfrak{p}_1^{k_1} \oplus \cdots \oplus B/\mathfrak{p}_g^{k_g}$. If $g > 1$ then there is a nontrivial idempotent element $e = (1, 0, \cdots, 0)$ in $B/\mathfrak{p}_1^{k_1}$ that lifts to an idempotent E in B. But B is a domain, so E has to be trivial, rendering $e = E + \mathfrak{p}_1^{k_1} = \mathfrak{p}_1^{k_1}$, which is absurd. Hence $g = 1$, that is, B has only one maximal ideal. Now completion of a Noetherian PID is a Noetherian domain, so B is a Dedekind ring. All nonzero primes of a Dedekind ring are maximal, but here since B is local, it has only one nonzero prime ideal. Hence B is a DVR. □

5.3 Dedekind Domain

A Noetherian domain R is a **Dedekind domain** if $R_{\mathfrak{p}}$ is a DVR for every prime ideal $\mathfrak{p}$ of R. It follows that every nonzero prime ideal of R is maximal. Indeed if $0 \subset \mathfrak{q} \subset \mathfrak{q}$, then then $R_{\mathfrak{p}}$ has three prime ideals.

6 Integrality

Proposition 6.1. *Let R be a ring and I an ideal of $R[x]$. The $M = R[x]/I$ is finitely generated as R-module if and only if I contains a monic polynomial. If I is generated by a monic polynomial of degree d, then M is free of rank d.*

Proposition 6.2. *integral extension iff finitely generated module*

6.1 Cohen-Seidenberg Theory

Cohen-Seidenberg theory, or going-up and going-down theorems, informs the correspondence of prime ideals between integral extension of domains.

Theorem 6.3. *Let $\varphi : A \to B$ be a ring homomorphism between integral domains A and B where B is a finitely generated A-module. Then*

(i) the induced map $\mathrm{Spec}(\varphi) : \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective with finite fibers;

(ii) if I is an ideal of B such that $I \cap A = 0$, then $I = 0$;

(iii) $L = \mathrm{Fr}(B)$ is a finite extension of $K = \mathrm{Fr}(A)$.

Proof. (i) A prime $\mathfrak{p} \in \mathrm{Spec}(A)$ is in the image of $\mathrm{Spec}(\varphi)$ if and only if it is in the support $\mathrm{Supp}(B)$ of B, which is a closed subset of $\mathrm{Spec}(A)$. Since A and B are integral domains, their zero ideals are prime, and the zero ideal of A is the image of the zero ideal of B. The Zariski closure of the zero ideal in $\mathrm{Spec}(A)$ is the whole $\mathrm{Spec}(A)$. Hence $\mathrm{Spec}(\varphi)$ is surjective.

d

□

Theorem 6.4 (Going-up)**.** *Let $A \to B$ be an integral extension of rings. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2$ be prime ideals of A. If $\mathfrak{q}_1 \in \mathrm{Spec}(B)$ lies over $\mathfrak{p}_1$, then there exists $\mathfrak{q}_2 \in \mathrm{Spec}(B)$ lying over $\mathfrak{p}_2$.*

Theorem 6.5 (Going-down)**.** *Let $A \to B$ be an integral extension of domains. Let $\mathfrak{p}_1 \subset \mathfrak{p}_2$ be prime ideals of A. If $\mathfrak{q}_2 \in \mathrm{Spec}(B)$ lies over $\mathfrak{p}_2$, then there exists $\mathfrak{q}_1 \in \mathrm{Spec}(B)$ lying over $\mathfrak{p}_1$.*

6.2 Jacobson Rings and Hilbert's Nullstellensatz

Hilbert's Nullstellensatz states that for an algebraically closed field k, if I is and ideal of $R = k[x_1, \cdots, x_n]$ and $f \in R$ vanishes on the common set of zeros of polynomials of I, then $f \in \sqrt{I}$. It can be proven ....

Proof. We first state and prove the *weak Nullstellensatz*:

> A family of polynomials of A with no common zeros generates the unit ideal of A.

Proof of the weak Nullstellensatz: Let $\mathfrak{m}$ be a maximal ideal of A. Then there is a natural map $\varphi : A \to A/\mathfrak{m} \cong k$ by $x_i \mapsto a_i$. Evidently $\mathfrak{n} = (x_1 - a_1, \cdots, x_n - a_n) \subset \ker \varphi = \mathfrak{m}$, so there is a surjective map $\tilde{\varphi} : A/\mathfrak{n} \to k$. Let $\tilde{\psi} : A \to A/\mathfrak{n}$ be the natural map, then $\tilde{\psi}(x_i) = \tilde{\psi}(a_i)$. Hence $\tilde{\psi}(f(x_1, \cdots, x_n)) = \tilde{\psi}(f(a_1, \cdots, a_n))$, so elements of $A/\mathfrak{a}$ are of the form $\tilde{\psi}(n)$ for $a \in k$. But $\tilde{\varphi}(\tilde{\psi}(a)) = \varphi(a) = a$, so in particular $\tilde{\varphi}(\tilde{\psi}(r)) = 0$ if and only if $r = 0$. Hence $\ker \tilde{\varphi}$ consists of only $\tilde{\psi}(0) = 0$, implying that $\tilde{\varphi}$ is injective. Hence $\mathfrak{m} = \mathfrak{n}$, that is, every maximal ideal of A is of the form $(x_1 - a_1, \cdots, x_n - a_n)$. Now if a family of polynomials of A lies in some maximal ideal $(x_1 - a_1, \cdots, x_n - a_n)$, then $(a_1, \cdots, a_n)$ is a common zero. Hence a family of polynomials with no common zeros doesn't lie in any maximal ideal, and thus generates the unit ideal of A.

We use the *Rabinowitsch trick* to prove Hilbert's Nullstellensatz. Since $A = k[x_1, \cdots, x_n]$ is Noetherian, let $\mathfrak{a} = (f_1, \cdots, f_m)$. If $f \in A$ vanishes on $Z(\mathfrak{a})$, then $f_1, \cdots, f_m, x_0 f + 1$ doe snot have common zeros in $A[x_0]$. By the weak Nullstellensatz, there exists $g_0, \cdots, g_m \in A[x_0]$ such that

$$1 = g_0 \cdot (x_0 f + 1) + g_1 f_1 + \cdots + g_m f_m$$

as elements in $A[x_0]$. Now substitute $x_0 = 1/f$ to get

$$1 = g_1(1/f, x_1, \cdots, x_m) f_1 + \cdots + g_m(1/f, x_1, \cdots, x_m) f_m$$

as elements in $\mathrm{Fr}(A)$. Multiply both sides by some power of f, we get $f^r = h_1 f_1 + \cdots + h_m f_m$ for $h_m \in A$. Hence $f \in \mathfrak{a}$. □

Somewhat deeper, Hilbert's Nullstellensatz is a consequence of the structure of Jacobson rings. This way k need to be a field.

A ring R is a **Jacobson ring** if every prime ideal $\mathfrak{p}$ of R is the intersection of maximal ideals containing $\mathfrak{p}$.

Lemma 6.6. *A ring R is a Jacobson ring if and only if the map $\mathrm{Spec}(R[s^{-1}]) \to \mathrm{Spec}(R)$ sends maximal ideals to maximal ideals for any $s \in R$.*

Proof. d □

Lemma 6.7. *Let A be a domain. If $K = \mathrm{Fr}(A)$ is a finitely generated A-module, then $A = k$.*

Proof. If there exists $x \in A$ with $1/x \in K - A$. Since K is a finitely generated A-module □

Theorem 6.8. *If R is a Jacobson ring and S a finitely generated R-algebra, then S is a Jacobson ring. Moreover, if $\mathfrak{q}$ is a maximal ideal of S, then $\mathfrak{q} \cap R$ is a maximal ideal of R, and $S/\mathfrak{q}$ is a finite extension of $R/\mathfrak{p}$.*

Proof. If $S = R[x_1, \cdots, x_n]/I$ satisfies the theorem, then so do all its quotient rings. Hence by induction it suffices to assume that $S = R[x_1, \cdots, x_n]$. Similarly, it also suffices to assume that $S = R[x]$. Assuming that S is a Jacobson ring, we first proof that the map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ sends maximal ideals to maximal ideals and induces finite extensions of corresponding residue fields.

Let $\mathfrak{q}$ be a maximal ideal of $R[x]$ and $\mathfrak{p} = \mathfrak{q} \cap R$. By taking $R/\mathfrak{p}$ instead of R, we may assume that R is a Jacobson domain and $\mathfrak{p} = 0$. It suffices to show that R is a field, so that $\mathfrak{p}$ is maximal. Since $R[x]$ is not a field, $\mathfrak{q}$ is nonzero. Let $f = a_n x^n + \cdots + a_0 \in R[x]$ be nonzero with $a_n \in R \setminus \{0\}$. Since $\mathfrak{q} \cap R = 0$ in R, $a_n \notin \mathfrak{q}$. Inverting a_n and setting $R' = R[a_n^{-1}]$, f is monic in $R'[x]$. Hence $R'[x]/(f)$ is a finitely generated R'-module. Since $a_n \notin \mathfrak{q}$, $\mathfrak{q}[a_n^{-1}]$ is a maximal ideal of $R'[x]$. Since $R'[x]/q[a_n^{-1}]$ is a quotient of $R'[x]/(f)$, the former, which is a field, is also a finitely generated R'-module. Hence R' is a field. Since R is a Jacobson ring, the image of maximal ideal 0 in R, which is 0, is maximal. Hence R is a field. Since $R = R'$, $R[x]/\mathfrak{q}$ is a finite field extension of R.

Now we proof that $S = R[x]$ is a Jacobson ring. □

Remark. Let k be algebraically closed and $R = k[x_1, \cdots, x_n]/I$ where I is an ideal. Since $k[x_1, \cdots, x_n]$ is Noetherian, I is generated by finitely many polynomials $p_1, \cdots, p_m$. Let $\mathfrak{m}$ be a maximal ideal of R. Consider the map $\varphi : R \to R/\mathfrak{m} = k$ by $x_i \mapsto \alpha_i$. If $\alpha = (\alpha_1, \cdots, \alpha_n) \in k$ is the common zero for all p_i, then $\alpha \in \mathfrak{m}$. Hence $\mathfrak{m}$ consists of the common zeros of polynomials that generate I.

If k is not algebraically closed, then apply Nullstellensatz to $R \otimes_k \overline{k}$. Maximal ideals of R are $\mathrm{Gal}(\overline{k}/k)$-orbits of common zeros of polynomials generating I. Then $R/\mathfrak{m}$ is a finite separable extension of k if and only if $\deg_k(R/\mathfrak{m})$ is the number of points in the corresponding orbit of $\mathfrak{m}$.

6.3 Noether Normalization

Now let's restrict the base ring R to be a field k. We have the following result.

Theorem 6.9 (Noether normalization lemma)**.** *If R is a finitely generated k-algebra, then there exists algebraically independent elements $x_1, \cdots, x_d \in R$ such that R is a finitely generated module over $S = k[x_1, \cdots, x_n] \subset R$.*

7 Completion

7.1 Idempotent Lifting

Let R be a ring. An element $e \in R$ is an **idempotent** if it satisfies $e(1-e) = 0$. Write $\mathrm{Idem}(R)$ for the set of idempotents of R.

Proposition 7.1. *Let R be a ring with nilpotent ideal I. For every idempotent $\bar{e} \in \mathrm{Idem}(R/I)$, there exists a lift $e \in \mathrm{Idem}(R)$.*

Proposition 7.2. *Let R be a ring. There is a bijection between $\mathrm{Idem}(R)$ and subsets of $\mathrm{Spec}(R)$ that are open and closed given by $e \mapsto V(e)$.*

Corollary 7.3. *Let R be a ring with nilpotent ideal I. Then $\mathrm{Idem}(R) \to \mathrm{Idem}(R/I)$ is bijective.*

Lemma 7.4. *Let R be a ring with nilpotent ideal I. Then $a \in R^\times$ if and only if $\bar{a} \in (R/I)^\times$, where $\bar{a}$ is the image of a in R/I.*

Proposition 7.5. *If $R = \hat{R}_I$, then $\mathrm{Idem}(R/I) = \mathrm{Idem}(R)$.*

Proof. We will show that $\mathrm{Idem}(R/I) = \mathrm{Idem}(R/I^2) = \cdots$. Since $R/I^{n+1} = (R/I^n)/(I^n/I^{n+1})$, by idempotent lifting lemma it suffices to show that I^n/I^{n+1} nilpotent. Indeed, any $a + I^{n+1}$ is a finite sum of $n+1$ elements from I, so that $a^2 \in I^n$. □

Theorem 7.6 (Hensel's lemma)**.** *Let R be a Noetherian ring with ideal I. A solution $a \in R/I$ of the equation $f(X) \in R[X]$ satisfying $f'(a) \in (R/I)^\times$ lifts uniquely to a solution of $f(X)$ in $\hat{R}_I$.*

Proof. Cring □

7.2 Exactness

While Localization is exact, completion is *not* exact in general. For instance, consider $R = k[t]$, $M' = M = \oplus_{n \in \mathbf{N}} R$, and $M'' = \oplus_{n\in\mathbf{N}} R/(t^n)$. The map $M' \to M$ is given by multiplication by t^n on the n-th summand. Then the short exact sequence

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

is no longer exact at $M^\wedge$ after completion with respect to (t). Indeed, $\xi = (t^2, t^3, \cdots)$ is in the kernel of $M^\wedge \to (M'')^\wedge$, yet ξ is not in the image of $(M')^\wedge \to M^\wedge$, for it would be the image of $(t, t, \cdots) \notin (M')^\wedge$.

However, completion is naturally right-exact, and with the extra Noetherian condition it is also left-exact. (?)

Lemma 7.7. *Let R be a ring with ideal I. Then $\hat{I}_I \subset \mathrm{rad}(\hat{R}_I)$.*

Proof. As $\hat{I}_I = \varprojlim_n I/I^n$ and $\hat{R}_I = \varprojlim_n R/I^n$, it suffices to check that $1 + I/I^n \subset (R/I^n)^\times$ for each n. Indeed, for $a \in I$, there exists $(1 - a + a^2 - \cdots \pm a^{n-1}$ □

Theorem 7.8. *Let R be a Noetherian ring with with ideal I. Let M be a finitely generated R-module with submodule N. We have a short exact sequence of $\hat{R}$-modules*

$$0 \longrightarrow \hat{N}_I \longrightarrow \hat{M}_I \longrightarrow (\hat{M/N})_I \longrightarrow 0.$$

Proof. Let $M/N = P$. For right-exactness, we show that $\hat{M} \to \hat{P}$ is surjective. Since M and P are finitely generated and $\hat{I} \in \mathrm{rad}(R)$, by a consequence of Nakayama's lemma of lifting generators, it suffices to show that $\hat{M}/\hat{I}\hat{M} \to \hat{P}/\hat{I}\hat{P}$ is surjective. Observe that $\hat{P}/\hat{I}\hat{P} = ()/I()$. Hence everything follows from the surjectivity of $M \to P$.

For left-exactness, we show that $\hat{N} \to \hat{M}$ as a consequence of the Artin-Rees lemma. □

8 Hilbert-Samuel function

8.1 Dimension

Let R be a ring. The (Krull) **dimension** $\dim(R)$ of R is the supremum of r for which there is a strict descending chain $\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_r$ of prime ideals of R. This notion of dimension is rather abstract. We associate two numerical invariants of R equal to $\dim(R)$ when R is a semilocal Noetherian ring. One is better for computation while the other has good geometric intuition.

Let $(R, \mathfrak{m})$ be a semilocal Noetherian ring and M a finitely generated R-module.

(i) Let $\delta(M)$ be the smallest number r for which there exists $x_1, \cdots, x_r \in \mathfrak{m}$ generating an ideal I of R satisfying $\ell(M/IM) < \infty$. Geometrically this is the smallest number of equation needed so that the intersection M/IM is of dimension zero.

(ii) Let $d(M) = \deg \sigma_M^I(n)$ be the degree of the Samuel function of M with I a definition ideal when n is large. This value does not depend of the choice of I. Note that the Samuel function of a module can be explicitly calculated.

Lemma 8.1. *Let R be a semilocal Noetherian ring. Let*

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

be a short exact sequence of finitely generated R-modules. Then $d(M) = \max\{d(M'), d(M'')\}$.

Theorem 8.2 (fundamental theorem of dimension theory)**.** *Let R be a semilocal Noetherian ring and M a finitely generated R-module. Then $\dim(R) = d(M) = \delta(M)$.*

Proof. We prove $d(M) \geq \dim(M)$, $\delta(M) \geq d(M)$, and $\dim(M) \geq \delta(M)$ consecutively.

For $d(M) \geq \dim(M)$. Suppose $M = A$, we proceed by induction on $d(R)$. Let $\mathfrak{m} = \mathrm{rad}(R)$. If $d(R) = 0$, then $\sigma_R(n) = l(R/\mathfrak{m}^n)$ is constant for large n, in which case $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. By Nakayama's lemma $\mathfrak{m}^n = 0$, which implies that $\mathfrak{m} \subset \mathrm{nil}(R)$, so that any prime ideal of R is maximal. It follows that $\dim(R) = 0$. Now let $d(R) > 0$. If $\dim(R) = 0$ then we are done; so suppose $\dim(R) > 0$. Let $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k$ be a chain of prime ideals of R. Choosing $x \in \mathfrak{p}_1 \setminus \mathfrak{p}_0$, we obtain a short exact sequence

$$0 \longrightarrow R/\mathfrak{p}_0 \xrightarrow{x} R/\mathfrak{p}_0 \longrightarrow S = R/(\mathfrak{p}_0 + xR) \longrightarrow 0,$$

from which $d(S) < d(R)$ by Lemma 8.11. By inductive hypothesis $\dim(S) \leq d(S) \leq d(R) - 1$. Since $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_k$ provides a chain of prime ideals of S, $k - 1 \leq \dim(S)$. Hence $k \leq d(R)$. Since this holds for any chain of prime ideals of R, $\dim(R) \leq d(R)$.

Now for general M, by Proposition 4.9 there is a chain $0 = M_0 \subset M_1 \subset \cdots \subset M_q = M$ of submodules of M such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for $\mathfrak{p}_i \in \mathrm{Spec}(R)$ for all i. From the short exact sequence of the form

$$0 \longrightarrow M_{i-1} \longrightarrow M_i \longrightarrow M/M_{i-1} \longrightarrow 0,$$

we have $d(M) = \max_i d(R/\mathfrak{p}_i)$ and $\mathrm{Supp}(M) = \bigcup_i \mathrm{Supp}(R/\mathfrak{p}_i)$. But

$$\dim(M) = \sup\{\mathrm{coht}(\mathfrak{p}) : \mathfrak{p} \in \mathrm{Supp}(M) = \mathrm{Supp}(R/\mathfrak{p}_i)\} = \max_i \dim(R/\mathfrak{p}_i).$$

It follows that $\dim(M) \leq d(M)$.

For $\delta(M) \geq d(M)$. If $\delta(M) = 0$, then $l(M) < \infty$, that is, $\sigma_M(n) < \infty$ for any n. Hence $d(M) = 0$. Now let $\delta(M) = s > 0$. Choose $x_1, \cdots, x_s \in \mathfrak{m}$ such that $l(M/(x_1, \cdots, x_s)M) < \infty$. Let $M_i = M/(x_1, \cdots, x_i)M$, so that $\delta(M_i) = \delta(M) - i$. Then

$$\begin{aligned} l(M_1/\mathfrak{m}^n M_1) &= l(M/(x_1 M + \mathfrak{m}^n M)) \\ &= l(M/\mathfrak{m}^n M) - l(x_1 M/(x_1 M \cap \mathfrak{m}^n M)) \\ &= l(M/\mathfrak{m}^n M) - l(M/(\mathfrak{m}^n M : x_1)) \geq l(M/\mathfrak{m}^n M) - l(M/\mathfrak{m}^{n-1} M). \end{aligned}$$

The second equality comes from a short exact sequence; the third equality can be checked manually: the map $M \to x_1 M/(x_1 M \cap \mathfrak{m}^n M)$ by $x \mapsto x_1 x + (x_1 M \cap \mathfrak{m}^n M)$ has kernel $(\mathfrak{m}^n M : x_1)$; the last inequality comes from $\mathfrak{m}^{n-1} M \subset (\mathfrak{m}^n M : x_1)$. Hence $\sigma_{M_1}(n) \geq \sigma_M(n) - \sigma_M(n-1)$. When n is large, both $\sigma_M(n)$ and $\sigma_M(n-1)$ has same degree $d(M)$, so $d(M_1) \geq d(M) - 1$. Repeating this, we have $d(M_s) \geq d(M) - s$. But $\delta(M_s) = 0$, so $d(M_s) = 0$, which implies that $s \geq d(M)$.

For $\dim(M) \geq \delta(M)$. By similar argument, it suffices to assume $M = A$. For $\dim(R) = d$, it suffices to find $x_1, \cdots, x_d \in \mathfrak{m}$ such that $l(R/(x_1, \cdots, x_d)) < \infty$. Proceed by induction. If $d = 0$, then R is Artinian and $l(R) < \infty$. Suppose $d > 0$. Let $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_r\}$ be the set of minimal prime ideals of R with $\dim(R/\mathfrak{p}_i) = d$ for all i, which is finite since R is Noetherian. Since $\mathfrak{m} \not\subset \mathfrak{p}_i$, there exists $x \in \mathfrak{m} \setminus \bigcup_i \mathfrak{p}_i$ by prime avoidance, and $\dim(\overline{R}) = \dim(R/(x)) \leq d - 1$. By inductive hypothesis, there exists $\overline{x}_1, \cdots, \overline{x}_{d-1} \in \mathfrak{m}$ such that $l(\overline{R}/(x_1, \cdots, x_{d-1})) < \infty$. But $R/(x_1, \cdots, x_{d-1}, x)$ is equal to $\overline{R}/(\overline{x}_1, \cdots, \overline{x}_{d-1})$, where $x_i \in R$ has image $\overline{x}_i$ in $\overline{R}$. Hence $x_1, \cdots, x_{d-1}, x \in \mathfrak{m}$ is the system we are looking for. □

In the case of R a Noetherian local ring with maximal ideal $\mathfrak{m}$, $l(R/I) < \infty$ implies that R/I is Artinian. Hence I is $\mathfrak{m}$-primary. We say that $\{a_1, \cdots, a_n \in R\}$ is a **system of parameters** of R if it generates an $\mathfrak{m}$-primary ideal. If M is a finitely generated R-module with $\dim M = n$, then $\{x_1, \cdots, x_n \in M\}$ is a **system of parameters** of M if $(M/(x_1, \cdots, x_n)M) < \infty$.

Corollary 8.3 (Krull's principal ideal theorem)**.** *Let R be a Noetherian ring and $I = (a_1, \cdots, a_n)$ an ideal of R. If $\mathfrak{p} \in \operatorname{Spec}(R/I)$ is minimal, then $\operatorname{ht}(\mathfrak{p}) \leq n$. In particular, if I is a principal ideal, then $\operatorname{ht}(\mathfrak{p}) \leq 1$.*

Proof. In the local ring $R_\mathfrak{p}$ ideal I is $\mathfrak{p}$-primary, so that $\delta(A_\mathfrak{p}) \leq n$. By the fundamental theorem, $\operatorname{ht}(\mathfrak{p}) = \dim(A_\mathfrak{p}) = \delta(A_\mathfrak{p})$. □

In particular, we know that the height of a proper ideal of a Noetherian ring is finite.

Proposition 8.4. *Let R be a Noetherian ring. Let $\mathfrak{p} \in \operatorname{Spec}(R)$ and $\operatorname{ht}(\mathfrak{p}) = n$. Then $\mathfrak{p}$ is minimal among $\operatorname{Spec}(R/I)$ for some ideal $I = (a_1, \cdots, a_n)$. For any $b \in \mathfrak{p}$, we have $\operatorname{ht}(\mathfrak{p}/(b)) \geq n - 1$; but if b is among $\{a_1, \cdots, a_n\}$, then $\operatorname{ht}(\mathfrak{p}/(b)) = n - 1$.*

Geometrically, modding out an element of $\mathfrak{p}$ decreases the height of $\mathfrak{p}$ by at most 1; if this element is a "building block", then the reduction is exactly 1.

9 Regular Rings

9.1 Regular Local Rings

Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$. The minimum number of elements of $\mathfrak{m}$ generating an $\mathfrak{m}$-primary ideal is $\delta(R) = \dim(R)$. Let $k = A/\mathfrak{m}$ be the residue filed. The minimum number of elements of $\mathfrak{m}$ generating $\mathfrak{m}$ is called the **embedding dimension** of R, written as $\operatorname{emb}\dim(R) = \operatorname{rank}_k(\mathfrak{m}/\mathfrak{m}^2) \geq \delta(R) = \dim(R)$. The ring R is a **regular local ring** of dimension d if $d = \operatorname{emb}\dim(R) = \dim(R)$.

Translating proposition 8.14, we have the following important observation.

Proposition 9.1. *If R is a regular local ring with $\{x_1, \cdots, x_n\}$ a regular system of generators, then $R/(x_1, \cdots, x_r)$ is a regular local ring of dimension $n - r$.*

Proposition 9.2. *A regular local ring is an integral domain.*

The following are two characterizations of regular local rings.

Proposition 9.3. *Let $(R, \mathfrak{m}, k)$ be a local Noetherian ring with $\operatorname{emb}\dim(R) = n$. Then R is a regular local ring if and only if $\operatorname{gr}_{\mathfrak{m}}(R) \cong k[x_1, \cdots, x_n]$ if and only if $\hat{R}_{\mathfrak{m}} \cong k[[x_1, \cdots, x_n]]$.*

9.2 Serre's homological characterization

Let R be a ring. Define its **global dimension** $\operatorname{gl}\dim(R)$ to be the supremum of $\operatorname{proj}\dim(M)$ for all R-modules M.

Theorem 9.4 (Serre)**.** *Let R be a Noetherian local ring. Then R is a regular local ring if and only if $\operatorname{gl}\dim(R) < \infty$, in which case $\operatorname{gl}\dim(R) = \dim(R)$.*

10 Connections to Differential Geometry

11 Appendix: Some Homological Algebra

Abelian cat...

11.1 Ext and Tor

Complex. Double complex (equivalence) injective/projective module and resolution
Hom and Ext Tensor and Tor
An element $x \in R$ is M**-regular** if there does not exists any $a \in M$ such that $ax = 0$.

Regular element calculation

The following lemma allows induction by dimension reduction.

Lemma 11.1 (Slicing lemma)**.** *Let R be a ring and M an R-module. Let $x \in R$ be both R-regular and M-regular. Let N be an R-module annihilated by x. Let $\overline{R} = R/xR$ and $\overline{M} = M/xM$. Then $\mathrm{Ext}^i_R(M, N) = \mathrm{Ext}^i_{\overline{R}}(\overline{M}, N)$ and $\mathrm{Tor}^R_i(M, N) = \mathrm{Tor}^{\overline{R}}_i(\overline{M}, N)$*

Proof. □

11.2 Flatness

7. (1) Yes, it's possible. Choose $f(t) = e^t$ to be the driving function. Then since $x' + x = 0$ has solution $x = Ce^{-t}$ all decaying to 0, by variation of constants we find that the solution for $y' + y = f(t)$ has solution $y(t) = e^{-t}(C + \int_0^t e^{2s} ds) = Ce^{-t} + e^t/2$ which blows up as $t \to \infty$. The initial condition does not influence the blowing-up phenomena.

(2) Conclusion: we can make all solutions bounded, but we cannot make them all to grow unbounded. As $f(t) = p(t)e^{\lambda t}$ is given, we choose a_i so that all roots of the characteristic polynomial $p(\lambda)$ satisfies $\mathrm{Re}(\lambda_i) < 0$. Notice that since $f(t)$ is bounded, $\mathrm{Re}(\lambda) \le 0$. So all solutions of of the forced ODE will be of the form $x(t) = q(t)e^{\lambda t} + p_i(t)e^{\lambda_i t}$ where p_i and q are polynomials. Since λ and $\mathrm{Re}(\lambda_i) < 0$ and $\mathrm{Re}(\lambda) \le 0$, all such $x(t)$ will be bounded.

On the other hand, there always exists a particular solution given by $q(t)e^{\lambda t}$, which does not grow unbounded.

8. (1) The ODE is $x' + ax = g(t)$ with $\lim_{t\to\infty} g(t) = b$, we need to show that all solutions satisfy $\lim_{t\to\infty} x(t) = b/a$.